Deep Security 20 ガイド

オンプレミスインストール

複数年契約について

お客さまが複数年契約(複数年分のサポート費用前払い)された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。

複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。

各製品のサポート提供期間は以下のWebサイトからご確認いただけます。
https://success.trendmicro.com/dcx/s/solution/000207383?language=ja

法人向け製品のサポートについて

・法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。

・法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

著作権について

本ドキュメントに関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本ドキュメントまたはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本ドキュメントの記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本ドキュメントおよびその記述内容は予告なしに変更される場合があります。

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、

Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDIオプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！ スマホお探しサポート、保険&デジタルライフサポート、おまかせ！ 迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポートプレミアム、Airサポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック! 、Trend Micro Security Master、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro Network One、らくらくサポート、Service One、超早得、先得、Trend Micro One、Workforce One、Security Go、Dock 365、TrendConnect、TREND MICRO FORUM、トレンドマイクロ知恵袋、Trend Cloud One、Trend Service One、およびAccelerating Youは、トレンドマイクロ株式会社の登録商標です。

本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

© 2026 Trend Micro Incorporated.All rights reserved

個人情報保護方針

トレンドマイクロは、次のWebサイトに規定されたトレンドマイクロのプライバシーポリシーに従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

最終更新日: 2026年1月

目次

目次 4

Trend Micro Deep Securityについて 116

Deep Security 20リリース戦略およびライフサイクルポリシー 116

サポートされるアップグレードパス 116

Deep Security 20のアップデートスケジュール 117

LTSリリースのサポート期間とアップグレードのベストプラクティス 117

サポートサービス 119

Agentプラットフォームサポートポリシー 120

Deep Security ライフサイクルの日付 121

Deep Security LTS ライフサイクル日付 121

Deep Security LTSリリースライフサイクル日付 121

Deep Security Virtual Applianceのリリースライフサイクルの日付 123

サポート拡張機能 123

過去のサポート拡張のアーカイブ 127

Deep Security FRライフサイクルの日付 128

Deep Security FRリリースライフサイクルの日付 128

サポート拡張機能 130

Deep Securityコンポーネントについて 130

Deep Security保護モジュールについて 131

侵入防御 132

不正プログラム対策 132

ファイアウォール 132

Webレピュテーション 132

変更監視 133

セキュリティログ監視 133

アプリケーションコントロール 133

デバイスコントロール 133
このリリースについて 134
新機能 134
Deep Security Managerの新機能 134
Deep Security Manager - 20.0.1123 (20 LTS 更新 2025-12-09) 134
新機能 134
機能強化 134
解決された問題 135
Deep Security Manager - 20.0.1112 (20 LTS 更新 2025-11-12) 135
新機能 135
機能強化 135
Deep Security Manager - 20.0.1092 (20 LTS 更新 2025-10-08) 135
新機能 135
解決された問題 136
Deep Security Manager - 20.0.1081 (20 LTS 更新 2025-09-15) 136
新機能 136
機能強化 136
解決された問題 136
Deep Security Manager - 20.0.1073 (20 LTS 更新 2025-08-20) 136
セキュリティ更新 137
Deep Security Manager - 20.0.1059 (20 LTS 更新 2025-07-09) 137
強化 137
解決された問題 137
Deep Security Manager - 20.0.1054 (20 LTS 更新 2025-06-11) 137
セキュリティ更新 137
Deep Security Manager - 20.0.1047 (20 LTS 更新 2025-05-12) 138
機能強化 138
Deep Security Manager - 20.0.1039 (20 LTS 更新 2025-04-16) 138
新機能 138

解決された問題 138
セキュリティ更新 139
Deep Security Manager - 20.0.1027 (20 LTS 更新 2025-03-12) 139
機能強化 139
解決済みの問題 139
セキュリティ更新 139
Deep Security Manager - 20.0.1017 (20 LTS 更新 2025-01-15) 139
新機能 140
機能強化 140
セキュリティアップデート 140
Deep Security Manager - 20.0.1003 (20 LTS 更新 2024-12-10) 140
機能強化 141
セキュリティ更新 141
Deep Security Manager - 20.0.993 (20 LTS 更新 2024-11-13) 141
新機能 141
機能強化 141
セキュリティアップデート 142
Deep Security Manager - 20.0.979 (20 LTS 更新 2024-10-16) 142
新機能 142
機能強化 142
解決済みの問題 142
セキュリティ更新 142
Deep Security Manager - 20.0.967 (20 LTS 更新 2024-09-18) 143
機能強化 143
解決済みの問題 143
セキュリティ更新 143
Deep Security Manager - 20.0.954 (20 LTS 更新 2024-08-21) 143
新機能 144
機能強化 144

解決済みの問題 144
Deep Security Manager - 20.0.940 (20 LTS アップデート2024-07-17) 144
新機能 145
機能強化 145
解決済みの問題 145
セキュリティアップデート 145
Deep Security Manager - 20.0.926 (20 LTS 更新 2024-06-19) 145
機能強化 146
解決済みの問題 146
セキュリティアップデート 146
Deep Security Manager - 20.0.913 (20 LTS アップデート2024-05-15) 146
機能強化 146
解決済みの問題 147
セキュリティアップデート 147
Deep Security Manager - 20.0.904 (20 LTS Update 2024-04-17) 147
新機能 147
強化 148
解決済みの問題 148
Deep Security Manager - 20.0.893 (20 LTS Update 2024-03-20) 148
機能強化 148
解決済みの問題 149
Deep Security Manager - 20.0.883 (20 LTS Update 2024-02-21) 149
新機能 149
機能強化 149
解決済みの問題 149
Deep Security Manager - 20.0.879 (20 LTS Update 2024-01-17) 149
新機能 150
機能強化 150
解決済みの問題 150

既知の問題 151
セキュリティアップデート 151
Deep Security Manager - 20.0.864 (20 LTS Update 2023-12-12) 151
機能強化 151
解決済みの問題 152
既知の問題 152
Deep Security Manager - 20.0.854 (20 LTS Update 2023-11-15) 152
新機能 152
機能強化 152
解決済みの問題 153
セキュリティアップデート 153
既知の問題 153
Deep Security Manager - 20.0.844 (20 LTS Update 2023-10-18) 153
新機能 153
機能強化 153
解決済みの問題 154
既知の問題 154
Deep Security Manager - 20.0.833 (20 LTS Update 2023-09-20) 154
機能強化 155
解決済みの問題 155
セキュリティアップデート 155
Deep Security Manager - 20.0.817 (20 LTS Update 2023-08-23) 156
機能強化 156
Deep Security Manager - 20.0.802 (20 LTS Update 2023-07-19) 156
機能強化 156
解決済みの問題 156
セキュリティアップデート 156
Deep Security Manager - 20.0.789 (20 LTS Update 2023-06-28) 157
新機能 157

機能強化 157
解決済みの問題 157
セキュリティアップデート 158
Deep Security Manager - 20.0.768 (20 LTS Update 2023-05-17) 158
新機能 158
解決済みの問題 158
Deep Security Manager - 20.0.759 (20 LTS Update 2023-04-19) 158
強化 159
解決済みの問題 159
Deep Security Manager - 20.0.741(20 LTSアップデート2023/03/15) 159
新機能 159
Deep Security Manager - 20.0.737(20 LTSアップデート2023/02/23) 159
機能強化 159
セキュリティアップデート 160
Deep Security Manager - 20.0.725(20 LTSアップデート2023/01/18) 160
解決済みの問題 160
セキュリティアップデート 160
Deep Security Manager - 20.0.716 (20 LTSアップデート2022-12-15) 161
解決済みの問題 161
Deep Security Manager-20.0.711(20 LTSアップデート2022-11-16) 161
機能強化 161
セキュリティ更新 161
Deep Security Manager - 20.0.703(20 LTSアップデート2022/10/19) 161
機能強化 162
解決済みの問題 162
Deep Security Manager - 20.0.686(20 LTSアップデート2022/09/21) 162
解決済みの問題 162
Deep Security Manager - 20.0.677(20 LTSアップデート2022/08/17) 163
新機能 163

機能強化 163
解決済みの問題 163
Deep Security Manager - 20.0.664(20 LTSアップデート2022/07/21) 164
機能強化 164
解決済みの問題 164
セキュリティアップデート 164
Deep Security Manager - 20.0.651(20 LTSアップデート2022/06/15) 164
強化 165
Deep Security Manager - 20.0.644(20 LTSアップデート2022/05/18) 165
解決済みの問題 165
セキュリティアップデート 165
Deep Security Manager - 20.0.635 (20 LTS アップデート2022-04-21) 166
新機能 166
解決済みの問題 166
Deep Security Manager - 20.0.619 (20 LTS アップデート2022/03/22) 167
新機能 167
機能強化 167
解決済みの問題 167
セキュリティアップデート 167
Deep Security Manager - 20.0.605(20 LTS アップデート2022/02/16) 168
機能強化 168
解決された問題 168
セキュリティアップデート 168
Deep Security Manager - 20.0.585(20 LTSアップデート2022/01/17) 169
新機能 169
機能強化 169
解決済みの問題 169
セキュリティアップデート 169
Deep Security Manager - 20.0.560 (20 LTSアップデート2021/12/16) 170

新機能 170
解決済みの問題 170
セキュリティアップデート 170
Deep Security Manager - 20.0.543(20 LTSアップデート2021/11/18) 170
機能強化 171
解決済みの問題 171
Deep Security Manager - 20.0.513 (20 LTSアップデート2021/10/14) 172
新機能 172
解決済みの問題 173
Deep Security Manager - 20.0.503 (20 LTSアップデート2021/09/23) 173
新機能 173
機能強化 173
解決済みの問題 174
セキュリティ更新 174
Deep Security Manager - 20.0.482(20 LTSアップデート2021-08-25) 174
機能強化 175
解決済みの問題 175
セキュリティアップデート 175
Deep Security Manager - 20.0.463(20 LTSアップデート2021/07/22) 175
機能強化 176
解決された問題 176
セキュリティアップデート 176
Deep Security Manager - 20.0.447(20 LTSアップデート2021/06/28) 177
新機能 177
強化 177
解決済みの問題 178
セキュリティアップデート 178
Deep Security Manager - 20.0.414(20 LTSアップデート2021/05/24) 178
拡張 178

解決された問題 179
Deep Security Manager - 20.0.393(20 LTSアップデート2021-04-27) 179
機能強化 179
解決済みの問題 179
セキュリティアップデート 181
Deep Security Manager - 20.0.366(20 LTS Update 2021-03-24) 181
新機能 181
機能強化 181
解決済みの問題 181
セキュリティアップデート 182
Deep Security Manager - 20.0.344(20 LTSアップデート2021-02-23) 182
強化 182
解決済みの問題 183
Deep Security Manager - 20.0.321(20 LTS Update 2021/01/26) 183
機能強化 183
解決された問題 183
セキュリティ更新 183
Deep Security Manager - 20.0.313(20 LTSアップデート2021-01-18) 184
新機能 184
機能強化 184
解決済みの問題 185
セキュリティアップデート 185
Deep Security Manager - 20.0.262(20 LTSアップデート2020-11-26) 186
新機能 186
強化機能 186
解決済みの問題 186
セキュリティアップデート 187
Deep Security Manager 20.0.198(20 LTSアップデート2020-10-19) 187
機能強化 187

解決済みの問題 187
セキュリティアップデート 187
Deep Security Manager 20.0.174(20 LTSアップデート2020-09-16) 188
新機能 188
管理と品質の向上 188
強化 188
解決済みの問題 189
セキュリティアップデート 189
お知らせ 190
Deep Security Manager 20(長期サポートリリース) 190
クロスアカウントロールを使用してAPI /rest/cloudaccounts/awsを使用してDeep SecurityにAWSアカウントを追加する場合の処理が必要 190
新機能 190
更新されたプラットフォームのサポート 190
セキュリティの向上 191
管理と品質の向上 192
機能強化 193
解決済みの問題 197
セキュリティアップデート 200
既知の問題 201
Deep Security Agentの新機能 201
Deep Security Agent - 20.0.3-860 (20 LTS 更新 2026-01-21) 202
新機能 202
解決された問題 202
Deep Security Agent - 20.0.2-29810 (20 LTS 更新 2025-12-24) 202
解決された問題 202
Deep Security Agent - 20.0.2-29760 (20 LTS アップデート2025-12-09) 203
新機能 203
強化機能 203

解決された問題 203
セキュリティ更新 204
既知の問題 204
Deep Security Agent - 20.0.2-26670 (20 LTS 更新 2025-11-12) 204
新機能 205
解決された問題 205
既知の問題 205
Deep Security Agent - 20.0.2-22850 (20 LTS 更新 2025-10-08) 206
解決された問題 206
Deep Security Agent - 20.0.2-20480 (20 LTS 更新 2025-09-17) 206
新機能 206
強化 206
解決された問題 206
Deep Security Agent - 20.0.2-17500 (20 LTS 更新 2025-08-13) 207
機能強化 207
解決された問題 207
Deep Security Agent - 20.0.2-14431 (20 LTS 更新 2025-07-09) 207
新機能 207
強化 208
解決された問題 208
Deep Security Agent - 20.0.2-12010 (20 LTS 更新 2025-06-11) 208
強化 208
解決された問題 208
セキュリティ更新 209
Deep Security Agent - 20.0.2-9811 (20 LTS 更新 2025-05-14) 209
新機能 209
強化 209
解決された問題 209
Deep Securityエージェント - 20.0.2-7600 (20 LTS 更新 2025-04-16) 210

新機能 210
解決された問題 210
Deep Securityエージェント- 20.0.2-4961 (20 LTS 更新 2025-03-12) 211
新機能 211
強化 211
解決された問題 211
既知の問題 211
Deep Securityエージェント- 20.0.2-1390 (20 LTS 更新 2025-01-15) 212
新機能 212
機能強化 212
解決された問題 212
セキュリティ更新 212
Deep Securityエージェント- 20.0.1-25771 (20 LTS Update 2024-12-10) 212
新機能 212
強化 213
解決された問題 214
セキュリティ更新 214
Deep Securityエージェント- 20.0.1-23340 (20 LTS 更新 2024-11-13) 214
強化 214
解決済みの問題 215
Deep Securityエージェント- 20.0.1-21510 (20 LTS更新 2024-10-16) 215
新機能 215
強化 215
解決された問題 216
Deep Security エージェント- 20.0.1-19250 (20 LTS Update 2024-09-18) 216
新機能 216
機能強化 216
解決済みの問題 216
セキュリティ更新 217

Deep Security Agent - 20.0.1-17380 (20 LTS アップデート2024-08-21) 217
機能強化 217
解決された問題 217
既知の問題 218
Deep Security Agent - 20.0.1-14610 (20 LTS アップデート2024-07-17) 218
新機能 218
機能強化 219
解決済みの問題 219
Deep Security Agent - 20.0.1-12510 (20 LTS アップデート2024-06-19) 219
機能強化 220
解決された問題 220
セキュリティアップデート 220
既知の問題 220
Deep Security Agent - 20.0.1-9400 (20 LTS Update 2024-05-16) 221
新機能 221
強化 221
解決済みの問題 221
セキュリティ更新 222
既知の問題 222
Deep Security Agent - 20.0.1-7380 (20 LTS Update 2024-04-24) 222
新機能 222
強化 223
解決済みの問題 223
Deep Security Agent - 20.0.1-4540 (20 LTS Update 2024-03-20) 224
新機能 224
機能強化 224
解決された問題 224
既知の問題 224
Deep Security Agent - 20.0.1-3180 (20 LTS Update 2024-02-29) 225

強化 225
解決された問題 225
既知の問題 226
Deep Security Agent - 20.0.1-690 (20 LTS Update 2024-01-17) 226
新機能 226
機能強化 226
解決済みの問題 226
既知の問題 227
Deep Security Agent - 20.0.0-8453 (20 LTS Update 2024-01-17) 227
解決済みの問題 227
強化 228
既知の問題 228
Deep Security Agent - 20.0.0-8438 (20 LTS Update 2023-12-12) 228
新機能 228
機能強化 228
解決済みの問題 229
セキュリティアップデート 229
既知の問題 229
Deep Security Agent - 20.0.0-8268 (20 LTS Update 2023-11-21) 230
新機能 230
解決済みの問題 230
既知の問題 231
Deep Security Agent - 20.0.0-8137 (20 LTS Update 2023-10-26) 231
新機能 231
既知の問題 232
Deep Security Agent - 20.0.0-7943 (20 LTS Update 2023-09-26) 232
新機能 232
機能強化 233
解決済みの問題 233

既知の問題 234
Deep Security Agent - 20.0.0-7719 (20 LTS Update 2023-08-29) 234
新機能 234
機能強化 234
解決済みの問題 235
Deep Security Agent - 20.0.0-7476 (20 LTS Update 2023-07-25) 235
機能強化 235
解決済みの問題 236
Deep Security Agent - 20.0.0-7303 (20 LTS Update 2023-06-28) 236
新機能 236
機能強化 236
解決済みの問題 237
Deep Security Agent - 20.0.0-7119 (20 LTS Update 2023-05-29) 237
機能強化 237
解決済みの問題 238
Deep Security Agent - 20.0.0-6912 (20 LTS Update 2023-05-02) 238
新機能 238
機能強化 238
解決された問題 239
Deep Security Agent - 20.0.0-6658 (20 LTS Update 2023-03-22) 240
新機能 240
機能強化 240
解決済みの問題 241
Deep Security Agent - 20.0.0-6313 (20 LTS Update 2023-01-31) 242
新機能 242
機能強化 243
解決された問題 243
既知の問題 244
Deep Security Agent - 20.0.0-5953 (20 LTS Update 2022-11-22) 244

新機能 244
機能強化 244
解決済みの問題 244
Deep Security Agent - 20.0.0-5761 (20 LTS Update 2022-10-21) 245
新機能 245
プラットフォームのサポート強化 245
機能強化 245
解決済みの問題 245
Deep Security Agent - 20.0.0-5512 (20 LTS Update 2022-09-22) 246
機能強化 246
解決済みの問題 247
セキュリティアップデート 247
Deep Security Agent - 20.0.0-5394 (20 LTS Update 2022-08-29) 247
新機能 247
機能強化 248
解決済みの問題 248
既知の問題 249
Deep Security Agent - 20.0.0-5137 (20 LTS Update 2022-07-26) 249
新機能 249
機能強化 249
解決済みの問題 250
セキュリティアップデート 250
既知の問題 251
Deep Security Agent - 20.0.0-4959 (20 LTS Update 2022-07-04) 251
新機能 251
機能強化 251
解決済みの問題 251
Deep Security Agent - 20.0.0-4726 (20 LTS Update 2022-05-31) 252
機能強化 252

解決済みの問題 252
セキュリティアップデート 253
Deep Security Agent - 20.0.0-4416 (20 LTS Update 2022-04-28) 253
機能強化 253
解決済みの問題 254
セキュリティアップデート 254
Deep Security Agent - 20.0.0-4185 (20 LTS Update 2022-04-06) 254
新機能 254
解決済みの問題 254
Deep Security Agent - 20.0.0-3964 (20 LTS Update 2022-03-01) 255
新機能 255
プラットフォームのサポートの強化 255
機能強化 255
解決済みの問題 255
Deep Security Agent - 20.0.0-3770 (20 LTS Update 2022-01-24) 256
新機能 256
機能強化 256
解決済みの問題 256
セキュリティアップデート 257
Deep Security Agent - 20.0.0-3445 (20 LTS Update 2021-11-24) 257
新機能 257
機能強化 258
解決済みの問題 258
セキュリティアップデート 259
Deep Security Agent - 20.0.0-3288 (20 LTS Update 2021-10-28) 259
新機能 259
プラットフォームのサポートの強化 260
機能強化 260
解決された問題 260

セキュリティアップデート 261
Deep Security Agent - 20.0.0-3165 (20 LTS Update 2021-10-08) 261
新機能 261
機能強化 262
解決済みの問題 262
セキュリティアップデート 262
Deep Security Agent - 20.0.0-2971 (20 LTSアップデート2021-09-08) 263
新機能 263
機能強化 263
解決済みの問題 263
セキュリティアップデート 265
Deep Security Agent-20.0.0-2593(20 LTS Update 2021-07-01) 265
新機能 265
解決済みの問題 265
セキュリティアップデート 265
Deep Security Agent - 20.0.0-2395(20 LTSアップデート2021-05-24) 266
新機能 266
プラットフォームのサポートの強化 266
機能強化 266
解決済みの問題 266
Deep Security Agent - 20.0.0-2204 (20 LTS Update 2021-04-12) 267
新機能 267
強化されたプラットフォームのサポート 267
解決済みの問題 268
Deep Security Agent - 20.0.0-2009(20 LTSアップデート2021-03-08) 268
機能強化 268
解決済みの問題 268
Deep Security Agent - 20.0.0-1876 (20 LTS Update 2021-02-08) 269
解決済みの問題 269

Deep Security Agent - 20.0.0-1822(20 LTSアップデート2021-01-18) 269
新機能 269
プラットフォームのサポートの強化 269
Deep Security Agent - 20.0.0-1681(20 LTSアップデート2021-01-04) 269
解決済みの問題 270
Deep Security Agent 20.0.0-1559(20 LTSアップデート2020/12/07) 270
新機能 270
機能強化 270
解決済みの問題 270
お知らせ 271
Deep Security Agent 20.0.0-1337(20 LTSアップデート2020/10/28) 271
解決済みの問題 272
Deep Security Agent 20.0.0-1304(20 LTSアップデート2020/10/21) 272
機能強化 272
解決済みの問題 272
Deep Security Agent 20.0.0-1194(20 LTSアップデート2020-10-05) 273
新機能 273
機能強化 273
解決済みの問題 274
セキュリティアップデート 275
Deep Security Agent 20(長期サポートリリース) 275
新機能 275
プラットフォームのサポートの強化 275
セキュリティの向上 276
管理と品質の向上 277
機能強化 278
解決済みの問題 279
セキュリティ更新 282
カーネルのサポート 283

既知の問題 283
Deep Security Agent - 20.0.3-860 (20 LTS 更新 2026-01-21) 283
新機能 283
解決された問題 283
Deep Security Agent - 20.0.2-29810 (20 LTS 更新 2025-12-24) 284
解決された問題 284
Deep Security Agent - 20.0.2-29760 (20 LTS アップデート2025-12-09) 284
強化 284
解決された問題 285
セキュリティ更新 285
既知の問題 285
Deep Security Agent - 20.0.2-26670 (20 LTS 更新 2025-11-12) 286
新機能 286
解決された問題 287
Deep Security Agent - 20.0.2-22850 (20 LTS 更新 2025-10-08) 287
強化機能 287
Deep Security Agent - 20.0.2-20480 (20 LTS 更新 2025-09-17) 287
機能強化 287
解決された問題 287
既知の問題 288
Deep Security Agent - 20.0.2-17700 (20 LTS 更新 2025-08-13) 288
強化 288
解決された問題 288
Deep Security Agent - 20.0.2-14490 (20 LTS 更新 2025-07-09) 288
新機能 288
強化 288
解決済みの問題 289
Deep Security Agent - 20.0.2-12290 (20 LTS 更新 2025-06-11) 289
機能強化 289

解決済みの問題 289
セキュリティアップデート 290
Deep Security Agent - 20.0.2-9810 (20 LTS 更新 2025-05-14) 290
機能強化 290
解決済みの問題 290
セキュリティアップデート 291
Deep Securityエージェント- 20.0.2-7600 (20 LTS 更新 2025-04-16) 291
新機能 291
機能強化 291
解決された問題 292
セキュリティアップデート 292
Deep Securityエージェント- 20.0.2-4960 (20 LTS 更新 2025-03-12) 292
機能強化 292
解決済みの問題 293
Deep Securityエージェント- 20.0.2-1390 (20 LTS 更新 2025-01-15) 293
新機能 293
機能強化 293
解決済みの問題 294
セキュリティ更新 294
Deep Securityエージェント- 20.0.1-25770 (20 LTS Update 2024-12-10) 294
新機能 294
強化 294
解決された問題 295
セキュリティ更新 295
Deep Securityエージェント- 20.0.1-23340 (20 LTS 更新 2024-11-13) 296
新機能 296
機能強化 296
解決済みの問題 296
セキュリティ更新 297

Deep Securityエージェント- 20.0.1-21510 (20 LTS更新 2024-10-16) 297
機能強化 297
解決された問題 297
セキュリティアップデート 298
Deep Security エージェント- 20.0.1-19250 (20 LTS Update 2024-09-18) 298
機能強化 298
解決済みの問題 298
セキュリティアップデート 298
Deep Security Agent - 20.0.1-17380 (20 LTS アップデート2024-08-21) 299
機能強化 299
解決済みの問題 299
セキュリティアップデート 300
既知の問題 300
Deep Security Agent - 20.0.1-14610 (20 LTS アップデート2024-07-17) 300
機能強化 300
解決済みの問題 301
Deep Security Agent - 20.0.1-12510 (20 LTS アップデート2024-06-19) 301
機能強化 301
解決済みの問題 301
既知の問題 302
Deep Security Agent - 20.0.1-9400 (20 LTS Update 2024-05-16) 302
機能強化 302
解決済みの問題 302
セキュリティアップデート 303
Deep Security Agent - 20.0.1-7380 (20 LTS Update 2024-04-24) 303
強化 303
解決された問題 303
Deep Security Agent - 20.0.1-4540 (20 LTS Update 2024-03-20) 304
機能強化 304

解決済みの問題 304
Deep Security Agent - 20.0.1-3180 (20 LTS Update 2024-02-29) 304
新機能 304
機能強化 305
解決済みの問題 305
セキュリティ更新 305
既知の問題 306
Deep Security Agent - 20.0.1-700 (20 LTS Update 2024-04-17) 306
機能強化 306
既知の問題 306
Deep Security Agent - 20.0.1-690 (20 LTS Update 2024-01-17) 306
新機能 307
機能強化 307
解決済みの問題 307
セキュリティアップデート 307
既知の問題 308
Deep Security Agent - 20.0.0-8438 (20 LTS Update 2023-12-12) 308
新機能 308
機能強化 308
解決済みの問題 308
セキュリティ更新 309
既知の問題 309
Deep Security Agent - 20.0.0-8268 (20 LTS Update 2023-11-21) 309
解決済みの問題 309
既知の問題 310
Deep Security Agent - 20.0.0-8137 (20 LTS Update 2023-10-26) 310
新機能 310
解決済みの問題 310
既知の問題 311

Deep Security Agent - 20.0.0-7943 (20 LTS Update 2023-09-26) 311
強化 311
解決済みの問題 311
Deep Security Agent - 20.0.0-7719 (20 LTS Update 2023-08-29) 311
新機能 312
機能強化 312
解決済みの問題 312
セキュリティアップデート 313
Deep Security Agent - 20.0.0-7476 (20 LTS Update 2023-07-25) 313
新機能 313
機能強化 313
解決済みの問題 314
Deep Security Agent - 20.0.0-7303 (20 LTS Update 2023-06-28) 314
機能強化 314
解決された問題 315
Deep Security Agent - 20.0.0-7119 (20 LTS Update 2023-05-29) 315
機能強化 315
解決済みの問題 316
既知の問題 316
Deep Security Agent - 20.0.0-6860 (20 LTS Update 2023-04-25) 316
機能強化 316
解決済みの問題 317
セキュリティ更新 317
Deep Security Agent - 20.0.0-6690 (20 LTS Update 2023-03-29) 318
新機能 318
機能強化 318
解決済みの問題 319
既知の問題 320
Deep Security Agent - 20.0.0-6313 (20 LTS Update 2023-01-31) 321

新機能 321
機能強化 321
解決済みの問題 321
Deep Security Agent - 20.0.0-5995 (20 LTS Update 2022-11-28) 322
新機能 322
機能強化 322
解決済みの問題 323
Deep Security Agent - 20.0.0-5810 (20 LTS Update 2022-10-27) 323
新機能 323
機能強化 324
解決済みの問題 324
既知の問題 324
Deep Security Agent - 20.0.0-5512 (20 LTS Update 2022-09-22) 325
機能強化 325
解決済みの問題 325
セキュリティアップデート 325
Deep Security Agent - 20.0.0-5394 (20 LTS Update 2022-08-29) 326
機能強化 326
解決済みの問題 326
既知の問題 327
Deep Security Agent - 20.0.0-5137 (20 LTS Update 2022-07-26) 327
新機能 327
機能強化 328
解決済みの問題 328
セキュリティアップデート 328
既知の問題 329
Deep Security Agent - 20.0.0-4959 (20 LTS Update 2022-07-04) 329
解決済みの問題 329
セキュリティアップデート 330

Deep Security Agent - 20.0.0-4726 (20 LTS Update 2022-05-31) 330
機能強化 330
解決済みの問題 330
セキュリティアップデート 331
Deep Security Agent - 20.0.0-4416 (20 LTS Update 2022-04-28) 331
機能強化 331
解決された問題 332
セキュリティアップデート 332
Deep Security Agent - 20.0.0-4185 (20 LTS Update 2022-04-06) 332
新機能 332
強化 333
解決済みの問題 333
Deep Security Agent - 20.0.0-3964 (20 LTS Update 2022-03-01) 333
新機能 333
機能強化 334
解決済みの問題 334
Deep Security Agent - 20.0.0-3771 (20 LTS Update 2022-01-24) 334
新機能 334
機能強化 335
解決済みの問題 335
セキュリティアップデート 335
Deep Security Agent - 20.0.0-3530 (20 LTS Update 2021-12-15) 336
新機能 336
重要な注意事項 336
解決された問題 336
Deep Security Agent - 20.0.0-3445 (20 LTS Update 2021-11-24) 336
新機能 337
機能強化 337
解決済みの問題 337

セキュリティアップデート 338
Deep Security Agent - 20.0.0-3288 (20 LTSアップデート2021-10-28) 338
新機能 338
解決済みの問題 339
セキュリティアップデート 339
Deep Security Agent - 20.0.0-3165 (20 LTSアップデート2021-10-08) 340
新機能 340
解決済みの問題 340
セキュリティアップデート 341
Deep Security Agent-20.0.0-2921(20 LTS Update 2021-08-30) 341
新機能 341
機能強化 341
解決済みの問題 341
セキュリティアップデート 342
Deep Security Agent-20.0.0-2740(20 LTS Update 2021-07-29) 342
強化 342
解決済みの問題 342
セキュリティアップデート 343
Deep Security Agent-20.0.0-2593(20 LTS Update 2021-07-01) 343
解決された問題 343
セキュリティアップデート 344
Deep Security Agent-20.0.0-2419(20 LTS Update 2021-06-02) 344
解決済みの問題 344
Deep Security Agent - 20.0.0-2204 (20 LTS Update 2021-04-12) 345
解決済みの問題 345
Deep Security Agent - 20.0.0-2009(20 LTSアップデート2021-03-08) 345
機能強化 346
解決された問題 346
Deep Security Agent - 20.0.0-1876 (20 LTS Update 2021-02-08) 346

解決済みの問題 346
Deep Security Agent - 20.0.0-1822(20 LTSアップデート2021-01-18) 346
解決済みの問題 347
Deep Security Agent - 20.0.0-1681(20 LTSアップデート2021-01-04) 347
Deep Security Agent 20.0.0-1559(20 LTSアップデート2020/12/07) 347
新機能 347
プラットフォームのサポート強化 347
セキュリティの向上 347
機能強化 347
解決済みの問題 348
お知らせ 348
Deep Security Agent 20.0.0-1337(20 LTSアップデート2020/10/28) 348
新機能 348
機能強化 349
解決済みの問題 349
セキュリティアップデート 350
既知の問題 350
Deep Security Agent 20(長期サポートリリース) 350
新機能 350
セキュリティの向上 351
品質と管理の向上 351
機能強化 352
解決済みの問題 353
セキュリティアップデート 355
既知の問題 355
アップグレードの通知 356
Deep Security Agent - 20.0.3-860 (20 LTS 更新 2026-01-21) 356
新機能 356
解決された問題 356

Deep Security Agent - 20.0.2-29760 (20 LTS アップデート2025-12-09) 357
機能強化 357
セキュリティ更新 357
Deep Security Agent - 20.0.2-26670 (20 LTS 更新 2025-11-12) 357
新機能 357
解決された問題 357
Deep Security Agent - 20.0.2-22850 (20 LTS 更新 2025-10-08) 358
既知の問題 358
Deep Security Agent - 20.0.2-20480 (20 LTS 更新 2025-09-17) 358
Deep Security Agent - 20.0.2-17500 (20 LTS 更新 2025-08-13) 358
Deep Security Agent - 20.0.2-14430 (20 LTS 更新 2025-07-09) 358
強化 358
解決された問題 359
Deep Security Agent - 20.0.2-12010 (20 LTS 更新 2025-06-11) 359
機能強化 359
解決された問題 359
セキュリティ更新 359
Deep Security Agent - 20.0.2-9810 (20 LTS 更新 2025-05-14) 359
機能強化 359
解決された問題 360
Deep Securityエージェント- 20.0.2-7600 (20 LTS 更新 2025-04-16) 360
Deep Securityエージェント- 20.0.2-4961 (20 LTS 更新 2025-03-12) 360
機能強化 360
Deep Securityエージェント- 20.0.2-1390 (20 LTS 更新 2025-01-15) 360
強化 361
解決された問題 361
Deep Securityエージェント- 20.0.1-25771 (20 LTS Update 2024-12-10) 361
解決済みの問題 361
Deep Securityエージェント- 20.0.1-23340 (20 LTS 更新 2024-11-13) 361

機能強化 361
解決された問題 361
Deep Securityエージェント- 20.0.1-21510 (20 LTS更新 2024-10-16) 362
Deep Security エージェント- 20.0.1-19250 (20 LTS Update 2024-09-18) 362
Deep Security Agent - 20.0.1-17380 (20 LTS アップデート2024-08-21) 362
解決済みの問題 362
Deep Security Agent - 20.0.1-14610 (20 LTS アップデート2024-07-17) 363
解決済みの問題 363
Deep Security Agent - 20.0.1-12510 (20 LTS アップデート2024-06-19) 363
解決済みの問題 363
Deep Security Agent - 20.0.1-9400 (20 LTS Update 2024-05-16) 363
解決された問題 363
Deep Security Agent - 20.0.1-7380 (20 LTS Update 2024-04-24) 364
機能強化 364
解決済みの問題 364
Deep Security Agent - 20.0.1-4540 (20 LTS Update 2024-03-20) 364
Deep Security Agent - 20.0.1-3180 (20 LTS Update 2024-02-29) 364
解決済みの問題 365
セキュリティアップデート 365
既知の問題 365
Deep Security Agent - 20.0.1-690 (20 LTS Update 2024-01-17) 365
機能強化 365
解決済みの問題 366
既知の問題 366
Deep Security Agent - 20.0.0-8438 (20 LTS Update 2023-12-12) 366
解決済みの問題 366
セキュリティアップデート 366
既知の問題 367
Deep Security Agent - 20.0.0-8268 (20 LTS Update 2023-11-21) 367

解決済みの問題 367
Deep Security Agent - 20.0.0-8137 (20 LTS Update 2023-10-26) 367
Deep Security Agent - 20.0.0-7943 (20 LTS Update 2023-09-26) 367
機能強化 368
Deep Security Agent - 20.0.0-7719 (20 LTS Update 2023-08-29) 368
機能強化 368
解決済みの問題 368
Deep Security Agent - 20.0.0-7476 (20 LTS Update 2023-07-25) 369
強化機能 369
解決済みの問題 369
Deep Security Agent - 20.0.0-7303 (20 LTS Update 2023-06-28) 369
機能強化 369
解決済みの問題 370
Deep Security Agent - 20.0.0-7119 (20 LTS Update 2023-05-29) 370
強化 370
解決済みの問題 370
Deep Security Agent - 20.0.0-6912 (20 LTS Update 2023-05-02) 370
機能強化 371
解決済みの問題 371
Deep Security Agent - 20.0.0-6658 (20 LTS Update 2023-03-22) 371
新機能 371
機能強化 371
解決済みの問題 372
Deep Security Agent - 20.0.0-6313 (20 LTS Update 2023-01-31) 373
機能強化 373
解決済みの問題 373
Deep Security Agent - 20.0.0-5953 (20 LTS Update 2022-11-22) 374
Deep Security Agent - 20.0.0-5761 (20 LTS Update 2022-10-21) 374
機能強化 374

解決済みの問題 374
Deep Security Agent - 20.0.0-5512 (20 LTS Update 2022-09-22) 374
機能強化 375
解決済みの問題 375
セキュリティアップデート 375
Deep Security Agent - 20.0.0-5394 (20 LTS Update 2022-08-29) 375
新機能 375
機能強化 375
解決済みの問題 376
既知の問題 376
Deep Security Agent - 20.0.0-5137 (20 LTS Update 2022-07-26) 376
機能強化 377
解決済みの問題 377
セキュリティアップデート 377
既知の問題 377
Deep Security Agent - 20.0.0-4959 (20 LTS Update 2022-07-04) 377
解決済みの問題 378
Deep Security Agent - 20.0.0-4726 (20 LTS Update 2022-05-31) 378
解決済みの問題 378
セキュリティアップデート 378
Deep Security Agent - 20.0.0-4416 (20 LTS Update 2022-04-28) 379
機能強化 379
解決済みの問題 379
セキュリティアップデート 379
Deep Security Agent - 20.0.0-4185 (20 LTS Update 2022-04-06) 379
解決済みの問題 380
Deep Security Agent - 20.0.0-3964 (20 LTS Update 2022-03-01) 380
新機能 380
機能強化 380

Deep Security Agent - 20.0.0-3770 (20 LTS Update 2022-01-24) 380
機能強化 380
解決済みの問題 381
セキュリティアップデート 381
Deep Security Agent - 20.0.0-3445 (20 LTS Update 2021-11-24) 381
機能強化 381
解決済みの問題 382
セキュリティアップデート 382
Deep Security Agent - 20.0.0-3288 (20 LTSアップデート2021-10-28) 382
新機能 382
解決済みの問題 383
セキュリティアップデート 383
Deep Security Agent - 20.0.0-3165 (20 LTSアップデート2021-10-08) 383
新機能 384
解決済みの問題 384
セキュリティアップデート 384
Deep Security Agent-20.0.0-2921(20 LTS Update 2021-08-30) 384
解決済みの問題 385
Deep Security Agent-20.0.0-2740(20 LTS Update 2021-07-29) 385
機能強化 385
解決済みの問題 385
セキュリティアップデート 386
Deep Security Agent-20.0.0-2593(20 LTS Update 2021-07-01) 386
解決された問題 386
セキュリティアップデート 386
Deep Security Agent - 20.0.0-2395(20 LTSアップデート2021-05-24) 387
新機能 387
解決された問題 387
Deep Security Agent - 20.0.0-2204 (20 LTS Update 2021-04-12) 387

新機能 387
強化されたプラットフォームのサポート 387
解決済みの問題 387
Deep Security Agent - 20.0.0-2009(20 LTSアップデート2021-03-08) 388
解決済みの問題 388
Deep Security Agent - 20.0.0-1876 (20 LTS Update 2021-02-08) 388
Deep Security Agent - 20.0.0-1822(20 LTSアップデート2021-01-18) 388
新機能 388
Deep Security Agent - 20.0.0-1681(20 LTSアップデート2021-01-04) 389
Deep Security Agent 20.0.0-1559(20 LTSアップデート2020/12/07) 389
新機能 389
機能強化 389
解決済みの問題 389
お知らせ 390
Deep Security Agent 20.0.0-1337(20 LTSアップデート2020/10/28) 390
解決済みの問題 390
Deep Security Agent 20.0.0-1304(20 LTSアップデート2020-10-21) 390
機能強化 391
解決済みの問題 391
Deep Security Agent 20.0.0-1194(20 LTSアップデート2020-10-05) 391
機能強化 391
解決済みの問題 391
セキュリティアップデート 392
Deep Security Agent 20(長期サポートリリース) 392
新機能 392
セキュリティの向上 392
品質と管理の向上 392
機能強化 393
解決済みの問題 394

セキュリティアップデート 397
Deep Security Virtual Applianceの新機能 397
新機能 398
セキュリティの向上 398
管理と品質の向上 398
拡張機能 398
問題を解決する 399
既知の問題 399
互換性 400
システム要件 400
エージェントの要件 400
Deep Security Agentのプラットフォーム 400
Linuxカーネルの互換性 400
オプションのLinuxカーネルサポートパッケージアップデートを無効にする 401
1台のコンピューターでカーネルサポートパッケージの更新を無効にする 402
複数のコンピューターでカーネルサポートパッケージの更新を無効にする 403
Linuxファイルシステムの互換性 403
Linux systemdのサポート 404
Linux Secure Bootのサポート 409
Deep Security Agent 20 LTS 409
Deep Security Agent 12 FR 412
Deep Security Agent 12 LTS 412
Deep Security Agent 11 LTS 413
SELinuxのサポート 413
各プラットフォームでサポートされている機能 417
サイジング 417
Deep Security Managerのサイジング 417
複数のサーバノード 418
データベースのサイジング 418

データベースのディスク容量の見積もり ... 420
Deep Security Agent のサイズとリソース消費 ... 420
Deep Security AgentおよびRelayのサイジング ... 421
推定 Deep Security Agent リソース消費量 ... 421
Windowsエージェント ... 421
Linuxエージェント ... 422
不正プログラム対策ソリューションプラットフォームサービスのCPUサイズ設定 ... 422
Deep Security Virtual Applianceのサイジング ... 425
Deep Security Managerのパフォーマンス機能 ... 427
パフォーマンスプロファイル ... 427
ディスク容量不足のアラート ... 427
データベースのディスク容量不足 ... 428
Managerのディスク容量不足 ... 428
ポート番号、URL、およびIPアドレス ... 428
Deep Securityのポート番号 ... 429
Deep SecurityのURL ... 434
はじめに ... **445**
ソフトウェアパッケージのデジタル署名の確認 ... 445
ソフトウェアZIPパッケージの署名の確認 ... 445
インストーラファイル (EXE、MSI、RPM、またはDEBファイル) の署名の確認 ... 447
EXEまたはMSIファイルの署名の確認 ... 448
RPMファイルの署名の確認 ... 448
DEBファイルの署名の確認 ... 450
Deep Security Managerを配信する ... 452
データベースを準備する ... 452
データベースの要件 ... 452
ソフトウェア要件 ... 453
Microsoft SQL Server Expressに関する注意事項 ... 453
ハードウェア要件 ... 454

ネットワーク要件 454
VMwareの要件 454
スケーリングの要件 454
データベースサーバをインストールする 455
データベースの設定 455
基本設定 455
マルチテナント設定 456
PostgreSQLチューニング(オプション) 456
基本設定 456
マルチテナント設定 456
基本設定 457
Oracle RACの設定 457
マルチテナント設定 457
準備チェックを実行する 458
Deep Security Managerをインストールする 459
開始前の準備 459
Managerをインストールする 460
インストールをテストします(マネージャにログオンします) 。 464
自己署名証明書を置換する 464
Deep Security Managerをサイレントモードでインストールする 464
開始前の準備 465
Windowsプラットフォームでサイレントインストールを実行する 465
Linuxプラットフォームでサイレントインストールを実行する 465
サイレントインストールのパラメータ 465
サンプルインストールの出力 466
インストールに成功した場合 467
インストールに失敗した場合 468
プロパティファイルのDeep Security設定 468
必須の設定 468

LicenseScreen ... 468
CredentialsScreen ... 469
オプションの設定 ... 469
LanguageScreen ... 469
UpgradeVerificationScreen ... 469
OldDataMigrationScreen ... 469
DatabaseScreen ... 470
AddressAndPortsScreen ... 472
CredentialsScreen ... 473
MasterKeyConfigurationScreen ... 473
SecurityUpdateScreen ... 473
SoftwareUpdateScreen ... 474
SmartProtectionNetworkScreen ... 475
RelayScreen ... 476
プロパティファイルの例 ... 477
アクティベーションコードを追加 ... 478
マルチテナントを設定する ... 478
マルチテナント環境の設定 ... 478
マルチテナントの要件 ... 479
マルチテナントを有効にする ... 480
テナントを作成する ... 480
テナントに送信されるメッセージの例 ... 481
確認リンクをメール: アカウント確認要求 ... 481
生成したパスワードをメール ... 482
SQL Server可用性グループにテナントデータベースを追加する ... 482
スケーラビリティのガイドライン ... 482
マルチテナントに関するヒント ... 483
攻撃の予兆IPリスト ... 483
複数のデータベースサーバを使用する ... 483

テナントの「削除の保留中」状態 483
[システム設定] のマルチテナントオプション 483
テナントを管理する 484
テナントのプロパティ 484
一般 484
モジュール 484
機能 485
統計 485
Deep Security Agentの有効化 485
テナントに表示される内容 486
エージェントによるアクティベーションの開始 487
テナントの診断 487
使用状況の監視 488
マルチテナントのダッシュボード 488
マルチテナントのレポート 488
セキュリティモジュールの累積使用状況レポート 489
セキュリティモジュールの使用状況レポート 489
テナントレポート 490
データベースのユーザアカウントを設定する 490
SQL Server 491
Oracle 495
PostgreSQL 497
複数のデータベースサーバを設定する 498
セカンダリデータベースを削除または変更する 498
API 498
マルチテナント環境のアップグレード 499
テナントをサポートする 500
Deep Security Virtual Appliance環境のマルチテナント 500
マルチテナント設定 501

データベースサーバ 503
新しいテナントテンプレート 503
保護の使用状況の監視 504
複数のノードを設定する 505
複数のノードにDeep Security Managerをインストールする 505
ロードバランサを設定する 505
Deep Securityでのロードバランサの設定 506
ノードを追加する 506
ノードを削除する 507
ノードのアップグレード 507
ノードのステータスを表示する 508
アクティビティグラフ付きネットワークマップ 508
ノード別ジョブ 509
種類別ジョブ 509
ノードおよび種類別ジョブの総数 510
アクティブなDeep Security Managerノードの表示 510
Deep Securityを配信するRelay 513
Deep Security Agentを配信する 514
Deep Security Agentソフトウェアの入手 514
ダウンロード可能なエージェントソフトウェアの表示 514
インポートされたエージェントソフトウェアのリストを表示する 515
エージェントソフトウェアのインポート 515
ダウンロードセンターから直接エージェントソフトウェアをインポートする 515
ヘルプセンターから間接的にエージェントソフトウェアをインポートする 516
エージェントソフトウェアのアップデートを自動的にインポートする 517
Agentのインストーラをエクスポートする 517
Solaris版とエージェントパッケージのマッピングテーブル 518
AIXエージェントパッケージの命名形式 519
Deep Securityデータベースからソフトウェアパッケージを削除する 519

シングルテナントモードでAgentパッケージを削除する 520
マルチテナントモードでAgentパッケージを削除する 520
カーネルサポートパッケージを削除する 520
AgentのLinux Secure Bootの設定 520
トレンドマイクロの公開鍵のダウンロード 521
トレンドマイクロの公開鍵をアップデートする 523
AWSのセキュアブートキーの登録 524
Google Cloud Platformのセキュアブートキーの登録 527
VMware vSphereプラットフォームのセキュアブートキーの登録 528
物理コンピュータのセキュアブートキーを登録する 529
Oracle Linux用セキュアブートキーの登録 531
Azureのセキュアブートキーを登録する 532
エージェントをインストールする 536
エージェントを手動でインストールする 537
Amazon WorkSpacesでのインストール 538
Windows 2012 Server Coreでのインストール 538
他の方法でエージェントをインストールする 543
インストール後のタスク 543
Amazon EC2およびWorkSpacesへのAgentのインストール 543
AWSアカウントをDeep Security Managerに追加する 544
通信方向を設定する 544
有効化の種類を設定する 545
ポートを開く 546
開放するポート 546
AgentをAmazon EC2インスタンスおよびWorkSpacesにインストールする 547
エージェントのインストールとアクティベーションを確認 548
ポリシーを割り当てる 548
エージェントをAMIまたはWorkSpaceバンドルにインストールする 549
AWSアカウントをDeep Security Managerに追加する 549

通信方向を設定する 550
有効化の種類を設定する 550
「マスター」Amazon EC2インスタンスまたはAmazon WorkSpaceを起動する 550
Agentをマスターにインストールする 550
Agentが適切にインストールされ有効化されたことを確認する 551
(推奨) 自動ポリシー割り当てを設定する 551
マスターに基づいてAMIまたはカスタムWorkSpaceバンドルを作成する 552
AMIを使用する 553
Azure VMにエージェントをインストールする 553
Google Cloud Platform VMにエージェントをインストールする 553
VMware vCloudへのAgentのインストール 556
vCloudアカウントのテナントユーザ向けの最小権限のロールを作成する 556
新しい仮想マシンに一意のUUIDを割り当てる 557
ゲスト仮想マシンでVMware Toolsの [OVF Environment Transport] を有効にする 557
VMware vCloud Organizationアカウントからのコンピュータのインポート 557
VMware vCloud Air仮想データセンターからコンピュータをインポートする 558
Agentの有効化 559
Agentを無効化する 560
エージェントの起動または停止 561
エージェントのインストールまたはアップデート時の一般的な問題 561
1. 不正プログラム対策エンジンがオフライン(Windows) 562
2. セキュリティアップデートに失敗した場合 562
3. Deep Security Agentのインストール後に発生するパフォーマンス/アプリケーションの問題(不正プログラム対策およびモジュール分離) 563
Deep Security Virtual Applianceを配信する 565
VMware環境の保護 565
Deep Security Virtual Applianceの機能 565
検索キャッシュ 565
検索ストームの最適化 565

管理の簡素化 566
Virtual ApplianceおよびNSXを使用するVMware環境 566
エージェントのみを使用したVMwareの配置 569
追加情報 569
Agentレスによる保護またはコンバインモードの保護の選択 569
Agentレスによる保護 570
コンバインモード 570
協調的保護からコンバインモードへの変換 570
保護機能ごとにクライアントまたはアプライアンスを選択する 571
vCloud Director環境で、エージェント起動の有効化を使用して複合モードを有効にする 572
アプライアンスを配信する前に 573
システム要件を確認する 573
NSX、Deep Security Managerなどのコンポーネントのインストールまたはバージョンアップ 573
NSX-Tの再登録 573
通信を設定する 574
(オプション) Deep Security Agentのインストール 574
(オプション) 高可用性の設定 575
次の手順 575
VMware DRSの設定 575
アプライアンスを配信する(NSX-T 3.x) 576
アプライアンスをインポートする 576
ファブリック設定の準備 577
ユーザインタフェースモードの切り替えの設定 577
Compute Managerを設定する 578
トランスポートゾーンの設定 579
トランスポートノードプロファイルを設定する 580
ホストを準備する 584
論理スイッチを作成する 586

Deep Security ManagerにvCenterを追加する 588
NSX-T 3.xにアプライアンスをインストールします。 589
サービスの配信を開始する 589
サービス配信を設定および開始する 590
サービス配信名の設定 590
Compute Managerを設定する 590
クラスタを設定する 590
データストアの設定 590
ネットワークを設定する 591
配置仕様の設定 591
サービスセグメントの設定 592
配置テンプレートを設定する 593
配信を監視および確認する 593
NSX-T 3.xの配置を監視する 594
vSphere Clientでの配置を監視する 594
Deep Security Managerでの配置を確認する 594
クラスタごとにすべての手順を繰り返します。 595
グループを作成して保護する 595
東西のセキュリティを設定する 597
サービスプロファイルを追加する 597
サービスチェーンを追加する 598
ネットワークイントロスペクションポリシーを追加する 599
VMを論理スイッチに接続する 600
Endpoint Protectionの設定 601
アクティベーションの設定 603
アクティベーションの準備 603
方法1:作成された「コンピュータ作成済み」イベントベースのタスク 604
方法2:「NSX Security Group Change」イベントベースのタスクを作成する 606
方法3:Deep SecurityポリシーをNSX-T 3.xと同期する 608

アクティベーションおよびポリシーの割り当ての実行 610
VMがアクティベートされ、ポリシーが割り当てられていることを確認する 610
次の手順 (新しい仮想マシンを追加する方法) 610
Applianceのインストール (NSX-V) 611
手順1: Deep Security Managerにアプライアンスパッケージをインポートします。 612
手順2: Deep Security ManagerにvCenterを追加する 612
手順3: ESXiサーバの準備 613
手順4: Guest Introspectionをインストールする 614
手順5: Deep Security Virtual ApplianceをNSX-Vにインストールする 618
手順6: NSXセキュリティグループとポリシーを作成する 619
手順7: NSX-Vで有効化を準備する 627
方法1:「コンピュータの作成」イベントベースタスクを作成する 629
方法2:「NSXセキュリティグループの変更」イベントベースタスクを作成する 630
方法3: Deep SecurityポリシーをNSX-Vと同期する 632
手順8: 有効化とポリシーの割り当てを開始する 634
手順9: 仮想マシンが有効化されて、ポリシーが割り当てられていることを確認する 634
次の手順 (新しい仮想マシンを追加する方法) 634
vCloud環境にアプライアンスを配信する 635
開始前の準備 635
vCloud仮想マシンのAgentレスによる保護を有効にする 636
マルチテナント環境を作成する 636
vCenterを追加してDeep Security Virtual Applianceを配置する 636
Deep SecurityでVMware vCloudリソースを使用できるように設定する 636
vCloudアカウントのテナントユーザ向けの最小権限のロールを作成する 636
新しい仮想マシンに一意のUUIDを割り当てる 637
ゲスト仮想マシンでVMware Toolsの [OVF Environment Transport] を有効にする 637
仮想マシンでVirtual Appliance保護を有効にする 638
VMware vCloud Organizationアカウントからコンピュータをインポートする 638
VMware vCloud Air仮想データセンターからコンピュータをインポートする 638

仮想マシンでVirtual Appliance保護を有効にする 639
NSX環境での自動ポリシー管理 639
「NSXセキュリティグループの変更」イベントベースタスク 640
タスクを実行する条件 641
実行可能な処理 642
vCenterがDeep Security Managerに追加されたときに作成されるイベントベースタスク 642
Deep Security ManagerからvCenterを削除する 643
Deep SecurityポリシーのNSXとの同期 644
DPDKモードを設定する 645
NSXセキュリティタグの設定 647
NSXセキュリティタグを適用するように不正プログラム対策を設定する 648
NSXセキュリティタグを適用するように侵入防御を設定する 649
アプライアンスのOVFの場所を設定する 650
Deep Security Virtual Applianceのメモリ割り当て 651
vCenterに配置する前にApplianceのメモリ割り当てを設定する 652
配置済みのApplianceのメモリ割り当てを設定する 653
アプライアンスを起動または停止する 653
Deep Security Notifierを配信する 654
インストールパッケージをコピーする 654
Windows版Deep Security Notifierをインストールする 654
管理者ガイド 655
コンピュータの追加 655
コンピュータの追加について 655
Managerにコンピュータを追加する 655
コンピュータのグループ化 655
コンピュータリストをエクスポートする 656
コンピュータを削除する 656
ローカルネットワークコンピュータの追加 656
Agentからのリモート有効化 656

コンピュータを手動で追加する 657
コンピュータを検出する 658
Active Directoryコンピュータを追加する 659
Active Directoryのその他のオプション 660
ディレクトリの削除 660
今すぐ同期 661
サーバ証明書を使用する 661
ユーザおよび連絡先をインポートする 661
Active Directoryオブジェクトの同期を維持する 662
Active Directoryとの同期を無効にする 663
Active Directoryとの同期からコンピュータグループを削除する 663
Active Directoryのユーザおよび連絡先を削除する 663
AWSインスタンスを追加する 664
AWSアカウントの追加について 664
AWSアカウントを追加する方法の概要 664
AWSアカウントを追加するとどうなりますか? 664
AWSアカウントを追加することのメリットは何ですか? 665
サポートされるAWSリージョン 665
マネージャーのインスタンスの役割を使用したAWSアカウントの追加 666
アクセスキーを使用してAWSアカウントを追加する 669
クロスアカウントロールを使用したAWSアカウントの追加 672
APIを使用してアカウントを追加する 677
Amazon WorkSpacesの追加 677
Amazon WorkSpacesを保護する(AWSアカウントをすでに追加している場合) 677
Amazon WorkSpacesを保護する(AWSアカウントをまだ追加していない場合) 678
AWSアカウントの管理 678
AWSアカウントの編集 679
AWSアカウントを削除する 679
AWSアカウントを同期する 679

AWSアカウントの外部IDを管理する 679
外部IDとは何ですか。 680
外部IDを設定する 680
外部IDを更新する 680
外部IDを取得する 682
外部IDの取得を無効にする 682
AWSリージョンの管理 683
Amazon Web Servicesのリージョンを追加する 683
Amazon Web Servicesのリージョンを表示する 683
Amazon Web Servicesのリージョンを削除する 684
AWS Outpostsで実行されているアカウントを保護する 684
Azureインスタンスを追加する 685
Deep Security用のAzureアプリケーションの作成 685
適切な役割を割り当てる 685
Azureアプリケーションを作成する 685
AzureアプリIDとActive Directory IDを記録する 686
アプリケーションシークレットを作成するか、アプリケーション証明書をアップロードします。 686
オプション1: クライアントシークレットを作成する(アプリケーションパスワード) 686
オプション2: アプリケーション証明書をアップロードする 687
サブスクリプションIDを記録する 687
Azureアプリケーションに役割とコネクタを割り当てる 687
Deep SecurityへのMicrosoft Azureアカウントの追加 688
Azureアカウントを追加することのメリットは何ですか? 688
Azureアカウントのプロキシを設定する 689
Microsoft AzureアカウントからDeep Securityに仮想マシンを追加する 689
Azure Resource Managerコネクタを使用してAzureクラシック仮想マシンを管理する 690
Azureアカウントを削除する 690
Azureアカウントを同期する 691
新しいAzure Resource Manager接続機能へのアップグレードについて 691

GCPインスタンスを追加する 692
Google Cloud Platformサービスアカウントを作成する 692
前提条件:Google APIを有効にする 692
GCPサービスアカウントを作成する 693
GCPサービスアカウントにプロジェクトを追加する 697
複数のGCPサービスアカウントを作成する 700
Google Cloud Platformアカウントを追加する 700
GCPアカウントを追加するとどのようなメリットがありますか? 701
GCPアカウントのプロキシ設定を行う 701
Deep SecurityにGCPアカウントを追加する 701
GCPアカウントを削除する 703
GCPアカウントを同期する 704
VMWare VMの追加 704
VMware vCenterの追加 704
vCenterの追加 705
vCenterのユーザアカウントの仕様 705
NSXユーザーアカウントの仕様 708
複数のvCenterを追加する 709
vCenter - FIPSモードを追加する 709
VMware vCloudでホストされる仮想マシンの追加 710
vCloudアカウントを追加することのメリットは何ですか。 711
クラウドアカウント用のプロキシ設定 711
Manager用のVMware vCloud Organizationアカウントを作成する 711
VMware vCloud Organizationアカウントからコンピュータをインポートする 712
VMware vCloud Airデータセンターからコンピュータをインポートする 712
クラウドアカウントのソフトウェアアップデートを設定する 713
クラウドアカウントを削除する 713
NSX ManagerのIPアドレスまたはFQDNの変更 714
保護されたNSXクラスタへのESXiの追加 714

CPU使用率を制御する ... 715
新しいクラウドコネクタ機能への移行 ... 715
Dockerコンテナの保護 ... 717
Deep SecurityによるDockerホストの保護 ... 718
Deep SecurityによるDockerコンテナの保護 ... 718
侵入防御の推奨検索に関する制限事項 ... 718
OpenShiftコンテナの保護 ... 718
OpenShiftホストのDeep Securityによる保護 ... 719
OpenShiftコンテナのDeep Securityによる保護 ... 719
ポリシーを設定する ... 719
ポリシーの作成 ... 719
新規ポリシーを作成する ... 720
ポリシーを作成するその他の方法 ... 721
ポリシーまたは個々のコンピュータの設定を編集する ... 721
ポリシーをコンピュータに割り当てる ... 722
ポリシーの自動アップデートを無効にする ... 722
ポリシーの変更を手動で送信する ... 723
ポリシーをエクスポートする ... 723
ポリシー、継承、およびオーバーライド ... 724
継承 ... 725
オーバーライド ... 726
オブジェクトのプロパティをオーバーライドする ... 727
ルールの割り当てをオーバーライドする ... 727
コンピュータまたはポリシーのオーバーライド項目をまとめて確認する ... 727
推奨設定の検索の管理と実行 ... 728
検索内容 ... 729
検索の制限 ... 730
Adobe Readerルールの推奨事項 ... 731
推奨設定の検索を実行する ... 731

予約タスクを作成して定期的に推奨設定の検索を実行する 732
継続検索を設定する 733
推奨設定の検索を手動で実行する 733
推奨設定の検索をキャンセルする 733
推奨設定の検索からルールまたはアプリケーションの種類を除外する 733
推奨設定を自動的に適用する 734
検索結果を確認して手動でルールを割り当てる 735
推奨ルールを設定する 736
一般的な脆弱性の追加ルールを実装する 736
トラブルシューティング: 推奨設定の検索失敗 738
通信 738
サーバリソース 738
タイムアウト値 738
コンピュータで使用可能なインタフェースの検出と設定 739
複数のインタフェースに対してポリシーを設定する 739
インタフェース制限を強制する 740
コンピュータエディタの [概要] セクション 740
[一般] タブ 740
コンピュータのステータス 742
保護モジュールのステータス 742
VMware仮想マシンの概要 743
[処理] タブ 744
有効化 744
ポリシー 744
Agentソフトウェア 744
サポート情報 745
[TPM] タブ 745
[システムイベント] タブ 746
[除外] タブ 746

USBデバイスの除外ルール数制限 746
ポリシーエディタの [概要] セクション 746
[一般] タブ 746
一般 746
継承 746
モジュール 747
[このポリシーを使用しているコンピュータ] タブ 747
[イベント] タブ 747
[除外] タブ 747
USBデバイス除外ルール数の制限 747
ネットワークエンジン設定 747
ユーザーモードソリューション 758
利用可能なモード 758
システム保護のためのドライバーの使用 759
サポートされているエージェント 759
ポリシーのルール、リスト、およびその他の共通オブジェクトの定義 761
共通オブジェクトについて 761
ルール 761
リスト 761
その他 762
ファイアウォールルールの作成 762
新しいルールを追加する 762
ルールの動作とプロトコルを選択する 763
パケットの送信元と送信先を選択する 765
ルールイベントとアラートを設定する 766
アラート 767
ルールのスケジュールを設定する 767
ルールにコンテキストを割り当てる 767
ルールが割り当てられているポリシーとコンピュータを確認する 767

ルールをエクスポートする 767
ルールを削除する 768
侵入防御ルールの設定 768
侵入防御ルールのリストを表示する 768
侵入防御ルールに関する情報を表示する 769
一般情報 769
詳細 769
侵入防御ルールのリストを表示する 769
一般情報 770
ID (トレンドマイクロのルールのみ) 770
関連付けられている脆弱性に関する情報を表示する (トレンドマイクロのルールのみ) 770
ルールを割り当てる/ルールの割り当てを解除する 771
アップデートされた必須ルールを自動割り当てする 771
ルールにイベントログを設定する 772
アラートを生成する 773
設定オプションを設定する (トレンドマイクロのルールのみ) 773
有効な時間を予約する 774
推奨設定から除外する 774
ルールのコンテキストを設定する 774
ルールの動作モードをオーバーライドする 775
ルールおよびアプリケーションの種類の設定をオーバーライドする 775
ルールをエクスポート/インポートする 776
変更監視 ルールの作成 776
新しいルールを追加する 777
変更監視ルール情報を入力する 777
ルールテンプレートを選択し、ルールの属性を定義する 778
レジストリ値テンプレート 778
ファイルテンプレート 778
カスタム (XML) テンプレート 779

トレンドマイクロが発行する変更監視ルールを設定する 779
ルールイベントとアラートを設定する 780
リアルタイムのイベント監視 780
アラート 780
ルールが割り当てられているポリシーとコンピュータを確認する 780
ルールをエクスポートする 780
ルールを削除する 780
ポリシーで使用するセキュリティログ監視 ルールを定義する 781
新しい セキュリティログ監視 ルールを作成します。 781
デコーダ 783
サブルール 784
グループ 784
ルール、ID、およびレベル 785
説明 786
デコード形式 786
一致項目 787
条件文 788
評価の階層 788
ログエントリのサイズに関する制限 789
コンポジットルール 790
例 791
セキュリティログ監視 ルールの重大度レベルと推奨される使用 797
strftime () 変換指定子 799
セキュリティログ監視 ルールを調べる 799
セキュリティログ監視 のルール構造とイベント照合プロセス 800
重複するサブルール 803
ポリシーで使用するディレクトリリストの作成 804
ディレクトリリストをインポート/エクスポートする 806
ディレクトリリストを使用するポリシーを表示 806

ポリシーで使用するファイル拡張子リストの作成 807
ファイル拡張子リストをインポート/エクスポートする 807
ファイル拡張子リストを使用する不正プログラム検索設定を確認する 807
ポリシーで使用するファイルリストの作成 808
ファイルリストをインポート/エクスポートする 810
ファイルリストを使用するポリシーを確認する 811
ポリシーで使用するIPアドレスリストの作成 811
IPリストをインポート/エクスポートする 811
IPリストを使用するルールを確認する 812
ポリシーで使用するポートリストの作成 812
ポートリストをインポート/エクスポートする 812
ポートリストを使用するルールを確認する 813
ポリシーで使用するMACアドレスリストの作成 813
MACリストをインポート/エクスポートする 813
MACリストを使用するポリシーを確認する 814
ポリシーで使用するコンテキストの定義 814
コンピュータがインターネットに接続されているかどうかを判別するオプションを設定する 814
コンテキストを定義する 815
ステートフルファイアウォールの設定の定義 815
ステートフル設定を追加する 816
ステートフル設定情報を入力する 816
パケットインスペクションオプションを選択する 816
IPパケットインスペクション 816
TCPパケットインスペクション 817
FTPオプション 818
UDPパケットインスペクション 819
ICMPパケットインスペクション 819
ステートフル設定をエクスポートする 820
ステートフル設定を削除する 820

ステートフル設定が割り当てられたポリシーとコンピュータを表示する 820
ルールに適用するスケジュールの定義 820
保護モジュールの設定 821
不正プログラム対策を設定する 821
不正プログラム対策について 821
不正プログラム検索の種類 822
リアルタイム検索 822
手動検索 822
予約検索 823
クイック検索 823
検索されるオブジェクトと順序 823
不正プログラム検索設定 824
不正プログラムイベント 824
スマートスキャン 824
機械学習型検索 825
脅威インテリジェンス 825
不正プログラムの種類 826
ウイルス 826
トロイの木馬 826
パッカー 827
スパイウェア/グレーウェア 827
Cookie 828
その他の脅威 828
潜在的な不正プログラム 828
不正プログラム対策を設定する 828
不正プログラム対策を有効化して設定する 828
不正プログラム対策モジュールを有効にする 829
実行するスキャンの種類を選択 829
検索除外を設定する 830

複数の検索リストの除外と含める設定 830
最新の脅威についてDeep Securityを更新する 831
不正プログラム検索と除外の設定 832
不正プログラム検索設定を作成または変更する 833
不正プログラム検索をテストする 834
特定の種類の不正プログラムを検索する 835
Windows AMSI保護を有効にする(リアルタイム検索のみ) 835
スパイウェア/グレーウェアを検索する 835
圧縮済み実行可能ファイルを検索する(リアルタイム検索のみ) 836
プロセスメモリを検索する 836
圧縮ファイルを検索する 836
埋め込みのMicrosoft Officeオブジェクトを検索する 837
Windows OSでNotifierの手動検索を有効にする 837
Linux OSでの手動検索の有効化 837
検索対象ファイルを指定する 838
検索対象 838
検索除外 839
除外するパターンのリストを作成して、ディレクトリ、ファイル、およびプロセスイメージファイルを除外する 839
ファイル除外のテスト 840
ディレクトリリストの構文 840
ファイルリストの構文 842
ファイル拡張子リストの構文 844
プロセスイメージファイルリストの構文 844
ネットワークディレクトリを検索する(リアルタイム検索のみ) 846
リアルタイム検索を実行するタイミングを指定する 846
不正プログラムの処理を設定する 846
不正プログラム修復処理をカスタマイズする 847
トレンドマイクロの推奨処理 848

不正プログラム検出のアラートを生成する 849
NSXセキュリティタグを適用する 849
ファイルのハッシュダイジェストにより不正プログラムファイルを特定する 849
コンピュータで通知を設定する 850
不正プログラム対策のパフォーマンスを向上させる 850
ディスク使用量を最小限に抑える 851
CPU使用率を最適化する 851
マルチスレッド処理を有効にする 852
RAM使用率を最適化する 853
Deep Security AgentとMicrosoft Defender ウイルス対策の共存 854
DSAの除外リストのMicrosoft Defenderウイルス対策アプリケーションファイル 855
Microsoft Defenderウイルス対策除外リストのDSAフォルダとプロセス 855
改ざん防止 856
Microsoft Defender Antivirus エンドポイント検出と応答 (EDR) のブロックモード 856
Virtual Applianceの検索キャッシュ 856
検索キャッシュ設定 857
不正プログラム検索のキャッシュ設定 858
変更監視の検索のキャッシュ設定 858
検索キャッシュの管理設定 858
初期設定を変更する場合の考慮事項 859
機械学習型検索を使用した脅威の検出 859
インターネットに接続されていることを確認する 860
機械学習型検索を有効にする 860
脅威インテリジェンスを使用した新たな脅威の検出 861
脅威インテリジェンスの仕組み 862
脅威インテリジェンスの前提条件を確認する 863
Trend Micro Vision Oneへの接続を設定する 863
Deep Discovery Analyzerへの接続を設定する 864
Trend Micro Apex Centralへの接続の設定 866

脅威インテリジェンスで使用する不正プログラム検索設定を作成する 868
コンピュータで脅威インテリジェンスを有効にする 869
サンドボックス分析にファイルを手動で送信する 869
誤ったアラームを引き起こしたファイルを許可する 869
不審なファイルに対する検索処理を設定する 870
Deep Securityで不審オブジェクトリストをアップデートする 870
マルチテナント環境での脅威インテリジェンスの設定 871
サポートされているファイルタイプ 871
Connected Threat Defense から脅威インテリジェンスへの移行 872
マルチテナントの移行 873
挙動監視による不正プログラム/ランサムウェア検索の強化 873
強化された検索保護 874
強化された検索を有効にする 875
強化スキャンで検出された問題に対処する 876
Agentをインターネットに直接接続できない場合の対処 881
Deep SecurityのSmart Protection 881
不正プログラム対策とSmart Protection 881
スマートスキャンの利点 881
スマートスキャンを有効にする 882
ファイルレピュテーションサービス用のSmart Protection Server 883
Webレピュテーションと Smart Protection 883
スマートフィードバック 884
不正プログラムの処理 884
検出した不正プログラムの確認と復元 884
検出ファイルのリストを参照する 885
検出ファイルを処理する 886
検出ファイルを検索する 887
検出ファイルを復元する 888
ファイルの検索除外を作成する 888

ファイルを復元する 891
検出ファイルを手動で復元する 891
高度な攻撃コードの除外を設定する 891
不正プログラム対策イベントから例外を作成する 892
不正プログラム対策の例外を手動で作成する 892
除外リストのワイルドカードのサポート 893
スパイウェア/グレーウェアの例外の処理方法 895
検索除外の推奨設定 896
信頼された証明書で署名されたファイルを除外する 896
保護対象のLinuxインスタンスにおける不正プログラム対策のデバッグログレベルの引き上げ 897
Webレピュテーションを設定する 898
Webレピュテーションモジュールを有効にする 898
Trend ツールバーを有効にする 899
Windows用ツールバーをインストールする 899
インラインモードとタップモードを切り替える 899
セキュリティレベルを適用する 900
セキュリティレベルを設定するには、次の手順に従います。 900
例外設定を作成する 901
URL例外設定を作成するには、次の手順に従います。 901
Smart Protection Serverを設定する 902
Smart Protection Serverへの接続の警告 903
詳細設定を編集する 903
ブロックページ 903
アラート 903
ポート 903
Webレピュテーションをテストする 903
侵入防御(IPS)を設定する 904
侵入防御 904

侵入防御 ルール 904
アプリケーションの種類 905
ルールアップデート 905
推奨設定の検索 905
動作モードを使用してルールをテストする 905
ルールの動作モードをオーバーライドする 906
侵入防御 イベント 907
安全な接続のサポート 907
コンテキスト 907
インタフェースのタグ付け 908
侵入防御の設定 908
検出モードで侵入防御 を有効にする 908
侵入防御のテスト侵入防御 910
推奨ルールを適用する 911
システムを監視する 912
システムパフォーマンスを監視する 912
侵入防御イベントを確認する 913
パケットまたはシステムのエラーに対して「Fail-Open」を有効にする 913
予防モードに切り替える 913
個々のルールについてのベストプラクティスを実装する 913
HTTPプロトコルデコードルール 913
クロスサイトスクリプティングルールと汎用的なSQLインジェクションルール 914
NSXセキュリティタグを適用する 914
侵入防御ルールの設定 914
侵入防御ルールのリストを表示する 915
侵入防御ルールに関する情報を表示する 915
一般情報 916
詳細 916
侵入防御ルールのリストを表示する 916

一般情報 917
ID (トレンドマイクロのルールのみ) 917
関連付けられている脆弱性に関する情報を表示する(トレンドマイクロのルールのみ) 917
ルールを割り当てる/ルールの割り当てを解除する 918
アップデートされた必須ルールを自動割り当てする 918
ルールにイベントログを設定する 919
アラートを生成する 920
設定オプションを設定する(トレンドマイクロのルールのみ) 920
有効な時間を予約する 920
推奨設定から除外する 921
ルールのコンテキストを設定する 921
ルールの動作モードをオーバーライドする 922
ルールおよびアプリケーションの種類の設定をオーバーライドする 922
ルールをエクスポート/インポートする 923
SQLインジェクション防御ルールの設定 923
SQLインジェクション攻撃とは 924
SQLインジェクション攻撃に共通する文字および文字列 924
Generic SQL Injection Preventionルールの仕組み 926
ルールおよび評価システムの実例 928
例1: トラフィックのログ記録と破棄が発生 928
例2: トラフィックのログ/破棄が発生しない 929
Generic SQL Injection Preventionルールを設定する 930
文字エンコードのガイドライン 933
アプリケーションの種類 935
アプリケーションの種類のリストを表示する 935
一般情報 935
接続 936
設定 936
オプション 936

割り当て対象 ... 936
TLSトラフィックの検査 ... 936
高度なTLSトラフィック検査の有効化 ... 937
受信トラフィックと送信トラフィックに高度なTLSトラフィック検査を使用する ... 937
SSLインスペクションを設定する(レガシー) ... 938
ポート設定を変更する ... 939
トラフィックがPerfect Forward Secrecy (PFS)で暗号化されている場合に侵入防御を使用する ... 939
SSL Inspectionを使用する場合のDiffie-Hellman暗号に関する特別な考慮事項 ... 940
サポートされている暗号化スイート ... 941
サポートされているプロトコル ... 947
TLSインスペクションのサポート ... 947
TLS検査サポートパッケージのアップデートの管理 ... 947
1つのエージェントでTLS検査サポートパッケージのアップデートを無効にする ... 947
ポリシーによるTLS検査サポートパッケージのアップデートの無効化 ... 948
回避技術対策の設定 ... 948
侵入防御のパフォーマンスに関するヒント ... 951
設定パッケージの最大サイズ ... 952
ファイアウォール設定 ... 953
ファイアウォールについて ... 953
ファイアウォールルール ... 953
Deep Securityファイアウォールの設定 ... 954
ファイアウォールルールを配信前にテストする ... 955
タップモードでテストする ... 955
インラインモードでテストする ... 956
「Fail-Open」の動作を有効にする ... 957
ファイアウォールをオンにする ... 958
初期設定のファイアウォールルール ... 958
デフォルトのバイパスルール(Deep Security Managerトラフィック用) ... 959

厳格または寛容なファイアウォール設計 960
厳格なファイアウォール 960
寛容なファイアウォール 960
ファイアウォールルールの処理 960
ファイアウォールルールの優先度 961
許可ルール 962
強制的に許可ルール 962
バイパスルール 962
推奨されるファイアウォールポリシールール 962
ファイアウォールルールをテストする 963
攻撃の予兆検索 964
ステートフルインスペクション 965
例 965
重要事項 966
ファイアウォールルールの作成 967
新しいルールを追加する 968
ルールの動作とプロトコルを選択する 968
パケットの送信元と送信先を選択する 971
ルールイベントとアラートを設定する 972
アラート 972
ルールのスケジュールを設定する 972
ルールにコンテキストを割り当てる 972
ルールが割り当てられているポリシーとコンピュータを確認する 973
ルールをエクスポートする 973
ルールを削除する 973
信頼済みトラフィックに対するファイアウォールのバイパス許可 973
信頼済みトラフィックのソースの新しいIPリストを作成する 974
IPリストを使用して信頼済みトラフィックの受信用と送信用のファイアウォールルールを作成する 974

信頼済みトラフィックが通過するコンピュータで使用されているポリシーにファイアウォールルールを割り当てる ... 974
ファイアウォールルールの処理と優先度 ... 975
ファイアウォールルールの処理 ... 975
許可ルールの詳細 ... 975
バイパスルールの詳細 ... 976
Deep Security Managerのトラフィックに関するバイパスルールの初期設定 ... 976
強制的に許可ルールの詳細 ... 977
ファイアウォールルールのシーケンス ... 977
ログに関する注意 ... 979
各ファイアウォールルールの関係 ... 979
ルール処理 ... 979
ルール優先度 ... 981
ルール処理およびルール優先度を集約する ... 981
ファイアウォールの設定 ... 982
一般 ... 982
ファイアウォール ... 982
ファイアウォールステートフル設定 ... 982
ポート検索 (コンピュータエディタのみ) ... 983
割り当てられたファイアウォールルール ... 983
インタフェース制限 ... 983
インタフェース制限 ... 984
インタフェースパターン ... 984
攻撃の予兆 ... 984
攻撃の予兆検索 ... 985
詳細 ... 987
イベント ... 987
ファイアウォールイベント ... 987
Oracle RACでのファイアウォール設定 ... 987

ノード間の接続を許可するルールを追加する 988
UDPポート42424を許可するルールを追加する 988
その他のRAC関連パケットを許可する 990
Oracle SQL Serverルールが割り当てられていることを確認する 992
回避技術対策の設定が「標準」に設定されていることを確認する 992
ステートフルファイアウォールの設定の定義 993
ステートフル設定を追加する 994
ステートフル設定情報を入力する 994
パケットインスペクションオプションを選択する 994
IPパケットインスペクション 994
TCPパケットインスペクション 995
FTPオプション 996
UDPパケットインスペクション 996
ICMPパケットインスペクション 997
ステートフル設定をエクスポートする 998
ステートフル設定を削除する 998
ステートフル設定が割り当てられたポリシーとコンピュータを表示する 998
オープンポートの検索 998
コンテナのファイアウォールルール 999
Kubernetesファイアウォールルール 999
Swarmファイアウォールルール 1000
デバイスコントロールの設定 1001
デバイスコントロールについて 1001
デバイスコントロールプロトコル 1001
デバイスの種類に対する処理 1001
USB自動実行 1002
デバイスコントロールの設定 1002
プロトコルの設定 1002
USBデバイスの例外を設定 1003

新しいデバイスを作成 1003
既存のデバイスの選択 1003
デバイスコントロールイベントのタグ付け 1003
ムーブ監視の設定 1004
変更監視 1004
変更監視の設定 1004
変更監視を有効にする 1005
推奨設定の検索を実行する 1006
変更監視ルールを適用する 1007
コンピュータのベースラインを構築する 1009
定期的に変更をスキャンする 1009
テスト変更監視 1009
変更監視スキャンの種類 1010
変更監視検索パフォーマンスの設定 1011
CPUの使用率を制限する 1011
コンテンツハッシュアルゴリズムを変更する 1011
仮想マシンの検索キャッシュ設定を有効にする 1012
変更監視イベントのタグ付け 1012
変更監視 ルールの作成 1012
新しいルールを追加する 1013
変更監視ルール情報を入力する 1013
ルールテンプレートを選択し、ルールの属性を定義する 1014
レジストリ値テンプレート 1014
ファイルテンプレート 1014
カスタム (XML) テンプレート 1015
トレンドマイクロが発行する変更監視ルールを設定する 1015
ルールイベントとアラートを設定する 1016
リアルタイムのイベント監視 1016
アラート 1016

ルールが割り当てられているポリシーとコンピュータを確認する 1016
ルールをエクスポートする 1016
ルールを削除する 1016
変更監視ルールのインポート 1017
変更監視 rules languages 1017
エンティティセット 1018
階層とワイルドカード 1018
構文とコンセプト 1019
includeタグ 1020
excludeタグ 1021
大文字/小文字の区別 1022
エンティティ機能 1022
ANDとOR 1024
評価の順序 1025
エンティティ属性 1025
簡略記法属性 1026
onChange属性 1027
環境変数 1027
環境変数のオーバーライド 1028
レジストリ値 1028
「..」の使用 1029
ベストプラクティス 1029
DirectorySet 1030
タグ属性 1030
エンティティセットの属性 1031
簡略記法による属性 1032
「key」の意味 1032
サブエレメント 1032
FileSet 1032

タグ属性 1033
エンティティセットの属性 1034
簡略記法による属性 1035
ディレクトリとしてマウントされたドライブ 1035
代替データストリーム 1035
「key」の意味 1036
サブエレメント 1037
FileSetのincludeおよびexcludeに固有の属性 1037
GroupSet 1037
タグ属性 1037
エンティティセットの属性 1038
簡略記法による属性 1038
「key」の意味 1038
includeとexclude 1038
InstalledSoftwareSet 1038
タグ属性 1039
エンティティセットの属性 1039
簡略記法による属性 1040
「key」の意味 1040
サブエレメント 1040
InstalledSoftwareSetsのincludeおよびexcludeに固有の属性 1040
PortSet 1041
タグ属性 1041
エンティティセットの属性 1041
「key」の意味 1042
IPV6 1042
「key」の照合 1043
サブエレメント 1043
PortSetのincludeおよびexcludeに固有の属性 1043

ProcessSet 1044
タグ属性 1045
エンティティセットの属性 1045
簡略記法による属性 1046
「key」の意味 1046
サブエレメント 1046
ProcessSetsのincludeおよびexcludeに固有の属性 1046
RegistryKeySet 1047
タグ属性 1048
エンティティセットの属性 1048
簡略記法による属性 1048
「key」の意味 1048
サブエレメント 1049
RegistryValueSet 1049
タグ属性 1049
エンティティセットの属性 1049
簡略記法による属性 1050
「key」の意味 1050
初期設定値 1050
サブエレメント 1051
ServiceSet 1051
タグ属性 1051
エンティティセットの属性 1052
簡略記法による属性 1053
「key」の意味 1053
サブエレメント 1053
ServiceSetのincludeおよびexcludeに固有の属性 1053
UserSet 1054
タグ属性 1054

エンティティセットの属性 1054
一般属性 1054
Windowsのみの属性 1055
Linux、AIX、およびSolarisの属性 1055
簡略記法による属性 1056
「key」の意味 1056
サブエレメント 1057
includeとexclude 1057
UserSetのincludeおよびexcludeに固有の属性 1057
WQLSet 1057
エンティティセットの属性 1059
「key」の意味 1061
include/exclude 1061
Virtual Applianceの検索キャッシュ 1062
検索キャッシュ設定 1062
不正プログラム検索のキャッシュ設定 1063
変更監視の検索のキャッシュ設定 1064
検索キャッシュの管理設定 1064
初期設定を変更する場合の考慮事項 1064
ログ検査の設定 1065
セキュリティログ監視 1065
セキュリティログ監視 1066
セキュリティログ監視モジュールをオンにする 1066
推奨設定の検索を実行する 1066
推奨されるセキュリティログ監視ルールを適用する 1067
セキュリティログ監視をテストする 1068
セキュリティログ監視イベントの転送と保存を設定する 1069
ポリシーで使用するセキュリティログ監視 ルールを定義する 1070
新しいセキュリティログ監視 ルールを作成します。 1071

デコーダ 1072
サブルール 1074
グループ 1074
ルール、ID、およびレベル 1074
説明 1076
デコード形式 1076
一致項目 1076
条件文 1077
評価の階層 1077
ログエントリのサイズに関する制限 1078
コンポジットルール 1079
例 1080
セキュリティログ監視 ルールの重大度レベルと推奨される使用 1086
strftime () 変換指定子 1088
セキュリティログ監視 ルールを調べる 1088
セキュリティログ監視 のルール構造とイベント照合プロセス 1089
重複するサブルール 1092
アプリケーションコントロールを設定する 1093
アプリケーションコントロール 1093
主な概念 1093
アプリケーションコントロールの仕組み 1094
アプリケーションコントロールインタフェースの紹介 1096
アプリケーションコントロール: ソフトウェア変更 ([処理]) 1096
アプリケーションコントロールルールセット 1097
セキュリティイベント 1098
アプリケーションコントロールで検出されるソフトウェア変更 1098
Deep Security Agent 10と11におけるファイルの比較方法の相違点 1099
アプリケーションコントロールの設定 1099
アプリケーションコントロールを有効にする 1100

新規および変更済みソフトウェアを監視する 1101
変更の処理のヒント 1103
変更の計画時にメンテナンスモードをオンにする 1104
アプリケーションコントロールのヒントと注意事項 1105
アプリケーションコントロールが有効であることを確認します 1106
アプリケーションコントロールイベントの監視 1107
ログに記録するアプリケーションコントロールイベントを選択する 1108
アプリケーションコントロールイベントログを表示する 1108
集約されたセキュリティイベントを解釈する 1108
アプリケーションコントロールアラートを監視する 1109
アプリケーションコントロールルールセットの表示と変更 1110
アプリケーションコントロールルールセットを表示する 1111
セキュリティイベント 1112
アプリケーションコントロールルールの処理を変更する 1113
個々のアプリケーションコントロールルールを削除する 1114
アプリケーションコントロールルールセットを削除する 1114
アプリケーションコントロールの信頼エンティティ 1114
信頼ルールセット 1115
信頼ルールセットを作成する 1115
信頼ルールセットの割り当てまたは割り当て解除 1117
信頼ルールセットを削除する 1119
信頼ルール 1120
信頼ルールの種類 1120
信頼ルールを作成する 1121
信頼ルールのプロパティを変更する 1123
信頼ルールを削除する 1125
信頼ルールのプロパティの種類 1125
プロセス名 1126
パス 1126

SHA-256 1127
ベンダ 1127
製品名 1128
署名者名 1128
発行者の一般名 1129
発行者の組織単位 1129
発行者の組織 1129
発行者の地域 1130
発行者の都道府県 1130
発行国 1131
アプリケーションコントロールイベントの集約と分析 1131
ドリフトイベント 1131
ドリフトイベントの信頼ルール 1132
セキュリティイベント 1134
セキュリティイベントの信頼ルール 1135
イベント分析出力 1136
信頼ルールのデバッグ 1138
コンサルト指標 1138
署名者情報の表示 1141
Linuxの信頼ルールプロパティの制限 1141
ソフトウェアの変更後にアプリケーションコントロールをリセットする 1141
共有ルールセットとグローバルルールセットを作成するためのAPIの使用 1142
共有ルールセットを作成する 1145
共有許可およびブロックルールからコンピュータ固有の許可およびブロックルールに切り替える 1146
Relayを介してアプリケーションコントロール共有ルールセットをインストールする 1147
単一テナント環境 1147
マルチテナント環境 1148
共有ルールセットを使用するリレーを使用する場合の考慮事項 1149

イベントとアラートを設定する 1150
Deep Securityイベントログについて 1150
Agentでのイベントログの場所 1150
イベントがManagerに送信されるタイミング 1150
イベントが保持される期間 1151
システムイベント 1151
セキュリティイベント 1151
ポリシーまたはコンピュータに関連付けられたイベントを確認する 1152
イベントの詳細を表示する 1152
リストをフィルタしてイベントを検索する 1153
イベントをエクスポートする 1153
ログのパフォーマンスを向上する 1154
ログとイベントの保存に関するベストプラクティス 1154
トラブルシューティング 1156
ログファイルのサイズを制限する 1156
イベントログのヒント 1158
不正プログラム対策 検索の失敗とキャンセル 1158
不正プログラム対策 検索失敗イベント 1158
不正プログラム対策 検索キャンセルイベント 1160
イベントを識別およびグループ化するためのタグの適用 1161
手動によるタグ付け 1162
自動タグ付け 1162
自動タグ付けルールに優先度を設定する 1163
セキュリティログ監視イベントを自動でタグ付けする 1163
信頼済みのソースを使用したタグ付け 1164
信頼済みのローカルコンピュータ 1165
イベントマッチングアルゴリズム 1165
信頼済みのローカルコンピュータに基づいてイベントにタグを付ける 1165
トレンドマイクロのソフトウェア安全性評価サービスに基づいてイベントにタグを付ける 1166

信頼済みの共通ベースラインに基づいてイベントにタグを付ける 1166
タグを削除する 1167
ログに記録するイベントの数を減らす 1167
イベントのランク付けによる重要度の数値化 1169
Webレピュテーション イベントリスク値 1170
ファイアウォールルールの重要度の値 1170
侵入防御 ルールの重要度の値 1170
変更監視 ルールの重大度の値 1170
セキュリティログ監視 ルール重大度の値 1171
資産評価 1171
イベントをSyslogサーバまたはSIEMサーバに転送する 1171
Deep SecurityイベントをSyslogまたはSIEMサーバに転送する 1171
イベント転送ネットワークトラフィックを許可する 1172
クライアント証明書を要求する 1172
Syslog設定の定義 1172
システムイベントを転送する 1175
セキュリティイベントを転送する 1175
イベント転送のトラブルシューティング 1176
Syslogメッセージ送信失敗アラート 1176
Syslog設定を編集できません 1176
Deep Security ManagerのSyslog設定セクションが表示されません。 1176
証明書が期限切れのためにSyslogが転送されない 1177
サーバ証明書が期限切れであるか変更されたためにSyslogが配信されない 1177
互換性 1177
syslogメッセージの形式 1177
CEFのsyslogメッセージの形式 1178
LEEF 2.0のsyslogメッセージの形式 1180
マネージャーから発信されたイベント 1180
システムイベントログの形式 1181

Agentで発生するイベント 1183
不正プログラム対策 イベントフォーマット 1183
アプリケーションコントロール イベント形式 1202
ファイアウォールイベントログの形式 1210
変更監視 ログイベント形式 1216
侵入防御 イベントログの形式 1219
セキュリティログ監視 イベント形式 1227
Webレピュテーション イベント形式 1231
デバイスコントロールイベントの形式 1233
Red Hat Enterprise Linuxでイベントログを受信するように設定する 1235
Red Hat Enterprise Linux 8以降でSyslogを設定する 1235
Red Hat Enterprise Linux 6または7でSyslogを設定する 1236
Red Hat Enterprise Linux 5でSyslogを設定する 1237
Amazon Simple Notification Serviceを設定する 1238
Amazon Simple Notification Serviceをセットアップする 1238
AWS認証を構成する 1238
IAMロールを使用する 1239
AWS Access Keysを使用する 1239
Amazon SNSトピックを作成する 1240
SNSを有効にする 1240
サブスクリプションを作成する 1241
JSON形式でのSNS設定 1241
Version 1241
Statement 1242
Topic 1242
Condition 1242
Bool 1243
Exists 1244
IpAddress 1244

NotIpAddress 1245
NumericEquals 1246
NumericNotEquals 1246
NumericGreaterThan 1247
NumericGreaterThanEquals 1248
NumericLessThan 1248
NumericLessThanEquals 1249
StringEquals 1250
StringNotEquals 1250
StringEqualsIgnoreCase 1251
StringNotEqualsIgnoreCase 1251
StringLike 1251
StringNotLike 1252
複数の文と複数の条件 1253
複数の文 1253
複数の条件 1254
SNS設定の例 1255
重大なすべての侵入防御イベントをSNSトピックに送信する 1255
イベントごとに異なるSNSトピックに送信する 1255
JSON形式のイベント 1256
有効なイベントプロパティ 1257
イベントプロパティのデータタイプ 1288
JSON形式のイベントの例 1289
システムイベント 1289
不正プログラム対策イベント 1290
リモートコンピュータにSNMP経由でシステムイベントを転送 1293
アラートの設定 1293
Deep Security Managerにアラートを表示する 1293
アラートを設定する 1294

アラートのメール通知を設定する 1294
アラートメールのオンとオフを切り替える 1296
アラートメールを受信するユーザを個別に設定する 1298
すべてのアラートメールの受信者を設定する 1299
メール通知のSMTPの設定 1299
Microsoft Exchange OnlineのOAuth 2.0を構成する 1300
前提条件 1300
Microsoft Entra IDを構成する 1300
手順1: Microsoft Entra IDでアプリケーションを登録する 1300
手順2: クライアントシークレットを作成する 1301
手順3: APIの権限を構成する 1301
Exchange Onlineを構成する 1301
手順4: テナントのSMTP AUTHを有効にする 1302
手順5: メールボックスのSMTP AUTHを有効にする 1302
手順6: Exchange Onlineでサービスプリンシパルを登録する 1303
Deep Security Managerを構成する 1303
手順 7: DSMでSMTP設定を構成する 1303
トラブルシューティング 1304
エラー: "535 5.7.139 認証に失敗しました。SmtpClientAuthenticationが無効です" 1304
エラー: "535 5.7.3 認証に失敗しました" 1304
エラー: "430 4.2.0 STOREDRV; メールボックスログオン失敗" 1305
アラートやその他のアクティビティに関するレポートの生成 1305
単独レポートを設定する 1305
予約レポートを設定する 1308
イベントとアラートのリスト 1309
事前定義アラート 1309
Agentイベント 1336
システムイベント 1342
アプリケーションコントロールイベント 1400

アプリケーションコントロールイベントで表示される情報 1401
アプリケーションコントロールイベント一覧 1401
不正プログラム対策イベント 1402
不正プログラム対策イベントの情報表示 1402
不正プログラム対策イベントの一覧 1403
デバイスコントロールイベント 1404
デバイスコントロールイベントについて表示される情報を教えてください。 1404
ファイアウォールイベント 1405
ファイアウォールイベントで表示される情報 1405
ファイアウォールイベント一覧 1407
侵入防御イベント 1413
侵入防御イベントで表示される情報 1414
侵入防御 イベントの追加情報を表示する 1415
侵入防御イベント一覧 1416
変更監視イベント 1419
変更監視イベントで表示される情報 1419
変更監視イベント一覧 1419
セキュリティログ監視イベント 1421
セキュリティログ監視イベントで表示される情報 1422
セキュリティログ監視のセキュリティイベント一覧 1423
Webレピュテーションイベント 1423
Webレピュテーションイベントで表示される情報 1423
許可するURLのリストにURLを追加する 1424
共通イベント、アラート、およびエラーのトラブルシューティング 1424
ファイアウォールモジュールが無効であるにも関わらず、ファイアウォールイベントが発生する理由 1424
イベントID 771「認識できないクライアントによる接続」のトラブルシューティング 1424
Deep Security Agentをアンインストールする 1425
コンピュータまたはクローンを再有効化する 1425

VMwareコネクタの同期の中断を修正する 1425
「Smart Protection Serverへの接続不能」エラーのトラブルシューティング 1425
エラーの詳細を確認する 1425
Deep Security Virtual Applianceの問題 1426
エラー: 有効化に失敗 1426
プロトコルエラー 1426
Agentから開始 1426
双方向の通信 1427
ホスト名解決不能 1427
エージェント/アプライアンスがありません 1427
ブロックされたポート 1427
重複するコンピュータ 1428
プロキシ経由のエンドポイント 1429
再インストールが必要です 1429
エラー: サポートされていないAgentバージョン 1429
エラー: 不正プログラム対策 エンジンオフライン 1429
Agentベースの保護 1430
エージェントがWindowsの場合： 1430
エージェントがLinuxにインストールされている場合： 1431
Agentレスによる保護 1431
エラー:デバイスコントロールエンジンがオフラインです 1432
AgentがWindowsの場合 1433
エラー: ステータスの確認の失敗 1433
エラー: 機能「dpi」のインストール失敗: 使用不可: フィルタ 1434
追加情報 1434
エラー: 仮想マシンを有効化した後に「変更監視エンジンがオフライン」およびその他のエラーが発生する 1434
エラー: インタフェースが非同期 1435
仮想マシンのインタフェースを確認する 1435

vCenterで仮想マシンのインタフェース情報を確認する 1436
Deep Security Managerでvmxファイルと仮想マシンのインタフェース情報を確認する 1436
Deep Security Virtual Applianceの仮想マシンのインタフェース情報を確認する 1437
回避策 1437
回避策1 1437
回避策2 1438
回避策3 1438
詳細なトラブルシューティング手順 1438
エラー: 侵入防御ルールのコンパイルに失敗しました 1439
侵入防御のベストプラクティスを適用する 1440
ルールを管理する 1440
個々のポートからアプリケーションの種類の割り当てを解除する 1441
エラー: セキュリティログ監視ルールで必要なログファイル 1441
ファイルの場所が必要な場合: 1442
リストされたファイルが保護対象マシンに存在しない場合: 1442
エラー: モジュールのインストール失敗 (Linux) 1442
エラー: このコンピュータに1つ以上のアプリケーションの種類の競合がある 1443
解決方法 1443
ポートを統合する 1444
継承オプションを無効にする 1444
エラー: クラウドアカウントに接続できない 1444
AWSアカウントのアクセスキーIDまたは秘密アクセスキーが無効である 1445
Deep Securityで使用するアカウントに間違ったAWS IAMポリシーが適用されている 1445
NAT、プロキシ、またはファイアウォールのポートが開いていないか、設定が正しくない 1445
エラー: インスタンスのホスト名を解決できない 1446
アラート: 変更監視情報の収集が遅延しています 1446
アラート: Managerの時刻が非同期 1446
アラート: Managerノードのメモリの警告しきい値を超過しました 1447
イベント: 最大TCP接続数 1447

警告:不正プログラム対策エンジンが提供する基本機能 1448
基本機能 1448
理由ID 1449
警告: Census、Good File Reputation、機械学習型検索サービスへの接続解除 1451
原因1: AgentまたはRelay有効化済みAgentがインターネットにアクセスできない 1452
原因2: プロキシは有効化されているが、適切に設定されていない 1452
警告:ディスク容量の不足 1453
ヒント 1453
警告:攻撃の予兆の検出 1453
攻撃の予兆の検出の種類 1453
推奨処理 1454
プロキシの設定 1455
プロキシの設定 1455
管理者にプロキシを登録する 1456
サポートされるプロキシプロトコル 1456
プロキシ経由でプライマリセキュリティアップデート元に接続する 1457
Deep Security Managerにプロキシ経由で接続する 1458
プロキシ経由でDeep Securityリレーに接続する 1459
Deep Securityソフトウェアのアップデート、CSSSなどにプロキシ経由で接続する 1460
プロキシ経由でクラウドアカウントに接続する 1461
Deep Discovery Analyzer にプロキシ経由で接続する 1461
プロキシ経由でApex Centralに接続する 1461
プロキシを介してSmart Protection Networkする 1462
プロキシ経由でWorkload Securityに接続 1463
プロキシを削除する 1463
プロキシ設定 1464
プロキシサーバを使用する 1464
Relayの設定 1465
リレーの動作 1465

Relay階層、コスト、パフォーマンス 1467
追加のリレーを配信する 1467
リレーの最適な数と位置を計画する 1468
地理的地域と距離 1469
ネットワークアーキテクチャと帯域幅の制限 1469
エアギャップ環境 1470
アップデート元を設定する 1470
Relayの設定 1472
Relayグループを作成する 1472
リレーを有効にする 1473
AgentをRelayグループに割り当てる 1474
AgentをRelayのプライベートIPアドレスに接続する 1475
AgentからRelay機能を削除する 1475
エージェント(保護されたコンピュータ)の管理 1476
コンピュータおよびAgentのステータス 1476
[ステータス]列 - コンピュータの状態 1476
[ステータス]列 - AgentまたはApplianceの状態 1477
[タスク]列 1478
コンピュータのエラー 1482
保護モジュールのステータス 1483
コンピュータでその他の処理を実行する 1484
コンピュータのアイコン 1487
各種コンピュータのステータス情報 1489
通常のコンピュータ 1489
Relay 1489
Deep Security Scanner 1490
Docker、Podman、およびCRI-Oホスト 1490
ESXiサーバ 1491
Virtual Appliance 1491

仮想マシンをAgentレスで保護する ... 1492
エージェントのバージョン管理を設定する ... 1492
エージェントのバージョンコントロールを設定する ... 1493
エージェントバージョン管理(URL要求あり) ... 1495
エージェントのバージョン管理FAQ ... 1495
NICチーミングの設定 ... 1497
Windows ... 1497
Solaris ... 1498
AgentとManagerの通信 ... 1499
ハートビートを設定する ... 1499
通信方向を設定する ... 1500
AgentとManagerの通信でサポートされている暗号化スイート ... 1502
Deep Security Agent 9.6の暗号化スイート ... 1502
Deep Security Agent 10.0の暗号化スイート ... 1503
Deep Security Agent 11.0、12.0、および20の暗号化スイート ... 1503
インターネットにアクセスできないAgentを設定する ... 1504
解決策 ... 1504
プロキシを使用する ... 1504
Smart Protection Serverをローカルにインストールする ... 1505
隔離されたネットワークでアップデートを取得する ... 1506
隔離されたネットワークでルールのアップデートを取得する ... 1508
トレンドマイクロのセキュリティサービスを使用する機能を無効にする ... 1509
AgentからのリモートAgentからの通信を使用してAgentを有効化して保護する ... 1511
AgentからのリモートAgentからの通信を有効にする ... 1511
Agentからの通信を有効にしたポリシーを作成または変更する ... 1512
Agentからのリモート有効化を有効にする ... 1512
Agentにポリシーを割り当てる ... 1512
インストールスクリプトを使用してAgentを有効にする ... 1512

Agentを有効化するときに自動的にアップグレードする 1513
Agentの自動アップグレードを有効にする 1513
Agentが正常にアップグレードされたことを確認する 1514
Deep SecurityでのiptablesのIPv6使用 1515
Deep Security Managerの実行に必要なルール 1516
Deep Security Agentの実行に必要なルール 1516
Deep SecurityによるiptablesルールのIPv6自動追加を防ぐ 1517
エージェントセルフプロテクションを有効化または無効化する 1517
Deep Security Managerを介してセルフプロテクションを設定する 1518
Command Lineを使用して自己防御を設定する 1518
WindowsでCommand Lineを使用する 1518
LinuxでCommand Lineを使用する 1519
Linuxの制限事項 1519
トラブルシューティング 1520
オフラインエージェントはDeep Securityによって保護されていますか? 1520
非アクティブなAgentのクリーンナップによるオフラインコンピュータの削除の自動化 1520
非アクティブなAgentのクリーンナップを有効にする 1521
長期間にわたってオフラインになっているコンピュータのDeep Securityによる継続保護 1521
オーバーライド設定による特定のコンピュータの削除の回避 1522
非アクティブなAgentのクリーンナップジョブによって削除されたコンピュータの監査証跡の確認 1522
システムイベントを検索する 1523
システムイベントの詳細 1523
2953 - 非アクティブなAgentのクリーンナップが正常に完了しました 1523
251 - コンピュータの削除 1523
716 - 不明なAgentの再有効化の試行 1524
Agentの設定 1524
ホスト名 1524
エージェント起動アクティベーション(AIA) 1524

Agentのアップグレード 1527
非アクティブなAgentのクリーンナップ 1527
データプライバシー 1527
Agentレスによるvcloud保護 1528
ユーザーモードソリューション 1528
利用可能なモード 1528
システム保護のためのドライバーの使用 1529
サポートされているエージェント 1529
Deep Security Notifier 1531
Notifierの仕組み 1532
Windows OSで手動検索を開始する 1536
ユーザを管理する 1537
ユーザの追加と管理 1537
Active Directoryとの同期 1537
ユーザを個別に追加または編集する 1538
ユーザのパスワードを変更する 1541
ユーザをロックアウトする/ロックアウトをリセットする 1541
ユーザに関連付けられたシステムイベントを表示する 1541
ユーザを削除する 1541
ユーザロールの定義 1541
役割を追加または編集する 1543
Full Access、Auditor、および新規の各役割の初期設定 1549
レポートのみを受信できるユーザの追加 1558
連絡先を追加または編集する 1558
連絡先を削除する 1559
ユーザ向けのAPIキーの作成 1559
既存のAPIキーをロックアウトする 1560
ロックアウトされたユーザ名のロック解除 1560
管理者としてユーザのロックを解除する 1560

コマンドラインから管理ユーザのロックを解除する 1560
SAML シングルサインオン (SSO) を実装する 1561
SAMLシングルサインオン(SSO) について 1561
SAMLとシングルサインオンとは 1561
Deep SecurityでのSAMLシングルサインオンの仕組み 1561
信頼関係を確立する 1561
ユーザIDからDeep Securityアカウントを作成する 1561
Deep SecurityでSAMLシングルサインオンを実装する 1562
SAMLシングルサインオンを設定する 1563
設定前の要件を設定する 1563
Deep SecurityをSAMLサービスプロバイダとして設定する 1564
Deep SecurityでSAMLを設定する 1564
IDプロバイダSAML メタデータドキュメントをインポートする 1565
SAMLユーザのDeep Securityの役割を作成する 1565
IDプロバイダの管理者に情報を提供する 1565
Deep Security Managerサービスプロバイダ SAML メタデータドキュメントをダウンロードする 1565
URNおよびDeep Security SAML メタデータドキュメントをIDプロバイダの管理者に送信する 1565
SAMLクレームの構造 1566
Deep Securityユーザ名 (必須) 1566
SAMLデータの例 (簡略版) 1566
Deep Securityユーザの役割 (必須) 1567
SAMLデータの例 (簡略版) 1567
最大セッション期間 (オプション) 1567
SAMLデータの例 (簡略版) 1567
言語設定 (オプション) 1568
SAMLデータの例 (簡略版) 1568
SAMLシングルサインオンをテストする 1568
設定を確認する 1568

診断パッケージを作成する 1569
サービスとIDプロバイダの設定 1569
SAMLシングルサインオンをMicrosoft Entra IDで設定する 1569
誰がこのプロセスに関与していますか? 1569
Deep SecurityをSAMLサービスプロバイダとして設定する 1570
Deep Securityサービスプロバイダの SAML メタデータドキュメントをダウンロードする 1571
Microsoft Entra IDを設定する 1571
Deep SecurityでSAMLを設定する 1572
Microsoft Entra ID メタデータドキュメントをインポートする 1572
SAMLユーザのDeep Securityの役割を作成する 1572
URNを取得する 1572
Microsoft Entra IDで役割を定義する 1572
サービスとIDプロバイダの設定 1573
SAML クレームの構造 1573
Deep Securityユーザ名 (必須) 1573
SAMLデータの例 (簡略版) 1573
Deep Securityユーザの役割 (必須) 1574
SAMLデータの例 (簡略版) 1574
最大セッション期間 (オプション) 1574
SAMLデータの例 (簡略版) 1574
言語設定 (オプション) 1575
SAMLデータの例 (簡略版) 1575
データベースの管理 1575
データベースの一般的なメンテナンス 1575
PostgreSQLを維持する 1576
ログローテーション 1577
例:日単位のデータベースのログローテーション 1578
ロック管理 1578
最大同時接続数 1578

有効キャッシュサイズ 1579
共有バッファ 1579
ワークメモリとメンテナンスワークメモリ 1579
チェックポイント 1579
ログ先行書き込み (WAL) 1579
自動バキューム設定 1580
Linux版PostgreSQL 1581
Transparent huge pages 1581
ホストベース認証 1581
Microsoft SQL Server Expressの管理 1581
Microsoft SQL Server Expressからエンタープライズへの移行 1581
データベースのバックアップと復元 1583
データベースをバックアップする 1583
データベースのみを復元する 1583
Deep Security Managerとデータベースの両方を復元します。 1583
オブジェクトをXML形式またはCSV形式でエクスポートする 1584
オブジェクトをインポートする 1585
Deep Security Managerの移動とカスタマイズ 1585
ダッシュボードのカスタマイズ 1585
日時の範囲の指定 1586
コンピュータおよびコンピュータグループの指定 1586
タグごとのフィルタ 1587
ダッシュボードのウィジェットを選択する 1588
監視: 1588
システム: 1589
ランサムウェア: 1589
不正プログラム対策: 1590
Webレピュテーション: 1590
ファイアウォール: 1590

侵入防御: 1591
変更監視: 1592
セキュリティログ監視: 1592
アプリケーションコントロール: 1593
レイアウトを変更する 1593
ダッシュボードのレイアウトを保存/管理する 1594
スマートフォルダによるコンピュータの動的なグループ化 1594
スマートフォルダを作成する 1595
スマートフォルダを編集する 1597
スマートフォルダのクローンを作成する 1597
サブフォルダを使用して検索を絞り込む 1597
サブフォルダを自動作成する 1598
検索可能なプロパティ 1599
一般 1599
AWS 1602
Azure 1604
GCP 1605
vCenter 1605
vCloud 1606
Active Directory 1606
演算子 1607
詳細なシステム設定のカスタマイズ 1609
プライマリテナントアクセス 1609
ロードバランサ 1609
マルチテナントモード 1610
Deep Security Managerプラグイン 1610
SOAP Webサービス API 1610
ステータス監視API 1610
エクスポート 1611

Whois 1611
ライセンス 1611
推奨設定の検索中のCPU使用率 1611
NSX 1611
ロゴ 1612
Manager AWS ID 1612
アプリケーションコントロール 1612
Deep Securityの強化 1616
Deep Securityの強化について 1616
Agentを使用したDeep Security Managerの保護 1617
Deep Security Agentの保護 1618
パブリックCAによって発行されたDeep Security Manager証明書チェーンをインポートする 1620
インポートされた証明書チェーンを削除 1621
Deep Security ManagerのTLS証明書を変更します。 1622
秘密鍵とJavaキーストアの生成 1623
署名付き証明書 (CSR) の 1625
署名された証明書をキーストアにインポートする 1626
キーストアを使用するためのDeep Security Managerの設定 1628
Deep Security Managerでの自己署名証明書の再生成 (概要) 1629
ロードバランサの証明書のアップデート 1631
Deep Security Managerとデータベース間の通信の暗号化 1633
Managerとデータベースの間の通信を暗号化する 1634
Microsoft SQL Serverデータベース 1634
Oracleデータベース 1635
PostgreSQL 1635
データベースサーバでAgentを実行する 1636
Managerとデータベース間の暗号化を無効にする 1636
Microsoft SQL Server 1637

Oracle Database 1637
PostgreSQL 1637
古いDeep Security Managerバージョンからのアップグレード 1638
Deep Security Managerをアップグレード 1638
Deep Security Managerのデータベースのパスワードの変更 1638
Microsoft SQL Serverのパスワードを変更する 1639
Oracleのパスワードを変更する 1639
PostgreSQLのパスワードを変更する 1640
HTTPセキュリティヘッダを設定する 1641
カスタマイズ可能なセキュリティヘッダ 1641
HTTPの厳密なトランスポートセキュリティ(HSTS) 1641
Content Security Policy (CSP) 1642
HTTP公開鍵ピンニング (HPKP) 1643
カスタマイズ可能なセキュリティヘッダを有効化する 1643
設定をリセットする 1644
HTTPの厳密なトランスポートセキュリティ 1644
Content Security Policy (CSP) 1644
Public Key Pinning Policy 1644
強制的に適用されるセキュリティヘッダ 1644
Cache-ControlおよびPragma 1644
X-XSS-Protection 1645
X-Frame-Options 1645
サポートされていないセキュリティヘッダ 1645
X-Content-Type-Options 1645
Deep Securityの暗号化アルゴリズムのアップグレード 1646
Windowsでアルゴリズムをアップグレードする 1646
Linuxでアルゴリズムをアップグレードする 1646
複数ノード環境でアルゴリズムをアップグレードする 1647
マルチテナント環境でアルゴリズムをアップグレードする 1647

ユーザパスワードルールの適用 1647
パスワード要件を指定する 1647
ログオンに別のIDプロバイダを使用する 1649
Deep Security Managerログオンページにメッセージを追加する 1649
ユーザに使用条件を提示する 1649
その他のセキュリティ設定 1649
多要素認証の設定 1649
多要素認証を有効にする 1650
多要素認証を無効にする 1652
サポートされる多要素認証 (MFA) アプリケーション 1652
MFAをトラブルシューティングする 1653
MFAデバイスを有効にしても機能しない場合の対処 1653
MFAデバイスが紛失または動作停止した場合の対処 1653
信頼された証明書の管理 1653
信頼された証明書をインポートする 1653
信頼された証明書を表示する 1654
信頼された証明書を削除する 1655
SSLの実装と資格情報のプロビジョニング 1656
Smart Protection Networkの接続を無効にした場合のトレンドマイクロへの情報の送信について 1657
Deep Securityのアップグレード 1657
アップグレードについて 1657
Deep Security Managerによるソフトウェアアップグレードの確認方法 1658
アップグレードのベストプラクティス 1659
Deep Securityによるアップデートの整合性の検証方法 1660
デジタル署名 1660
チェックサム 1661
セキュリティ更新プログラムの適用 1661
セキュリティ更新プログラムを起動する 1662

セキュリティアップデートのステータスを確認する 1662
パターンファイルのアップデートの詳細を表示 1663
ルールのアップデートに関する詳細の復元、インポート、または表示 1663
セキュリティ更新プログラムを構成する 1664
ルールの自動パッチを有効にする 1665
自動 不正プログラム対策 エンジンのアップデートを有効にする 1665
古いクライアントのセキュリティ更新を有効にする 1666
最新のセキュリティ更新プログラムの警告のしきい値を変更します。 1666
新しいパターンファイルアップデートアラートのメールの無効化 1666
ソフトウェアアップデートを配布するWebサーバの使用 1667
Webサーバのシステム要件 1667
フォルダ構造をコピーする 1667
新しいソフトウェアリポジトリを使用するようにAgentを設定する 1669
Deep Security Managerをアップグレード 1670
開始前の準備 1670
マネージャをアップグレードする 1671
古いバージョンのReleaseが2つ以上ある場合はマネージャをアップグレードしてください 1671
マルチノード配置でマネージャをアップグレードする 1672
マルチテナント環境でマネージャをアップグレードする 1673
アップグレードするとどうなりますか? 1673
アップグレード後のタスク 1673
マネージャのバージョンアップのトラブルシューティング(ログファイル) 1674
マネージャのバージョンアップに失敗しました(ロールバック) 1674
Deep Security Relay 1675
マネージャからリレーをアップグレードする 1675
インストーラを手動で実行してリレーをアップグレードする 1676
Deep Security Agentのアップグレード 1676
アップグレードを開始する前に 1676
アラートからAgentをアップグレードする 1678

複数のエージェントを一度にアップグレードする 1678
[クライアント]ページからエージェントをアップグレードします。 1679
アクティベーション時にエージェントをアップグレードする 1679
予約タスクからAgentをアップグレードする 1679
エージェントを手動でアップグレードする 1680
ds_adm.fileの内容 1682
仮想アプライアンスに組み込まれているエージェントを自動的にアップグレードする 1683
Agentアップグレードのベストプラクティス 1684
Deep Security Virtual Applianceのバージョンアップ 1684
新しいアプライアンスソフトウェアが使用可能かどうかを確認する 1685
現在使用しているAppliance SVMと組み込みのAgentのバージョンを確認する 1685
新しいAppliance SVMがあるかどうかを確認する 1685
新しいAgentがあるかどうかを確認する 1686
アプライアンスをバージョンアップする前に 1686
システム要件とサポートされているNSXのバージョンを確認する 1686
vCenterおよびNSXアカウントのアクセス許可を確認する 1686
NSX-Tの再登録 1686
新しいアプライアンスZIPをマネージャにインポートします。 1687
次の手順 1688
Applianceをアップグレードする 1688
既存のAppliance SVMを自動的にアップグレードする 1688
手順1: ManagerでAppliance SVMをアップグレードする 1689
「Appliance (SVM) のアップグレード失敗」システムイベントのトラブルシューティング 1691
手順2: アップグレードが成功したことを確認します。 1692
既存のAppliance SVMを手動でアップグレードする 1692
手順1: 検出ファイルを確認または復元する 1692
手順2: ゲスト仮想マシンを別のESXiホストに移行する 1692
手順3: 古いAppliance SVMをアップグレードする 1693
手順4: メンテナンスモードがオフになっていることを確認する 1698

手順5: 新しいAppliance SVMが有効化されていることを確認する 1698
手順6: 最後の手順 1699
アプライアンスSVMに組み込まれているエージェントをアップグレードします 1699
互換性テーブル: アプライアンス、エージェント 1700
データベースのアップグレード 1701
アップグレードパス 1701
データベースのアップグレード 1701
エラー: データベースサーバへの安全な接続を確立できませんでした 1702
NSXライセンスをアップグレードして、利用できるDeep Securityの機能を増やす 1702
NSX-T 3.xライセンスのアップグレード 1703
NSX-Vライセンスをアップグレードします 1703
手順1: NSXライセンスをアップグレードする 1704
手順2: Deep SecurityをNSXからすべて削除する 1707
手順3: Deep Security Virtual Applianceを再インストールする 1707
エージェントレスソリューションをNSX-VからNSX-Tに移行する 1707
移行シナリオ1 1708
移行前 1708
ステップ1: 移行のためのNSX-Tインフラストラクチャの準備 1709
ステップ2: 新しいアプライアンスをインポートする 1709
ステップ3: 移行する 1709
ステップ4: 新しい配信とそのセキュリティ機能を確認する 1710
ステップ5: Deep Security ManagerからのNSX-Vのアンインストール 1710
移行シナリオ2 1711
移行前 1711
ステップ1: NSX-TネットワークとvCenterインフラストラクチャの準備 1711
ステップ2: 新しいアプライアンスをインポートする 1711
ステップ3: 移行する 1712
ステップ4: 新しい配信とそのセキュリティ機能を確認する 1714
ステップ5: NSX-Vをクリーンナップする 1715

NSX-Tのセキュリティグループをアップデートする 1715
セキュリティポリシーをNSX-VからNSX-Tに移行する 1722
現在のNSX-V設定を確認する 1722
NSX-Tのゲストイントロスペクション設定を再作成します 1724
NSX-Tのネットワークイントロスペクション設定を再作成する 1725
Deep Securityのアンインストール 1727
Deep Securityのアンインストール 1727
Deep Security Relayのアンインストール 1727
WindowsでのRelayのアンインストール 1727
LinuxでのRelayアンインストール 1728
Deep Security Agentをアンインストールする 1728
WindowsでのAgentアンインストール 1728
LinuxでのAgentアンインストール 1729
Solaris 10でのAgentアンインストール 1730
Solaris 11でのAgentアンインストール 1730
AIXでのAgentアンインストール 1730
Red Hat OpenShiftでのAgentアンインストール 1730
Deep Security Notifierをアンインストールする 1730
Deep Security Managerをアンインストールする 1730
WindowsでManagerをアンインストールする 1731
LinuxでManagerをアンインストールする 1731
NSX環境からのDeep Securityのアンインストール 1731
Deep Securityを自動的にアンインストールします 1732
NSX-T 3.xからのDeep Securityの手動アンインストール 1733
NSX-V環境からのDeep Securityの手動アンインストール 1740
Deep Security Managerのメモリ使用量を設定する 1745
インストーラーの最大メモリ使用量を設定する 1745
Deep Security Managerの最大メモリ使用量を設定する 1745
Deep Security Managerの再起動 1746

Linux ... 1746
Windows ... 1746
Windowsデスクトップ ... 1746
コマンドプロンプト ... 1746
PowerShell ... 1747
ライセンス情報の確認 ... 1747
現在のライセンスを確認する ... 1747
ライセンスの詳細を表示 ... 1748
ライセンスの追加またはアップグレード ... 1748
Deep Security を Trend Vision One Endpoint Security - Server & Workload Protection にアップグレード ... 1749
Trend Vision One Endpoint Security - Server & Workload Protectionにアップグレード ... 1749
Trend Vision One Endpoint Security - Server & Workload Protectionを構成する ... 1750
APIキーを作成 ... 1750
Trend Vision One Endpoint Security - Server & Workload Protectionの地域を決定する ... 1750
Trend Vision One Endpoint Security - Server & Workload Protectionへのリンクを準備する ... 1751
その他のDeep Security設定の移行 ... 1752
VMwareコネクタとデータセンターゲートウェイ ... 1752
コンピュータグループとスマートフォルダ ... 1752
プロキシ設定 ... 1753
イベントとアラートのログ ... 1753
追加設定 ... 1753
ネットワークと通信の設定 ... 1754
必要なポート、プロトコル、およびURL ... 1754
プロキシ設定 ... 1754
検索されたサイズ使用率 ... 1754
Relay の設定 ... 1755
Deep SecurityおよびTrend Vision One Endpoint Security - Server & Workload Protection APIを使用してアップグレード ... 1755

クラウドアカウントをTrend Vision One Endpoint Security - Server & Workload Protectionに移行する 1757
前提条件 1757
AWSアカウントの移行 1757
移行ツールを使用して他のクラウドアカウントを移行する 1758
VMware vCloudアカウントの移行 1759
エージェントをTrend Vision One Endpoint Security - Server & Workload Protectionに移行する 1759
前提条件 1759
移行ツールを使用してエージェントを移行する 1760
移動ステータスを確認する 1761
スマートフォルダを使用して移動ステータスを表示する 1765
トラブルシューティング 1766
管理対象外のエージェントを手動で復元する 1766
エージェントを停止できなかった場合 1766
エージェントを起動できなかった場合 1767
重複したエンドポイントレコードエラーと不正な保護の管理値エラーを解決する 1767
エージェントを移行するその他の方法 1767
Deep Security を Trend Cloud One - Endpoint & Workload Security に移行する 1768
Trend Cloud One - Endpoint & Workload Securityに移行 1768
Workload Security アカウント、ユーザー、ロール、および認証を設定する 1769
ロールとAPIキーを作成 1769
Workload Securityへのリンクを準備する 1770
その他のDeep Security設定の移行 1770
VMwareコネクタとデータセンターゲートウェイ 1771
コンピュータグループとスマートフォルダ 1771
プロキシ設定 1771
イベントとアラートのログ 1771
追加設定 1772
Trend Micro Vision One (XDR) 登録 1772

ネットワークと通信の設定 1772
必要なポート、プロトコル、およびURL 1773
プロキシ設定 1773
検索されたサイズ使用率 1773
Relay の設定 1774
Deep Security APIとWorkload Security APIを使用した移行 1774
ポリシーをTrend Cloud One - Endpoint & Workload Securityに移行する 1775
前提条件 1775
制限事項 1776
移行ツールを使用してポリシーを移行する 1776
ポリシーを移行するその他の方法 1777
共通オブジェクトをTrend Cloud One - Endpoint & Workload Securityに移行する 1778
前提条件 1778
移行ツールを使用して共通オブジェクトを移行する 1778
クラウドアカウントをTrend Cloud One - Endpoint & Workload Securityに移行する 1779
前提条件 1780
AWSアカウントを移行する場合 1780
制限事項 1780
クロスアカウントロールを使用して追加されたAWSアカウントを移行する 1780
新しいクロスアカウントロールを作成する 1781
既存のクロスアカウントロールを再利用する 1781
移行ツールを使用して他のクラウドアカウントを移行する 1783
VMware vCloudアカウントの移行 1783
エージェントをTrend Cloud One - Endpoint & Workload Securityに移行する 1784
前提条件 1784
移行ツールを使用してエージェントを移行する 1785
移動ステータスを確認する 1786
スマートフォルダを使用して移動ステータスを表示する 1789
トラブルシューティング 1790

管理対象外のエージェントを手動で復元する 1790
エージェントを停止できなかった場合 1790
エージェントを起動できなかった場合 1791
エージェントを移行するその他の方法 1791
DevOps、automation、および Api 1792
DevOps、自動化、およびAPIについて 1792
Trend Micro Hybrid クラウドセキュリティコマンドラインインタフェース(THUS) 1793
コマンドラインの基本 1793
dsa_control 1794
dsa_control options 1795
Agentからのリモート有効化 (「dsa_control -a」) 1799
Agentからのハートビート有効化コマンド(「dsa_control -m」) 1799
Deep Security Agentの有効化 1805
Windows 1806
Linux、AIX、およびSolaris 1806
Agentからのハートビート有効化コマンド 1806
Windows 1806
Linux、AIX、およびSolaris 1806
不正プログラムの手動検索を開始する 1806
Windows 1806
Linux、AIX、およびSolaris 1807
診断パッケージを作成する 1807
Agentをリセットする 1807
Windows 1807
Linux、AIX、およびSolaris 1807
dsa_query 1807
dsa_queryのオプション 1807
CPU使用率とRAM使用量を確認する 1808
Windows 1808

LinuxおよびSolaris 1809
AIX 1809
ds_agentプロセスまたはサービスが実行されていることを確認する 1809
Windows 1809
Linux、AIX、およびSolaris 1809
LinuxでAgentを再起動する 1809
Solarisでエージェントを再起動する 1809
AIXでエージェントを再起動する 1809
dsa_scan 1810
dsa_scanのオプション 1810
dsa_scanの出力 1811
終了コードの検索 1812
dsm_c 1814
dsm_cオプション 1814
リターンコード 1824
Deep Security APIを使用したタスクの自動化 1824
従来のREST APIおよびSOAP API 1825
ステータス監視APIを有効にする(オプション) 1825
Webサービスユーザアカウントを作成する 1825
Deep Security予約タスクの設定 1826
予約タスクを作成する 1826
予約タスクを有効または無効にする 1828
予約レポートを設定する 1829
コンピュータの追加または変更時にタスクを自動的に実行する(イベントベースのタスク) 1829
イベントベースタスクを作成する 1829
既存のイベントベースタスクを編集または停止する 1829
監視できるイベント 1830
条件 1830
それぞれの条件と説明のリスト 1831

Java正規表現の例 1833
処理 1833
実行順序 1834
イベントベースタスクを一時的な無効にする 1836
AWSオートスケーリングとDeep Security 1836
Agentをプレインストールする 1836
インストールスクリプトでAgentをインストールする 1837
オートスケーリングの結果としてDeep Securityからインスタンスを削除する 1839
Azure Virtual Machine Scale SetsとDeep Security 1839
手順1: (推奨) AzureアカウントをDeep Security Managerに追加する 1840
手順2: インストールスクリプトを準備する 1840
手順3: カスタムスクリプト拡張機能を介してAgentをVMSSインスタンスに追加する 1841
例1: Agentを含む新しいVMSSを作成する 1841
例2: 既存のVMSSにAgentを追加する 1844
GCP自動スケーリングとDeep Security 1846
Agentをプレインストールする 1846
インストールスクリプトでAgentをインストールする 1847
GCP MIGの結果としてDeep Securityからインスタンスを削除します。 1849
インストールスクリプトを使用したコンピュータの追加と保護 1849
インストールスクリプトを生成する 1849
トラブルシューティングおよびヒント 1852
エージェントのダウンロードURL形式 1853
エージェントのダウンロードURL形式 1854
<dsm fqdn>パラメータ 1854
<ファイル名>パラメータ 1854
<エージェントバージョン>パラメータ 1855
<エージェントのバージョン>をスクリプトに明示的に含める必要がありますか? 1855
<プラットフォーム>,<arch>、および<filename>パラメータ 1856
例 1859

下位互換性の除外設定 1860
エージェントバージョンコントロールを使用して、返されるエージェントバージョンを定義する 1860
例 1861
<エージェントバージョン>パラメータとエージェントバージョン管理の間の相互作用 1861
クラウドプロバイダーのタグ/ラベルを使用してポリシーを自動的に割り当てる 1861
信頼とコンプライアンス 1863
コンプライアンスについて 1863
エージェントパッケージの整合性チェック 1863
トラブルシューティング 1864
サポートされるDeep Security Relayのバージョン 1865
Deep SecurityによるPCI DSS要件への対応 1865
コモンクライテリアの設定 1865
手順1: Deep Securityのインストール 1866
手順2: FIPSモードを有効にする 1867
手順3: 不正アクセスを防ぐためにDeep Securityを強化する 1867
手順4: 強力なパスワードポリシーを適用する 1868
手順5: 従来のAPIを無効にする 1868
手順6: アラートのメール通知を設定する 1868
次の手順(動作確認済みの設定での運用) 1869
GDPR 1869
FIPS 140のサポート 1870
Deep SecurityをFIPSモードで操作する際の違い 1871
Deep Security ManagerでFIPSモードが有効になっているか確認する 1871
FIPSモードのシステム要件 1871
Deep Security Managerの要件 1871
Deep Security Agentの要件 1872
Deep Security Virtual Applianceの要件 1872
Deep Security ManagerでFIPSモードを有効にする 1873
WindowsでDeep Security ManagerのFIPSモードを有効にする 1873

LinuxでDeep Security ManagerのFIPSモードを有効にする 1873
FIPSモードで外部サービスに接続する 1873
保護しているコンピュータのOSのFIPSモードを有効にする 1874
保護しているコンピュータでDeep Security AgentのFIPSモードを有効にする 1875
Windows AgentのFIPSモードを有効にする 1875
Linux AgentでFIPSモードを有効にする 1875
Deep Security Virtual ApplianceでFIPSモードを有効にする 1876
FIPSモードをPostgreSQLデータベースで使用する 1876
Microsoft SQL ServerデータベースでFIPSモードを使用する 1879
FIPSモードを無効にする 1880
Deep Securityでの脆弱性管理検索トラフィックのバイパス 1881
脆弱性検索プロバイダのIP範囲またはアドレスから新しいIPリストを作成する 1881
受信および送信検索トラフィック用のファイアウォールルールを作成する 1882
新規ファイアウォールルールをポリシーに割り当てて、脆弱性検索をバイパスする 1883
Deep SecurityでのTLS 1.2の使用 1883
TLS 1.2とDeep Security Agentの互換性 1885
TLS 1.2のアーキテクチャ 1885
TLS 1.2を使用するようにコンポーネントをアップグレードする 1887
Deep Security Managerを確認してアップグレードする 1888
Deep Security Managerデータベースを確認する 1888
Deep Security Agentを確認する 1888
Deep Security Relayを確認する 1889
Deep Security Virtual Applianceを確認する 1889
TLS 1.2を強制する 1889
TLS 1.2を強制できるコンポーネント 1890
TLS 1.2を強制した場合の動作 1890
初期設定でTLS 1.2が強制されるかどうか 1890
TLS 1.2の強制が可能になる場合の条件 1890
Deep Security ManagerでTLS 1.2を強制する 1891

Deep Security RelayでTLS 1.2を強制する 1891
ManagerのGUIポート(4119) でのみTLS 1.2を強制する 1892
TLS 1.2の強制をテストする 1892
初期のTLS (1.0) を有効にする 1893
Deep Security ManagerとDeep Security RelayでTLS 1.0を有効にする 1894
ManagerのGUIポートでTLS 1.0を有効にする(4119) 1894
インストールスクリプトでTLS 1.0を有効にする 1895
TLS 1.2が強制されているかどうかを確認する 1895
TLS 1.2の強制後のAgent、Virtual Appliance、Relayのインストールに関するガイドライン 1896
TLS 1.2が強制されているときのAgent、Virtual Appliance、およびRelayのインストールに関するガイドライン 1896
TLS 1.2の強制後にインストールスクリプトを使用する場合のガイドライン 1896
TLS 1.2の強力な暗号化スイートの有効化 1897
環境を確認する 1897
Deep Securityコンポーネントをアップデートする 1898
TLS 1.2の強力な暗号化スイートを有効にするためのスクリプトを実行する 1898
スクリプトの動作を確認する 1899
nmapを使用してManagerを確認する 1899
nmapを使用してRelayを確認する 1900
nmapを使用してAgentを確認する 1901
TLS 1.2の強力な暗号化スイートを無効にする 1902
法的開示 1903
プライバシーと個人データの収集に関する規定 1903
Deep Security製品使用状況データ収集 1903
法律上の免責事項 1903
Hot Fix 1904
メジャーリリース、アップデート、パッチ、Service Pack 1904
統合 **1905**
AWS Control Towerとの統合 1905

概要 1905
AWS Control Towerとの統合 1905
AWS Control Towerの統合をアップグレードする 1906
AWS Control Tower統合の削除 1906
AWS Systems Manager Distributorとの統合 1906
IAMポリシーを作成する 1907
役割を作成し、ポリシーを割り当てます。 1907
パラメータの作成 1907
AWS Systems Manager Distributorとの統合 1908
コンピュータを保護する 1908
Cisco Identity Services Engine (ISE) と統合する 1908
前提条件Cisco ISE接続設定 1909
Deep Security ManagerでCisco ISE接続を構成する 1911
Cisco ISE接続ステータスリスト 1912
モニタとトラブルシューティング 1913
SAP NetWeaverとの統合 1915
Deep SecurityおよびSAPコンポーネント 1916
Deep Security ScannerとSAP NetWeaverの統合を有効にする 1918
Deep Security Scannerをアクティブ化 1918
Agentをインストールする 1919
Deep Security ManagerにSAPサーバを追加してエージェントを有効化する 1920
セキュリティプロファイルを割り当てる 1923
Agentを使用するようにSAPを設定する 1926
トレンドマイクロのスキャナグループを設定する 1927
トレンドマイクロのウイルススキャンプロバイダを設定する 1933
トレンドマイクロのウイルススキャンプロファイルを設定する 1939
ウイルススキャンインタフェースをテストする 1948
Java 環境でトレンドマイクロ スキャナー グループを構成する 1954
Java環境でトレンドマイクロウイルススキャンプロバイダを設定する 1956

Java環境でトレンドマイクロウイルススキャンプロファイルを設定する 1958
Java環境でウイルススキャンインターフェースをテストする 1963
サポートされているMIMEタイプ 1963
Trend Vision Oneと統合する 1967
Trend Vision One (XDR) と統合する 1967
Trend Vision One (XDR) に登録 1968
セキュリティイベントをTrend Vision One (XDR)に転送 1968
アクティビティデータをTrend Vision One (XDR)に転送 1969
インストールスクリプトを生成する 1969
エージェントインストーラーをダウンロードする 1970
Trend Vision One Service Gatewayとの統合 1970
サポートされているService Gatewayのバージョン 1970
システム要件 1970
Service Gatewayの配信 1971
Service Gatewayフォワードプロキシを統合する 1971
Service Gateway ActiveUpdate Serviceを統合する 1971
ActiveUpdateサービスを有効にする 1971
Deep Security ActiveUpdateソースURLを取得 1972
ActiveUpdate Serviceを構成する 1972
ActiveUpdate Serviceを構成する 1972
Service Gateway Smart Protectionサービスを統合する 1972
Smart Protectionサービスを有効にする 1972
Deep Securityポリシーでローカルファイルレピュテーションサービスを構成する 1973
Deep Securityポリシーでローカルwebレピュテーションサービスを構成する 1973
よくある質問 **1973**
保護をオンにするとWindowsマシンのネットワーク接続が失われる理由 1973
Deep Securityに関するニュースの取得方法 1974
Solarisゾーンでのエージェント保護はどのように機能しますか? 1974
侵入防御 (IPS)、ファイアウォール、およびWebレピュテーション 1975

共有IPネットワークインタフェースを使用する非グローバルゾーン 1975
専用IPネットワークインタフェースを使用する非グローバルゾーン 1975
不正プログラム対策、変更監視、およびセキュリティログ監視 1976
AWS GovCloud(US) インスタンスを保護するにはどうすればよいですか? 1976
AWS GovCloud(US) のAWSインスタンスの管理者によるインスタンスの保護 1977
Azure Governmentのインスタンスを保護するにはどうすればいいですか? 1977
グローバルAzureのマネージャを使用してAzure Governmentのインスタンスを保護する 1979
Deep Security AgentはAmazonインスタンスメタデータサービスをどのように使用しますか 1979
AWS Elastic Beanstalk環境でオフライン環境に対するハートビートアラートを最小限に抑える方法 1980
Azureクラウドコネクタを使用してAzureサーバを追加できない 1981
Deep SecurityでAzureサブスクリプションの一部の仮想マシンが表示されない 1982
Log4jの脆弱性に対するDeep Securityの対応範囲 1982
Log4jの脆弱性に対する仮想パッチの適用 1983
影響を受ける可能性のあるホストの特定 1985
セキュリティログ監視 ルールを使用してアクティビティを調査する 1985
この脆弱性に関するトレンドマイクロのその他のリソース 1985
トラブルシューティング 1986
オフラインエージェント 1986
原因 1986
Agentが実行されていることを確認する 1987
DNSを検証する 1988
送信ポートを許可する(Agentからのハートビート) 1988
受信ポートを許可する(Managerからのハートビート) 1989
Amazon AWS EC2インスタンスでICMPを許可する 1990
Solaris 11でのアップグレードの問題を解決する 1990
CPU使用率が高い 1991
Agent配信での問題の診断 (Windows) 1992
VMwareの「不正プログラム対策ドライバがオフライン」ステータス 1992

Windowsプラットフォーム用不正プログラム対策のアップデート失敗 1992
互換性のない他のトレンドマイクロ製品の不正プログラム対策コンポーネント 1993
互換性のないサードパーティ製品の不正プログラム対策コンポーネント 1993
証明書がトレンドマイクロによって署名されていない場合 1993
署名された証明書が信頼されていない場合 1994
署名された証明書が適切な目的で認証されていない場合 1994
その他/不明なエラー 1994
Agentレスによる仮想マシンのパフォーマンスの問題 1995
原因: 限られたリソース 1995
原因: 不正プログラム対策 1995
原因: ネットワークトラフィック 1995
原因: ポリシー 1996
原因: CPU使用率が高い 1996
原因: セキュリティアップデート 1996
セキュリティアップデートの接続 1997
SQL Serverドメイン認証の問題 1997
手順1: ホスト名とドメインを確認する 1998
手順2: servicePrincipalName (SPN) を確認する 1999
手順2a: SQL Serverサービスを実行しているアカウント(SID) を特定する 2000
手順2b: Active Directoryでアカウントを確認する 2002
手順2c: SPNで使用するFQDNを特定する 2003
手順2d: 初期設定のインスタンスを使用しているのか、名前付きインスタンスを使用しているのかを特定する 2003
ケース1: ローカル仮想アカウントでSPNを設定する 2004
ケース2: ドメインアカウントでSPNを設定する 2006
ケース3:管理されたサービスアカウントでSPNを設定する 2008
ケース4: フェールオーバークラスタのSPNを設定する 2010
SPNリファレンス 2012
SPNのデバッグのヒント 2012

手順3: krb5.confファイルを確認する(Linuxのみ) 2013
手順4: システム時計を確認する 2015
手順5: ファイアウォールを確認する 2015
手順6: dsm.propertiesファイルを確認します 2016
複数のAmazon Virtual Private Cloud (VPC) からのAgent通信でMTUが原因で発生する問題の回避 2017
診断パッケージの作成 2019
Deep Security Managerの診断 2019
Deep Security Managerのデバッグログを有効にする 2019
Deep Security Manager の Java Flight Recorder を有効にする 2020
Deep Security Managerの診断パッケージを作成する 2021
Deep Security Agentの診断 2021
Deep Security Managerを使用してAgentの診断パッケージを作成する 2022
保護されているコンピュータでCLIを使用してAgentの診断パッケージを作成する 2022
DebugViewを使用してデバッグログを収集する 2023
詳細な診断パッケージのプロセスメモリを増やす 2024
旧バージョンのソフトウェアの削除 2025
Azure コード署名のトラブルシューティング 2025
IoTイベント過負荷アラートのトラブルシューティング 2027
SELinuxアラートのトラブルシューティング 2027
SELinuxがDeep Security Agentサービスをブロックする 2027
Berkeley Packet Filter (BPF) 操作がブロックされる 2028
ネットワークエンジンのステータス (Windows OS) 2030
ネットワークエンジンステータスの警告 2030
ドライバのステータスの確認 2031
ネットワークエンジンステータスの警告を無効にする 2031
PDF 2031
Deep Security管理ガイド 2031
Deep Securityのベストプラクティスガイド 2032

Trend Micro Deep Securityについて

Deep Security 20リリース戦略およびライフサイクルポリシー

Deep Security 20は、長期サポート(LTS) リリースです。リリース管理とライフサイクルの変更は、お客様やパートナーがより簡単に行えるように設計されています。

- Deep Security 20のアップデートには、新機能と修正の両方が含まれています。
- 機能リリース(FR) は利用できなくなりました。

Deep Security Managerは古いバージョンのDeep Security Agentをサポートしていますが、可能であればエージェントをアップグレードするべきです。新しいエージェントのリリースは、より高いセキュリティと保護、高品質、パフォーマンスの向上、OSリリースとの同期を維持するための更新を提供します。定期的なソフトウェアのアップグレードにより、エージェントの修正が必要な場合、一度の更新で済み、サポートされているアップグレードパスに沿って複数の更新をインストールする必要がなくなります。各エージェントにはサポート終了日があります。詳細は、Deep Security Agent LTSライフサイクル日およびDeep Security Agent FRライフサイクル日を参照してください。

サポートされるアップグレードパス

Deep Securityは、アップグレード対象のリリースがサポート期間内である限り、すべてのDeep Securityコンポーネントの最後の2つのメジャーリリースからのアップグレードをサポートします。アップグレードされるバージョンがサポートされていることを確認するために、LTSリリースのサポート期間またはFRリリースのサポート期間を参照してください。

サポート終了日まで次のバージョンからDeep Security 20にアップグレードできます。

- Deep Security 11(LTS)
- Deep Security 12(LTS)
- Deep Security 12(FR)

また、現在サポートされているDeep Security 20リリースを最新のアップデートリリースにアップデートすることもできます。以前のリリースへのロールバックはサポートされていません。

Deep Security 20のアップデートスケジュール

以前のLTSリリースと同様に、Deep Security 20のアップデートは毎月リリースされます。必要に応じて(重大な修正や脆弱性のためなど)、より頻繁にリリースされることがあります。

各コンポーネントは独立してリリースされる場合があります。異なるプラットフォーム(Windows、Linux、Unix)のエージェントも別々にリリースされる場合があります。アップデートには、1つ以上のコンポーネントおよびプラットフォームが含まれることがあります。通常、グローバルリリースプロセスはリリース日から1週間以内に完了し、その時点でダウンロードセンターを通じてアップデートが利用可能になります。

現在サポートされているソフトウェアリリースに修正が必要な場合、トレンドマイクロはサポート期間中に直接適用できるアップデートをリリースします。例えば、Deep Security 20 Update 2を使用していて問題が発生した場合、最新のアップデート(例えば、Deep Security 20 Update 10)がリリースされると、Update 2からUpdate 10に直接アップデートすることができます。

LTSリリースのサポート期間とアップグレードのベストプラクティス

ソフトウェアの更新プロセスは、明確に定義され、定期的にスケジュールされ、理想的には自動化されるべきであり、すべてのコンポーネントが定期的に更新されるようにしてください。

次の表は、更新のリリース時間枠、リリースされたコンポーネントのサポート期間、およびアップグレード戦略を決定する際に考慮すべき事項をまとめたものです。

Deep Security 20 LTSのアップデートは複数年にわたっており、2023年にサポート期間が変更されました。2023年以前は、サポートはアップデートのリリース年に基づいていましたが、2023年以降は特定のリリース日に基づいています。例えば、リリースされたすべてのDeep Security 20 LTSのアップデート:

- 2020年の標準サポートは2023年12月31日まで、延長サポートは2024年12月31日までです。
- 2021年の標準サポートは2024年12月31日まで、延長サポートは2025年12月31日までです。
- 2022年の標準サポートは2025年12月31日まで、延長サポートは2026年12月31日までです。
- 2023年7月25日に標準サポートが2026年7月24日まで、延長サポートが2027年7月24日まで提供されます。
- 2024年3月20日に標準サポートは2027年3月19日まで、延長サポートは2028年3月19日まで提供されます。

コンポーネント	更新がリリースされました	サポート	アップグレードに関する考慮事項
Deep Security	LTSアップデートは毎	2023年	

コンポーネント	更新がリリースされました	サポート	アップグレードに関する考慮事項
Manager	月リリースされます	以前: リリース年から3年間の標準サポート。 リリース年の4年後まで延長サポート。 2023年以降: リリース日から3年間の標準サポート。 リリース日から4年間の延長サポート。	
Deep Security Agent	LTSアップデートは毎月リリースされます	2023年以前: リリース年から3年間の標準サポート。 リリース年の4年後まで延長サポート。 2023年以降: リリース日から3	LTS Agentは、サポート期間内の過去2回のメジャーリリース(Deep Security Agent 11.0からDeep Security Agent 20 LTSなど) からのアップグレードをサポートします。サポート対象のリリースを常に使用し、1回のアップグレードで最新のソフトウェアにアップグレードできるように、定期的なアップグレードを計画してください。

コンポーネント	更新がリリースされました	サポート	アップグレードに関する考慮事項
		年間の標準サポート。リリース日から4年間の延長サポート。	
Deep Securityエージェント(そのプラットフォームの最新エージェントが古いリリースであるプラットフォーム)	LTSアップデートは毎月リリースされます	プラットフォーム固有	プラットフォームでサポートされているのが、古いリリースのDeep Security Agentのみである場合 (たとえば、Windows 2000では9.6のAgent、Red Hat Enterprise Linux 5では10.0のAgent)、そのプラットフォームの最新のAgentを使用し、アップデートがリリースされたらアップグレードしてください。各プラットフォームでサポートされるAgentのバージョンの詳細については、"Deep Security Agentのプラットフォーム" on page 400を参照してください。
Deep Security Relay	LTSアップデートは毎月リリースされます	Agentと同じ	Deep Security Relayは、Relay機能を有効にしたDeep Security Agentです。Agentのアップグレードの推奨事項とサポートポリシーがRelayにも適用されます。
Deep Security Virtual Appliance	Deep Securityの各LTSリリースでリリース	リリース年から5年後までサポート。詳細については製品Q&Aを参照してください。	アプライアンスのSVM - 毎年アップグレードを計画しています。 組み込みAgent - 次のいずれかのスケジュールを使用してアップグレードを計画してください: • 少なくとも年に一度 • 新しい互換性のあるAgentが使用可能な場合はいつでも • 定期的にサポート対象のリリースにアップグレードし、1回のアップグレードで最新のソフトウェアにアップグレードできるようにします。

サポートサービス

サポートサービスについては製品Q&Aを参照してください。

Agentプラットフォームサポートポリシー

トレンドマイクロは、長年にわたってOSを使用し続ける必要がある場合があることを認識しています。エージェントプラットフォームサポートポリシーは、プラットフォームの寿命にわたって予測可能なサポートを提供するように設計されています。

- 多くのプラットフォームがサポートされています。"Deep Security Agentのプラットフォーム" on page 400を参照してください。

- プラットフォームは、少なくともOSベンダーの延長サポート終了日までサポートされます。トレンドマイクロはこの日付を超えてサポートを延長する場合があります。ただし、OSベンダーがプラットフォームをサポートしなくなった場合、OSベンダーのサポートなしでは一部の技術的な問題を解決できないリスクがあります。このような事態が発生した場合、トレンドマイクロは直ちに通知しますが、機能の喪失が生じる可能性があります。

- トレンドマイクロは、プラットフォームのサポートを終了する必要がある場合、事前に通知します。

- ソフトウェアの一般提供 (GA) 後、OSベンダーがプラットフォームのサポートを停止しない限り、トレンドマイクロはサポートライフサイクルを短縮しません。

- エージェントバージョンのサポート期間を考慮してください。例えば、エージェント11.0、12.0など (LTSリリース) は、3年間の標準サポートと4年間の延長サポートがあります。それ以上の期間OSを使用する予定がある場合は、常にサポートされているエージェントバージョンを使用するために、定期的にエージェントをアップグレードする準備をしておく必要があります。

- 通常、Agentの新しいバージョンは、サポートされているすべてのプラットフォーム用にリリースされます。ただし、古いプラットフォームをサポートするには、配信に以前のリリースのAgentを含める必要がある場合があるため、サポート終了日は適宜調整されます。

  たとえば、Windows 2000の最新のAgentはDeep Security Agent 9.6であるため、他の配信環境ではDeep Security Agent 11.0が使用されていても、Deep Security Manager 11.0でサポートされます。したがって、このコンテキストでは、古いAgentはDeep Security Deep Security 11.0のEOLを使用します。

ヒント: OSベンダーから最新のパフォーマンスおよびセキュリティアップデートを取得するために、トレンドマイクロはエージェントが利用可能な最新のOSバージョンにアップグレードすることを強くお勧めします。

Deep Security ライフサイクルの日付

Deep Security LTS ライフサイクル日付

RSSで登録

トレンドマイクロの最新のサポート終了通知を参照して、マイルストーンの定義と標準的なタイムラインの詳細をご確認ください。

Deep Security Managerは古いバージョンのエージェントの使用をサポートしています ("Deep Security Agentのプラットフォーム" on page 400を参照) が、トレンドマイクロはエージェントを定期的にアップグレードすることを推奨します。新しいエージェントのリリースには、追加のセキュリティ機能と保護、品質の向上、パフォーマンスの改善、および各プラットフォームベンダーのリリースに同期するための更新が含まれています。

詳細については、"Deep Security 20リリース戦略およびライフサイクルポリシー" on page 116をご覧ください。機能リリースに関する情報については、"Deep Security FRライフサイクルの日付" on page 128をご覧ください。

日本地域向けの製品は、地域固有のポリシーに基づいて取り扱われます。詳細については、End-of-Life トレンドマイクロ製品およびバージョンをご覧ください。

Deep Security LTSリリースライフサイクル日付

次の表は、各Deep Security長期サポート(LTS) リリースの日付を示しています。これらの日付は、リリース内のすべてのコンポーネント(マネージャ、エージェント、リレー、セキュリティ更新) のライフサイクルを定義しますが、"サポート拡張機能" on page 123に記載されている項目は除外されます。

Version	コンポーネント	プラットフォーム	GA date	標準サポートの終了	拡張サポート終了(EOL)
Deep Security 9.0	すべて	すべて	2013年2月11日	2017年12月31日	Deep Security 10.0で拡張サポートが導入されました。用語と定義については、トレンドマイクロ End-of-Life Notice を参照してください。 これらのバージョンはサポート終

Version	コンポーネント	プラットフォーム	GA date	標準サポートの終了	拡張サポート終了(EOL)
Deep Security 9.5	すべて	すべて	2014年8月13日	2018年8月17日	了となりました。
Deep Security 9.6	すべて	すべて	2015年8月12日	2018年8月12日	
Deep Security 10.0	すべて	すべて	09-Mar-2017	2020年3月9日	09-Mar-2021
Deep Security 11.0	すべて	すべて	2018年5月22日	2021年5月23日	2022年5月22日
Deep Security 12.0	すべて	すべて	20 Jun-2019	2022年6月20日	2023年6月20日
Deep Security 20(一般提供および2020年にリリースされたすべてのアップデート)	すべて	すべて	2020	2023年12月31日	2024年12月31日
Deep Security 20(2021年にリリースされたすべてのアップデート)	すべて	すべて	2021	2024年12月31日	2025年12月31日
Deep Security 20(2022年にリリースされたすべてのアップデート)	すべて	すべて	2022	2025年12月31日	2026年12月31日
Deep Security 20(2023年以降にリリースされたすべてのアップデート)	すべて	すべて	2023年以降	リリース日からちょうど3年後	リリース日からちょうど4年後

Deep Security Virtual Applianceのリリースライフサイクルの日付

日本地域向けの製品は、地域固有のポリシーに基づいて取り扱われます。詳細については、Trend Micro Deep Security Virtual Appliance の製品サポート終了に関するご案内をご覧ください。

サポート拡張機能

次の表は、上記のライフサイクルの日付の特定の拡張子を定義しています。

プラットフォーム	コンポーネント	Version	アップデート済み (EOL)	詳細情報
Windows 2000	Agent	Deep Security 9.6	2025年12月31日 1	トレンドマイクロ Server and Endpoint Protection エージェント更新されたバイナリのための最小Windowsバージョン要件 2023年2月中旬以降 Deep Security Windows 2000 プラットフォームサポート更新 Windows 2003、Windows XP、および Windows 2000 ベースのシステムを保護するための Trend Micro Deep Security の使用方法に関する最新ガイダンス "Agentプラットフォームサポートポリシー" on page 120に従ってサポートを継続します
Windows 2003	Agent	Deep Security 10.0	2025年12月31日 1	トレンドマイクロ Server and Endpoint Protection エージェント更新されたバイナリのための最小Windowsバージョン要件 2023年2月中旬以降 Deep Security Windows 2003 プラットフォームサポート更新。 Windows 2003、Windows XP、および Windows 2000 ベースのシステムを保

プラットフォーム	コンポーネント	Version	アップデート済み (EOL)	詳細情報
				護するための Trend Micro Deep Security の使用方法に関する最新ガイダンス "Agentプラットフォームサポートポリシー" on page 120に従ってサポートを継続します
Windows XP	Agent	Deep Security 10.0 Update 25 以前	20-Jul-2024	トレンドマイクロ Server and Endpoint Protection エージェント更新されたバイナリのための最小Windowsバージョン要件 2023年2月中旬以降 Windows 2003、Windows XP、および Windows 2000 ベースのシステムを保護するための Trend Micro Deep Security の使用方法に関する最新ガイダンス "Agentプラットフォームサポートポリシー" on page 120に従ってサポートを継続します
Windows 7	Agent	Deep Security 20.0.0	2026年12月31日	2024年から、2024年1月のアップデートリリースにおけるDeep Security Agentバージョン改訂のプラットフォームサポート更新に従って、限定的なサポートが提供されます
Windows Server 2008	Agent	Deep Security 20.0.0	2026年12月31日	2024年から、限定的なサポートが提供され、条件付きの修正が利用可能になります。詳細は、2024年1月のアップデートリリースにおけるDeep Security Agentバージョン改訂のプラットフォームサポート更新をご覧ください

プラットフォーム	コンポーネント	Version	アップデート済み (EOL)	詳細情報
Windows 8.1	Agent	Deep Security 20.0.0	2026年12月31日	2024年から、2024年1月のアップデートリリースにおけるDeep Security Agentバージョン改訂のプラットフォームサポート更新に従って、限定的なサポートが提供されます
CloudLinux 5 (32ビットおよび64ビット)	Agent	Deep Security 9.6	2025年12月31日 1	"Agentプラットフォームサポートポリシー" on page 120に従ってサポートを継続します
クラウドLinux 6 (32ビット)	Agent	Deep Security 10.0	2025年12月31日 1	"Agentプラットフォームサポートポリシー" on page 120に従ってサポートを継続します
Cloud Linux 6 (64ビット)	Agent	Deep Security 11.0	2025年12月31日 1	"Agentプラットフォームサポートポリシー" on page 120に従ってサポートを継続します
Debian 6	Agent	Deep Security 9.6	2025年12月31日 1	"Agentプラットフォームサポートポリシー" on page 120に従ってサポートを継続します
Debian 7	Agent	Deep Security 12.0	2025年12月31日 1	"Agentプラットフォームサポートポリシー" on page 120に従ってサポートを継続します
Debian 8	Agent	Deep Security 20.0.0	2026年12月31日	2024年から、2024年1月のアップデートリリースにおけるDeep Security Agentバージョン改訂のプラットフォームサポート更新に従って、限定的なサポートが提供されます
Oracle Linux 5	Agent	Deep Security 10.0	2025年12月31日 1	"Agentプラットフォームサポートポリシー" on page 120に従ってサポートを継続します
Red Hat Enterprise	Agent	Deep Security	2025年12月31	"Agentプラットフォームサポートポリシー" on page 120

プラットフォーム	コンポーネント	Version	アップデート済み (EOL)	詳細情報
Linux 5		10.0	日 1	
SUSE Linux Enterprise Server 11	Agent	Deep Security 12.0	2025年12月31日 1	"Agentプラットフォームサポートポリシー" on page 120
Ubuntu 10、12	Agent	Deep Security 9.6	2025年12月31日 1	"Agentプラットフォームサポートポリシー" on page 120に従ってサポートを継続します
Ubuntu 14	Agent	Deep Security 10.0	2025年12月31日 1	"Agentプラットフォームサポートポリシー" on page 120に従ってサポートを継続します
CentOS 5	Agent	Deep Security 10.0	2025年12月31日 1	"Agentプラットフォームサポートポリシー" on page 120に従ってサポートを継続します
AIX 6.1	Agent	Deep Security 20.0.0	2026年12月31日	2024年から、2024年1月のアップデートリリースにおけるDeep Security Agentバージョン改訂のプラットフォームサポート更新に従って、限定的なサポートが提供されます

脚注:

1

このプラットフォームは現在、古いバージョンのDeep Security Agentを使用してサポートされています。このプラットフォームのサポートはこの日付以降延長されません。"Agentプラットフォームサポートポリシー" on page 120も参照してください。日本地域のレガシーOSサポートについては、End-of-Life トレンドマイクロ製品とバージョンを参照してください。

過去のサポート拡張のアーカイブ

プラットフォーム	コンポーネント	Version	アップデート済み(EOL)	詳細情報
すべて	Appliance	Deep Security 9.5	2018年8月12日	このEOLを適用するには、Deep Security Virtual Appliance 9.5の組み込みエージェントをバージョン9.6にアップグレードする必要があります。これを行わない場合は、2018年8月17日のEOL日が適用されます。組み込みエージェントをバージョン9.6以降にアップグレードしても、EOL期間は延長されません。
Windows 2000	Agent	Deep Security 8.0	2018年8月12日	Deep Security Windows 2000 プラットフォームサポート更新 Windows 2003、Windows XP、および Windows 2000 ベースのシステムを保護するための Trend Micro Deep Security の使用方法に関するガイダンスを更新しました
Solaris	Agent	Deep Security 9.0	2017年12月31日	
HP-UX	Agent	Deep Security 9.0	2020年3月9日	Deep Security Manager 10.0でのみサポートされています。 Deep Securityを使用したHP-UXプラットフォームのサポート
AIX	Agent	Deep Security 9.0	2020年12月31日	
Windows XP Embedded	Agent	Deep Security 9.6	2021年3月9日	
SUSE Linux Enterprise	Agent	Deep Security	2021年5月23	Deep Security SuSE Enterprise Linux 10 プラットフォームサポート

プラットフォーム	コンポーネント	Version	アップデート済み (EOL)	詳細情報
Server 10 SP3、SP4 (32 ビットおよび64 ビット)		9.6	日	更新

Deep Security FR ライフサイクルの日付

RSSで登録

Please refer to トレンドマイクロの最新のEnd-of-Life Policyをご参照ください。マイルストーンの定義と標準的なタイムラインについての詳細情報があります。

注意: ソフトウェアリリースの数を減らし、サポートポリシーの理解を簡素化するために、トレンドマイクロはDeep Security 20のリリース後、Feature Releases (FR)のリリースを終了します。"Deep Security 20リリース戦略およびライフサイクルポリシー" on page 116をご覧ください。

日本地域向けの製品は、地域固有のポリシーに基づいて取り扱われます。詳細については、End-of-Life トレンドマイクロ製品およびバージョンをご覧ください。

Deep Security FR リリースライフサイクルの日付

次の表は、各Deep Security機能リリース(FR)の日付を示しています。これらの日付は、リリース内のすべてのコンポーネント(マネージャー、エージェント、リレー、セキュリティ更新)のライフサイクルを定義しますが、"サポート拡張機能" on page 130に記載されている項目は除外されます。

Version	コンポーネント	プラットフォーム	ビルド番号	GA date	サポートの終了
Deep Security 10.1	すべて	すべて	10.1.*	2017年7月11日	2018年11月22日
Deep Security 10.2	すべて	すべて	10.2.*	2017年11月24日	2018年11月22日

Version	コンポーネント	プラットフォーム	ビルド番号	GA date	サポートの終了
Deep Security 10.3	すべて	すべて	10.3.*	2018年1月18日	2018年11月22日
Deep Security 11.1	すべて	すべて	11.1.*	2018年7月16日	2012年12月20日
Deep Security 11.2	すべて	すべて	11.2.*	2018年10月10日	2012年12月20日
Deep Security 11.3	すべて	すべて	11.3.*	2019年1月7日	2012年12月20日
Deep Security 12 FR 2019-10-23	Manager	すべて	12.5.349	2019年10月23日	2021年4月23日
Deep Security 12 FR 2019/12/12	Manager	すべて	12.5.494	2017年12月12日	2021年6月12日
Deep Security 12 FR 2020/01/27	Manager	すべて	12.5.613	2020年1月27日	2021年7月27日
Deep Security 12 FR 2020/03/09	Agent	Windows	12.5.0-713	2020年3月9日	2021年9月9日
Deep Security 12 FR 2020/03/09	Manager	すべて	12.5.732	2020年3月9日	2021年9月9日
Deep Security 12 FR 2020/04/02	Agent	Linux	12.5.0-814	2020年4月2日	2021年10月2日
Deep Security 12 FR 2020/04/16	Agent	Windows	12.5.0-834	2020年4月16日	2021年10月16日
Deep Security 12 FR 2020/04/29	Manager	すべて	12.5.855	2020年4月29日	2021年10月29

Version	コンポーネント	プラットフォーム	ビルド番号	GA date	サポートの終了
					日
Deep Security 12 FR 2020/05/19	Agent	Linux	12.5.0-936	2020年5月20日	2021年11月19日
Deep Security 12 FR 2020-06-17	Manager	すべて	12.5.985	2020年6月17日	2021年12月17日
Deep Security 12 FR 2020-06-17	Agent	すべて	12.5.0-1033	2020年6月17日	2021年12月17日

サポート拡張機能

次の表は、上記のライフサイクルの日付の特定の拡張子を定義しています。

バージョン	コンポーネント	プラットフォーム	アップデートされたlife of life	詳細情報
Deep Security 10.1、10.2、10.3	Deep Security AgentのLinuxカーネルアップデート	Linux	2019年11月22日	Deep Security 10.x 機能 リリースエージェントのための Linux カーネル更新の拡張
Deep Security 11.1、11.2、11.3	Deep Security AgentのLinuxカーネルアップデート	Linux	2020年12月31日	Deep Security Agentオペレーティングシステム用 カーネルバージョンパッケージのインポート

Deep Securityコンポーネントについて

Trend Micro Deep Securityは、物理サーバ、仮想サーバ、およびクラウドサーバに高度なサーバセキュリティを提供します。企業のアプリケーションやデータを保護し、緊急でのパッチ適用を必要とすることなくデータ漏えいやビジネスの中断を防ぎます。この包括的な中央管理プラットフォームにより、セキュリティに関する処理を簡素化すると同時に、仮想化およびクラウドプロジェクトのROIを向上できます。

Deep Securityで使用可能な保護モジュールについては、"Deep Security保護モジュールについて" belowを参照してください。

Deep Securityは、保護のために連携して使用する、次のコンポーネントで構成されています。

- Deep Security Managerは、集中管理されたWebベースの管理コンソールで、管理者がセキュリティポリシーを設定し、施行コンポーネント(Deep Security Virtual ApplianceおよびDeep Security Agent) に保護を配信するために使用します。
- Deep Security Virtual Appliance は、VMware vSphere環境向けに構築されたセキュリティ仮想マシンで、vShield環境の仮想マシンに不正プログラム対策および整合性監視の保護モジュールをエージェントなしで提供します。NSX環境では、不正プログラム対策、変更監視、ファイアウォール、侵入防御、Webレピュテーションの各モジュールをAgentレスで利用できます。
- のDeep Security Agentの は、アプリケーション制御、アンチマルウェア、Webレピュテーションサービスを提供するコンピュータに直接展開セキュリティエージェントである、ファイアウォール、侵入防止、整合性の監視、およびそれがインストールされているコンピュータにログ検査保護。
- Deep Security Agentには、Relay モジュールが含まれています。リレー対応エージェントは、Deep Securityコンポーネントのネットワーク全体にソフトウェアおよびセキュリティのアップデートを配信します。
- Deep Security Notifier は、Windowsタスクバーのアプリケーションで、セキュリティステータスとイベントに関する情報をローカルコンピュータに送信します。また、リレー対応エージェントの場合は、ローカルコンピュータから配信されるセキュリティアップデートに関する情報も提供します。

Deep Security保護モジュールについて

Trend Micro Deep Securityでは、緊密に統合された次の各モジュールを使用して、セキュリティ機能を簡単に拡張できます。

- "侵入防御 " on the next page
- "不正プログラム対策 " on the next page
- "ファイアウォール " on the next page
- "Webレピュテーション " on the next page
- "変更監視 " on page 133
- "セキュリティログ監視 " on page 133
- "アプリケーションコントロール" on page 133
- "デバイスコントロール" on page 133

侵入防御

侵入防御モジュールは、受信/送信トラフィックを検査することで不審なアクティビティを検出してブロックし、既知またはゼロデイの脆弱性に対する攻撃を防ぎます。Deep Securityでは「仮想パッチ」をサポートしており、パッチが適用されるまでの間、侵入防御ルールを使用して既知の脆弱性に対する攻撃にさらされないようにすることができます。これは、さまざまな規制に準拠する際に重要な役割を果たします。新しいルールを自動で受信するようにDeep Securityを設定すれば、新たな脆弱性が検出された場合も、いち早く対応するルールを受け取ることができます。

侵入防御モジュールは、コード修正が完了するまでの間、SQLインジェクション攻撃、クロスサイトスクリプティング攻撃、およびその他のWebアプリケーションの脆弱性からWebアプリケーションとデータを保護します。

詳細については、"侵入防御の設定" on page 908を参照してください。

不正プログラム対策

不正プログラム対策モジュールは、WindowsおよびLinuxのワークロードを不正プログラム、スパイウェア、トロイの木馬などの不正なソフトウェアから保護します。Trend Micro™ Smart Protection Network™により強化された不正プログラム対策モジュールを使用すると、不正プログラムを特定および削除し、コマンドおよび制御サーバとして知られているドメインをただちにブロックできます。

詳細については、"不正プログラム対策を有効化して設定する" on page 828を参照してください。

ファイアウォール

ファイアウォールモジュールは受信/送信トラフィックを制御し、監査用にファイアウォールログを生成します。

詳細については、"Deep Securityファイアウォールの設定" on page 954を参照してください。

Webレピュテーション

最近の攻撃の多くは、不正プログラムを配信するURLにアクセスすることから始まります。Webレピュテーションモジュールは、犯罪者が使用する不正ドメインや既知のC&Cサーバへのアクセスをブロックするコンテンツフィルタを提供します。WebレピュテーションモジュールはTrend Micro Smart Protection Networkと連携しているため、新たな脅威を迅速かつ正確に特定することが可能です。

詳細については、"Webレピュテーションを設定する" on page 898を参照してください。

変更監視

変更監視モジュールでは、インスタンスに対する許可された変更と許可されない変更の両方を追跡し、意図しない不正な変更があった場合にアラートを受け取ることができます。許可されない変更を検出する機能は、クラウドセキュリティ戦略における非常に重要な要素です。この機能によって、インスタンスの感染につながる可能性のある変更に対する可視性が提供されるためです。

詳細については、"変更監視の設定" on page 1004を参照してください。

セキュリティログ監視

セキュリティログ監視モジュールは、システムログをキャプチャして分析し、PCI DSSの要件や組織独自の内部要件に対する監査証拠を提供します。多数のログエントリの中から重要なセキュリティイベントを識別するのに役立ちます。セキュリティログ監視で見つかった不審なイベントをSIEMシステムまたは中央ログサーバに転送するように設定して、関連付け、レポート、およびアーカイブに使用することができます。

詳細については、"セキュリティログ監視" on page 1066を参照してください。

アプリケーションコントロール

アプリケーションコントロールモジュールは、コンピュータの元のソフトウェアと比較し、未承認ソフトウェアや新規ソフトウェアなどの変更点を監視します。アプリケーションコントロールが有効になると、すべてのソフトウェアの変更が記録され、新しいソフトウェアまたは変更されたソフトウェアがファイルシステム上で検出されるとイベントが作成されます。Deep Security Agentで変更が検出されると、ソフトウェアを許可またはブロックしたり、必要に応じてコンピュータをロックダウンできます。

詳細については、" アプリケーションコントロール が有効であることを確認します" on page 1106を参照してください。

デバイスコントロール

デバイスコントロールモジュールは、コンピュータに接続された外部ストレージデバイスへのアクセスを制御します。デバイスコントロールは、データの損失や漏えいを防ぎ、ファイル検索と組み合わせてセキュリティリスクから保護します。

詳細については、「"デバイスコントロールの設定" on page 1001」を参照してください。

このリリースについて

新機能

Deep SecurityのLTSリリースは、毎年提供されており、新機能、既存の機能の拡張機能、およびバグ修正が含まれています。LTSのリリースには、"LTSリリースのサポート期間とアップグレードのベストプラクティス" on page 117に記載されているように、長期サポートが含まれます。LTSリリースが一般公開されると、LTSリリースに対するアップデートは、修正と細かい機能強化のみに限定されます。

Deep Security 20を使用すると、各 コンポーネント(マネージャ、エージェント、アプライアンス)を個別にリリースできます。さまざまなプラットフォームのクライアント(Windows、Linux、Unix)も個別にリリースできます。アップデートには、1つ以上のコンポーネントとプラットフォームが含まれる場合があります。

読む:

- "Deep Security Managerの新機能" below
- "Deep Security Agentの新機能" on page 201
- "Deep Security Virtual Applianceの新機能" on page 397

Deep Security Managerの新機能

Deep Security Manager - 20.0.1123 (20 LTS 更新 2025-12-09)

リリース日: 2025年12月9日

ビルド番号: 20.0.1123

新機能

Ubuntu Linux 24のARMアーキテクチャのサポート: Deep Security Managerは、Ubuntu Linux 24のARMアーキテクチャをサポートします。DSA-12857

機能強化

- Deep Security Managerは現在、スパイウェアイベントでのファイルハッシュ(MD5、SHA1、SHA256)をサポートしています。DSM-1429/DSA-13232

解決された問題

- システムイベントは、常に完全な説明付きでCSVファイルにエクスポートできるわけではありませんでした。これには特定の2205イベントが含まれていました。PCT-77413/DSM-1465
- 期限切れのパスワードを持つユーザは、次回のログイン時にパスワード変更を促されませんでした。PCT-77392/DSM-1395

Deep Security Manager - 20.0.1112 (20 LTS 更新 2025-11-12)

リリース日: 2025年11月12日

ビルド番号: 20.0.1112

新機能

Windows Server 2025のサポート: Deep Security ManagerはWindows Server 2025をサポートしました。DSM-929

Windows 11バージョン25H2のサポート: Deep Security ManagerはWindows 11バージョン25H2をサポートするようになりました。DSA-12978/DSA-12967

Rocky Linux 10のサポート: Deep Security ManagerはRocky Linux 10をサポートしました。DSA-12906/DSA-12903

機能強化

- パスワードが変更されるとユーザはログアウトされます。DSM-1344
- 展開スクリプトによって疑わしいプロキシユーザ名が検出されました。DSM-1336
- Describe a TenantAPIレスポンスにactivationCodesフィールドが含まれていません。PCT-69880/DSM-1261

Deep Security Manager - 20.0.1092 (20 LTS 更新 2025-10-08)

リリース日: 2025年10月8日

ビルド番号: 20.0.1092

新機能

Red Hat Enterprise Linux 10のサポート: Deep Security ManagerはRed Hat Enterprise Linux 10をサポートするようになりました。DSM-1335

解決された問題

- AWSのワンクリックアップグレードバナーが「進行中」ステータスで停止しました。PCT-77674/DSM-1388

Deep Security Manager - 20.0.1081 (20 LTS 更新 2025-09-15)

リリース日: 2025年9月15日

ビルド番号: 20.0.1081

新機能

Cisco Identity Services Engine (ISE) との統合: Deep Security Managerは、迅速な脅威封じ込めのためにCisco ISEと統合されました。DSM-1000

機能強化

- Deep Security Agentのアクティベーションは、システムクロックが許容される閾値を超えて前方にずれた場合にブロックされます。PCT-54410/DSM-1006
- センサスクエリを有効にするおよび良好なファイルレピュテーションクエリを有効にする設定がコンピュータ> 設定 > 一般 > センサス、良好なファイルレピュテーション、および機械学習型検索サービスのネットワーク設定に追加されました。PCT-36275/DSM-1201

解決された問題

- AWS Marketplaceの一部のサードパーティ製Oracle Linuxインスタンスが、AWSコネクタインスタンスメタデータによって既知のプラットフォームとして検出されませんでした。DSM-1284
- Workload Securityの移行はVARCHAR(2000)の制限を超えたため失敗しました。PCT-62228/DSM-1112/DSM-1357
- SAML構成で、戻るボタンをクリックした後、予期しない誤った入力値が元の入力値に置き換えられました。DSM-1093/DSM-975

Deep Security Manager - 20.0.1073 (20 LTS 更新 2025-08-20)

リリース日: 2025年8月20日

ビルド番号: 20.0.1073

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DSM-1241

最高共通脆弱性評価システム (CVSS) スコア: 8.8

最高の重大度: 高

Deep Security Manager - 20.0.1059 (20 LTS 更新 2025-07-09)

リリース日: 2025年7月9日

ビルド番号: 20.0.1059

強化

- UAE向けの新しいリージョンAE-1がDeep Security Manager移行ツールに追加されました (サポート > Trend Vision One Endpoint Securityへのアップグレード)。DSM-1041

解決された問題

- スマートフォルダエディタのカレンダーが曜日を誤った順序で表示していました。DSM-1214

Deep Security Manager - 20.0.1054 (20 LTS 更新 2025-06-11)

リリース日: 2025年6月11日

ビルド番号: 20.0.1054

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある情報開示の慣行に従い、すべての影響を受けたリリースに対するパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が提供されます。DSM-975/DSM-923

最高共通脆弱性評価システム (CVSS) スコア: 6.1

重大度: 中

Deep Security Manager - 20.0.1047 (20 LTS 更新 2025-05-12)

リリース日: 2025年5月12日

ビルド番号: 20.0.1047

機能強化

- Active Directoryコネクタ同期中の重複ホストマージのサポート。PCT-51213/DSM-968
- 診断ログウィザードのSyslog Issuesオプションを通じて、syslog関連情報の収集をサポート。DSM-902
- Linuxのドライバーレスモードでは、不正プログラム対策モジュールのステータスが警告の代わりに表示されるようになりました。DSM-884

Deep Security Manager - 20.0.1039 (20 LTS 更新 2025-04-16)

リリース日: 2025年4月16日

ビルド番号: 20.0.1039

新機能

VMware Cloud Director 10.6のサポート: Deep Security Managerは、VMware Cloud Directorバージョン10.6をサポートするようになりました。DSA-921

解決された問題

- システムは、AWS中華人民共和国リージョンに接続する際に、必要な中華人民共和国専用エンドポイントsts.cn-north-1.amazonaws.com.cnの代わりに誤ってsts.cn-north-1.amazonaws.comエンドポイントを使用しました。PCT-55611/DSM-1042
- 変更監視、セキュリティログ監視、侵入防御、またはファイアウォールの新しいルールがルール更新として記録されました。PCT-53113/DSM-996
- 予備のDSRUを削除する際に、既に適用されていたDeep Securityルール更新 (DSRU) が削除されました。PCT-46867/DSM-918
- パフォーマンスプロファイルがスレッドプールサイズが小さいものに切り替えられたとき、誤解を招くエラーメッセージが表示されました。DSM-839/DSM-837
- 送信ポリシージョブの数がタスクバーに誤って表示されていました。PCT-6652/DSM-347/WS-11383

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が提供されることに注意してください。VRTS-13713/DSM-912/WS-13713

最高共通脆弱性評価システム (CVSS) スコア: 2.7

最高深刻度: 低

Deep Security Manager - 20.0.1027 (20 LTS 更新 2025-03-12)

リリース日: 2025年3月12日

ビルド番号: 20.0.1027

機能強化

- Deep Security ManagerでTomcatサーバのバージョンが更新されました。VRTS-13896/DSM-955/DSM-947

解決済みの問題

- Deep Security AgentのTrend Vision One - Server & Workload Protectionへの移行は、移行中に誤ったパブリックCAが使用されたため失敗しました。DSM-995/DSM-1023/WS-10344

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DSM-885/DSM-632

最高共通脆弱性評価システム (CVSS) スコア: 5.3

最高の深刻度: 中

Deep Security Manager - 20.0.1017 (20 LTS 更新 2025-01-15)

リリース日: 2025年1月15日

ビルド番号: 20.0.1017

新機能

Windows Server 2025のサポート: Deep Security Agentは、FIPSモードを含むWindows Server 2025をサポートしました。DSA-7953

FIPSモードが有効なマルチテナントサポート: Deep Security Managerは、連邦情報処理規格 (FIPS) モードが有効な場合にマルチテナントをサポートします。DSM-846

機能強化

- Deep Security Managerの著作権情報が2025年に更新されました。DSM-412
- 新しくインストールされたDeep Security Managerでは、デフォルトのベースライン情報がDeep Security Agentに保存されるようになりました。詳細については、大量の変更監視ベースラインデータによるデータベースのパフォーマンス問題を参照してください。PCT-28475/PCT-19324/DSM-651
- 管理 > システム設定 > プロキシのレガシー説明を更新しました。DSM-758/DSM-749
- 変更監視のsyslogメッセージにEntityTypeフィールドが追加されました。PCT-39385/PCT-47161/DSM-911
- AWS Security Token Service (STS) エンドポイントのテスト手順が改善され、制限されたファイアウォールルールによる問題を回避できるようになりました。PCT-42974/DSM-942
- Deep Security ManagerでTomcatサーバのバージョンが更新されました。VRTS-13877/VRTS-13889/DSM-947/DSM-914

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対するパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DSM-812/DSM-809

最高共通脆弱性評価システム (CVSS) スコア: 5.5

重大度: 中

Deep Security Manager - 20.0.1003 (20 LTS 更新 2024-12-10)

リリース日: 2024年12月10日

ビルド番号: 20.0.1003

機能強化

- リアルタイム不正プログラム対策のCPU使用率は、Linux上でDeep Security Managerコンソールを使用して設定できるようになりました。オプションは、無制限、低、極低のCPU使用率です。DSM-881
- 未使用のシステムイベントは、Deep Security Managerコンソール (管理 > システム設定 > システムイベント) に表示されなくなりました。PCT-3185/PCT-26855/PCT-34591/SEG-179061/DSM-279

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある情報開示の慣行に従い、すべての影響を受けるリリースに対するパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が提供されます。DSM-874/DSM-886

最高共通脆弱性評価システム (CVSS) スコア: 8.5

最高の重大度: 高

Deep Security Manager - 20.0.993 (20 LTS 更新 2024-11-13)

リリース日: 2024年11月13日

ビルド番号: 20.0.993

新機能

Windows 10およびWindows 11でのアプリケーションコントロールのサポート: Deep Security Manager 20.0.993以降では、Windows 10およびWindows 11でアプリケーションコントロールがサポートされるようになりました。DSM-819

機能強化

- 推奨スキャンの経過時間とメモリ使用量の削減。PCT-42518/DSM-896
- トラブルシューティングをより効率的にするためのカスタム入力フィールド。DSM-796
- Trend Vision One登録トークンダイアログのエラーメッセージを改善しました。このメッセージは、ユーザが無効なトークンを入力したときに表示されます。DSM-731
- セキュリティモジュールが無効になっていると、推奨スキャンは実行されません。PCT-11993/PCT-36524/DSM-464

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DSM-879

最高共通脆弱性評価システム (CVSS) スコア: 5.9

重大度: 中

Deep Security Manager - 20.0.979 (20 LTS 更新 2024-10-16)

リリース日: 2024年10月16日

ビルド番号: 20.0.979

新機能

Red Hat Enterprise 9 (PowerPCリトルエンディアン) のサポート: Deep Security Manager 20.0.979以降はRed Hat Enterprise 9 (PowerPCリトルエンディアン) をサポートしています。

機能強化

- Deep Security Managerは、FIPSモードが有効な場合にSAML Single Sign-On (SSO) をサポートします。PCT-17482/DSM-428

解決済みの問題

- vCenterコネクタをNSX-v/Tを導入せずに使用している場合、Deep Security ManagerがDeep Security Virtual Applianceのバージョンを確認した際に、Deep Security Managerのログが記録されないことがあります。DSM-822

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DSM-754

最高共通脆弱性評価システム (CVSS) スコア: 5.3

重大度: 低

Deep Security Manager - 20.0.967 (20 LTS 更新 2024-09-18)

リリース日: 2024年9月18日

ビルド番号: 20.0.967

機能強化

- Deep Security Managerのパフォーマンスプロファイルに新しいより高い容量オプションが追加されました。PCT-1686/PCT-5853/PCT-6181/PCT-7244/PCT-15098/PCT-16008/PCT-18026/DSM-525
- SAP Scannerのステータスは現在、より多くの情報を提供し、他の保護モジュールのステータスの隣に移動されました。DSM-572
- いくつかのエラーメッセージをより情報豊かに改善しました。DSM-788

解決済みの問題

- AWSコネクタは、Deep Security Manager 20.0.904でオプションとしてAWS GovCloudリージョンが欠落しており、同期の問題を引き起こす可能性がありました。PCT-26434/PCT-29880/PCT-30450/DSM-626

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある情報開示の慣行に従い、すべての影響を受けるリリースに対するパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が提供されます。DSM-735/DSM-741

最高共通脆弱性評価システム (CVSS) スコア: 5.8

重大度: 低

Deep Security Manager - 20.0.954 (20 LTS 更新 2024-08-21)

リリース日: 2024年8月21日

ビルド番号: 20.0.954

新機能

ユーザモードソリューション: ユーザモードは、カーネルサポートがないシステムで不正プログラム対策の基本機能を通じてイベント生成と保護を提供するために、Deep Security Manager UIから有効にすることができます。

機能強化

- アプリケーションコントロール Trust Entities ルールのパスプロパティは、ドライブ文字を必要とせずに、ユニバーサルネーミングコンベンション (UNC) パスでワイルドカードを使用できるようになりました。SF06976162/SEG-189907/WS-4290
- アプリケーションコントロール Software Changes ページ (Actions) には、ソフトウェア変更属性または署名者情報(署名者名、発行者共通名、発行者組織単位、発行者組織、発行者所在地、ベンダー、製品名、プロセス名、インストールパス、ファイルパス) が含まれるようになりました。DSM-662
- Service Gateway は、Deep Security Manager(ソフトウェアアップデート、CSSS、ニュースアップデート、製品登録およびライセンス) のプロキシとして構成できるようになりました(管理 > システム設定 > プロキシ > プロキシサーバの使用) 。DSM-518

解決済みの問題

- Deep Security Agentの更新がアプリケーションコントロールのソフトウェア変更イベントを引き起こすことがあります。SF07441007/PCT-9653/PCT-16914/WS-6246
- Deep Security Manager サポートボタンが「404 ページが見つかりません」エラーを引き起こしていました。DSM-784
- Trust Entities によって生成されたアプリケーションコントロールイベントは、ルールセットに関連付けられていても、RULESET 列に「None」と表示されます (Events & Reports > アプリケーションコントロール Events)。DSM-779
- 一部のシステムでKernel Support Package (KSP)が予期せず削除されました。SF08057187/PCT-30396/PCT-36420/DSM-718

Deep Security Manager - 20.0.940 (20 LTS アップデート2024-07-17)

リリース日: 2024年7月17日

ビルド番号: 20.0.940

新機能

Trend Vision One 統合強化: 侵入防御 System ルールが Deep Security Manager で適用され、Trend Vision One - Server & Workload Protection に送信できるようになりました。

Trend Vision One 移行ツール: Deep Security Manager から Trend Vision One Endpoint Security - Server & Workload Protection への移行を支援するツールが利用可能になりました。

機能強化

- Deep Security Manager は、PostgreSQL 15 & 16、AWS Aurora PostgreSQL 15 & 16、および AWS RDS PostgreSQL 15 & 16 をサポートするようになりました。PCT-5186/PCT-32769/DSM-144

解決済みの問題

- リモートデスクトッププロトコルの使用が一部のWindows Server 2022システムで失敗しました。DSM-695
- オンプレミスポリシーまたはDeep Securityエージェントを Trend Vision Oneエンドポイントセキュリティに移行ツールを使用して移行すると、Invalid 'expires' attributeエントリがserver0.logファイルに生成されました。これは移行に影響しませんでした。DSM-657

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。VRTS-11981/DSM-517

最高共通脆弱性評価システム (CVSS) スコア: 9.8

最高の重大度: 重大

Deep Security Manager - 20.0.926 (20 LTS 更新 2024-06-19)

リリース日: 2024年6月19日

ビルド番号:20.0.926

機能強化

- プロセスメモリスキャンにカスタムアクションを設定できるようになりました。プロセスメモリスキャンはリアルタイム、オンデマンド、マニュアルスキャンに適用されます。これには、Deep Security Agentバージョン20.0.1-12510以降が必要です。DSM-539/DSM-656
- エージェントイベント1005: ドライバのアップグレードおよび1007: ドライバのアップグレードに成功しましたのイベントレベルが、警告から情報に変更されました。DSM-440

解決済みの問題

- Deep Security Virtual Appliancesは、管理コンソールでエージェントのアップグレードが推奨されているアラートを見ても、アップグレード可能として表示されない場合があります。PCT-23179/PCT-27324/DSM-589
- 新しいDSRUバージョンを適用し、DSMサービスを再起動せずにロールバックする場合、推奨スキャンは誤って新しいバージョンを引き続き使用し続けます。DSM-577

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある情報開示の慣行に従い、共通脆弱性識別子(CVE)の詳細は、すべての影響を受けるリリースに対するパッチが利用可能になった後にのみ、一部のセキュリティアップデートで利用可能です。VRTS-11810/VRTS-12278/DSM-483/DSM-568

最高共通脆弱性評価システム(CVSS)スコア: 7

最高の重大度: 高

Deep Security Manager - 20.0.913 (20 LTS アップデート2024-05-15)

リリース日: 2024年5月15日

ビルド番号: 20.0.913

機能強化

- TLSトラフィック検査の詳細設定に、受信トラフィックと送信トラフィックを検査するための個別の設定が追加されました。DSM-190
  注意:送信トラフィック検査を有効にするには、エージェント側で追加の設定手順を実行する必要があります。

- Deep Security Managerで、Trend Cloud One - Endpoint & Workload Security移行ウィザードからのService Gatewayプロキシの設定がサポートされるようになりました。Service Gatewayプロキシの使用は、配信されたすべてのDeep Security Agentがバージョン20.0.1-3180以降である場合にのみサポートされます。PCT-12854/DSM-367
- ProxyAPIを使用してService Gatewayプロキシ情報を取得するときに、[hostName] フィールドにデバイスのホスト名が表示されるようになりました。デバイスのIPアドレス情報を提供するために、新しい「ips」フィールドが追加されました。DSM-533

解決済みの問題

- ポリシーでプロキシが設定されている場合、新しいテナントテンプレートを作成すると、内部サーバエラーが発生することがありました。新しいテナントテンプレートの作成時に、ポリシーからプロキシ設定が削除されました。PCT-4709/DSM-306
- Deep Security Managerから証明書のアップデート要求が送信されたときに、Trend Vision OneからHTTP 400エラーが返されました。DSM-593

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能です。VRTS-12054/PCT-25774/DSM-161/DSM-519

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度: 高

Deep Security Manager - 20.0.904 (20 LTS Update 2024-04-17)

リリース日: 2024年4月17日

ビルド番号: 20.0.904

新機能

クロスアカウントAWSロール登録: シードリージョンとセキュリティトークンサービス (STS) エンドポイントの選択は、AWSコネクタウィザードとDeep Security ManagerのAWSアカウントプロパティページを使用して実行できるようになりました。

強化

- Deep Security ManagerでOracle Database 23cがサポートされるようになりました。DSM-366
- Cloud One Endpoint & Workload SecurityのMigration APIのデフォルトのタイムアウトが60秒に変更されました。以前の初期設定は10秒でしたが、Deep Security ManagerからAgentが転送される前にタイムアウトになることがありました。タイムアウトは、`settings.configuration.defaultWorkloadSecurityMigrationApiTimeout`を使用して10 ~ 1200秒 (20分) の範囲で設定できます。PCT-21902/PCT-22361/PCT-22860/PCT-22249/DSM-579
- Deep Security Managerのサードパーティライセンスがアップデートされました。DSM-564
- 一部のシステム設定でのAzureコネクタのパフォーマンスが向上しました。DSM-472

解決済みの問題

- Deep Security Virtual ApplianceのOVFファイルのIPアドレス ([コンピュータ]→[プロパティ]→[NSX設定]→[一般]) への変更が適用されないことがありました。PCT-20529/PCT-23331/DSM-545
- 一部のAzure VM構成で、パブリックIPとネットワークセキュリティグループが仮想マシンの概要に表示されませんでした。DSM-459
- データベース接続の問題により、使用中のDeep Security Agentインストーラが Deep Security Managerによって削除されることがありました。SEG-188888/PCT-7221/PCT-15200/DSM-348
- Deep Security Managerのコンソールでは、プラットフォームが「Windows 10」と表示されるはずのWindows 10 Enterpriseマルチセッションが「Windows Server 2019」と表示されていました。SEG-131712/DS-69474/DSM-326

Deep Security Manager - 20.0.893 (20 LTS Update 2024-03-20)

リリース日: 2024年3月20日

ビルド番号: 20.0.893

機能強化

- 不正プログラム対策手動検索をDeep Security Manager for Linuxプラットフォームのポリシーから設定できるようになりました。DSM-433

解決済みの問題

- イベント転送条件 StringLike および StringNotLike は、Descriptionの複数行でフォーマットされたJSONでは機能しませんでした。SF07518120/PCT-12618/DSM-448
- Deep Security Managerで、トレンドマイクロAdversary Tactics and Techniques Detectionのパターンバージョン(管理 > アップデート> セキュリティ> パターンファイル) がトレンドマイクロUpdate Serverから利用可能になる前に表示されることがありました。DSM-439

Deep Security Manager - 20.0.883 (20 LTS Update 2024-02-21)

リリース日: 2024年2月21日

ビルド番号: 20.0.883

新機能

- Deep Security Managerで、Trend Micro Endpoint BasecampのXDRデバイスIDの動的アップデートがサポートされるようになりました。DSM-250

機能強化

- Webレピュテーションサービスのバックエンドクエリでは、新規インストールおよび新規テナントに対してデフォルトでポート443が使用されるようになりました。PCT-10486/DSM-445
- 不正プログラム対策の設定で、機械学習型検索とWindowsの不正プログラム対策検索インタフェース(AMSI) の設定の初期設定が推奨としてマークされるようになりました。PCT-3844/DSM-301

解決済みの問題

- Deep Security Managerでファイアウォール、Webレピュテーションサービス、または侵入防御システムが有効になっていると、Deep Security Agent 20.0.0-7943、20.0.0-8137、20.0.0-8268、または20.0.0-8438へのアップグレードに失敗することがありました。DSM-473

Deep Security Manager - 20.0.879 (20 LTS Update 2024-01-17)

リリース日: 2024年1月17日

ビルド番号: 20.0.879

新機能

- Deep Security Managerで、NSX ManagerのIPアドレスまたは完全修飾ドメイン名 (FQDN) を変更できるようになりました。DSM-83/DSM-405

機能強化

- Deep Security ManagerでTomcatのバージョンがアップデートされました。DSM-431/DSM-160
- Deep Security Managerのサポートサイトで、無効になりそうなURLが多数更新されました。DSM-352
- Deep Security Managerの著作権情報が2024年に更新されました。DSM-133
- Deep Security Virtual ApplianceのユーザにDeep Security Deep Security ApplianceのEOLステータスを通知する専用のバナーがDeep Security Manager内に表示されるようになりました。DS-76857/DSM-131
- VRTS-10045、VRTS-10068、VRTS-10070のセキュリティアップデート。DSM-133
- Deep Security Managerの著作権情報が2024年に更新されました。DSM-133
- VMware vCenter Connectorが削除されたときに、Deep Security Managerでサービス参照IDを強制的に削除できるようになりました。このサービス参照IDは、トレンドマイクロサービスをセキュリティプロファイルにバインドするためにVMware NSX-Tによって自動的に作成されます。SEG-160298/DSM-49
- 古いコンピュータのステータスは、「最新ではありません (不正プログラム対策設定がオフ)」、「最新ではありません (不正プログラム対策がオフライン)」、および「最新ではありません (Agentがオフライン)」という3つの異なるステータスで表されるようになります。これは、セキュリティパターンステータスウィジェットの機能に直接影響し、ステータスが「Agentがオフライン」、「不正プログラム対策設定がオフ」、および「不正プログラム対策がオフライン」のDeep Security Agentが旧版の詳細検索の結果に含まれないようにします。DSM-135

解決済みの問題

- Azure Connectorで、フレキシブルオーケストレーションモードを使用したAzure仮想マシンスケールセットの同期の問題が発生しました。DSM-436
- Apex Centralに情報がなかったため、Syslogに転送したり、ログビューに表示したりできませんでした。MCPコンテンツがアップデートされて感染ファイルのFileSHA1が含まれていないためです。SEG-192045/PCT-6042/DSM-435
- 不正プログラム対策設定APIのBehaviorMonitoringEnabledプロパティの値が欠落していたため、UIとAPI間の接続が切断されました。PCT-5360/DSM-411

既知の問題

- Deep Deep Security Managerでファイアウォール、Webレピュテーションサービス、または侵入防御システムが有効になっていると、Deep Security Agent 20.0.0 ~ 7943、20.0.0 ~ 8137、20.0.0 ~ 8268、または20.0.0 ~ 8438へのアップグレードに失敗することがあります。DSM-473

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、特定のセキュリティアップデートのCVE (Common Vulnerabilities and Exposures) 詳細が利用可能であることに注意してください。DSM-402

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度 : 高

Deep Security Manager - 20.0.864 (20 LTS Update 2023-12-12)

リリース日 : 2023年12月12日

ビルド番号 : 20.0.864

機能強化

- Microsoftの製品名の変更を反映するようにDeep Security ManagerのUIが更新されました。Azure Active DirectoryがMicrosoft Entra IDになりました。DSM-214
- Deep Security Managerレポート ([イベントとレポート]→[レポートの生成]) は、分類リストから [カスタム] を選択して名前フィールドに入力することで、カスタム分類を使用して生成できるようになりました。SF06301702/SEG-167348/DS-76507/DSM-8
- Deep Security Managerでは、Deep Security Virtual Appliance エージェントソフトウェアのアップグレードを20.0.0バージョンに制限するようになりました。バージョン20.0.1のエージェントはサポートされないことに注意してください。DSM-311
- エージェントの最新バージョンを使用するオプション (コンピュータ > 詳細 > アクション > エージェントソフトウェアのアップグレード) を使用して、サポートが限定されているプラットフォームの Deep Security Agent をアップグレードすると、20.0.1 エージェントバージョンはそのプラットフォームではサポートされていないという警告が表示されるようになりました。DSM-342/DSM-343/DSM-344

解決済みの問題

- Deep Security Manager 20.0.797にアップグレードした後、Apex Centralコンソールの[Deep Securityコンポーネントの概要] ウィジェットに何も表示されませんでした。DSM-236
- [コンピュータ] または [ポリシー]>[上書き] から[削除] または [すべて削除] を使用しても、[アプリケーションコントロールの信頼エンティティの上書き] 設定が削除されませんでした。DSM-120
- [すべてのルールに対するアラート(ルールの設定に関係なく)] が有効になっている場合 ([アラート]>[アラートの設定]>[不正プログラム対策アラート]>[アラート情報]>[オプション])、SAPは生成されたGet Events Failedエラーを検索します。SF05087843/SEG-173393/DS-77098/DSM-28
- `greater than` パラメータを使用したDeep Security Manager APIの検索で、誤った結果が返されることがありました。DSM-325
- Deep Security Managerを再起動するまで、[Agentのアップグレードの予約]画面に誤ったバージョンのエージェントが表示されることがありました。DSM-329

既知の問題

- Deep Deep Security Managerでファイアウォール、Webレピュテーションサービス、または侵入防御システムが有効になっていると、Deep Security Agent 20.0.0 ~ 7943、20.0.0 ~ 8137、20.0.0 ~ 8268、または20.0.0 ~ 8438へのアップグレードに失敗することがあります。DSM-473

Deep Security Manager - 20.0.854 (20 LTS Update 2023-11-15)

リリース日: 2023年11月15日

ビルド番号: 20.0.854

新機能

- Deep Security Managerでは、FIPSモードが有効な場合に強力な暗号化スイートがサポートされるようになりました。DSM-211

機能強化

- Deep Security Managerでは、2024年1月に予定されているDeep Security Agentのバージョン管理リビジョン20.0.1がサポートされるようになりました。DSM-121

解決済みの問題

- 長いメモを含む侵入防御イベントを使用すると、「イベントの取得失敗 (内部サーバエラー)」というエラーメッセージが表示されました。DSM-327
- DNS設定が不完全な一部の環境で、HostNameルックアップが停止していました。DSM-307

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けたリリースに対するパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能です。VRTS-11238/DSM-290

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度: 高

既知の問題

- Deep Deep Security Managerでファイアウォール、Webレピュテーションサービス、または侵入防御システムが有効になっていると、Deep Security Agent 20.0.0 ~ 7943、20.0.0 ~ 8137、20.0.0 ~ 8268、または20.0.0 ~ 8438へのアップグレードに失敗することがあります。DSM-473

Deep Security Manager - 20.0.844 (20 LTS Update 2023-10-18)

リリース日: 2023年10月18日

ビルド番号: 20.0.844

新機能

- Deep Security Managerでは、ポリシーからエージェントの手動検索を設定できるようになりました。DSM-16

機能強化

- [イベントとレポート] の詳細検索で、侵入防御イベントを「フロー」値でフィルタできるようになりました。
  [フロー] フィールドが侵入防御の syslog イベントに追加されました。SF06798790/SEG-177960/DS-77724/DSM-9

- MD5またはSHA-1ファイルハッシュを使用して、アプリケーションコントロールのグローバルブロック別ハッシュルールを設定できるようになりました。(以前はSHA-256のみを使用できました。) SEG-108464/DS-74144/DSM-18
- プロセス名プロパティを使用するアプリケーションコントロール信頼エンティティルールを、Deep Security ManagerのUIでワイルドカードを使用して設定できるようになりました。DS-75316/DSM-18
- 信頼エンティティのプロセス名プロパティで、ローカルエリアネットワーク上のファイルまたは周辺機器への汎用名前付け規則 (UNC) パスを使用できるようになりました。DS-77133/DSM-18
- 信頼エンティティの [対象による許可] ルールでプロセス名プロパティを使用できるようになりました。DS-77364/DSM-18

解決済みの問題

- 役割のプロパティの設定時に、[コンピュータの権限] タブの [警告/エラーのクリア] 権限に変更を適用すると、コンソールに誤った結果が表示されました。DSM-195
- アプリケーションコントロールの共有ルールセットによって、アプリケーションコントロールをサポートしていないシステムに対してポリシーアップデートが実行されることがありました。DS-76766/DSM-18
- 信頼エンティティルールによってAgentで自動承認されたソフトウェアは、共有ルールセットに自動的に追加されなくなりました。これにより、対応する信頼エンティティのルールが適用されなくなった場合に、ソフトウェアが承認されたままになるのを防ぐことができます。DS-74855/DSM-18

既知の問題

- Deep Security Notifier は、Windows で Anti-Malware Protected Process Light (AM-PPL) として展開された場合、起動に失敗することがあります。回避策として、Notifier を AM-PPL として展開することはデフォルトで無効にされています。詳細は Deep Security Notifier サービスが開始または停止できない を参照してください。DSM-297

Deep Security Manager - 20.0.833 (20 LTS Update 2023-09-20)

リリース日: 2023年9月20日

ビルド番号: 20.0.833

機能強化

- 警告とエラーをクリアする権限「canClearWarningsAndErrors」を役割に個別に付与できるようになりました。SF06516228/SEG-168657/DS-77463
- 必要な権限を持たないユーザがデバイスコントロール設定を編集しようとしたときに表示されるエラーメッセージを変更しました。SEG-180964/C1WS-14961/DSM-56
- リアルタイム不正プログラム対策設定の一部の初期設定値が変更されました: DS-77469/C1WS-13588/DSM-36
  - 機械学習型検索: 放置→隔離
  - Windows Antimalware Scan Interface (AMSI): 放置→終了
- スマートフォルダの作成時に、[vCenter Power State] が [コンピュータのプロパティ] オプションになりました。DSM-6/DS-77643
- スマートフォルダのコンピュータのプロパティオプションがアルファベット順に並べ替えられるようになりました。DSM-6/DS-77643

解決済みの問題

- Webコンソールで、AIX 7.3エージェントの [プラットフォーム] フィールドにOSバージョンが表示されないことがありました。DS-72424/DSM-128
- 保護されているコンピュータの数が多い場合、[ユーザ管理]→[役割]→[役割のプロパティ] 画面が読み込まれませんでした。SEG-170672/DS-76826/C1WS-12373/DSM-10
- [不正プログラム対策]→[詳細設定]→[ファイルハッシュ不正プログラム対策] でSHA256が選択されている場合、ファイルのSHA256ハッシュ値がSNS不正プログラム対策イベントに含まれるようになりました。SEG-168652/DS-76448/C1WS-14048/DSM-7
- Deep Security Managerで、予約タスクの実行中に誤った日付が次回実行時に設定されることがありました。この結果、Java DateTimeExceptionが発生し、内部サーバエラーが表示されました。これにより、予約タスクが正常に機能しなくなる可能性がありました。SF07190612/SF07191522/SEG-192240/SEG-192321/DSM-169

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能です。VRTS-10326/DSM-158

最高共通脆弱性評価システム (CVSS) スコア: 6.1

最高の重大度:中

Deep Security Manager - 20.0.817 (20 LTS Update 2023-08-23)

リリース日:2023年8月23日

ビルド番号:20.0.817

機能強化

- Deep Security Managerコンソールに、Trend Micro LightWeight Filter Driverのステータスに関する詳細情報が表示されるようになりました。DS-77465
- セキュリティモジュール使用状況レポートにデバイスコントロール情報を追加します。DS-77319

Deep Security Manager - 20.0.802 (20 LTS Update 2023-07-19)

リリース日:2023年7月19日

ビルド番号:20.0.802

機能強化

- Deep Security Managerがアップデートされ、SQL Server 2022データベースのサポートが追加されました。SF06543523/SEG-169639/SEG-171432/DS-76501
- コンピュータがPodmanホストの場合、コンピュータの詳細にPodmanのバージョンが表示されるようになりました。DS-76683

解決済みの問題

- 新しい予約タスクを作成するときに、[予約タスク] リストに表示される[次回の実行時刻] の値が正しくありませんでした。SF06593263/SEG-171126/DS-76900
- Amazon LinuxプラットフォームでAgentソフトウェアのアップグレード処理が失敗することがありました。DSM-14
- Deep Security ManagerがVision One Service Gatewayと同期できないことがありました。SF06928392/SEG-182692/DSM-19

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリ

リースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。VRTS-6038/DSM-32/DSM-55

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度: 高

Deep Security Manager - 20.0.789 (20 LTS Update 2023-06-28)

リリース日: 2023年6月28日

ビルド番号: 20.0.789

新機能

Trend Vision Oneのインベントリのサポート: Deep Security ManagerとVision Oneの統合で、エンドポイントインベントリ、インベントリグループ、およびインベントリコンプライアンスがサポートされるようになりました。

機能強化

- Deep Security ManagerでPostgreSQL 14がサポートされるようになりました。SF06514546/SEG-169342/DS-76494
- Deep Security ManagerでAWS Aurora PostgreSQL 14がサポートされるようになりました。DS-77594
- Deep Security ManagerでVMware Cloud Director 10.4がサポートされるようになりました。SEG-152378/DS-74227
- Deep Security ManagerでAWS RDS PostgreSQL 14がサポートされるようになりました。DS-76494
- 推奨設定の検索におけるルールの処理を改善。24-024.dsruを適用した後、Deep Security Managerのバージョンが20.0.789(20 LTS Update 2023-06-28) より前の場合、推奨設定の検索が正しく動作しません。PCT-27452/PCT-27565

  詳細はDSM 20.0.789未満でのDSRU 24-024以降のルール適用によるCPU使用率高騰をご参照ください。

解決済みの問題

- エージェントの移行ポップアップウィンドウを開くと、Deep Security Managerコンソールがフリーズすることがあります。SEG-180945/DS-78114

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。VRTS-9496/DS-77146

最高共通脆弱性評価システム (CVSS) スコア: 4.3

最高の重大度 : 中

Deep Security Manager - 20.0.768 (20 LTS Update 2023-05-17)

リリース日 : 2023年5月17日

ビルド番号 : 20.0.768

新機能

デバイスコントロール: Deep Security Manager バージョン 20.0.768 以降は、Windows Server プラットフォーム向けにデバイスコントロールをサポートし、保護されたエンドポイントに接続された外部ストレージデバイスを保護します。これには Deep Security Agent 20.0.0.6313 以降が必要です。詳細については、プラットフォーム別サポート機能を参照してください。

解決済みの問題

- Deep Security Managerで、マルチテナント環境で実行されているDeep Security Agentについて、誤った情報を含むテナントレポートが生成されることがありました。SF06301702/SEG-162798/DS-76311
- Deep Security Managerのダッシュボードで、ステータスウィジェットとイベント履歴ウィジェットにイベントが表示されないことがありました。SF06492268/SEG-168155/DS-76201

Deep Security Manager - 20.0.759 (20 LTS Update 2023-04-19)

リリース日 : 2023年4月19日

ビルド番号 : 20.0.759

強化

- エージェントのアップグレードの予約タスクを設定するときに、エージェントのバージョン管理を使用できるようになりました。SF06094463 / SEG-159727 / DS-74710
- 製品名の変更に伴い、Trend Micro Vision Oneに関する記述はすべてTrend Micro Vision Oneに変更されました。DS-76215

解決済みの問題

- 特定の条件下で、Deep Securityイベントで「コンポーネント「高度な脅威検索エンジン」が削除されました」という誤ったレポートが表示されることがありました。SF05801044 / SEG-147779 / DS-75232
- ホスト数が50,000を超える環境で、管理コンソールの一部のリストがパフォーマンスの問題を引き起こしていました。SF05874881/SEG-149417/DS-72746
  影響を受けるリストには、[システムイベント]、[コンピュータ]、[単一レポート]、[予約レポート]、[予約タスク]、[アラート]、および[ダッシュボード] の下のリストが含まれますが、これらに限定されません。

Deep Security Manager - 20.0.741(20 LTSアップデート2023/03/15)

リリース日 : 2023年3月15日

ビルド番号 : 20.0.741

新機能

Service Gateway: Deep Security Manager バージョン20.0.741 以降では、フォワードプロキシ機能を提供するService Gateway がサポートされるようになりました。

Deep Security Manager - 20.0.737(20 LTSアップデート2023/02/23)

リリース日 : 2023年2月23日

ビルド番号 : 20.0.737

機能強化

- Deep Security Manager 20.0.737以降は、Red Hat Enterprise Linux 9 (64-bit)をサポートしています。SF06130289/SEG-157410/DS-74295

- Deep Security Manager は、サポートされていない証明書を使用しているエージェントに対して、RSA-2048 および SHA-256 への証明書更新を強制します。Deep Security Agent バージョン20.0.0-6313 以降は SHA-1 をサポートしません。詳細については、Deep Security 暗号アルゴリズムのアップグレードを参照してください。DS-76297
- Deep Security Managerがアップデートされ、API スマートフォルダ機能が追加されました。DS-75375

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けたリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DS-75668/DS-75924

最高共通脆弱性評価システム (CVSS) スコア: 8.1

最高の深刻度: 高

Deep Security Manager - 20.0.725(20 LTSアップデート2023/01/18)

リリース日 : 2023年1月18日

ビルド番号 : 20.0.725

解決済みの問題

- コンソールコマンドでsettings.configuration.addPlatformInSyslogMessageがtrueに設定されている場合、syslog転送のためにOS(オペレーティングシステム) フィールドを含むようにDeep Security Managerを更新しました。詳細については、Deep Security Manager (DSM)のsyslogメッセージにAWSインスタンスIDまたはOSフィールドを追加するを参照してください。DS-73163

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けたリリースに対するパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DS-74793

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度 : 高

Deep Security Manager - 20.0.716 (20 LTSアップデート2022-12-15)

リリース日:2022年12月15日

ビルド番号:20.0.716

解決済みの問題

- コンピュータのリストをCSVにエクスポートするときに、Docker ホストおよびCRI-Oホストのフィールド値が正しく含まれていませんでした。SF05232601 / SEG-131041 / DS-73391
- AWSコネクタ経由で登録すると、Deep Security Managerは、ロッキーLinux 8を不明なLinux OSとしてレポートします。DS-71999

Deep Security Manager-20.0.711(20 LTSアップデート2022-11-16)

リリース日:2022年11月16日

ビルド番号:20.0.711

機能強化

- Deep Security Managerがアップデートされ、Google Cloud Platformを使用するコンピュータのプロジェクトIDが追加されました。SF05811253/SEG-147466/DS-72694

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けたリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DS-74218

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度: 高

Deep Security Manager - 20.0.703(20 LTSアップデート2022/10/19)

リリース日:2022年10月19日

ビルド番号:20.0.703

機能強化

- 多要素認証が有効になっている場合、アカウントのパスワードを変更するには、ユーザの古いパスワードに加えてユーザのMFAコードを確認する必要があります。DS-73341
- Deep Security Managerがアップデートされ、コンピュータのステータスバーで信頼エンティティのルールセットの変更がユーザに通知されるようになりました。DS-70956
- Deep Security Managerがアップデートされ、アプリケーションコントロールの信頼ルールの `paths` プロパティフィールドで疑問符を使用して、パス内の1文字を追加できるようになりました。DS-71604
- 信頼エンティティルールに関するDeep Security ManagerのUIツールチップがアップデートされ、最新のワイルドカード機能が説明されました。DS-69964
- 最新のSOAP(Simple Object Access Protocol) コンポーネントを使用するようにDeep Security Managerがアップデートされ、古いバージョンに影響する脆弱性から保護されます。DS-73080

解決済みの問題

- Deep Security Manager によって生成されたレポート(イベントとレポート > レポートの生成) で中国語の文字が正しく表示されませんでした。SF05883379 / SEG-149459 / DS-72858
- 不正プログラム対策イベントで、無効なUnicodeエンコーディングのファイルパスが表示されることがありました。01746052 / SEG-46912 / DSSEG-3653
- 管理者が設定したアプリケーションコントロールルールの権限が、ユーザに対応する機能を提供しませんでした。たとえば、権限が [非表示] に設定されているルールは引き続きユーザに表示され、カスタム設定でユーザが新しいルールを作成できないようにしても、ルールは表示されます。DS-68693
- 信頼エンティティ管理 (ポリシー > 共通オブジェクト > アプリケーション制御ルール > 信頼エンティティ) で、信頼ルールセットの編集ウィンドウの水平スクロールバーが、ウィンドウの下部に表示されるルールを覆っていました。DS-70435

Deep Security Manager - 20.0.686(20 LTSアップデート2022/09/21)

リリース日 : 2022年9月21日

ビルド番号 : 20.0.686

解決済みの問題

- Deep Security AgentでAPIを使用してアプリケーションコントロール共有ルールセットが正常に作成された場合、同じエージェント上でAPIを使用して別の共有ルールセットを作成できませんで

した。DS-71034

- 不正プログラム対策レポート(イベントとレポート> レポートの生成) の項目で、Deep Security Managerが誤った状態を表示することがありました。SF05780825 / SEG-149707 / DS-72871
- 「継続的な推奨スキャンを実行する」を「はい」に設定し、「継続的なスキャン間隔」を4週間に設定すると(「コンピュータまたはポリシー」>「設定」>「一般」>「推奨スキャン」)、Deep Security Managerは設定された間隔よりもはるかに頻繁にスキャンを実行しました。SF05658685/SEG-148153/DSSEG-7707

Deep Security Manager - 20.0.677(20 LTSアップデート2022/08/17)

リリース日:2022年8月17日

ビルド番号:20.0.677

新機能

Windows Server 2022 サポート: Deep Security Manager バージョン20.0.677 以降は、Windows Server 2022 をサポートします。

機能強化

- Deep Security Managerがアップデートされ、ユーザのログイン情報が暗号化されるようになりました。DS-71448

解決済みの問題

- [イベントとレポート]→[ファイアウォールイベント] で、[処理] および [次を含む] フィルタを使用して [Fail Open: Deny] を検索すると、検索結果に一致するイベントが表示されませんでした。SF05740930/SEG-146282/DS-72636
- OSの種類がないVMware vCloudアカウントで、同期に失敗していました。SF05830546 / SEG-147983 / DS-72518
- 25 を超える仮想データセンターを持つVMware vCloud コネクタは、Deep Security Manager で 25 しか表示されませんでした。SEG-147252 / DS-72376
- Deep Security RelayをvCenterコネクタに移動すると、Deep Security Managerで元のホスト名が失われました。SF05519505 / SEG-140015 / DS-72596
- Deep Security Managerで、予期しないコンピュータアップデートシステムイベントが生成されることがありました。SF05496967/SEG-138407/DSSEG-7672

Deep Security Manager - 20.0.664(20 LTSアップデート2022/07/21)

リリース日 : 2022年7月21日

ビルド番号 : 20.0.664

機能強化

- Deep Security Managerがアップデートされ、デフォルトでポート443 (およびポート80および8080) が「有害な可能性があるWebページを監視するポート」 ([コンピュータまたはポリシー]→[Webレピュテーション]→[詳細]) に追加されました。この変更により、ポート443でのWebレピュテーションSSL検査のサポートが、今後リリースされるDeep Security Agentのバージョンに備えられるようになります。
- Deep Security Managerがアップデートされ、`-disablemfa` パラメータが追加されました。このパラメータを使用すると、ユーザは、`dsm_c` コマンドラインを使用してパスワードをリセットするときに、多要素認証 (MFA) を無効にできます。DS-69590

解決済みの問題

- Deep Security ManagerがMicrosoft Active Directory (AD) ユーザと同期できないことがありました。SEG-138257 / SF05452498 / DS-70873

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DS-71624

最高共通脆弱性評価システム (CVSS) スコア: 9.8

最高の重大度 : 重大

Deep Security Manager - 20.0.651(20 LTSアップデート2022/06/15)

リリース日 : 2022年6月15日

ビルド番号 : 20.0.651

強化

- Deep Security Managerがアップデートされ、イベントの原因を示すID、推奨される処理へのリンクなど、不正プログラム対策の詳細が提供されるようになりました。また、SIEMが有効な場合、イベントのシステムログエントリが生成されるようになりました。DS-70595
- Deep Security Managerがアップデートされ、古いバージョンのエージェントインストーラパッケージが削除され、ディスク容量を節約できるようになりました。DS-67840
- Deep Security Managerがアップデートされ、[Active Directoryの追加]ウィザードでActive Directoryコンピュータの追加時にコンピュータの作成に関連するイベントベースのタスクが実行されるようになりました。DS-68877
- Deep Security Managerをアップデートして、8.0および9.0のDeep Security Agentのサポートを終了しました。これらのバージョンはサポート終了日を過ぎているためです。詳細については、「Deep Security LTSライフサイクルの日付」を参照してください。DS-70332

Deep Security Manager - 20.0.644(20 LTSアップデート2022/05/18)

リリース日:2022年5月18日

ビルド番号:20.0.644

解決済みの問題

- Deep Security Managerで列をグループ別に並べ替えた場合([ポリシー] > [共通オブジェクト] > [ルール]または[コンピュータ] > [コンピュータ]の下)、一部のルールが正しく表示されませんでした。SEG-127353/DS-68348
- Agentの有効化でループが発生し、Deep Security Managerで大量のメモリが消費されることがありました。DS-71234

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子(CVE)の詳細が利用可能です。DS-71244/DS-65171

最高共通脆弱性評価システム(CVSS)スコア:7.5

最高の重大度:高

Deep Security Manager - 20.0.635 (20 LTS アップデート2022-04-21)

リリース日 : 2022年4月21日

ビルド番号 : 20.0.635

新機能

高度なTLSトラフィック検査: Deep Security Managerに高度なTLSトラフィック検査を設定するオプションが追加され、TLS資格情報を手動で設定する必要がなくなり、より多くの暗号化のサポートが追加されました。ポリシーのプロパティを表示して、機能のステータスを確認できます (ポリシー > 侵入防御 > 一般 > Advanced TLS Traffic Inspection)。詳細については、高度なTLSトラフィック検査を有効にするを参照してください。

AzureおよびGCPコネクタの移行のサポート: AzureおよびGCP (Google Cloud Platform) コネクタをDeep Security ManagerからTrend Micro Cloud One - Workload Securityに移行できるようになりました。詳細については、クラウドアカウントをWorkload Securityに移行するを参照してください。

解決済みの問題

- Deep Security Managerは、SNMP (Simple Network Management Protocol) を使用するシステム設定のsystemEventIDエラーに関連付けられた番号を受信していませんでした。SEG-122864/04711592/DS-67387
- Deep Security Managerで、IPアドレスなどの数値文字列を含む侵入防御イベントが原因で、Get Events Failed `NumberFormatException` エラーが発生することがありました。SEG-120226/SF04838989/DSSEG-7216
- Deep Security ManagerがvCloudと同期できないことがありました。SEG-135846 / SF05409802 / DS-70336
- Deep Security Managerで、コンピュータの移動イベントが正しく表示されませんでした。DS-70669
- 既存のアプリケーションコントロールローカルルールセットを持つDeep Security AgentがDeep Security Managerから削除されても、そのAgentのルールセットがManagerに表示されたままになっていました (ポリシー > アプリケーションコントロールルール > ソフトウェアルールセットの下)。DS-68173
- REST API を使用して Document Exploit Protection の`critical-and-heuristic`パラメータを選択した場合、Deep Security Manager ではマルウェアスキャン設定 ([コンピュータ]または[ポリシー] > [マルウェア対策] > [一般] > [編集]) にその選択が表示されません。DS-67975

Deep Security Manager - 20.0.619 (20 LTS アップデート2022/03/22)

リリース日 : 2022年3月22日

ビルド番号 : 20.0.619

新機能

Amazon Linux 2 の FIPS モード: Deep Security Manager バージョン 20.0.619 以降は、AWS Marketplace デプロイメントの FIPS モードをサポートしています。これは、Deep Security Agent バージョン 20.0.0-2971 以降でサポートされています。

機能強化

- Deep Security Managerがアップデートされ、トレンドマイクロFeedbackがSmart Protection Networkで共有されることを指す場合に、*匿名*ではなく*保護*という用語が使用されるようになりました。DS-70101

解決済みの問題

- モジュールのライセンスの有効期限が切れている場合、Deep Security Managerはポリシーを Trend Micro Cloud One - Workload Security に移行できませんでした。DS-69595
- セキュリティモジュール使用状況累積レポート(イベントとレポート> レポートの生成) で、アプリケーション コントロールの使用時間がシステム使用時間に正しく含まれていませんでした。DS-67494
- Deep Security Manager の信頼エンティティの[新規ルールセット]ウィンドウ(信頼エンティティ> 信頼ルールセット> 新規) の[OK]ボタンと[閉じる]ボタンが、一部の画面解像度でブロックされていました。DS-68838
- Deep Security Agents for Linuxの挙動監視ステータスは、Deep Security Managerのバージョン20.0.312以降で一貫性がありませんでした。挙動監視の検出を無効にしても、マネージャコンソールに、不正プログラム対策リアルタイム検索または高度なリアルタイム検索の初期設定で有効になっていたように表示されることがありました。DS-69536
- Deep Security AgentでFIPSモードが有効になっていてDeep Security Managerでは有効になっていないときに、接続の問題がありました。DS-70038

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある情報開示の慣行に従い、すべての影響を受け

るリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。SEG-132505/SF05278860/DS-69608/DS-69764

最高共通脆弱性評価システム (CVSS) スコア: 9.8

最高の重大度: 重大

Deep Security Manager - 20.0.605(20 LTS アップデート2022/02/16)

リリース日: 2022年2月16日

ビルド番号: 20.0.605

機能強化

- Deep Security Manager を更新し、ユーザーがリアルタイムのコンテナ保護を切り替えられるようにしました (コンピュータまたはポリシー設定 > 一般から)。この設定はデフォルトで有効になっています。SEG-115751/DS-68963

解決された問題

- フォルダ名でスマートフォルダをフィルタすると、存在しないフォルダまたはグループの結果が表示されることがありました。SEG-120786/SF04858677/DSSEG-7220
- NSX セキュリティグループの変更 (管理 > イベントベースタスク) のイベントベースタスク設定が有効になっている場合、仮想マシンが NSX セキュリティグループから削除されると、Deep Security Manager によって仮想マシンの自動アクティベーションがトリガーされます。DS-36694
- Deep Security Managerで、移動失敗 (応答なし) システムイベントの説明が正しく表示されませんでした。DS-69407

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。VRTS-5866/DS-62223

最高共通脆弱性評価システム (CVSS) スコア: 8.2

最高の重大度: 高

Deep Security Manager - 20.0.585(20 LTSアップデート2022/01/17)

リリース日 : 2022年1月17日

ビルド番号 : 20.0.585

新機能

アプリケーションコントロールの信頼エンティティ: この機能を使用すると、環境内のソフトウェアの変更を自動承認するように信頼ルールを設定できるため、手動で管理する必要があるソフトウェアの変更やセキュリティイベントの数を減らすことができます。詳細については、「アプリケーションコントロールの信頼エンティティ」を参照してください。

機能強化

- Trend Micro Cloud One - Workload Securityへの移行:
  - Deep Security Managerには、共通オブジェクト(ルールと不正プログラム設定を除く)をWorkload Securityアカウントに移行するための新しい `commonobjectmigrationtask` APIとUIが含まれています。
  - Deep Security Managerには、Deep Security Managerに接続されているAWSアカウントをWorkload Securityアカウントに移行するための新しい `connectormigrationtasks` APIとUIが含まれています。
- Trend Micro Endpoint Basecamp(セキュリティイベントをTrend Micro Vision Oneに転送するために必要) のインストールに使用するインストールスクリプトが、新しい証明書発行者の組織名でアップデートされました。

解決済みの問題

- 認証情報を必要としないプロキシを使用してSecurity Managerが設定されている場合、Deep Security AgentをWorkload Securityに移動できませんでした。DS-68710

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある情報開示の慣行に従い、すべての影響を受けるリリースに対するパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DS-68725、DS-67244

最高共通脆弱性評価システム (CVSS) スコア: 9.1

重大度が最も高い: 重大

Deep Security Manager - 20.0.560 (20 LTSアップデート2021/12/16)

リリース日:2021年12月16日

ビルド番号:20.0.560

新機能

信頼された証明書検出の例外: Deep Security Manager バージョン20.0.560 以降では、ポリシーの詳細 & 不正プログラム対策 & 高度な設定 タブから信頼された証明書検出の例外を設定して、デジタル証明書に基づいてファイルを不正プログラム対策スキャンから除外できるようになりました。これは現在、Windows プラットフォーム上の Deep Security Agent バージョン20.0.0-3445 以降でサポートされています。詳細については、信頼された証明書で署名されたファイルを除外する を参照してください。

解決済みの問題

- Deep Security Managerは、1000台を超えるコンピュータを含むグループからセキュリティ設定を取得できませんでした。SF05006314 / SEG-124719 / DS-67938
- オブジェクトの有効期限が終了した後も、Deep Security ManagerからDeep Security Agentに不審オブジェクトが送信されていました。DS-67917
- VMware Cloud Director 10.3または10.3.1にアップグレードされた仮想マシンが接続されているにもかかわらず、Deep Security Managerに表示されませんでした。SEG-123585 / SF04968350 / DS-67513

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある情報開示の慣行に従い、すべての影響を受けるリリースに対するパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が提供されます。DS-68162/DS-65579

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度:高

Deep Security Manager - 20.0.543(20 LTSアップデート2021/11/18)

リリース日:2021年11月18日

ビルド番号:20.0.543

機能強化

- Deep Security Managerがアップデートされ、Trend Micro Vision One のプロモーションバナーが、ユーザによって消去されてから24時間非表示になります。DS-55349
- Azureコネクタを追加する際に、Azureアプリケーション証明書認証を使用できるようになりました。詳細については、"Deep SecurityへのMicrosoft Azureアカウントの追加" on page 688を参照してください。DS-63762
- Deep Security ManagerからWorkload Security への移行が次のように強化されています。
  - Workload Securityへの移行時の接続の問題をより適切に処理できるようにDeep Security Managerがアップデートされ、コンソールUIがブロックされたり、ロードループでスタックしたりすることがなくなりました。DS-67841
  - Deep Security Managerがアップデートされ、Workload Securityに移行するDeep Security Agentのコンピュータグループリストに、コネクタによって生成されたコンピュータグループが表示されなくなりました。DS-67776
  - Deep Security Managerの移動失敗システムイベントがアップデートされ、Workload Security側のイベントの詳細が追加されました。DS-67921
  - Workload Securityに移行するコンピュータと同じホスト名を持つ非アクティブ化されたコンピュータを確認するようにDeep Security Managerがアップデートされました。一致するホスト名が見つかった場合、Managerはタスクに移動失敗のマークを付ける代わりに、既存のコンピュータをアップデートするようになりました。DS-67527
  - Deep Security Managerのポリシー移行ページ(サポート > Workload Securityへの移行 > 設定) を更新し、移行前にルールアップデートを最新にする必要があること、およびWorkload Securityの共通オブジェクトの名前が移行されるオブジェクトと同じ場合は上書きされることに、注意を促すようにしました。DS-67777
  - Deep Security Managerがアップデートされ、移行できないコンピュータの [Migrate to Workload Security] オプション (コンピュータを右クリックすると表示される) が削除されました。DS-67666

解決済みの問題

- カーネルサポートパッケージとエージェントインストーラのバージョンが同じ場合、ソフトウェアアップデートが失敗することがありました。DS-67547
- Deep Security Managerのシステムイベントの説明フィールドに「説明」が表示されないことがありました。DS-66878

- Deep Security Managerで、有効化されていないエージェントに関するアラートが受信されることがありました。DS-64523
- アップデート後、Deep Security Managerは以前のバージョンのオンラインヘルプファイルのコピーを保持していました。SEG-120770 / SF04858311 / DS-66969
- Deep Security Managerの[コンピュータ] タブで、[最終通信] 列が正しく並べ替えられないことがありました。SEG-120751/SF04862693/DS-67579
- Deep Security Managerは、特定の設定のエージェント/ Applianceから開始されたエージェント(AIA) をWorkload Securityに移行できませんでした。SEG-124938 / DS-67861
- [コンピュータレベルで設定を上書きして移行] オプションが選択されている場合、Deep Security Managerでルール割り当ての移行が誤って試行され、Workload Securityへの移行が失敗することがありました。DS-67528
- Oracle Databaseを使用するDeep Security Managerの場合、移行が成功した場合でも、Workload Securityへの移行を要求するコンピュータのステータスが [移動中] になります。DS-67930
- Deep Security Managerで、移行中にコンピュータがWorkload Security に移動できないというランタイム例外が発生することがありました。DS-67932

Deep Security Manager - 20.0.513 (20 LTSアップデート2021/10/14)

リリース日 : 2021年10月14日

ビルド番号 : 20.0.513

新機能

Deep Security ManagerのUIを使用したWorkload Securityへの移行 : Deep Security Managerでは、Deep Security ManagerのUIを使用したTrend Micro Cloud One Workload SecurityへのAgentとポリシー設定の移動がサポートされるようになりました。これには以下が含まれます。

- UIを使用したAgentの移行
- UIを使用した設定の移行
- コンピュータレベルでオーバーライドされた設定を使用したAgentの移行
- 1回のBatchComputerMoveTask APIコールで複数のエージェントを同時に移動する

詳細については、Workload Securityへの移行を参照してください。

解決済みの問題

- Trend Micro Vision One (XDR) ステータスの同期中に、Deep Security ManagerがSandbox as a Serviceステータスの同期に失敗することがありました。DS-66122

Deep Security Manager - 20.0.503 (20 LTSアップデート2021/09/23)

リリース日 : 2021年9月23日

ビルド番号: 20.0.503

新機能

カーネルパッケージの更新を管理: このアップデートでは、カーネルサポートパッケージを管理する新しい方法を導入します。Deep Security Managerは、Linuxでエージェントが再起動する際にカーネルパッケージを自動的に更新するオプションを提供します。詳細については、"オプションのLinuxカーネルサポートパッケージアップデートを無効にする" on page 401を参照してください。

機能強化

- Deep Security Managerがアップデートされ、Trend Micro Vision One for 脅威インテリジェンス (Connected Threat Defense) と統合されました。DS-61106

- Deep Security Managerがアップデートされ、コンソール(dsm_c) コマンドを使用して変更監視ベースラインデータを削除できるようになりました。ベースラインデータを削除しても、変更監視から受ける保護には影響しませんが、次のものは削除されます。
  - Managerコンソールからベースラインデータを表示するオプション
  - 自動タグ付けのソースとしてTrusted Common Baselineを使用する機能
  - 変更監視ベースラインレポートを生成する機能

  ベースラインが大きくなり、ワークロードがより動的になるにつれて、Deep Security Manager コンソールで Integrity Monitoring ベースラインをサポートする能力がますます困難になっています。私たちは、お客様のパフォーマンスおよび運用ニーズを満たすために、Integrity Monitoring の設計を進化させることに取り組んでいます。お客様との議論を通じて、現在の形では、Integrity Monitoring がベースラインデータを維持するために必要なパフォーマンスおよび運用のオーバーヘッドを相殺する価値を常に提供しているわけではないことが判明しました。ベースラインデータの無効化に関する詳細は、大量の Integrity Monitoring ベースラインデータによるデータベースのパフォーマンス問題 を参照してください。DS-60498

解決済みの問題

- Deep Security Managerで[有効化時のアップグレード] と[イベントベースのタスク] が同時に有効になっていると、Deep Security Agentの自動アップグレードが失敗することがありました。SEG-105646/SF04249597/DS-62190
- Deep Security Managerコンソールのコマンドで、LDAPSサーバ証明書に対して信頼済み証明書を追加できないことがありました。SEG-116063 / SF04716472 / DS-65277
- Workload Securityへの移行に使用されるいくつかのAPIキー項目がWorkload Security リンクAPIドキュメントから欠落していました。DS-66022
- 複数のvCenterコネクタが頻繁にvMotionを実行する環境では、Deep Security Managerでデッドロックが発生し、不正プログラム対策対策、ファイアウォール、および侵入防御のエンジンオフラインエラーが発生することがありました。SEG-115729/SF04696226/DS-65311
- Deep Security Managerがコンピュータの情報を取得できず、VMware NSXの同期が失敗することがありました。SEG-117202 / DS-65610
- IPv6を使用できない環境でも、Deep Security Virtual AppliancのIPv6アドレスがDeep Security Managerコンソールに表示されることがありました。SEG-118810 / SF04806948 / DS-66263
- Deep Security Managerの予約レポート([イベント] および [予約レポート]) で、[ポリシーを使用] のコンピュータフィルタを設定した場合でも、生成されたレポートにすべてのコンピュータが表示される場合がありました。SF04676734/SEG-116345/DS-65336
- Deep Security Managerで、デフォルトのリアルタイム検索ファイルリストまたはディレクトリリストの除外が重複した名前で作成されていると、Deep Security Agentのアップグレードが失敗することがありました。DS-65746

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある情報開示の慣行に従い、すべての影響を受けたリリースに対するパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。VRTS-5934/DS-63325/DS-65607

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度: 高

Deep Security Manager - 20.0.482(20 LTSアップデート2021-08-25)

リリース日 : 2021年8月25日

ビルド番号:20.0.482

機能強化

- Deep Security ManagerがアップデートされFIPSモードのPostgreSQL 12およびPostgreSQL 13がサポートされるようになりました。詳細については、「FIPS 140-2 support」を参照してください。DS-63876
- Deep Security ManagerのWorkload Security Link APIがアップデートされ、Workload Securityへの移行時に「https」を含むURLがサポートされるようになりました。DS-65095

解決済みの問題

- 毎日実行するように設定されたDeep Security Managerの予約タスク([管理] > [予約タスク]) が、1時間ごとに実行されることがありました。SEG-108098 / DS-64247
- Deep Security Managerの[コンピュータ] 画面で、[LAST MANUAL SCAN FOR MALWARE] および [LAST SCHEDULED SCAN FOR MALWARE] 列が正しく並べ替えられないことがありました。
- プライマリテナントで資格情報を使用してプロキシサーバを有効にしている場合、テナントがライセンスをアップデートできないことがありました([管理] > [システム設定] > [プロキシ] > [Deep Security Manager (ソフトウェアアップデート、CSSS、ニュースアップデート、製品登録とライセンス管理)]) 。

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、共通脆弱性識別子 (CVE) の詳細は、すべての影響を受けるリリースに対するパッチが利用可能になった後にのみ、一部のセキュリティアップデートで利用可能です。VRTS-5932/DS-63442/DS-51695/ VRTS-5930/DS-63071/ VRTS-5929/DS-63072

最高共通脆弱性評価システム (CVSS) スコア: 6.5

最高の重大度:中

Deep Security Manager - 20.0.463(20 LTSアップデート2021/07/22)

リリース日:2021年7月22日

ビルド番号:20.0.463

機能強化

- Deep Security Managerがアップデートされ、不正プログラム対策 検索インタフェース(AMSI) に2つの異なる処理オプションが追加されました。[放置]または[終了]を選択できるようになりました。DS-63691
- Deep Security Managerがアップデートされ、新しいMigratePolicy APIコマンドを使用したWorkload Securityへのポリシーの移行がサポートされるようになりました。このコマンドは、Deep Securityポリシーを現在のオンプレミスManagerからCloud One Workload Securityテナントに移行するプロセスを自動化します。DS-63316
- Deep Security Managerがアップデートされ、vCenterのリホームプロセス中に仮想マシンのIPアドレスにアクセスできるかどうかが確認されるようになりました。DS-63514

解決された問題

- Deep Security Managerは、複数のネットワークインタフェースカード(NIC) を備えたシステムでメールを送信できないことがありました。DS-63254
- Agentからのリモート有効化(AIA) を使用するDeep Security Agentで、証明書のアップデート後にオフラインになることがありました。DS-58106
- エージェントバージョンレポート([イベントとレポート] > [レポートの生成]) を生成すると、実際に選択されたオプションに関係なく、[コンピューター フィルター] セクションで [すべてのコンピューター] が選択されたかのようにレポートが生成されます。DS-64133
- タグによるスマートフォルダのフィルター処理は、自動タグ付けで追加された新しいイベントに対して正しく機能しませんでした(イベントとレポート> イベント>(イベントタイプを選択) > 自動タグ付け) 。DS-61210
- vCenter上の仮想マシンに複数のIPアドレスがある場合、Deep Security Managerが正しいIPアドレスを選択できないことがありました。SEG-109694 / SF04486485 / DS-63235
- Deep Security Managerでは、以前に削除された古いカーネルサポートパッケージ(KSP) が再ダウンロードされることがありました。SEG-101335 / 04121383 / DS-60849

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DS-64012/ VRTS-5931/DS-63070

最高共通脆弱性評価システム (CVSS) スコア: 6.8

最高の重大度 : 中

Deep Security Manager - 20.0.447(20 LTSアップデート2021/06/28)

リリース日 : 2021年6月28日

ビルド番号 : 20.0.447

新機能

Agentの親の変更: Deep Security Managerでは、新しいMoveAgent APIコマンドを使用したTrend Micro Cloud One Workload SecurityへのAgentの移動がサポートされるようになりました。このコマンドは、有効化されたDeep Security Agentの親を現在のオンプレミスManagerからWorkload Securityテナントに変更するプロセスを自動化します。ペアレント化に失敗した場合、エージェントは以前の設定を保持したままオンプレミスManagerで再度有効化します。

Deep Security ManagerとWorkload Security Managerでは機能が異なるため、予期しない動作を防止するために移動タスクが拒否される場合があります。エージェントを移動する前に、次の設定を無効にする必要があります。

- FIPS 140-2: FIPS 140-2のサポートが有効な場合、Deep Security Managerは移動タスクを拒否します。
- Deep Security Virtual Appliance: Deep Security Virtual Appliance (エージェントレスまたは統合モード) によって保護されているコンピュータは、移動タスクを拒否します。
- SAP NetWeaver統合 : SAP NetWeaver統合を使用するAgentは、移動タスクを受け入れます。ただし、Workload Securityに移動すると、SAP NetWeaver統合は Workload Securityでサポートされるまで利用できなくなります。

強化

- Deep Security Managerを更新して、PostgreSQL12およびPostgreSQL13データベースのサポートを追加しました。DS-59911
- Deep Security Manager UIで機械学習型検索の横に表示されていたWindowsロゴを削除しました。機械学習型検索は現在、すべてのWindowsエージェントおよびバージョン20.0.0-2395以降のLinuxエージェントでサポートされています。DS-62929
- Deep Security Managerを更新して、どのエージェントバージョンが挙動監視のパスアクションをサポートしているかを記載しました: WindowsではDeep Security Agent 20.0.0-1559以降、LinuxではDeep Security Agent 20.0.0-1822以降。DS-62937
- アクティビティデータ転送の説明 (管理 > システム設定 > Trend Micro Vision One) を更新し、スクリプトの展開に関する詳細情報を提供しました。DS-63278

- 一部のプラットフォームのサポートを改善するために、Endpoint Basecamp 展開スクリプト(管理 > システム設定 > Trend Micro Vision One > アクティビティデータ転送) を更新し、スクリプト展開エラー メッセージをよりわかりやすいものに更新しました。SEG-109629/DS-63157

解決済みの問題

- Deep Security Manager のテナントページ (管理 > テナント) で、一部の列がイベントまたはジョブの数全体ではなく、最初の桁のみに基づいて並べ替えられていました。SEG-107657/DS-62544
- Deep Security Managerは、多数のセキュリティプロファイルを持つデータベースにクエリを実行するときにメモリを大量に消費していました。SEG-103097 / SF04265571 / DS-61490
- 不正プログラム対策 リアルタイム検索 構成 ポリシーが継承された値に正しくリセットされないことがありました。DS-63835
- システムイベントメッセージには、間違ったオペレーティングシステムを参照する情報が含まれている場合がありました。SF04443281 / SEG-111629 / DS-64089

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある情報開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能です。DS-63110/DS-61049

最高共通脆弱性評価システム (CVSS) スコア: 5.8

最高の重大度 : Low

Deep Security Manager - 20.0.414(20 LTSアップデート2021/05/24)

リリース日 : 2021年5月24日

ビルド番号 : 20.0.414

拡張

- Deep Security Managerがアップデートされ、特定されたファイルのダウンロードメカニズムが強化されました。これには、Agentから開始されたDeep Security Agentからダウンロードする機能や、特定されたファイルにダウンロードの進行状況を示す新しい[ファイルステータス] フィールドが追加されました。DS-60741

解決された問題

- 一部の構成では、内部エラーによりユーザーがDeep Security Best Practice Guide Reportを生成できませんでした。SF04154114/SEG-99975/DS-60897
- アカウントのアクセス許可の問題により、Trend Micro Vision One 登録が失敗したり、間違ったステータスが表示されたりすることがありました(Administration> System Settings> Trend Micro Vision Oneの下) 。DS-61893
- Deep Security Managerに接続時に問題が発生し、コンピュータの適切なインポートが妨げられ、Deep Security Relaysがアクティベートまたは無効化されないことがありました。DS-58417
- Deep Security Managerは、監査者の役割を持つユーザーが ファイアウォール ルール(ポリシー> ルール> ファイアウォール ルール) を表示できないようにすることがありました。SF04220398 / SEG-102016 / DS-60847
- 日本語コンテンツへのDeepSecurity Managerリンクは、エアギャップオンラインヘルプパッケージ(管理>更新>ローカル) を使用したセットアップでロードできませんでした。04442246 / SEG-108814 / DS-63080
- データベース接続が不安定な場合、Deep SecurityManagerはスケジュールされたタスクの処理を停止することがありました。DSSEG-6689 / DS-62963

Deep Security Manager - 20.0.393(20 LTSアップデート2021-04-27)

リリース日 : 2021年4月27日

ビルド番号 : 20.0.393

機能強化

- Deep Security Manager を更新し、イベントが「次の期間より古いイベントを自動的に削除」オプション (管理 > システム設定 > ストレージ) のいずれかによって消去された場合に、イベントの説明にメッセージが追加されるようにしました。DS-59349
- Deep Security Manager を更新し、最大 TCP 接続数 (コンピュータ> コンピュータ> 詳細 > 設定 > 詳細) をデフォルトで 1000000 に増やしました。DS-61032

解決済みの問題

- キー値に特殊文字が含まれていると、Deep Security Managerのバージョンアップに失敗することがありました。SEG-99875 / SF04106715 / DS-60581
- 一部の設定で不正プログラム対策予約検索が機能していません。DS-54952

- 多くのポリシーが存在し、または役割に割り当てられている場合、Deep Security Managerコンソールのロード時間が通常よりも遅くなることがありました。SEG-90429 / SF03787758 / DS-58871
- 「次の期間より古いサーバーログを自動的に削除する」設定 (管理 > システム設定 > ストレージ) が、プライマリテナントにのみ表示されるはずなのに、テナントに表示されていました。DS-58669
- ライセンスプロパティ(管理 > ライセンス > 詳細の表示) の更新手順の表示 URL が壊れていました。SEG-104258/SF04308332/DS-61343
- Deep Security ManagerがAWSコネクタと同期できないことがあります。SEG-102091 / SF04198233 / DSSEG-6726
- Deep Security Managerは、リージョンデータが予期せずデータベース内で変更された場合に、一部のAWSコネクタのログオン情報を検証できませんでした。SEG-97924 / DS-60541
- Deep Security Managerが、既存のリアルタイム不正プログラム検索設定(ポリシー>共通オブジェクト>その他の>不正プログラム検索設定) にアクセスできないことがあります。SEG-86700 / SF03646616 / DS-55577
- データプルーニングの不具合 (管理 > システム設定 > ストレージ) により、多数のイベントが発生し、Deep Security Manager とデータベース間でパフォーマンスの問題が発生することがありました。SEG-97589/SF04073627/DS-61356
- Deep Security Manager のシステム イベント レポート ([イベントとレポート] > [レポートの生成]) で、データが欠落した状態でレポートが生成される場合がありました。DS-61752
- Deep Security Manager では、パスワードで保護された単一レポートまたはパスワードで保護されたスケジュールレポート ([イベントとレポート] > [レポートの生成]) を生成できない場合がありました。SEG-105241/SF04341549/DS-61718
- Azure コネクタのパスワードの更新 (コンピュータ > コンピュータ > Azure コネクタを右クリック > プロパティ > 接続) が機能しないことがあり、アカウントが Deep Security Manager との接続を失う原因となることがありました。DS-60479
- Deep Security Managerで、NSXがインストールされているvCenter Connectorを削除できないことがあります。DS-61101
- ダッシュボードのDeep Security Managerの不正プログラム対策対策ステータスに、誤った情報が表示されることがありました。SEG-103625/SF04271447/DS-61598
- セキュリティモジュール使用状況累積レポート(イベントとレポート > レポートの生成) を生成するときに、アプリケーション制御時間が計算されませんでした。SEG-100505/SF04174981/DS-60675

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能です。DS-51780/DS-61318

最高共通脆弱性評価システム (CVSS) スコア: 8.2

最高の重大度 : 中

Deep Security Manager - 20.0.366(20 LTS Update 2021-03-24)

リリース日 : 2021年3月24日

ビルド番号 : 20.0.366

新機能

Trend Micro Vision One (XDR) 用の Trend Micro Endpoint Basecamp の導入 : Trend Micro Vision One (XDR) にオンボードした後、Trend Micro Endpoint Basecamp エージェント導入スクリプト([サポート] > [導入スクリプト]) を選択して、Linux または Windows プラットフォーム上の Deep Security Agent とともに自動的に導入できるようになりました。

機能強化

- Deep Security Managerがアップデートされ、Trend Micro Vision One (XDR) の登録時にエラーメッセージとそのトラブルシューティングに必要な処理がわかりやすくなりました。DS-61057

解決済みの問題

- Deep Security Manager システムイベントレポート([イベントとレポート] > [レポートの生成]) の [システムイベント数による最もアクティブなコンピュータのランキング] セクションにデータがない場合がありました。DS-28985
- ダッシュボードの不正プログラム検索ステータスに誤ったデータが表示されることがありました。DS-57263
- Deep Security Manager のセキュリティアップデートの概要 (管理 > アップデート > セキュリティ) では、管理 > スケジュールされたタスクにスケジュールされたタスクがあっても、スケジュールされたタスクがないと表示される場合があります。SEG-97381/DS-60271

- [コンピュータ] タブの [コンピュータ] 検索フィールドに特定の用語を入力すると、検索に失敗し、内部サーバエラーが表示されます。SEG-98108/SF03976840/DS-60133
- 表示のみの権限を持つユーザが、Deep Security Managerのアプリケーションコントロールルールセットの処理を変更できました。SEG-81133/03347924/DS-61041

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能です。DS-61209/VRTS-4382/03116764/DS-49429

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度: 高

Deep Security Manager - 20.0.344(20 LTSアップデート2021-02-23)

リリース日: 2021年2月23日

ビルド番号: 20.0.344

強化

- Deep Security Managerの不正プログラム対策 初期設定のリアルタイム検索除外が更新され、パフォーマンスが向上しました。DS-55169
- Deep Security ManagerのUIがアップデートされ、Trend Micro XDRの名前がTrend Micro Vision Oneに変更されました。DS-60273
- Deep Security Managerが更新され、CentOS 8およびRedHat 8の配置スクリプトのサポートが追加されました。DS-60413
- Trend Micro Vision One tab [詳細] リンクが更新され、ユーザのロケールの言語 (EN/JP) に基づいたコンテンツが参照されるようになりました。DS-60487
- Deep Securityソフトウェアのページが更新され、不正なリンクが修正されました。DS-60494
- Deep Security Manager を更新し、非アクティブ エージェントのクリーンアップのオプションとして2日間を追加しました (管理 > エージェント > 非アクティブ エージェントのクリーンアップ)。SEG-91358/SF03711833/DS-59591
- Deep Security AgentのIPが到達不能であるとき、そしてマネージャーが開始した通信が有効になっているときのvCenter接続性を向上させるためのDeep Security Managerを更新しました。DS-58526

- Deep Security Managerが更新され、ポート32767-65535のサポートが追加されました。SEG-98840 / SF04119337 / DS-60122
- Deep Security ManagerのXDR Basecamp(XBC) 配信スクリプトUIがアップデートされ、オンラインヘルプセンターの最新プラットフォームサポート情報へのリンクが提供されます。DS-60206

解決済みの問題

- コンピュータ>Active Directoryの追加 とAzureアカウントの追加 の両方のオプションを使用してVMを管理した場合、ホストのアップデートとリホームの問題が発生しました。SEG-97266 / SF03911224 / DS-59853
- Deep Security Managerの不正プログラム対策 プロテクションステータスウィジェット([ダッシュボード]タブ) で、データの表示に失敗することがありました。DS-48046
- SAMLアイデンティティプロバイダとのDeep Security Managerの統合が、すべての役割が予想される形式と一致しない場合に失敗することがありました。SEG-90158 / SF03783432 / DS-57687

Deep Security Manager - 20.0.321(20 LTS Update 2021/01/26)

リリース日 : 2021年1月26日

ビルド番号 : 20.0.321

機能強化

- Deep Security Manager を更新し、プラットフォーム メニュー (管理 > システム設定 > Trend Micro Vision One) から選択したときに正しい導入スクリプトが表示されるようになりました。DS-59825
- Deep Security ManagerがVMWare Cloud Director 10.2以降でNSX-Tのエージェントレスモードをサポートするようにアップデートされました。DS-54044

解決された問題

- [セキュリティアップデートの確認] の複数の予約タスクを同時に実行すると、アップデートがスキップされることがありました。DS-59715

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリ

リースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DS-59917

最高共通脆弱性評価システム (CVSS) スコア: 6.1

最高の重大度 : 中

Deep Security Manager - 20.0.313(20 LTSアップデート2021-01-18)

リリース日 : 2021年1月18日

ビルド番号 : 20.0.313

新機能

Trend Micro Endpoint Basecampエージェント: Trend Micro Endpoint Basecamp (XBC) エージェントは、Trend Micro Vision Oneのオンボーディングに従って、XDRツールと機能をDeep Securityに統合します。詳細については、"Trend Vision One (XDR) と統合する" on page 1967を参照してください。

機能強化

- Managerのアドレス「 」フィールドを編集するのではなく、NSX Managerの削除[ ]ボタン(の[プロパティ]→NSX Managerの) を使用して、NSXマネージャをより簡単に変更できるようにvCenterがアップデートされました。DS-58377
- Deep Security ・マネージャがアップデートされ、初期設定でトレンドマイクロの Vision One がオンボーディング体験後および有料ライセンスへの移行後に有効になりました。DS-58788
- Deep Security Managerから[News]ボタンが削除されました。製品の変更に関する最新ニュースについては、の新機能を参照してください。DS-58808
- Deep Security ManagerおよびDeep Security Agentのパッケージ名は、ダウンロードセンターで調整されています。DS-56806
- Trend Micro Vision One の問題をログに記録するオプション(の[管理]→[システム情報]→[診断ログ] ...) を含めるようにDeep Security Managerがアップデートされました。DS-58533
- Deep Security Manager のデフォルトリアルタイム検索設定 (コンピュータ> 詳細 > 不正プログラム対策 > 一般 > リアルタイム検索 > 不正プログラム検索設定) を更新して、デフォルトで挙動監視と機械学習型検索を有効にしました。後のバージョンの Deep Security エージェント (Windows エージェント20.0.0.1559 以降、および Linux エージェント20.0.0-1822 以降) では、デフォルトでカスタムアクションの使用が Pass に設定され、不正プログラム対策イベントが記録されます。以前のバージョンのエージェントでは、不正プログラムの可能性 のアクションが Pass に設定されている場合、挙動監視と予測機械が無効になります。DS-59282

- トレンドマイクロのVision Oneに関連する設定と機能がオンボーディング後に一貫性を持たせるようDeep Security Managerがアップデートされました。DS-58788
- Deep Security Managerがアップデートされ、コンピュータの検索APIとコンピュータの一覧表示APIのパフォーマンスが向上しました。DS-56722

解決済みの問題

- Deep Security Managerインストーラがオペレーティングシステムで少なくとも16GBのRAMを検出した場合、最高のパフォーマンスを得るために推奨されるように、8GBのRAMをJava仮想マシンに自動的に割り当てていませんでした。SEG-87319/03645194 / DS-55701
- 一部の環境でDeep Security Managerがエージェントと通信できず、エージェントのオフライン問題が発生しました。SEG-86783 / SF03637359 / DS-56400
- 不正プログラム対策の予約タスクが、タイムアウトしたときに、[予約タスクのスキップ] イベントが予期したとおりにトリガされずに再開されることがありました。DS-59252
- 複数のIPを持つDeep Security Agentの優先IPアドレスの設定に使用されるDeep Security Managerコンソールコマンドが機能しない場合があり、一部のエージェントを接続できないことがありました。DS-58878
- 一部の設定では、Deep Security Managerのバージョンアップインストールに失敗していました。SEG-95357 / SF03988405 / DS-59222
- Deep Security Managerによって、リレーのバージョンが正しくインストールされないことがあります。DS-59634
- Trend Micro Vision Oneの登録に対するDeep Securityのライセンス確認が失敗することがありました。DS-59645
- ポリシーの設定 (ポリシー > 詳細 > 設定 > 全般) を変更した後、「ポリシーの変更をコンピューターに自動的に送信」または「継続的な推奨スキャンを実行する」で「すべての設定を固有にリセット」ボタンが機能しませんでした。DS-56830
- [ダッシュボード] タブの [コンピュータのステータス] でリンクがクリックできないことがあり、Agent/Applianceのアップグレード推奨 (新しいバージョンが利用可能) のアラートが [アラート] タブのリストビューで開かれることがありました。DS-57968

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある情報開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DS-33781/DS-58415/DS-58917/DS-51741/DS-59636

最高共通脆弱性評価システム (CVSS) スコア: 9.8

最高の重大度 : 重大

Deep Security Manager - 20.0.262(20 LTSアップデート2020-11-26)

リリース日 : 2020年11月26日

ビルド番号 : 20.0.262

新機能

Trend Micro Vision Oneとの統合 : Trend Micro Vision Oneは、メール、エンドポイント、サーバー、クラウドワークロード、ネットワークなど、複数のベクターから収集されたデータを使用して、効果的な専門分析とグローバル脅威インテリジェンスを適用します。詳細については、"Trend Vision One (XDR) と統合する" on page 1967を参照してください。

挙動監視と機械学習のカスタム処理 : このリリースでは、挙動監視および機械学習型検索のカスタム処理を指定できます。

強化機能

- スマートフォルダの [コンピュータの説明]フィールドを検索条件として使用できます。SEG-85288/DS-55034
- "エージェントレスソリューションをNSX-VからNSX-Tに移行する" on page 1707ヘルプセンターの記事を追加しました。DS-51619

解決済みの問題

- スマートフォルダエディタで、コンピュータの種類が [物理コンピュータ] ではなく[未定義] と表示されていました。DS-32765
- [vCenterコネクタのプロパティ]ページで、ユーザがNSX Managerの を削除し、NSX-T Managerを再登録したときに、ネットワーク関連の機能が表示されます。サポートされていません(NSXライセンスに制限されています) 。DS-56411
- AWSがバージョン条件が選択されたスマートフォルダサブフォルダに追加されたときに、内部サーバエラーが発生しました。DS-50785
- ログ検査 または 侵入防御 ルールが追加されたとき、Webアプリケーション ファイアウォール によってページがブロックされることがありました。DS-56448

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けたリリースに対するパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。DS-57603

最高共通脆弱性評価システム (CVSS) スコア: 3.7

重大度: 低

Deep Security Manager 20.0.198(20 LTS アップデート2020-10-19)

リリース日: 2020年10月19日

ビルド番号: 20.0.198

機能強化

- Activation Failedイベントの説明が拡張され、イベントの発生理由が示されました。DS-29719

解決済みの問題

- スタンドアロンクライアントをVMware VMにインストールしてからvCenterをDeep Security Managerに追加した場合、1台のVMのマネージャで重複するコンピュータレコードが表示されます。DS-55316
- Policies > Settings > Advancedの設定を変更できませんでした。Inheritedオプションを解除できませんでした。DS-56309
- 管理 > 更新 > セキュリティページの読み込みに時間がかかりました。

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能です。DS-54102/DS-53674

最高共通脆弱性評価システム (CVSS) スコア: 6.5

最高の重大度: 中

Deep Security Manager 20.0.174(20 LTSアップデート2020-09-16)

リリース日 : 2020年9月16日

ビルド番号 : 20.0.174

新機能

管理と品質の向上

エージェントバージョンレポート: エージェントのバージョン数の概要を表示できるように、エージェントバージョンレポートが作成されました。特定のエージェントバージョンを使用して、各バージョンで使用されているエージェントの総数の割合と、オフラインになっているクライアントの数とオンラインでのクライアント数の概要 Deep Security Agentのプラットフォーム(OS).レポートを生成するには、イベント&レポート>レポートの生成>単一レポート>新しい>エージェントバージョンレポートを参照してください。

アゼル政府の改善: Azure政府リソースは、Deep Security Manager Azureコネクタ経由で追加できます(コンピュータ>Add>Azureアカウントの追加).詳細については、Azure Governmentのインスタンスを保護するにはどうすればよいですかを参照してください。

データベースの暗号化: Deep Security Managerとデータベース間の通信を暗号化するプロセスが簡素化されました。詳細については、"Deep Security Managerとデータベース間の通信の暗号化" on page 1633を参照してください。

強化

- GCPアカウントのプロパティの設定を変更する際に、GCPサービスアカウントの確認にかかる時間が短縮されました。以前は、自動生成されたGCPプロジェクトが多数存在していましたが、これには長い時間がかかりました。SEG-81743 / SF03452889 / DS-53515
- ユーザープロパティウィンドウ(コンソールの上部にある電子メールをクリックして ユーザープロパティを選択) にリストされているページャー番号、電話番号、および携帯電話番号を更新し、30桁を超えるように構成できるようにしました。
- コンソールの「マイユーザーの概要」と「ユーザーおよび連絡先レポート」(「イベントとレポート」>「レポートの生成」>「単一レポート」) を更新し、過去 30 日間に発生したログインを反映するようにしました。SEG-81216/03407489/DSSEG-5897
- VMware Cloud Director (vCloud) 10.1.1 (NSX-Vのみ)のサポートを追加しました。
- 「予約レポートの送信に失敗しました」というエラーメッセージが改善されました。詳細な説明が追加されています。詳細については、トラブルシューティング: 予約レポートの送信に失敗しましたを参照してください。SEG-77886/03221276 / DS-54615

- New 不正プログラム Scan Configuration Properties (Policies > Common Objects > 不正プログラム Scans > New)のデフォルト設定を、Default Malware Scan Configuration Propertiesのデフォルト設定に合わせて更新しました。

解決済みの問題

- Deep Security Managerのダッシュボードにあるコンピュータステータスウィジェットに、管理下のコンピュータの正しい数が表示されませんでした。DS-53294
- Deep Security Agentの信頼された証明書は自動的には更新されませんでした。SEG-79146 / SF03240076 / DS-52488
- 保護対象のコンピュータの数が制限を超えていない場合でも、AWS Contract License Exceededアラートが発生することがありました。SEG-82932/SF03491496/DSSEG-5974
- vCloudのインポートされたVMをアクティベーションできませんでした。SEG-75542/03189161 / DS-53447
- コンソールで、不正なセキュリティログ監視のステータスが表示されることがありました。/ DS-54630
- 一部の侵入防御ルールは、[検出のみ] モードでのみ動作するように設計されていますが、ポリシーとコンピュータのページで動作を変更できました。DS-54667
- 不適切な数のオーバーライドが コンピュータ/ポリシーエディタ> オーバーライドをオーバーライドします。SEG-83802/03513073 / DS-54710
- タスクの作成時に不正な挙動が発生した、予約タスクに関する権限の問題がありました。SEG-78610 / SF03320936 / DS-53292
- MasterAdminがすべてのコンピュータに対して予約タスクを作成できませんでした。DS-55522
- ダッシュボードのランサムウェアイベント履歴に誤った情報が表示されていました。DS-55494

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある情報開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能です。DS-52678 /DS-21167 /DS-53059

最高共通脆弱性評価システム (CVSS) スコア: 7.0

最も深刻なレベル: 高

お知らせ

Red Hat Enterprise Linux 5および6は、Deep Security Managerのサポート対象プラットフォームではなくなりました。サポートされているDeep Security Managerプラットフォームの一覧については、"システム要件 " on page 400を参照してください。

Deep Security Manager 20(長期サポートリリース)

リリース日 : 2020年7月30日

ビルド番号 : 20.0.60

クロスアカウントロールを使用してAPI /rest/cloudaccounts/awsを使用してDeep SecurityにAWSアカウントを追加する場合の処理が必要

AWSのベストプラクティスにより良く整合し、AWS accountのセキュリティを向上させるために、トレンドマイクロはクロスアカウントロールを使用して新しいAWS accountをDeep Securityに追加するプロセスを変更しました。以前は、認証のためにクロスアカウントロールを使用する際、Deep Securityはロール ARNとロールによって信頼される外部IDの2つの情報を必要としていました。これが変更され、Deep Securityが外部IDを提供し、提供されたロールがこの外部IDをIAM信頼ポリシーに含めることを要求する新しいプロセスになりました。この変更により、共有Deep Security環境でのセキュリティが強化され、常に強力な外部IDが使用されることが保証されます。マネージャ生成の外部IDを使用してクロスアカウントロールを追加する新しいプロセスの詳細については、"クロスアカウントロールを使用したAWSアカウントの追加" on page 672を参照してください。

要確認 :

外部IDをマネージャーが生成したものに切り替えます: "外部IDを更新する" on page 680。

API `/rest/cloudaccounts/aws` でクロスアカウントロールを使用している場合は、API /rest/cloudaccounts/aws でクロスアカウントロールを使用している場合に必要なアクション を参照してください。

新機能

更新されたプラットフォームのサポート

- Red Hat Enterprise Linux 8 (64ビット)
- Windows Server 2019 (64ビット)
- Oracle 18データベースのサポート

- Oracle 19cデータベースのサポート
- PostgreSQL 11データベースのサポート
- SQL Server 2019データベースのサポート

Google Cloud Platform: Google Cloud Platform (GCP) はDeep Securityと統合されています。オンラインになる、または削除される新しいGCPインスタンスや、保護されているインスタンスを確認できます。オンプレミスやデータセンターで複数のクラウドを使用している場合、Deep Securityはすべての環境に対する可視性を提供できます。この機能はDeep Security Agent 12.0以降がインストールされたVMで利用可能です。詳細については、"Google Cloud Platformアカウントを追加する" on page 700を参照してください。

Red Hat Enterprise Linux 6のサポート終了: Red Hat Enterprise Linux 6は、Deep Security Managerのサポート対象プラットフォームではなくなりました。オペレーティングシステムをアップグレードします。

セキュリティの向上

NSX-T環境での仮想マシンの保護: トレンドマイクロでは、ファイアウォール Service 侵入防御およびゲストイントロWebレピュテーションションの最新テクノロジを統合してい変更監視。保護します。

NSX-T環境でのシームレスなネットワーク保護 : Deep Security Managerは、ゲストVMのネットワーク設定を、同じクラスタ内のすべてのDeep Security Virtual Applianceに送信します。その結果、アプライアンスは、1つのESXiホストから同じクラスタ内の別のESXiホストへのvMotionの移行中および実行後に、ネットワーク機能を使用するゲストコンピュータの保護を維持できるようになります。この機能は、NSX-T環境にのみ適用されます。この環境では、ゲストコンピュータがネットワーク機能のオーバーライドなしで割り当てられたポリシーを使用しています。

NSX-T環境で継続的な不正プログラム対策の保護 : Deep Security ManagerはゲストVMを不正プログラム対策のリアルタイム設定を、同じクラスタ内のすべてのDeep Security Virtual Applianceに適用します。これにより、vMotionを1つのESXiホストから別のESXiホストに移行中および移行後に、不正プログラム対策のリアルタイム機能を使用するゲストコンピュータの保護をアプライアンスで維持できるようになります。同じクラスタ。この機能は、NSX-T環境にのみ適用されます。

エージェントのバージョン管理: エージェントのバージョン管理により、セキュリティオペレーションチームは、展開スクリプトやアクティベーション時のアップグレードなどの機能で使用できるDeep Security Agentの特定のバージョンを管理できます。これにより、環境で使用されるDeep Security Agentに対する管理が強化されます。詳細については、"エージェントのバージョン管理を設定する" on page 1492を参照してください。

管理と品質の向上

Red HatとCentOSプラットフォームを区別する: Deep Security Managerは、Red HatとCentOSのプラットフォームとオペレーションを区別できます。

Google Cloud Platformの可視性、保護、および管理(GCP):

- VMはプロジェクトに編成されており、どのGCP VMが保護されているか、保護されていないかを簡単に確認できます。
- GCPインスタンスラベル、GCPネットワークタグ、およびその他のインスタンス属性に基づいてポリシーを自動的に割り当てます(自動スケーリング) 。
- 管理を簡素化するために、GCPインスタンスラベル、GCPネットワークタグ、およびその他のインスタンス属性に基づいて、関連するGCPインスタンスをスマートフォルダにグループ化します。

REST APIを使用したGoogleおよびAWSアカウントの自動化 : 一般的なタスクを実行するためのAPIがより多くの自動化されたデプロイメントに移行するにつれて、Deep SecurityはREST APIを提供し、AWSとGoogle Cloudアカウントの両方をDeep Securityに追加します。

不正プログラム対策 の有効な推奨事項: 不正プログラム対策 システムで何が起こっているかを理解するために、多くの 不正プログラム対策 イベントがアップデートされ、取り消しまたは失敗の詳細が表示されます。が発生しました。これらのイベントは、手動、クイック、または予約の不正プログラム対策検索で発生します。強化された詳細は、Deep Security Managerのイベントで提供されるほか、SIEMまたはAWS SNSを介して提供されます。

NSX-Tネットワークスループットの向上: トレンドマイクロでは、Data Plane Development Kit (DPDK) を導入することで、従来の技術であるRaw Socketと比較してネットワークスループットを3倍高速化しました。

クラウドインスタンスメタデータの検索 : [コンピュータ]ページで、クラウドインスタンスメタデータの検索または高度な検索を行う機能が追加されました。これにより、特定のラベル、ネットワークタグなどを含むワークロードを簡単に見つけることができます。

Instance Metadata Service Version 2 (IMDSv2) サポート: このリリースではIMDSv2がサポートされています。詳細については、"Deep Security AgentはAmazonインスタンスメタデータサービスをどのように使用しますか" on page 1979を参照してください

アクティベーション時のアップグレード: Deep Security Managerには、管理 > システム設定 > エージェント > アクティベーション時にLinux/Windowsエージェントを自動的にアップグレードするオプションが追加されました。これにより、エージェントがアクティベートまたは再アクティベートされる際に、管理 > システム設定 > アップデート > ソフトウェア > エージェントバージョン管理で指定されたバージョンにLinuxおよびWindowsコンピュータ上のDeep Security Agentを自動的にアップグレードすることができます。詳細

については、"Agentを有効化するときに自動的にアップグレードする" on page 1513を参照してください。

予約検索タスクとイベントベースのタスクの可視性の向上：予約検索タスクとイベントベースのタスクが改善されました。これには、検索の可視性と未完了の個別の理由不正プログラム対策検索と推奨される処理を実行します。

クラウドアカウントへのチャージバックを可能にするレポート機能の強化：セキュリティモジュール使用レポートに、保護されたインスタンスのクラウドアカウントID(AWSアカウントID、Azure契約ID、またはGCPプロジェクトID) が含まれるようになりました。

複数のvCenters： Deep Security Managerで複数のvCenterを追加し、同じNSX-Tデータセンターに関連付けることができます。NSX Data Center for vSphere (NSX-V), 複数のvCenterの使用をサポートしていない場合、またはNSX-T Managerが別のDeep Security Managerクラスタに登録されている場合) を使用している場合は、上書き警告メッセージが表示されます。

機能強化

UI改善点：

- 不正プログラム対策のイベントにCSV形式でエクスポートされたファイルハッシュ値が追加されました (イベント&レポート>不正プログラム対策 Export>CSVにエクスポート)。SEG-61890 / SF02510024 / DS-53441</ p>
- [システム情報]画面のメモリに関連する説明が更新され、より正確で理解しやすくなりました。
- イベントが発生した理由を含めることで、挙動監視イベントの説明が改善されました。
- コンピュータタブにGCPネットワークタグの列が追加されました。
- インスタンスID、ラベル、ネットワークタグなどのGCP情報がコンピュータエディタ>Overview>一般に追加されました。
- ComputersページにCloud Instance Metadataフィールドが追加されました。
- 管理>ユーザ管理>の役割>新しい>コンピュータ権限>選択されたコンピュータに進行状況バーが追加され、ロード中のコンピュータリストのステータスが示されます。
- 1つのハートビートに多数のエージェントイベントがある場合、複数のイベント検索イベントに分割されます。
- Relay管理機能を強化しました。アラートの説明に「Relay Group Assigned」アラートの解決策を提供し、リレーを削除しました。テナントRelayグループを使用しているテナントの数。
- 「データベースタイプ」と「データベースサーバ」列が管理>テナントに追加されました。
- サポートされていないカーネルにコンピュータがアップグレードされたかどうかを示す「Kernel Unsupported」システムイベントが追加されました。

- [手動不正プログラム検索キャンセル完了]システムイベントの理由IDが追加されました。理由IDは、REST API呼び出し、SNS情報、およびSIEM情報に表示されます。
- 「TrendMicroDsPacketData」フィールドがDeep Security Manager経由でSyslog転送されるファイアウォールイベントに追加されました。
- エージェントインストーラーの署名を検証するチェックボックスをサポート> デプロイメントスクリプトに追加しました。詳細については、"ソフトウェアパッケージのデジタル署名の確認" on page 445を参照してください。
- 計画IDがAzure Marketplaceの請求用かどうかを指定することで、「ライセンス変更済み」イベントの説明が改善されました。
- サービストークン設定をデータソースGUIDに変更しました。管理 > システム設定 > Managed Detection and Response。
- 「GUID」列がComputersページに追加されました。このため、コンピュータをエージェントGUIDで検索できます。
- 管理>Updates>Software>Localに検索バーが含まれています。
- スマートフォルダを作成する際に、Agentのバージョンに基づいてコンピュータをフィルタするフィルタ条件として[バージョン]を選択できるようになりました。
- すべての空のAWS領域、VPC、サブネット、およびディレクトリを非表示にする機能が追加され、Computersページで混乱が減り、ロード速度が向上します。
- 1つのイベントで1つのハートビート内の同一のエージェントイベントを集約しました。
- Policies>List>Port Listsページを更新しました。
- スマートフォルダを作成するときに、[コンピュータ]ページの[タスク]列に表示される値をフィルタするフィルタ条件として[タスク]を選択できるようになりました。たとえば、「Scheduled Malware Scan Pending(Offline) 」がタスクとして含まれるすべてのコンピュータをリストするスマートフォルダを作成できます。さらに、Deep Security APIを使用してコンピュータを検索する場合は、tasks/agentTasks および tasks/applianceTasks フィールドの値を検索できるようになります。
- Deep Security Managerでは、信頼する証明書が重複してインポートされないようになりました。
- Computers>Add Account同期スケジューリングが再設計され、テナントごとにさらに多くのコネクタが処理され、アイドル状態のスレッド時間が短縮され、コネクタが無効なアカウント情報との同期頻度が低くなりました。
- 初期設定では、ダッシュボードの[マイユーザの概要]ウィジェットには過去24時間以内に発生したログインに関する情報のみが表示されます。
- パケットデータをDeep Security Managerに送信しないように選択するには、管理>エージェント>データプライバシーに進み、いいえを選択します。。

- Deep Security Managerの診断パッケージには、暗号化機能があります。パッケージとログを暗号化するには、管理>診断パッケージの作成>AES 256暗号化を有効化し、パスワードを入力します。

  注意: 暗号化されたzipは、Windowsの初期設定のZIP抽出ツールを使用して解凍できないため、7Zip、WinZipなどのサードパーティのツールで解凍する必要があります。

- 診断パッケージとログから潜在的に機密性の高い情報を修正しました。

イベントベースのタスク:

- アカウント名、ラベル、ネットワークタグなどを含むGCPセキュリティ自動化のサポートをタスク条件に追加することで、イベントベースのタスクの機能が向上しました。
- 特定のパブリックベンダーのタスクの範囲を制限するために、イベントベースのタスクの条件に「クラウドベンダー」を導入しました(AWSやGCP).など)

コマンド:

- 次のコマンドが追加されました。

  ```
  dsm_c -action changesetting -name
  com.trendmicro.ds.antimalware:settings.configuration.maxSelfExtractRTScanSizeMB -value 512
  ```

  Deep Security Agentが対象ファイルの種類を判別できなかった場合、検索エンジンはそのファイルをメモリにロードして自己解凍ファイルかどうかを確認します。これらのサイズの大きいファイルが多数ある場合、検索エンジンは大量のメモリを消費します。上記のコマンドを使用すると、ファイルサイズの制限は、対象ファイルをロードするために512MBに設定されます。ファイルサイズが設定された制限を超えると、検索エンジンはこのプロセスをスキップしてファイルを直接検索します。

  この拡張機能を実装するには

  1. Deep Security Managerでコマンドを実行して、データベース内の値を変更します。
  2. 設定を配信するには、対象のDeep Security Agentにポリシーを送信します。

- Deep Security管理者がポリシーページの侵入防御, 変更監視 および セキュリティログ監視 タブから未解決の推奨検索結果を非表示にする機能が追加されました。未解決の推奨検索結果を非表示にするには、次のコマンドを使用します。

  侵入防御:

  ```
  dsm_c -action changesetting -name
  ```

```
com.trendmicro.ds.network:settings.configuration.showUnresolvedRecommendationsInfoInPolicyPage -value false
```

変更監視:

```
dsm_c -action changesetting -name com.trendmicro.ds.integrity:settings.configuration.showUnresolvedRecommendationsInfoInPolicyPage -value false
```

セキュリティログ監視:

```
dsm_c -action changesetting -name com.trendmicro.ds.loginspection:settings.configuration.showUnresolvedRecommendationsInfoInPolicyPage -value false
```

拡張予約タスク:

- タスクが有効になりましたの名前がに変更されました。予約タスクウィザードの最後の画面でタスクを有効にします。
- クラウドアカウントを同期すると、vCloudおよびAzureコネクタのみがサポートされるようになりました。
- 不正プログラム対策検索と侵入防御タスクのComputer/group選択の詳細がリストビューで表示されるようになりました

仮想アプライアンス:

- NSX-T環境でDeep Security Virtual Applianceで保護されたゲストVMを自動有効化する機能が追加されました。
- "VMware NSXポリシー構成の競合"システムイベントを追加しました。このイベントは、Deep Security ManagerがEndpoint ProtectionおよびNetwork Introspection(E-W) のために異なるセキュリティポリシーが設定されたNSX-Tグループを検出した場合に生成されます。
- Deep Security Managerがアップデートされ、仮想マシンのハードウェア情報が不足していてもvCloudアカウントを追加できるようになりました。
- NSX-T ManagerでDeep Security Virtual Appliance SVMをアップグレードすると、新しいSVMがゲストVMを保護していることがDeep Security Managerによって検出され、アップグレード後にこれらのVMが自動的にアクティベートされます。
- Deep Security ManagerのvCloudコネクタがアップグレードされ、vCloud 9.7およびvCloud 10.0がサポートされます。
- Deep Security ManagerポリシーをNSX-T環境と同期する機能が追加されました。

- NSX-T Managerを使用したvCenterコネクタの削除時の操作性が向上しました。以前は、サービスプロファイル、エンドポイントルールとサービスの配信、またはvCenterの削除が失敗するため、NSX-Tコンポーネントを手動で削除する必要がありました。
- Deep Security ManagerはLDAPアカウント情報を使用してNSX-T Data Centerに接続できるようになりました。以前は、ローカルのNSX-Tアカウントアカウント情報のみを使用できます。

その他:

- 不正プログラム対策の処理が失敗すると、結果が[Syslog結果]フィールドに表示されます。

解決済みの問題

- 管理>ユーザ管理>ユーザ>ユーザの現在のアカウント>設定でライセンスされていないモジュールを非表示にするオプションが選択された場合、すべてのモジュール隠されていたSEG-77037/03228448 / DS-51202
- 侵入防御処理が侵入防御、「ファイアウォール」に選択された場合、変更監視またはセキュリティログ監視のルールに従って、コンピュータは新しいポリシーで自動的にアップデートされませんでした。SEG-66986 / SF02684105 / DSSEG-5201
- 場合によっては、スマートフォルダを編集できませんでした。SEG-74078 / SF03120830 / DSSEG-5450
- 侵入防御処理が侵入防御、「ファイアウォール」に選択された場合、変更監視またはセキュリティログ監視のルールに従って、コンピュータは新しいポリシーで自動的にアップデートされませんでした。DS-50216 / SEG-77260
- 「放置」とマークされた不正プログラム対策イベントは、ダッシュボードまたは不正プログラム対策イベントで正しくカウントされませんでした。DS-49364 / SEG-70872
- エージェントがAWSメタデータなしでアクティベーションを実行した後、後でハートビートを実行した場合、クラウドプロバイダがアップデートされていないため、コンピュータが適切にリホームされません。DS-50713 / SEG-77150
- コンピュータページでステータスライト> 等しい > 管理された[Green]で高度な検索を実行し、CSVにエクスポートを選択した場合、CSVファイルにはリストされたコンピュータが含まれていませんでした。DS-49936/SEG-74140
- ログインエンドポイントが変更されたため、Azureの政府部門でAzureアカウントを追加できませんでした。これは、Azure Marketplaceの配信にのみ適用されます。DS-52399
- VMware ESXをアップグレードした後、vCenterを手動で再同期して新しいプラットフォーム情報を確認する必要がありました。DS-50053
- テナントの場合、セキュリティモジュール使用状況レポートは、デフォルトのフルアクセスロールにアクセス権がある場合にのみ表示されました。(SEG-70494/SF02940195/DS-47492)

- Internet Explorerでサインアップページが正しく表示されませんでした。(SEG-73072 / SF03075345 / DS-48944)
- 大規模なボディを持ついくつかのメールがキューに入れられたとき、バッチではなくすべてを一度にロードしていたため、大量のメモリが使用されていました。(SEG-71863 / SF03024164 / DS-49833)
- ダッシュボードで「タグなし」フィルタが選択された場合、一部のウィジェットでは引き続きタグ付きアイテムが表示されます。(SEG-63290 / SF02585007 / DS-43795)
- マルチテナント設定のテナントは、リレーをプライマリテナントリレーグループに移動することができました。これにより、リレーがリレー管理ページから消えることがありました。テナントがリレーをプライマリテナントリレーグループに移動することは現在防止されています。(SEG-57715/02322762/DS-47509)
- 同じSVGファイルをダウンロードするリクエストが1,000件以上あった場合、ファイルがキャッシュされていなかったため、パフォーマンスの問題が発生しました。(SEG-64280/DS-45002)
- 「同じコンピュータ名の新しいコンピュータをアクティベートする」が選択された場合、同じ仮想UUIDを持つAIAホストが失敗します。(SEG-66346/02725330 / DS-45423)
- 一部のマルチテナント環境では、テナントとしてログインできませんでした。詳細については、Deep Security 9.0 の既知の問題を参照してください。(SF02873892/SEG-68674/DS-46391)
- 整合性モニタリングが有効で、アンチマルウェアが無効になっている場合、「セキュリティ更新: エージェント/アプライアンスのパターン更新に失敗しました」という警告メッセージが表示されます。(SEG-68454/SEG-67859/DS-32205)
- 不正プログラム検索の設定画面で、詳細タブの内容が一般タブをクリックします。(SEG-64701 / SF02657864 / DS-44176)
- Deep Security Managerには、コンピュータやフォルダが大量にある場合に、一部のページにコンピュータのツリーをロードする際に問題が発生しました。(SEG-58089 / SF02345427 / DS-44424)
- AWSコネクタが同期できません。(SEG-66472 / DS-45029)
- 「Security Module Usage Report」のCSV出力の列名が、データ列.(SEG-66717 / SF02619240 / DS-45130)と部分的に位置がずれています。
- 不正プログラムスキャン構成ウィンドウ(コンピュータ/ポリシー > 不正プログラム対策 > 一般 > 手動検索 > 編集 > 詳細設定 で圧縮ファイルのスキャンを選択) 、抽出するファイルの最大数 設定は、無制限を意味する0 に設定できませんでした。(SEG-65997/02685854/DS-45081)
- PostgreSQLを使用しているDeep Security Managerによって、イベントがAWS SNSに転送されていないことがありました。(SEG-67362 / SF02798561 / DS-45594)

- 多数のホストおよび保護ルールが設定された環境にDeep Security Managerを配置した場合、管理者は一部のホストからデータのみを要求した場合でも、すべてのホストのデータをロードすることがあります。(SF02552257 / SEG-62563 / DS-43188)
- 起動時に、Deep Security Managerはイベントテーブルのデータベーススキーマを検証します。ログは、実際にはアップデートが必要ない場合でも、スキーマがアップデートされたと常に示しています。(DS-43196)
- Active Directoryの同期が完了しないことがあります。(SEG-52485 / DS-38203)
- 親ポリシーでカスタム回避技術対策の姿勢が選択されている場合(ポリシーエディタ設定>詳細>ネットワークエンジン設定>回避技術対策姿勢>が「カスタム」), を選択しました。この設定は下位ポリシーには表示されませんでした。(SF02434648 / SEG-60410 / DS-41597)
- Linuxシステムでは、同時に開いているファイルの初期設定の最大数がDeep Security Managerのニーズを満たしていなかったため、マネージャはファイルハンドルの取得に失敗しました。その結果、Deep Security Managerの機能がランダムに失敗し、ログに「ファイルが多すぎます」というメッセージが表示されていました。(SEG-59895 / DS-43192)
- [アクティビティ概要]ウィジェットで、データベースのサイズが正しく表示されないことがあります。(SF02449882 / SEG-63362 / DS-43946)
- [アラート設定]ページを[オン]列でソートすると、アラートの数が正しく表示されないことがありました。(SF02578797 / SEG-63560 / DS-43685)
- 特定のスマートフォルダの検索条件により、IllegalStateExceptionエラーが発生しました。(SF02436019 / SEG-60330 / DS-41369)
- 「Managerノードステータス」ダッシュボードウィジェットのメモリ使用率が最後に記録されたシステムメモリ使用率と一致しませんでした。(SF02218013 / SEG-55761 / DS-39149)
- Deep Security Managerのポリシー>侵入防御のルール>アプリケーションの種類>(DNSクライアントの選択) >のプロパティ>一般、ポートリストが更新されると、ポート設定は「Any」に変わります。(SEG-55634 / DS-39444)
- このオプションが利用できなかったため、攻撃の予兆アラートを無効にできませんでした。(SEG-49907 / DS-35122)
- 一部のAzure仮想マシンの種類が正しく分類されていません。(SF01885266 / SEG-48561 / DS-33951)
- AWS Marketplaceの課金請求のユーザに、課金ジョブが処理されたときにシステムイベントでエラーが報告されることがあります。(SF1899351 / SEG-48580 / DS-33955)
- 変更監視詳細な変更と推奨のレポートがスマートフォルダに対して実行されていません。(SF2056260 / SEG-51781 / DS-35886)

- [コンピュータ]ページがステータス別にグループ化されている場合、グループごとにコンピュータの総数が正しく表示されないことがあります。(SF01655622 / SEG-44858 / DS-37769)
- Deep Security Managerが大文字と小文字を区別するMicrosoft SQLデータベースとVMware NSXの両方に接続されている場合、Deep Security Managerのアップグレード準備チェックは失敗し、アップグレードをブロックすることがあります。(SF02060051 / SEG-52044 / DS-38405)
- ユーザが自分の役割にアクセスできないコンピュータグループに対して予約検索を開始できたため、エラーが発生しました。(SF02119582 / SEG-53275 / DS-38892)
- データベースに仮想UUIDが重複していると、Deep Security Agentがオフラインになることがありました。(SF01722554 / SEG-41425 / DS-39272)
- ライセンスの期限切れに関する誤ったアラートがときどき発生しました。(SF01484611 / SEG-41437 / DS-33831)
- $記号を含むローカル鍵の秘密鍵を使用すると、Deep Security Managerのアップグレードまたは新規インストールが停止しました。(SF02013831 / SEG-57243 / DS-39526)
- Deep SecurityはSIGARというオープンソースライブラリを使用していましたが、これはもはや維持管理もサポートもされていません。これにより、アプリケーションがクラッシュしたり、今後意図しないその他の問題が発生する可能性があります。(SF02184158 / SEG-54629 / DS-39394)
- 無効なSNMPサーバ名またはunresolvable SNMPサーバ名が管理>システム設定>イベント転送>SNMPに設定されていると、SIEM&SNSも失敗しました。(SF02339427 / SEG-57996 / DS-39865)
- Deep Security Managerホスト名がDNS解決によって取得されなかった場合、SIEMイベント転送を使用した「Deep Security Manager経由のイベントの転送」は機能しません。(SEG-50655 / DS-37374)
- AWS SNS経由でエクスポートされたイベントには、HostOwnerIDが含まれていません。これは、AWSアカウントIDに対応しています。(SF02420860 / SEG-59870 / DS-41089)
- Deep Security Managerのコンピュータまたはポリシーエディタの不正プログラム対策>一般>リアルタイム検索>スケジュール>編集、スケジュールがコンピュータとポリシーに正しく割り当てられていても、[割り当て先]タブが空になることがありました。(SF02374723 / SEG-58761 / DS-41036)

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロによる脆弱性に対する保護方法の詳細については、「脆弱性対策」を参照してください。(DS-45446/DS-44955/DS-43627/DS-28754/DS-32322/DS-33833/DS-26068)

最高共通脆弱性評価システム (CVSS) スコア: 9.8

最高の重大度 : 重大

- JREを最新のJavaアップデート(8.0.241/8.43.0.6) に更新しました。
- Deep Security Managerで使用されるサードパーティのライブラリがアップデートされました。(DS-24214)
- Apache Tomcatを8.5.53にアップグレードしました。(VRTS-4652)

既知の問題

- Oracleデータベースを使用している場合、このアップグレードにはデータベーススキーマが変更されるため、通常よりも時間がかかります。Deep Security Managerのアップグレードの詳細については、Deep Security Managerのバージョンアップを参照してください。
- 新しいDeep Security Virtual Applianceが配信されると、ローカルWebサーバを使用してTrend Micro Deep Security Virtual Applianceソフトウェアパッケージを保存している場合、VM名は「Trend Micro_Custom -<version>」と表示されます。これは、アプライアンスの整合性には影響しません。
- SQL 2008の内部テスト中に発見された問題により、トレンドマイクロはSQL 2008がDeep Security Managerデータベースである場合、Deep Securityの機能リリースへのアップグレードをブロックします。Microsoft SQL Server 2008はMicrosoftによってサポートされなくなり、したがって最新のDeep Security Managerリリースのデータベースとしての使用はテストおよびサポートされなくなりました。Microsoftからの詳細情報については、SQL Server 2008およびSQL Server 2008 R2のサポート終了を参照してください。Deep Security Managerで使用可能なデータベースの完全なリストについては、"システム要件 " on page 400のシステム要件を参照してください。(DS-36715)
- NSX-TがDeep Securityとサードパーティサービスに同時に同じサービスチェーンをバインドするように設定されている場合、Deep SecurityからvCenterアカウントを自動的に削除することは失敗します。この問題は、NSX-T APIがDeep Securityに関連するサービスプロファイルを持つサービスチェーンを変更することを許可しないために発生します。この問題を回避するには、vCenterを手動で削除してください。詳細については、"NSX環境からのDeep Securityのアンインストール" on page 1731を参照してください。DS-47944
- Deep Security ManagerはNSX-T Managerバージョン2.xをサポートしていません。NSX-T Managerをバージョン3.0.0以降にバージョンアップします。DS-50387

Deep Security Agentの新機能

Linux

Deep Security Agent - 20.0.3-860 (20 LTS 更新 2026-01-21)

リリース日: 2025年1月21日

ビルド番号: 20.0.3-860

新機能

Endpoint Event Viewer: Endpoint Event Viewerにアクセスして、管理されたコンピュータ全体のセキュリティおよびシステムイベントを期間、重大度、イベントの発生元、アクションでフィルタリングして表示します。これはTrend Vision One - サーバ & Workload Protectionのみでサポートされています。

解決された問題

- Deep Security Agentは、syslogホスト名が64文字を超えるとクラッシュしました。PCT-87531/DSA-14252
- Webレピュテーションサービスを有効にすると、システムメモリの使用量が継続的に増加しました。PCT-80352/DSA-13866
- Deep Security Agentは、エージェントが予期していた形式と異なるHTTP/2パケットを処理する際に、時々クラッシュすることがありました。PCT-85552/DSA-13755
- Deep Security Agentが再起動した後、侵入防御検出が時々動作を停止しました。PCT-82352/DSA-13755

Deep Security Agent - 20.0.2-29810 (20 LTS 更新 2025-12-24)

リリース日: 2025年12月24日

ビルド番号: 20.0.2-29810

解決された問題

- アプリケーションコントロールは、ルールセットの更新が適用されたときにインベントリを保持できませんでした。詳細については、Trend Vision One™サーバ&Workload Protection、Cloud One Workload Security、およびDeep Securityアプリケーションコントロールがルールの更新時にインベントリを保存できない場合がありますを参照してください。DSA-13750

Deep Security Agent - 20.0.2-29760 (20 LTS アップデート2025-12-09)

リリース日: 2025年12月09日

ビルド番号: 20.0.2-29760

新機能

Ubuntu 24.04 (AWS Arm-based Graviton 2) のサポート: Deep Security Agent 20.0.2-29760以降はUbuntu 24.04 (AWS Arm-based Graviton 2) をサポートします。これにはDeep Security Manager 20.0.1123以降が必要です。

強化機能

- ファイアウォールと侵入防御システムのイベントは、データが利用可能な場合、プロセスとユーザ情報を表示します。これはすべての顧客に段階的に展開されています。DSA-13741
- Deep Security Relayを使用するエージェントのために、Deep Security Agentの設定ファイルで強力な暗号化方式 (app.relay.strongciphers=true) と最小のTransport Layer Security (TLS) バージョン (app.relay.restrictRelayMinimumTLSProtocol=TLSv1.2) を設定できるようになりました。DSA-2163
- 高度な脅威検索エンジンがバージョン25.560に更新されました。DSA-12306

解決された問題

- Deep Security Agentは、新しいRPMライブラリ(rpm-4.16.1.3-39.el9.x86_64以上/rpm-4.19.1.1-20.el10.x86_64以上) を使用する一部のRed Hat Package Manager (RPM) ベースのLinuxディストリビューションで起動できませんでした。詳細については、Red Hat Enterprise Linux (RHEL) バージョン9または10のシステムパッケージを更新後にTrend Micro™ Deep Security™ Agent (DSA) およびTrend Vision One™ XDR for Endpointsが起動できないを参照してください。PCT-84361/V1E-116239
- 一部のシステムでファイルコレクションまたはカスタムスクリプト機能を使用したログのアップロードに失敗しました。この問題はTrend Vision Oneのみに影響しました。V1E-115291
- アプリケーションコントロールは、許可されるべきシェルを通じて実行されるいくつかのアプリケーションをブロックしました。PCT-83681

- Deep Security Agent 20.0.2.22850または20.0.2.26670にアップグレードした後、強化された推奨検索が無効になり、自動的に再有効化されませんでした。この問題が発生した場合、システムは36時間後に従来の推奨検索を使用するように戻り、機能の継続を確保しました。この問題はEndpoint & Workload Securityにのみ影響しました。WS-13982

セキュリティ更新

このリリースにはサードパーティライブラリの更新が含まれています。DSA-13181/DSA-13204

既知の問題

- アプリケーションコントロールは、ルールセットの更新が適用されたときにACインベントリを保持できません。

  推奨されるアクション:
  - アプリケーションコントロールを実行しているエージェントがバージョン20.0.2-29760にアップグレードされていない場合、これらのエージェントをアップグレードしないでください。
  - アプリケーションコントロールを実行しているエージェントがすでにバージョン20.0.2-29760にアップグレードされている場合、次の手順を順番に実行してください。
    a. アプリケーションコントロールが有効になっているすべての20.0.2-29760エージェントに対してアプリケーションコントロールのブロックモードを無効にします。
    b. アプリケーションコントロールが有効になっているすべてのエージェントを以前のエージェントバージョンにダウングレードします。
    c. 必要に応じて、これらのエージェントに対してアプリケーションコントロールのブロックモードを再度有効にしてください。

  詳細については、Trend Vision One™サーバ&Workload Protection、Cloud One Workload Security、およびDeep Securityアプリケーションコントロールがルールを更新する際にインベントリの保存に失敗する可能性がありますを参照してください。DSA-13750

Deep Security Agent - 20.0.2-26670 (20 LTS 更新 2025-11-12)

リリース日: 2025年11月12日

ビルド番号: 20.0.2-26670

新機能

ユーザベースのファイアウォール: ファイアウォールルールはユーザアカウントに基づいて設定できるようになりました。この機能はすべての顧客に段階的に展開されています。

強化されたHTTP/2サポート: 侵入防御システムエンジンは、現在、受信HTTP/2接続をサポートしています。この機能は、安定性とパフォーマンスの向上を確保するために、バックエンドの更新を通じて段階的に展開されます。(このリリースには、HTTP/2の処理とセキュリティの向上を目的とした修正も含まれています。PCT-77306/DSA-13105)

Rocky Linux 10のサポート: Deep Security Agent 20.0.2-26670以降は、SELinux、Secure Boot、FIPSモードのサポートを含むRocky Linux 10をサポートします。

Debian Linux 13のサポート: Deep Security Agent 20.0.2-26670以降は、Secure BootサポートおよびFIPSモードサポートを含むDebian Linux 13をサポートします。これにはDeep Security Manager 20.0.1112以降が必要です。

Red Hat Enterprise Linux 8 (64-bit IBM Z) 不正プログラム対策手動検索のサポート:: Deep Security Agent 20.0.2-26670以降は、Red Hat Enterprise Linux 8 (64-bit IBM Z) に対して不正プログラム対策手動検索のみをサポートします。これにはDeep Security Manager 20.0.1112以降が必要です。このプラットフォームにはセキュリティ更新は提供されません。

Red Hat Enterprise Linux 9 (64-bit IBM Z) 不正プログラム対策手動検索のサポート:: Deep Security Agent 20.0.2-26670以降は、Red Hat Enterprise Linux 8 (64-bit IBM Z) の不正プログラム対策手動検索のみをサポートします。これにはDeep Security Manager 20.0.1112以降が必要です。このプラットフォームにはセキュリティ更新は提供されません。

解決された問題

- dsa_scanを使用してスキャンできなかったファイルが自動的に感染ファイルとして分類されていました。DSA-10037
- 高度なTLSトラフィック検査が、Linuxカーネルバージョン6.11から6.14を実行している環境でDockerコンテナのクラッシュを引き起こしました。DSA-13372

既知の問題

- 高度なTLSトラフィック検査は、Linuxカーネルバージョン6.11から6.14で実行されているDockerコンテナで誤動作を引き起こすことがあります。DSA-13371

Deep Security Agent - 20.0.2-22850 (20 LTS 更新 2025-10-08)

リリース日: 2025年10月08日

ビルド番号: 20.0.2-22850

解決された問題

- ネットワークデバイスの問題により、一部のシステムがクラッシュしました。PCT-74972/DSA-12698
- 複数のプロセスが同時にdsa_filterドライバーを更新すると、システムクラッシュが発生することがあります。PCT-76239/DSA-12697

Deep Security Agent - 20.0.2-20480 (20 LTS 更新 2025-09-17)

リリース日: 2025年9月17日

ビルド番号: 20.0.2-20480

新機能

Oracle Linux 10: Deep Security Agent 20.0.2-20480以降は、SELinux、Secure Boot、FIPSモードのサポートを含むOracle Linux 10をサポートします。これにはDeep Security Manager 20.0.1081以降が必要です。

強化

- セキュリティログ監視はディレクトリ名でグロブ文字をサポートするようになりました。PCT-8309

解決された問題

- アプリケーションコントロールが有効な状態でDeep Security Agentを実行すると、一部のシステムでメモリリークが発生しました。DSA-12148
- Deep Security Agentで高度なTLSトラフィック検査を使用すると、特定のサードパーティソフトウェアがシステム上で実行されている場合に高いCPU使用率が発生しました。PCT-55552/DSA-11921

- Podmanシステムサービスの実行が一部のシステムでDeep Security Agentの機能に干渉しました。(Command Lineを使用してPodman情報を取得する場合、エージェントには影響しません。) PCT-16544/PCT-47917/PCT-63773/DSA-4452

Deep Security Agent - 20.0.2-17500 (20 LTS 更新 2025-08-13)

リリース日: 2025年8月13日

ビルド番号: 20.0.2-17500

機能強化

- すべてのAgent-PGPCore*およびAgent-Core*ファイルは、Deep Security Agentのアップグレード完了後にアプリフォルダから削除されました。DSA-10996

解決された問題

- カーネルサポートパッケージファイルの整合性チェックは、ほぼ同時に複数のコピーがダウンロードされた場合に失敗することがあります。PCT-66493/DSA-11495
- Deep Security Agentはハートビート接続を確立する際にクラッシュすることがあります。PCT-66595/DSA-11386
- Deep Security Agentは、LinuxカーネルバージョンがDeep Security Managerにインポートされた最新のKernel Support Package (KSP) でサポートされなくなった場合、Kernel Support Package (KSP) をインストールできないことがありました。PCT-66447/DSA-11366

Deep Security Agent - 20.0.2-14431 (20 LTS 更新 2025-07-09)

リリース日: 2025年7月9日

ビルド番号: 20.0.2-14431

新機能

Red Hat Enterprise Linux 10: Deep Security Agent 20.0.2.14431以降は、SELinux、Secure Boot、FIPSモードのサポートを含むRed Hat Enterprise Linux 10をサポートします。これにはDeep Security Manager 20.0.1054以降が必要です。

強化

- 高度なTLSトラフィック検査が有効になっている場合、接続がブロックされていない限り、Deep Security Agentは接続を高速化するためにパケットを挿入します。PCT-63207/DSA-10919

解決された問題

- 侵入防御システム、Webレピュテーションサービス、およびファイアウォール保護モジュールは、無効化されている場合でもオフラインステータスを表示しました。PCT-66070/PCT-66493/PCT-67224/DSA-11160
- オンデマンド検索は、Deep Security Agentのアクティベーションまたは再起動後に自動検索がトリガーされるまで手動で開始できませんでした。WS-12581
- 予期しないプロセス値が検出された場合、強化推奨検索が失敗しました。WS-12572
- 不正プログラム対策、Webレピュテーションサービス、および変更監視のエンジンがオフラインになることがあるファイルディスクリプタリークが発生しました。PCT-70783/DSA-11618

Deep Security Agent - 20.0.2-12010 (20 LTS 更新 2025-06-11)

リリース日: 2025年6月11日

ビルド番号: 20.0.2-12010

強化

- デフォルトで有効化されているWebレピュテーションサービスは、ウェブサイトのリスクレベルを判断する際にサーバ名表示 (SNI) クエリを使用します。
- アクティビティモニタリングはJavaServer Page (JSP) ファイルをサポートしました。V1E-54751

解決された問題

- Deep Security AgentはSSLハンドシェイク中に時々クラッシュしました。PCT-55526/DSA-9902

- Vision Oneエンドポイントセキュリティバージョン管理ポリシーが有効になっている場合、Deep Security Agent保護モジュールの展開が時々失敗し、5102「そのようなファイルやディレクトリはありません」エラーが発生しました。DSA-10398

セキュリティ更新

このリリースにはサードパーティライブラリの更新が含まれています。DSA-10530

Deep Security Agent - 20.0.2-9811 (20 LTS 更新 2025-05-14)

リリース日: 2025年5月14日

ビルド番号: 20.0.2-9811

新機能

Red Hat Enterprise Linux 9 (AWS Arm-based Graviton 2): Deep Security Agent 20.0.2-9810以降は、SELinuxサポートを含むRed Hat Enterprise Linux 9 (AWS Arm-based Graviton 2) をサポートします。これにはDeep Security Manager 20.0.1047以降が必要です。

強化

Webレピュテーションサービスは、疑わしいまたは悪意のあるサイトへのhttpプロキシ接続をブロックする際に、200 OKページではなく403 Forbiddenを指すようになりました。PTC-60576/DSA-10325

解決された問題

- 高度なTLSを使用したDeep Security Agentの構成が一部のシステムをフリーズさせました。PCT-63207/DSA-10380
- WebレピュテーションイベントのURL列に情報が欠落していることがありました。PCT-60576/DSA-10090
- 侵入防御システムが有効になっていると、一部のシステムで範囲内の操作に対してUBSANの範囲外エラーが発生しました。PCT-63329/DSA-10353
- Deep Security Agent診断パッケージの処理を改善し、不完全なデータが含まれないようにしました。DSA-10270
- Deep Security Agentは、Kernel Package UpdateがNoに設定されている場合、Deep Security Relayからカーネルサポートパッケージをダウンロードできないことがありました。

詳細については、Deep Security Agent (DSA) reports "Protection Module Deployment Failed (Event ID 5102)" PCT-61830/DSA-10249を参照してください

- OSは互換性のない環境ツールのため、Deep Security Agent不正プログラム対策カーネルモジュールをロードできませんでした。PCT-34454/PCT-41680/PCT-46866/DSA-9349
- オフライン予約検索が、使用すべきDeep Security Agentのタイムゾーンではなく、Server & Workload Protectionのタイムゾーンを使用することがあり、週次および日次検索が誤った時間に開始され、月次検索が月の最終日に開始されると高いCPU使用率を引き起こすことがありました。PCT-55169/DSA-9303
- セキュリティアップデートが失敗した場合、Deep Security Agentが複数のシステムサービスを停止することがあります。PCT-62050/DSA-10168

Deep Securityエージェント - 20.0.2-7600 (20 LTS 更新 2025-04-16)

リリース日: 2025年4月16日

ビルド番号: 20.0.2-7600

新機能

動的インテリジェンスモード: 動的インテリジェンスモードにより、Deep Securityエージェントは検出された脅威、ユーザの挙動、システム構成に基づいて、セキュリティ対応を最適化するために監視レベルを自動的に調整できます。

解決された問題

- カーネルサポートパッケージの更新がWebレピュテーションサービスの動作を停止させ、侵入防御システムがルールのコンパイルエラーに遭遇しました。DSA-6398
- 不正プログラム対策エンジンは、パターン更新後にクラッシュすることがあります。DSA-9208
- 「エージェントによる不正プログラムのスケジュールスキャンのトリガーを有効にする」が有効になっていると、スケジュールスキャンが誤った日付や時間にトリガーされることがあります。PCT-21726/DSA-6938

Deep Securityエージェント - 20.0.2-4961 (20 LTS 更新 2025-03-12)

リリース日: 2025年3月12日

ビルド番号: 20.0.2-4961

新機能

バージョン管理ポリシー: Deep Securityエージェントは、バージョン管理ポリシーの高度な設定をサポートするようになり、Trend Vision Oneバージョン管理ポリシーがTrend Micro Endpoint Basecamp (XBC) エージェントをインストールしたエンドポイントのカーネルサポートの更新を管理できるようになりました。詳細については、Version Control Policiesを参照してください。

これは現在プレリリース中であり、Trend Vision One - サーバ&ワークロード保護のみサポートされています。DSA-9384

強化

- dsa_scanコマンドには、大きなファイルを管理するためのscanLargeFileオプションが含まれるようになりました。DSA-8825

解決された問題

- SAP Scannerは、4096バイトを超えるCSVファイルを誤って分類することがありました。PCT-51974/DSA-9139
- Deep Securityエージェントは、いくつかのネットワークプロトコルでTLS 1.3を使用するとパフォーマンスが低下することがありました。DSA-6959

既知の問題

- カーネルサポートパッケージの更新により、Webレピュテーションサービスが機能しなくなり、侵入防御システムがルールコンパイルエラーに遭遇します。この問題の詳細および回避策については、トレンドマイクロ™ Deep Security™におけるWebレピュテーションサービス (WRS) が機能しないおよび侵入防御システム (IPS) のルールコンパイルエラーを参照してください。DSA-6398

Deep Securityエージェント - 20.0.2-1390 (20 LTS 更新 2025-01-15)

リリース日: 2025年1月15日

ビルド番号: 20.0.2-1390

新機能

ユーザベースのファイアウォールイベント: ファイアウォールイベントには、可能な限りユーザ名が含まれるようになりました。この機能はプレビュー段階であり、現在は一部の顧客のみが利用可能です。

機能強化

- Deep Securityエージェントは、パフォーマンスを向上させるためにパケットを順番に処理するようにキューに入れるようになりました。DSA-6916

解決された問題

- Deep Securityエージェントは、高度なTLSトラフィック検査が有効になっているときに接続の問題が発生することがありました。DSA-8577

セキュリティ更新

このリリースには、サードパーティライブラリの更新が含まれています。DSA-7696/DSA-7697/DSA-8042

Deep Securityエージェント - 20.0.1-25771 (20 LTS Update 2024-12-10)

リリース日: 2024年12月10日

ビルド番号: 20.0.1-25771

新機能

バージョン管理ポリシー: Deep Securityエージェントは、バージョン管理ポリシーをサポートするようになりました。これにより、Trend Vision Oneのバージョン管理ポリシーを使用して、Trend

Micro Endpoint Basecamp (XBC) エージェントがインストールされているエンドポイントのエージェントおよびコンポーネントの更新を管理できます。詳細については、Version Control Policiesを参照してください。これは現在プレリリース中であり、Trend Vision One - Server & Workload Protectionのみサポートされています。

隔離の自動クリーンアップ: Deep Security Agentは、隔離フォルダのディスク使用量が最大量を超えた場合に、隔離フォルダ内のファイルの一部を自動的に削除します。最大ディスク使用量 (デフォルトでは1024 MB) は、コンピュータ(またはポリシー)> 不正プログラム対策 > 詳細 > 検出されたファイルから設定できます。この機能は現在、Cloud One Workload Securityでのみ利用可能です。

強化

- Deep Securityエージェント20.0.1.25771以降は、Ubuntu 22.04のFIPSモードをサポートしています。DSA-7699
- Deep Securityエージェントは、64ビットLinuxオペレーティングシステムでOpenJDK 8を実行しているApache Tomcatサーバー上の侵入防御のための高度なTLSトラフィック検査をサポートするようになりました。DSA-8244
- Deep Security SAP Scannerは、Microsoft Outlookアイテム (MSG) 形式のメールに添付されたパスワード保護された圧縮ファイルを検出した場合に、その結果をSAPアプリケーションに報告できるようになりました。SF07873657/PCT-23367/DSA-7716
- 不正プログラム対策の挙動監視の検出レベルと防止レベルを設定できるようになりました。DSA-6796
- Deep Securityエージェントは、リレープロキシがTrend Vision One Service Gateway Forward Proxy Serviceであるかどうかを検出し、接続にリレープロキシを使用するかどうかを決定するためにService Gatewayドメイン許可リストを使用します。SF07267852/PCT-29311/DSA-6274
- Trend Cloud One - Endpoint & Workload Securityは、Deep Security Agentを介してTrend Vision One Endpoint Securityエージェントをインストールできるようになりました。DSA-7532
- Deep Securityエージェントは、不正プログラム対策、挙動監視、機械学習型検索のリアルタイム検索における検出感度を微調整するための追加オプションをサポートするようになりました。この強化機能は、Trend Cloud One - Endpoint & Workload Securityでのみ利用可能です。DSA-6062
- メモリファイルディスクリプタ(memfd) を介して起動される可能性のある悪意のあるプロセスに対する検出と保護が向上しました。DSA-6009

解決された問題

- パケットデータを含むイベントが不正なパケットサイズで記録されていました。PCT-45556/DSA-8074
- 一部の不正プログラム対策が有効なシステムでメモリリークが発生しました。DSA-8243
- 一部のシステムでメモリの問題が発生し、不正プログラム対策が停止しました。PCT-46330/DSA-8156
- Deep Security SAP Scannerは、同じ内容のファイルが2つ以上圧縮ファイルに含まれている場合に、スキャン失敗を誤って報告することがありました。PCT-38781/DSA-7324
- 変更監視スキャンの後に変更監視が無効にされた場合、Deep Securityエージェントの CPU使用率が通常よりも高くなりました。SF07991055/PCT-31459/DSA-6195
- エージェントセルフプロテクションが有効になっている場合、再起動が原因で一部のシステムがハングすることがありました。PCT-27574/PCT-29800/DSA-6007
- SAPが有効になっていると、重複する除外パスが作成されることがあり、SAPを無効にしても残ることがありました。DSA-7595

セキュリティ更新

このリリースには、サードパーティライブラリの更新が含まれています。DSA-7124

Deep Securityエージェント - 20.0.1-23340 (20 LTS 更新 2024-11-13)

リリース日: 2024年11月13日

ビルド番号: 20.0.1-23340

強化

- Deep Security Agent 20.0.1-23340以降では、Red Hat Enterprise Linux 9 (PowerPCリトルエンディアン) の追加サポートが追加されました。詳細については、Deep Security 20 LTSまたはTrend Cloud One - Endpoint & Workload Securityのプラットフォーム別サポート機能をご覧ください。DSA-7234

- Webレピュテーションサービスは、Webサイトのリスクレベルを判断する際にサーバー名表示 (SNI) クエリを使用できるようになりました。DSA-7314
- 機械学習型検索サービスの接続タイムアウトが9秒に延長され、「Census、ファイルレピュテーション、機械学習型検索サービスの切断」イベント(イベントID 945) の数を減らすようにしました。DSA-5321

解決済みの問題

- アプリケーションコントロールがブロックモードで動作しているとき、一部のディレクトリ内のファイルがブロックされるべきところを許可されていました。PCT-38516/DSA-7613
- Deep SecurityエージェントでTransport Layer Security (TLS) 1.3を使用して高度なTLSトラフィック検査を有効にした場合、一部のシステムでカーネルパニッククラッシュが発生しました。PCT-43009/DSA-7787
- 一部のシステムで、無効なメモリアドレスの取得によりOSクラッシュが発生しました。PCT-33865/DSA-6335

Deep Securityエージェント - 20.0.1-21510 (20 LTS更新 2024-10-16)

リリース日: 2024年10月16日

ビルド番号: 20.0.1-21510

新機能

Red Hat Enterprise Linux 9 (PowerPC little-endian) のサポート: Deep Security Agent 20.0.1-21510以降は、Red Hat Enterprise Linux 9 (PowerPC little-endian) に対して不正プログラム対策およびSAP Scannerをサポートします。これにはDeep Security Manager 20.0.979以降が必要です。

強化

- 高度な脅威検索エンジンがバージョン24.5に更新されました。DSA-7354
- Deep Securityエージェントは現在、不正プログラム対策プロセスパスの除外におけるワイルドカード*の使用をサポートしており、Linuxプラットフォーム向けに段階的に展開されています。DSA-6384

解決された問題

- アプリケーションコントロールとFIPSの両方が有効になっていると、高CPU使用率が発生します。DSA-6842
- SAP Scannerライブラリがエージェントへの接続を再確立した際、SAP Scannerライブラリから送信されたスキャン要求が時々拒否されることがありました。SF08196066/PCT-34824/DSA-7608
- 特定の形式 (CSVなど) のファイルをスキャンする際に、Deep Security SAP Scannerがクラッシュすることがありました。PCT-41353/DSA-7609

Deep Security エージェント - 20.0.1-19250 (20 LTS Update 2024-09-18)

リリース日: 2024年9月18日

ビルド番号: 20.0.1-19250

新機能

Ubuntu 24.04 サポート: Deep Security エージェント20.0.1-19250 以降は、Secure Boot サポートを含む Ubuntu 24.04 をサポートします。これには Deep Security Manager 20.0.954 以降が必要です。

機能強化

- Deep Securityエージェントを更新して、古いバージョンのSAP Scannerとの互換性を向上させました。SF08196066/PCT-34824/DSA-6819
- Deep Security エージェントは、Alibaba Cloud コネクタタイプをサポートするようになりました。DSA-6018

解決済みの問題

- Deep Security エージェントが、アプリケーションコントロールとFIPSの両方が有効になっているシステムで高いCPU使用率を引き起こしました。DSA-6842
- 不正プログラム対策エンジンがXDR Endpoint Sensorを使用しているシステムでDeep Securityエージェントの起動中に正しく起動しませんでした。DSA-7158

- オペレーティングシステム情報の検出に問題があると、Deep Securityエージェントが Rocky Linux 9にインストールされないことがありました。PCT-26151/DSA-5630

セキュリティ更新

このリリースには、サードパーティライブラリの更新が含まれています。DSA-6156/DSA-6942

Deep Security Agent - 20.0.1-17380 (20 LTS アップデート2024-08-21)

リリース日: 2024年8月21日

ビルド番号: 20.0.1-17380

機能強化

- Webレピュテーションサービス"Smart Protection Serverへの接続不能" イベントには、説明フィールドにFQDNまたはIPアドレス情報が含まれるようになりました。DSA-5408
- SAP Scannerは、Society for Worldwide Interbank Financial Telecommunication (SWIFT) メッセージをテキストファイルとして分類します。SF07895338/PCT-24359/DSA-5790
- SAP Scanner は、互換性のあるファイル拡張子に JavaScript を関連付けるようになりました。詳細については、サポートされているMIME タイプを参照してください。SF08102626/PCT-31518/DSA-6192

解決された問題

- 不正プログラム対策エンジンが時々クラッシュしました。DSA-5536
- SAP Scannerは、データが1行にフォーマットされている場合、有効なCSVファイルを誤って分類しました。SF07967718/PCT-26844/DSA-6102
- SAP Scanner は時々画像ファイルをASPスクリプトとして誤認識しました。SF07764878/PCT-20406/DSA-6122
- カーネルサポートパッケージ (KSP) はインポート後に自動的に再読み込みされませんでした。DSA-6159
- Deep Security Agent は、一部のポリシー構成フィールドに中括弧が含まれている場合、ポリシーを読み込むことができませんでした。DSA-6189

- ホスト名に非ASCII文字が含まれている場合、Deep Securityエージェントのアクティベーションに失敗しました。PCT-32214/DSA-6268
- Deep Security Agent が Trend Micro Endpoint Basecamp (XBC) エージェントと統合されている場合、完全にシャットダウンできないことがあります。SF08143019/PCT-32915/DSA-6347
- Deep Securityエージェントがインストール中に一時ディレクトリ`/opt/ds_agent@tmp`を誤って作成しました。DSA-6412
- 侵入防御がDeep Securityエージェントで有効になっている場合、サードパーティアプリケーションがソースポートを再利用すると接続の問題が発生することがあります。SF07685331/PCT-20541/DSA-5596
- 不正プログラム対策がクラスタ共有ボリューム上のファイルにアクセスしたとき、Hyper-Vホストがクラッシュしました。SF05713918/SF05850687/SF07038125/SEG-146660/SEG-148664/SEG-186072/PCT-41910/PCT-5467/DSSEG-7664

既知の問題

- Deep Security Agent アプリケーションコントロールが高いCPU使用率を引き起こします。PCT-36414
- 不正プログラム対策エンジンが、XDR Endpoint Sensor を使用しているシステムで Deep Security エージェントの起動中に正しく起動しません。DSA-7158

Deep Security Agent - 20.0.1-14610 (20 LTS アップデート2024-07-17)

リリース日: 2024年7月17日

ビルド番号: 20.0.1-14610

新機能

SUSE Linux Enterprise Server 15 (AWS Arm-based Graviton 2) のサポート: Deep Security Agent 20.0.1-14610 以降は SUSE Linux Enterprise Server 15 (AWS Arm-based Graviton 2) をサポートします。これには Deep Security Manager 20.0.926 以降が必要です。DSA-4836

機能強化

- SAP Scanner は、次の MIME タイプを互換性のあるファイル拡張子に関連付けます。詳細については、SAP NetWeaver と統合する を参照してください。
  - TrueType フォント(TTF)。SF08102626/PCT-31518/DSA-6049
  - Javaアーカイブ(JAR)。SF08102626/PCT-31518/DSA-6044
  - Apple QuickTime File Format (QTFF)。SF07967718/SF07840151/PCT-22825/PCT-26844/DSA-5887/DSA-5567
  - Microsoft Advanced Systems Format (ASF). SF07967718/PCT-26844/DSA-5886

解決済みの問題

- Deep Security Agentは依然としてサービスゲートウェイの接続をテストしようとしました。DSA-5814
- Deep Security Agent の再起動が原因で、アプリケーションコントロールがドリフトイベントを報告することがあります。SF07813110/PCT-25731/DSA-5798
- Deep Security AgentはService GatewayのプライマリIPアドレスのみを使用できました。DSA-4513
- 変更監視 real-time scans が時々イベントを生成できないことがありました。SF07269768/PCT-21721/DSA-5877
- ユーザモードからカーネルモードに切り替えると(コンピュータ または ポリシー > システム > 一般 > システム保護のためにドライバを使用するかどうかを選択) 、Deep Security Agent がリアルタイムの不正プログラム対策保護を失うことがありました。DSA-6090

Deep Security Agent - 20.0.1-12510 (20 LTS アップデート2024-06-19)

リリース日 : 2024年6月19日

ビルド番号 :20.0.1-12510

機能強化

- Deep Security Agent 20.0.1-12510 以降は、Red Hat Enterprise Linux 8.6 (PowerPC リトルエンディアン) に対する追加サポート(SAP Scanner を含む) を追加します。詳細については、Deep Security 20 LTS または Trend Cloud One - Endpoint & Workload Security のプラットフォーム別サポート機能を参照してください。DSA-4835
- Advanced TLS Traffic Inspectionは、"Inbound TLS/SSLトラフィックの検査"と"Outbound TLS/SSLトラフィックの検査"のために別々の設定をサポートしています。詳細な設定手順については、https://help.deepsecurity.trendmicro.com/20_0/on-premise/ja-jp/intrusion-prevention-ssl-traffic.htmlを参照してください。

解決された問題

- 不正プログラム対策が基本的な機能しか持っていなかった頃、一部のシステムが停止することがありました。DSA-4821
- 不正プログラム対策が有効になっている場合、Deep Security Agentが完全にシャットダウンできない場合がありました。PCT-26090/DSA-5492

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-12022/DSA-5484

最高共通脆弱性評価システム (CVSS) スコア: 5.5

最高の深刻度:中

既知の問題

- インバウンドTLS/SSLトラフィックの検査とアウトバウンドTLS/SSLトラフィックの検査がAdvanced TLS Inspection設定で同時に有効になっている場合、パフォーマンスに影響があります。詳細については、Deep Securityにおける双方向TLS検査のパフォーマンスへの影響を参照してください。DSA-5959

- ユーザモードからカーネルモードに切り替えると(コンピュータまたは ポリシー> システム > 一般 > システム保護のためにドライバを使用するかどうかを選択) 、Deep Security Agentがリアルタイムの不正プログラム対策保護を失うことがあります。DSA-6090
- ユーザモードに切り替える(コンピュータまたは ポリシー> システム > 一般 > システム保護のためにドライバを使用するかどうかを選択) と、不正プログラム対策のリアルタイム保護が失われることがあります。DSA-6104

Deep Security Agent - 20.0.1-9400 (20 LTS Update 2024-05-16)

リリース日: 2024年5月16日

ビルド番号: 20.0.1-9400

新機能

ユーザーモードソリューション: ユーザーモードは、Trend Cloud One - Endpoint & Workload Security または Deep Security Manager のUIから有効にでき、カーネルサポートがないシステムに対して不正プログラム対策の基本機能を通じてイベント生成と保護を提供します。

強化

- SAPScannerで SCANLOGPATH パラメータがサポートされるようになりました。詳細については、「 SAP NetWeaverとの統合 」を参照してください。PCT-21958/DSA-4924
- Deep Security Agentをアップデートして、プロキシを使用する設定の優先度を向上させました。DSA-4817/PCT-21750
- Deep Security Agentで、Trend Micro Endpoint Basecamp (XBC) エージェントから Service Gatewayの設定を取得できるようになりました。DSA-4841/V1E-13468

解決済みの問題

- プロキシ設定の再設定後にDeep Security Agentのセキュリティアップデートが失敗することがありました。PCT-18382/DSA-5390
- Webレピュテーションサービスを有効にしてDeep Security Agentを使用すると、一部のアプリケーションパフォーマンス監視 (APM) アプリケーションが正常に機能しませんでした。SF04072723/SEG-97952/PCT-15716/DSA-4750

- 初期設定のポリシーでSecurity-Enhanced Linux (SELinux) 適用モードを使用しているシステムでは、Deep Security Agentの不正プログラム対策ドライバとネットワークドライバをロードできませんでした。PCT-14630/DSA-4917
- Deep Security AgentがLinuxシステムのファイアウォールのポート設定を検出できないことがあり、その結果、エージェントのファイアウォールが機能に必要なポートを許可できませんでした。SF07650853/PCT-16253/DSA-4849
- 不正プログラム対策のオンデマンド検索でファイル記述子が正しく使用されないことがあり、「不正なファイル記述子」ログエラーが発生していました。DSA-4051
- 不正プログラム対策エンジンが時々クラッシュすることがあります。PCT-25789/DSA-4051

セキュリティ更新

このリリースには、サードパーティ製ライブラリのアップデートが含まれています。DSA-4187

既知の問題

- このリリースには、不正プログラム対策エンジンの状態を不正確に報告するため、Oracle Linux 6(32ビット) 用のDeep Security Agentパッケージが含まれていません。DSA-5557
- ユーザモードからカーネルモードに切り替えると(コンピュータまたは ポリシー > システム > 一般 > システム保護のためにドライバを使用するかどうかを選択) 、Deep Security Agentがリアルタイムの不正プログラム対策保護を失うことがあります。DSA-6090
- ユーザモードに切り替える(コンピュータまたは ポリシー > システム > 一般 > システム保護のためにドライバを使用するかどうかを選択) と、不正プログラム対策のリアルタイム保護が失われることがあります。DSA-6104

Deep Security Agent - 20.0.1-7380 (20 LTS Update 2024-04-24)

リリース日: 2024年4月24日

ビルド番号: 20.0.1-7380

新機能

ユーザーモードソリューション: この機能は、カーネルサポートがないシステムでFanotifyとeBPFを使用して基本的な不正プログラム対策機能を提供します。このモードではDeep Security

エージェントはランタイムコンテナワークロードを保護できません。

強化

- Deep Security Agent 20.0.1-7380以降では、SUSE Linux Enterprise Server 12 (PowerPCリトルエンディアン) に対する追加サポート(SAP Scannerを含む) が追加されました。詳細については、Deep Security 20 LTS または Trend Cloud One - Endpoint & Workload Security のプラットフォーム別サポート機能を参照してください。DSA-2626
- Deep Security Agent 20.0.1-7380 以降は、SUSE Linux Enterprise Server 15 (PowerPC little-endian) に対する追加サポート(SAP Scanner を含む) を追加します。詳細については、Deep Security 20 LTS または Trend Cloud One - Endpoint & Workload Security のプラットフォーム別サポート機能を参照してください。DSA-2630
- Deep Security Agentで、Trend Vision One Service Gatewayの除外がサポートされるようになりました。現時点では、Trend Cloud One - Endpoint & Workload Security ユーザのみがサポートされます。V1E-17754
- Deep Security Agentのプロキシ設定は、Trend Vision One Proxy Managerで設定できます。V1E-14557

解決済みの問題

- クラウド環境で実行されているDeep Security AgentをTrend Cloud One -Endpoint & Workload Securityで有効化できないことがありました。DSA-4861
- SAPScannerが有効な場合、Deep Security Agentのアップグレード時に、「SAP:不正プログラム対策の準備ができていません」または「SAP: ウイルス検索サービスが正しく動作していません」というシステムイベントが表示されることがありました。これらのシステムイベントメッセージは、Deep Security Agentモジュールの再起動によってトリガされました。機能への影響はありませんでした。DSA-4603
- tm_netagent プロセスが実行されていると、TLS検査を使用している一部のシステムでDeep Security AgentのCPU使用率が高くなります。PCT-22031/DSA-4805
- トレンドマイクロService Gateway Generic Caching Service (GCS) をTrend Vision Oneから有効にした後、Deep Security ManagerおよびTrend Cloud One - Endpoint & Workload Securityで、Deep Security Agentとの通信時に「ステータスの確認に失敗しました」というエラーが表示されました。DSA-4763
- ローカルのSmart Protection Serverで、誤った数のDeep Security Agentが表示されることがありました。DSA-3780

Deep Security Agent - 20.0.1-4540 (20 LTS Update 2024-03-20)

リリース日: 2024年3月20日

ビルド番号: 20.0.1-4540

新機能

CPU使用率制御: この機能は、不正プログラム対策リアルタイム検索のCPU使用率を制限するための3つの事前定義されたモードを提供します (コンピュータ> 設定 > 一般 > CPU使用率制御)。これは現在、Trend Cloud One - Endpoint & Workload Securityの顧客のみがサポートされています。DSA-2465

機能強化

- SAP Scannerは、Deep Security Agent 20.0.1-4540以降のRed Hat Enterprise Linux 9でサポートされるようになりました。DSA-4213
- Deep Security AgentのSAP Scannerのステータスがコンソールに表示されるようになりました。DSA-3329
- Deep Security Agentのバージョンが SAPScannerライブラリに表示されます。SF07483850/PCT-10077/DSA-3304

解決された問題

- 一部のシステムでは、Deep Security AgentからSmart Protection Serverへの接続が失われると、CPU使用率が高くなり、パフォーマンスの問題が発生しました。SF07552865/PCT-12430/DSA-3784
- Deep Security Agentは、AutoCADで生成された `.dwg` ファイルのMIMEタイプを誤ってAutoCAD 2004からAutoCAD 2024に分類しました。SF07027236/SEG-186079/PCT-5797/DSA-2901

既知の問題

- SAPScannerが有効な場合、Deep Security Agentのアップグレード時に、システムイベントによって「SAP:不正プログラム対策の準備ができていません」または「SAP: ウイルス検索サービスが正常に動作していません」というメッセージが一時的に表示されることがあります。これは、Deep Security Agentモジュールの再起動が原因です。機能への影響はありません。DSA-4572

- トレンドマイクロService Gateway Generic Caching Service (GCS) をTrend Vision Oneから有効にすると、Deep Security ManagerおよびTrend Cloud One - Endpoint & Workload SecurityがDeep Security Agentと通信する際に「ステータスの確認に失敗しました」というエラーを表示します。詳細については、Service Gateway Generic Caching Serviceを有効にした後にDeep Security Agentが「ステータスの確認に失敗しました」と報告するを参照してください。DSA-2756

Deep Security Agent - 20.0.1-3180 (20 LTS Update 2024-02-29)

リリース日: 2024年2月29日

ビルド番号: 20.0.1-3180

強化

- Deep Security Scanner (SAP) は、Microsoft Officeマクロを含むファイルをアクティブコンテンツとしてレポートするようになりましたが、以前は不正プログラムとして識別されていました。PCT-5979/DSA-3911

解決された問題

- Trend Vision One Service Gatewayを使用したオンプレミスDeep Security ManagerからTrend Cloud One - Endpoint&Workload SecurityへのAgentの移行に失敗しました。この問題は、他のプロキシサービスを使用して移行する場合にも発生する可能性があります。PCT-16649/DSA-4144
- Deep Security Agent SAP Scannerで想定される`.msg`ファイルのMIMEタイプが正しくありませんでした。PCT-5797/DSA-4050
- Deep Security Agentで侵入防御またはWebレピュテーションサービスを有効にすると、TLS検査プロセス (tm_netagent) のエラーログローテーションの問題が発生することがありました。DSA-3965
- システム設定のキーワードが正しく解釈されなかったため、Deep Security Agentを起動できませんでした。SEG-156447/PCT-8768/DSA-3897
- IPv6設定を自動検出できなかったため、アップデート中にスマートスキャンがハングしました。DSA-3287

- Fanotifyが有効になっているシステムにDeep Security Agentがインストールされている場合、不正プログラム対策プロセスの再起動または停止によってシステムがフリーズすることがありました。PCT-6047/SEG-190061/DSA-4474

既知の問題

- 実行可能ファイルのコピーを実行すると、アプリケーションコントロールの信頼エンティティブロック別の信頼ルールが正しく機能しないことがあります。PCT-11105/DSA-3324

Deep Security Agent - 20.0.1-690 (20 LTS Update 2024-01-17)

リリース日: 2024年1月17日

ビルド番号: 20.0.1-690

新機能

コマンドライン検索: Deep Security Agentで、コマンドラインインタフェースから`dsa_scan`を使用して起動されるオンデマンド検索がサポートされるようになりました。

現在、この機能はTrend Cloud One - Endpoint & Workload Securityのユーザのみが利用できます。詳細については、「コマンドラインの基礎」を参照してください。V1E-6993

機能強化

- 2024年以降、Deep Security Agentのバージョン管理が20.0.0から20.0.1に改訂されます。これには、Deep Security Manager 20.0.883以降が必要です。DSA-3584。

  詳細については、20.0.1 Linux Kernel Support Package (KSP)をサポートするためのDSM/DSAの準備状況をご覧ください。

解決済みの問題

- Deep Security AgentがローカルのSmart Protection Serverに接続できないことがありました。DSA-3564
- FIPSモードが無効な場合、Deep Security Agentは、エージェントで指定された設定ではなく、システム環境変数で指定されたOpenSSL設定を使用していました。PCT-4914/DSA-2651/DSA-2737/DSA-2738

- SAPScannerが有効な場合、Deep Security Agentでネットワークエラーが誤ってログに記録されていました。DSA-3548
- ファイル拡張子を含まずにSAPScannerの許可リストに追加されたファイルが、許可されるはずのときにブロックされていました。SF06565062/SEG-170933/DS-77132/DSA-3424
- Fanotifyが有効なシステムでDeep Security Agentを使用している場合、ファイルを隔離するとシステムがフリーズすることがありました。PCT-6047/SEG-190061/DSA-2473

既知の問題

- Deep Security Agent 20.0.1-690 へのアップデートが、Trend Cloud One - Endpoint & Workload Security で Deep Security Relay を使用している場合、20.0.0 の一部のバージョンからのアップデートで失敗することがあります。詳細については、自己展開された Workload Security Relay の 20.0.0-3445 以降からバージョン 20.0.1 へのリモートアップグレードの失敗 DSA-3317 を参照してください
- Deep Security Agent 20.0.1-690 のリリースに伴い、トレンドマイクロは カーネルサポートパッケージ (KSP) のバージョン番号を 20.0.0 から 20.0.1 に変更します。これにより、一部のエージェントバージョンで最新のカーネルドライバのダウンロードに問題が発生する可能性があります。KSP の改訂後もカーネルサポートを維持するために、ユーザは Deep Security Agent 20.0.0-8453 以降にアップグレードすることをお勧めします。詳細については、Deep Security Agent (DSA) Linux のカーネルドライバダウンロードの問題を参照してください。DSA-3588
- 侵入防御またはWebレピュテーションサービスをDeep Security Agentで有効にすると、TLS検査プロセス(tm_netagent)のエラーログローテーションの問題が発生する可能性があります。詳細については、Deep SecurityにおけるTLS検査プロセスのエラーログローテーションの問題を参照してください。DSA-3773

Deep Security Agent - 20.0.0-8453 (20 LTS Update 2024-01-17)

リリース日: 2024年1月17日

ビルド番号: 20.0.0-8453

解決済みの問題

- Deep Security Agent 20.0.0-7943、20.0.0-8137、20.0.0-8268、または20.0.0-8438へのアップグレードが、ファイアウォール、Webレピュテーションサービス、または侵入防御

システムが有効になっている場合に失敗することがありました。

この問題はTrend Cloud One - Endpoint & Workload Securityでは解決されていますが、Deep Security Manager 20.0.854、20.0.864、および20.0.879には引き続き影響します。詳細については、ネットワークモジュールが有効になっている場合のLinux用Deep Security Agentバージョン20.0.0-7943から20.0.0-8438へのインストールまたはアップグレードの失敗を参照してください。DSA-3834

強化

- Deep Security Agentを更新して、20.0.1カーネルサポートパッケージをサポートしました。2024年にLinuxカーネルのサポートを継続するためには、Deep Security Agentを20.0.0-8453+にアップグレードしてください。詳細については、1月2024年更新リリースのDeep Security Agent (DSA)バージョン改訂のプラットフォームサポート更新を参照してください。DSA-1217

既知の問題

- Deep Security Agent は、ローカルの Smart Protection Server に接続できないことがあります。この問題は 20.0.1-690 で修正されています。詳細については、プロキシ使用時の Deep Security Agent (DSA) とSmart Protection Server (SPS) の接続問題 を参照してください。DSA-3564

Deep Security Agent - 20.0.0-8438 (20 LTS Update 2023-12-12)

リリース日: 2023年12月12日

ビルド番号: 20.0.0-8438

新機能

Debian 12のサポート: Deep Security Agent 20.0.0-8438以降では、セキュアブートのサポートを含むDebian 12がサポートされます。これには、Deep Security Manager 20.0.864以降が必要です。DSA-1408

機能強化

- CPUとディスクの使用率が高くならないように、一部のファイルタイプを検索リストから削除します。SF07099651/SEG-188688/DSA-2010

- エージェントの自己保護により、高度なTLSトラフィック検査プロセス(tm_netagent)が保護され、管理者権限を持つローカルユーザがこのプロセスを停止できないようになりました。DSA-1042/DSA-1043
- Telemetryは、すべてのネットワークインタフェースのIPv4アドレスとIPv6アドレスをレポートするようになりました。V1E-4543

解決済みの問題

- ローカルのSmart Protection Serverと設定されたプロキシを使用している場合、Webレピュテーションサービスがプロキシ経由でトラフィックを不適切に送信することがありました。Webレピュテーションサービスは、クエリをローカルのSmart Protection Serverに直接送信するようになりました。DSA-2981
- 大量の不審オブジェクトリストをロードすると、メモリリークが発生することがありました。SF06904914/SEG-182231/DSA-1370

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。DSA-2722

最高共通脆弱性評価システム (CVSS) スコア: 9.8

最高の重大度: 重大

既知の問題

- 侵入防御またはWebレピュテーションサービスをDeep Security Agentで有効にすると、TLS検査プロセス(tm_netagent)のエラーログローテーションの問題が発生する可能性があります。詳細については、Deep SecurityにおけるTLS検査プロセスのエラーログローテーションの問題を参照してください。DSA-3773
- Deep Security Agent 20.0.0-8438 へのアップグレードは、ファイアウォール、Webレピュテーションサービス、または侵入防御システムが有効になっている場合に失敗することがあります。

  この問題は、Trend Cloud One - Endpoint & Workload Security 用の Deep Security

Agent 20.0.0-8453 以降で解決されていますが、Deep Security Manager 20.0.854、20.0.864、および 20.0.879 には引き続き影響します。詳細については、ネットワークモジュールが有効になっている場合の Linux 用 Deep Security Agent バージョン 20.0.0-7943 から 20.0.0-8438 へのインストールまたはアップグレードの失敗 を参照してください。DSA-3834

- Deep Security Agent は、ローカルの Smart Protection Server に接続できないことがあります。この問題は 20.0.1-690 で修正されています。詳細については、プロキシ使用時の Deep Security Agent (DSA) とSmart Protection Server (SPS) の接続問題 を参照してください。DSA-3564

Deep Security Agent - 20.0.0-8268 (20 LTS Update 2023-11-21)

リリース日: 2023年11月21日

ビルド番号: 20.0.0-8268

新機能

- Deep Security Agentでトレンドマイクロ Service Gateway Generic Caching Service (GCS) がサポートされるようになりました。DSA-2035
- Deep Security Agentでは、Debian 10およびDebian 11でFIPSモードがサポートされるようになりました。これには、Deep Security Manager 20.0.854以降が必要です。DSA-1955

解決済みの問題

- システムがスリープモード(動作状態のS0低電力アイドルモード。モダンスタンバイとも呼ばれます) から復帰した後、Deep Security不正プログラム対策が期待どおりに機能しないことがありました。SF07326571/PCT-5476/DSA-2485
- Deep Security Virtual Applianceをバージョン20.0.0-7943または20.0.0-8137にアップグレードした後、Deep Securityで保護されている仮想マシンのステータスがオフラインと表示されました。Deep Security Virtual Appliance自体は正常に機能しており、ステータスが [管理対象 (オンライン)] と表示されていました。SF07317008/SF07313849/SF07331882/PCT-4330/PCT-4607/PCT-4899/DSA-2259

- Deep Security Agentでは、Microsoft Word、Excel、PowerPointで生成された.xmlファイル、およびAutoCADおよびR2000で生成された.dwgファイルのMIMEタイプが誤って分類されていました。SF07027236/SEG-186079/DSA-2202

既知の問題

- スマートスキャンパターンファイルのアップデート中にLinux仮想マシンがフリーズしました。回避策として、/opt/ds_agent/lib/libvmpd_scanctrl.so=icrc_try_update=0 キーをds_am.ini ファイルを選択して、DSAサービスを再起動します。SF07031242/PCT-5795/DSA-2616
- 侵入防御またはWebレピュテーションサービスをDeep Security Agentで有効にすると、TLS検査プロセス(tm_netagent)のエラーログローテーションの問題が発生する可能性があります。詳細については、Deep SecurityにおけるTLS検査プロセスのエラーログローテーションの問題を参照してください。DSA-3773
- Deep Security Agent 20.0.0-8268 へのアップグレードは、ファイアウォール、Webレピュテーションサービス、または侵入防御システムが有効になっている場合に失敗することがあります。

  この問題は、Trend Cloud One - Endpoint & Workload Security 用の Deep Security Agent 20.0.0-8453 以降で解決されていますが、Deep Security Manager 20.0.854、20.0.864、および 20.0.879 には引き続き影響します。詳細については、ネットワークモジュールが有効になっている場合の Linux 用 Deep Security Agent バージョン 20.0.0-7943 から 20.0.0-8438 へのインストールまたはアップグレードの失敗 を参照してください。DSA-3834

Deep Security Agent - 20.0.0-8137 (20 LTS Update 2023-10-26)

リリース日: 2023年10月26日

ビルド番号: 20.0.0-8137

新機能

Miracle Linux 9のサポート: Deep Security Agent 20.0.0-8137以降では、FIPSモードとセキュアブートのサポートを含むMiracle Linux 9がサポートされます。これには、Deep Security Manager 20.0.844以降が必要です。

既知の問題

- Deep Security Agent 20.0.0-8137 へのアップグレードは、ファイアウォール、Webレピュテーションサービス、または侵入防御システムが有効になっている場合に失敗することがあります。

  この問題は、Trend Cloud One - Endpoint & Workload Security 用の Deep Security Agent 20.0.0-8453 以降で解決されていますが、Deep Security Manager 20.0.854、20.0.864、および 20.0.879 には引き続き影響します。詳細については、ネットワークモジュールが有効な場合の Linux 用 Deep Security Agent バージョン 20.0.0-7943 から 20.0.0-8438 へのインストールまたはアップグレードの失敗 を参照してください。DSA-3834
- Deep Security Deep Security Virtual Appliance 20.0.0 ~ 7943で保護されているゲスト仮想マシンのステータスが、[オフライン] または [ステータスの確認に失敗しました (アクティベーションが必要)] と表示されます。
  SF07317008/SF07313849/SF07331882/PCT-4330/PCT-4607/PCT-4899/DSA-2259

Deep Security Agent - 20.0.0-7943 (20 LTS Update 2023-09-26)

リリース日: 2023年9月26日

ビルド番号: 20.0.0-7943

新機能

Red Hat Enterprise Linux 8.6 (PowerPC little-endian) オンデマンド検索のサポート: Deep Security Agent 20.0.0-7943以降では、Red Hat Enterprise Linux 8.6 (PowerPC little-endian) の不正プログラム対策オンデマンド検索機能のみがサポートされます。これには、Deep Security Manager 20.0.817以降が必要です。現在、このプラットフォームではセキュリティアップデートはサポートされていません。

SUSE Linux Enterprise Server 12 (PowerPC little-endian) オンデマンド検索のサポート: Deep Security Agent 20.0.0-7943以降では、SUSE Linux Enterprise Server 12 (PowerPC little-endian) の不正プログラム対策オンデマンド検索機能のみがサポートされます。これには、Deep Security Manager 20.0.817以降が必要です。現在、このプラットフォームではセキュリティアップデートはサポートされていません。

SUSE Linux Enterprise Server 15 (PowerPC little-endian) オンデマンド検索のサポート: Deep Security Agent 20.0.0-7943以降では、SUSE Linux Enterprise Server 15 (PowerPC little-endian) の不正プログラム対策オンデマンド検索機能のみがサポートされます。これには、Deep Security Manager 20.0.817以降が必要です。現在、このプラットフォームではセキュリティアップデートはサポートされていません。

注意:
現時点では、セキュリティアップデートはPowerPCプラットフォームではサポートされていません。RHEL 8.6、SUSE 12、およびSUSE 15では、高度な脅威検索エンジン(ATSE) のステータスが正しく表示されず、次のアラートが予想されます。

- セキュリティアップデート: セキュリティアップデートの確認とダウンロードに失敗しました (Agent/Applianceエラー)
- ステータス: 期限切れ

機能強化

- コマンドラインからプロキシ情報を取得するための新しいコマンドが追加されました。
  `dsa_query -c GetProxyInfo`
  `dsa_query -c GetProxyInfo details=true`
  DSA-864
- カーネルモジュールの署名の検証に使用されるトレンドマイクロのすべての公開鍵が、Deep Security Agentパッケージに初期設定で含まれるようになりました。
  SF06915385/SEG-185980/DSA-1569
- エージェントパターンの更新を正しく表示するには、Deep Security Agent 20.0.0-7943以降にはDeep Security Manager 20.0.759以降が必要です。詳細については、Deep Security Agent 20.0.0-7943の互換性のないエージェント/アプライアンスバージョンエラーを参照してください。SEG-190866/SEG-191017/DSA-1531

解決済みの問題

- ファイルまたはフォルダの除外リストにDeep Security Managerからのパスが含まれていない場合、Deep Security Agentはそのファイルを無視していました。PCT-1066/DSA-1873

既知の問題

- 侵入防御またはWebレピュテーションサービスをDeep Security Agentで有効にすると、TLS検査プロセス(tm_netagent)のエラーログローテーションの問題が発生する可能性があります。詳細については、Deep SecurityにおけるTLS検査プロセスのエラーログローテーションの問題を参照してください。DSA-3773
- ファイアウォール、Webレピュテーションサービス、または侵入防御システムが有効になっていると、Deep Security Agent 20.0.0-7943へのアップグレードに失敗することがあります。

  この問題は、Trend Cloud One - Endpoint&Workload SecurityのDeep Security Agent 20.0.0-8453以降で解決されていますが、Deep Security Manager 20.0.854、20.0.864、および20.0.879では引き続き影響を受けます。DSA-3834
- Deep Security Deep Security Virtual Appliance 20.0.0-7943で保護されているゲスト仮想マシンのステータスが、[オフライン] または [ステータスの確認に失敗しました(アクティベーションが必要)] と表示されます。SF07317008/SF07313849/SF07331882/PCT-4330/PCT-4607/PCT-4899/DSA-2259

Deep Security Agent - 20.0.0-7719 (20 LTS Update 2023-08-29)

リリース日: 2023年8月29日

ビルド番号: 20.0.0-7719

新機能

Miracle Linux 8のサポート: Deep Security Agent 20.0.0-7719以降では、FIPSモードを含むMiracle Linux 8がサポートされるようになりました。これには、Deep Security Manager 20.0.817以降が必要です。

機能強化

- スマートスキャンが無効になっている場合、Deep Security Agentでスマートスキャンエージェントパターンがアップデートされなくなり、ネットワーク帯域幅が節約されます。SEG-186625/DSA-1063

- Deep Security Agentでダウンロードされる増分パターンアップデートの数が減り、ネットワーク帯域幅が節約されるようになりました。(Deep Security Relayとして設定されたAgentでは、すべてのパターンアップデートがダウンロードされます。) DSA-1000
- ユーザがURLにアクセスしようとし、ブロックされたときにリダイレクトされるWebレピュテーションサービスの「ブロックページ」が、チェコ語またはポーランド語で表示できるようになりました。DSA-444
- 高度な脅威検索エンジンがバージョン22.6に更新されました。DSA-453

解決済みの問題

- 一部のシステムで、Deep Security Agentサービス (ds_agent) の停止に通常より時間がかかりました。SEG-187365/DSA-1212
- Deep Security Agentで、セキュリティアップデートがスケジュールされていない場合でも、アップデートが実行されることがありました。SEG-187449/DSA-1064
- 一部のシステムでDeep Security AgentのCPU使用率が高くなりました。SEG-185563/DSA-756
- TLS検査パッケージのアップデートにより、`ds_nuagent` サービスが予期せず停止することがありました。DSA-1319

Deep Security Agent - 20.0.0-7476 (20 LTS Update 2023-07-25)

リリース日: 2023年7月25日

ビルド番号: 20.0.0-7476

機能強化

- dsa-connectサービスがアップデートされ、CPUパフォーマンスが向上しました。C1WS-12970
- Deep Security Agent 20.0.0-7476で、Red Hat Enterprise Linux 9のFIPSモードがサポートされるようになりました。DS-77642
- Deep Security Agent Scanner (SAP) がアップデートされ、SAP NetWeaverによって確立された最大512の並列クライアント接続を受け入れるようになりました。以前の接続制限は256でした。SF06983349/SEG-184190/DS-78229

解決済みの問題

- Smart Protection ServerとWebレピュテーションサービスとの接続が切断されることがありました。SF06423462/SEG-166651/DSSEG-7858

Deep Security Agent - 20.0.0-7303 (20 LTS Update 2023-06-28)

リリース日: 2023年6月28日

ビルド番号: 20.0.0-7303

新機能

Amazon Linux 2023のサポート: Deep Security Agent 20.0.0-7303以降で、FIPSモードを含むAmazon Linux 2023がサポートされるようになりました。これには、Deep Security Manager 20.0.789以降が必要です。

注意: リリース時点では、Amazon Linux 2023はまだFIPSの認定を受けていません。最新のサポート情報については、Amazon Linux 2023リリースノートを参照してください。

Amazon Linux 2023 (AWS Arm-based Graviton 2): Deep Security Agent 20.0.0-7303以降は、AWS Graviton 2上のAmazon Linux 2023をサポートしています。これにはDeep Security Manager 20.0.789以降が必要です。

Advanced TLS Traffic Inspectionは、Oracle Linux 9 (64ビット)、Red Hat Enterprise Linux 9 (64ビット)、およびUbuntu 22.04 (64ビット) をサポートするようになりました。

機能強化

- Deep Security Agentでは、fe80:0:0:0:0:0:0:1/24やfe80::01など、CIDRまたは二重コロン表記を使用したIPv6アドレスがサポートされるようになりました。SF04849178/SEG-122076/DS-67280
- Webレピュテーションサービスで、OSのプロキシ設定で使用されるポートが自動的に監視されるようになりました。DS-77233
- 不要なプロキシ予約タスクがDeep Security Virtual Applianceから削除されました。これにより、`メッセージ送信の待機中にタイムアウトしました` および `タスクの作成中にエラーが発生しました...` というエラーがログに記録されるのを防ぐことができます。SF06844880/SEG-179554/DS-77440

解決済みの問題

- セキュアブートが有効になっていて、署名キーがロードされていない場合、不正プログラム対策がfanotify機能を使用するとシステムがクラッシュしていました。SF06464888/SEG-167771/DS-76161
- 侵入防御(IPS)が正しいペイロード値を読み取らない場合があり、ルールが誤動作する可能性があります。DS-74647
- Deep Security Agentは、Endpoint Sensorが使用されていない場合でも、ハートビートのたびに「dsa-connect has not provided status」をレポートしていました。C1WS-14696
- Deep Security Relay 20.0.0-7119では、改良されたRelayを使用すると、セキュリティアップデートとソフトウェアアップデートが提供されませんでした。SF06935222/SEG-183184/DS-78201
- 特定の条件下で、Deep Security Agentの接続数がオーバーフローすることがありました。DS-76902
- 一部のMQTTメッセージが繰り返し送信され、dsa-connectがシャットダウンループでスタックすることがありました。DS-76709

Deep Security Agent - 20.0.0-7119 (20 LTS Update 2023-05-29)

リリース日: 2023年5月29日

ビルド番号: 20.0.0-7119

機能強化

- 特定のシナリオで、MQTT接続の認証情報がDeep Security Agentのログファイル(`ds_agent.log`)に入力されていました。SEG-174560/C1WS-13282
- 一部のシステムでメモリ不足が発生すると、Deep Security Agentがクラッシュしました。SF06704797/SEG-175243/DSSEG-7875
- エージェントセルフプロテクションは、現在、Advanced TLSインスペクションプロセス(`ds_nuagent`)を保護し、管理者権限を持つローカルユーザがそれを停止するのを防ぎます。DS-74080

  SELinuxを使用しているRed Hat Enterprise Linux 7 (64-bit)システムは、このアップデート後に権限の問題を回避するためにいくつかの手動設定が必要になる場合があり

ます。詳細については、Deep SecurityのRedHat 7 SELinux強制モードでのds_nuagentに対するBPF許可拒否を参照してください。

- Deep Security Agentは、事前定義されたグループ内で実行され、送信トラフィックを受け入れるようになりました。DS-77415

解決済みの問題

- Deep Security Agentでは、感染した圧縮ファイルに複数の感染ファイルが含まれていても、その圧縮ファイルに対する不正プログラム対策イベントが1つしか報告されませんでした。DS-76339
- 接続を置き換えた後、Deep Security Agentは、最大4分間、以前の接続にまだ接続されているかのようにメトリクスをレポートしました。DS-77453
- 不正プログラム対策を有効にすると、一部のシステムでDeep Security AgentのCPU使用率が高くなりました。DS-77758

Deep Security Agent - 20.0.0-6912 (20 LTS Update 2023-05-02)

リリース日:2023年5月2日

ビルド番号:20.0.0-6912

新機能

Red Hat Enterprise Linux Workstation 7のサポート: Deep Security Agent 20.0.0-6912以降では、セキュアブートのサポートを含むRed Hat Enterprise Linux Workstation 7がサポートされるようになりました。これには、Deep Security Manager 20.0.759以降が必要です。

AlmaLinux 9のサポート: Deep Security Agent 20.0.0-6912以降では、セキュアブートのサポートを含むAlmaLinux 9がサポートされるようになりました。これには、Deep Security Manager 20.0.759以降が必要です。

機能強化

- Deep Security Agentがアップデートされ、プロキシプローブの接続タイムアウトを設定できるようになりました。`ds_agent.ini`. SF06664116/SEG-173848/DS-77182

  プロキシプローブラインの例 `ds_agent.ini` 設定ファイル:
  `dsa.proxymanager.ProbeTimeoutInSec=120`

- Deep Security Agentインストーラは、エージェントインストーラで証明書の署名にSHA-1が使用されたことを検出した場合、エージェントをアップデートできないようになりました。これにより、Deep Security Agent 20.0.0-6313以降ではRSA-2048およびSHA-256が必要になるため、エージェントがアップデートされて応答しなくなることがなくなります。証明書のアップグレードの詳細については、「Deep Security暗号化アルゴリズムのアップグレード」を参照してください。DS-76499
- Deep Security Agentがアップデートされ、MQTTの接続品質が向上し、接続タイムアウトの発生が減少しました。DS-76840
- Deep Security Agentに、不正プログラム対策イベントのパスとPID (プロセスID) が含まれるようになりました。SF05682761 / SEG-147452 / DS-72909

解決された問題

- FIPSモードを有効にしてプロキシ経由で接続すると、Deep Security AgentでIoTデバイスとの接続に問題が発生することがありました。SEG-174776 / DS-77197
- Deep Security Agentの不正プログラム対策モジュールが、IPC (プロセス間通信) タイムアウト後に再起動できないことがありました。DS-76889 / SEG-169218
- Deep Security Agentネットワークドライバと一部のサードパーティ製品との互換性の問題により、システムがクラッシュしました。SEG-156743 / DS-75377
- Smart Protection ServerにHTTPS経由で接続すると、Deep Security Virtual Applianceがクラッシュすることがありました。SEG-169451 / DS-76968
- ドライバの再起動後に、Deep Security Agentがネットワークドライバのステータスを正しくレポートしないことがありました。C1WS-12896
- Webレピュテーションサービスを有効にすると、Deep Security Agentによって一部のシステムが予期せずシャットダウンしていました。SF06680505 / SEG-174730 / DSSEG-7866
- ファイル拡張子なしでSAP Scannerの許可リストに追加されたファイルは、許可されるはずのときにブロックされていました。SF06565062 / SEG-170933 / DS-77132
- Relayから新しいプラグインをダウンロードした後にDeep Security Agentがクラッシュすることがありました。DS-76961
- Deep Security Agentが原因で、一部のシステムが予期せず再起動します。SF06584000 / SEG-171147 / DSSEG-7851

Deep Security Agent - 20.0.0-6658 (20 LTS Update 2023-03-22)

リリース日: 2023年3月22日

ビルド番号: 20.0.0-6658

新機能

Oracle Linux 9のサポート: Deep Security Agent 20.0.0-6658以降とDeep Security Manager 20.0.737以降では、FIPSモードとセキュアブートのサポートを含むOracle Linux 9がサポートされるようになりました。

サービスゲートウェイ: Deep Security Agent 20.0.0-6658以降とDeep Security Manager 20.0.741以降では、転送プロキシ機能を提供するサービスゲートウェイ機能がサポートされるようになりました。

機能強化

- アプリケーションコントロールの信頼エンティティのパスルールでファイル名を指定せずにワイルドカードを使用する場合、ワイルドカードは、ルールのパスに一致するディレクトリ内のすべてのファイルに適用されるようになりました。以前は、グロブスター(**)ワイルドカードはパスルールのディレクトリとサブディレクトリに適用され、対照的にシングルスター(*)ワイルドカードはパスルールのディレクトリ内でのみ一致していました。DS-75133
- Webレピュテーションサービスに、OSプラットフォームのメタデータが含まれるようになりました。DS-75453
- SAPScannerによって生成される不正プログラム対策イベントにファイルハッシュが含まれるようになりました。DS-75648/SEG-165491
- アプリケーションコントロールは、.HTML、.HTM、および.JSファイルのWebブラウザでの実行をチェックするようになりました。DS-75102
- Deep Security Agentでは、プロセスの完全なコマンドラインがDeep Security Managerに送信されるようになり、推奨設定の検索のルールの推奨設定が改善されました。以前は、Agentは各プロセスのコマンドラインの最初の2048文字のみを送信していました。C1WS-11728
- Deep Security Agent 20.0.0-6658以降とDeep Security Manager 20.0.737以降では、Ubuntu 22.04のセキュアブートがサポートされるようになりました。DS-73729

- Deep Security Agent 20.0.0-6658以降では、Proxy Manager for Trend Micro Vision One (XDR) 脅威インテリジェンス - User-Defined 不審オブジェクト(UDSO) がサポートされるようになりました。DS-75365

- Deep Security Agentのログシステムがアップデートされ、ユーザの問題をより効率的にデバッグするための追加情報とトレースが提供されるようになりました。Agentはそれぞれ2MBのログファイル (dsa-connect-X.log) を5つ生成します。以前はそれぞれ1MBのログファイルが3つでした。C1WS-9598

  ロガーは、オンデマンドのJSON設定ファイル (dsa-connect.ini または dsa-connect.conf) をサポートし、次の設定オプションを使用できます。

  - Debug: デバッグログメッセージを有効にします (初期設定: false)
  - Count: 生成するログファイルの数 (初期設定: 5)
  - Size: 各ログファイルの最大サイズ (バイト) (初期設定: 2097152)

  設定ファイルの例:

  ```
  { "Debug": true, "Count": 5, "Size": 2097152 }
  ```

- Deep Security Agent は、RedHat または SUSE にデプロイされた場合、最大 1024 のプロセスタスクを持つことができます。PCT-25908/DSA-5507

解決済みの問題

- コンソール(Computer または Policy > 侵入防御 > 一般 > Advanced TLS Traffic Inspection) からAdvanced TLS Traffic Inspection の "Inspect TLS/SSL traffic" オプションが "No" に設定された場合でも、ドライバー側の SSL パケットが処理されることがありました。DS-76160
- Deep Security Agentカーネルサポートパッケージのダウンロードが中断され、「Agent Integrity Check Failed」警告と「Kernel Unsupported」エラーが生成されることがありました。SEG-169497/DS-76545
- Deep Security Agentの侵入防御システムが、「TCP輻輳フラグ」を適切にブロックできないことがありました。DS-76182
- 一部のシステムでは、不正プログラム対策の動作監視にドライバの問題があり、カーネル警告が発生していました。SF06254724/SEG-163042/ORCA-762
- 不正プログラム対策スマートスキャンを有効にすると、IPC接続の問題により一部のシステムがクラッシュしました。SEG-169132/C1WS-10821

- ファイル処理に問題があり、アップデート中にファイルを削除できないため、Deep Security Agentのセキュリティアップデートに失敗しました。DS-75907
- 一部のシステムで、プロセススレッドのタイムアウトにより、不正プログラム対策エンジンが予期せず再起動することがありました。SF06524736/SEG-169218/DS-76656
- SOCKSプロキシを使用した場合、Deep Security AgentはHTTP URLに対するWebレピュテーションサービスの評価を提供できませんでした。DS-73482/DS-73364
- Agentのパッケージに署名がないため、Deep Security Agentのアップグレードが失敗することがありました。SF06045259/SEG-154576/DS-73668
- Deep Security Agentで、一部のシステムで高度な脅威検索エンジン(ATSE) コンポーネントが削除されたことを示すシステムイベントが誤って生成されていました。SEG-147779 / DS-75463
- 一部のシステムでの接続の問題を解決するために、Deep Security Agentがアップデートされ、MQTTタイムアウトが30分から2時間に延長されました。C1WS-11835
- 一部のシステムで、Deep Security Agentが不正プログラム対策スマートスキャンサービスに接続できませんでした。SEG-168468/DS-76433
- システムでDeep Security Agentが原因でパフォーマンスの問題が発生し、コンテナ環境のアプリケーションコントロールイベントが大量に生成されていました。SF06538377/SEG-169605/DS-76594

Deep Security Agent - 20.0.0-6313 (20 LTS Update 2023-01-31)

リリース日 : 2023年1月31日

ビルド番号 : 20.0.0-6313

新機能

エージェントセルフプロテクション: この機能は、ローカルシステム上のユーザがエージェントを改ざんするのを防ぎます。詳細およびエージェントセルフプロテクションの設定方法については、エージェントセルフプロテクションの有効化または無効化を参照してください。

Rocky Linux 9のサポート: Deep Security Agent 20.0.0-6313以降とDeep Security Manager 20.0.716以降では、FIPSモードとセキュアブートのサポートを含むRocky Linux 9がサポートされるようになりました。DS-73727

機能強化

- Deep Securityでは、SHA-1アルゴリズムで署名された証明書はサポートされなくなりました。エージェントがDeep Security Managerと通信するために、SHA-256を使用して発行されたSSL/TLS証明書が必要になりました。C1WS-5676

  警告: Deep Security AgentとDeep Security Manager間の通信エラーを防ぐために、Deep Security暗号アルゴリズムをアップグレードする手順に従ってください。
  暗号アルゴリズムをアップグレードする前にDeep Security Agent 20.0.0-6313以降に更新した場合は、OpenSSL 3がSHA-1アルゴリズムの証明書を拒否する際のDeep Security Agent (DSA)オフラインの手順に従ってください。

- 不正プログラム対策と動作の監視を有効にすると、Deep Security Agent 20.0.0-6313以降とDeep Security Manager 20.0.716以降で不審な動作が監視され、MITRE攻撃シナリオに対する保護が強化されます。DS-73644
- Deep Security Agent 20.0.0-6313以降とDeep Security Manager 20.0.711以降では、Oracle Linux 8のFIPSモードがサポートされるようになりました。DS-73778

解決された問題

- アプリケーションコントロールを有効にすると、Deep Security Agentのステータスが「アプリケーションコントロールルールセットのアップデート中」のままになることがありました。DS-74627
- コンポーネントのアップデートの場合、Deep Security Agentはプロキシを使用する場合と使用しない場合とで試行し、試行ごとにイベントを生成します。イベントレポートをより簡単にするために、この動作が変更され、アップデートが成功した場合、エージェントは最後に成功したイベントのみを表示するようになりました。SF06207160/SEG-160085/DSSEG-7765
- Deep Security Agentがクラッシュし、Deep Security Managerとの接続で問題が発生すると、不正プログラム対策オフラインイベントが発生しました。SF06061098/SEG-154701/DS-74665
- Webレピュテーションを有効にすると、コンソールコマンドに入力された一部の文字が正しく解析されませんでした。たとえば、コマンドに入力されたアンダースコア(_)はダッシュ(-)に置き換えられました、大文字のZが小文字のzに置き換えられました。DS-74335
- アプリケーションコントロールが、ネームスペースモードで実行されているプログラムのブロックに失敗することがありました。SF05929869/SEG-151363/DS-74116

- 特定のコンソールコマンドを実行した後、変更監視でイベントの作成に失敗することがありました(例: passwd または mv コマンド)。05718251/SEG-148552/DS-72643
- 以前のアプリケーションコントロールイベントが意図したとおりにデータベースから削除されませんでした。events.db ファイルサイズが無制限に増加します。SF06172729/SEG-159548/DS-74706
- 変更監視イベントの生成がプロセスまたはシステムのクラッシュによって中断されると、誤ったイベントが作成される可能性があります。SF05508030/SEG-138756/DS-72470

既知の問題

- Deep Security Agent は一部のシステムで接続の問題が発生しており、「イベントID 9012、Smart Protection Server がスマートスキャンのために切断されました」というエラーメッセージが表示されます。詳細および一時的な回避策については、Deep Security に表示される Smart Protection Server 切断メッセージ を参照してください。SF06512673/SEG-168468

Deep Security Agent - 20.0.0-5953 (20 LTS Update 2022-11-22)

リリース日 : 2022年11月22日

ビルド番号 : 20.0.0-5953

新機能

エージェントセルフプロテクション: この機能は、ローカルシステム上のユーザがエージェントを改ざんするのを防ぎます。詳細およびエージェントセルフプロテクションの設定方法については、エージェントセルフプロテクションの有効化または無効化を参照してください。

機能強化

- Deep Security Agent 20.0.0-5953以降とDeep Security Manager 20.0.711以降では、Oracle Linux 8のFIPSモードがサポートされるようになりました。

解決済みの問題

- アプリケーションコントロールで、名前空間モードで実行されているプログラムのブロックに失敗することがありました。SF05929869 / SEG-151363 / DS-74116

- 変更監視で、特定のコンソールコマンドの実行後にイベントの作成に失敗することがありました(例 : passwd または mv コマンド) 。05718251 / SEG-148552 / DS-72643
- 古いアプリケーションコントロールイベントが意図したとおりにデータベースから削除されず、events.db ファイルのサイズが無制限に増加していました。SF06172729 / SEG-159548 / DS-74706
- 変更監視イベントの生成がプロセスまたはシステムクラッシュによって中断された場合、正しくないイベントが作成される可能性がありました。SF05508030 / SEG-138756 / DS-72470

Deep Security Agent - 20.0.0-5761 (20 LTS Update 2022-10-21)

リリース日 : 2022年10月21日

ビルド番号 : 20.0.0-5761

新機能

プラットフォームのサポート強化

- Oracle Linux 7でのSAP Scanner のサポート: Oracle Linux 7用 のDeep Security Agentで、SAP Scannerがサポートされるようになりました。VO-1849

機能強化

- Deep Security Agentがアップデートされ、Webレピュテーションサービス用の追加のメタデータ(UserAgent や Referrerなど) が追加されました。DS-72196
- Deep Security Agentがアップデートされ、エージェント診断パッケージに変更監視データベースが追加されました。DS-73293
- 侵入防御を使用してTLSトラフィックを検査するときにNULL暗号をサポートするようにDeep Security Agentがアップデートされました。DS-71085
- System Vパッケージに依存せずにDeep Security Agentを配信できるようになりました。DS-73588

解決済みの問題

- セキュリティログ監視を有効にすると、Deep Security Agentで「異常な再起動の検出」イベントが生成されることがありました。SF05951130 / SEG-151372 / DS-73737

- アプリケーションコントロールをメンテナンスモードで実行中にDeep Security Agentサービスが停止すると、サービスの停止後に作成された実行可能ファイルが意図したとおりに自動承認されませんでした。SF05961688 / SEG-152045 / DS-73570
- 詳細なTLSトラフィック検査を有効にすると、Deep Security Agentでメモリの問題が発生し、一部のアプリケーションが実行できなくなりました。SEG-150631 / DS-74039
- アプリケーションコントロールでメンテナンスモードが有効になっているときにソフトウェアの名前を変更またはコピーした場合、ソフトウェアインベントリでは元のファイル名または場所で認証されたままになります。DS-74015
- vMotionを使用する仮想マシンが予期せずに無効化され、「オフライン(要アクティベート)」ステータスが表示されることがありました。SEG-153050 / DS-73807
- Edge Relayを使用して、TLSインスペクションサポートパッケージをDeep Security Agentにダウンロードできませんでした。DS-73789
- RedHat Enterprise Linuxコンピュータで、不正プログラム対策を有効にすると、システムがクラッシュすることがありました。SEG-155143 / DS-74008

Deep Security Agent - 20.0.0-5512 (20 LTS Update 2022-09-22)

リリース日:2022年9月22日

ビルド番号:20.0.0-5512

機能強化

- Deep Security Agentカーネルデバイスモジュールファイルが Security-Enhanced Linux (SELinux) 要件に準拠するようにアップデートされました。DSSEG-7378
- Deep Security Agentで、ホスト情報が追加の詳細とともにレポートされるようになりました。DS-72609
- Deep Security Agentは、インストールされたソフトウェアのホストメタデータを詳細情報とともにレポートするようになりました。DS-72608
- Deep Security Agentがアップデートされ、オンデマンド検索と予約検索のマルチスレッドサポートが追加されました。DS-72797 / DS-72798
- Deep Security AgentとDeep Security Manager 20.0.677以降では、OSライブラリの変更に応じた高度なTLSトラフィック検査の自動アップデートがサポートされるようになりました([コンピュータ]または[ポリシー] > [設定] > [TLS検査パッケージのアップデート])。DS-72828

解決済みの問題

- アプリケーションコントロールをオフにして再度オンにしても、信頼エンティティの設定が再適用されていませんでした。SF05930535 / SEG-152439 / DS-73312
- 必要な署名鍵をインポートせずにセキュアブートを使用するシステムにDeep Security Agentをインストールすると、「理由ID:11」のコードが生成されるべきところ、「理由ID:13」の不正プログラム対策エラーコードが生成されました。理由IDの詳細については、「警告:不正プログラム対策エンジンが提供する基本機能」を参照してください。DS-72891
- Deep Security Agentから予期しない形式のホストメタデータが報告されました。DS-73411

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-8100/VRTS-8101/DS-73087/DS-72528

最高共通脆弱性評価システム (CVSS) スコア: 7.0

最高の重大度:高

Deep Security Agent - 20.0.0-5394 (20 LTS Update 2022-08-29)

リリース日:2022年8月29日

ビルド番号:20.0.0-5394

新機能

Ubuntu 22.04 (AWS ArmベースGraviton 2) のサポート: Deep Security Agent 20.0.0-5394以降とDeep Security Manager 20.0.677以降がUbuntu 22.04 (AWS ArmベースGraviton 2) でサポートされるようになりました。

機能強化

- ファイル記述子の数が異常に多い場合、Deep Security Agentプロセスが自動的に再起動するようになりました。このイベントの発生回数を追跡するカウンタが追加されました。SF05212995/SEG-130431/DS-72616
- アプリケーションコントロールで、実行可能でない拡張子を持つ実行可能ファイルのソフトウェア変更が検出されるようになりました。DS-70805
- Deep Security Agentがアップデートされ、TLS接続での動的ポートを使用したパケット検査のサポートが追加されました。DS-71078
- Deep Security Agentがアップデートされ、高度なTLS検査のメトリックがさらに追加されました。DS-72833

解決済みの問題

- 動的ポートを使用したUDP接続でTLS検査を実行すると、OSがクラッシュすることがありました。SEG-151169 / DS-73043
- 一致または正規表現フィールドで変数に「$」文字を使用すると、セキュリティセキュリティログ監視エンジンがオフラインになる問題を修正しました。SEG-146965 / SEG-146966 / DS-72325
- 不正プログラム対策がファイル記述子をリークすることがありました。SF05212995 / SEG-130431 / DS-72979
- 新しいゲスト仮想マシンに対してリアルタイム不正プログラム対策をオフにしたポリシーを割り当てると、同じDeep Security Virtual Applianceに登録されている他のすべてのゲスト仮想マシンに対して、リアルタイム不正プログラム対策がオフになることがありました。SEG-146057 / DS-72856
- アプリケーションコントロールは、メンテナンスモード中もネットワークファイルへのアクセスをブロックしていました。SF04922652 / SEG-131710 / DS-72037
- アプリケーションコントロールが有効な場合、Adobeプラグインで予期しないセキュリティイベントが生成されていました。SF05823607 / SEG-148570 / DS-72679
- エージェントのアップデート中に特定の設定ファイルをロードすると、Deep Security Agentで「リビジョンの不一致(-10039) 」エラーが返されていました。DS-72499
- アプリケーションコントロールインベントリの検索が完了する前に、Deep Security Agentがソフトウェアの変更の検出をレポートしていました。DS-72071

- パッチが適用されたサードパーティ製ライブラリ。パッチ適用前は、Deep Security Virtual Applianceエージェントがクラッシュすることがありました。SF05559993 / SEG-140234 / DS-72510

既知の問題

- 複数のカスタムスクリプトタスクを実行すると、新しいタスクは以前の未完了のタスクによって上書きされます。カスタムスクリプトタスクを1つずつ実行して、この問題を回避できます。この問題は、今後のリリースで修正される予定です。DS-72699

Deep Security Agent - 20.0.0-5137 (20 LTS Update 2022-07-26)

リリース日 : 2022年7月26日

ビルド番号 : 20.0.0-5137

新機能

高度なTLSトラフィック検査: Deep Security Agent 20.0.0-5137以降では、システムアップデートまたはパッケージアップデートを実行するプラットフォームに高度なTLSトラフィック検査のサポートが追加されます。現在、この機能はTrend Cloud One - Workload Securityでのみサポートされています。Deep Security Manager (オンプレミス) のサポートは今後追加される予定です。

Red Hat 9のサポート: Deep Security Agent 20.0.0-5137以降とDeep Security Manager 20.0.651以降では、Red Hat 9がサポートされるようになりました。

Amazon Linux 2のサポート: Deep Security Agent 20.0.0-5137以降とDeep Security Manager 20.0.651以降で、Amazon Linux 2 for AWS Graviton 3がサポートされるようになりました。

機能強化

- Deep Security Agent を更新して、Red Hat OpenShift の不正プログラム対策サポートを追加しました。DS-72368
- Deep Security Agentがアップデートされ、リアルタイムでの不正プログラム対策のCPU使用率が削減され、コンテナのパフォーマンスが向上します。以前は、すべてのファイルが読み取り/書き込み時に検索されていました。書き込み時の不正プログラム対策ファ

イルの検索が遅延されました(ファイルはキューに追加され、バックグラウンドで検索されます) 。DS-65581

- Deep Security Agent Scanner (SAP) で、追加の詳細を含む感染レポートが生成されるようになりました。DS-71660
- 送信接続の「ゼロ設定」SSLプロセスを改善するためにDeep Security Agentがアップデートされました。DS-70715
- Deep Security Agentがアップデートされ、信頼エンティティの機能が向上しました。信頼ルールのワイルドカードサポートに、多くのサブディレクトリに一致するglobstar `\*\*` が含まれるようになりました。Single star `\*` は現在のディレクトリ内でのみ一致します。Single star `\*` を使用して多数のフォルダを照合していた既存のルールは機能しなくなり、globstar `\*\*`を使用するように変更する必要があります。DS-71817

解決済みの問題

- Deep Security Agent Scanner (SAP) は、.SARファイルタイプに対して重複した不正プログラム対策イベントを表示することがありました。DS-71879
- Deep Security Agent SAP Scanner でMIME(.TTF) ファイルを検出できませんでした。DS-55897
- 特定の設定の組み合わせを持つ侵入防御ルールをコンパイルできませんでした。DS-71889
- Deep Security Agentの一部のシステムで接続の問題がありました。DS-72219

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性からどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。
VRTS-7102/VRTS-7070/VRTS-7041/VRTS-7039/DSSEG-7636

最高共通脆弱性評価システム (CVSS) スコア: 4.4

重大度 : 中

既知の問題

- 複数のカスタムスクリプトタスクを実行すると、新しいタスクは以前の未完了のタスクによって上書きされます。カスタムスクリプトタスクを1つずつ実行して、この問題を回避できます。この問題は、今後のリリースで修正される予定です。DS-72699

Deep Security Agent - 20.0.0-4959 (20 LTS Update 2022-07-04)

リリース日 : 2022年7月4日

ビルド番号 : 20.0.0-4959

新機能

Ubuntu 22.04 : Deep Security Agent 20.0.0-4959以降でUbuntu 22.04がサポートされるようになりました。これには、Deep Security Manager 20.0.651以降が必要です。

Ubuntu 20.04のFIPSモード: Deep Security Agent 20.0.0-4959以降で、Ubuntu 20.04のFIPSモードがサポートされるようになりました。

機能強化

- Deep Security Agent 20.0.0-4959以降とDeep Security Manager 20.0.0-414以降では、Fanotifyを使用するシステムでの不正プログラム対策のサポートが改善されました。以前は、「不正プログラム対策エンジンオフライン」イベントによって、これらのシステムの不正プログラム対策機能が中断されていました。これで、「基本的な機能を備えた不正プログラム対策」イベントが記録され、ユーザは基本的なファイル検索機能を維持しますが、機械学習型検索などの高度な検索メカニズムは維持しません。DS-68552

解決済みの問題

- Deep Security Agent Scanner (SAP) の接続に問題があり、一部のシステムで正しいライブラリをロードできませんでした。DS-71623
- Deep Security Agent Scanner ライブラリが原因でSAPアプリケーションがクラッシュすることがありました。DS-71849
- 不正プログラム対策で、一部のシステムの不変ファイルまたは追加専用ファイルを削除できませんでした。VRTS-7110 / DS-52383

- コマンドライン(`dsa_control -b`) を使用すると、Deep Security Relay が、閉じたネットワーク環境でのアップデートに必要なバンドルファイルの抽出に失敗しました。SF05715642 / SEG-144571 / DSSEG-7600
- セキュリティログ監視が有効な場合、Deep Security Agents 20.0.0 ~ 4726にアップグレードすると、「Get Events Failed」および「Command Not Found」アラートが発生します。SF05738607 / SEG-145679 / DS-72117
- 不正プログラム対策と変更監視が有効になっている場合、Deep Securityエージェントが高いCPU使用率を引き起こしました。SF05169148/SEG-129522/DS-69594
- 不正プログラム対策を有効にすると、ISOバックアップを実行していたOSがDeep Security Agentでクラッシュすることがありました。SF05532786 / SEG-139280 / DS-71299
- アプリケーションコントロールのメンテナンスモードがエージェントで有効になっている場合に、ただちにDeep Security Managerにステータスを報告するようにDeep Security Agentがアップデートされました。DS-71617
- Deep Security Agentで、「無効」または「不正な形式」のプロキシURLを参照する不明確なエラーログエントリが作成されることがありました。SEG-144613 / DS-71866

Deep Security Agent - 20.0.0-4726 (20 LTS Update 2022-05-31)

リリース日 : 2022年5月31日

ビルド番号 : 20.0.0-4726

機能強化

- Deep Security Relay がアップデートされ、潜在的なトラブルシューティングに備えてステータスとその他のメトリックが記録されるようになりました。DS-65763

解決済みの問題

- 信頼エンティティの「対象別に許可」ルールで、ブロックする予定のないプロセスがブロックされることがありました。SF04922652/SEG-131710/DS-71060
- 一部の設定で、Deep Security Agentによって「作成/削除」の変更監視イベントの誤検出が報告されました。SF05434164 / SEG-136425 / DS-70656
- Deep Security Agent Scanner ライブラリは、Linuxシステム上の高度に中断されたSAPアプリケーションで正常に動作しませんでした。これによりファイルが検索されました

が、結果をSAPアプリケーションにレポートできない可能性があります。SF05390384 / SEG-136659 / DS-71251

- アップグレード後、Deep Security Agentは継続的に「セキュリティアップデートの実行中」レポートをDeep Security Managerに送信していました。SF05253107 / SEG-131983 / DS-69747
- Deep Security Agent がパッケージの不完全な署名ファイルを取得しないように、Deep Security Relay を更新しました。SF05332854/SEG-134394/DS-71228
- サーバ名インジケータ(SNI) で無効な形式を使用すると、Deep Security Agentで接続の問題が発生していました。SEG-127761 / DS-70806
- Deep Security Agentの異常な再起動により、「不正プログラム対策エンジンがオフライン」エラーが発生することがありました。SEG-140234 / DS-71333
- Applianceの配置時にIPプールのセカンダリDNS設定が行われていませんでした。SF05215036 / SEG-134844 / DSSEG-7535

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。DS-52329

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度 : 高

Deep Security Agent - 20.0.0-4416 (20 LTS Update 2022-04-28)

リリース日 : 2022年4月28日

ビルド番号 : 20.0.0-4416

機能強化

- Deep Security Agentがアップデートされ、「Bypass Network Scanner」ルールが適用された場合の侵入防御のパフォーマンスが向上しました。DS-69515

解決済みの問題

- 侵入防御を有効にすると、パケット転送エラーにより一部のシステムがクラッシュしていました。SEG-136843 / DSSEG-7524

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-7132/DS-70518

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度 : 高

Deep Security Agent - 20.0.0-4185 (20 LTS Update 2022-04-06)

リリース日 : 2022年4月6日

ビルド番号 : 20.0.0-4185

新機能

Advanced TLS トラフィック検査 : Advanced TLS トラフィック検査により、Perfect Forward Secrecy(PFS) などの最新の暗号で暗号化されたTLS トラフィックを検査する機能が追加されます。また、HTTPSサーバの仮想パッチも強化され、Log4jなどの脆弱性に対する保護に役立ちます。

解決済みの問題

- コマンドラインを使用して不正プログラム対策の手動検索を実行すると、Deep Security Agentが受信接続を受信できなくなることがありました。SF05385865 / SEG-135256 / DS-70364
- Deep Security Agentでは、Agentのアップグレード中に「アプリケーションコントロールエンジンオフライン」エラーが生成され、アップグレードの完了後に「アプリケーションコントロールエンジンのオンライン復帰」というメッセージが表示されていました。アップグレードによってこれらのイベントがトリガされるべきではありませんでした。DS-69888

- メンテナンスモードで実行している場合でも、アプリケーションコントロールが認識できないソフトウェアをブロックすることがありました。SF05234969/SEG-133594/DS-69752
- Webレピュテーションサービスを有効にすると、Deep Security AgentでSSL接続の問題が発生していました。DS-67675
- Deep Security Agentは、ポリシーのアップデート中に大量のシステムリソースを消費することがありました。SEG-134417 / DS-69810

Deep Security Agent - 20.0.0-3964 (20 LTS Update 2022-03-01)

リリース日 : 2022年3月1日

ビルド番号 : 20.0.0-3964

新機能

脅威インテリジェンス: 脅威インテリジェンス (旧称Connected Threat Defense) は、新たな脅威に対するマルウェア対策を強化します。詳細については、「脅威インテリジェンスを使用して新たな脅威を検出する」を参照してください。

プラットフォームのサポートの強化

- Deep Security Agent 20.0.0-3964以降は、次のプラットフォームでサポートされるようになりました。
  - Red Hat 8 (AWS ArmベースのGraviton 2) (Deep Security Manager 20.0.605+が必要)
  - Debian 11 (Deep Security Manager 20.0.605以降が必要)

機能強化

- 侵入防御イベントの [元のIP (XFF)] フィールドから文字列内の不審な文字 ($など) を除外するようにDeep Security Agentがアップデートされました。SEG-129905/DS-68989

解決済みの問題

- リアルタイムの変更監視を有効にすると、ファイルを編集して削除した後に変更監視の削除イベントが生成されていませんでした。DS-69057

- Deep Security Agentにより、コンテナを保護するシステムのCPU使用率が高くなっていました。Deep Security Managerでコンテナ保護を有効または無効にできるようになりました([コンピュータ](または[ポリシー]) > [設定] > [コンテナの保護]) 。SEG-115751/DSSEG-7334

Deep Security Agent - 20.0.0-3770 (20 LTS Update 2022-01-24)

リリース日 : 2022年1月24日

ビルド番号 : 20.0.0-3770

新機能

ゼロ設定IPS検査 : Deep Security Agentに、証明書を手動でインポートせずにTLS暗号化トラフィックを検査する侵入防御の機能が追加されました。これにより、より多くの暗号スイートのサポートも追加されます。この機能は、Trend Micro Cloud One - Workload Securityのお客さまを始めとして、Linuxプラットフォーム向けに段階的に展開されています。

CRI-Oのサポート: Deep Security Agentの「CRI-Oエンジンのバージョン」と、コンテナの不正プログラム対策イベント情報がDeep Security Managerに表示されるようになりました。CRI-Oは現在、Deep Security Manager (オンプレミス) でのみサポートされています。Trend Micro - Cloud One Workload Securityのサポートは後で追加される予定です。

機能強化

- Deep Security Agentがアップデートされ、ManagerでTLS 1.2の強力な暗号化を使用している場合に、侵入防御 からDeep Security Managerへの接続が可能になりました。DS-69042
- Deep Security Agentがアップデートされ、[LastIpUsed]フィールドにホストのIPアドレスが正しく表示されるようになりました。以前は、ロードバランサまたはプロキシIPのいずれかを使用する環境では、このフィールドにロードバランサまたはプロキシIPが表示されていました。SF05283977 / SEG-133073

解決済みの問題

- Deep Security Agentがネットワークインタフェースコントローラ(NIC) と競合して、複数のNICを備えたシステムがクラッシュすることがありました。05048124 / SEG-126094 / DS-68730

- 変更監視がタイムアウトすると、「ユーザ」または「グループ」エンティティに対して誤った「作成」または「削除」イベントが生成されることがありました。SEG-117739 / DS-66885
- アプリケーションコントロール、不正プログラム対策、およびリアルタイムの変更監視 が、特定の組み合わせの変更監視 ルールを持つDeep Security Agentで正常に機能しませんでした。DS-68494
- Deep Security Agentで解析の問題が発生し、「不正プログラム対策エンジンがオフライン」エラーが発生していました。SF05171312 / SEG-129367 / DSSEG-7428

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。DS-68180

最高共通脆弱性評価システム (CVSS) スコア: 9.1

最高の重大度 : 高

Deep Security Agent - 20.0.0-3445 (20 LTS Update 2021-11-24)

リリース日 : 2021年11月24日

ビルド番号 : 20.0.0-3445

新機能

オンプレミス環境のAgentメトリックの収集 : SEGのトラブルシューティングのためにオンプレミスでAgentのメトリックを収集できるようになりました。これらのメトリックは、Windowsでは `C:\ProgramData\Trend Micro\Deep Security Agent\metrics` ディレクトリに、Linux、AIX、およびSolarisでは `/var/opt/ds_agent/metrics` ディレクトリにZIPファイルとして保存されます。ZIPファイルは、ローカルファイルシステムで定期的にローテーションされます。各ZIPファイルのサイズは約1MBで、最大100個のファイルが含まれます。メトリクスは診断パッケージとともに収集されます。

機能強化

- Deep Security Managerに接続できない場合、Deep Security Agentがクラッシュすることがありました。DS-67654
- Deep Security Agentでは、セキュリティ強化のために初期設定でCBC暗号スイートが使用されなくなりました。DS-67204
- Deep Security Relayから新しいモジュールを取得できない場合、ローカルにインストールされたカーネルモジュールを使用するようにDeep Security Agentがアップグレードされました。DS-66599
- Deep Security Agentがアップデートされ、Cloud One Workload Securityのアプリケーションコントロール信頼エンティティの「ソースから無視」ルールの「プロセス名」プロパティの使用がサポートされるようになりました。DS-67322
- Deep Security Agentのデータベースサイズ管理がアップデートされ、ディスク容量の使用が最適化されました。DS-67347

解決済みの問題

- Deep Security Relayに対するファイルアクセス権限が不十分なため、エージェントのインストーラが失敗することがありました。DS-67278
- Deep Security Agentで、インストール中に誤った「そのようなファイルまたはディレクトリはありません」というエラーメッセージが表示されることがありました。DS-67317
- アップグレードが成功した場合でも、アップグレード中にDeep Security Agentでプラグインのインストールが失敗することがありました。DS-67336
- アップグレード後にDeep Security Agentを起動できないことがありました。SF04943063 / SEG-123155 / DS-67475
- Deep Security Agentでは、オンデマンドの不正プログラム検索時にファイルのアクセス時間が変更されることがありました。DS-67119
- Deep Security AgentとMQTTの接続がオフラインになり、エージェントの再起動が必要になることがありました。DS-67487
- Deep Security Agentは、先頭と末尾にスペースが含まれるSAP NetWeaver MIMEタイプの検索要求を適切に処理できませんでした。DS-67448
- 不正プログラム対策 リアルタイム検索を有効にすると、変更されていないファイルがDeep Security Agentで検索されることがありました。DS-67806

- Deep Security Agentによってシステムがクラッシュすることがありました。SEG-123338 / DS-67445

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある情報公開の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-6489/DSSEG-7210/DS-65113/DS-67367

最高共通脆弱性評価システム (CVSS) スコア: 9.8

最高の重大度: 高

Deep Security Agent - 20.0.0-3288 (20 LTS Update 2021-10-28)

リリース日: 2021年10月28日

ビルド番号: 20.0.0-3288

新機能

カーネルサポートパッケージのアップデート: コンピュータまたはポリシーエディタの新しい [エージェントの再起動時にカーネルパッケージを自動的にアップデート] オプションを使用して、カーネルサポートパッケージのアップデートをいつ実行するかを選択できるようになりました。

Agentインストーラの進化: Deep Security Agentインストーラは、ほとんどのAgentコンテンツをインストールするようになりました。これにより、次の変更が行われます。

- ほとんどのプラットフォームのインストーラパッケージが若干大きくなるなど、エージェントのサイズ要件が大きくなりました。
- 保護対象のコンピュータにすべてのエージェントコンテンツがインストールされます。ポリシーまたはManagerコンソールによってプラグインが有効化されるまで、コンピュータ上のコンテンツはアンロードされたままになります。
- すべてのプラグインインストールで、エージェントにすでにインストールされているコンテンツが使用されるため、エージェントがRelayに依存することが大幅に減少しました。これにより、Relayに接続せずにプラグインをインストールできるため、Relay通信によるプラグインのインストールの問題が軽減されます。

プラットフォームのサポートの強化

- Deep Security Agent 20.0.0-3288以降では、次のプラットフォームがサポートされるようになりました。
  - AlmaLinux 8 (Deep Security Manager 20.0.503以降が必要)
  - Rocky Linux 8 (Deep Security Manager 20.0.543以降が必要)
  - Ubuntu 20.04 (AWS ArmベースGraviton 2) (Deep Security Manager 20.0.503+が必要)
  - Ubuntu 18.04 (AWS ArmベースGraviton 2) (Deep Security Manager 20.0.482+が必要)
- Secure Bootのサポート: Deep Security Agentで、Oracle Linux 7 (UEK-R5とUEK-R6の両方) と、Secure Bootが有効なOracle Linux 8がサポートされるようになりました。

機能強化

- Deep Security Agent 10.0 から20.0 へのアップグレードでは、「NIC バイパス」構成 (ネットワークインターフェイスのバイパスに使用) が保持されるようになりました。DS-64985
- カーネルモジュールからコンテナファイルイベントを除外できるようになりました。DS-65547

解決された問題

- 不正プログラム対策 の更新が失敗することがあり、「セキュリティアップデート: Agent/Applianceでのパターンファイルのアップデート失敗」エラーが発生することがありました。04763356 / SEG-119138 / DS-66569
- Deep Security Agent Scanner ライブラリをSAP NetWeaverでロードできないことがありました。DS-67530
- 侵入防御が有効になっていると、一部の設定でDeep Security Agentによってシステムがクラッシュする問題がありました。SF04931669 / SEG-123338 / DS-67441
- SAPが統合され実行されている場合、Deep Security AgentはMP4ファイルをブロックしていました。04660120 / SEG-117094 / DSSEG-7254
- Deep Security Agentがプロキシ経由でManagerに接続できないことがありました。DS-65929

- 証明書失効リスト(CRL) が一致しないため、アップグレード中にDeep Security Agent でパッケージ署名エラーが表示されることがありました。DS-65056

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。DS-46018/DSSEG-7210/DSSEG-7217

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度 : 高

Deep Security Agent - 20.0.0-3165 (20 LTS Update 2021-10-08)

リリース日 : 2021年10月8日

ビルド番号 : 20.0.0-3165

注意 : Deep Security Agent 20.0.0.3165がTrend Micro Cloud One - Workload Security ユーザにリリースされました。ただし、Deep Security Agentソフトウェアのダウンロードページからは入手できず、Deep Security Managerを使用しているユーザにはリリースされません。

新機能

- AlmaLinux 8のサポート: Deep Security AgentがAlmaLinux 8でサポートされるようになりました。
- Ubuntu 18.04 (AWS Arm-based Graviton 2) のサポート: Deep Security AgentはUbuntu 18.04 (AWS Arm-based Graviton 2) でサポートされるようになりました。
- Oracle Linux 7のサポート: セキュアブートを使用するOracle Linux 7(uek-R5とuek-R6の両方) でDeep Security Agentがサポートされるようになりました。
- カーネルサポートパッケージの更新 : コンピュータまたはポリシーエディタで、新しい「エージェントの再起動時にカーネルパッケージを自動的にアップデート」オプションを使用して、カーネルサポートパッケージの更新を実行するタイミングを選択できるようになりました。

- Agentインストーラの進化：Deep Security Agentインストーラは、ほとんどのAgentコンテンツをインストールするようになりました。これにより、次の変更が行われます。
  - ほとんどのプラットフォームのインストーラパッケージが若干大きくなるなど、エージェントのサイズ要件が大きくなりました。
  - 保護対象のコンピュータにすべてのエージェントコンテンツがインストールされます。ポリシーまたはManagerコンソールによってプラグインが有効化されるまで、コンピュータ上のコンテンツはアンロードされたままになります。
  - すべてのプラグインインストールで、エージェントにすでにインストールされているコンテンツが使用されるため、エージェントがRelayに依存することが大幅に減少しました。これにより、Relayに接続せずにプラグインをインストールできるため、Relay通信によるプラグインのインストールの問題が軽減されます。

機能強化

- Deep Security Agentを更新して、バージョン10.0から20.0にアップグレードされたエージェントが「NICバイパス」構成(ネットワークインターフェースのバイパスに使用)を失わないようにしました。DS-64985
- カーネルモジュールからコンテナファイルイベントを除外できるようになりました。DS-65547

解決済みの問題

- Deep Security Agentがプロキシ経由でManagerに接続できないことがありました。DS-65929

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。DSSEG-7210/DSSEG-7217

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度：高

Deep Security Agent - 20.0.0-2971 (20 LTSアップデート2021-09-08)

リリース日 : 2021年9月8日

ビルド番号 : 20.0.0-2971

新機能

Red Hat Enterprise Linux 8のFIPSモード: Deep Security Agent 20.0.0-2971以降で、Red Hat Enterprise Linux 8のFIPSモードがサポートされるようになりました。

Amazon Linux 2のFIPSモード: Deep Security Agent 20.0.0-2971以降で、Amazon Linux 2のFIPSモードがサポートされるようになりました。

機能強化

- Deep Security Agentがアップデートされ、ファイル、プロセス、およびネットワークイベントの統合ドライバを使用してパフォーマンスと互換性が向上しました。DS-61784
- Deep Security Agentがアップデートされ、TLSトラフィックの検査が改善されました。この機能は、Trend Micro Cloud One (Workload Security) のユーザから段階的に公開されています。DS-15576
- Deep Security Agentがアップデートされ、Agentの配信時および有効化時のDeep Security Managerとの接続が改善されました。DS-62547

解決済みの問題

- NFS形式のフォルダを使用するシステムで、Deep Security Agentが原因でパフォーマンスの問題が発生することがありました。SF04816680 / SEG-118993 / DS-66280
- 変更監視を有効にすると、Deep Security AgentでCPU使用率が高くなることがありました。DS-65986
- Deep Security Agent 20.0.0-2740 fr Linuxは一部のシステムでパフォーマンスおよびサードパーティ互換性の問題を引き起こしていました。このエージェントはトレンドマイクロDownload Centerから削除されました。詳細についてはDownload Center からのDeep Security Agent (DSA) Build 20.0.0-2740 for Linux の削除を参照してください。
- Deep Security Agentコンソールのコマンドで、Deep Security RelayまたはDeep Security Managerのプロキシ情報が返されないことがありました。DS-65419

- Deep Security Agentで、[イベントとレポート]の項目が正しく表示されないことがありました。DSSEG-7057
- SystemD (Linux Service Manager) プロセスの制限により、Deep Security AgentがRPMベースのプラットフォームでタスクを作成または管理できないことがありました。SF04543580 / SEG-113833 / DS-65550
- Deep Securityエージェント不正プログラム対策リアルタイム検索の除外が、コンテナ環境内で失敗することがありました。DS-65528
- Deep Security Agent 不正プログラム対策リアルタイム検索ディレクトリの除外で、ファイル名がUTF-8形式でない場合に失敗することがありました。SEG-115198 / DS-65495
- 不正プログラム対策を有効にすると、Deep Security Agentで「ディスク容量不足」アラートが発生し、Agentがクラッシュしたり、他のプログラムが正常に動作しなくなることがありました。SF04584157 / SEG-113377 / DS-64405
- Deep Security Agentで、Agentから開始される(dsa_control) コンソールコマンドの一部を実行できませんでした。04564385 / SEG-112050 / DSSEG-6990
- Deep Security Managerとの接続の確立中に、Deep Security Agentがクラッシュすることがありました。04634804 / SEG-113539 / DS-64862
- SSL接続の確立中に、Deep Security Agentの接続が切断されることがありました。SF04323898 / SEG-107451 / DS-64268
- 古いバージョンのOSを使用しているシステムでは、Deep Security AgentがWebアプリケーションに接続できないことがありました。SF04451029 / SEG-109652 / DS-64528
- コンソールコマンドを使用して以前の(RPMパッケージ) アップグレードが実行された場合、Deep Security Agentのアップグレード(管理>アップデート>ソフトウェア) が失敗することがありました。SF04586071 / SEG-113583 / DS-64978
- Webレピュテーションを有効にすると、Deep Security Agentによって一部のサードパーティソフトウェアで接続の問題が発生しました。SF04072723/SEG-97952/DSSEG-6963
- 変更監視を有効にすると、一部のシステムでDeep Security Managerの認証サーバのCPU使用率が高くなりました。04488319 / SEG-110088 / DS-63855
- 変更監視のリアルタイム検索を有効にすると、Deep Security Agentでネットワークドライブ上のファイルが削除されないことがありました。SEG-108636 / C1WS-1787

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。SF04613197/SEG-113566/DS-64050

最高共通脆弱性評価システム (CVSS) スコア: 9.8

最高の重大度 : 高

Deep Security Agent-20.0.0-2593(20 LTS Update 2021-07-01)

リリース日 : 2021年7月1日

ビルド番号 : 20.0.0-2593

新機能

Ubuntu 18.04のFIPSモード: Deep Security Agent 20.0.0-2593以降で、Ubuntu 18.04のFIPSモードがサポートされるようになりました。

解決済みの問題

- 変更監視のアラートがトリガされても、[イベントとレポート] タブに表示されないことがありました。04266346/SEG-103731/DS-62992
- Deep Security Agentは、エージェントとマネージャーの通信の問題が原因で、複数の「セキュリティログ監視 エンジン初期化」アラートをトリガーすることがありました。SF03968169 / SEG-95731 / DS-60840
- アプリケーションコントロールは、PowerShellによって生成された「.tmp」ファイルが原因で複数の「アプリケーションコントロール ソフトウェア変更が検出されました」イベントを検出していました。C1WS-1608

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセ

キュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-5850/DS-54705

最高共通脆弱性評価システム (CVSS) スコア: 4.4

最高の重大度 : 中

Deep Security Agent - 20.0.0-2395(20 LTSアップデート2021-05-24)

リリース日 : 2021年5月24日

ビルド番号 : 20.0.0-2395

新機能

プラットフォームのサポートの強化

- アプリケーションコントロールと変更監視 for Amazon Linux 2 (AWS Arm-based Graviton 2): Deep Security Agentは、AWS Graviton 2上のAmazon Linux 2に対してアプリケーションコントロールと変更監視をサポートするようになりました。DS-62775

機能強化

- Deep Security Agent 20.0.0-2395以降では、Entrustのルート認証局 (G2) 証明書がサポートされるようになりました。G2以外のセキュリティ証明書の有効期限は2022/07/09です。それ以降は、Deep Security Agent 20.0.0-2395以降にのみ最新の不正プログラム対策スマートスキャン保護が適用されます。DS-63010
- Deep Security Agentが機械学習型検索 サポートDS-62857
- Deep Security Agentの不正プログラム対策 初期設定がアップデートされ、ローカルホストからのファイルアクセスのみが監視され、一部のファイルシステムに対する互換性が向上しました。DS-62222

解決済みの問題

- 不正プログラム対策 リアルタイム検索で「読み取り中」の設定が適切に検出されないことがある(コンピュータ>詳細>不正プログラム対策>一般>リアルタイム検索>不正プログラム検索の構成>編集>アドバンスド>リアルタイム検索) 。SEG-104496 / DS-61836

- 一部の環境でOSを誤って識別したため、Deep Security Agentをインストールできませんでした。DSSEG-2915 / DS-28321
- アップグレード失効リスト(CRL) が一致していないため、Deep Security Agentでパッケージシグネチャエラーが発生することがありました。DS-62154
- 不正プログラム対策リアルタイム検索 によりCPU使用率が高くなることがありました。04331007 / SEG-107814 / DS-62593
- AWSワークスペース上のDeep Security Agentの [コンピュータ] [ ]タブで、接続の問題によってホスト情報がオフラインまたは重複して表示されることがありました。SF04198134 / SEG-102818 / DS-61666
- 不正プログラム対策リアルタイム検索 により、一部の設定で意図しないファイルの変更が発生しました。DS-62412
- Deep Security Agent は、パッケージが見つからないためにアップグレードに失敗することがあります。SF04302125/SEG-104084/DS-62692
- 不正プログラム対策カーネルモジュールは、ネットワークディレクトリスキャンが無効になっている場合、リモート共有ストレージ上のファイルアクティビティをバイパスしないことがありました。DS-62985

Deep Security Agent - 20.0.0-2204 (20 LTS Update 2021-04-12)

リリース日 : 2021年4月12日

ビルド番号: 20.0.0-2204

新機能

強化されたプラットフォームのサポート

- Amazon Linux 2 (AWS ArmベースのGraviton 2) 向けの不正プログラム対策とセキュリティログ監視のサポート: Deep Security Agent 20.0.0-2204以降では、不正プログラム対策、ファイアウォール、侵入防御、セキュリティログ監視、およびWebレピュテーション保護モジュールがサポートされています。高度な脅威検索エンジン(ATSE) の更新は現在、AWS Graviton 2上のAmazon Linux 2ではサポートされていませんが、将来のリリースで追加される予定です。

解決済みの問題

- 不正プログラム対策を有効にすると、Deep Security Agentによって「プロセスの停止」が発生することがあります。SEG-104452/DS-61593
- アプリケーションコントロールがブロックモードの場合、場合によっては適切なソフトウェアインベントリを作成できませんでした。DS-58813
- Webレピュテーションが有効になっていると、システムがクラッシュすることがありました。SF04258834 / SEG-102756 / DS-61067
- 変更監視リアルタイム検索が有効になっていると、NFSボリューム上のディレクトリを削除できないことがあります。SF03977538 / SEG-98656 / DS-61062
- 侵入防御が有効になっていると、一部の設定でシステムがクラッシュすることがあります。SF04286712 / SEG-103971 / DS-61274
- プロキシサーバの問題により、Trend Micro Vision One (XDR) に登録した後にDeep Security Agentとの接続に問題が発生することがありました。SF04318864 / SEG-104847 / DS-61516

Deep Security Agent - 20.0.0-2009(20 LTSアップデート2021-03-08)

リリース日 : 2021年3月8日

ビルド番号 : 20.0.0-2009

機能強化

- CPU情報(論理コア数) を含めるようにDeep Security Agentがアップデートされ、診断とパフォーマンスの追跡が改善されました。DS-60011

解決済みの問題

- 古いMQTT接続が適切にクリーンナップされなかったため、MQTT接続はオフラインになりました。SF04236908/SEG-102056/DS-60893
- ファイアウォール、侵入防御、およびWebレピュテーションが有効になっていると、システムがクラッシュすることがありました。SF03992370/SEG-100828/DS-60589
- Deep Security Virtual Applianceの再起動後、保護されているVMにアクセスできなくなることがありました。SEG-94723/SF03949466/DS-58962

Deep Security Agent - 20.0.0-1876 (20 LTS Update 2021-02-08)

リリース日: 2021年2月8日

ビルド番号: 20.0.0-1876

解決済みの問題

- Deep Security AgentがWebサーバへのSSL接続を確立できないことがありました。 DS-59893

Deep Security Agent - 20.0.0-1822(20 LTSアップデート2021-01-18)

リリース日 : 2021年1月20日

ビルド番号 : 20.0.0-1822

新機能

プラットフォームのサポートの強化

- Amazon Linux 2 (AWS ArmベースのGraviton 2): Deep Security Agentは、AWS Graviton 2上のAmazon Linux 2をサポートしました。エージェントは現在、ファイアウォール、侵入防御、およびWebレピュテーション保護モジュールをサポートしています。他の保護モジュールも近日中に対応予定です。

Behavior Monitoring for Linux: このリリースでは、Linuxプラットフォームでの挙動監視のサポートが追加されています。

Deep Security Agent - 20.0.0-1681(20 LTSアップデート2021-01-04)

リリース日 : 2021年1月4日

ビルド番号 : 20.0.0-1681

解決済みの問題

- ドライバの競合により、Deep Security Agentがハングアップして再起動が必要になりました。SEG-94278 / SF03941184 / DS-59020
- セキュアブートに関連するエラーが発生した場合、ユーザはプラグインのインストールをブロックされなくなり、Deep Security Managerに「セキュアブート」エラーメッセージが表示されます。代わりに、「エンジンがオフラインです」というエラーメッセージが表示されます。ユーザは、ds_agent.logの「Secure Boot」エントリでエラーの詳細を確認できます。DS-58374
- SecureBoot環境で、カーネルバージョン5.3.18-24.37(初期設定)以降のSUSE15 SP2カーネルモジュールのロードに失敗しました。SEG-93737 / DS-58373
- 不正プログラム対策 が新しいドライバを完全にロードする前に再起動することがあり、AMエンジンがオフラインになることがあります。DS-58475

Deep Security Agent 20.0.0-1559(20 LTSアップデート2020/12/07)

リリース日 : 2020年12月7日

ビルド番号 : 20.0.0-1559

新機能

TLSの方向性: Managerのハートビートポートは、TLSクライアントとTLSサーバの両方として機能できるようになりました。今後のエージェントは、TLSサーバではなくTLSクライアントとして接続します。これにより、接続のTCPレイヤと同じ方向でTLSセッションを開始する必要があるプロキシまたはファイアウォールを介したAgentからの接続の問題が解決されます。

機能強化

- Deep Securityの改善 Relayのパフォーマンスを継承します。DS-55527
- メモリ使用率が向上し、パフォーマンスが向上します。DS-53012
- 不正プログラム対策 のオンデマンド検索が期待どおりに機能していません。DS-58346

解決済みの問題

- Deep Security AgentがSecure Boot状態を正しく検出しませんでした。SEG-89042/03730368 / DS-57014

- dsa_filterによってカーネルパニックが発生したため、「atomic during scheduling」エラーが発生しました。DS-56514
- 不正プログラム対策 イベントには、特定のシナリオでファイルハッシュが含まれていませんでした。SEG-91779 / SF03818756 / DS-57453
- 不正プログラム対策 ドライバは、初期化中に警告メッセージを表示しました。SEG-92204/03784490 / DS-57605
- Deep Security Agent 20.0.0-1194にアップグレードすると、「侵入防御 ルールのコンパイル失敗」および「セキュリティアップデート失敗」のエラーが時々正しく行われませんでした。SEG-90503/03789013 / DS-56904
- 不正プログラム対策 リアルタイム検索が有効になっていた場合、Rancher Kubernetesポッドを正常に終了できないことがありました。SEG-87824 / SF03695639 / DS-58220
- 整合性監視 が有効化されたときに、大量のCPUが使用されました。SEG-88619/03720485 / DS-56613
- アプリケーションコントロールイベントが同じインシデントに対して複数回発生しました。SEG-86213 / SF03620055 / DS-57298
- セキュリティアップデートは新しいコンピュータでは自動的に実行されませんでした。SEG-91484 / SF03828068 / DS-57688

お知らせ

このエージェントのアップデートでは、エージェントマネージャ通信に使用されるTLS証明書の検証がどのように実装されるかが変更されています。エージェントのアクティベーション中に次の警告が表示された場合：

```
[Warning/2] | SSLVerifyCallback() - verify error 20: unable to get local issuer certificate
```

最も根本的な根本原因は、エージェントがマネージャによって証明書に提示されている証明書を検証できないことです。信頼された証明書を固定する必要はありません。この証明書が適用されない場合は無視してください。ただし、信頼された証明書を使用する場合は、Deep Security Agentをアクティベートする前に、"パブリックCAによって発行されたDeep Security Manager証明書チェーンをインポートする" on page 1620 によって発行する手順に従ってください。

Deep Security Agent 20.0.0-1337(20 LTSアップデート2020/10/28)

リリース日：2020年10月28日

ビルド番号：20.0.0-1337

解決済みの問題

- Linuxで不正プログラム対策 リアルタイム検索が有効になっていた場合、サードパーティのセキュリティソフトウェアとの互換性の問題により、システムがクラッシュすることがありました。SF03700563 / SEG-88135 / DS-54799
- セキュアブートはアクティブでないときにアクティブになっています。SEG-85550 / DS-55052

Deep Security Agent 20.0.0-1304(20 LTSアップデート2020/10/21)

リリース日 : 2020年10月21日

ビルド番号 : 20.0.0-1304

機能強化

- 変更監視 検索完了時刻が秒単位で1000単位で表示されるようにアップデートしました。DS-54680

解決済みの問題

- エージェントレスの保護対象VMの場合、[Policies]→[侵入防御]→[一般] → [Recommendation]の設定はグレー表示になります。DS-56665
- 「アプリケーションコントロールルールセットをRelayから提供する」が有効になっていると、不要なRelayエラーイベントが発生しました。DS-50905
- ファイルシステムフックを有効にしたリアルタイム不正プログラム対策は、古いカーネルバージョンでは機能しませんでした。SEG-82411 / DS-54271
- Deep Security Agentは、セキュリティ更新プログラムの例外を受信したためのDeep Security Managerは、セキュリティ更新プログラムのタイムアウトを報告しました。SEG-82072 / DS-54720
- Deep Security Managerで セキュリティログ監視 ステータスが正しく表示されないことがありました。SEG-77081 / DS-54719
- dsa_queryコマンドで、不正プログラム対策 パターンが正しく表示されませんでした。DS-55389
- 不正プログラム対策 ドライバは、カーネルにロードする前に互換性を確認しませんでした。SEG-88135

Deep Security Agent 20.0.0-1194(20 LTSアップデート2020-10-05)

リリース日 : 2020年10月5日

ビルド番号 : 20.0.0-1194

新機能

Linuxでのリアルタイム不正プログラム対策 検索のパフォーマンスが改善されました: Deep Security Agent for Linuxの不正プログラム対策 リアルタイム検索が改善され、応答時間が短縮され、処理が高速化され、CPU使用率が低下します。以前は、すべてのファイルがread/write.で検索されていました現在、不正プログラム対策 検索の方が効率的で、書き込み中のファイル検索が遅延されます(ファイルはキューに追加され、バックグラウンドで検索されます) 。

差別化されたプラットフォーム : Deep Security Managerでは、Red HatおよびCentOSのプラットフォームと運用を区別できるようになりました。DS-52682

継続的なネットワーク検索: vMotionを使用してゲスト仮想マシンを同じクラスタ内の別のESXiホストに移行した後、Deep Security Virtual Applianceのネットワーク検索が中断した場所から遅延なく続行されるようになりました。この機能は、NSX-T Data Centerを使用しており、ゲストマシンがネットワーク機能のオーバーライドなしのポリシーを使用している場合にのみ適用されます。DS-50482

機能強化

- リアルタイムの変更監視 は、ベースディレクトリで指定されたディレクトリと明示的に一致します。以前は、ベースディレクトリで開始されたすべてのパスに一致していました。DS-52692
- 変更監視 は、LinuxおよびUnixプラットフォームの「setuid」属性と「setgid」属性に対する変更を検出します。DS-52061
- カーネルパニックを防ぐため、Cephはファイルシステムのカーネルフックから除外されました。SEG-75664 / SF03131718 / DS-50298
- 推奨設定の検索と変更監視 が有効になりました。DS-50478
- [管理]→[システム設定]→[Agent] にある[同じ名前のコンピュータがすでに存在する場合] 設定の範囲が、アクティブ化されていない既存のコンピュータに適用されるように拡張されました。以前は、ライセンス認証された既存のコンピュータにのみ適用されていました。DS-51800

解決済みの問題

- セキュアブートはアクティブでないときにアクティブになっています。DS-55052
- Deep Security Agentは、UEFI Secure Bootが有効なプラグインをインストールできませんでした。DS-54041
- Deep Security Agentのバージョンアップ後、「アプリケーションコントロール ルールセットの送信に失敗しました」というエラーが発生することがありました。DS-49828
- Deep Security Virtual Applianceの不正プログラム対策 エンジンは、Censusサーバの応答の署名者フィールドが空の場合にオフラインになりました。DS-49807
- 不正プログラム対策 ディレクトリ除外(ワイルドカード使用)が、サブディレクトリと正しく一致していません。DS-50245
- Linux上のDeep Security Agentがクラッシュすることがある問題SEG-76460 / SF03218198 / DS-50852
- Deep Security Agentからネットワークインタフェース情報が正しくないことが報告されました。SEG-77161 / DS-51397
- Deep Security Virtual ApplianceでEICARテストファイルが検出されませんでした。SEG-71955 / SF02955546 / DS-49387
- アプリケーションコントロール には、拡張子「.bash」のスクリプトはインベントリに含まれていません。その結果、これらのスクリプトはロックダウンモードでブロックされます。DS-50696
- 不正プログラム対策 ドライバにより、autofsが使用されたLinuxプラットフォームでシステムハングアップが発生しました。DS-51926
- 変更監視 が有効になっていると、ファイルの所有者が存在しないユーザに誤って変更されました。DS-52058
- Deep Security Agentのアップグレードに問題があり、変更監視 または セキュリティログ監視 が有効になっていると、エージェントがオンラインにならないことがあります。DS-50672
- カーネルパニックがWebレピュテーション, ファイアウォール、または 侵入防御 が有効になったときに発生しました。SEG-80201 / DSSEG-5846 / DS-52975
- 不正プログラム対策 のリアルタイム検索がLinuxで有効になっていた場合、procfsのバッファが検証されなかったため、システムがクラッシュすることがありました。SEG-80183 / DS-53204

- 新しいパケットを含む再送信パケットが送信されると、「サポートされていないSSLバージョン」の侵入防御 イベントが生成されることがありました。SEG-73893 / DSSEG-5866 / DS-53144
- Deep Securityリアルタイム不正プログラム対策 がLinuxシステムで有効にされた場合、CPU使用率が高くなります。SEG-75739 / DS-52976

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-3704/DS-41233

最高共通脆弱性評価システム (CVSS) スコア: 4.4

最高の重大度 : 中

Deep Security Agent 20(長期サポートリリース)

リリース日 : 2020年7月30日

ビルド番号 : 20.0.0.877

新機能

プラットフォームのサポートの強化

- Ubuntu 20.04 (64ビット)
- Cloud Linux 8(64ビット)
- Debian Linux 10(64ビット)
- Oracle Linux 8 (64ビット)
- SUSE Linux Enterprise Server 15 (64ビット)
- Red Hat Enterprise Linux 8 (64ビット)
- CentOS 8 (64ビット)

SystemDのサポート: SystemDはLinuxサービスマネージャで、サービスで依存関係を宣言できます。これにより、カーネルモジュールやその他のサービスのシーケンスのロードとアンロードを実行できます。どのプラットフォームがサポートされているかについては、"Linux systemdのサポート" on page 404 サポートされているプラットフォームについては、を参照してください。DS-37395

Secure Bootサポート: Deep Security Agentは、Secure Bootを有効にしたLinux OSを追加サポートします。詳細については、"Linux Secure Bootのサポート" on page 409を参照してください。

セキュリティの向上

エージェントの整合性チェック: Deep Securityは、Deep Security Agentでの署名を検証して、ソフトウェアファイルが署名時から変更されていないことを確認します。

NSX-T環境での仮想マシンの保護: 最新のVMware Service InsertionテクノロジとGuest Introspectionテクノロジが統合されました。これにより、侵入防御、Webレピュテーション、ファイアウォール、変更監視、およびエージェントレス保護を使用したNSX-Tホストでの推奨設定の検索を使用してゲスト仮想マシンを保護できます。

シームレスなネットワーク保護 : Deep Security Managerは、ゲストVMのネットワーク設定を、同じクラスタ内のすべてのDeep Security Virtual Applianceに送信します。その結果、アプライアンスは、1つのESXiホストから同じクラスタ内の別のESXiホストへのvMotionの移行中および実行後に、ネットワーク機能を使用するゲストコンピュータの保護を維持できるようになります。この機能は、NSX-T環境にのみ適用されます。この環境では、ゲストコンピュータがネットワーク機能のオーバーライドなしで割り当てられたポリシーを使用しています。

SELinuxのサポート: Red Hat Enterprise Linux 7およびRed Hat Enterprise Linux 8では、SELinux(Security-Enhanced Linux) 強制モードがサポートされています。Deep Security Agentは、初期設定のSELinuxポリシーと互換性があります。

> 注意 : ds_agentなどの不正プログラム対策ソフトウェアは、システムを保護するために一意のドメインで実行する必要があります。SELinuxポリシーのその他のカスタマイズまたは設定は、ds_agentのためにブロックがブロックまたは失敗することがあります。

SSLの強化 : Deep SecurityはSSL証明書でハンドシェイクhello_request(rfc5246) および拡張子_then_mac(rfc7366) を暗号化します。

Continuous 不正プログラム対策 保護 : Deep Security Managerは、ゲストVMの不正プログラム対策 リアルタイム設定を、同じクラスタ内のすべてのDeep Security Virtual Appliance

に送信します。これにより、vMotionを1つのESXiホストから別のESXiホストに移行中および移行後に、不正プログラム対策のリアルタイム機能を使用するゲストコンピュータの保護をアプライアンスで維持できるようになります。同じクラスタ。この機能は、NSX-T環境にのみ適用されます。

管理と品質の向上

環境内のAgentのバージョンアップを自動化する: Deep Securityにより、新しいAgentを有効化した場合に新しいバージョンにバージョンアップできるかどうかを柔軟に判断できます。これは、アプリケーションチームが期限切れのバージョンのAgentを含む古いゴールドイメージを使用している場合に特に役立ちます。アクティベーション時のアップグレードを有効にし、Agentバージョン管理を使用して環境内で使用するAgentのラインナップを定義するだけで、古いAgentがオンラインになってアクティベートされると、自動的にアップグレードされます。

NSX-Tネットワークスループットの向上: Data Plane Development Kit (DPDK) の導入により、ネットワークスループットが従来のテクノロジと比較して3倍高速化されました。

サポートされているパスへのアップグレード: アクティベーション時のアップグレード機能では、コンピュータ上のAgentが最新の2つのメジャーリリース以降にのみアップグレードされます。Agentが条件を満たしていない場合は、過去2回のメジャーリリース内のリリースにAgentを手動でアップグレードする必要があります。次に、アクティベーション時のアップグレード機能によって新しいバージョンが検出され、指定されたリリースへのアップグレードが完了します。

認証情報が正しくないAWSアカウントの保護: 以前は、Deep SecurityでAWSアカウントの認証情報を正しく入力しないと、エージェントを有効化できませんでした。これは、資格情報が正しく入力されていないか、Deep Securityで対応するアップデートを行わずに資格情報が変更されたために発生した可能性があります。多くの場合、単純な設定エラーであるこの状況で保護を維持するために、コンピュータはアカウントの外部で作成され、エージェントのアクティベーションが許可されます。

インスタンスメタデータサービスバージョン2(IMDSv2) のサポート: このリリースでは、IMDSv2がサポートされています。詳細については、「 "Deep Security AgentはAmazonインスタンスメタデータサービスをどのように使用しますか" on page 1979

検索失敗の処理可能な推奨事項: Deep Security Agentには、予約された不正プログラム検索がキャンセルされた理由と、その対策を推奨する処理に関する情報が表示されます。詳細については、"不正プログラム対策 検索の失敗とキャンセル" on page 1158を参照してください。

プロセスの除外設定:プロセス除外設定が次のように改善されました。

- プロセスの除外項目が正しく機能しない理由に関する情報が提供されるため、問題のトラブルシューティングや、解決するための処理を確認できます。
- プロセスの例外設定ワークフローが改善され、より堅牢になりました。

機能強化

- 変更監視では、LinuxおよびUnixプラットフォームの「setuid」属性と「setgid」属性に対する変更が検出されます。
- AWSコネクタでワークスペース同期機能が有効になっていない場合のAmazon WorkSpacesの配信のハートビート処理が改善されました。
- 管理>システム設定>エージェントの同じ名前のコンピュータがすでに存在する場合の範囲が拡張され、既存のコンピュータに適用されます。非アクティブ化されたコンピュータ。これまでは、既存のアクティベートされたコンピュータにのみ適用されていました。
- Deep Security Agentのアクティベーションの経験が次のように改善されました。
  - 強化されたエージェントは のDeep Security Managerで(例えば、成功メッセージまたはそれ以降のDeep Security Managerのバージョンを説明するメッセージが必要) アクティベーションステータスを表示することによって、活性化の経験を-initiated。
- vMotionを使用してゲスト仮想マシンを同じクラスタ内の別のESXiホストに移行した後、Deep Security Virtual Applianceの不正プログラム対策リアルタイム検索が、中断したところから遅延なく続行されるようになりました。この機能は、NSX-T環境にのみ適用されます。
- 検索エンジンのURIパスの長さの制限が増加しました。
- Deep Security Agent 不正プログラム対策が、IntelliScanが無効になっているときにデータタイプに関係なく圧縮ファイルを検索できるようになりました。
- Docker pullコマンドを実行すると、Linuxリアルタイムの不正プログラム対策のパフォーマンスが向上しました。
- NSX-T環境でDeep Security Virtual Applianceで保護されたゲストVMの自動アクティブ化に要する時間が短縮されました。

  注意: この機能を使用するには、Deep Security Manager FR 2019-12-12以降が必要です。

- イベント管理の合理化により、エージェントのパフォーマンスが向上します。

- CLIコマンドを使用して、各エージェントのための一般的なスキャンキャッシュを有効または無効にする機能を追加しました。
- 不正プログラム検索失敗イベントの説明を拡張して、考えられる理由を示しました。
- Linuxでの不正プログラム対策カーネルレベルの除外が強化されました。ネットワークディレクトリ検索が無効になっていると、リモートファイルシステムからのファイルイベントはDeep Security Agentによって処理されなくなります。
- プロセス名、コンテナID、コンテナ名、イメージ名、イメージの通知、ポッドIDなどの侵入防御イベントに対するプロセスおよびコンテナの情報を取得する機能が追加されました。

解決済みの問題

- Linuxで不正プログラム対策のリアルタイム検索が有効になっていた場合、procfsのバッファが検証されなかったため、システムがクラッシュすることがありました。SEG-80183 / DS-53204
- LinuxでDeep Securityリアルタイム不正プログラム対策が有効になっていたため、CPU使用率が高くなりました。SEG-75739 / SF03036857 / DS-52976
- Cephはカーネルパニックを引き起こしました。SEG-75664 / SF03131718 / DS-50298
- Deep Security Agentがクラッシュすることがあります。SEG-76460 / SF03218198 / DS-50852
- Deep Security Agentからネットワークインタフェース情報が正しくないことが報告されました。SEG-77161 / DS-51397
- Deep Security Virtual ApplianceはEicarファイルを検出しませんでした。SEG-71955 / SF02955546 / DS-49387
- アプリケーションコントロールでは、拡張子「.bash」のスクリプトはインベントリに含まれていませんでした。その結果、これらのスクリプトはロックダウンモードでブロックされていました。SEG-73174 / DS-50696
- Deep Security Virtual Applianceがオフラインになることがありました。SEG-53294/DS-46728
- ファイアウォールをオフにしても、インタフェース分離機能がオンのままでした。SEG-32926/DS-27099
- Red Hat Enterprise Linux 5または6、またはCentOS 5または6環境で、ユーザまたはグループが作成または削除されていない場合でも、次のルールに関連する変更変更監

視イベントが表示されました: 1008720 - ユーザとグループ - アクティビティの作成と削除。SEG-22509/DS-25250

- 変更監視イベントで、Unicodeエンコーディングの不正なファイルパスが表示されました。SEG-45239/DS-33911
- 不正プログラム対策イベントで、Unicodeエンコーディングが無効な空白のファイルパスが表示されました。SEG-46912/DS-34011
- Deep Security Agentのパケットエンジンの特定のデータ構造がクリーンアップされる前にクリーンアップされたため、カーネルパニックが発生し、システムがクラッシュしていました。SF01423970/SEG-43481/DS-34436
- dsa_filter.koがネットワークデバイスの情報を取得しているときに、カーネルパニックが発生しました。SEG-50480/DS-35192
- Linux環境でJavaを実行しているSAPシステムで、Deep Security Scannerからエラーコードが返され、エラーメッセージは返されませんでしたが、起動に失敗していました。SF01339187/SEG-38497/SEG-33163/DS-31330
- redirfsが原因でカーネルパニックが発生しました。SF01137463/SEG-34751/DS-32182
- Deep Securityの不正プログラム対策により、ファイルシステムのマウント時にfusermountプロセスが失敗しました。SF01531697/SEG-43146/DS-32753
- Deep Security Agentの侵入防御モジュールが、ペイロードゼロのUDPパケットを通知なしでドロップしました。SEG-39711/DS-32799
- Webレピュテーションの場合、Deep Security Agentからプロキシに不正な認証情報が送信され、プロキシからHTTP 407が返されました。SF01704358/SEG-45004/DS-32077
- Deep Security Agent GSCHドライバで、別のサードパーティ製ファイルシステムで問題が発生しました。SF01248702/SEG-44565/DS-33155)
- Deep Security不正プログラム対策の環境変数のオーバーライドがLinuxで機能しませんでした。SEG-43362/DS-31328
- SSLメッセージの詳細ログを有効にして出力すると、Deep Security Agentプロセスがクラッシュする可能性がありました。SF01745654/SEG-45832/DS-33007
- 複数のSmart Protection Serverが設定されている場合、無効なsps_indexが原因でDeep Security Agentプロセスがクラッシュすることがありました。SF01415702/SEG-42919/DS-33008

- Deep Security AgentでGetDockerVersionエラーが発生したため、ポリシーの送信処理に失敗しました。SF1939658/SEG-49191/DS-34222
- Deep Security AgentからDeep Security Managerへの応答として無効なJSONオブジェクトが送信されたため、Deep Security Managerのログファイルにエラーが発生しました。SF01919585/SEG-48728/DS-34022
- 変更変更監視が有効な場合、特定の条件下でds_agentプロセスがクラッシュすることがありました。SEG-50728/DS-35446
- Deep Security AgentをUbuntu 18.04にインストールできませんでした。SF01593513/SEG-43300/DS-37359
- 作業中のパケットオブジェクトが誤って削除されたため、Deep Security Agentネットワークエンジンがクラッシュしました。SF01526046/SF02159742/SEG-55453/DS-38812
- リアルタイムの変更変更監視ファイル検索イベントにUnicodeユーザ名を表示できませんでした。SF02187371/SEG-56645/DS-39398
- [ファイアウォールインタフェースの無視] が設定されていると、エージェントのオペレーティングシステムがクラッシュすることがありました。SF01775560/SEG-49866/DS-39339
- Deep Security Agentは、Python拡張モジュール (PYD) ファイルをアプリケーションコントロールのインベントリに追加しませんでした。SF01804378/SEG-47425/DS-33690
- ユーザモードで処理中のファイルオープンイベントが多すぎるため、CPU使用率が高くなります。SF02179544/SEG-55745/DS-39638
- Deep Securityリアルタイム不正プログラム対策が有効なときにメッセージキューにアクセスしているときに、「mq_getattr: Bad file descriptor」エラーが発生しました。SF02042265/SEG-52088/DS-39890
- Deep Security不正プログラム対策ドライバによってLinuxカーネルログが大量に送信されました。SF02299406/SEG-57561/DS-41589
- 実行権限で開かれた非実行可能ファイルにより、生成されるべきではないセキュリティイベントとドリフトが発生していました。SF01780211/SEG-46616/DSSEG-3607
- アプリケーションコントロールが有効で、ホストアプリケーションが大量の非実行可能ファイルを作成しているときに、CPU使用率が高くなりました。SF02179544/SEG-55745/DS-41142
- Deep Security Agentのリアルタイム不正プログラム対策検索はDebian 10 64ビットでは機能しませんでした。

- ゲスト仮想マシンがESXiホスト間で頻繁に移行されると(vMotionを使用して)、仮想マシンで状態ファイルを保存できないことがありました。このため、移行後、新しいESXiサーバでDeep Security Managerによって仮想マシンが自動的に再有効化されるまで、ゲストはDeep Security Virtual Applianceによる保護を失うことになります。DSSEG-4341/DS-38221
- LinuxでDeep Security Agentをアンインストールすると、アンインストールログに入力ミスがありました。DSSEG-4139/DS-34504
- Deep Security 不正プログラム対策でサンプルの不正プログラムファイルが検出されましたが、自動的には削除されませんでした。SF02230778/SEG-55891/DS-40687
- Deep Security AgentがDeep Security as a Service上のDeep Security Managerにプロキシ経由で接続している場合、検出されたファイルを削除できませんでした。SF01979829/SEG-51013/DS-37252
- ルール1006540「X-Forwarded-For HTTPヘッダログを有効にする」を適用すると、Deep Securityで侵入防御イベントのX-Forwarded-Forヘッダが正しく抽出されます。ただし、「Invalid Traversal」などのURL侵入は、ヘッダが解析される前にHTTP要求文字列で検出されます。侵入防御エンジンが強化され、ヘッダの解析後にX-Forwarded-Forヘッダを検索するようになりました。SEG-60728/DSSEG-5094
- Deep Security AgentからDeep Security Managerへの応答として無効なJSONオブジェクトが送信されたため、Deep Security Managerのログファイルにエラーが発生しました。SF01919585/SEG-48728/DSSEG-4995

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-3704/VRTS-3176

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度 : 高

- NGINXが1.16.1にアップデートされました(DSSEG-4600)
- curl 7.67.0にアップデートされました。

- openssl-1.0.2tにアップデートされました。
- JREを最新のJava Update(8.0.241/8.43.0.6) にアップデートしました

カーネルのサポート

現在サポートされているLinuxカーネルを確認するには、"Linuxカーネルの互換性" on page 400.

Linuxカーネルサポートのリリース履歴を表示するには、Deep Security Agentの新機能のLinuxの項目を参照してください。

既知の問題

- リアルタイム不正プログラム対策が有効な場合、autofsの使用は現在サポートされていません。リアルタイム不正プログラム対策を有効にしてautofsを使用すると、一部のマウントポイントが正常にアンマウントされます。SEG-58841

Windows

Deep Security Agent - 20.0.3-860 (20 LTS 更新 2026-01-21)

リリース日: 2025年1月21日

ビルド番号: 20.0.3-860

新機能

Endpoint Event Viewer: Endpoint Event Viewerにアクセスして、管理されたコンピュータ全体のセキュリティおよびシステムイベントを期間、重大度、イベントの発生元、アクションでフィルタリングして表示します。これはTrend Vision One - サーバ & Workload Protectionのみでサポートされています。

解決された問題

- Deep Security Agentは、syslogホスト名が64文字を超えるとクラッシュしました。PCT-87531/DSA-14252
- Webレピュテーションサービスを有効にすると、システムメモリの使用量が継続的に増加しました。PCT-80352/DSA-13866

- Deep Security Agentは、エージェントが予期していた形式と異なるHTTP/2パケットを処理する際に、時々クラッシュすることがありました。PCT-85552/DSA-13755
- Deep Security Agentが再起動した後、侵入防御検出が時々動作を停止しました。PCT-82352/DSA-13755
- Deep Security Agentは、Trend Vision One - サーバ&Workload Protectionによって管理されている場合、Deep Security Notifierにステータスを送信できませんでした。詳細については、トレンドマイクロ™ Deep Security™ NotifierがDeep Security Agentに対して「不明/到達不能」ステータスを表示するを参照してください。PCT-87617/PCT-87643/PCT-87679/PCT-87740/PCT-87829/DSA-14115

Deep Security Agent - 20.0.2-29810 (20 LTS 更新 2025-12-24)

リリース日: 2025年12月24日

ビルド番号: 20.0.2-29810

解決された問題

- アプリケーションコントロールは、ルールセットの更新が適用されたときにインベントリを保持できませんでした。詳細については、Trend Vision One™サーバ&Workload Protection、Cloud One Workload Security、およびDeep Securityアプリケーションコントロールがルールの更新時にインベントリを保存できない場合がありますを参照してください。DSA-13750

Deep Security Agent - 20.0.2-29760 (20 LTS アップデート2025-12-09)

リリース日: 2025年12月09日

ビルド番号: 20.0.2-29760

強化

- ファイアウォールと侵入防御システムのイベントは、データが利用可能な場合、プロセスとユーザ情報を表示します。これはすべての顧客に段階的に展開されています。DSA-13741

- Deep Security Relayを使用するエージェントのために、Deep Security Agentの設定ファイルで強力な暗号化方式 (app.relay.strongciphers=true) と最小のTransport Layer Security (TLS) バージョン (app.relay.restrictRelayMinimumTLSProtocol=TLSv1.2) を設定できるようになりました。DSA-2163
- 高度な脅威検索エンジンがバージョン25.560に更新されました。DSA-11917

解決された問題

- 一部のシステムでファイルコレクションまたはカスタムスクリプト機能を使用したログのアップロードに失敗しました。この問題はTrend Vision Oneのみに影響しました。V1E-115291
- 特定のシステムでDeep Security Agentとデバイスコントロールを有効にしている場合、ソフトウェアのビルドに時間がかかりました。PCT-76169/V1E-114202
- Trend Vision One - Deep Security Agentは、Trend Vision One Endpoint Securityのソフトウェア情報タブの最終更新日列を表示しませんでした。V1E-64601
- 不正プログラム対策は、OSが低電力モードで動作しているとき (例えば、ラップトップの画面がオフまたは閉じている場合) に動作を停止することがあります。DSA-13698/DSA-11913
- Deep Security Agent 20.0.2.22850または20.0.2.26670にアップグレードした後、強化された推奨検索が無効になり、自動的に再有効化されませんでした。この問題が発生した場合、システムは36時間後に従来の推奨検索を使用するように戻り、機能の継続を確保しました。この問題はEndpoint & Workload Securityにのみ影響しました。WS-13982

セキュリティ更新

このリリースには、サードパーティライブラリの更新が含まれています。DSA-7695/DSA-13181/DSA-13204

既知の問題

- アプリケーションコントロールは、ルールセットの更新が適用されたときにACインベントリを保持できません。

  推奨されるアクション:

- アプリケーションコントロールを実行しているエージェントがバージョン20.0.2-29760にアップグレードされていない場合、これらのエージェントをアップグレードしないでください。
- アプリケーションコントロールを実行しているエージェントがすでにバージョン20.0.2-29760にアップグレードされている場合、次の手順を順番に実行してください。
  a. アプリケーションコントロールが有効になっているすべての20.0.2-29760エージェントに対してアプリケーションコントロールのブロックモードを無効にします。
  b. アプリケーションコントロールが有効になっているすべてのエージェントを以前のエージェントバージョンにダウングレードします。
  c. 必要に応じて、これらのエージェントに対してアプリケーションコントロールのブロックモードを再度有効にしてください。

詳細については、Trend Vision One™サーバ&Workload Protection、Cloud One Workload Security、およびDeep Securityアプリケーションコントロールがルールを更新する際にインベントリの保存に失敗する可能性があります を参照してください。DSA-13750

Deep Security Agent - 20.0.2-26670 (20 LTS 更新 2025-11-12)

リリース日: 2025年11月12日

ビルド番号: 20.0.2-26670

新機能

ユーザベースのファイアウォール: ファイアウォールルールはユーザアカウントに基づいて設定できるようになりました。この機能はすべての顧客に段階的に展開されています。

強化されたHTTP/2サポート: 侵入防御システムエンジンは、現在、受信HTTP/2接続をサポートしています。この機能は、安定性とパフォーマンスの向上を確保するために、バックエンドの更新を通じて段階的に展開されます。(このリリースには、HTTP/2の処理とセキュリティの向上を目的とした修正も含まれています。PCT-77306/DSA-13105)

Windows 11 25H2サポート: Deep Security Agent 20.0.2-26670以降はWindows 11バージョン25H2をサポートしています。

解決された問題

- 一部のSmart Protection Server接続問題に対してイベントの生成に失敗しました。PCT-55362/DSA-11534
- Webレピュテーションサービスは、Google Chromeバージョン140以降でブラウザがシークレットモードで実行されているときに動作しませんでした。DSA-13161
- Deep Security Agentは、MQTTコードの問題により時々クラッシュしました。PCT-79555/DSA-3839

Deep Security Agent - 20.0.2-22850 (20 LTS 更新 2025-10-08)

リリース日: 2025年10月08日

ビルド番号: 20.0.2-22850

強化機能

- 高度なTLSトラフィック検査は、Windows 11、Windowsサーバ2022、およびWindowsサーバ2025でTLS 1.3をサポートするようになりました。DSA-12834

Deep Security Agent - 20.0.2-20480 (20 LTS 更新 2025-09-17)

リリース日: 2025年9月17日

ビルド番号: 20.0.2-20480

機能強化

- セキュリティログ監視はディレクトリ名でグロブ文字をサポートするようになりました。PCT-8309

解決された問題

- アプリケーションコントロールが有効な状態でDeep Security Agentを実行すると、一部のシステムでメモリリークが発生しました。DSA-12148
- リアルタイム検索の設定が存在しない場合、隔離されたファイルの復元は失敗します。PCT-73666/DSA-12139

既知の問題

- Webレピュテーションサービスは、Google Chromeバージョン140以降でブラウザがシークレットモードで実行されている場合、動作しません。DSA-13001

Deep Security Agent - 20.0.2-17700 (20 LTS 更新 2025-08-13)

リリース日: 2025年8月13日

ビルド番号: 20.0.2-17700

強化

- Deep Security Agentは、不正プログラム対策ソリューションプラットフォームが一時フォルダを作成する際に、適切なパス文字列の使用を確保します。PCT-60262/DSA-11532

解決された問題

- Deep Security Agentはハートビート接続を確立する際にクラッシュすることがあります。PCT-66595/DSA-11386

Deep Security Agent - 20.0.2-14490 (20 LTS 更新 2025-07-09)

リリース日: 2025年7月9日

ビルド番号: 20.0.2-14490

新機能

エージェントインターフェース: エージェントインターフェースは、Trend Vision Oneがエージェントおよびコンポーネントの更新を管理し、Trend Micro Endpoint Basecamp (XBC) エージェントがインストールされたエンドポイントのスキャンをトリガーすることを可能にします。これは現在、Trend Vision One - サーバ & Workload Protection のみサポートされています。

強化

- 高度なTLSトラフィック検査が有効になっている場合、接続がブロックされていない限り、Deep Security Agentは接続を高速化するためにパケットを挿入します。PCT-

63207/DSA-10919

解決済みの問題

- オンデマンド検索は、Deep Security Agentのアクティベーションまたは再起動後に自動検索がトリガーされるまで手動で開始できませんでした。WS-12581
- リモートアップグレード後、Deep Security Agentは言語設定をシステムのデフォルト言語に変更しました。PCT-52649/DSA-11221
- 検出レベルを上げた後、機械学習型検索によって以前は安全と判断されていたファイルが、スキャンから除外されるべきではないのに除外されていました。DSA-11204

Deep Security Agent - 20.0.2-12290 (20 LTS 更新 2025-06-11)

リリース日: 2025年6月11日

ビルド番号: 20.0.2-12290

機能強化

- デフォルトで有効化されているWebレピュテーションサービスは、ウェブサイトのリスクレベルを判断する際にサーバ名表示 (SNI) クエリを使用します。
- アクティビティモニタリングはJavaServer Page (JSP) ファイルをサポートしました。V1E-54751
- プロセスメモリ検索結果は、同じプロセス識別子 (PID) によって複数の検索がトリガーされた場合の検索の原因に関する追加情報を提供します。詳細は、Vision Oneエンドポイントセキュリティ検索アプリで「trigger_info」を検索することで確認できます (XDR Threat Investigation > Search)。現時点では、疑わしい検出のみがtrigger_infoをサポートしています。DSA-9085

解決済みの問題

- Deep Security AgentはSSLハンドシェイク中に時々クラッシュしました。PCT-55526/DSA-9902
- 予期しないレジストリ値のため、拡張推奨検索が失敗しました。WS-12303
- Webレピュテーションサービスが有効化されたとき、x86アーキテクチャのシステムでDeep Security Agentが時々クラッシュしました。DSA-11060

- Trend Vision OneのVersion Control Policiesを使用する際、Deep Security Agentのアップグレードが時々失敗することがありました。PCT-52924/PCT-61392/PCT-62122/DSA-10972
- Deep Security Agentのインクリメンタルパターンアップデートが、フルパターンアップデートが代替のダウンロードオプションとして利用可能な場合でも、時々失敗しました。PCT-64289/PCT-65578/DSA-10953
- 不正プログラム対策ソリューションプラットフォーム (AMSP) がログを書き込もうとすると、システムが時々ハングすることがありました。PCT-41894/PCT-48493/PCT-51094/PCT-54129/PCT-54163/PCT-61016/PCT-64506/DSA-10327

セキュリティアップデート

このリリースにはサードパーティライブラリの更新が含まれています。DSA-10530

Deep Security Agent - 20.0.2-9810 (20 LTS 更新 2025-05-14)

リリース日: 2025年5月14日

ビルド番号: 20.0.2-9810

機能強化

- トレンドマイクロDeep Security Webレピュテーションアプリ(dsa-wrs-app.exe) は、トレンドマイクロWebレピュテーションアプリと呼ばれるようになりました。DSA-9779
- Webレピュテーションサービスは、疑わしいまたは悪意のあるサイトへのhttpプロキシ接続をブロックする際に、200 OKページではなく403 Forbiddenを指すようになりました。PTC-60576/DSA-10325

解決済みの問題

- 高度なTLSを使用したDeep Security Agentの構成が一部のシステムをフリーズさせました。PCT-63207/DSA-10380
- WebレピュテーションイベントのURL列に情報が欠落していることがありました。PCT-60576/DSA-10090
- 一部のシステムでブルースクリーン (BSoD) エラーが発生しました。PCT-60927/DSA-10191

- オフライン予約検索が、使用すべきDeep Security Agentのタイムゾーンではなく、Server & Workload Protectionのタイムゾーンを使用することがあり、週次および日次検索が誤った時間に開始され、月次検索が月の最終日に開始されると高いCPU使用率を引き起こすことがありました。PCT-55169/DSA-9303
- Deep Security Agentの再起動時にブルースクリーン(BSoD) エラーが発生することがありました。PCT-63627/DSA-10364
- Deep Security Agentを無効にしてから有効にすると、イベントとレポート> 不正プログラム対策イベントからイベントが欠落する可能性があります。PCT-53209/DSA-9707

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある情報開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が利用可能になります。VRTS-13942/DSA-9225

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度 : 高

Deep Securityエージェント - 20.0.2-7600 (20 LTS 更新 2025-04-16)

リリース日 : 2025年4月16日

ビルド番号 : 20.0.2-7600

新機能

動的インテリジェンスモード: 動的インテリジェンスモードにより、Deep Securityエージェントは検出された脅威、ユーザの挙動、システム構成に基づいて、セキュリティ対応を最適化するために監視レベルを自動的に調整できます。

機能強化

- Webレピュテーションサービスは、Windows Server 2025上のMicrosoft EdgeおよびGoogle Chrome用の「Trend Micro Toolbar for Enterprise」ブラウザ機能拡張をサ

ポートするようになりました。DSA-9538

解決された問題

- トレンドマイクロソリューションプラットフォームサービス (coreServiceShell.exe) が予期せずクラッシュしました。PCT-52712/DSA-9932
- Pure Storageソリューションがインストールされた環境では、時々パフォーマンスの問題が発生していました。PCT-47586/DSA-9553
- ドライバーの問題により、ブルースクリーン (BSoD) エラーが発生することがあります。PCT-55477/DSA-8421
- システムが休止状態から復帰する際に、PowerPointがクラッシュすることがありました。PCT-48516/DSA-8421

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が提供されることに注意してください。VRTS-13942/DSA-10038

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最も深刻なレベル: 高

Deep Securityエージェント - 20.0.2-4960 (20 LTS 更新 2025-03-12)

リリース日: 2025年3月12日

ビルド番号: 20.0.2-4960

機能強化

- dsa_scanコマンドには、大きなファイルを管理するためのscanLargeFileオプションが含まれるようになりました。DSA-8785
- キャッシュメカニズムの導入と不要な操作の削減により、SAPスキャンがより高速になりました。DSA-7219

- Deep Securityエージェントは、デバイスコントロールイベントをシステムのセキュリティ情報およびイベント管理 (SIEM) に直接記録できるようになりました。V1E-40316

解決済みの問題

- SAP Scannerは、4096バイトを超えるCSVファイルを誤って分類することがありました。PCT-51974/DSA-9139
- Windows Base Filtering Engineサービスが実行されていない場合、トレンドマイクロWindowsフィルタリングプラットフォーム (TBIMWFP) ドライバが停止中にクラッシュすることがあります。PCT-38921/PCT-53750/DSA-9154
- 証明書関連のエラーイベントが、イベント説明フィールドにある解決策記事へのリンクが古くなって生成されていました。これらのリンクは「404ページが見つかりません」につながっていました。PCT-54305/DSA-9113

Deep Securityエージェント - 20.0.2-1390 (20 LTS 更新 2025-01-15)

リリース日: 2025年1月15日

ビルド番号: 20.0.2-1390

新機能

Windows Server 2025のサポート: Deep Security Agent 20.0.2-1390以降は、FIPSモードのサポートを含むWindows Server 2025をサポートします。これにはDeep Security Manager 20.0.1017以降が必要です。

ユーザベースのファイアウォールイベント: ファイアウォールイベントには、可能な限りユーザ名が含まれるようになりました。この機能はプレビュー段階であり、現在は一部の顧客のみが利用可能です。

機能強化

- Deep Securityエージェントは、パフォーマンスを向上させるためにパケットを順番に処理するようにキューに入れるようになりました。DSA-6916
- Deep Securityエージェントを更新してスパイウェア対策を強化しました。PCT-18199/DSA-5889

解決済みの問題

- Deep Securityエージェントは、高度なTLSトラフィック検査が有効になっているときに接続の問題が発生することがありました。DSA-8577

セキュリティ更新

このリリースには、サードパーティライブラリの更新が含まれています。DSA-7695/DSA-8042

Deep Securityエージェント - 20.0.1-25770 (20 LTS Update 2024-12-10)

リリース日: 2024年12月10日

ビルド番号: 20.0.1-25770

新機能

バージョン管理ポリシー: Deep Securityエージェントは、バージョン管理ポリシーをサポートするようになりました。これにより、Trend Vision Oneのバージョン管理ポリシーを使用して、Trend Micro Endpoint Basecamp (XBC) エージェントがインストールされているエンドポイントのエージェントおよびコンポーネントの更新を管理できます。詳細については、Version Control Policiesを参照してください。これは現在プレリリース中であり、Trend Vision One - Server & Workload Protectionのみサポートされています。

強化

- Deep Security Agentを更新して、CPU使用率が中 (コンピュータまたはポリシー > 設定 > 一般 > CPU使用率の制御) に設定されている場合のオンデマンドスキャンの時間を短縮しました。DSA-8171
- Deep Security SAP Scannerは、Microsoft Outlookアイテム (MSG) 形式のメールに添付されたパスワード保護された圧縮ファイルを識別した場合に、結果をSAPアプリケーションに報告できるようになりました。SF07873657/PCT-23367/DSA-7562
- Deep Securityエージェントは、リレープロキシがTrend Vision One Service Gateway Forward Proxy Serviceであるかどうかを検出し、接続にリレープロキシを使用するかどうかを決定するためにService Gatewayドメイン許可リストを使用します。SF07267852/PCT-29311/DSA-6274

- Trend Cloud One - Endpoint & Workload Securityは、Deep Security Agentを介してTrend Vision One Endpoint Securityエージェントをインストールできるようになりました。DSA-7532
- Deep Securityエージェントは、既存の検出 (不正プログラム名、または不正プログラム対策や挙動監視のルールID) をコンピュータまたはポリシー > 不正プログラム対策 > 詳細からルール例外リストに追加できるようになりました。DSA-6318
- Deep Securityエージェントは、不正プログラム対策、挙動監視、機械学習型検索、プロセスメモリ検索、およびリアルタイム検索のためのWindows Antimalware Scan Interfaceの検出感度を微調整するための追加オプションをサポートするようになりました。この強化機能は、Trend Cloud One - Endpoint & Workload Securityでのみ利用可能です。DSA-6062
- Deep Securityエージェントは現在、不正プログラム対策プロセスパスの除外にワイルドカード*の使用をサポートしており、Windowsプラットフォーム向けに段階的に展開されています。PCT-36703/DSA-7768

解決された問題

- パケットデータを含むイベントが不正なパケットサイズで記録されていました。PCT-45556/DSA-8074
- 変更監視スキャンの後に変更監視が無効にされた場合、Deep Securityエージェントの CPU使用率が通常よりも高くなりました。SF07991055/PCT-31459/DSA-6195
- 特殊文字を含むファイルやフォルダーの不正プログラム対策手動スキャンが時々失敗することがありました。PCT-43895/DSA-8126
- トレンドマイクロWindowsフィルタリングプラットフォーム (TBIMWFP) ドライバーが一部のシステムでメモリリークを引き起こし、通常よりも高いメモリ使用量につながりました。DSA-7968
- Deep Security SAP Scannerは、同じ内容のファイルが2つ以上圧縮ファイルに含まれている場合に、スキャン失敗を誤って報告することがありました。PCT-38781/DSA-7557
- 不正プログラム対策ソリューションプラットフォーム (AMSP) サービスが一部のシステムでクラッシュしていました。PCT-41566/DSA-7952

セキュリティ更新

このリリースには、サードパーティライブラリの更新が含まれています。DSA-7124

このリリースにはセキュリティアップデートが含まれています。脆弱性に対するトレンドマイクロの保護についての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが利用可能になった後にのみ、特定のセキュリティアップデートのCVE (Common Vulnerabilities and Exposures) 詳細が利用可能になります。
VRTS-13016/DSA-7645

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度 : 高

Deep Securityエージェント - 20.0.1-23340 (20 LTS 更新 2024-11-13)

リリース日 : 2024年11月13日

ビルド番号 : 20.0.1-23340

新機能

Windows 11, バージョン24H2のサポート: Deep Securityエージェント20.0.1-23340以降はWindows 11, バージョン24H2をサポートします。

機能強化

- Webレピュテーションサービスは、Webサイトのリスクレベルを判断する際にサーバー名表示 (SNI) クエリを使用できるようになりました。DSA-7314
- 高度なトランスポート層セキュリティ(TLS) 検査は、Windowsローカルセキュリティ機関 (LSA) 保護をサポートできるようになりました。DSA-5642

解決済みの問題

- アプリケーションコントロールがブロックモードで動作しているとき、一部のディレクトリ内のファイルがブロックされるべきところを許可されていました。PCT-38516/DSA-7613
- Deep Securityエージェントは、不正プログラム対策の手動検索を実行する際に、ファイルハンドルリークを引き起こすことがありました。DSA-7676

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。脆弱性に対する保護方法の詳細については、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることにご注意ください。VRTS-13428//VRTS-13017/DSA-7666/DSA-7646

最高共通脆弱性評価システム (CVSS) スコア: 6.7

重大度: 中

Deep Securityエージェント - 20.0.1-21510 (20 LTS更新 2024-10-16)

リリース日: 2024年10月16日

ビルド番号: 20.0.1-21510

機能強化

- フェイルセーフを追加して、ファイアウォールドライバがシステムをブルースクリーン (BSoD) ループに陥らせるのを防ぎます。DSA-7448
- ファイアウォールドライバが初期化されるときに、新しいWindowsイベントをログに追加します。イベントには、Windowsベースフィルタリングエンジンの状態変更と、tbimwfpドライバによって登録された結果が含まれます。DSA-7547

解決された問題

- アプリケーションコントロールとFIPSの両方が有効になっていると、高CPU使用率が発生します。DSA-6842
- Windows Base Filtering Engine Serviceが実行されていない場合、Deep Securityエージェントがシステムをクラッシュさせることがあります。PCT-38921/DSA-7334
- SAP ScannerライブラリがDeep Securityエージェントへの接続を再確立した際、SAP Scannerライブラリから送信されたスキャン要求が時々拒否されることがありました。SF08196066/PCT-34824/DSA-7608
- 特定の形式 (CSVなど) のファイルをスキャンする際に、Deep Security SAP Scannerがクラッシュすることがありました。PCT-41353/DSA-7609

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対する保護方法の詳細については、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることにご注意ください。VRTS-12953/DSA-7559

最高共通脆弱性評価システム (CVSS) スコア: 8.0

最高の重大度: 高

Deep Security エージェント - 20.0.1-19250 (20 LTS Update 2024-09-18)

リリース日: 2024年9月18日

ビルド番号: 20.0.1-19250

機能強化

- Deep Securityエージェントを更新して、古いバージョンのSAP Scannerとの互換性を向上させました。SF08196066/PCT-34824/DSA-6819
- Deep Security エージェントは、Alibaba Cloud コネクタタイプをサポートするようになりました。DSA-6018
- Webレピュテーションサービスは、Windows 10 (64-bit)、Windows 11、Windows Server 2016、Windows Server 2019、およびWindows Server 2022上のMozilla FirefoxでHTTPSを使用する際に保護を提供できるようになりました。DSA-6770

解決済みの問題

- Deep Security エージェントが、アプリケーションコントロールとFIPSの両方が有効になっているシステムで高いCPU使用率を引き起こしました。DSA-6842

セキュリティアップデート

このリリースには、サードパーティライブラリの更新が含まれています。DSA-6156/DSA-6942

Deep Security Agent - 20.0.1-17380 (20 LTS アップデート2024-08-21)

リリース日: 2024年8月21日

ビルド番号: 20.0.1-17380

機能強化

- Webレピュテーションサービス "Smart Protection Server Disconnected" イベントには、説明フィールドにFQDNまたはIPアドレス情報が含まれるようになりました。DSA-5408
- SAP Scannerは、Society for Worldwide Interbank Financial Telecommunication (SWIFT) メッセージをテキストファイルとして分類します。SF07895338/PCT-24359/DSA-5790
- SAP Scanner は、互換性のあるファイル拡張子に JavaScript を関連付けるようになりました。詳細については、サポートされている MIME タイプ を参照してください。SF08102626/PCT-31518/DSA-6192
- uAgentWscHandler.exe は、新しいプロセスであり、Windows 不正プログラム対策 Protected Process Light テクノロジーをサポートし、Windows 10 または Windows 11 の Windows セキュリティセンターと統合されます。DSA-5138
- 高度な脅威検索エンジンがバージョン24.550に更新されました。DSA-5968

解決済みの問題

- SAP Scanner は、データが1行にフォーマットされている場合、有効なCSVファイルを誤って分類することがあります。SF07967718/PCT-26844/DSA-6102
- SAP Scanner は時々画像ファイルをASPスクリプトとして誤認識しました。SF07764878/PCT-20406/DSA-6122
- Deep Security Agent は、一部のポリシー構成フィールドに中括弧が含まれている場合、ポリシーを読み込むことができませんでした。DSA-6189
- Deep Security Agentは、ホスト名に非ASCII文字が含まれている場合、アクティベートに失敗します。PCT-32214/DSA-6268
- Deep Security Agent は、Advanced TLS 検査が有効になっている場合、オペレーティングシステムのクラッシュを引き起こすことがありました。PCT-34149/DSA-6346

- 不正プログラム対策を有効にすると、一部のCitrix 仮想デスクトップインフラストラクチャ (VDI) 環境でブルースクリーン (BSoD) エラーが発生しました。PCT-26799/DSA-6036
- 侵入防御がDeep Securityエージェントで有効になっている場合、サードパーティアプリケーションがソースポートを再利用すると接続の問題が発生することがあります。SF07685331/PCT-20541/DSA-5596

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。脆弱性に対する保護方法の詳細については、脆弱性対応をご覧ください。責任ある情報公開の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることにご注意ください。VRTS-12301/DSA-5967/DSA-6150

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度 : 高

既知の問題

- Deep Security Agent アプリケーションコントロールが高いCPU使用率を引き起こします。PCT-36414

Deep Security Agent - 20.0.1-14610 (20 LTS アップデート2024-07-17)

リリース日 : 2024年7月17日

ビルド番号 : 20.0.1-14610

機能強化

- SAP Scanner は、次の MIME タイプを互換性のあるファイル拡張子に関連付けます。詳細については、SAP NetWeaver と統合するを参照してください。
  - TrueType フォント (TTF)。SF08102626/PCT-31518/DSA-6049
  - Javaアーカイブ (JAR)。SF08102626/PCT-31518/DSA-6044
  - Apple QuickTime File Format (QTFF)。SF07967718/SF07840151/PCT-22825/PCT-26844/DSA-5887/DSA-5567

- Microsoft Advanced Systems Format (ASF). SF07967718/PCT-26844/DSA-5886

解決済みの問題

- Deep Security Agent は引き続きサービスゲートウェイの接続をテストしようとします。DSA-5814
- Deep Security Agent の再起動が原因で、アプリケーションコントロールがドリフトイベントを報告することがあります。SF07813110/PCT-25731/DSA-5798
- Deep Security AgentはService Gatewayのプライマリ IPアドレスのみを使用できました。DSA-4513
- 変更監視 real-time scans が時々イベントを生成できないことがありました。SF07269768/PCT-21721/DSA-5877
- 不正プログラム対策の設定ファイルサイズが一部のシステムでSAP Scannerのパフォーマンスに影響を与えていました。SF08057009/PCT-30380/DSA-5987

Deep Security Agent - 20.0.1-12510 (20 LTS アップデート2024-06-19)

リリース日: 2024年6月19日

ビルド番号:20.0.1-12510

機能強化

- Advanced TLS Traffic Inspectionは、"Inbound TLS/SSLトラフィックの検査"と"Outbound TLS/SSLトラフィックの検査"のために別々の設定をサポートしています。詳細な設定手順については、https://help.deepsecurity.trendmicro.com/20_0/on-premise/ja-jp/intrusion-prevention-ssl-traffic.htmlを参照してください。

解決済みの問題

- VDI環境では、Webレピュテーションサービスが高いCPU使用率を引き起こす可能性があります。PCT-24431/PCT-28543/PCT-29364/PCT-29712/PCT-30043/PCT-30401/PCT-30669/DSA-5766

- IoT機能が有効になっていない場合、エッジリレーはオペレーティングシステムのプロキシ構成を使用できません。PCT-16603/DSA-5422

既知の問題

- インバウンドTLS/SSLトラフィックの検査とアウトバウンドTLS/SSLトラフィックの検査がAdvanced TLS Inspection設定で同時に有効になっている場合、パフォーマンスに影響があります。詳細については、Deep Securityにおける双方向TLS検査のパフォーマンスへの影響を参照してください。DSA-5959

Deep Security Agent - 20.0.1-9400 (20 LTS Update 2024-05-16)

リリース日: 2024年5月16日

ビルド番号: 20.0.1-9400

機能強化

- SAPScannerで SCANLOGPATH パラメータがサポートされるようになりました。詳細については、「SAP NetWeaverとの統合」を参照してください。PCT-21958/DSA-4924
- Deep Security Agentをアップデートして、プロキシを使用する設定の優先度を向上させました。DSA-4817/PCT-21750
- Deep Security Agentで、Trend Micro Endpoint Basecamp (XBC) エージェントからService Gatewayの設定を取得できるようになりました。DSA-4841/V1E-13468
- Webレピュテーションサービスは、Windows 10 (64ビット)、Windows 11、Windows Server 2016、Windows Server 2019、およびWindows Server 2022で、Google ChromeブラウザのシークレットモードとMicrosoft EdgeブラウザのInPrivateモードでHTTPS保護をサポートするようになりました。DSA-4296

解決済みの問題

- プロキシ設定の再設定後にDeep Security Agentのセキュリティアップデートが失敗することがありました。PCT-18382/DSA-5390
- Webレピュテーションサービスを有効にしてDeep Security Agentを使用すると、一部のアプリケーションパフォーマンス監視 (APM) アプリケーションが正常に機能しませんでした。SF04072723/SEG-97952/PCT-15716/DSA-4750

- 複数のSmart Protection Serverを使用すると、スマートスキャンが接続されている場合でも、「スマートスキャンに対してSmart Protection Serverが切断されました」という警告が生成されることがありました。PCT-13313/DSA-4488
- エージェントアップデートの適用後にDeep Security Agentのセキュリティアップデートが失敗することがありました。PCT-23614/DSA-5371

セキュリティアップデート

このリリースには、サードパーティ製ライブラリのアップデートが含まれています。DSA-4187

Deep Security Agent - 20.0.1-7380 (20 LTS Update 2024-04-24)

リリース日: 2024年4月24日

ビルド番号: 20.0.1-7380

強化

- Deep Security Agentで、Trend Vision One Service Gatewayの除外がサポートされるようになりました。現時点では、Trend Cloud One - Endpoint & Workload Securityユーザのみがサポートされます。V1E-17754
- Deep Security Agentのプロキシ設定は、Trend Vision One Proxy Managerで設定できます。V1E-14557
- Deep Security Agentで、プロセスメモリ検索のカスタム処理「ActiveAction」または「Pass」がサポートされるようになりました。現時点では、Windowsプラットフォームの Trend Cloud One - Endpoint & Workload Securityユーザのみがサポートされます。DSA-3621

解決された問題

- クラウド環境で実行されているDeep Security AgentをTrend Cloud One -Endpoint & Workload Securityで有効化できないことがありました。DSA-4861
- SAPScannerが有効な場合、Deep Security Agentのアップグレード時に、「SAP:不正プログラム対策の準備ができていません」または「SAP: ウイルス検索サービスが正しく動作していません」というシステムイベントが表示されることがありました。これらのシステムイベントメッセージは、Deep Security Agentモジュールの再起動によってトリガされました。機能への影響はありませんでした。DSA-4603

Deep Security Agent - 20.0.1-4540 (20 LTS Update 2024-03-20)

リリース日: 2024年3月20日

ビルド番号: 20.0.1-4540

機能強化

- Deep Security AgentのSAP Scannerのステータスがコンソールに表示されるようになりました。DSA-3329
- Deep Security Agentのバージョンが SAPScannerライブラリに表示されます。SF07483850/PCT-10077/DSA-3304
- Trend Cloud One - Endpoint & Workload Securityが管理するDeep Security Agentの停止にかかる時間が短縮されました。DSA-4208
- 不正プログラム対策イベント(イベントとレポート> 不正プログラム対策イベント) に、ファイルまたはフォルダが作成および変更された日時が表示されるようになりました。SF07199253/PCT-1378/DSA-3578

解決済みの問題

- Deep Security Agentは、AutoCADで生成された `.dwg` ファイルのMIMEタイプを誤ってAutoCAD 2004からAutoCAD 2024に分類しました。SF07027236/SEG-186079/PCT-5797/DSA-2901

Deep Security Agent - 20.0.1-3180 (20 LTS Update 2024-02-29)

発売日: 2024年2月29日

ビルド番号: 20.0.1-3180

新機能

- 不正プログラム対策は、デフォルトでTrend Cloud Oneの高度なプロセスメモリ検索をサポートするようになりました。プロセスメモリ検索は、手動検索および予約検索の設定で利用可能です (リアルタイム検索の設定に加えて)。プロセスメモリ検索の実行するアクションオプションは、リアルタイム検索、手動検索、および予約検索の設定で利用可能です。DSA-4242

機能強化

- Deep Security Scanner (SAP) は、Microsoft Officeマクロを含むファイルをアクティブコンテンツとしてレポートするようになりましたが、以前は不正プログラムとして識別されていました。PCT-5979/DSA-3911

解決済みの問題

- Trend Vision One Service Gatewayを使用したオンプレミスDeep Security ManagerからTrend Cloud One - Endpoint&Workload SecurityへのAgentの移行に失敗しました。この問題は、他のプロキシサービスを使用して移行する場合にも発生する可能性があります。PCT-16649/DSA-4144
- Windows Server 2008 R2のリモートデスクトップサービスがTLS検査プロセス (tm_netagent) によってブロックされました。PCT-12049/PCT-12172/PCT-13878/DSA-3944
- 挙動監視の除外は、大文字と小文字が区別されるため、適用できないことがありました。PCT-16168/PCT-16005/PCT-16476/CTSKA-27/DSA-4116
- 想定されるMIMEタイプ .msg Deep Security Agent SAP Scannerによるファイルが正しくありません。PCT-5797/DSA-4050
- Deep Security Agentで侵入防御またはWebレピュテーションサービスを有効にすると、TLS検査プロセス (tm_netagent) のエラーログローテーションの問題が発生することがありました。DSA-3965
- ローカルでの上書きにパスワードが必要な場合、Deep Security Agentのセルフプロテクションがローカルで無効になった後にパスワードが確認されました。PCT-10861/DSA-3293
- Deep Security Agentをアンインストールしても、Deep Security Agentに関連付けられているすべてのフォルダが削除されませんでした。DSA-2460

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-11708/DSA-3702

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度:高

既知の問題

- 実行可能ファイルのコピーを実行しているときに、アプリケーションコントロールの信頼エンティティの「ターゲットごとにブロック」信頼ルールが正しく機能しないことがあります。PCT-11105/DSA-3324

Deep Security Agent - 20.0.1-700 (20 LTS Update 2024-04-17)

リリース日:2024年4月17日

ビルド番号:20.0.1-700

機能強化

- Deep Security Agentをアップデートして、プロキシを使用する設定の優先度を向上させました。現時点では、Windows x64プラットフォームを使用しているTrend Cloud One - Endpoint & Workload Securityのユーザのみがサポートされます。DSA-4817/PCT-21750

既知の問題

- Deep Security Agent 20.0.1.700 への更新が、Deep Security Relay を使用している場合、一部の 20.0.0 バージョンで失敗します。詳細については、自己展開された Workload Security Relay の 20.0.0-3445 以降からバージョン 20.0.1 へのリモートアップグレードの失敗 を参照してください。DSA-3317
- Deep Security Agent で侵入防御 または Web レピュテーションサービスを有効にすると、TLS インスペクションプロセス (tm_netagent) のエラーログローテーションの問題が発生する可能性があります。詳細については、Deep Security の TLS インスペクションプロセスエラーログローテーションの問題 を参照してください。DSA-3773

Deep Security Agent - 20.0.1-690 (20 LTS Update 2024-01-17)

リリース日:2024年1月17日

ビルド番号:20.0.1-690

新機能

コマンドライン検索: Deep Security Agentで、コマンドラインから`dsa_scan`を使用して起動されるオンデマンド検索がサポートされるようになりました。

現在、この機能はTrend Cloud One - Endpoint & Workload Securityのユーザのみが利用できます。詳細については、「コマンドラインの基礎」を参照してください。V1E-6993

機能強化

- 2024年以降、Deep Security Agentのバージョン管理が20.0.0から20.0.1に改訂されます。これにはDeep Security Manager 20.0.883以降が必要です。DSA-3584

  詳細については、2024年1月のアップデートリリースにおけるDeep Security Agent (DSA) バージョン改訂のプラットフォームサポート更新をご覧ください。

解決済みの問題

- Deep Security AgentがローカルのSmart Protection Serverに接続できないことがありました。DSA-3564
- 一部のシステムでDeep Security Agentがドメインコントローラにルーティングするときにメモリリークが発生することがありました。DSA-3266
- Windows APIがPortable Executable (PE) ファイルのデジタル署名を検証している場合、Deep Security Agentが起動時にフリーズすることがありました。DSA-3626
- FIPSモードが無効な場合、Deep Security Agentは、エージェントで指定された設定ではなく、システム環境変数で指定されたOpenSSL設定を使用していました。PCT-4914/DSA-2651/DSA-2737/DSA-2738

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。V1E-10952

最高共通脆弱性評価システム (CVSS) スコア: 9.8

最高の重大度: 重大

既知の問題

- Deep Security Agent 20.0.1-690 へのアップデートが、Trend Cloud One - Endpoint & Workload Security で Deep Security Relay を使用している場合、20.0.0 の一部のバージョンからのアップデートで失敗することがあります。詳細については、自己展開された Workload Security Relay の 20.0.0-3445 以降からバージョン 20.0.1 へのリモートアップグレードの失敗 DSA-3317 を参照してください
- 侵入防御またはWebレピュテーションサービスをDeep Security Agentで有効にすると、TLS検査プロセス(tm_netagent)のエラーログローテーションの問題が発生する可能性があります。詳細については、Deep SecurityにおけるTLS検査プロセスのエラーログローテーションの問題を参照してください。DSA-3773

Deep Security Agent - 20.0.0-8438 (20 LTS Update 2023-12-12)

リリース日: 2023年12月12日

ビルド番号: 20.0.0-8438

新機能

Windows 11バージョン23H2のサポート: Deep Security Agent 20.0.0-8438以降では、Windows 11バージョン23H2がサポートされます。DSA-2255

機能強化

- CPUとディスクの使用率が高くならないように、一部のファイルタイプを検索リストから削除します。SF07099651/SEG-188688/DSA-2010
- エージェントの自己保護により、高度なTLSトラフィック検査プロセス(tm_netagent)が保護され、管理者権限を持つローカルユーザがこのプロセスを停止できないようになりました。DSA-1042/DSA-1043

解決済みの問題

- ローカルのSmart Protection Serverと設定されたプロキシを使用している場合、Webレピュテーションサービスがプロキシ経由でトラフィックを不適切に送信することがありました。Webレピュテーションサービスは、クエリをローカルのSmart Protection Serverに直接送信するようになりました。DSA-2981

- 不正プログラム対策モードがポリシー設定と一致しない場合がありました。SF07117203/SEG-191043/PCT-7856/DSA-2561
- 大量の不審オブジェクトリストをロードすると、メモリリークが発生することがありました。SF06904914/SEG-182231/DSA-1370

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-11015/DSA-2156

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度: 高

既知の問題

- 侵入防御またはWebレピュテーションサービスをDeep Security Agentで有効にすると、TLS検査プロセス(tm_netagent)のエラーログローテーションの問題が発生する可能性があります。詳細については、Deep SecurityにおけるTLS検査プロセスのエラーログローテーションの問題を参照してください。DSA-3773
- Deep Security Agent は、ローカルの Smart Protection Server に接続できないことがあります。この問題は 20.0.1-690 で修正されています。詳細については、プロキシ使用時の Deep Security Agent (DSA) の Smart Protection Server (SPS) との接続問題 DSA-3564 を参照してください

Deep Security Agent - 20.0.0-8268 (20 LTS Update 2023-11-21)

リリース日: 2023年11月21日

ビルド番号: 20.0.0-8268

解決済みの問題

- システムがスリープモード(動作状態のS0低電力アイドルモード。モダンスタンバイとも呼ばれます) から復帰した後、Deep Security不正プログラム対策が期待どおりに機能しないことがありました。SF07326571/PCT-5476/DSA-2485

- Deep Security Agentでは、Microsoft Word、Excel、PowerPointで生成された.xmlファイル、およびAutoCADおよびR2000で生成された.dwgファイルのMIMEタイプが誤って分類されていました。SF07027236/SEG-186079/DSA-2202

既知の問題

- 侵入防御またはWebレピュテーションサービスをDeep Security Agentで有効にすると、TLS検査プロセス(tm_netagent)のエラーログローテーションの問題が発生する可能性があります。詳細については、Deep SecurityにおけるTLS検査プロセスのエラーログローテーションの問題を参照してください。DSA-3773

Deep Security Agent - 20.0.0-8137 (20 LTS Update 2023-10-26)

リリース日: 2023年10月26日

ビルド番号: 20.0.0-8137

新機能

- プロセスメモリスキャン: 不正プログラム対策の手動およびスケジュールスキャンは、実行中のプロセスのメモリをスキャンするプロセスメモリスキャンをサポートするようになりました。これには、Deep SecurityManager 20.0.844以降が必要です。
  この機能は、11月のDeep SecurityManagerおよびTrend Cloud One - Workload Securityのリリースで無効になります。詳細については、Deep Securityエージェント20.0.0-8137を使用する際のランダムプロセスの高メモリ使用量をご覧ください

解決済みの問題

- Windowsネットワーク負荷分散 (NLB) がインストールされ、ユニキャストモードが設定されているコンピュータで侵入防御システムを有効にすると、ネットワーク負荷分散のパフォーマンスが影響を受けることがありました。SF06426122/SEG-169878/DSSEG-7852
- Deep Security Agent 20.0.0-7719でエージェントセルフプロテクションが有効になっている場合、Windowsのシステムログにアクセス違反エラーが表示されることがありました。DSA-1962

既知の問題

- 侵入防御またはWebレピュテーションサービスをDeep Security Agentで有効にすると、TLS検査プロセス(tm_netagent)のエラーログローテーションの問題が発生する可能性があります。詳細については、Deep SecurityにおけるTLS検査プロセスのエラーログローテーションの問題を参照してください。DSA-3773

Deep Security Agent - 20.0.0-7943 (20 LTS Update 2023-09-26)

リリース日: 2023年9月26日

ビルド番号: 20.0.0-7943

強化

- エージェントパターンの更新を正しく表示するには、Deep Security Agent 20.0.0-7943以降がDeep Security Manager 20.0.759+を必要とします。詳細については、Deep Security Agent 20.0.0-7943の非互換エージェント/アプライアンスバージョンエラーを参照してください。SEG-190866/SEG-191017/DSA-1531
- コマンドラインからプロキシ情報を取得するための新しいコマンドが追加されました。`dsa_query -c GetProxyInfo` `dsa_query -c GetProxyInfo details=true`。DSA-864
- Webレピュテーションサービスは、Windows 10 (64ビット)、Windows 11、Windows Server 2016、Windows Server 2019、およびWindows Server 2022のMicrosoft Edge用の「トレンドマイクロツールバー for Enterprise」ブラウザ拡張機能をサポートするようになりました。DSA-1565

解決済みの問題

- セキュリティセキュリティログ監視を有効にすると、Windows Server 2019システムでDeep Security Agentがクラッシュすることがありました。DS-77766

Deep Security Agent - 20.0.0-7719 (20 LTS Update 2023-08-29)

リリース日: 2023年8月29日

ビルド番号: 20.0.0-7719

新機能

新しい言語のサポート: Deep Security Agentでポーランド語とチェコ語がサポートされるようになりました。

機能強化

- スマートスキャンが無効になっている場合、Deep Security Agentでスマートスキャンエージェントパターンがアップデートされなくなり、ネットワーク帯域幅が節約されます。SEG-186625/DSA-1063
- Deep Security Agentでダウンロードされる増分パターンアップデートの数が減り、ネットワーク帯域幅が節約されるようになりました。Deep Security Relayとして設定されているAgentでも、すべてのパターンアップデートがダウンロードされることに注意してください。DSA-1000
- ユーザがブロックされたURLにアクセスしようとしたときにWebレピュテーションサービスがリダイレクトするブロックページをチェコ語またはポーランド語で表示できるようになりました。DSA-444
- Anti-Malware Solution Platform (AMSP) サービスの準備が完了すると、Deep Security Agentによってセキュリティアップデートが自動的に開始されるようになりました。以前は、AMSPの準備が完了する前にセキュリティアップデートが実行されると失敗し、「不正プログラム対策エンジンオフライン」および「Agent/Applianceでのパターンアップデートの失敗」エラーが発生することがありました。DSA-1020

解決済みの問題

- 一部のシステムで、Deep Security Agentサービス (ds_agent) の停止に通常より時間がかかりました。SEG-187365/DSA-1212
- Deep Security Agentで、セキュリティアップデートがスケジュールされていない場合でも、アップデートが実行されることがありました。SEG-187449/DSA-1064
- 不正プログラム対策を有効にすると、Deep Security Agentが一部のサードパーティ製アプリケーションのパフォーマンスに影響を及ぼしました。SEG-182065/DSA-790
- 一部のシステムでDeep Security AgentのCPU使用率が高くなりました。SEG-185563/DSA-756
- デバイスコントロールによって、許可されるはずのWindows Serverストレージエリアネットワーク (SAN) ドライブがブロックされました。SEG-178278/V1E-3895

- 一部のAzure VMで、ネットワークドライバがネットワークインターフェイスに自動的にバインドできませんでした。DSA-1040

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-7976/DSA-1386

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度: 高

Deep Security Agent - 20.0.0-7476 (20 LTS Update 2023-07-25)

リリース日: 2023年7月25日

ビルド番号: 20.0.0-7476

新機能

Deep Security Agentの右クリック検索: Deep Security Agentでは、ファイルまたはフォルダを右クリックして[検索]を選択することで、Windowsのファイルエクスプローラから手動検索を開始できるようになりました。現時点では、この機能を使用できるのは、Trend Vision One EndpointユーザおよびTrend Cloud One - Endpoint&Workloadユーザのみです。

機能強化

- AMSPサービスが正しくインストールされていないために不正プログラム対策がオフラインになっている場合、Deep Security Agentは、エージェントサービスの起動時にAMSPの再インストールを試行するようになりました。DSSEG-7903/SEG-181443
- dsa-connectサービスがアップデートされ、CPUパフォーマンスが向上しました。C1WS-12970
- Deep Security Agentがアップデートされ、Windows 10デスクトッププラットフォーム用のNotifier Anti-Malware Protected Process Light (AM-PPL) サービスがサポートされるようになりました。これには、Deep Security Manager 20.0.789 ~ 20.0.833が必要です。DS-77160

- Windows Server 2012 R2、2016、および2019の高度なTLSトラフィック検査の範囲が改善されました。SEG-182585/DSA-583

解決済みの問題

- Smart Protection ServerとWebレピュテーションサービスとの接続が切断されることがありました。SF06423462/SEG-166651/DSSEG-7858
- 侵入防御が有効になっていると、システムがクラッシュすることがありました。SF06983729/SEG-184423/DSSEG-7907
- Deep Security Managerコンソールから起動されたDeep Security Agentのアップグレードが、一部のシステム設定で失敗し、MSIエラーコード1601:「Windowsインストーラにアクセスできません」を返すことがありました。SEG-177789/DS-78084
- Deep Security Agentは、ネットワークモジュールが有効であっても、モジュールが無効であると報告することがありました(イベントID 1013、Trend Micro LightWeight Driverはすべてのネットワークインタフェースでバインドできませんでした)。SEG-184701/SEG-182649/DSA-686
- Deep Security Agentがアップデートされ、Dell MACアドレスパススルーを使用するシステムがサポートされるようになりました。SEG-177651/DSA-455

Deep Security Agent - 20.0.0-7303 (20 LTS Update 2023-06-28)

リリース日: 2023年6月28日

ビルド番号: 20.0.0-7303

機能強化

- Deep Security Agentでは、fe80:0:0:0:0:0:0:1/24やfe80::01など、CIDRまたは二重コロン表記を使用したIPv6アドレスがサポートされるようになりました。SF04849178/SEG-122076/DS-67280
- Webレピュテーションサービスで、OSのプロキシ設定で使用されるポートが自動的に監視されるようになりました。DS-77233
- 特定のプロセスが暗号化されていない接続を介してバックアップパケットを送信している場合、侵入防御によって検索フローが最適化され、CPUへの影響が軽減されます。SF06456142/SEG-166877/DS-76500

解決された問題

- アプリケーションコントロールがメンテナンスモードのときに、不正ソフトウェアの削除ツール(MSRT)のインストールが失敗することがありました。SF06446534/SEG-172729/DS-77094
- 侵入防御(IPS)が正しいペイロード値を読み取らない場合があり、ルールが誤動作する可能性があります。DS-74647
- Deep Security Agentは、Endpoint Sensorが使用されていない場合でも、ハートビートのたびに「dsa-connect has not provided status」をレポートしていました。C1WS-14696
- 特定の機能が有効になっていると、Deep Security Agentのアップグレードに失敗しました。SF06794868/SEG-177789/DS-78008
- プロキシを使用してDeep Security Managerに接続できないと、Deep Security Agentがクラッシュすることがありました。DS-77786
- アプリケーションコントロールが有効な場合、一部のバージョンのWindowsでMSIファイルのインストールが失敗することがありました。SF06509811/SEG-170485/DS-76906
- Deep Security Relay 20.0.0-7119では、改良されたRelayを使用すると、セキュリティアップデートとソフトウェアアップデートが提供されませんでした。SF06935222/SEG-183184/DS-78201
- 一部のMQTTメッセージが繰り返し送信され、dsa-connectがシャットダウンループでスタックすることがありました。DS-76709

Deep Security Agent - 20.0.0-7119 (20 LTS Update 2023-05-29)

リリース日: 2023年5月29日

ビルド番号: 20.0.0-7119

機能強化

- アプリケーションコントロールを有効にすると、一部のシステムでMSIファイルのインストールが失敗します。SF06509811/SEG-170485/DS-76906
- Agentセルフプロテクションにより、高度なTLS検査プロセス(ds_nuagent)が保護され、管理者権限を持つローカルユーザがこのプロセスを停止できないようになりました。DS-74080

- Deep Security Agent 20.0.0-7119以降では、dsa-connect サービスでFIPSモードがサポートされるようになりました。詳細については、プラットフォームごとのサポート機能を参照してください。C1WS-7467

解決済みの問題

- Deep Security Agentでは、感染した圧縮ファイルに複数の感染ファイルが含まれていても、その圧縮ファイルに対する不正プログラム対策イベントが1つしか報告されませんでした。DS-76339
- 接続を置き換えた後、Deep Security Agentは、最大4分間、以前の接続にまだ接続されているかのようにメトリクスをレポートしました。DS-77453
- TLSトラフィックの詳細検査が有効になっている場合、OSを再起動するとDeep Security Agentが「サービスの停止」画面で停止することがありました。SF06494167/SEG-170082/DS-76880
- 一部のシステムでエージェントのアップデート中にDeep Security Notifierサービス (ds_notifier) が原因でメモリリークが発生しました。SF06454240/SEG-167684/DSSEG-7863

既知の問題

- Deep Security Agent バージョン 20.0.0-6860、20.0.0-6690、または 20.0.0-7119 へのアップグレードを Deep Security Manager コンソールを使用して行うと、アップグレードが失敗することがあります。アップグレードが失敗した後、Deep Security Agent サービスが停止し、マネージャーコンソールから「エージェント オフライン」と表示されることがあります。SEG-177789、SEG-177748、SEG-178496、SEG-178742、SEG-177423、SEG-178470、SEG-178940、SEG-178956

Deep Security Agent - 20.0.0-6860 (20 LTS Update 2023-04-25)

リリース日 : 2023年4月25日

ビルド番号 : 20.0.0-6860

機能強化

- Deep Security Agentがアップデートされ、プロキシプローブの接続タイムアウトを設定できるようになりました。ds_agent.ini. SF06664116/SEG-173848/DS-77182

プロキシプローブラインの例 `ds_agent.ini` 設定ファイル:
`dsa.proxymanager.ProbeTimeoutInSec=120`

- Deep Security Agentが改善され、接続がオンラインのときに「MQTT Connection Offline」警告が誤って送信されないようになりました。SEG-171358 / C1WS-12979
- Deep Security Agentがアップデートされ、MQTTの接続品質が向上し、接続タイムアウトの発生が減少しました。DS-76840
- Deep Security Agentインストーラは、エージェントインストーラで証明書の署名にSHA-1が使用されたことを検出した場合、エージェントをアップデートできないようになりました。これにより、Deep Security Agent 20.0.0-6313以降ではRSA-2048およびSHA-256が必要になるため、エージェントがアップデートされて応答しなくなることがなくなります。証明書のアップグレードの詳細については、「Deep Security暗号化アルゴリズムのアップグレード」を参照してください。DS-76499
- オンデマンド検索が失敗した場合のTrend Micro Deep Security Notifierのエラーメッセージで、より詳細な情報が提供されるようになりました。VO-2132

解決済みの問題

- Deep Security Agentは、Windows 2008プラットフォームでリモートシェル、ファイルコレクション、またはネットワーク隔離を使用するために必要なサードパーティ製ライブラリをロードできませんでした。DS-75176
- Deep Security Agentがシステムの起動時にフリーズすることがあり、Windows Service Control Managerサービスで「開始時にサービスが停止しました」イベント(イベントID 7022) が生成されることがありました。DS-77212
- 不正プログラム対策機械学習型検索を有効にすると、Powershellによって開始されたファイル操作で共有違反が発生することがありました。SF05904706 / SEG-150738 / DSSEG-7695
- Webレピュテーションサービスを有効にすると、Deep Security Agentによって一部のシステムが予期せずシャットダウンしていました。SF06680505 / SEG-174730 / DSSEG-7866
- ドライバの再起動後に、Deep Security Agentがネットワークドライバのステータスを正しくレポートしないことがありました。C1WS-12896

セキュリティ更新

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行

に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-8320/DSSEG-7865

最高共通脆弱性評価システム (CVSS) スコア: 2.9

重大度: 低

Deep Security Agent - 20.0.0-6690 (20 LTS Update 2023-03-29)

リリース日: 2023年3月29日

ビルド番号: 20.0.0-6690

新機能

サービスゲートウェイ: Deep Security Agent 20.0.0-6690以降とDeep Security Manager 20.0.741以降では、転送プロキシ機能を提供するサービスゲートウェイ機能がサポートされるようになりました。

機能強化

- Deep Security Agent のインストールは、オペレーティングシステムが Azure Code Signing (ACS) の要件を満たしているかどうかを確認するための事前チェックを実行するようになりました。詳細については、トレンドマイクロ Server and Endpoint Protection エージェントの最小 Windows バージョン要件 を参照してください。DS-75552
- アプリケーションコントロールで、Microsoft Windowsのコントロールパネルアプレット (.CPL) ファイルの実行がチェックされるようになりました。DS-74587
- アプリケーションコントロールで、Microsoft Compiled HTML Help (.CHM) ファイルの実行がチェックされるようになりました。DS-74828
- アプリケーションコントロールの信頼エンティティのパスルールでファイル名を指定せずにワイルドカードを使用する場合、ワイルドカードは、ルールのパスに一致するディレクトリ内のすべてのファイルに適用されるようになりました。以前は、グロブスター (**) ワイルドカードはパスルールのディレクトリとサブディレクトリに適用され、対照的にシングルスター (*) ワイルドカードはパスルールのディレクトリ内でのみ一致していました。DS-75133
- WebレピュテーションサービスにOSプラットフォームのメタデータが含まれるようになりました。DS-75453

- Deep Security Agent 20.0.0-6690以降では、Proxy Manager for Trend Micro Vision One (XDR) 脅威インテリジェンス - ユーザ定義の不審オブジェクト(UDSO) がサポートされるようになりました。DS-75365
- Deep Security Agentのログシステムがアップデートされ、ユーザの問題をより効率的にデバッグするための追加情報とトレースが提供されるようになりました。Agentはそれぞれ2MBのログファイル (dsa-connect-X.log) を5つ生成します。以前はそれぞれ1MBのログファイルが3つでした。C1WS-9598

  ロガーは、オンデマンドのJSON設定ファイル (dsa-connect.ini または dsa-connect.conf) をサポートし、次の設定オプションを使用できます。
  - Debug: デバッグログメッセージを有効にします (初期設定: false)
  - Count: 生成するログファイルの数 (初期設定: 5)
  - Size: 各ログファイルの最大サイズ (バイト) (初期設定: 2097152)

  設定ファイルの例:

  ```
  { "Debug": true, "Count": 5, "Size": 2097152 }
  ```
- Webレピュテーションサービスのブラウザ拡張機能を使用すると、トレンドマイクロツールバーfor Chromeで、すべてのフレームのコンテンツスクリプトのURLを検査できるようになりました。DS-75387
- SAPScannerによって生成される不正プログラム対策イベントにファイルハッシュが含まれるようになりました。DS-75648/SEG-165491

解決済みの問題

- Deep Security Agentのイベントとモジュールステータスの変更がコンソールに表示されないことがありました。DS-46344/SEG-67100/SEG-101719/SEG-112311
- 不正プログラム対策の「ネットワークディレクトリ検索を有効にする」オプションが有効になっている場合 (コンピュータまたは ポリシー > 不正プログラム対策 > 一般 > リアルタイム検索 > 不正プログラム検索設定 > 詳細 > ネットワークディレクトリ検索))、不正プログラムが検出されましたが、対応するイベントが記録されない場合がありました。SF06198579/SEG-160763/DSSEG-7786
- コンソール(Computer または Policy > 侵入防御 > 一般 > Advanced TLS Traffic Inspection) からAdvanced TLS Traffic Inspection の "Inspect TLS/SSL traffic" オプ

ションが "No" に設定された場合でも、ドライバー側の SSL パケットが処理されることがありました。DS-76160

- Deep Security Agentの侵入防御システムが、「TCP輻輳フラグ」を適切にブロックできないことがありました。DS-76182
- 不正プログラム対策スマートスキャンを有効にすると、IPC接続の問題により一部のシステムがクラッシュしました。SEG-169132/C1WS-10821
- 一部のシステムでの接続の問題を解決するために、Deep Security Agentがアップデートされ、MQTTタイムアウトが30分から2時間に延長されました。C1WS-11835
- Deep Security Agentで、一部のシステムで高度な脅威検索エンジン(ATSE) コンポーネントが削除されたことを示すシステムイベントが誤って生成されていました。SEG-147779/DS-75463
- Agentパッケージに署名がないため、Deep Security Agentのアップグレードが失敗することがありました。SF06045259/SEG-154576/DS-73668
- アプリケーションコントロールは、.HTML、.HTM、および.JSファイルのWebブラウザでの実行をチェックするようになりました。DS-75102
- SOCKSプロキシを使用している場合、Deep Security AgentはHTTP URLに対するWebレピュテーションサービスの評価を提供できませんでした。DS-73482/DS-73364
- ファイル処理に問題があり、アップデート中にファイルを削除できないため、Deep Security Agentのセキュリティアップデートに失敗しました。DS-75907
- Deep Security Agent Scanner (SAP) は、ファイル名に一つ以上の末尾ドット.が含まれるファイルのレポートを生成できませんでした。SF06181341/SEG-166326/DS-76404

既知の問題

- Deep Security Agent 20.0.0-6313以降では、Windows 2008プラットフォームでリモートシェル、ファイルコレクション、またはネットワーク隔離を使用するために必要なサードパーティ製ライブラリをロードできません。Windows 2008システムでこれら3つの機能が必要な場合は、エージェントをアップグレードしないでください。DS-75176
- Deep Security Agent の更新により、いくつかのシステムで Deep Security Manager に不明なエラーイベント(ID: 740) が表示されることがあります。この問題は将来の Deep Security Manager リリースで解決される予定です。詳細については、Deep Security Manager の未認識のエージェント/アプライアンスエラーイベント(イベントID 1010 - 1013) を参照してください。DS-76813

Deep Security Agent - 20.0.0-6313 (20 LTS Update 2023-01-31)

リリース日 : 2023年1月31日

ビルド番号 : 20.0.0-6313

新機能

Windows 10 22H2のサポート: Deep Security Agent 20.0.0-6313以降とDeep Security Manager 20.0.716以降では、Windows 10 22H2がサポートされるようになりました。

機能強化

- Deep Securityでは、SHA-1アルゴリズムで署名された証明書はサポートされなくなりました。エージェントがDeep Security Managerと通信するために、SHA-256を使用して発行されたSSL証明書が必要になりました。C1WS-5676

  警告 : Deep Security AgentとDeep Security Manager間の通信エラーを防ぐために、Deep Security暗号アルゴリズムをアップグレードする手順に従ってください。暗号アルゴリズムをアップグレードする前にDeep Security Agent 20.0.0-6313以降に更新した場合は、OpenSSL 3がSHA-1アルゴリズムの証明書を拒否したときのDeep Security Agentオフラインの手順に従ってください。

- 不正プログラム対策と動作監視を有効にすると、MITRE攻撃シナリオに対する保護を強化するために、Deep Security Agentで不審な動作が監視されるようになりました。この機能を使用するには、Deep Security Manager 20.0.711以降が必要です。DS-73644
- Deep Security Agentがアップデートされ、「Trend Micro Trend ツールバー for Enterprise」Chromeブラウザ拡張機能がサポートされるようになり、Webレピュテーションサービスの HTTPS保護が強化されました。DS-74870

解決済みの問題

- アプリケーションコントロールを有効にすると、Deep Security Agentのステータスが「アプリケーションコントロールルールセットのアップデート中」のままになることがありました。DS-74627
- Deep Security AgentのTLSプロトコルレコードレイヤの問題により、一部のシステムがクラッシュしました。SF06297487 / SEG-162236 / DSSEG-7774

- Deep Security AgentがDeep Security Managerまたはエージェントのコマンドラインツールと通信しているときに、ファイルハンドルリークが発生することがありました。DS-75111
- コンポーネントのアップデートの場合、Deep Security Agentはプロキシを使用する場合と使用しない場合とで試行し、試行ごとにイベントを生成します。イベントレポートをより簡単にするために、この動作が変更され、アップデートが成功した場合、エージェントは最後に成功したイベントのみを表示するようになりました。SF06207160/SEG-160085/DSSEG-7765
- Webレピュテーションを有効にすると、コンソールコマンドに入力された一部の文字が正しく解析されませんでした。たとえば、コマンドに入力されたアンダースコア(_)はダッシュ(-)に置き換えられました、大文字のZが小文字のzに置き換えられました。DS-74335

Deep Security Agent - 20.0.0-5995 (20 LTS Update 2022-11-28)

リリース日:2022年11月28日

ビルド番号:20.0.0-5995

新機能

Windows 11 22H2のサポート: Deep Security Agent 20.0.0-5995以降とDeep Security Manager 20.0.711以降では、Windows 11 22H2がサポートされるようになりました。

機能強化

- WebレピュテーションサービスのHTTPS保護を拡張するChromeブラウザ拡張機能、「トレンドマイクロツールバーfor Enterprise」をサポートするようにDeep Security Agentがアップデートされました。現時点でサポートされているのは、Trend Micro Cloud One - Workload Security ユーザのみです。DS-74568
- Webレピュテーションサービスがアップデートされ、Webブラウザ拡張機能でマルチスレッド処理がサポートされるようになり、クエリ率が向上します。DS-74098
- Deep Security Agentがアップデートされ、コンソールの[イベントとレポート]にコマンドライン挙動監視違反の詳細が追加されました。>イベント>不正プログラム対策イベント DS-72866

解決済みの問題

- ファイルハンドルリークがDeep Security Notifier (notifier.exe) で発生し、システムメモリの使用率が高くなっていました。DS-74325
- Workload Securityで、OSプロキシを有効にすると([管理]→[システム設定]→[プロキシ]で、[設定されたプロキシにアクセスできない場合にAgentによるOSプロキシの適用または直接接続を許可する] を[はい] に設定)、Agentが必要とするプロキシデータがOS側にない場合にDeep Security Agentがクラッシュしていました。SEG-158968/DS-75034
- アプリケーションコントロールをメンテナンスモードで実行しているときに、共有違反により、アクセス可能であったはずの実行可能ファイルがブロックされることがありました。SF04922652 / SEG-131710 / DS-74592
- アプリケーションコントロールは、GitBashシェル(sh.exe) を使用して実行されるスクリプトをブロックできませんでした。DS-73827
- Deep Security Agentにより、古い[ELAMパターンファイル]コンポーネントが[セキュリティアップデート]画面に表示され、セキュリティアップデートのステータスが[最新でない]になりました。このパターンは未使用だったため、常に古いコンポーネントとして表示されていました。SEG-158345 / DSSEG-7745
- Deep Security Agentで、ユーザのグループによって設定されたアクセスレベルよりも高いアクセスレベルが許可されることがありました。たとえば、「Users」グループは、読み取り専用アクセス権がある場合でもファイルを変更できました。SEG-157530 / DSSEG-7737
- 不正プログラム対策を有効にすると、Deep Security AgentドライバによってWindows Server 2008を実行している一部のシステムがクラッシュしました。SF05926337 / SEG-157388 / DSSEG-7739

Deep Security Agent - 20.0.0-5810 (20 LTS Update 2022-10-27)

リリース日 : 2022年10月27日

ビルド番号 : 20.0.0-5810

新機能

インストール済みソフトウェアのレポート: Deep Security Agentは、Microsoft Windowsインストーラの追加の詳細情報とともにインストール済みソフトウェアをレポートするようになりまし

た。これは現在、Trend Micro Cloud One Workload Security ユーザのみが使用できます。

機能強化

- Deep Security Agentがアップデートされ、Webレピュテーションサービス用の追加のメタデータ(UserAgent や Referrerなど) が追加されました。DS-72196
- Deep Security Agentがアップデートされ、エージェント診断パッケージに変更監視データベースが追加されました。DS-73293
- 侵入防御を使用してTLSトラフィックを検査するときにNULL暗号をサポートするようにDeep Security Agentがアップデートされました。DS-71085

解決済みの問題

- 不正プログラム対策 挙動監視が有効になっている場合、Deep Security Agent 20.0.0-5761 のアンインストールまたはアップグレードにより、一部のシステムがクラッシュすることがありました。詳細については、Deep Security Agent 20.0.0-5761 のアンインストール中に発生したBSODをご覧ください。DS-74322
- セキュリティログ監視を有効にすると、Deep Security Agentで「異常な再起動の検出」イベントが生成されることがありました。SF05951130 / SEG-151372 / DS-73737
- アプリケーションコントロールをメンテナンスモードで実行中にDeep Security Agentサービスが停止すると、サービスの停止後に作成された実行可能ファイルが意図したとおりに自動承認されませんでした。SF05961688 / SEG-152045 / DS-73570
- アプリケーションコントロールでメンテナンスモードが有効になっているときにソフトウェアの名前を変更またはコピーした場合、ソフトウェアインベントリでは元のファイル名または場所で認証されたままになります。DS-74015
- vMotionを使用する仮想マシンが予期せずに無効化され、「オフライン(要アクティベート) 」ステータスが表示されることがありました。SEG-153050 / DS-73807
- Edge Relayを使用して、TLSインスペクションサポートパッケージをDeep Security Agentにダウンロードできませんでした。DS-73789
- アプリケーションコントロールインベントリ作成の進行中、エージェントがオフラインとして表示されることがありました。DS-72189

既知の問題

- Windows上でDeep Security Agent 20.0.0-5761を20.0.0-5810にアップグレードした後、コンピュータがクラッシュする問題を解決するために再起動が必要です。問題の回

避策を含む詳細については、Deep Security Agent 20.0.0-5761のアンインストール中に発生したBSODを参照してください。DS-74383

Deep Security Agent - 20.0.0-5512 (20 LTS Update 2022-09-22)

リリース日:2022年9月22日

ビルド番号:20.0.0-5512

機能強化

- Deep Security Agentで、OSライブラリの変更に応じたAdvanced TLS Traffic Inspectionの自動アップデートがサポートされるようになりました([コンピュータ] または [ポリシー] > [設定] > [TLS検査パッケージのアップデート])。これには、Deep Security Manager 20.0.677以降が必要です。DS-72828

解決済みの問題

- 変更監視イベント(イベントとレポート>変更監視) が作成され、[KEY] 列と[TYPE] 列に「N/A」と表示されました。SF05533287/SEG-139293/DS-71899
- Deep Security Agentをアップデートして期限切れのTLSセッションキーを削除すると、一部のシステムがクラッシュしていました。SF06007238 / SEG-153175 / DS-73404
- 不正プログラム対策を有効にすると、一部のコンピュータが「セキュリティアップデートを実行中」の状態でフリーズします。SF05106626/SEG-129777/DSSEG-7500
- Deep Security Agentのセルフプロテクションが有効になっている場合、高度なTLS検査サービスを有効または無効にすると、WindowsサービスControl Managerで「イベントID 7006」が発生しました。DS-73305
- Deep Security Agentから予期しない形式のホストメタデータが報告されました。DS-73411

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-8100/VRTS-8101/DS-73087/DS-72528

最高共通脆弱性評価システム (CVSS) スコア: 7.0

最高の重大度 : 高

Deep Security Agent - 20.0.0-5394 (20 LTS Update 2022-08-29)

リリース日 : 2022年8月29日

ビルド番号 : 20.0.0-5394

機能強化

- アプリケーションコントロールで、実行可能でない拡張子を持つ実行可能ファイルのソフトウェア変更が検出されるようになりました。DS-70805
- 診断パッケージの生成時に収集される情報に、WindowsのSYSTEMユーザネットワークドライブとマウントポイントを追加しました。DS-71816
- Deep Security Agentがアップデートされ、TLS接続での動的ポートを使用したパケット検査のサポートが追加されました。DS-71078
- AppLockerで作成されたテストPowerShellスクリプトをアプリケーションコントロールが自動的に認証するようにDeep Security Agentがアップデートされました。DS-71762
- 挙動監視の除外でワイルドカード文字がサポートされるようになりました。DS-71976
- Deep Security Agentがアップデートされ、高度なTLS検査のメトリックがさらに追加されました。DS-72833

解決済みの問題

- 動的ポートを使用したUDP接続でTLS検査を実行すると、OSがクラッシュすることがありました。SEG-151169 / DS-73043
- 一致または正規表現フィールドで変数に「$」文字を使用すると、セキュリティセキュリティログ監視エンジンがオフラインになる問題を修正しました。SEG-146965 / SEG-146966 / DS-72325
- 新しいゲスト仮想マシンに対してリアルタイム不正プログラム対策をオフにしたポリシーを割り当てると、同じDeep Security Virtual Applianceに登録されている他のすべてのゲスト仮想マシンに対して、リアルタイム不正プログラム対策がオフになることがありました。SEG-146057 / DS-72856
- 挙動監視を有効にすると、Deep Security AgentによってWindows上のDockerが起動しなくなることがありました。SF05709278 / SEG-146323 / DSSEG-7660

- アプリケーションコントロールは、メンテナンスモード中もネットワークファイルへのアクセスをブロックしていました。SF04922652 / SEG-131710 / DS-72037
- アプリケーションコントロールが有効な場合、Adobeプラグインで予期しないセキュリティイベントが生成されていました。SF05823607 / SEG-148570 / DS-72679
- Deep Security Agentは、Windowsで接続メトリックやログイベントについて不正なPID情報を取得することがありました。DS-72526
- エージェントのアップデート中に特定の設定ファイルをロードすると、Deep Security Agentで「リビジョンの不一致(-10039)」エラーが返されていました。DS-72499
- アプリケーションコントロールインベントリの検索が完了する前に、Deep Security Agentがソフトウェアの変更の検出をレポートしていました。DS-72071
- 不正プログラム対策がクラスタ共有ボリューム上のファイルにアクセスすると、Hyper-Vホストがクラッシュしていました。SF05713918 / SF05850687 / SEG-146660 / SEG-148664 / DSSEG-7664

既知の問題

- 複数のカスタムスクリプトタスクを実行すると、新しいタスクは以前の未完了のタスクによって上書きされます。カスタムスクリプトタスクを1つずつ実行して、この問題を回避できます。この問題は、今後のリリースで修正される予定です。DS-72699

Deep Security Agent - 20.0.0-5137 (20 LTS Update 2022-07-26)

リリース日:2022年7月26日

ビルド番号:20.0.0-5137

新機能

高度なTLSトラフィック検査: Deep Security Agent 20.0.0-5137以降では、システムアップデートまたはパッケージアップデートを実行するプラットフォームに高度なTLSトラフィック検査のサポートが追加されます。現在、この機能はTrend Micro - Cloud One Workload Securityでのみサポートされています。Deep Security Manager(オンプレミス)のサポートは今後追加される予定です。

機能強化

- Deep Security Agent 20.0.5137以降のWindowsでは、追加の証明書「Microsoft Identity Verification Root Certificate Authority 2020」を使用します。詳細については、Deep SecurityおよびTrend Cloud One - Endpoint & Workload SecurityでのVeriSign、DigiCert、USERTrust RSA証明書の更新を参照してください。DS-72711
- Deep Security Agent Scanner (SAP) で、追加の詳細を含む感染レポートが生成されるようになりました。DS-71660
- 送信接続の「ゼロ設定」SSLプロセスを改善するためにDeep Security Agentがアップデートされました。DS-70715
- Deep Security Agentがアップデートされ、信頼エンティティの機能が向上しました。信頼ルールのワイルドカードサポートに、多くのサブディレクトリに一致するglobstar `\*\*` が含まれるようになりました。Single star `\*` は現在のディレクトリ内でのみ一致します。Single star `\*` を使用して多数のフォルダを照合していた既存のルールは機能しなくなり、globstar `\*\*`を使用するように変更する必要があります。DS-71817

解決済みの問題

- 不正プログラム対策を有効にすると、Deep Security Agentでドライバの競合が発生し、一部のサードパーティ製アプリケーションがフリーズします。SF05570686/SEG-140749/DSSEG-7650
- Deep Security AgentのScanner (SAP) ライブラリのインストールが、ホストに必要な証明書が最新でないために失敗することがありました。DS-71917
- Deep Security Agent SAP ScannerでMIME(.TTF) ファイルを検出できませんでした。DS-55897
- 特定の設定の組み合わせを持つ侵入防御ルールをコンパイルできませんでした。DS-71889

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性からどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-7102/VRTS-7070/VRTS-7041/VRTS-7039/DSSEG-7636

最高共通脆弱性評価システム (CVSS) スコア: 4.4

重大度:中

既知の問題

- 複数のカスタムスクリプトタスクを実行すると、新しいタスクは以前の未完了のタスクによって上書きされます。カスタムスクリプトタスクを1つずつ実行して、この問題を回避できます。この問題は、今後のリリースで修正される予定です。DS-72699

Deep Security Agent - 20.0.0-4959 (20 LTS Update 2022-07-04)

リリース日:2022年7月4日

ビルド番号:20.0.0-4959

解決済みの問題

- Deep Security Agentにより、WMIプロバイダサービス(WmiPrvSE.exe) を実行しているシステムのCPU使用率が増加しました。05528968 / SEG-142736 / DS-71626
- Deep Security Agent Scanner (SAP) レポートに、.SARファイルが間違った順序で表示されました。DS-71651
- Deep Security Agentで競合が発生したため、TMUMHドライバがロードされず(Windows 11およびWindows 2022) 、場合によってはシステムクラッシュが発生しました(すべてのWindowsプラットフォームに影響します) 。SEG-143164 / DSSEG-7596
- コマンドライン(`dsa_control -b`) を使用すると、Deep Security Relay が、閉じたネットワーク環境でのアップデートに必要なバンドルファイルの抽出に失敗しました。SF05715642 / SEG-144571 / DSSEG-7600
- Deep Security Agent 20.0.0-4726へのアップデートで、セキュリティログ監視を有効にすると、「Get Events Failed」および「Command Not Found」アラートが発生しました。SF05738607 / SEG-145679 / DS-72117
- 不正プログラム対策と変更監視が有効になっている場合、Deep Securityエージェントが高いCPU使用率を引き起こしました。SF05169148/SEG-129522/DS-69594
- 不正プログラム対策を有効にすると、ソフトウェアのアップグレード後のサービスの再起動によって、Deep Security Agentで「不正プログラム対策 エンジンがオフライン」エラーが生成されました。SF05521775 / SEG-144639 / DSSEG-7615

- 不正プログラム対策を有効にすると、Deep Security Agentがシステムクラッシュやシステムメモリ使用率の増加を引き起こしたり、イベントレポートの配信に失敗したりすることがありました。SF05475742 / SEG-142632 / DSSEG-7626
- アプリケーションコントロールのメンテナンスモードがエージェントで有効になっている場合に、ただちにDeep Security Managerにステータスを報告するようにDeep Security Agentがアップデートされました。DS-71617
- Deep Security Agentで、「無効」または「不正な形式」のプロキシURLを参照する不明確なエラーログエントリが作成されることがありました。SEG-144613 / DS-71866

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-7633/DS-71687

最高共通脆弱性評価システム (CVSS) スコア: 6.2

最高の重大度 : 中

Deep Security Agent - 20.0.0-4726 (20 LTS Update 2022-05-31)

リリース日 : 2022年5月31日

ビルド番号 : 20.0.0-4726

機能強化

- Deep Security Relay がアップデートされ、潜在的なトラブルシューティングに備えてステータスとその他のメトリックが記録されるようになりました。DS-65763

解決済みの問題

- 信頼エンティティの「許可対象別」ルールで、ブロックする予定のないプロセスがブロックされることがありました。SF04922652/SEG-131710/DS-71060
- 一部の設定で、Deep Security Agentによって「作成/削除」の変更監視イベントの誤検出が報告されました。SF05434164 / SEG-136425 / DS-70656

- Deep Security Agent がパッケージの不完全な署名ファイルを取得しないように、Deep Security Relay を更新しました。SF05332854/SEG-134394/DS-71228
- サーバ名インジケータ(SNI) で無効な形式を使用すると、Deep Security Agentで接続の問題が発生していました。SEG-127761 / DS-70806
- Deep Security Agentの異常な再起動により、「不正プログラム対策エンジンがオフライン」エラーが発生することがありました。SEG-140234 / DS-71333
- 侵入防御を有効にすると、一部のシステムでパケット転送エラーが発生してクラッシュしていました。SEG-136843 / DSSEG-7524

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-7090/DSSEG-7541/DS-52329

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度 : 高

Deep Security Agent - 20.0.0-4416 (20 LTS Update 2022-04-28)

リリース日 : 2022年4月28日

ビルド番号 : 20.0.0-4416

機能強化

- Deep Security Agentがアップデートされ、「Bypass Network Scanner」ルールが適用された場合の侵入防御のパフォーマンスが向上しました。DS-69515
- 一部のシステム設定でWindows Defenderをパッシブモードで実行中に不正プログラム対策モジュールの有効化をサポートするようにDeep Security Agentがアップデートされました。DS-69161。現在、これは次のバージョンを実行しているシステムでのみサポートされています。

- Defender(AM) 製品/エンジンのバージョン:
  - AMProductVersion:4.18.2202.4
  - AMEngineVersion:1.1.18900.3
- Windowsサーバおよびデスクトップバージョン:
  - Windows Server 2016以降
  - Windows 10 x64 RS5以降
- Deep Security Agent 20.0.0-4416以降

解決された問題

- 一部のシステム設定で、Deep Security Agentがエージェントのアップグレード中に複数の「不正プログラム対策エンジンがオフライン」イベントを生成していました。SF04500910 / SEG-129316 / DSSEG-7458

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-7132/DS-70518

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度:高

Deep Security Agent - 20.0.0-4185 (20 LTS Update 2022-04-06)

リリース日:2022年4月6日

ビルド番号:20.0.0-4185

新機能

Advanced TLSトラフィック検査:Advanced TLSトラフィック検査により、Perfect Forward Secrecy(PFS) などの最新の暗号で暗号化されたTLSトラフィックを検査する機能が追加されます。また、HTTPSサーバの仮想パッチも強化され、Log4jなどの脆弱性に対する保護に役立ちます。

強化

- Deep Security Agentがアップデートされ、Windowsのアップグレード時に加えられたソフトウェア変更に対してアプリケーションコントロール設定が適切に実行されるようになりました。これまで、Windowsのアップグレードに関連するソフトウェアの変更を自動承認する信頼ルールは、アプリケーションコントロールがロックダウンモードの場合に失敗していました。DS-69579
- 不正プログラム対策インストールの証明書が見つからない場合、Deep Security Agentは証明書の詳細をDeep Security Managerに転送するようになりました。不足している特定の証明書は、Managerの [イベントとレポート] > [システムイベント] に表示されます。DS-69074

解決済みの問題

- コマンドラインを使用して不正プログラム対策の手動検索を実行すると、Deep Security Agentが受信接続を受信できなくなることがありました。SF05385865 / SEG-135256 / DS-70364
- Deep Security Agentでは、Agentのアップグレード中に「アプリケーションコントロールエンジンオフライン」エラーが生成され、アップグレードの完了後に「アプリケーションコントロールエンジンのオンライン復帰」というメッセージが表示されていました。アップグレードによってこれらのイベントがトリガされるべきではありませんでした。DS-69888
- メンテナンスモードで実行している場合でも、アプリケーションコントロールが認識できないソフトウェアをブロックすることがありました。SF05234969 / SEG-133594 / DS-69752
- Deep Security Agentは、ポリシーのアップデート中に大量のシステムリソースを消費することがありました。SEG-134417 / DS-69810

Deep Security Agent - 20.0.0-3964 (20 LTS Update 2022-03-01)

リリース日 : 2022年3月1日

ビルド番号 : 20.0.0-3964

新機能

脅威インテリジェンス: 脅威インテリジェンス (旧称Connected Threat Defense) は、新たな脅威に対するマルウェア対策を強化します。詳細については、「脅威インテリジェンスを使用して新たな脅威を検出する」を参照してください。

機能強化

- 侵入防御イベントの[元のIP (XFF)]フィールドから文字列内の不審な文字(`$`など)を除外するようにDeep Security Agentがアップデートされました。SEG-129905/DS-68989

解決済みの問題

- Deep Security Agentは、セルフプロテクションのパスワードの検証に失敗した場合でも、ポリシーの変更パラメータを受け入れていました。SF05177188/SEG-129643/DS-69293
- Deep Security Agentが有効化後に予期せずオフラインになることがありました。SEG-130280
- 侵入防御が有効になっていると、SSL接続の確立で「サポートされていないSSLバージョン」イベントが発生していました。SF04955719/SEG-127437/DS-68689
- Deep Security Agentで予期しない「ログファイル削除エラー」システムイベントが生成されていました。DS-69641
- Deep Security Agentで、不要なユーザ(作成/削除)またはグループ(追加/削除/アップデート)イベントが作成されることがありました。DS-62413

Deep Security Agent - 20.0.0-3771 (20 LTS Update 2022-01-24)

リリース日:2022年1月26日

ビルド番号:20.0.0-3771

新機能

ゼロ設定IPS検査: Deep Security Agentに、証明書を手動でインポートせずにTLS暗号化トラフィックを検査する侵入防御の機能が追加されました。これにより、より多くの暗号スイートのサポートも追加されます。この機能は、Trend Micro Cloud One - Workload Securityのお客さまを始めとして、Windowsプラットフォーム向けに段階的に展開されています。

Windows 21H2のサポート: Deep Security Agent 20.0.0-3771以降でWindows 21H2がサポートされるようになりました。

機能強化

- Deep Security AgentがアップデートされDeep Security ManagerがTLS 1.2の強力な暗号を使用している場合に侵入防御からDeep Security Managerに接続できるようになりました。DS-69042

解決済みの問題

- Windows 11でプロキシアドレスに予期せず「http://」プレフィックスが追加されると、Deep Security Agentとプロキシをペアリングできませんでした。このプレフィックスは、LAN設定画面 (コントロールパネル > ネットワークとインターネット > インターネットオプション > 接続 > LAN設定) からアドレスにアクセスし、[OK] を選択して画面を閉じた場合に追加されました。DS-68568
- 不正プログラム対策 がアップデート中にオフラインの場合、Deep Security Agentのセキュリティアップデートが失敗し、「AMSP」イベントが生成されました。SF04696674 / SEG-120215 / DSSEG-7287
- アプリケーションコントロール、不正プログラム対策、およびリアルタイムの変更監視 が、特定の組み合わせの 変更監視 ルールを持つDeep Security Agentで正常に機能しませんでした。DS-68494
- Deep Security Agentがアップデートされ、リアルタイムの 不正プログラム対策 検索の初期設定で「書き込み遅延検索」が有効になるため、応答時間が長くなり、処理が速くなり、CPU使用率が低下します。以前は、初期設定ではすべてのファイルが読み取り/書き込み時に検索されていました。今後は書き込み時の 不正プログラム対策 ファイルの検索が遅延されます(ファイルはキューに追加され、バックグラウンドで検索されます) 。DS-66344
- スマートスキャン が有効になっていると、Deep Security Agentは、セキュリティアップデート中に予期された差分アップデートファイルではなく、フルサイズのパターンファイルアップデートファイルをダウンロードしていました。SEG-124937/ DSSEG-7317

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-6187/DS-65070/DS-68180

最高共通脆弱性評価システム (CVSS) スコア: 9.1

最高の重大度:高

Deep Security Agent - 20.0.0-3530 (20 LTS Update 2021-12-15)

リリース日:2021年12月15日

ビルド番号:20.0.0-3530

新機能

- OSプロキシのサポート: Deep Security Agent 20.0.0-3530以降 (Windows版) では、コンピュータのOSからプロキシ設定を適用して、Trend Micro Cloud One - Workload Security、Deep Security Relay、およびその他のトレンドマイクロバックエンドサービスに自動的に接続できるようになりました。エージェントが設定したプロキシの接続が失われました。現時点では、この機能を利用できるのは特定のWorkload Securityユーザのみです。

重要な注意事項

- 現在Windows 11で、プレフィックス「http://」にアクセスし ([コントロール パネル]→[ネットワークとインターネット]→[インターネットオプション]→[接続]→[LAN設定])、[OK] を選択してウィンドウを閉じた後、そのプレフィックスがプロキシアドレスに予期せず追加された場合、Deep Security Agentとプロキシのペアリングが失敗します。この問題は、今後のリリースで修正される予定です。DS-68568

解決された問題

- スマートスキャンが有効になっていると、Deep Security Agentは、セキュリティアップデート中に予期された差分ファイルではなく、フルサイズのパターンファイルアップデートファイルをダウンロードしました。DSSEG-7317

Deep Security Agent - 20.0.0-3445 (20 LTS Update 2021-11-24)

リリース日:2021年11月24日

ビルド番号:20.0.0-3445

新機能

- 不正プログラム対策オフライン予約検索: Deep Security Agent 20.0.0-3445以降では、オフライン予約検索機能が追加され、エージェントがCloud One Workload Securityに接続されていないときに不正プログラム対策予約検索を実行できるようになりました。現時点では、この機能を利用できるのはCloud One Workload Securityの一部のユーザのみです。
- Windows 11のサポート: Deep Security Agent 20.0.0-3445以降でWindows 11がサポートされるようになりました。
- Windows Server 2022のサポート: Deep Security Agent 20.0.0-3445以降でWindows Server 2022がサポートされるようになりました。

機能強化

- Deep Security Agentがアップデートされ、Deep Security Notifierをロックして(コマンドプロンプトから`msiexec /I "Notifier's installer name" LockAppSettingsDefault=1`を使用してインストールした場合)ユーザが通知を非表示にできないようになりました。DS-64527
- Deep Security Managerに接続できない場合、Deep Security Agentがクラッシュすることがありました。DS-67654
- Deep Security Agentでは、セキュリティ強化のために初期設定でCBC暗号スイートが使用されなくなりました。DS-67204
- Deep Security Agentがアップデートされ、Cloud One Workload Securityのアプリケーションコントロール信頼エンティティの「ソースから無視」ルールの「プロセス名」プロパティの使用がサポートされるようになりました。DS-67322
- Deep Security Agentのデータベースサイズ管理がアップデートされ、ディスク容量の使用が最適化されました。DS-67347

解決済みの問題

- 不正プログラム対策を有効にすると、一部のシステムでDeep Security Agentによってサードパーティ製ソフトウェアの接続の問題が発生していました。SF04087024 / SEG-125579 / DSSEG-7321
- アップグレードが成功した場合でも、アップグレード中にDeep Security Agentでプラグインのインストールが失敗することがありました。DS-67336

- 期限切れの証明書がホストから削除されると、不正プログラム対策プラグインのアップデートが失敗し、「不正プログラム対策 コンポーネントアップデート」イベントが作成されました。SEG-117871 / DS-66139
- Deep Security Agentでのモジュールのインストールが完了する前に不正プログラム検索 が開始された場合、再起動後にシステムがクラッシュし、「不正プログラム対策 エンジンがオフライン」エラーが発生することがありました。SEG-108355 / DS-63721
- Deep Security Agentは、先頭と末尾にスペースが含まれるSAP NetWeaver MIMEタイプの検索要求を適切に処理できませんでした。DS-67448
- Windows Active Directoryドメインコントローラ上のDeep Security Agentに対して、「UserSet」または「GroupSet」を使用する変更監視ルールを有効にすると、CPUとメモリが過剰に消費されることがありました。Deep Security Agent 20.0.0-3445では、Windows Active Directoryドメインコントローラでこれらの種類の変更監視ルールがブロックされ、「適用変更監視ルール」イベントが生成されます。DS-65965

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある情報公開の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-6489/DSSEG-7210/DS-65113/VRTS-6207/DSSEG-7026

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度: 高

Deep Security Agent - 20.0.0-3288 (20 LTSアップデート2021-10-28)

リリース日: 2021年10月28日

ビルド番号: 20.0.0-3288

新機能

- Agentインストーラの進化: Deep Security Agentインストーラは、ほとんどのAgentコンテンツをインストールするようになりました。これにより、次の変更が行われます。

- ほとんどのプラットフォームのインストーラパッケージが若干大きくなるなど、エージェントのサイズ要件が大きくなりました。
- 保護対象のコンピュータにすべてのエージェントコンテンツがインストールされます。ポリシーまたはManagerコンソールによってプラグインが有効化されるまで、コンピュータ上のコンテンツはアンロードされたままになります。
- すべてのプラグインインストールで、エージェントにすでにインストールされているコンテンツが使用されるため、エージェントがRelayに依存することが大幅に減少しました。これにより、Relayに接続せずにプラグインをインストールできるため、Relay通信によるプラグインのインストールの問題が軽減されます。

解決済みの問題

- Deep Security Agent 20.0.0-3165で、コンピュータでセキュリティアップデートを実行すると、「不正プログラム対策コンポーネントのアップデート失敗」イベントが生成されることがありました。この問題は、Deep Security Agent 20.0.0-3288で修正されました。SF04937346 / SEG-122765 / DSSEG-7268
- 侵入防御を有効にすると、Deep Security AgentでCPU使用率が高くなり、システムがクラッシュすることがありました。DS-65902
- 侵入防御が有効になっていると、一部の設定でDeep Security Agentによってシステムがクラッシュする問題がありました。SF04931669 / SEG-123338 / DS-67441
- SAPが統合され実行されている場合、Deep Security AgentはMP4ファイルをブロックしていました。04660120 / SEG-117094 / DSSEG-7254
- Deep Security Agentがプロキシ経由でManagerに接続できないことがありました。DS-65929
- Deep Security Agentが不正プログラム対策コンポーネントの実行時ステータスをクエリすると、CPU使用率が急増する問題がありました。DSSEG-7222
- Deep Security Agentは、Managerとの接続を初期化する前にメタデータの準備ができていることを常に確認するわけではありませんでした。DS-51103
- 証明書失効リスト(CRL)が一致しないため、アップグレード中にDeep Security Agentでパッケージ署名エラーが表示されることがありました。DS-65056

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行

に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。DS-46018/DSSEG-7210/DSSEG-7217

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度: 高

Deep Security Agent - 20.0.0-3165 (20 LTSアップデート2021-10-08)

リリース日: 2021年10月8日

ビルド番号: 20.0.0-3165

注意: Deep Security Agent 20.0.0.3165がTrend Micro Cloud One - Workload Securityユーザにリリースされました。ただし、Deep Security Agentソフトウェアのダウンロードページからは入手できず、Deep Security Managerを使用しているユーザにはリリースされません。

新機能

- Agentインストーラの進化: Deep Security Agentインストーラは、ほとんどのAgentコンテンツをインストールするようになりました。これにより、次の変更が行われます。
  - ほとんどのプラットフォームのインストーラパッケージが若干大きくなるなど、エージェントのサイズ要件が大きくなりました。
  - 保護対象のコンピュータにすべてのエージェントコンテンツがインストールされます。ポリシーまたはManagerコンソールによってプラグインが有効化されるまで、コンピュータ上のコンテンツはアンロードされたままになります。
  - すべてのプラグインインストールで、エージェントにすでにインストールされているコンテンツが使用されるため、エージェントがRelayに依存することが大幅に減少しました。これにより、Relayに接続せずにプラグインをインストールできるため、Relay通信によるプラグインのインストールの問題が軽減されます。

解決済みの問題

- Deep Security Agentがプロキシ経由でManagerに接続できないことがありました。DS-65929

- Deep Security Agentが不正プログラム対策コンポーネントのランタイムステータスをクエリすると、CPU使用率が急増することがありました。DSSEG-7222
- Deep Security Agentは、Managerとの接続を初期化する前に、メタデータの準備ができていることを常に確認していました。DS-51103

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。DSSEG-7210/DSSEG-7217

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度: 高

Deep Security Agent-20.0.0-2921(20 LTS Update 2021-08-30)

リリース日: 2021年8月30日

ビルド番号: 20.0.0-2921

新機能

国勢調査のフィードバック: Deep Security Agent 20.0.0-2921以降では、トレンドマイクロスマートフィードバックが有効になっている場合に、国勢調査ファイルのフィードバックをSmart Protection Network (SPN) に送信できるようになりました ([システム設定] [>スマートフィードバック])。

機能強化

- Deep Security Agentがアップデートされ、「HiveNightmare」攻撃コードが検出されるようになりました。DS-65217

解決済みの問題

- アプリケーションコントロールを有効にすると、.MSIファイルの起動時にDeep Security Agentがクラッシュすることがありました。SF04647983 / SEG-114894 / DSSEG-7032

- Deep Security Agentコンソールのコマンドで、Deep Security Relay またはDeep Security Managerのプロキシ情報が返されないことがありました。DS-65419
- Deep Security Agentで、[イベントとレポート]の項目が正しく表示されないことがありました。DSSEG-7057

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性からどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。DSSEG-7046/DS-65668

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度: 高

Deep Security Agent-20.0.0-2740(20 LTS Update 2021-07-29)

リリース日: 2021年7月29日

ビルド番号: 20.0.0-2740

強化

- Deep Security Agentがアップデートされ、TLSトラフィックの検査が改善されました。この機能は、Trend Micro Cloud One (Workload Security) のユーザから段階的に公開されています。DS-15576
- Deep Security Agentがアップデートされ、Agentの配信時および有効化時のDeep Security Managerとの接続が改善されました。DS-62547

解決済みの問題

- アプリケーションコントロールを有効にすると、Deep Security Managerコンソールで「.tmp」という拡張子の付いたファイルによって「アプリケーションコントロールソフトウェアの変更の検出」イベントが大量に生成されていました。04671615/ SEG-115017 / DS-65043

- Deep Security Agentで、Agentから開始される(dsa_control) コンソールコマンドの一部を実行できませんでした。04564385 / SEG-112050 / DSSEG-6990
- Deep Security Managerとの接続の確立中に、Deep Security Agentがクラッシュすることがありました。04634804 / SEG-113539 / DS-64862
- SSL接続の確立中に、Deep Security Agentの接続が切断されることがありました。SF04323898 / SEG-107451 / DS-64268
- 古いバージョンのOSを使用しているシステムでは、Deep Security AgentがWebアプリケーションに接続できないことがありました。SF04451029 / SEG-109652 / DS-64528
- Webレピュテーションを有効にすると、Deep Security Agentによって一部のサードパーティソフトウェアで接続の問題が発生しました。SF04072723/SEG-97952/DSSEG-6963

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。SF04613197/SEG-113566/DS-64050

最高共通脆弱性評価システム (CVSS) スコア: 9.8

最高の重大度 : 高

Deep Security Agent-20.0.0-2593(20 LTS Update 2021-07-01)

リリース日 : 2021年7月1日

ビルド番号 : 20.0.0-2593

解決された問題

- Deep Security Agentは、エージェントとマネージャーの通信の問題が原因で、複数の「セキュリティログ監視 エンジン初期化」アラートをトリガーすることがありました。SF03968169 / SEG-95731 / DS-60840
- ディープセキュリティエージェントで アプリケーションコントロール を有効にした後、不正プログラム対策 がオフラインになることがありました。SF04532752 / SEG-110572 / DS-63406

- アプリケーションコントロールは、PowerShellによって生成された「.tmp」ファイルが原因で複数の「アプリケーションコントロール ソフトウェア変更が検出されました」イベントを検出していました。C1WS-1608
- Citrix Virtual AppまたはDesktopユーザーは、不正プログラム対策 がDeepSecurity Agentに対して有効になっていると、灰色の画面(エラーコード1003/1005) が発生することがありました。DS-64318
- 不正プログラム対策 は、Windows WMIサービスがファイルに繰り返しアクセスすると、システムのCPU使用率が高くなることがありました。SEG-109271 / DSSEG-6983

セキュリティアップデート

このリリースには セキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-5850/DS-54705

最高共通脆弱性評価システム (CVSS) スコア: 4.4

最高の重大度 : 中

Deep Security Agent-20.0.0-2419(20 LTS Update 2021-06-02)

リリース日 : 2021年6月2日

ビルド番号 : 20.0.0-2419

解決済みの問題

- Deep Security Agent 20.0.0-2395 for Windows は常に「期限切れ」のセキュリティ更新 ステータスが表示されていました。このエージェントはトレンドマイクロ Download Centerから削除されました。詳細についてはDeep Security Agent 20.0.0-2395 for Windows の削除を参照してください。SF04537047/SEG-110737/DS-63424
- 変更監視のアラートがトリガされても、[イベントとレポート] タブに表示されないことがありました。04266346/SEG-103731/DS-62992
- 不正プログラム対策 スキャンのキューに入れられたアイテムにより、通常のDeep SecurityAgentのCPU使用率よりも高くなることがありました。DS-63106

- アップグレード失効リスト(CRL) が一致していないため、Deep Security Agentでパッケージシグネチャエラーが発生することがありました。DS-62154
- 接続の問題が原因でホスト情報が不十分な場合、AWSワークスペースのDeep SecurityAgentの Computers タブにオフラインまたは重複したリストが表示されることがありました。SF04198134 / SEG-102818 / DS-61666
- Deep Security Agent は、パッケージが見つからないためにアップグレードに失敗することがあります。SF04302125/SEG-104084/DS-62692

Deep Security Agent - 20.0.0-2204 (20 LTS Update 2021-04-12)

リリース日 : 2021年4月12日

ビルド番号: 20.0.0-2204

解決済みの問題

- アプリケーションコントロールがブロックモードの場合、場合によっては適切なソフトウェアインベントリを作成できませんでした。DS-58813
- Webレピュテーションが有効になっていると、システムがクラッシュすることがありました。SF04258834 / SEG-102756 / DS-61067
- 不正プログラム対策セルフプロテクションが有効になっていると、サードパーティのソフトウェアをインストールできないことがあります。SEG-101840 / DSSEG-6694
- 挙動監視の除外が正しく機能しない場合があります。SF03775351 / SEG-89899 / DSSEG-6718
- 不正プログラム対策が有効になっていると、一部のシステムでネットワーク転送速度が著しく低下します。SF04299217 / SEG-103986 / DSSEG-6780
- 不正プログラム対策の挙動監視の除外が正しく機能しない場合があります。SF04259521 / SEG-102792 / DSSEG-6714

Deep Security Agent - 20.0.0-2009(20 LTSアップデート2021-03-08)

リリース日 : 2021年3月8日

ビルド番号 : 20.0.0-2009

機能強化

- CPU情報(論理コア数)を含めるようにDeep Security Agentがアップデートされ、診断とパフォーマンスの追跡が改善されました。DS-60011

解決された問題

- 古いMQTT接続が適切にクリーンナップされなかったため、MQTT接続はオフラインになりました。SF04236908/SEG-102056/DS-60893
- 挙動監視は、イベントを生成せずにプログラムをブロックすることがありました。SF03604820/SEG-86752/DS-60526
- 不正プログラム対策が有効にされたときに、大量のCPUが使用されました。SF04106889/SEG-99034/DS-60526
- Deep Security Agentは、不正プログラム対策の手動検索中にクラッシュすることがあります。SEG-100231/DSSEG-6664

Deep Security Agent - 20.0.0-1876 (20 LTS Update 2021-02-08)

リリース日: 2021年2月8日

ビルド番号: 20.0.0-1876

解決済みの問題

- 侵入防御をパッシブモードで実行していると、Deep Security Agentがクラッシュすることがありました。DS-57497

Deep Security Agent - 20.0.0-1822(20 LTSアップデート2021-01-18)

リリース日: 2021年1月20日

ビルド番号: 20.0.0-1822

解決済みの問題

- Windows Updateが実行されると、[メンテナンスモード]アプリケーションコントロールが自動的に無効になりました。SF03905860/SEG-93631/DS-58413

Deep Security Agent - 20.0.0-1681(20 LTSアップデート2021-01-04)

リリース日 : 2021年1月4日

ビルド番号 : 20.0.0-1681

このリリースには、一般的な改善が含まれます。

Deep Security Agent 20.0.0-1559(20 LTSアップデート2020/12/07)

リリース日 : 2020年12月7日

ビルド番号 : 20.0.0-1559

新機能

プラットフォームのサポート強化

- Windows 10 20H2

セキュリティの向上

TLSの方向性: Managerのハートビートポートは、TLSクライアントとTLSサーバの両方として機能できるようになりました。今後のエージェントは、TLSサーバではなくTLSクライアントとして接続します。これにより、接続のTCPレイヤと同じ方向でTLSセッションを開始する必要があるプロキシまたはファイアウォールを介したAgentからの接続の問題が解決されます。

機能強化

- Deep Securityの改善 変更されたパッケージのみをチェックすることで、のパフォーマンスを継承します。DS-55527
- メモリ使用率が向上し、パフォーマンスが向上します。DS-53012

- Deep Security Agentでは、挙動監視および機械学習型検索のカスタム処理がサポートされるようになりました。DS-48081

解決済みの問題

- 整合性監視 が有効化されたときに、大量のCPUが使用されました。SEG-88619/03720485 / DS-56613
- アプリケーションコントロールイベントが同じインシデントに対して複数回発生しました。SEG-86213 / SF03620055 / DS-57298
- セキュリティアップデートは新しいコンピュータでは自動的に実行されませんでした。SEG-91484 / SF03828068 / DS-57688

お知らせ

このエージェントのアップデートでは、エージェントマネージャ通信に使用されるTLS証明書の検証がどのように実装されるかが変更されています。エージェントのアクティベーション中に次の警告が表示された場合:

```
[Warning/2] | SSLVerifyCallback() - verify error 20: unable to get local issuer certificate
```

最も根本的な根本原因は、エージェントがマネージャによって証明書に提示されている証明書を検証できないことです。信頼された証明書を固定する必要はありません。この証明書が適用されない場合は無視してください。ただし、信頼された証明書を使用する場合は、Deep Security Agentをアクティベートする前に、"パブリックCAによって発行されたDeep Security Manager証明書チェーンをインポートする" on page 1620 によって発行する手順に従ってください。

Deep Security Agent 20.0.0-1337(20 LTSアップデート2020/10/28)

リリース日:2020年10月28日

ビルド番号:20.0.0.1337

新機能

サポートされているパスへのアップグレード: アクティベーション時のアップグレード機能では、コンピュータ上のAgentが最新の2つのメジャーリリース以降にのみアップグレードされます。Agentが条件を満たしていない場合は、過去2回のメジャーリリース内のリリースにAgentを手動で

アップグレードする必要があります。次に、アクティベーション時のアップグレード機能によって新しいバージョンが検出され、指定されたリリースへのアップグレードが完了します。

機能強化

- アプリケーションコントロールによって自動的に認識されるように、さまざまな実行可能ファイルが信頼されたインストーラとして追加されました。SF03568205 / SEG-85141 / DS-54884
- の[管理]→[システム設定]→[エージェント] の[同じ名前のコンピュータがすでに存在する場合]設定の範囲を拡張して、既存の非アクティブ化されたコンピュータに適用します。これまでは、既存のアクティベートされたコンピュータにのみ適用されていました。DS-51800 / DS-51879
- リアルタイムの変更監視は、ベースディレクトリで指定されたディレクトリと明示的に一致します。以前は、ベースディレクトリで開始されたすべてのパスに一致していました。DS-52692
- 変更監視Deep Security Managerの検索完了時刻が秒単位で1000単位で表示されるようにアップデートしました。DS-54680

解決済みの問題

- エージェントのみとエージェント-好みの設定を有効にした複合モードでは、のDeep Security Notifierは時々高いCPUの原因となった、オンとオフのWindowsアクションセンターのウイルス対策状況を回しました。DS-54799
- Deep Security Agentのバージョンアップ後、「アプリケーションコントロール ルールセットの送信に失敗しました」というエラーが発生することがありました。DS-49828
- 不正プログラム対策の挙動監視機能により、時々誤報が発生していました。DS-44974
- 整合性監視が有効になっていると、ファイルの所有者が存在しないユーザに誤って変更されました。DS-52058
- 「アプリケーションコントロールセットをRelayから提供する」が有効になっていると、不要なRelayエラーイベントが発生しました。DS-50905
- Deep Security AgentがWindows Server上のDockerエンジンのバージョンを検出できなかったため、予期せずクラッシュしました。DS-29590

- Deep Security Agentは、セキュリティ更新プログラムの例外を受信したためのDeep Security Managerは、セキュリティ更新プログラムのタイムアウトを報告しました。SEG-82072 / DS-54720
- リアルタイムの不正プログラム対策検索で検出の問題が発生しました。DS-50286
- Deep Security Managerでログ検査のステータスが正しく表示されないことがありました。SEG-77081 / DS-54719
- 新しいパケットを含む再送信パケットが送信されると、「サポートされていないSSLバージョン」の侵入防御イベントが生成されることがありました。DS-53144

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-3704/DS-41233

最高共通脆弱性評価システム (CVSS) スコア: 4.4

最高の重大度 : 中

既知の問題

Deep Security Relayが同じ場所に配置されたRelayまたは独立したRelayをアップグレードしているときに、「不正プログラム対策保護がないか、期限切れ」および「セキュリティアップデート: セキュリティアップデートの確認とダウンロード失敗 (Agent/Applianceエラー)」というアラートが表示されることがあります。自動的に解決され、それぞれのアラートがクリアされるまで、20分以上かかります。以降のDeep Security Agentのアップグレードを正常に実行するには、Deep Security Relayのアラートが自動的にクリアされるまでお待ちください。DS-54056

Deep Security Agent 20(長期サポートリリース)

リリース日 : 2020年7月30日

ビルド番号 : 20.0.0.877

新機能

セキュリティの向上

エージェントの整合性チェック: Deep Security Agentで署名が検証され、署名後にソフトウェアファイルが変更されていないことが確認されます。

不正な認証情報でAWSアカウントを保護する: 以前は、Deep SecurityでAWSアカウントの認証情報を間違って入力すると、エージェントを有効化できませんでした。これは、資格情報が正しく入力されていないか、Deep Securityで対応するアップデートを行わずに資格情報が変更されたために発生した可能性があります。多くの場合、単純な設定エラーであるこの状況で保護を維持するために、コンピュータはアカウントの外部で作成され、エージェントのアクティベーションが許可されます。

SSLの強化 : Deep SecurityはSSL証明書でハンドシェイクhello_request(rfc5246) および拡張子_then_mac(rfc7366) を暗号化します。

品質と管理の向上

エージェントのアップグレードでの再起動要件の削除: 以前は、新しいエージェントのアップグレードを完了するためにWindowsサーバの再起動が必要になる状況がいくつかありました。リブートする必要があるときのDeep Security Agentの11.0、12.0、または任意のWindowsオペレーティングシステム上の20.0からのアップグレードは完全にアップグレードDeep Securityエージェントの結果として影響されないようにアプリケーションを有効にする、削除されました。

環境内のクライアントのバージョンアップを自動化する: Deep Securityは、新しいエージェントを有効にした場合に新しいバージョンにバージョンアップできるかどうかを柔軟に判断できます。これは、アプリケーションチームが古いバージョンのエージェントを含む古いゴールデンイメージを使用している場合に特に役立ちます。アクティベーション時のアップグレードを有効にし、Agentバージョン管理を使用して環境内で使用するAgentのラインナップを定義するだけで、古いAgentがオンラインになってアクティベートされると、自動的にアップグレードされます。

インスタンスメタデータサービスバージョン2(IMDSv2) のサポート: IMDSv2は、Deep Security Manager FR 2020-04-30でサポートされています。詳細については、「 "Deep Security AgentはAmazonインスタンスメタデータサービスをどのように使用しますか" on page 1979

検索失敗の処理可能な推奨事項: Deep Security Agentには、予約された不正プログラム検索がキャンセルされた理由と、その対策を推奨する処理に関する情報が表示されます。詳細については、"不正プログラム対策 検索の失敗とキャンセル" on page 1158を参照してください。

不正プログラム対策 リアルタイムファイル検索レポート: Deep Securityは、不正プログラム対策 リアルタイム検索によって検索される上位10個のファイルを特定します。この情報を使用してファイル除外を設定し、不要な検索を回避できるため、パフォーマンスの評価およびチューニングの出発点となります。収集されたデータを含む「AmTopNScan.txt」ファイルは、次の方法を使用して生成できます。

- コマンドdsa_control --AmTopNScanにより
- 診断サービスによる

プロセスの除外設定:プロセス除外設定が次のように改善されました。

- プロセス除外項目が正しく機能しない理由に関する情報が提供されるようになったため、問題のトラブルシューティングを行い、解決するために実行する処理を知ることができます。
- プロセスの例外設定ワークフローが改善され、より堅牢になりました。

セキュリティログ監視用のWindowsイベントチャネル:Windowsイベントチャネルのログでは、WindowsプラットフォームでOSおよびアプリケーションのログを追跡するための新しいオプションが提供されます。より新しいWindows Vista。イベントチャネルを使用して、後で確認できるセキュリティログ監視イベントを収集できます。

機能強化

- AWSコネクタでワークスペース同期機能が有効になっていない場合のAmazon WorkSpacesの配信のハートビート処理が改善されました。
- 変更監視およびアプリケーションコントロールの不正プログラム対策への依存、そのため、不正プログラム対策を機能させるためにインストールする必要はありません。
- Deep Security Agent 不正プログラム対策が、IntelliScanが無効になっているときにデータタイプに関係なく圧縮ファイルを検索できるようになりました。
- バージョン9.5以降のvCloudコネクタへのエージェントレスモードのサポートが追加されました。
- Deep Security Managerにアクティベーションステータス(たとえば、Deep Security Managerの新しいバージョンが必要であることを示す成功メッセージやメッセージなど) を表示することで、エージェント起動アクティベーションの体験を強化しました。
- 不正プログラム検索失敗イベントの説明を拡張して、考えられる理由を示しました。
- イベント管理の合理化により、エージェントのパフォーマンスが向上します。

- CLIコマンドを使用してAgentごとに検索キャッシュを有効化/無効化できる機能が追加されます。
- Deep Security Agentの遅延アップグレードのサポートが追加され、アップグレードを実行した後に不正プログラム対策のオフライン問題が軽減されます。

解決済みの問題

- Deep Security Agentのバージョンアップ後、「アプリケーションコントロール ルールセットの送信に失敗しました」というエラーが発生することがありました。DS-49828
- アプリケーションコントロールと不正プログラム対策が有効になっていると、アプリケーションコントロールがオフラインで表示されることがありました同時に。
- セキュリティセキュリティログ監視監視によるSQLiteデータベースへのアクセス方法が原因で、Deep Security Agentが予期せず再起動しました。DS-48395
- ファイアウォールをオフにしても、インタフェース分離機能が有効のままでした。SEG-32926/DS-27099
- システムロケールがトルコ語に設定されている場合、Webレピュテーション、ファイアウォール、侵入防御、およびセキュリティログ監視を正しく有効にできませんでした。DS-48916
- 変更監視イベントで、Unicodeエンコーディングの不正なファイルパスが表示されました。SEG-45239/DS-33911
- アプリケーションコントロールがブロックモードで有効になっているときに、Windows Updateの手順がブロックされました。SF02092464/SEG-53938/DS-38578
- Deep Security Agentの侵入防御モジュールが、ペイロードゼロのUDPパケットを通知なしでドロップしました。SEG-39711/DS-32799
- Webレピュテーションの場合、Deep Security Agentからプロキシに不正な認証情報が送信され、プロキシからHTTP 407が返されました。SF01704358/SEG-45004/DS-32077
- Deep SecurityのNotifier.exeプロセスでCPU使用率が高くなりました。SF01716752/SEG-45507/DS-33645
- 接続が復元されても、「Smart Protection Serverがスマートスキャンのために切断されました」アラートが自動的にクリアされませんでした。SF1609675/SEG-43574/DS-32947
- Windowsドライバがスピンロックを正しく解除せず、システムがハングすることがありました。SF01990859/SEG-50709/DS-36066

- SSLメッセージの詳細ログを有効にして出力すると、Deep Security Agentプロセスがクラッシュすることがありました。SF01745654/SEG-45832/DS-33007
- 複数のSmart Protection Serverが設定されている場合、無効なsps_indexが原因でDeep Security Agentプロセスがクラッシュすることがありました。SF01415702/SEG-42919/DS-33008
- Deep Security AgentでGetDockerVersionエラーが発生したため、ポリシーの送信処理に失敗しました。SF1939658/SEG-49191/DS-34222
- Deep Security AgentからDeep Security Managerへの応答として無効なJSONオブジェクトが送信されたため、Deep Security Managerのログファイルにエラーが発生しました。SF01919585/SEG-48728/DS-34022
- 変更変更監視が有効な場合、特定の条件下でds_agentプロセスがクラッシュすることがありました。SEG-50728/DS-35446
- 作業中のパケットオブジェクトが誤って削除されたため、Deep Security Agentネットワークエンジンがクラッシュしました。SF01526046/SF02159742/SEG-55453/DS-38812
- Deep Security Agentが異常終了し、「Notifierアプリにデータを送信できません」というメッセージが表示されます。ds_agent.logのエラーメッセージ。SEG-21208/DS-33134/DS-21352
- システムの地域形式が「中国語 (繁体字、香港特別行政区)」の場合、Deep Security Notifierで繁体字ではなく簡体字が表示されました。SEG-48075/DS-34778
- リアルタイムの変更変更監視ファイル検索イベントにUnicodeユーザ名を表示できませんでした。SF02187371/SEG-56645/DS-39398
- Deep Security Agentは、Python拡張モジュール (PYD) ファイルをアプリケーションコントロールのインベントリに追加しませんでした。SF01804378/SEG-47425/DS-33690
- ユーザモードで処理中のファイルオープンイベントが多すぎるため、CPU使用率が高くなりました。SF02179544/SEG-55745/DS-39638
- レジストリ値の変更を監視するように初期設定のSTANDARD属性が設定されている場合、変更変更監視イベントに[種類]属性が表示されませんでした。SF02412251/SEG-59848/DS-41118
- 実行権限で開かれた非実行可能ファイルにより、生成されるべきではないセキュリティイベントとドリフトが発生していました。SF01780211/SEG-46616/DSSEG-3607

- アプリケーションコントロールが有効で、ホストアプリケーションが大量の非実行可能ファイルを作成しているときに、CPU使用率が高くなりました。SF02179544/SEG-55745/DS-41142
- アプリケーションコントロールがブロックモードで有効になっているときに、Windows Updateの手順がブロックされました。SF02092464/SEG-53938/DS-39981
- ユーザエージェント文字列が古いため、Deep Securityでセキュリティアップデートをダウンロードできませんでした。SF02043400/SEG-52069/DS-41316
- コンピュータがドキュメントファイルをファイルサーバに書き込む場合、不正プログラム対策はファイルを頻繁に検索する必要がありました。SF01949194/SEG-49854/DS-40100
- Deep Security Agentがサイズの大きいファイルのウイルスを検索すると、大量のメモリが消費されました。SF01572110/SEG-48704/DS-43114

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-3704/VRTS-3176

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度 : 高

- NGINXが1.16.1にアップデートされました。DSSEG-4600
- curl 7.67.0にアップデートされました。
- openssl-1.0.2tにアップデートされました。
- JREを最新のJava Update (8.0.241/8.43.0.6) にアップデートしました

既知の問題

- Deep Security Agentをアップグレードした後、「Sending アプリケーションコントロール Ruleset Failed」エラーが発生する場合があります。この問題を解決するには、影響を受けたコンピュータを右クリックし、アクション > 警告/エラーのクリアを選択し、その後ポリシーの送信を選択してください。

- Windows 2008でDeep Security Agentをアップグレードすると、不正プログラム対策がオフラインになることがあります。これが発生した場合は、Deep Security Agentを完全にアンインストールし、サーバを再起動してから、エージェントを再インストールしてください。

アップグレードの通知

- アプリケーションコントロールを有効にしている場合、ソフトウェアインベントリの自動再構築中にパフォーマンスが一時的に低下することがあります。DS-41775

UNIX

Deep Security Agent - 20.0.3-860 (20 LTS 更新 2026-01-21)

リリース日: 2025年1月21日

ビルド番号: 20.0.3-860

新機能

Endpoint Event Viewer: Endpoint Event Viewerにアクセスして、管理されたコンピュータ全体のセキュリティおよびシステムイベントを期間、重大度、イベントの発生元、アクションでフィルタリングして表示します。これはTrend Vision One - サーバ & Workload Protectionのみでサポートされています。

解決された問題

- Deep Security Agentは、syslogホスト名が64文字を超えるとクラッシュしました。PCT-87531/DSA-14252
- Webレピュテーションサービスを有効にすると、システムメモリの使用量が継続的に増加しました。PCT-80352/DSA-13866
- Deep Security Agentは、エージェントが予期していた形式と異なるHTTP/2パケットを処理する際に、時々クラッシュすることがありました。PCT-85552/DSA-13755
- Deep Security Agentが再起動した後、侵入防御検出が時々動作を停止しました。PCT-82352/DSA-13755

Deep Security Agent - 20.0.2-29760 (20 LTS アップデート2025-12-09)

リリース日: 2025年12月09日

ビルド番号: 20.0.2-29760

機能強化

- ファイアウォールと侵入防御システムのイベントは、データが利用可能な場合、プロセスとユーザ情報を表示します。これはすべての顧客に段階的に展開されています。DSA-13741

セキュリティ更新

このリリースにはサードパーティライブラリの更新が含まれています。DSA-13204

Deep Security Agent - 20.0.2-26670 (20 LTS 更新 2025-11-12)

リリース日: 2025年11月12日

ビルド番号: 20.0.2-26670

新機能

ユーザベースのファイアウォール: ファイアウォールルールはユーザアカウントに基づいて設定できるようになりました。この機能はすべての顧客に段階的に展開されています。

強化されたHTTP/2サポート: 侵入防御システムエンジンは、現在、受信HTTP/2接続をサポートしています。この機能は、安定性とパフォーマンスの向上を確保するために、バックエンドの更新を通じて段階的に展開されます。(このリリースには、HTTP/2の処理とセキュリティの向上を目的とした修正も含まれています。PCT-77306/DSA-13105)

解決された問題

- AIXプラットフォーム用Deep Security Agentにライブラリが欠落しているため、ファイアウォールおよび侵入防御システムのイベントを収集できませんでした。DSA-13176

Deep Security Agent - 20.0.2-22850 (20 LTS 更新 2025-10-08)

リリース日: 2025年10月08日

ビルド番号: 20.0.2-22850

既知の問題

- このリリースでは、侵入防御システムまたはファイアウォールが有効になっている場合にイベント収集を妨げる問題のため、AIX用のDeep Security Agentパッケージが除外されています。詳細については、トレンドマイクロ™ Deep Security™のAIXプラットフォームでライブラリが不足しているため、ファイアウォールおよびIPSイベントを収集できませんを参照してください。DSA-13176

Deep Security Agent - 20.0.2-20480 (20 LTS 更新 2025-09-17)

リリース日: 2025年9月17日

ビルド番号: 20.0.2-20480

このリリースには一般的な改善が含まれています。

Deep Security Agent - 20.0.2-17500 (20 LTS 更新 2025-08-13)

リリース日: 2025年8月13日

ビルド番号: 20.0.2-17500

このリリースには一般的な改善が含まれています。

Deep Security Agent - 20.0.2-14430 (20 LTS 更新 2025-07-09)

リリース日: 2025年7月9日

ビルド番号: 20.0.2-14430

強化

- 高度なTLSトラフィック検査が有効になっている場合、接続がブロックされていない限り、Deep Security Agentは接続を高速化するためにパケットを挿入します。PCT-

63207/DSA-10919

解決された問題

- オンデマンド検索は、Deep Security Agentのアクティベーションまたは再起動後に自動検索がトリガーされるまで手動で開始できませんでした。WS-12581

Deep Security Agent - 20.0.2-12010 (20 LTS 更新 2025-06-11)

リリース日: 2025年6月11日

ビルド番号: 20.0.2-12010

機能強化

- デフォルトで有効化されているWebレピュテーションサービスは、ウェブサイトのリスクレベルを判断する際にサーバ名表示 (SNI) クエリを使用します。

解決された問題

- Deep Security AgentはSSLハンドシェイク中に時々クラッシュしました。PCT-55526/DSA-9902

セキュリティ更新

このリリースにはサードパーティライブラリの更新が含まれています。DSA-10530

Deep Security Agent - 20.0.2-9810 (20 LTS 更新 2025-05-14)

リリース日: 2025年5月14日

ビルド番号: 20.0.2-9810

機能強化

Webレピュテーションサービスは、疑わしいまたは悪意のあるサイトへのhttpプロキシ接続をブロックする際に、200 OKページではなく403 Forbiddenを指すようになりました。PTC-60576/DSA-10325

解決された問題

- 高度なTLSを使用したDeep Security Agentの構成が一部のシステムをフリーズさせました。PCT-63207/DSA-10380
- Webレピュテーションイベントの URL列に情報が欠落していることがありました。PCT-60576/DSA-10090

Deep Securityエージェント - 20.0.2-7600 (20 LTS 更新 2025-04-16)

リリース日: 2025年4月16日

ビルド番号: 20.0.2-7600

このリリースには、一般的な改善が含まれます。

Deep Securityエージェント - 20.0.2-4961 (20 LTS 更新 2025-03-12)

リリース日: 2025年3月12日

ビルド番号: 20.0.2-4961

機能強化

- `dsa_scan`コマンドには、大きなファイルを管理するための`scanLargeFile`オプションが含まれるようになりました。DSA-8825

Deep Securityエージェント - 20.0.2-1390 (20 LTS 更新 2025-01-15)

リリース日: 2025年1月15日

ビルド番号: 20.0.2-1390

強化

- Deep Securityエージェントは、パフォーマンスを向上させるためにパケットを順番に処理するようにキューに入れるようになりました。DSA-6916

解決された問題

- Deep Securityエージェントは、高度なTLSトラフィック検査が有効になっているときに接続の問題が発生することがありました。DSA-8577

Deep Securityエージェント - 20.0.1-25771 (20 LTS Update 2024-12-10)

リリース日: 2024年12月10日

ビルド番号: 20.0.1-25771

解決済みの問題

- パケットデータを含むイベントが不正なパケットサイズで記録されていました。PCT-45556/DSA-8074

Deep Securityエージェント - 20.0.1-23340 (20 LTS 更新 2024-11-13)

リリース日: 2024年11月13日

ビルド番号: 20.0.1-23340

機能強化

- Webレピュテーションサービスは、Webサイトのリスクレベルを判断する際にサーバー名表示 (SNI) クエリを使用できるようになりました。DSA-7314

解決された問題

- アプリケーションコントロールがブロックモードで動作しているとき、一部のディレクトリ内のファイルがブロックされるべきところを許可されていました。PCT-38516/DSA-7613

Deep Securityエージェント- 20.0.1-21510 (20 LTS更新 2024-10-16)

リリース日: 2024年10月16日

ビルド番号: 20.0.1-21510

このリリースには、一般的な改善が含まれます。

Deep Security エージェント- 20.0.1-19250 (20 LTS Update 2024-09-18)

リリース日: 2024年9月18日

ビルド番号: 20.0.1-19250

このリリースには、一般的な改善が含まれます。

Deep Security Agent - 20.0.1-17380 (20 LTS アップデート2024-08-21)

リリース日: 2024年8月21日

ビルド番号: 20.0.1-17380

解決済みの問題

- Deep Security Agent は、一部のポリシー構成フィールドに中括弧が含まれている場合、ポリシーを読み込むことができませんでした。DSA-6189
- Deep Security Agentは、ホスト名に非ASCII文字が含まれている場合、アクティベートに失敗します。PCT-32214/DSA-6268
- 侵入防御がDeep Securityエージェントで有効になっている場合、サードパーティアプリケーションがソースポートを再利用すると接続の問題が発生することがあります。SF07685331/PCT-20541/DSA-5596

Deep Security Agent - 20.0.1-14610 (20 LTS アップデート2024-07-17)

リリース日: 2024年7月17日

ビルド番号: 20.0.1-14610

解決済みの問題

- 変更監視 real-time scans が時々イベントを生成できないことがありました。SF07269768/PCT-21721/DSA-5877
- AIXプラットフォーム用のDeep Security Agentは、サポートされているロケールを設定しないと起動できないことがありました。DSA-5876

Deep Security Agent - 20.0.1-12510 (20 LTS アップデート2024-06-19)

リリース日: 2024年6月19日

ビルド番号:20.0.1-12510

解決済みの問題

- 不正プログラム対策が有効になっている場合、Deep Security Agentが完全にシャットダウンできない場合がありました。PCT-26090/DSA-5492

Deep Security Agent - 20.0.1-9400 (20 LTS Update 2024-05-16)

リリース日: 2024年5月16日

ビルド番号: 20.0.1-9400

解決された問題

- Webレピュテーションサービスを有効にしてDeep Security Agentを使用すると、一部のアプリケーションパフォーマンス監視 (APM) アプリケーションが正常に機能しませんでした。SF04072723/SEG-97952/PCT-15716/DSA-4750

- AIXプラットフォームでの不正プログラム対策の予約検索に、除外されるはずのネットワークファイルシステム (NFS) のコンテンツが含まれていました。PCT-13912/DSA-4098

Deep Security Agent - 20.0.1-7380 (20 LTS Update 2024-04-24)

リリース日: 2024年4月24日

ビルド番号: 20.0.1-7380

機能強化

- Deep Security Agentで、Trend Vision One Service Gatewayの除外がサポートされるようになりました。現時点では、Trend Cloud One - Endpoint & Workload Securityユーザのみがサポートされます。V1E-17754
- Deep Security Agent for AIXプラットフォームがアップデートされ、削除前スクリプトのタイムアウトが120秒に延長されました。PCT-19843/DSA-4839

解決済みの問題

- クラウド環境で実行されているDeep Security AgentをTrend Cloud One -Endpoint & Workload Securityで有効化できないことがありました。DSA-4861

Deep Security Agent - 20.0.1-4540 (20 LTS Update 2024-03-20)

リリース日: 2024年3月20日

ビルド番号: 20.0.1-4540

このリリースには、一般的な改善が含まれます。

Deep Security Agent - 20.0.1-3180 (20 LTS Update 2024-02-29)

発売日: 2024年2月29日

ビルド番号: 20.0.1-3180

解決済みの問題

- Trend Vision One Service Gatewayを使用したオンプレミスDeep Security ManagerからTrend Cloud One - Endpoint&Workload SecurityへのAgentの移行に失敗しました。この問題は、他のプロキシサービスを使用して移行する場合にも発生する可能性があります。PCT-16649/DSA-4144
- Deep Security Agentで侵入防御またはWebレピュテーションサービスを有効にすると、TLS検査プロセス (tm_netagent) のエラーログローテーションの問題が発生することがありました。DSA-3965

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-11708/DSA-3702

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度: 高

既知の問題

- 実行可能ファイルのコピーを実行しているときに、アプリケーションコントロールの信頼エンティティの「ターゲットごとにブロック」信頼ルールが正しく機能しないことがあります。PCT-11105/DSA-3324

Deep Security Agent - 20.0.1-690 (20 LTS Update 2024-01-17)

リリース日: 2024年1月17日

ビルド番号: 20.0.1-690

機能強化

- 2024年以降、Deep Security Agentのバージョン管理が20.0.0から20.0.1に改訂されます。これにはDeep Security Manager 20.0.883以降が必要です。DSA-3584。

詳細については、2024年1月のアップデートリリースにおけるDeep Security Agent (DSA) バージョン改訂のプラットフォームサポート更新をご覧ください。

解決済みの問題

- Deep Security Agentがローカルの Smart Protection Serverに接続できないことがありました。DSA-3564

既知の問題

- Deep Security Agent 20.0.1-690 へのアップデートが、Trend Cloud One - Endpoint & Workload Security で Deep Security Relay を使用している場合、20.0.0 の一部のバージョンからのアップデートで失敗することがあります。詳細については、自己展開された Workload Security Relay の 20.0.0-3445 以降からバージョン 20.0.1 へのリモートアップグレードの失敗 DSA-3317 を参照してください

Deep Security Agent - 20.0.0-8438 (20 LTS Update 2023-12-12)

リリース日: 2023年12月12日

ビルド番号: 20.0.0-8438

解決済みの問題

- ローカルのSmart Protection Serverと設定されたプロキシを使用している場合、Webレピュテーションサービスがプロキシ経由でトラフィックを不適切に送信することがありました。Webレピュテーションサービスは、クエリをローカルのSmart Protection Serverに直接送信するようになりました。DSA-2981

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。DSA-2722

最高共通脆弱性評価システム (CVSS) スコア: 9.8

最高の重大度: 重大

既知の問題

- Deep Security Agent は、ローカルの Smart Protection Server に接続できないことがあります。この問題は 20.0.1-690 で修正されています。詳細については、プロキシ使用時の Deep Security Agent とSmart Protection Server の接続問題 DSA-3564 を参照してください

Deep Security Agent - 20.0.0-8268 (20 LTS Update 2023-11-21)

リリース日: 2023年11月21日

ビルド番号: 20.0.0-8268

解決済みの問題

- システムがスリープモード(動作状態のS0低電力アイドルモード。モダンスタンバイとも呼ばれます) から復帰した後、Deep Security不正プログラム対策が期待どおりに機能しないことがありました。SF07326571/PCT-5476/DSA-2485
- Deep Security Agentでは、Microsoft Word、Excel、PowerPointで生成された `.xml` ファイル、およびAutoCADおよびR2000で生成された `.dwg` ファイルのMIMEタイプが誤って分類されていました。SF07027236/SEG-186079/DSA-2202
- 大量の不審オブジェクトリストをロードすると、メモリリークが発生することがありました。SF06904914/SEG-182231/DSA-1370

Deep Security Agent - 20.0.0-8137 (20 LTS Update 2023-10-26)

リリース日: 2023年10月26日

ビルド番号: 20.0.0-8137

このリリースには、一般的な改善が含まれます。

Deep Security Agent - 20.0.0-7943 (20 LTS Update 2023-09-26)

リリース日: 2023年9月26日

ビルド番号: 20.0.0-7943

機能強化

- コマンドラインからプロキシ情報を取得するための新しいコマンドが追加されました。
  `dsa_query -c GetProxyInfo`
  `dsa_query -c GetProxyInfo details=true`
  DSA-864
- エージェントパターンの更新を正しく表示するには、Deep Security Agent 20.0.0-7943以降にはDeep Security Manager 20.0.759以降が必要です。詳細については、Deep Security Agent 20.0.0-7943の互換性のないエージェント/アプライアンスバージョンエラーを参照してください。SEG-190866/SEG-191017/DSA-1531

Deep Security Agent - 20.0.0-7719 (20 LTS Update 2023-08-29)

リリース日: 2023年8月29日

ビルド番号: 20.0.0-7719

機能強化

- スマートスキャンが無効になっている場合、Deep Security Agentでスマートスキャンエージェントパターンがアップデートされなくなり、ネットワーク帯域幅が節約されます。SEG-186625/DSA-1063
- Deep Security Agentでダウンロードされる増分パターンアップデートの数が減り、ネットワーク帯域幅が節約されるようになりました。Deep Security Relayとして設定されているAgentでも、すべてのパターンアップデートがダウンロードされることに注意してください。DSA-1000
- ユーザがURLにアクセスしようとし、ブロックされたときにリダイレクトされるWebレピュテーションサービスの「ブロックページ」が、チェコ語またはポーランド語で表示できるようになりました。DSA-444
- 侵入防御では、動的ポート番号が10001 ~ 65535の接続について検索するバイト数を制限できるようになりました。DS-78036
- 高度な脅威検索エンジンがバージョン22.6に更新されました。DSA-453

解決済みの問題

- 一部のシステムで、Deep Security Agentサービス(ds_agent)の停止に通常より時間がかかりました。SEG-187365/DSA-1212

- Deep Security Agentで、セキュリティアップデートがスケジュールされていない場合でも、アップデートが実行されることがありました。SEG-187449/DSA-1064
- 一部のシステムでDeep Security AgentのCPU使用率が高くなりました。SEG-185563/DSA-756

Deep Security Agent - 20.0.0-7476 (20 LTS Update 2023-07-25)

リリース日: 2023年7月25日

ビルド番号: 20.0.0-7476

強化機能

- dsa-connectサービスがアップデートされ、CPUパフォーマンスが向上しました。C1WS-12970

解決済みの問題

- Deep Security Agentの20.0.0.6313から新しいバージョンへのアップグレードが失敗し、「異常な再起動が検出されました」という警告が表示されることがありました。SF06897730/SEG-180989/DS-78063

Deep Security Agent - 20.0.0-7303 (20 LTS Update 2023-06-28)

リリース日: 2023年6月28日

ビルド番号: 20.0.0-7303

機能強化

- Deep Security Agentでは、fe80:0:0:0:0:0:0:1/24やfe80::01など、CIDRまたは二重コロン表記を使用したIPv6アドレスがサポートされるようになりました。SF04849178/SEG-122076/DS-67280
- Webレピュテーションサービスで、OSのプロキシ設定で使用されるポートが自動的に監視されるようになりました。DS-77233

解決済みの問題

- AIX上のDeep Security Agentを新しいバージョンにアップグレードしようとすると、クラッシュすることがありました。SF06643647/SEG-173140/DS-77359
- 侵入防御(IPS)が正しいペイロード値を読み取らない場合があり、ルールが誤動作する可能性があります。DS-74647
- Deep Security Agentは、Endpoint Sensorが使用されていない場合でも、ハートビートのたびに「dsa-connect has not provided status」をレポートしていました。C1WS-14696
- 一部のMQTTメッセージが繰り返し送信され、dsa-connectがシャットダウンループでスタックすることがありました。DS-76709

Deep Security Agent - 20.0.0-7119 (20 LTS Update 2023-05-29)

リリース日: 2023年5月29日

ビルド番号: 20.0.0-7119

強化

- Deep Security Agent for Solarisがアップデートされ、Azure Data Explorerダッシュボードでのインタフェース遅延メトリクスの収集を有効にするオプションが追加されました。DS-77025

解決済みの問題

- 特定のシナリオで、MQTT接続の認証情報がDeep Security Agentのログファイル(`ds_agent.log`)に入力されていました。SEG-174560/C1WS-13282
- Deep Security Agentでは、感染した圧縮ファイルに複数の感染ファイルが含まれていても、その圧縮ファイルに対する不正プログラム対策イベントが1つしか報告されませんでした。DS-76339
- 接続を置き換えた後、Deep Security Agentは、最大4分間、以前の接続にまだ接続されているかのようにメトリクスをレポートしました。DS-77453

Deep Security Agent - 20.0.0-6912 (20 LTS Update 2023-05-02)

リリース日: 2023年5月2日

ビルド番号: 20.0.0-6912

機能強化

- Deep Security Agentがアップデートされ、プロキシプローブの接続タイムアウトを設定できるようになりました。ds_agent.ini. SF06664116/SEG-173848/DS-77182

  プロキシプローブラインの例 ds_agent.ini 設定ファイル:
  dsa.proxymanager.ProbeTimeoutInSec=120
- Deep Security Agentがアップデートされ、MQTTの接続品質が向上し、接続タイムアウトの発生が減少しました。DS-76840

解決済みの問題

- ドライバの再起動後に、Deep Security Agentがネットワークドライバのステータスを正しくレポートしないことがありました。C1WS-12896
- Webレピュテーションサービスを有効にすると、Deep Security Agentによって一部のシステムが予期せずシャットダウンしていました。SF06680505 / SEG-174730 / DSSEG-7866
- Relayから新しいプラグインをダウンロードした後にDeep Security Agentがクラッシュすることがありました。DS-76961

Deep Security Agent - 20.0.0-6658 (20 LTS Update 2023-03-22)

リリース日: 2023年3月22日

ビルド番号: 20.0.0-6658

新機能

サービスゲートウェイ: Deep Security Agent 20.0.0-6658以降とDeep Security Manager 20.0.741以降では、転送プロキシ機能を提供するサービスゲートウェイ機能がサポートされるようになりました。

機能強化

- Webレピュテーションサービスに、OSプラットフォームのメタデータが含まれるようになりました。DS-75453

- Deep Security Agentのログシステムがアップデートされ、ユーザの問題をより効率的にデバッグするための追加情報とトレースが提供されるようになりました。Agentはそれぞれ2MBのログファイル (dsa-connect-X.log) を5つ生成します。以前はそれぞれ1MBのログファイルが3つでした。C1WS-9598

  ロガーは、オンデマンドのJSON設定ファイル (dsa-connect.ini または dsa-connect.conf) をサポートし、次の設定オプションを使用できます。
  - Debug: デバッグログメッセージを有効にします (初期設定: false)
  - Count: 生成するログファイルの数 (初期設定: 5)
  - Size: 各ログファイルの最大サイズ (バイト) (初期設定: 2097152)

  設定ファイルの例:

  ```
  { "Debug": true, "Count": 5, "Size": 2097152 }
  ```

解決済みの問題

- コンソール(Computer または Policy > 侵入防御 > 一般 > Advanced TLS Traffic Inspection) からAdvanced TLS Traffic Inspection の「Inspect TLS/SSL traffic」オプションが「No」に設定されている場合でも、ドライバー側の SSL パケットが処理されることがありました。DS-76160
- Deep Security Agentの侵入防御システムが、「TCP輻輳フラグ」を適切にブロックできないことがありました。DS-76182
- 不正プログラム対策スマートスキャンを有効にすると、IPC接続の問題により一部のシステムがクラッシュしました。SEG-169132/C1WS-10821
- ファイル処理に問題があり、アップデート中にファイルを削除できないため、Deep Security Agentのセキュリティアップデートに失敗しました。DS-75907
- 一部のシステムで、プロセススレッドのタイムアウトにより、不正プログラム対策エンジンが予期せず再起動することがありました。SF06524736/SEG-169218/DS-76656
- SOCKSプロキシを使用した場合、Deep Security AgentはHTTP URLに対するWebレピュテーションサービスの評価を提供できませんでした。DS-73482/DS-73364
- Agentパッケージに署名がないため、Deep Security Agentのアップグレードが失敗することがありました。SF06045259/SEG-154576/DS-73668

- Deep Security Agentで、一部のシステムで高度な脅威検索エンジン(ATSE) コンポーネントが削除されたことを示すシステムイベントが誤って生成されていました。SEG-147779 / DS-75463
- 一部のシステムでの接続の問題を解決するために、Deep Security Agentがアップデートされ、MQTTタイムアウトが30分から2時間に延長されました。C1WS-11835

Deep Security Agent - 20.0.0-6313 (20 LTS Update 2023-01-31)

リリース日 : 2023年1月31日

ビルド番号 : 20.0.0-6313

機能強化

- Deep Securityでは、SHA-1アルゴリズムで署名された証明書はサポートされなくなりました。エージェントがDeep Security Managerと通信するために、SHA-256を使用して発行されたSSL証明書が必要になりました。C1WS-5676

> 警告 : Deep Security AgentとDeep Security Manager間の通信エラーを防ぐために、Deep Security暗号アルゴリズムをアップグレードする手順に従ってください。
> 暗号アルゴリズムをアップグレードする前にDeep Security Agent 20.0.0-6313以降に更新した場合は、OpenSSL 3がSHA-1アルゴリズムの証明書を拒否する際のDeep Security Agent (DSA)オフラインの手順に従ってください。

解決済みの問題

- Deep Security Agent for AIXプラットフォームがアップデートされ、高度な脅威検索エンジン(ATSE) バージョン21.600がサポートされるようになりました。DS-75323
- コンポーネントのアップデートの場合、Deep Security Agentはプロキシを使用する場合と使用しない場合とで試行し、試行ごとにイベントを生成します。イベントレポートをより簡単にするために、この動作が変更され、アップデートが成功した場合、エージェントは最後に成功したイベントのみを表示するようになりました。SF06207160/SEG-160085/DSSEG-7765
- Deep Security Agentのログファイル (`ds-agent.log`) ローテーションに失敗し、意図したよりも多くのディスク容量を使用することがありました。SF05306459/SEG-137003/DS-72899

- Webレピュテーションを有効にすると、コンソールコマンドに入力された一部の文字が正しく解析されませんでした。たとえば、コマンドに入力されたアンダースコア(_)はダッシュ(-)に置き換えられました、大文字のZが小文字のzに置き換えられました。DS-74335

Deep Security Agent - 20.0.0-5953 (20 LTS Update 2022-11-22)

リリース日:2022年11月22日

ビルド番号:20.0.0-5953

このリリースには、一般的な改善が含まれます。このリリースには、Solarisプラットフォーム用のエージェントのみが含まれていることに注意してください。

Deep Security Agent - 20.0.0-5761 (20 LTS Update 2022-10-21)

リリース日:2022年10月21日

ビルド番号:20.0.0-5761

機能強化

- Deep Security Agentがアップデートされ、Webレピュテーションサービス用の追加のメタデータ(UserAgent や Referrerなど) が追加されました。DS-72196
- Deep Security Agentがアップデートされ、エージェント診断パッケージに変更監視データベースが追加されました。DS-73293
- 侵入防御を使用してTLSトラフィックを検査するときにNULL暗号をサポートするようにDeep Security Agentがアップデートされました。DS-71085

解決済みの問題

- セキュリティログ監視を有効にすると、Deep Security Agentで「異常な再起動の検出」イベントが生成されることがありました。SF05951130 / SEG-151372 / DS-73737
- vMotionを使用している仮想マシンが予期せず非アクティブ化され、[オフライン(アクティベーションが必要)] ステータスが表示されることがありました。SEG-153050/DS-73807

Deep Security Agent - 20.0.0-5512 (20 LTS Update 2022-09-22)

リリース日:2022年9月22日

ビルド番号 : 20.0.0-5512

機能強化

- Deep Security Agentがアップデートされ、オンデマンド検索と予約検索のマルチスレッドサポートが追加されました。DS-72797 / DS-72798

解決済みの問題

- Deep Security Agentから予期しない形式のホストメタデータが報告されました。DS-73411

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-8100/VRTS-8101/DS-73087/DS-72528

最高共通脆弱性評価システム (CVSS) スコア: 7.0

最高の重大度 : 高

Deep Security Agent - 20.0.0-5394 (20 LTS Update 2022-08-29)

リリース日 : 2022年8月29日

ビルド番号 : 20.0.0-5394

新機能

AIX 7.3サポート: Deep Security Agent 20.0.0-5394以降とDeep Security Manager 20.0.677以降がAIX 7.3をサポートしました。

機能強化

- アプリケーションコントロールで、実行可能でない拡張子を持つ実行可能ファイルのソフトウェア変更が検出されるようになりました。DS-70805

- Deep Security Agentがアップデートされ、TLS接続での動的ポートを使用したパケット検査のサポートが追加されました。DS-71078
- Deep Security Agentがアップデートされ、高度なTLS検査のメトリックがさらに追加されました。DS-72833

解決済みの問題

- 動的ポートを使用したUDP接続でTLS検査を実行すると、OSがクラッシュすることがありました。SEG-151169 / DS-73043
- 一致または正規表現フィールドで変数に「$」文字を使用すると、セキュリティセキュリティログ監視エンジンがオフラインになる問題を修正しました。SEG-146965 / SEG-146966 / DS-72325
- 新しいゲスト仮想マシンに対してリアルタイム不正プログラム対策をオフにしたポリシーを割り当てると、同じDeep Security Virtual Applianceに登録されている他のすべてのゲスト仮想マシンに対して、リアルタイム不正プログラム対策がオフになることがありました。SEG-146057 / DS-72856
- アプリケーションコントロールは、メンテナンスモード中もネットワークファイルへのアクセスをブロックしていました。SF04922652 / SEG-131710 / DS-72037
- アプリケーションコントロールが有効な場合、Adobeプラグインで予期しないセキュリティイベントが生成されていました。SF05823607 / SEG-148570 / DS-72679
- エージェントのアップデート中に特定の設定ファイルをロードすると、Deep Security Agentで「リビジョンの不一致(-10039) 」エラーが返されていました。DS-72499
- アプリケーションコントロールインベントリの検索が完了する前に、Deep Security Agentがソフトウェアの変更の検出をレポートしていました。DS-72071

既知の問題

- 複数のカスタムスクリプトタスクを実行すると、新しいタスクは以前の未完了のタスクによって上書きされます。カスタムスクリプトタスクを1つずつ実行して、この問題を回避できます。この問題は、今後のリリースで修正される予定です。DS-72699

Deep Security Agent - 20.0.0-5137 (20 LTS Update 2022-07-26)

リリース日 : 2022年7月26日

ビルド番号 : 20.0.0-5137

機能強化

- Deep Security Agentがアップデートされ、信頼エンティティの機能が向上しました。信頼ルールのワイルドカードサポートに、多くのサブディレクトリに一致するglobstar `\*\*` が含まれるようになりました。Single star `\*` は現在のディレクトリ内でのみ一致します。Single star `\*` を使用して多数のフォルダを照合していた既存のルールは機能しなくなり、globstar `\*\*`を使用するように変更する必要があります。DS-71817

解決済みの問題

- 特定の設定の組み合わせを持つ侵入防御ルールをコンパイルできませんでした。DS-71889

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性からどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。
VRTS-7102/VRTS-7070/VRTS-7041/VRTS-7039/DSSEG-7636

最高共通脆弱性評価システム (CVSS) スコア: 4.4

重大度: 中

既知の問題

- 複数のカスタムスクリプトタスクを実行すると、新しいタスクは以前の未完了のタスクによって上書きされます。カスタムスクリプトタスクを1つずつ実行して、この問題を回避できます。この問題は、今後のリリースで修正される予定です。DS-72699

Deep Security Agent - 20.0.0-4959 (20 LTS Update 2022-07-04)

リリース日: 2022年7月4日

ビルド番号: 20.0.0-4959

解決済みの問題

- セキュリティログ監視が有効な場合、Deep Security Agent 20.0.0-4726にアップグレードすると、「Get Events Failed」および「Command Not Found」アラートが発生します。SF05738607 / SEG-145679 / DS-72117
- 不正プログラム対策と変更監視が有効になっている場合、Deep Securityエージェントが高いCPU使用率を引き起こしました。SF05169148/SEG-129522/DS-69594
- 不正プログラム対策を有効にすると、ISOバックアップを実行していたOSがDeep Security Agentでクラッシュすることがありました。SF05532786 / SEG-139280 / DS-71299
- Deep Security Agentで、「無効」または「不正な形式」のプロキシURLを参照する不明確なエラーログエントリが作成されることがありました。SEG-144613 / DS-71866

Deep Security Agent - 20.0.0-4726 (20 LTS Update 2022-05-31)

リリース日 : 2022年5月31日

ビルド番号 : 20.0.0-4726

解決済みの問題

- AIXサーバで、システムの `LIBPATH` または `LD_LIBRARY_PATH` 環境変数が定義されていると、Deep Security Agentが起動しないことがありました。DS-70882
- 一部の設定で、Deep Security Agentによって「作成/削除」の変更監視イベントの誤検出が報告されました。SF05434164 / SEG-136425 / DS-70656
- サーバ名インジケータ(SNI) で無効な形式を使用すると、Deep Security Agentで接続の問題が発生していました。SEG-127761 / DS-70806
- Deep Security Agentの異常な再起動により、「不正プログラム対策エンジンがオフライン」エラーが発生することがありました。SEG-140234 / DS-71333

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。DS-52329

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度 : 高

Deep Security Agent - 20.0.0-4416 (20 LTS Update 2022-04-28)

リリース日 : 2022年4月28日

ビルド番号 : 20.0.0-4416

機能強化

- Deep Security Agentがアップデートされ、「Bypass Network Scanner」ルールが適用された場合の侵入防御のパフォーマンスが向上しました。DS-69515

解決済みの問題

- 侵入防御を有効にすると、一部のシステムでパケット転送エラーが発生してクラッシュしていました。SEG-136843 / DSSEG-7524

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-7132/DS-70518

最高共通脆弱性評価システム (CVSS) スコア: 7.5

最高の重大度 : 高

Deep Security Agent - 20.0.0-4185 (20 LTS Update 2022-04-06)

リリース日 : 2022年4月6日

ビルド番号 : 20.0.0-4185

解決済みの問題

- コマンドラインを使用して不正プログラム対策の手動検索を実行すると、Deep Security Agentが受信接続を受信できなくなることがありました。SF05385865 / SEG-135256 / DS-70364
- メンテナンスモードで実行している場合でも、アプリケーションコントロールが認識できないソフトウェアをブロックすることがありました。SF05234969 / SEG-133594 / DS-69752
- セキュリティログ監視で、1桁の日付形式を含むシステムログを解析できませんでした。SF04562942 / SEG-115435 / DS-69757

Deep Security Agent - 20.0.0-3964 (20 LTS Update 2022-03-01)

リリース日 : 2022年3月1日

ビルド番号 : 20.0.0-3964

新機能

脅威インテリジェンス: 脅威インテリジェンス (旧称Connected Threat Defense) は、新たな脅威に対するマルウェア対策を強化します。詳細については、「脅威インテリジェンスを使用して新たな脅威を検出する」を参照してください。

機能強化

- 侵入防御イベントの [元のIP (XFF)] フィールドから文字列内の不審な文字 ($など) を除外するようにDeep Security Agentがアップデートされました。SEG-129905/DS-68989

Deep Security Agent - 20.0.0-3770 (20 LTS Update 2022-01-24)

リリース日 : 2022年1月24日

ビルド番号 : 20.0.0-3770

機能強化

- Deep Security Agentがアップデートされ、Deep Security ManagerがTLS 1.2の強力な暗号を使用している場合に侵入防御からDeep Security Managerに接続できるように

なりました。DS-69042

解決済みの問題

- アプリケーションコントロール、不正プログラム対策、およびリアルタイムの変更監視 が、特定の組み合わせの変更監視 ルールを持つDeep Security Agentで正常に機能しませんでした。DS-68494

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。DS-68180

最高共通脆弱性評価システム (CVSS) スコア: 9.1

最高の重大度 : 高

Deep Security Agent - 20.0.0-3445 (20 LTS Update 2021-11-24)

リリース日 : 2021年11月24日

ビルド番号 : 20.0.0-3445

機能強化

- セキュリティ強化のため、初期設定でTLS 1.2の強力な暗号化スイートを使用するようにDeep Security Agentがアップデートされました。エージェントは以前、初期設定でCBC暗号スイートを使用していました。DS-67204
- Deep Security Agentがアップデートされ、Cloud One Workload Securityのアプリケーションコントロール信頼エンティティの「ソースから無視」ルールの「プロセス名」プロパティの使用がサポートされるようになりました。DS-67322
- Deep Security Agentのデータベースサイズ管理がアップデートされ、ディスク容量の使用が最適化されました。DS-67347

解決済みの問題

- Deep Security Managerに接続できない場合、Deep Security Agentがクラッシュすることがありました。DS-67654
- Deep Security Agentによって接続の問題、CPU使用率の増加、またはシステムのクラッシュが発生することがありました。SEG-120758 / SEG-123885 / DS-67291

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-6489/DSSEG-7210/DS-65113

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度 : 高

Deep Security Agent - 20.0.0-3288 (20 LTSアップデート2021-10-28)

リリース日 : 2021年10月28日

ビルド番号 : 20.0.0-3288

新機能

- Agentインストーラの進化 : Deep Security Agentインストーラは、ほとんどのAgentコンテンツをインストールするようになりました。これにより、次の変更が行われます。
  - ほとんどのプラットフォームのインストーラパッケージが若干大きくなるなど、エージェントのサイズ要件が大きくなりました。
  - 保護対象のコンピュータにすべてのエージェントコンテンツがインストールされます。ポリシーまたはManagerコンソールによってプラグインが有効化されるまで、コンピュータ上のコンテンツはアンロードされたままになります。
  - すべてのプラグインインストールで、エージェントにすでにインストールされているコンテンツが使用されるため、エージェントがRelayに依存することが大幅に減少しまし

た。これにより、Relayに接続せずにプラグインをインストールできるため、Relay通信によるプラグインのインストールの問題が軽減されます。

解決済みの問題

- Deep Security Agentがプロキシ経由でManagerに接続できないことがありました。DS-65929
- 一部のユーザで、ランタイムCPU数が予想よりも多いときに問題が発生し、クラッシュすることがありました。DS-65757
- 証明書失効リスト(CRL)が一致しないため、アップグレード中にDeep Security Agentでパッケージ署名エラーが表示されることがありました。DS-65056

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。DS-46018/DSSEG-7210/DSSEG-7217

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度: 高

Deep Security Agent - 20.0.0-3165 (20 LTSアップデート2021-10-08)

リリース日: 2021年10月8日

ビルド番号: 20.0.0-3165

注意: Deep Security Agent 20.0.0.3165がTrend Micro Cloud One - Workload Securityユーザにリリースされました。ただし、Deep Security Agentソフトウェアのダウンロードページからは入手できず、Deep Security Managerを使用しているユーザにはリリースされません。

新機能

- Agentインストーラの進化：Deep Security Agentインストーラは、ほとんどのAgentコンテンツをインストールするようになりました。これにより、次の変更が行われます。
  - ほとんどのプラットフォームのインストーラパッケージが若干大きくなるなど、エージェントのサイズ要件が大きくなりました。
  - 保護対象のコンピュータにすべてのエージェントコンテンツがインストールされます。ポリシーまたはManagerコンソールによってプラグインが有効化されるまで、コンピュータ上のコンテンツはアンロードされたままになります。
  - すべてのプラグインインストールで、エージェントにすでにインストールされているコンテンツが使用されるため、エージェントがRelayに依存することが大幅に減少しました。これにより、Relayに接続せずにプラグインをインストールできるため、Relay通信によるプラグインのインストールの問題が軽減されます。

解決済みの問題

- Deep Security Agentがプロキシ経由でManagerに接続できないことがありました。DS-65929
- 一部のユーザで、ランタイムCPU数が予想よりも多いときに問題が発生し、クラッシュすることがありました。DS-65757

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。DSSEG-7210/DSSEG-7217

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度：高

Deep Security Agent-20.0.0-2921(20 LTS Update 2021-08-30)

リリース日：2021年8月30日

ビルド番号：20.0.0-2921

解決済みの問題

- Deep Security Agentコンソールのコマンドで、Deep Security Relay またはDeep Security Managerのプロキシ情報が返されないことがありました。DS-65419
- Deep Security Agentで、[イベントとレポート]の項目が正しく表示されないことがありました。DSSEG-7057

Deep Security Agent-20.0.0-2740(20 LTS Update 2021-07-29)

リリース日 : 2021年7月29日

ビルド番号 : 20.0.0-2740

機能強化

- Deep Security Agentがアップデートされ、Agentの配信時および有効化時のDeep Security Managerとの接続が改善されました。DS-62547

解決済みの問題

- Deep Security Agentで、Agentから開始される(dsa_control) コンソールコマンドの一部を実行できませんでした。04564385 / SEG-112050 / DSSEG-6990
- Deep Security Managerとの接続の確立中に、Deep Security Agentがクラッシュすることがありました。04634804 / SEG-113539 / DS-64862
- SSL接続の確立中に、Deep Security Agentの接続が切断されることがありました。SF04323898 / SEG-107451 / DS-64268
- 古いバージョンのOSを使用しているシステムでは、Deep Security AgentがWebアプリケーションに接続できないことがありました。SF04451029 / SEG-109652 / DS-64528
- Webレピュテーションを有効にすると、Deep Security Agentによって一部のサードパーティソフトウェアで接続の問題が発生しました。SF04072723/SEG-97952/DSSEG-6963
- 変更監視 を有効にすると、一部のシステムでDeep Security Managerの認証サーバのCPU使用率が高くなりました。04488319 / SEG-110088 / DS-63855

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。SF04613197/SEG-113566/DS-64050

最高共通脆弱性評価システム (CVSS) スコア: 9.8

最高の重大度 : 高

Deep Security Agent-20.0.0-2593(20 LTS Update 2021-07-01)

リリース日 : 2021年7月1日

ビルド番号 : 20.0.0-2593

解決された問題

- Deep Security Agentは、エージェントとマネージャーの通信の問題が原因で、複数の「セキュリティログ監視 エンジン初期化」アラートをトリガーすることがありました。SF03968169 / SEG-95731 / DS-60840
- 変更監視のアラートがトリガされても、[イベントとレポート] タブに表示されないことがありました。04266346/SEG-103731/DS-62992
- 一部の構成で、Deep SecurityAgentが正しいプラットフォームを検出できませんでした。03804296 / SEG-90864 / DS-57809
- アプリケーションコントロールは、PowerShellによって生成された「.tmp」ファイルが原因で複数の「アプリケーションコントロール ソフトウェア変更が検出されました」イベントを検出していました。C1WS-1608

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-5850/DS-54705

最高共通脆弱性評価システム (CVSS) スコア: 4.4

最高の重大度:中

Deep Security Agent - 20.0.0-2395(20 LTSアップデート2021-05-24)

リリース日:2021年5月24日

ビルド番号:20.0.0-2395

新機能

- Deep Security Agent 20.0.0-2395以降では、Entrustのルート認証局 (G2) 証明書がサポートされるようになりました。G2以外のセキュリティ証明書の有効期限は2022/07/09です。それ以降は、Deep Security Agent 20.0.0-2395以降にのみ最新の不正プログラム対策スマートスキャン保護が適用されます。DS-63010

解決された問題

- Deep Security Agentは、証明書失効リスト(CRL) の不一致が原因で、アップグレード中にパッケージ署名エラーを表示することがありました。DS-62154

Deep Security Agent - 20.0.0-2204 (20 LTS Update 2021-04-12)

リリース日:2021年4月12日

ビルド番号: 20.0.0-2204

新機能

強化されたプラットフォームのサポート

- AIXに対する不正プログラム対策のサポート: Deep Security Agent 20.0.0-2204以降では、AIX 6.1、AIX 7.1、およびAIX 7.2に対する不正プログラム対策がサポートされるようになりました。

解決済みの問題

- 不正プログラム対策を有効にすると、Deep Security Agentによって「プロセスの停止」が発生することがあります。SEG-104452/DS-61593

- アプリケーションコントロールがブロックモードの場合、場合によっては適切なソフトウェアインベントリを作成できませんでした。DS-58813
- Webレピュテーションが有効になっていると、システムがクラッシュすることがありました。SF04258834 / SEG-102756 / DS-61067

Deep Security Agent - 20.0.0-2009(20 LTSアップデート2021-03-08)

リリース日 : 2021年3月8日

ビルド番号 : 20.0.0-2009

解決済みの問題

- 古いMQTT接続が適切にクリーンナップされなかったため、MQTT接続はオフラインになりました。SF04236908/SEG-102056/DS-60893

Deep Security Agent - 20.0.0-1876 (20 LTS Update 2021-02-08)

リリース日 : 2021年2月8日

ビルド番号 : 20.0.0-1876

Deep Security Agent - 20.0.0-1822(20 LTSアップデート2021-01-18)

リリース日 : 2021年1月20日

ビルド番号 : 20.0.0-1822

新機能

AIXに対する不正プログラム対策のサポート: Deep Security Agent 20.0.0-1822以降では、AIX 7.1および7.2に対する不正プログラム対策がサポートされるようになりました。

Deep Security Agent - 20.0.0-1681(20 LTSアップデート2021-01-04)

リリース日 : 2021年1月4日

ビルド番号 : 20.0.0-1681

このリリースには、一般的な改善が含まれます。

Deep Security Agent 20.0.0-1559(20 LTSアップデート2020/12/07)

リリース日 : 2020年12月7日

ビルド番号 : 20.0.0-1559

新機能

TLSの方向性: Managerのハートビートポートは、TLSクライアントとTLSサーバの両方として機能できるようになりました。今後のエージェントは、TLSサーバではなくTLSクライアントとして接続します。これにより、接続のTCPレイヤと同じ方向でTLSセッションを開始する必要があるプロキシまたはファイアウォールを介したAgentからの接続の問題が解決されます。

機能強化

- Deep Securityの改善 変更されたパッケージのみをチェックすることで、のパフォーマンスを継承します。DS-55527
- メモリ使用率が向上し、パフォーマンスが向上します。DS-53012

解決済みの問題

- 変更監視が有効になっているSolarisサーバーで、「Unix - Monitor Processes Running From '/tmp' Directories (ATT&CK T1059)」というルールが割り当てられた場合、変更監視ルールで「サポートされていない機能」が参照されたため、ルールのコンパイルエラーが生成されました。DS-55884
- 整合性監視 が有効化されたときに、大量のCPUが使用されました。SEG-88619/03720485 / DS-56613
- アプリケーションコントロールイベントが同じインシデントに対して複数回発生しました。SEG-86213 / SF03620055 / DS-57298

- セキュリティアップデートは新しいコンピュータでは自動的に実行されませんでした。SEG-91484 / SF03828068 / DS-57688

お知らせ

このエージェントのアップデートでは、エージェントマネージャ通信に使用されるTLS証明書の検証がどのように実装されるかが変更されています。エージェントのアクティベーション中に次の警告が表示された場合:

```
[Warning/2] | SSLVerifyCallback() - verify error 20: unable to get local issuer certificate
```

最も根本的な根本原因は、エージェントがマネージャによって証明書に提示されている証明書を検証できないことです。信頼された証明書を固定する必要はありません。この証明書が適用されない場合は無視してください。ただし、信頼された証明書を使用する場合は、Deep Security Agentをアクティベートする前に、"パブリックCAによって発行されたDeep Security Manager証明書チェーンをインポートする" on page 1620によって発行する手順に従ってください。

Deep Security Agent 20.0.0-1337(20 LTSアップデート2020/10/28)

リリース日:2020年10月28日

ビルド番号:20.0.0.1337

解決済みの問題

- SolarisでDeep Security Agentを使用している場合、特定のポートが開かれたユーザIDに関する情報にエージェントがアクセスできなかったため、変更監視 ポート検索機能が機能しませんでした。リスニングポートの情報を保存できないことに起因して発生していました。本Updateの適用後は、Solaris Agentのポート検索機能が変更され、useridの「n/a」文字列が保存されるようになり、この問題が修正されます。これにより残りのポート情報を保存して、ポート検索機能で使用できるようになります。ただし、ユーザIDに基づく検索除外/対象については、この情報を使用できないため正常に機能しません。DS-53922

Deep Security Agent 20.0.0-1304(20 LTSアップデート2020-10-21)

リリース日:2020年10月21日

ビルド番号:20.0.0.1304

機能強化

- 変更監視Deep Security Managerの検索完了時刻が秒単位で1000単位で表示されるようにアップデートしました。DS-54680

解決済みの問題

- Deep Security Agentは、セキュリティ更新プログラムの例外を受信したためのDeep Security Managerは、セキュリティ更新プログラムのタイムアウトを報告しました。SEG-82072 / DS-54720
- Deep Security Managerで ログ検査の ステータスが正しく表示されないことがありました。SEG-77081 / DS-54719

Deep Security Agent 20.0.0-1194(20 LTSアップデート2020-10-05)

リリース日 : 2020年10月5日

ビルド番号 : 20.0.0.1194

機能強化

- の[管理]→[システム設定]→[エージェント] の[同じ名前のコンピュータがすでに存在する場合]設定の範囲を拡張して、既存の非アクティブ化されたコンピュータに適用します。これまでは、既存のアクティベートされたコンピュータにのみ適用されていました。DS-51800
- 変更監視 は、LinuxおよびUnixプラットフォームの「setuid」属性と「setgid」属性に対する変更を検出します。DS-52061

解決済みの問題

- 不正プログラム ディレクトリ除外(ワイルドカード使用) が、サブディレクトリと正しく一致していません。DS-50245
- Deep Security Agentがアップグレード時にSolaris 10でクラッシュしました。SEG-72634 / SF02975849 / DS-49295
- 整合性監視 が有効になっていると、ファイルの所有者が存在しないユーザに誤って変更されました。DS-52058

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-3704/DS-41233

最高共通脆弱性評価システム (CVSS) スコア: 4.4

最高の重大度 : 中

Deep Security Agent 20(長期サポートリリース)

リリース日 : 2020年7月30日

ビルド番号 : 20.0.0.877

新機能

セキュリティの向上

SSLの強化 : Deep SecurityはSSL証明書でハンドシェイクhello_request(rfc5246) および拡張子_then_mac(rfc7366) を暗号化します。

エージェントの整合性チェック: Deep Security Agentで署名が検証され、署名後にソフトウェアファイルが変更されていないことが確認されます。

品質と管理の向上

サポートされているパスへのアップグレード: アクティベーション時のアップグレード機能では、コンピュータ上のAgentが最新の2つのメジャーリリース以降にのみアップグレードされます。Agentが条件を満たしていない場合は、過去2回のメジャーリリース内のリリースにAgentを手動でアップグレードする必要があります。次に、アクティベーション時のアップグレード機能によって新しいバージョンが検出され、指定されたリリースへのアップグレードが完了します。

検索失敗の処理可能な推奨事項 : Deep Security Agentには、予約された不正プログラム検索がキャンセルされた理由と、その対策を推奨する処理に関する情報が表示されます。詳細については、"不正プログラム対策 検索の失敗とキャンセル" on page 1158を参照してください。

不正プログラム対策 リアルタイムファイル検索レポート: Deep Securityは、不正プログラム対策 リアルタイム検索によって検索される上位10個のファイルを特定します。この情報を使用してファイル除外を設定し、不要な検索を回避できるため、パフォーマンスの評価およびチューニングの出発点となります。収集されたデータを含む「AmTopNScan.txt」ファイルは、次の方法を使用して生成できます。

- コマンドdsa_control --AmTopNScanにより
- 診断サービスによる

プロセスの除外設定: プロセス除外設定が次のように改善されました。

- プロセス除外項目が正しく機能しない理由に関する情報が提供されるようになったため、問題のトラブルシューティングを行い、解決するために実行する処理を知ることができます。
- プロセスの例外設定ワークフローが改善され、より堅牢になりました。

環境内のクライアントのバージョンアップを自動化する: Deep Securityは、新しいエージェントを有効にした場合に新しいバージョンにバージョンアップできるかどうかを柔軟に判断できます。これは、アプリケーションチームが古いバージョンのエージェントを含む旧バージョンのゴールドイメージを使用している場合に特に役立ちます。アクティベーション時にバージョンアップを有効にして、エージェントバージョン管理を使用して環境内で使用するクライアントのラインナップを定義します。古いエージェントがオンラインでアクティベートされると自動的にアップグレードされます。

機能強化

- 変更監視では、LinuxおよびUnixプラットフォームの「setuid」属性と「setgid」属性に対する変更が検出されます。
- AWSコネクタでワークスペース同期機能が有効になっていない場合のAmazon WorkSpacesの配信のハートビート処理が改善されました。
- 管理>システム設定>エージェントの同じ名前のコンピュータがすでに存在する場合の範囲が拡張され、既存のコンピュータに適用されます。非アクティブ化されたコンピュータ。これまでは、既存のアクティベートされたコンピュータにのみ適用されていました。
- 検索エンジンのURIパスの長さの制限が増加しました。
- Deep Security Agent 不正プログラム対策が、IntelliScanが無効になっているときにデータタイプに関係なく圧縮ファイルを検索できるようになりました。
- イベント管理の合理化により、エージェントのパフォーマンスが向上します。

- CLIコマンドを使用して、各エージェントのための一般的なスキャンキャッシュを有効または無効にする機能を追加しました。
- Deep Security Agent 不正プログラム対策が、IntelliScanが無効になっているときにデータタイプに関係なく圧縮ファイルを検索できるようになりました。

解決済みの問題

- Deep Security Agentのバージョンアップ後、「アプリケーションコントロール ルールセットの送信に失敗しました」というエラーが発生することがありました。DS-49828
- アプリケーションコントロールと不正プログラム対策が有効になっていると、アプリケーションコントロールがオフラインで表示されることがありました同時に。
- 表示されたパケットヘッダデータに、冗長なペイロードデータが含まれていました。DS-45792
- SSL処理に問題があるため、SSL復号化中にメモリリークが発生しました。SEG-68263/DS-44360
- 特定のDeep Security Agentサーバで、アクティブなアップデートプロセス中にCPU使用率が100%に急上昇し、パターンのマージに失敗しました。SEG-66210/02711299/DS-46429
- 不正プログラム対策の準備が完了する前にセキュリティアップデートが実行された場合、セキュリティアップデートは失敗していました。DS-36952
- ルール「1002875: Unixのソフトウェアの追加と削除」を適用してリアルタイムの変更変更監視を有効にすると、RPMデータベースがロックされる可能性がありました。SEG-67275/SF02663756/DS-48524
- システムロケールがトルコ語に設定されている場合、Webレピュテーション、ファイアウォール、侵入防御、およびセキュリティログ監視を正しく有効にできませんでした。SEG-71825/SF03021819/DS-48916
- 特定のライブラリを正しくリンクしないと、Deep Security Agentが不安定になる可能性があります。SEG-72958/03071960/DS-49324
- ワイルドカードを使用した不正プログラム対策の除外で、サブディレクトリが正しく一致しませんでした。SF03131855/SEG-74892/DS-50245
- アプリケーションコントロールが有効で、ホストアプリケーションが大量の非実行可能ファイルを作成しているときに、CPU使用率が高くなりました。SF02179544/SEG-55745/DS-41142

- 実行権限で開かれた非実行可能ファイルにより、生成されるべきではないセキュリティイベントとドリフトが発生していました。SF01780211/SEG-46616/DSSEG-3607
- Deep Security Agentは、Python拡張モジュール (PYD) ファイルをアプリケーションコントロールのインベントリに追加しませんでした。SF01804378/SEG-47425/DS-33690
- リアルタイムの変更変更監視ファイル検索イベントにUnicodeユーザ名を表示できませんでした。SF02187371/SEG-56645/DS-39398
- 作業中のパケットオブジェクトが誤って削除されたため、Deep Security Agentネットワークエンジンがクラッシュしました。SF01526046/SF02159742/SEG-55453/DS-38812
- 変更変更監視が有効な場合、特定の条件下でds_agentプロセスがクラッシュすることがありました。SEG-50728/DS-35446
- Deep Security AgentからDeep Security Managerへの応答として無効なJSONオブジェクトが送信されたため、Deep Security Managerのログファイルにエラーが発生しました。SF01919585/SEG-48728/DS-34022
- Deep Security AgentでGetDockerVersionエラーが発生したため、[ポリシーの送信] 処理に失敗しました。SF1939658/SEG-49191/DS-34222
- 複数のSmart Protection Serverが設定されている場合、無効なsps_indexが原因でDeep Security Agentプロセスがクラッシュすることがありました。SF01415702/SEG-42919/DS-33008
- Webレピュテーションの場合、Deep Security Agentは不正な資格情報をプロキシに送信しました。プロキシはHTTP 407を返しました。(SF01704358 / SEG-45004 / DS-32077)
- Deep Security Agentの侵入防御モジュールが、ペイロードゼロのUDPパケットを通知なしでドロップしました。SEG-39711/DS-32799
- 変更監視イベントで、Unicodeエンコーディングの不正なファイルパスが表示されました。SEG-45239/DS-33911
- ファイアウォールをオフにしても、インタフェース分離機能がオンのままでした。SEG-32926/DS-27099
- ルール1006540「X-Forwarded-For HTTPヘッダログを有効にする」を適用すると、Deep Securityで侵入防御イベントのX-Forwarded-Forヘッダが正しく抽出されます。ただし、「Invalid Traversal」などのURL侵入は、ヘッダが解析される前にHTTP要求文字列で検出されます。侵入防御エンジンが強化され、ヘッダの解析後にX-Forwarded-Forヘッダを検索するようになりました。SEG-60728/DS-42332

- Deep Security AgentからDeep Security Managerへの応答として無効なJSONオブジェクトが送信されたため、Deep Security Managerのログファイルにエラーが発生しました。SEG-48728/SF01919585/DS-34022
- クラスタを持つSolarisサーバでは、Deep Security 侵入防御モジュールの負荷が高くなり、クラスタのプライベートトラフィックが検査されます。余分な負荷が原因で、レイテンシの問題、ノードの追いつき、および同期イベントの損失が発生しました。

  これで、エージェント上のPacket Processing Engineを設定して、指定されたインターフェイスでトラフィック検査をバイパスできるようになりました。コンピュータの特定のインタフェースがクラスタのプライベートトラフィック専用の場合、この設定を使用して、このインタフェースとの間で送受信されるパケットの検査をバイパスできます。これにより、バイパスされたインタフェースやその他のインタフェースでパケット処理が高速化されます。

  この設定を使用してトラフィック検査をバイパスすることはセキュリティ上の危険です。潜在的な遅延のメリットが関連するリスクを上回るかどうかは、エンドユーザが決定します。また、クラスタ内のノードだけが、そのインタフェースがバイパスされているサブネットにアクセスできるかどうかを判断する必要があります。

  バイパスを実装するには、次の手順を実行します。

1. Deep Security Agentを、この修正が含まれている最新のビルドにアップグレードします。
2. / etcディレクトリに「ds_filter.conf」という名前のファイルを作成します。
3. /etc/ds_filter.conf ファイルを開きます。
4. クラスタ通信に使用されるすべてのNICカードのMACアドレスを次のように追加します。

   ```
   MAC_EXCLUSIVE_LIST=XX:XX:XX:XX:XX,XX:XX:XX:XX:XX
   ```

5. 保存します。
6. 変更が有効になるまで60秒間待ちます。

/etc/ds_filter.conf ファイル内 :

- MAC_EXCLUSIVE_LIST行は、ファイル内の最初の行である必要があります。
- MACアドレスのすべての文字は大文字である必要があります。
- 各バイトの先行ゼロを含める必要があります。

  有効なMAC_EXCLUSIVE_リスト:

  ```
  MAC_EXCLUSIVE_LIST=0B:3A;12:F8:32:5E
  ```

```
MAC_EXCLUSIVE_LIST=0B:3A;12:F8:32:5E,6A:23:F0:0F:AB:34
```

無効なMAC_EXCLUSIVE_リスト:

```
MAC_EXCLUSIVE_LIST=B:3A;12:F8:32:5E
```

```
MAC_EXCLUSIVE_LIST=0b:3a;12:F8:32:5e,6a:23:F0:0F:ab:34
```

```
MAC_EXCLUSIVE_LIST=0B:3A;12:F8:32:5E
```

MACアドレスが無効な場合、インタフェースはバイパスされません。行の先頭に正確な文字列「MAC_EXCLUSIVE_LIST=」がない場合、インタフェースはバイパスされません。DSSEG-4055

セキュリティアップデート

このリリースにはセキュリティアップデートが含まれています。トレンドマイクロが脆弱性に対してどのように保護するかについての詳細は、脆弱性対応をご覧ください。責任ある開示の慣行に従い、すべての影響を受けるリリースに対してパッチが提供された後にのみ、選択されたセキュリティアップデートの共通脆弱性識別子 (CVE) の詳細が公開されることに注意してください。VRTS-3704/VRTS-3176

最高共通脆弱性評価システム (CVSS) スコア: 7.8

最高の重大度 : 高

- NGINXが1.16.1にアップデートされました。DSSEG-4600
- curl 7.67.0にアップデートされました。
- openssl-1.0.2tにアップデートされました。
- JREを最新のJava Update (8.0.241/8.43.0.6) にアップデートしました

macOS (Cloud One Workload Security でのみサポート)

Deep Security Virtual Applianceの新機能

リリース日 : 2020年7月30日

ビルド番号 : 20.0.0.877

Deep Security Virtual Applianceは、2027年8月2日をもって製品サポートサービスを終了いたします。

新機能

セキュリティの向上

NSX-Tの保護機能のサポート:推奨設定の検索、侵入防御の偵察検索、および変更監視は、NSX-T環境では有効になっています。

Deep Security Virtual Applianceでのシームレスな不正プログラム対策保護:vMotionを使用してゲストVMを同じクラスター内の別のESXiホストに移行した後、Deep Security Virtual Applianceのネットワークスキャンと不正プログラム対策スキャンは、中断することなく、遅延なく続行されます。この機能は、NSX-Tデータセンターを使用していて、ゲスト機能がネットワーク機能のオーバーライドのないポリシーを使用している場合にのみ適用されます。

NSX-T環境でのVMの保護:最新のVMwareサービス挿入とゲストイントロスペクションテクノロジが統合され、侵入防御、Webレピュテーション、ファイアウォール、変更監視、およびエージェントレス保護機能を備えたNSX-Tホストでの推奨検索

管理と品質の向上

NSX-Tネットワークスループットの向上:データプレーン開発キット(DPDK), を導入することで、以前のテクノロジと比較してネットワークスループットが3倍高速になりました。

拡張機能

- NSX-T環境でDeep Security Virtual Applianceで保護されたゲストVMの自動アクティブ化に要する時間が短縮されました。
- "VMware NSXポリシー構成の競合"システムイベントを追加しました。このイベントは、Deep Security ManagerがEndpoint ProtectionおよびNetwork Introspection(E-W) のために異なるセキュリティポリシーが設定されたNSX-Tグループを検出した場合に生成されます。
- Deep Security Managerがアップデートされ、仮想マシンのハードウェア情報が不足していてもvCloudアカウントを追加できるようになりました。
- 既存の非アクティベーションコンピュータに適用するには、管理>システム設定>エージェントの[同じ名前のコンピュータがすでに存在する場合]設定の範囲を拡張してください。これまでは、既存のアクティベートされたコンピュータにのみ適用されていました。
- NSX-T ManagerでDeep Security Virtual Appliance SVMをアップグレードすると、新しいSVMがゲストVMを保護していることがDeep Security Managerによって検出され、アップグレード後にこれらのVMが自動的にアクティベートされます。

- Deep Security ManagerのvCloudコネクタがアップグレードされ、vCloud 9.7およびvCloud 10.0がサポートされます。
- Deep Security Managerポリシーを NSX-T環境と同期する機能が追加されました。
- NSX-T Managerを使用したvCenterコネクタの削除時の操作性が向上しました。以前は、サービスプロファイル、エンドポイントルールとサービスの配信、またはvCenterの削除が失敗するため、NSX-Tコンポーネントを手動で削除する必要がありました。

問題を解決する

- Deep Security Virtual Applianceがオフラインになることがありました。SEG-53294
- Deep Security Virtual Applianceの不正プログラム対策エンジンは、Censusサーバの応答の署名者フィールドが空の場合にオフラインになりました。SEG-73047
- ゲストVMが頻繁にESXiホスト間で移行された場合(vMotion), を使用して、VMが状態ファイルを保存できないことがあります。このため、新しいESXiサーバの下でDeep Security Managerによってが自動的に再アクティベートされるまで、Deep Security Virtual Applianceの保護期間は数分かかります。(DSSEG-4341 / DS-38221)
- Deep Security Virtual ApplianceはEicarファイルを検出しませんでした。SEG-71955 / SF02955546 / DS-49387

既知の問題

- NSX-Tが同じサービスチェーンをDeep Securityとサードパーティのサービスに同時にバインドするように設定されている場合、Deep SecurityからのvCenterアカウントの自動削除は失敗します。この問題は、NSX-T APIが、関連するサービスプロファイルを使用してDeep Securityでサービスチェーンを変更できないために発生します。この問題を回避するには、vCenterを手動で削除してください。詳細については、「"NSX環境からのDeep Securityのアンインストール" on page 1731」を参照してください。DS-47944
- Deep Security ManagerはNSX-T Managerバージョン2.xをサポートしていません。NSX-T Managerをバージョン3.0.0以降にバージョンアップします。DS-50387

互換性

システム要件

システム要件については、次のWebサイトを参照してください。

Deep Security:
https://help.deepsecurity.trendmicro.com/20_0/on-premise/system-requirements.html

Cloud One - Workload Security:
https://cloudone.trendmicro.com/docs/workload-security/system-requirements

Deep Security Agentのサポートされるプラットフォームについては以下のページをご確認ください。
https://cloudone.trendmicro.com/docs/jp/workload-security/agent-compatibility

エージェントの要件

Deep Security Agentのプラットフォーム

本バージョンのDeep Security Managerで管理対象となるAgentおよびプラットフォームの一覧は下記のページでご確認ください。

https://help.deepsecurity.trendmicro.com/20_0/on-premise/agent-compatibility.html

以下のプラットフォームについては日本語版ではサポート対象外となります。

- Windows 2000

- Windows XP

- Windows Server 2003

レガシーOSのサポートポリシーについては下記のページをご確認ください。

https://success.trendmicro.com/dcx/s/solution/000262459?language=ja

Linuxカーネルの互換性

Deep Securityは、次のLinuxカーネルスコープをサポートしています。

- 一般カーネル。すべてのユーザが使用できる汎用Linuxカーネルが含まれます。これらのカーネルは、「Deep Security Agentプラットフォームの互換性」に記載されているサポート対象のOSパートナーによって提供されます。
- 次の拡張サポートカーネルを選択します。
  - Red Hat Enterprise Linux (RHEL)。詳細については、Extended Update Support (EUS)を参照してください。
  - SuSE Enterprise Server (SLES)。詳細については、「サービスパックの長期サポート(LTSS)」を参照してください。

サポートされるLinuxカーネルは、エージェントのバージョンによって異なります。

- Deep Security Agent 20のLinuxカーネルサポート
- Deep Security Agentの機能リリース(12.5) Linuxカーネルのサポート
- Deep Security Agent 12.0のLinuxカーネルサポート
- Deep Security Agent 11.3のLinuxカーネルサポート
- Deep Security Agent 11.2のLinuxカーネルサポート
- Deep Security Agent 11.1のLinuxカーネルサポート
- Deep Security Agent 11.0のLinuxカーネルサポート
- Deep Security Agent 10.3のLinuxカーネルサポート
- Deep Security Agent 10.2のLinuxカーネルサポート
- Deep Security Agent 10.1のLinuxカーネルサポート
- Deep Security Agent 10.0のLinuxカーネルサポート
- Deep Security Agent 9.6 SP1のLinuxカーネルサポート
- Deep Security Agent 9.5 SP1のLinuxカーネルサポート

エージェントがスクリプトおよび自動ワークフローでサポートするLinuxカーネルのJSONリストを使用することもできます。

オプションのLinuxカーネルサポートパッケージアップデートを無効にする

Deep Security Agentに次のいずれかのセキュリティモジュールが有効になっている場合、エージェントがロードされてセキュリティ保護を提供するためには、互換性のあるカーネルモジュールをlocalhostにインストールする必要があります

- 不正プログラム対策
- アプリケーションコントロール
- ファイアウォール
- 変更監視
- 侵入防御
- Webレピュテーションサービス

互換性のあるカーネルモジュールがインストールされていない場合、Deep Security Agentは、エージェントの再起動時にカーネルパッケージを自動的に更新設定が有効かどうかに関係なく、最新のカーネルサポートパッケージをダウンロードしてインストールします。

互換性のあるカーネルモジュールがすでにインストールされていて、エージェントの再起動時にカーネルパッケージを自動的に更新する設定が有効になっている場合、Deep Security Agentは最新のカーネルサポートパッケージをダウンロードしてインストールします。

Deep Security Agentがアップグレードされると、以前にインストールされたカーネルモジュールはエージェントと互換性がなくなります。これは、エージェントのバージョンがカーネルサポートパッケージよりも新しいためです。そのため、エージェントはエージェントが再起動する際にカーネルパッケージを自動的に更新する設定が有効かどうかに関係なく、最新のカーネルサポートパッケージをダウンロードしてインストールします。

Linuxカーネルを新しいバージョンにアップグレードすると、以前にインストールされたカーネルモジュールはLinuxカーネルと互換性がなくなります。そのため、エージェントはエージェントが再起動する際にカーネルパッケージを自動的に更新する設定が有効かどうかに関係なく、最新のカーネルサポートパッケージをダウンロードしてインストールします。

以前のエージェントバージョンでは、エージェントが再起動されたりコンピュータが再起動されたりすると、カーネルドライバの更新プロセスが常にRelayから最新のカーネルサポートパッケージをダウンロードしていました。エージェント20.0.0-3067以降およびDeep Security Manager 20.0.503以降では、パフォーマンスを向上させるためにオプションのカーネルサポートパッケージの更新を無効にすることができます。詳細については、"各プラットフォームでサポートされている機能" on page 417を参照してください。

1台のコンピューターでカーネルサポートパッケージの更新を無効にする

1. Deep Security Managerで、[コンピュータ]に進みます。
2. カーネルサポートパッケージのアップデートを無効にするコンピュータをダブルクリックします(または、コンピュータを選択してから[詳細]を選択します)。
3. [設定]を選択します。エージェントの再起動時にカーネルパッケージを自動的に更新するから、

Noを選択します。
4. 変更を保存します。

複数のコンピューターでカーネルサポートパッケージの更新を無効にする

1. Deep Security Managerで、[ポリシー]に移動します。
2. カーネルサポートパッケージのアップデートを無効にする複数のコンピュータを保護するポリシーをダブルクリックします(または、ポリシーを選択してから[詳細]を選択します)。
3. [設定]を選択します。エージェントの再起動時にカーネル パッケージを自動的に更新するから、Noを選択します。
4. 変更を保存します。

Linuxファイルシステムの互換性

リアルタイム不正プログラム対策には、互換性のあるファイルシステムフックが必要です。Linuxプラットフォームでは、さまざまなファイルシステムを使用できます。互換性のあるファイルシステムを次の表に示します。

注意: ネットワークファイルシステムを保護するには、不正プログラム検索の設定で、[ネットワークディレクトリ検索を有効にする] を選択する必要があります。詳細については、「"ネットワークディレクトリを検索する(リアルタイム検索のみ)" on page 846」を参照してください。

ファイルシステムの種類		エージェントのバージョン											
		20	12 FR	12.0	11.3	11.2	11.1	11.0	10.3	10.2	10.1	10.0	9.6
ディスクファイルシステム	ext2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	ext3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	ext4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	XFS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Btrfs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	VFAT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
光ディスク	ISO 9660	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

ファイルシステムの種類		エージェントのバージョン											
		20	12 FR	12.0	11.3	11.2	11.1	11.0	10.3	10.2	10.1	10.0	9.6
特殊なファイルシステム	tmpfs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	aufs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	OverlayFS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ネットワークファイルシステム(この下にある「注意」を参照してください)	NFSv3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	NFSv4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	SMB	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	CIFS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	FTP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Linux systemdのサポート

エージェントの一部のバージョンでは、Linux用 systemd がサポートされます。

✓ – サポートされます。アップデートでサポートが追加された場合は、必要な最小バージョンが脚注に示されます。

• – これらのリリースのサポートはまもなく終了します。できるだけ早くアップグレードしてください。

オペレーティングシステム	エージェントのバージョン			
	20 LTS	12 FR	12 LTS	11 LTS
AlmaLinux 8 (64ビット)	✓ 9			
AlmaLinux 9 (64ビット)	✓ 16			
Amazon Linux 2 (64ビット)				
Amazon Linux 2 (AWS ARMベースのGraviton 2)	✓ 7			

オペレーティングシステム	エージェントのバージョン			
	20 LTS	12 FR	12 LTS	11 LTS
Amazon Linux 2 (AWS ARMベースのGraviton 3)	✓ 12			
Amazon Linux 2023 (64 ビット)	✓ 17			
Amazon Linux 2023 (AWS ARMベースのGraviton 2)	✓ 17			
CloudLinux 8 (64 ビット)	✓	✓ 5		
Debian Linux 10(64 ビット)	✓	✓	✓ 3	✓ 4
Debian Linux 11 (64 ビット)	✓ 10			
Debian Linux 12 (64 ビット)	✓ 21			
Debian Linux 13 (64 ビット)	✓ 30			
Miracle Linux 8 (64 ビット)	✓ 18			
Miracle Linux 9 (64 ビット)	✓ 20			
Oracle Linux 7 (64 ビット)	✓	✓	✓ 3	✓ 2
Oracle Linux 8 (64 ビット)	✓	✓	✓ 6	✓ 4
Oracle Linux 9 (64 ビット)	✓ 15			
Oracle Linux 10 (64 ビット)	✓ 29			
Red Hat Enterprise Linux 7 (64 ビット)	✓	✓	✓ 3	✓ 2
Red Hat Enterprise Linux 8 (64 ビット)	✓	✓	✓	✓ 1
Red Hat Enterprise Linux 8(AWS ARMベースのGraviton 2)	✓ 10			
Red Hat Enterprise Linux 8.6 (PowerPC little-endian)	✓ 19			
Red Hat Enterprise Linux 9 (64 ビット)	✓ 12			

オペレーティングシステム	エージェントのバージョン			
	20 LTS	12 FR	12 LTS	11 LTS
Red Hat Enterprise Linux 9 (PowerPC リトルエンディアン)	✓ 26			
Red Hat Enterprise Linux 9 (64-bit Arm (aarch64))	✓ 27			
Red Hat Enterprise Linux 10 (64ビット)	✓ 28			
Rocky Linux 8 (64ビット)	✓ 9			
Rocky Linux 9 (64ビット)	✓ 14			
Rocky Linux 10 (64ビット)	✓ 30			
SUSE Linux Enterprise Server 12 (PowerPC little-endian)	✓ 22			
SUSE Linux Enterprise Server 15 (64ビット)	✓	✓	✓	✓ 2
SUSE Linux Enterprise Server 15 (PowerPC little-endian)	✓ 22			
SUSE Linux Enterprise Server 15 SP5 (AWS Armベース Graviton2)	✓ 24			
Ubuntu 18.04 (64ビット)	✓	✓		
Ubuntu 18.04 (AWS ARMベースのGraviton 2)	✓ 9			
Ubuntu 20.04 (64ビット)	✓			
Ubuntu 20.04 (AWS ARMベースのGraviton 2)	✓ 9			
Ubuntu 22.04 (64ビット)	✓ 11			
Ubuntu 22.04 (AWS ARMベースのGraviton 2)	✓ 13			
Ubuntu 24.04 (64ビット)	✓ 25			
Ubuntu 24.04 (AWS ArmベースGraviton2)	✓ 31			

脚注:

1
Deep Security Agent 11.0.0-796 U12 (2019-06-22) 以降が必要です。

2
Deep Security Agent 11.0.0-871 U13 (2019-07-26) 以降が必要です。

3
Deep Security Agent 12.0.0-481 U1 (2019-08-09) 以降が必要です。

4
Deep Security Agent 11.0.0-946 U14 (2019-08-29) 以降が必要です。

5
Deep Security Agent 12.5.0-936 FR (2020-05-19) 以降が必要です。

6
Deep Security Agent 12.0.0-563 U2 (2019-09-13) 以降が必要です。

7
Deep Security Agent 20.0.0-1822 (20 LTS Update 2021-01-18) 以降が必要です。

8
Deep Security Agent 20.0.0-3165 (20 LTS Update 2021-10-08) 以降が必要です。

9
Deep Security Agent 20.0.0-3288 (20 LTS Update 2021-10-28) 以降が必要です。

10
Deep Security Agent 20.0.0-3964 (20 LTS Update 2022-03-01) 以降が必要です。

11
Deep Security Agent 20.0.0-4959 (20 LTS Update 2021-07-04) 以降が必要です。

12
Deep Security Agent 20.0.0-5137 (20 LTS Update 2022-07-26) 以降が必要です。

13
Deep Security Agent 20.0.0-5394 (20 LTS Update 2022-08-29) 以降が必要です。

14
Deep Security Agent 20.0.0-6313 (20 LTS Update 2023-01-31) 以降が必要です。

15

Deep Security Agent 20.0.0-6658 (20 LTS Update 2023-03-22) 以降が必要です。

16

Deep Security Agent 20.0.0-6912 (20 LTS Update 2023-05-02) 以降が必要です。

17

Deep Security Agent 20.0.0-7303 (20 LTS Update 2023-06-28) 以降が必要です。

18

Miracle Linux 8は、Deep Security Agent 20.0.0-7719 (20 LTS Update 2023-08-29) 以降のRed Hat Enterprise Linux 8でサポートされます。

19

Deep Security Agent 20.0.0-7943 (20 LTS Update 2023-09-26) 以降が必要です。

20

Miracle Linux 9は、Deep Security Agent 20.0.0-8137 (20 LTS Update 2023-10-26) 以降のRed Hat Enterprise Linux 9でサポートされます。

21

Deep Security Agent 20.0.0-8438 (20 LTS Update 2023-12-12) 以降が必要です。

22

Deep Security Agent 20.0.1-7380 (20 LTS Update 2024-04-24) 以降が必要です。

23

Deep Security Agent 20.0.1-12510 (20 LTS Update 2024-06-26) 以降が必要です。

24

Deep Security Agent 20.0.1-14610 (20 LTS Update 2024-07-20) 以降が必要です。

25

Deep Security Agent 20.0.1-19250 (20 LTS Update 2024-09-18) 以降が必要です。

26
Deep Security Agent 20.0.1-21510 (20 LTS Update 2024-10-16) 以降が必要です。

27

Deep Security Agent 20.0.2-7600 (20 LTS Update 2025-04-16) 以降が必要です。

28

Deep Security Agent 20.0.2-14431 (20 LTS Update 2025-07-09) 以降が必要です。

29

Deep Security Agent 20.0.2-20480 (20 LTS Update 2025-09-24) 以降が必要です。

30

Deep Security Agent 20.0.2-26670 (20 LTS Update 2025-11-20) 以降が必要です。

31

Deep Security Agent 20.0.2-29370 (20 LTS Update 2025-12-09) 以降が必要です。

Linux Secure Bootのサポート

Linux用の一部のバージョンのDeep Security Agent (DSA) はSecure Bootをサポートしています。エージェントのLinux Secure Bootの設定も参照してください。

DSA 20 LTSでは、各Linux OSが対応するSecure Boot公開鍵 (DS2022.der、DS20_V2.derなど) に関連付けられています。これらの鍵には異なる有効期限があります。詳細については、エージェントのLinux Secure Bootを構成するの「トレンドマイクロ公開鍵を更新する - 公開鍵の有効期限が切れました」を参照してください。

関連情報:Deep Securityのリリースライフサイクルとサポートポリシーを参照してください。

Deep Security Agent 20 LTS

次の表は、DSA 20 LTSがSecure Bootをサポートするオペレーティングシステムを示しています。

VMwareと物理マシンは、表に含まれるすべてのオペレーティングシステムでサポートされています。
Azure、AWS、およびGCPのサポートは特定のオペレーティングシステムに限定されています。

オペレーティングシステム	セキュアブート公開鍵	必須DSAビルド	Azure VMでのサポート[1]
AlmaLinux 9 (64ビット)	DS2022.der	20.0.0-6912 (20 LTSアップデート 2023-05-02) 以降	✓
CentOS 7 (64ビット)	DS2022.der[2]		
CentOS 8 (64ビット)	DS2022.der[2]		
Debian Linux 10(64ビット)	DS2022.der[2]		
Debian Linux 11 (64ビット)	DS2022.der		
Debian Linux 12 (64ビット)	DS2022.der	20.0.0-8438 (20 LTS アップデート 2023-12-12) 以降	✓
Debian Linux 13 (64ビット)	DS2022.der	20.0.2-26670 (20 LTSアップデート 2025-11-20) 以降	✓
Miracle Linux 9 (64ビット)	DS2022.der	20.0.0-8137 (20 LTS Update 2023-10-26) 以降のRed Hat Enterprise Linux 9	
Oracle Linux 7 (64ビット)	DS20_V2.der	20.0.0-3165 (20 LTSアップデート 2021-10-08) 以降	
Oracle Linux 8 (64ビット)	DS20_V2.der	20.0.0-3288 (20 LTSアップデート 2021-10-28) 以降	✓[3]
Oracle Linux 9 (64ビット)	DS2022.der		✓[3]
Oracle Linux 10 (64ビット)	DS2022.der	20.0.2-20480 (20 LTSアップデート 2025-09-24) 以降	✓[3]
Red Hat Enterprise Linux 7 (64ビット)	DS2022.der[2]		
Red Hat Enterprise Linux 8 (64ビット)	DS2022.der[2]		✓

オペレーティングシステム	セキュアブート公開鍵	必須DSAビルド	Azure VMでのサポート[1]
Red Hat Enterprise Linux 9 (64ビット)	DS2022.der		✓
Red Hat Enterprise Linux 10 (64ビット)	DS2022.der		✓
Red Hat Enterprise Linux Workstation 7 (64-bit)	DS2022.der[2]	20.0.0-6912 (20 LTSアップデート 2023-05-02) 以降	
Rocky Linux 9 (64ビット)	DS2022.der	20.0.0-6313 (20 LTSアップデート 2023-01-31) 以降	
Rocky Linux 10 (64ビット)	DS2022.der	20.0.2-26670 (20 LTSアップデート 2025-11-20) 以降	
SUSE Linux Enterprise Server 12 (64ビット)	DS2022.der[2]		
SUSE Linux Enterprise Server 15 (64ビット)	DS2022.der, DS20_V2.der[2]		✓
Ubuntu 16.04 (64ビット)	DS2022.der[2]		
Ubuntu 18.04 (64ビット)	DS2022.der[2]		✓
Ubuntu 20.04 (64ビット)	DS2022.der[2]		✓
Ubuntu 22.04 (64ビット)	DS2022.der	20.0.0-6658 (20 LTSアップデート 2023-03-22) 以降	✓
Ubuntu 24.04 (64ビット)	DS2022.der	20.0.1-19250 (20 LTSアップデート 2024-09-18) 以降	

Deep Security Agent 12 FR

次の表は、DSA 12 FRがSecure Bootをサポートするオペレーティングシステムを示しています。

VMwareおよび物理マシンは、表に含まれるすべてのオペレーティングシステムでサポートされていますが、AWS、GCP、およびAzureはサポートされていません。セキュアブートのサポートも参照してください。

OS
CentOS 7 (64-bit)
CentOS 8 (64-bit)
Debian Linux 10(64ビット)
Red Hat Enterprise Linux 7 (64ビット)
Red Hat Enterprise Linux 8 (64-bit)
SUSE Linux Enterprise Server 12 (64-bit)
SUSE Linux Enterprise Server 15 (64-bit)
Ubuntu 16.04 (64-bit)
Ubuntu 18.04 (64-bit)

このDSAリリースには、公開鍵および必要なDSAビルドに関する情報は適用されません。

Deep Security Agent 12 LTS

次の表は、DSA 12 LTSがSecure Bootをサポートするオペレーティングシステムを示しています。

VMwareおよび物理マシンは、表に含まれるすべてのオペレーティングシステムでサポートされていますが、AWS、GCP、およびAzureはサポートされていません。セキュアブートのサポートも参照してください。

OS	Secure Boot公開鍵
CentOS 7 (64-bit)	DS12.der

OS	Secure Boot公開鍵
Red Hat Enterprise Linux 7 (64ビット)	DS12.der

必要なDSAビルドに関する情報は適用されませんのでご注意ください。

Deep Security Agent 11 LTS

次の表は、DSA 11 LTSがSecure Bootをサポートするオペレーティングシステムを示しています。

VMwareと物理マシンは、表に含まれるすべてのオペレーティングシステムでサポートされていますが、AWS、GCP、およびAzureはサポートされていません。セキュアブートのサポートも参照してください。

OS	セキュアブート公開鍵
CentOS 7 (64-bit)	DS11_2022.der
Red Hat Enterprise Linux 7 (64ビット)	DS11_2022.der

必要なDSAビルドに関する情報は適用されませんのでご注意ください。

脚注:

1

詳細については、Azure仮想マシンの信頼できる起動 - サポートされているオペレーティングシステムを参照してください

2

DS20.derは2024年11月26日に期限切れになりました。DS2022.derに置き換えられました。

3

Red Hat互換カーネル (RHCK) のみサポートしています。Unbreakable Enterprise Kernel (UEK) はサポートしていません。

SELinuxのサポート

Security-Enhanced Linux (SELinux) の強制モードは、特定のOSとエージェントの組み合わせで、デフォルトのSELinuxポリシーを使用してサポートされています。

✓ – サポートされます。アップデートでサポートが追加された場合は、必要な最小バージョンが脚注に示されます。

• – これらのリリースのサポートはまもなく終了します。できるだけ早くアップグレードしてください。

オペレーティングシステム	エージェントのバージョン		
	20 LTS	12 FR	12 LTS
AlmaLinux 8 (64ビット)	✓		
AlmaLinux 9 (64-bit)	✓		
Amazon Linux (64ビット)	✓		
Amazon Linux 2 (64ビット)	✓		
Amazon Linux 2 (AWS ArmベースのGraviton2)	✓		
Amazon Linux 2 (AWS ArmベースのGraviton3)	✓		
Amazon Linux 2023 (64ビット)	✓		
Amazon Linux 2023 (AWS ArmベースのGraviton2)	✓		
CentOS 6 (64ビット)	✓		
CentOS 7 (64ビット)	✓		
CentOS 8 (64ビット)	✓		
CloudLinux 8 (64-bit)	✓		
Miracle Linux 8 (64-bit)	✓		
Miracle Linux 9 (64-bit)	✓		
Oracle Linux 6 (32ビット)	✓		
Oracle Linux 6 (64ビット)	✓		
Oracle Linux 7 (64ビット)	✓		

オペレーティングシステム	エージェントのバージョン		
	20 LTS	12 FR	12 LTS
Oracle Linux 8 (64ビット)	✓		
Oracle Linux 9 (64ビット)	✓		
Oracle Linux 10 (64ビット)	✓		
Red Hat Enterprise Linux 6 (32ビットおよび64ビット)	✓		
Red Hat Enterprise Linux 7 (64ビット)	✓	✓ 1	✓ 2
Red Hat Enterprise Linux Workstation 7 (64-bit)	✓		
Red Hat Enterprise Linux 8 (64ビット)	✓	✓ 1	✓ 2
Red Hat Enterprise Linux 8 (AWS ArmベースのGraviton2)	✓		
Red Hat Enterprise Linux 8.6 (PowerPC little-endian)	✓		
Red Hat Enterprise Linux 9 (64ビット)	✓		
Red Hat Enterprise Linux 9 (PowerPC リトルエンディアン)	✓		
Red Hat Enterprise Linux 9 (64-bit Arm (aarch64))	✓		
Red Hat Enterprise Linux 10 (64ビット)	✓		
Rocky Linux 8 (64ビット)	✓		
Rocky Linux 9 (64ビット)	✓		
Rocky Linux 10 (64ビット)	✓		
SUSE Linux Enterprise Server 15 (64ビット)	✓		
SUSE Linux Enterprise Server 15 SP5 (AWS Armベース Graviton2)	✓		

不正プログラム対策ソフトウェアであるエージェントは、コンピュータ全体を保護するために制限されていないドメインで実行する必要があります。追加のSELinuxポリシーのカスタマイズや設定は、エージェン

トをブロックする可能性があります。アラートが発生した場合は、SELinuxアラートのトラブルシューティングを参照してください。

脚注:

1

Deep Security Agent 12.5.0-936 FR (2020-05-19) 以降が必要です。

2

Deep Security Agent 12.0.0-1026 U9 (2020-05-04) 以降が必要です。

各プラットフォームでサポートされている機能

Deep Security 20.0でサポートされる機能は、OSとプラットフォーム、仮想環境のOSとプラットフォーム、およびインストールされているDeep Security Agent (ある場合) のバージョンによって異なります。

詳細については以下を参照してください。https://help.deepsecurity.trendmicro.com/20_0/on-premise/supported-features-by-platform.html

サイジング

Deep Securityの配置のサイジングのガイドラインは、ネットワーク、ハードウェア、およびソフトウェアの規模によって異なります。

Deep Security Managerのサイジング

Deep Security Managerのサイジングの推奨値は、エージェントの数によって異なります。

Agentの数	CPUの数	RAM	JVMプロセスメモリ	Managerノードの数	推奨ディスク容量
<500	2	16 GB	8 GB	2	200 GB
500 ~ 1000	4	16 GB	8 GB	2	200 GB
1000 ~ 5000	4	16 GB	8 GB	2	200 GB
5000 ~ 10000	8	16 GB	12 GB	2	200 GB
10000 ~ 20000	8	24 GB	16 GB	2	200 GB

最大限のパフォーマンスを発揮するには、Deep Security Managerプロセスに十分なJava仮想マシン(JVM) メモリを割り当てることが重要です。"Deep Security Managerのメモリ使用量を設定する" on page 1745を参照してください。

Deep Security Managerの推奨設定の検索はCPU負荷が高くなります。推奨設定の検索を実行する頻度を決定する際には、パフォーマンスへの影響を考慮してください。"推奨設定の検索の管理と実行" on page 728を参照してください。

多数の仮想マシンが同時に再起動され、各AgentがDeep Security Managerとの接続を同時に再確立すると、リソースの使用量が急増する場合があります。

複数のサーバノード

可用性とスケーラビリティを向上させるには、ロードバランサを使用し、2台のサーバ(「ノード」) に同じバージョンのDeep Security Managerをインストールします。これらを同じデータベースに接続します。

各Managerノードがすべてのタスクを実行できます。あるノードが他のノードよりも重要ということはありません。すべてのノードにログインでき、Agent、Appliance、およびRelayはどのノードにも接続できます。1つのノードで障害が発生してもサービスは継続され、データが失われることはありません。

必要となるデータベースのCPU、メモリ、およびディスク容量は、以下の要素によって異なります。

データベースのサイジング

最小ディスク容量 = (2 x Deep Securityのデータサイズ) + トランザクションログ

- 保護されているコンピュータの数
- Deep Security Agentをインストールするプラットフォームの数
- 1秒あたりに記録されるイベント(ログ) の数 (有効になっているセキュリティ機能に関連)
- イベントの保持期間
- データベーストランザクションログのサイズ

最小ディスク容量 = (2 x Deep Securityのデータサイズ) + トランザクションログ

たとえば、データベースとトランザクションログのサイズが40GBの場合は、データベーススキーマのアップグレード中に80GB (40 x 2) の空きディスク容量が必要です。

ディスクの空き容量を増やすには、使用されていないプラットフォーム用の不要なAgentパッケージ("Deep Securityデータベースからソフトウェアパッケージを削除する" on page 519を参照)、トランザクションログ、不要なイベントレコードを削除します。

イベントの保持期間は設定可能です。セキュリティイベントの場合、保持期間はポリシー、個々のコンピュータ設定、またはその両方で設定されます。"ポリシー、継承、およびオーバーライド" on page 724と"ログとイベントの保存に関するベストプラクティス" on page 1154を参照してください。

Deep Securityファイアウォールまたは侵入防御機能を使用する、トラフィックの多いコンピュータでは、1秒あたりに記録するイベント数が多くなるため、パフォーマンスの高いデータベースが必要になることがあります。また、ローカルのイベント保持期間の調整も必要になる場合があります。

- イベントをローカルではなくリモートに保存します。イベントの保持期間を長くする必要がある場合は (コンプライアンスのためなど)、イベントをSIEMまたはSyslogサーバに転送してから、削除機能を使用してローカルコピーを削除します("Deep SecurityイベントをSyslogまたはSIEMサーバに転送する" on page 1171を参照)。

  アプリケーションコントロールと変更監視の一部の操作 (ベースラインの再構築、変更の検索、およびインベントリの変更の検索) では、すべてのレコードがローカルに保持され、削除されることも転送されることもありません。

- 侵入防御を有効にする前に、保護されているコンピュータのソフトウェアにパッチを適用します。推奨設定の検索では、脆弱なOSを保護するために、より多くのIPSルールが割り当てられます。セキュリティイベントが増えると、ローカルまたはリモートのディスク使用量が増加します。
- TCP、UDP、ICMP用のステートフルファイアウォールなど、頻繁にログを記録する不要なセキュリティ機能を無効にします。

Deep Securityファイアウォールまたは侵入防御機能を使用する、トラフィックの多いコンピュータでは、1秒あたりに記録するイベント数が多くなるため、パフォーマンスの高いデータベースが必要になることがあります。また、ローカルのイベント保持期間の調整も必要になる場合があります。

多くのファイアウォールイベントが予想される場合は、許可されたポリシー外のイベントを無効にすることを検討してください。"ファイアウォールの設定" on page 982を参照してください。

"Deep Security Managerのパフォーマンス機能" on page 427も参照してください。

データベースのディスク容量の見積もり

以下の表は、デフォルトのイベント保持設定でのデータベースディスクスペースを推定しています。有効な保護モジュールの合計ディスクスペースが2 or more modulesの値を超える場合は、より小さい推定値を使用してください。例えば、Deep Security 不正プログラム対策、侵入防御システム、および変更監視を使用して750台のエージェントを展開することができます。個々の推奨設定の合計は320 GB(20 GB + 100 GB + 200 GB) ですが、2 or more modulesの推奨設定は300 GBです。したがって、300 GBと見積もることになります。

Agentの数	不正プログラム対策	Web レピュテーションサービス	セキュリティログ監視	ファイアウォール	侵入防御	アプリケーションコントロール	変更監視	2つ以上のモジュール
1 ~ 99	10 GB	15 GB	20 GB	20 GB	40GB	50 GB	50 GB	100 GB
100 ~ 499	10 GB	15 GB	20 GB	20 GB	40GB	100 GB	100 GB	200 GB
500 ~ 999	20 GB	30 GB	50 GB	50 GB	100 GB	200 GB	200 GB	300 GB
1000 ~ 9999	50 GB	60 GB	100 GB	100 GB	200 GB	500 GB	400 GB	600 GB
10,000 ~ 20,000	100 GB	120 GB	200 GB	200 GB	500 GB	750 GB	750 GB	1 TB

データベースのディスク容量は、個々のDeep Security Agentプラットフォームの数に伴って増加します。たとえば、30のAgent (Agentプラットフォームごとに最大5つのバージョン) がある場合、データベースサイズが約5GB増加します。

Deep Security Agent のサイズとリソース消費

次の表は、一般的に使用される機能の組み合わせを使用した環境でのリソース消費の見積もりを示しています。

Deep Security AgentおよびRelayのサイジング

Deep Security AgentおよびRelayのCPU、RAM、ディスクスペースの割り当てに関する要件については、Deep Security Agentの要件およびDeep Security Relayの要件を参照してください。

推定 Deep Security Agent リソース消費量

"Deep Security Virtual Applianceのメモリ割り当て" on page 651も参照してください。

Windowsエージェント

有効なモジュール							RAM
不正プログラム対策	Webレピュテーションサービス	アプリケーションコントロール	変更監視	セキュリティログ監視	ファイアウォール	侵入防御	
✓							156 MB
						✓	148 MB
✓	✓						150 MB
✓	✓					✓	308 MB
✓			✓	✓		✓	280 MB
✓	✓	✓	✓	✓		✓	390 MB
✓	✓	✓	✓	✓	✓	✓	361 MB

Linuxエージェント

有効なモジュール								RAM
不正プログラム対策	Webレピュテーションサービス	アクティビティ監視	アプリケーションコントロール	変更監視	セキュリティログ監視	ファイアウォール	侵入防御	
✓								315 MB
						✓	✓	172 MB
✓							✓	399 MB
✓	✓	✓						312 MB
✓	✓	✓					✓	448 MB
✓				✓	✓		✓	413 MB
✓	✓	✓		✓	✓		✓	492 MB
✓	✓	✓	✓	✓	✓		✓	538 MB

不正プログラム対策ソリューションプラットフォームサービスのCPUサイズ設定

DPDKモードを有効にするには、"DPDKモードを設定する" on page 645してください。

- 不正プログラム対策
- アクティビティ監視

- アプリケーションコントロール
- 変更監視

Applianceが多数の仮想マシンを保護していて、タイムアウトエラーにより推奨設定の検索が失敗する場合は、"推奨設定の検索の管理と実行" on page 728を参照してタイムアウト値を大きくしてください。

- AMSPによる全体的なCPU使用率は約10%です。これには、プロセスの作成、ファイル操作、およびネットワーク操作イベントが含まれます。
- 異なるCPU消費計算方法はより大きなCPU使用結果をもたらす可能性があるため、コアごとのアプローチ(CPU消費をコア数で割る) を取ることをお勧めします。

次の表は、さまざまなVMの組み合わせに対するLinuxエージェントのAMSP CPU消費量とイベント処理能力の詳細なテスト結果を提供します。すべて共通のポリシー(AM、SENSOR、WRSなど) を使用しています。

OVFファイル	vCPU	vRAM
vCPU: 2 RAM: 4 GB	全体: 23% コアごとのCPU使用率: 12.5%	1秒あたり3,523件のイベント、内訳は次のとおりです: • 非同期プロセス: 1秒あたり550 • 同期プロセス: 1秒あたり280 • 非同期ファイル: 1,295毎秒 • ファイル同期: 1,397/秒 • asyncNetwork: 1.2 per second
vCPU: 4 RAM: 8 GB	全体: 43% コアごとのCPU使用率: 10.75%	1秒あたり4,651件のイベント、内訳は次のとおりです: • 非同期プロセス: 751/秒 • 同期プロセス: 1秒あたり377 • 非同期ファイル: 1,705毎秒

OVFファイル	vCPU	vRAM
		• ファイル同期: 1,817/秒 • asyncNetwork: 1秒あたり0.9
vCPU: 8 RAM: 16 GB	全体: 70% コアごとのCPU使用率: 8.75%	1秒あたり5,841イベント、以下を含む: • 非同期プロセス: 1秒あたり970 • 同期プロセス: 1秒あたり485 • 非同期ファイル: 1秒あたり2,128 • ファイル同期: 1秒あたり2,257 • asyncNetwork: 1秒あたり0.9
vCPU: 16 RAM: 32 GB	全体: 127% コアごとのCPU使用率: 7.9%	1秒あたり6,275件のイベント、内訳は以下の通り: • 非同期プロセス: 1,011/秒 • 同期プロセス: 1秒あたり505 • 非同期ファイル: 1秒あたり2,308 • ファイルを同期: 1秒あたり2,450 • asyncNetwork: 1 per second
vCPU: 32 RAM: 64 GB	全体: 120% コアごとのCPU使用率: 3.75%	1秒あたり4,425件のイベント、内訳は以下の通りです: • 非同期プロセス: 749/秒 • 同期プロセス: 1秒あたり375 • 非同期ファイル: 1,603毎秒

OVFファイル	vCPU	vRAM
		• ファイル同期: 1,697/秒 • asyncNetwork: 1 per second
vCPU: 64 RAM: 128 GB	全体: 96% コアごとのCPU使用率: 1.5%	1秒あたり4,346件のイベント、内訳は以下の通りです: • 非同期プロセス: 703毎秒 • 同期プロセス: 1秒あたり352 • 非同期ファイル: 1,600毎秒 • ファイル同期: 1,690/秒 • asyncNetwork: 1 per second

Deep Security Virtual Applianceのサイジング

Deep Security Virtual Appliance ソフトウェアは、一連の Open Virtualization Format (OVF) ファイルとして提供されます。各ファイルには、異なる展開サイズとタイプに対して異なるリソースセットが割り当てられています。次の表を使用して、環境に最適な OVF ファイルを選択できます。

"Deep Security Virtual Applianceのメモリ割り当て" on page 651も参照してください。

OVFファイル	vCPU	vRAM	ディスク容量	仮想ハードウェアバージョン	NSXタイプ	保護されているVMの最大数	DPDKのサポート
dsva.ovf	2	4 GB	20 GB	13 (ESXi 6.5+)	NSX-V	10	不可
dsva-small.ovf	4	8 GB	20 GB	13 (ESXi 6.5+)	NSX-V	50	不可
dsva-medium.ovf	6	16 GB	20 GB	13 (ESXi 6.5+)	NSX-V	200	不可

OVFファイル	vCPU	vRAM	ディスク容量	仮想ハードウェアバージョン	NSXタイプ	保護されているVMの最大数	DPDKのサポート
dsva-large.ovf	8	24 GB	20 GB	13 (ESXi 6.5+)	NSX-V	300	不可
dsva-<20.x.x-xxxx>-C2M4-small.ovf	2	4 GB	20 GB	13 (ESXi 6.5+)	NSX-T	10	不可
dsva-<20.x.x-xxxx>-C4M8-small.ovf	4	8 GB	20 GB	13 (ESXi 6.5+)	NSX-T	10(DPDKが有効な場合) 50(DPDKが無効)	はい*
dsva-<20.x.x-xxxx>-C6M16-medium.ovf	6	16 GB	20 GB	13 (ESXi 6.5+)	NSX-T	200(DPDKが無効の場合)	不可
dsva-<20.x.x-xxxx>-C8M16-medium.ovf	8	16 GB	20 GB	13 (ESXi 6.5+)	NSX-T	DPDKが有効な150	はい*
dsva-<20.x.x-xxxx>-C8M24-large.ovf	8	24 GB	20 GB	13 (ESXi 6.5+)	NSX-T	DPDKが無効な300(DPDKが無効)	不可
dsva-<20.x.x-xxxx>-C12M24-large.ovf	12	24 GB	20 GB	13 (ESXi 6.5+)	NSX-T	300(DPDKが有効な場合)	はい*

* Data Plane Development Kit (DPDK) モードを有効にするには、"DPDKモードを設定する" on page 645を参照してください。

注意:
前述の要件は機能に依存しています:

- 変更監視: 大規模なVDI環境 (ESXiホストあたりの仮想マシンが50以上) では、Deep Security Virtual Applianceではなく、Deep Security Agentを使用してください。
- 不正プログラム対策: 要件は、VMware Guest Introspectionのバージョンによって異なる場合があります。VMware Configuration Maximumsツールを使用してください。
- ファイアウォール、Webレピュテーション、または侵入防御: 要件は、VMware Network Introspection (NSX) のバージョンによって異なる場合があります。VMware Configuration Maximumsツールを参照してください。

ヒント:
上記の要件は、以下の機能によって変化する場合があります。

侵入防御ルールの数	ApplianceのvRAM使用量
350 ~ 400	24 GB
500 ~ 600	30 GB
600 ~ 700	40GB
700以上	50 GB以上

Applianceが多数の仮想マシンを保護していて、タイムアウトエラーにより推奨設定の検索が失敗する場合は、"推奨設定の検索の管理と実行" on page 728を参照してタイムアウト値を大きくしてください。

Deep Security Managerのパフォーマンス機能

パフォーマンスプロファイル

Deep Security Manager は、各ジョブが CPU、データベース、およびエージェントまたはアプライアンスに与える影響を考慮した最適化された同時ジョブスケジューラを使用します。デフォルトでは、新しいインストールは専用マネージャー用に最適化されたより高い容量パフォーマンスプロファイルを使用します。他のリソース集約型ソフトウェアがインストールされているシステムに Deep Security Manager をインストールする場合は、Standard パフォーマンスプロファイルを使用する方が望ましいかもしれません。パフォーマンスプロファイルを変更するには、管理 > マネージャーノードに移動し、マネージャーノードを選択してプロパティを開き、メニューを使用して変更を行います。

パフォーマンスプロファイルは、マネージャーが受け入れるエージェントまたはアプライアンスによって開始された接続の数も制御します。各パフォーマンスプロファイルのデフォルトは、受け入れられた、遅延した、および拒否されたハートビートの量を効果的にバランスします。

ディスク容量不足のアラート

データベースのディスク容量不足

Deep Security ManagerはデータベースからDisk Fullのエラーメッセージを受け取ると、自身のハードドライブにイベントを書き込み、状況を知らせるメールメッセージをすべてのユーザに送信します。この動作は構成できません。

複数のマネージャーノードを実行している場合、イベントはイベントを処理しているノードのディスクに書き込まれます。複数のノードを実行する方法の詳細については、"複数のノードにDeep Security Managerをインストールする" on page 505を参照してください。

データベースのディスク容量の問題が解決されると、Managerは、ローカルに保存されたデータをデータベースに書き込みます。

Managerのディスク容量不足

Deep Security Managerがインストールされているコンピュータの利用可能なディスク容量が10%未満になると、マネージャーは低ディスク容量アラートを生成します。このアラートは通常のアラートシステムの一部であり、設定可能です。詳細については、"アラートの設定" on page 1293を参照してください。

複数のManagerノードを実行している場合、アラートには対象ノードが記載されます。

Managerで利用可能なディスク容量が5 MB未満になると、Managerはすべてのユーザにメールメッセージを送信してシャットダウンします。利用可能なディスク容量が5 MBを超えるまで、Managerを再起動することはできません。

Managerは手動で再起動する必要があります。

複数のノードを実行している場合、ディスク容量不足のノードだけがシャットダウンします。他のマネージャーノードは引き続き動作します。

ポート番号、URL、およびIPアドレス

このドキュメントでは、Deep Securityの初期設定のポート番号、URL、IPアドレス、およびプロトコルについて説明します。ポート、URL、またはIPアドレスが設定可能な場合は、関連する設定ページへのリンクが表示されます。

- "Deep Securityのポート番号" on the next page
- "Deep SecurityのURL" on page 434

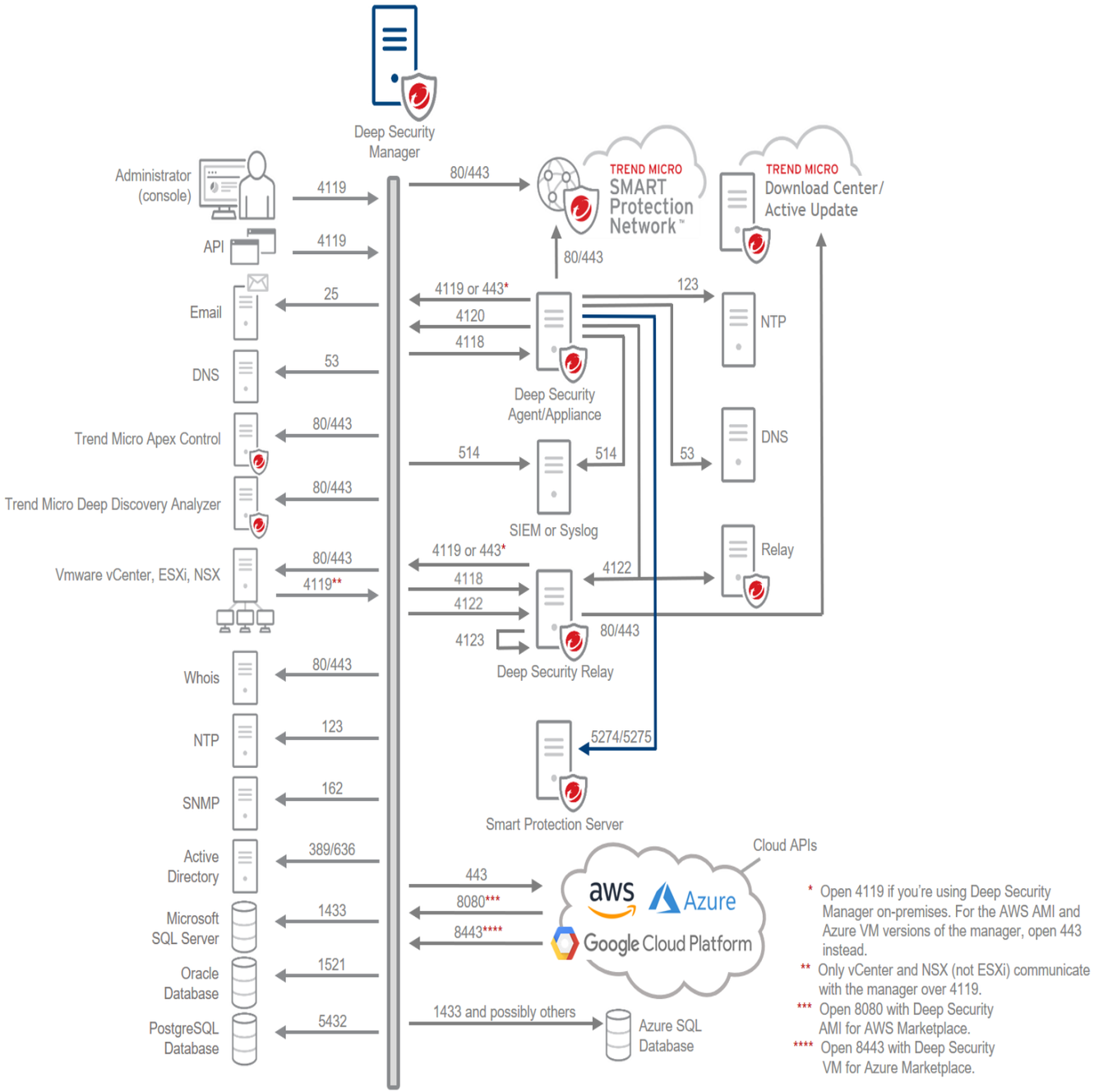
注意: ネットワークでプロキシまたはロードバランサを使用している場合は、このページに表示されているコンポーネントに直接接続するのではなく、接続するようDeep Securityを設定できます。詳細については、"プロキシの設定" on page 1455 および "ロードバランサ" on page 1609を参照してください。

注意: このページのポートの他に、Deep Securityでは、ソケット(送信元ポート)を開くときにエフェメラルポートが使用されます。まれに、これらがブロックされて接続の問題が生じることがあります。詳細については、「"ブロックされたポート" on page 1427」を参照してください。

Deep Securityのポート番号

次の図は、Deep Securityシステムの初期設定のポートを示しています:

Trend Micro Deep Security(オンプレミス) 20



次の表に、初期設定のポートの詳細を示します。この表で必須としてリストされているポートは、Deep Securityシステムが正常に機能するために開く必要があります。オプションとしてリストされているポートは、配置する機能またはコンポーネントに応じて開かれる場合があります。ポート番号はポートと呼ばれます。

ポートの種類	初期設定のポート番号とプロトコル
Deep Security Agent / Appliance待機中(受信)ポート	必須ポート: • 4118 / HTTPS - Deep Security Agent/ appliance ポートです。エージェントが開始した通信を使用する予定の場合は、4118 / HTTPSを閉じたままにしてください。双方向またはマネージャーが開始した通信を使用する予定がある場合のみ開きます。初期設定では、双方向通信が使用されます。そのため、ここでは4118 / HTTPSが「必須」としてリストされています。詳細については、「"AgentとManagerの通信" on page 1499」を参照してください。
Deep Security Agentの/ Appliance送信ポート	必須ポート: • 53 / DNS over TCPまたはUDP – DNSサーバポート • 80 / HTTP、443 / HTTPS - Smart Protection Network ポート、Smart Protection Server (ファイルレピュテーション用) • 123 / NTP over UDP – NTPサーバポート • 4119 / HTTPS - Deep Security Manager GUIおよびAPIポートです。このポートは、配信スクリプトを使用している場合にエージェントソフトウェアをダウンロードするためにも使用されます。 • 4120 / HTTPS – Deep Security Managerエージェントのハートビートポート。双方向またはエージェントが開始した通信を使用している場合は、4120 / HTTPSを許可します。マネージャーが開始した通信を使用している場合は、これを閉じてください。初期設定では、双方向通信が使用されます。そのため、4120 / HTTPSが「'.必須」としてここにリストされています。詳細については、「"AgentとManagerの通信" on page 1499」を参照してください。 • 4122 / HTTPS - Deep Security リレー ポートです。 注意: AWS AMIおよびAzure VMバージョンのManagerを使用する場合は、ポート4119ではなくポート443を開きます。 オプションのポート:

ポートの種類	初期設定のポート番号とプロトコル
	• 514 / Syslog over UDP - SIEMまたはSyslogサーバポートです。エージェントがセキュリティイベントをSIEMまたはSyslogサーバに直接送信するようにする場合は、ポート514を許可します。ポート番号 は、マネージャで設定可能な です。 • 5274/HTTP、5275/HTTPS – Webレピュテーション用のSmart Protection Serverポート。ポート5274および5275は、ファイアウォールではなく、Webレピュテーションのみに必要です。ローカルネットワークまたは仮想プライベートネットワーク(VPC) でSmart Protection Serverをホストする場合、エージェントやアプライアンスがクラウドベースのSmart Protection Networkに80/HTTPおよび443/HTTPSで接続する代わりに、ポート5274および5275を許可します。詳細については、Smart Protection Serverドキュメントを参照してください。
Deep Security Deep Security Relayポート(受信ポート)	• エージェントに待機ポートを許可する(リレーにも適用されるため) • 4122 / HTTPS – Deep Securityリプレイポート。 • 4123 – このポートはエージェントとその内部Relay間の通信に使用されます。
Deep Security Relay送信ポート	• 80 / HTTP、443 / HTTPS – トレンドマイクロのアップデートServer/Active アップデートおよびダウンロードセンターポート • 4119 / HTTPS – Deep Security Manager GUIおよびAPIポート。 • 4122 – 他のDeep Securityリレーのポート。
Deep Security Managerの受信ポート(受信ポート)	必須ポート: • 4119 / HTTPS - Deep Security Manager GUIおよびAPIポートです。このポートは、配信スクリプトを使用している場合にエージェントソフトウェアをダウンロードするためにも使用されます。. 共有およびグローバル アプリケーションコントロール ルールセットにも使用されます。ルールセットがリレーからダウンロードされている場合は除きます。 • 4120 / HTTPS – Deep Security Managerエージェントのハートビートポート。双方向またはエージェントが開始した通信を使用している場合は、4120 / HTTPSを許可します。マネージャーが開始した通信を使用している場合は、これを閉じてください。初期設定では、双方向通信が使用されます。そのため、4120 / HTTPSが「'.必須」としてここにリストされています。詳細については、「"AgentとManagerの通信" on page 1499」を参照してください。

ポートの種類	初期設定のポート番号とプロトコル
Deep Security Manager(送信ポート)	必須ポート: • 53 / DNS over TCPまたはUDP - DNSサーバポート • 80 / HTTP、443 / HTTPS - これらのポートは、さまざまなDeep Securityクラウドサービス、Smart Protection Networkサービス、Trend Micro Apex Central, Deep Discovery Analyzer、VMwareコンポーネント(vCenter、ESXi、NSX), Whoisサーバ、AWS API、およびAzure API、Google Cloud Platform(GCP) API 80および443は、アクセスされるサービスに応じて設定できます。Trend Micro Apex Central および Deep Discovery Analyzer ポート, NSXおよびvCenterポート、および Whoisポートを設定できます。 • 123 / NTP over UDP - NTPサーバのポート番号。NTPサーバには、Trend Micro Apex Centralを使用できます。 • Deep Security Managerのデータベースサーバのポート番号。次から選択: • 1433 / SQL over TCPまたはUDP - Microsoft SQLデータベース ポート • 1433 / SQL over TCP - Azure SQLデータベースポート • 1521 / SQL over TCP - Oracleデータベース ポート • 5432 / SQL over TCP - PostgreSQLデータベースデータベース • 11000-11999 / SQLおよび14000-14999 / SQL over TCP - Azure SQLデータベースの追加ポートです。Allow port 11000-11999 and 14000-14999-1433に加えて - Azure SQLデータベースを使用しており、Deep Security Managerが内でAzureクラウド境界をで実行している場合に許可します。マネージャが外のをAzureクラウド境界で実行している場合は、ポート1433のみがAzure SQLデータベースに接続されている必要があります。詳細については、this Azure documentを参照してください。 • 4118 / HTTPS - Deep Security Agent/ appliance ポートです。エージェントが開始した通信を使用する予定の場合は、4118 / HTTPSを閉じたままにしてください。双方向またはマネージャーが開始した通信を使用する予定がある場合のみ開きます。初期設定では、双方向通信が使用されます。そのため、ここでは4118 / HTTPSが「必須」としてリストされています。詳細については、「"AgentとManagerの通信" on page 1499」を参照してください。 • 4122 / HTTPS - Deep Security リレー ポートです。 オプションのポート: • 25 / TCP over SMTP - メールサーバのポート番号。 メール通知が必要な場合はポート25を許可します。はManagerで設定可能です。

ポートの種類	初期設定のポート番号とプロトコル
	• 162 / SNMP over TCPまたはUDP - SNMPマネージャポート。"リモートコンピュータにSNMP経由でシステムイベントを転送" on page 1293を使用してシステムイベントをリモートコンピュータに転送します。 • 514 / Syslog over UDP - SIEMまたはSyslogサーバポートです。ポート514を許可する場合Deep Securityイベントを外部SIEMまたはSyslogサーバに転送します。514はマネージャで設定可能なです。 • 389 / LDAP、636 / LDAPS、両方向TCP - Active Directoryポートです。許可するポート389と636を許可するActive Directoryからマネージャにコンピュータを追加します。389および636は、Active Directoryサーバが別のポートを使用している場合、マネージャで設定可能なです。 • 4119 – Deep Security Virtual Applianceを使用している場合はポート4119を許可します。このポートは、Deep Security Virtual Applianceの配置時にでOVFを取得するために使用されます。

Deep SecurityのURL

環境内で許可されるURLを制限するには、次の表に示すように、ファイアウォールが送信元から送信先へのトラフィックを許可するようにする必要があります。FQDNごとに、関連付けられたHTTPおよびHTTPS URLへのアクセスを許可する必要があります。たとえば、FQDN files.trendmicro.comの場合、http://files.trendmicro.com:80およびhttps://files.trendmicro.com:443にアクセスを許可します。

送信元	送信先のサーバまたはサービスの名前	送信先の完全修飾ドメイン名(FQDN)
APIクライアント	Deep Security API	• <ManagerのFQDNまたはIP>:4119/webservice/Manager?WSDL • <ManagerのFQDNまたはIP>:4119/api • <ManagerのFQDNまたはIP>:4119/rest
従来のREST APIクライアント	Deep Securityの従来のREST APIのステータス監視API	• <ManagerのFQDNまたはIP>:4119/rest/status/manager/ping

送信元	送信先のサーバまたはサービスの名前	送信先の完全修飾ドメイン名(FQDN)
Deep Security Manager、Deep Security Agent/アプライアンス、Deep Security Relay	ダウンロードセンターまたはWebサーバ ソフトウェアをホストします。	• files.trendmicro.com
Deep Security Manager	Smart Protection Network - ソフトウェア安全性評価サービス(CSSS) イベントのタグ付けと変更監視のために使用されます。	• grid-global.trendmicro.com
Deep Security Manager	トレンドマイクロのVision One "Trend Vision One (XDR) と統合する" on page 1967と統合します。	• *.xdr.trendmicro.com:443 • *.xbc.trendmicro.com:443 • *.mgcp.trendmicro.com:443 • *.manage.trendmicro.com:443 • *.xdr.trendmicro.co.jp:443(日本の地域向け)
Deep Security Agent/Appliance	Smart Protection Network - Global Censusサービス 挙動監視、および機械学習型検索のために使用されます。	20.0以降のクライアント/ appliance 接続先: • ds2000-en-census.trendmicro.com • ds2000-jp-census.trendmicro.com 12.0以降のクライアント/ appliance 接続先: • ds1200-en-census.trendmicro.com • ds1200-jp-census.trendmicro.com 11.0以降のクライアント/ appliance 接続先:

送信元	送信先のサーバまたはサービスの名前	送信先の完全修飾ドメイン名(FQDN)
		• ds1100-en-census.trendmicro.com • ds1100-jp-census.trendmicro.com 10.2および10.3エージェント/ appliance 接続先: • ds1020-en-census.trendmicro.com • ds1020-jp-census.trendmicro.com • ds1020-sc-census.trendmicro.com 10.1および10.0エージェント/ appliance 接続先: • ds1000-en.census.trendmicro.com • ds1000-jp.census.trendmicro.com • ds1000-sc.census.trendmicro.com • ds1000-tc.census.trendmicro.com
Deep Security Agent/Appliance	Smart Protection Network - Good File Reputationサービス 挙動監視、機械学習型検索、およびプロセスメモリ検索のために使用されます。	20.0以降のクライアント/ appliance 接続先: • deepsec20-en.gfrbridge.trendmicro.com • deepsec20-jp.gfrbridge.trendmicro.com 12.0以降のクライアント/ appliance 接続先: • deepsec12-en.gfrbridge.trendmicro.com • deepsec12-jp.gfrbridge.trendmicro.com 11.0以降のクライアント/ appliance 接続先:

送信元	送信先のサーバまたはサービスの名前	送信先の完全修飾ドメイン名(FQDN)
		• deepsec11-en.gfrbridge.trendmicro.com • deepsec11-jp.gfrbridge.trendmicro.com 10.2および10.3エージェント/ appliance 接続先: • deepsec102-en.gfrbridge.trendmicro.com • deepsec102-jp.gfrbridge.trendmicro.com 10.1および10.0エージェント/ appliance 接続先: • deepsec10-en.grid-gfr.trendmicro.com • deepsec10-jp.grid-gfr.trendmicro.com • deepsec10-cn.grid-gfr.trendmicro.com
Deep Security Agent/Appliance	Smart Protection Network - スマートフィードバック	20.0以降のクライアント/ appliance 接続先: • ds200-en.fbs25.trendmicro.com • ds200-jp.fbs25.trendmicro.com 12.0以降のエージェント/ appliance 接続先: • ds120-en.fbs25.trendmicro.com • ds120-jp.fbs25.trendmicro.com 11.0以降のクライアント/ appliance 接続先: • deepsecurity1100-en.fbs25.trendmicro.com

送信元	送信先のサーバまたはサービスの名前	送信先の完全修飾ドメイン名(FQDN)
		• deepsecurity1100-jp.fbs25.trendmicro.com 10.0エージェント/ appliance 接続先: • deepsecurity1000-en.fbs20.trendmicro.com • deepsecurity1000-jp.fbs20.trendmicro.com • deepsecurity1000-sc.fbs20.trendmicro.com
Deep Security Agent/Appliance	Smart Protection Network - スマートスキャンサービス	20.0以降のクライアント/ appliance が接続先: • ds20.icrc.trendmicro.com • ds20-jp.icrc.trendmicro.com 12.0以降のクライアント/ appliance 接続先: • ds120.icrc.trendmicro.com • ds120-jp.icrc.trendmicro.com 11.0以降のクライアント/ appliance 接続先: • ds110.icrc.trendmicro.com • ds110-jp.icrc.trendmicro.com 10.2および10.3エージェント/ appliance 接続先: • ds102.icrc.trendmicro.com • ds102-jp.icrc.trendmicro.com

送信元	送信先のサーバまたはサービスの名前	送信先の完全修飾ドメイン名(FQDN)
		• ds102-sc.icrc.trendmicro.com.cn 10.1および10.0エージェント/ appliance 接続先: • ds10.icrc.trendmicro.com • ds10.icrc.trendmicro.com/tmcss/ • ds10-jp.icrc.trendmicro.com/tmcss/ • ds10-sc.icrc.trendmicro.com.cn/tmcss/ 9.6および9.5エージェント/ appliance 接続先: • iaufdbk.trendmicro.com • ds96.icrc.trendmicro.com • ds96-jp.icrc.trendmicro.com • ds96-sc.icrc.trendmicro.com.cn • ds95.icrc.trendmicro.com • ds95-jp.icrc.trendmicro.com • ds95-sc.icrc.trendmicro.com.cn
Deep Security Agent/Appliance	Smart Protection Network - 機械学習型検索	20.0以降のクライアント/ appliance 接続先: • ds20-en-b.trx.trendmicro.com • ds20-jp-b.trx.trendmicro.com • ds20-en-f.trx.trendmicro.com • ds20-jp-f.trx.trendmicro.com

送信元	送信先のサーバまたはサービスの名前	送信先の完全修飾ドメイン名(FQDN)
		12.0以降のクライアント/ appliance 接続先: • ds120-en-b.trx.trendmicro.com • ds120-jp-b.trx.trendmicro.com • ds120-en-f.trx.trendmicro.com • ds120-jp-f.trx.trendmicro.com 11.0以降のクライアント/ appliance 接続先: • ds110-en-b.trx.trendmicro.com • ds110-jp-b.trx.trendmicro.com • ds110-en-f.trx.trendmicro.com • ds110-jp-f.trx.trendmicro.com 10.2および10.3エージェント/ appliance 接続先: • ds102-en-f.trx.trendmicro.com • ds102-jp-f.trx.trendmicro.com • ds102-sc-f.trx.trendmicro.com
Deep Security Agent/Appliance	Smart Protection Network - Webレピュテーションサービス	20.0以降のクライアント/ appliance 接続先: • ds20-0-en.url.trendmicro.com • ds20-0-jp.url.trendmicro.com 12.0以降のクライアント/ appliance 接続先:

送信元	送信先のサーバまたはサービスの名前	送信先の完全修飾ドメイン名(FQDN)
		• ds12-0-en.url.trendmicro.com • ds12-0-jp.url.trendmicro.com 11.0以降のエージェント/ appliance が接続先: • ds11-0-en.url.trendmicro.com • ds11-0-jp.url.trendmicro.com 10.2および10.3エージェント/ appliance 接続先: • ds10-2-en.url.trendmicro.com • ds10-2-sc.url.trendmicro.com.cn • ds10-2-jp.url.trendmicro.com 10.1および10.0エージェント/ appliance 接続先: • ds100-jp.url.trendmicro.com • ds100-sc.url.trendmicro.com • ds100-jp.url.trendmicro.com 9.6および9.5エージェント/ appliance 接続先: • ds96-jp.url.trendmicro.com • ds96-jp.url.trendmicro.com • ds95-jp.url.trendmicro.com • ds95-jp.url.trendmicro.com

送信元	送信先のサーバまたはサービスの名前	送信先の完全修飾ドメイン名(FQDN)
Deep Security Manager	ヘルプとサポート	• help.deepsecurity.trendmicro.com • success.trendmicro.com/product-support/deep-security
Deep Security Manager	ライセンスと登録サーバ	• licenseupdate.trendmicro.com • clp.trendmicro.com • olr.trendmicro.com
Deep Security Manager	ニュースフィード	• news.deepsecurity.trendmicro.com • news.deepsecurity.trendmicro.com/news.atom • news.deepsecurity.trendmicro.com/news_ja.atom
Deep Security Agentコンピュータ上のブラウザ、およびDeep Security Managerへのログインに使用したコンピュータ	Site Safety	(任意)以下のURLへのリンクがマネージャUI内と、クライアントの[管理者がこのページへのアクセスをブロックしました]ページにあります。 • sitesafety.trendmicro.com • jp.sitesafety.trendmicro.com
Deep Security RelayおよびDeep Security Agent / Appliance	アップデートサーバ セキュリティアップデートをホストします。	• iaus.activeupdate.trendmicro.com • iaus.trendmicro.com • ipv6-iaus.trendmicro.com • ipv6-iaus.activeupdate.trendmicro.com

送信元	送信先のサーバまたはサービスの名前	送信先の完全修飾ドメイン名(FQDN)
Deep Security Manager	AWSとAzure URL Deep Security Managerに AWS アカウントを追加するための 手順、Azure アカウントを追加するための手順、Google Cloud Platform (GCP) サービスアカウントを追加するための手順に使用されます。	AWS URL • AWSのこちらのページ内にある、下記の各見出しの下に表示されているAWSエンドポイントのURL。 • Amazon Elastic Compute Cloud (Amazon EC2) • AWS Security Token Service (AWS STS) • AWS Identity and Access Management (IAM) • Amazon WorkSpaces Azure URL • login.windows.net (認証) • login.microsoftonline.com(認証) • management.azure.com (Azure API) • login.microsoftonline.us(Azure Governmentへの認証) • management.usgovcloudapi.net(Azure Governmentへの認証) • management.core.windows.net (Azure API) 注意: management.core.windows.net URLは、Azureアカウントを Managerに追加するためにDeep Security Manager 9.6で利用可能なv1 Azureコネクタを使用した

送信元	送信先のサーバまたはサービスの名前	送信先の完全修飾ドメイン名(FQDN)
		場合にのみ必要です。Deep Security Manager 10.0以降では、v2コネクタが使用され、このURLにアクセスする必要はありません。 GCP URL • oauth2.googleapis.com(認証) • googleapis.com (GCP API) • cloudresourcemanager.googleapis.com(GCP API)
Deep Security Manager	テレメトリサービス 保護対象の"Deep Security製品使用状況データ収集" on page 1903に使用されます。	• telemetry.deepsecurity.trendmicro.com
Deep Security Manager	有効化 アクティベーションコードを使用してDeep Security Managerを有効化したり、Trend Vision Oneと統合するために使用します。	• flywheel.xdr.trendmicro.com

はじめに

ソフトウェアパッケージのデジタル署名の確認

Deep Securityをインストールする前に、ソフトウェアのZIPパッケージとインストーラファイルのデジタル署名を確認してください。正しいデジタル署名は、ソフトウェアがトレンドマイクロからの正規品であり、破損または改ざんされていないことを示します。

- "ソフトウェアZIPパッケージの署名の確認" below
- "インストーラファイル (EXE、MSI、RPM、またはDEBファイル) の署名の確認" on page 447

ソフトウェアのチェックサム、およびセキュリティアップデートおよびDeep Security Agentモジュールのデジタル署名も検証できます。"Deep Securityによるアップデートの整合性の検証方法" on page 1660および"AgentのLinux Secure Bootの設定" on page 520を参照してください。

ソフトウェアZIPパッケージの署名の確認

Deep Security Agent、Deep Security Virtual Appliance、およびオンラインヘルプは、ZIPパッケージで提供されます。これらのパッケージはデジタル署名されています。ZIPファイルのデジタル署名は、次の方法で確認できます。

管理者との間でZIPをインポートまたはエクスポートすることにより

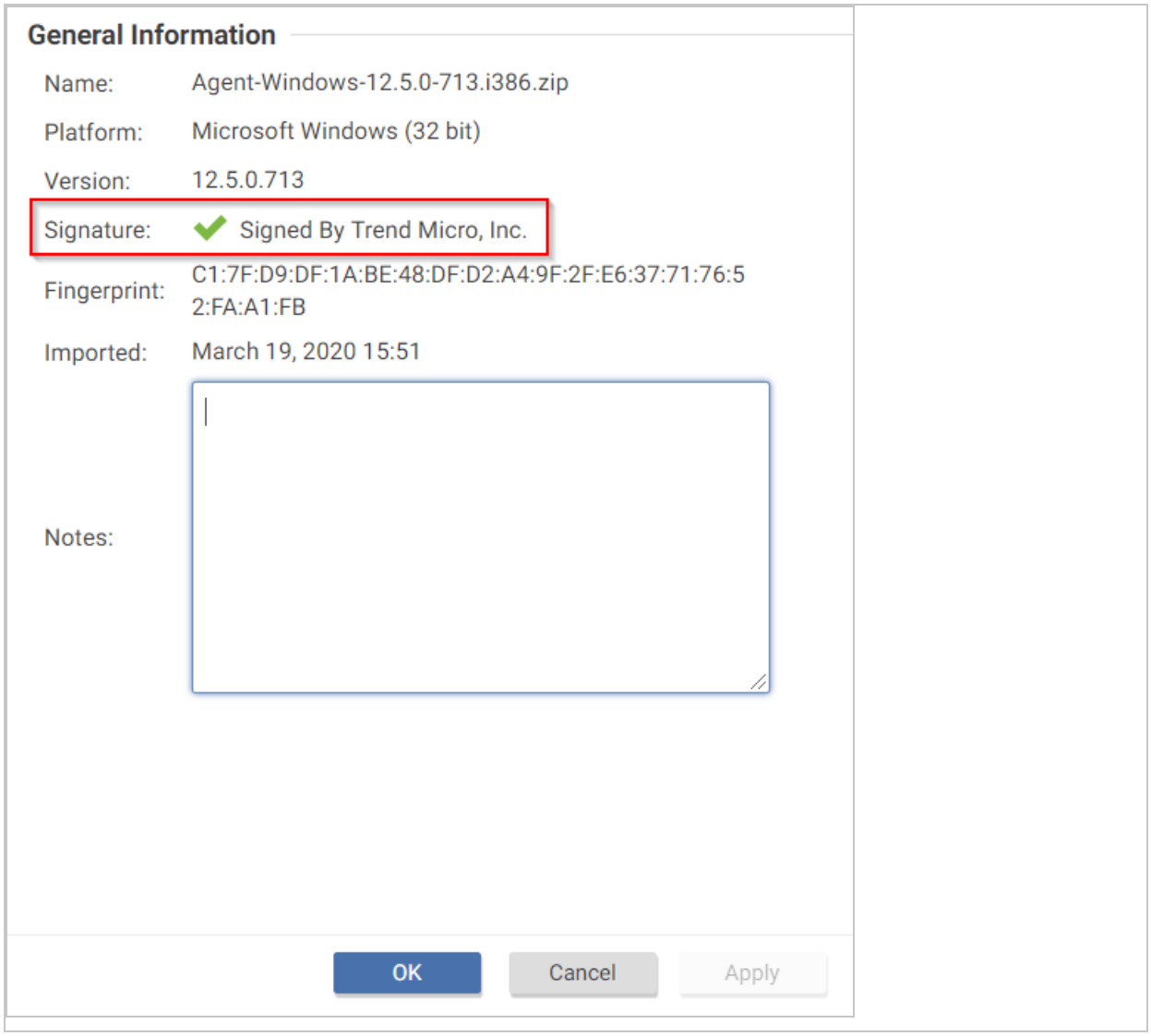
> 指示に従ってインポートまたはエクスポートa ZIPファイル"エージェントソフトウェアのインポート" on page 515または"Agentのインストーラをエクスポートする" on page 517。
>
> Managerはインポートまたはエクスポート時に、ZIPファイルのデジタル署名を確認します。署名が有効な場合、Managerはインポートまたはエクスポートの続行を許可します。署名が無効または見つからない場合、Managerは処理を拒否し、ZIPを削除してイベントをログに記録します。

ZIPのプロパティファイルを表示することで

---

1. Deep Security Managerにログインします。
2. 上部の[管理]をクリックします。
3. 左側のアップデート>ソフトウェア>ローカルを展開します。
4. デジタル署名を確認するZIPパッケージを見つけてダブルクリックします。存在しない場合は、インポートします。

ZIPファイルの[プロパティ]画面が開き、Managerによってデジタル署名が確認されます。署名が有効な場合、次の図に示すように、[署名]フィールドに緑色のチェックマークが表示されます。署名が有効でないか、存在しない場合、ManagerはZIPを削除し、イベントをログに記録します。



jarsignerを使用する

Managerで確認できない場合は、jarsigner Javaユーティリティを使用してa ZIPの署名を確認します。たとえば、Deep Securityソフトウェアのページなど、Manager以外のソースからエージェントのZIPパッケージを取得し、エージェントを手動でインストールするとします。このシナリオでは、Managerが関与しないため、jarsignerユーティリティを使用します。

jarsignerを使用して署名をチェックするには

1. お使いのコンピュータに最新のJava Development Kitをインストールしてください。
2. ZIPをダウンロードします。
3. JDK内のjarsignerユーティリティを使用して、署名を確認します。コマンドは次のとおりです。

   ```
   jarsigner -verify -verbose -certs -strict <ZIP_file>
   ```

   例:

   ```
   jarsigner -verify -verbose -certs -strict Agent-RedHat_EL7-11.2.0-124.x86_64.zip
   ```

4. エラー(エラーがある場合)と証明書の内容を読んで、署名が信頼できるかどうかを判断します。

インストーラファイル(EXE、MSI、RPM、またはDEBファイル)の署名の確認

Deep Security Agent、Deep Security Manager、およびDeep Security Notifierのインストーラは、RSAを使用してデジタル署名されています。インストーラは、Windows上のEXEまたはMSIファイル、Linux OS上のRPMファイル(Amazon、CloudLinux、Oracle、Red Hat、およびSUSE)、またはDebianおよびUbuntuのDEBファイルです。

注意: 以下の手順では、インストーラファイルでデジタル署名を手動で確認する方法について説明します。この確認を自動化したい場合は、これをAgentインストールスクリプトに含めることができます。インストールスクリプトの詳細については、"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849を参照してください。

確認するインストーラファイルの種類に対応する指示に従います。

- "EXEまたはMSIファイルの署名の確認" below
- "RPMファイルの署名の確認" below
- "DEBファイルの署名の確認" on page 450

EXEまたはMSIファイルの署名の確認

1. EXEファイルまたはMSIファイルを右クリックし、[プロパティ]を選択します。
2. [デジタル署名]タブをクリックし、署名を確認します。

RPMファイルの署名の確認

まず、GnuPGをインストールします。

> まだインストールされていない場合は、署名を確認する予定のエージェントコンピュータにGnuPGをインストールしてください。このユーティリティには、署名キーをインポートし、デジタル署名を確認するために必要なGPGコマンドラインツールが含まれています。
>
> ほとんどのLinuxディストリビューションでは、GnuPGがデフォルトでインストールされています。

次に、署名キーをインポートします。

1. エージェントのZIPファイルのルートフォルダにある3trend_public.ascファイルを探します。ASCファイルには、デジタル署名の検証に使用できるGPG公開署名キーが含まれています。
2. 必要に応じて、ハッシュユーティリティを使用してASCファイルのSHA-256ハッシュダイジェストを確認します。ハッシュは次のとおりです。

   c59caa810a9dc9f4ecdf5dc44e3d1c8a6342932ca1c9573745ec9f1a82c118d7 - エージェントバージョン20.0.0-2593以前の場合

   bd3b00763db11cee2a6b990428d506f11cf86c68354388fe9cc41fa7e6c9ddae - エージェントバージョン20.0.0-2971以降の場合

   7a7509c5458c762f6a341820a93e09f0f1b9dd3258608753e18d26575e9c730f - エージェントバージョン20.0.1-3180以降の場合

3. シグネチャをチェックするエージェントコンピュータで、ASCファイルをインポートします。次のコマンドを使用します。

> 注意: コマンドでは大文字と小文字が区別されます。

```
gpg --import 3trend_public.asc
```

次のメッセージが表示されます。

```
gpg: directory `/home/build/.gnupg' created
gpg: new configuration file `/home/build/.gnupg/gpg.conf' created
gpg: WARNING: options in `/home/build/.gnupg/gpg.conf' are not yet active during this run
gpg: keyring `/home/build/.gnupg/secring.gpg' created
gpg: keyring `/home/build/.gnupg/pubring.gpg' created
gpg: /home/build/.gnupg/trustdb.gpg: trustdb created
gpg: key E1051CBD: public key "Trend Micro (trend linux sign) <alloftrendetscodesign@trendmicro.com>" imported
gpg: Total number processed: 1
gpg: imported: 1 (RSA: 1)
```

4. GPGパブリック署名キーをASCファイルからエクスポートします。

   ```
   gpg --export -a 'Trend Micro' > RPM-GPG-KEY-CodeSign
   ```

5. GPGパブリック署名鍵をRPMデータベースにインポートします。

   ```
   sudo rpm --import RPM-GPG-KEY-CodeSign
   ```

6. GPGパブリック署名キーがインポートされたことを確認します。

   ```
   rpm -qa gpg-pubkey*
   ```

7. インポートされたGPG公開鍵のフィンガープリントが表示されます。トレンドマイクロの鍵は:

   `gpg-pubkey-e1051cbd-5b59ac99` - エージェントバージョン20.0.0-2593以前の場合

   `gpg-pubkey-e1051cbd-6030cc3a` - エージェントバージョン20.0.0-2971以降の場合

   `gpg-pubkey-e1051cbd-659d0a3e` - エージェントバージョン20.0.1-3180以降の場合

署名鍵がインポートされ、エージェントRPMファイルのデジタル署名のチェックに使用できます。

最後に、RPMファイルの署名を確認します。

RPMファイルの署名を手動で検証するか、"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849に記載されているように、展開スクリプトにチェックを実行させることができます。

手動チェックを実行するには、次のコマンドを実行してください:

```
rpm -K Agent-PGPCore-<OS agent version>.rpm
```

例:

```
rpm -K Agent-PGPCore-RedHat_EL7-11.0.0-950.x86_64.rpm
```

必ずAgent-PGPCore-<...>.rpmファイルで前述のコマンドを実行してください。Agent-Core-<...>.rpmで実行しても動作しません。エージェントZIPにAgent-PGPCore-<...>.rpmファイルが見つからない場合は、新しいZIPを使用してください。具体的には:

- Deep Securityエージェント11.0 update 15以降のアップデート

  or

- Deep Securityエージェント12 update 2以降

  or

- Deep Security Agent 20以降

署名の検証に成功すると、次のメッセージが表示されます。

```
Agent-PGPCore-RedHat_EL7-11.0.0-950.x86_64.rpm: rsa sha1 (md5) pgp md5 OK
```

DEBファイルの署名の確認

まず、dpkg-sigユーティリティをインストールします。

署名を確認するエージェントコンピュータにdpkg-sigがインストールされていない場合は、インストールします。このユーティリティには、署名キーをインポートしてデジタル署名を確認するために必要なGPGコマンドラインツールが含まれています。

次に、署名キーをインポートします。

1. エージェントのZIPファイルのルートフォルダにある3trend_public.asc ファイルを探します。ASCファイルには、デジタル署名の検証に使用できるGPG公開署名キーが含まれています。
2. 必要に応じて、ハッシュユーティリティを使用してASCファイルのSHA-256ハッシュダイジェストを確認します。ハッシュは次のとおりです。

   c59caa810a9dc9f4ecdf5dc44e3d1c8a6342932ca1c9573745ec9f1a82c118d7 - エージェントバージョン20.0.0-2593以前の場合

   bd3b00763db11cee2a6b990428d506f11cf86c68354388fe9cc41fa7e6c9ddae - エージェントバージョン20.0.0-2971以降の場合

   7a7509c5458c762f6a341820a93e09f0f1b9dd3258608753e18d26575e9c730f - エージェントバージョン20.0.1-3180以降の場合

3. 署名を確認するエージェントコンピュータで、ASCファイルをGPGキーリングにインポートします。次のコマンドを使用します。

   gpg --import 3trend_public.asc

   次のメッセージが表示されます。

   gpg: key E1051CBD: public key "Trend Micro (trend linux sign) <alloftrendetscodesign@trendmicro.com>" imported

   gpg: Total number processed: 1

   gpg: imported: 1 (RSA: 1)

4. オプションで、トレンドマイクロのキー情報を表示します。次のコマンドを使用します。

   gpg --list-keys

   次のようなメッセージが表示されます。

   ```
   /home/user01/.gnupg/pubring.gpg
   ------------------------------
   pub 2048R/E1051CBD 2018-07-26 [expires: 2021-07-25]
   uid Trend Micro (trend linux sign) <alloftrendetscodesign@trendmicro.com>
   sub 2048R/202C302E 2018-07-26 [expires: 2021-07-25]
   ```

最後に、DEBファイルの署名を確認します。

DEBファイルの署名を手動で検証するか、"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849に記載されているように、展開スクリプトにチェックを実行させることができます。

手動チェックを実行するには、次のコマンドを入力してください:

```
dpkg-sig --verify <agent_deb_file>
```

<agent_deb_file> はエージェントのDEBファイルの名前とパスです。たとえば、次のとおりです。

```
dpkg-sig --verify Agent-Core-Ubuntu_16.04-12.0.0-563.x86_64.deb
```

処理メッセージが表示されます。

```
Processing Agent-Core-Ubuntu_16.04-12.0.0-563.x86_64.deb...
```

署名が正常に確認されると、次のメッセージが表示されます。

```
GOODSIG _gpgbuilder CF5EBBC17D8178A7776C1D365B09AD42E1051CBD 1568153778
```

Deep Security Managerを配信する

データベースを準備する

データベースの要件

Deep Security Managerではデータベースサーバを使用します。Deep Security Managerをインストールする前に、次の要件を満たすデータベースサーバをインストールする必要があります。

- "ソフトウェア要件" on the next page
- ハードウェア要件
- ネットワーク要件
- VMwareの要件
- "スケーリングの要件" on page 454

要件を確認したら、でデータベースサーバをインストールする準備が整いました。

ソフトウェア要件

Deep Securityは、次のデータベースをサポートしています。

- PostgreSQL 17.n (Core、Amazon RDS、Amazon Auroraのディストリビューションのみ)
- PostgreSQL 16.n (Core、Amazon RDS、Amazon Auroraのディストリビューションのみ)
- PostgreSQL 15.n (Core、Amazon RDS、Amazon Auroraのディストリビューションのみ)
- PostgreSQL 14.n (Core、Amazon RDS、Amazon Auroraのディストリビューションのみ)
- Microsoft SQL Server 2022 とそのサービス パック
- Microsoft SQL Server 2019 とそのサービスパック
- Microsoft SQL Server 2017 とそのサービスパック
- Microsoft SQL Server 2016 とそのサービス パック
- Microsoft SQL リレーショナルデータベースサービス (RDS)
- Azure SQL Database (except マルチテナント)
- Oracle 19c をソフトウェアとしてデプロイする場合、または Amazon RDS で使用する場合
- ソフトウェアとして展開されたOracle 23c

次の点に注意してください。

- Microsoft SQL Server Expressは、ご限られた構成でのみサポートされます。"Microsoft SQL Server Expressに関する注意事項" belowを参照してください。
- Microsoft SQL Server は、データベースのコンテインメントが NONE に設定されている場合にのみサポートされます。詳細については、コンテインドデータベース を参照してください。
- Oracle Database Express (XE) はサポートされていません。
- Oracle Container Database (CDB) の構成は、Deep Security Managerのマルチテナントではサポートされていません。

Microsoft SQL Server Expressに関する注意事項

製品Q&A「Deep Security 10 以降でサポートされる無償版データベースについて」内の「Microsoft SQL Server Express使用時の注意点」をご確認ください。

ハードウェア要件

- データベースのCPU、メモリ、およびディスクの空き容量は、"データベースのサイジング" on page 418の推奨設定に準じている必要があります。
- データベースは、Managerノードから独立した専用のサーバにインストールします。

  データベースとManagerノードが同居するとシステム負荷が大幅に高まるため、データベースは独立した専用のサーバにインストールすることを推奨します。

  同居する場合は、各プログラムのシステム要件に記載された値を足し合わせた値以上になるようにサイジングする必要があります。

ネットワーク要件

- データベースは、Deep Security Managerと同じネットワークに配置する必要があります。ネットワーク間の通信を円滑にするために、LANには1 GBのLAN接続が必要です。(WAN接続は推奨されません)。これは、Deep Security Managerノードを追加する場合にも該当します。Deep Security Managerからデータベースへの接続の待ち時間は、2ミリ秒以内が推奨されます。
- クラウドでホストされているデータベースは、("multi-AZ"), の複数の可用性ゾーンを使用しないでください。ネットワークの待ち時間が長くなります。

VMwareの要件

VMware環境では、Deep Security Managerとそのデータベースは常に同じESXiホストで実行する必要があります。これを設定するには

1. vCenter Web Clientで、[Host and Clusters] に移動してクラスタを選択します。
2. [Manage] タブに移動して、[VM/Host Rules]→[Add] をクリックします。
3. ルールの名前を入力します。
4. [Enable rule] を選択します。
5. [Type] で [Keep Virtual Machines Together] を選択します。
6. [Add] をクリックし、Managerとデータベースの仮想マシンを選択します。

スケーリングの要件

- スケーラビリティとサービスのアップタイムのために、データベースの負荷分散、ミラーリング、および高可用性(HA) メカニズムを使用する必要があります。セットアップの詳細については、データベースベンダーのドキュメントを参照してください。
- データベースを複製する場合は、データベース複製に対してデータベースミラーリングを使用する必要があります。データベース複製テクノロジでは、複製時にデータベーステーブルに列が追加さ

れることがあります。Deep Securityデータベーススキーマが変更され、重大なエラーが発生する可能性があります。Deep Securityは、スキーマを変更しないフェールオーバー保護テクノロジと連携します。

データベースサーバをインストールする

データベース要件を確認したら、データベースサーバをインストールできます。 手順については、データベースプロバイダのドキュメントを参照してください。

ヒント: すばやく簡単にセットアップするには、postgreSQLを使用してください。無料です。このリンクからダウンロードできます。: PostgreSQL ソフトウェアダウンロードページ

データベースサーバをインストールしたら、を設定する準備が整いました。

データベースの設定

のデータベースのインストール後、Deep Security Managerを設定できます。

まず、データベースインスタンス、データベースユーザ、およびその他のベンダー固有の設定を構成します。次のセクションのいずれかを参照してください:

PostgreSQLの設定

基本設定

1. psql や pgAdmin などのクライアントプログラムを使用して、PostgreSQL データベースサーバーに接続します。
2. 次のコマンドを実行して、空のデータベースインスタンスと適切な権限を持つデータベースユーザを作成します

```
CREATE DATABASE "<database-name>";
CREATE ROLE "<dsm-username>" WITH PASSWORD '<password>' LOGIN;
GRANT ALL ON DATABASE "<database-name>" TO "<dsm-username>";
GRANT CONNECT ON DATABASE "<database-name>" TO "<dsm-username>";
ALTER DATABASE "<database-name>" OWNER TO "<dsm-username>";
```

このユーザは、Deep Security Managerによってデータベースインスタンスに接続するために使用されます。

マルチテナント設定

Deep Security Managerに複数のテナントがある場合

- メインデータベース名を短くします。これにより、テナントのデータベース名が読み取りやすくなります(たとえば、メインデータベースが「dsm」の場合、最初のテナントのデータベース名は「dsm_1」、2番目のテナントのデータベース名は「dsm_2」などとなります) 。
- テナント用の新しいデータベースおよびロールを作成する権限も付与します。

  ALTER ROLE <dsm-username> CREATEDB CREATEROLE;

PostgreSQLチューニング(オプション)

"PostgreSQLを維持する" on page 1576を参照してください。

Microsoft SQL Serverの設定

基本設定

1. Microsoft SQL に接続し、Microsoft SQL Server Management Studio(SSMS) を開きます。
2. 空のデータベースインスタンスを作成します。このデータベースインスタンスはDeep Security Managerで使用されます。
3. db_owner 権限を持つデータベースアカウントを作成します。このアカウントは、Deep Security Managerによってデータベースへの接続に使用されます。
4. データベースインスタンスの TCP/IP プロトコルを有効にします (https://docs.microsoft.com/en-us/previous-versions/bb909712(v=vs.120)?redirectedfrom=MSDN)を参照) 。
5. 接続タイムアウトを設定します。[SQL管理スタジオ]→[SQL Serverプロパティ]→[接続]→リモートクエリタイムアウトを選択し、0(タイムアウトなし) を選択します。この設定により、各データベーススキーマの移行処理に時間がかかっても、アップグレード時にデータベース接続がタイムアウトしなくなります。

マルチテナント設定

Deep Security Managerに複数のテナントがある場合

- メインデータベース名を短くします。これにより、テナントのデータベース名が読み取りやすくなります(たとえば、メインデータベースが「dsm」の場合、最初のテナントのデータ

ベース名は「dsm_1」、2番目のテナントのデータベース名は「dsm_2」などとなります)。

- また、Deep Security Managerで使用されるデータベースアカウントにdbcreator権限を付与します。

Oracleデータベースの構成

基本設定

1. SQL * PlusまたはSQL Developerなどのクライアント・プログラムを使用してOracle Databaseに接続します。
2. 「Oracle Listener」サービスを開始します。TCP接続が許可されていることを確認します。
3. 空のデータベースインスタンスを作成します。このデータベースインスタンスはDeep Security Managerで使用されます。
4. Deep Security Managerがデータベースに接続するために使用するデータベースアカウントを作成します。アカウントを作成する際は、次のガイドラインに従ってください。
   - CONNECT および RESOURCE の役割とUNLIMITED TABLESPACE, CREATE SEQUENCE, CREATE TABLE および CREATE TRIGGER 権限を割り当てます。
   - Deep Security Managerのデータベースユーザ名には特殊文字を使用しないでください。Oracleでは、引用符で囲めばデータベースユーザオブジェクトの設定時に特殊文字を使用できますが、Deep Securityでは、データベースユーザの特殊文字がサポートされていません。

Oracle RACの設定

Oracle RACを使用している場合は、ファイアウォール モジュールを無効にするか、["Oracle RACでのファイアウォール設定" on page 987]の手順に従ってファイアウォールの設定をカスタマイズします。

マルチテナント設定

Deep Security Managerに複数のテナントがある場合

- メインデータベース名を短くします。これにより、テナントのデータベース名が読み取りやすくなります(たとえば、メインデータベースが「MAINDB」の場合、最初のテナントのデータベース名は「MAINDB_1」、2番目のテナントのデータベース名は「MAINDB_2」になります(以下同様))。

- また、Deep Security Managerのデータベースユーザに CREATE USER, DROP USER, ALTER USER, GRANT ANY PRIVILEGE および GRANT ANY ROLE を付与します。
- Oracleコンテナデータベース(CDB) の設定は使用しないでください。では、Deep Security Managerのマルチテナントで がサポートされていません。

次に、次の設定を行ってください

1. 時刻とタイムゾーンの両方を同期させます。データベースとDeep Security Managerサーバの両方で同じ時間ソースを使用します。
2. Deep Security Managerとデータベースサーバ間のネットワーク接続を許可します。"ポート番号、URL、およびIPアドレス" on page 428を参照してください。
3. オプションで暗号化を設定します。"Deep Security Managerとデータベース間の通信の暗号化" on page 1633を参照してください。

データベースを準備したら、Deep Security Managerをインストールできます。

準備チェックを実行する

Managerのインストーラで準備状況チェックを実行して、Deep Security Managerのインストール環境を準備できます。何もインストールされませんが、インストーラは システム要件に準拠していることを確認するためにインストール環境を確認します。その後、Deep Security Managerを実際にインストールする前に、問題の修正に使用できるレポートが生成されます。たとえば、ディスク領域を解放したり、vRAMをさらに割り当てたり、新しいOSをインストールしたりする必要があります。準備ができていない場合は、インストーラをキャンセルして準備完了に戻ることができます。

準備確認を実行するには

管理者のグラフィカルなインタラクティブインストーラを実行して、画面にアクセスしてチェックを実行するオプションが表示されるまで進みます。詳細は、"Deep Security Managerをインストールする" on the next pageのインストールを参照してください。

サイレントレディネスチェックを実行するには

マネージャのサイレントインストーラを `-t` オプションを使用して実行し、インストーラを準備確認モードで実行するよう指示します。詳細については、"Deep Security Managerをサイレント

モードでインストールする" on page 464

- Windowsの例 :

  ```
  Manager-Windows-<Version>.x64.exe -q -console -Dinstall4j.language=<ISO code> -varfile <PropertiesFile> -t
  ```

- Linuxの例 :

  ```
  Manager-Linux-<バージョン>.x64.sh [-q] [-console] -t [-Dinstall4j.language=<ISOコード>] [-varfile <プロパティファイル>]
  ```

注意 : Linuxでは、コンピュータの実際の状態よりも少ないRAMしか検出されない可能性があります。コンピュータの総RAMを確認するには、スーパーユーザアカウントでログインし、次のように入力します。grep MemTotal /proc/meminfo

---

Deep Security Managerをインストールする

トピック:

- "開始前の準備" below
- "Managerをインストールする" on the next page
- "インストールをテストします(マネージャにログオンします) 。" on page 464
- "自己署名証明書を置換する" on page 464を置換します。

ヒント: Deep Security Managerのサポート対象の配置モデルは、Deep Security Best Practiceガイド(PDF) の3.3項に記載されています。マネージャノードの自動スケーリングはではサポートされていません。

開始前の準備

次のインストール前のタスクが完了していることを確認してください。

1. Managerのシステム要件を確認してください。: "システム要件 " on page 400を参照してください。
2. データベースの準備 : "データベースの要件" on page 452, "データベースサーバをインストールする" on page 455および "データベースの設定" on page 455を設定します。

3. ポートを開く: 適切なポート番号で管理者との間で送受信する送受信を許可してください。"Deep Securityのポート番号" on page 429を参照してください。
4. URLの許可: マネージャサーバとの間のURLの制限を計画している場合は、"Deep SecurityのURL" on page 434に記載されているURLを許可してください。
5. クロックの同期: マネージャのサーバのOSクロックをデータベースの時計と同期します。両方のコンピュータで同じNTPサービスを使用する必要があります。
6. DNSの設定: 適切なレコードでDNSを設定して、マネージャ、エージェント、アプライアンス、およびリレーがDNS検索クエリを実行できるようにします。または、IPアドレスを使用するか、マネージャのhostsファイルにエントリを追加します。サーバのDNS名は、0000-dsm.example.comのように数字から始まることはできません。存在する場合は、インストールログに次の情報が表示されます。

   java.io.IOException: DNSName components must begin with a letter
7. マネージャソフトウェアをダウンロード: https://help.deepsecurity.trendmicro.com/ja-jp/software.htmlから入手できます。
8. マネージャのインストーラファイルのデジタル署名を確認します。"インストーラファイル (EXE、MSI、RPM、またはDEBファイル) の署名の確認" on page 447を参照してください。
9. 準備完了チェックを実行します。"準備チェックを実行する" on page 458。

Managerをインストールする

"開始前の準備" on the previous pageを開始する前に、マネージャをインストールする準備ができました。次のいずれかを使用できます。

- グラフィカルなインタラクティブインストーラ(以下の手順に従ってください)
- サイレントインストーラ("Deep Security Managerをサイレントモードでインストールする" on page 464のサイレントインストールを参照)

グラフィカルなインタラクティブインストーラを実行するには

1. LinuxにインストールするGUIが表示されるようにX Windowsシステムがインストールされていることを確認してください。
2. インストーラをroot、スーパーユーザ、または(Windowsの場合) Administratorとして実行します。
3. インストーラの特定のセクションに必要な情報を入力する方法の詳細については、以下のセクションを参照してください。

新規インストールまたはアップグレードの選択

インストーラによって既存のManagerのインストールが検出された場合は、新規インストールまたはアップグレードの選択画面が表示されます。

- 新規インストール(既存または新規のデータベースを使用できます):Deep Securityソフトウェアをインストールし、データベースを初期化します。
- アップグレードのアップグレード:このオプションでは、新しいDeep Securityソフトウェアがインストールされますが、既存のコンピュータの詳細、ポリシー、侵入防御ルール、ファイアウォールルールなどは保持されます。必要に応じてデータベーススキーマが更新されます。必要に応じて、データは新しい形式に移行されます。

警告:[新規インストール(既存または新規のデータベースを使用可能)]を選択すると、以前のインストールからすべてのデータが削除されます。

データベース接続の詳細の設定

1. [データベース]画面で、[Microsoft SQL Server, Oracle Database]または[PostreSQL]("データベースの設定" on page 455を設定します。
2. [ホスト名]フィールドに、データベースホスト名を入力します。
3. [データベース名]に、Deep Securityで使用するために作成した空のデータベースの名前を入力します。
4. Microsoft SQL Serverを選択した場合、マネージャの接続設定は認証の種類によって異なります。
   - SQL Server認証:SQLユーザのユーザ名およびパスワードを入力します。
   - Active Directory認証:Active Directoryユーザのユーザ名(ドメインなし)とパスワードを入力し、[Advanced]をクリックして、ドメインを個別に入力します。Active Directory認証は、Kerberos認証またはWindowsドメイン認証とも呼ばれます。

   注意:"SQL Serverドメイン認証の問題" on page 1997も参照してください。

   注意:Microsoft SQL Serverでは、Windowsワークグループ認証はサポートされていません。
5. Oracle Database または PostgreSQLを選択した場合は、Deep Securityで使用するために作成した空のデータベースに対する権限を持つデータベース・ユーザのユーザ名とパスワードを入力します。

マスターキーの設定

[マスターキー]画面で、マスターキーを設定します。このキーは、マネージャのデータベース、dsm.properties ファイル、および configuration.properties ファイルのパスワードの暗号化に使用されます。次のいずれかのオプションを選択します。

- 後でを設定します。このオプションを選択すると、マスターキーは生成されません。代わりに、インストーラはハードコードされたシードを使用して上記のパスワードを暗号化します。暗号化されたパスワードの先頭には 1が付いています(例 : database.Oracle.password=1***) 。後で、ハードコードされたシードの代わりにマスターキーを使用することにしたければ、dsm_c -action masterkey コマンドを使用して切り替えることができます。詳細については、"コマンドラインの基本" on page 1793を参照してください。
- Amazon Web Services (AWS) Key Management Service (KMS) を使用します。これは、ローカルファイルに依存しないため、キーのプロビジョニングに推奨される方法です。このオプションを選択すると、インストーラはAWS KMSと通信して、256ビットの対称カスタママスターキー(CMK) を取得します。このキーは、上記のパスワードの暗号化に使用されます。まだAWS KMSにCMKがない場合は、AWSの手順に従ってを作成してください。CMKのARNを、マネージャのインストーラの Amazon リソース名 (ARN) フィールドに指定します。ARNを検索するには、AWSの手順に従ってください。暗号化されたパスワードの先頭には DMKが付いています(例 : database.Oracle.password=DMK***) 。
- ローカル環境変数(自動作成) を使用します。このオプションを選択すると、インストーラはマスターキーを生成し、これを使用して前述のパスワードを暗号化します。暗号化されたパスワードのプレフィックスは DMKです。インストーラは、Secret フィールドで指定したシークレットを使用してマスターキーを暗号化し、暗号化されたキーを「name」が「LOCAL_KEY_SECRET」のローカル環境変数に格納します。秘密には次のものを含める必要
  - 大文字
  - 小文字の手紙
  - 数字
  - 特殊文字
  - 8〜64文字の間

  警告 : このシークレットは、Deep Security Managerの初期設定時および の追加マネージャノードのインストール時に必要になるため、削除しないでください。

注意: LOCAL_KEY_SECRET値は、データベースを暗号化する実際のマスターキーを生成する目的で、salt(鍵生成プロセスに提供される一意の追加データ) です。鍵がなければ、データベースを盗む人はそれを復号化できません。塩がなければ、鍵自体は再計算できません。このシークレットのクライアント管理部分は、キー生成プロセスを独自の追加データでカスタマイズするためのオプションとして提供されています。しかし、塩の有無にかかわらず、実際のキーはクリアテキストでは保存されません。また、この文字列は、読み取り専用の権限を持つファイルに保存されます。

同じ場所に配置されたリレーをインストールするかどうかを選択する

Deep Securityには少なくとも1つのリレーが必要です。Relayは保護対象のコンピュータにセキュリティアップデートを配布します。リレーの詳細については、"追加のリレーを配信する" on page 1467。

Deep Security Managerインストーラを実行すると、そのローカルディレクトリ内でエージェントインストーラの完全なZIPパッケージが検索されます。(Relayはその機能を有効にしたAgentです。)ZIPが見つからない場合、マネージャのインストーラはインターネット上のトレンドマイクロダウンロードセンターからダウンロードしようとします。

- どちらかの場所でAgentインストーラが見つかった場合、Managerのインストーラは、最新のRelayをインストールするよう提案します。

ヒント:
次の理由から、トレンドマイクロではサーバ上にRelayをインストールすることを推奨します。

- Managerにとってローカルなリレーを提供する。
- Relayがインストールされた古いコンピュータを廃止した場合も、少なくとも1つのRelayが常に使用可能となる。

警告: Managerのインストーラがそのサーバに追加しても、Relay機能が有効になるだけです。セキュリティの初期設定は適用されません。Deep Security Managerでサーバを保護するには、はそのエージェントにセキュリティポリシーを適用します。

- エージェントのインストーラが見つからない場合は、エージェントをダウンロードしてインストールしたり、後でリレーすることができます。

インストールをテストします(マネージャにログオンします) 。

インストーラの処理が完了すると、「Trend Micro Deep Security Manager」サービスが自動的に開始されます。Deep Security ManagerのGUIにログインするには、Webブラウザを開いて次の場所に移動します。

```
https://[host_name]:[port]/
```

[host_name] はDeep Security Managerをインストールしたサーバのアドレスまたはドメイン名で、[port] はインストール時に指定したManagerのポートです。

例:

```
https://example.dsm.com:4119/
```

自己署名証明書を置換する

Deep Securityをはじめてインストールする場合、Deep Security Managerがエージェント、アプライアンス、リレー、およびWebブラウザとの安全な接続中に自身を識別するために使用する自己署名サーバ証明書が作成されます。有効期限は824日間です。ただし、信頼された認証機関(CA) によって署名されていないため、Webブラウザに警告が表示されます。これらの警告を削除してセキュリティを強化するには、Deep Securityのサーバ証明書を信頼されたCAによって署名された証明書に置き換えることを検討してください。詳細については、"Deep Security ManagerのTLS証明書を変更します。" on page 1622の置換を参照してください。

Deep Security Managerをサイレントモードでインストールする

トピック:

- "開始前の準備" on the next page
- Windowsプラットフォームでサイレントインストールを実行する
- Linuxプラットフォームでサイレントインストールを実行する
- "サイレントインストールのパラメータ" on the next page

- "サンプルインストールの出力" on the next page
- "プロパティファイルのDeep Security設定" on page 468のDeep Security設定
- プロパティファイルの例

開始前の準備

"Deep Security Managerをインストールする" on page 459のインストールですべてのインストール前のタスクを完了していることを確認してください。

Windowsプラットフォームでサイレントインストールを実行する

Windowsプラットフォームでサイレントインストールを開始するには、インストールパッケージと同じフォルダでコマンドプロンプトを開いて、次のコマンドを入力します。

```
Manager-Windows-<Version>.x64.exe -q -console -Dinstall4j.language=<ISO code> -varfile
<PropertiesFile>
```

上記のコマンドのパラメータと変数の詳細については、"サイレントインストールのパラメータ" belowを参照してください。

Linuxプラットフォームでサイレントインストールを実行する

注意: このコマンドを実行する前に、インストールパッケージに対する実行権限を付与してください。

Linuxプラットフォームでサイレントインストールを開始するには、インストールパッケージと同じディレクトリで次のコマンドを入力します。

```
Manager-Linux-<Version>.x64.sh -q -console -Dinstall4j.language=<ISO code> -varfile <PropertiesFile>
```

上記のコマンドのパラメータと変数の詳細については、"サイレントインストールのパラメータ" belowを参照してください。

サイレントインストールのパラメータ

`-q`を指定すると、インストーラが無人 (サイレント) モードで実行されます。

`-console`を指定すると、コンソール (stdout) にメッセージが表示されます。

`-Dinstall4j.language=<ISO code>` を指定すると、他の言語を利用できる場合に初期設定のインストール言語 (英語) を変更できます。ISOの標準の言語識別子を使用して言語を指定します。

- 日本語: ja
- 簡体字中国語: zh_CN

-varfile <PropertiesFile>では、Deep Security Managerのインストール中に適用する各種設定を含んだ標準Javaプロパティファイルへのフルパスを<PropertiesFile>に指定します。各プロパティは、対応するGUI画面や、WindowsのDeep Security Managerインストールの設定を指定します。たとえば、[アドレスとポート] 画面のDeep Security Managerのアドレスは、次のように指定されています。

AddressAndPortsScreen.ManagerAddress=

このファイル内のほとんどのプロパティには初期設定値が割り当てられているため、省略できます。

使用可能な設定の詳細については、プロパティファイル"プロパティファイルのDeep Security設定" on page 468Deep Security設定を参照してください。

-tを指定すると、通常のインストールではなく、インストーラによるシステムチェックが実行されます。

サンプルインストールの出力

ここでは、インストールに成功した場合の出力例を示し、その次にインストールに失敗した場合 (ライセンスが無効な場合) の出力例を示します。トレース内の [Error] タグは、エラーであることを示します。

インストールに成功した場合

```
Stopping Trend Micro Deep Security Manager Service...
 Checking for previous versions of Trend Micro Deep Security Manager...
 Upgrade Verification Screen settings accepted...
 The installation directory has been set to C:\Program Files\Trend Micro\Deep Security Manager.
 Database Screen settings accepted...
 License Screen settings accepted...
 Address And Ports Screen settings accepted...
 Credentials Screen settings accepted...
 Security Update Screen settings accepted...
 Software Update Screen settings accepted...
 Smart Protection Network Screen settings accepted...
 All settings accepted, ready to execute...
 Extracting files ...
 Setting Up...
 Connecting to the Database...
 Creating the Database Schema...
 Creating MasterAdmin Account...
 Recording Settings...
 Creating Temporary Directory...
 Installing Reports...
 Installing Modules and Plug-ins...
 Creating Help System...
 Validating and Applying Activation Codes...
 Configure Localizable Settings...
 Setting Default Password Policy...
 Creating Scheduled Tasks...
 Creating Asset Importance Entries...
 Creating Auditor Role...
 Optimizing...
 Importing Software Packages...
 Configuring Relay For Install...
 Importing Performance Profiles...
 Recording Installation...
 Clearing Sessions...
 Creating Properties File...
 Creating Shortcut...
 Configuring SSL...
 Configuring Service...
 Configuring Java Security...
 Configuring Java Logging...
```

```
Cleaning Up...
Starting Deep Security Manager...
Finishing installation ...
```

インストールに失敗した場合

この例では、プロパティファイルに無効なライセンス文字列が含まれていた場合に生成される出力を示します。

```
Stopping Trend Micro Deep Security Manager Service...
Detecting previous versions of Trend Micro Deep Security Manager...
Upgrade Verification Screen settings accepted...
Database Screen settings accepted...
Database Options Screen settings accepted...
[ERROR] The license code you have entered is invalid.
[ERROR] License Screen settings rejected...
Rolling back changes...
```

プロパティファイルのDeep Security設定

設定プロパティファイル内の各エントリは、次の形式になっています。

`<Screen Name>.<Property Name>=<Property Value>`

設定プロパティファイルには、必須の値とオプションの値があります。

注意: オプションのプロパティに無効な値を入力した場合は、インストーラによって代わりに初期設定値が使用されます。

必須の設定

LicenseScreen

プロパティ	指定できる値	初期設定値
LicenseScreen.License.-1	<すべてのモジュールのアクティベーションコード>	<なし>

または

プロパティ	指定できる値	初期設定値
LicenseScreen.License.0	<不正プログラム対策のアクティベーションコード>	<なし>
LicenseScreen.License.1	<ファイアウォール/侵入防御のアクティベーションコード>	<なし>
LicenseScreen.License.2	<変更監視のアクティベーションコード>	<なし>
LicenseScreen.License.3	<セキュリティログ監視のアクティベーションコード>	<なし>

CredentialsScreen

プロパティ	指定できる値	初期設定値
CredentialsScreen.Administrator.Username	<マスター管理者のユーザ名>	<なし>
CredentialsScreen.Administrator.Password	<マスター管理者のパスワード>	<なし>

オプションの設定

LanguageScreen

プロパティ	指定できる値	初期設定値	備考
sys.languageId	en_US ja	en_US	• 「en_US」=英語。 • 「ja」=日本語。

UpgradeVerificationScreen

この画面は、既存のインストールが検出された場合の処理を決定します。

注意: 既存のインストールが検出されないかぎり、この設定は参照されません。

プロパティ	指定できる値	初期設定値
UpgradeVerificationScreen.Overwrite	• True • False	False

Trueを指定すると、新規インストールが実行され、既存のデータベース内のすべてのデータが破棄されます。False値を指定すると、既存のインストールを修復するオプションが提供されます。

警告: この値をTrueに設定すると、データベース内の既存データがすべて上書きされます。この処理中にプロンプトは表示されません。

OldDataMigrationScreen

この画面では、データを保持する日数を定義します。この設定が0の場合、すべての履歴データが保持されますが、アップグレードにかかるが長くなる可能性があります。データ移行時、サイレントインストールで移行されたレコードの割合が10%単位で表示されます。

注意: データベーススキーマをアップグレードするためにデータ移行が必要な既存のインストールが検出されないかぎり、この設定は参照されません。

プロパティ	指定できる値	初期設定値
OldDataMigrationScreen.HistoricalDays	<整数>	0

DatabaseScreen

この画面ではデータベースタイプを定義したり、オプションとして、特定のデータベースタイプにアクセスする場合に必要なパラメータを定義したりできます。

注意: 対話式インストールでは、[詳細] をクリックしてMicrosoft SQL Serverのインスタンス名およびドメインを定義できます。このフィールドはダイアログに表示されます。無人インストールではダイアログが表示されないため、これらの引数は次に示すDatabaseScreen設定で指定します。

プロパティ	指定できる値	初期設定値	備考
DatabaseScreen.DatabaseType	• Microsoft SQL Server • Oracle • PostgreSQL	Microsoft SQL Server	なし
DatabaseScreen.Hostname	• <データベースのホスト名またはIPアドレス> • <現在のホスト名>	<現在のホスト名>	なし ポート番号は <hostname>:<port>の形式で指定できます。例: example:123
DatabaseScreen.DatabaseName	<文字列>	dsm	
DatabaseScreen.Transport	• Named Pipes • TCP	名前付きパイプ	SQL Serverの場合のみ必須
DatabaseScreen.Username	<データベースのユーザー名>	<なし>	Managerがデータベースサーバへの認証に使用するユーザ名。既存のデータベースアカウントと一致する必要があります。Deep Security Managerのデータベース権限は、このユーザの権限に対応することに

プロパティ	指定できる値	初期設定値	備考
			なります。たとえば、読み取り専用権限のデータベースアカウントを選択した場合、Deep Security Managerはデータベースに書き込みできません。Microsoft SQL ServerおよびOracleには必須です。
DatabaseScreen.Password	<データベースのパスワード>	<なし>	Managerがデータベースサーバへの認証に使用するパスワード。Microsoft SQL ServerおよびOracleには必須です。
DatabaseScreen.SQLServer.Instance	<文字列>	<なし>	単一のサーバまたはプロセッサで複数のインスタンスを使用可能なMicrosoft SQL Serverでのみ使用します。初期設定のインスタンスは1つだけで、他のインスタンスはすべて名前付きインスタンスです。Deep Security Managerデータベースインスタンスが初期設定ではない場合、インスタンス名をここに入力します。値は既存のインスタンスに一致する必要があり、空白にすると、初期設定のインスタンスが指定されます。
DatabaseScreen.SQLServer.Domain	<文字列>	<なし>	Microsoft SQL Serverにのみ使用します。SQL Serverへの認証に使用されるWindowsドメインです。前述のDatabaseScreen.UsernameおよびDatabaseScreen.Passwordは、該当するドメイン内でのみ有効です。
DatabaseScreen.SQLServer.UseDefaultCollation	• True • False	False	Microsoft SQL Serverにのみ使用します。照合(順序)は、文字列の並べ替え方法と比較方法を決定します。値が「False」

プロパティ	指定できる値	初期設定値	備考
			の場合、Deep Securityは、テキスト型の列の照合にLatin1_General_CS_ASを使用します。「True」の場合は、SQL Serverデータベースで指定した照合方法を使用します。照合順序の詳細については、SQL Serverのドキュメントを参照してください。

AddressAndPortsScreen

この画面では、このコンピュータのホスト名、URL、またはIPアドレスと、Managerのポート番号を定義します。

プロパティ	指定できる値	初期設定値	備考
AddressAndPortsScreen.ManagerAddress	<Managerのホスト名、URL、またはIPアドレス>	<現在のホスト名>	なし
AddressAndPortsScreen.ManagerPort	<ポート番号>	4119	"ポート番号、URL、およびIPアドレス" on page 428を参照してください。
AddressAndPortsScreen.HeartbeatPort	<ポート番号>	4120	"ポート番号、URL、およびIPアドレス" on page 428を参照してください。
AddressAndPortsScreen.NewNode	• True • False	False	Trueを指定すると、現在のインストールが新しいノードになります。データベース内に既存データが見つかった場合は、このインストールが新しいノードとして追加されます。マルチノードセットアップは常にサイレントインストールです。注意:「新規ノード」インストールのための既存のデータベース情報は、DatabaseScreenプロパティで指定します。

CredentialsScreen

プロパティ	指定できる値	初期設定値	備考
CredentialsScreen.UseStrongPasswords	• True • False	False	Trueを指定すると、Deep Security Managerで強固なパスワードの使用が強制されます。

MasterKeyConfigurationScreen

プロパティ	指定できる値	初期設定値	備考
MasterKeyConfigurationScreen.KeyConfigType	• Do not configure • Local Key • KMS	Do not configure	値が設定されている場合、インストーラはKMSまたはローカルの秘密鍵を使用してカスタムのマスターキーを生成します。値が設定されていない場合は、代わりにハードコードされたシードが使用されます。「masterkey」も参照してください。 代わりに、インストーラが完了した後でmasterkeyコマンドを実行する必要があります。
MasterKeyConfigurationScreen.ARN	<AWS ARN>	<なし>	KMSキーのAmazon Resource Name (ARN)。MasterKeyConfigurationScreen.KeyConfigType がKMSの場合にのみ使用されます。
MasterKeyConfigurationScreen.LocalKey	<文字列>	<なし>	インストーラがLOCAL_KEY_SECRETローカル環境変数を設定するときに使用する値。MasterKeyConfigurationScreen.KeyConfigType がLocal Keyの場合にのみ使用されます。

SecurityUpdateScreen

プロパティ	指定できる値	初期設定値	備考
SecurityUpdateScreen.UpdateComponents	• True • False	True	True の場合は、セキュリティアップデートを自動的にチェックする予約タスクがDeep

プロパティ	指定できる値	初期設定値	備考
			Security Managerで作成されます。予約タスクは、インストールの完了時に実行されます。
SecurityUpdateScreen.Proxy	• True • False	False	True を指定すると、Deep Security Managerは、プロキシ経由でインターネットに接続して、トレンドマイクロからセキュリティアップデートをダウンロードします。
SecurityUpdateScreen.ProxyType	• HTTP • SOCKS4 • SOCKS5	<なし>	プロキシで使用されるプロトコル。
SecurityUpdateScreen.ProxyAddress	<有効なIPv4またはIPv6のアドレスあるいはホスト名>	<なし>	なし
SecurityUpdateScreen.ProxyPort	<プロキシポート>	<なし>	"ポート番号、URL、およびIPアドレス" on page 428を参照してください。
SecurityUpdateScreen.ProxyAuthentication	• True • False	False	True を指定すると、プロキシに認証資格情報が必要になります。
SecurityUpdateScreen.ProxyUsername	<文字列>	<なし>	なし
SecurityUpdateScreen.ProxyPassword	<文字列>	<なし>	なし

SoftwareUpdateScreen

プロパティ	指定できる値	初期設定値	備考
SoftwareUpdateScreen.UpdateSoftware	• True • False	True	True を指定すると、ソフトウェアアップデートを自動的にチェックする予約タスクがDeep Security Managerで作成されます。予約タスクは、インストールの完了時に実行されます。
SoftwareUpdateScreen.Proxy	• True • False	False	True を指定すると、Deep Security Managerは、プロキシ経由でインターネットに接続して、トレンドマイクロから

プロパティ	指定できる値	初期設定値	備考
			ソフトウェアアップデートをダウンロードします。
SoftwareUpdateScreen.ProxyType	• HTTP • SOCKS4 • SOCKS5	<なし>	プロキシで使用されるプロトコル。
SoftwareUpdateScreen.ProxyAddress	<有効なIPv4またはIPv6のアドレスあるいはホスト名>	<なし>	なし
SoftwareUpdateScreen.ProxyPort	<整数>	<なし>	"ポート番号、URL、およびIPアドレス" on page 428を参照してください。
SoftwareUpdateScreen.ProxyAuthentication	• True • False	False	True を指定すると、プロキシに認証資格情報が必要になります。
SoftwareUpdateScreen.ProxyUsername	<文字列>	<なし>	なし
SoftwareUpdateScreen.ProxyPassword	<文字列>	<なし>	なし

SmartProtectionNetworkScreen

この画面では、トレンドマイクロスマートフィードバックを有効にするかどうかを定義します。オプションとして業種を定義することもできます。

プロパティ	指定できる値	初期設定値	備考
SmartProtectionNetworkScreen.EnableFeedback	• True • False	False	True を指定すると、トレンドマイクロスマートフィードバックが有効になります。
SmartProtectionNetworkScreen.IndustryType	• Not specified • Banking • Communications and media • Education	<なし>	値が入力されていない場合は、Not specified と同じ結果になりま

プロパティ	指定できる値	初期設定値	備考
	• エネルギー • Fast-moving consumer goods (FMCG) • Financial • Food and beverage • Government • Healthcare • Insurance • Manufacturing • Materials • Media • Oil and gas • Real estate • Retail • Technology • Telecommunications • Transportation • Utilities • Other		す。

RelayScreen

この画面では、Deep Security RelayをDeep Security Managerと同じコンピュータにインストールするかどうかを定義します。

プロパティ	指定できる値	初期設定値	備考
RelayScreen.Install	• True • False	False	True を指定すると、Deep Security RelayがDeep Security Managerコンピュータにインストールされます。 False を指定すると、Deep Security RelayがDeep

プロパティ	指定できる値	初期設定値	備考
			Security Managerにインストールされません(サイレントインストールの場合)。または、Relayをインストールするかどうか尋ねる画面が表示されます(通常インストールの場合)。

プロパティファイルの例

一般的なプロパティファイルの例を次に示します。

```
AddressAndPortsScreen.ManagerAddress=10.xxx.xxx.xxx
AddressAndPortsScreen.NewNode=True
UpgradeVerificationScreen.Overwrite=False
LicenseScreen.License.-1=XY-ABCD-ABCDE-ABCDE-ABCDE-ABCDE-ABCDE
DatabaseScreen.DatabaseType=Microsoft SQL Server
DatabaseScreen.Hostname=10.xxx.xxx.xxx
DatabaseScreen.Transport=TCP
DatabaseScreen.DatabaseName=XE
DatabaseScreen.Username=DSM
DatabaseScreen.Password=xxxxxxx
AddressAndPortsScreen.ManagerPort=4119
AddressAndPortsScreen.HeartbeatPort=4120
CredentialsScreen.Administrator.Username=masteradmin
CredentialsScreen.Administrator.Password=xxxxxxxx
CredentialsScreen.UseStrongPasswords=False
SecurityUpdateScreen.UpdateComponents=True
SecurityUpdateScreen.Proxy=False
SecurityUpdateScreen.ProxyType=
SecurityUpdateScreen.ProxyAddress=
SecurityUpdateScreen.ProxyPort=
SecurityUpdateScreen.ProxyAuthentication=False
SecurityUpdateScreen.ProxyUsername=
SecurityUpdateScreen.ProxyPassword=
SoftwareUpdateScreen.UpdateSoftware=True
SoftwareUpdateScreen.Proxy=False
SoftwareUpdateScreen.ProxyType=
SoftwareUpdateScreen.ProxyAddress=
SoftwareUpdateScreen.ProxyPort=
SoftwareUpdateScreen.ProxyAuthentication=False
SoftwareUpdateScreen.ProxyUsername=
```

```
SoftwareUpdateScreen.ProxyPassword=
RelayScreen.Install=True
SmartProtectionNetworkScreen.EnableFeedback=False
```

アクティベーションコードを追加

1つまたは複数のアクティベーションコードをマネージャに入力する必要があります。インストール時にそれらを指定しなかった場合。

注意: アクティベーションコードはライセンスとも呼ばれます。

アクティベーションコードを入力するには

1. Deep Security Managerにログインします。
2. 上部にある[Administration]をクリックします。
3. 左側の[Licenses]をクリックします。
4. メイン画面で、[Enter New Activation Code]をクリックします。
5. 販売店から取得したアクティベーションコードを入力します。
6. [次へ] [ ]の順にクリックし、終了したらウィザードを閉じます。

マルチテナントを設定する

マルチテナント環境の設定

Deep Securityのマルチテナント機能を使用すると、1つのDeep Security Manager内に個別の管理環境を作成できます。これにより、各テナントが独自の設定とポリシーを持ち、自分のイベントをモニタすることができます。これは、別々のステージング環境と本番環境を作成したい場合や、組織内の異なるビジネスユニットのために個別の環境を作成する必要がある場合に便利です。また、サービスモデルで顧客にDeep Securityを提供するためにマルチテナントを使用することもできます。

マルチテナントを有効にすると、あなた(プライマリテナント)は通常のDeep Security Managerのインストールのすべての機能を保持します。ただし、その後に作成するテナントは、システムの設定方法に基づいて、Deep Securityの機能へのアクセスがさまざまな程度に制限される可能性があります。

注意: FIPSモードはマルチテナント環境ではサポートされていません。詳細については、"FIPS 140のサポート" on page 1870を参照してください。

このトピックの内容:

- "マルチテナントの要件" below
- "マルチテナントを有効にする" on the next page
- "テナントを作成する" on the next page
- "スケーラビリティのガイドライン" on page 482
- "マルチテナントに関するヒント" on page 483
- "テナントを管理する" on page 484
- "マルチテナント環境の設定" on the previous page
- "使用状況の監視" on page 488
- "データベースのユーザアカウントを設定する" on page 490
- "API" on page 498
- "マルチテナント環境のアップグレード" on page 499
- "テナントをサポートする" on page 500
- "Deep Security Virtual Appliance環境のマルチテナント" on page 500

マルチテナントの要件

次のいずれかでマルチテナントを設定することはできません:

- Deep Security Manager VM for Azure Marketplace
- Azure SQLデータベース

マルチテナントにはアクティベーションコードが必要です。マルチテナントには追加のデータベース要件もあります。詳細については、"データベースの要件" on page 452 および "データベースのユーザアカウントを設定する" on page 490を参照してください。

スケーラビリティを最大化するために、複数ノードのDeep Security Managerを使用することをお勧めします ("複数のノードにDeep Security Managerをインストールする" on page 505を参照)。すべてのManagerノードが、任意のテナントのGUI、ハートビート、またはジョブの要求を処理します。バックグラウンド処理については、各テナントに、ジョブの処理待ち、メンテナンス、およびその他のバックグラウンドタスクを処理するManagerノードが割り当てられます。タスクは、Managerノードが追加またはオフラインにされたときに、残りのノードに再調整されます。

マルチテナントを有効にすると、Deep Security Managerの現在のインストール環境がプライマリテナント(t0)になり、他のテナントの作成などの特別な権限を付与されます。他のテナントは特定の機能の使用を制限されており、Deep Security Managerでそれらの機能のUIを表示する権限を持っていません。たとえば、プライマリ以外のテナントが他のテナントを作成することはできません。詳細については、"マルチテナント環境の設定" on the previous pageを参照してください。

マルチテナントを有効にする

1. Deep Security Managerで、管理 > システム設定 > 詳細設定に移動します。マルチテナントオプションエリアで、マルチテナントを有効にするをクリックして、マルチテナント構成ダイアログを開きます。
2. マルチテナント構成ダイアログで、マルチテナントアクティベーションコードを入力し、次へをクリックしてください。
3. 使用したいライセンスモードを選択してください。
   - プライマリテナントからライセンスを継承: すべてのテナントにプライマリテナントと同じライセンスを使用します。準備環境でマルチテナントを使用する場合や、同じ組織内の部門ごとにテナントを設定する場合は、このオプションが推奨されます。
   - テナントごとのライセンス: この構成では、テナントを作成する際にDeep Security APIを使用してライセンスを提供することができます。または、テナントが初めてDeep Security Managerにサインインする際にライセンスを入力することができます。
4. [次へ] をクリックします。

   ダイアログが閉じると、管理 > システム設定 > テナントが表示され、マルチテナントオプションを設定できます。

マルチテナントを有効にすると、無効にしたり、プライマリテナントを削除したりすることはできませんのでご注意ください。

テナントを作成する

マルチテナントモードが有効になったら、[管理]→[テナント] からテナントを管理できます。

テナントの追加に必要なデータベースのユーザアカウントの権限の詳細については、"データベースのユーザアカウントを設定する" on page 490を参照してください。

1. Deep Security Managerで、管理 > テナントに移動し、新規をクリックして新規テナントダイアログを開きます。
2. 新しいテナントダイアログで、テナントアカウント名を入力します。プライマリテナント用に予約されているPrimary以外の任意の名前を使用できます。
3. テナントへの連絡に使用されるメールアドレスを入力してください。
4. ロケールを選択して、テナントのDeep Security Managerユーザインターフェースの言語を決定します。
5. タイムゾーンを選択します。イベントの時間は、イベントが発生したシステムのタイムゾーンではなく、このタイムゾーンを基準にして表示されます。

6. Deep Securityインストールで複数のデータベースを使用している場合、新しいテナントアカウントを保存するデータベースサーバをDeep Securityに自動的に選択させる(自動 -- 優先なし)か、特定のサーバを使用するかを選択します。新しいテナントを受け入れていないデータベースサーバはリストに表示されません。
7. 新しいテナントアカウントの最初のユーザのユーザ名を入力します。
8. 次の3つのパスワードオプションのうち1つを選択します。

    - メールなし: テナントの最初のユーザのユーザ名とパスワードを設定します。メールは送信されません。
    - 確認リンクをメール: テナントの最初のユーザのパスワードを設定します。ただし、ユーザが確認メールのリンクをクリックするまでアカウントは有効になりません。メール確認によって、ユーザがアカウントにアクセスする前に、指定されたメールアドレスがユーザのものであることを確認できます。
    - 生成したパスワードをメール: パスワードを指定せずにテナントを生成できます。

    3つのオプションはすべて、APIにより利用可能となります。メール確認オプションは、一般ユーザが登録するのに適しています。テナントの作成者がプログラムではなく人であることを確認する方法として、CAPTCHAが推奨されています。
9. 次へをクリックしてテナントの作成に進みます。スキーマの作成と初期データの投入により、最大で4分かかることがあります。これにより、各新しいテナントが最新の構成を持ち、特に複数のデータベースサーバー間でデータベーステンプレートを管理する負担が軽減されます。

各テナントデータベースには約100 MBのディスク容量のオーバーヘッドがあります(初期設定でシステムに入力されるルール、ポリシー、およびイベントに起因)。

Deep Security APIを使用してテナントの作成と構成を自動化できます。例については、Deep Security Automation Centerのテナントの作成と管理ガイドを参照してください。

テナントに送信されるメッセージの例

確認リンクをメール: アカウント確認要求

Welcome to Deep Security! To begin using your account, click the following confirmation URL. You can then access the console using your chosen password.

Account Name: ExampleCorp

User name: admin

Click the following URL to activate your account:

https://managerIP:portnumber/SignIn.screen?confirmation=1A16EC7A-D84F-D451-05F6-706095B6F646&tenantAccount=ExampleCorp&username=admin

生成したパスワードをメール

1通目のメール: アカウントとユーザ名の通知

Welcome to Deep Security! A new account has been created for you. Your password will be generated and provided in a separate email.

Account Name: ExampleCorp

Username: admin

You can access Deep Security using the following URL:

https://managerIP:portnumber/SignIn.screen?tenantAccount=ExampleCorp&username=admin

2通目のメール: パスワード通知

This is the automatically generated password for your Deep Security account. Your Account Name, Username, and a link to access Deep Security will follow in a separate email.

Password: z3IgRUQ0jaFi

SQL Server可用性グループにテナントデータベースを追加する

Deep Security ManagerがSQL Server Always On可用性グループに接続されている場合、新しいテナントデータベースを既存の可用性グループに自動的に追加することはできません。SQL Server Always On可用性グループデータベースに接続されたDSMのテナントを追加または削除するに記載されている手順に従って手動で行うことができます。

スケーラビリティのガイドライン

テナント数が50 ~ 100、またはこれを超える環境では、スケーラビリティの問題を避けるために次のガイドラインに従う必要があります。

- Deep Security Managerノードセット1つにつき作成するテナント数は最大2000です。
- 1つのデータベースサーバで作成するテナント数は最大300です。
- プライマリテナントには別のデータベースサーバを使用し、他のテナントは含めません。
- 1テナントあたりのエージェント数は3000に制限します。
- エージェントの総数は20000に制限します。

- 使用するDeep Security Managerノードは最大2つです。
- Relayを同じ場所に配置して使用しません。

マルチテナントでは、複数のデータベース(Microsoft SQLを使用する場合)または複数のユーザ(Oracleを使用する場合)が使用されます。規模を拡大する場合は、Deep Security Managerを複数のデータベースサーバに接続し、使用可能な一連のデータベースサーバに新しいテナントを自動的に分散させることができます。"データベースのユーザアカウントを設定する" on page 490を参照してください。

マルチテナントに関するヒント

攻撃の予兆IPリスト

マルチテナント環境では、テナントがDeep Security ManagerのIPアドレスを「攻撃の予兆を無視」IPリスト([ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト]の順に選択)に追加することが必要になる場合があります。これは、「攻撃の予兆の検出: ネットワークまたはポートの検索」警告が表示されないようにするためです。

複数のデータベースサーバを使用する

マルチテナントでは、複数のデータベース(Microsoft SQLを使用する場合)または複数のユーザ(Oracleを使用する場合)が使用されます。規模を拡大する場合は、Deep Security Managerを複数のデータベースサーバに接続し、使用可能な一連のデータベースサーバに新しいテナントを自動的に分散させることができます。"データベースのユーザアカウントを設定する" on page 490を参照してください。

テナントの「削除の保留中」状態

テナントは削除できますが、処理はすぐに実行されません。Deep Securityでは、レコードを削除する前に、テナント関連のすべてのジョブが完了している必要があります。最も頻度の低いジョブは毎週実行されるため、テナントは最大で約7日間、「削除の保留中」状態のままになる可能性があります。

Deep Security ManagerがSQL Server Always On可用性グループに接続されている場合、テナントが削除されても、対応するデータベースは自動的に可用性グループから削除されません。データベース管理者は、SQL Server Always On可用性グループデータベースに接続されたDSMのテナントを追加または削除するに記載された手順に従って手動でこれを行うことができます。

[システム設定]のマルチテナントオプション

[管理]→[システム設定]→[テナント]では、次のオプションを設定できます。

「初期設定のRelayグループ」内のRelayの使用をテナントに許可 (割り当てられていないRelay): プライマリテナントで設定されているRelay有効化済みAgentにテナントが自動的にアクセスできるようにします。これにより、セキュリティアップデート用に専用のRelay有効化済みAgentをテナント側で設定する必要がなくなります。

予約タスク「スクリプトの実行」の使用をテナントに許可: スクリプトは、システムへのアクセスを潜在的な危険にさらす可能性があります。ただし、スクリプトはファイルシステムのアクセス権を使用してDeep Security Managerにインストールする必要があるため、リスクを軽減できます。

テナントを管理する

[管理]→[テナント] には、全テナントのリストが表示されます。テナントのステータスは次のいずれかです。

- 作成: 作成済みですが、アクティベーションのメールがテナントのユーザに送信されていません。
- 確認が必要です: 作成されましたが、テナントユーザに送信された確認メール内のアクティベーションリンクがクリックされていません。この状態を手動で上書きすることができます。
- 有効: 完全にオンラインで管理されている状態です。
- 一時停止: ログオンが許可されていません。
- 削除の保留中: テナントは削除できますが、すぐにではありません。保留中のジョブが終了するまで、テナントは最大で7日間、「削除の保留中」状態になることがあります。
- データベースアップグレード失敗: アップグレードに失敗したテナントです。[データベースアップグレード] ボタンで、この問題を解決できます。

テナントのプロパティ

テナントをダブルクリックすると、テナントの [プロパティ] 画面が表示されます。

一般

ロケール、タイムゾーン、およびステータスを変更できます。変更は既存のテナントユーザには影響しません (新しいユーザ、およびユーザ固有ではないUIの一部にのみ変更が反映されます)。

データベース名は、このテナントに使用されているデータベースの名前です。ハイパーリンクを介して、テナントデータベースのプロパティにアクセスできます。

モジュール

モジュールタブでは、保護モジュールの表示オプションを提供します。選択された表示設定は、どのテナントにどのモジュールを表示するかを調整するために使用できます。デフォルトでは、すべての未ライセンスのモジュールは非表示になっています。これを変更するには、未ライセンスのモジュールを常に非

表示にするの選択を解除します。また、選択されたモジュールはテナントごとに表示することもできます。

デフォルトでは、テナントごとのライセンスを使用する場合、各テナントは自分のライセンスされたモジュールのみを表示します。

プライマリテナントからライセンスを継承を選択すると、すべてのテナントがプライマリテナントであるあなたがライセンスを持っているすべての機能を確認できます。プライマリテナントのライセンスされていないモジュールは、ライセンスされていないモジュールを常に非表示にするのオプションを選択解除しても、他のテナントには非表示になります。

テスト環境でDeep Securityを評価していて、完全なマルチテナントインストールがどのようなものかを確認したい場合は、マルチテナントデモモードを有効にできます。デモモードでは、マネージャはそのデータベースに、シミュレートされたテナント、コンピュータ、イベント、アラート、およびその他のデータを投入します。最初は7日分のデータが生成されますが、マネージャのダッシュボード、レポート、およびイベントページにデータが継続的に投入されるように、新しいデータが継続的に生成されます。

警告: 本番環境でデモモードを使用しないでください。使用すると、デモデータが実際のデータと混ざり、実際の攻撃や不正プログラムがあるかどうかを判断するのが難しくなる可能性があります。

機能

管理者は、特定のテナントの特定の機能を有効または無効にすることができます。これらの使用可能な機能は、時間とともに変化する場合があります。

イベント転送の拡張説明を有効にすると、Deep SecurityはAmazon SNSまたはSIEMに転送されるイベントの完全な説明を含みます。そうでない場合、説明は省略されます。SAMLアイデンティティプロバイダ統合、Amazon WorkSpaces統合、アプリケーション(アプリケーションコントロール)、およびAPIレート制限(オートメーションセンター内)はデフォルトで有効になっています。

統計

統計タブには、現在のテナントに関する情報が表示されます。これには、データベースのサイズ、処理されたジョブ、ログイン、セキュリティイベント、システムイベントが含まれます。スパークラインは、過去24時間の概要を示します。

Deep Security Agentの有効化

エージェントのアクティベーションタブには、コンピュータ上でエージェントをアクティベートするために実行できるコマンドが表示されます。このコマンドは、このテナントのコンピュータのエージェントインストールディレクトリに関連しています。アクティベーションは、Deep Security Managerが安全に接続し、テナン

トがポリシーを割り当てたり、Deep Security Managerから他の設定手順を実行したりするために必要です。

テナントに表示される内容

マルチテナントが有効になっている場合、サインインページには追加のアカウント名フィールドがあります。

テナントは、ユーザ名とパスワードに加えてアカウント名を入力する必要があります。アカウント名があるので、ユーザ名が重複していてもかまいません。たとえば、複数のテナントが同じActive Directoryサーバと同期する場合です。

あなた(主テナント)としてログインする際は、アカウント名を空白のままにするか、Primaryを使用してください。

Deep Security Manager UIの一部の機能はテナントユーザには利用できません。以下の領域はテナントには非表示です:

- マネージャノードコンポーネント
- マルチテナントコンポーネント
- [管理]→[システム情報]
- 管理>ライセンス(継承が選択されている場合)
- [管理]→[Managerノード]
- [管理]→[テナント]
- [管理]→[システム設定]
  - テナントタブ
  - セキュリティタブ > サインインメッセージ
  - 更新タブ > プライマリテナントからリレーを使用するテナントの許可設定
  - 詳細タブ > ロードバランサー
  - 詳細タブ > プラグ可能セクション
- テナントに関係がないヘルプの内容
- テナントに関係がない一部のレポート
- マルチテナントオプションに基づくその他の機能
- 一部のアラートも非表示になります。

- ハートビートサーバの失敗
- Managerのディスク容量不足
- Managerがオフライン
- Managerの時刻が非同期
- 新しいバージョンの Deep Security Managerが利用可能
- コンピュータ数がデータベースの上限を超過
- ライセンスの継承が有効になっている場合、ライセンス関連のアラート

テナントからは、プライマリテナントのマルチテナント機能や、他のテナントのデータは確認できません。また、プライマリテナントの権限が必要な一部のAPIも制限されます(他のテナントの作成など)。

テナントユーザが使用できる機能と使用できない機能の詳細については、"マルチテナント設定" on page 501を参照してください。

すべてのテナントは、複数のユーザアカウントで役割に基づいたアクセス制御 (RBAC) を使用して、アクセスをさらに分割することもできます。また、ユーザのActive Directory統合を使用して、認証をドメインに委任することもできます。この場合も、テナントの認証にテナントのアカウント名が必要です。

エージェントによるアクティベーションの開始

Agentからのリモート有効化は、すべてのテナントで初期設定で有効になっています。

プライマリテナントにおけるAgentからのリモート有効化とは異なり、他のテナントユーザが有効化を実行するには、パスワードとテナントIDが必要です。

テナントは、管理 > アップデート > ソフトウェア > ローカルに移動し、エージェントソフトウェアを選択してからデプロイメントスクリプトを生成をクリックすることで、エージェントによるアクティベーションに必要な引数を確認できます。例えば、Windowsコンピュータでのエージェントによるアクティベーションのスクリプトは次のようになります。

```
dsa_control -a dsm://<host or IP>:4120/ "tenantID:XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"
"token:XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"
```

テナントの診断

Managerの診断パッケージに含まれるデータは機密性が高いので、テナントからこのパッケージにアクセスすることはできません。ただし、テナントは、コンピュータエディタを開き、[概要]→[処理]の順に移動して[診断パッケージの作成]を選択することで、Agentの診断情報を生成することができます。

使用状況の監視

Deep Security Managerはテナントの使用状況に関するデータを記録します。これを表示するには、ダッシュボードのテナント保護アクティビティ、テナントプロパティウィンドウの統計タブ、およびレポートに移動します。この情報は、レガシーREST APIのステータスモニタリングを通じてもアクセス可能で、管理 > システム設定 > 詳細 > ステータスモニタリングAPIに移動して有効または無効にできます。

環境に応じて、表示するテナント情報の種類をカスタマイズするには、従来のREST APIのステータス監視を使用します。企業では、事業単位ごとの使用状況を確認する場合に便利です。また、この情報を使用してDeep Securityシステム全体の使用状況を監視し、異常の兆候を検出することができます。たとえば、1つのテナントでセキュリティイベントアクティビティが急増している場合は、攻撃を受けている可能性があります。

マルチテナントのダッシュボード

マルチテナントが有効になっているとき、プライマリテナントのユーザには、テナントの使用状況を監視できる次のダッシュボードウィジェットが追加されます。

- テナントのデータベース使用状況
- テナントのジョブアクティビティ
- テナントの保護アクティビティ
- テナントのセキュリティイベントアクティビティ
- テナントのログオンアクティビティ
- テナントのシステムイベントアクティビティ
- テナント

同じ情報を、[管理]→[テナント] (一部はオプションの列) と、テナントの [プロパティ] 画面の [統計] タブで確認できます。

この情報によって、システム全体の使用状況を監視し、異常の兆候を検出することができます。たとえば、1つのテナントでセキュリティイベントアクティビティが急増している場合は、攻撃を受けている可能性があります。

マルチテナントのレポート

必要な情報が含まれているレポートを生成するには、[イベントとレポート]→[レポートの生成] の順に移動して、ドロップダウンメニューから生成するレポートを選択します。マルチテナント環境のレポートと含まれる情報は次のとおりです。

セキュリティモジュールの累積使用状況レポート

- テナント
- ホスト名
- ID
- 不正プログラム対策
- ネットワーク時間
- システムセキュリティ
- SAPシステム
- 企業時間

セキュリティモジュールの使用状況レポート

- テナント
- ID
- ホスト名
- 表示名
- コンピュータグループ
- インスタンスの種類
- 開始日
- 開始時刻
- 停止時刻
- 期間 (秒)
- 不正プログラム対策
- Webレピュテーション
- ファイアウォール
- 侵入防御
- 変更監視
- セキュリティログ監視
- アプリケーションコントロール
- SAP

テナントレポート

- テナント名
- データベースサイズ
- ピーク時のホスト数
- 保護時間
- 保護されている時間の割合

データベースのユーザアカウントを設定する

各テナントのデータの大部分は別個のデータベースに保存されます。このデータベースは、他のテナントと同じデータベースサーバに共存させることも、専用のデータベースサーバに分離することもできます。いずれの場合も、一部のデータはプライマリデータベース (Deep Security Managerとともにインストールされたデータベース) だけに保存されます。複数のデータベースサーバが利用可能な場合、テナントは、負荷が最も低いデータベースに作成されます。

データベースへの各テナントのデータの分割には、次のメリットがあります。

- データ削除: テナントを削除すると、製品でサポートされているテナントのデータがすべて削除されます。
- バックアップ: 各テナントのデータに、それぞれ異なるバックアップポリシーを適用できます。これは、準備環境と実稼働環境でテナントを使用し、準備環境のバックアップ要件が厳しくない場合に便利です (バックアップは、Deep Security Managerを設定した管理者が実行します)。
- 調整: 将来、すべてのデータベースサーバで負荷を均等に分散するための再調整が可能です。

Microsoft SQL Server、Oracle、PostgreSQLはデータベースの概念に対して異なる用語を使用していることに注意してください。以下の表をご参照ください。

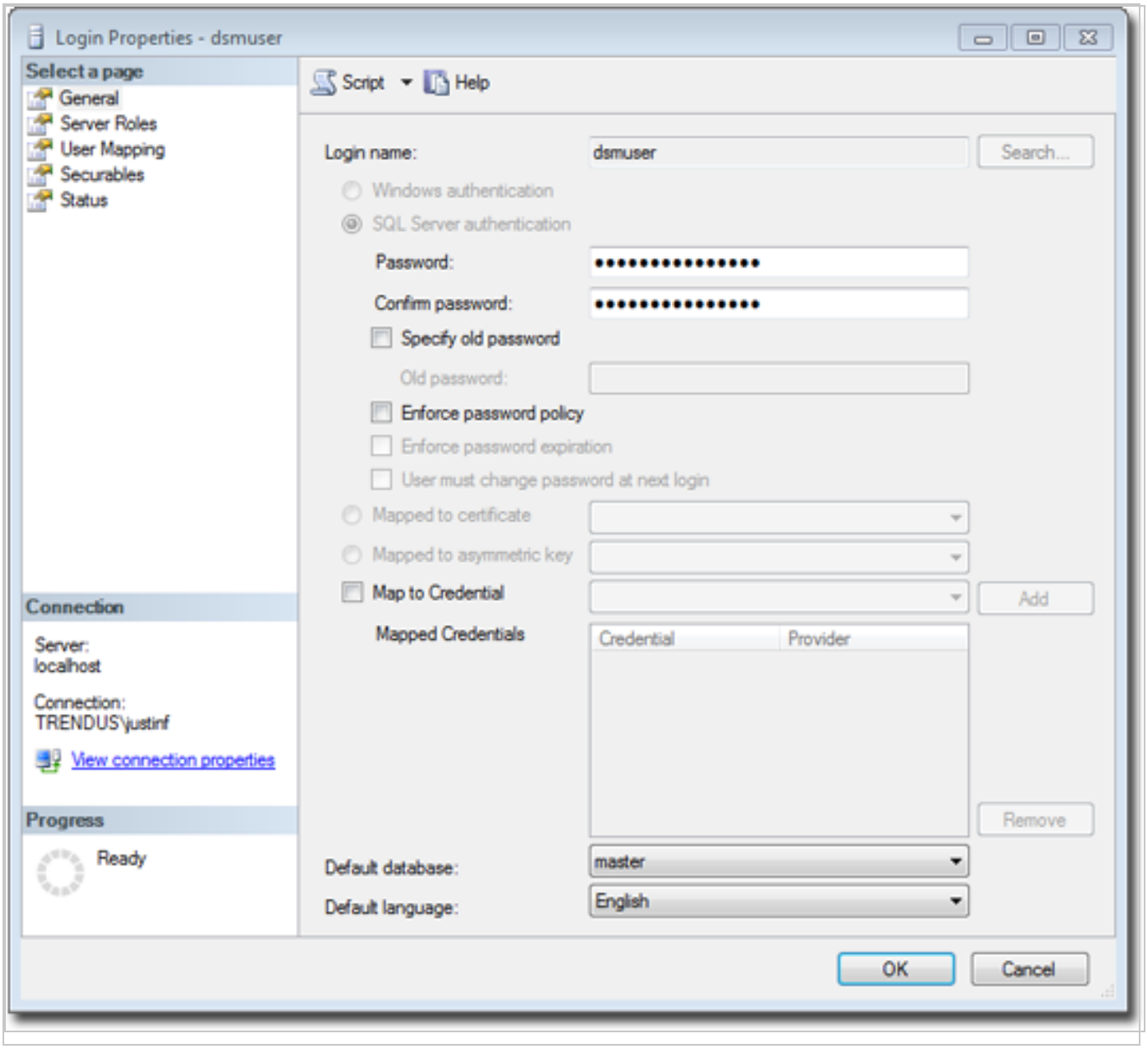
概念	SQL Serverの用語	Oracleの用語	PostgreSQLの用語
複数のテナントが実行されるプロセス	データベースサーバ	データベース	データベースサーバ
単一のテナントのデータ	データベース	表領域/ユーザ	データベース

以下の説明では、SQL ServerとOracleの両方に対してMicrosoft SQL Serverの用語が使用されています。

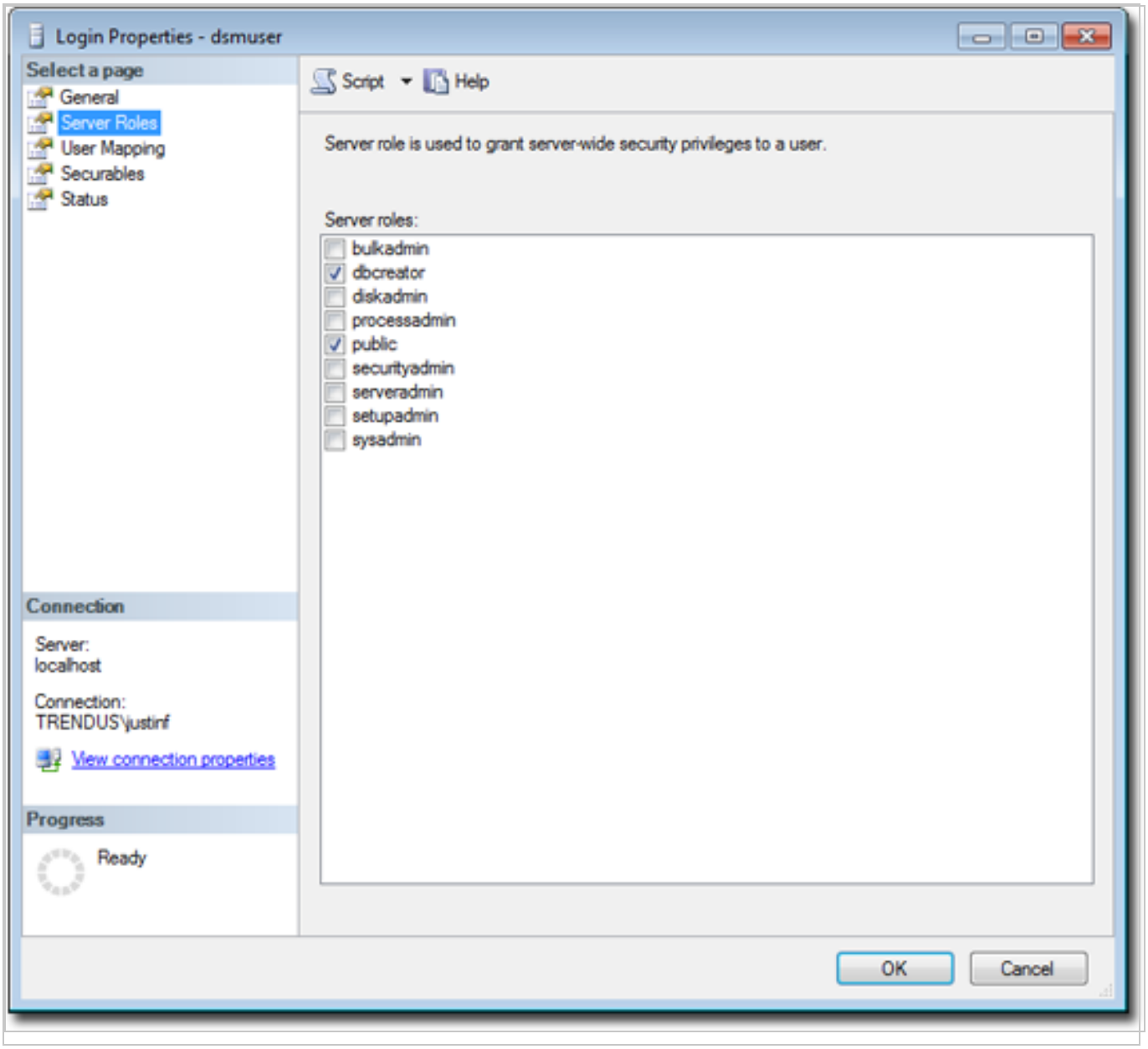
SQL Server

マルチテナントでは、新しいテナントを作成する際にDeep Securityがデータベースを作成できる必要があるため、SQL Serverデータベースユーザにはdbcreatorロールが必要です。

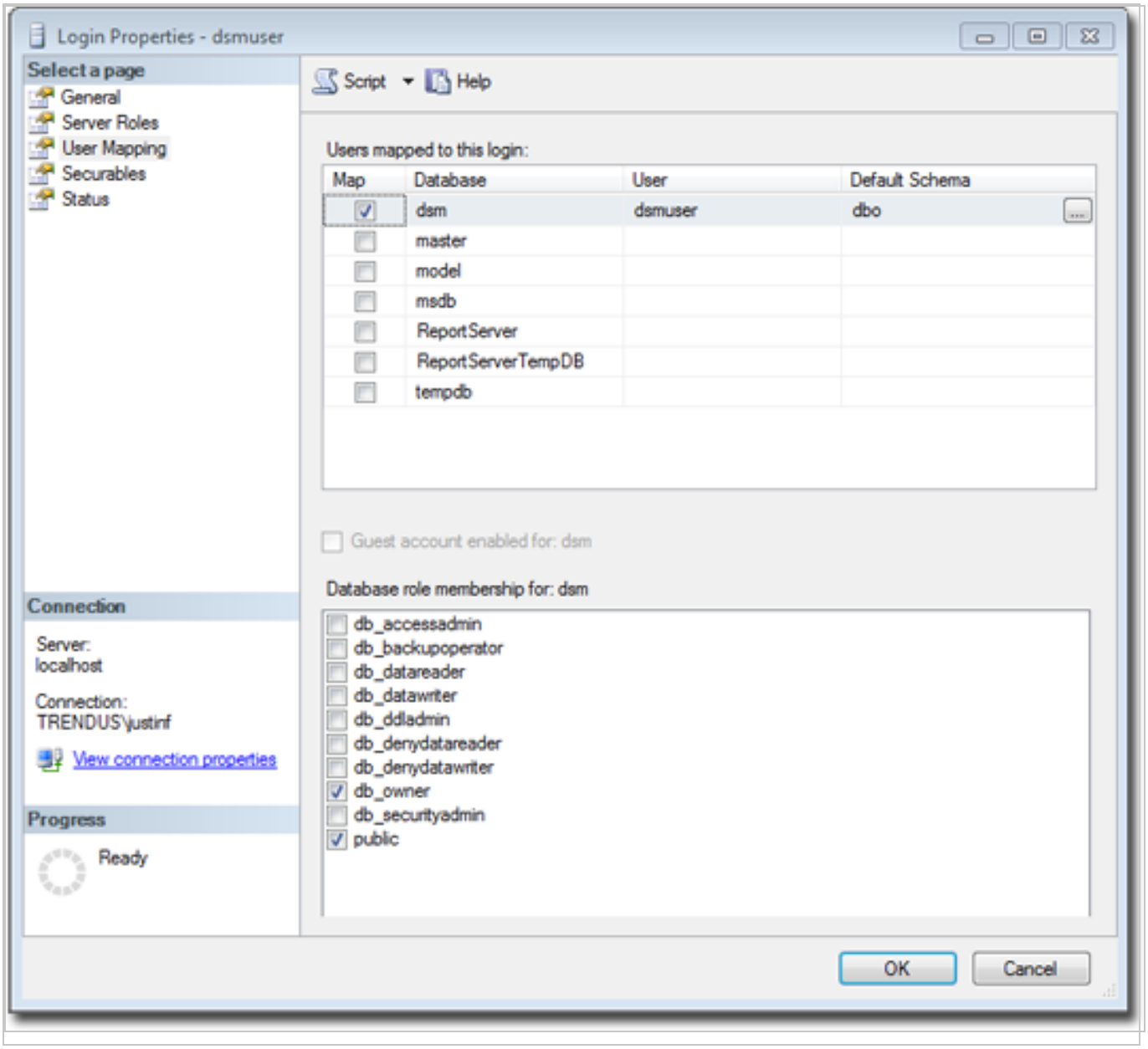
メインデータベース名には短い名前を使用することをお勧めします。これにより、テナントのデータベース名が読みやすくなります。Deep Securityは、メイン(プライマリテナントの) SQLデータベース名からテナントのデータベース名を派生させます。例えば、メインデータベースがdsmと名付けられている場合、最初のテナントのデータベースはdsm_1、2番目のテナントのデータベース名はdsm_2となります。



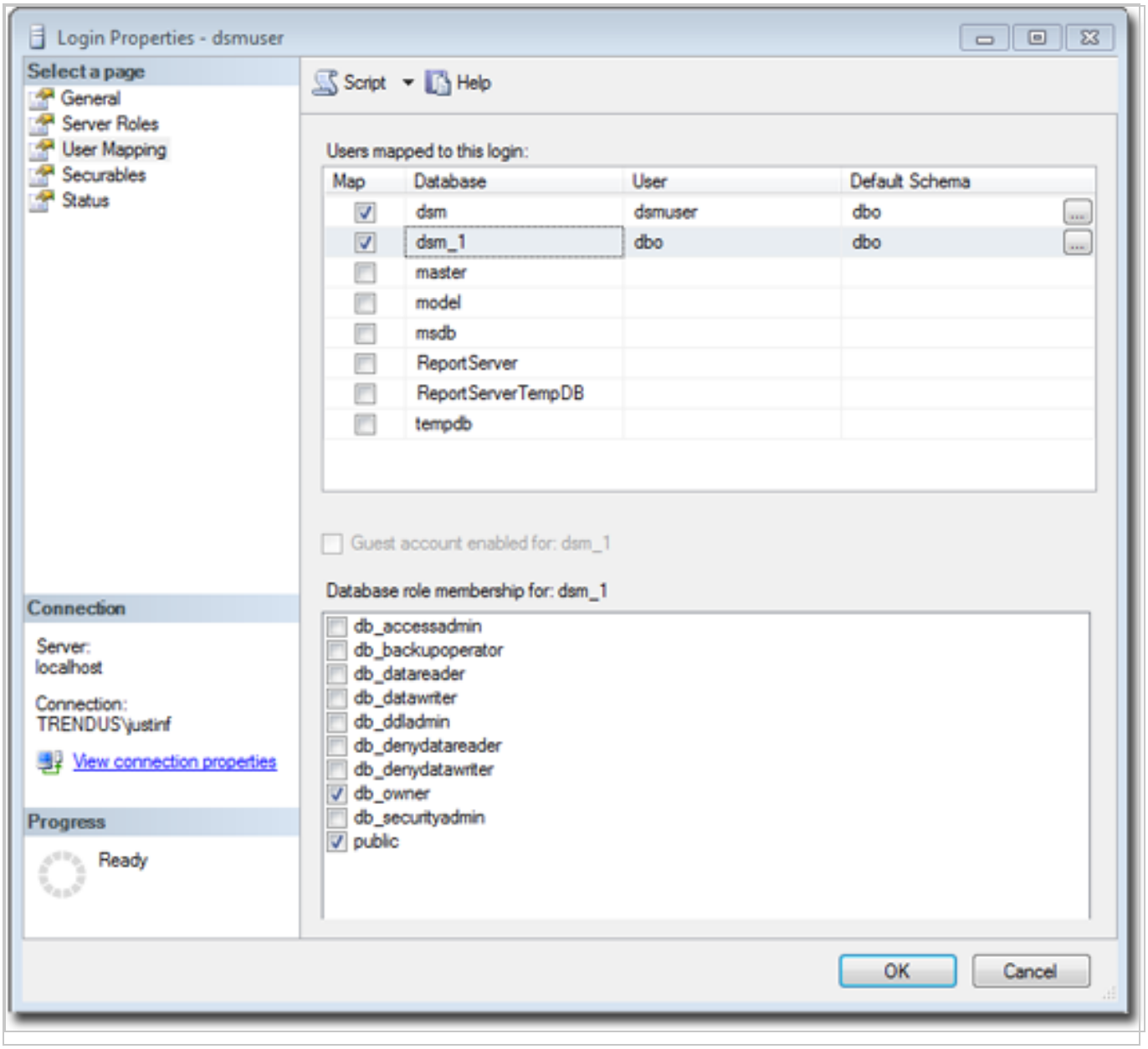
プライマリテナントのユーザのロールについては、メインデータベースのDB所有者を割り当てます。



権限を制限して、スキーマの変更とデータのアクセスのみを許可することもできます。



dbcreatorロールを持つと、そのアカウントが作成したデータベースは自動的に同じユーザが所有します。例えば、最初のテナントが作成された後のユーザのプロパティは次の通りです:



セカンダリデータベースサーバで最初のアカウントを作成するには、dbcreatorサーバロールのみが必要です。ユーザーマッピングは必要ありません。

SQL Server Always On可用性における一般的な接続問題のトラブルシューティング方法については、SQL Server Always On可用性グループデータベースに接続した際のDSMの一般的な問題のトラブルシューティングを参照してください。

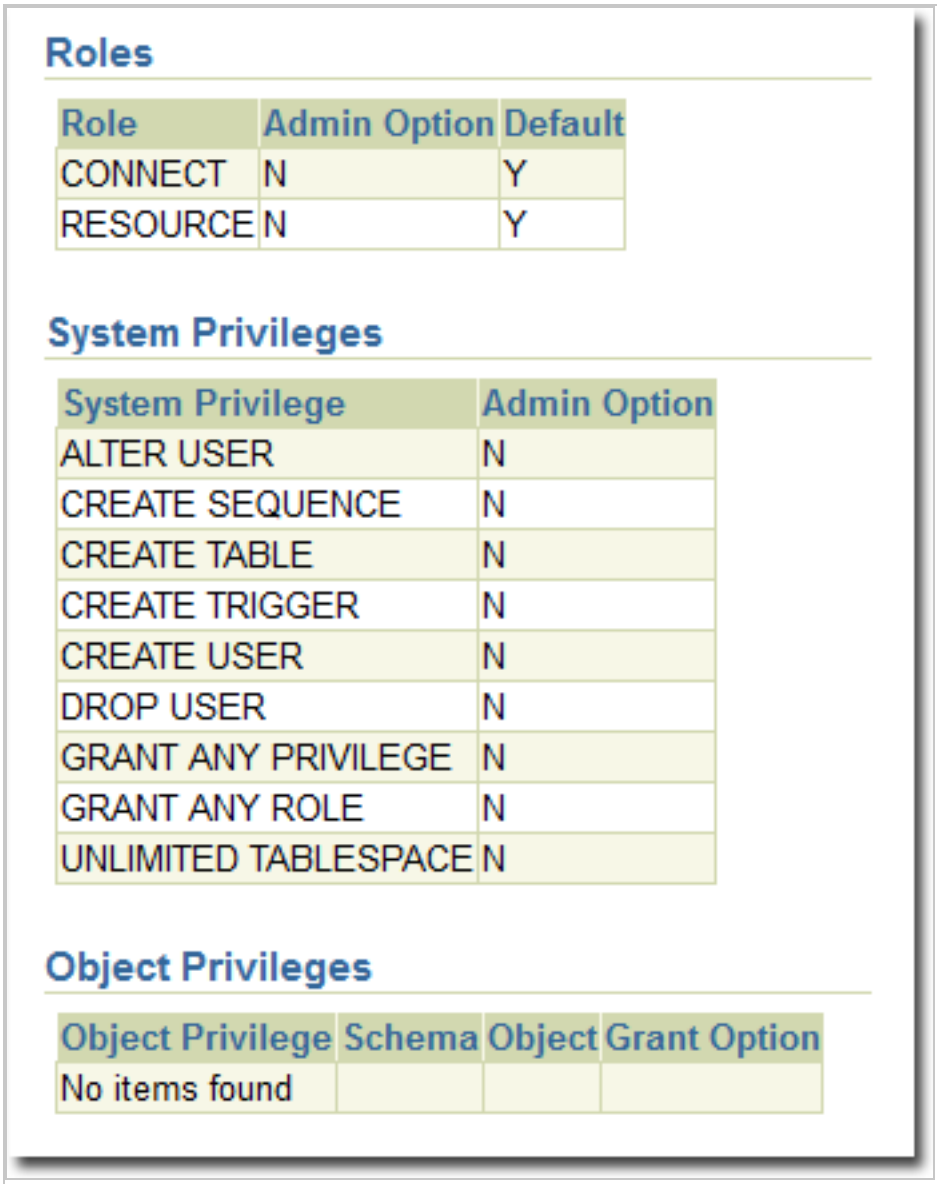
Oracle

Oracleにおけるマルチテナントは、Microsoft SQL Serverの場合と似ていますが、重要な違いがいくつかあります。SQL Serverでは、データベースサーバごとにユーザアカウントが1つですが、Oracleではテナントごとにユーザアカウントが1つです。Deep Securityをインストールしたユーザがプライマリテナントに対応付けられます。このユーザには、追加のユーザやテーブルスペースを割り当てる権限を付与できます。

Oracleではデータベースオブジェクト名に引用符で囲まれた特殊文字を許可していますが、Deep Securityではデータベースオブジェクト名に特殊文字をサポートしていません。詳細については、データベースオブジェクト名と修飾子を参照してください。

メインデータベース名には短い名前を使用することをお勧めします。これにより、テナントのデータベース名が読みやすくなります。Deep Securityは、メイン(プライマリテナント)のOracleデータベース名からテナントのデータベース名を派生させます。例えば、メインデータベースがMAINDBという名前の場合、最初のテナントのデータベースはMAINDB_1、2番目のテナントのデータベース名はMAINDB_2というようになります。

マルチテナントが有効になっている場合は、以下のOracle権限を割り当てる必要があります。



Roles

Role	Admin Option	Default
CONNECT	N	Y
RESOURCE	N	Y

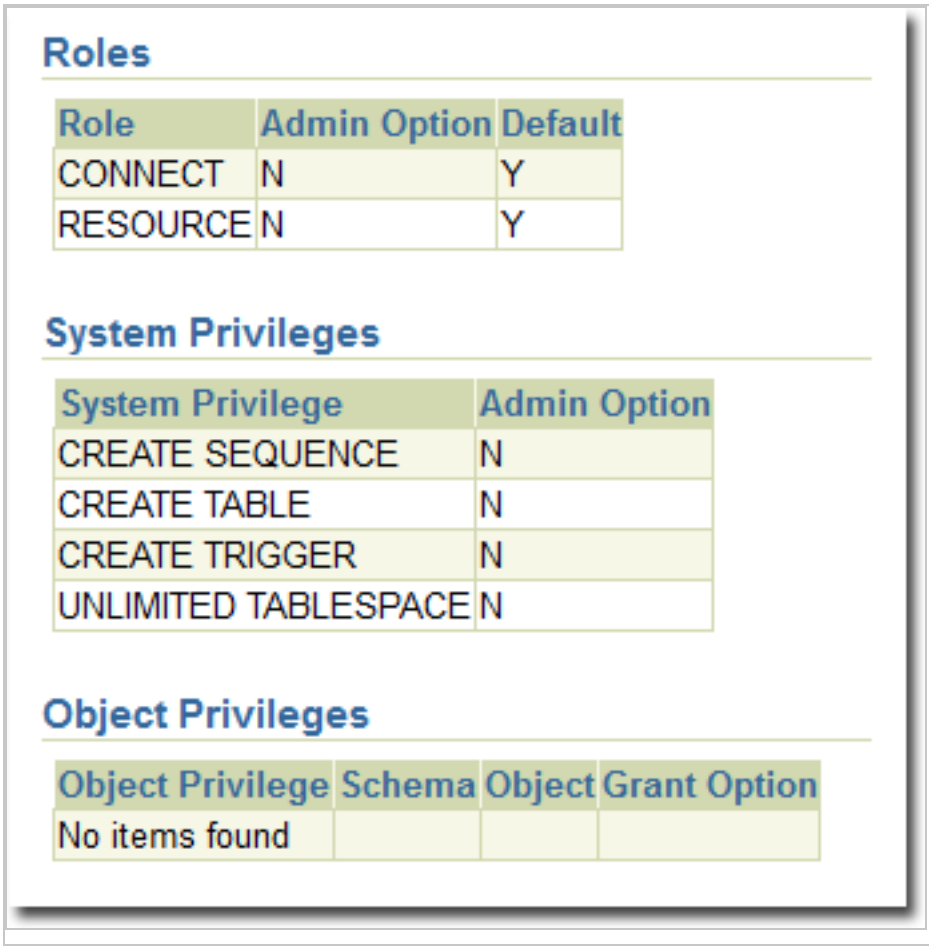
System Privileges

System Privilege	Admin Option
ALTER USER	N
CREATE SEQUENCE	N
CREATE TABLE	N
CREATE TRIGGER	N
CREATE USER	N
DROP USER	N
GRANT ANY PRIVILEGE	N
GRANT ANY ROLE	N
UNLIMITED TABLESPACE	N

Object Privileges

Object Privilege	Schema	Object	Grant Option
No items found			

テナントは、長いランダムパスワードを持つユーザとして作成され、次の権限が付与されます。



Roles

Role	Admin Option	Default
CONNECT	N	Y
RESOURCE	N	Y

System Privileges

System Privilege	Admin Option
CREATE SEQUENCE	N
CREATE TABLE	N
CREATE TRIGGER	N
UNLIMITED TABLESPACE	N

Object Privileges

Object Privilege	Schema	Object	Grant Option
No items found			

Oracleのセカンダリサーバ用に、最初のユーザアカウント(ブートストラップユーザアカウント)を作成する必要があります。このユーザは、ほとんどの場合、テーブルスペースを持ちます。設定は、プライマリユーザアカウントと同じです。

PostgreSQL

ユーザは、新しいデータベースとロールを作成する権限を持つ必要があります。

```
ALTER ROLE [username] CREATEDB CREATEROLE;
```

セカンダリデータベースサーバでは、ホスト名、ユーザ名、およびパスワードが必要です。ユーザ名には、追加のユーザ(役割)とデータベースを作成する権限が必要です。

メインデータベース名には短い名前を使用することをお勧めします。これにより、テナントのデータベース名が読みやすくなります。Deep Securityは、メイン(プライマリテナント)のPostgreSQLデータベース名からテナントのデータベース名を派生させます。例えば、メインデータベースがdsmと名付けられている

場合、最初のテナントのデータベースはdsm_1、2番目のテナントのデータベース名はdsm_2となります。

複数のデータベースサーバを設定する

初期設定では、すべてのテナントがDeep Security Managerと同じデータベースサーバ上に作成されます。スケーラビリティを高めるために、Deep Security Managerではデータベースサーバを追加できます(追加データベースサーバはセカンダリデータベースと呼ばれることがあります)。テナントを追加するときに、新しいテナントアカウントを格納するデータベースサーバをDeep Securityで自動的に選択するオプションを選択するか、または特定のサーバを指定できます。

さらにデータベースを設定するには、管理 > システム設定 > テナントに移動します。データベースサーバーセクションでデータベースサーバーを表示をクリックし、次に新規をクリックします。

Microsoft SQL Serverの場合、セカンダリデータベースサーバにはホスト名、ユーザ名、およびパスワードが必要です(名前付きインスタンスとドメイン)。Deep Security Managerのデータベースユーザは、以下の権限を持つ必要があります。

- データベースの作成
- データベースの削除
- スキーマの定義

このアカウントは、データベースの作成だけでなく、作成されたデータベースに対する認証にも使用されます。

Oracleでは、マルチテナント展開は異なるモデルを使用します。新しいデータベース定義は、テーブルスペースにバインドされたユーザを定義し、それが追加のOracleユーザの作成をブートストラップします。

セカンダリデータベースを削除または変更する

サーバにテナントが存在しない場合、プライマリデータベース以外のデータベースサーバを削除できます。

セカンダリサーバのホスト名、ユーザ名、パスワード、または詳細が変更された場合は、Deep Security Managerコンソールでこれらの値を変更できます。プライマリ・データベースの値を変更するには、Deep Security Managerのすべてのノードを停止し、dsm.propertiesファイルを新しい詳細で編集する必要があります。

API

Deep Security Managerには次のためのAPIが含まれています。

1. マルチテナントの有効化
2. テナントの管理
3. 監視データのアクセス
4. チャージバックデータ(保護の利用状況) のアクセス
5. セカンダリデータベースサーバの管理

また、従来のSOAP APIには、3つ目のパラメータとしてテナントアカウント名を受け取る新しい認証メソッドがあります。

APIの詳細については、「"Deep Security APIを使用したタスクの自動化" on page 1824」を参照してください。

マルチテナント環境のアップグレード

1. すべてのデータベースをバックアップします。
   - Microsoft SQLおよびPostgreSQLでは、メインのデータベースが1つとテナントごとのデータベースがあります。
   - Oracleでは、すべてのテナント情報が1つのマネージャデータベースに含まれますが、テナントごとに追加のユーザが作成されます。各ユーザに専用のテーブルがあります。
2. マネージャをアップグレードします。インストーラーは次のことを行います:
   - 他のマネージャノードが存在する場合、それらをシャットダウンしてからアップグレードを開始します
   - データベーススキーマを更新します。
   - データをプライマリテナント(t0) の新しい構造に移行します。
   - 他のテナントのデータを移行します (各バッチに5つ)。
3. すべてのテナントを含めてマネージャが完全にアップグレードされた後、次のマネージャノードがあればアップグレードします。詳細については、"マルチテナント環境のアップグレード" above のマネージャのバージョンアップを参照してください。

次の点に注意してください:

- t0の移行が失敗した場合、インストーラーは復旧できません。続行しません。データベースをバックアップから復元し、再試行してください。
- プライマリ以外のテナントの移行に失敗した場合、インストーラは続行しますが、の[管理]→[テナント]の各テナントのステータスは、[データベースのアップグレードが必要](オフライン) に設定されます。バックアップから復元してインストーラを再度実行するか、該当するテナントの移行を再試行できます。
- テナントの移行を再試行するには、テナントのインタフェースを使用します。再試行を強制できない場合は、サポート担当者にお問い合わせください。

テナントをサポートする

特に、テナントに対する最上位サポート担当者であるMSSPの場合、プライマリテナントは他のテナントのユーザインタフェースにログインする必要があるかもしれません。

これを行うには、管理 > テナントに移動します。テナント名を右クリックし、として認証を選択します(テナントがアクセスを無効にしている場合、このオプションは利用できない可能性があります)。これにより、そのテナント内でフルアクセス権を持つ一時的なユーザアカウントが作成され、すぐにそのアカウントにログインします。一時アカウント名は、プライマリテナント内のユーザ名に続くsupport_です。

たとえば、メインテナントのユーザー名がjdoeで、テナントT1内に一時的なアカウントを作成した場合、すぐにsupport_jdoeとしてT1にログインされます。

一時的なサポートアカウントは、ログアウトするかセッションがタイムアウトすると削除されます。テナントは、一時的なサポートアカウントの作成、ログイン、ログアウト、および削除に関するシステムイベントを確認できます。

プライマリテナントのユーザは、より多くの診断ツールや情報にアクセスできます。

1. [管理]→[システム情報]には、テナントのメモリ使用量とスレッドの状態に関するより多くの情報が表示されます。
2. 各Managerノードのディスク上のserver#.logログファイル(server0.logなど)には、各イベントに関連するテナントの名前と、該当する場合にはユーザの名前が表示されます。

場合によっては、UIで利用できないアクションを実行したり、テナントの設定を変更したりする必要があるかもしれません。これは通常、トレンドマイクロのサポートからの依頼によるものです。Command Lineで-tenantname<tenant-name>引数を追加して、そのテナントに設定変更やアクションを適用します。引数が省略された場合、コマンドはプライマリテナントに適用されます。

Deep Security Virtual Appliance環境のマルチテナント

VMware環境にDeep Securityを導入する場合、vCenterとそのコネクタをプライマリテナント内に設定し、vCloud Connectorをその他のテナント内に設定することができます。正しく設定された場合、プライマリテナントでは、ESXiサーバ、Deep Security Virtual Appliance、およびその他のインフラストラクチャを確認でき、他のテナントでは、vCloud環境でテナントが所有するAgentレスに保護された仮想マシンのみを確認できます。

このような環境を有効にするには、[管理]→[システム設定]→[Agent]の順に移動し、[Applianceによるの仮想マシンの保護を許可]チェックボックスをオンにします。

vCloudとの統合の詳細については、"VMware vCloudへのAgentのインストール" on page 556を参照してください。

マルチテナント設定

[テナント] タブは、マルチテナントモードを有効にしている場合のみ表示されます。

- マルチテナントライセンスモード: マルチテナントのライセンスモードは、マルチテナントの設定後に変更できます。ただし、このモードを継承からテナント単位に切り替えると、ライセンス許可されているモジュールが既存のテナントで使用できなくなるので注意が必要です。
- 予約タスク「スクリプトの実行」の使用をテナントに許可: スクリプトは、システムへのアクセスを潜在的な危険にさらす可能性があります。ただし、スクリプトはファイルシステムのアクセス権を使用してManagerにインストールされるため、リスクを軽減できます。
- 「コンピュータの検索」の実行をテナントに許可 (直接および予約タスクとして): 検出を許可するどうかを指定します。ネットワーク検出が禁止されているサービスプロバイダ環境での実行には適していない場合があります。
- 「ポートの検索」の実行をテナントに許可 (直接および予約タスクとして): ポートの検索を実行できるかどうかを指定します。ネットワーク検索が禁止されているサービスプロバイダ環境での実行には適していない場合があります。
- VMware vCenterの追加をテナントに許可: vCenterとの接続を許可するかどうかをテナントごとに指定します。インターネットなどの安全ではないネットワークやパブリックネットワーク経由で接続を行う場合、通常はこのオプションを無効にする必要があります。
- クラウドアカウントの追加をテナントに許可: クラウド同期の設定をテナントに許可するかどうかを指定します。通常、クラウド同期はすべてのセットアップに対し適用されます。
- LDAPディレクトリとの同期をテナントに許可: ユーザとコンピュータの両方をディレクトリ(コンピュータはLDAPまたはActive Directory、ユーザはActive Directoryのみ) と同期することをテナントに許可するかどうかを指定します。インターネットなどの安全ではないネットワークやパブリックネットワーク経由で接続を行う場合、通常はこのオプションを無効にする必要があります。
- イベント転送のSIEMの設定を各テナントに許可: SIEMの設定を[イベントの転送] タブに表示します。
- SNSの設定をテナントに許可: SNSの設定を[イベントの転送] タブに表示します。
- SNMPの設定をテナントに許可: リモートコンピュータへのシステムイベントの転送をテナントに許可します (SNMP経由)。このオプションを選択しない場合は、すべてのテナントが [イベントの転送] タブの設定をすべてのイベントタイプに使用し、SyslogはDeep Security Managerを介して転送されます。
- [パスワードを忘れた場合] オプションを表示: パスワードのリセット画面に進むリンクをログオン画面に表示します。この機能を使用するには、[管理]→[システム設定]→[SMTP] タブでSMTP設定を正しく指定しておく必要があります。

- [アカウント名とユーザ名を記憶] オプションを表示: ユーザのアカウント名とユーザ名を記憶してログオン画面の該当するフィールドに自動的に入力するためのオプションを表示します。
- プライマリテナントからのアクセス管理をテナントに許可: 初期設定では、プライマリテナントは、[管理]→[テナント] 画面の [テナントとしてログオン] オプションを使用してテナントのアカウントにログオンできます。[プライマリテナントからのアクセス管理をテナントに許可] オプションをオンにすると、プライマリテナントからDeep Security環境へのアクセスを許可するか禁止するかをテナントが指定できるようになります ([管理]→[システム設定]→[詳細])。このオプションをオンにした場合、テナント環境の初期設定ではプライマリテナントのアクセスが禁止されます。

  注意: プライマリテナントがテナントのアカウントにアクセスするたび、テナントのシステムイベントにアクセスが記録されます。

- プライマリテナントの不審オブジェクトリストとサンドボックス分析の設定の使用をテナントに許可: Deep Discovery Analyzer およびTrend Micro Apex Central 設定をプライマリテナントがテナントと共有できるようにします。詳細については、「"脅威インテリジェンスを使用した新たな脅威の検出" on page 861」を参照してください。
- 「初期設定のRelayグループ」のRelayの使用をテナントに許可: テナントは、プライマリテナントに設定されているRelayに自動的にアクセスできます。その結果、テナントはセキュリティアップデート専用のRelayを設定する必要がなくなります。

  注意: 管理→システム設定 の Updates タブで、の選択を解除することで、テナントは「共有」リレーの使用を拒否できます。プライマリテナントRelay グループを初期設定の Relay グループ (割り当てられていないリレーの場合) として使用する。それから、リレーを設定する必要があります。

  注意: リレーが共有される場合、プライマリテナントはリレーを最新の状態に保つ必要があります。これを実現するには、一定の間隔で Download Security Update の予約済みタスクをすべてのリレーに対して作成できます。

- 新規テナントでのセキュリティアップデートの自動ダウンロードを有効化: 新しいテナントアカウントが作成されると同時に、最新のセキュリティアップデートの有無を確認してダウンロードします。

- 次のオプションをロックして非表示 (すべてのテナントがプライマリテナントの設定を使用):
  - データ[Agents]タブのプライバシーオプション: プライマリテナントがデータのプライバシー設定を行うことを許可します。この設定は、[管理]→[システム設定]→[Agent] タブの [暗号化されたトラフィック (SSL) のパケットデータの取り込みを許可] にのみ適用されます。
  - [SMTP]タブのすべてのオプション: [SMTP]タブのすべての設定をロックします。
  - [Storage]タブのすべてのオプション: [Storage]タブのすべての設定をロックします。

データベースサーバ

初期設定では、すべてのテナントがDeep Security Managerがインストールされたデータベースサーバと同じデータベースサーバに作成されます。追加のスケーラビリティを実現するために、Deep Security Managerではデータベースサーバの追加をサポートしています。詳細については、"マルチテナント環境の設定" on page 478を参照してください。

新しいテナントテンプレート

テナントテンプレートを使用すると、新しいテナントに対してカスタマイズされた「すぐに使える」エクスペリエンスを作成できます。この機能は、いくつかのサンプルが適用されない、または特別な例を作成する必要があるサービスプロバイダ(MSSP) 環境で役立ちます。

注意: 既存のテナントは、新しいテンプレートを作成しても影響を受けません。

1. プライマリテナントとしてログインします。
2. 新しいテナントを作成します。
3. ログアウトし、新しいテナントとしてログオンします。
4. (ポリシーの追加、削除、または変更などのポリシーの例) and/or セキュリティアップデートのバージョン(新しいバージョンの).の適用など)

   テナントはサンプルポリシーを出発点として使用し、独自のニーズに合わせてカスタマイズする必要があります。

   注意: セキュリティ更新プログラムパッケージには有効なデジタル署名が必要です。無効なセキュリティ更新プログラムを指定した場合、新しいテナントの作成は失敗します。"アップグレードについて" on page 1657も参照してください。
5. ログアウトし、プライマリテナントとして再度ログインします。
6. テナントテンプレートウィザードを実行します。
7. テナントを選択してスナップショットを作成します。

テンプレートにはが含まれます:

- 最新のセキュリティアップデートルール(作成時にテンプレートに適用されていたアップデート。トレンドマイクロによって提供された侵入防御ルール、変更監視ルール、セキュリティログ監視ルールなど)
- ポリシーファイアウォールルール
- IPリスト
- MACリスト

- ディレクトリリスト
- ファイルリスト
- ファイル拡張子リスト
- ポートリスト
- コンテキスト
- スケジュール
- ファイアウォールステートフル設定
- 不正プログラム検索設定

テンプレートexclude:

- カスタム侵入防御ルール
- カスタムのアプリケーションの種類
- カスタム変更監視ルール
- カスタムセキュリティログ監視ルール
- カスタムセキュリティログ監視デコーダ
- ダッシュボード
- アラートの設定
- システム設定
- 予約タスク
- イベントベースタスク
- ユーザ
- 役割
- 連絡先情報

保護の使用状況の監視

Deep Securityは、保護対象のコンピュータに関する情報を収集します。この情報は、[テナント] ウィジェットと[テナントの保護アクティビティ] ウィジェットのダッシュボードに表示されます。また、テナントレポートでもこの情報を確認でき、従来のREST API経由で取得できます。

注意: 最も基本的なケースでは、レポートまたはAPIを使用してDeep Security Managerの使用時間に対する割合(%)を確認できます。一般に「ショーバック」または「チャージバック」と呼ばれるこの情報は、さまざまな形で使用できます。高度な使い方としては、テナントコンピュータのOSなどの特性に基づいたカスタム請求に使用できます。

これらのオプションを使用して、追加で記録するテナントコンピュータの情報を指定します。

複数のノードを設定する

複数のノードにDeep Security Managerをインストールする

Deep Security Managerを*の1台*のサーバで実行する代わりに、*の複数*のサーバ(「ノード」)にDeep Security Managerをインストールして、1つの共有データベースに接続できます。これにより、以下が向上します。

- 信頼性
- 可用性
- スケーラビリティ
- パフォーマンス

任意のノードにログインでき、各ノードは全種類のタスクを実行できます。あるノードが他のノードよりも重要ということはありません。1つのノードでエラーが発生してもサービスのダウンタイムは発生せず、データ損失も生じません。Deep Security Managerは、すべてのオンラインノードが実行する、分散プール内の多くの同時アクティビティを処理します。ユーザ入力によって発生するものでないアクティビティはすべてジョブとしてパッケージされ、利用可能な任意のManager上で実行されます。ただし、キャッシュのクリアなど、各ノードで実行される一部の「ローカル」ジョブは例外です。

各ノードでは、同じDeep Security Managerソフトウェアバージョンを実行する必要があります。アップグレードするときは、アップグレードする最初のManagerがすべてのタスクを一時的に引き継ぎ、他のノードをシャットダウンします。Administration> Manager Nodesの場合、他のノードのステータスは「オフライン」になり、アップグレードが必要であることが示されます。アップグレードするとノードは自動的にオンラインに戻り、処理を再開します。

ロードバランサを設定する

大規模な配置のためにDeep Security Managerの複数のサーバノードを配置する場合、ロードバランサを使用すると、クライアントやアプライアンスとの接続を分散できます。仮想IPを使用するロードバランサは、Deep Securityが通常必要とする複数のポート番号ではなく、TCP 443などの単一の受信ポート番号を提供することもできます。

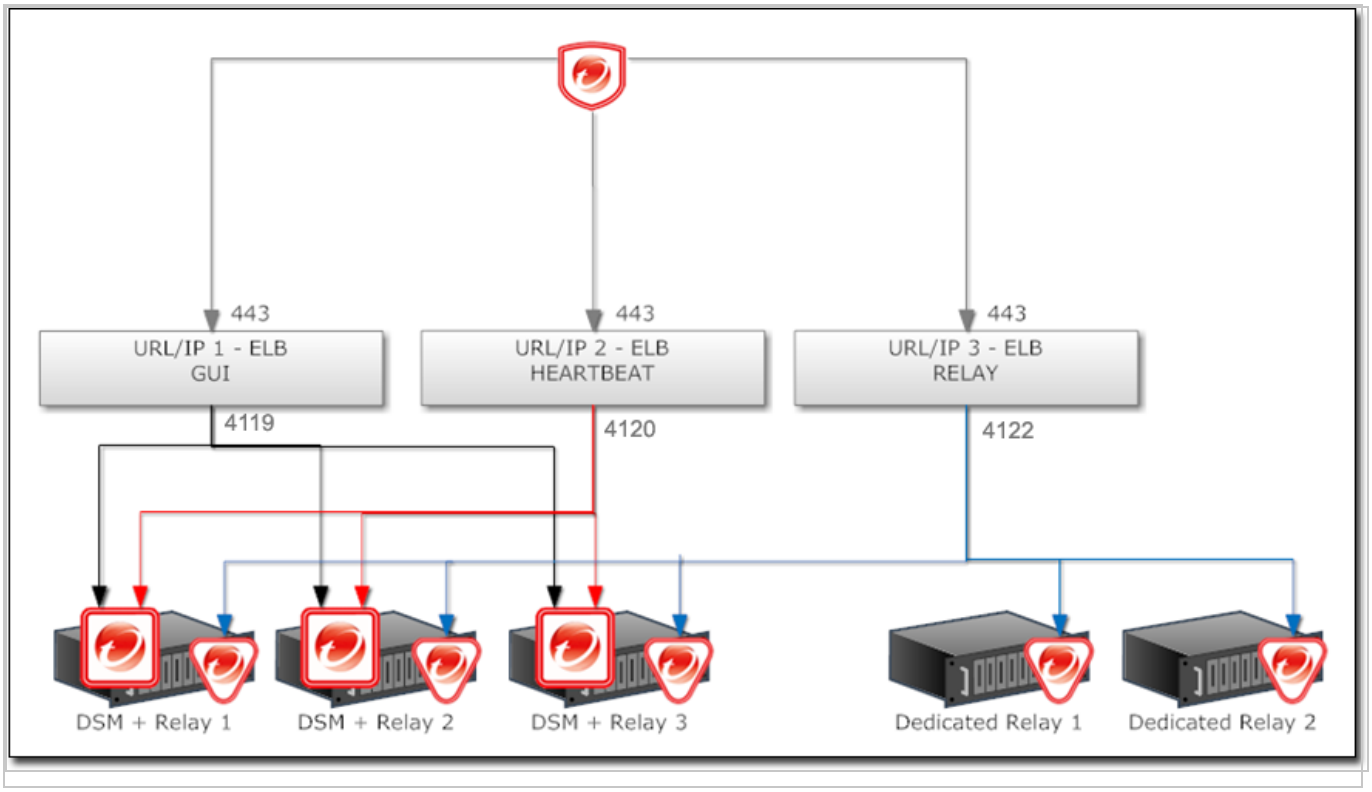
TCP接続に基づいて負荷を分散します。SSL終端は使用しません。これにより、接続全体が同じManagerノード内で確実に行われます。次の接続は、別のノードに分散される可能性があります。

詳細なDeep Security Managerの配信推奨事項については、"Deep Securityのベストプラクティスガイド" on page 2032(英語)を参照してください。

Deep Securityでのロードバランサの設定

初期設定では、複数ノードのManagerから、すべてのノードのアドレスが、すべてのAgentとVirtual Applianceに提供されます。AgentとVirtual Applianceは、接続しようとするときに、リストのノードをランダムに選択します。接続できない場合は、リストにある別のノードを試し、接続が成功するか、ノードがなくなるまでこのプロセスを続けます。接続できるノードがなかった場合は、次のハートビートまで待ってから再度実行します。

ノードが追加または削除されるたびに、アップデートされたリストがすべてのエージェントおよび仮想アプライアンスに送信されます。それまでは、古いノードへの接続は失敗する可能性があり、新しいノードは使用されません。そのため、通信が遅くなり、ネットワークトラフィックが増加します。これを避けるために、代わりに、ロードバランサのアドレスを介して接続するようにAgentとVirtual Applianceを設定します。



ノードを追加する

1. "ロードバランサを設定する" on the previous pageを設定します。
2. 1つのサーバノードにDeep Security Managerをインストールした後、別のサーバでインストーラを再度実行します。に配信します。以下のガイドラインに従ってください。

- すべてのノードに同じバージョンのManagerをインストールします。
- インストーラの複数のインスタンスを実行しないを同時に起動するデータベースの破損など、予期しない結果につながる可能性があります。
- すべてのノードを同じデータベースに接続します。
- すべてのノードが同じマスターキーを使用していることを確認します(設定されている場合)。
- マスターキーを常に使用可能にして、必要に応じてすべてのノードで暗号化された設定プロパティと個人データを復号化して読み取るようにします。詳細については、「masterkey」を参照してください。
- インストーラがマスターキーページに次のテキストを表示する場合:マスターキーへのアクセスに使用されるローカルシークレットを入力します。同じDeep Security Managerに属するすべてのノードを同じローカル秘密情報で設定する必要があります。このページで、最初のノードの設定時に指定したシークレットを入力します。詳細については、"Managerをインストールする" on page 460のインストールを参照してください。
- 同じタイムゾーンを使用するように各Managerノードのシステム時計を設定します。データベースも同じタイムゾーンを使用する必要があります。タイムゾーンが異なる場合、ManagerのTime Out of Syncエラーが発生します。

ノードを削除する

サーバを削除または交換する前に、サーバをDeep Security Managerノードのプールから削除する必要があります。

1. サービスを停止するか、削除するノード上のDeep Security Managerをアンインストールしてください。

   ステータスが「オフライン」になる必要があります。

2. 他のノードのDeep Security Managerにログインします。
3. [管理]→[Managerノード]に移動します。
4. 削除するノードをダブルクリックします。

   ノードの[プロパティ]画面が表示されます。

5. [オプション]エリアで[廃止]をクリックします。

ノードのアップグレード

マネージャノードのアップグレードの詳細については、"マルチノード配置でマネージャをアップグレードする" on page 1672の手順に従ってください。

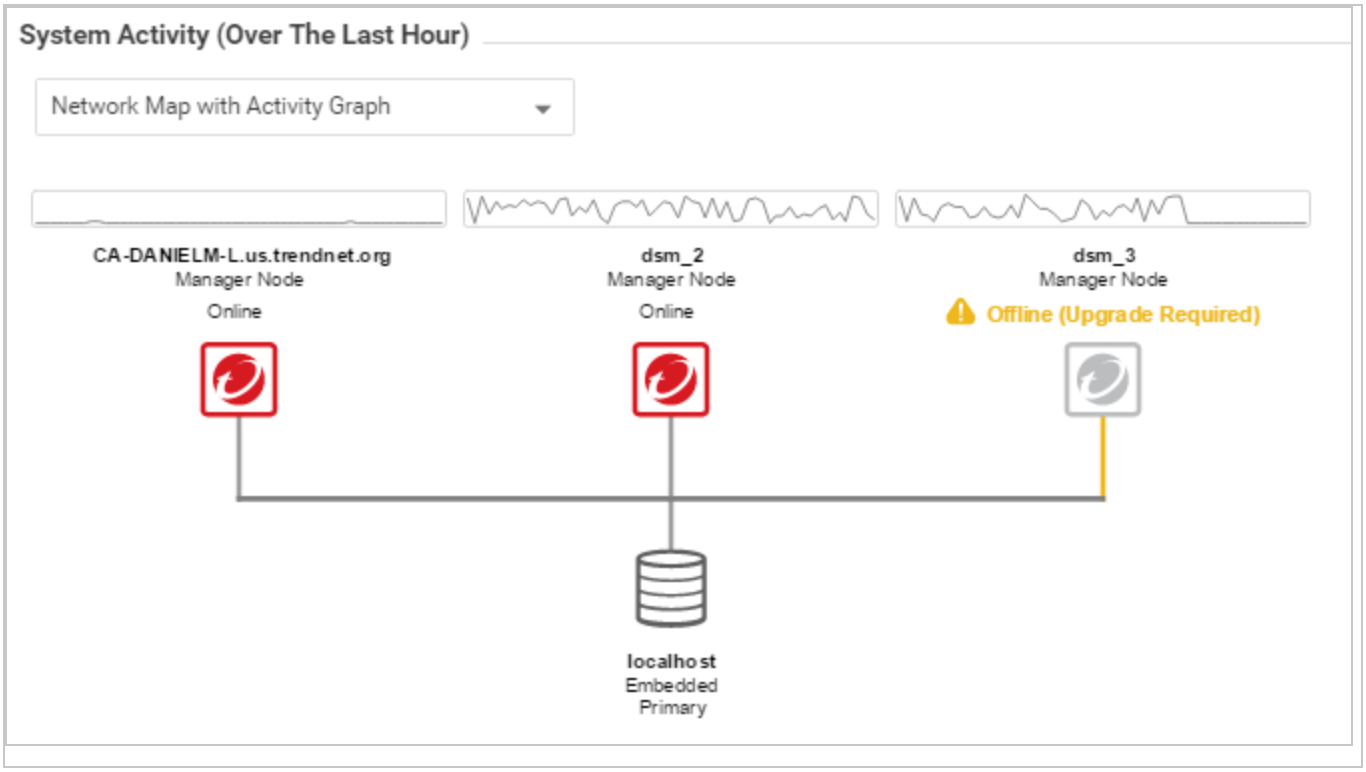
ノードのステータスを表示する

すべてのDeep Security Managerノード、ステータス、統合アクティビティ、および処理中のジョブを表示するには、の[管理]→[システム情報]の順に選択します。ドロップダウンメニューから、表示するグラフを選択します。

アクティビティグラフ付きネットワークマップ

[システムのアクティビティ] エリアの [アクティビティグラフ付きネットワークマップ] には、インストール済みのすべてのManagerノードとその現在のステータスのマップ、および過去1時間以内の関連アクティビティが表示されます。ノードには、次の状態があります。

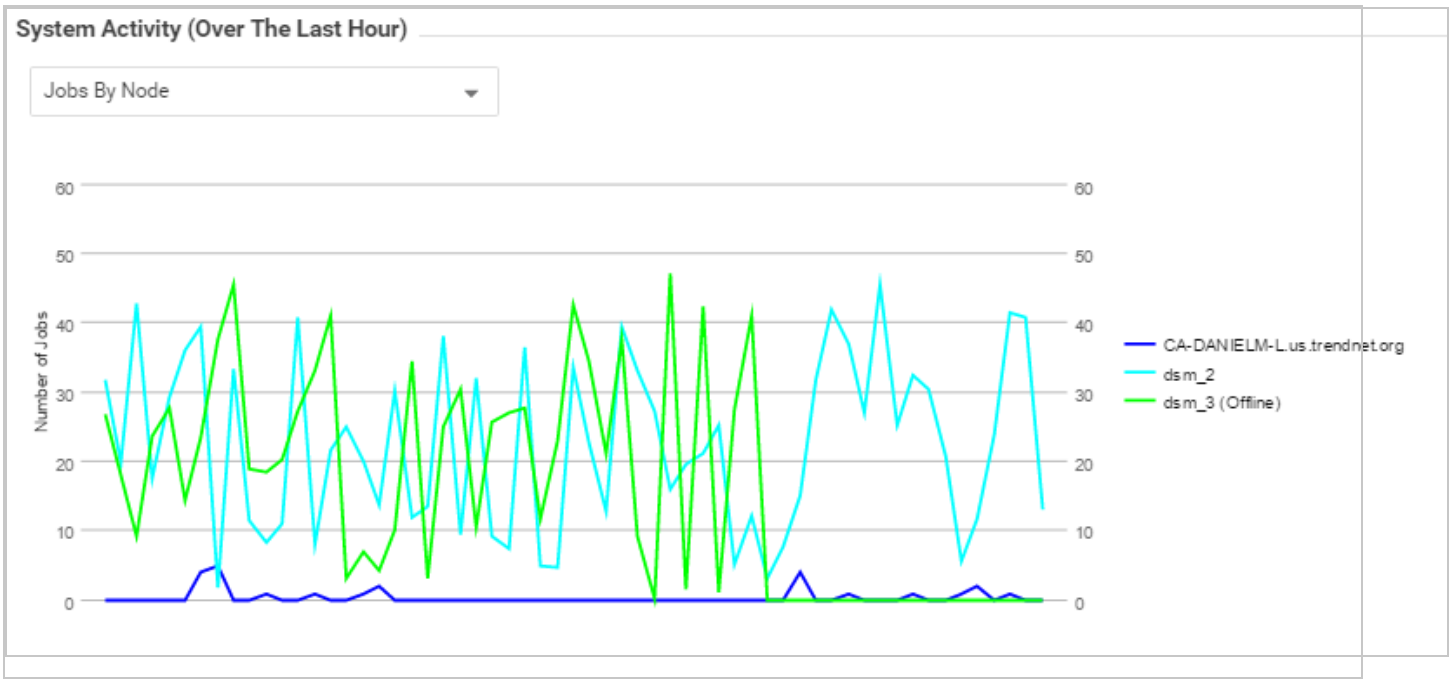
- オンライン
- オフライン
- オフライン(アップグレードが必要)



注意: Deep Security Managerのすべてのノードは、他のすべてのノードの正常性を定期的にチェックします。Managerノードはネットワーク接続が3分を超えて失われているとオフラインと判断されます。このノードのタスクは残りのノードが引き受けます。

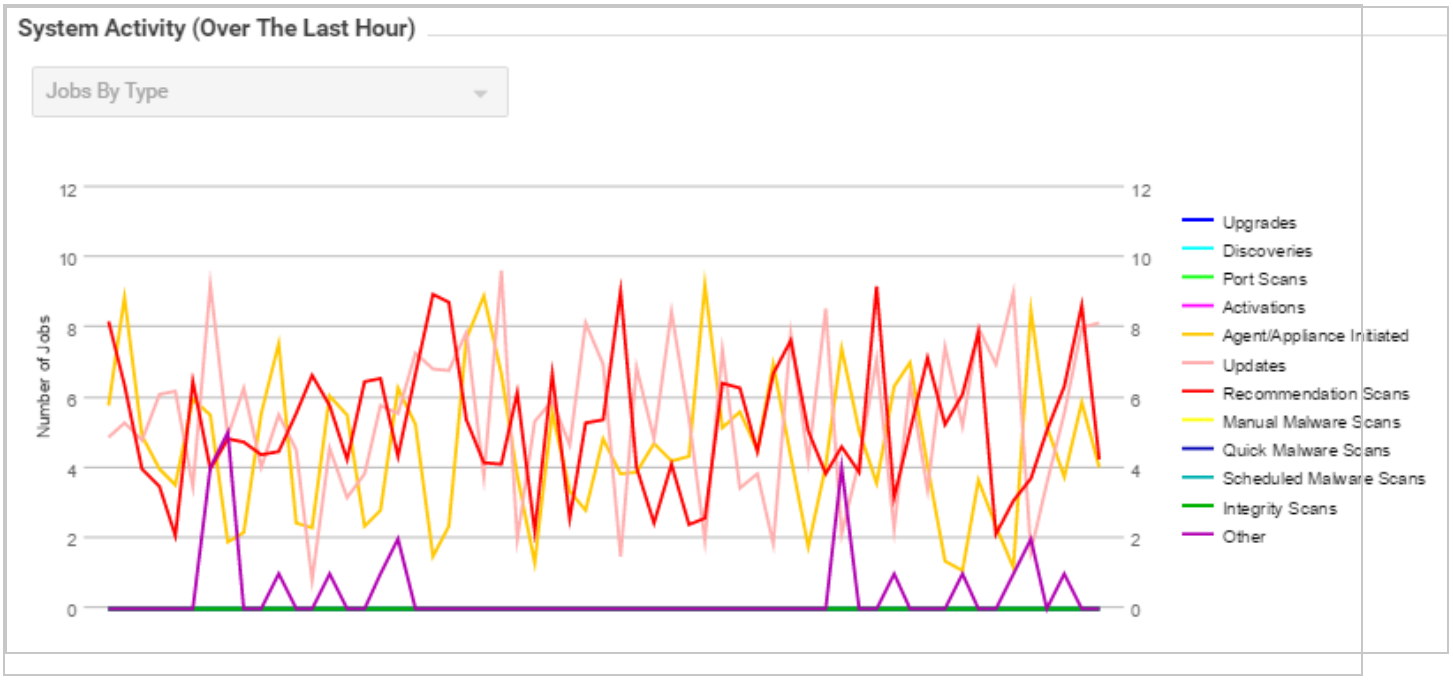
ノード別ジョブ

このグラフは、過去1時間以内に実行されたジョブの数をノード別に表示します。



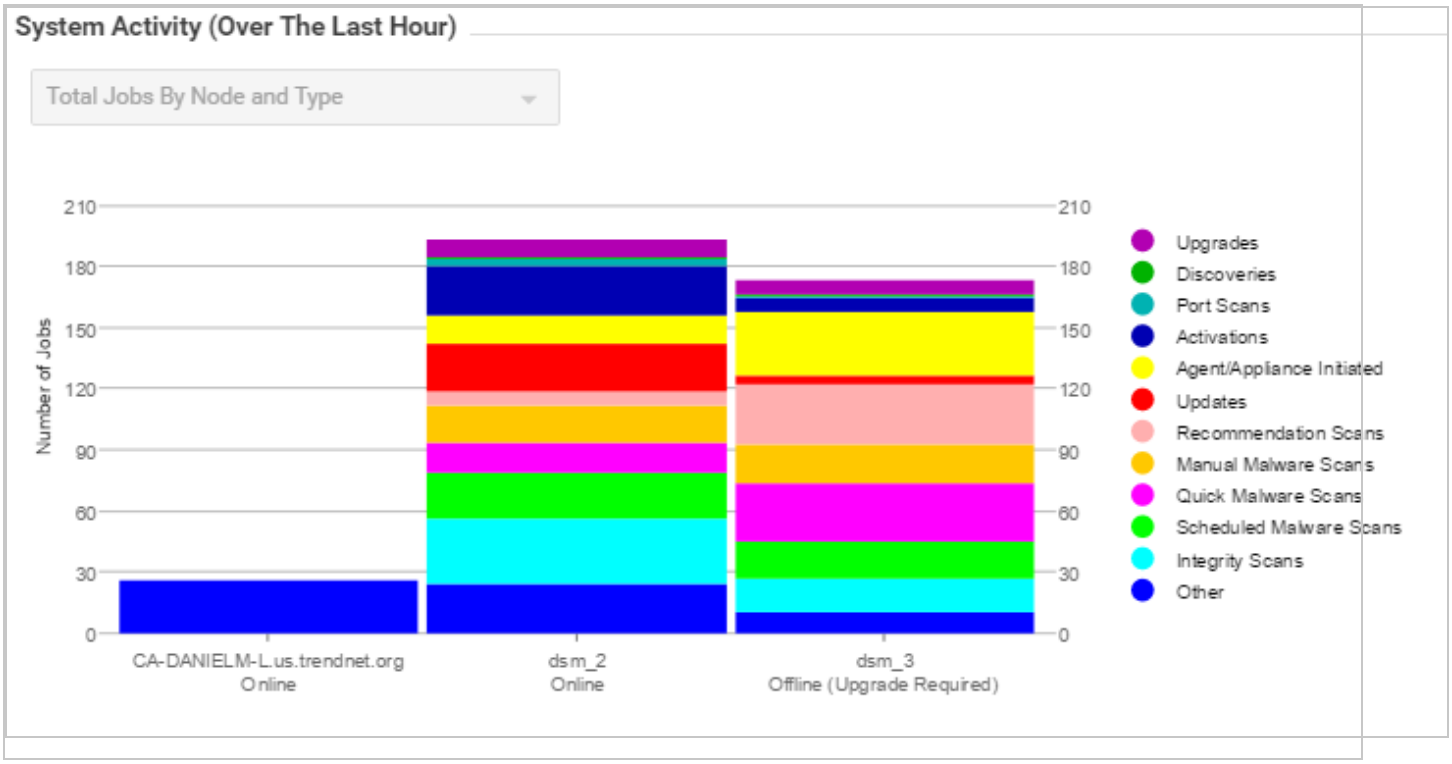
種類別ジョブ

このグラフは、過去1時間以内に実行されたジョブを種類別に表示します。



ノードおよび種類別ジョブの総数

このグラフは、過去1時間以内に実行されたジョブをノードごとの種類別に表示します。



アクティブなDeep Security Managerノードの表示

すべてのアクティブな Deep Security Manager ノードのリストを表示するには、管理 > マネージャーノードに移動します。"複数のノードにDeep Security Managerをインストールする" on page 505 も参照してください。

Managerノードの1つの詳細を表示するには、リスト内の行をダブルクリックします。プロパティウィンドウには次の内容が表示されます

- ホスト名: Deep Security Manager がインストールされているコンピュータのホスト名。
- 説明: Managerノードの説明。
- パフォーマンスプロファイル: Deep Security Manager のパフォーマンスは、CPU の数、利用可能な帯域幅、データベースの応答性など、いくつかの要因によって影響を受ける可能性があります。マネージャーのデフォルトのパフォーマンス設定は、ほとんどのインストール環境に適するように設計されています。しかし、パフォーマンスの問題が発生した場合、サポートプロバイダーが 1 つ以上の Deep Security Manager ノードに割り当てられたパフォーマンスプロファイルを変更することを提案するかもしれません。サポートプロバイダーに相談せずにこれらの設定を変更しないでく

ください。

注意: 以下の各表に記載されているエンドポイントのディスクおよびネットワークにおける同時ジョブ操作には、不正プログラム検索、変更監視検索、攻撃の予兆検索、コンピュータへのポリシーのアップデートの送信、およびセキュリティアップデートの配布が含まれます。

- アグレッシブ: このパフォーマンスプロファイルは、Deep Security Manager が専用サーバーにあるインストールに最適化されています。例えば、アグレッシブ パフォーマンスプロファイルを使用して、一般的な同時操作がマネージャーノードごとにどのように分散されるかを示します

処理	2コアシステム	8コアシステム
有効化	10	20
アップデート	25	50
推奨設定の検索	10	20
ステータスの確認	100	100
AgentまたはApplianceからのハートビート	アクティブ 20 処理待ち 40	アクティブ 50 処理待ち 40
エンドポイントのディスクおよびネットワークにおける同時ジョブ数	50	50
ESXi1台あたりのエンドポイントのディスクおよびネットワークにおける同時ジョブ数	3	3

- 標準: このパフォーマンスプロファイルは、Deep Security Manager とデータベースが同じコンピュータにあるインストールに最適化されています。例えば、標準 パフォーマンスプロファイルを使用して、いくつかの一般的な同時操作がマネージャーノードごとにどのように分散されるかを示します

処理	2コアシステム	8コアシステム
有効化	5	10
アップデート	16	46
推奨設定の検索	3	9
ステータスの確認	65	100
AgentまたはApplianceからのハートビート	アクティブ 20 処理待ち 40	アクティブ 50 処理待ち 40
エンドポイントのディスクおよびネットワークにおける同時ジョブ数	50	50
ESXi1台あたりのエンドポイントのディスクおよびネットワークにおける同時ジョブ数	3	3

- 無制限のエージェントディスクおよびネットワーク使用:この設定はアグレッシブと同じですが、コンピュータのディスクおよびネットワークを使用する場合の制限はありません。

処理	2コアシステム	8コアシステム
有効化	10	20
アップデート	25	50
推奨設定の検索	10	20
ステータスの確認	100	100
AgentまたはApplianceからのハートビート	アクティブ 20 処理待ち 40	アクティブ 50 処理待ち 40
エンドポイントのディスクおよびネットワークにおける同時ジョブ数	無制限	無制限
ESXi1台あたりのエンドポイントのディスクおよびネットワークにおける同時ジョブ数	無制限	無制限

- より高い容量: この設定は、アグレッシブや無制限のエージェントディスクおよびネットワーク使用量よりも高い容量を持ち、同時により多くのジョブを消費することができます。このパフォーマンスプロファイルでは、より大きなメモリ使用量が予測されます。必要に応じて、メモリやJVMサイズを増やすことができます。

Operation	2コアシステム	8コアシステム
有効化	15	45
アップデート	39	114
推奨設定の検索	15	45
ステータスの確認	259	同じ(259)
AgentまたはApplianceからのハートビート	アクティブ 20 処理待ち 40	アクティブ 50 処理待ち 40
エンドポイントのディスクおよびネットワークにおける同時ジョブ数	100	100
ESXi1台あたりのエンドポイントのディスクおよびネットワークにおける同時ジョブ数	3	3

同時にアップデートできるコンポーネントの数は、すべてのパフォーマンスプロファイルで、Relayグループあたり100個に制限されています。

- ステータス: 現在ログインしているDeep Security Managerノードから見てノードの状態がオンラインかどうか、アクティブかどうかを示します。
- オプション: マネージャーノードを廃止することができます。ノードを廃止するには、ノードがオフライン(アンインストールまたはサービス停止) である必要があります。

Deep Securityを配信するRelay

A Deep Security Relayは、Deep Securityソフトウェアおよびセキュリティアップデートを他のエージェントに再配信するように設定されたエージェントです。および仮想アプライアンスにインストールします。これは、配置の規模に役立ちます。

環境内に少なくとも1つのリレーが必要です。このリレーは、Deep Security Managerと共同で配置した場合にすでにインストールされている場合があります。確認するには

1. Deep Security Managerにログインします。
2. 上部の[管理]をクリックします。
3. 左側のナビゲーションペインで[Relay管理]をクリックします。
4. メイン画面にリレーアイコン( ) が表示されている場合、リレーはすでに配信されています。

最初のリレーを配信するには

1. リレーコンピュータが要件を満たしていることを確認してください。"Deep Security Agent のサイズとリソース消費" on page 420および"システム要件 " on page 400を満たしている必要があります。
2. 該当するポート番号のリレーとの間の送受信通信が許可されていることを確認してください。"Deep Securityのポート番号" on page 429を参照してください。
3. リレーがプロキシ経由で接続する必要がある場合は、"プロキシ経由でプライマリセキュリティアップデート元に接続する" on page 1457を参照してください。
4. 選択したコンピュータにエージェントを配信します。"Deep Security Agentソフトウェアの入手" on the next pageおよび"エージェントをインストールする" on page 536を参照してください。
5. エージェントをリレーとして有効にします。
   a. Deep Security Managerにログインします。
   b. 上部の[管理]をクリックします。
   c. 左側のナビゲーションペインで[Relay管理]をクリックします。
   d. リレーを配置するリレーグループを選択します。リレーグループが存在しない場合は、ドメイングループを作成してください。
   e. リレーグループを選択して、リレーを配置するグループを決定します。リレーグループが存在しない場合は、作成してください。Linuxを使用している場合は、ユーザーnobodyとリレーグループnogroupを作成してください。
   f. 使用可能なコンピュータで、配信したばかりのエージェントを選択します。
   g. Relayとグループに追加をクリックします。
   h. Relayとグループに追加をクリックします。

   エージェントはリレーとして有効にされ、リレーアイコン( ) が表示されます。

注意: 複数のリレーを使用することをお勧めします。これは、基本的なDeep Securityの配信を実行した後に設定できます。詳細については、"追加のリレーを配信する" on page 1467を参照してください。

Deep Security Agentを配信する

Deep Security Agentソフトウェアの入手

Deep Security Agentをインストールするには、エージェントインストーラをダウンロードし、エージェントの保護モジュールのパッケージをDeep Security Managerにロードする必要があります。

警告: サードパーティの配信システムを使用している場合でも、インストールされているすべてのDeep Security Agentソフトウェアをを Deep Security Managerのデータベースにインポートする必要があります。Deep Security Agentを初めて有効化すると、セキュリティポリシーで現在有効になっている保護モジュールのみがインストールされます。後で新しい保護モジュールを有効にすると、Deep Security Agentはそのプラグインをを Deep Security Managerからダウンロードしようとします。そのソフトウェアが存在しない場合、エージェントは保護モジュールをインストールできない可能性があります。

このトピックの内容:

- "ダウンロード可能なエージェントソフトウェアの表示" below
- "インポートされたエージェントソフトウェアのリストを表示する" on the next page
- "エージェントソフトウェアのインポート" on the next page
- "Agentのインストーラをエクスポートする" on page 517
- "Solaris版とエージェントパッケージのマッピングテーブル" on page 518
- "AIXエージェントパッケージの命名形式" on page 519
- "Deep Securityデータベースからソフトウェアパッケージを削除する" on page 519

ダウンロード可能なエージェントソフトウェアの表示

Deep Security Managerにインポートできるソフトウェアの完全なリストを表示するには、Deep Security Managerから起動するか、ヘルプセンターから起動します。

Deep Security Managerから起動するには

1. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]→[ダウンロードセンター]の順に選択します。
2. 必要に応じて、上部のリストから[バージョン] または [プラットフォーム] を選択して、バージョンまたはプラットフォーム別にソフトウェアのリストを整理します。
3. 必要に応じて、右上の検索ボックスに検索文字列を入力してソフトウェアを検索します。

ヘルプセンターから開始するには:

1. Deep Securityのヘルプセンターで、左側の[Software]をクリックします。Deep Security Softwareのページが表示されます。
2. 長期サポートリリースの場合は [メジャーリリース (LTS)] タブをクリックし、機能リリースの場合は [機能リリース (FR)] タブをクリックします。詳細については、「"Deep Security 20リリース戦略およびライフサイクルポリシー" on page 116」を参照してください。

インポートされたエージェントソフトウェアのリストを表示する

Deep Security Managerにインポートしたソフトウェアのリストを表示するには、次の手順を実行します。

1. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]→[ローカル] に進みます。インポートされたすべてのソフトウェアが表示されます。
2. 必要に応じて、上部のリストから[バージョン] または [プラットフォーム] を選択して、バージョンまたはプラットフォーム別にソフトウェアのリストを整理します。

エージェントソフトウェアのインポート

エージェントアップデートの配信にDeep Security Managerを使用しない場合でも、Deep Security Managerにソフトウェアをインポートする必要があります。インポート方法は次のとおりです。

- "ダウンロードセンターから直接エージェントソフトウェアをインポートする" below)
- "ヘルプセンターから間接的にエージェントソフトウェアをインポートする" on the next page
- "エージェントソフトウェアのアップデートを自動的にインポートする" on page 517

ダウンロードセンターから直接エージェントソフトウェアをインポートする

1. Deep Security Managerコンピュータがインターネットにアクセスできることを確認してください。サポートされていない場合は、代わりにヘルプセンターから"ヘルプセンターから間接的にエージェントソフトウェアをインポートする" on the next page。
2. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]→[ダウンロードセンター] に進みます。

3. 上部のリストから[プラットフォーム] を選択します。
4. プラットフォームを展開して、使用可能なエージェントを表示します。
5. [VERSION]フィールドで目的のバージョンを探して、インポートアイコンをクリックします。次のガイドラインに従います。

   - 長期サポート(LTS) リリースまたは機能リリース(FR)。を選択できます。LTSおよびFRの詳細については、"Deep Security 20リリース戦略およびライフサイクルポリシー" on page 116を参照してください。
   - Solarisエージェントをインポートする場合、選択するエージェントの詳細については、「"Solaris版とエージェントパッケージのマッピングテーブル" on page 518 」を参照してください。
   - AIXエージェントをインポートする場合は、「"AIXエージェントパッケージの命名形式" on page 519」で命名形式を確認してください。命名形式はエージェントのバージョンによって異なります。

   Deep Security Managerはインターネットに接続してトレンドマイクロのダウンロードセンターからソフトウェアをダウンロードします。次に、マネージャは、ソフトウェアパッケージ上のデジタル署名をチェックします。マネージャーが終了すると、そのエージェントの[IMPORTED]列に緑のチェックマークが表示されます。ソフトウェアパッケージがの[管理]→[アップデート]→[ソフトウェア]→[ローカル]に表示されます。

   パッケージをインポートできない場合は、代わりに間接的にインポートすることもできます。

ヘルプセンターから間接的にエージェントソフトウェアをインポートする

Deep Security Managerがエアギャップ環境にある(インターネットに接続されていない) 場合、または直接インポートが機能しない場合は、エージェントソフトウェアを間接的にインポートしてみてください。

1. インターネットにアクセスできるコンピュータで、Deep Securityのヘルプセンターにアクセスします。
2. 左側の[Software]をクリックします。Deep Securityソフトウェアページが表示されます。
3. 必要なソフトウェアZIPをダウンロードします。長期サポート(LTS) リリースおよび機能リリースの詳細については、"Deep Security 20リリース戦略およびライフサイクルポリシー" on page 116を参照してください。
4. ソフトウェアZIPをDeep Security Managerコンピュータに移動します。
5. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]→[ローカル]の順に選択します。
6. メインペインで [インポート] をクリックして、ZIPファイルをインポートします。ManagerはZIPファイルのデジタル署名を確認し、有効な場合はインポートを続行します。

エージェントソフトウェアのアップデートを自動的にインポートする

Deep Security Managerでダウンロードセンターで最新のソフトウェアを検索し、ローカルのインベントリに自動的にインポートできます。Deep Security Managerは、すでにインポートされたソフトウェアにのみアップデートをインポートします。

アップデートは、番号の最後のセットのみが変更されるビルドです。たとえば、エージェントのバージョン12.0.0.111をすでにインポートしている場合、次のバージョンは12.0.0.111のアップデートビルドであるため、自動的にインポートされます。

12.0.0.112
12.0.0.113
12.0.0.123

ただし、次のバージョンは自動的にインポートされません。

12.1.0.222
11.0.0.333
10.0.0.111

Deep Security Managerでエージェントのアップデートビルドをローカルインベントリに自動的にインポートするには、次の手順を実行します。

1. Deep Security Managerで、[管理]→[システム設定]→[アップデート]の順に選択します。
2. ローカルにダウンロードしたソフトウェアの最新版を自動的にダウンロードセンターから取得へのアップデートを自動的にダウンロードを選択します。
3. [保存] をクリックします。

   設定によってDeep Security Managerにソフトウェアがインポートされますが、AgentまたはApplianceソフトウェアが自動的にアップデートされるわけではないことに注意してください。"Deep Security Agentのアップグレード" on page 1676のアップグレードに進みます。

Agentのインストーラをエクスポートする

エージェントインストーラは、次の手順でDeep Security Managerからダウンロードできます。

1. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]→[ローカル] に進みます。
2. リストからエージェントを選択します。同じエージェントの複数のバージョンをインポートした場合は、最新バージョンのソフトウェアの [最新] 列に緑色のチェックマークが表示されます。

   Solarisエージェントを探している場合は、"Solaris版とエージェントパッケージのマッピングテーブル" on the next page で、どのエージェントを選択するかを確認してください。

3. [エクスポート]→[インストーラのエクスポート] をクリックします。

   次に、Managerはソフトウェアパッケージのデジタル署名を確認します。署名が有効な場合は、エクスポートが続行されます。

4. エージェントインストーラを保存します。エージェントを手動でインストールする場合は、Deep Security Agentをインストールするコンピュータに Agentを保存します。

Deep Security Agentをインストールするには、エージェントの完全なZIPパッケージではなく、エクスポートされたエージェントインストーラ(プラットフォームに応じて.msi、.rpm、.pkg、.p5p、または.bffファイル)のみを使用します。他のzip形式のエージェントコンポーネントと同じフォルダからエージェントインストーラを実行すると、コンピュータで有効になっていない場合でも、すべての保護モジュールがインストールされます。これにより、余分なディスク領域が消費されます。比較のために、.msi、.rpm、.pkg、.p5p、または.bffファイルを使用した場合、エージェントは、設定で必要な場合にのみ保護モジュールをダウンロードしてインストールします。

Agentのインストール、有効化、およびセキュリティポリシーによる保護の適用は、コマンドラインスクリプトを使用して実行できます。詳細については、「"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849」を参照してください。

Deep Security APIを使用して、Agentのインストールを自動化するためのインストールスクリプトを生成できます。詳細については、「Generate an agent deployment script」を参照してください。

Solaris版とエージェントパッケージのマッピングテーブル

エージェントのインポートおよびエクスポート時に選択するエージェントパッケージがわからない場合は、次のマッピング表を確認してください。

Solaris版とエージェントパッケージのマッピングテーブル

Agentをインストールする対象	このエージェントパッケージを選択	ヘルプセンターオプション
Solaris 10 Updates 4-6 (64ビット、SPARCまたはx86)	エージェント- Solaris_5.10_U5-xx.x.x-xxx。<sparc|.x86_64>.zip	Solaris_5.10_U5
Solaris 10 Updates 7-11 (64ビット、SPARCまたはx86)	エージェント- Solaris_5.10_U7-xx.x.x-xxx。<sparc|.x86_64>.zip	Solaris_5.10_U7
Solaris 11.0 (1111)-11.3 (64ビット、SPARCまたはx86)	エージェント-solaris_5.11-xx.x.x-	Solaris_5.11

Agentをインストールする対象	このエージェントパッケージを選択	ヘルプセンターオプション
	xxx。<sparc|.x86_64>.zip	
Solaris 11.4 (64ビット、SPARCまたはx86)	エージェント- Solaris_5.11_U4-xx.x.x-xxx。<sparc|.x86_64>.zip	Solaris_5.11_U4

次の点に注意してください。

- [ヘルプセンターのオプション] 列には、ヘルプセンターの [Deep Securityソフトウェア] 画面にあるAgentリストから選択するオプションが表示されます。
- xx.x.x.xxxは、エージェントのビルド番号です。例: 12.0.0-682
- <sparc|.x86_64> は、sparc または .x86_64のいずれかで、Solarisプロセッサによって異なります。

AIXエージェントパッケージの命名形式

命名形式は、エージェントのバージョンによって異なります。

- Deep Security Agent 12 for AIX: Agent-AIX-<agent_release>-<agent_build>.powerpc.zip 。たとえば、Agent-AIX-12.0.0-1234.powerpc.zipです。
- Deep Security Agent 9.0 for AIX: Agent-AIX_<AIX_version>-<agent_release>-<build>.powerpc.bff.gz.zip。例えば、Agent-AIX_5.3-9.0.0-5625.powerpc.bff.gz.zip。

使用しているAIXのバージョンに必要なAgentの詳細については、「"Deep Security Agentのプラットフォーム" on page 400」を参照してください。

Deep Securityデータベースからソフトウェアパッケージを削除する

ディスク容量を節約するために、Deep Security Managerは定期的にDeep Securityデータベースから未使用のパッケージを削除します。保持する古いパッケージの最大数を設定するには、[システム設定]→[ストレージ]の順に選択します。

注意: Deep Security Virtual Applianceは、64ビットRed Hat Enterprise Linux用Deep Security Agentと同じ保護モジュールを使用します。そのため、有効化されたDeep Security Virtual Applianceがある場合に、64ビット版のRed Hat Enterprise Linux Agentソフトウェアパッケージをデータベースから削除しようとすると、ソフトウェアが使用中であることを示すエラーメッセージが表示されます。

削除できるパッケージは次のとおりです。

- agent
- カーネルサポート

シングルテナントモードでAgentパッケージを削除する

シングルテナントモードでは、現在Agentで使用されていないエージェントパッケージ (Agent-*platform-version*.zip) がDeep Securityによって自動的に削除されます。または、未使用のエージェントパッケージを手動で削除することもできます。未使用のソフトウェアパッケージのみ削除できます。

Windows版とLinux版のAgentパッケージについては、使用中のパッケージ (Agentインストーラと同じバージョンのパッケージ) のみ削除できません。

マルチテナントモードでAgentパッケージを削除する

マルチテナントモードでは、未使用のエージェントパッケージ (Agent-*platform-version*.zip) は自動的に削除されません。ユーザとテナントがDeep Securityデータベース内の同じソフトウェアリポジトリを共有している場合でも、プライバシー上の理由から、Deep Securityではテナントがソフトウェアを使用しているかどうかを判断できません。プライマリテナントであるDeep Securityでは、自分のアカウントのどのコンピュータでも実行されていないソフトウェアを削除できますが、ソフトウェアパッケージを削除する前に、他のテナントが使用していないことを確認してください。

カーネルサポートパッケージを削除する

シングルテナントモードとマルチテナントモードの両方で、未使用のカーネルサポートパッケージ (KernelSupport-*platform-version*.zip) が自動的に削除されます。次の両方の条件が満たされている場合、カーネルサポートパッケージを削除できます。

- グループIDが同じAgentパッケージがない。
- 同じグループIDでビルド番号がより新しいカーネルサポートパッケージが別にある。

また、使用されていないカーネルサポートパッケージを手動で削除することもできます。Linux版のカーネルサポートパッケージについては、最新版のパッケージのみ削除できません。

AgentのLinux Secure Bootの設定

Deep Security Agent for Linuxの一部のバージョンは、Unified Extensible Firmware Interface (UEFI) セキュアブートと互換性があります。

Secure Bootが有効になっている場合、コンピュータのLinuxカーネルは、各カーネルモジュールのPKI署名をロード前に確認します。署名されていないカーネルモジュールや無効な署名のモジュールはロードされません。次のDeep Security Agentの機能はカーネルモジュールをインストールします:

- 不正プログラム対策
- Webレピュテーション
- ファイアウォール
- 変更監視
- 侵入防御
- アプリケーションコントロール

これらの機能をセキュアブートで使用するには、トレンドマイクロの公開鍵をコンピュータのファームウェアに登録して、これらのカーネルモジュールの署名の検証を有効にする必要があります。

方法はプラットフォームによって異なります。

- AWSのセキュアブートキーの登録
- Google Cloud Platformのセキュアブートキーの登録
- VMware vSphereのセキュアブートキーの登録
- 物理コンピュータのセキュアブートキーを登録する
- Oracle Linux用セキュアブートキーの登録
- Azure用のセキュアブートキーを登録する

トレンドマイクロの公開鍵のダウンロード

セキュアブートコンピュータに登録する前に、カーネルモジュールの署名の検証に使用するトレンドマイクロの公開鍵をダウンロードする必要があります。キーファイルのダウンロードで問題が発生した場合は、右クリックして[名前を付けてリンク先を保存]を選択します。

公開鍵はDER形式でエンコードされます。

- DS2022.der

  SHA-256証明書ハッシュ: BB FA 4A B8 3C 61 A0 3F 1D D0 4B A7 A4 51 75 E7 D7 EF D3 C8 4B F3 D9 FE A0 CE AB B9 2A F4 8E 92

- DS20_V2.der

SHA-256証明書ハッシュ: B3 36 43 7B 12 B3 EB 6A 4E 4A 44 62 40 4F 1F BD 21 32 70 77 4C 33 7D 1C 5A 58 7C 99 83 F7 30 C7

カーネル5.3.18-24.34-default以降のSuSE 15にエージェントを配備する場合、カーネルモジュールの署名の検証が変更されたため、DS20_v2.derが必要です。

- DS11_2022.der

  SHA-256証明書ハッシュ: BB FA 4A B8 3C 61 A0 3F 1D D0 4B A7 A4 51 75 E7 D7 EF D3 C8 4B F3 D9 FE A0 CE AB B9 2A F4 8E 92

  エージェントバージョン11の古い公開鍵 (DS11.der with SHA-1ハッシュ7D 96 56 5C 3A 77 B7 A7 24 49 D5 6A A5 0C 28 AA D7 3B 0B fB) の有効期限は2022年12月5日です。この日付以降にエージェントを使用するには、この新しい公開鍵を登録する必要があります。そうしないと、コンソールに「エンジンオフライン」エラーメッセージが表示され、コンピュータが保護されません。

また、トレンドマイクロの公開鍵の署名チェーンを検証するために必要な中間認証局 (CA) 証明書をダウンロードする必要があります。CA証明書は、DER形式でエンコードされたX.509 v3 CRTファイルです。

- MicWinProPCA2011_2011-10-19.crt

  Microsoft Windows製品版PCA 2011

  SHA-256証明書ハッシュ: E8 E9 5F 07 33 A5 5E 8B AD 7B E0 A1 41 3E E2 3C 51 FC EA 64 B3 C8 FA 6A 78 69 35 FD DC C7 19 61

- MicCorUEFCA2011_2011-06-27.crt

  Microsoft Corporation UEFI CA 2011

  SHA-256証明書ハッシュ: 48 E9 9B 99 1F 57 FC 52 F7 61 49 59 9B FF 0A 58 C4 71 54 22 9B 9F 8D 60 3A C4 0D 35 00 24 85 07

- MicCorKEKCA2011_2011-06-24.crt

  Microsoft Corporation KEK CA 2011

  SHA-256証明書ハッシュ: A1 11 7F 51 6A 32 CE FC BA 3F 2D 1A CE 10 A8 79 72 FD 6B BE 8F E0 D0 B9 96 E0 9E 65 D8 02 A5 03

トレンドマイクロの公開鍵をアップデートする

次のいずれかに該当する場合は、署名済みのトレンドマイクロカーネルモジュールの登録済み公開鍵をアップデートする必要があります。

エージェントを後のメジャーリリースにアップグレードします

> エージェントのすべてのメジャーリリース(エージェント12.0および20.0など) では、セキュアブートカーネルモジュールの署名の公開鍵が更新されます。新しいカーネルモジュールの署名は、古い公開鍵では検証できません。そのため、エージェントをアップグレードする場合は、新しい公開鍵も登録する必要があります。

公開鍵の有効期限が切れています

エージェントバージョン	Key	有効期限	コメント,メモ,注釈,説明,補足,comment
20	DS2022.der	2031年11月24日	新しい交換用キーは、有効期限の1年前にリリースされる予定です。
	DS20.der	2024年11月26日	DS20.derはDS2022.derに置き換えられました。DS2022.derはDS20.derの有効期限が切れる前に登録されている必要があります。
	DS20_V2.der	2026年10月24日	• 5.3.18-24.34-default以降のSUSE 15カーネルでは必須です。 • DS20_V2.derは、有効期限が切れるとDS2022.derに置き換えられます。DS20_V2.derの有効期限が切れる前にDS2022.derが登録されていることを確認します。
12	DS12.der	2024年11月26日	DS12.derは有効期限が切れたため、DS2022.derに置き換えられました。DS2022.derはDS12.derの有効期限前に登録されている必要があります。

エージェントバージョン	Key	有効期限	コメント,メモ,注釈,説明,補足,comment
11	DS11_2022.der	2031年11月24日	
	DS11.der	2022年12月5日	

Deep Security Agent 20でSecure Bootを使用するには、DS2022.derキーとDS20_V2.derキーを登録することが重要です。

Linuxカーネルモジュールの署名検証が変更されました

Linuxカーネルを更新すると、カーネルモジュールの署名を検証する方法が変更されることがあります。これにより、登録された公開鍵を置き換える必要があるかもしれません。

例えば、SuSE 15はカーネルバージョン5.3.18-24.34-defaultでEKUコード署名検証を追加し、新しい公開鍵バージョンDS20_v2.derが必要でした。

警告: これらのいずれかの理由でセキュアブートの公開鍵が無効になり、その公開鍵を置き換えないと、「エンジンがオフラインです」というエラーメッセージがコンソールに表示され、コンピュータが保護されなくなる可能性があります。

AWSのセキュアブートキーの登録

1. 必要なものをダウンロードセキュアブート用のCA証明書とトレンドマイクロの公開鍵.
2. プラットフォームキーがない場合は、AWSのドキュメントを参照して、でセキュアブートプラットフォームキーを生成してください。

   警告: 起動時にロードされるすべてのデバイス(GPUなど)のファームウェアにアクセスできる場合にのみ、プラットフォームキーを置き換えます。新しいプラットフォームキーを使用するように

ファームウェアの署名チェーンをアップデートできない場合、セキュアブートによってインスタンスが完全に起動できなくなる可能性があります。

3. セキュアブートをサポートするLinuxディストリビューションのAMIからEC2仮想マシンインスタンスを作成します。
4. そのインスタンスのコンソールで、Machine Owner Key (MOK) コマンド`mokutil` `uefivars`とPythonをインストールします。

   たとえば、Red Hat Enterprise Linuxでは、次のコマンドを実行します。

   ```
   yum install mokutil
   yum install python3
   curl -L -o uefivars.zip https://github.com/awslabs/python-uefivars/archive/refs/heads/main.zip
   unzip uefivars.zip
   ```

   DebianまたはUbuntuで、次のコマンドを実行します。

   ```
   sudo apt-get update
   sudo apt-get install efitools
   sudo apt-get install python3
   curl -L -o uefivars.zip https://github.com/awslabs/python-uefivars/archive/refs/heads/main.zip
   unzip uefivars.zip
   ```

5. CA証明書とトレンドマイクロの公開鍵をインスタンスにアップロードします。
6. UEFI署名リスト(`.esl`) ファイル内に、各プラットフォームキー、CA証明書、およびトレンドマイクロ公開キーを配置します。それらを1つのファイルに結合し、バイナリ(`.bin`) 形式に変換します。

   たとえば、使用するトレンドマイクロの公開鍵に応じて、次のコマンドを入力します。

   ```
   # Convert your platform key into signatures list format
   cert-to-efi-sig-list YOUR_PLATFORM_KEY.crt YOUR_PLATFORM_KEY.esl
   # Convert CA certificates
   sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output MS_CA_KEK.esl MicCorKEKCA2011_2011-06-24.crt
   ```

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output MS_CA_
PROD.esl MicWinProPCA2011_2011-10-19.crt

sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output MS_CA_UEFI.esl
MicCorUEFCA2011_2011-06-27.crt

# Convert Trend Micro public keys

sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output TREND_UEFI_
db_DS11.esl DS11_2022.der

sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output TREND_UEFI_
db_DS20_v2.esl DS20_v2.der

sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output TREND_UEFI_
db_DS2022.esl DS2022.der

# Combine CA and vendor public keys into one signatures list

cat MS_CA_PROD.esl MS_CA_UEFI.esl TREND_UEFI_db_DS11.esl TREND_UEFI_db_
DS12.esl TREND_UEFI_db_DS20.esl TREND_UEFI_db_DS20_v2.esl TREND_UEFI_db_
DS2022.esl > ALL_SIGNATURES_db.esl

cp *.esl /root/

# Combine all and convert to binary

./python-uefivars-main/uefivars.py -i none -o aws -O YOUR_BINARY_SIGNING_CHAIN.bin -P
./YOUR_PLATFORM_KEY.esl -K ./MS_CA_KEK.esl --db ./ALL_SIGNATURES_db.esl
```

ここで、77fa9abd-0359-4d32-bd60-28f4e78f784b は、Microsoft CorporationのKEK CA 2011証明書の SignatureOwner フィールドのGUIDです。

7. .bin ファイルをダウンロードします。
8. インスタンスの新しいEC2スナップショットを作成します。
9. [AWS Cloudshell] に移動し、[処理] →[ファイル]→[ファイルのアップロード] の順に選択し、バイナリファイルを選択します。
10. スナップショットIDとアップロードした .bin ファイルを使用して、新しいAMIを作成します。

    たとえば、次のコマンドを入力できます。

```
aws ec2 register-image --name LIFT-UBUNTU20SecureBootX64 --uefi-data $(cat YOUR_
BINARY_SIGNING_CHAIN.bin) --block-device-mappings "DeviceName=/dev/sda1,Ebs=
```

```
{SnapshotId={{YOUR-SNAPSHOT-ID}},DeleteOnTermination=true}" --architecture x86_64 --root-device-name /dev/sda1 --virtualization-type hvm --boot-mode uefi
```

11. カスタマイズしたイメージを使用して、セキュアブートが有効な新しいインスタンスを作成します。
12. 次のコマンドを実行して、鍵がMOKリストに正常に登録されたことを確認します。

    ```
    mokutil --db | grep Trend
    ```

    カーネルがトレンドマイクロの公開鍵を正常にロードしたことを確認します。

    ```
    dmesg | grep証明書
    ```

Google Cloud Platformのセキュアブートキーの登録

1. 必要なものをダウンロードセキュアブート用のCA証明書とトレンドマイクロの公開鍵。
2. プラットフォームキーがない場合は、Google Cloud Platformのドキュメントを参照して、でプラットフォームキーを生成してください。

   警告: 起動時にロードされるすべてのデバイス(GPUなど)のファームウェアにアクセスできる場合にのみ、プラットフォームキーを置き換えます。新しいプラットフォームキーを使用するようにファームウェアの署名チェーンをアップデートできない場合、セキュアブートによってインスタンスが完全に起動できなくなる可能性があります。

3. セキュアブートで使用するCA証明書とトレンドマイクロの公開鍵を使用して、カスタマイズされた仮想マシンイメージを作成します。

   たとえば、次のコマンドを入力します。

   ```
   gcloud compute images create [IMAGE_NAME] \
   --source-image=[SOURCE_IMAGE] \
   --source-image-project=[SOURCE_PROJECT] \
   --platform-key-file=YOUR_PLATFORM_KEY.der \
   --signature-database-file=./MicCorUEFCA2011_2011-06-27.crt,./MicWinProPCA2011_2011-10-19.crt,./DS2022.der,./DS20_v2.der,./DS11_2022.der[,OTHER_EXISTING_KEYS] \
   --guest-os-features=UEFI_COMPATIBLE
   ```

公開鍵はDERまたはBIN形式である必要があります。それぞれをカンマ(,)で区切ります。コマンドの使用方法とAPIの詳細については、Google Cloud Platformのドキュメントを参照してください。

このコマンドを入力すると、既存のすべてのセキュアブートキーが上書きされるため、既存のセキュアブートキーをすべて含める必要があります。これらを含めない場合、それらは削除され、カーネルモジュールはロードされません。

4. カスタマイズしたイメージを使用して、セキュアブートが有効な新しい仮想マシンインスタンスを作成します。
5. 次のコマンドを実行して、キーが正常に登録されたことを確認します。

```
grep 'Trend' /proc/keys
```

VMware vSphereプラットフォームのセキュアブートキーの登録

コンピュータがUnbreakable Enterprise Kernel Release 6 Update 3 (UEK R6U3) for Oracle Linuxより前のリリースを使用している場合を除き、次の手順に従ってVMware vSphere仮想化プラットフォームのセキュアブートキーを登録します。

1. 必要なものをダウンロードセキュアブート用のCA証明書とトレンドマイクロの公開鍵。
2. セキュアブートを有効にするコンピュータで、コンピュータ所有者キー(MOK)コマンド`mokutil`をインストールします。

   たとえば、Red Hat Enterprise Linuxでは、次のコマンドを入力します。

   ```
   yum install mokutil
   ```

   DebianまたはUbuntuでは、次のコマンドを入力します。

   ```
   sudo apt-get update
   ```

   ```
   sudo apt-get install efitools
   ```

3. トレンドマイクロの公開鍵をMOKリストに追加します。複数の鍵はスペースで区切ります(該当する場合)。次の例は、Deep Security Agentのバージョンが20.0.0.7119より前の場合に実行するコマンドを示しています。

   ```
   mokutil --import /opt/ds_agent/DS2022.der /opt/ds_agent/DS20_v2.der
   ```

次の例は、Deep Security Agentバージョン20.0.0.7119以降を使用している場合に実行するコマンドを示しています。

```
mokutil --import /opt/ds_agent/secureboot/DS2022.der /opt/ds_agent/secureboot/DS20_v2.der
```

プロンプトが表示されたら、後で使用するパスワードを入力します。

4. コンピュータを再起動します。
5. Shim UEFIキー管理コンソールが開いたら、任意のキーを押して続行します。
6. [MOK管理の実行] 画面で、[MOKの登録] を選択します。
7. 公開鍵の詳細を確認する必要がある場合は、[鍵Xの表示] を選択します。[Enroll MOK] 画面に戻るには、任意のキーを押します。
8. [キーを登録しますか?] 画面で [続行] を選択します。
9. [はい] を選択し、以前に入力したパスワードを入力します。
10. [システムを再起動する必要があります] 画面で、[OK] を選択します。
11. キーがMOKリストに正常に登録されていることを確認します。
    - ほとんどのLinuxディストリビューションでは、次のコマンドを入力します。

      ```
      mokutil --test-key /opt/ds_agent/${certificate_file}.der
      ```

    - Debian Linux 11、12、または13の場合、次のコマンドを入力してください:

      ```
      keyctl show %:.platform | grep 'Trend'
      ```

物理コンピュータのセキュアブートキーを登録する

Unbreakable Enterprise Kernel Release 6 Update 3 (UEK R6U3) for Oracle Linuxより前のリリースを使用している場合を除き、次の手順に従って物理コンピュータのセキュアブートキーを登録します。

1. 必要なセキュアブート用のCA証明書とトレンドマイクロの公開鍵をダウンロードします。
2. プラットフォームキーがない場合は、Linuxディストリビューションのドキュメントを参照してセキュアブートプラットフォームキーを生成してください。

警告: 起動時にロードされるすべてのデバイス(GPUなど)のファームウェアにアクセスできる場合にのみ、プラットフォームキーを置き換えます。新しいプラットフォームキーを使用するようにファームウェアの署名チェーンをアップデートできない場合、セキュアブートによってインスタンスが完全に起動できなくなる可能性があります。

3. セキュアブートを有効にするコンピュータで、コンピュータ所有者キー(MOK)コマンド`mokutil`をインストールします。

   たとえば、Red Hat Enterprise Linuxでは、次のコマンドを入力します。

   ```
   yum install mokutil
   ```

   DebianまたはUbuntuでは、次のコマンドを入力します。

   ```
   sudo apt-get update
   ```

   ```
   sudo apt-get install efitools
   ```

4. トレンドマイクロの公開鍵をMOKリストに追加します。複数の鍵はスペースで区切ります(該当する場合)。次の例は、Deep Security Agentのバージョンが20.0.0.7119より前の場合に実行するコマンドを示しています。

   ```
   mokutil --import /opt/ds_agent/DS2022.der /opt/ds_agent/DS20_v2.der
   ```

   次の例は、Deep Security Agentバージョン20.0.0.7119以降を使用している場合に実行するコマンドを示しています。

   ```
   mokutil --import /opt/ds_agent/secureboot/DS2022.der /opt/ds_agent/secureboot/DS20_v2.der
   ```

   プロンプトが表示されたら、後で使用するパスワードを入力します。

5. コンピュータを再起動します。
6. Shim UEFIキー管理コンソールが開いたら、任意のキーを押して続行します。
7. [MOK管理の実行]画面で、[MOKの登録]を選択します。
8. 公開鍵の詳細を確認する必要がある場合は、[鍵Xの表示]を選択します。[Enroll MOK]画面に戻るには、任意のキーを押します。
9. [キーを登録しますか?]で[続行]を選択します。画面に表示されます。
10. [はい]を選択し、以前に入力したパスワードを入力します。

11. [システムを再起動する必要があります] 画面で、[OK] を選択します。
12. キーがMOKリストに正常に登録されていることを確認します。
    - ほとんどのLinuxディストリビューションでは、次のコマンドを入力します。

      ```
      mokutil --test-key /opt/ds_agent/${certificate_file}.der
      ```

    - Debian Linux 11、12、または13の場合、次のコマンドを入力してください:

      ```
      keyctl show %:.platform | grep 'Trend'
      ```

Oracle Linux用 セキュアブートキーの登録

Unbreakable Enterprise Kernel Release 6 Update 3 (UEK R6U3) for Oracle Linuxでは、セキュアブートに必要な手順が若干異なります。UEKを使用すると、カーネルは組み込みのキーリングにあるキーのみを信頼します。したがって、トレンドマイクロの公開鍵を使用してカーネルを再コンパイルする必要があります。これによりカーネル自体が変更されるため、新しいカーネルブートイメージにも署名する必要があります。

1. 必要なものをダウンロードセキュアブート用のCA証明書とトレンドマイクロの公開鍵。
2. セキュアブートで使用するカーネルイメージおよびカーネルモジュールの署名については、Oracle Linuxのドキュメントを参照してください。
3. カーネルイメージへのモジュール証明書の挿入の手順が表示されたら、`pubkey.der` をトレンドマイクロの公開鍵の名前に置き換えます。例:

   ```
   sudo /usr/src/kernels/$(uname -r)/scripts/insert-sys-cert -s /boot/System.map$(uname -r) -z /boot/vmlinuz$(uname -r) -c ./DS20_v2.der
   ```

4. 残りの手順を続行して、カーネルブートイメージに署名します。
5. 次のコマンドを実行して、キーが`builtin_trusted_keys`キーリングにリストされていることを確認します。

   ```
   sudo keyctl show %:.builtin_trusted_keys | grep 'Trend'
   ```

Azure のセキュアブートキーを登録する

1. 必要なセキュアブート用の CA 証明書とトレンドマイクロの公開鍵をダウンロードします。
2. 次の手順でSecure Bootをサポートするlinuxディストリビューションイメージから世代2のAzure VMを作成します。

   a. 世代2がサポートされているVMイメージを選択してください。
   b. Azure ポータルで 仮想マシンの作成 ページに移動します。
   c. セキュリティの種類 リストから信頼された起動仮想マシンを選択します。
   d. セキュリティ機能の構成で、セキュアブートを有効にするを選択します。

   次の条件を満たすカスタムイメージ用の第2世代Azure VMを既にお持ちの場合は、前の手順をスキップしてください。

   - セキュリティタイプは信頼された起動仮想マシンとして指定されています。
   - セキュアブートを有効にするセキュリティ機能が選択されています。

3. Azure VMが停止していることを確認し、VMディスク名をメモしてください。
4. az login コマンドをローカルで、またはAzureのCloud Shellを通じて実行します。
5. 次のスクリプトを1行ずつ実行して、共有アクセス署名 (SAS) URL を生成してください。

```
read -p 'Your Subscription ID: ' subscriptionId
read -p 'Your Resource Group Name: ' resourceGroupName
read -p 'Your Disk Name for Exporting: ' diskName
read -p 'Input the Expiry Duration for SAS URL in seconds (for example, 3600): ' sasExpiryDuration
read -p 'Your Storage Account Name to Hold this VHD file: ' storageAccountName
read -p 'Your Storage Container Name: ' storageContainerName
read -p 'Your Storage Account Key: ' storageAccountKey
read -p 'Your Destination VHD File Name: ' destinationVHDFileName
az account set --subscription $subscriptionId
sas=$(az disk grant-access --resource-group $resourceGroupName --name $diskName --duration-in-seconds $sasExpiryDuration --query [accessSas] -o tsv)
```

```
az storage blob copy start --destination-blob $destinationVHDFileName --destination-container $storageContainerName --account-name $storageAccountName --account-key $storageAccountKey --source-uri $sas
```

6. 次のファイルの内容をコピーして、CreateSIGFromOSvhdWithCustomUEFIKey.jsonとして保存してください:

```
{ "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json", "contentVersion": "1.0.0.0", "parameters": { "galleryName": { "defaultValue": "{{ change to custom gallary name for the deployed template }}", "type": "String", "metadata": { "description": "Name of the gallery" } }, "imageDefinitionName": { "defaultValue": "{{ change to custom image definition name }}", "type": "String", "metadata": { "description": "Name of the image definition" } }, "versionName": { "defaultValue": "{{ change to custom image version }}", "type": "String", "metadata": { "description": "Name of the image version" } }, "storageAccountName": { "defaultValue": "{{ change to custom storage account name contains the exported OS vhd }}", "type": "string", "metadata": { "description": "Storage account name containing the OS vhd" } }, "vhdURI": { "defaultValue": "{{ change to custom vhd URL of the exported OS vhd }}", "type": "String", "metadata": { "description": "OS vhd URL" } }, "imagePublisher": { "defaultValue": "{{ change to custom image publisher name }}", "type": "String", "metadata": { "description": "Publisher name of the image" } }, "offer": { "defaultValue": "{{ change to custom image offer name }}", "type": "String", "metadata": { "description": "Offer of the image" } }, "sku": { "defaultValue": "{{ change to custom image sku name }}", "type": "String", "metadata": { "description": "Sku of the image" } }, "osType": { "defaultValue": "Linux", "allowedValues": [ "Windows", "Linux" ], "type": "String", "metadata": { "description": "Operating system type" } }, "gallerySecurityType": { "defaultValue": "TrustedLaunchSupported", "type": "String", "allowedValues": [ "TrustedLaunchSupported", "TrustedLaunchAndConfidentialVMSupported" ], "metadata": { "description": "Gallery Image security type" } }, "customDBKeyDS20V2": { "defaultValue": "MIIFyzCCA7OgAwIBAgIJAOqCjczOdriRMA0GCSqGSIb3DQEBCwUAMGsxGjAYBgNVBAoMEVRyZW5kIE1pY3JvLCBJbmMuMSUwIwYDVQQDDBxUcmVuZCBNaWNybyBEZWVwIFNlY3VyaXR5IDIwMSYwJAYJKoZIhvcNAQkBFhdjc3VwcG9ydEB0cmVuZG1pY3JvLmNvbTAeFw0yMDExMjQwOTIzNTFaFw0yNjEwMjQwOTIzNTFaMGsxGjAYBgNVBAoMEVRyZW5kIE1pY3JvLCBJbmMuMSUwIwYDVQQDDBxUcmVuZCBNaWNybyBEZWVwIFNlY3VyaXR5IDIwMSYwJAYJKoZIhvcNAQkBFhdjc3VwcG9ydEB0cmVuZG1pY3JvLmNvbTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAK5e7V+I80gksQSQR74uxAZyIldKaLVqBob/J6Fbca8zt7pdxCLeebu6S3yT0DRiaS5UsIWO21v9q09cuqd0GoDCCaImNdMpCfTB91OZf9t3gHili0cTUyzkktT8n4g2/xw2mzoXBrm5PvX2psCFwBFh3FE7Mb5VgeA/Bh8uz7jpV9+7+TjouHQ9DXgV2dIDD2QacvtvaGyFqssNLKoKOnEm6+7o0/CI/9eIzJT0YKzqS2BFY13ANHVTJieNVrfI9dIu1XxU7ABQ8
```

LOVI835CAIJGJyYtIhnu2bCei7AGZzPYP7Way7djOvmG+2t+NopIE/RMTknsn3NQMJtrUi4oJ
OAwI36z8dMDBASUUCpgIK12C9z6vHeINrE4z/tiUFYei2OBsLB/yNP9HIoVDq4CMvcrZzwWb
UtxmtcbTIW/uU1LOsqV92aHIMA3ZivLvvAPvIr4/8NltTvEy5N/CsxUxAeC21AbE9OXDyyE/9C+
VB16YvrqQIEm5IW1Q0/fmmO6rBwy3Uu+4vZcUkq0QbOji/XcNbu17Cfg5fMuuLKu7kwqtl0JZx
hZ0XBNdmhOL+XfwrZbZvCqXIKFZo1QsXsbFIoiOWVakXDonUTLPLJX5n5/7iIrw7hiUViPvTrk
AUSjUm5OIu1p+hkKjGDHehdU4XX2bv9rrLAh3vIKxQSCTdIAgMBAAGjcjBwMAwGA1UdEwE
B/wQCMAAwCwYDVR0PBAQDAgeAMBMGA1UdJQQMMAoGCCsGAQUFBwMDMB0GA1U
dDgQWBBQ50RP6qbc9bEOp0jufVa+TgZWLlzAfBgNVHSMEGDAWgBQ50RP6qbc9bEOp0juf
Va+TgZWLlzANBgkqhkiG9w0BAQsFAAOCAgEAXBhNUgJeKlB/ZwwsIjJsGXa9IPczWfTklg85
hZILCT5KhcxI36zs6AEdtbW5pjV/hN+bV5LD84ZHoAa76ib4iHdU5nK4Q35AhWFdXMTCjg5b
m78lESkyC7vLljj1ITy2K3k+CgZosDXSe9V77AIN43+R4wwqbsI/FEuXmLw8UHW1DSQphjzc
NGXAdbJVXhGoYLLBpyZ/OSFqhcqWwTtHZukrivtfix8fAQZ1GvfPZA0NlseXbSh883aERqwgP
/etvdkUFuby0P66YTSaGZ4Dc9Q5NB4sJ+W/GcSz7Tnn2cF/hZor9ErjC+AUD0nvhn0IaJxzcCp
z53XjFD8K/XeHVpBP8FqHFCoh7Ro4WcYBFR+DfoCc9Xq6tovWFZIcokybM7AmYw3DDisclkf
MZFmhxi+yZQ6fmN9evVp2g7X/+w+hHrV38pnpz323186ALqSXShBPqG3HcQRvjdnS1Ve1nS
8UKvy+ae+0+TKR9KTD+jQsL9daW4NfaSaBetFmdnbuNRIlKXscgoSne+Qi3YhtI93BoOnfpxE
bWB4sWnSHkDO9iekSa42tabtCaY1d1MHxdYtdEBb1Gx5aWI8CmsZoWB0xRrk1NG7S8Mi+u
x/2LiOfECkm1mpzaUY0w4dKfTT7/YeVAm1zgumWX+T0dsDc5Sc3t7AxiLHSmTxtYphFT4c=",
"type": "String", "metadata": { "description": "Custom UEFI DB DS20_V2.der in base64 format" }
}, "customDBKeyDS2022": { "defaultValue":
"MIIFzzCCA7egAwIBAgIJAIfzdTk2xdt2MA0GCSqGSIb3DQEBCwUAMG0xGjAYBgNVBAoME
VRyZW5kIE1pY3JvLCBJbmMuMScwJQYDVQQDDB5UcmVuZCBNaWNybyBEZWVwIFNlY3
VyaXR5IDIwMjIxJjAkBgkqhkiG9w0BCQEWF2NzdXBwb3J0QHRyZW5kbWljcm8uY29tMB4XD
TIxMTEyNjA2MzI0OVoXDTMxMTEyNDA2MzI0OVowbTEaMBgGA1UECgwRVHJlbmQgTWljc
m8sIEluYy4xJzAlBgNVBAMMHlRyZW5kIE1pY3JvIERlZXAgU2VjdXJpdHkgMjAyMjEmMCQG
CSqGSIb3DQEJARYXY3N1cHBvcnRAdHJlbmRtaWNyby5jb20wggIiMA0GCSqGSIb3DQEBA
QUAA4ICDwAwggIKAoICAQCWb6JAyvw0PoMfHEMoBtj3hsRS8q5TPFoa6vDrAOcJZf0MTw3
NZjlbnNzVP/Ri4J5DGpOWDXLte0ngugtdAG+w3y8UY8K2agEq1ehGIB3iUz45zPqDiQWs/hua
fj96q9FzNlWkLJT+M0E2l0qpNJ9NlyphbQ+cnccm1fHrNOMNtEbm31nW4DVD9VyB7BFf4NR
S2h4FiDjRqUTAREMfk84MReQNEP98kPZLXR3ajE4MTZztYF6INR68nK9Jzig/vJjMRpMwFp+
VkQaFnbiti6hbfRjS/GbCW62aJJCTHEavbyJKKY1+MRG406lYVIpH632iyvHfj2ni+B7lLvfi5qag
+27mX+rBxlqLGuiwNu0geGv5GTlmDyx2onNWRz1akk5GJUloY2xG9ak92o6WsnDdJCXlFHyt
Pc0R+FleZ/nNNpyzPYr1V8pqWenk+wpVcA7BsuRHofWYzut98GkjGYWXXjsipaDt1V2tTKNex
FgzMCUIi/tJGmUe3U6czS4zk3tXiTq2Z3kZvrV59nRWJ+QEdax0ICNZH6AEqNNajgvcvP9WcZ
mOtgozNxoJuQrCETMKcPQ+JgLbSAiZU7zLIp1z7XF358G7Azu/AGFpJ0orSpZ9f2J7f1WQ8C
sHUgz9KISw6P7b8j160CCEbLBxcRnORCGSeVpO5tdKt4a7oiI5wwIDAQABo3IwcDAMBgNV
HRMBAf8EAjAAMAsGA1UdDwQEAwIHgDATBgNVHSUEDDAKBggrBgEFBQcDAzAdBgNVH

Q4EFgQUnbiI6RHtI1sidPNZk/35mq9EaWAwHwYDVR0jBBgwFoAUnbiI6RHtI1sidPNZk/35mq9EaWAwDQYJKoZIhvcNAQELBQADggIBADsauvVNB9jPnIkOJY48eayLDfDN6JMriDA8Q0s0X9EZtTBMcRSNGIQjtyr4LOCOMNrUGMG2XFKHa8S17QYtcFM/2Y+t7aOilSTokWTkwC9jU1XBESH7fV44d/fYEO5yD3LBYw5BIEgSqJg39rdWWWOD6N1CGRwH3SZwT1aeDj7+YqCYXIUFR/jUm6SXyenoxIISkn6Ymf3PiI3GtnqqxW1+VfkL6YOa715/3ZxqdWfvf1ArUL0spEtQEm4yHwdCuhPWbIG1RKejSFSLk92B/RdxqvYXiCxZ5SLziOLsIvW0s48LrQ0TEr/HWhiuJ2Q//NSSCIIUYy9f6CwXnW38xmI+zZu/I8qJ5smI19JfO77HeRGACNSp2GC/C2mamLb1dSXSDKG6YomcrEFSO9oII/gfi6hwCw5Lx21/dD2SBjKMnwBYGRvDsovE2BQ26GnzvKQbJZW+kN6s5Gi3L0C56kSLLZUFJUxkKFN2//Qyu0cMC0oeecr+CYDxAHD2FMf4HGJAAScnk9mcEhxYs+B2IW/nCaRjbYvUg1LdaOR9oCXH14rh+FJ9DZmR84ia/YArHOJXSX/ziy0ftePgAGqQBmHNIPDA0TSGUYg/P5fcfYTT2bKO6lV/uXiqmDQuuCm1ietUpaTAJ0kWdDxhDzJem+N1qABRpuT93xbaapiX3199", "type": "String", "metadata": { "description": "Custom UEFI DB DS2022.der in base64 format" } } }, "variables": { "linuxSignatureTemplate": "MicrosoftUefiCertificateAuthorityTemplate", "windowsSignatureTemplate": "MicrosoftWindowsTemplate" }, "resources": [{ "type": "Microsoft.Compute/galleries", "apiVersion": "2022-01-03", "name": "[parameters ('galleryName')]", "location": "[resourceGroup().location]", "tags": { "AzSecPackAutoConfigReady": "true" }, "properties": { "identifier": {} } }, { "type": "Microsoft.Compute/galleries/images", "apiVersion": "2022-08-03", "name": "[concat (parameters('galleryName'), '/', parameters('imageDefinitionName'))]", "location": "[resourceGroup().location]", "dependsOn": ["[resourceId('Microsoft.Compute/galleries', parameters('galleryName'))]"], "tags": { "AzSecPackAutoConfigReady": "true" }, "properties": { "hyperVGeneration": "V2", "architecture": "x64", "osType": "[parameters('osType')]", "osState": "Generalized", "identifier": { "publisher": "[parameters('imagePublisher')]", "offer": "[parameters ('offer')]", "sku": "[parameters('sku')]" }, "features": [{ "name": "SecurityType", "value": "TrustedLaunchSupported" }], "recommended": { "vCPUs": { "min": 1, "max": 16 }, "memory": { "min": 1, "max": 32 } } } }, { "type": "Microsoft.Compute/galleries/images/versions", "apiVersion": "2022-08-03", "name": "[concat(parameters('galleryName'), '/',parameters ('imageDefinitionName'),'/', parameters('versionName'))]", "location": "[resourceGroup ().location]", "dependsOn": ["[resourceId('Microsoft.Compute/galleries/images', parameters ('galleryName'), parameters('imageDefinitionName'))]", "[resourceId ('Microsoft.Compute/galleries', parameters('galleryName'))]"], "properties": { "publishingProfile": { "targetRegions": [{ "name": "[resourceGroup().location]", "regionalReplicaCount": 1 }] }, "storageProfile": { "osDiskImage": { "hostCaching": "ReadOnly", "source": { "uri": "[parameters ('vhdURI')]", "storageAccountId": "[resourceId('Microsoft.Storage/storageAccounts', parameters ('storageAccountName'))]" } } }, "securityProfile": { "uefiSettings": { "signatureTemplateNames": ["[if(equals(parameters('osType'),'Linux'), variables('linuxSignatureTemplate'), variables ('windowsSignatureTemplate'))]"], "additionalSignatures": { "db": [{ "type": "x509", "value": ["[parameters('customDBKeyDS20')]"] }, { "type": "x509", "value": ["[parameters

('customDBKeyDS20V2')]"] }, { "type": "x509", "value": ["[parameters('customDBKeyDS2022')]"] }] } } } }] }

7. CreateSIGFromOSvhdWithCustomUEFIKey.jsonファイルの"parameters"セクション内の{{ }}の値を次の点に注意して置き換えてください。

   - 前のCreateSIGFromOSvhdWithCustomUEFIKey.jsonファイルはカスタム展開の例です。DS20_v2.derとDS2022.derはすでにBase64形式で記入されています。

   - 別の公開鍵をテンプレートに登録するには、次のコマンドを使用して鍵をBase64形式に変換し、その後JSONファイルに鍵を追加してください。

     openssl base64 -in <Trend_Micro_public_key> -A

8. Azure CLIを使用してテンプレートデプロイメントによる共有イメージギャラリー(SIG)イメージを作成する方法は以下の通りです。

   az deployment group create --resource-group <resource-group-name> --template-file CreateSIGFromOSvhdWithCustomUEFIKey.json

9. カスタムデプロイメントイメージでAzure VMを作成します。

10. 次のコマンドを実行して、キーがMachine Owner Key (MOK) リストに正常に登録されていることを確認してください。

    mokutil --db | grep Trend

11. 次のコマンドを実行して、カーネルがトレンドマイクロの公開鍵を読み込んだことを確認してください:

    dmesg | grep cert

詳細については、セキュアブートUEFIキーを参照してください。

エージェントをインストールする

トピック:

- "エージェントを手動でインストールする" on the next page
- "他の方法でエージェントをインストールする" on page 543
- "インストール後のタスク" on page 543

エージェントを手動でインストールする

開始する前に、次の内容を確認してください。

1. エージェントのシステム要件を確認しました。"システム要件 " on page 400を参照してください。
2. Windowsのみ:"Deep Security AgentとMicrosoft Defender ウイルス対策の共存" on page 854
3. 適切なポート番号でエージェントとの間で送受信を許可する送受信の通信。"Deep Securityのポート番号" on page 429を参照してください。
4. エージェントソフトウェアをManagerにインポートしました。"エージェントソフトウェアのインポート" on page 515を参照してください。
5. エージェントソフトウェアがManagerからエクスポートされました。"Agentのインストーラをエクスポートする" on page 517を参照してください。

次に、エージェントをインストールします。使用しているプラットフォームの手順に従ってください。

エージェントをWindowsにインストールする

1. エージェントZIPをコンピュータにコピーして解凍します。
2. インストールファイル (.MSIファイル) をダブルクリックして、インストーラパッケージを実行します。

   注意: Windows Server 2012 R2 Server Coreの場合は、次のコマンドを使用してインストーラを起動します. msiexec / i Agent-Core-Windows-12.x-xxxx.x86_64.msi
3. 最初の画面で [次へ] をクリックしてインストールを開始します。
4. 使用許諾契約書: 使用許諾契約書の内容をご確認いただき同意できる場合は、使用許諾内容に同意し、[次へ] をクリックします。
5. インストール先フォルダ: Deep Security Agentのインストール先を選択し、[次へ] をクリックします。
6. Trend Micro Deep Security Agentのインストール準備完了: [インストール] をクリックしてインストールを続行します。
7. 完了: インストールが正常に完了したら、[完了] をクリックします。

これで、Deep Security Agentはコンピュータにインストールされ、稼働しています。コンピュータを起動するたびに、Deep Security Agentが起動します。

注意: AgentをWindows Server 2012 Server Coreにインストールする場合は、Notifierは含まれません。

注意: インストール中、ネットワークインタフェースが停止し、復旧までに数秒間かかります。DHCPを使用している場合、新しい要求が生成されるため、復旧した接続に対して別のIPアドレスが割り当てられる可能性があります。

Amazon WorkSpacesでのインストール

- エラーコード「2503」でDeep Security Agentの.msiファイルをインストールできない場合は、次のいずれかを実行する必要があります。
  - C:\Windows\Tempフォルダを編集して、ユーザの書き込み権限を許可します。
    または
  - コマンドプロンプトを管理者として開いて、.msiファイルを実行します。

注意: Amazonは、新しく導入されたAmazon WorkSpacesのこの問題を修正しています。

Windows 2012 Server Coreでのインストール

- Deep Securityでは、Deep Security Agentのインストール後に、Windows Server 2012のサーバモードをServer Coreモードとフル (GUI) モードの間で切り替えることはできません。
- Hyper-V環境でServer Coreモードを使用している場合、Server Coreコンピュータを別のコンピュータからリモートで管理するにはHyper-Vマネージャを使用する必要があります。Server CoreコンピュータにDeep Security Agentをインストールしてファイアウォールを有効にしている場合は、リモート管理接続がファイアウォールでブロックされます。Server Coreコンピュータをリモートで管理するには、ファイアウォール機能をオフにしてください。
- Hyper-Vには、ゲスト仮想マシンをHyper-Vサーバ間で移動するための移行機能があります。Hyper-Vサーバ間の接続はDeep Securityのファイアウォールでブロックされるため、この移行機能を使用する場合はファイアウォール機能をオフにする必要があります。

Red Hat、Amazon、SUSE、Oracle、Alma、Rocky、Miracle、またはCloud Linuxにエージェントをインストールする

---

1. エージェントZIPをコンピュータにコピーして解凍します。
2. Agentをインストールします。

```
# sudo rpm -i <package name>
Preparing... ########################################### [100%]
1:ds_agent ########################################### [100%]
Loading ds_filter_im module version ELx.x [ OK ]
Starting ds_agent: [ OK ]
```

インストールが完了すると、Deep Security Agentは自動的に起動します。

UbuntuまたはDebianにエージェントをインストールする

1. エージェントZIPをコンピュータにコピーして解凍します。
2. Agentをインストールします。

```
sudo dpkg -i <installer deb file>
```

Agentを起動、停止、リセットするには:

SysV initスクリプトの使用:

- 開始: `/etc/init.d/ds_agent start`
- 停止: `/etc/init.d/ds_agent stop`
- リセット: `/etc/init.d/ds_agent reset`
- 再起動: `/etc/init.d/ds_agent restart`
- ステータスの表示: `svcs -a | grep ds_agent`

systemdコマンドの使用:

- 開始: `systemctl start ds_agent`
- 停止: `systemctl stop ds_agent`
- 再起動: `systemctl restart ds_agent`
- ステータスの表示: `systemctl status ds_agent`

エージェントをSolarisにインストールする

注意: Deep Security Agentのインストールは、グローバルゾーンでのみサポートされています。

Deep Security Agentをサポートするには、次のライブラリをインストールする必要があります。

Solaris 10: SUNWgccruntime

Solaris 11.0 - 11.3: gcc-45-runtime

Solaris 11.4: なし; gcc-c-runtimeバージョン7.3が初期設定でインストールされています

1. エージェントインストーラパッケージを、エージェントをインストールするコンピュータにコピーします。
2. ZIPファイルを解凍します。
3. GZファイルを解凍します。

   ```
   gunzip <agent_GZ_file>
   ```

   エージェントインストーラファイル(P5PまたはPKG) を使用できるようになりました。

4. Agentをインストールします。インストールコマンドの例を以下に示します。Solarisバージョン、Solarisゾーン、Solarisプロセッサ、およびDeep Securityエージェントのパッケージ名に合わせてコマンドを変更します。
   - Solaris 11の場合、ゾーンが1つの場合は、大域ゾーンで次のコマンドを実行します。

     x86: `pkg install -g file:///mnt/Agent-Solaris_5.11-xx.x.x-xxxx.x86_64/Agent-Core-Solaris_5.11-xx.x.x-xxxx.x86_64.p5p pkg:/security/ds-agent`

     SPARC: `pkg install -g file:///mnt/Agent-Solaris_5.11-xx.x.x-xxxx.sparc/Agent-Core-Solaris_5.11-xx.x.x-xxxx.sparc.p5p pkg:/security/ds-agent`

   - Solaris 11の場合、ゾーンが複数ある場合は、大域ゾーンで次のコマンドを実行します。

     ```
     mkdir <path>
     ```

     ```
     pkgrepo create <path>
     ```

     ```
     pkgrecv -s file://<path_to_agent_p5p_file> -d <path> '*'
     ```

     ```
     pkg set-publisher -g <path> trendmicro
     ```

```
pkg install pkg://trendmicro/security/ds-agent
```

```
pkg unset-publisher trendmicro
```

```
rm -rf <path>
```

- Solaris 10の場合は、次のいずれかのコマンドを実行します。

  x86: `pkgadd -G -d Agent-Core-Solaris_5.10_Ux-xx.x.x-xxx.x86_64.pkg`

  SPARC: `pkgadd -G -d Agent-Core-Solaris_5.10_Ux-xx.x.x-xxx.sparc.pkg`

Agentを起動、停止、リセットするには:

- 開始: `svcadm enable ds_agent`
- 停止: `svcadm disable ds_agent`
- リセット: `/opt/ds_agent/dsa_control -r`
- 再起動: `svcadm restart ds_agent`
- ステータスの表示: `svcs -a | grep ds_agent`

Solaris 11でAgentをアンインストールするには:

```
pkg uninstall pkg:/security/ds-agent
```

Solaris 10でAgentをアンインストールするには:

```
pkgrm -v ds-agent
```

AIXにエージェントをインストールする

1. エージェントZIPをコンピュータにコピーして解凍します。GZファイルが使用可能になります。
2. GZファイルを別の場所に移動します。
3. gunzipを使用してGZファイルを展開します。BFFファイルが使用可能になります。インストーラファイルです。
4. BFFファイルをAIXコンピュータにコピーします。
5. BFFファイルを`/tmp`などの一時フォルダに配置します。
6. Agentをインストールします。

   `/ tmp> installp -a -d /tmp/<agent_BFF_file_name> ds_agent`

ここで、<agent_BFF_file_name> は、抽出したBFFインストーラファイルの名前に置き換えられます。

Agentのドライバを開始、停止、ロード、アンロードするには:

- 開始: startsrc -s ds_agent
- 停止: stopsrc -s ds_agent
- ドライバのロード: /opt/ds_agent/ds_fctrl load
- ドライバのアンロード: /opt/ds_agent/ds_fctrl unload

Red Hat OpenShiftにエージェントをインストールする

開始前の準備:

1. Helm v3以降がインストールされていることを確認します。
2. エージェントソフトウェアがDeep Security Managerにインポートされていることを確認してください。詳細については、"Deep Security Agentソフトウェアの入手" on page 514を参照してください。
3. Agentからのリモート有効化(AIA)が有効になっていることを確認します。AIAは、インストールスクリプトをインストール後にエージェントを有効にする場合に必要です。詳細については、「"Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511」を参照してください。

エージェントのインストール:

1. Deep Securityコンソールの右上隅で、サポート→インストールスクリプトをクリックします。
2. [OpenShift Agentのインストール]を選択します。
3. *(オプション)* セキュリティポリシー、コンピュータグループ、Relayグループ、Deep Security Managerへの接続に使用するプロキシ、Relayへの接続に使用するプロキシのオプションを選択します。
   インストールスクリプトジェネレータがスクリプトを表示します。
4. 次のうち1つを実行します:
   - [クリップボードにコピー]をクリックし、任意のインストールツールにインストールスクリプトを貼り付けます。
   - [ファイルに保存]をクリックします。

他の方法でエージェントをインストールする

エージェントを手動でインストールしない場合は、次のいずれかの方法を使用できます。

- 配置スクリプト: 配置スクリプトをマネージャ内で生成し、クライアントを使用してエージェントをインストールします。詳細については、「 "インストールスクリプトを使用したコンピュータの追加と保護" on page 1849
- Deep Security API: このAPIを使用して、コンピュータへのAgentのインストールを自動化するためのインストールスクリプトを生成します。Deep Security Automation Centerに スクリプトを使用してDeep Security ManagerおよびAgent を配信するを参照してください。
- SCCM: エージェントをインストールし、有効にし、ポリシーを適用するには、Microsoft System Center Configuration Manager(SCCM) を使用してください。SCCMを使用するには、[管理]→[システム設定]→[Agent] の順に選択し、Agentからのリモート有効化を有効にします。
- テンプレート: VMテンプレートにエージェントを含めます。"エージェントをAMIまたはWorkSpaceバンドルにインストールする" on page 549参照してください。ど"Azure VMにエージェントをインストールする" on page 553。

インストール後のタスク

エージェントをインストールした後、次のインストール後のタスクがインストールプロセスの一部として完了していない場合は、そのタスクを実行する必要があります。

- "Agentの有効化" on page 559
- "ポリシーをコンピュータに割り当てる" on page 722

Amazon EC2およびWorkSpacesへのAgentのインストール

Deep SecurityエージェントはAmazon WorkSpacesのWindowsデスクトップのみをサポートしています。Linuxデスクトップはサポートされていません。

既存のAmazon EC2インスタンスおよびAmazon WorkSpacesをDeep Securityで次のように保護できます:

1. "AWSアカウントをDeep Security Managerに追加する" on the next page
2. "通信方向を設定する" on the next page
3. "有効化の種類を設定する" on page 545
4. "ポートを開く" on page 546
5. "AgentをAmazon EC2インスタンスおよびWorkSpacesにインストールする" on page 547

6. "エージェントのインストールとアクティベーションを確認" on page 548
7. "ポリシーを割り当てる" on page 548

代わりにエージェントが組み込まれた新しいAmazon EC2インスタンスやAmazon WorkSpacesを起動したい場合は、"エージェントをAMIまたはWorkSpaceバンドルにインストールする" on page 549を参照してください。

Amazon EC2 インスタンスを保護した後に Amazon WorkSpaces を保護するには、"Amazon WorkSpacesを保護する(AWSアカウントをすでに追加している場合)" on page 677を参照してください。

AWSアカウントをDeep Security Managerに追加する

AWSアカウントをDeep Security Managerに追加する必要があります。これらのAWSアカウントには、Deep Securityで保護したいAmazon EC2インスタンスとAmazon WorkSpacesが含まれています。

詳細については、"AWSアカウントの追加について" on page 664を参照してください。

AWSアカウントを追加すると、次のようになります。

- 既存のAmazon EC2インスタンスおよびAmazon WorkSpacesはDeep Security Managerに表示されます。エージェントがインストールされていない場合、ステータスは未管理 (不明)となり、横に灰色のドットが表示されます。エージェントがすでにインストールされている場合、ステータスは管理 (オンライン)となり、横に緑色のドットが表示されます。
- このAWSアカウントでAWSを通じて起動する新しいAmazon EC2インスタンスまたはAmazon WorkSpacesは、Deep Security Managerによって自動検出され、コンピュータのリストに表示されます。

通信方向を設定する

通信方向をエージェント開始、マネージャ開始、または双方向のいずれかに設定する必要があります:

1. Deep Security Managerにログインします。
2. 通信方向を設定するには、"通信方向を設定する" on page 1500に記載されている指示に従い、以下のガイドラインを考慮してください。
   - [Agent/Applianceから開始] では、Amazon EC2インスタンスまたはAmazon WorkSpacesで受信ポートを開く必要はありません。ただし、[双方向] および [Managerから開始] では開く必要があります。
   - [Agent/Applianceから開始] は、Amazon EC2インスタンスまたはAmazon WorkSpaceで受信ポートを開く必要がないため、最も安全なオプションです。

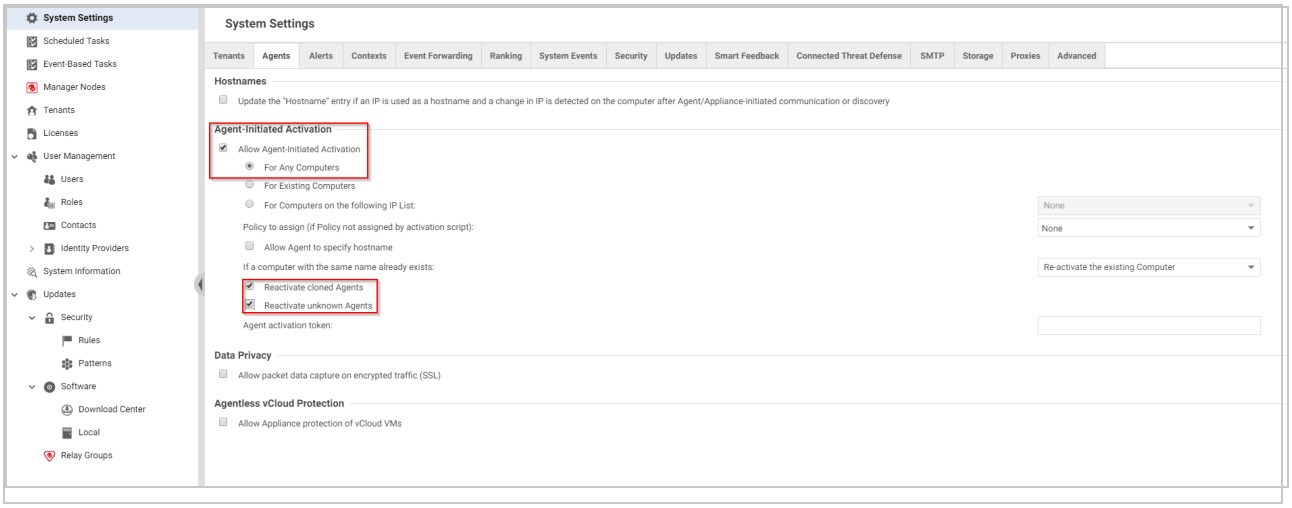
3. Amazon WorkSpacesを使用していて、通信方向を双方向またはマネージャー開始に設定する場合、さらなる構成を進める前に、各WorkSpaceにエラスティックIPアドレスを手動で割り当ててください。これにより、WorkSpaceにDeep Security Managerが接続できるパブリックIPが割り当てられます。EC2インスタンスには既にパブリックIPアドレスが使用されているため、これは必要ありません。WorkSpacesはプライベートIPアドレスを使用します。

有効化の種類を設定する

アクティベーションは、エージェントをマネージャに登録するプロセスです。エージェントによるアクティベーションを許可するかどうかを指定する必要があります。許可しない場合は、マネージャによるアクティベーションのみが許可されます。

1. Deep Security Managerにログインします。
2. 上部の[管理]をクリックします。
3. 左側で[システム設定]をクリックします。
4. エージェントタブが選択されていることを確認してください。
5. エージェントによるアクティベーションを許可を選択または選択解除し、次の点に留意してください:
   - Agentからのリモート有効化では、Amazon EC2インスタンスまたはAmazon WorkSpacesに対する受信ポートを開く必要はありません。ただし、Managerからのリモート有効化では開く必要があります。
   - Agentからのリモート有効化を有効にしても、Managerからのリモート有効化は引き続き機能します。
   - エージェントが開始したアクティベーションは、Managerが開始したに通信方向を設定しても機能します。
6. エージェントによるアクティベーションを許可を選択した場合は、クローンされたエージェントを再アクティベートおよび不明なエージェントの再アクティベートを有効化も選択してください。詳細については、"Agentの設定" on page 1524を参照してください。
7. [保存]をクリックします。
8. Amazon WorkSpacesを使用していて、エージェントによる起動を許可していない場合は、各WorkSpaceに弾性IPアドレスを手動で割り当ててください。これにより、各Amazon WorkSpaceに他のコンピュータから接続可能なパブリックIPが割り当てられます。EC2インスタンスについて

は、既にパブリックIPアドレスを使用しているため、これは必要ありません。



ポートを開く

Amazon EC2インスタンスまたはAmazon WorkSpacesに必要なポートが開いていることを確認する必要があります。

1. Amazon EC2に対するポートを次のように開きます。
   a. AWSマネジメントコンソールにログインします。
   b. [EC2]→[Network & Security]→[Security Groups] の順に選択します。
   c. EC2インスタンスに関連付けられたセキュリティグループを選択し、[Actions]→[Edit outbound rules] の順に選択します。
   d. 必要なポートを開いてください。詳細については、"開放するポート" belowを参照してください。
2. Amazon WorkSpacesに対するポートを次のように開きます。
   a. Amazon WorkSpacesを保護しているファイアウォールソフトウェアに移動し、ポートを開いてください。

これで、Deep Security AgentとDeep Security Managerが通信できるように必要なポートが開かれました。

開放するポート

通常:

- エージェントからマネージャへの通信には、アウトバウンドTCPポート(デフォルトでは443または80)を開く必要があります
- ManagerからAgentへの通信では、受信TCPポート(4118) を開く必要があります。

具体的には:

- 通信方向をエージェント/アプライアンス開始に設定する場合、アウトバウンドTCPポート443または80を開いてください。
- 通信方向をマネージャー開始に設定する場合、インバウンドTCPポート4118を開いてください。
- 通信方向を双方向に設定する場合、アウトバウンドTCPポート443または80、およびインバウンドTCPポート4118の両方を開いてください。
- エージェントによるアクティベーションを許可を有効にした場合、通信方向に関係なく、アウトバウンドTCPポート443または80を開いてください。
- エージェントによるアクティベーションを許可を無効にした場合、通信方向に関係なくインバウンドTCPポート4118を開いてください。

AgentをAmazon EC2インスタンスおよびWorkSpacesにインストールする

次のいずれかのオプションを使用して、Amazon EC2インスタンスおよびAmazon WorkSpacesにエージェントをデプロイする必要があります。

1. デプロイメントスクリプトを使用して、インストール、アクティベート、およびポリシーの割り当てを行います。

   これは、多くのAmazon EC2インスタンスおよびAmazon WorkSpacesにエージェントを展開する必要がある場合に最適なオプションです。

   このオプションでは、Amazon EC2インスタンスまたはAmazon WorkSpacesでインストールスクリプトを実行する必要があります。このスクリプトはAgentをインストールして有効化し、ポリシーを割り当てます。詳細については、"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849を参照してください。

2. 手動でインストールしてアクティベート。

   これは、少数のEC2インスタンスとAmazon WorkSpacesにエージェントをデプロイする必要がある場合に最適なオプションです。次の操作を行う必要があります:

   a. Deep Security Agentソフトウェアを入手し、Amazon EC2インスタンスまたはAmazon WorkSpaceにコピーしてインストールします。詳細については、"Deep Security Agentソフトウェアの入手" on page 514と"エージェントをインストールする" on page 536を参照してください。
   b. エージェントを有効化します。エージェント(エージェントによる有効化が有効になっている場合)またはDeep Security Managerで有効化できます。詳細については、"Agentの有効化" on page 559を参照してください。

Amazon EC2インスタンスまたはAmazon WorkSpaceにDeep Securityエージェントをインストールしてアクティベートしました。選択したオプションによっては、ポリシーが割り当てられている場合とそうでない場合があります。デプロイメントスクリプトを使用することを選択した場合、アクティベーション中にエージェントにポリシーが割り当てられました。エージェントを手動でインストールしてアクティベートすることを選択した場合、ポリシーは割り当てられていないため、ポリシーを割り当てる必要があります。

エージェントのインストールとアクティベーションを確認

エージェントが正しくインストールおよび有効化されていることを確認する必要があります。

1. Deep Security Managerにログインします。
2. 上部の [コンピュータ] をクリックします。
3. 左側で、Amazon EC2インスタンスまたはAmazon WorkSpaceがコンピュータ > *your_AWS_account* > *your_region*の下に表示されていることを確認します。WorkSpaces サブノード内の WorkSpacesを探します。
4. メイン画面で、Amazon EC2インスタンスまたはAmazon WorkSpacesの [ステータス] が [管理対象 (オンライン)] で、緑色のドットが横に表示されていることを確認します。

ポリシーを割り当てる

デプロイスクリプトを実行してエージェントをインストールおよびアクティベートした場合は、この手順をスキップしてください。スクリプトはすでにポリシーを割り当てているため、これ以上の操作は必要ありません。

Agentを手動でインストールして有効化した場合は、Agentにポリシーを割り当てる必要があります。ポリシーを割り当てると、コンピュータが保護されるように必要な保護モジュールがAgentに送信されます。

ポリシーを割り当てるには、"ポリシーをコンピュータに割り当てる" on page 722を参照してください。

ポリシーを割り当てると、Amazon EC2インスタンスまたはAmazon WorkSpaceが保護されます。

エージェントをAMIまたはWorkSpaceバンドルにインストールする

Agentが「統合」されている新しいAmazon EC2インスタンスとAmazon WorkSpacesを起動する場合は、このページを参照してください。

ただし、次の場合にはそれぞれの手順に従ってください。

- *既存の*Amazon EC2インスタンスおよびAmazon WorkSpaces(Deep Security) を保護する方法については、"Amazon EC2およびWorkSpacesへのAgentのインストール" on page 543にエージェントをインストールするを参照してください。
- Amazon EC2インスタンスを保護した後にAmazon WorkSpacesを保護する場合は、"Amazon WorkSpacesを保護する(AWSアカウントをすでに追加している場合)" on page 677を参照してください。

「Agentの統合」はパブリックAMIをベースにしてEC2インスタンスを起動するプロセスで、AgentをEC2インスタンスにインストールした後にこのカスタムEC2イメージをAMIとして保存します。このAMI (Agentが「統合」されている) を新しいAmazon EC2インスタンスの起動時に選択できます。

同様に、Deep Security Agentを複数のAmazon WorkSpacesに配信する場合は、エージェントを含むカスタムの「WorkSpaceバンドル」を作成できます。カスタムバンドルを新しいAmazon WorkSpacesの起動時に選択できます。

AMIを統合し、事前にインストールされ、有効化されたAgentを使用してカスタムWorkSpaceバンドルを作成するには、次の手順に従います。

1. "AWSアカウントをDeep Security Managerに追加する" below
2. "通信方向を設定する" on the next page
3. "有効化の種類を設定する" on the next page
4. "「マスター」Amazon EC2インスタンスまたはAmazon WorkSpaceを起動する" on the next page
5. "Agentをマスターにインストールする" on the next page
6. "Agentが適切にインストールされ有効化されたことを確認する" on page 551
7. "(推奨) 自動ポリシー割り当てを設定する" on page 551
8. "マスターに基づいてAMIまたはカスタムWorkSpaceバンドルを作成する" on page 552
9. "AMIを使用する" on page 553

AWSアカウントをDeep Security Managerに追加する

Deep Security ManagerにAWSアカウントを追加する必要があります。これらは、保護するAmazon EC2インスタンスおよびAmazon WorkSpacesを含むAWSアカウントです。

詳細については、"AWSアカウントの追加について" on page 664を参照してください。

通信方向を設定する

通信方向は、[Agent/Applianceから開始]、[Managerから開始]、または [双方向] のいずれかに設定する必要があります。

手順については、"Amazon EC2およびWorkSpacesへのAgentのインストール" on page 543の"通信方向を設定する" on page 544を参照してください。

有効化の種類を設定する

Agentからのリモート有効化を許可するかどうかを示す必要があります。

手順については、"Amazon EC2およびWorkSpacesへのAgentのインストール" on page 543の"有効化の種類を設定する" on page 545を参照してください。

「マスター」Amazon EC2インスタンスまたはAmazon WorkSpaceを起動する

「マスター」Amazon EC2インスタンスまたはAmazon WorkSpaceを起動する必要があります。マスターインスタンスは、これから作成するEC2 AMIまたはWorkSpaceバンドルの基になります。

1. AWSで、Amazon EC2インスタンスまたはAmazon WorkSpacesを起動します。詳細については Amazon EC2ドキュメントとAmazon WorkSpacesドキュメントを参照してください。
2. このインスタンスを「マスター」とします。

Agentをマスターにインストールする

マスターにAgentをインストールして有効にする必要があります。このプロセスでは、オプションでポリシーをインストールできます。

手順については、"Amazon EC2およびWorkSpacesへのAgentのインストール" on page 543の"AgentをAmazon EC2インスタンスおよびWorkSpacesにインストールする" on page 547を参照してください。

ヒント: AgentをAMIまたはWorkSpaceバンドルに統合し、後から新しいAgentを使用する場合は、バンドルをアップデートして新しいAgentを追加するのが理想的です。ただし、これが不可能な場合は、[Agentを有効化するときに自動的にアップグレードする] 設定を使用できます。その結果、AMIまたはバンドル内のAgentが自動的に有効化されたときに、Deep Security ManagerはそのAgentを自動的に最新バージョンにアップグレードできるようになります。詳細については、"Agentを有効化するときに自動的にアップグレードする" on page 1513を参照してください。

Agentが適切にインストールされ有効化されたことを確認する

続行する前に、マスターにAgentが適切にインストールされ、有効化されていることを確認する必要があります。

手順については、"Amazon EC2およびWorkSpacesへのAgentのインストール" on page 543の"エージェントのインストールとアクティベーションを確認" on page 548を参照してください。

(推奨) 自動ポリシー割り当てを設定する

マスターにAgentをどのようにインストールしたかによって、自動ポリシー割り当てを設定する必要があります。

- インストールスクリプトを使用した場合、ポリシーはすでに割り当てられており、追加の処理は必要ありません。
- Agentを手動でインストールして有効にした場合は、Agentにポリシーが割り当てられていないため、ポリシーを割り当ててマスターを保護する必要があります。マスターに基づいて起動されるAmazon EC2インスタンスおよびAmazon WorkSpacesも保護されます。

マスターにポリシーを割り当て、マスターを使用して今後EC2インスタンスまたはWorkSpaceにポリシーを自動割り当てする場合は、次の手順に従います。

1. Deep Security Managerで、次のパラメータを使用してイベントベースのタスクを作成します。
   - [イベント] を[Agentからのリモート有効化] に設定します。
   - [ポリシーの割り当て] を割り当てるポリシーに設定します。
   - (オプション) 条件を[クラウドインスタンスのメタデータ] に設定して、
     - [tagKey] を[EC2] に[tagValue.*]を[True]にします (EC2インスタンスの場合)。
       または
     - [tagKey]を[WorkSpaces] に、[tagValue.*]を[True] にします (WorkSpacesの場合)

     上記のイベントベースタスクは次のように設定されます。
     `EC2=true` または or `WorkSpaces=true`がAmazon EC2インスタンスまたはWorkSpaceに存在する場合は、Agentが有効化されると、指定されたポリシーを割り当てます。
     このキー/値ペアがAmazon EC2インスタンスまたはWorkSpaceに存在しない場合、ポリシーは割り当てられません (Agentの有効化は維持されます)。条件を設定しないと、有効化時に無条件でポリシーが割り当てられます。

イベントベースタスクの作成の詳細については、"クラウドプロバイダーのタグ/ラベルを使用してポリシーを自動的に割り当てる" on page 1861を参照してください。

2. 前の手順でDeep Security Managerでキーと値のペアを追加した場合は、次の手順を実行します。
   a. AWSにログインします。
   b. マスターEC2インスタンスまたはWorkSpaceを特定します。
   c. タグに [Key] は [EC2] または [WorkSpaces] を、[Value] は [True] を設定して、マスターに追加します。
   詳細については、タグ付けに関するAmazon EC2のドキュメントとタグ付けに関するAmazon WorkSpaceのドキュメントを参照してください。
   これで、自動ポリシー割り当てが設定されました。マスターを使用して起動した新しいAmazon EC2インスタンスおよびAmazon WorkSpaceは、自動的に有効化され (Agentはマスターで事前に有効化されるため)、イベントベースタスクでポリシーが自動的に割り当てられます。
3. マスターEC2インスタンスまたはWorkSpaceで、エージェントでアクティベーションコマンドを再実行するか、Deep Security Managerの再有効化の再アクティベートボタンをクリックして、エージェントを再度アクティベートします。詳細については、"Agentの有効化" on page 559を参照してください。
   再有効化を実行すると、イベントベースタスクがポリシーをマスターに割り当てます。これでマスターは保護されます。

AMIまたはカスタムWorkSpaceバンドルを作成する準備ができました。

マスターに基づいてAMIまたはカスタムWorkSpaceバンドルを作成する

注意: AWSからAMIを作成するときは、AWSオプションを選択しないでください。再起動しない。で作成されたイメージ再起動なしオプションは、エージェントによって保護されません。

- LinuxでAMIを作成する場合は、このAmazonドキュメントを参照してください。
- WindowsでAMIを作成する場合は、このAmazonドキュメントを参照してください。
- カスタムWorkSpaceバンドルを作成するには、このAmazonドキュメントを参照してください。

Agentが事前にインストールされ、有効化されたAMIまたはWorkSpaceバンドルが作成されました。

AMIを使用する

カスタムAMIまたはWorkSpaceバンドルを作成すると、今後のAmazon EC2インスタンスおよびAmazon WorkSpacesのベースとして使用できます。カスタムAMIまたはバンドルを使用すると、Deep Security Agentは自動的に起動し、自身をアクティベートして、割り当てられた保護ポリシーを適用します。Deep Security Managerのステータスが管理対象で、その横に緑色の点が表示されます。

Azure VMにエージェントをインストールする

Microsoft Azureクラウドで実行されているVMインスタンスにエージェントをインストールするには、Deep Security Agentをインストールする必要があります。これには複数の方法があります。

- RightScale、Chef、Puppet、SSHなどの配置ツールを使用して、エージェントを自動的に配置するためのDeep Security配置スクリプトを生成できます。詳しい手順については、"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849を参照してください。
- 既存の仮想マシンにカスタムスクリプト拡張を追加して、Deep Security Agentを配信および有効化できます。そのためには、Azure管理ポータルで既存の仮想マシンに移動し、次の手順に従ってインストールスクリプトをAzure仮想マシンにアップロードして実行します。

既存の仮想マシンにカスタムスクリプト拡張を追加するには

1. Azureポータルにログインします。
2. プレビューポータルに切り替えて、カスタムスクリプトを追加する仮想マシンをクリックします。
3. [Settings]ブレードで[Extensions]、[Extensions]ブレードで[Add extension]をクリックし、[New Resource]ブレードで[Custom Script]を選択して、[Create]をクリックします。
4. [Script File (required)]の[Add Extension]ブレードで、[upload]をクリックし、保存した.ps1インストールスクリプトを選択して、[OK]をクリックします。



Google Cloud Platform VMにエージェントをインストールする

Deep Securityで既存のGoogle Cloud Platform(GCP) VMインスタンスを保護する場合は、このページをお読みください。

既存のGCP VMを保護するには

1. Deep Security ManagerにGCPサービスアカウントを追加します。手順については、"Google Cloud Platformアカウントを追加する" on page 700を参照してください。
2. 通信方向をエージェント/ ApplianceInitiatedに設定します。手順については、"通信方向を設定する" on page 1500の設定を参照してください。
3. エージェント起動によるアクティベーションの設定(AIA).) 手順については、"Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511を使用したエージェントのアクティベートと保護。
4. Deep Securityコンポーネントが GCP VMおよびGCP APIにアクセスできるようにポートを開きます。開くポートの詳細については、"ポート番号、URL、およびIPアドレス" on page 428を参照してください。ポートを開く方法については、this GCP webpageを参照してください。
5. GCP VMにエージェントを配信するDeep Security Agent *12以降( )* を使用する必要があります。

   エージェントを配信するには、次の2つのオプションがあります。

オプション	使用する場合は...	命令
オプション1: 配信スクリプトを使用して、ポリシーをエージェントにインストール、アクティブ化、および割り当てます。	多くのクライアントをGCP VMに配信する必要があります。	手順については、"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849 の追加および保護を参照してください。
オプション2: エージェントを手動でインストールして有効にする	いくつかのエージェントを配置するだけで済みます。	a. Deep Security Agentソフトウェアを入手して、GCP VMにコピーしてから、インストールしてください。詳細については、"Deep Security Agentソフト

オプション	使用する場合は...	命令
		ウェアの入手" on page 514 b. Agentを有効化します。これは、エージェントまたはDeep Security Managerで実行できます。詳細については、"Agentの有効化" on page 559

6. エージェントが正しくインストールされ、アクティベートされていることを確認します。
   a. Deep Security Managerにログインします。
   b. 上部の [コンピュータ] をクリックします。
   c. 左側のナビゲーションペインで、Computers> *your_GCP_service_account*> *your_GCP_project* の下にGCP VMが表示されていることを確認します。
   d. メイン画面で、GCP VMがステータス(管理対象(オンライン)) と表示され、その横に緑色の点があることを確認します。
7. エージェントを手動でインストールして有効化した場合は、ポリシーを割り当てます。手順については、"ポリシーをコンピュータに割り当てる" on page 722に割り当てるを参照してください。ポリシーを割り当てると、コンピュータが保護されるように必要な保護モジュールがAgentに送信されます。

   注意: 配置スクリプトを実行してエージェントをインストールおよびアクティベートする場合は、ポリシーの割り当て手順をスキップしてください。スクリプトがポリシーをすでに割り当てているため、これ以上の処理は必要ありません。

   ポリシーを割り当てたら、GCP VMが保護されます。

VMware vCloudへのAgentのインストール

vCloudとの統合を可能にするには、テナントがvCloudの「クラウドアカウント」のインポートに使用するユーザアカウントに、最小限の権限セットを割り当てる必要があります。また、新しい仮想マシンに一意のUUIDを割り当てるようにvCenterデータベースを設定する必要があります。

注意: vCloud環境にDeep Securityセキュリティ保護をエージェントなしで配置するには、代わりに"vCloud環境にアプライアンスを配信する" on page 635でエージェントレス保護を配信するを参照してください。

vCloudアカウントのテナントユーザ向けの最小権限のロールを作成する

vCloud Directorで作成した、Deep Securityのテナントが Deep Security Managerにクラウドアカウントを追加するために使用するユーザアカウントには、の[すべての権限]→[一般]→[管理者ビュー権限]の権限のみが必要です。

1. vCloud Directorにログインします。
2. [System] タブで [Administration] をクリックします。
3. 左側のナビゲーションパネルで [Roles] をクリックします。
4. 「プラス」記号 (+) をクリックして新しいロール (「DS_User」など) を作成します。
5. [All Rights]→[General] フォルダの [Administrator View] 権限を選択します。
6. [OK] をクリックします。

これで、Deep Security ManagerにvCloudリソースをインポートするユーザアカウントにこの役割を割り当てることができます。

注意: Deep Securityのユーザにこの資格情報を提供する際は、vCloud OrganizationのIPアドレスも通知してください。また、vCloudのリソースをDeep Security Managerにインポートする際は、ユーザ名に「@orgName」を含めるように指示してください。たとえば、vCloudアカウントのユーザ名がuserで、アカウントのアクセス権を付与されたvCloud OrganizationがCloudOrgOneである場合、Deep Securityのユーザは、vCloudのリソースをインポートするときにユーザ名として「user@CloudOrgOne」と入力する必要があります。(vCloud管理者の場合、@systemを使用します)。

注意: クラウドアカウントで保護されているインスタンスへの接続にプロキシサーバを使用するよう、Deep Security Managerを設定できます。プロキシ設定は、[管理]→[システム設定]→[プロキシ]→[プロキシサーバの使用]→[Deep Security Manager (クラウドアカウント)] で行います。

新しい仮想マシンに一意のUUIDを割り当てる

Deep Securityでは、保護対象のすべての仮想マシンに一意のUUIDを割り当てる必要があります。vAppテンプレートから作成した仮想マシンにはUUIDを重複して割り当てることができるため、問題が発生する場合があります。固有のUUIDを割り当てるようにvCloudデータベースを設定するには、VMwareナレッジベースの記事2002506に従って、CloneBiosUuidOnVmCopyプロパティをゼロ(0)に設定します。

ゲスト仮想マシンでVMware Toolsの [OVF Environment Transport] を有効にする

ゲスト仮想マシンでVMware Toolsの [OVF Environment Transport] を有効にすると、guestInfo.ovfEnv環境変数がDeep Security Managerに公開され、Agentで仮想マシンを一意に識別することが容易になります。これにより、仮想マシンの誤認リスクが低減されます。

1. vCloud Directorで仮想マシンの [Properties] 画面を開き、[Guest OS Customization] タブに進んで [Enable guest customization] チェックボックスをオンにします。[OK] をクリックします。
2. vCenterで同じ仮想マシンを選択し、[Properties] 画面を開いて [Options] タブに進みます。
3. [vApp Options] をクリックし、[Enabled] オプションを選択します。これで [OVF Settings] が公開されます。
4. [OVF Settings] で、[OVF Environment Transport] エリアの [VMware Tools] チェックボックスをオンにします。[OK] をクリックします。

仮想マシンが実行中の場合は、変更を有効にするために再起動する必要があります。

Deep Securityで使用されるデータは、プロパティvmware.guestinfo.ovfenv.vcenteridおよびvmware.guestinfo.ovfenv.vcloud.computernameから取得されます。

VMware vCloud Organizationアカウントからのコンピュータのインポート

注意: vCloud組織アカウントはテナント別に追加する必要があります(プライマリテナントではない).

1. Deep Security Managerで、[コンピュータ] セクションに移動し、ナビゲーションパネルで [コンピュータ] を右クリックし、[vCloudアカウントの追加] を選択してvCloudアカウント追加ウィザードを開きます。
2. 追加するリソースの名前と説明を入力します(Deep Security Managerでの表示に使用されます)。
3. vCloudのアドレスを入力します(vCloud Directorホストコンピュータのホスト名です)。

4. ユーザ名とパスワードを入力します。

   注意: ユーザ名は、username@vcloudorganizationの形式にします。

5. [次へ] をクリックします。
6. Deep Security Managerによってクラウドリソースへの接続が確認され、インポート処理の概要が表示されます。[完了] をクリックします。

VMware vCloudのリソースが、Deep Security Managerのナビゲーションパネル内の [コンピュータ] の下に、それぞれ別個の項目として表示されます。

クラウドプロバイダのリソースを追加したら、コンピュータにAgentをインストールして有効化し、ポリシーを割り当てる必要があります ("エージェントをインストールする" on page 536または"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849と"Agentの有効化" on the next pageを参照してください)。

VMware vCloud Air仮想データセンターからコンピュータをインポートする

1. Deep Security Managerで、[コンピュータ] セクションに移動し、ナビゲーションパネルで [コンピュータ] を右クリックし、[vCloudアカウントの追加] を選択してvCloudアカウント追加ウィザードを開きます。
2. 追加するVMware vCloud Air仮想データセンターの名前と説明を入力します(Deep Security Managerでの表示に使用されます)。
3. VMware vCloud Air仮想データセンターのアドレスを入力します。

   注意: VMware vCloud Air仮想データセンターのアドレスを確認するには、次の手順を実行します。

   a. VMware vCloud Airポータルにログインします。
   b. [Dashboard] タブで、Deep Securityにインポートするデータセンターをクリックします。[Virtual Data Center Details] 情報画面が表示されます。
   c. [Virtual Data Center Details] 画面の [Related Links] セクションで、[vCloud Director API URL] をクリックします。vCloud Director APIの完全なURLが表示されます。
   d. Deep Securityにインポートする VMware vCloud Air仮想データセンターのアドレスとして、完全なURLのうちホスト名の部分だけを使用します。

4. ユーザ名とパスワードを入力します。

   注意: ユーザ名は、username@virtualdatacenteridの形式にします。

5. [次へ] をクリックします。
6. Deep Security Managerによって仮想データセンターへの接続が確認され、インポート処理の概要が表示されます。[完了] をクリックします。

VMware vCloud Airのデータセンターが、Deep Security Managerのナビゲーションパネル内の[コンピュータ]の下に、それぞれ別個の項目として表示されます。

クラウドプロバイダのリソースを追加したら、コンピュータにAgentをインストールして有効化し、ポリシーを割り当てる必要があります("エージェントをインストールする" on page 536または"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849と"Agentの有効化" belowを参照してください)。

Agentの有効化

ヒント: Agentをまだインストールしていない場合は、"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849または"エージェントをインストールする" on page 536を参照してAgentをインストールしてください。

インストールされているエージェントがコンピュータを保護したり、リレーに変換したりする前に、Deep Security Managerを使用してエージェントをアクティベートする必要があります。有効化により、最初の通信時にManagerにAgentが登録されます。

そのためには、次のいずれかの方法があります。

- ManagerからAgentを有効化します。[コンピュータ]に移動し、AgentまたはApplianceを有効化または再有効化するコンピュータを右クリックして、[処理]→[有効化/再有効化]の順に選択します(または、コンピュータの[詳細]画面で[有効化]または[再有効化]をクリックします)。
- インストールスクリプトを使用してAgentを有効化します。詳細については、"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849を参照してください。
- Agentがインストールされているコンピュータからを有効化します。次のコマンドを実行します。
  `dsa_control -a dsm://<dsm_host_or_IP>:<port>/`
  ここで、
  `<dsm_host_or_IP>`はDeep Security Managerのホスト名またはIPアドレスに置き換えられ、
  `<port>`はDeep Security Managerのハートビートポート(初期設定では4120)に置き換えられます。
  その他のパラメータなど、このコマンドの詳細については、"コマンドラインの基本" on page 1793を参照してください。
- イベントベースタスク(「コンピュータの作成(システムによる)」イベント)を使用してAgentを有効化して、コンピュータがManagerに接続したとき、またはManagerがLDAPディレクトリ、クラウドアカウント、vCenterと同期したときに自動的にコンピュータを有効化します。詳細については、"コンピュータの追加または変更時にタスクを自動的に実行する(イベントベースのタスク)" on page 1829を参照してください。

有効化の前は、AgentまたはApplianceは次のいずれかのステータスになっています。

- Agent/Applianceなし: 次のいずれかの状況を示しています。
  - 初期設定のポートでAgentまたはApplianceが実行されていないか、待機中ではありません。
  - AgentまたはApplianceはインストールされ実行中ですが、別のManagerと連携しており、通信がAgent/Applianceから開始されるように設定されています。この場合、Agentまたは Applianceは このManagerを待機していません。この問題を解決するには、コンピュータから Agentを無効化します。
- 有効化が必要: AgentまたはApplianceはインストールされ待機中で、Managerによる有効化の準備ができています。
- 再有効化が必要: AgentまたはApplianceはインストールされ待機中で、Managerによる再有効化を待機しています。
- 無効化が必要: AgentまたはApplianceはインストールされ待機中ですが、別のManagerによってすでに有効化されています。
- 不明: 状態情報のないコンピュータが、インポート済みのコンピュータリストの一部としてインポートされました。または、LDAPディレクトリ検出プロセスによって、コンピュータが追加されました。

有効化が正常に実行されると、AgentまたはApplianceの状態はオンラインになります。有効化に失敗すると、コンピュータは有効化の失敗ステータスになり、カッコ内に失敗の理由が表示されます。このリンクをクリックすると、有効化の失敗理由の詳細を示すシステムイベントが表示されます。

注意: IPv6トラフィックは、Deep Security 8.0以前のAgentとApplianceでサポートされていますが、初期設定ではブロックされています。Deep Security 8.0のAgentとApplianceでIPv6トラフィックを許可するには、**コンピュータエディタまたは ポリシーエディタ**[1]を開いて、[設定]→[詳細]→[ネットワークエンジンの詳細設定] の順に移動します。[バージョン8以降のAgentとApplianceでIPv6をブロック] オプションを[いいえ] に設定します。

Agentを無効化する

コンピュータのコントロールをあるDeep Security Managerインストールから別のDeep Security Managerインストールに転送する場合は、エージェントまたはアプライアンスを現在のマネージャで無効にしてから、新しいマネージャで再度有効化する必要があります。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(または ポリシーを選択して[詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(または コンピュータを選択して[詳細] をクリック) します。

エージェントまたはアプライアンスは、通常、エージェントまたはアプライアンスを管理しているDeep Security Managerから非アクティブ化できます。Deep Security Managerがエージェントまたはアプライアンスと通信できない場合は、手動で非アクティブ化を実行する必要があります。以下のコマンドを実行するには、ローカルのコンピュータに対する管理者権限が必要です。

WindowsでAgentを無効にするには

1. コマンドラインから、Agentのディレクトリ(初期設定ではC:\Program Files\Trend Micro\Deep Security Agent)に移動します。
2. 次のコマンドを実行します。dsa_control -r

LinuxでAgentを無効にするには

1. 次のコマンドを実行します。/opt/ds_agent/dsa_control -r

エージェントの起動または停止

WindowsでAgentを起動または停止するには

- 開始：`sc start ds_agent`
- 停止：`sc stop ds_agent`

LinuxでAgentを起動または停止するには

SysV initスクリプトの使用：

- 開始：`/etc/init.d/ds_agent start`
- 停止：`/etc/init.d/ds_agent stop`

systemdコマンドの使用：

- 開始：`systemctl start ds_agent`
- 停止：`systemctl stop ds_agent`

Deep Security Virtual Applianceに組み込まれているエージェントを開始または停止するには、「"アプライアンスを起動または停止する" on page 653。

エージェントのインストールまたはアップデート時の一般的な問題

ここでは、Agentのインストール時またはアップデート時に発生する可能性のある3つの一般的な問題について説明します。

一般な役立つリンク

https://help.deepsecurity.trendmicro.com/aws/ja-jp/welcome.html

https://success.trendmicro.com/dcx/s/product?language=ja&product=deep-security

1. 不正プログラム対策エンジンがオフライン(Windows)

通常、この問題は、不正プログラム対策モジュールが適切にインストールされていないか、ドライバ/サービスが実行されていないWindowsコンピュータで発生します。Agent側で、タスクバーのDeep Security Notifierアプリに「ドライバがオフライン/インストールされていません」というステータスが表示されます。このエラーを報告しているサーバにMicrosoftのアップデートからルート証明書の初期アップデートがインストールされていない場合は、サーバにパッチを適用し、Agentをアンインストールしてサーバを再起動し、Agentを再インストール/再有効化する必要があります。

ほとんどの場合、この問題はAgentをアンインストール、再起動、および再インストール/再有効化することで解決されます。

WindowsコンピュータからDeep Security Agentをクリーンナップする手順については、Deep Security Agentを手動でアンインストールする手順を含む、以下の3番目の記事を参照してください。Agentを手動でアンインストールする必要は必ずしもありませんが、通常のアンインストールと再起動が完了した後は、ファイルの場所、レジストリエントリ、およびクリーンナップするサービスが指示に含まれています。

役立つリンク:

Deep Security および Trend Cloud One - Endpoint & Workload Security で VeriSign、DigiCert、USERTrust RSA 証明書を更新中

エラー: アンチマルウェアエンジンがオフラインです

Trend Micro Deep Security の手動アンインストール手順

2. セキュリティアップデートに失敗した場合

Deep Security Agentが環境内の指定されたDeep Security Relay と通信できない場合、サーバは最新の不正プログラム対策パターンを実行しないリスクがあるため、優先度の高い問題である可能性があります。

セキュリティアップデートの失敗をトラブルシューティングする場合、最も一般的な原因は、Deep Security AgentとDeep Security Relay間のネットワーク接続にあります。以下のリンク先の記事では、2つのコンポーネント間で接続を確認し、TCP通信が機能していることを確認するための手順をいくつか紹介しています。

PowershellのTest-NetConnectionやLinuxサーバのtelnet / curlなどのユーティリティを使用すると、AgentとManager間のTCP通信が開いていることを確認できます。TCP接続が開いている場合、SSLインスペクションを実行している2つのデバイスの間にデバイスが存在するか、2つのポイント間の暗号化された接続に干渉している可能性があります。

通常、Agentのds_agent.logファイルにはセキュリティアップデートを実行できない理由が記載されており、行の先頭に「エラー」または「警告」と表示されます。アップデート試行時間とログファイル内の時間を関連付けて、アップデートが失敗した根本原因を特定します。

ログファイルの場所:

- Windows - `C:\ProgramData\Trend Micro\Deep Security Agent\diag`
- Linux- `/var/opt/ds_agent/diag`

役立つリンク:

https://help.deepsecurity.trendmicro.com/aws/ja-jp/security-update-connectivity.html

https://www.trendmicro.com/ja_jp/business/products/downloads.html

3. Deep Security Agentのインストール後に発生するパフォーマンス/アプリケーションの問題(不正プログラム対策およびモジュール分離)

Deep Security Agentを配信する前に、適切なセキュリティ設定をサーバに適用する必要があります。これは、不正プログラム対策/Securityソフトウェアでは一般的であり、インストールされたサーバやアプリケーションが活動のレビューの増加によって悪影響を受けないようにします。

このセクションではDeep Securityコンソールのステータスについては直接説明していませんが、新しいサーバにDeep Security Agentを配信した後にトラブルシューティングが必要になる、最も一般的な設定の調整の1つです。サーバのパフォーマンスが影響を受けたり、アプリケーションの機能が影響を受けたりした場合は、まず、問題を引き起こしている可能性のあるDeep Securityモジュールを特定する必要があります。

最初に、サーバ上のどのプロセスが他のプロセスよりも多くのCPU / RAMを使用しているかによって、パフォーマンスの問題を特定できます。Windowsコンピュータには、通常、原因となる2つのサービスがあります。dsa.exeまたはcoreServiceShell.exeです。dsa.exeはコンピュータで実行されるAgentプロセスのコアで、coreServiceShell.exeは不正プログラム対策モジュールの一部です。Linuxサーバでは、これらのプロセスの名前はそれぞれds_agentとds_amです。

どのプロセスがリソースを消費しているかに関係なく、リソースの使用率の増加に関与している保護モジュールを絞り込みます。Deep Security Managerコンソールから個々のモジュールを1つずつオフにす

ることで、リソース使用率の低下を監視できます。その場合、その動作は最新の無効なモジュールによるものと考えられます。

CoreServiceShell.exeまたはds_amプロセスが大量のCPUを使用している場合、これは通常、リアルタイム不正プログラム対策エンジンがサーバ上で大量の読み取り/書き込みトランザクションを検索しており、ジョブを完了するためにより多くのリソースを必要とすることを示しています。

この大量のアクティビティは、安全であることがわかっているデータ/アプリケーションの除外を追加することで削減できます。リソース使用率を削減する最も一般的な方法は、不正プログラム対策モジュールに起因する他のアプリケーションの問題を解決することです。これは、サーバで実行されている安全なアプリケーションを特定し、プロセスイメージ除外を実装することです。プロセスイメージの除外は、Microsoft SQL Serverの場合はsqlsvr.exeなど、安全であることがわかっている、サーバ上で実行されているプロセスのフルパスへのポインタです。このプロセスを除外すると、sqlsvr.exeプロセスによってアクセスされたファイルはリアルタイムエンジンによって検索されなくなります。これらの調整を行うには、Deep Security Managerでコンピュータ/ポリシーの検索設定を編集し、除外する適切なプロセスを含める必要があります。

不正プログラム対策モジュールによって影響を受けるアプリケーションでは、除外を適用した後に、サーバから追加情報を収集するなど、追加のトラブルシューティングが必要になる場合があります。不正プログラム対策関連のアプリケーションの問題が発生したサーバでは、C:\Program Files\Trend Micro\AMSP\AmspConfig.iniファイルを編集することで、追加のデバッグログを有効にできます。DebugLevel = 0の行をDebugLevel = 1または2に変更します(2は詳細情報をログに記録します)。Trend Micro Deep Security Agentおよびソリューションプラットフォームサービスを再起動して、変更を有効にします。これらのログオプションを元に戻すには、DebugLevelを0に戻して、同じサービスの再起動を実行します。

Linuxサーバで、ds_amプロセスのPIDを特定します:

```
$ ps aux | grep ds_am
```

デバッグレベルを上げます(コマンドを複数回実行してレベルを1つ上げる):

```
kill -USR1 $(PID_for_ds_am)
```

デバッグレベルを下げるには(コマンドを複数回実行してレベルを1つ下げる):

```
kill -USR2 $(PID_for_ds_am)
```

問題を再現し、コマンドライン(リンク)から診断パッケージを収集します。これには、調整されたログレベルの追加情報が含まれます(注意:Deep Security Managerから診断パッケージを収集すると、コマンドラインで収集されなかった追加情報が含まれます)。この診断パッケージをサポートチームに提供して、潜在的な問題の確認と特定に役立てることができます。

役立つリンク:

https://help.deepsecurity.trendmicro.com/aws/ja-jp/high-cpu-usage.html

Deep Security Virtual Applianceを配信する

VMware環境の保護

Deep Security Virtual Applianceは、2027年8月2日をもって製品サポートサービスを終了いたします。

Trend Micro Deep SecurityはVMwareと緊密に連携し、Agentレスによるセキュリティをハイパーバイザレベルで提供します。このセキュリティを提供するのがDeep Security Virtual Applianceです。Applianceは、NSX Managerを使用してクラスタレベルで配置され、同じESXiホスト上の仮想マシンを保護します。

このページのトピック:

- "Deep Security Virtual Applianceの機能" below
- "Virtual ApplianceおよびNSXを使用するVMware環境" on the next page
- "エージェントのみを使用したVMwareの配置" on page 569
- "追加情報" on page 569

Deep Security Virtual Applianceの機能

検索キャッシュ

検索キャッシュを使用すると、複数のコンピュータを同じファイルで検索する場合に、不正プログラム検索の結果を使用できます。元のゲスト仮想マシンを検索する際、Applianceは検索対象ファイルの属性を追跡します。他の仮想マシンを検索する際には、各ファイルの追跡した属性を比較します。属性が同じ後続のファイルを再び完全に検索する必要がないため、全体的な検索時間が短縮されます。ほぼ同じイメージの仮想デスクトップインフラストラクチャ(VDI)などでは、検索キャッシュを使用することでパフォーマンスに与える影響を大幅に削減できます。

検索ストームの最適化

同時に多数の検索が実行されると、「検索ストーム」が発生し、パフォーマンスが低下します。通常、検索ストームは、大規模なVDI環境で発生します。不正プログラム検索を実行する場合、ウイルス検

索アプライアンスは検索キャッシュの機能を使用して、検索の嵐の最中にリソースの使用状況を最適化できます。

管理の簡素化

一般に、Deep Security Virtual Applianceを各ESXiホストに1つずつ配置することは、複数のVMにDeep Security Agentを配置するより簡単です。NSXを使用している場合は、新しいESXiホストがクラスタに追加されると、NSX Managerによって自動的にDeep Securityサービスが配信されるため、さらに管理の手間を節約できます。

また、Virtual Applianceを使用するとネットワークの柔軟性も向上します。Deep Security Agentは、それぞれがネットワークに接続してDeep Security ManagerとRelayを解決する必要があります。Deep Security Virtual Applianceを使用した場合、このネットワーク接続が必要なのはVirtual Applianceのみで、各仮想マシンへの接続は必要ありません。

インフラストラクチャと仮想マシンが別々のチームによって管理される場合があります。Virtual Applianceを使用すると、ハイパーバイザレベルで保護を実施して各仮想マシンを保護できるため、インフラストラクチャチームは保護を追加するために仮想マシンにアクセスする必要がありません。

Virtual ApplianceおよびNSXを使用するVMware環境

Deep Security Virtual Applianceを使用してゲスト仮想マシンを保護する場合は、VMware NSX Data Center for vSphere (NSX-V) またはNSX-T Data Centerを使用する必要があります。NSX-VおよびNSX-Tのライセンスには、いくつかのタイプがあります。これらのライセンスの種類は、それぞれがサポートするDeep Securityの機能とともに、次の表に示されています。

注意: Deep Security Virtual Applianceでサポートされるサポート対象の機能とサブ機能の詳細については、"各プラットフォームでサポートされている機能" on page 417を参照してください。

	Deep Security Virtual Appliance環境							
	NSX for vSphere(NSX-V) 6.4.x			NSX for vSphere(NSX-V) 6.4.x and NSX-T 3.x				
	標準 または NSX for vShield Endpoint (無料)	詳細	**Enterprise**	NSX Data Center Standard または NSX for vShield Endpoint (無料)	**NSX Data Center Professional**	**NSX Data Center Advanced**	**NSX Data Center Enterprise Plus**	**NSX Data Center for Remote Office Branch Office**
不正プログラム対策	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1
変更監視とアプリケーションコントロール	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1	✓ 1
ファイアウォール	X	✓	✓	X	X	✓	✓	✓
侵入防御	X	✓	✓	X	X	✓	✓	✓
Webレピュテーション	X	✓	✓	X	X	✓	✓	✓
セキュリティログ監視	X	X	X	X	X	X	X	X

	Deep Security Virtual Appliance環境							
	NSX for vSphere(NSX-V) 6.4.x			NSX for vSphere(NSX-V) 6.4.x and NSX-T 3.x				
	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard または NSX for vShield Endpoint (無料)	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office
アプリケーションコントロール	X	X	X	X	X	X	X	X

[1] Windowsゲスト仮想マシンでのみ使用可

機能がアプライアンスでサポートされていない場合(Xの), それは、エージェントを通じて調達することができます。Virtual Applianceの機能を補うためにAgentをインストールすることを、コンバインモードと呼びます。

コンバインモードを検討する場合、以下が主要なポイントとなります。

- 管理: Deep Securityには、さまざまなオーケストレーションツール (Chef、Puppetなど) を使用してDeep Security Agentのインストールをスクリプト化できる、インストールスクリプトが用意されています。インストールスクリプトを使用するとAgentを簡単にインストールでき、Agentの有効化およびポリシーの割り当ても可能です。インストールスクリプトを使用することで、VMware環境にAgentをインストールする際の手動操作や管理コストを減らすことができます。
- "検索キャッシュ" on page 565 のパフォーマンス改善と"検索ストームの最適化" on page 565: 複合モードでは、仮想アプライアンスは検索キャッシュ機能とウイルス検索の嵐の最適化を実行します。これにより、インストールが必要なのはネットワークドライバのみとなるため、各仮想マシンでAgentが占有するスペースを抑えることができます。

Deep Security Virtual Appliance環境を設定する方法の詳細については、"アプライアンスを配信する(NSX-T 3.x)" on page 576か、"Applianceのインストール (NSX-V)" on page 611

エージェントのみを使用したVMwareの配置

仮想アプライアンスまたはNSXなしでVMware環境を保護するには、Deep Security Agentを各VMに配信する必要があります。このシナリオでは、Agentがすべての保護を提供するため、Deep Security Virtual Applianceは必要ありません。Deep Security Agentを使用することで、Deep Securityの主な機能をすべて利用できます。つまり、不正プログラム対策, 変更監視, ファイアウォール, 侵入防御, Webレピュテーション, セキュリティログ監視とアプリケーションコントロールの3つの機能を使用できます。加えて、Agentには次の特性があります。

- 軽量 (Smart Agent)。指定した保護モジュール(不正プログラム対策および変更監視など)のみが、マネージャで設定したポリシーに従ってインストールされます。さらに、Deep Securityには「推奨設定の検索」と呼ばれる機能があり、これを使用すると、保護している特定のワークロードに必要なルールだけを割り当てることができます。
- Windowsクライアントには不正プログラム対策検索キャッシュが含まれており、頻繁にアクセスされる以前に検索されたファイルのハッシュが格納されているため、再スキャンする必要はありません。

Agentをインストールするため、トレンドマイクロではさまざまなオーケストレーションツール (Chef、Puppetなど) で使用できるインストールスクリプトを提供しています。手動でAgentをインストールすることもできます。

追加情報

- Deep Security Webサイト:https://www.trendmicro.com/ja_jp/business/products/hybrid-cloud/deep-security-data-center.html

Agentレスによる保護またはコンバインモードの保護の選択

仮想マシン(VM)を保護する場合は、他の種類のコンピュータと同様にDeep Security Agentをインストールできます。Deep Security 9.6以降では、VMを保護する2つの方法があります。

- Agentレスによる保護 (Virtual Applianceを使用)
- AgentベースとAgentレスを組み合わせて保護 (コンバインモード)

Agentレスによる保護

不正プログラム対策ツール変更監視Deep Security Agentをインストールせずに保護を提供できます。VMにインストールされたVMware Toolsドライバは、セキュリティ処理をDeep Security Virtual Applianceにオフロードできます。

注意: Linux仮想マシンでは、Deep Security Virtual Applianceではなく、Deep Security Agentが不正プログラム対策保護を実行します。

注意: Deep Security 9.5以前では、Deep Security Agentをインストールせずにを保護するために、Deep Security Virtual Applianceおよびフィルタドライバを使用します。従来、Filter Driverは ESXiサーバにインストールされ、ハイパーバイザでネットワークトラフィックをインターセプトして Applianceに送信するために使用されていました。VMwareはvShield(VMsafe-NET APIドライバ) をサポートしていないため、古いドライバはDeep Security 20ではサポートされていないため、削除する必要があります。

Agentレスによる保護ではApplianceと保護するコンピュータとの間の高速接続が必要なため、コンピュータとApplianceの距離が離れている(リモートESXiサーバまたは別のデータセンターにある) 場合はAgentレスを使用しないでください。

"vCloud環境にアプライアンスを配信する" on page 635も参照してください。

コンバインモード

Deep Security Virtual Applianceでサポートされていないその他の保護機能が必要な場合は、各VMにDeep Security Agentをインストールする必要がありますが、Deep Security Virtual Applianceを使用して保護機能を提供してパフォーマンスを向上させることもできます。。ApplianceとAgentの両方を使用する方法は「コンバインモード」と呼ばれます。

コンバインモードでは、Applianceが不正プログラム対策と変更監視を提供し、Deep Security Agentがその他の機能を提供します。

協調的保護からコンバインモードへの変換

- 協調的保護: Deep Security 9.5では、仮想マシン上のAgentがオフラインの場合、代わりにDeep Security Virtual Applianceから保護機能が提供されます。ただし、各機能についてどちらを使用するかを個別に設定することはできません。

- コンバインモード: Deep Security 9.6 では、それぞれの保護機能について、Agentまたは Applianceのどちらを使用するかを個別に設定できます。ただし、優先する保護ソースがオフラインの場合、もう一方の保護ソースが代わりに使用されることはありません。

Deep Security 10.0以降では、「保護ソース」の設定により、*両方の*動作が提供されます。

- 各機能をAgentとApplianceのどちらから提供するか
- 優先する保護 (AgentまたはAppliance) を利用できない場合にもう一方を代わりに使用するかどうか

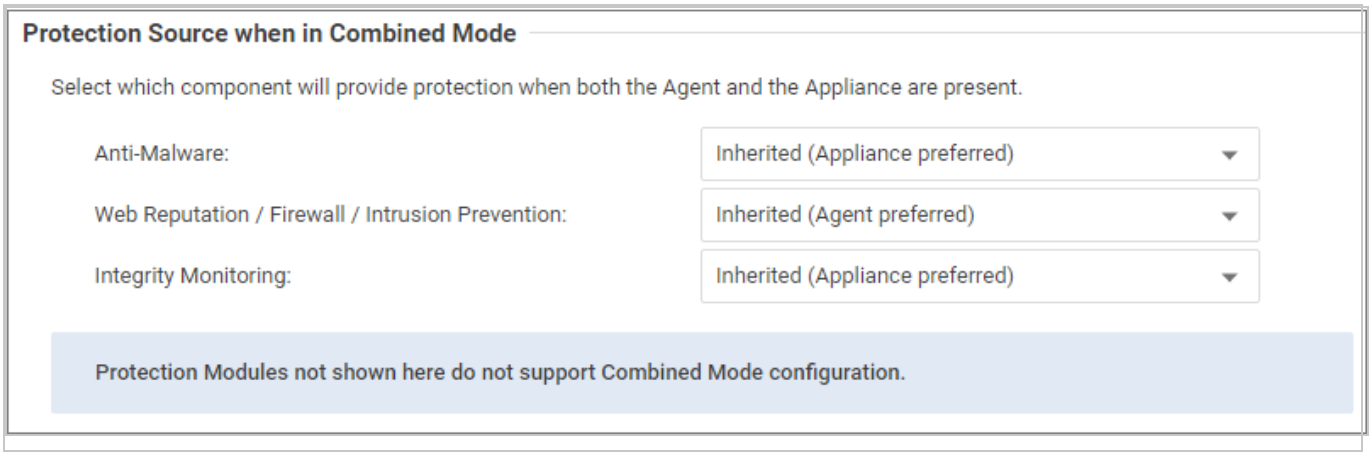
したがって、以前の調整アプローチのような動作が必要な場合は、Deep Security 9.6へのアップグレードを避け、Deep Security 9.5からDeep Security 10.0に、次にDeep Security 9.1にアップグレードしてから12にアップグレードすることをお勧めします。

保護機能ごとにクライアントまたはアプライアンスを選択する

コンピュータをApplianceまたはAgentで保護できる場合は、各保護機能をどちらが提供するかを選択できます。

注意: セキュリティログ監視とアプリケーションコントロールには、この設定はありません。現在のVMwareの統合テクノロジでは、Deep Security Virtual Applianceではこれらの機能を提供できません。

保護ソースを設定するには、VMware vCenterをDeep Security Managerにインポートしてから、**コンピュータエディタまたはポリシーエディタ**[1]で、[設定]→[一般] の順に移動します。



[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

各保護モジュールまたはモジュールグループに対して、次のいずれかを選択します。

- Applianceのみ: 仮想マシンにAgentがあり、Deep Security Virtual Applianceが無効化または削除されている場合でも、Applianceからのみ保護を提供します。

  警告: Scanner (SAP) が必要な場合、Applianceは使用しないでください。Deep Security Agentの不正プログラム対策が必要です。

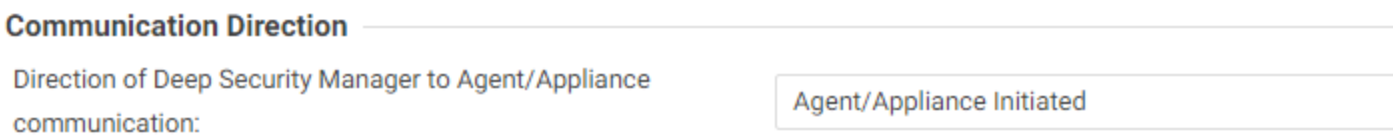
  ヒント: Agentで不正プログラム対策が有効になっている場合、Anti-malware Solution Platform (AMSP) がダウンロードされてサービスとして起動されます。このサービスが不要な場合は、[不正プログラム対策] で [Applianceのみ] を選択してください。これにより、Applianceが無効化されている場合でも、AMSPサービスが起動されることはありません。

- Appliance優先: ESXiサーバに有効化されたApplianceがある場合は、そのApplianceが保護を提供します。ただし、Applianceが無効化または削除された場合は、Agentが代わりに保護を提供します。
- Agentのみ: 有効化されたApplianceがある場合でも、Agentからのみ保護を提供します。
- Agent優先: 仮想マシンに有効化されたAgentがある場合は、そのAgentが保護を提供します。しかし、有効化されたAgentがない場合は、Applianceが代わりに保護を提供します。

vCloud Director環境で、エージェント起動の有効化を使用して複合モードを有効にする

vCloud Directorの仮想マシンのホスト名がDeep Security Managerから解決できない場合は、エージェント起動のアクティベーションを使用して複合モードを有効にしてください。vCloud Directorの仮想マシンで複合モードを有効にするには

1. コンピュータに移動し、対象のvCloud Directorコンピュータを右クリックして、[アクティベーション]を選択します。
2. 対象のvCloud Directorコンピュータをダブルクリックし、ポップアップウィンドウで[設定>全般]を選択します。コミュニケーションの方向をAgent/Appliance 開始に変更します。



3. 対象のvCloud DirectorコンピュータにDeep Security Agentをインストールし、エージェントを有効にします。

アプライアンスを配信する前に

Deep Security Virtual Applianceを配信する前に、次のタスクを完了してください。

注意: アプライアンスをアップグレードする場合は、代わりに"Deep Security Virtual Applianceのバージョンアップ" on page 1684を参照してください。

システム要件を確認する

- この表で、サポートされているNSXのライセンスとバージョンを確認します。
- システム要件を確認します。

NSX、Deep Security Managerなどのコンポーネントのインストールまたはバージョンアップ

システム要件を確認したら、次の手順を実行します。

- NSXをインストールまたはバージョンアップして、必要な機能をサポートするライセンスを使用していることを確認してください。
- Deep Security Managerをインストールまたはアップグレードします。
- その他の必要なソフトウェアとハードウェアをインストールまたはアップグレードします。

NSX-Tの再登録

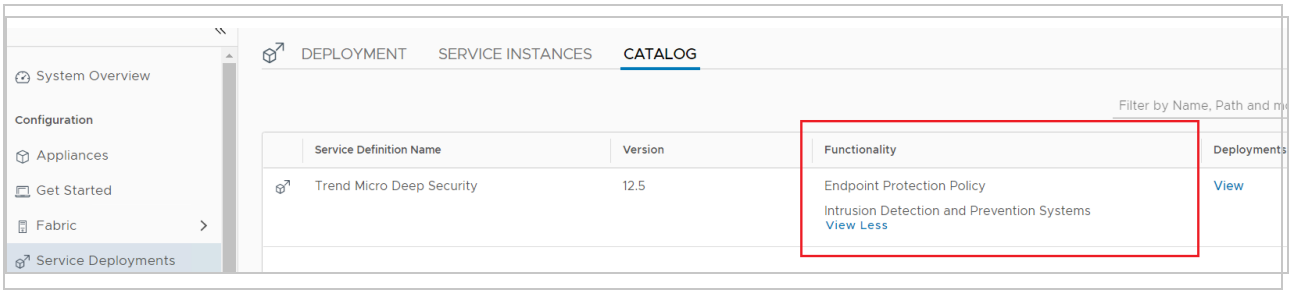
以前にDeep Security Managerに"VMware vCenterの追加" on page 704の手順を使用してNSX-Tを追加した場合は、このセクションを参照してください。

NSX-Tを再登録する必要がある場合があります。

NSX-Tを再登録する必要があるかどうかを確認するには

1. NSX-T Managerに移動し、システム>サービス配信>CATALOGをクリックします。
2. エンドポイント保護ポリシーと侵入検知および予防システムの両方が存在することを確認してく

ださい(下の図を参照) 。そうでない場合、再登録が必要であることを意味します。



NSX-Tを再登録するには

1. Deep SecurityをNSX環境からアンインストールします。詳細については、"NSX環境からのDeep Securityのアンインストール" on page 1731を参照してください。
2. マネージャーにNSXを再登録してください。"VMware vCenterの追加" on page 704を参照してください。

通信を設定する

- 適切なポート番号で、アプライアンスとの送受信を許可します。"Deep Securityのポート番号" on page 429を参照してください。
- 仮想アプライアンス(VMwareの用語で「サービスVM」とも呼ばれる) が、管理ネットワークレベルでパートナーService Manager(コンソール) と通信できることを確認します。詳細については、このEast-West Traffic Introspection のサービス配信または NSX-Vヘルプページを参照してください。

(オプション) Deep Security Agentのインストール

- 必要な機能がエージェントレスで使用できない場合は、VMにエージェントをインストールし、仮想アプライアンスとエージェントで保護の義務が共有されるように「複合モード」を使用してください。
- ゲスト仮想マシンがネットワークカードに直接アクセスできるように設定した場合は、それらの仮想マシンにAgentをインストールしてください。この場合は、パケットをインターセプトすることができないため、ゲスト内にAgentをインストールすることをお勧めします。詳細については、"Agentレスによる保護またはコンバインモードの保護の選択" on page 569を参照してください。

(オプション) 高可用性の設定

高可用性のためにVMware DRS(Distributed Resource Scheduler) を使用する場合は(HA), DRSの設定) 。

次の手順

これで、アプライアンスを配信する準備ができました。VMware環境に応じて、次のいずれかのページに進んでください。

- "アプライアンスを配信する(NSX-T 3.x) " on the next page
- "Applianceのインストール (NSX-V)" on page 611
- "vCloud環境にアプライアンスを配信する" on page 635

VMware DRSの設定

高可用性のためにVMware DRS(Distributed Resource Scheduler) を使用する予定の場合(HA), Deep Security Virtual Applianceをインストールする前にDRSを設定してください。DRSが設定されたら、すべてのESXiサーバ(バックアップESXiサーバ), を含む) に仮想アプライアンスを配信し、アフィニティ設定を使用します。は、それらを各ESXiサーバに「固定」します。これにより、HAフェイルオーバーの後でもエージェントレス保護が適用されたままになります。

警告: アプライアンスがインストールされているESXiサーバからDRXがVMを移動した場合、そのVMは保護されなくなります。元のESXiサーバに戻ると、VMは再び保護されません。では、アプライアンスを備えたESXiサーバ上にVMを移動したときにVMを再度有効化して保護するためのイベントベースのタスクを作成しない限り、そのVMは再びABecEFGに保護されません。詳細については、"コンピュータの追加または変更時にタスクを自動的に実行する(イベントベースのタスク) " on page 1829を参照してください。

警告: ApplianceにはvMotionを適用しないでください。各アプライアンスを特定のESXiサーバに保持します。DRS設定で、[無効](推奨) または[手動]を選択します。または、ストレージを共有ストレージではなくローカルストレージに配置することもできます。仮想アプライアンスがローカルストレージに配置されると、DRSはvMotionを適用しません。詳細については、VMwareのドキュメントを参照してください。

アプライアンスを配信する(NSX-T 3.x)

日本地域向けの製品は、地域固有のポリシーに基づいて取り扱われます。詳細については、Trend Micro Deep Security Virtual Appliance の製品サポート終了に関するご案内をご覧ください。

ここでは、新しいアプライアンスの配置を実行する方法について説明します。

既存のアプライアンスの配置をアップグレードする場合は、代わりに"Deep Security Virtual Applianceのバージョンアップ" on page 1684を参照してください。

アプライアンスを配信するには、次の手順を実行します。

- "アプライアンスをインポートする" below
- "ファブリック設定の準備" on the next page
- "Deep Security ManagerにvCenterを追加する" on page 588
- "NSX-T 3.xにアプライアンスをインストールします。" on page 589
- "グループを作成して保護する" on page 595
- "東西のセキュリティを設定する" on page 597
- "Endpoint Protectionの設定" on page 601
- "アクティベーションの設定" on page 603
- "次の手順 (新しい仮想マシンを追加する方法)" on page 610

アプライアンスをインポートする

"アプライアンスを配信する前に" on page 573のタスクを完了したら、アプライアンスZIPをDeep Security Managerにインポートする準備ができました。

ヒント: アプライアンスのZIPをインポートする代わりに、OVFファイルをURL の場所に配置して、NSXがより高速にダウンロードできるようにすることもできます。詳細については、"アプライアンスのOVFの場所を設定する" on page 650を参照してください。

1. 移動先:

   https://help.deepsecurity.trendmicro.com/ja-jp/software.html

2. Deep Security Virtual Applianceパッケージをダウンロードします。システム要件のバージョン要件を確認してください。

複数バージョンのアプライアンスをインポートできます。マネージャは、最新のパッケージを選択します。

3. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]→[ローカル] に進みます。
4. [インポート] をクリックして、パッケージをDeep Security Managerにアップロードします。

   インポート時、Deep Security Manager は も仮想アプライアンスVMのOSと互換性のあるエージェントを自動的にダウンロードおよびインポートします。このエージェントには、Deep Security Agent for 64ビットRed Hat Enterprise Linuxと同じ保護モジュールがあります。
5. 別の組み込みエージェントを指定する場合は、管理> システム設定> アップデートにアクセスし、仮想アプライアンスの配信。初期設定では、仮想アプライアンスの配信オプションは最新のバージョン(推奨) に設定されています。これは、マネージャに、インポートされた最新の組み込みエージェントを使用するように仮想アプライアンスをアップグレードすることを示します。必要に応じて、この設定を変更します。

これで、アプライアンスがインポートされました。

ファブリック設定の準備

Fabric設定を準備する必要があります。

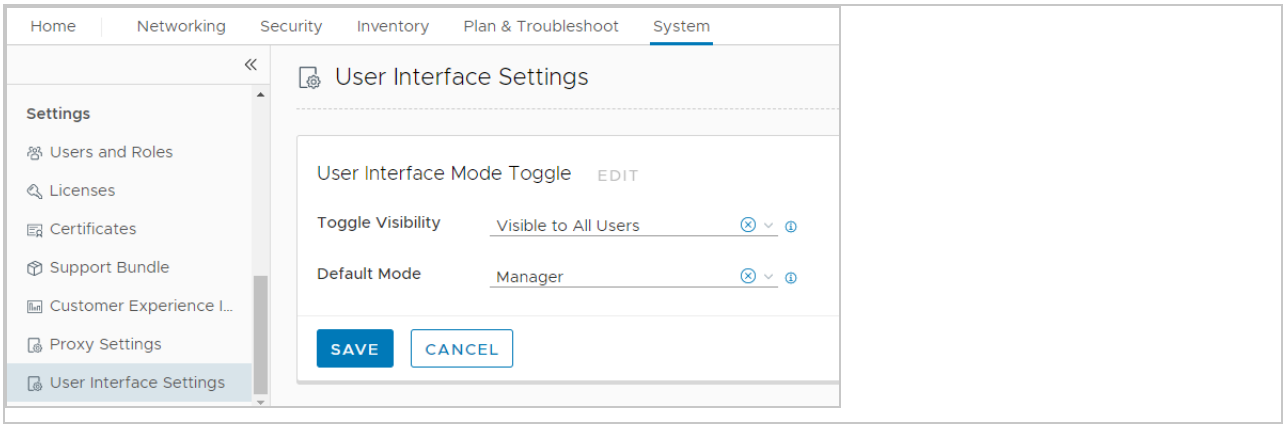
- "ユーザインタフェースモードの切り替えの設定" below
- "Compute Managerを設定する" on the next page
- "トランスポートゾーンの設定" on page 579
- "トランスポートノードプロファイルを設定する" on page 580
- "ホストを準備する" on page 584
- "論理スイッチを作成する" on page 586

ユーザインタフェースモードの切り替えの設定

まず、NSX-T Managerのユーザインタフェース設定を行い、後で設定するために別のモードにアクセスできるようにします。

1. NSX-T Managerの上部にある[システム]をクリックし、左側のユーザインタフェースの設定をクリックしてください。

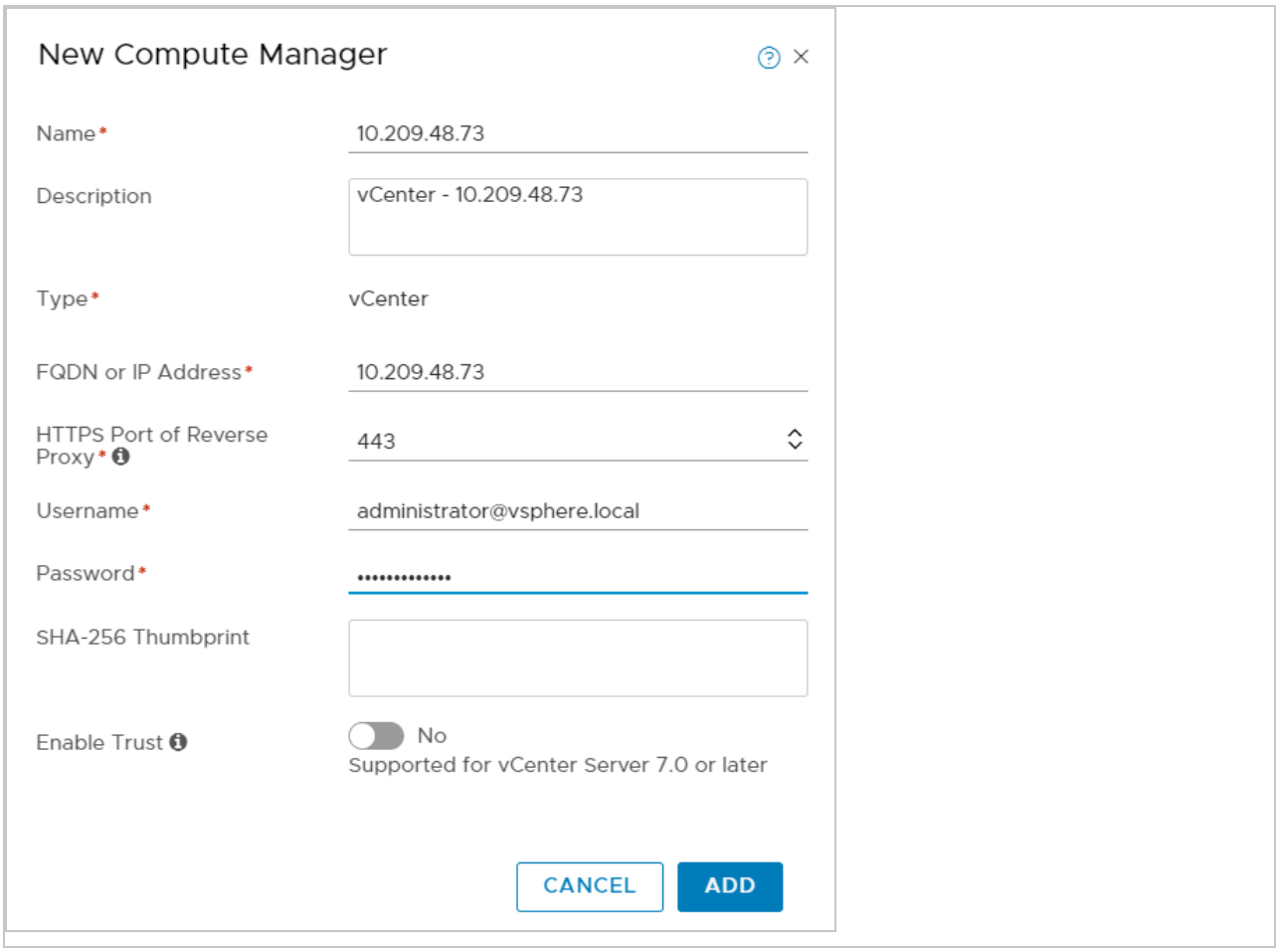
2. 必要に応じて、表示/非表示の切り替えと初期設定の表示を設定します。



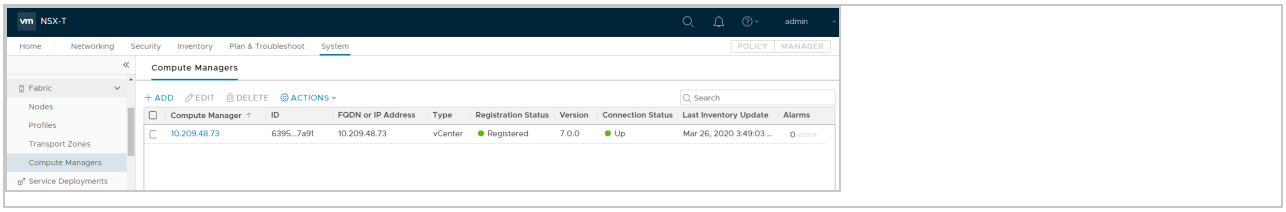
Compute Managerを設定する

次に、vCenterをCompute Managerとして追加します。

1. vCenterとESXiサーバが管理用に設定されていることを確認します。
2. NSX-T Managerで、上部にある[System]をクリックしてから、左側で[Fabric]→[Compute Managers]の順にクリックします。
3. [+ADD]をクリックします。
4. 新規Compute Managerダイアログボックスが表示されます。
5. vCenterの情報をフィールドに入力します。この例では、vCenterは10.209.48.73です。



6. [Add] をクリックします。vCenterが追加されます。



7. vCenterの [Registration Status] が [Registered] で、[Connection Status] が [Up] であることを確認します。

これで、vCenterの追加が完了しました。

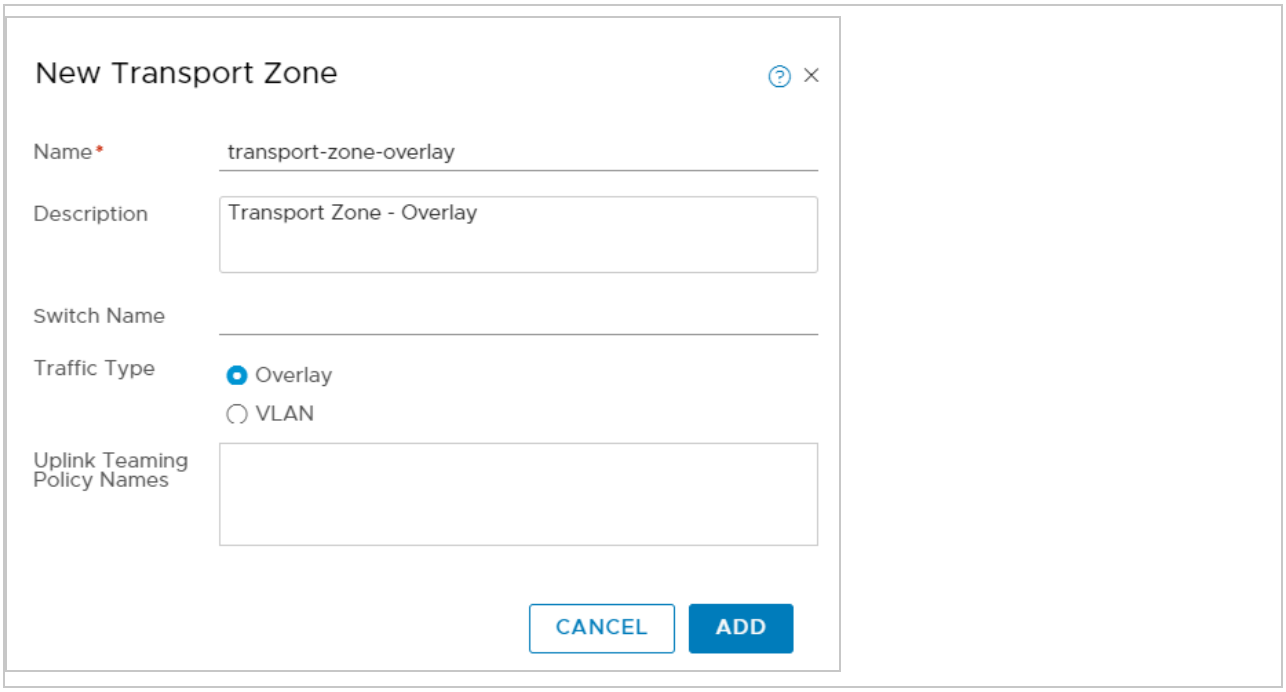
トランスポートゾーンの設定

次に、オーバーレイ転送ゾーンが存在することを確認します。作成していない場合は、次の手順を実行します。

ヒント: すでにゾーンがある場合はゾーンを使用できます。ゾーンを作成する必要はありません。

1. それでもNSX-T Managerの場合は、システム>ファブリック>転送ゾーンにアクセスしてください。
2. オーバーレイのトラフィックタイプを使用するトランスポートゾーンがすでに存在するかどうかを確認してください。
3. オーバーレイトランスポートゾーンが存在しない場合は、+追加をクリックしてゾーンを作成してください。

   [New Transport Zone] ダイアログボックスが表示されます。



4. 名前にトランスポートゾーン名を設定します。例:transport-zone-overlay
5. トラフィックの種類をオーバーレイに設定します。
6. [ADD] をクリックします。

   オーバーレイ転送ゾーンが作成されます。

トランスポートノードプロファイルを設定する

次に、Deep Securityのトランスポートノードのプロファイルを作成します。

ヒント: トランスポートノードプロファイルをすでに使用している場合は、トランスフォームノードプロファイルを使用できます。作成する必要はありません。

1. それでもNSX-T Managerの左側のメニューで[Fabric>Profiles]をクリックし、メイン画面でTransport Node Profiles。

2. + ADD をクリックして、トランスポートノードプロファイルを作成します。

   [Add Transport Node Profile] ダイアログボックスが表示されます。

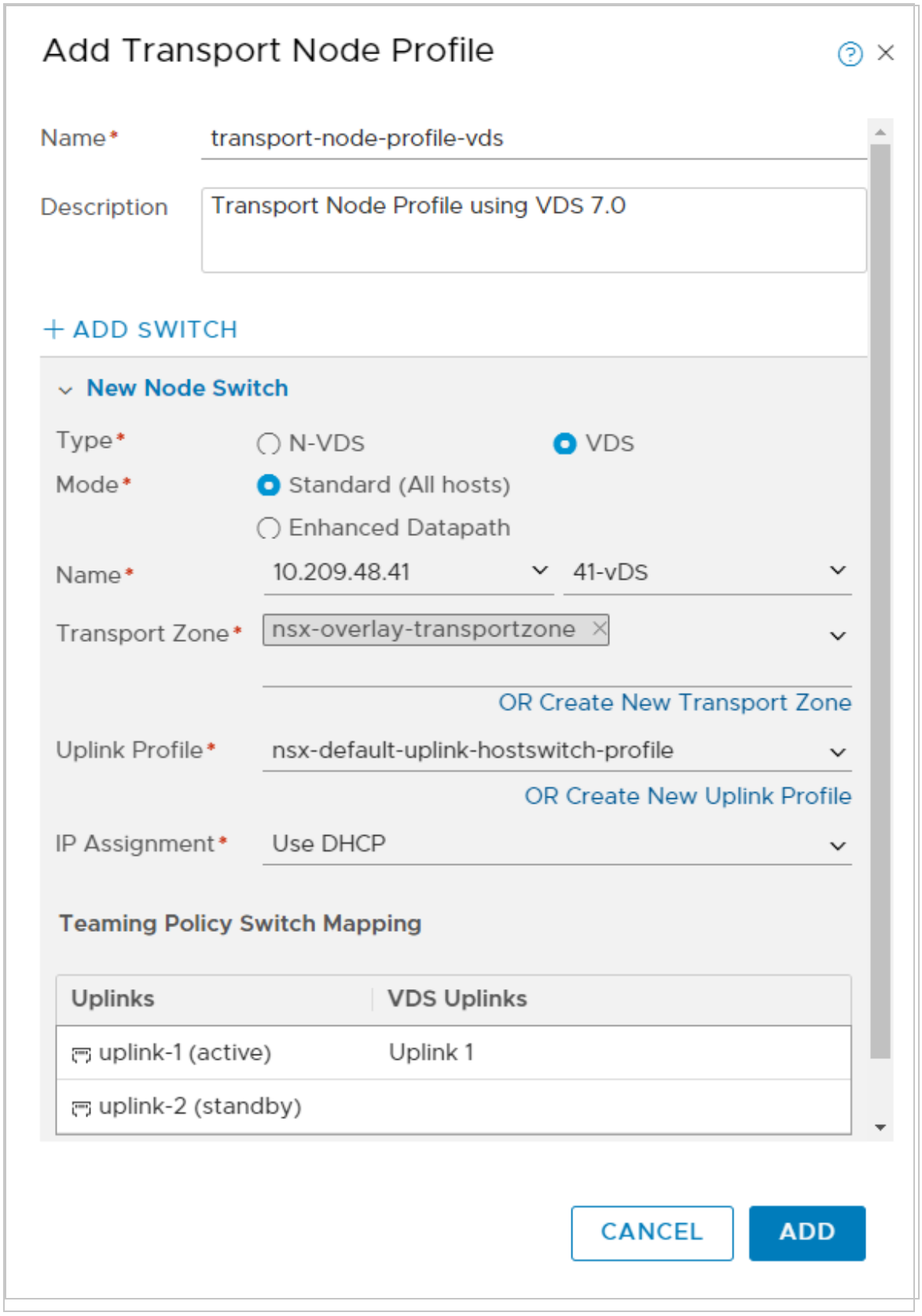
3. 要件に応じてノードスイッチプロファイルを追加する

   注意: VMware は、ESXi 7.0 を使用した新しい NSX の展開に VDS 7.0 を使用することを推奨します。以前の NSX-T バージョンからアップグレードした場合は、N-VDS を引き続き使用できます。詳細については、Deep Security LTS リリースとVMware 互換性マトリックス、Deep Security 機能リリースとVMware 互換性マトリックス、および NSX-T リリースノートを参照してください。

   方法1: VDS ノードのスイッチプロファイルを追加する

   以下のようにフィールドに入力します。

   - 名前に対して、名前を入力します。例 : transport-node-profile。
   - 説明に対して、説明を入力します。例 :Transport Node Profile
   - [新しいノードのスイッチ]で、のを選択し、[VDS]を選択します。
   - Nameに対して、vCenterおよびVDSを選択します。
   - Transport Zoneの場合は、前の手順で作成した転送ゾーンを選択します。例 :transport-zone-overlay
   - [Uplink Profile] には、[nsx-default-uplink-hostswitch-profile] を選択します。
   - IP割り当てに対して、いずれかのオプションを選択します。
   - チーミングポリシースイッチマッピングで、アップリンクに VDS アップリンクを割り当てます。この例では、Uplink 1 をuplink-1(active) に割り当てています。実行可能なアップリンクは、vCenterコンソールで確認できます。ホストをクリックして、の[設定]→[ネットワーク]→[仮想スイッチ]の順に選択します。


Add Transport Node Profile
Name*
transport-node-profile-vds
Description
Transport Node Profile using VDS 7.0
+ ADD SWITCH
New Node Switch
Type*
N-VDS
VDS
Mode*
Standard (All hosts)
Enhanced Datapath
Name*
10.209.48.41
41-vDS
Transport Zone*
nsx-overlay-transportzone
OR Create New Transport Zone
Uplink Profile*
nsx-default-uplink-hostswitch-profile
OR Create New Uplink Profile
IP Assignment*
Use DHCP
Teaming Policy Switch Mapping
Uplinks
VDS Uplinks
uplink-1 (active)
Uplink 1
uplink-2 (standby)
CANCEL
ADD

方法2: N-VDS ノードスイッチプロファイルを追加する

以下のようにフィールドに入力します。

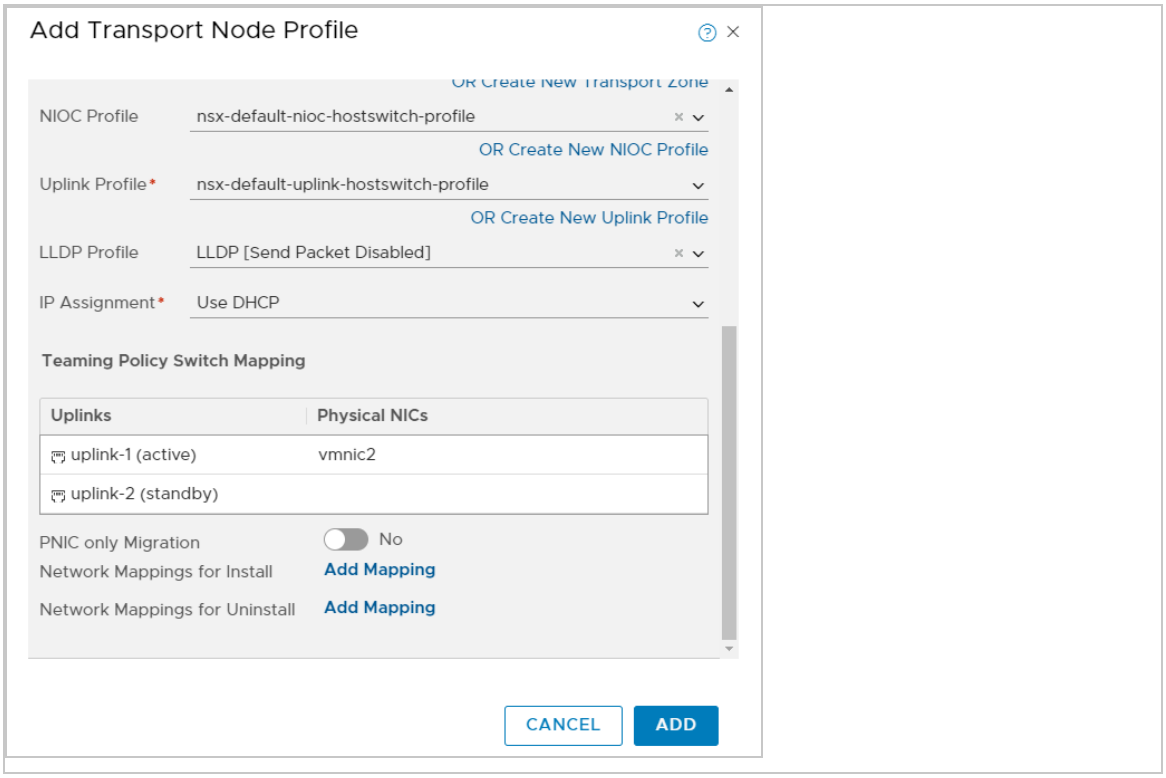
- 名前に対して、名前を入力します。例:transport-node-profile
- 説明に対して、説明を入力します。例:Transport Node Profile
- [新規ノードスイッチ]の下で、タイプに対して、[N-VDS]を選択します。
- モードの場合は、いずれかのオプションを選択します。この例では、標準(すべてのホスト) を選択しました。
- Nameに対して、スイッチの名前を入力します。例:n-vds-overlay
- Transport Zoneの場合は、前の手順で作成した転送ゾーンを選択します。例: transport-zone-overlay。
- [NIOC Profile] には、[nsx-default-nioc-hostswitch-profile] を選択します。
- アップリンクプロファイルの場合は、[nsx-default-uplink-hostswitch-profile]を選択します。
- LLDP Profileに対して、いずれかのオプションを選択します。
- IP割り当てに対して、いずれかのオプションを選択します。
- Teaming Policy Switch Mappingで、有効な物理NICをアップリンクに割り当てます。この例では、vmnic2 をuplink-1(active) に割り当てています。

注意: 割り当てられたNICは、ESXiサーバで使用可能である必要があります。この例では、ESXiホストには vmnic2 があり、N-VDS n-vds-overlayに使用できます。

それぞれの値の詳細を確認するには、ダイアログボックスの上部にある

をクリックします。

ダイアログボックスの下部が次のようになります。



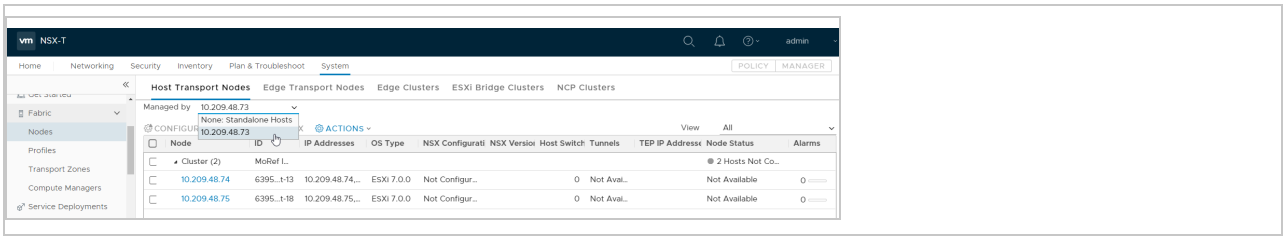
4. フィールドに入力したら、追加をクリックします。

   transport-node-profileというトランスポートノードプロファイルが作成されます。

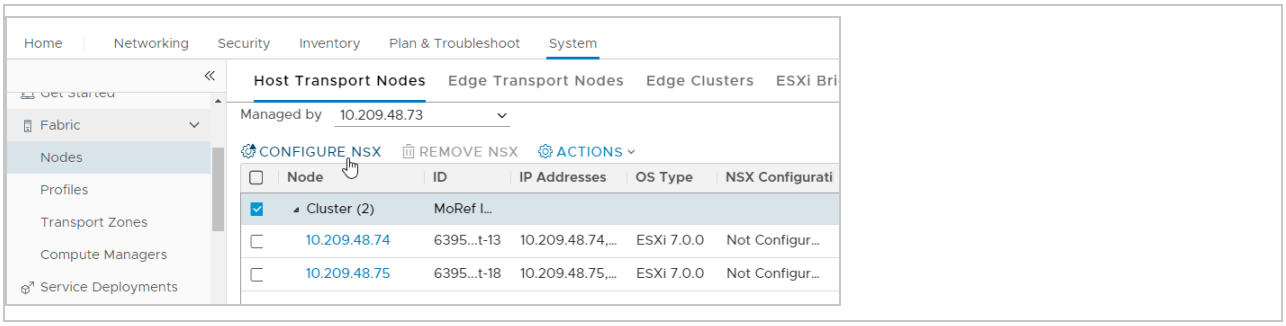
ホストを準備する

次に、Deep Security転送プロファイルをクラスタに適用します。

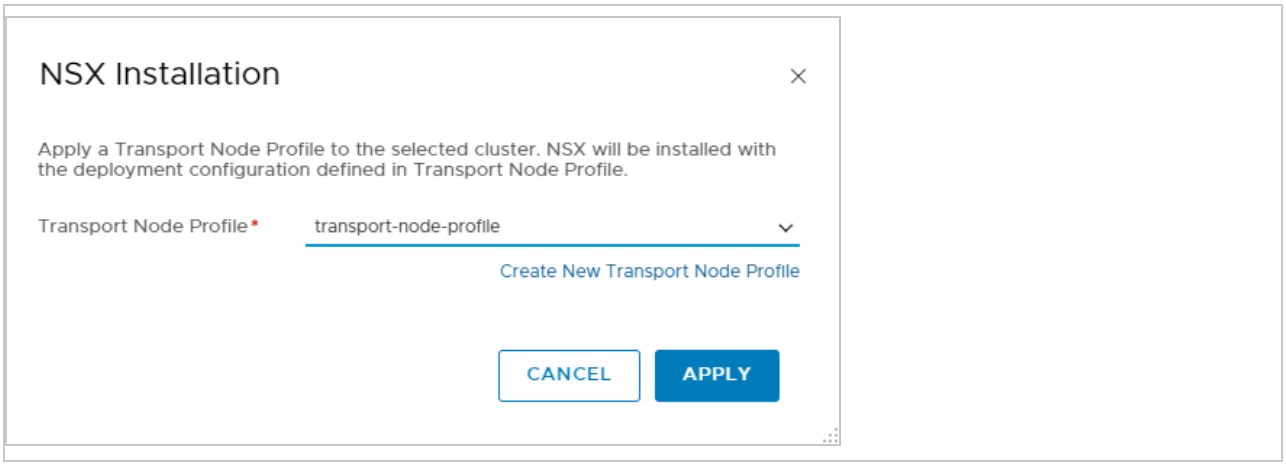
1. それでもNSX-T Managerで[Fabric>Nodes]をクリックし、メイン画面で[Host Transport Nodes]をクリックします。
2. 管理者のドロップダウンリストから、以前に追加したvCenterを選択します。この例では、vCenterは10.209.48.73です。



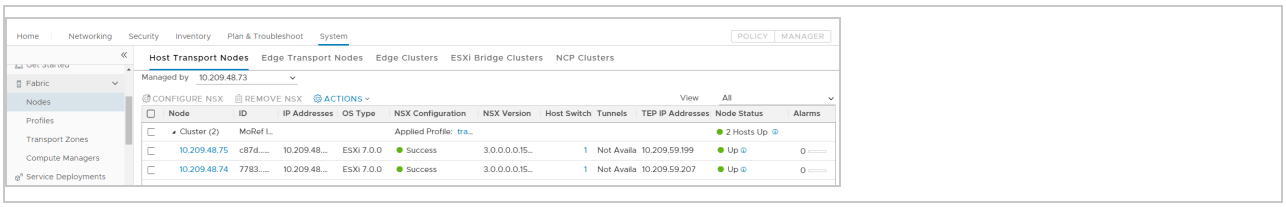
3. Deep Security Virtual Applianceで保護する仮想マシンが含まれているクラスタを選択します。複数のクラスタが存在する場合は、Deep Security Virtual Applianceで保護するクラスタをすべて選択します。
4. [NSXを設定]をクリックします。



5. 配信プロファイルの選択ドロップダウンリストから、転送ノードプロファイルまたは転送ノードプロファイルの呼び出し対象を選択します。



6. [SAVE] をクリックします。次の処理が行われます。
   - Deep Securityトランスポートノードプロファイルがクラスタに適用されます。
   - プロファイルの適用中は、プロファイルの適用メッセージが表示され、各ノードでインストールの進行状況を確認できます。
   - 操作が完了すると、各ノードのNSX設定が成功に変わり、ノードのステータスがに変更されます。アップします。ESXiサーバが複数ある場合は、そのすべてが [Success] および [Up] としてマークされる必要があります。



これで、対象クラスタが設定されました。

論理スイッチを作成する

次に、NSX Data Center Advanced、NSX Data Center Enterprise Plus、またはNSX Data Center for Remote Office Branch Office Editionを使用している場合は、ネットワークトラフィック検査のためにロジックスイッチを設定する必要があります。別のエディションのNSXを使用している場合は、このセクションをスキップしてください。

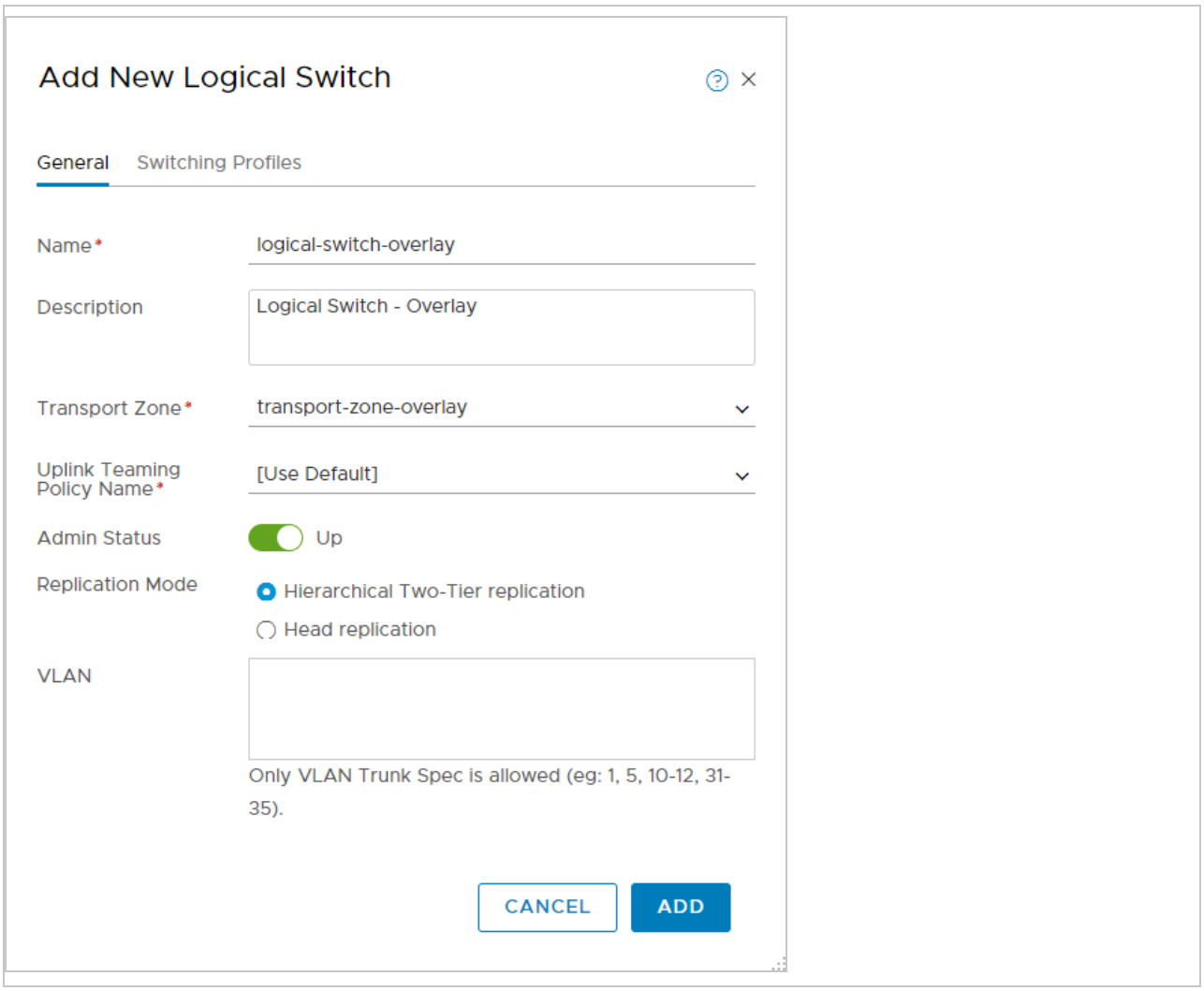
ヒント: 既に論理スイッチがある場合は、論理スイッチを使用できます。論理スイッチを新規に作成する必要はありません。

1. それでもNSX-T Managerの上部にある場合は、[ネットワーク]をクリックして、管理者に切り替えてください。
2. 左側の[論理スイッチ]をクリックします。
3. メイン画面で、[+ ADD]をクリックします。

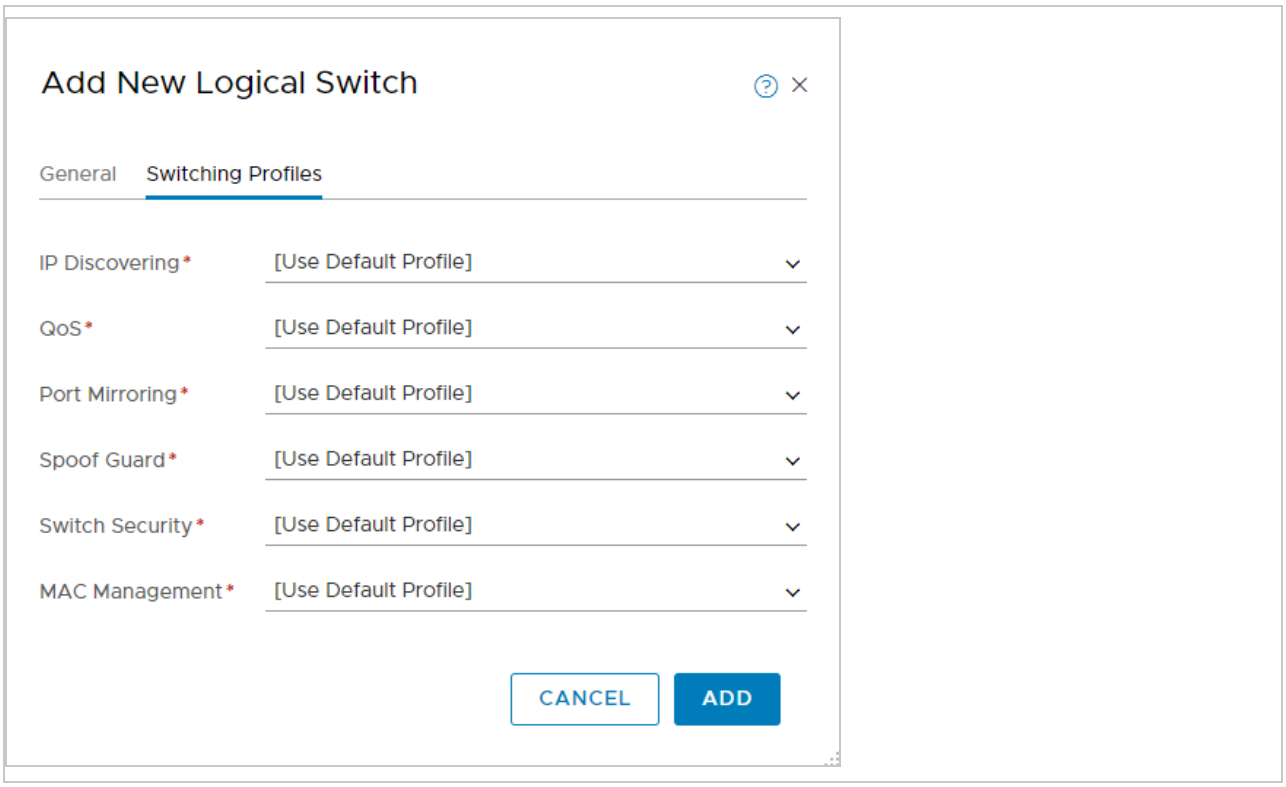
   新しい論理スイッチの追加ダイアログボックスが表示されます。

4. [一般] タブで、次の項目を設定します。

   - 名前には、論理スイッチの名前を入力します。例:logical-switch-overlay
   - Transport Zoneの場合は、以前に作成したオーバーレイ転送ゾーンを選択します。例 : transport-zone-overlay
   - Uplink Teaming Policy Nameの場合は、[Use Default]を選択します。
   - 管理者ステータスについては、初期設定値のままにしてください。
   - 複製モードの場合は、いずれかのオプションを選択します。
   - VLANの場合は、このフィールドは空白のままにしてください。

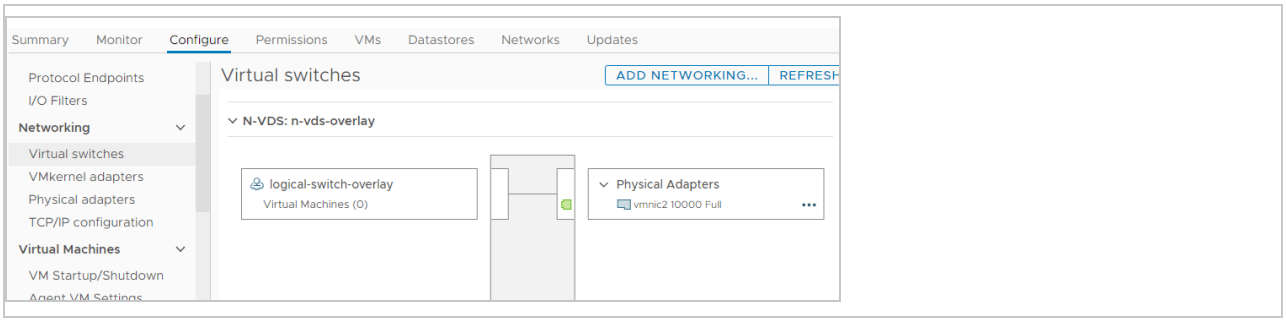


5. プロファイルの切り替えタブで、各項目に必要なプロファイルを選択します。この例では、すべてのアイテムに対して[初期設定のプロファイルを使用]を維持しています。



6. [ADD] をクリックします。

   論理スイッチが作成されます。ホスト上のスイッチのステータスは、vSphere Clientを介して確認できます。



これで、NSX-T Managerでファブリック設定の準備ができました。

Deep Security ManagerにvCenterを追加する

vCenterを追加する必要があります。

"VMware vCenterの追加" on page 704の手順に従ってください。

完了後:

- ゲストVMがDeep Security Managerに表示されます。
- Trend Micro Deep SecurityサービスがNSX-Tに登録されています。

NSX-T 3.xにアプライアンスをインストールします。

日本地域向けの製品は、地域固有のポリシーに基づいて取り扱われます。詳細については、Trend Micro Deep Security Virtual Applianceの製品サポート終了に関するご案内をご覧ください。

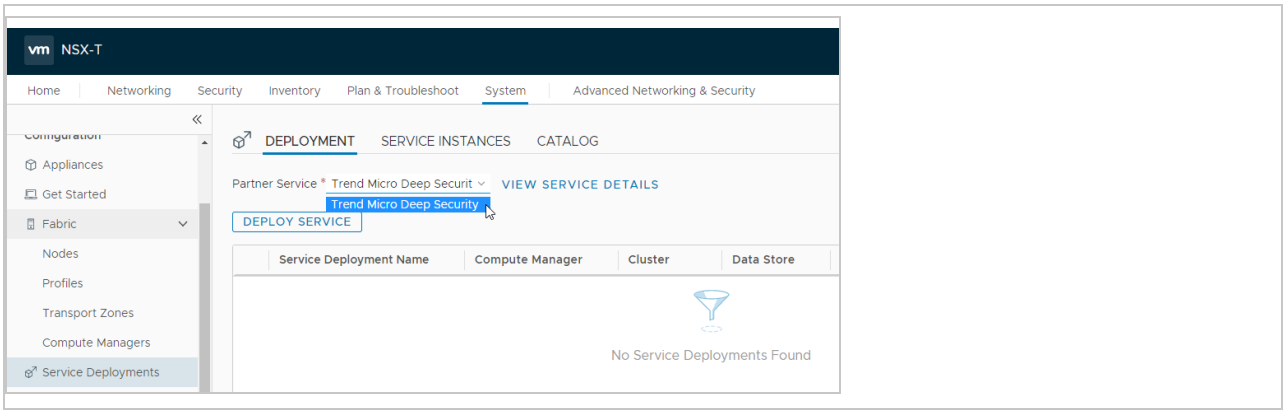
NSX-T 3.xにアプライアンスをインストールする必要があります。

次の手順に従います。

- "サービスの配信を開始する" below
- "サービス配信を設定および開始する" on the next page
- "配信を監視および確認する" on page 593
- "配信を監視および確認する" on page 593
- "クラスタごとにすべての手順を繰り返します。" on page 595

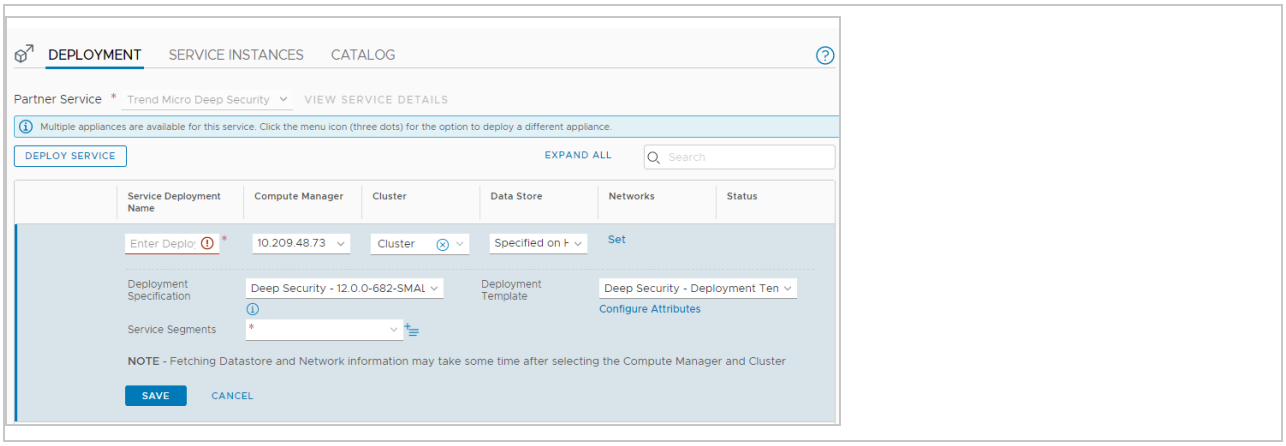
サービスの配信を開始する

1. NSX-T Managerで[システム]をクリックし、左側で[サービス配信]を選択します。



2. Partner ServiceリストからTrend Micro Deep Securityを選択します。このTrend Micro Deep Securityサービスは、Deep Security ManagerでvCenterを追加したときに登録されています。
3. サービスのデプロイをクリックしてください。

   青色のパネルが表示されます。



4. 青いパネルに記入し、"サービス配信を設定および開始する" belowに記載されているようにしてください。

サービス配信を設定および開始する

下記の説明に従ってサービスの配信フィールドに入力してから、SAVEをクリックして配信を開始してください。

サービス配信名の設定

サービスデプロイメント名フィールドに名前を入力します。複数のクラスターがある場合、デプロイするクラスターの名前を含む名前を使用することを検討してください。クラスターは同じページのクラスター見出しの下に一覧表示されます。例:dsva-vc73-cluster。

Compute Managerを設定する

Compute Managerのドロップダウンリストから、以前に追加したvCenterを選択します。この例では、vCenterは10.209.48.73です。

クラスタを設定する

クラスタドロップダウンリストから、以前に設定したクラスタを選択します。Trend Micro Deep Securityサービスが、このクラスタのすべてのESXiサーバにインストールされます。クラスタが複数ある場合、ここでは1つだけ選択します。別のクラスタを選択するために後でこの手順に戻ることもできます。

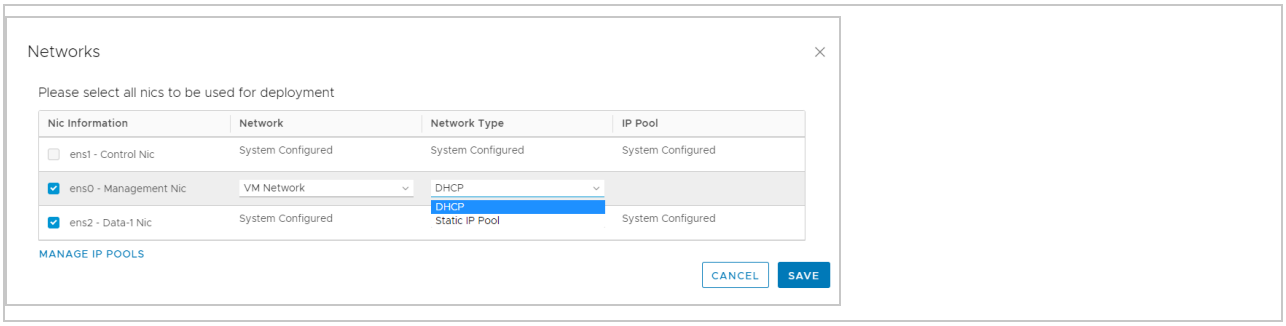
データストアの設定

データストアのドロップダウンリストから、お使いの環境に適したオプションを選択します。この例では、[Specified on Host] を選択しています。

ネットワークを設定する

ネットワークの下で:

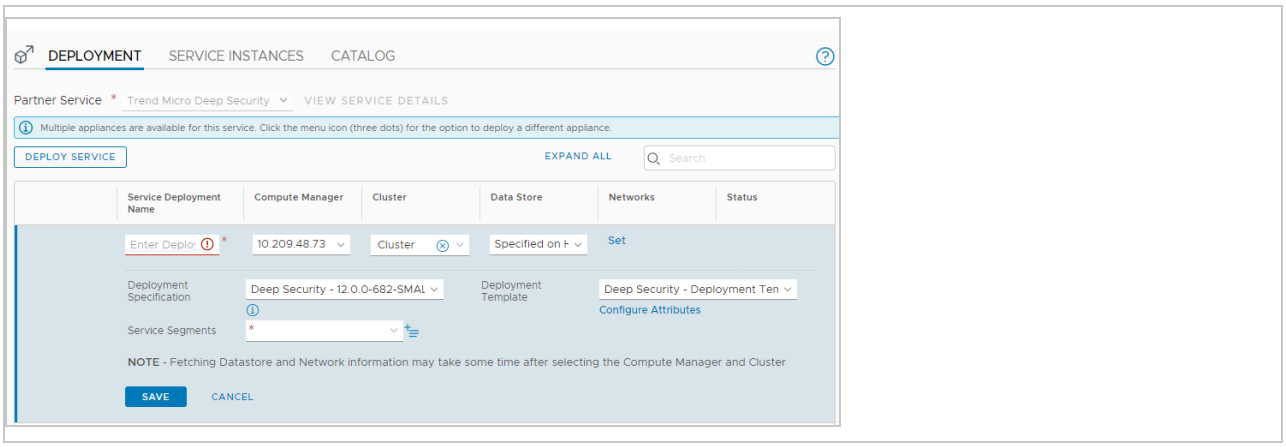
1. 使用可能な設定または詳細の編集をクリックします。
2. ens0 - 管理NICチェックボックスをオンにします。
3. 使用する[Network]および[Network Type]を選択します。
4. 東西のセキュリティ機能を取得するには、ens2 - Data-1 NICチェックボックスをオンにします。
5. SAVEをクリックして、ネットワーク設定を保存します。



配置仕様の設定

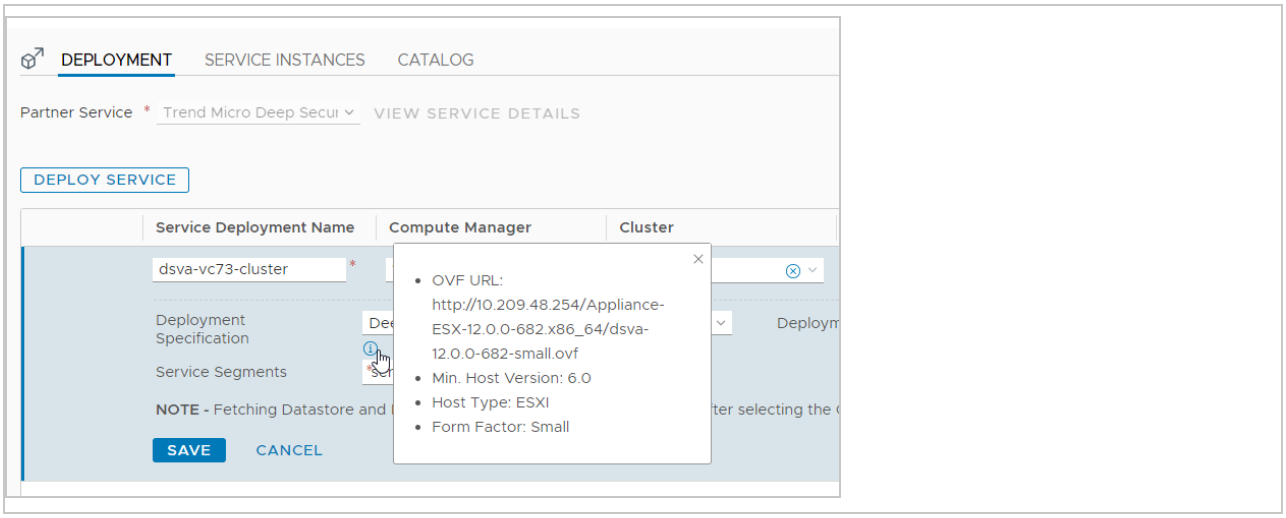
配信仕様ドロップダウンリストから:

1. Deep Security -<バージョン>-SMALL-small、MEDIUM - medium、またはを選択します。大規模 - 大規模なオプションを選択します。これは、配置のサイズに応じて異なります。配信のサイズがわからない場合は、"Deep Security Virtual Applianceのサイジング" on page 425の情報を確認してください。例では、Deep Security - 12.0.0-682-SMALL-Smallを選択しています。
2. OVFがURLの場所に設定されている場合は、前回と同じサイズのOVFを選択してください。たとえば、小さいOVFのURLを以前に設定した場合は、配信仕様の下にある小さなOVFを選択してください。



3. アプライアンスOVFをNSXからダウンロードするOVF URLを表示するには、[ ]をクリックします。

   注意: OVFの別のURLを指定した場合は、そのURLが代わりに使用されます。

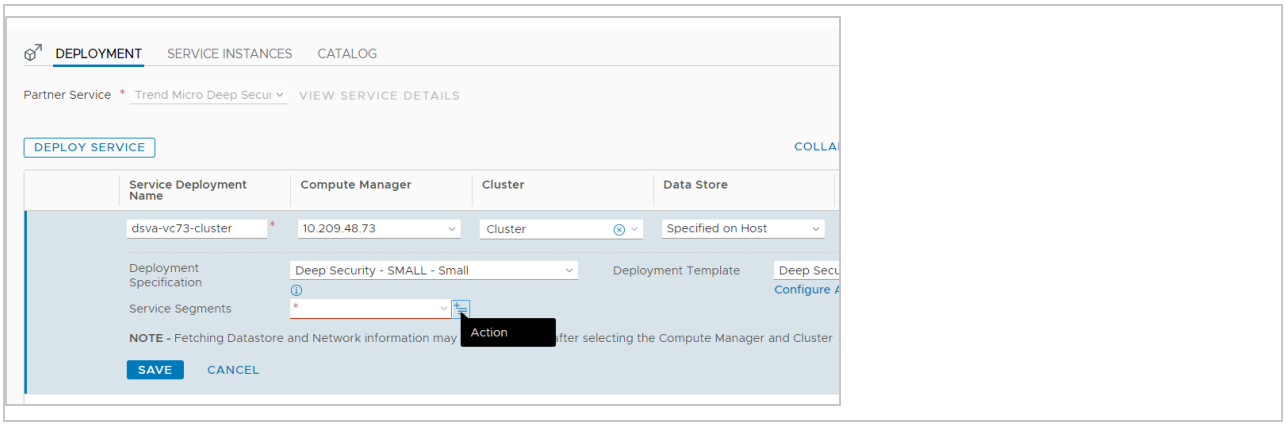


サービスセグメントの設定

サービスセグメントドロップダウンリストから、オーバーレイ転送ゾーンを使用するように設定されているサービスセグメントを選択します。

まだサービスセグメントがない場合は、次の手順でサービスセグメントを作成します。

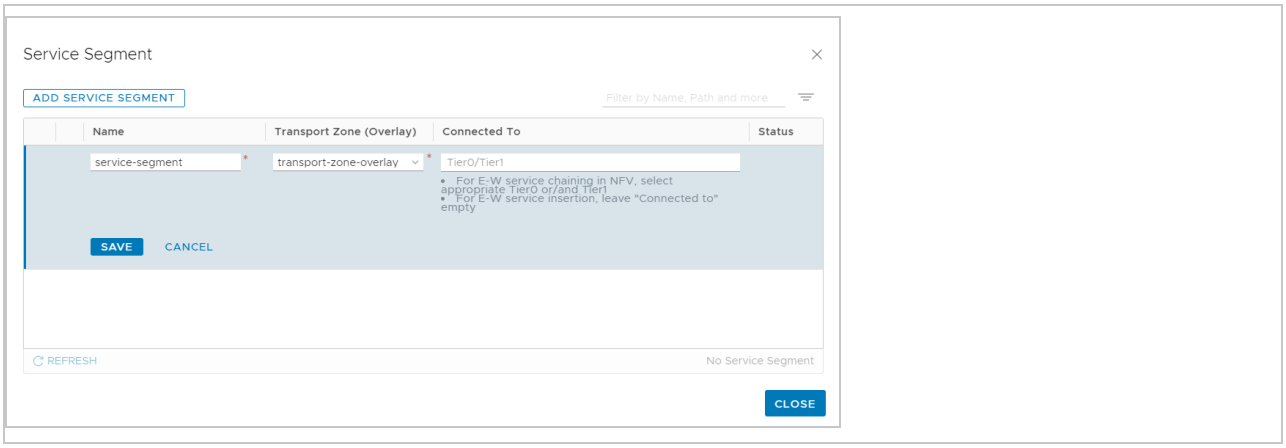
1. Actionをクリックします。



   サービスセグメントダイアログボックスが表示されます。

2. [ADD SERVICE SEGMENT]をクリックします。
3. 名前の下に、service-segmentなどの名前を入力します。

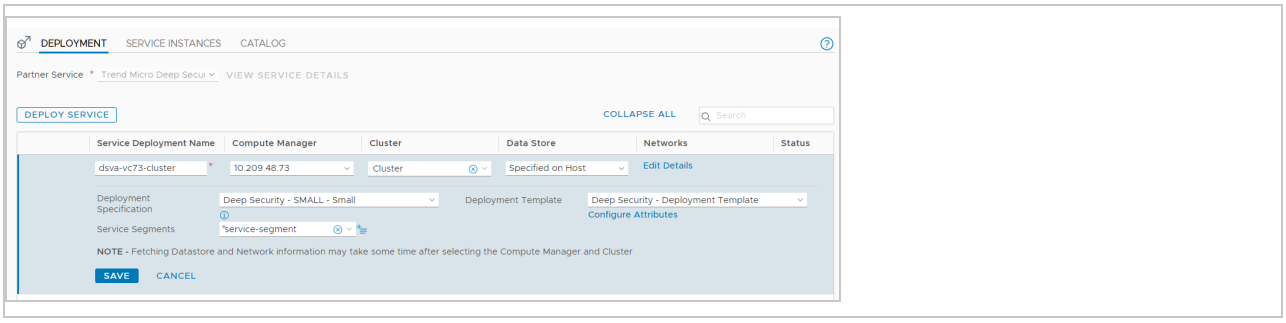
4. トランスポートゾーン(オーバーレイ) で、トランスポートゾーンオーバーレイ、または使用しているオーバーレイトランスポートゾーンを選択します。
5. Connected Toは空のままにしてください。
6. SAVEをクリックし、CLOSEします。サービスセグメントが作成されます。
7. サービスセグメントのドロップダウンリストから、作成したサービスセグメントを選択します。



配置テンプレートを設定する

1. 配信テンプレートのドロップダウンリストから、Deep Security - 配信テンプレートを選択します。
2. (オプション) DPDKモードでアプライアンスのCPU使用率を設定する場合は、[属性の設定]をクリックし、dpdkModeフィールドを変更します。。DPDKの詳細とアプライアンスとの連携方法については、"DPDKモードを設定する" on page 645を参照してください。

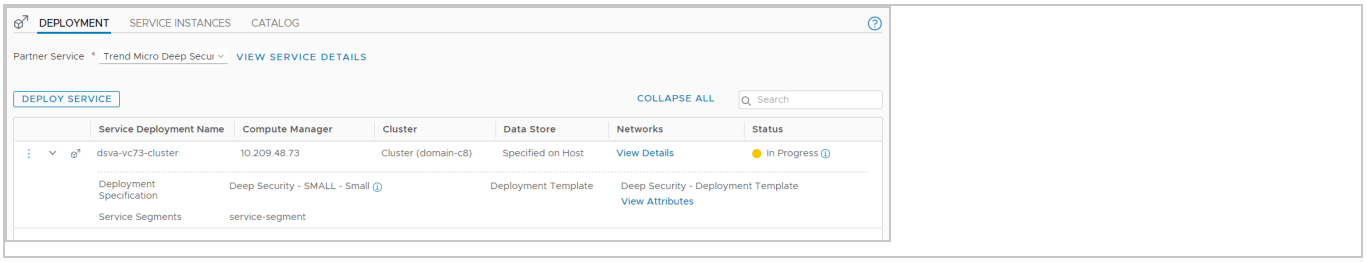
   サービスのインストールの詳細は次のようになります。



配信を監視および確認する

配信を開始したら、NSX-T 3.xおよびvSphere Clientで監視し、Deep Security Managerで確認できます。

NSX-T 3.xの配置を監視する



NSX-T Managerの [Status] 列に、[In Progress] と表示されます。

インストールが完了すると、[Status] が [Up] に変更されます。

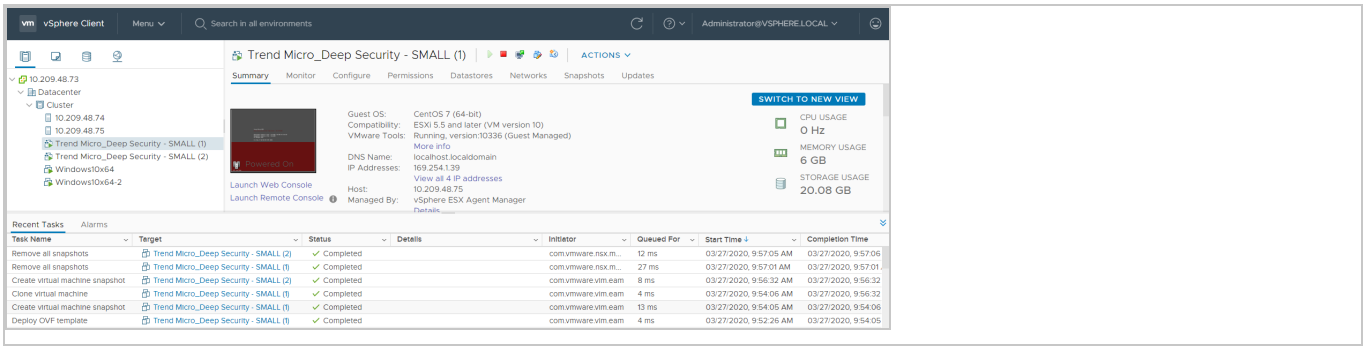
割り当てたクラスタにESXiサーバが複数ある場合は、Trend Micro Deep Securityサービスが各ESXiサーバにインストールされます。サービスは次のように分類され、区別されます。

- Trend Micro_Deep Security - SMALL(最初のESXiサーバの場合は1) ()
- Trend Micro_Deep Security - SMALL(2番目のESXiサーバの場合は2) ()
- ... などです。

vSphere Clientでの配置を監視する

vSphere Clientを介してvCenterにアクセスすることで、配信のステータスを確認できます。vSphere Clientにはさらに詳しく進行状況が表示されます。[Status] が [Complete] に変更されるまで待ちます。

下の画像で、Trend Micro Deep Securityサービスが2つ、左側にリスト表示されているのがわかります。クラスタにESXiサーバが2つあるため、サービスが2つインストールされました。

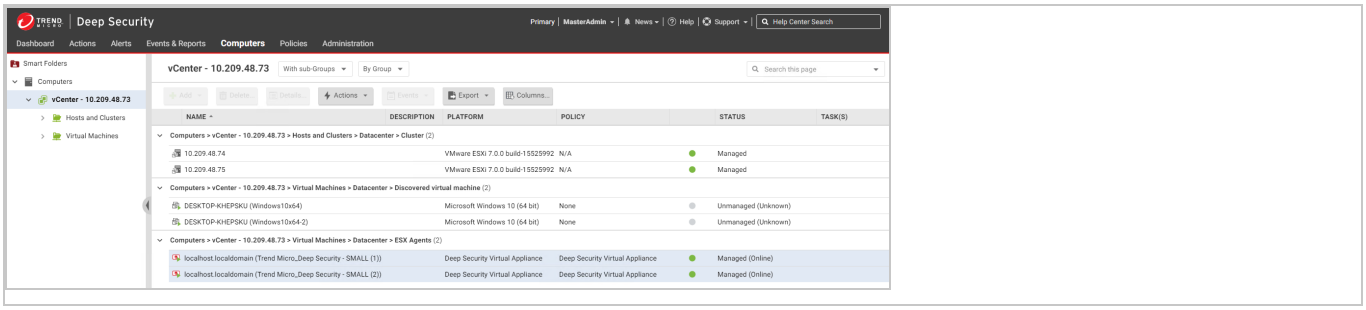


Deep Security Managerでの配置を確認する

あなたはクリックコンピュータでのDeep Security Managerの展開を確認することができるTrend Micro Deep Securityサービスが展開されたのvCenterを展開し、左側の後、上部にと。

Deep Security Virtual Applianceのプラットフォームを使用して、仮想マシン>データセンター> ESXエージェントの下にTrend Micro_Deep Security(1) が表示されます。クラスタ内のESXiサーバごとにVirtual Applianceが1つあるのを確認できます。

注意: Deep Security Managerに仮想マシンが表示されますが、仮想マシンはこの時点では保護されていません。



クラスタごとにすべての手順を繰り返します。

各クラスタの"NSX-T 3.xにアプライアンスをインストールします。" on page 589のすべての手順を繰り返します。

NSX-T 3.xにアプライアンスがインストールされました。

グループを作成して保護する

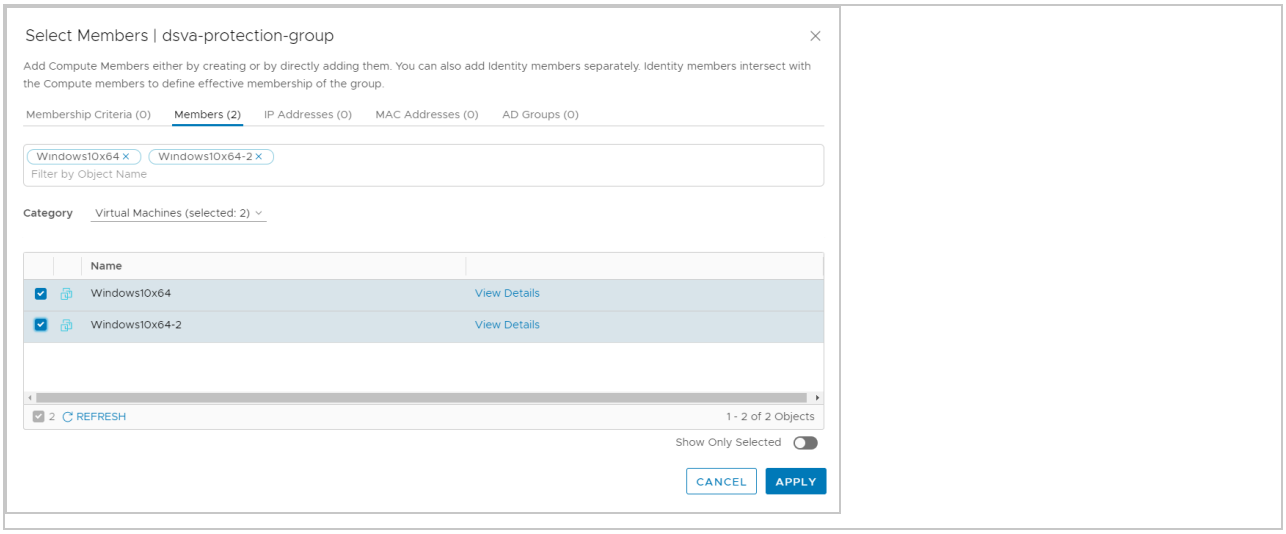
Deep Security Virtual Applianceを使用して保護する仮想マシンを含むグループを作成する必要があります。

1. NSX-T Managerの上部で[広告枠]をクリックし、POLICYに切り替えてから、左側でグループを参照してください。
2. [ADD GROUP] をクリックして、Deep Security Virtual Applianceで保護される仮想マシンが含まれるグループを作成します。以下のようにフィールドに入力します。
   - [Name] には、グループの名前を入力します。例:dsva-protection-group
   - Compute Membersの場合は、メンバーを設定してグループ内のどのVMを選択するかを選択します。

     注意: 以下の手順では、メンバーを追加する最も簡単な方法を説明します。[Membership Criteria] などを使用する、より複雑な方法については、NSX-Tのドキュメントを参照してください。

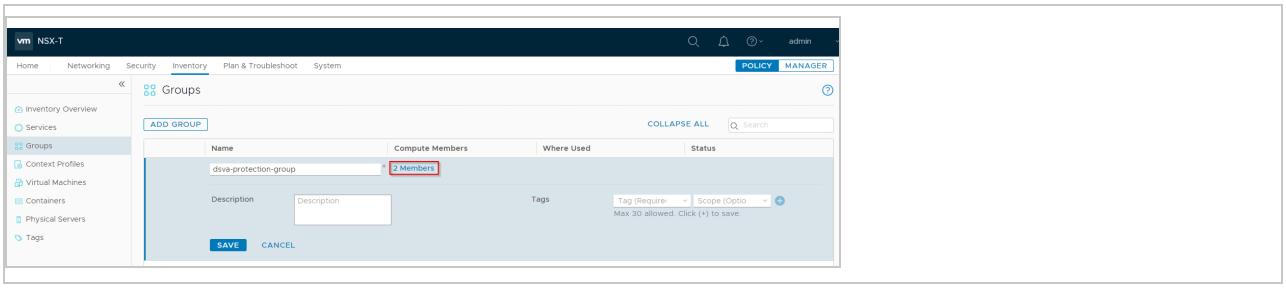
3. 上部の[メンバー(0)]をクリックし、[Select]ドロップダウンリストで[VirtualMachine(selected : 0)]を選択します。
4. VMが表示されていない場合は、更新をクリックしてください。
5. グループに追加するゲストVMを選択します。選択した仮想マシンは、Deep Security Virtual Applianceによって保護されます。

   [Select Members] ダイアログボックスは次のようになります。



6. 上部付近にある[Members] タブで仮想マシンの数を確認します。上記の例では、件数が2 - メンバー(2) になっています。
7. [APPLY] をクリックします。

   [ADD GROUP] ページには、更新された数が表示されます。



8. [SAVE] をクリックします。

   これでメンバーが含まれたグループを追加することができました。複数のグループを作成する手順を繰り返してもかまいません。

東西のセキュリティを設定する

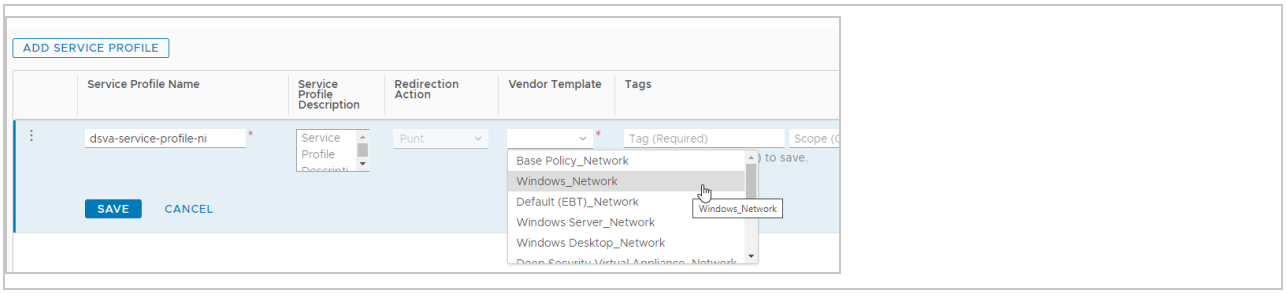
east-westセキュリティを設定するには、変更監視、侵入防御、ファイアウォール、およびWebレピュテーション機能を使用します。

east-westセキュリティを設定するには、次の手順を実行します。

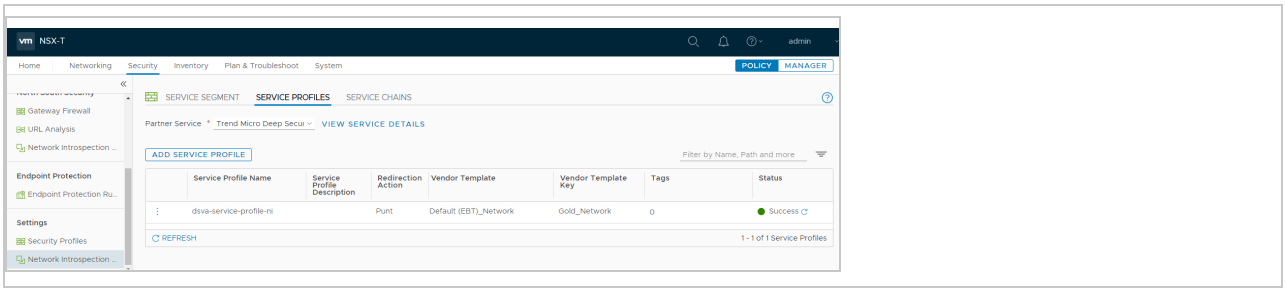
- "サービスプロファイルを追加する" below
- "サービスチェーンを追加する" on the next page
- "ネットワークイントロスペクションポリシーを追加する" on page 599します。
- "VMを論理スイッチに接続する" on page 600

サービスプロファイルを追加する

1. NSX-T Managerで、上部のセキュリティをクリックし、POLICYに切り替えてから、左側でSettingsを選択し、ネットワークイントロスペクション設定をクリックします。
2. メイン画面で、[SERVICE PROFILES] をクリックします。
3. [Partner Service] ドロップダウンリストから、[Trend Micro Deep Security] を選択します (選択されていない場合)。
4. サービスを追加して、次のフィールドに情報を入力します。
   - サービスプロファイル名には、名前を指定します。例:dsva-service-profile-ni
   - [Service Profile Description] では、説明を入力します。例:Deep Security Service Profile for Network Introspection
   - ベンダーテンプレートの場合は、初期設定(EBT)_ネットワーク) を選択します。このテンプレートは、Trend Micro Deep Securityサービスと同時にロードされました。



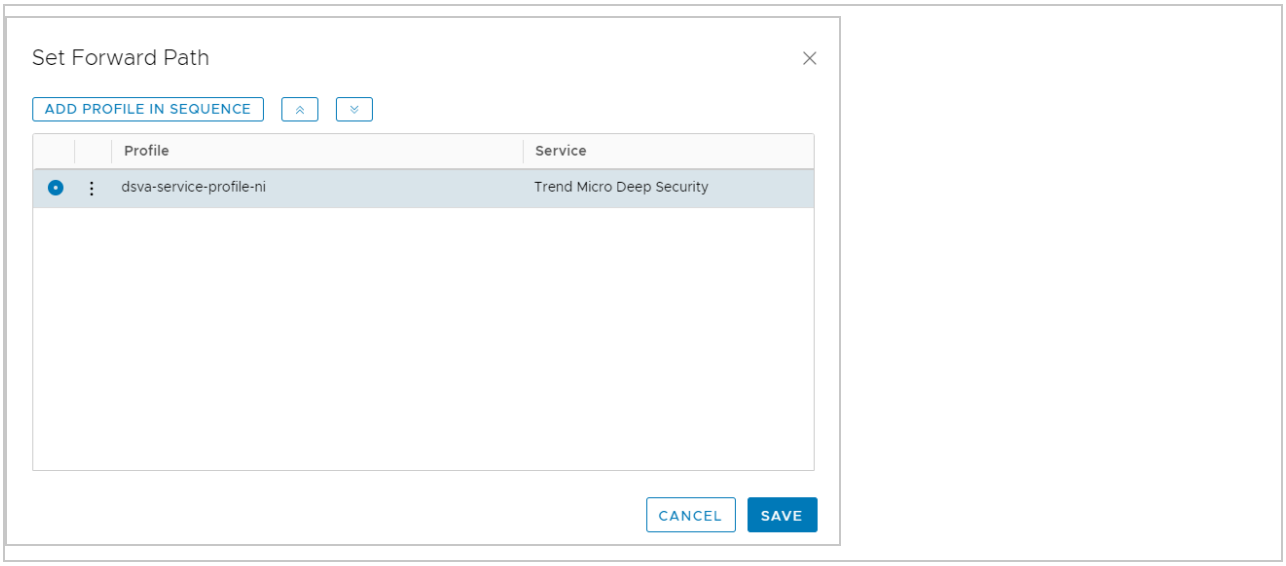
5. ADDSERVICE PROFILEページは次のようになります。



6. [SAVE] をクリックします。

サービスチェーンを追加する

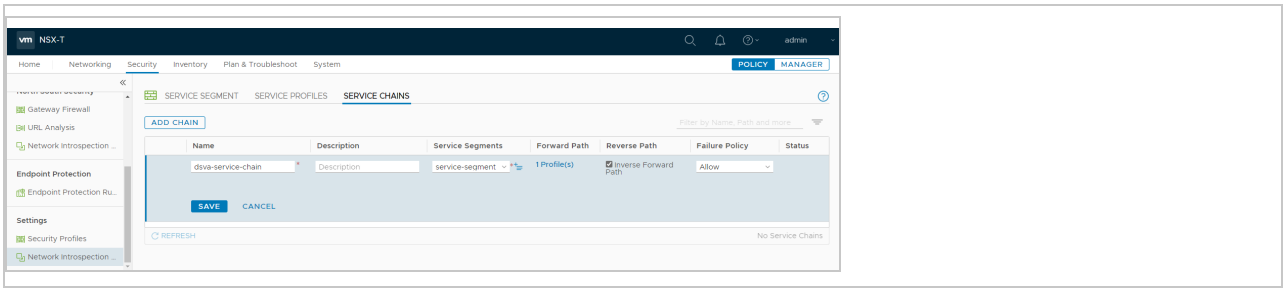
1. メイン画面で、サービスチェーンタブをクリックし、ADD CHAINをクリックします。次の手順に従ってフィールドに入力します。
2. 名前には名前を指定します。例:dsva-service-chain
3. サービスセグメントの場合は、以前に作成したサービスセグメントを選択します。例:サービスセグメント
4. 転送パスの場合:
   - [転送経路を設定]をクリックして、ダイアログボックスを開きます。
   - ADDPROFILE IN SEQUENCEをクリックして、以前に作成したサービスプロファイルを追加します。この例では、dsva-service-profile-niを選択しました。
   - [ADD] をクリックします。
   - [SAVE] をクリックします。



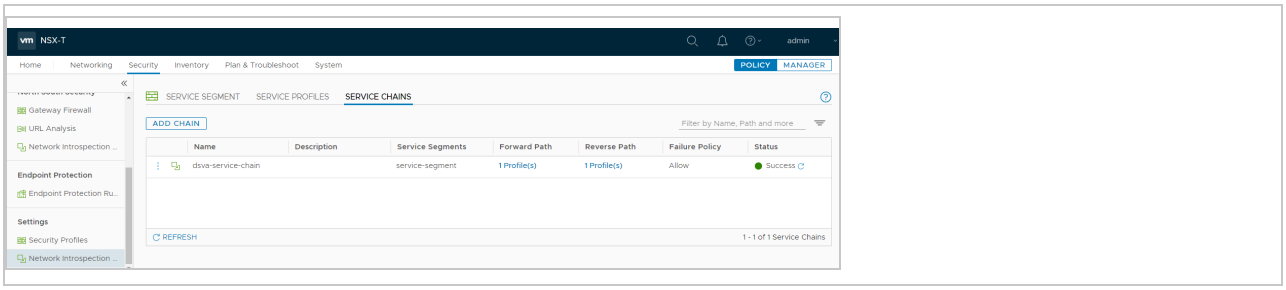
SERVICE CHAINSページに戻ります。SERVICE 以下のチェーン設定を続行してください。

5. リバースパスの場合は、逆転送パスチェックボックスをオンにしてください。
6. 失敗ポリシーの場合は、許可を選択します。

   サービスチェーンは次のようになります。



7. [SAVE] をクリックします。



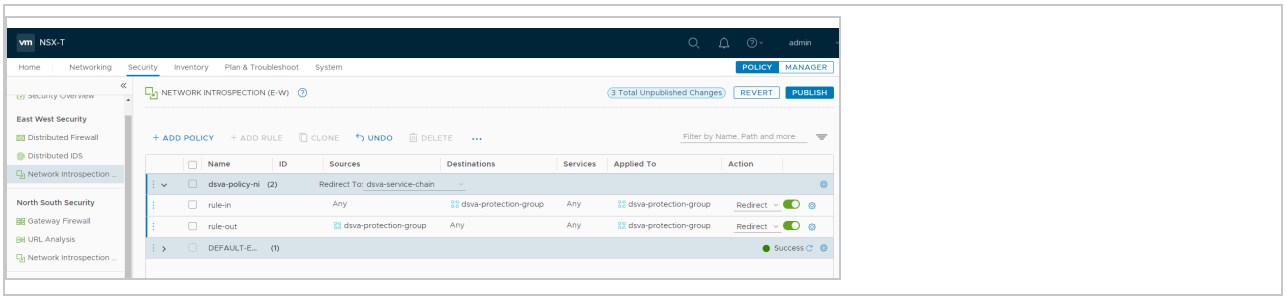
ネットワークイントロスペクションポリシーを追加する

1. 上部のセキュリティをクリックして、POLICYに切り替えてから、左側でEast West Securityに移動して、Network Introspection(EW) をクリックしてください。
2. メイン画面で、[+ポリシーを追加]をクリックします。
3. 名前列で、新しいポリシーのセル内をクリックし、名前を変更します。たとえば、dsva-policy-niを使用します。リダイレクト先でサービスチェーンを選択します。この例では、dsva-service-chainを使用しています。
4. dsva-policy-niの横にあるチェックボックスをオンにして、+追加ルールをクリックします。dsva-policy-niにルールが表示されます。2つのルールが必要なため、+追加ルールを再度クリックしてください。
5. 受信トラフィックの1次ルールを設定します。
   - 名前にルールの名前を入力します。例:rule-in
   - ソースについては、任意のキーワードを使用してください。
   - 送信先の場合は、dsva-protection-groupを選択します。
   - サービスについては、任意のキーワードを使用してください。
   - Applied Toの場合は、dsva-protection-groupを選択します。
   - Actionの場合は、リダイレクトを選択します。

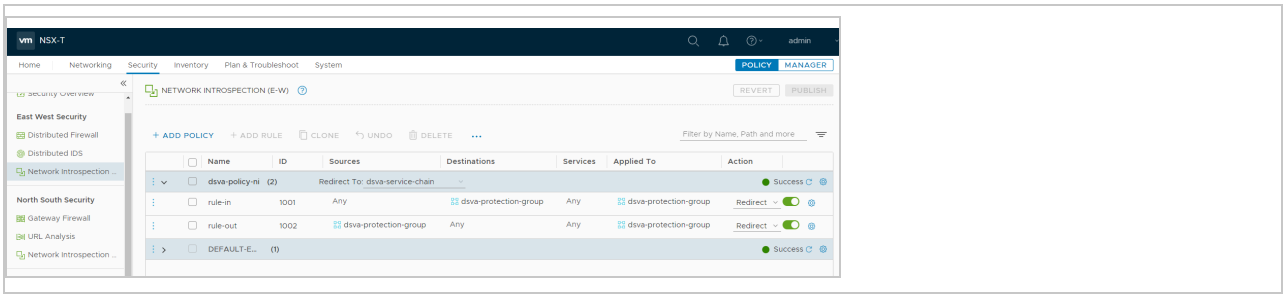
6. 送信トラフィックの2番目のルールを設定します。
   - 名前にルールの名前を入力します。例:rule-out
   - Sourcesについては、dsva-protection-groupを選択してください。
   - Destinationsの場合は、Anyをそのまま使用してください。
   - サービスについては、任意のキーワードを使用してください。
   - Applied Toの場合は、dsva-protection-groupを選択します。
   - Actionの場合は、リダイレクトを選択します。

   dsva-protection-group内のVMと、dsva-service-chainで指定されている初期設定(EBT)_Networkテンプレート)の間にマッピングがあります。

   ポリシーは次のようになります。



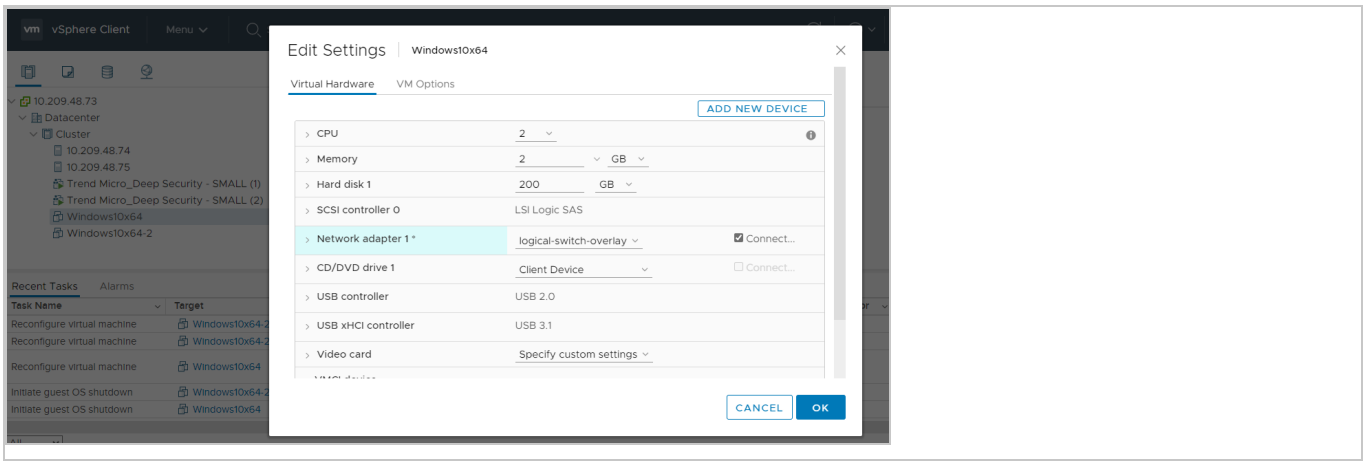
7. [PUBLISH] をクリックして、ポリシーとルールの作成を終了します。



VMを論理スイッチに接続する

グループのVMをNSX-Tの東西のセキュリティで保護するには、以前の手順で作成した論理スイッチに接続されているVMを使用します。

この例では、ネットワークアダプタ1を論理スイッチオーバーレイに接続しました。VMがこのスイッチに接続されていることを確認するには、vSphere ClientからvCenterにアクセスします。



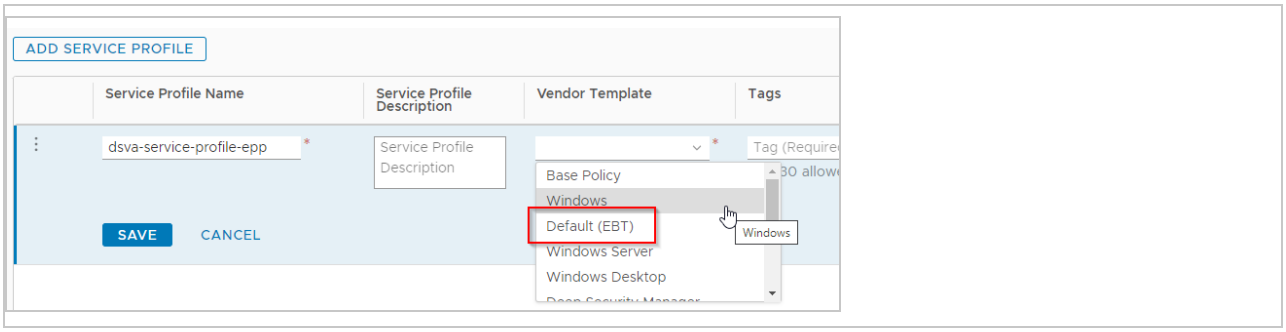
NSX-Tでeast-westセキュリティが設定されました。

Endpoint Protectionの設定

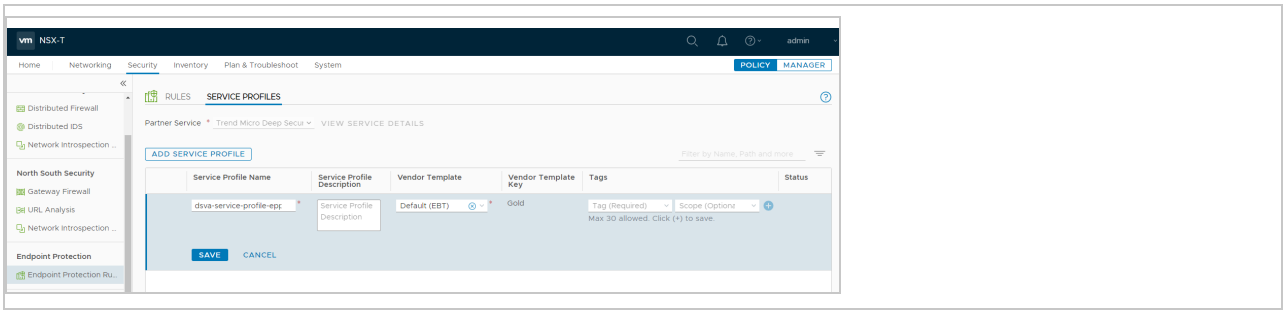
エンドポイント保護を設定するには、Deep Security Virtual Applianceの不正プログラム対策機能が適用された*既存の*VMを保護する必要があります。

次の手順に従って、Deep Security Virtual Applianceのサービスプロファイルを設定します。

1. それでもNSX-T Managerの場合は、上部のセキュリティをクリックし、上部にある[ポリシー]を選択してから、左側の[検索]をクリックします。Endpoint Protectionを選択し、エンドポイント保護ルールをクリックします。
2. メイン画面で、[SERVICE PROFILES] をクリックします。
3. [Partner Service] ドロップダウンリストから、[Trend Micro Deep Security] を選択します (選択されていない場合)。
4. サービスを追加して、次のフィールドに情報を入力します。
   - サービスプロファイル名には、名前を指定します。例:dsva-service-profile-epp
   - [Service Profile Description] では、説明を入力します。例:Deep Security Service Profile for Endpoint Protection
   - [Vendor Template] では、[Default (EBT)] を選択します。このテンプレートは、Trend Micro Deep Securityサービスと同時にロードされました。

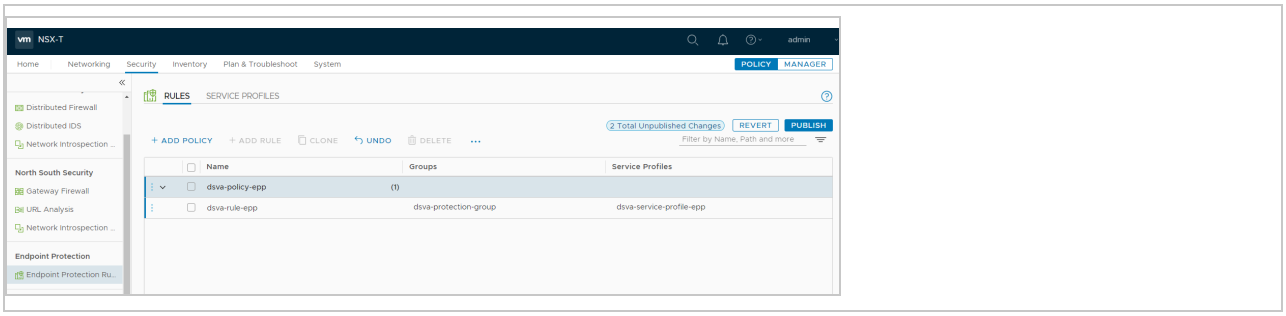


ADDSERVICE PROFILEページは次のようになります。



5. [SAVE] をクリックします。
6. メイン画面で[ルール]タブを選択し、+ポリシーを追加します。
7. 名前列で、新しいポリシーのセル内をクリックし、名前を変更します。たとえば、dsva-policy-eppを使用します。
8. dsva-policy-eppの横のチェックボックスをオンにして、+追加ルールをクリックします。dsva-policy-eppにルールが表示されます。
9. ルールに名前を付けて、対応するグループとサービスプロファイルを選択します。たとえば、ルールdsva-rule-eppに名前を付け、dsva-protection-group およびdsva-service-profile-eppを選択します。dsva-protection-groupのVMとdsva-service-profile-eppで指定されているDefault(EBT)テンプレートとの間にマッピングが作成されました。

ポリシーは次のようになります。



10. [PUBLISH] をクリックして、ポリシーとルールの作成を終了します。

    NSX-TでEndpoint Protectionを設定しました。

アクティベーションの設定

トピック:

- "アクティベーションの準備" below
- "アクティベーションおよびポリシーの割り当ての実行" on page 610
- "VMがアクティベートされ、ポリシーが割り当てられていることを確認する" on page 610

アクティベーションの準備

これでアクティベーションを準備する必要があります。次の方法を使用できます.1、2、または3:

- "方法1:作成された「コンピュータ作成済み」イベントベースのタスク" on the next page
- "方法2:「NSX Security Group Change」イベントベースのタスクを作成する" on page 606
- "方法3:Deep SecurityポリシーをNSX-T 3.xと同期する" on page 608に同期する

どの方法を選択するかわからないここで役立つ情報は次のとおりです。

- 一部のメソッドは一部のNSXバージョンではサポートされません。詳細については、次の表を参照してください。
- 方法1: この方法では、システムで新しく作成したVMが自動的にアクティベートされ、ポリシーが割り当てられます。
- 方法2: この方法では、指定されたNSXセキュリティグループに移動されると、新しいVMと既存のVMが自動的にアクティベートされ、ポリシーが割り当てられます。
- 方法3: この方法では、指定されたNSXセキュリティグループに移動されると、新しいVMと既存のVMがアクティベートされ、ポリシーが割り当てられます。詳細を表示この方法では、仮想マシンを指定されたNSXセキュリティグループに移動すると、新規および既存の仮想マシンが有効化され、ポリシーが割り当てられます。ただし、方法2とは異なり、Deep SecurityのポリシーはDeep Securityのイベントベースのタスクではなく、VMwareのUIを介して割り当てられます。

Deep Security Virtual Appliance環境									
	NSX for vSphere(NSX-V) 6.4.x								NSX-T 3.x
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	すべてのライセンスタイプ
方法1	✓	✓	✓	✓	✓	✓	✓	✓	✓
方法2	X	✓[1]	✓[1]	X	X	✓[1]	✓[1]	✓[1]	✓
方法3	X	✓[1]	✓[1]	X	X	✓[1]	✓[1]	✓[1]	✓

[1] VMwareのNetwork Introspection Serviceが必要です。

•には、次のソフトウェアの組み合わせが必要です: のDeep Security ManagerのFR 2019年12月12日(ビルド12.5.494) 以降のDeep Security AgentのLinuxのFR 2020年4月2日(とをビルド12.5.0-814) またはそれより新しい。

方法1: 作成された「コンピュータ作成済み」イベントベースのタスク

手順を展開する

次の手順はタスクベースです。イベントベースタスクに関する詳細については、"NSX環境での自動ポリシー管理" on page 639を参照してください。

1. Deep Security Managerで、上部にある[Administration]をクリックします。
2. 左側で、[イベントベースタスク] をクリックします。
3. メイン画面で、[新規] をクリックします。
4. [イベント] ドロップダウンリストから[コンピュータの作成 (システムによる)] を選択します。[次へ] をクリックします。
5. [コンピュータの有効化] を選択して5分に設定します。
6. [ポリシーの割り当て] を選択し、Windows Server 2016など、ドロップダウンリストからポリシーを選択します。矢印をクリックすると、子ポリシーを表示できます。[次へ] をクリックします。
7. イベントベースタスクがトリガされたときに制限する条件を指定します。次の条件を追加します。

   [vCenter名] が<ご使用のvCenter名>と一致する

8. イベントベースタスクがトリガされたときにさらに制限する条件を追加します。たとえば、すべてのWindows仮想マシンに接頭語「Windows」を含めるという命名規則を仮想マシンに使用している場合は、次のように設定します。

   [コンピュータ名] がWindows*と一致する

   [次へ] をクリックします。

9. [名前] フィールドで、Activate Windows Server 2016など、割り当てたポリシーを反映させるタスクの名前を入力します。
10. [タスクの有効化] を選択して[完了] をクリックします。
11. 割り当て時に計画したDeep Securityポリシーごとに追加のイベントベースタスクを作成します。イベントベースタスクのイベントタイプには [コンピュータの作成 (システムによる)] を指定し、コンピュータを有効化してポリシーの割り当てを実行できるように設定する必要があります。

    新しく作成した仮想マシンを有効化してポリシーを割り当てられるようにイベントベースタスクを設定しました。仮想マシンが作成されるとすぐに、[コンピュータの作成 (システムによる)] イベントベースタスクのすべてがレビューされます。タスクの条件が一致すると、タスクがトリガされます。また、仮想マシンが有効化され、関連するポリシーが割り当てられます。

方法2:「NSX Security Group Change」イベントベースのタスクを作成する

手順を展開する

次の手順はタスクベースです。イベントベースタスクに関する詳細については、"NSX環境での自動ポリシー管理" on page 639を参照してください。

開始するには、イベントベースのタスクアクティベーションを作成または変更します。

1. Deep Security Managerで、上部にある[Administration]をクリックします。
2. 左側で、[イベントベースタスク] をクリックします。
3. メイン画面で、*<your_vCenter_name>*というイベントベースのタスクを探します。それは存在することもあれば存在しないこともあります。
4. アクティベーションのイベントベースのタスクが存在する場合は、ダブルクリックして以下の表を確認して、正しく設定されていることを確認してください。存在しない場合は、新規をクリックしてウィザードを実行し、下の表を確認してください。
5. 複数のvCenter Serverをマネージャに追加した場合は、イベントベースのタスクをさらにアクティベーションできます。

注意: 次の表の設定は、表示順序とは異なる順序で表示されることがあります。

[Activate]イベントベースのタスクを設定するには、...を設定します。	To...
Name	アクションを反映するタスクの名前とConditionsに割り当てられたvCenter(例 : _vCenter_名>を有効にする) 。
イベント	NSXセキュリティグループの変更 NSXセキュリティグループの変更イベントは、マネージャがデータプレーンから通知を受信したときに実行されます(Deep Security Virtual Appliance).
タスクの有効化	有効です。
コンピュータの有効化	5
ポリシーの割り当て	ポリシー(例 : Windowsデスクトップ) 。矢印をクリックすると、下位ポリシーを表示できます。

[Activate]イベントベースのタスクを設定するには、...を設定します。	To...
条件	イベントベースのタスクが実行されたときに制限する必須条件: • [vCenter名] が<ご使用のvCenter名>と一致する トリガをさらに制限するためのオプションの条件の例: • [Appliance保護が利用可能] が [True] と一致する。 • [Appliance保護が有効化済み] が [False] と一致する。 • [NSXセキュリティグループ名] が.+ (任意を意味する) に一致する。

次に、イベントベースのタスク「非アクティブ化」を作成または変更します。

1. Deep Security Managerのメイン画面で、イベントベースの「*<your_vCenter_name>*を無効にするタスクを探してください。それは存在することもあれば存在しないこともあります。
2. イベントベースのタスク「非アクティブ化」が存在する場合は、ダブルクリックして以下の表を確認して、正しく設定されていることを確認してください。存在しない場合は、新規をクリックしてウィザードを実行し、下の表を確認してください。
3. 複数のvCenter Serverをマネージャに追加した場合は、イベントベースのタスクをさらに非アクティブ化に作成します。

注意: 次の表の設定は、表示順序とは異なる順序で表示されることがあります。

[Deactivate]イベントベースのタスクを設定するには、...を設定します。	To...
Name	アクションを反映するタスクの名前とConditionsで割り当てられたvCenter(例: _vCenter_名>を無効にする) 。
イベント	NSXセキュリティグループの変更 NSXセキュリティグループの変更イベントは、マネージャがデータプレーンから通知を受信したときに実行されます(Deep

[Deactivate]イベントベースのタスクを設定するには、...を設定します。	To...
	Security Virtual Appliance).
タスクの有効化	有効です。
コンピュータを無効化します	有効です。
条件	• [Appliance保護が有効化済み] が [True] と一致しり。 • [NSXセキュリティグループ名] が^$ (なしを意味する) と一致する。 • [vCenter名] が<ご使用のvCenter名>と一致する

イベントベースのタスクを設定して、VMをアクティベートします。タスクの条件が満たされると、タスクが実行され、VMがアクティベートされます(関連付けられたポリシー).が割り当てられます) 。

方法3: Deep SecurityポリシーをNSX-T 3.xと同期する

手順を展開する

次の手順はタスクベースです。ポリシー同期の詳細については、"Deep Securityポリシーの NSXとの同期" on page 644を参照してください。

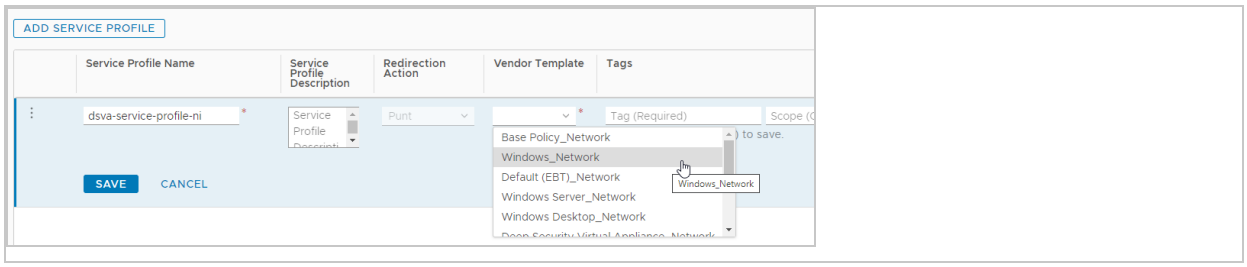
開始するには、Deep Security Managerを設定します。

1. Deep Security Managerにログインします。
2. Deep Security ManagerをNSXと同期するには、すべてのポリシーの名前が一意であることを確認します。初期設定のすべてのポリシーに一意の名前を指定します。
3. 画面上部の [コンピュータ] をクリックします。
4. 左側で、同期を有効にするvCenterを右クリックして [プロパティ] を選択します。
5. [NSX設定] タブで、[Deep SecurityポリシーとNSXサービスプロファイルの同期] を選択します。[OK] をクリックします。

次に、ポリシーがNSX-T Managerにロードされていることを確認します。

---

1. NSX-T Managerで、上部のセキュリティをクリックし、POLICYモードに切り替えます。
2. 左側にある[設定]を見つけ、ネットワークイントロスペクション設定をクリックします。
3. メイン画面で[サービス]をクリックし、パートナーサービスのドロップダウンリストからを選択します。Trend Micro Deep Securityを参照してください。
4. サービスを追加します。
5. ベンダーテンプレートドロップダウンリストを確認します。Deep Securityポリシーは<Deep_Security_Policy_Name>_Networkの形式でこのリストに表示されます。
6. これで、ポリシーがロードされていることを確認できました。
7. メイン画面に戻るには、キャンセルをクリックしてください。



Deep SecurityポリシーをNSXのベンダーテンプレートとして追加しました。

最後に、east-westセキュリティとEndpoint Protectionを再設定します。

1. "グループを作成して保護する" on page 595し、手順をもう一度実行してグループをさらに作成してください。例：Windows_Group。
2. "東西のセキュリティを設定する" on page 597し、手順をもう一度実行してください。今回はベンダーテンプレートからDeep Securityポリシーを1つ選択してください。>(初期設定(EBT)_ネットワーク)ではなく)、新しいグループの1つを選択します。
3. "Endpoint Protectionの設定" on page 601に戻り、手順をもう一度実行します。今回は、ベンダテンプレートからDeep Securityポリシーのいずれかを選択します(初期設定(EBT)ではなく新しいグループのいずれかを選択してください。ポリシーとグループは、east-westセキュリティの用途に一致する必要があります。

   警告：特定のグループに対してEast-West SecurityとEndpoint Protectionのテンプレートが一致していることを確認してください。たとえば、east-westセキュリティでMyWindowsPolicy_Networkを選択した場合は、[Endpoint Protection]でMyWindowsPolicyを選択します。

   これで、ポリシーの同期が設定され、既存および新しく作成されたVMをアクティベートすることができます。

アクティベーションおよびポリシーの割り当ての実行

仮想マシンの有効化とポリシーの割り当ての準備が完了しました。

- 方法1を選択した場合は、vCenterを手動で同期する必要があります。Deep Security Managerに移動し、左側のvCenterを右クリックして、[同期]を選択します。これで、既存の仮想マシンが保護されました。
- 方法2または3を選択した場合、すべてのVMをアクティベートし、ポリシーを自動的に割り当てる必要があります。確認するには、次の手順を参照してください。

VMがアクティベートされ、ポリシーが割り当てられていることを確認する

VMがアクティベートされ、ポリシーが正常に割り当てられたことを確認する必要があります。

確認するには

1. Deep Security Managerで、上部の[コンピュータ]をクリックします。
2. 左側で、[コンピュータ]→[<ご使用のvCenter>]→[仮想マシン]を選択します。
3. [タスク]列および[ステータス]列を確認します。(列が表示されていない場合は、上部で[列]をクリックして追加します)。[タスク]列に[有効化中]と表示され、仮想マシンのステータスが[非管理対象(不明)]から[非管理対象(Agentなし)]や[管理対象(オンライン)]に変わります。仮想マシンのステータスが[VMware Toolsがインストールされていない]になることがありますが、これは一時的です。
4. [POLICY]列で、正しいDeep Securityポリシーが割り当てられていることを確認します。

これで、Deep Security Virtual Applianceが配置され、VMが保護されました。

次の手順(新しい仮想マシンを追加する方法)

アプライアンスを配信したら、新しいVMを追加する必要があります。

次の手順に従って、新しいVMをシステムに追加してDeep Securityで保護する方法を確認してください。

方法1を選択した場合、新しいVMを追加するには(「コンピュータ作成」のイベントベースのタスク):を作成します。

- vCenterで新しい仮想マシンを作成します。これにより、[コンピュータの作成(システムによる)]イベントベースタスクが開始し、新しい仮想マシンの有効化およびポリシーの割り当てが行われます。

方法2を選択した場合に新しいVMを追加するには、次の手順に従います(「NSX Security Group Change」イベントベースのタスク):を作成します)。

- 仮想マシンを作成するか、仮想マシンをNSXセキュリティグループのいずれかに移動します。これにより、[NSXセキュリティグループの変更] イベントベースタスクが開始し、新しい仮想マシンの有効化およびポリシーの割り当てが行われます。

方法3を選択した場合に新しいVMを追加するには(Deep SecurityポリシーをNSX):と同期します)

- 仮想マシンを作成するか、仮想マシンをNSXセキュリティグループのいずれかに移動します。これにより、新しい仮想マシンを有効化してポリシーが割り当てられます。

Applianceのインストール (NSX-V)

"アプライアンスを配信する前に" on page 573のタスクを完了したら、NSX Data Center for vSphere (NSX-V).) にアプライアンスを配信する準備ができました。以下の手順に従ってください。

- "手順1: Deep Security Managerにアプライアンスパッケージをインポートします。" on the next pageにインポートします。
- "手順2: Deep Security ManagerにvCenterを追加する" on the next page
- "手順3: ESXiサーバの準備" on page 613
- "手順4: Guest Introspectionをインストールする" on page 614
- "手順5: Deep Security Virtual ApplianceをNSX-Vにインストールする" on page 618
- "手順6: NSXセキュリティグループとポリシーを作成する" on page 619
- "手順7: NSX-Vで有効化を準備する" on page 627
- "手順8: 有効化とポリシーの割り当てを開始する" on page 634
- "手順9: 仮想マシンが有効化されて、ポリシーが割り当てられていることを確認する" on page 634
- "次の手順 (新しい仮想マシンを追加する方法)" on page 634

新しいOSの脆弱性から保護するために"Applianceをアップグレードする" on page 1688することもできます。

手順1: Deep Security Managerにアプライアンスパッケージをインポートします。

"アプライアンスを配信する前に" on page 573のタスクを完了したら、アプライアンスZIPをDeep Security Managerにインポートする準備ができました。

ヒント: アプライアンスのZIPをインポートする代わりに、OVFファイルをURLの場所に配置して、NSXがより高速にダウンロードできるようにすることもできます。詳細については、"アプライアンスのOVFの場所を設定する" on page 650を参照してください。

1. 移動先:

   https://help.deepsecurity.trendmicro.com/ja-jp/software.html

2. Deep Security Virtual Applianceパッケージをダウンロードします。システム要件のバージョン要件を確認してください。

   複数バージョンのアプライアンスをインポートできます。マネージャは、最新のパッケージを選択します。

3. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]→[ローカル]に進みます。

4. [インポート]をクリックして、パッケージをDeep Security Managerにアップロードします。

   インポート時、Deep Security Managerはも仮想アプライアンスVMのOSと互換性のあるエージェントを自動的にダウンロードおよびインポートします。このエージェントには、Deep Security Agent for 64ビットRed Hat Enterprise Linuxと同じ保護モジュールがあります。

5. 別の組み込みエージェントを指定する場合は、管理> システム設定> アップデートにアクセスし、仮想アプライアンスの配信。初期設定では、仮想アプライアンスの配信オプションは最新のバージョン(推奨)に設定されています。これは、マネージャに、インポートされた最新の組み込みエージェントを使用するように仮想アプライアンスをアップグレードすることを示します。必要に応じて、この設定を変更します。

手順2: Deep Security ManagerにvCenterを追加する

"VMware vCenterの追加" on page 704の手順に従ってください。

完了後:

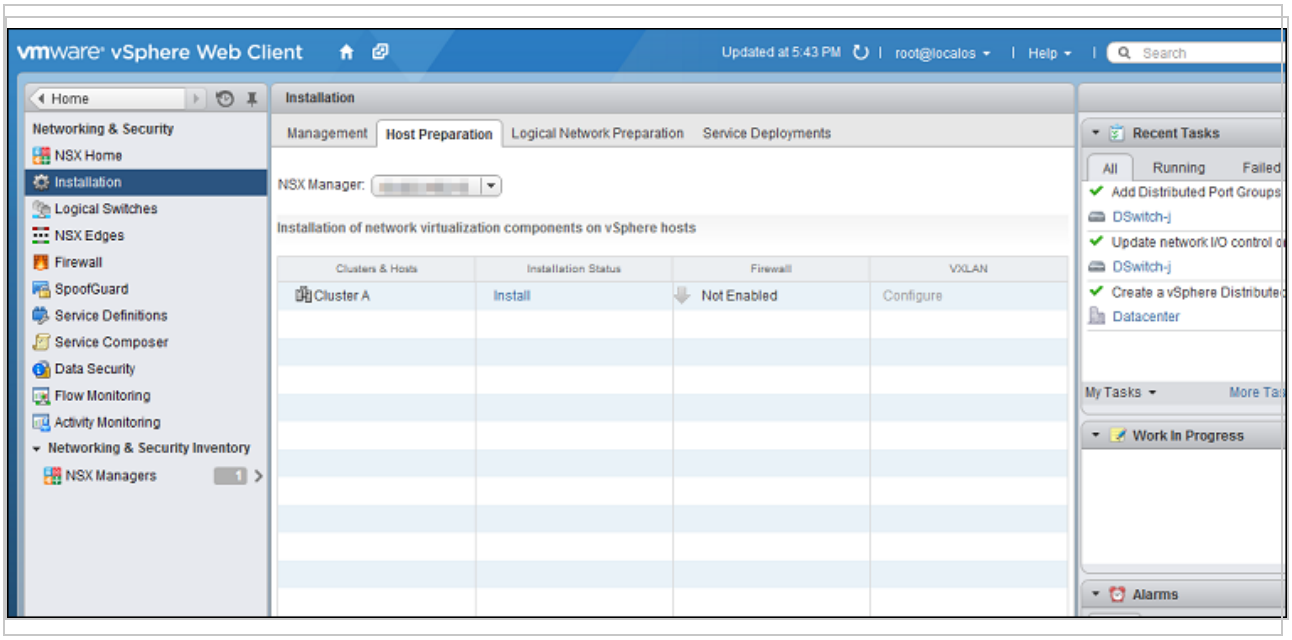
- ゲストVMがDeep Security Managerに表示されます。
- Trend Micro Deep SecurityサービスがNSX-Tに登録されています。

手順3: ESXiサーバの準備

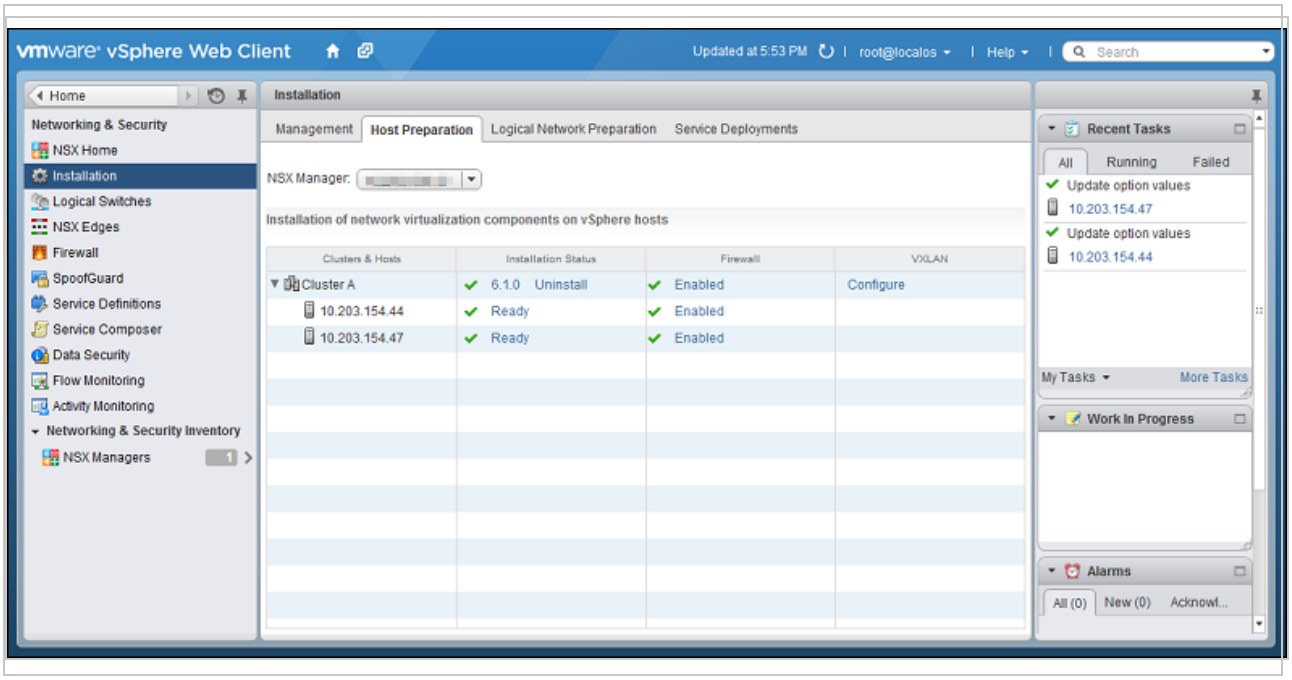
NSX Advanced EditionまたはNSX Enterprise Editionを使用する場合は、ネットワークトラフィックの監視に必要なドライバをインストールして、ESXiサーバを準備する必要があります。この処理はクラスタ上で実行します。

別のエディションのNSXを使用している場合は、このセクションをスキップしてください。

1. vSphere Web Clientで、[Home]→[Networking & Security]→[Installation]→[Host Preparation] の順に移動します。



2. Deep Securityで保護するNSXクラスタを [Clusters & Hosts] リストから見つけて、[Installation Status] 列で [Install] をクリックします。インストールが完了すると、ドライバのバージョンが [Installation Status] 列に表示されます。



以上でESXiホストの準備が完了しました。ホストの準備に関するより詳しい手順については、VMwareのドキュメントを参照してください。

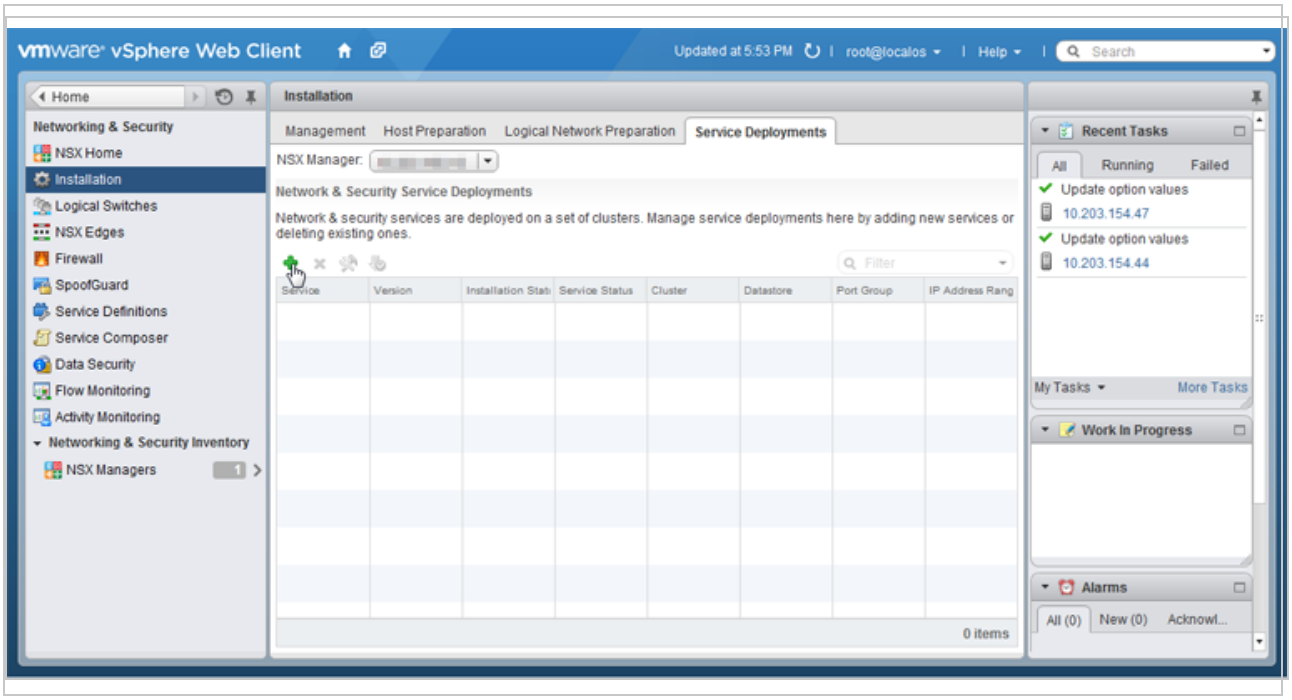
手順4: Guest Introspectionをインストールする

不正プログラム対策や侵入防御など、ファイルベースでの保護対策を仮想マシンに対して行うには、Guest Introspectionサービスを ESXiサーバにインストールする必要があります。

ゲストイントロスペクションサービスは、ファイルイントロスペクション(vsepflt) ドライバとネットワークイントロスペクション(vnetflt) ドライバの2つのドライバで構成されます。

警告: 不正プログラム対策および侵入防御は、Guest Introspectionをインストールしないと機能しません。

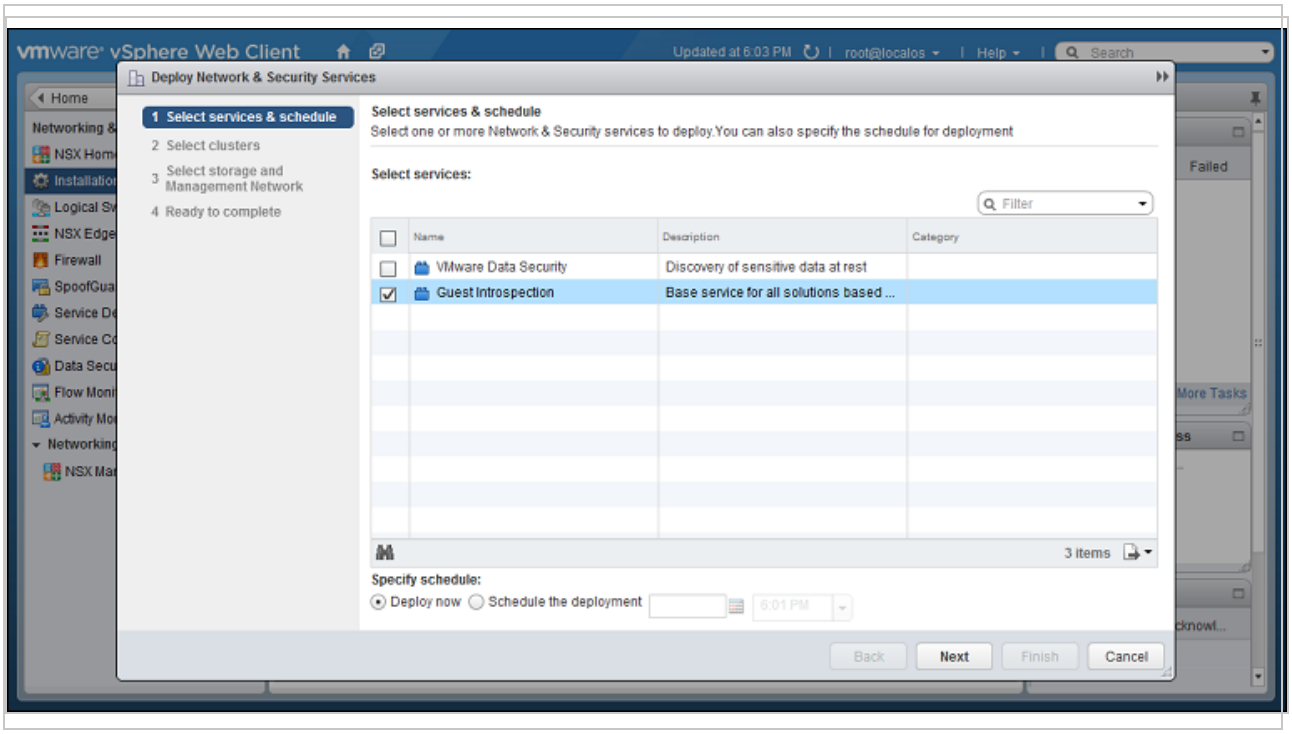
1. vSphere Web Clientで、[Home]→[Networking]→[Security]→[Installation] の順に選択し、[Service Deployments] タブをクリックします。



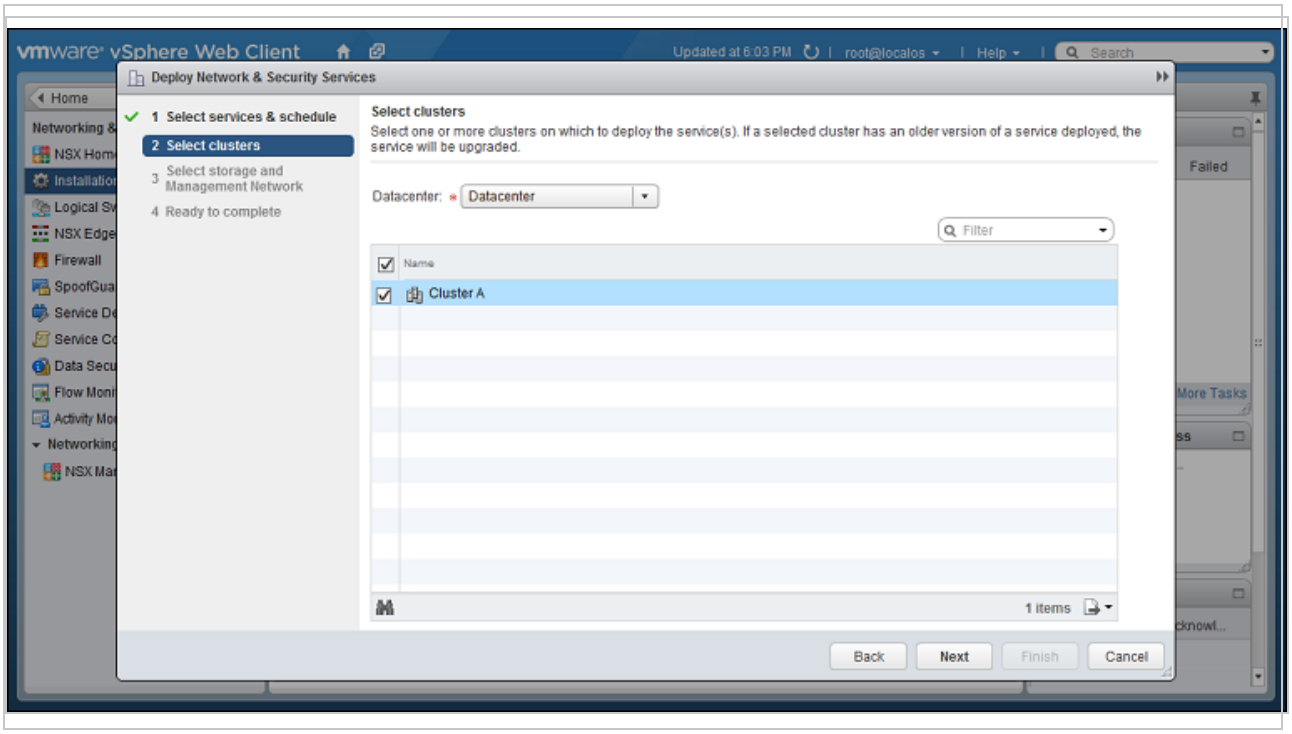
2. 緑色のプラスアイコン ( ) をクリックします。

   [Deploy Network & Security Services] 画面が表示されます。

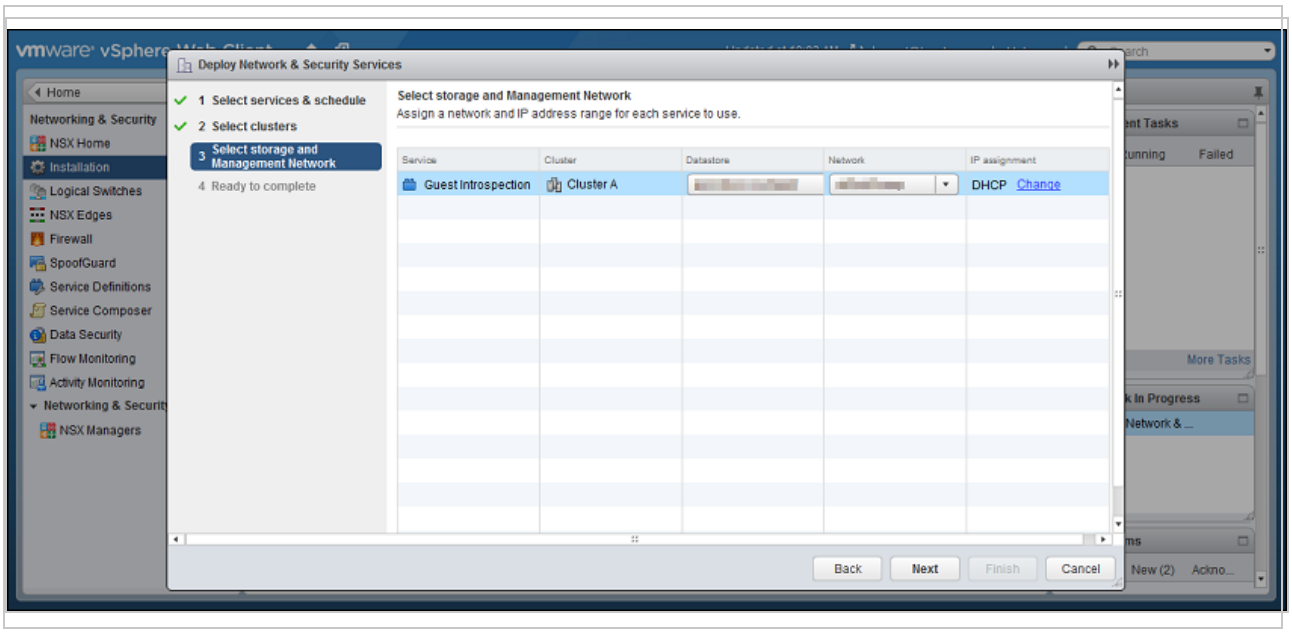
3. [Guest Introspection] を選択し、[Next] をクリックします。



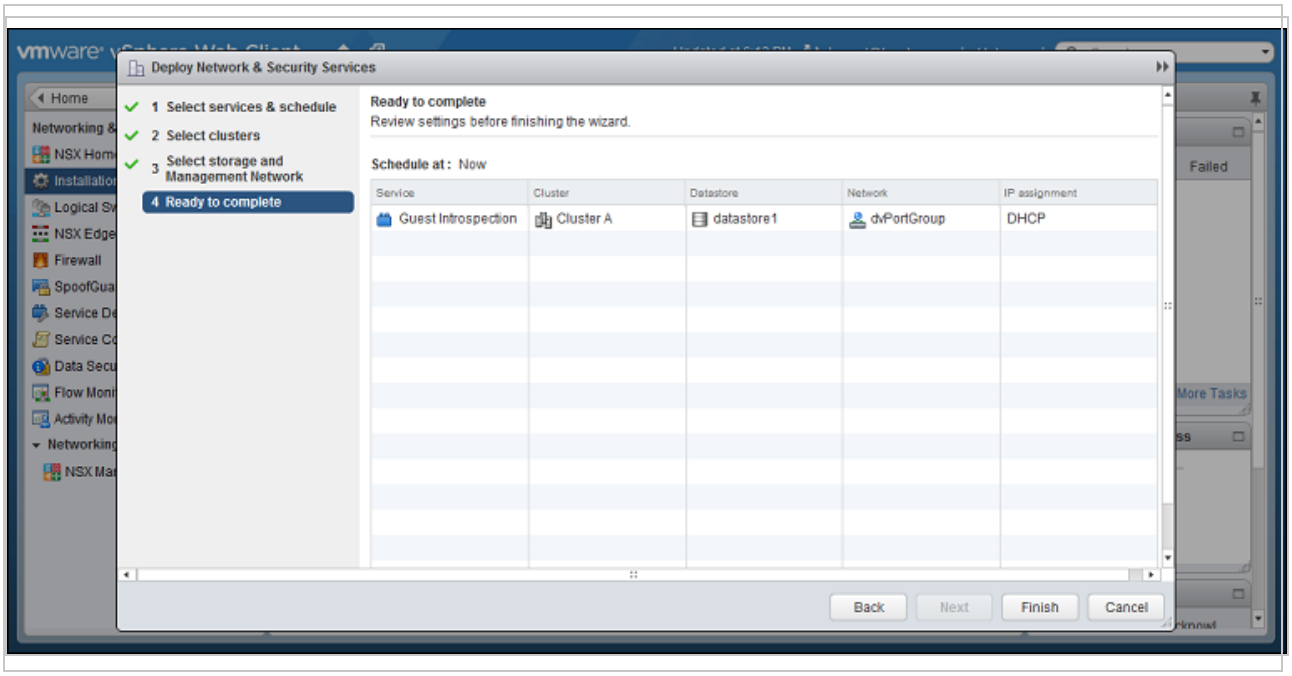
4. 保護するESXiサーバおよび仮想マシンを含むクラスタを選択し、[Next] をクリックします。



5. データストア、NSXクラスタで使用する分散ポートグループ、およびIP割り当ての方法を選択し、[Next] をクリックします。



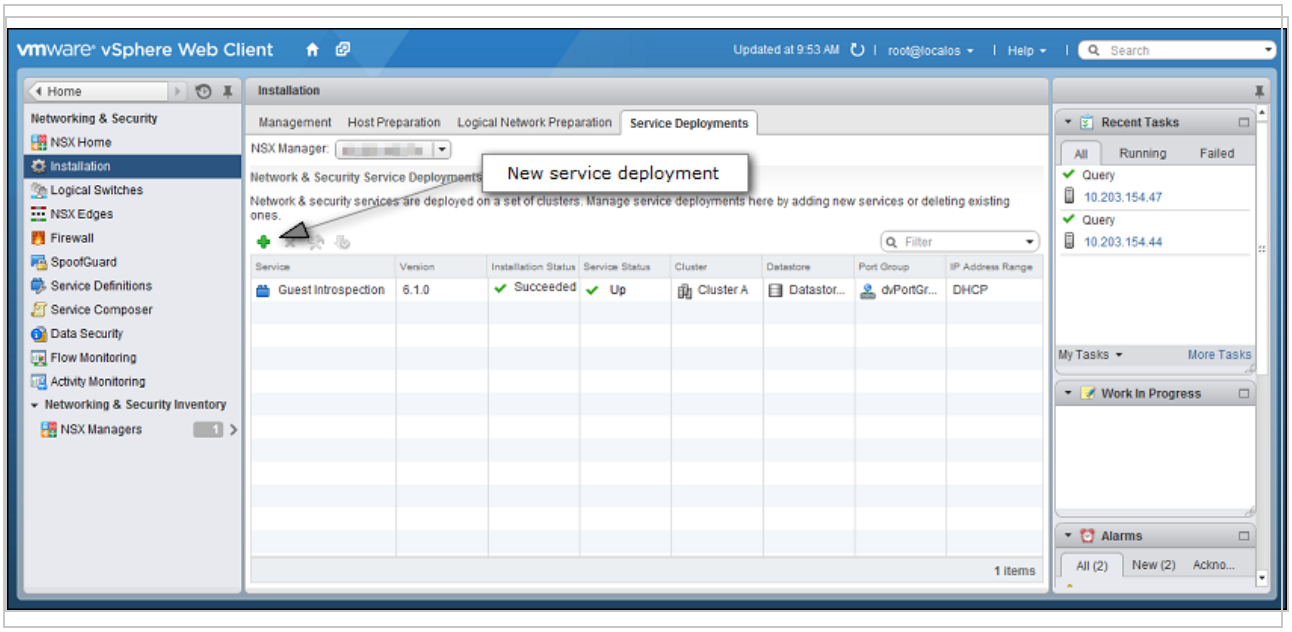
6. 設定を確認し、[Finish] をクリックします。



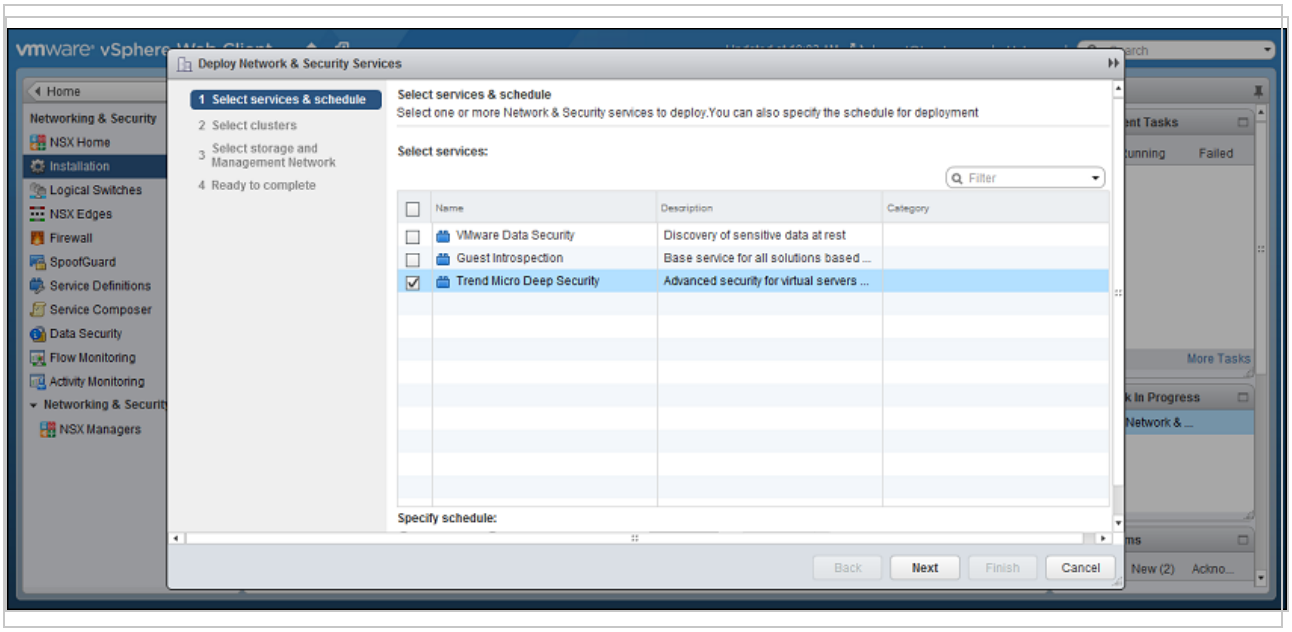
ESXiサーバにGuest Introspectionサービスがインストールされます。この処理には数分かかることがあります。完了すると、[Installation Status] が「Succeeded」になります。最新のステータスを表示するには、vSphere Web Client画面の更新が必要なことがあります。

手順5: Deep Security Virtual ApplianceをNSX-Vにインストールする

1. vSphere Web Clientで、[Home]→[Networking and Security]→[Installation]→[Service Deployments] の順に選択します。
2. 緑色のプラス記号 () をクリックします。

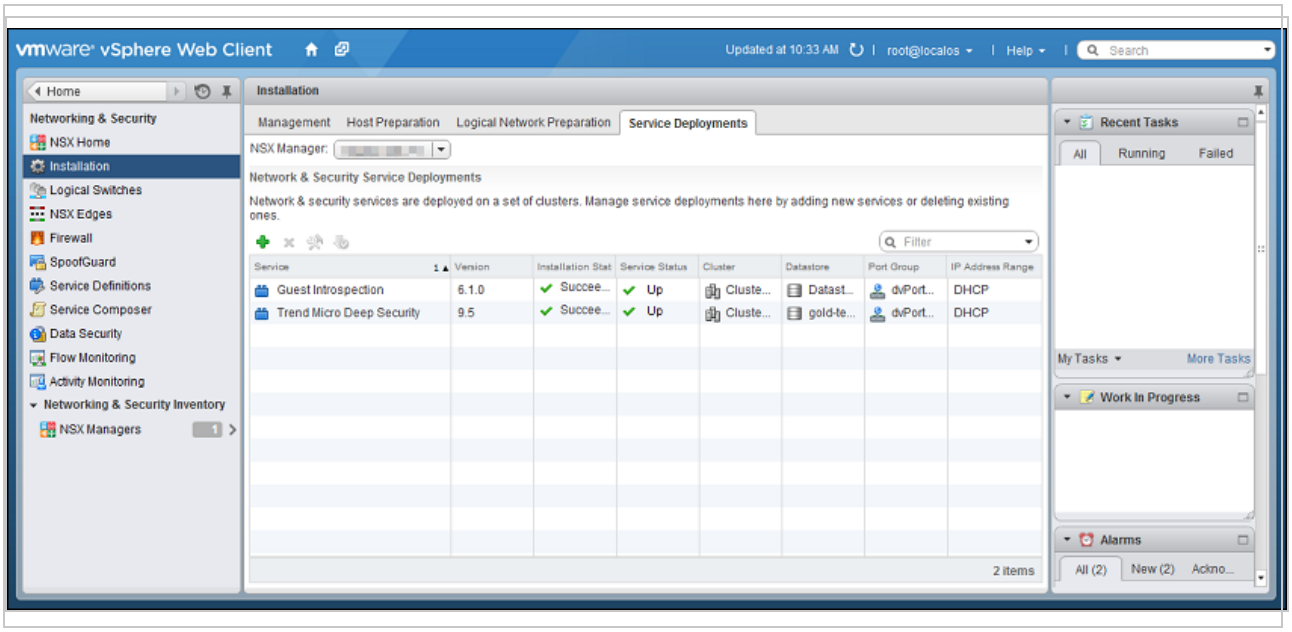


3. 表示された新しいウィンドウで、[Trend Micro Deep Security] サービスを選択し、[Next] をクリックします。このサービスが表示されない場合は、vCenterがDeep Security Managerにまだ追加されていない可能性があります。詳細については、"手順2: Deep Security ManagerにvCenterを追加する" on page 612を参照してください。



4. [完了] をクリックします。

   配信が完了すると、クラスタ内のネットワークとセキュリティサービスの配信のリストに、Trend Micro Deep Securityサービスが表示されます。

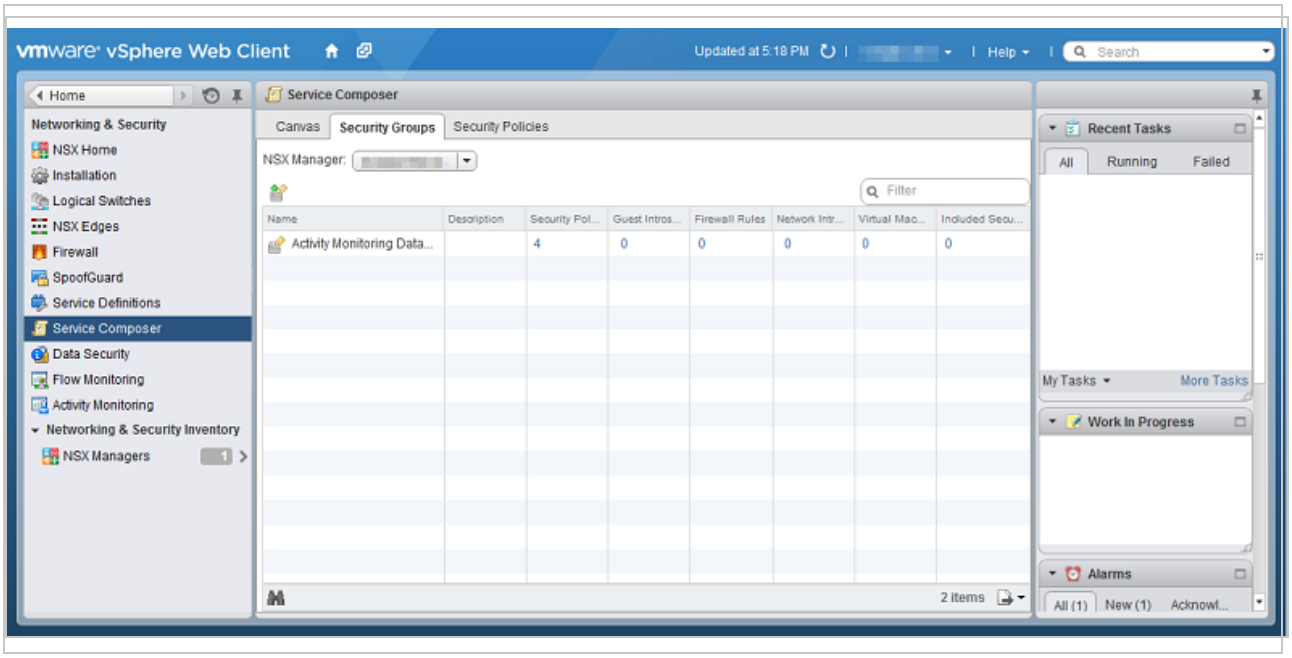


手順6: NSXセキュリティグループとポリシーを作成する

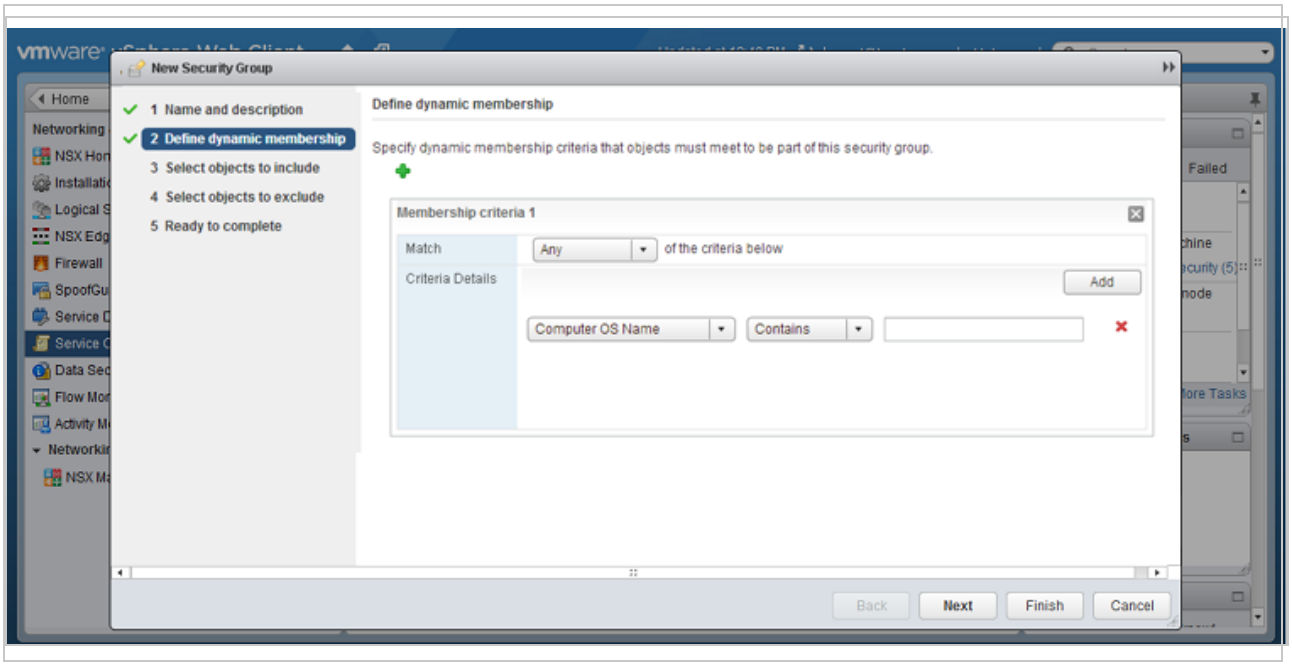
開始するには、Deep Security Virtual Applianceで保護する仮想マシンを含むNSXセキュリティグループを作成します。

1. vSphere Web Clientで、[Home]→[Networking & Security]→[Service Composer]→[Security Groups] の順に選択します。

2. [New Security Group] ( ) をクリックします。

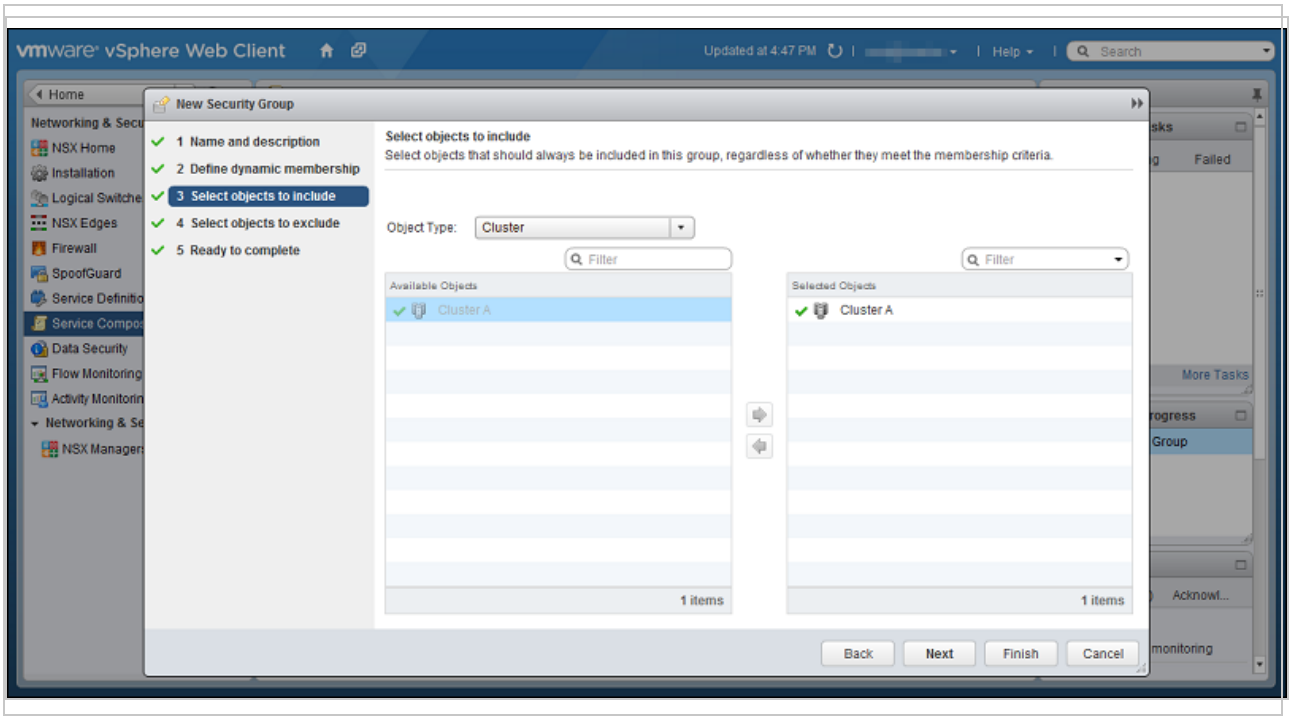


3. Define Dynamic Membership: このグループのメンバーシップを特定のフィルタ条件に基づいて制限する場合は、その条件を入力します。



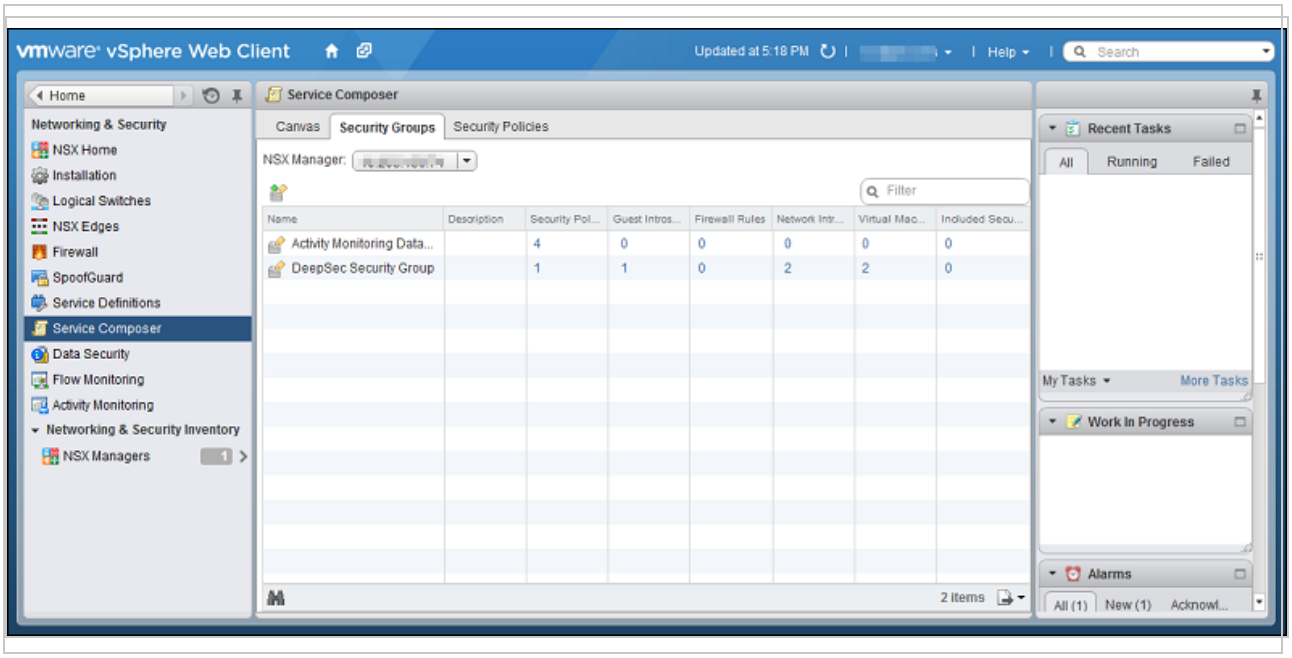
4. 含めるオブジェクトを選択します。

   NSXセキュリティグループのオブジェクトを追加または削除する方法は、多数あります。ここでは、保護対象のESXiホストと仮想マシンを含むNSXクラスタを追加します。[Select objects to include] のオプションで、[Object Type] メニューの [Cluster] を選択し、保護対象の仮想マシンを含むNSXクラスタを [Selected Objects] 列に移動します。



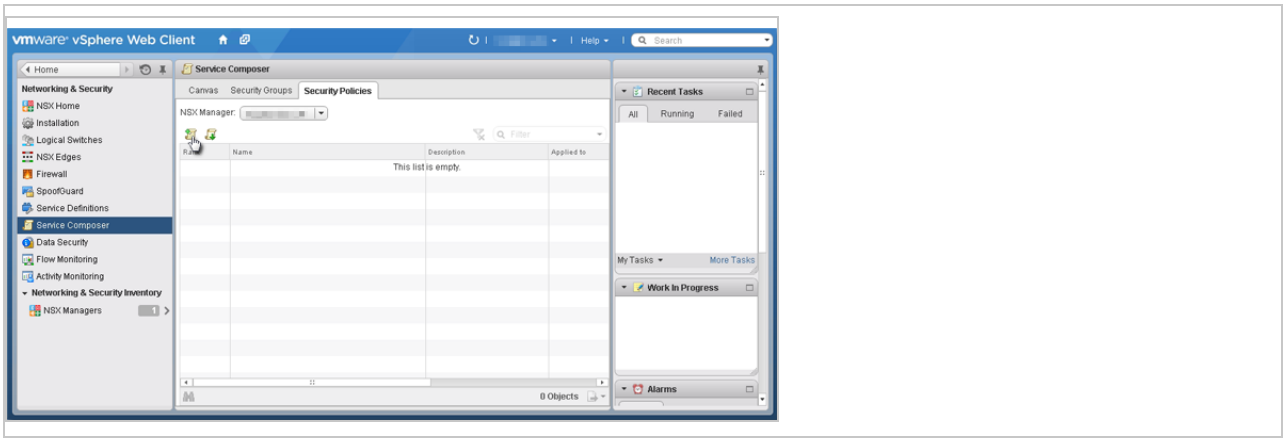
注意: VM が複数のセキュリティグループに含まれている場合、Deep Security Manager のコンピュータに移動して VM の名前を検索すると、検索結果に複数回表示されます。詳細については、ホストが複数の NSX セキュリティグループにある場合、コンピュータページに重複したホストレコードが表示される を参照してください。

5. [Finish] をクリックして新しいセキュリティグループを作成し、[Security Groups] タブに戻って新しいセキュリティグループが表示されることを確認します。



次に、NSXセキュリティポリシーを作成します。

1. vSphere Web Clientで、[Home]→[Networking and Security]→[Service Composer]→[Security Policies] の順に選択します。
2. [New Security Policy] をクリックします。

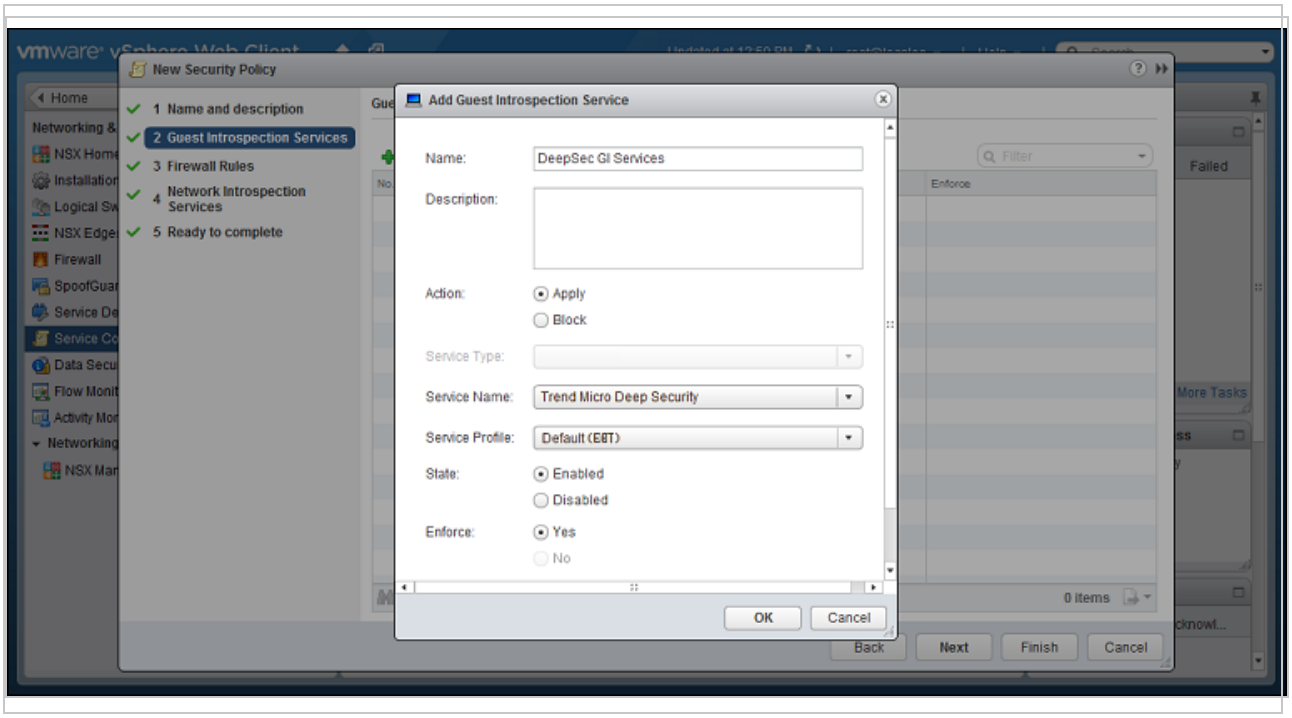


3. Guest Introspection Services: 不正プログラム対策または侵入防御モジュールを使用している場合は、Guest Introspection Servicesを設定します。

   警告: 不正プログラム対策および侵入防御は、Guest Introspectionをインストールしないと機能しません。

   緑色のプラス記号 () をクリックしてEndpointサービスを追加します。Endpointサービスの名前を指定し、次のように設定します。

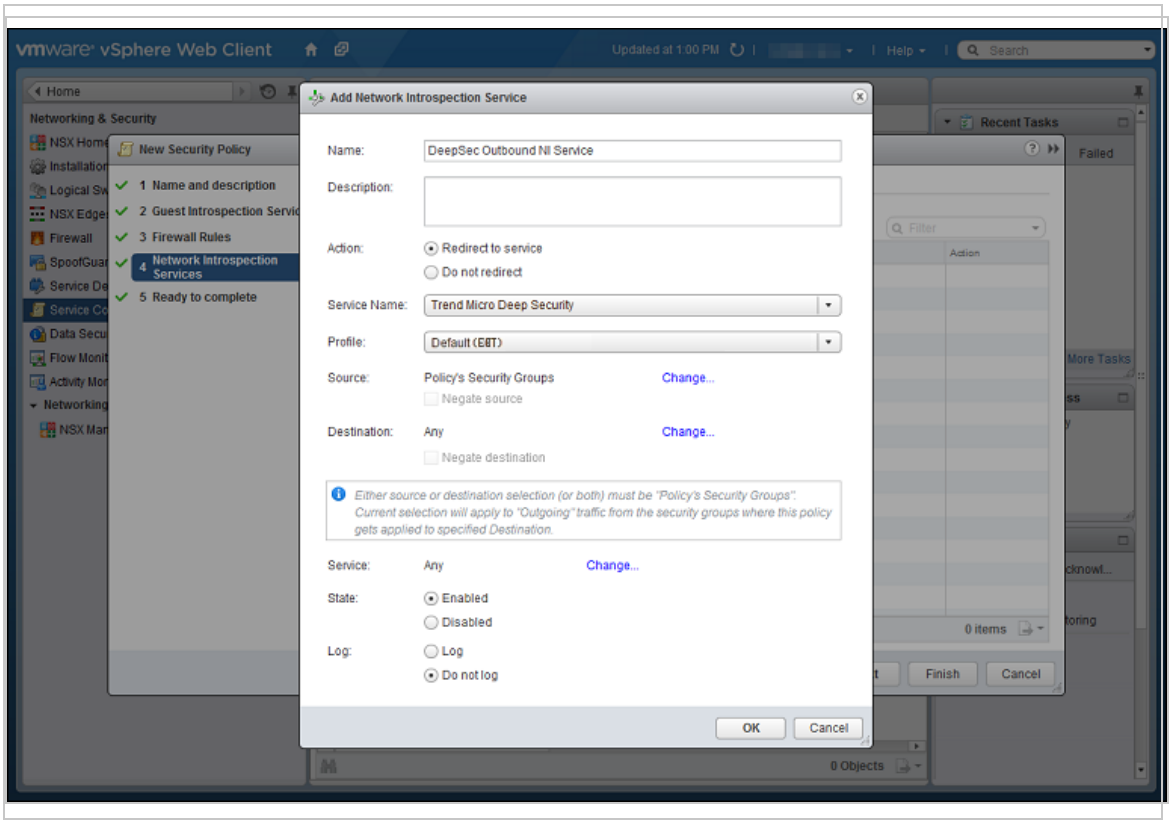
- Action: Apply
- Service Name: Trend Micro Deep Security
- サービスプロフィール: 初期設定 (EBT) を選択します。これは、Deep Security Managerでイベントベースのタスクを実行するように設定されたプロファイル設定です。
- State: Enabled
- Enforce: Yes



[OK] をクリックし、[Next] をクリックします。

4. Firewall Rules: この設定は変更しません。[次へ] をクリックします。
5. Network Introspection Services: Network Introspection ServicesはNSX AdvancedおよびEnterpriseでのみ利用可能で、Webレピュテーション、ファイアウォール、または侵入防御モジュールを使用している場合にのみ設定する必要があります。NSXセキュリティポリシーにNetwork Introspectionサービスを2つ追加します。1つは送信トラフィック用でもう1つは受信トラフィック用です。
   a. 最初に、送信用のサービスを追加します。[Network Introspection Services] オプションで、緑色のプラス記号をクリックして新しいサービスを作成します。[Add Network Introspection Service] 画面で、サービスの名前を指定し (「Outbound」という語句を含めることを推奨)、次のように設定します。

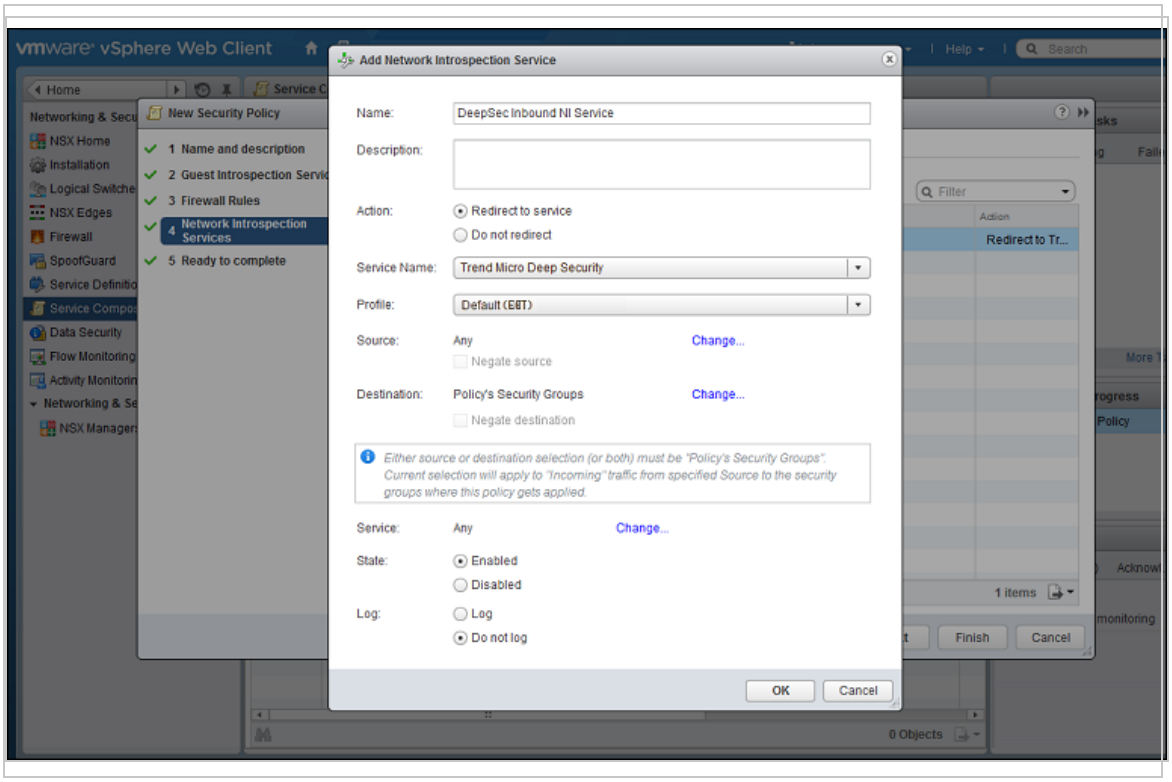
- Action: Redirect to service
- Service Name: Trend Micro Deep Security
- サービスプロフィール: 初期設定 (EBT) を選択する
- Source: Policy's Security Groups
- Destination:Any
- Service:Any
- State: Enabled
- Log: Do not log



b. 次に、受信用のサービスを追加します。[Network Introspection Services] オプションで、緑色のプラス記号をクリックして新しいサービスを作成します。[Add Network Introspection Service] 画面で、サービスの名前を指定し (「Inbound」という語句を含めることを推奨)、次のように設定します。

- サービスにリダイレクト: はい
- Service Name: Trend Micro Deep Security
- サービスプロフィール: 初期設定 (EBT) を選択する

- Source:Any
- Destination: Policy's Security Groups
- Service:Any
- State: Enabled
- Log: Do not log

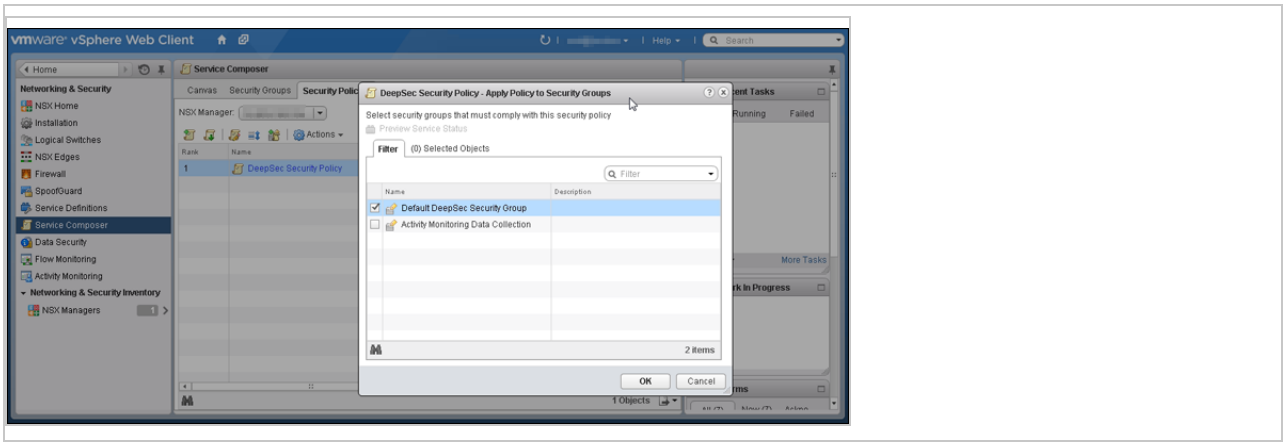


c. [Add Network Inspection Service] 画面で [OK] をクリックし、[Finish] をクリックして完了してから [New Security Policy] 画面を閉じます。

これで、Deep Security用のNSXセキュリティポリシーが作成されました。

最後に、作成したNSXセキュリティポリシーを、作成したNSXセキュリティグループに関連付けます。

1. 引き続き、vSphere Web Clientの [Home]→[Networking & Security]→[Service Composer] 画面の [Security Policies] タブを使用します。
2. 新しいセキュリティポリシーを選択した状態で、[Apply Security Policy] アイコン ( ) をクリックします。
3. [Apply Policy to Security Groups] 画面で、保護する仮想マシンが含まれているセキュリティグループを選択し、[OK] をクリックします。



これで、NSXセキュリティグループの仮想マシンにNSXセキュリティポリシーが適用されました。

これで、NSXセキュリティグループとポリシーの作成が完了しました。これらのNSXセキュリティグループに追加されたVMはDeep Security Managerでアクティベートされ、Deep Securityポリシーが割り当てられます。

手順7: NSX-Vで有効化を準備する

アクティベーションを準備するには、方法1,2、または3を使用できます。

- "方法1:「コンピュータの作成」イベントベースタスクを作成する" on page 629
- "方法2:「NSXセキュリティグループの変更」イベントベースタスクを作成する" on page 630
- "方法3: Deep SecurityポリシーをNSX-Vと同期する" on page 632に同期する

どの方法を選択するかわからないここで役立つ情報は次のとおりです。

- 一部のメソッドは一部のNSXバージョンではサポートされません。詳細については、次の表を参照してください。
- 方法1: この方法では、システムで新しく作成したVMが自動的にアクティベートされ、ポリシーが割り当てられます。
- 方法2: この方法では、指定されたNSXセキュリティグループに移動されると、新しいVMと既存のVMが自動的にアクティベートされ、ポリシーが割り当てられます。
- 方法3: この方法では、指定されたNSXセキュリティグループに移動されると、新しいVMと既存のVMがアクティベートされ、ポリシーが割り当てられます。詳細を表示 この方法では、仮想マシンを指定されたNSXセキュリティグループに移動すると、新規および既存の仮想マシンが有効化され、ポリシーが割り当てられます。ただし、方法2とは異な

り、Deep SecurityのポリシーはDeep Securityのイベントベースのタスクではなく、VMwareのUIを介して割り当てられます。

Deep Security Virtual Appliance環境									
	NSX for vSphere(NSX-V) 6.4.x								NSX-T 3.x
方法	標準 または NSX for vShield Endpoint (無料)	詳細	Enterprise	NSX Data Center Standard	NSX Data Center Professional	NSX Data Center Advanced	NSX Data Center Enterprise Plus	NSX Data Center for Remote Office Branch Office	すべてのライセンスタイプ
方法1	✓	✓	✓	✓	✓	✓	✓	✓	✓
方法2	X	✓[1]	✓[1]	X	X	✓[1]	✓[1]	✓[1]	✓
方法3	X	✓[1]	✓[1]	X	X	✓[1]	✓[1]	✓[1]	✓

[1] VMwareのNetwork Introspection Serviceが必要です。

•には、次のソフトウェアの組み合わせが必要です: のDeep Security ManagerのFR 2019年12月12日(ビルド12.5.494) 以降のDeep Security AgentのLinuxのFR 2020年4月2日(とをビルド12.5.0-814) またはそれより新しい。

方法1:「コンピュータの作成」イベントベースタスクを作成する

手順を展開する

次の手順はタスクベースです。イベントベースタスクに関する詳細については、"NSX環境での自動ポリシー管理" on page 639を参照してください。

1. Deep Security Managerで、上部にある[Administration]をクリックします。
2. 左側で、[イベントベースタスク] をクリックします。
3. メイン画面で、[新規] をクリックします。
4. [イベント] ドロップダウンリストから[コンピュータの作成 (システムによる)] を選択します。[次へ] をクリックします。
5. [コンピュータの有効化] を選択して5分に設定します。
6. [ポリシーの割り当て] を選択し、Windows Server 2016など、ドロップダウンリストからポリシーを選択します。矢印をクリックすると、子ポリシーを表示できます。[次へ] をクリックします。
7. イベントベースタスクがトリガされたときに制限する条件を指定します。次の条件を追加します。

   [vCenter名] が<ご使用のvCenter名>と一致する

8. イベントベースタスクがトリガされたときにさらに制限する条件を追加します。たとえば、すべてのWindows仮想マシンに接頭語「Windows」を含めるという命名規則を仮想マシンに使用している場合は、次のように設定します。

   [コンピュータ名] がWindows*と一致する

   [次へ] をクリックします。

9. [名前] フィールドで、Activate Windows Server 2016など、割り当てたポリシーを反映させるタスクの名前を入力します。
10. [タスクの有効化] を選択して[完了] をクリックします。
11. 割り当て時に計画したDeep Securityポリシーごとに追加のイベントベースタスクを作成します。イベントベースタスクのイベントタイプには [コンピュータの作成 (システムによる)] を指定し、コンピュータを有効化してポリシーの割り当てを実行できるように設定する必要があります。

    新しく作成した仮想マシンを有効化してポリシーを割り当てられるようにイベントベースタスクを設定しました。仮想マシンが作成されるとすぐに、[コンピュータの作成 (システムによる)] イベントベースタスクのすべてがレビューされます。タスクの条件が一致すると、タ

スクがトリガされます。また、仮想マシンが有効化され、関連するポリシーが割り当てられます。

方法2:「NSXセキュリティグループの変更」イベントベースタスクを作成する

手順を展開する

次の手順はタスクベースです。イベントベースタスクに関する詳細については、"NSX環境での自動ポリシー管理" on page 639を参照してください。

開始するには、イベントベースのタスクアクティベーションを作成または変更します。

1. Deep Security Managerで、上部にある[Administration]をクリックします。
2. 左側で、[イベントベースタスク] をクリックします。
3. メイン画面で、*<your_vCenter_name>*というイベントベースのタスクを探します。それは存在することもあれば存在しないこともあります。
4. アクティベーションのイベントベースのタスクが存在する場合は、ダブルクリックして以下の表を確認して、正しく設定されていることを確認してください。存在しない場合は、新規をクリックしてウィザードを実行し、下の表を確認してください。
5. 複数のvCenter Serverをマネージャに追加した場合は、イベントベースのタスクをさらにアクティベーションできます。

注意: 次の表の設定は、表示順序とは異なる順序で表示されることがあります。

[Activate]イベントベースのタスクを設定するには、...を設定します。	To...
Name	アクションを反映するタスクの名前とConditionsに割り当てられたvCenter(例 : _vCenter_名>を有効にする) 。
イベント	NSXセキュリティグループの変更 NSXセキュリティグループの変更イベントは、マネージャがデータプレーンから通知を受信したときに実行されます(Deep Security Virtual Appliance).
タスクの有効化	有効です。

[Activate]イベントベースのタスクを設定するには、...を設定します。	To...
コンピュータの有効化	5
ポリシーの割り当て	ポリシー(例 : Windowsデスクトップ) 。矢印をクリックすると、下位ポリシーを表示できます。
条件	イベントベースのタスクが実行されたときに制限する必須条件 : • [vCenter名] が<ご使用のvCenter名>と一致する トリガをさらに制限するためのオプションの条件の例 : • [Appliance保護が利用可能] が [True] と一致する。 • [Appliance保護が有効化済み] が [False] と一致する。 • [NSXセキュリティグループ名] が.+ (任意を意味する) に一致する。

次に、イベントベースのタスク「非アクティブ化」を作成または変更します。

1. Deep Security Managerのメイン画面で、イベントベースの「*<your_vCenter_name>*を無効にするタスクを探してください。それは存在することもあれば存在しないこともあります。
2. イベントベースのタスク「非アクティブ化」が存在する場合は、ダブルクリックして以下の表を確認して、正しく設定されていることを確認してください。存在しない場合は、新規をクリックしてウィザードを実行し、下の表を確認してください。
3. 複数のvCenter Serverをマネージャに追加した場合は、イベントベースのタスクをさらに非アクティブ化に作成します。

注意 : 次の表の設定は、表示順序とは異なる順序で表示されることがあります。

[Deactivate]イベントベースのタスクを設定するには、...を設定します。	To...
Name	アクションを反映するタスクの名前とConditionsで割り当てられたvCenter(例 : _vCenter_名>を無効にする) 。

[Deactivate]イベントベースのタスクを設定するには、...を設定します。	To...
イベント	NSXセキュリティグループの変更 NSXセキュリティグループの変更イベントは、マネージャがデータプレーンから通知を受信したときに実行されます(Deep Security Virtual Appliance).
タスクの有効化	有効です。
コンピュータを無効化します	有効です。
条件	• [Appliance保護が有効化済み] が [True] と一致しり。 • [NSXセキュリティグループ名] が^$ (なしを意味する) と一致する。 • [vCenter名] が*<ご使用のvCenter名>*と一致する

イベントベースのタスクを設定して、VMをアクティベートします。タスクの条件が満たされると、タスクが実行され、VMがアクティベートされます(関連付けられたポリシー).が割り当てられます) 。

方法3: Deep SecurityポリシーをNSX-Vと同期する

手順を展開する

次の手順はタスクベースです。ポリシー同期の詳細については、"Deep Securityポリシーの NSXとの同期" on page 644を参照してください。

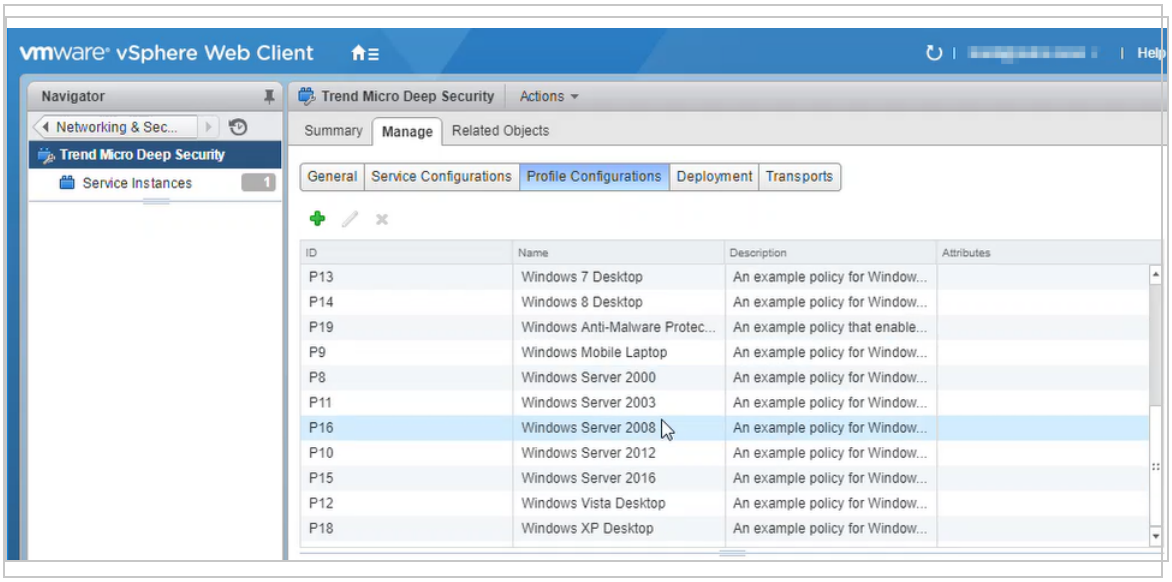
開始するには、Deep Security Managerを設定します。

1. Deep Security Managerにログインします。
2. Deep Security ManagerをNSXと同期するには、すべてのポリシーの名前が一意であることを確認します。初期設定のすべてのポリシーに一意の名前を指定します。
3. 画面上部の [コンピュータ] をクリックします。
4. 左側で、同期を有効にするvCenterを右クリックして [プロパティ] を選択します。

5. [NSX設定] タブで、[Deep SecurityポリシーとNSXサービスプロファイルの同期] を選択します。[OK] をクリックします。

次に、ポリシーがvSphereにロードされていることを確認します。

1. vSphere Web Clientのホームページで、[Networking & Security]ボタンをクリックします。[NSX Home] が表示されます。
2. 左側で、[Service Definitions] をクリックします。
3. メイン画面の [Services] タブで、[Trend Micro Deep Security] を右クリックして [Edit settings] を選択します。
4. メイン画面で、[Manage] タブを選択し、ここで [Profile Configurations] を選択します。
5. Deep Securityポリシーがロードされていることを確認します。ポリシーは、同じ名前を持つ個別のNSXプロファイル設定として表示されます。各プロファイル設定には、P1、P2、P3のような「P」から始まるIDを指定します。「P」はDeep Securityポリシーに基づいていることを示します。



これで、Deep SecurityポリシーがNSXのプロファイル設定として追加されました。

最後に、セキュリティグループとポリシーを再設定します。

1. "手順6:NSXセキュリティグループとポリシーを作成する" on page 619に戻り、手順をもう一度実行します。ただし、今回は残りの手順で調整を行います。
2. 複数のNSX セキュリティグループを作成します。
3. 複数のNSXセキュリティポリシーを作成します。ポリシーごとに、Guest Introspection ServicesおよびNetwork Introspection Services(受信および送信の両方) サービスプ

ロファイルを、ロードしたばかりのDeep Securityポリシーのいずれかに設定します。
4. NSXセキュリティポリシーをNSXセキュリティグループに関連付けます。

手順8: 有効化とポリシーの割り当てを開始する

仮想マシンの有効化とポリシーの割り当ての準備が完了しました。

- 方法1を選択した場合は、vCenterを手動で同期する必要があります。Deep Security Managerに移動し、左側のvCenterを右クリックして、[同期]を選択します。これで、既存の仮想マシンが保護されました。
- 方法2または3を選択した場合、すべてのVMをアクティベートし、ポリシーを自動的に割り当てる必要があります。確認するには、次の手順を参照してください。

手順9: 仮想マシンが有効化されて、ポリシーが割り当てられていることを確認する

確認するには

1. Deep Security Managerで、上部の[コンピュータ]をクリックします。
2. 左側で、[コンピュータ]→[<ご使用のvCenter>]→[仮想マシン]を選択します。
3. [タスク]列および[ステータス]列を確認します。(列が表示されていない場合は、上部で[列]をクリックして追加します)。[タスク]列に[有効化中]と表示され、仮想マシンのステータスが[非管理対象(不明)]から[非管理対象(Agentなし)]や[管理対象(オンライン)]に変わります。仮想マシンのステータスが[VMware Toolsがインストールされていない]になることがありますが、これは一時的です。
4. [POLICY]列で、正しいDeep Securityポリシーが割り当てられていることを確認します。

これで、Deep Security Virtual Applianceが配置され、VMが保護されました。

次の手順(新しい仮想マシンを追加する方法)

次の手順に従って、新しいVMをシステムに追加してDeep Securityで保護する方法を確認してください。

方法1を選択した場合、新しいVMを追加するには(「コンピュータ作成」のイベントベースのタスク):を作成します。

- vCenterで新しい仮想マシンを作成します。これにより、[コンピュータの作成 (システムによる)] イベントベースタスクが開始し、新しい仮想マシンの有効化およびポリシーの割り当てが行われます。

方法2を選択した場合に新しいVMを追加するには、次の手順に従います(「NSX Security Group Change」イベントベースのタスク):を作成します) 。

- 仮想マシンを作成するか、仮想マシンをNSXセキュリティグループのいずれかに移動します。これにより、[NSXセキュリティグループの変更] イベントベースタスクが開始し、新しい仮想マシンの有効化およびポリシーの割り当てが行われます。

方法3を選択した場合に新しいVMを追加するには(Deep Securityポリシーを NSX):と同期します)

- 仮想マシンを作成するか、仮想マシンをNSXセキュリティグループのいずれかに移動します。これにより、新しい仮想マシンを有効化してポリシーが割り当てられます。

vCloud環境にアプライアンスを配信する

VMware vCloudとの統合により、マルチテナントインストールのプライマリテナントは、Deep Security ManagerにvCenterを追加し、コネクタを設定し、Deep Security Virtual Applianceを配信および管理できます。その後、テナントはvCloud Organizationsをクラウドアカウントとしてインポートし、エージェントレスDeep Securityの保護を適用できます。

このトピックの内容:

- "開始前の準備" below
- "vCloud仮想マシンのAgentレスによる保護を有効にする" on the next page
- "マルチテナント環境を作成する" on the next page
- "vCenterを追加してDeep Security Virtual Applianceを配置する" on the next page
- "Deep SecurityでVMware vCloudリソースを使用できるように設定する" on the next page
- "仮想マシンでVirtual Appliance保護を有効にする" on page 638

開始前の準備

"アプライアンスを配信する前に" on page 573のタスクを完了してください。

vCloud仮想マシンのAgentレスによる保護を有効にする

1. Deep Security Managerコンソールで、[管理]→[システム設定]→[Agent] の順に選択します。
2. ApplianceによるvCloud仮想マシンの保護を許可チェックボックスをオンにします。
3. [保存] をクリックします。

マルチテナント環境を作成する

マルチテナント環境を作成するために必要なタスクは、主に2つあります。マルチテナントの有効化とテナントの作成です。これらのタスクの実施方法に関する詳細な手順、マルチテナント環境の要件と推奨事項については、"マルチテナント環境の設定" on page 478を参照してください。

vCenterを追加してDeep Security Virtual Applianceを配置する

プライマリテナントでvCenterを追加し、Deep Security Virtual Applianceを配置する必要があります。手順については、"アプライアンスを配信する(NSX-T 3.x) " on page 576または"Applianceのインストール (NSX-V)" on page 611) を参照してください。

Deep SecurityでVMware vCloudリソースを使用できるように設定する

Deep Securityとの統合のためのVMware vCloudリソースを設定するには

- vCloudアカウントのテナントユーザ向けの最小権限のロールを作成する
- "新しい仮想マシンに一意のUUIDを割り当てる" on the next page
- ゲスト仮想マシンでVMware Toolsの [OVF Environment Transport] を有効にする

vCloudアカウントのテナントユーザ向けの最小権限のロールを作成する

vCloud Directorで作成した、Deep Securityのテナントが Deep Security Managerにクラウドアカウントを追加するために使用するユーザアカウントには、の[すべての権限]→[一般]→[管理者ビュー権限]の権限のみが必要です。

1. vCloud Directorにログインします。
2. [System] タブで [Administration] をクリックします。
3. 左側のナビゲーションパネルで [Roles] をクリックします。
4. 「プラス」記号 (+) をクリックして新しいロール (「DS_User」など) を作成します。
5. [All Rights]→[General] フォルダの [Administrator View] 権限を選択します。
6. [OK] をクリックします。

これで、Deep Security ManagerにvCloudリソースをインポートするユーザアカウントにこの役割を割り当てることができます。

注意: Deep Securityのユーザにこの資格情報を提供する際は、vCloud OrganizationのIPアドレスも通知してください。また、vCloudのリソースをDeep Security Managerにインポートする際は、ユーザ名に「@orgName」を含めるように指示してください。たとえば、vCloudアカウントのユーザ名がuserで、アカウントのアクセス権を付与されたvCloud OrganizationがCloudOrgOneである場合、Deep Securityのユーザは、vCloudのリソースをインポートするときにユーザ名として「user@CloudOrgOne」と入力する必要があります。(vCloud管理者の場合、@systemを使用します)。

注意: クラウドアカウントで保護されているインスタンスへの接続にプロキシサーバを使用するよう、Deep Security Managerを設定できます。プロキシ設定は、[管理]→[システム設定]→[プロキシ]→[プロキシサーバの使用]→[Deep Security Manager (クラウドアカウント)] で行います。

新しい仮想マシンに一意のUUIDを割り当てる

Deep Securityでは、保護対象のすべての仮想マシンに一意のUUIDを割り当てる必要があります。vAppテンプレートから作成した仮想マシンにはUUIDを重複して割り当てることができるため、問題が発生する場合があります。固有のUUIDを割り当てるようにvCloudデータベースを設定するには、VMwareナレッジベースの記事2002506に従って、`CloneBiosUuidOnVmCopy` プロパティをゼロ(`0`) に設定します。

ゲスト仮想マシンでVMware Toolsの [OVF Environment Transport] を有効にする

ゲストVM上のVMware ToolsのOVF Environment Transportを有効にすると、guestInfo.ovfEnv 環境変数が公開され、エージェントはVMをDeep Security Managerに対して一意に識別できるようになります。これにより、仮想マシンの誤認リスクが低減されます。

1. vCloud Directorで、VMの[Properties] [ ]画面を開き、[Guest OS Customization]タブに移動し、の[Guest customization を有効にする]チェックボックスをオンにします。[OK] をクリックします。
2. vCenterで同じ仮想マシンを選択し、[Properties] 画面を開いて [Options] タブに進みます。
3. [vApp Options] をクリックし、[Enabled] オプションを選択します。これで [OVF Settings] が公開されます。
4. OVF Settingsで、OVF Environment Transport 領域の[VMware Tools]チェックボックスをオンにします。[OK] をクリックします。

仮想マシンが実行中の場合は、変更を有効にするために再起動する必要があります。

Deep Securityで使用されるデータは、プロパティvmware.guestinfo.ovfenv.vcenteridおよびvmware.guestinfo.ovfenv.vcloud.computernameから取得されます。

仮想マシンでVirtual Appliance保護を有効にする

仮想アプライアンスの保護を有効にするには、テナントがvCloud Organizationアカウントをインポートし、エージェントレスDeep Security保護を適用する必要があります。

注意: vCloud組織アカウントはテナント別に追加する必要があります(プライマリテナントではない).

VMware vCloud Organizationアカウントからコンピュータをインポートする

1. Deep Security Managerで、[コンピュータ] セクションに移動し、ナビゲーションパネルで [コンピュータ] を右クリックし、[vCloudアカウントの追加] を選択してvCloudアカウント追加ウィザードを開きます。
2. [名前] に表示名を、[説明] に追加メモを入力します。
3. [アドレス] にvCloud Directorのホスト名を入力します。
4. ユーザ名とパスワードを入力します。

   注意: ユーザ名は、username@vcloudorganizationの形式にします。
5. [次へ] をクリックします。
6. Deep Security Managerは、クラウドリソースへの接続を確認し、インポート処理の概要を表示します。[完了] をクリックします。

VMware vCloudのリソースが、Deep Security Managerのナビゲーションパネル内の [コンピュータ] の下に、それぞれ別個の項目として表示されます。

VMware vCloud Air仮想データセンターからコンピュータをインポートする

1. Deep Security Managerで、[コンピュータ] セクションに移動し、ナビゲーションパネルで [コンピュータ] を右クリックし、[vCloudアカウントの追加] を選択してvCloudアカウント追加ウィザードを開きます。
2. 追加するVMware vCloud Air仮想データセンターの名前と説明を入力します(Deep Security Managerでの表示に使用されます)。
3. VMware vCloud Air仮想データセンターのアドレスを入力します。

   VMware vCloud Air仮想データセンターのアドレスを確認するには、次の手順を実行します。

   a. VMware vCloud Airポータルにログインします。
   b. [Dashboard] タブで、Deep Securityにインポートするデータセンターをクリックします。[Virtual Data Center Details] 情報画面が表示されます。
   c. [Virtual Data Center Details] 画面の [Related Links] セクションで、[vCloud Director API URL] をクリックします。vCloud Director APIの完全なURLが表示されます。

   d. Deep SecurityにインポートするVMware vCloud Air仮想データセンターのアドレスとして、完全なURLのうちホスト名の部分だけを使用します。
4. ユーザ名とパスワードを入力します。

   注意: ユーザ名は、username@virtualdatacenteridの形式にします。

5. [次へ] をクリックします。
6. Deep Security Managerによって仮想データセンターへの接続が確認され、インポート処理の概要が表示されます。[完了] をクリックします。

VMware vCloud Airのデータセンターが、Deep Security Managerのナビゲーションパネル内の [コンピュータ] の下に、それぞれ別個の項目として表示されます。

仮想マシンでVirtual Appliance保護を有効にする

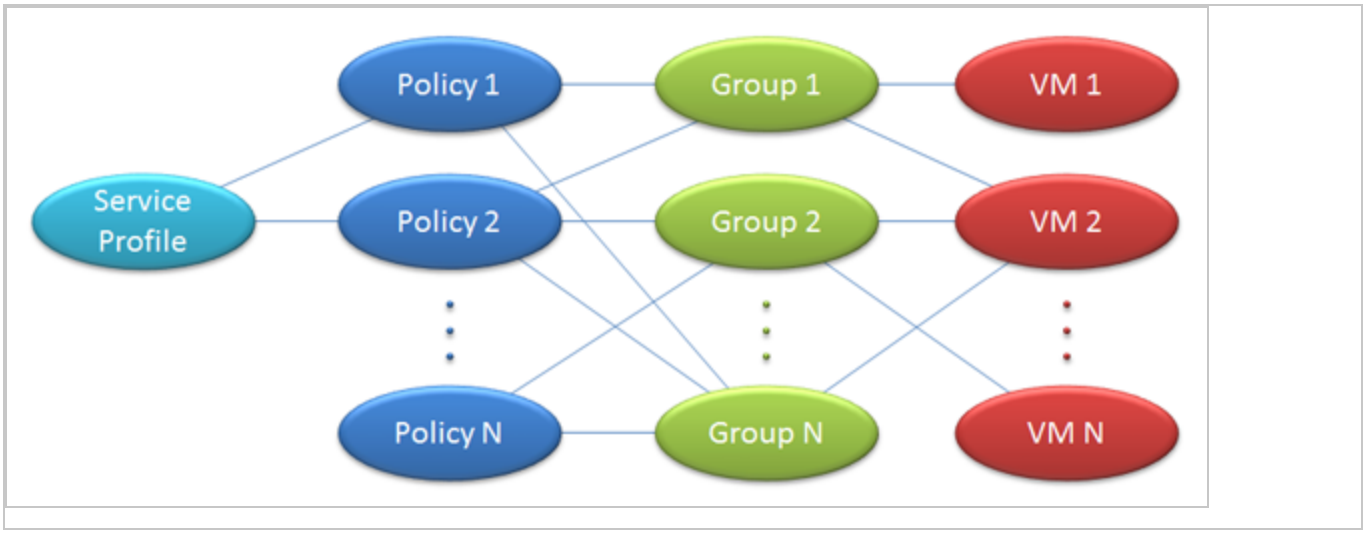
Virtual Appliance保護を有効にするには、[コンピュータ] リストで仮想マシンを右クリックし、[処理]→[有効化] をクリックします。

NSX環境での自動ポリシー管理

注意: NSXへのDeep Securityポリシーの同期を有効にしている場合は、NSXセキュリティグループの変更イベントベースタスクを使用する必要はありません。ポリシー同期の詳細については、"Deep SecurityポリシーのNSXとの同期" on page 644を参照してください。

NSX環境のVMのセキュリティ設定は、VMのNSXセキュリティグループの変更に基づいて自動的に変更できます。セキュリティ設定の自動化は、NSX Security Group Changeイベントベースのタスクを使用して実行されます。

仮想マシンはNSXセキュリティグループ、NSXセキュリティグループはNSXセキュリティポリシー、NSXセキュリティポリシーはNSXサービスプロファイルに、それぞれ関連付けられます。



「NSXセキュリティグループの変更」イベントベースタスク

Deep Securityには、特定の条件で特定のイベントが検出されたときに処理を実行するように設定できるイベントベースタスク(EBT)があります。NSXセキュリティグループの変更EBTを使用すると、仮想マシンが属しているNSXセキュリティグループへの変更が検出されたときに、その仮想マシンの保護設定を変更できます。

注意: NSXセキュリティグループの変更EBTは、Default (EBT) NSXサービスプロファイルに関連付けられたNSXセキュリティグループへの変更のみを検出します。同様に、1つの仮想マシンが複数のグループ/ポリシーに関連付けられている場合でも、Deep SecurityはDefault (EBT) NSXサービスプロファイルに関連付けられたグループとポリシーに関連する変更のみを監視およびレポートします。

このタスクを変更するには、Deep Security Managerで [管理]→[イベントベースタスク] に進みます。

NSXセキュリティグループの変更EBTは、次のいずれかのイベントが発生した場合に開始されます。

- Default (EBT) NSXサービスプロファイルに間接的に関連付けられたNSXグループに仮想マシンが追加された場合。
- Default (EBT) NSXサービスプロファイルに関連付けられたNSXグループから仮想マシンが削除された場合。
- Default (EBT) NSXサービスプロファイルに関連付けられたNSXポリシーがNSXグループに適用された場合。
- Default (EBT) NSXサービスプロファイルに関連付けられたNSXポリシーがNSXグループから削除された場合。
- NSXポリシーがDefault (EBT) NSXサービスプロファイルに関連付けられます。

- NSXポリシーがDefault (EBT) NSXサービスプロファイルから削除されます。
- Default (EBT) NSXサービスプロファイルに関連付けられたNSXグループの名前が変更された場合。

変更によって影響を受ける仮想マシンごとにイベントがトリガされます。

タスクを実行する条件

次の条件を「NSXセキュリティグループの変更」イベントベースタスクに適用して、処理を実行する前にテストすることができます。

- コンピュータ名: ゲスト仮想マシンのホスト名。
- ESXi名: ゲスト仮想マシンが実行されているESXiのホスト名。
- フォルダ名: ESXiフォルダ構造にあるゲスト仮想マシンのフォルダ名。
- NSXセキュリティグループ名: 変更されたNSXセキュリティグループの名前。
- プラットフォーム: ゲスト仮想マシンのOS。
- vCenter名: ゲスト仮想マシンが属するvCenterの名前。
- Appliance保護が利用可能: 仮想マシンがホストされているESXi上にDeep Security Virtual Applianceがあり、仮想マシンを保護できる。仮想マシンの状態が有効化済みになっているかどうかは問いません。
- Appliance保護が有効化済み: Deep Security Virtual Applianceを使用して、有効化されている仮想マシンをホストしているESXi上の仮想マシンを保護できます。
- 最後に使用されたIPアドレス: 仮想マシンコンピュータの現在の、または最後に確認されたIPアドレス。

これらの条件およびイベントベースタスクの概要については、"コンピュータの追加または変更時にタスクを自動的に実行する(イベントベースのタスク) " on page 1829を参照してください。

NSXセキュリティグループ名条件は、NSXセキュリティグループの変更イベントベースタスクへの変更に対するものです。

プロパティが変更された、仮想マシンが属しているNSXセキュリティグループに一致するJava正規表現を受け付けます。次の2つの特殊なケースがあります。

- いずれかのグループのメンバーシップに対する一致。この場合に推奨される正規表現は「+」です。
- グループのメンバーシップに対する不一致。この場合に推奨される正規表現は「^$」です。

他の正規表現としては、特定のグループ名または部分名 (複数のグループに一致) などがあります。

注意: この条件に適合する可能性のあるグループのリストには、Default (EBT) NSXサービスプロファイルのポリシーに関連付けられたグループのみが含まれます。

実行可能な処理

仮想マシンが属しているNSXセキュリティグループへの変更を検出したときに、仮想マシンに対して次の処理を実行できます。

- コンピュータの有効化: Deep Security Virtual Applianceによる保護を有効化します。この処理は、Deep Securityで保護されたNSXセキュリティグループに仮想マシンを移動した場合に使用します。
- コンピュータの無効化: Deep Security Virtual Applianceによる保護を無効化します。この処理は、Deep Securityで保護されたNSXセキュリティグループから仮想マシンを移動した場合に使用します。仮想マシンが保護されなくなるため、Deep Securityで保護されたNSXセキュリティグループから仮想マシンを移動したときにこの処理が実行されない場合は、アラートが発生します。
- ポリシーの割り当て: Deep Securityポリシーを仮想マシンに割り当てます。
- Relayグループの割り当て: Relayグループを仮想マシンに割り当てます。

vCenterがDeep Security Managerに追加されたときに作成されるイベントベースタスク

NSX Managerと連携したvCenterをDSMに追加したときに、2つのイベントベースタスクを作成できます。vCenterの追加ウィザードの最後の画面にチェックボックスが表示されます。オンにした場合、2つのイベントベースタスクが作成されます。1つは、保護が追加されたときに仮想マシンを有効化し、もう1つは、保護が削除されたときに仮想マシンを無効化します。

最初のイベントベースタスクは、次のように設定されます。

- 名前: <vCenter名>を有効化します。この<vCenter名>は、vCenterプロパティの[名前]フィールドに表示される値です。
- イベント: NSXセキュリティグループの変更
- タスクの有効化: True
- 処理: 5分間の遅延後にコンピュータを有効化します
- 条件:
  - vCenter名: EBTはvCenter固有のため、<vCenter名>が一致している必要があります。
  - Appliance保護が利用可能: True。有効化されたDeep Security Virtual Applianceが同じESXi上に配置されている必要があります。

- Appliance保護が有効化済み: False。無効化されている仮想マシンにのみ適用されます。
- NSXセキュリティグループ:「.+」。1つ以上のDeep Securityグループのメンバーである必要があります。

たとえばDeep Security保護ポリシーを適用したり、別のRelayグループを割り当てたりして、このイベントベースタスクに関連付けられた処理を変更できます。既存のイベントベースタスクの処理 (およびその他のプロパティ) は、Deep Security Managerの [管理]→[イベントベースタスク] 画面で編集できます。

2つ目のイベントベースタスクは、次のように設定されます。

- 名前: <vCenter名>を無効化します。この<vCenter名>は、vCenterプロパティの [名前] フィールドに表示される値です。
- イベント: NSXセキュリティグループの変更
- タスクの有効化: False
- 処理: コンピュータを無効化します
- 条件:
  - vCenter名: <vCenter名>。イベントベースタスクはvCenter固有のため、一致する必要があります。
  - Appliance保護が有効化済み: True。有効化されている仮想マシンにのみ適用されます。
  - NSXセキュリティグループ:「^$」。グループのメンバーであってはなりません。

    注意: イベントベースタスクは初期設定で無効化されています。vCenterのインストールの完了後に、必要に応じて有効化したりカスタマイズしたりできます。

注意: 複数のイベントベースタスクが同一条件で開始される場合、タスクはタスク名のアルファベット順に実行されます。

Deep Security ManagerからvCenterを削除する

vCenterをDeep Security Managerから削除すると、次の条件を満たすすべてのイベントベースタスクが無効化されます。

1. vCenter名の条件は、削除するvCenterの名前に一致します。

   注意: これは完全一致である必要があります。複数のvCenter名に一致するイベントベースタスクは、無効化されません。

2. イベントベースタスク「イベントタイプ」は、「NSXセキュリティグループの変更」です。他のタイプのイベントベースタスクは、無効化されません。

Deep Security ManagerからvCenterを削除するには、最初にNSXからDeep Securityを削除する必要があります。NSXからDeep Securityを削除する手順と、Deep Security ManagerからvCenterを削除する手順については、"NSX環境からのDeep Securityのアンインストール" on page 1731を参照してください。

Deep Securityポリシーの NSXとの同期

Deep Securityで仮想マシンを保護する方法は2種類あります。

- イベントベースタスクを使用して仮想マシンを有効化および無効化し、初期設定のポリシーを適用または削除します。詳細については、「"vCenterがDeep Security Managerに追加されたときに作成されるイベントベースタスク" on page 642」を参照してください。
- Deep SecurityポリシーをNSXと同期します。この方法については、この後の説明を参照してください。

保護する各仮想マシンは、NSXセキュリティポリシーが割り当てられたNSXセキュリティグループに属している必要があります。NSXセキュリティポリシーの設定時には、NSXサービスプロファイルを選択します。Deep Security 9.6までは、Deep Securityで使用するNSXサービスプロファイルは1つだけでした。Deep Security 9.6 SP1以降では、すべてのDeep SecurityポリシーをNSXと同期することが可能になり、それぞれのDeep Securityポリシーに対応するNSXサービスプロファイルが作成されるようになりました。Deep Securityでは、このサービスプロファイルのことを「マッピングされたサービスプロファイル」と呼びます。

ポリシーの同期を有効にする

注意: Deep Security ポリシーをNSXと同期するには、すべてのポリシーの名前が一意である必要があります。

1. Deep Security Managerで、[コンピュータ] 画面に移動し、同期を有効にするvCenterを右クリックします。
2. [プロパティ] をクリックします。
3. [NSX設定] タブで、[Deep SecurityポリシーとNSXサービスプロファイルの同期] を選択します。[OK] をクリックします。

次の手順

1. Deep Security Virtual Applianceを使用してVMを保護するには、いくつかの手順が必要です。特定の順序で完了する必要があります。手順の詳細については、"アプライアンスを配信する(NSX-T 3.x) " on page 576, "Applianceのインストール (NSX-V)" on page 611、または "Applianceをアップグレードする" on page 1688をアップグレードします。

仮想マシンに割り当てられたポリシーを変更または削除する

マッピングされたサービスプロファイルで仮想マシンを保護する場合、ポリシーの割り当てをDeep Security Managerで変更することはできません。VMを保護するために使用するプロファイルを変更するには、vSphere Web Client(NSX-V) またはNSX-T Data Centerコンソール(NSX-T).) からNSXセキュリティポリシーまたはNSXセキュリティグループを変更する必要があります。

グループに対するNSXセキュリティポリシーの割り当てを解除すると、そのグループに属する仮想マシンがDeep Security Managerで無効化されます。

ポリシーの名前を変更する

Deep Security Managerでポリシーの名前を変更すると、NSXサービスプロファイルの名前も変更されます。

ポリシーを削除する

Deep Security Managerでポリシーを削除すると、対応するNSXサービスプロファイルも使用中でなければ削除されます。対応するNSXサービスプロファイルが使用中の場合は、Deep Security Managerと同期されなくなり、無効になったことがわかるように名前が変更されます。このNSXサービスプロファイルは、後で使用されなくなると自動的に削除されます。

VMware vRealize

VMware vRealizeでブループリントを設定する場合、ブループリントにNSXセキュリティグループまたはNSXセキュリティポリシーのどちらかを割り当てることができます。セキュリティグループとセキュリティポリシーのどちらも、マッピングされたサービスプロファイルを使用できます。

DPDKモードを設定する

注意: Trend Microでは、NSX-T Data Center 3.xのみでこの機能がサポートされます。

インテル®データ・プレーン開発キット(DPDK) は、VMware Network Introspectionを使用するサービスのパケット処理を高速化するために、VMwareに統合されたオープンソース・ライブラリの集まりです。Deep Securityの場合、これらのサービスはファイアウォール、侵入防御、およびWebレピュテーションを選択します。

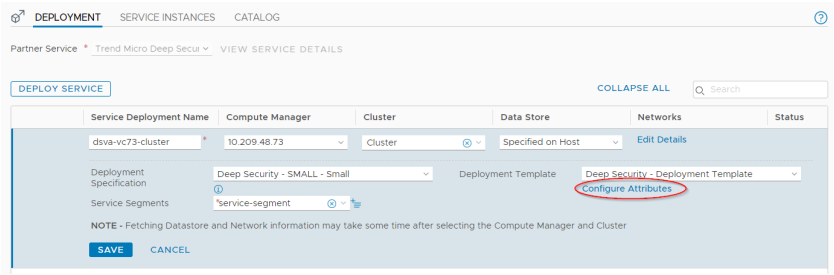
DPDKで提供されるパフォーマンスの向上を利用するには、DPDKモードでDeep Security Virtual Applianceを次のように設定できます。

開始前の準備:

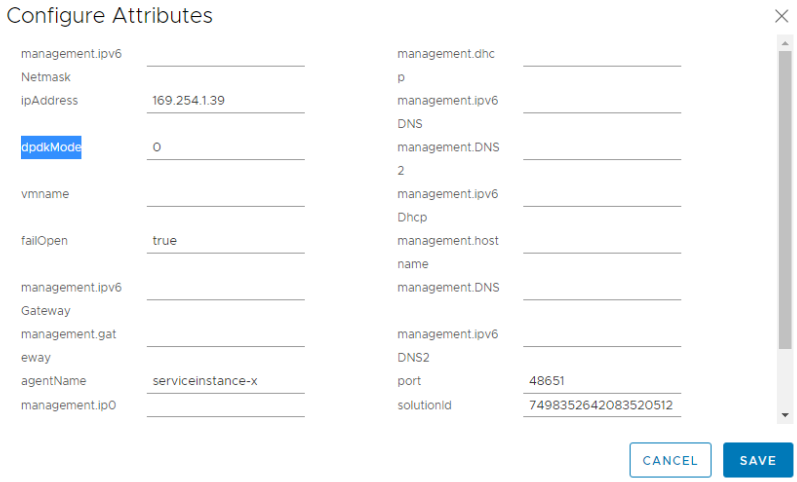
1. "システム要件 " on page 400を確認してください。DPDKモードには特定の要件があります。
2. VMwareでDPDKが設定されていることを確認してください。概要については、このVMWare DPDKドキュメントを参照してください。
3. アプライアンスの配置時にDPDKモードが設定されていることを確認します。すでにアプライアンスを起動している場合は、再デプロイする必要があります。

DPDKモードを設定します。

1. アプライアンスの配信を開始して("アプライアンスを配信する(NSX-T 3.x) " on page 576) 、" サービス配信を設定および開始する" on page 590をNSX-T 3.xに"NSX-T 3.xにアプライアンスをインストールします。" on page 589。
2. 属性の設定をクリックします。



属性の設定ダイアログボックスが表示されます。



3. Deep Security Virtual Applianceのサイズに応じて、dpdkModeフィールドを探して値を変更します。可能な値は次のとおりです。
   - -1 : Deep Security Virtual Applianceは、DPDKモードの最適なCPU使用率を決定します。具体的には:
     - アプライアンスのOVFの>= 8のCPUが割り当てられている場合、DPDKモードでは4つのCPUが割り当てられます。
     - アプライアンスのOVFに4～7のCPUが割り当てられている場合、DPDKモードでは2つのCPUが割り当てられます。
     - アプライアンスのOVFに2～3個のCPUが割り当てられている場合、DPDKモードでは、1個のCPUが割り当てられます。
   - 0(初期設定の): DPDKモードを無効にします。Deep Security Virtual Applianceは、RAWソケットモードを使用してネットワークイントロスペクションを実行します。
4. アプライアンスの配信を開始するには、SAVEをクリックしてください。
5. 配信を監視および確認する方法については、"配信を監視および確認する" on page 593してください。

NSXセキュリティタグの設定

Agentレスによる保護を使用している場合、不正プログラム対策または侵入防御 (IPS) モジュールが脅威を検出したときに保護対象の仮想マシンにNSXセキュリティタグを適用するようにDeep Security Virtual Applianceを設定できます。NSXセキュリティタグをNSX Service Composerで使用することで、感染した仮想マシンの隔離など、特定のタスクを自動化することができます。NSXのタグ付けおよび動的なNSXセキュリティグループの割り当ての詳細については、VMwareのドキュメントを参照してください。

注意: VMware NSXセキュリティタグは、Deep Securityのイベントタグとは*異なります*。NSXのタグ付けは、VMware vSphere環境で実行されます。つまり、Deep Securityのイベントタグは、Deep Securityデータベース内で使用されます。

このページのトピック:

- "NSXセキュリティタグを適用するように不正プログラム対策を設定する" on the next page
- "NSXセキュリティタグを適用するように侵入防御を設定する" on page 649

NSXセキュリティタグを適用するように不正プログラム対策を設定する

不正プログラムが検出されたときにNSXセキュリティタグを適用するように不正プログラム対策モジュールを設定するには、次の手順に従います。

1. **コンピュータエディタまたはポリシーエディタで、**[1][不正プログラム対策]→[詳細]→[NSXセキュリティのタグ付け] に移動します。
2. [オン] を選択してこの機能を有効にします。
3. [NSXセキュリティタグ] ドロップダウンリストで、不正プログラムが検出されたときにNSXで割り当てるNSXセキュリティタグの名前を選択します。オプションは次のとおりです。
   - ANTI_VIRUS.VirusFound.threat=low
   - ANTI_VIRUS.VirusFound.threat=medium
   - ANTI_VIRUS.VirusFound.threat=high

   たとえば、[ANTI_VIRUS.VirusFound.threat=low] を選択した場合は、仮想マシンで不正プログラムが検出されたときに、ANTI_VIRUS.VirusFound.threat=lowという名前のNSXセキュリティタグが仮想マシンに割り当てられます。タグの名前は不正プログラムの脅威レベルには関連付けられていないため、不正プログラムの脅威レベルが高い場合でも「low」タグが適用されます(逆の場合も同様です)。
4. オプションとして、[修復処理に失敗した場合にのみ、NSXセキュリティタグを適用する] を選択すると、不正プログラム対策モジュールによる修復処理が失敗したときにのみ、NSXセキュリティタグを適用できます(実行される修復処理は、有効になっている不正プログラム検索設定によって異なります。どの不正プログラム検索設定が有効になっているかを確認するには、**コンピュータエディタまたはポリシーエディタ**[2]で、[不正プログラム対策]→[一般] タブに移動し、[リアルタイム検索]、[手動検索]、および [予約検索] の各エリアを確認します)。
5. オプションで、[この後の不正プログラム検索が不正プログラム検出イベントが生成されずに完了した場合、以前に適用されたNSXセキュリティタグを削除] を選択することもできます。このオプションを選択すると、その後の不正プログラム検索で不正プログラムが検出されなかった場合に、セキュリティタグが削除されます。この設定は、すべての不正プログラム検索の種類が同じ場合にのみ使用してください。
6. [保存] をクリックします。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

[2] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

NSXセキュリティタグを適用するように侵入防御を設定する

NSXセキュリティタグを適用するように侵入防御モジュールを設定するには、**コンピュータエディタまたはポリシーエディタ**[1]で、[侵入防御]→[詳細]→[NSXセキュリティのタグ付け] に移動します。

侵入防御イベントには、イベントを引き起こした侵入防御ルールの重要度によって決定される重要度があります。侵入防御ルールの重要度を設定するには、**コンピュータエディタまたはポリシーエディタ**[2]で、[侵入防御]→[一般]→[現在割り当てられている侵入防御ルール] の順に選択し、ルールをダブルクリックします。必要に応じて、[重要度] フィールドを変更します。

侵入防御ルールの重要度とNSXタグは次のように対応します。

IPSルールの重要度	NSXセキュリティタグ
重大	IDS_IPS.threat=high
高	IDS_IPS.threat=high
中	IDS_IPS.threat=medium
低	IDS_IPS.threat=low

タグ付けの重要度は、仮想マシンにNSXセキュリティタグが適用される侵入防御ルールの最小重要度を指定することで設定できます。

[NSXセキュリティタグの適用を開始するルール重要度] 設定のオプションは次のとおりです。

- 初期設定 (タグを適用しない): NSXタグは適用されません。
- 重大: 重要度が「重大」である侵入防御ルールが実行されたときに、NSXタグが適用されます。
- 高: 重要度が「高」または「重大」である侵入防御ルールが実行されたときに、NSXタグが適用されます。
- 中: 重要度が「中」、「高」、または「重大」である侵入防御ルールが実行されたときに、NSXタグが適用されます。
- 低: 重要度が「低」、「中」、「高」、または「重大」である侵入防御ルールが実行されたときに、NSXタグが適用されます。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

[2] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

防御モードと検出のみモードでは、ルールに別々の設定が適用されます。動作モードの詳細については、"動作モードを使用してルールをテストする" on page 905を参照してください。

アプライアンスのOVFの場所を設定する

初期設定では、Deep Security Virtual Appliance OVFファイルは https://<deep_security_manager_host>:4119/dsva/dsva.ovfに配置されています。必要に応じて、OVFを別の場所(別のWebサーバなど)に配置してから、マネージャにそのOVFを指すことができます。次のようにします。

- 信頼性を向上させ、NSXによるアプライアンスのOVFのダウンロード速度を向上させます。
- 接続の問題によりNSXで配信エラーが修正されました。*インストールユニットのインストールに失敗しました. ovf/vib URLが正しい形式でアクセス可能であること、およびovf環境のすべてのプロパティがサービス属性で設定されていることを確認してください。ログで詳細を確認してください。*

アプライアンスOVFの場所を設定するには

まず、アプライアンスのZIPパッケージ(OVFファイル):が含まれています)を取得します。

1. Deep Security Managerで、上部にある[Administration]をクリックします。
2. 左側の[Updates]→[Software]→[Local]の順に展開します(仮想アプライアンスの), またはUpdates→Software→Download Center ( ).を使用していない場合)を展開します。
3. 仮想アプライアンスのZIPファイルを検索します。Appliance-ESX-<appliance_version>.x86_64.zipという名前です。
4. [エクスポート]→[パッケージのエクスポート] []の順にクリックします。ZIPがローカルコンピュータにダウンロードされます。

次に、アプライアンスファイルをWebサーバに配置します。

1. ZIPファイルを解凍します。
2. ZIPファイルのルートで、dsva.ovfおよびsystem.vmdkファイルを検索します。

   注意: ZIPファイルのバージョンが12 Update 3(12.0.682)以上の場合は、代わりに*.ovf、*.vmdk、*.mf、および*.certファイルを参照してください。サイズの異なる複数のファイルが配置されます。

3. これらのファイルは、ESXiおよびマネージャサーバからアクセス可能なWebサーバに配置します。
4. Webサーバで、コピーした各ファイルタイプのMIMEタイプを追加します。MIMEタイプについては、次の表で説明します。MIMEタイプをWebサーバに追加する方法の詳細については、Webサーバのドキュメントを参照してください。

ファイル拡張子	MIMEタイプ
ovf	application/vmware
vmdk	application/octet-stream
mf	text/cache-manifest
証明書	application/x-x509-user-cert

最後に、新しいOVFの場所を参照するようにマネージャを設定します。

1. Deep Security Managerで、上部の[コンピュータ]をクリックします。
2. 左側で、Computersを展開し、vCenterを右クリックして、[Properties]を選択します。
3. [NSX設定][]タブをクリックします。
4. Deep Security Managerデータベース</g>ではなく、ローカルWebサーバでホストDeep Security Virtual Applianceソフトウェアパッケージを選択します。
5. URLからVirtual Appliance OVFの下に、OVFファイルのURLの場所を入力します。例:
   - https://my.webserver.com/dsva/dsva.ovf

     または

   - https://my.webserver.com/dsva/dsva-12.0.0-682_small.ovf

   選択するOVFファイルのヘルプについては、"Deep Security Virtual Applianceのサイジング" on page 425を参照してください。
6. [OK]をクリックします。

これで、アプライアンスOVFにマネージャおよびESXiサーバからアクセスできるようになります。アプライアンスを新しい場所から配置できるようになりました。アプライアンスの配信またはバージョンアップの手順については、「"アプライアンスを配信する(NSX-T 3.x)" on page 576、"Applianceのインストール(NSX-V)" on page 611、またはDeep Security Virtual Applianceを"Applianceをアップグレードする" on page 1688。

Deep Security Virtual Applianceのメモリ割り当て

vSphere(NSX-V) NSXデータセンター環境では、Deep Security Virtual Applianceは初期設定で4GBのRAMを使用します。RAMがさらに必要になる場合は、アプライアンスの設定を変更する必要があります。設定を変更するには、2通りの方法があります。

- Applianceの設定を変更してからvCenterにインポートします。そうすると、それ以降インストールするすべてのApplianceに反映されます。
- vCenterにインポートし、ESXiに配置してから、Applianceのメモリ割り当てを個別に変更します。

Applianceに割り当てるRAMのサイズについては、"Deep Security Virtual Applianceのサイジング" on page 425を参照してください。

vCenterに配置する前にApplianceのメモリ割り当てを設定する

注意: このトピックは、NSX-T 3.0 Data Center環境には適用されません。

Applianceの初期設定のメモリ割り当てを変更するには、vCenterにインポートする前にApplianceのOVFファイルで割り当ての設定を編集する必要があります。

1. ApplianceのZIPをDeep Security Managerにインポートして、Applianceのパッケージフォルダが、<DSM_Install>\temp\Appliance-ESX-<appliance_version>に完全にダウンロードされるのを待ちます。

   警告: ApplianceのZIPは、OVFでメモリ割り当て設定を変更する前にインポートする必要があります。これらのタスクを逆の順番で実行すると、変更したOVFファイルが原因となってデジタル署名の確認でエラーが発生し、その結果インポートが失敗します。

2. テキストエディタで、<DSM_install>\temp\Appliance-ESX-<appliance_version>にあるdsva.ovfを開きます。
3. ご使用の環境に合わせて、初期設定のメモリ割り当て(4096MB)を編集します。詳細については、"Deep Security Virtual Applianceのサイジング" on page 425を参照してください。

   ```
   <Item>
   <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
   <rasd:Description>Memory Size</rasd:Description>
   <rasd:ElementName xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_
   ResourceAllocationSettingData">4096 MB of memory</rasd:ElementName>
   <rasd:InstanceID xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_
   ResourceAllocationSettingData">2</rasd:InstanceID>
   <rasd:Reservation>4096</rasd:Reservation>
   <rasd:ResourceType>4</rasd:ResourceType>
   <rasd:VirtualQuantity>4096</rasd:VirtualQuantity>
   </Item>
   ```

4. OVFファイルを保存します。

5. 複数のApplianceパッケージをDeep Security Managerにインポートした場合は、それぞれの\Appliance-ESX-<appliance_version>フォルダにあるdsva.ovfを変更します。

これで、Virtual Appliance OVFファイルをvCenterにインストールできるようになりました。"アプライアンスを配信する(NSX-T 3.x) " on page 576か、"Applianceのインストール (NSX-V)" on page 611してください。

配置済みのApplianceのメモリ割り当てを設定する

警告: Applianceのメモリ割り当て設定を変更するには、Applianceの仮想マシンをパワーオフする必要があります。Applianceによって保護される仮想マシンは、再びパワーオン状態になるまで保護されません。回避策として、可能な場合はAgentベースの保護を一時的に設定します。

1. VMware vSphere Web ClientでApplianceを右クリックし、[Power]→[Shut Down Guest] の順に選択します。
2. 再度Applianceを右クリックし、[Edit Settings] を選択します。仮想マシンの [Properties] 画面が表示されます。
3. [Hardware] タブで、[Memory] を選択してメモリ割り当ての値を変更します。
4. [OK] をクリックします。
5. 再度Applianceを右クリックし、[Power]→[Power On] の順に選択します。

アプライアンスを起動または停止する

Deep Security Virtual Applianceを開始または停止するには、Deep Security Agentを起動または停止する必要があります。これは、ホストコンピュータでのみローカルで実行できます。

LinuxでAgentを起動または停止するには

SysV initスクリプトの使用:

- 開始: /etc/init.d/ds_agent start
- 停止: /etc/init.d/ds_agent stop

systemdコマンドの使用:

- 開始: systemctl start ds_agent
- 停止: systemctl stop ds_agent

Deep Security Notifierを配信する

Deep Security Notifierは、Windowsの物理マシンまたは仮想マシン用のユーティリティです。不正プログラムが検出された場合や、不正なURLがブロックされた場合にローカル通知を送信します。Deep Security Notifierは、Deep Security AgentをWindowsコンピュータにインストールするときに自動的にインストールされます。ここで説明するスタンドアロンのインストール環境は、Deep Security Virtual Applianceで保護されている、AgentレスによるWindows仮想マシンで使用することを想定しています。詳細については、「"Deep Security Notifier" on page 1531」を参照してください。

インストールパッケージをコピーする

インストールファイルをコンピュータにコピーします。

Windows版Deep Security Notifierをインストールする

注意: WindowsコンピュータにDeep Security Notifierをインストールして実行するには、管理者権限が必要です。

1. インストールファイルをダブルクリックして、インストーラパッケージを実行します。[次へ] をクリックして、インストールを開始します。
2. 使用許諾契約書の内容をご確認いただき同意できる場合は、使用許諾内容に同意し、[次へ] をクリックします。
3. [インストール] をクリックして、インストールを続行します。
4. [完了] をクリックして、インストールを完了します。

これで、このコンピュータにDeep Security Notifierがインストールされて実行され、Windowsタスクバーに Notifierアイコンが表示されます。不正プログラムが検出されるか、URLがブロックされると、通知機能にポップアップ通知が表示されます。トレイアイコンをダブルクリックして通知ステータスと設定画面を開くと、手動で無効にすることができます。

注意: Deep Security Notifierに情報が表示されるためには、Virtual Applianceで保護されている仮想マシンに不正プログラム対策モジュールのライセンスがあり、モジュールが有効になっている必要があります。

管理者ガイド

コンピュータの追加

コンピュータの追加について

Deep Security Managerの Computers のページでは、Deep Securityで保護されているコンピュータを管理し、監視することができます。

この画面は定期的に自動更新され、最新情報が表示されます(更新頻度はユーザごとに変更できます。[管理]→[ユーザ管理]→[ユーザ] の順に選択し、ユーザアカウントをダブルクリックして [プロパティ] 画面を表示します。[設定] タブの [更新頻度] セクションで更新頻度を変更します)。

Managerにコンピュータを追加する

注意: コンピュータにインストールした後は、エージェントをDeep Security Managerでアクティベートする必要があります。アクティベーションの実行中、Deep Security Managerはエージェントに指紋を送信します。エージェントは、その一意のフィンガープリントを持つマネージャからの指示のみを受け入れます。

注意: 以前にDeep Security Virtual ApplianceによってAgentレスで保護されていた仮想マシンにAgentをインストールする場合は、Managerから仮想マシンを再有効化してコンピュータ上のAgentを登録する必要があります。

コンピュータは コンピュータページから追加できます。

コンピュータのグループ化

組織でコンピュータグループを作成すると、ポリシーの適用と管理のプロセスを迅速化できるため、便利です。グループは、[コンピュータ] 画面の左側のツリー構造に表示されます。新しいグループを作成するには、新しいコンピュータグループを作成するコンピュータグループを選択して、[追加]→[グループの作成] の順にクリックします。

グループにコンピュータを移動するには、コンピュータを選択して、[処理]→[グループへの移動] の順にクリックします。ポリシーは、コンピュータグループレベルではなく、コンピュータレベルで適用されることに注

意してください。コンピュータグループ間でコンピュータを移動しても、そのコンピュータに割り当てられているポリシーへの影響はありません。

グループを削除するには、グループを右クリックして、[グループの削除] をクリックします。コンピュータが含まれていないコンピュータグループおよびサブグループのないコンピュータグループのみ削除できます。

"スマートフォルダによるコンピュータの動的なグループ化" on page 1594もできます。

コンピュータリストをエクスポートする

[コンピュータ] 画面で [エクスポート] をクリックして、コンピュータリストをXMLまたはCSVファイルにエクスポートできます。エクスポートは、コンピュータの情報をバックアップしたり、他のレポートシステムと統合したり、別のDeep Security Managerにコンピュータを移行したりする場合に便利です。(エクスポートすると、新しいManagerでコンピュータの再検出や検索が必要ありません)。

注意: エクスポートされるコンピュータファイルには、割り当てられたポリシー、ファイアウォールルール、ファイアウォールステートフル設定、または侵入防御ルールは含まれません。この設定情報をエクスポートするには、[ポリシー] 画面にあるポリシーのエクスポートオプションを使用します。

コンピュータを削除する

コンピュータを削除すると(コンピュータを選択して [削除] をクリック)、そのコンピュータに関連するすべての情報も削除されます。コンピュータを再度検出する場合は、ポリシーおよび以前に割り当てられていたルールを割り当て直す必要があります。

ローカルネットワークコンピュータの追加

Agentからのリモート有効化

Deep Security Managerが保護するコンピュータとの通信を開始できない場合(たとえば、コンピュータが別のローカルネットワーク上にあるか、ファイアウォール), で保護されているコンピュータの場合は、コンピュータはマネージャに接続を開始する必要があります。これには、Agentを有効化するための通信も含まれます。エージェント起動によるアクティベーションを使用するには、コンピュータにDeep Security Agentをインストールしてから、Deep Security Managerと通信するようにエージェントに指示する一連のコマンドラインの手順を実行する必要があります。通信中、Deep Security Managerはエージェントをアクティベートし、さらにセキュリティポリシーの割り当て、コンピュータをコンピュータグループのメンバーにするなど、さまざまな処理を実行するように指示することもできます。

大量のコンピュータを一度にDeep Security Managerに追加する場合は、コマンドラインの説明に従ってスクリプトを作成してプロセスを自動化できます。Agentからのリモート有効化、スクリプト、コマンドラインオプションの詳細については、"コマンドラインの基本" on page 1793を参照してください。

コンピュータを手動で追加する

IPアドレスまたはホスト名を指定して、手動でコンピュータを個別に追加できます。

1. [コンピュータ] 画面に移動し、ツールバーの[追加]→[コンピュータの追加] をクリックして新規コンピュータウィザードを開きます。
2. 新しいコンピュータのIPアドレスまたはホスト名を入力します。
3. 割り当てるポリシーをリストから選択します。
4. 新しいコンピュータがセキュリティアップデートのダウンロード元として使用するRelayグループを選択します。
5. [次へ] をクリックしてコンピュータの検索を開始します。

コンピュータが検出され、そのコンピュータにAgentがインストールされていて稼働中の場合は、コンピュータリストにコンピュータが追加されて、Agentが有効になります。

注意: Agentの「有効化」とは、ManagerがAgentと通信して、一意の「フィンガープリント」をAgentに送信する処理です。この場合、エージェントはこのフィンガープリントを使用してDeep Security Managerを一意に識別し、他のマネージャからの指示に同意できません。

コンピュータにポリシーが割り当てられている場合、そのポリシーはAgentに配信され、ポリシーを設定するすべてのルールと設定によってコンピュータが保護されます。

Relayグループによって配信されるセキュリティアップデートには、新しい不正プログラムパターンファイルが初期設定で含まれています。[9.0 (およびそれ以前) のAgentをサポート] オプション ([管理]→[システム設定]→[アップデート] 画面) を有効にしている場合は、エンジンのアップデートも含まれます。

コンピュータが検出されましたが、Deep Security Agentが存在しない場合、コンピュータはコンピュータリストに追加できますが、依然としてコンピュータにエージェントをインストールする必要があるというメッセージが表示されます。コンピュータにAgentをインストールしたら、コンピュータリストでコンピュータを検索して右クリックし、コンテキストメニューの [有効化/再有効化] を選択する必要があります。

コンピュータが検出されない場合 (Managerでは認識できない場合)、コンピュータの追加は可能ですが、コンピュータがManagerで認識されるようになった後、上記と同様にコンピュータを有効化する必要があります。

コンピュータを検出する

検出操作では、ネットワーク上の表示可能なコンピュータを検索します。検出操作を開始するには、[コンピュータ] 画面に移動し、[追加]→[検出] の順にクリックします。[コンピュータの検出] 画面が表示されます。

検索範囲を制限するためのいくつかのオプションがあります。検出された各コンピュータのポート検索を実行するように選択できます。

注意: ポート検索で多数のコンピュータを検出または検索する場合は、完了までに時間がかかり、パフォーマンスが低下することがあります。

コンピュータを検出するときは、コンピュータの追加先のコンピュータグループを指定できます。選択したコンピュータグループの構成方法によっては、複数のネットワークセグメントを検索する場合に、「新しく検出されたコンピュータ」または「ネットワークセグメントXで新しく検出されたコンピュータ」というコンピュータグループを作成すると便利なことがあります。その後、検出されたコンピュータを、プロパティに基づいて別のコンピュータグループに移動し、有効にすることができます。

検出を実行する際にManagerは、まだリストされていないネットワーク上の表示可能なコンピュータを検索します。コンピュータが見つかると、ManagerはAgentが存在するかどうかの検出を試行します。検出が完了すると、Managerは検出したすべてのコンピュータを表示します。[ステータス] 列にはコンピュータのステータスが表示されます。

注意: 検出操作で確認されるのは、新しく検出されたコンピュータのステータスのみです。すでに一覧表示されているコンピュータのステータスをアップデートするには、選択したコンピュータを右クリックし、[処理]→[ステータスの確認] の順にクリックします。

検出操作後のコンピュータの状態は、次のいずれかになります。

- 検出済み (Agentなし): コンピュータが検出されましたが、Agentが存在しません。また、インストール済みのAgentが以前に有効にされており、Agentからの通信用に設定されている場合にも、コンピュータがこの状態になる可能性があります。この場合、Agentを無効にしてから再度有効にする必要があります(また、Agentがインストールされているが稼働中でない場合にも、「Agentなし」とレポートされます)。
- 検出済み (有効化が必要): Agentがインストールされ待機中で、有効にされていますが、Managerによって管理されていません。この状態は、このManagerが一時Agentを管理していましたが、Agentの公開鍵がManagerのデータベースに存在しなくなったことを示します。コンピュータがManagerから削除された後に再び検出される場合は、これに該当する可能性があります。

このコンピュータでAgentの管理を開始するには、コンピュータを右クリックし、[有効化/再有効化]を選択します。再度有効にしたコンピュータのステータスは「オンライン」に変更されます。

- 検出済み (無効化が必要): Agentはインストールされ待機中ですが、別のManagerによってすでに有効にされています。この場合、AgentをこのManagerで有効にする前に、いったん無効に(リセット) する必要があります。Agentの無効化は、そのAgentを有効にしたManagerを使用して行う必要があります。または、コマンドラインを使用してAgentをリセットできます。ManagerからAgentを無効にするには、コンピュータを右クリックし、[処理]→[無効化] を選択します。Agentをコマンドラインから無効にする場合は、"Agentをリセットする" on page 1807を参照してください。
- 検出された(アクティベートされた):エージェントは、現在のマネージャによってインストールおよびアクティベートされています。この場合、次のハートビートでステータスは「オンライン」に変わります。エージェントの管理を開始するには、コンピュータを右クリックして、[Activate/Reactivate]を選択します。再度有効にしたコンピュータのステータスは「オンライン」に変更されます。

注意: 検出操作では、vCenterで仮想マシンとして実行されているコンピュータ、Microsoft Active Directoryのコンピュータ、またはその他のLDAPディレクトリのコンピュータは検出されません。

Active Directoryコンピュータを追加する

Deep Securityは、Microsoft Active DirectoryなどのLDAPサーバを使用してコンピュータの検出やユーザアカウントとその連絡先の作成を行うことができます。Deep Security Managerはサーバにクエリを実行し、ディレクトリ内の構造に従ってコンピュータグループを表示します。

Deep SecurityをFIPSモードで使用している場合は、Active DirectoryのSSL証明書をDeep Security Managerにインポートしてから、マネージャをディレクトリに接続する必要があります。"信頼された証明書の管理" on page 1653を参照してください。

1. Deep Security Managerで、[コンピュータ] をクリックします。
2. メイン画面で、[追加]→[Active Directoryの追加] の順にクリックします。
3. Active Directoryサーバのホスト名またはIPアドレス、名前、説明、およびポート番号を入力します。アクセス方法と資格情報も入力します。次のガイドラインに従います。
    - アクセス方法がLDAPSである場合、[サーバのアドレス] は、Active DirectoryのSSL証明書で使用されている共通名 (CN) と一致している必要があります。
    - [名前] はActive Directoryのディレクトリ名と一致していなくてもかまいません。
    - [サーバのポート] は、Active DirectoryのLDAPポートまたはLDAPSポートです。初期設定は389 (LDAPおよびStartTLS) および636 (LDAPS) です。
    - [ユーザ名] にはドメイン名が含まれている必要があります。例:`EXAMPLE/Administrator`

- Deep SecurityをFIPSモードで使用している場合は、[信頼する証明書]セクションの[接続テスト]をクリックして、Active DirectoryのSSL証明書がDeep Security Managerに正常にインポートされているかどうかを確認します。

[次へ] をクリックして続行します。

4. ディレクトリのスキーマを指定します。(スキーマをカスタマイズしていない場合は、Microsoft Active Directoryサーバの初期設定値のままでかまいません。)

   Deep Security Manager内の各コンピュータの [詳細] 画面には、[説明]フィールドがあります。Active Directoryの「コンピュータ」オブジェクトクラスの属性を使用して [説明] フィールドに入力するには、[コンピュータの詳細の属性] テキストボックスに属性名を入力します。

   Active Directoryサーバと同期されたDeep Security Managerでこの構造を自動的に保持する場合は、[予約タスク]を選択して、このディレクトリを同期します。ディレクトリの追加が完了すると、予約タスクウィザードが表示されます。この設定は、予約タスクウィザード([管理]→[予約タスク]) を使用して後から行うことができます。

5. [次へ] をクリックして続行します。

6. Managerによるディレクトリのインポートが完了すると、追加されたコンピュータのリストが表示されます。[完了] をクリックします。

   [コンピュータ] 画面にディレクトリ構造が表示されます。

Active Directoryのその他のオプション

Active Directory構造を右クリックすると、次のオプションが表示されます。これらのオプションは、ディレクトリ以外のコンピュータグループには使用できません。

- ディレクトリの削除
- 今すぐ同期

ディレクトリの削除

Deep Security Managerからディレクトリを削除する場合、次のオプションがあります。

- ディレクトリおよびすべての下位コンピュータ/グループをDeep Security Managerから削除します: ディレクトリのデータをすべて削除します。
- ディレクトリを削除しますが、コンピュータのデータおよびグループの階層は維持します: インポートされたディレクトリ構造を、同じ構成の通常のコンピュータグループに変換します。Active Directoryサーバとのリンクは解除されます。

- ディレクトリを削除し、コンピュータのデータを維持しますが、グループの階層は削除します: Active Directoryサーバへのリンクを削除し、ディレクトリ構造を破棄し、すべてのコンピュータを同じコンピュータグループに配置します。

今すぐ同期

Deep Security Managerを手動で起動してActive Directoryサーバと同期し、コンピュータグループの情報を更新できます。

ヒント: この処理は、予約タスクを作成して自動化できます。

サーバ証明書を使用する

Active DirectoryサーバでSSLを有効にしていない場合は有効にします。

コンピュータの検出にはSSL/TLSまたは暗号化されていないクリアテキストを使用できますが、ユーザアカウント(パスワードや連絡先を含む)のインポートには認証とSSL/TLSが必要です。

SSL/TLS接続には、Active Directoryサーバのサーバ証明書が必要です。SSL/TLSのハンドシェイクで、この証明書がサーバを証明する識別情報としてサーバからクライアントに渡されます。この証明書には、自己署名証明書または認証局 (CA) が署名した証明書を使用できます。サーバに証明書があるかどうかを確認するには、Active DirectoryサーバでInternet Information Services (IIS) Managerを開いて、[サーバー証明書] を選択します。サーバに署名入りのサーバ証明書がない場合はインストールする必要があります。

ユーザおよび連絡先をインポートする

Deep Securityは、Active Directoryからユーザアカウント情報をインポートし、対応するDeep Securityユーザまたは連絡先を作成できます。この機能には次の利点があります。

- ユーザはActive Directoryで定義されたネットワークパスワードを使用できる。
- 管理者は、Active Directory内からアカウントを集中的に削除できます。
- Active Directory内の既存情報を利用できるため、連絡先情報 (メール、電話番号など) の保守が簡単になる。

ユーザと連絡先の両方をActive Directoryからインポートできます。Deep Security Managerの設定権限があるユーザです。連絡先は、Deep Security Manager通知のみを受信できます。同期ウィザードを使用すると、ユーザとしてインポートするActive Directoryオブジェクトと、連絡先としてインポートするActive Directoryオブジェクトを選択できます。

成功したのDeep Securityユーザーまたは連絡先としてのDeep SecurityへのActive Directoryのユーザーアカウントをインポートするには、Active Directoryのユーザーアカウントが のuserPrincipalName 属性値を持っている必要があります。userPrincipalName属性は、Active Directoryのアカウント所有者の「ユーザログオン名」に相当します。

1. [管理]→[ユーザ管理] の順にクリックし、[ユーザ] または [連絡先] をクリックします。
2. [ディレクトリとの同期] をクリックします。
   ユーザまたは連絡先情報をはじめてインポートする場合は、サーバ情報の画面が表示されます。それ以外の場合は、ディレクトリとの同期ウィザードが表示されます。
3. 適切なアクセスオプションを選択し、ログオン資格情報を入力して、[次へ] をクリックします。
4. 同期するグループを左の列から選択し、[>>] をクリックして右の列に追加し、[次へ] をクリックします。

   ヒント: 複数のグループを選択するには、<Shift> または <Ctrl> キーを押しながらグループをクリックします。
5. すべてのディレクトリグループメンバーに同じDeep Securityの役割を割り当てるか、ディレクトリグループのメンバーシップに基づいてDeep Securityの役割を割り当てるかを選択し、リストから初期設定の役割を選択して、[ ] [次へ] []の順にクリックします。
6. ディレクトリグループメンバシップに基づいてDeep Securityの役割を割り当てた場合は、グループごとに同期オプションを指定し、[次へ]の順にクリックします。

   同期後、インポートしたオブジェクト数を示すレポートが生成されます。

   同期が完了する前に、ユーザおよび連絡先を定期的に同期する予約タスクを作成することもできます。
7. [完了] をクリックします。

インポートしたオーガニック(インポートされていない) Deep Securityアカウントとインポートされたアカウントの違いを確認できます。これらのアカウントの一般情報は変更できません。

Active Directoryオブジェクトの同期を維持する

一度インポートしたActive Directoryオブジェクトは、Active Directoryサーバと継続的に同期して、最新のアップデートを反映させる必要があります。これにより、たとえば、Active Directoryで削除されたコンピュータもDeep Security Managerで削除されます。Deep Security Managerにインポートされた Active Directoryオブジェクトを Active Directoryと同期させて保持するには、ディレクトリデータを同期する予約タスクを設定することが不可欠です。コンピュータのインポートウィザードには、これらの予約タスクを作成するためのオプションが用意されています。

このタスクは予約タスクウィザードを使用して作成することもできます。必要に応じて同期を実行するには、コンピュータの場合は [今すぐ同期] オプションを使用し、ユーザおよび連絡先の場合は [ディレクトリとの同期] ボタンを使用します。

必ずしもユーザおよび連絡先の同期を維持するための予約タスクを作成する必要はありません。ログオン時、Deep Security Managerはユーザがactive Directoryに存在するかどうかを確認します。ユーザ名とパスワードが有効で、そのユーザが同期が有効になっているグループに属している場合、ユーザはDeep Security Managerに追加され、ログインできるようになります。

Active Directory内のアカウントを無効にしても、削除しないと、そのユーザはDeep Security Managerに表示され、アクティブになります。

Active Directoryとの同期を無効にする

Deep Security Managerがコンピュータグループとユーザアカウントの両方に対してActive Directoryと同期するのを停止できます。

Active Directoryとの同期からコンピュータグループを削除する

1. [コンピュータ] に移動します。
2. ディレクトリを右クリックし、[ディレクトリの削除] を選択します。
3. Deep Security Managerとの同期が中断された場合に、このディレクトリのコンピュータのリストをどのように処理するかを次の中から選択します。
   - Deep Security Managerからディレクトリおよびすべての下位コンピュータ/グループを削除します。: このディレクトリの構造を削除します。
   - ディレクトリを削除しますが、コンピュータのデータおよびグループの階層は維持します: フォルダやコンピュータに対するユーザおよび役割ごとのアクセス権限を含む、既存の構造を維持します。
   - ディレクトリを削除し、コンピュータのデータを維持しますが、グループの階層は削除します: ディレクトリにちなんだ名前を持つグループ内のフラットなコンピュータのリストにディレクトリ構造を変換します。新しいコンピュータグループでは、以前の構造と同じユーザおよび役割ごとのアクセス権限が維持されます。
4. 確認して処理を開始します。

Active Directoryのユーザおよび連絡先を削除する

コンピュータグループのディレクトリクエリを削除する場合と異なり、ユーザと連絡先のクエリを削除すると、Deep Security Managerからすべてのアカウントが削除されます。その結果、Directory Serverからインポートされたユーザアカウントでdeep Security Managerにログインしている間は削除できません。この処理を実行すると、エラーが表示されます。

1. [ユーザ] または [連絡先] で [ディレクトリとの同期] をクリックします。
2. [同期を中止する] を選択して、[OK] をクリックします。
3. [完了] をクリックします。

AWSインスタンスを追加する

AWSアカウントの追加について

トピック:

- "AWSアカウントを追加する方法の概要" below
- "AWSアカウントを追加するとどうなりますか? " below
- "AWSアカウントを追加することのメリットは何ですか? " on the next page
- "サポートされるAWSリージョン" on the next page

AWSアカウントを追加する方法の概要

Deep Security ManagerにAWSアカウントを追加する方法はいくつかあります。

- "マネージャーのインスタンスの役割を使用したAWSアカウントの追加" on page 666を使用してAWSアカウントを追加します。Deep Security Managerが</g> AWS内で <g id="0">の場合、この方法を使用します。
- "アクセスキーを使用してAWSアカウントを追加する" on page 669を使用してAWSアカウントを追加します。Deep Security ManagerがAWS外のの場合は、この方法を使用します。
- "クロスアカウントロールを使用したAWSアカウントの追加" on page 672を使用してAWSアカウントを追加します。このメソッドは、複数のAWSアカウントを追加する場合に使用します。

AWSアカウントを追加するとどうなりますか?

Deep SecurityにAWSアカウントを追加すると、そのアカウントのすべてのAmazon EC2およびAmazon WorkSpaceインスタンスがDeep Security Managerにインポートされ、次のいずれかの場所で表示されます。

- EC2インスタンスは、[コンピュータ]→[<ご使用のAWSアカウント>]→[<ご使用のリージョン>]→[<ご使用のVPC>]→[<ご使用のサブネット>] の左側に表示されます。
- Amazon WorkSpacesは、左側の Computers>*_AWS_アカウント> your_region*>WorkSpacesの下に表示されます。

インポートの完了後は、他のコンピュータと同じようにEC2とWorkSpaceのインスタンスを管理できます。これらのインスタンスはツリー構造であり、コンピュータグループとして扱われます。

注意: 以前にAmazon EC2インスタンスまたはAmazon WorkSpacesを個々のコンピュータとして追加した場合、そのアカウントがAWSアカウントの一部である場合、アカウントをインポートした後、インスタンスは上記のツリー構造に移動されます。

AWSアカウントを追加することのメリットは何ですか?

個別のEC2インスタンスとワークスペース(「Deep Security Manager」→「コンピュータ」→「コンピュータの追加」), を使用) を追加するのではなく、AWSアカウント(Deep Security Manager→ コンピュータ→AWSアカウントの追加) の利点は次のとおりです。

- EC2およびWorkspaceのインベントリの変更は、Deep Security Managerに自動的に反映されます。たとえば、AWSでいくつかのEC2またはWorkSpaceインスタンスを削除すると、これらのインスタンスは自動的にマネージャから非表示になります。一方、の[コンピュータ]→[コンピュータの追加]を使用する場合、AWSから削除されたEC2およびWorkSpaceのインスタンスは、手動で削除されるまでマネージャに表示されたままです。
- EC2およびWorkSpaceのインスタンスは、マネージャの[AWS region]→[VPC]のサブネットに編成されており、どのインスタンスが保護されているか、どのインスタンスが保護されていないかを簡単に確認できます。AWSアカウントがないと、すべてのEC2インスタンスとWorkSpaceインスタンスが同じルートレベルの Computersに表示されます。
- イベントベースタスク(EBT) でAWSメタデータを使用してポリシーの割り当てを簡素化できます。スマートフォルダでメタデータを使用して、AWSインスタンスを編成することもできます。

サポートされるAWSリージョン

Deep Security Managerの[コンピュータ]→[追加]→[AWSアカウントの追加] オプションは、iam.amazonaws.comでグローバルAWS IDアクセス管理(IAM) サービスを使用するAWS領域のみをサポートします。お住まいの地域でグローバルサービスが使用されているかどうかを確認するには、this tableを参照してください。

次の地域では、ではではグローバルIAMサービス(iam.amazonaws.com):) を使用していません。

- 中国(北京)
- 中国(寧夏回族自治区)
- AWS GovCloud(米国 - 東)
- AWS GovCloud (米国)

上記の地域およびグローバルIAMサービスを使用しない地域では、Deep Security REST APIを使用してEC2およびWorkSpaceのインスタンスをManagerにロードできます。トレンドマイクロでは、このサンプルスクリプトを提供しています。

マネージャーのインスタンスの役割を使用したAWSアカウントの追加

次の手順に従って、Managerインスタンスの役割を使用してDeep Security ManagerにAWSアカウントを追加します。Deep Security ManagerがAWSの内部で実行されている場合は、この方法を使用します。

注意:「AWS Primary Account」という用語は、Deep Security Managerが配置されているAWSアカウントの説明に使用されます。

まず、AWSプライマリアカウントにログインします。

1. Amazon Web Services at https://aws.amazon.com/.にアクセスしてください
2. AWSプライマリアカウントを使用してログインします。

次に、IAMポリシーを設定します。

1. Amazon Web Services Consoleで、IAM サービスに移動します。
2. 左側のナビゲーションペインで [Policies] をクリックします。

   注意: この画面にはじめてアクセスした場合は、[Get Started] をクリックする必要があります。
3. [Create policy] をクリックします。
4. [JSON] タブを選択します。
5. テキストボックスに次のJSONコードをコピーします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cloudconnector",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
```

```
            "ec2:DescribeSubnets",
            "ec2:DescribeTags",
            "ec2:DescribeVpcs",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeSecurityGroups",
            "workspaces:DescribeWorkspaces",
            "workspaces:DescribeWorkspaceDirectories",
            "workspaces:DescribeWorkspaceBundles",
            "workspaces:DescribeTags",
            "iam:ListAccountAliases",
            "iam:GetRole",
            "iam:GetRolePolicy",
            "sts:AssumeRole"
        ],
        "Effect": "Allow",
        "Resource": "*"
    }
  ]
}
```

注意: "sts:AssumeRole" 権限は、で(クロスアカウントロールを使用して) マネージャにAWSアカウントを追加する場合にのみ必要です。。

注意: "iam:GetRole" および "iam:GetRolePolicy" の権限はオプションですが、追加のAWS権限が必要なManagerへのアップデートが発生したときにDeep Securityが正しいポリシーを持っているかどうかを判断できるため、推奨されます。

6. [Review policy] をクリックします。
7. ポリシーの名前と説明を指定します。例の名前: Deep_Security_Policy。
8. [Create policy] をクリックします。これでポリシーを使用する準備ができました。

次に、manager instance roleを作成します。

1. [IAM] サービスに移動します。
2. [Roles] をクリックします。
3. [Create role] をクリックします。
4. [AWS service] ボックスが選択されていることを確認します。
5. サービスリストで [EC2] をクリックします。オプションがさらに表示されます。

---

6. [EC2 Allows EC2 instances to call AWS services on your behalf] をクリックします。[Next: Permissions] をクリックします。
7. 作成したIAMポリシーの横にあるチェックボックスをオンにします。[Next: Review] をクリックします。
8. [Role name] と[Role description] を入力します。
   ロールの例：Deep_Security_Manager_Instance_Role
9. [Create role] をクリックします。

次に、AWSのManagerにManagerインスタンスの役割を追加します。

1. [EC2] サービスに移動します。
2. 左側の[インスタンス]をクリックし、Deep Security Managerがインストールされている EC2インスタンスの横にあるチェックボックスをオンにします。
3. [Actions]→[Instance Settings]→[Attach/Replace IAM Role] の順にクリックします。
4. IAMの役割 ドロップダウンリストから、マネージャのインスタンスの役割 (Deep_Security_Manager_Instance_Role).) を選択します。
5. [Apply] をクリックします。

これで、IAMポリシーが正しいマネージャインスタンスの役割が作成され、Deep Security ManagerのEC2インスタンスに関連付けられました。

次に、ManagerでManagerインスタンスの役割を設定します。

1. Deep Security Managerで、上部にある[Administration]をクリックします。
2. 左側にある[システム設定] をクリックします。
3. メイン画面の [詳細] タブをクリックします。
4. 下にスクロールして、[Manager AWS ID] セクションを探します。
5. [Managerインスタンスロールを使用] が選択されていることを確認します。

   注意: Managerインスタンスロールを使用 の使用が表示されない場合は、Deep Security Managerがインストールされているec2インスタンスに役割が関連付けられていることを確認してください.、次に "Deep Security Managerの再起動" on page 1746を再起動します。再起動時、Deep Securityはマネージャのec2インスタンスの役割を検出し、Managerインスタンスロールを使用 オプションを表示します。

6. [保存] をクリックします。

最後に、AWSプライマリアカウントをマネージャに追加します。

1. Deep Security Managerで、上部の[コンピュータ]をクリックします。
2. メイン画面で、[追加]→[AWSアカウントの追加]の順にクリックします。
3. [Managerインスタンスロールを使用]を選択します。
4. AWSプライマリアカウントにAmazon WorkSpacesが含まれている場合は、[Amazon WorkSpacesを含める]を選択してAmazon EC2インスタンスに含めることができます。このチェックボックスをオンにすると、Amazon WorkSpacesがDeep Security Managerのツリー構造内の正しい場所に表示され、正しい料金が請求されます。
5. [Next]をクリックします。

Deep Security Managerは、Amazon EC2インスタンスに接続されているManagerインスタンスの役割を使用して、AWSプライマリアカウントのEC2およびWorkSpaceインスタンスをDeep Security Managerに追加します。

これで、Deep Security ManagerにAWSプライマリアカウントが追加されました。このAWSアカウントにあるAmazon EC2インスタンスとAmazon WorkSpacesがロードされます。

上記のタスクの完了後、Amazon EC2およびWorkSpaceインスタンスにエージェントをインストールしていない場合は、インストールしてください。

アクセスキーを使用してAWSアカウントを追加する

次の手順に従って、アクセスキーを使用してDeep Security ManagerにAWSアカウントを追加します。Deep Security ManagerがAWS外のサーバ上にある場合、または別の方法を試しても動作しない場合は、アクセスキーを使用してください。その他のすべてのシナリオでは、を使用してAWSアカウントを追加することをお勧めします。(セキュリティ上の理由から、管理オーバーヘッドを作成する), のために、キーを定期的に更新する必要があるため、アクセスキーの使用はお勧めしません。)

注意: このトピックでは、「AWS Primary Account」という用語を使用して、マネージャに追加するEC2インスタンスとWorkSpaceインスタンスを含むAWSアカウントについて説明します。

まず、AWSプライマリアカウントにログインします。

1. Amazon Web Services at https://aws.amazon.com/.にアクセスしてください
2. AWSのプライマリアカウントを使用してログインします。

次に、IAMポリシーを設定します。

---

1. Amazon Web Services Consoleで、IAM サービスに移動します。
2. 左側のナビゲーションペインで [Policies] をクリックします。

   注意: この画面にはじめてアクセスした場合は、[Get Started] をクリックする必要があります。

3. [Create policy] をクリックします。
4. [JSON] タブを選択します。
5. テキストボックスに次のJSONコードをコピーします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cloudconnector",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeTags",
        "iam:ListAccountAliases",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "sts:AssumeRole"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

> 注意: "sts:AssumeRole" 権限は、で(クロスアカウントロールを使用して) マネージャにAWSアカウントを追加する場合にのみ必要です。。

> 注意: "iam:GetRole" および "iam:GetRolePolicy" の権限はオプションですが、追加のAWS権限が必要なManagerへのアップデートが発生したときにDeep Securityが正しいポリシーを持っているかどうかを判断できるため、推奨されます。

6. [Review policy] をクリックします。
7. ポリシーの名前と説明を指定します。例の名前: `Deep_Security_Policy`。
8. [Create policy] をクリックします。これでポリシーを使用する準備ができました。

次に、アクセスキーIDと秘密鍵を持つIAMユーザを作成します。

1. [IAM] サービスに移動します。
2. [Users] をクリックします。
3. [Add user] をクリックします。
4. ユーザ名を入力します。例: Deep_Security_IAM_User。
5. [Access type] では [Programmatic access] を選択します。
6. [Next: Permissions] をクリックします。
7. [Attach existing policies directly] ボックスをクリックします。
8. 作成したIAMポリシーを探し、その横にあるチェックボックスをオンにします。
9. [Next: Review] をクリックします。
10. [Create user] をクリックします。アクセスキーIDと秘密アクセスキーがテーブルに表示されます。
11. アクセスキーIDと秘密アクセスキーを安全な場所にコピーします。後で必要になります。

次に、アクセスキーをマネージャに追加します。

1. Deep Security Managerにログインします。
2. 上部の [管理] をクリックします。
3. 左側にある [システム設定] をクリックします。
4. メイン画面の [詳細] タブをクリックします。
5. 下にスクロールして、[Manager AWS ID] の見出しを探します。
6. [アクセスキー - Managerの識別に使用されるAWSユーザのアクセスキー] の横に、作成済みのIAMユーザのアクセスキーを入力します。

---

7. [秘密鍵 - Managerの識別に使用されるAWSユーザの秘密アクセスキー] の横に、作成済みのIAMユーザの秘密鍵を入力します。
8. [保存] をクリックします。

最後に、AWS Primary AccountとそのアクセスキーをManagerに追加します。

1. 上部の [コンピュータ] をクリックします。
2. [追加]→[AWSアカウントの追加] の順にクリックします。
3. [AWSアクセスキーを使用] を選択します。
4. AWSプライマリアカウントのIAMユーザ アクセスキーID および Secret Access Key を入力します。
5. AWSプライマリアカウントにAmazon WorkSpacesが含まれている場合は、[Amazon WorkSpacesを含める]を選択してAmazon EC2インスタンスに含めることができます。このチェックボックスをオンにすると、Amazon WorkSpacesがDeep Security Managerのツリー構造 内の正しい場所に表示され、正しい料金が請求されます。

   AWSプライマリアカウントのAmazon EC2インスタンスとAmazon WorkSpacesがロードされます。

上記のタスクの完了後、Amazon EC2およびWorkSpaceインスタンスに エージェント をインストールしていない場合は、インストールしてください。

クロスアカウントロールを使用したAWSアカウントの追加

次の手順に従って、クロスアカウントの役割を使用してAWSアカウントを追加します。複数のAWSアカウントを追加する場合は、クロスアカウントの役割を使用します。

次の手順では、AWSアカウントに次の名前を追加することを想定しています。

- AWSプライマリアカウント
- AWSアカウントA

ヒント: また、Deep Security APIを介してクロスアカウントロールを追加することもできます。詳細については、"APIを使用してアカウントを追加する" on page 677 でアカウントを追加するを参照してください。

まず、AWSプライマリアカウントを追加します。

- AWS内のにマネージャがいる場合は、"マネージャーのインスタンスの役割を使用したAWSアカウントの追加" on page 666 を使用してAWSアカウントを追加し、AWSプライマリアカウントを追加します。
- AWS外のにマネージャーがいる場合は、のすべてのタスクを"アクセスキーを使用してAWSアカウントを追加する" on page 669 を使用してAWSアカウントを追加してください。

次に、AWS Primary Account identifierを探します。

AWSプライマリアカウントをマネージャインスタンスアカウントロールを使用して追加した場合は、次の手順を実行します。

1. AWS Primary Accountにログインしていることを確認してください。
2. IAMサービスに移動します。
3. [Roles] をクリックします。
4. "マネージャーのインスタンスの役割を使用したAWSアカウントの追加" on page 666を使用してAWSアカウントを追加します。次に例を示します。`Deep_Security_Manager_Instance_Role`
5. リスト内のロールを選択して、詳細を表示します。
6. 画面の上部にある [Role ARN] フィールドを探します。その値は次のようになります。`arn:aws:iam::1111111111:role/Deep_Security_Manager_Instance_Role`
7. ARNのロールアカウントIDをメモします。数字 (`1111111111`).) です。後でクロスアカウントロールを作成する必要があります。

AWS プライマリアカウントをアクセスキーを使用して追加した場合は、次の手順を実行します。

1. AWS Primary Accountにログインしていることを確認してください。
2. AWSの右上で [Support]→[Support Center] の順にクリックします。
3. 右上の勘定番号 (`1111111111`、この例では).) を確認してください。後でクロスアカウントロールを作成する必要があります。

次に、外部IDを取得します。

1. Deep Security Managerにログインします。
2. 上部の [コンピュータ] をクリックします。
3. [追加]→[AWSアカウントの追加]をクリックします。ウィザードが表示されます。

---

4. 隠された外部IDの横にある目のアイコンをクリックして表示します。このIDの詳細については、"外部IDとは何ですか。" on page 680を参照してください。
5. 外部IDを安全な場所にコピーします。次の手順で、AWSアカウントAと追加するその他のAWSアカウントを設定する必要があります。
6. (オプション)ウィザードとマネージャを閉じます。

次に、AWSアカウントAのIAMポリシーを設定します。

> 注意: このIAMポリシーは、AWSプライマリアカウントのポリシーと同じですが、sts:AssumeRole 権限は必要ありません。

1. AWSアカウントAにログインしていることを確認してください。
2. Amazon Web Services Consoleで、IAM サービスに移動します。
3. 左側のナビゲーションペインで [Policies] をクリックします。

   > 注意: この画面にはじめてアクセスした場合は、[Get Started] をクリックする必要があります。

4. [Create policy] をクリックします。
5. [JSON] タブを選択します。
6. テキストボックスに次のJSONコードをコピーします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cloudconnector",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspaceDirectories",
```

```
            "workspaces:DescribeWorkspaceBundles",
            "workspaces:DescribeTags",
            "iam:ListAccountAliases",
            "iam:GetRole",
            "iam:GetRolePolicy"
        ],
        "Effect": "Allow",
        "Resource": "*"
    }
  ]
}
```

注意: "iam:GetRole" および "iam:GetRolePolicy" の権限はオプションですが、追加のAWS権限が必要なManagerへのアップデートが発生したときにDeep Securityが正しいポリシーを持っているかどうかを判断できるため、推奨されます。

7. [Review policy] をクリックします。
8. ポリシーの名前と説明を指定します。例の名前：Deep_Security_Policy_Cross。
9. [Create policy] をクリックします。これでポリシーを使用する準備ができました。

次に、AWSアカウントAのクロスアカウントロールを作成します。

1. AWSアカウントAにログインしていることを確認してください。
2. [IAM] サービスに移動します。
3. 左側のナビゲーションペインで [Roles] をクリックします。
4. メイン画面で、[Create role] をクリックします。
5. [Another AWS account] ボックスをクリックします。
6. [アカウントID]フィールドに次の情報を入力します。
   - AWS内でDeep Security Manager *を使用している場合は*、と入力します。前の手順でメモしたAWS Primary Accountのアカウント IDを入力します。次に例を示します。1111111111
   - AWSの外部でDeep Security Manager *を使用している場合は*、と入力します。次に例を示します。1111111111
7. [Options] の横にある [Require external ID] を有効にします。外部ID フィールドに、以前にマネージャから取得した外部IDを入力します。
8. [Next: Permissions] をクリックします。

---

9. 作成したIAMポリシー(例 : Deep_Security_Policy_Cross) を選択し、をクリックします。[次へ]: を確認します。
10. [Review] ページで、役割名と説明を入力します。ロール名の例 : Deep_Security_Role_Cross。
11. メインの役割ページで、作成した役割を検索します(Deep_Security_Role_Cross).
12. 検索した役割をクリックします。
13. [の役割] [ARN]の上部にあるフィールドを探します。それは次のようになります: arn:aws:iam::2222222222:role/Deep_Security_Role_Cross
14. ロールのARN 値に注意してください。後で必要になります。

これで、AWS Account Aの下にクロスアカウントの役割が設定され、正しいポリシーが含まれ、AWS Primary Accountの アカウントIDまたはManagerのインスタンスの役割 が参照されます。

次に、AWS Account Aをマネージャに追加します。

1. Deep Security Managerにログインします。
2. 上部の [コンピュータ] をクリックします。
3. [追加]→[AWSアカウントの追加] の順にクリックします。
4. [クロスアカウントロールを使用] を選択します。
5. AWSアカウントAのアカウント間 ロールARNを入力します。クロスアカウントロールを作成した時点でこれが以前の例です。この例では、次のとおりです。arn:aws:iam::2222222222:role/Deep_Security_Role_Cross
6. AWSアカウントAにAmazon WorkSpacesが含まれている場合は、[Amazon WorkSpacesを含める] を選択して、Amazon EC2インスタンスとAmazon WorkSpacesを追加します。このチェックボックスをオンにすると、Amazon WorkSpacesがDeep Security Managerの ツリー構造 内の正しい場所に表示され、正しい料金が請求されます。
7. [次へ] をクリックします。
   AWSアカウントAのAmazon EC2インスタンスとAmazon WorkSpacesがロードされます。

AWSアカウントAがマネージャに追加されました。

上記のタスクの完了後、Amazon EC2およびWorkSpaceインスタンスに エージェント をインストールしていない場合は、インストールしてください。

APIを使用してアカウントを追加する

1. 外部IDをまだ取得していない場合は、Deep Security `/api/awsconnectorsettings` エンドポイントにコールして取得してください(`ExternalId` パラメータ).このIDの詳細については、"外部IDとは何ですか。" on page 680
2. AWSでは、クロスアカウントロールのIAM信頼ポリシーで外部IDを指定します。
3. `/api/awsconnectors` API エンドポイントを使用してAWS アカウントをDeep Security に追加します。`/rest/cloudaccounts/aws` API は非推奨となっているため、使用しないでください。API `/rest/cloudaccounts/aws` でクロスアカウントロールを使用している場合の対応が必要の詳細については、`/rest/cloudaccounts/aws` API のサポートがどのくらい続くか、および新しいエンドポイントに移行するためのヒントをご覧ください。

Amazon WorkSpacesの追加

Amazon WorkSpacesは、Amazon Web Services (AWS) で実行される仮想クラウドデスクトップです。Deep Securityで保護するには、次のいずれかの手順に従います。

- "Amazon WorkSpacesを保護する(AWSアカウントをすでに追加している場合)" below
- "Amazon WorkSpacesを保護する(AWSアカウントをまだ追加していない場合)" on the next page

注意: Deep Security AgentはAmazon WorkSpaces Windowsデスクトップのみをサポートします.Windowsデスクトップは Linuxデスクトップをサポートしていません。

上記セクションのいずれかの手順の完了後:

- Amazon WorkSpacesがDeep Security Managerの左側の Computers > *your_AWS_account* > *your_region* > WorkSpacesの下に表示されます。
- Amazon WorkSpacesはDeep Security Agentで保護されています。

Amazon WorkSpacesを保護する(AWSアカウントをすでに追加している場合)

すでにAWSアカウントをDeep Security Managerに追加している場合(Amazon EC2インスタンス), を保護するために、このセクションの手順を実行してDeep SecurityをAmazon WorkSpacesと連携させて設定してください) 。

1. Deep Security Managerをバージョン10.3以上にアップグレードします。"Deep Security Managerをインストールする" on page 459を参照してください。
2. Amazon WorkSpaceを起動し、Deep Security Agent 10.2以降をインストールして有効にします。詳細については、"Amazon EC2およびWorkSpacesへのAgentのインストール" on page 543

を参照してください。オプションで、カスタムWorkSpaceバンドルを作成し、多数のユーザに配信できるようにします。インストール、有効化、およびバンドル作成の詳細については、"エージェントをAMIまたはWorkSpaceバンドルにインストールする" on page 549を参照してください。

3. Amazon WorkSpacesの権限を含むようにIAMポリシーを変更します。
   a. Deep Security Managerに追加されたアカウントでAWSにログインします。
   b. [IAM] サービスに移動します。
   c. Deep Security IAMポリシーを検索します。左側の[Policies]にあるポリシー名を参照するか、ポリシーを参照するDeep Security IAMの役割またはIAMユーザを探して、そのポリシーをクリックできます。
   d. Deep Security IAMポリシーを次の図のように変更します。"クロスアカウントロールを使用したAWSアカウントの追加" on page 672。このポリシーには、Amazon WorkSpacesの権限が含まれます。複数のAWSアカウントをDeep Securityに追加した場合、IAMポリシーはすべてのAWSアカウントでアップデートする必要があります。
4. Deep Security Managerで、AWSアカウントを編集します。
   a. 左側でAWSアカウントを右クリックし、[プロパティ] を選択します。
   b. [Amazon WorkSpacesを含める] を有効にします。
   c. [保存] をクリックします。

これで、Amazon WorkSpacesがDeep Securityに追加されました。

Amazon WorkSpacesを保護する(AWSアカウントをまだ追加していない場合)

AWSアカウントをDeep Security Managerにまだ追加していない場合は、次のいずれかの手順を実行します。

- 既存のAmazon WorkSpacesを保護する場合、"Amazon EC2およびWorkSpacesへのAgentのインストール" on page 543を参照してください。
- Agentが「統合」されている新しいAmazon WorkSpacesを起動できるようにするには、"エージェントをAMIまたはWorkSpaceバンドルにインストールする" on page 549を参照してください。

AWSアカウントの管理

トピック:

- "AWSアカウントの編集" on the next page
- "AWSアカウントを削除する" on the next page
- "AWSアカウントを同期する" on the next page

AWSアカウントの編集

Deep Security ManagerでAWSアカウントの設定を編集できます。AWSアカウントにAmazon WorkSpacesを含めるよう設定する必要がある場合などに、この編集が必要になることがあります。
AWSアカウントを編集するには

1. Deep Security Managerにログインします。
2. 上部の[コンピュータ]をクリックします。
3. 左側で、AWSアカウント名を右クリックして[のプロパティ]を選択します。
4. 設定を編集して、[OK]をクリックします。

AWSアカウントを削除する

Deep Security ManagerからAWSアカウントを削除すると、そのアカウントはDeep Securityデータベースと基になるコンピュータから永久に削除されます。AWSを使用しているアカウントは影響を受けず、インスタンスにインストールされたDeep Security Agentはインストールされ、実行され、保護を提供します(ただし、セキュリティアップデートは受信されません)。AWSアカウントからコンピュータを再インポートする場合、Trend Micro Deep Security Agentは次の予約期間に最新のセキュリティアップデートをダウンロードします。

1. Deep Security Managerで、上部にある[Computers]をクリックします。
2. ナビゲーションパネルでAWSアカウントを右クリックし、[AWSアカウントを削除]を選択します。
3. アカウントを削除することを確認します。
   アカウントがDeep Security Managerから削除されました。

AWSアカウントを同期する

AWSアカウントを同期(同期)すると、Deep Security ManagerはAWS APIに接続して、最新のAWS EC2インスタンスとWorkSpaceインスタンスを取得して表示します。

強制的に同期を強制するには

1. Deep Security Managerで、[コンピュータ]をクリックします。
2. 左側で、AWSアカウントを右クリックし、[同期する]を選択します。[]をクリックします。

10分ごとに発生するバックグラウンド同期もあり、この間隔は設定できません。同期を強制すると、バックグラウンドの同期は影響を受けず、元のスケジュールに従って引き続き実行されます。

AWSアカウントの外部IDを管理する

注意:AWSアカウントの外部IDは、がクロスアカウントロールを使用してAWSアカウントを追加した場合にのみ使用されます。

トピック:

- "外部IDとは何ですか。" below
- "外部IDを設定する" below
- "外部IDを更新する" below
- "外部IDを取得する" on page 682
- "外部IDの取得を無効にする" on page 682

外部IDとは何ですか。

クロスアカウントロールのARNに加えて、外部IDは1つのAWSロールから別のAWSロールへのアクセスを許可するために使用されます。外部IDは、アカウントの役割を引き受けたいサードパーティのサービスによって提供されます。そのサービスが自分の代わりに機能することを信頼する場合は、その外部IDをクロスアカウントの役割に追加します。この場合、Deep Securityは、AWSアカウントに代わって外部IDを提供するサードパーティのサービスです。Deep Securityは、このアクセスを使用してAWSアカウントの情報を同期し、リソースの最新レコードを維持します。詳細については、次のAWSドキュメントを参照してください。AWSリソースへのアクセスを許可する際に外部IDを使用する方法

備考:

- 外部IDは、クロスアカウントロールを使用してAWSアカウントを追加する場合にのみ使用されます。
- 同じ外部IDが、クロスアカウントの役割を使用して追加されたすべてのAWSアカウントに使用されます。テナントごとにIDが1つあります。

外部IDを設定する

外部IDを設定することは、クロージャアカウントの役割を追加するプロセスの一歩です。詳細については、"クロスアカウントロールを使用したAWSアカウントの追加" on page 672 を使用したAWSアカウントの追加を参照してください。

外部IDを更新する

以前にクロスアカウントの役割を使用してAWSアカウントを追加した場合、ユーザ定義の外部IDが指定されている可能性があります。AWSのベストプラクティスとより整合性をとるために、管理者定義の外部IDに切り替えることをお勧めします。

注意: 以前にユーザ定義の外部IDで追加されたAWSアカウントは引き続き通常どおりに機能します。

ユーザまたは管理者定義の外部IDを使用しているかどうかを判断する

現在、ユーザ定義のIDか管理者定義の外部IDのどちらを使用しているかわからない場合は、次の手順に従って確認してください。

1. Deep Security Managerにログインします。
2. Computersをクリックします。
3. クロスアカウントロールを使用して追加されたAWSアカウントを右クリックし、[プロパティ][]を選択します。
4. 外部IDの横にアップデートリンクが表示されている場合は、ユーザ定義の外部IDが現在使用中であるため、アップデートする必要があります。アップデートリンクが表示されない場合は、マネージャ定義の外部IDが現在使用されているため、処理は必要ありません。
5. クロスアカウントロールを使用して、マネージャに追加されたアカウントごとにこの手順を繰り返します。

外部IDをマネージャからアップデートする

1. まだDeep Security Managerにログオンしていない場合は、アップデートするAWSアカウントを右クリックして、[プロパティ][]の順に選択します。
2. 外部IDの横に表示されるUpdateリンクをクリックします。Updateリンクが表示されなくなります。
3. 外部IDをメモします。次の手順でクロスアカウントの役割を設定する必要があります。
4. 外部IDが更新されたAWSアカウントにログインします。クロスアカウントロールのIAMポリシーを更新するには、古い外部IDを新しいアカウントIDに置き換えます。
5. プロパティ画面に戻り、適用をクリックして変更を適用します。

   アカウントのユーザ定義の外部IDがマネージャ定義の外部IDに更新されました。

6. クロスアカウントロールを使用して、マネージャに追加されたアカウントごとにこの手順を繰り返します。

Deep Security APIを使用して外部IDをアップデートする

1. 新しいマネージャ定義の外部IDがまだない場合は、`/api/awsconnectorsettings` エンドポイントを呼び出して取得します(`ExternalId` パラメータ).
2. クロスアカウントロールが設定されているAWSアカウントにログインします。クロスアカウントロールのIAMポリシーを更新するには、古い外部IDを新しいアカウントIDに置き換えま

す。クロスアカウントロールを使用してマネージャに追加されたアカウントごとに、この手順を繰り返します。

3. /api/awsconnectors エンドポイントを使用して、更新中のアカウントに対して Update 処理を実行します。その CrossAccountRoleARN パラメータは、現在のARNと同じ役割に設定されます。要求オブジェクトに外部IDを指定しないでください。

   アカウントのユーザ定義の外部IDが、マネージャ定義の外部IDに更新されました。

外部IDを取得する

クロスアカウントで使用する外部IDを取得するには、いくつかの方法があります。

[アカウントの追加]ウィザードを介して

- "クロスアカウントロールを使用したAWSアカウントの追加" on page 672 を使用したAWSアカウントの追加を参照してください。ここでは、ウィザードを使用して外部IDを取得する方法について説明します。

Deep Security APIを介して

- /api/awsconnectorsettings エンドポイントを呼び出して取得します(ExternalId パラメータ).

外部IDの取得を無効にする

外部IDへの不正アクセスを防ぐために、マネージャーで外部IDを表示および取得する機能を無効にしたい場合があります。IDを一度取得して、秘密管理者などの安全な場所に保存してから、他のすべてのユーザの検索を無効にすることができます。

注意: いつでも検索を有効にすることができます。

検索を無効にするには

1. Deep Security Managerにログインします。
2. 上部の[管理] をクリックします。
3. メイン画面で、[Security]タブをクリックします。
4. [AWS外部IDの取得と表示を有効にする]の選択を解除します。
5. [Save] をクリックします。

ヒント: 役割を使用して外部IDへのアクセスを禁止することもできます。詳細については、"ユーザロールの定義" on page 1541を参照してください。

AWSリージョンの管理

Amazon Web Servicesのリージョンを追加する

AWSクラウドアカウント追加ウィザードを使用してクラウドアカウントを追加するときにEC2リソースをホストしているAmazon Web Services (AWS) のリージョンが表示されない場合は、このリージョンを手動で追加します。

1. Deep Security Managerをホストしているサーバで、次のコマンドを入力します。

   ```
   dsm_c -action addregion -region REGION -display DISPLAY -endpoint ENDPOINT
   ```

   パラメータは次のとおりです。

パラメータ	説明	例
REGION	Amazon Web Servicesのリージョン ID。	ca-east-1
DISPLAY	AWSクラウドアカウント追加ウィザードで使用するリージョンの表示文字列。	Canada East (Ottawa)
ENDPOINT	リージョンで使用するAmazon Elastic Compute Cloud (EC2) エンドポイントの完全修飾ドメイン名。	ec2.ca-east-1.amazonaws.com

   注意: Deep Security ManagerがLinuxサーバで実行されている場合は、sudo を使用してコマンドを実行するか、rootなどのスーパーユーザアカウントを使用する必要があります。

2. 特定のAWSリージョンで信頼された証明書をインポートする必要がある場合は (ほとんどありません)、"信頼された証明書の管理" on page 1653を参照してください。

Amazon Web Servicesのリージョンを表示する

CLIを使用して追加したAWSリージョンを表示できます。

Deep Security Managerをホストしているサーバで、次のコマンドを入力します。

```
dsm_c -action listregions
```

注意: Deep Security ManagerがLinuxサーバで実行されている場合は、sudo を使用してコマンドを実行するか、rootなどのスーパーユーザアカウントを使用する必要があります。

Amazon Web Servicesのリージョンを削除する

CLIを使用して追加したAWSリージョンを削除できます。リージョンの既存のクラウドアカウントは削除されるまで引き続き使用できますが、管理者はそのリージョンに新しいクラウドアカウントを作成できなくなります。

1. Deep Security Managerをホストしているサーバで、次のコマンドを入力します。

   ```
   dsm_c -action listregions
   ```

2. 削除するリージョンのIDを検索します。
3. 次のコマンドを入力します。

   ```
   dsm_c -action removeregion -region REGION
   ```

   REGIONパラメータは必須です。

パラメータ	説明	例
REGION	Amazon Web Servicesのリージョン ID。	ca-east-1

注意: Deep Security ManagerがLinuxサーバで実行されている場合は、sudo を使用してコマンドを実行するか、rootなどのスーパーユーザアカウントを使用する必要があります。

AWS Outpostsで実行されているアカウントを保護する

Deep Securityは、AWS Outposts で実行されるAWSアカウントをサポートします。

AWS Outpostsのアカウントを保護するには

1. "マネージャーのインスタンスの役割を使用したAWSアカウントの追加" on page 666を使用してAWSアカウントを追加します。.

   注意: AWS アカウントをDeep Security Managerに追加すると、Computersページには、Outpostが接続されているAWSリージョンの一部としてリソースが表示されます。EC2インスタンスの場合、OutpostラックのARNがインスタンスのメタデータに追加されます。

2. "Amazon EC2およびWorkSpacesへのAgentのインストール" on page 543してください。
3. Agentを有効化します ("Agentの有効化" on page 559を参照してください)。
4. "ポリシーの作成" on page 719します。

注意: 高可用性がサポートされています。詳細については、"複数のノードにDeep Security Managerをインストールする" on page 505にインストールするを参照してください。

Azureインスタンスを追加する

Deep Security用のAzureアプリケーションの作成

ご使用の動作環境で、Microsoft Entra IDのグローバル管理者ロールとAzureサブスクリプションのサブスクリプション所有者ロールの両方が指定されたアカウントを使用して、Deep Security ManagerがAzureリソースにアクセスできるようにすることが適していない場合があります。代わりに、Azureリソースへの読み取り専用アクセスを提供するDeep Security Manager用のAzureアプリケーションを作成することができます。

Azureサブスクリプションが複数あり、すべてのサブスクリプションが同じActive Directoryに関連付けられている場合は、すべてのサブスクリプションで利用できる単一のDeep Security Azureアプリケーションを作成できます。

Azureアプリケーションを作成するには、次の手順を実行する必要があります:

1. "適切な役割を割り当てる" below
2. "Azureアプリケーションを作成する" below
3. "AzureアプリIDとActive Directory IDを記録する" on the next page
4. "サブスクリプションIDを記録する" on page 687
5. "Azureアプリケーションに役割とコネクタを割り当てる" on page 687

適切な役割を割り当てる

Azureアプリケーションを作成するには、アカウントにMicrosoft Entra IDのユーザ管理者ロールとAzureサブスクリプションのユーザアクセス管理者ロールが必要です。これらのロールをAzureアカウントに割り当ててから進めてください。

Azureアプリケーションを作成する

1. [Microsoft Entra ID] ブレードで、[アプリの登録] をクリックします。
2. [New registration] をクリックします。
3. [Name] (Deep Security Azureコネクタなど) を入力します。
4. [Supported account types] で、[Accounts in this organizational directory only] を選択します。
5. [Register] をクリックします。

   [アプリ登録] リストに、指定したNameと共にAzureアプリケーションが表示されます。

AzureアプリIDとActive Directory IDを記録する

1. [アプリ登録]リストで、Azureアプリケーションをクリックします。
2. [Application (client) ID] を記録します。
3. [Directory (tenant) ID] を記録します。

アプリケーションシークレットを作成するか、アプリケーション証明書をアップロードします。

1. 証明書とシークレットタブで、使用するアプリケーション資格情報の種類を選択します。
   - オプション1: クライアントシークレット(アプリケーションパスワード)
   - オプション2: 証明書

   Azureでは複数のアプリケーション資格情報を作成できますが、Deep Security Managerでは、Azureアカウントに1つの資格情報(アプリケーションシークレットまたはアプリケーション証明書) のみが必要でした。

2. 使用する資格情報の種類に応じて、オプション1またはオプション2(下記) のいずれかの手順に従います。

オプション1: クライアントシークレットを作成する(アプリケーションパスワード)

1. [New client secret] をクリックします。
2. クライアントシークレットの[説明]を入力します。
3. 適切な [Duration] を選択します。この時間が経過すると、クライアントシークレットが期限切れになります。
4. [Add] をクリックします。

   クライアントシークレットの[Value]が表示されます。

5. クライアントシークレットの値を記録します。AzureアプリケーションをDeep Securityに登録する際に、アプリケーションパスワードとして使用する必要があります。

   クライアントシークレットの値は一度しか表示されないため、この時点で必ず記録してください。ここで記録しておかないと、後でクライアントシークレットを再生成して新しい値を取得することが必要になります。

   クライアントシークレットの値が期限切れになった場合は、再生成して、古い値が関連付けられているAzureアカウントで値を更新する必要があります。

オプション2: アプリケーション証明書をアップロードする

1. X.509 PEMテキスト形式の証明書を準備します。

   証明書は公開署名または自己署名のいずれかであり、有効期限が切れていない必要があります。秘密でプライベートキーが保護されている場合、Deep Security ManagerでAzureアカウントを設定する際に証明書のプライベートキーとオプションのパスフレーズまたは秘密が必要です。RSAキーのサイズは少なくとも2048ビットでなければなりません。

   Deep Security Managerは現在、バイナリ形式の証明書をサポートしていません。

2. [Upload certificate]ボタンをクリックします。
3. アップロードする証明書ファイルを選択してください。
4. [Add] をクリックします。

無効な資格情報または構成 (例えば、RSAキーが短すぎる) を提供すると、Azureコネクタは「Azure Entra IDに認証できません。資格情報または構成が無効です」というエラーメッセージを表示します。

サブスクリプションIDを記録する

1. 左側の [All Services] に移動し、[Subscriptions] をクリックします。

   サブスクリプションのリストが表示されます。

   サブスクリプションが左側に表示されない場合は、画面の上部にある検索ボックスを使用して検索します。

2. 各サブスクリプションに関連付けたいAzureアプリケーションのサブスクリプションIDを記録してください。後でAzureアカウントをDeep Securityに追加する際にIDが必要になります。

Azureアプリケーションに役割とコネクタを割り当てる

1. すべてのサービス > サブスクリプションの下で、Azureアプリケーションに関連付けたいサブスクリプションをクリックします。

   必要に応じて、後で別のサブスクリプションをAzureアプリケーションに関連付けることができます。

2. [Access Control (IAM)] をクリックします。
3. メインペインで、追加をクリックし、メニューから役割の割り当てを追加を選択します。
4. [Role] で「Reader」と入力し、表示される [Reader] ロールをクリックします。
5. [Assign access to] で、[User, user group, or service principal] を選択します。
6. [メンバーを選択] で、Azureアプリケーションの[名前] (Deep Security Azure Connectorなど) を入力します。

"Azureアプリケーションを作成する" on page 685の手順3で選択した[名前]と共に、Azureアプリケーションが表示されます。

7. [Save] をクリックします。
8. Azureアプリケーションを別のサブスクリプションに関連付ける場合は、そのサブスクリプションに対してこの手順 ("Azureアプリケーションに役割とコネクタを割り当てる" on the previous page) を繰り返します。

この時点で、"Deep SecurityへのMicrosoft Azureアカウントの追加" belowの手順に従うことにより、Deep Securityを設定してAzure仮想マシンを追加できるようになります。

Deep SecurityへのMicrosoft Azureアカウントの追加

Deep Security ManagerをインストールしたらMicrosoft AzureアカウントをDeep Security Managerに接続してMicrosoft Azure仮想マシンを追加および保護できます。仮想マシンは [コンピュータ] 画面に表示され、その他のコンピュータと同じように管理できます。

このセクションのトピック:

- "Azureアカウントを追加することのメリットは何ですか? " below
- "Azureアカウントのプロキシを設定する" on the next page
- "Microsoft AzureアカウントからDeep Securityに仮想マシンを追加する" on the next page
- "Azure Resource Managerコネクタを使用してAzureクラシック仮想マシンを管理する" on page 690
- "Azureアカウントを削除する" on page 690
- "Azureアカウントを同期する" on page 691

Azureアカウントを追加することのメリットは何ですか?

個別のAzure仮想マシン(Deep Security Manager→ コンピュータ→コンピュータの), の追加) ではなく、Azureアカウント(Deep Security Manager→ コンピュータ→Azureアカウントの追加) の追加による利点は次のとおりです。

- Azure仮想マシンインベントリの変更は、自動的にDeep Security Managerに反映されます。たとえば、Azureでいくつかのインスタンスを削除すると、それらのインスタンスは自動的にマネージャから消えます。対照的に、の[コンピュータ]→[コンピュータの追加]を使用している場合、Azureから削除されたAzureインスタンスは、手動で削除されるまでManagerに残ります。

- 仮想マシンはマネージャで独自のブランチに編成されており、どのAzureインスタンスが保護されており、保護されていないかを簡単に確認できます。Azureアカウントがないと、すべての仮想マシンがComputersの同じルートレベルに表示されます。

Azureアカウントのプロキシを設定する

Azureアカウントのリソースにプロキシサーバを使用してアクセスするようDeep Security Managerを設定できます。詳細については、"プロキシ経由でクラウドアカウントに接続する" on page 1461を参照してください。

Microsoft AzureアカウントからDeep Securityに仮想マシンを追加する

以下の手順に従って、Microsoft AzureアカウントをDeep Securityに追加します。

1. 開始する前に、Deep Security用のAzureアプリケーションを作成します。
2. Deep Security Managerで、[コンピュータ]→[追加]→[Azureアカウントの追加]に移動します。

   注意: Deep Security Manager 12.0以降では、「クイック」モードを利用できなくなりました。以前のリリースでクイックモードを使用した場合でも、お使いの環境に影響はありません。新しいAzureクラウドアカウントのすべてで、詳細方式を使用する必要があります。

3. [表示名]を入力したら、手順1で記録した次のAzureアクセス情報を入力します。
   - ディレクトリID
   - サブスクリプションID
   - アプリケーションID

   注意: AzureクラシックコネクタからAzure Resource Managerコネクタにアップグレードする場合は、既存のコネクタの表示名とサブスクリプションIDが使用されます。

   注意: Azureサブスクリプションが複数ある場合は、[サブスクリプションID]フィールドで1つだけサブスクリプションを指定します。残りは後から追加できます。

4. 使用するアプリケーション資格情報の種類(Password または Certificate)を選択し、資格情報を指定します。
   - パスワード:
     - [Application Password]フィールドに、クライアントシークレットを入力します。
   - 証明書:
     - [Certificate]の横にある[をクリックしファイル]を選択して証明書をアップロードします。
     - 秘密鍵の横にある[をクリックしファイル]を選択して、秘密鍵をアップロードします。

- 秘密鍵がパスワードで保護されている場合は、Private Key Password(オプション) に入力します。

注意: 証明書はX.509 PEMテキスト形式で、有効期間内である必要があります。バイナリ形式はサポートされていません。

5. [次へ] をクリックします。
6. 概要情報を確認し、[完了] をクリックします。
7. 毎回異なるサブスクリプションIDを指定して、Azureサブスクリプションごとにこの手順を繰り返します。

Azureの仮想マシンは、Deep Security Managerのコンピュータページの独自の項目の下に表示されます。

ヒント: Azureアカウント名を右クリックし、[同期する]をクリックして、Azure VMの最新セットを確認できます。

ヒント: このアカウントに含まれるすべての仮想マシンが表示されます。特定の仮想マシンのみを表示する場合は、スマートフォルダを使用して結果を絞り込みます。詳細については、"スマートフォルダによるコンピュータの動的なグループ化" on page 1594を参照してください。

注意: 以前このAzureアカウントで仮想マシンを追加したことがある場合は、[コンピュータ] ツリーのこのアカウントの下に仮想マシンが移動します。

Azure Resource Managerコネクタを使用してAzureクラシック仮想マシンを管理する

Azure Resource Managerコネクタでは、Azureクラシックコネクタを使用して追加した仮想マシンも管理できます。このため、1つのコネクタでAzureクラシック仮想マシンとAzure Resource Manager仮想マシンの両方を管理することが可能です。

詳細については、"新しいAzure Resource Manager接続機能へのアップグレードについて" on the next pageを参照してください。

1. [コンピュータ] 画面で、[コンピュータ] ツリーの [Azureクラシックポータル] を右クリックし、[プロパティ] をクリックします。
2. [Resource Manager接続を有効化] をクリックします。
3. [次へ] をクリックします。該当する前述の手順に従います。

Azureアカウントを削除する

Deep Security ManagerからAzureアカウントを削除すると、そのアカウントはDeep Securityデータベースから完全に削除されます。これによるAzureアカウントへの影響はありません。Deep Security Agentがインストールされた仮想マシンは引き続き保護されますが、セキュリティ上のアップデートは受け取りません。これらの仮想マシンを後で同じAzureアカウントからインポートする場合、Deep Security Agentは次の予約アップデート時に最新のセキュリティアップデートをダウンロードします。

1. [コンピュータ] 画面を開き、ナビゲーションパネルでMicrosoft Azureアカウントを右クリックし、[クラウドアカウントの削除...] を選択します。
2. アカウントを削除することを確認します。
3. アカウントはDeep Security Managerから削除されます。

Azureアカウントを同期する

Azureアカウントを同期(同期) すると、Deep Security ManagerはAzure APIに接続し、Azure VMの最新のセットを取得して表示します。

強制的に同期を強制するには

1. Deep Security Managerで、[コンピュータ] をクリックします。
2. 左側でAzureアカウントを右クリックし、[Synchronize Now]を選択します。

10分ごとに発生するバックグラウンド同期もあり、この間隔は設定できません。同期を強制すると、バックグラウンドの同期は影響を受けず、元のスケジュールに従って引き続き実行されます。

新しいAzure Resource Manager接続機能へのアップグレードについて

次にAzureクラウドアカウントをDeep Security Managerに追加しようとすると、新しいResource Manager接続機能にアップグレードすることを示すメッセージが表示されます。基本的に、この新しい機能により、Deep SecurityはResource Managerインタフェースを使用してAzure仮想マシンに接続できます。Azureユーザには周知のことですが、Azureの初期設定のデプロイモデルは、クラシックモデルから新しいResource Managerに変更になっています。初期設定ではこのモデルを使用して新しいリソースが配信されるため、Deep Securityはこれらの VM リソースをResource Managerインタフェースとの通信が可能な場合にのみ[コンピュータ]ページにのみ表示できます。したがって、Deep Securityをこの新しい機能にアップグレードできるようにした場合、Resource Manager配置モデルまたは従来の配置モデルで配置されたVMリソースが[コンピュータ]ページに表示されます。

次の2つの点に注意してください。

- この新しい機能をDeep Security 10にアップグレードできます。Azure Marketplaceコンソール用の新しいDeep Security Manager VMですでに使用可能であり、アップグレードは必要ありませ

ん。

- このアップグレードを実行するまで、Resource Managerを使用して配置されたVMはDeep Securityによって完全に保護されていますが、[コンピュータ]ページでVMを確認できるようにするには、コンピュータオブジェクトとして追加する必要があります。詳細については、"Deep SecurityでAzureサブスクリプションの一部の仮想マシンが表示されない" on page 1982を参照してください。

GCPインスタンスを追加する

Google Cloud Platformサービスアカウントを作成する

以下は、Deep Securityで使用するGoogle Cloud Platform(GCP) サービスアカウントを作成するために必要なすべての情報です。

ヒント: Deep Security Managerで使用するGCPサービスアカウントを作成する理由については、"GCPアカウントを追加するとどのようなメリットがありますか? " on page 701。

トピック:

- "前提条件 : Google APIを有効にする" below
- "GCPサービスアカウントを作成する" on the next page
- "GCPサービスアカウントにプロジェクトを追加する" on page 697
- "複数のGCPサービスアカウントを作成する" on page 700

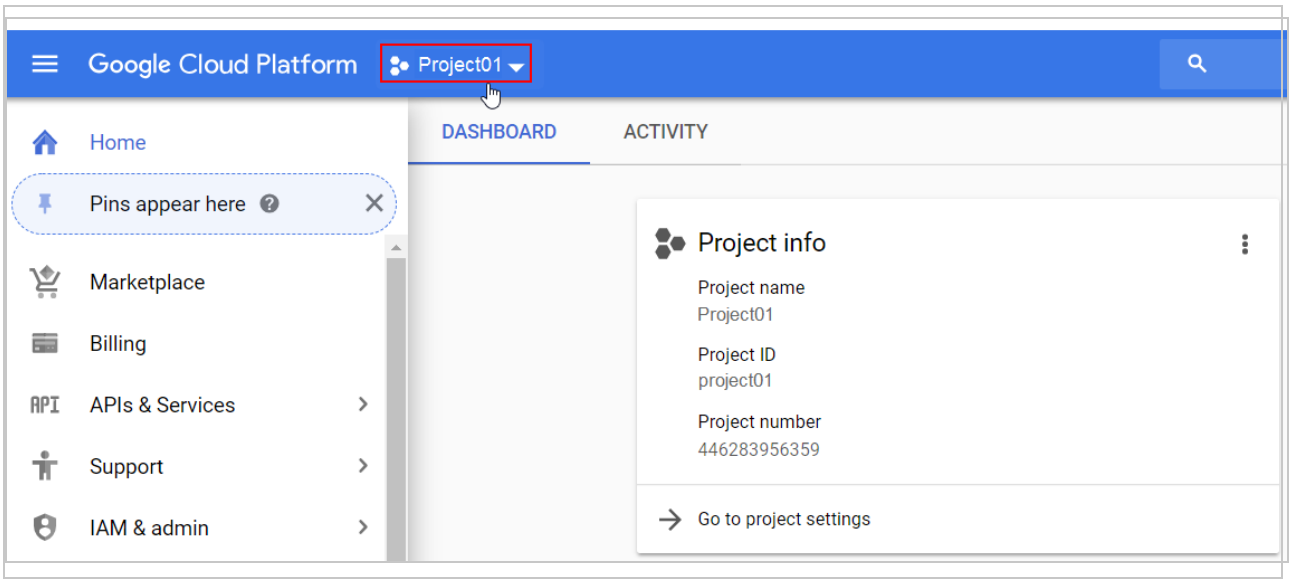
前提条件 : Google APIを有効にする

Deep Security ManagerのGCPサービスアカウントを作成する前に、既存のGCPアカウントでいくつかのGoogle APIを有効にする必要があります。

次の手順に従って、各プロジェクト内でこれらのAPIを有効にします。

1. 既存のGCPアカウントを使用してGoogle Cloud Platformにログインします。このアカウントは、Deep Securityで保護するVMを含むすべてのGCPプロジェクトにアクセスできる必要があります。
2. 画面の上部で、Deep Security Managerに追加するVMを含むプロジェクトを選択します。複数のプロジェクトがある場合は、後から選択できます。

   次に例を示します。Project01



3. 上部にある[Google Cloud Platform]をクリックして、[ホーム]画面を開いていることを確認します。
4. 左側のツリー表示から、[APIs&サービス]→[ダッシュボード]の順に選択します。
5. [+ ENABLE APIS ANDSERVICES]をクリックします。
6. 検索ボックスに cloud resource manager API と入力し、[Cloud Resource Manager API]ボックスをクリックします。
7. [ENABLE]をクリックします。
8. 手順5～7を繰り返し、compute engine API と入力して[Compute Engine API]ボックスをクリックします。
9. この手順の手順1～9を、Deep Security Managerに追加するVMを含む他のプロジェクトに対して繰り返します。

GCPでAPIを有効または無効にする方法の詳細については、Googleの次のページを参照してください。

https://cloud.google.com/apis/docs/getting-started

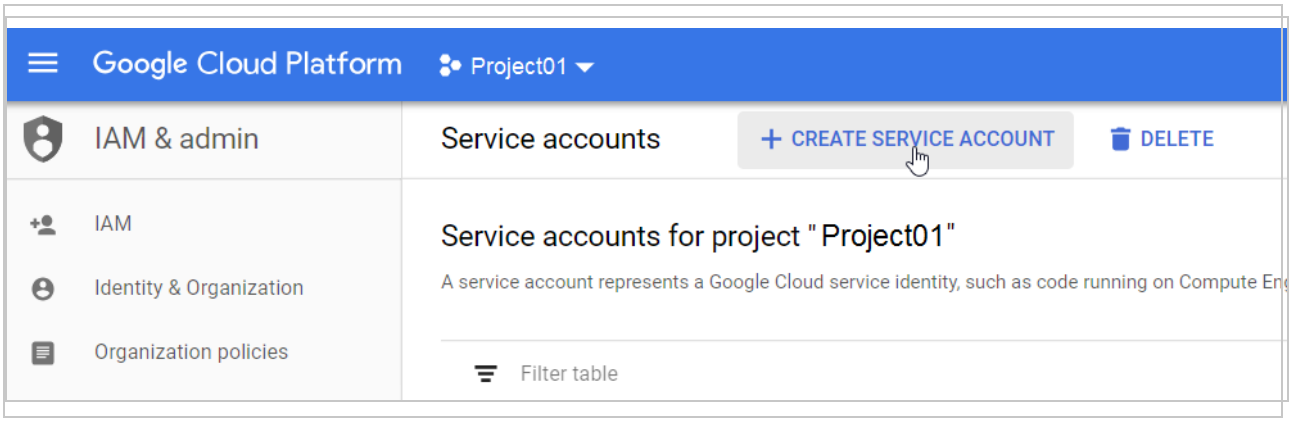
GCPサービスアカウントを作成する

注意: サービスアカウントとは、特定の種類のGoogleアカウントで、個々のエンドユーザではなく、アプリケーションまたはVMに関連付けられています。Deep Security Managerは、Google APIを呼び出すためのサービスアカウントのIDを想定しているため、ユーザは直接関与しません。

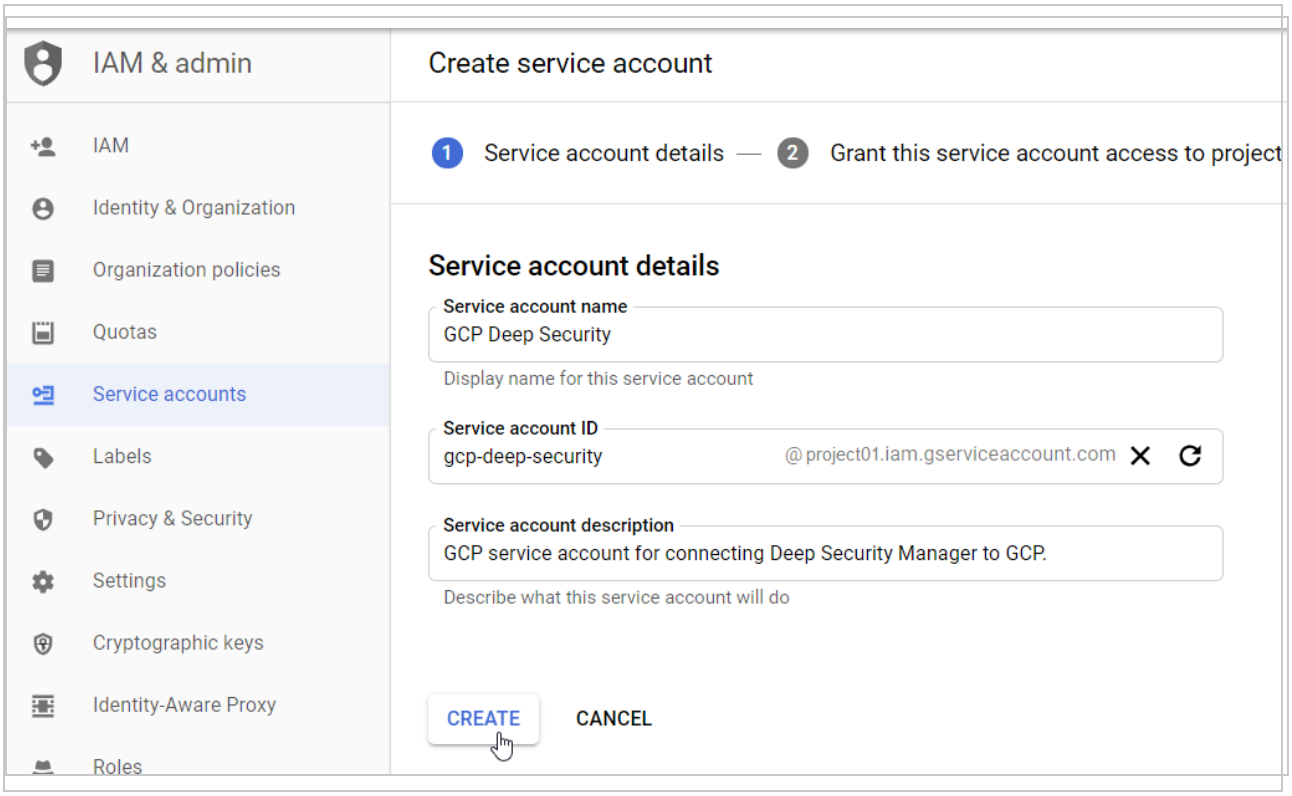
Deep Security Managerのサービスアカウントを作成するには、次の手順に従ってください。

1. 開始する前に、GCP APIが有効になっていることを確認してください。"前提条件:Google APIを有効にする" on the previous pageを有効にします。

2. 既存のGCPアカウントを使用してGoogle Cloud Platformにログインします。
3. 上部で、プロジェクトを選択します。複数のプロジェクトがある場合は、いずれかを選択できます。例：Project01。
4. 上部にある[Google Cloud Platform]をクリックして、[ホーム]画面を開いていることを確認します。
5. 左側のツリー表示から、[IAM&admin]→[サービスアカウント]の順に選択します。
6. [+サービスの作成]をクリックします。



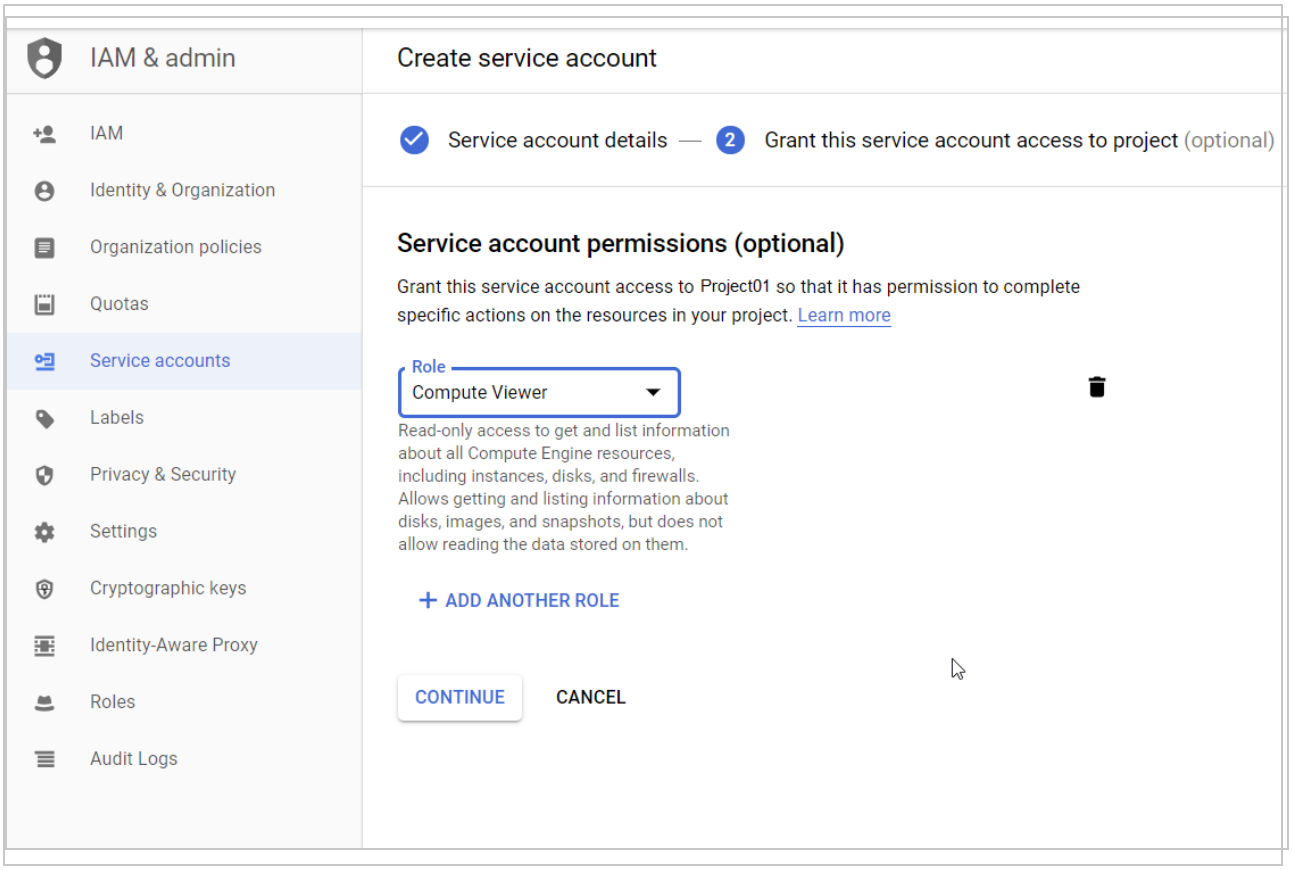
7. サービスアカウント名、ID、および説明を入力します。



例：

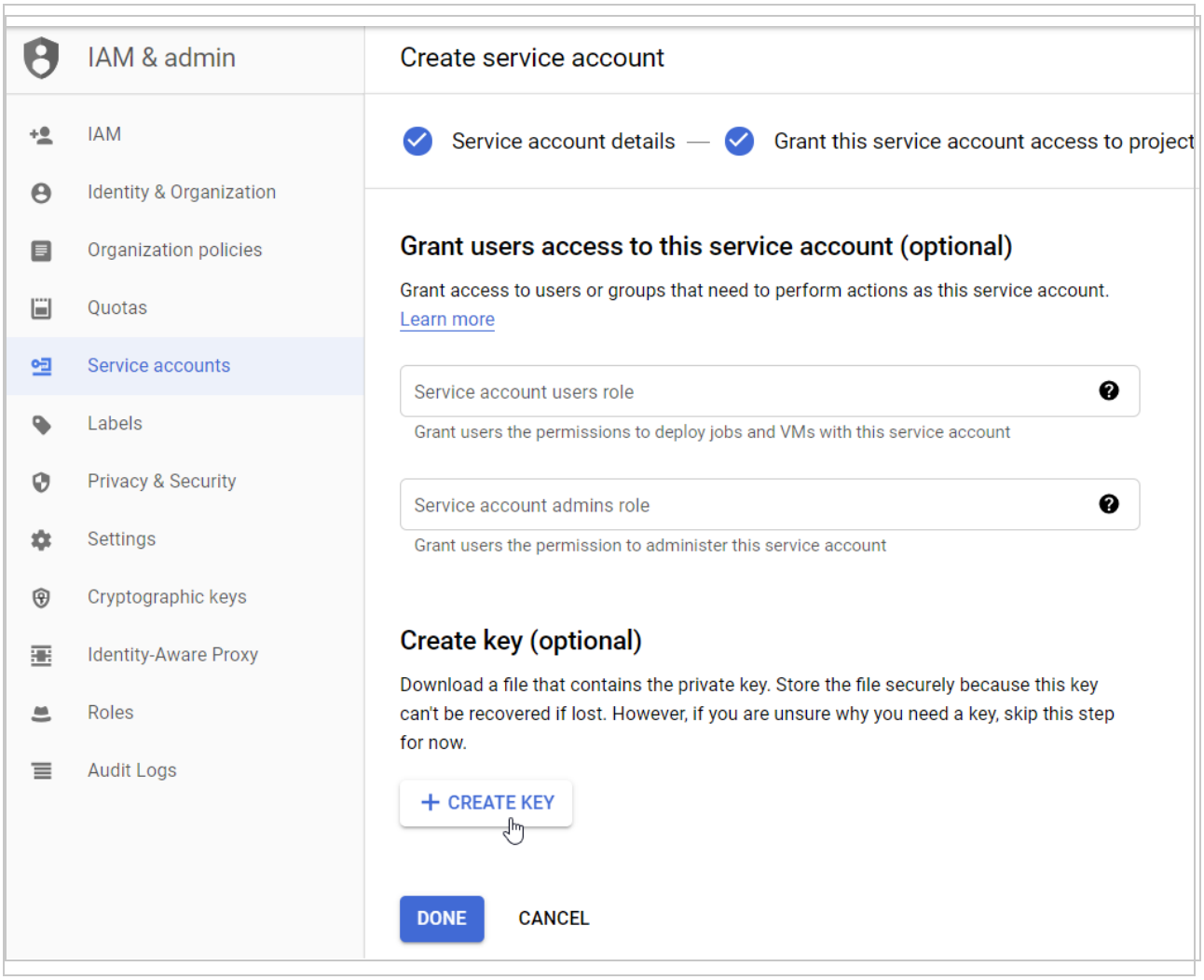
- サービスアカウント名：GCP Deep Security
- サービスアカウントID：gcp-deep-security@<your_project_ID>.iam.gserviceaccount.com
- サービスアカウントの説明：GCP service account for connecting Deep Security Manager to GCP.

8. [Create]をクリックします。
9. 役割の選択ドロップダウンリストで、Compute Engine> Compute Viewerの役割を選択するか、フィルタ対象の種類領域内をクリックして、compute viewer と入力します。
10. [CONTINUE]をクリックします。

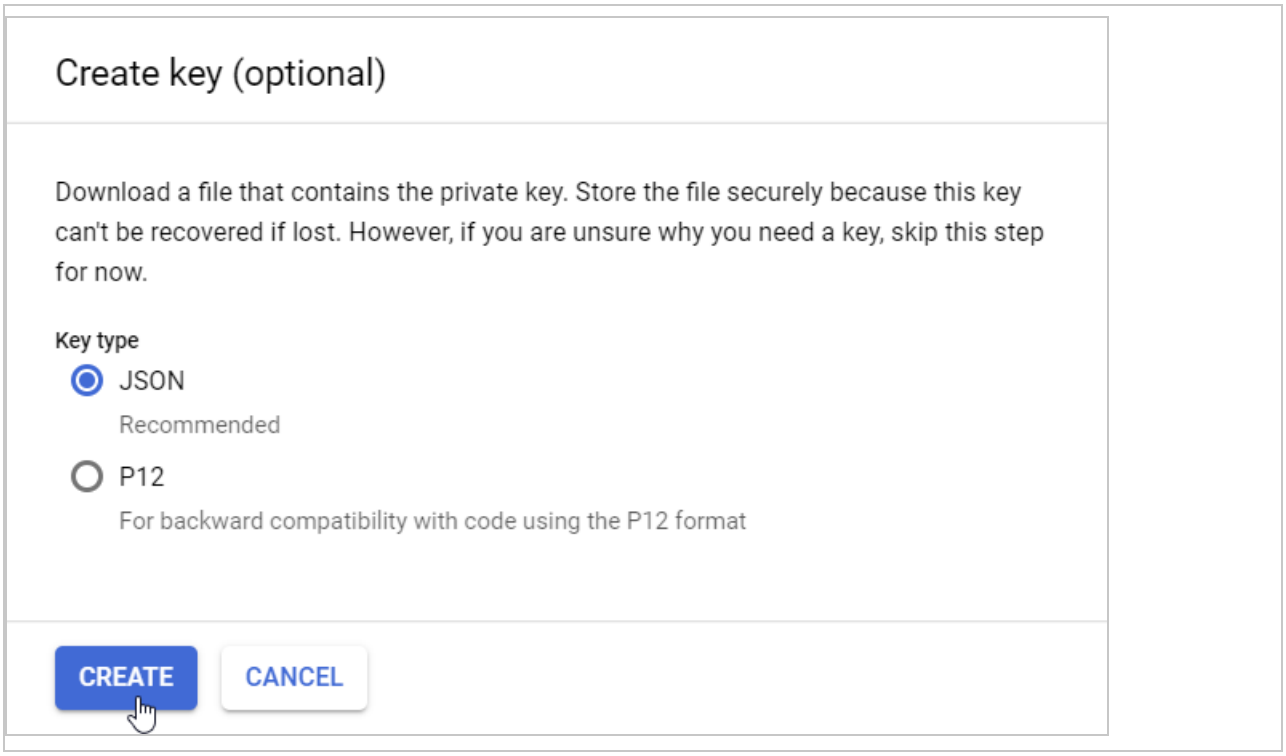


Compute Viewerの役割が割り当てられました。

11. + CREATE KEYをクリックします。



12. JSON を選択し、[CREATE]をクリックします。



キーが生成され、JSONファイルに配置されます。

13. キー(JSONファイル) を安全な場所に保存します。
14. JSONファイルは、後でアップロードするためにDeep Security Managerからアクセス可能な場所に置いてください。ファイルを移動または配布する必要がある場合は、安全な方法を使用してファイルを移動または配布してください。
15. [DONE]をクリックします。

これで、必要な役割を持つGCPサービスアカウントと、JSON形式のサービスアカウントキーが作成されました。サービスアカウントは、選択したプロジェクト(Project01), では作成されますが、追加のプロジェクトに関連付けることもできます。詳細については、次のセクションを参照してください。

> 注意: IAMアクセス許可がシステム全体に適用されるまでには60秒～7分かかります。詳細については、このGoogleの記事 を参照してください。

GCPサービスアカウントにプロジェクトを追加する

GCPに複数のプロジェクトがある場合は、作成したサービスアカウントに関連付ける必要があります。その後、Deep Security Managerにサービスアカウントを追加すると、すべてのプロジェクト(および基に

なるVM) がDeep Security Managerに表示されます。

注意: プロジェクトがたくさんある場合は、複数のGCPアカウントに分割することもできます(後述の説明を参照) 。マルチGCPアカウントのセットアップの詳細については、"複数のGCPサービスアカウントを作成する" on page 700を参照してください。

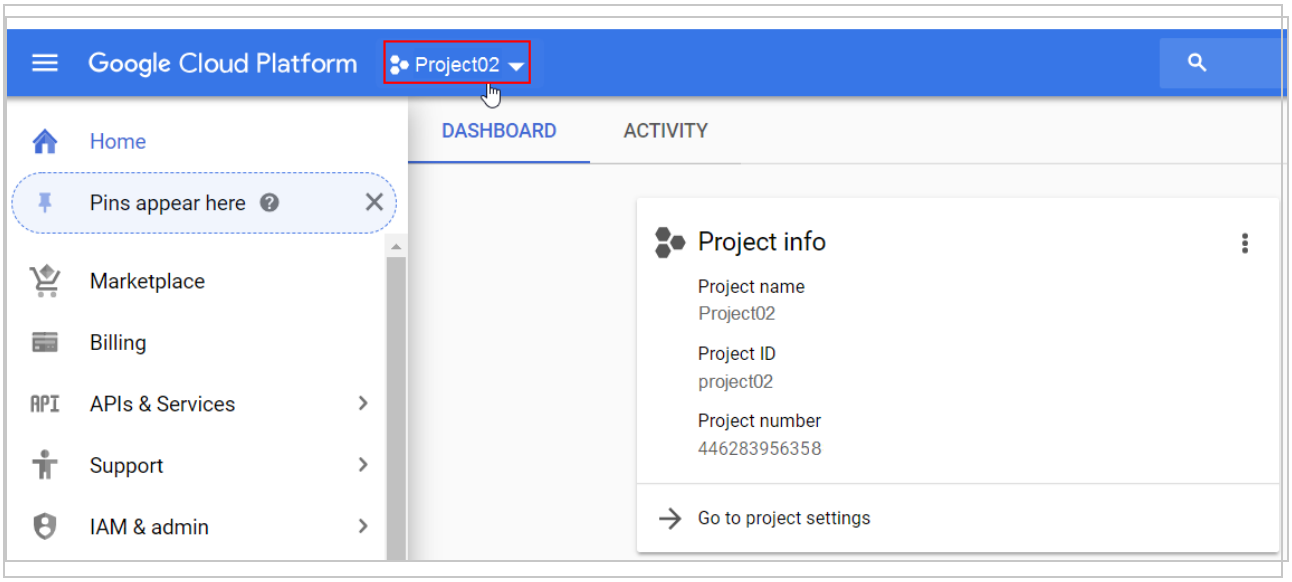
追加のプロジェクトを1つのサービスアカウントに関連付けるには、次の手順に従ってください。

1. 開始する前に、"前提条件 : Google APIを有効にする" on page 692 および "GCPサービスアカウントを作成する" on page 693を作成します。
2. 作成したGCPサービスアカウントのメールを次のように指定します。
   a. Google Cloud Platformの上部にあるドロップダウンリストから、GCPサービスアカウントを作成したプロジェクトを選択します(例 : Project01).
   b. 左側で、[IAM&管理者]→[サービスアカウント]の順に展開します。
   c. メイン画面で、[メール]列の下にあるGCPサービスアカウントのメールを確認します。例 :

      gcp-deep-security@project01.iam.gserviceaccount.com

      サービスアカウントのメールには、そのサービスが作成されたプロジェクトの名前が含まれています。

   d. このアドレスをメモするか、クリップボードにコピーしてください。
3. Google Cloud Platformの場合は、上部のドロップダウンリストから*別*のプロジェクトを選択してください。例 : Project02。



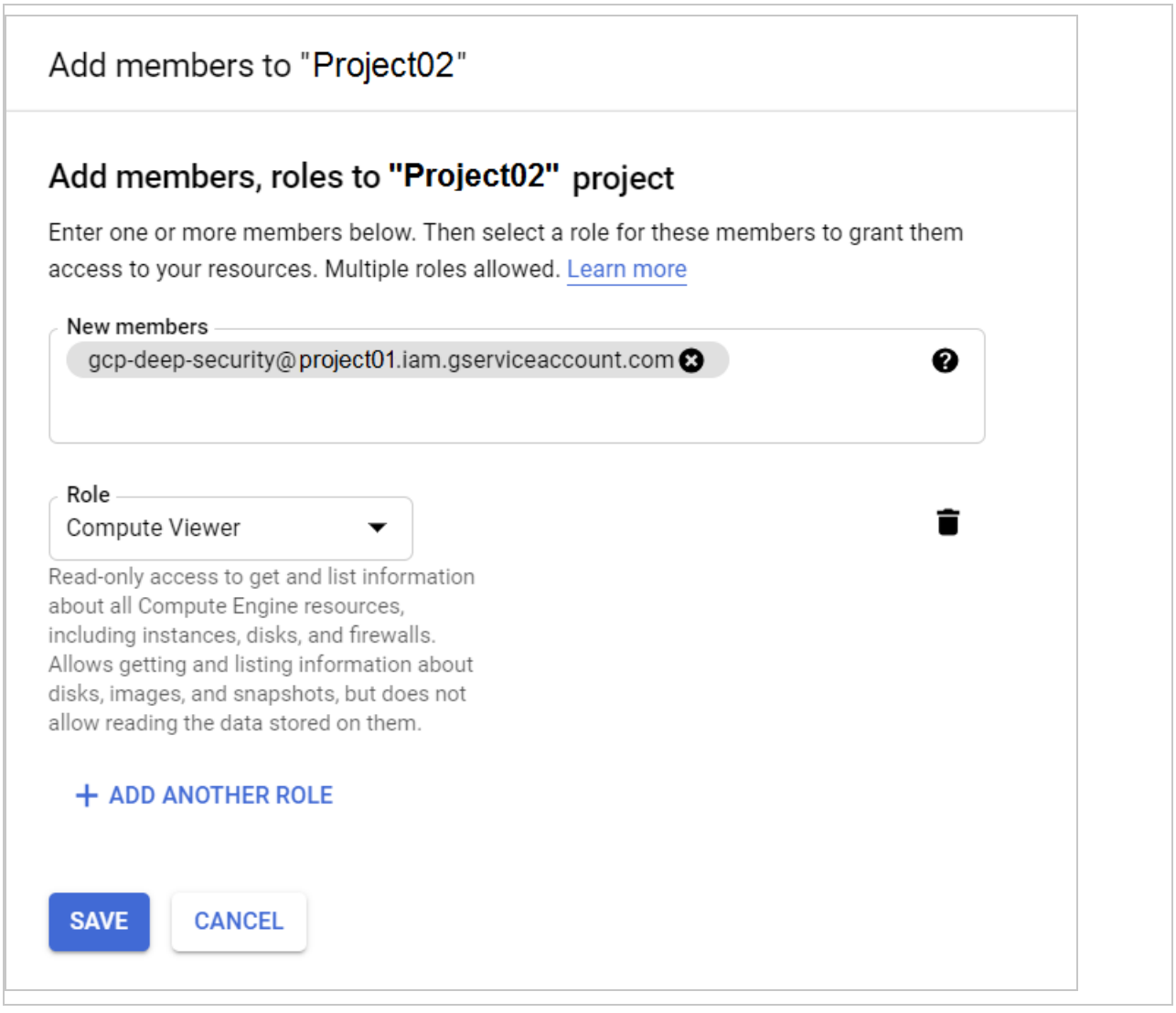
4. 上部にある[Google Cloud Platform]をクリックして、[ホーム]画面を開いていることを確認します。

5. 左側のツリー表示から、[IAM&admin]→[IAM]の順にクリックします。
6. メイン画面上部の[ADD]をクリックします。
7. [新規メンバー] [ ]フィールドに、Project01 GCPサービスアカウントのメールアドレスを貼り付けます。例：

   gcp-deep-security@project01.iam.gserviceaccount.com

   ヒント: また、メールアドレスの入力を開始して、フィールドに自動入力することもできます。

8. 役割の選択[ ]ドロップダウンリストで、Compute Engine> Compute Viewer の役割を選択するか、の内部をクリックして領域をフィルタ処理し、compute viewer と入力して compute viewer と入力します。



Compute Viewerの役割を持つサービスアカウントがProject02に追加されました。

9. [SAVE] をクリックします。
10. GCPサービスアカウントに関連付けるプロジェクトごとに、この手順で手順1～9を繰り返します。

サービスアカウントの作成方法の詳細については、Googleの次のページを参照してください。

https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances

作成したGCPアカウントをDeep Security Managerに追加する準備ができました。"Google Cloud Platformアカウントを追加する" belowに進んでください。

複数のGCPサービスアカウントを作成する

通常、では、Deep Security Managerの単一のGCPサービスアカウントを作成し、すべてのプロジェクトをDeep Security Managerに関連付けます。この設定は簡単で、少数のプロジェクトで小規模な組織にも適しています。ただし、多数のプロジェクトがある場合は、同じGCPサービスアカウントの下にあるすべてのプロジェクトを管理しにくくなる可能性があります。このシナリオでは、プロジェクトを複数のGCPサービスアカウントに分割できます。プロジェクトを組織の財務/営業部門に分散していると仮定して、これを設定する方法は次のとおりです。

1. Deep Security ManagerのFinance GCP Deep Security GCPサービスアカウントを作成します。
2. 財務関連プロジェクトをFinance GCP Deep Securityに追加します。
3. Deep Security ManagerのMarketing GCP Deep Security GCPサービスアカウントを作成します。
4. マーケティング関連のプロジェクトをMarketing GCP Deep Securityに追加します。

   詳細な手順については、"GCPサービスアカウントを作成する" on page 693 および "GCPサービスアカウントにプロジェクトを追加する" on page 697

5. GCPサービスアカウントを作成したら、"Google Cloud Platformアカウントを追加する" belowの手順に従って、Deep Security Managerに1つずつ追加します。

Google Cloud Platformアカウントを追加する

Google Cloud Platform(GCP) アカウントをDeep Securityに追加すると、そのアカウントに関連付けられているすべてのGCP VMインスタンスがDeep Security Managerにインポートされ、次の場所に表示されます。

- Deep Security Manager> Computers>*自分の_GCP_service_account>_GCP_プロジェクト*

インポートしたGCP VMインスタンスは、他のコンピュータと同様に管理できます。

注意: Deep Security ManagerにGCPアカウントを追加することは、Deep Security APIを介してGCPコネクタを追加することに相当します。

トピック:

- "GCPアカウントを追加するとどのようなメリットがありますか? " below
- "GCPアカウントのプロキシ設定を行う" below
- "Deep SecurityにGCPアカウントを追加する" belowにGCPアカウントを追加する
- "GCPアカウントを削除する" on page 703
- "GCPアカウントを同期する" on page 704

GCPアカウントを追加するとどのようなメリットがありますか?

個別のGCP VM(Deep Security Manager→ コンピュータ→コンピュータ), の追加) を追加する代わりに、(Deep Security Manager→ コンピュータ→GCPアカウントの追加 を使用して) GCPアカウントを追加すると、次の利点があります。

- GCP VMインベントリの変更は、自動的にDeep Security Managerに反映されます。たとえば、GCPでいくつかのVMインスタンスを削除した場合、それらのインスタンスは自動的にマネージャから非表示になります。対照的に、[コンピュータ]→[コンピュータの追加]を使用している場合、削除したGCPインスタンスは手動で削除するまでマネージャに残ります。
- VMはマネージャでプロジェクトに編成されているため、どのGCP VMが保護されており、保護されていないかを簡単に確認できます。GCPアカウントがない場合、すべてのGCP VMがComputersの同じルートレベルに表示されます。

GCPアカウントのプロキシ設定を行う

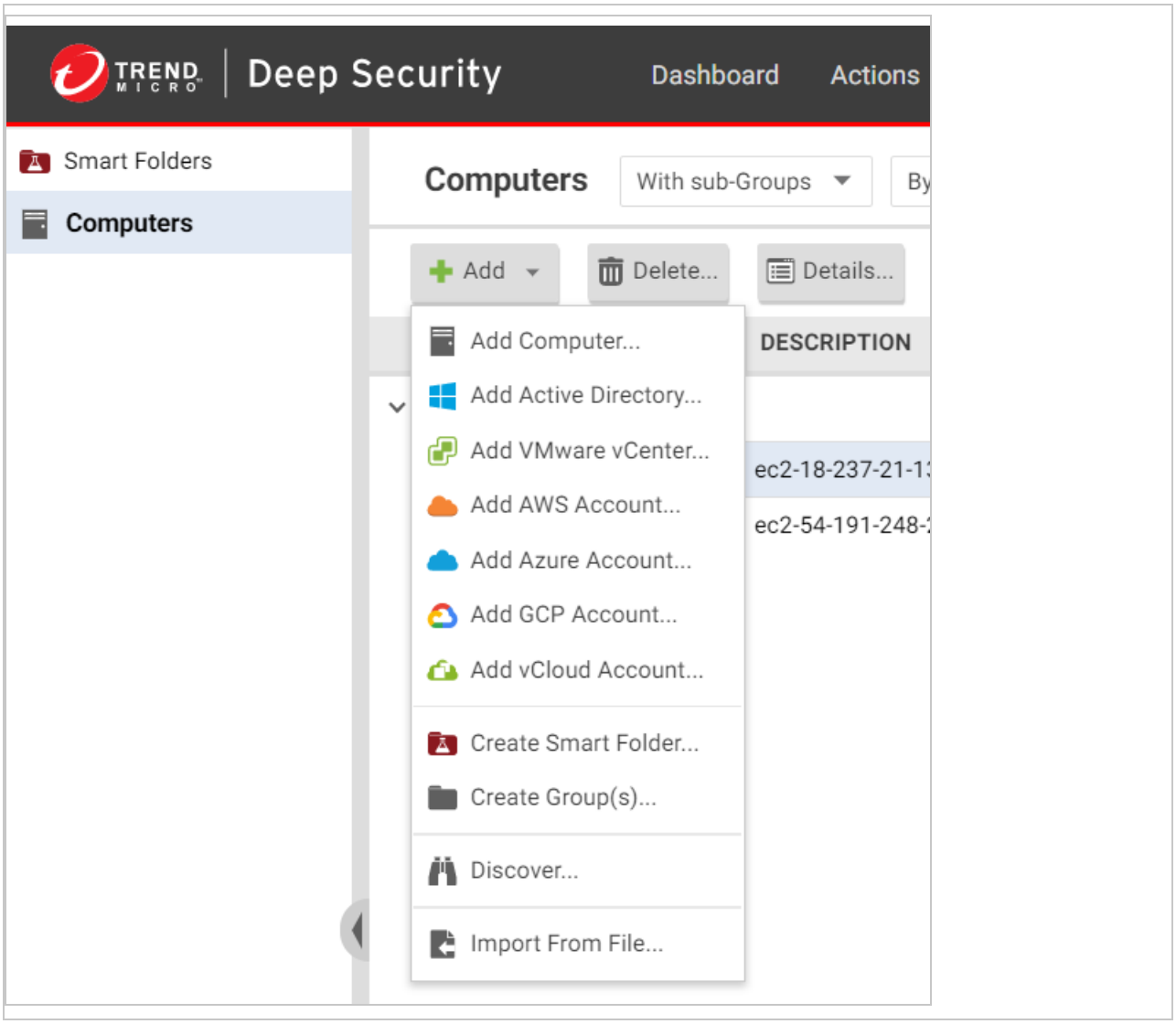
オプションで、Deep Security Managerでプロキシサーバを使用してGCPサービスアカウント内のリソースにアクセスするように設定できます。詳細については、"プロキシ経由でクラウドアカウントに接続する" on page 1461を参照してください。

Deep SecurityにGCPアカウントを追加する

Deep Security ManagerにGCPアカウントを追加するには

1. 完了していない場合は、"Google Cloud Platformサービスアカウントを作成する" on page 692を作成します。

2. Deep Security Managerで、[Computers]→[Add]→[Add GCP Account]の順に選択します。

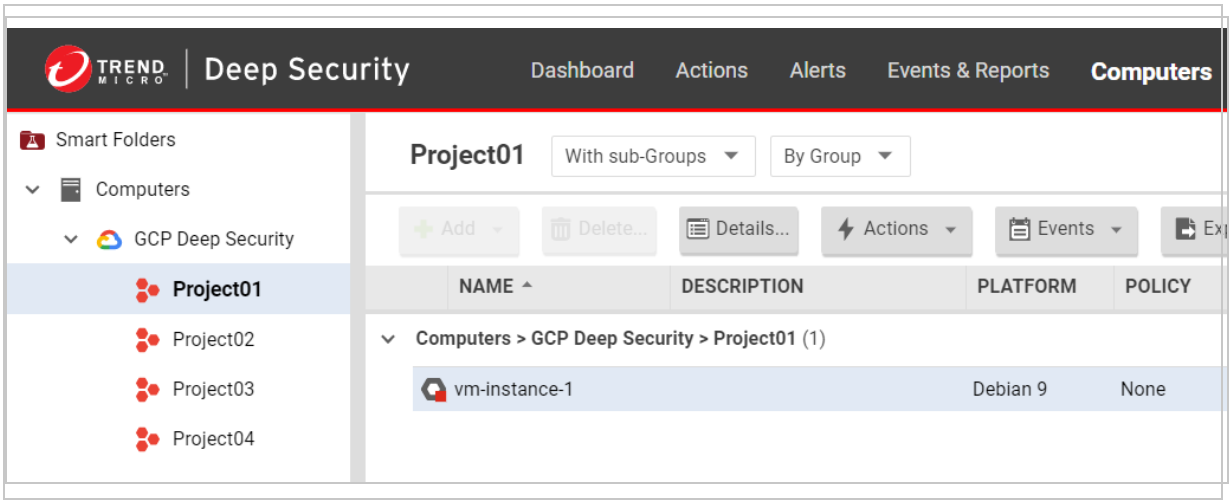


3. 表示名を入力します。GCPサービスアカウント名を使用することをお勧めします。例：GCP Deep Security, Finance GCP Deep Security, Marketing GCP Deep Security。
4. サービスアカウントキーを選択します。このキーは、GCPサービスアカウントの作成時に以前に保存したJSONファイルです。詳細については、"Google Cloud Platformサービスアカウントを作成する" on page 692 の作成を参照してください。
5. [次へ] []の順にクリックします。
6. 概要情報を確認し、[Close]をクリックします。

   次の処理が行われます。

- Deep Security Managerは、GCPサービスアカウントとそれに関連するプロジェクトをComputersページの左側のブランチに表示します(下の図の).を参照)。関連付けられているVMがメイン画面に表示されます。GCPサービスアカウント名を右クリックして、[同期する]( )を選択すると、最新の一連のGCP VMが表示されます。
- 以前に), で説明したの[コンピュータ]→[コンピュータの追加] オプション(の[コンピュータ]→[GCPアカウントの追加] オプション) ではなく、このサービスアカウントからVMインスタンスを追加した場合、これらのVMは追加したばかりのサービスアカウントの正しいプロジェクトに移動されます。この移動は、*Deep Security Agent 12.0以降*がインストールされているVMに対してのみ実行されます。12.0より前のエージェントを使用しているVMは、ルートComputersフォルダの下に残ります。

  次の図は、インポートされたGCPサービスアカウント、プロジェクト、およびVMを示しています。



7. 追加するGCPサービスアカウントごとに、この手順を繰り返します。

   これで、Deep Security ManagerにGCPサービスアカウントが追加されました。まだ展開していない場合は、["Google Cloud Platform VMにエージェントをインストールする" on page 553 にエージェントをインストールする]に進んでください。

GCPアカウントを削除する

Deep Security ManagerからGCPアカウントを削除すると、そのアカウントがDeep Securityデータベースから完全に削除されます。これはGCPアカウントには影響しません。Deep Security Agentがインストールされているインスタンスは引き続き保護されますが、セキュリティアップデートは受信されません。これらのVMインスタンスでDeep Security Agentを後で再アクティベーションすると、Deep Security Agentは次の予約アップデート時に最新のセキュリティアップデートをダウンロードします。

GCPアカウントを削除するには

1. Deep Security Managerで、上部にある[Computers]をクリックします。
2. 左側のツリー表示でGCPアカウントを右クリックし、[ ] [クラウドアカウントの削除] []の順に選択します。
3. アカウントを削除することを確認します。

   アカウントはDeep Security Managerから削除されます。

GCPアカウントを同期する

GCPアカウントを同期(同期) すると、Deep Security ManagerはGCP APIに接続して、最新の一連のGCP VMを取得して表示します。

強制的に同期を強制するには

1. Deep Security Managerで、[コンピュータ] をクリックします。
2. 左側で、GCPアカウントを右クリックし、[同期する]を選択します。[]をクリックします。

10分ごとに発生するバックグラウンド同期もあり、この間隔は設定できません。同期を強制すると、バックグラウンドの同期は影響を受けず、元のスケジュールに従って引き続き実行されます。

VMWare VMの追加

VMware vCenterの追加

VMware vCenterをDeep Security Managerにインポートしてから、仮想マシンをエージェントレスで、でエージェントで、または複合モードで保護できます。(これらのオプションについては、"Agentレスによる保護またはコンバインモードの保護の選択" on page 569を参照してください。)

注意: vShield Managerを使用しているvCenterはインポートできません。vShield Managerからサポート対象のVMware製品への移行については、"Deep Security Managerをインストールする" on page 459を参照してください。

vCenterの追加には、次のオプションがあります。

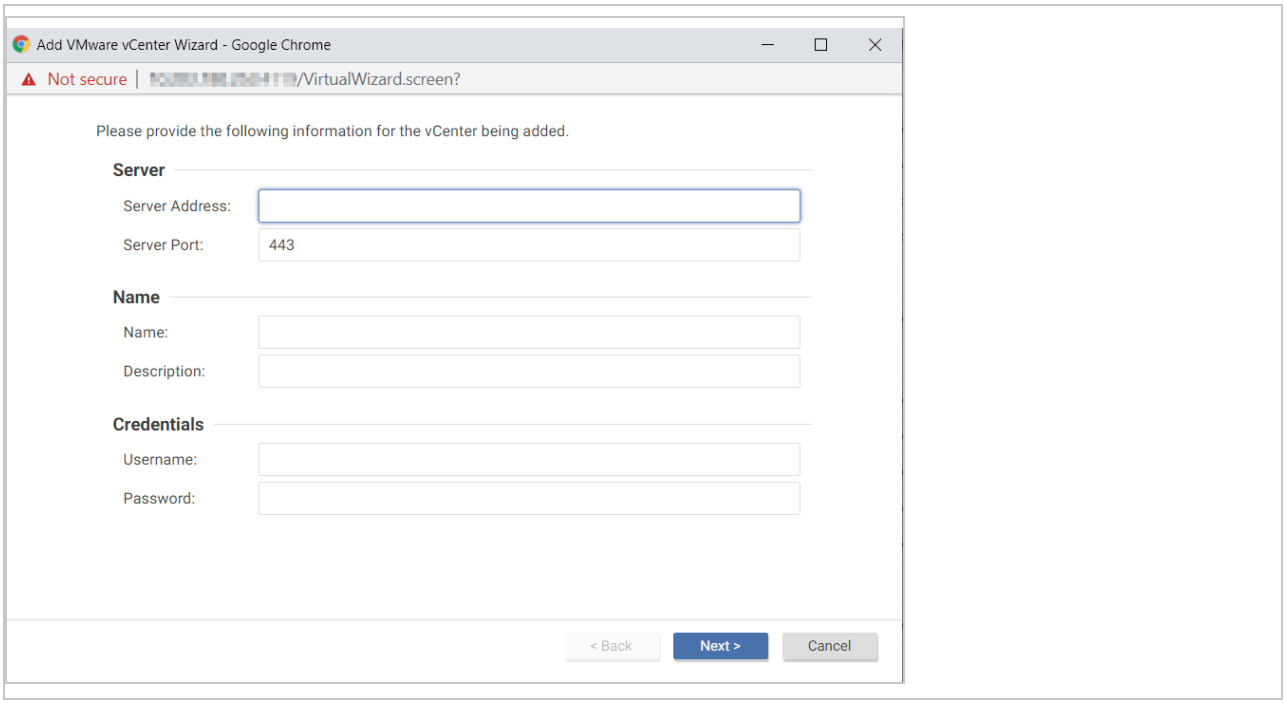
- "vCenterの追加" on the next pageを追加
- "複数のvCenterを追加する" on page 709
- "vCenter - FIPSモードを追加する" on page 709

注意: Deep Security Managerは、アクティブモードまたはパッシブモードで vCenter High Availability 環境をサポートします。

vCenterの追加

1. Deep Security Managerで、[コンピュータ]→[追加]→[VMware vCenterの追加] の順に移動します。

   次の画面が表示されます。



2. vCenter情報を入力:
   - サーバアドレス: vCenter ServerのIPアドレス(またはDNSが設定されており、FQDNをIPアドレス).に解決できる場合はホスト名)
   - サーバポート: vCenterに接続するためのポート番号(初期設定では443)).
   - 名前 : マネージャに表示されるvCenterの名前。
   - 説明 : vCenterの説明。
   - ユーザー名とパスワード: vCenter またはNSXのユーザー名とパスワードを入力します>ユーザーアカウント。このアカウントは、次の表の要件を満たす必要があり、VMインベントリをvCenterとDeep Security Managerとの間で同期する必要があります。

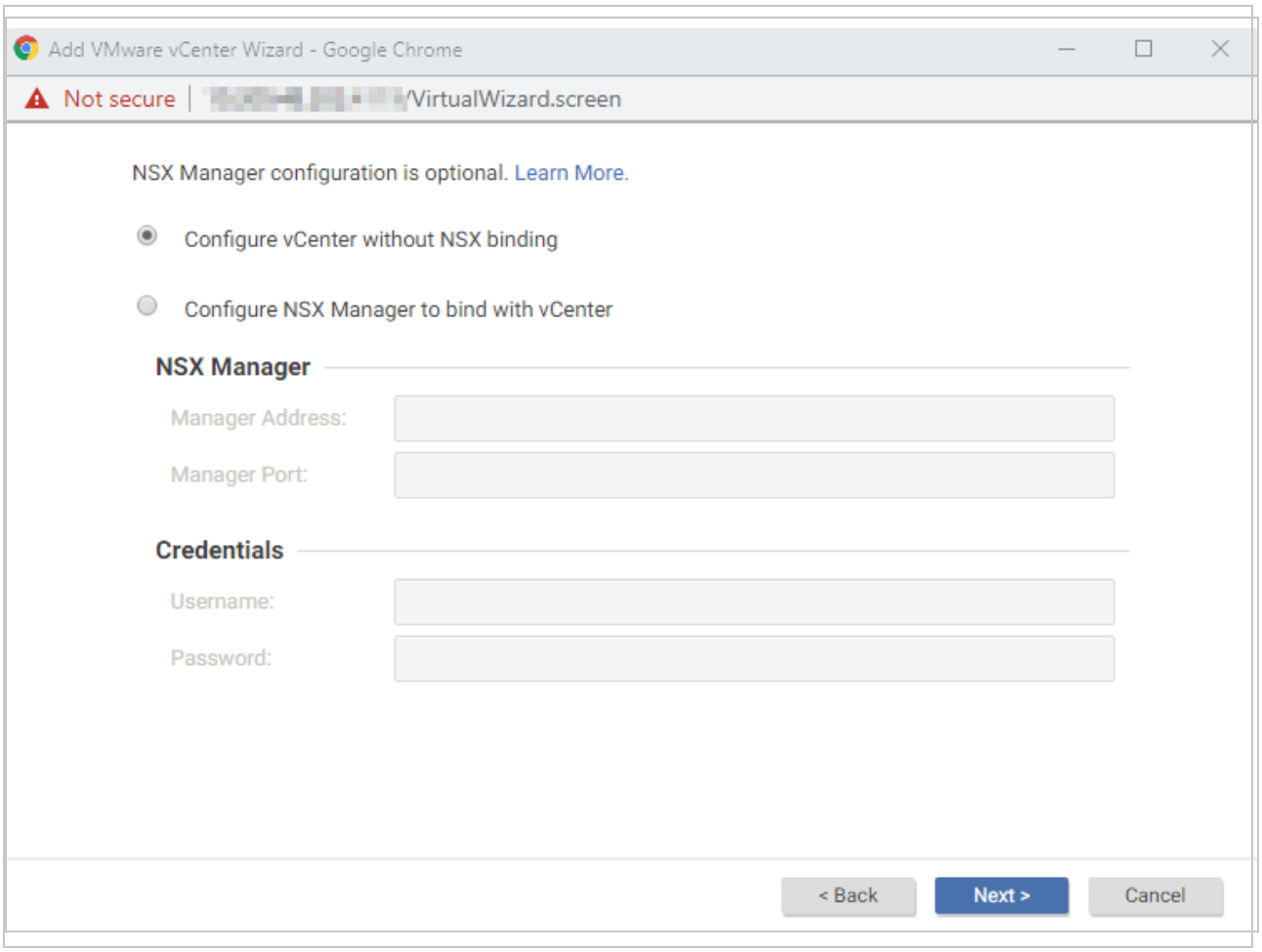
   注意 : vCenterのホストおよびクラスタまたは仮想マシンレベルで読み取り専用または管理者の役割を適用すると、同期の問題が発生します。

   vCenterのユーザアカウントの仕様

保護方法	NSXタイプ	vCenterのユーザアカウントの仕様
エージェントレスモードまたは複合モード	VMware NSX Data Center for vSphere (NSX-V)	vCenterのユーザアカウントには、次の2つの役割が必要です。 • NSX Managerで割り当てられたエンタープライズ管理者ロール。NSX-V Managerでのロールの割り当てについては、VMwareのこちらの記事を参照してください。 • vCenterでデータセンターレベルで割り当てられた管理者ロール
	VMware NSX-T Data Center (NSX-T)	vCenterのユーザアカウントには、次の役割が必要です。 • vCenterでデータセンターレベルで割り当てられた管理者ロール
エージェントのみ	NSX-VまたはNSX-Tの統合なし	vCenterのユーザアカウントには、vCenterの読み取り専用の役割(または権限以上の権限を持つ別の役割)がデータセンターレベルで存在する必要があります。

3. vCenterのTLS (SSL)証明書を受け入れます。
4. [Next]をクリックします。

   次の画面が表示されます。



注意: NSXバインディングのオプションがページの上部に表示されない場合は、以前のバージョンのManagerを使用しているためです。マネージャをFR 2019-12-12にアップグレードして、オプションを確認してください。

5. 次のようにページに記入します。

注意: 詳細については、NSX-T Manager Cluster Virtual IPアドレス (VIP) を参照してください。NSX-T Manager Cluster Deployment with Deep Security。

- を選択してNSX Managerを設定し、vCenter とバインドしてから、エージェントレスまたは複合モードの保護を使用する場合は、NSX情報を次のように入力します。それ以外の場合は、[NSXバインディングなしでvCenterを設定する] の順に選択し、[次へ] をクリックします。
- マネージャーアドレス: NSXマネージャーのIPアドレス(またはDNSが構成されていてFQDNをIPアドレスに解決できる場合はホスト名) 。
- Managerポート: NSX Managerに接続するポート番号です(初期設定では443) 。

- ユーザー名 および パスワード: NSXまたはvCenterユーザーアカウントのユーザー名 とパスワード。このアカウントは、次 の表 に示 す仕 様 に一 致 する必 要 があります。このユーザは、NSXセキュリティポ リシーおよびセキュリティグループをDeep Security Managerと同 期 するために必 要 となります。

NSXユーザーアカウントの仕 様

NSXタイプ	ユーザアカウントの仕 様
VMware NSX Data Center for vSphere (NSX-V)	ユーザアカウントは次 である必 要 があります。 • NSXビルトイン管 理 者 アカウント(完 全 な権 限 を持 つ). または • 次 の2つのロールを持 つvCenterユーザアカウント: • NSX Managerで割 り当 てられたエンタープライズ管 理 者 ロール。NSX-V Managerでのロールの割 り当 てについては、VMwareのこちらの記 事 を参 照 してください。 • vCenterでデータセンターレベルで割 り当 てられた管 理 者 ロール(クラスタレベルでこのロールが割 り当 てられている場 合 はエラーが発 生 します)。
VMware NSX-T Data Center (NSX-T)	ユーザアカウントは次 である必 要 があります。 • NSXビルトイン管 理 者 アカウント(エンタープライズ管 理 者 、フルアクセス許 可 あり)). または • 次 の役 割(または同 等 以 上 の権 限 を持 つその他 の役 割) を持 つLDAPアカウント情 報 を持 つNSX-Tユーザアカウント): • Endpoint ProtectionのGIパートナー管 理 者 • E-Wネットワークイントロスペクション用 のNetxパートナー管 理 者 VMwareの各 種 ロールに割 り当 てられた権 限 の詳 細 については、VMwareのこちらの記 事 を参 照 してください。NSX-T Managerでのロール

NSXタイプ	ユーザアカウントの仕様
	の割り当ての詳細については、VMwareのこちらの記事を参照してください。

6. [Next] をクリックします。
7. NSXおよびvCenterの情報を確認し、[完了]をクリックします。
8. 「VMware vCenterの追加に成功しました」というメッセージが表示されます。[閉じる] をクリックします。[コンピュータ] 画面にvCenterが表示されます。

ヒント: vCenterを追加する場合に[このvCenterの保護対象NSXセキュリティグループに追加された仮想マシンを自動的に有効化する、イベントベースタスクを作成します。]をオンにすると、イベントベースタスクが2つ作成されます。1つは、保護が追加されたときに仮想マシンを有効化し、もう1つは、保護が削除されたときに仮想マシンを無効化します。詳細については、"NSX環境での自動ポリシー管理" on page 639を参照してください。

前述のようにNSX情報を入力した場合、Deep Security ManagerはNSX Manager内にDeep Securityサービスを登録します。この登録により、ESXiサーバへのDeep Securityサービスの配信が許可されます。

大規模環境では、このプロセスが完了するまで時間がかかることがあります。vCenterの [最近のタスク] セクションで、実行中のアクティビティがないか確認してください。

Deep Security Managerは、Deep Security Managerに表示される情報(VMの数、ステータスなど)を最新の状態に維持するため、このVMware vCenterとのリアルタイム同期を維持します。

複数のvCenterを追加する

複数のvCentreをDeep Security Managerに追加するには

1. "vCenterの追加" on page 705の追加]の手順に従って、最初のvCenterおよびNSX Managerを追加します。
2. "vCenterの追加" on page 705 を次のvCentersおよび関連するNSX Managerに追加します。

vCenter - FIPSモードを追加する

Deep Security ManagerがFIPSモードの場合にvCenterを追加するには

1. vCenterおよびNSX ManagerのTLS(SSL)証明書をDeep Security Managerにインポートしてから、ManagerにvCenterを追加します。"信頼された証明書の管理" on page 1653を参照してください。

2. "vCenterの追加" on page 705を追加します。これらの手順はまったく同じですが、FIPSモードの場合は、vCenterページの[信頼する証明書]セクションが表示されます。[接続テスト]をクリックして、vCenterのSSL証明書がDeep Security Managerに正常にインポートされているかどうかを確認します。エラーがない場合は、[次へ]の順にクリックし、ウィザードを続行します。

VMware vCloudでホストされる仮想マシンの追加

クラウドプロバイダアカウントからDeep Security Managerにリソースをインポートすると、アカウント内のコンピュータはローカルネットワーク上の任意のコンピュータと同様に管理されます。

Deep Security Managerにクラウドリソースをインポートするには、まずクラウドプロバイダサービスリソースにアクセスするアカウントをDeep Securityユーザが持っている必要があります。Deep Security Managerにクラウドアカウントをインポートする各のDeep Securityのユーザーのために、トレンドマイクロはクラウドリソースにアクセスすることのDeep Security Managerの専用アカウントを作成することをお薦めします。つまり、仮想マシン自体にアクセスして制御する1つのアカウントと、Deep Security Managerがそれらのリソースに接続するための別のアカウントが必要です。

注意: Deep Security専用のアカウントを持つことで、いつでも権限を絞り込んでこのアカウントを取り消すことができます。Deep Securityに読み取り専用のアクセス権または秘密鍵を常時付与することをお勧めします。

注意: Deep Security Managerは、クラウドリソースをインポートしてセキュリティを管理するためにのみ読み取り専用のアクセス権しか必要としません。

注意: FIPSモードを有効にした場合は、VMware vCloudでホストされる仮想マシンを追加できません。"FIPS 140のサポート" on page 1870を参照してください。Azureアカウントを追加することのメリットは何ですか?

このセクションのトピック:

- "vCloudアカウントを追加することのメリットは何ですか。" on the next page
- "クラウドアカウント用のプロキシ設定" on the next page
- "Manager用のVMware vCloud Organizationアカウントを作成する" on the next page
- "VMware vCloud Organizationアカウントからコンピュータをインポートする" on page 712
- "VMware vCloud Airデータセンターからコンピュータをインポートする" on page 712
- "クラウドアカウントのソフトウェアアップデートを設定する" on page 713
- "クラウドアカウントを削除する" on page 713

vCloudアカウントを追加することのメリットは何ですか。

個々のvCloudリソースを追加する代わりに(Deep Security Manager> コンピュータ> コンピュータの), の追加を使用) 、vCloudアカウントを追加すると(Deep Security Manager> コンピュータ> vCloudアカウントの追加を使用) 、次のような利点があります。

- クラウドリソースインベントリの変更は、自動的にDeep Security Managerに反映されます。たとえば、vSphereから多数のインスタンスを削除すると、それらのインスタンスは自動的にマネージャから非表示になります。対照的に、[コンピュータ]→[コンピュータの追加]を使用する場合、vCenterから削除されたクラウドインスタンスは手動で削除されるまでマネージャに表示されたままです。
- クラウドリソースは、マネージャで独自のブランチに編成されているため、保護対象リソースと保護対象リソースを簡単に確認できます。vCloudアカウントがないと、クラウドリソースはすべてComputersの同じルートレベルに表示されます。

クラウドアカウント用のプロキシ設定

クラウドアカウントで保護されているインスタンスへの接続にプロキシサーバを使用するよう、Deep Security Managerを設定できます。プロキシ設定は、[管理]→[システム設定]→[プロキシ]→[プロキシサーバの使用]→[Deep Security Manager (クラウドアカウント - HTTPプロトコルのみ)] で行います。

Manager用のVMware vCloud Organizationアカウントを作成する

1. VMware vCloud Directorにログインします。
2. [System] タブで、[Manage And Monitor] に移動します。
3. 左側のナビゲーションペインで [Organizations] をクリックします。
4. Deep Securityユーザのアクセス権を付与する組織をダブルクリックします。
5. [Organizations] タブで [Administration] をクリックします。
6. 左側のナビゲーションペインで [Members]→[Users] の順にクリックします。
7. 「プラス」記号 (+) をクリックして新しいユーザを作成します。
8. 新しいユーザの資格情報などの情報を入力し、ユーザの [Role] で [Organization Administrator] を選択します。

   注意: [Organization Administrator] は、新しいユーザアカウントに割り当て可能な定義済みのシンプルなロールです。ただし、アカウントに必要な権限は [All Rights]→[General]→[Administrator View] のみなので、この権限のみを付与した新しいvCloudロールの作成を検討してください。Deep Security統合のためのvCloudリソースの準備の詳細については、「"vCloud環境にアプライアンスを配信する" on page 635」を参照してください。
9. [OK] をクリックしてユーザのプロパティ画面を閉じます。

これで、vCloudアカウントにDeep Security Managerによるアクセスの準備が整いました。

注意:
VMware vCloudリソースをDeep Security Managerにインポートするには、vCloudのアドレス、ユーザ名、およびパスワードの入力を求めるメッセージが表示されます。

ユーザ名には「@orgName」を含める必要があります。また、vCloudのリソースをDeep Security Managerにインポートする際は、ユーザ名に「@orgName」を含めるように指示してください。たとえば、vCloudアカウントのユーザ名がuserで、アカウントのアクセス権を付与されたvCloud OrganizationがCloudOrgOneである場合、Deep Securityのユーザは、vCloudのリソースをインポートするときにユーザ名として「user@CloudOrgOne」と入力する必要があります。

(vCloud管理者の場合、@systemを使用します)。

VMware vCloud Organizationアカウントからコンピュータをインポートする

1. Deep Security Managerで、[コンピュータ]に移動します。
2. ナビゲーションパネルで[コンピュータ]を右クリックし、[vCloudアカウントの追加]を選択してvCloudアカウント追加ウィザードを開きます。
3. [名前]と[説明]に、追加するリソースを入力します。(Deep Security Managerでの表示に使用されます)。
4. [アドレス]に、vCloud Directorのホスト名とアドレスを入力します。
5. [ユーザ名]と[パスワード]に、vCloudの認証資格情報を入力します。ユーザ名は、username@vcloudorganizationの形式で指定する必要があります。
6. [次へ]をクリックします。
7. Deep Security Managerによってクラウドリソースへの接続が確認され、インポート処理の概要が表示されます。[完了]をクリックします。

VMware vCloudリソースは、Deep Security Managerの[コンピュータ]にあるそれぞれのブランチの下に表示されます。

VMware vCloud Airデータセンターからコンピュータをインポートする

1. Deep Security Managerで、[コンピュータ]セクションに移動し、ナビゲーションパネルで[コンピュータ]を右クリックし、[vCloudアカウントの追加]を選択してvCloudアカウント追加ウィザードを開きます。
2. 追加するvCloud Airデータセンターの名前と説明を入力します(Deep Security Managerでの表示に使用されます)。
3. vCloud Airデータセンターのアドレスを入力します。

   vCloud Airデータセンターのアドレスを確認するには、次の手順を実行します。

a. vCloud Airポータルにログインします。
b. [Dashboard] タブで、Deep Securityにインポートするデータセンターをクリックします。[Virtual Data Center Details] 画面が表示されます。
c. [Virtual Data Center Details] 画面の [Related Links] セクションで [vCloud Director API URL] をクリックします。vCloud Director APIの完全なURLが表示されます。
d. Deep Securityにインポートするvcloud Airデータセンターのアドレスとして、(完全なURLではなく) ホスト名のみを使用します。

4. [ユーザ名] と[パスワード] に、仮想データセンターの資格情報を入力します。ユーザ名は、「username@virtualdatacenterid」の形式で指定する必要があります。
5. [次へ] をクリックします。
6. Deep Security ManagerによってvCloud Airデータセンターへの接続が確認され、インポート処理の概要が表示されます。[完了] をクリックします。

VMware vCloud Airデータセンターは、Deep Security Managerの [コンピュータ] に、それぞれ別個の項目として表示されます。

クラウドアカウントのソフトウェアアップデートを設定する

リレーはDeep Security Agent内のモジュールで、セキュリティおよびソフトウェアのアップデートをダウンロードおよび配信します。通常、Deep Security Managerは、新しいアップデートが使用可能になったときにリレーに通知します。リレーがアップデートを取得した後、エージェントはリレーからアップデートを取得します。

ただし、Deep Security Managerがエンタープライズ環境にあり、クラウド環境でコンピュータを管理している場合、クラウド内のリレーはDeep Security Managerと通信できない可能性があります。この問題を解決するには、トレンドマイクロのダウンロードセンターからDeep Security Managerに接続できない場合にソフトウェアのアップデートを直接取得することができます。このオプションを有効にするには、に移動します。[管理]→[システム設定]→[アップデート]下のソフトウェアのアップデート、select Deep Security Managerにアクセスできない場合にトレンドマイクロのダウンロードセンターからソフトウェアアップデートをダウンロードできるようにするには。

クラウドアカウントを削除する

Deep Security Managerからクラウドプロバイダアカウントを削除すると、そのアカウントがDeep Securityデータベースから完全に削除されます。クラウドプロバイダを使用しているアカウントは影響を受けず、インスタンスにインストールされたDeep Security Agentはインストールされ、実行され、保護機能が提供されます(ただし、セキュリティアップデートは受信されません) 。クラウドプロバイダアカウントからコンピュータを再インポートする場合、Trend Micro Deep Security Agentは次に推奨される機会に最新のセキュリティアップデートをダウンロードします。

1. [コンピュータ] 画面を開き、ナビゲーションパネルでクラウドプロバイダアカウントを右クリックし、[クラウドアカウントの削除...] を選択します。
2. アカウントを削除することを確認します。
3. アカウントはDeep Security Managerから削除されます。

NSX ManagerのIPアドレスまたはFQDNの変更

Deep Security Managerでは、次のいずれかが発生した場合にNSX ManagerのIPアドレスまたは完全修飾ドメイン名 (FQDN) を変更できます。

- NSX-VをNSX-Tに直接移行することはできません (「NSX-VからNSX-TへのAgentレスソリューションの移行」を参照)。
- NSX Managerはすでに Deep Security Managerで設定されています。

特定のvCenterのIPアドレスは、次のように変更できます。

1. NSX ManagerのIPアドレスをNSX Clusterの仮想IPアドレスに変更します。
2. [証明書の追加/アップデート] をクリックします。
3. [接続テスト] をクリックして、仮想IPアドレスへの接続を確認します。
4. [OK] または [適用] をクリックして設定を終了します。

保護されたNSXクラスタへのESXiの追加

すでにDeep Security Virtual Applianceがインストールされているクラスタ内のESXiサーバを保護している場合に、そのクラスタに別のESXiを追加する場合は、次の手順に従って新しいESXiサーバが保護されていることを確認してください。

1. 開始する前に、アプライアンスをクラスタに配置していることを確認してください。手順については、"アプライアンスを配信する(NSX-T 3.x) " on page 576または"Applianceのインストール (NSX-V)" on page 611を参照してください。
2. ESXiをデータセンターに追加します。*クラスタには直接追加しないでください。*
3. 必要に応じてESXiを仮想分散スイッチ(vDS) に接続します。NSX-Tの場合は、ESXiホストにNSX-T Virtual Distributed Switch(N-VDS).) のNICが使用可能であることを確認します。これらのNICは、ファブリック設定に従ってNSX-T Managerによって自動的に設定されます。
4. ESXiをクラスタに移動します。クラスタがNSX-Tで設定されている場合は、NSX-T Managerのインストール進行状況がシステム>ファブリック>ホスト転送ノードに表示されます。

ESXiホストをクラスタに移動すると、NSXによってDeep Securityサービスが自動的に配信されます。

注意: NSX Managerへの接続は、FIPSモードでサポートされています。"FIPS 140のサポート" on page 1870を参照してください。

CPU使用率を制御する

Deep SecurityエージェントのCPU使用率制御は、Linuxで不正プログラム対策が有効になっているエージェントで利用可能です。

Deep Securityコンソールを使用して、次のようにCPU使用率を構成できます:

1. エージェントのCPU使用率制御を有効にしたいコンピュータを開きます。
2. 設定 > 一般をクリックします。
3. CPU使用率制御の下で、次のCPU保護モードのいずれかを選択してください。
   - 極低: 新しく作成および変更されたファイルの非同期遅延リアルタイム検索。不正プログラム対策 > 一般 > リアルタイム検索 > 不正プログラム検索設定 > 編集で機械学習型検索および挙動監視を有効または無効にすることはできません。
   - 低: 一定期間内に新規作成および変更されたファイルと実行ファイルに対する同期リアルタイム検索。
   - 無制限: リアルタイム検索による完全な保護 (デフォルト)。

新しいクラウドコネクタ機能への移行

以前にクラウドアカウントの追加を使用してAmazon Web ServicesリソースをDeep Security Managerにインポートした場合、それらのリソースはコンピュータでAWSリージョンごとに整理されています。複数のAWSリージョンがある場合は、ウィザードを複数回実行した可能性があります。

最新バージョンのDeep Securityでは、AWSインスタンスをAWSアカウント名の下にまとめ、AWSリージョン、VPC、およびサブネットを含む階層に整理して表示できるようになりました。

AWSリソースを移行する前に、Deep SecurityからAWSアカウントへのアクセスを許可するポリシーを編集してください。

1. AWSマネジメントコンソールにログインし、[Identity and Access Management (IAM)] に移動します。
2. 左側のポリシーをクリックします。
3. ポリシーのリストで、Deep SecurityからAWSアカウントへのアクセスを許可するポリシーを選択します。
4. [Policy Document] タブに移動し、[Edit] をクリックします。

5. ポリシードキュメントを編集し、次のJSONコードを追加します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "cloudconnector",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs",
                "iam:ListAccountAliases",
                "sts:AssumeRole"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

"sts:AssumeRole" の権限は、クロスアカウントロールアクセスを使用している場合にのみ必要です。IAMロールの詳細については、AWS アカウント間で IAM ロールを使用してアクセスを委任する を参照してください。

6. [Save as default version] を選択します。

Deep Security ManagerでAWSリソースを移行するには

1. [コンピュータ] に移動します。
2. 左側でAWSリージョンを右クリックし、[Amazonアカウントにアップグレード] を選択します。
3. [完了] をクリックします。
4. 閉じる をクリックします。

AWSインスタンスはAWSアカウント名の下にまとめられ、AWSリージョン、VPC、およびサブネットを含む階層に整理して表示されます。

Dockerコンテナの保護

Docker環境の導入にはメリットがあるのはもちろんですが、同時にDockerホストのOS自体が攻撃の対象になることに注意が必要です。他のソフトウェアの導入同様に、OSの強化や環境に応じたベストプラクティス(Center for Internet Security (CIS) のDocker Benchmarkなど)を利用することで、最初に強固な基盤を構築することが重要になります。Deep Securityを導入することで、トレンドマイクロの広範囲にわたる物理的、仮想的、およびクラウドワークロード、Trend Micro Smart Protection Networkのリアルタイムの脅威情報へのアクセスを利用できるようになります。。Deep Securityは、環境の保護だけでなく、継続的なコンプライアンス要件への対応と維持にも役立ちます。サポート対象のDockerのエディションとリリースについては、"Deep Security Agentのプラットフォーム" on page 400を参照してください。

Deep Securityは、Linuxディストリビューションで動作するDockerホストおよびコンテナを保護します。Deep Securityでは次のことが可能です。

- アイコンとスマートフォルダにより、環境内のDockerホストを特定、検索、および保護する
- 新たに見つかった脆弱性に対して仮想パッチを適用することで、Dockerホストおよびコンテナを脆弱性に対する既知またはゼロデイの攻撃コードから保護する
- 不正プログラム対策検出をリアルタイムで提供し、Dockerホストで使用されるファイルシステムに対して手動およびスケジュールされたスキャンを行います。
- コンテナ内で使用されているファイルシステムに対するリアルタイムの不正プログラム検出を提供する
- 次の手法を使用して、継続的なコンプライアンスの維持と環境の保護のためにDockerホストの変更をアサートする
  - Dockerデーモンに加えて実行を許可するアプリケーションを制御することで、Dockerホストでのアプリケーションの不正な実行を防御する
  - Dockerホストのシステムファイルに対して予想外の変更が発生しないように監視する
  - OSログ内の不審なイベントを通知します。

Deep SecurityによるDockerの保護はOSレベルで機能するため、コンテナではなく、DockerホストのOSにDeep Security Agentをインストールする必要があります。

注意: ポッド内のコンテナ間の通信はサポートされていません。

Deep Security 10.1以降、Trend Micro Deep Securityは、Dockerをswarmモードでサポートし、オーバーレイネットワークを使用します。

Deep SecurityによるDockerホストの保護

Dockerホストの保護には、次のDeep Securityモジュールを使用できます。

- 侵入防御 (IPS)
- 不正プログラム対策
- 変更監視
- セキュリティログ監視
- アプリケーションコントロール
- ファイアウォール
- Webレピュテーション

Deep SecurityによるDockerコンテナの保護

Dockerコンテナの保護には、次のDeep Securityモジュールを使用できます。

- 侵入防御
- 不正プログラム対策 (リアルタイムスキャンのみ対応; スケジュールスキャンおよび手動スキャンはサポートされていません)

侵入防御の推奨検索に関する制限事項

Deep Securityの侵入防御はホストレベルで動作しますが、公開されたコンテナポート番号のコンテナトラフィックも保護されます。Dockerでは複数のアプリケーションを同じDockerホスト上で実行できるため、単一の侵入防御ポリシーがすべてのDockerアプリケーションに適用されます。そのため、推奨設定の検索はDocker環境に対しては推奨されません。

OpenShiftコンテナの保護

Red Hat OpenShiftを使用すると、Kubernetesクラスタの内部および外部のアプリケーションで、最も適切な場所でアプリケーションを実行できます。OpenShiftの基本的なセキュリティには、セキュリティ強化とFIPS(連邦情報処理標準)準拠の暗号化(FIPS 140-2レベル1)が含まれます。

安全な基盤を構築したら、Deep SecurityをOpenShift環境に追加すると、物理、仮想、およびクラウドのワークロードを保護するトレンドマイクロの豊富な経験に加えて、Trend Micro Smart Protection Networkからのリアルタイムの脅威情報にアクセスできるようになります。Deep Securityは、環境の保護だけでなく、継続的なコンプライアンス要件への対応と維持にも役立ちます。

Deep Securityは、Red Hat Linuxディストリビューションで実行されているOpenShiftホストおよびコンテナを保護します。Deep Securityでは次のことが可能です。

- 環境内のOpenShiftホストの特定、検出、および保護
- OpenShift ホスト上およびコンテナー内で使用されるファイルシステムに対して、"不正プログラム対策を有効化して設定する" on page 828 を提供します。

注意: ポッド内のコンテナ間の通信はサポートされていません。

OpenShiftホストのDeep Securityによる保護

OpenShiftホストの保護には、次のDeep Securityモジュールを使用できます。

- 不正プログラム対策 (オンデマンド検索を除く)

OpenShiftコンテナのDeep Securityによる保護

OpenShiftコンテナの保護には、次のDeep Securityモジュールを使用できます。

- 不正プログラム対策 (オンデマンド検索を除く)

ポリシーを設定する

ポリシーの作成

ポリシーでは、ルールや設定をまとめて保存し、複数のコンピュータに簡単に割り当てることができます。**ポリシーエディタ**[1]でポリシーを作成および編集し、1台以上のコンピュータに割り当てることができます。また、ポリシーエディタに似た**コンピュータエディタ**[2]を使用して、特定のコンピュータに設定を適用することもできますが、コンピュータエディタで設定を編集するよりも特殊なポリシーを作成することを推奨します。

[1] ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。

[2] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。

ヒント: ポリシーの作成と設定は、Deep Security APIを使用して自動化できます。例については、Deep Security Automation Centerにあるガイド「Create and Configure Policies」を参照してください。

このトピックの内容:

- "新規ポリシーを作成する" below
- "ポリシーを作成するその他の方法" on the next page
- "ポリシーまたは個々のコンピュータの設定を編集する" on the next page
- "ポリシーをコンピュータに割り当てる" on page 722
- "ポリシーの自動アップデートを無効にする" on page 722
- "ポリシーの変更を手動で送信する" on page 723
- "ポリシーをエクスポートする" on page 723

新規ポリシーを作成する

1. [ポリシー]→[新規]→[新規ポリシー] の順にクリックします。
2. ポリシーの名前を入力します。既存のポリシーの設定を新規ポリシーに継承する場合は、[継承元] リストからポリシーを選択します。[次へ] をクリックします。

   ヒント: 継承の詳細については、"ポリシー、継承、およびオーバーライド" on page 724を参照してください。
3. 既存のコンピュータの設定をこのポリシーのベースにするかどうかを選択し、[次へ] をクリックします。
4. 手順3で [はい] を選択した場合は、以下を実行します。
   a. 新規ポリシーのベースとして使用するコンピュータを選択し、[次へ] をクリックします。
   b. 新規ポリシーに対して有効にする保護モジュールを指定します。既存のポリシーから設定を継承する場合は、それらの設定が表示されます。[次へ] をクリックします。
   c. 次の画面で、新規ポリシーに組み込むプロパティを選択し、[次へ] をクリックします。設定を確認し、[完了] をクリックします。
5. 手順3で [いいえ] を選択した場合は、新規ポリシーに対して有効にする保護モジュールを指定します。既存のポリシーから設定を継承する場合は、それらの設定が表示されます。[完了] をクリックします。
6. [閉じる] をクリックします。次にポリシーの設定を編集できます。手順については"ポリシーまたは個々のコンピュータの設定を編集する" on the next pageを参照してください。

ポリシーを作成するその他の方法

[ポリシー] 画面ではいくつかの方法でポリシーを作成できます。

- 前述した手順で新規ポリシーを作成します。
- [新規]→[ファイルからインポート] の順に選択してXMLファイルからポリシーをインポートします。
- 注意: ポリシーをインポートする場合、ポリシーを作成したシステムと受け取るシステム両方に最新のセキュリティアップデートが適用されていることを確認してください。ポリシーを受け取るシステムが古いセキュリティアップデートを実行していると、最新のシステムのポリシーで参照されている一部のルールがそのシステムにない可能性があります。
- 既存のポリシーを複製し、変更して名前を変更します。複製するポリシーを右クリックして [複製] をクリックします。
- コンピュータの推奨設定の検索に基づいて新規ポリシーを作成します。[コンピュータ] 画面に移動し、コンピュータを右クリックして [処理]→[推奨設定の検索] の順に選択します。検索が終了したら、[ポリシー] 画面に戻り、[新規] をクリックして新規ポリシーウィザードを起動します。プロンプトが表示されたら、新規ポリシーのベースを「既存のコンピュータの現在の設定」にします。次に、コンピュータのプロパティから [推奨されるアプリケーションの種類と侵入防御ルール]、[推奨される変更監視ルール]、および [推奨されるセキュリティログ監視ルール] を選択します。
- 注意: ポリシーは、現在コンピュータにどのようなルールが割り当てられていたとしても、そのコンピュータの推奨エレメントのみで構成されます。

ポリシーまたは個々のコンピュータの設定を編集する

[ポリシー] 画面には、階層型のツリー構造で既存のポリシーが表示されます。ポリシーの設定を編集するには、ポリシーを選択し、[詳細] をクリックしてポリシーエディタを開きます。

コンピュータエディタとポリシーエディタ[1]には以下のセクションがあります。

- 概要("ポリシーエディタの [概要] セクション" on page 746 と "コンピュータエディタの [概要] セクション" on page 740 が異なります)
- 不正プログラム対策

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

- Webレピュテーション
- デバイスコントロール
- ファイアウォール
- 侵入防御
- 変更監視
- セキュリティログ監視
- アプリケーションコントロール
- インタフェースの種類
- 設定
- オーバーライド

ポリシーをコンピュータに割り当てる

1. [コンピュータ] に移動します。
2. コンピュータリストからコンピュータを選択し、右クリックして [処理]→[ポリシーの割り当て] の順に選択します。
3. 階層ツリーからポリシーを選択し、[OK] をクリックします。

次のいずれかが実行されます。

- 通信方向を [Managerから開始] または [双方向] に設定している場合、ポリシーはAgentコンピュータにただちに送信されます。
- 通信方向を [Agent/Applianceから開始] に設定している場合、ポリシーは次のAgentハートビートが発生したときに送信されます。

階層ツリーの子ポリシーで親ポリシーの設定やルールを継承またはオーバーライドする方法については、"ポリシー、継承、およびオーバーライド" on page 724を参照してください。

ポリシーをコンピュータに割り当てた後も、定期的に推奨設定の検索を実行して、コンピュータ上にあるすべての脆弱性を保護してください。詳細については、"推奨設定の検索の管理と実行" on page 728を参照してください。

ポリシーの自動アップデートを無効にする

初期設定では、セキュリティポリシーが変更された場合、変更内容はそのポリシーを使用するコンピュータに自動的に送信されます。これを変更して、自動送信を無効にできます。この場合、手動でポリシーを送信する必要があります。

1. 設定するポリシーの**ポリシーエディタ**[1]を開きます。
2. [設定]→[一般]→[ポリシーの変更をすぐに送信] の順に選択します。
3. ポリシー変更の自動送信を許可するには、[ポリシーの変更をコンピュータに自動的に送信] の隣にある [はい] を選択します。自動送信を無効にして手動送信のみを許可するには、[いいえ] を選択します。
4. [保存] をクリックして変更を適用します。

ポリシーの変更を手動で送信する

ポリシーを変更し、ポリシーの変更を特定のコンピュータに手動で送信する場合は、次の手順に従います。

1. [コンピュータ] に移動します。
2. コンピュータリストから自分のコンピュータをダブルクリックします。
3. ナビゲーション画面で [概要] が選択されていることを確認します。
4. メイン画面で [処理] タブをクリックします。
5. [ポリシー] で、[ポリシーの送信] をクリックします。

次のいずれかが実行されます。

- 通信方向を [Managerから開始] または [双方向] に設定している場合、ポリシーはAgentコンピュータにただちに送信されます。
- 通信方向を [Agent/Applianceから開始] に設定している場合、ポリシーは次のAgentハートビートが発生したときに送信されます。

ポリシーをエクスポートする

ポリシーをXMLファイルにエクスポートするには、ポリシーツリーからポリシーを選択し、[エクスポート]→[選択したアイテムをXML形式でエクスポート(インポート用)] の順にクリックします。

エクスポートされたポリシーは、同じマルチノードクラスタ内の別のDeep Security Managerによってのみインポートできます。Workload Securityへの移行が目的である場合は、Workload Securityへのポリシーの移行方法に関する記事を参照してください。

> 注意: Deep Security Managerでは、カスタムルールを使用したポリシーのエクスポートおよびインポートはサポートされません。

[1] ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック)します。

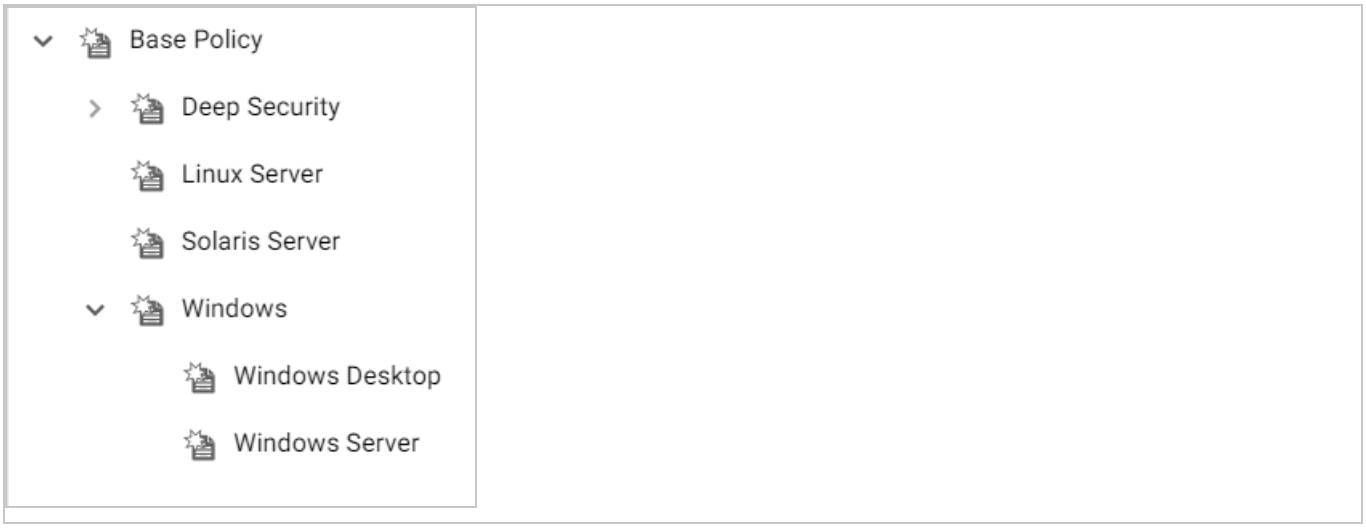
注意: 選択したポリシーをXMLにエクスポートすると、子ポリシー(存在する場合)もエクスポートパッケージに追加されます。エクスポートパッケージには、ポリシーに関連するすべての実際のオブジェクトが含まれます。ただし、侵入防御ルール、セキュリティログ監視ルール、変更監視ルール、およびアプリケーションの種類は含まれません。

ポリシー、継承、およびオーバーライド

Deep Securityのポリシーは、階層構造で作成されます。管理者は、最初に1つ以上のベースポリシーを作成し、そこから複数レベルの子ポリシーを作成し、細分化していきます。つまり、最上位のポリシーで広範囲に適用するルールや設定を割り当ててから、子ポリシーのレベルで対象を絞って具体化し、最終的に個々のコンピュータレベルでルールや設定を割り当てることができます。

ポリシーツリーの下位になるほど設定が詳細になるだけでなく、ポリシーツリーの上位の設定から下位の設定をオーバーライドできます。

Deep Securityは、環境に合わせて独自のポリシーを設計するための開始テンプレートとして使用できる一連のポリシーを提供します。



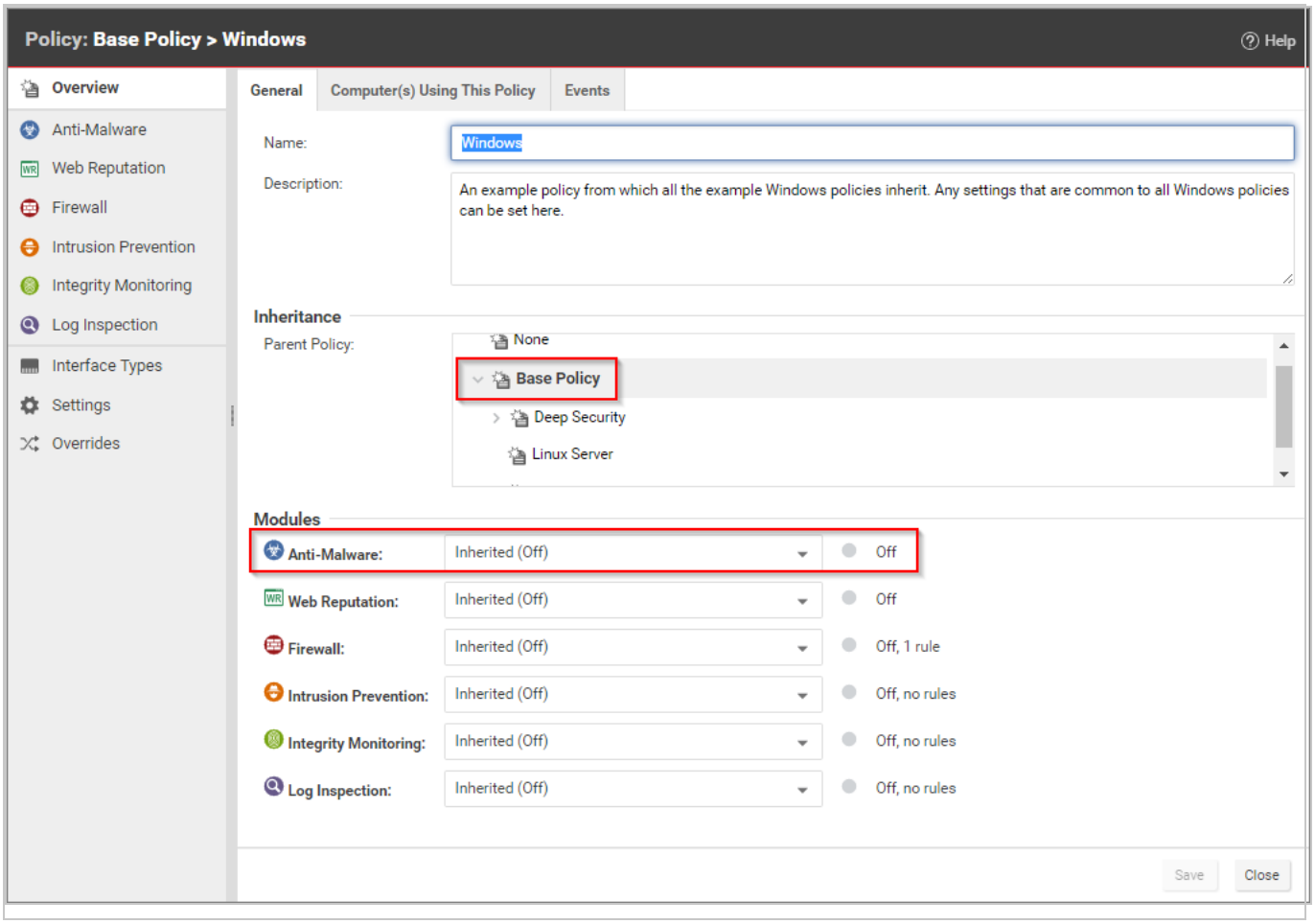
このトピックの内容:

- "継承" on the next page
- "オーバーライド" on page 726
- "コンピュータまたはポリシーのオーバーライド項目をまとめて確認する" on page 727

継承

子ポリシーは、親ポリシーから設定を継承します。これにより、すべてのコンピュータに適用する設定とルールが定義された親ベースポリシーから始まるポリシーツリーを作成できます。さらに、この親ポリシーには、より対象を具体化した設定を含む子および子孫のポリシーのセットを追加できます。ポリシーツリーは、環境に適した分類システムに基づいて構築できます。たとえば、Deep Securityに付属するポリシーツリー内のブランチには、Deep Security Managerをホストするサーバ用に設計されたポリシーとDeep Security Virtual Appliance用に設計されたポリシーの2つの下位ポリシーがあります。これは役割に基づいたツリー構造です。また、Deep Securityには、特定のOS (Linux、Solaris、およびWindows) 向けに設計された3つのブランチがあります。Windowsブランチには、さまざまなサブタイプのWindows OS用の子ポリシーが用意されています。

[概要] 画面のWindowsポリシーエディタでは、Windowsポリシーがベースポリシーの子として作成されたことを確認できます。ポリシーの不正プログラム対策設定は [継承 (オフ)] です。

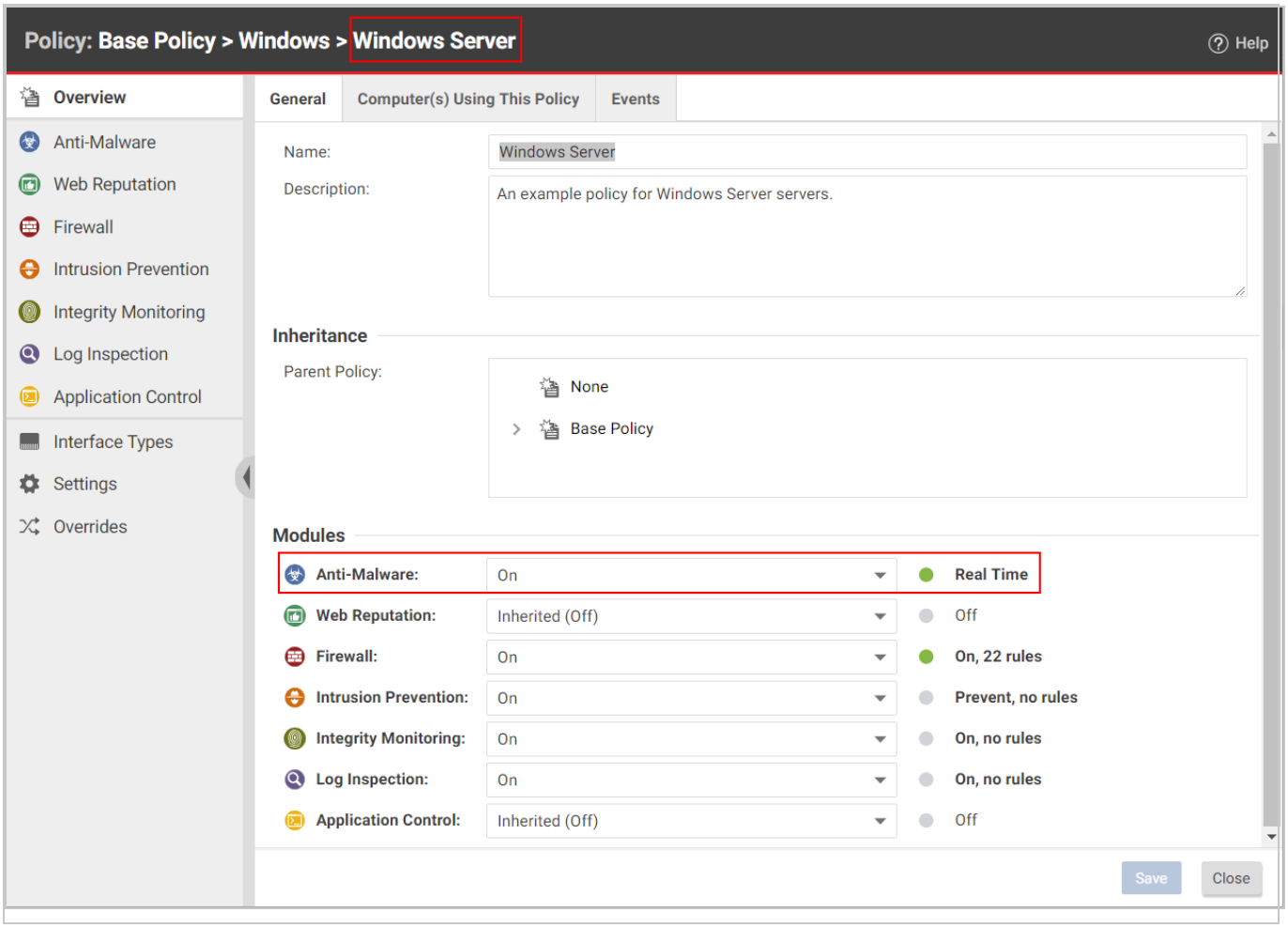


つまり、この設定は親ベースポリシーから継承されます。また、ベースポリシーの不正プログラム対策設定を[オフ]から[オン]に変更する場合は、Windowsポリシーの設定も変更されます(これにより、Windowsポリシーの設定は[継承 (オン)]になります。カッコ内の値は、継承された現在の設定を示しています)。

オーバーライド

[オーバーライド]画面には、対象のポリシーまたは特定のコンピュータレベルでオーバーライドされた設定の数が表示されます。このレベルのオーバーライドを取り消すには、[削除]ボタンをクリックします。

次の例では、Windows ServerポリシーがWindowsポリシーの子ポリシーとなっています。ここでは、不正プログラム対策設定は継承されていません。オーバーライドされ、[オン]になっています。



ヒント: オーバーライドの確認、作成、削除は、Deep Security APIを使用して自動化できます。例については、Deep Security Automation Centerにあるガイド「Configure Computers to Override Policies」を参照してください。

オブジェクトのプロパティをオーバーライドする

このポリシーに含まれる侵入防御ルールは、Deep Security Managerによって保存されている侵入防御ルールのコピーであり、他のポリシーで使用できます。特定のルールのプロパティを変更する場合は、ルールのプロパティをグローバルに変更して、そのルールを使用しているすべてのインスタンスに変更を適用するか、またはプロパティをローカルで変更して、その変更をローカルにのみ適用します。コンピュータまたはポリシーのエディタの初期設定の編集モードはローカルです。[現在割り当てられている侵入防御ルール] エリアにあるツールバーの [プロパティ] をクリックすると、[プロパティ] 画面で行うすべての変更が表示され、その変更がローカルにのみ適用されます(ルール名などの一部のプロパティはローカルでは編集できません。これらはグローバルでのみ編集できます)。

ルールを右クリックすると、コンテキストメニューが表示されます。このメニューから2つのプロパティ編集モードオプションを選択できます。[プロパティ] を選択すると、ローカルエディタ画面が表示されます。[プロパティ(グローバル)] を選択すると、グローバルエディタ画面が表示されます。

Deep Securityで共有される大部分の共通オブジェクトのプロパティを、ポリシー階層内のすべてのレベルおよびその下位の個々のコンピュータレベルでオーバーライドできます。

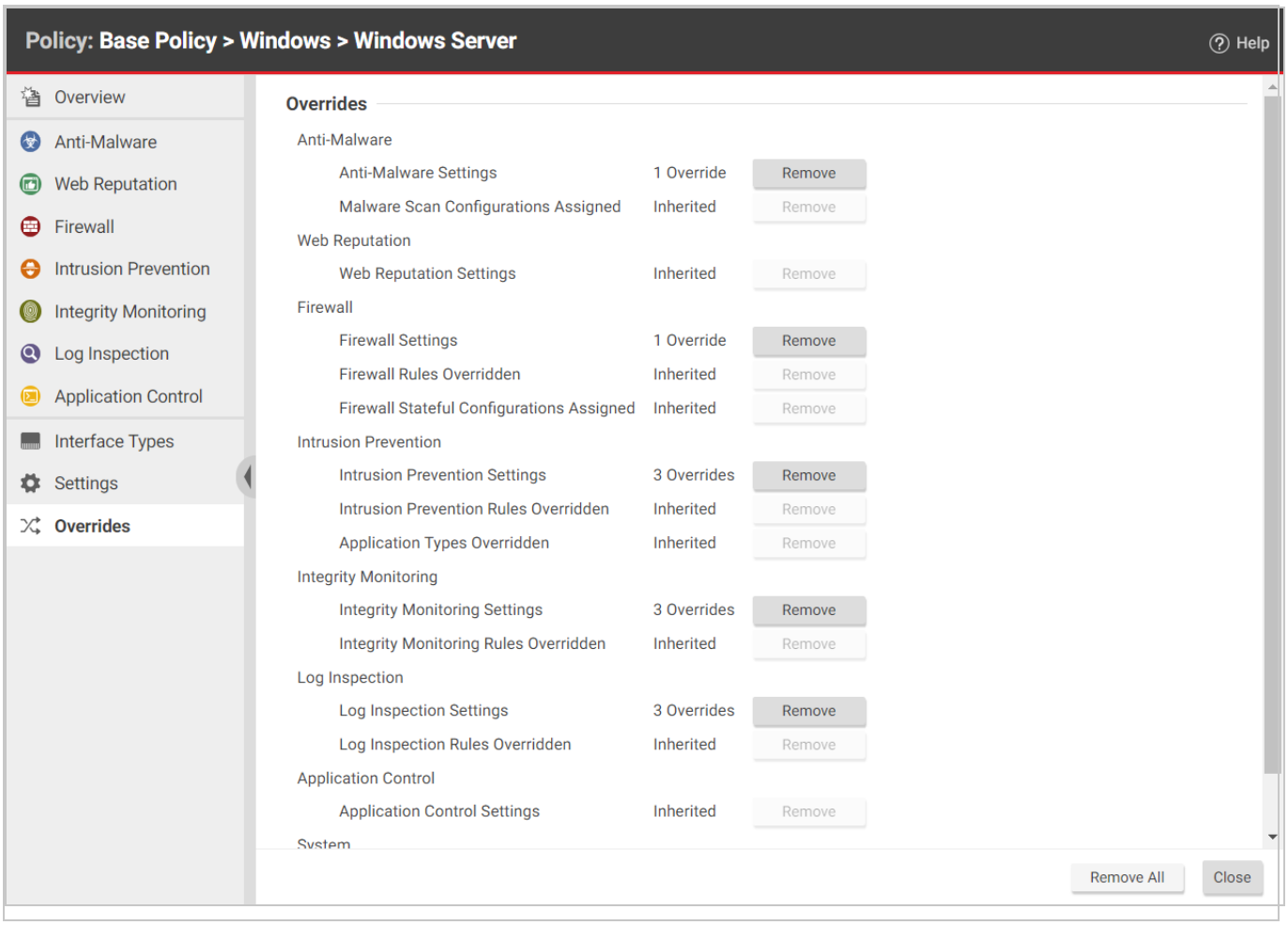
ルールの割り当てをオーバーライドする

ポリシーレベルまたはコンピュータレベルで、追加のルールをいつでも割り当てることができます。ただし、特定のポリシーレベルまたはコンピュータレベルで有効なルールの割り当てをローカルで解除することはできません。これは、そのルールの割り当てが親ポリシーから継承されているためです。このようなルールの割り当ては、ルールが最初に割り当てられたポリシーレベルで解除する必要があります。

ヒント: オーバーライドする設定が多数ある場合は、親ポリシーのブランチを作成することを検討してください。

コンピュータまたはポリシーのオーバーライド項目をまとめて確認する

ポリシーまたはコンピュータでオーバーライドした設定の数を確認するには、コンピュータまたはポリシーのエディタで [オーバーライド] 画面に移動します。



保護モジュール別のオーバーライド項目が表示されます。[削除] ボタンをクリックすれば、システムまたはモジュールのオーバーライド項目を元に戻すことができます。

推奨設定の検索の管理と実行

Deep Securityは、コンピュータで推奨検索を実行して、侵入防御、整合性監視、および適用または削除する必要があるログ検査ルールを識別します。

ヒント: 推奨設定の検索は、実装すべきルールリストを確立するための適切な開始ポイントとなりますが、推奨設定の検索では検出されない重要な追加ルールがいくつかあります。これらのルールは手動で実装する必要があります。"一般的な脆弱性の追加ルールを実装する" on page 736を参照してください。

推奨設定の検索を設定し、個々のコンピュータまたはポリシーレベルで推奨されたルールを実装できます。大規模な環境の場合、トレンドマイクロでは、ポリシーを使用して推奨設定を管理することを推

奨します。これにより、1つのソース(ポリシー)からすべてのルールを割り当てることができます。各コンピュータで個々のルールを管理する必要はありません。そのため、一部のルールが、それを必要としていないコンピュータに割り当てられる可能性があります。しかし、パフォーマンスにわずかな影響が及ぶことよりも、ポリシーを通じて行われる処理によって管理が簡素化されるメリットの方が重要です。ポリシーで推奨設定の検索を有効にする場合は、Windowsルールが Linuxコンピュータに割り当てられないように、またはその逆が行われないように、WindowsコンピュータとLinuxコンピュータの検出用に別のポリシーを使用してください。

- "検索内容" below
- "検索の制限" on the next page
- "Adobe Readerルールの推奨事項" on page 731
- "推奨設定の検索を実行する" on page 731
- "推奨設定を自動的に適用する" on page 734
- "検索結果を確認して手動でルールを割り当てる" on page 735
- "推奨ルールを設定する" on page 736
- "一般的な脆弱性の追加ルールを実装する" on page 736
- "トラブルシューティング: 推奨設定の検索失敗" on page 738

検索内容

Deep Securityクライアントは、推奨検索の実行中に次のことについてOSを検索します。

- インストール済みアプリケーション
- Windowsレジストリ
- オープンポート
- ディレクトリリスト
- ファイルシステム
- 実行中のプロセスとサービス
- 環境変数
- ユーザ

Deep Security Virtual Applianceは、仮想マシンでAgentlessの推奨検索を実行できますが、Windowsプラットフォームでのみ実行できます。また、OSの検索には次の制限があります。

- インストール済みアプリケーション
- Windowsレジストリ

- ファイルシステム

検索の制限

技術的または論理的な一部の制限により、ソフトウェアの種類によっては、ルールが正確には推奨されない、またはまったく推奨されないものになります。

- UnixシステムまたはLinuxシステムでは、推奨設定の検索エンジンが、Apache Struts、Wordpress、JoomlaなどのOSの初期設定のパッケージマネージャを使用してインストールされていないソフトウェアを検出できない可能性があります。標準のパッケージマネージャを使用してインストールされたアプリケーションについては、問題はありません。
- UnixシステムまたはLinuxシステムでは、ブラウザやメディアプレーヤなどのデスクトップアプリケーションの脆弱性またはローカルの脆弱性に関するルールは推奨設定の検索に含まれません。
- 一般的なWebアプリケーション保護ルールは推奨設定の検索に含まれません。
- スマートルールは通常、主要な脅威または特定の脆弱性に対応していない限り、推奨設定の検索に含まれません。スマートルールは、1つ以上の既知または未知の (ゼロデイ) 脆弱性に対応します。Deep Security Managerのルールリストでは、スマートルールは [種類] 列に「スマート」と表示されています。
- コンテンツ管理システム (CMS) に関連するルールを扱っているときには、推奨設定の検索でCMSインストールとインストールされているバージョンを検出できません。CMSとともにインストールされているプラグインとそのバージョンも検出できません。そのため、推奨設定の検索で、Webサーバがインストールされ、PHPがシステムでインストールまたは実行されていることが検出されると、すべてのCMS関連の侵入防御ルールが推奨されます。これにより、ルールが過度に推奨されることになりますが、セキュリティのニーズと精度のバランスが取れます。
- 次のWeb技術に関する推奨設定では、必要以上のルールが提案されることがあるため、調整が必要な場合があります。
  - Red Hat JBoss
  - Eclipse Jetty
  - Apache Struts
  - Oracle WebLogic
  - WebSphere
  - Oracle Application Testing Suite
  - Oracle Golden Gate
  - Nginx

- OpenSSLルールは、OpenSSLが明示的にインストールされている場合にのみ、Windowsで推奨されます。アプリケーションが内部で使用しているOpenSSLが別のパッケージとしてインストールされていない場合は、推奨設定の検索では検出されません。
- Linuxシステムでは、Webブラウザのみが該当ベクタである場合は、Java関連の脆弱性のルールは推奨されません。
- 推奨設定の検索では、初期設定のChromeインストールに含まれているAdobe Flash Playerプラグインは検出できません。推奨設定は、Chromeバージョンに基づいて決められます。つまり、不必要なルールが推奨されることがあります。
- 推奨設定の検索は、Deep Security Managerバージョン20.0.789(20 LTS Update 2023-06-28) 以前では動作しません。

Adobe Readerルールの推奨事項

Common Vulnerabilities and Exposures(CVE) に対処するために、Adobe Readerのルールが推奨され、自動的に適用されます。これらのAdobe CVEのほとんどは攻撃に使用されておらず、ほとんどの場合、概念実証(PoC) を利用できませんが、Adobeのコアソフトウェアにはパッチが適用されていません。これにより、多くのルールが適用されたままになり、パフォーマンスの問題が発生する可能性があります。

多数のルールによって発生する潜在的なパフォーマンスの問題を軽減するために、トレンドマイクロでは、攻撃で使用されているか、CVEが検出されてから1年以内にPoCが公開されているAdobe Readerルールのみを推奨します。環境に関するすべての推奨事項を確認することをお勧めします。

推奨設定の検索を実行する

環境の変更は推奨されるルールに影響を与えることがあるため、推奨設定の検索は定期的に実行することをお勧めします (推奨設定の検索は週1回の頻度で実行することをお勧めします)。トレンドマイクロは、毎週火曜日に新しい侵入防御ルールをリリースするので、推奨設定の検索をこれらのリリースの直後に予約することをお勧めします。推奨設定の検索中はCPUサイクル、メモリ、ネットワーク帯域幅などのシステムリソースの使用量が増えるため、検索はピーク時以外に予約することをお勧めします。

推奨設定の検索実行にはいくつかの方法があります。

- 予約タスク: 設定したスケジュールに従って推奨設定の検索を実行する予約タスクを作成します。予約タスクはすべてのコンピュータ、1台のコンピュータ、定義したコンピュータグループ、または特定のポリシーで保護されているすべてのコンピュータに割り当てることができます。"予約タスクを作成して定期的に推奨設定の検索を実行する" on the next page を参照してください。

- 継続検索: 該当ポリシーで保護されるすべてのコンピュータで定期的に推奨設定の検索が実行されるようにポリシーを設定します。継続検索は、個々のコンピュータにも設定できます。このような検索では、実行済みの最後の検索のタイムスタンプが確認され、設定された間隔後に以降の検索が実行されます。こうすることで、環境内で異なる時間に推奨設定の検索が実行されます。この設定は、Agentが2 ~ 3日以上オンラインにならない可能性がある環境で役立ちます (たとえば、頻繁にインスタンスを構築および廃止するクラウド環境など)。"継続検索を設定する" on the next pageを参照してください。
- 手動検索: 1台以上のコンピュータで推奨設定の検索を1回実行します。手動検索は、プラットフォームやアプリケーションを最近大きく変更し、予約タスクを待つのではなく、強制的に新しい推奨設定を確認したい場合に便利です。"推奨設定の検索を手動で実行する" on the next pageを参照してください。
- コマンドライン: Deep Securityのコマンドラインインタフェースを使用して推奨検索を開始します。"コマンドラインの基本" on page 1793を参照してください。
- API: Deep Security APIを介して推奨検索を開始します。"Deep Security APIを使用したタスクの自動化" on page 1824を参照してください。

注意: 予約タスクと進行中の検索では、それぞれ独自の設定で個別に推奨検索を実行できます。予約タスクまたは継続検索のどちらかを使用してください (ただし両方は使用しないでください)。

推奨設定の検索が実行されると、推奨設定の作成の対象となるすべてのコンピュータでアラートが発令されます。

予約タスクを作成して定期的に推奨設定の検索を実行する

1. Deep Security Managerで、[管理]→[予約タスク] ページに移動します。
2. ツールバーの [新規] をクリックし、[新規予約タスク] を選択して新規予約タスクウィザードを表示します。
3. [種類] リストで [コンピュータの推奨設定を検索] を選択して、検索を実行する頻度を選択します。[次へ] をクリックします。
4. 手順3で選択した内容に応じて、次の画面で検索の頻度をより詳細に指定できます。該当する項目を選択し、[次へ] をクリックします。
5. 検索対象のコンピュータを選択し、[次へ] をクリックします。

   注意: すべてのコンピュータ、個々のコンピュータ、コンピュータのグループ、または特定のポリシーが割り当てられているコンピュータを選択できます。大規模な環境の場合は、ポリシーを通じて、推奨設定の検索を含むすべての処理を実行することを推奨します。

6. 新しい予約タスクの名前を指定し、終了時にタスクを実行するかどうか ([[完了] でタスクを実行]) を選択して、[完了] をクリックします。

継続検索を設定する

1. Deep Security Managerで、**コンピュータまたはポリシーエディタ**[1]を開きます。個々のコンピュータまたはポリシーを使用しているすべてのコンピュータに対して検索を設定するかどうかを指定します。

   注意: 大規模な環境の場合は、ポリシーを通じて、推奨設定の検索を含むすべての処理を実行することを推奨します。

2. [設定] をクリックします。[推奨設定]の[一般]タブで、推奨設定の継続的な検索を実行 設定で、進行中の推奨検索を有効または無効にします。[継続検索の間隔] 設定で、検索を実行する間隔を指定します。どちらの設定も、コンピュータまたはポリシーの親から継承できます (継承の仕組みの詳細については"ポリシー、継承、およびオーバーライド" on page 724を参照してください)。

推奨設定の検索を手動で実行する

1. Deep Security Managerで、[Computers]ページに移動します。
2. 検索対象のコンピュータ(複数台も可) を選択します。
3. [処理]→[推奨設定の検索] の順にクリックします。

推奨設定の検索をキャンセルする

推奨設定の検索は開始前にキャンセルできます。

1. Deep Security Managerで、[Computers]ページに移動します。
2. 検索をキャンセルするコンピュータ(複数台も可) を選択します。
3. [処理]→[推奨設定の検索のキャンセル] をクリックします。

推奨設定の検索からルールまたはアプリケーションの種類を除外する

推奨設定の検索結果に特定のルールまたはアプリケーションの種類を含めたくない場合は、それらを検索から除外できます。

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。

1. Deep Security Managerで、**コンピュータまたはポリシーエディタ**[1]を開きます。

   注意: 大規模な環境の場合は、ポリシーを通じて、推奨設定の検索を含むすべての処理を実行することを推奨します。

2. 除外するルールの種類に応じて、[侵入防御]画面、[変更監視]画面、または[セキュリティログ監視]画面に移動します。
3. [一般]タブで、[割り当て/割り当て解除](ルールの場合)または[アプリケーションの種類](アプリケーションの種類の場合)をクリックします。
4. 除外するルールまたはアプリケーションの種類をダブルクリックします。
5. [オプション]タブに進みます。ルールの場合は、[推奨設定から除外]を[はい]または[継承(はい)]に設定します。アプリケーションの種類の場合は、[推奨設定から除外]チェックボックスをオンにします。

推奨設定を自動的に適用する

推奨設定の検索結果が適切な場合に自動的に適用するようにDeep Securityを設定できます。

1. Deep Security Managerで、**コンピュータまたはポリシーエディタ**[2]を開きます。

   注意: 大規模な環境の場合は、ポリシーを通じて、推奨設定の検索を含むすべての処理を実行することを推奨します。

2. 自動的に実装するルールの種類に応じて、[侵入防御]画面、[変更監視]画面、および/または[セキュリティログ監視]画面に移動します(設定は保護モジュールごとに独立して変更できます)。
3. [一般]タブの[推奨設定]の設定を[はい]または[継承(はい)]に変更します。

しかし、すべての推奨設定を自動的に実装できるわけではありません。次のような例外があります。

- 適用する前に設定が必要なルール。
- 推奨設定の検索から除外されたルール。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

[2] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

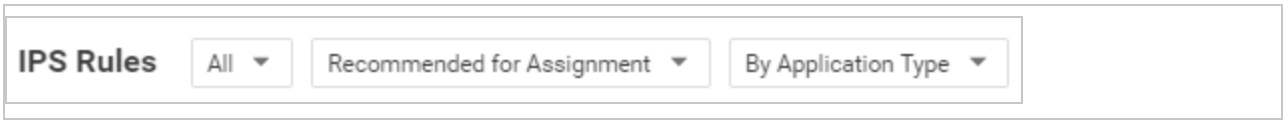
- 自動的に割り当てられた、または割り当て解除されたが、ユーザがオーバーライドしたルール。たとえば、Deep Security自動的にルールが割り当てられた後で割り当て解除された場合、ルールは次回の推奨検索のあとに再割り当てされません。
- ポリシー階層の上位のレベルで割り当てられたルールは、下位のレベルでは割り当てを解除できません。ポリシーレベルでコンピュータに割り当てられたルールは、ポリシーレベルで割り当てを解除する必要があります。
- トレンドマイクロから発行されたものであるが、誤判定のリスクの可能性があるルール(ルールの説明を参照してください)。

検索結果を確認して手動でルールを割り当てる

最新の推奨設定の検索結果は、**コンピュータエディタまたはポリシーエディタ**[1]の保護モジュールの[一般]タブ([侵入防御]、[変更監視]、および[セキュリティログ監視])に表示されます。

次の例は、ポリシーを使用して侵入防御の推奨設定の検索結果を扱う方法を示しています。

1. 推奨設定の検索が完了したら、検索したコンピュータに割り当てられているポリシーを開きます。
2. [侵入防御]→[一般]の順に選択します。存在する場合は未解決の推奨設定の数が[推奨設定]セクションに表示されます。
3. [現在割り当てられている侵入防御ルール]エリアの[割り当て/割り当て解除]をクリックしてルールの割り当て画面を開きます。
4. ルールを[アプリケーションの種類別]でソートし、フィルタの表示メニューから[割り当てを推奨]を選択します。

   すると、割り当てが推奨されているが割り当てられていないルールのリストが表示されます。

5. ルールをポリシーに割り当てるには、ルール名の横にあるチェックボックスをオンにします。 アイコンが表示されているルールには、設定できる設定オプションがあります。 アイコンが表示されているルールには、ルールを有効にする前に設定する必要がある設定があります。

   また、複数のルールを一度に割り当てるには、<Shift> キーまたは <Control> キーを使用してルールを選択し、選択項目を右クリックして[ルールの割り当て]をクリックします。

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

ヒント: 推奨設定の検索の結果には、ルールの割り当てを解除する推奨設定を含めることもできます。この処理は、アプリケーションをアンインストールする場合、ベンダからのセキュリティパッチを適用する場合、または不要なルールが手動で適用されている場合に行うことができます。割り当ての解除が推奨されているルールを表示するには、フィルタの表示メニューから[割り当て解除を推奨] を選択します。

注意: 推奨ルールには完全フラグ ( ) が示されます。部分フラグ ( ) は、アプリケーションの種類に属する一部のルールのみが推奨されているアプリケーションの種類を示します。

推奨ルールを設定する

適用前に設定が必要なルールもあります。たとえば、一部のセキュリティログ監視ルールでは、変更について監視するログファイルの場所を指定する必要があります。この場合、推奨設定が作成されるコンピュータでアラートが発令されます。アラートのテキストには、ルールの設定に必要な情報が含まれます。ポリシーエディタまたはコンピュータエディタで アイコンが表示されているルールには、設定できる設定オプションがあります。アイコンが表示されているルールには、ルールを有効にする前に設定する必要がある設定があります。

一般的な脆弱性の追加ルールを実装する

推奨設定の検索は、実装する必要があるルールリストを作成するための適切な開始ポイントとなりますが、一般的な脆弱性には推奨設定の検索では特定されない追加のルールがいくつかあります。これらのルールは「防御」(ブロック) モードで実装される前に慎重に設定しテストする必要があるためです。これらのルールを設定およびテストし、ポリシーで手動で有効にすることをお勧めします(または個々のコンピュータの場合は):

ヒント: 次のリストに、設定すべき最も一般的な追加ルールを示します。Deep Security Managerのその他のルールを確認するには、種類が「スマート」または「ポリシー」のルールを検索します。

ルール名	アプリケーションの種類
1007598 - Identified Possible Ransomware File Rename Activity Over Network Share	DCERPCサービス
1007596 - Identified Possible Ransomware File Extension Rename Activity Over Network Share	DCERPCサービス

ルール名	アプリケーションの種類
1006906 - Identified Usage Of PsExec Command Line Tool	DCERPCサービス
1007064 - Executable File Uploaded On System32 Folder Through SMB Share	DCERPCサービス
1003222 - Block Administrative Share	DCERPCサービス
1001126 - DNS Domain Blocker	DNSクライアント
1000608 - Generic SQL Injection Prevention 詳細については"SQLインジェクション防御ルールの設定" on page 923を参照	Webアプリケーション共通
1005613 - Generic SQL Injection Prevention - 2	Webアプリケーション共通
1000552 - Generic Cross Site Scripting (XSS) Prevention	Webアプリケーション共通
1006022 - Identified Suspicious Image With Embedded PHP Code	Webアプリケーション共通
1005402 - Identified Suspicious User Agent In HTTP Request	Webアプリケーション共通
1005934 - Identified Suspicious Command Injection Attack	Webアプリケーション共通
1006823 - Identified Suspicious Command Injection Attack - 1	Webアプリケーション共通
1005933 - Identified Directory Traversal Sequence In Uri Query Parameter	Webアプリケーション共通
1006067 - Identified Too Many HTTP Requests With Specific HTTP Method	Webサーバ共通
1005434 - Disallow Upload Of A PHP File	Webサーバ共通
1003025 - Web Server Restrict Executable File Uploads	Webサーバ共通
1007212 - Disallow Upload Of An Archive File	Webサーバ共通

ルール名	アプリケーションの種類
1007213 - Disallow Upload Of A Class File	Webサーバ共通

トラブルシューティング: 推奨設定の検索失敗

サーバでの推奨設定の検索失敗の場合は、次の手順に従って問題を解決します。トラブルシューティング後も問題が解決しない場合は、Agentから診断パッケージを作成して、サポートに問い合わせてください。

通信

通常、通信障害が発生すると、エラーメッセージ本文に「プロトコルエラー」が示されます。

Deep Security MangerからAgentへの受信ファイアウォールを開いていなかった場合は、ポートを開くか、Agentからの通信に切り替えます。詳細については、"Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511を参照してください。

サーバリソース

サーバのCPUリソースとメモリリソースを監視します。検索中にメモリまたはCPUが使い尽くされそうになる場合は、リソースを増やします。

タイムアウト値

推奨設定の検索のタイムアウト値を大きくします。

1. コマンドプロンプトを開いて、Deep Security Managerのインストールフォルダに移動します。
2. 以下のコマンドを入力します(マルチテナント環境の場合は、テナント名を追加します)。

   ```
   dsm_c -action changesetting -name settings.configuration.agentSocketTimeoutOverride -value 1200
   ```

   ```
   dsm_c -action changesetting -name settings.configuration.defaultSocketChannelTimeout -value 1200000
   ```

   ```
   dsm_c -action changesetting -name settings.configuration.recoScanKeepAliveTimeInterval -value 180000
   ```

3. Deep Security Virtual Applianceを使用している場合は、次のコマンドも入力します。

   ```
   dsm_c -action changesetting -name settings.configuration.timeoutEpsecScanRequest -value 1770
   ```

```
dsm_c -action changesetting -name settings.configuration.timeoutDsamCommandChannel -value
1800
```

コンピュータで使用可能なインタフェースの検出と設定

コンピュータエディタとポリシーエディタの [インタフェース] セクション (コンピュータエディタ) と[インタフェースの種類] セクション (ポリシーエディタ) には、コンピュータで検出されたインタフェースが表示されます。インタフェースが複数割り当てられたポリシーがコンピュータに割り当てられている場合、ポリシーで定義されたパターンと一致するインタフェースが検出されます。

ポリシーエディタの [インタフェースの種類] セクションにはこの他にも以下の機能があります。

複数のインタフェースに対してポリシーを設定する

コンピュータに複数のインタフェースがある場合は、ファイアウォールルールなどのポリシーの各種エレメントを各インタフェースに割り当てることができます。

1. ポリシーエディタで [インタフェースの種類] をクリックします。
2. [ネットワークインタフェースの種類] セクションで、[ルールを特定のインタフェースに適用] を選択します。
3. 表示された [インタフェースの種類] セクションで、名前とパターン照合文字列を入力します。

インタフェースの種類の名前は、参照用でのみ使用されます。一般的な名前には、「LAN」、「WAN」、「DMZ」、「Wi-Fi」などがありますが、どのような名前をネットワークのトポロジーで使用してもかまいません。

すべてのコンテナネットワークインタフェースとホスト仮想インタフェースに使用されるインタフェース名は「integrated_veth」であり、MACアドレスは02:00:00:00:00:00です。

パターン照合ではワイルドカードによるインタフェース名の照合ができ、インタフェースを適切な種類へ自動マッピングします。たとえば、「ローカル エリア接続 *」、「eth*」、「Wireless *」などのように照合します。自動でインタフェースをマッピングできないときは、アラートがトリガされます。その際は、特定のコンピュータのコンピュータエディタの [インタフェース] 画面から手動でマッピングできます。

注意: Deep Securityがこれらのエントリに一致しないコンピュータ上のインタフェースを検出した場合、マネージャはアラートをトリガします。

インタフェース制限を強制する

インタフェース制限が有効な場合、ファイアウォールでは、ローカルコンピュータのインタフェース名が、正規表現パターンと照合されます。インタフェース制限を強制するには、ポリシーエディタまたはコンピュータエディタの [ファイアウォール]→[インタフェース制限] タブにある [インタフェース制限の有効化] オプションをクリックして、コンピュータのインタフェース名と一致する文字列パターンを優先度順に入力します。

警告: インタフェース制限を有効にする前に、インタフェースパターンを適切な順序で設定し、必要な文字列パターンをすべて追加し、不要なパターンは削除してください。優先度が最も高いパターンのインタフェースのみが、トラフィックの転送を許可されます。それ以外のインタフェース (リスト内にある残りのパターンのいずれかと一致するインタフェース) は、「制限」されます。制限されたインタフェースは、ファイアウォールの [許可] ルールを使用して特定のトラフィックを許可しないかぎり、すべてのトラフィックをブロックします。

[1つのアクティブインタフェースに制限] を選択すると、優先度が最も高いパターンのインタフェースが複数見つかった場合でも、1つのインタフェースからのトラフィックのみが許可されます。

注意: Deep Securityは、POSIX基本正規表現を使用してインタフェース名を照合します。基本的なPOSIX正規表現の詳細については、https://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap09.html#tag_09_03を参照してください。

コンピュータエディタの [概要] セクション

コンピュータエディタの [概要] 画面には、次のタブがあります。

- "[一般] タブ" below
- "[処理] タブ" on page 744
- "[TPM] タブ" on page 745
- "[システムイベント] タブ" on page 746
- "[除外] タブ" on page 746

[一般] タブ

- ホスト名: [コンピュータ] 画面の [名前] 列に表示されます。名前は、コンピュータのIPアドレスまたはコンピュータのホスト名のいずれかを指定する必要がありますIPアドレスの代わりにホスト名を

使用する場合は、完全修飾ホスト名または相対ホスト名のいずれも使用できます。解決できるホスト名、またはDeep Security Managerがアクセスできる有効なIPアドレスを指定する必要があります。これは、Deep Security Managerとエージェントコンピュータ間の通信がホスト名に基づいているためです。Relay有効化済みAgentでは、Relayグループ内のすべてのコンピュータが、指定したIPアドレスまたはホスト名にアクセスできる必要があります。Deep Security Managerが対象コンピュータにアクセスできない場合、通信方向は[Agent / Appliance Initiated]([設定]→[コンピュータ]) に設定する必要があります。

- 前回使用されたIP: <IP_address>: コンピュータで前回使用されたIP。前回使用されたIP に、Deep Security Agentのホストの IPアドレスが表示されないことがあります。代わりに、プロキシ、ロードバランサ、エラスティックロードバランサ(ELB), など、Deep Security Managerとの通信にAgentが使用するIPアドレス) になります。
- 表示名: [表示名] 列、およびホスト名の値の横にある丸カッコ内に表示されます。
- 説明: コンピュータの説明です。
- プラットフォーム: コンピュータのOSの詳細は、ここに表示されます。
- グループ: コンピュータの所属するコンピュータグループがリストに表示されます。コンピュータの割り当てを既存の別のコンピュータグループに変更できます。
- ポリシー: このコンピュータに割り当てたポリシーです (存在する場合)。

  注意: ルールがポリシーとは独立して割り当てられている場合は、コンピュータでポリシーの割り当てを解除しても、そのルールが引き続きコンピュータ上で有効となることがあるので注意してください。

- 資産の重要度 : Deep Security Managerは、セキュリティイベントの重要度を定量化するためにランキングシステムを使用します。ルールには重要度 (高、中、低など) が割り当てられ、資産 (コンピュータ) には「資産の重要度」レベルが割り当てられます。これらのレベルは、数値で表記されます。コンピュータでルールがトリガされると、資産の重要度の値とルールの重要度の値が乗算されます。この結果がスコアとなり、イベントを重要度別にソートする際に使用されます(イベントのランク付けは [イベント] 画面で参照できます)。この [資産の重要度] リストを使用して、コンピュータに資産の重要度を割り当てます(ルールおよび資産の重要度レベルを表す数値は、[管理]→[システム設定]→[ランク付け] で編集できます)。
- セキュリティアップデートのダウンロード元: このコンピュータ上のAgent/Applianceがセキュリティアップデートのダウンロード元として使用するRelayグループをリストから選択します(AgentがRelayとして機能している場合には表示されません)。

コンピュータのステータス

[ステータス] エリアには、コンピュータの最新情報と、そのコンピュータで有効になっている保護モジュールの最新情報が表示されます。1行目には、コンピュータがAgentまたはAppliance (コンバインモードの場合はその両方) によって保護されているかどうかが表示されます。

- ステータス:
  - コンピュータが管理対象外の場合、ステータスには、AgentまたはApplianceの有効性に関する状態が表示されます。ステータスには「検出済み」または「新規」が表示され、その後のカッコ内にAgentまたはApplianceの状態が示されます (「Agent/Applianceなし」、「不明」、「再有効化が必要」、「有効化が必要」、または「無効化が必要」)。
  - コンピュータが管理対象で、コンピュータのエラーがない場合は、ステータスに「管理対象」と表示され、その後のカッコ内にAgentまたはApplianceの状態が示されます (「オンライン」または「オフライン」)。
  - コンピュータが管理対象で、AgentまたはApplianceが変更の検索やAgentのアップグレード (インストールプログラムの送信) などの処理を実行している場合は、そのタスクのステータスが表示されます。
  - コンピュータに、「オフライン」、「アップデートの失敗」などのエラーがある場合、ステータスにはそのエラーが表示されます。複数のエラーが存在する場合、ステータスには「複数のエラー」と表示され、その下に各エラーが一覧表示されます。

保護モジュールのステータス

Deep Security 9.5以降では、保護モジュールは必要に応じてAgentに配信されます。Agentが最初にインストールされた時点では、コアモジュールだけが含まれています。

Status 領域には、Deep Securityモジュールの状態に関する情報が表示されます。このステータスには、Agent上のモジュールの状態と、Deep Security Managerでのその設定が反映されます。「オン」のステータスは、モジュールがDeep Security Managerで設定されており、Deep Security Agentにインストールされ、Deep Security Agentで動作していることを示します。

モジュールが「オン」で動作している場合、ステータスライトは緑色になります。個別にルールを割り当て可能なモジュールの場合、ステータスライトが緑色になるためには、少なくとも1つのルールが割り当てられている必要があります。

- 不正プログラム対策: 不正プログラム対策保護がオンとオフのどちらであるか、およびリアルタイム検索または手動検索のどちらについて設定されているかを示します。
- Webレピュテーション: Webレピュテーションがオンとオフのどちらであるかを示します。
- デバイスコントロール: デバイスコントロールがオンとオフのどちらであるかを示します。

- ファイアウォール: ファイアウォールのオン/オフの状態と有効なルールの数を示します。
- 侵入防御: 侵入防御のオン/オフの状態と有効なルールの数を示します。
- 変更監視: 変更監視のオン/オフの状態と有効なルールの数を示します。
- セキュリティログ監視: セキュリティログ監視のオン/オフの状態と有効なルールの数を示します。
- アプリケーションコントロール: アプリケーションコントロールがオンとオフのどちらであるかを示します。
- Scanner (SAP): Deep Security ScannerSAP機能のステータス。
- オンライン: Managerが現在AgentまたはApplianceと通信可能かどうかを示します。
- 前回の通信: Managerがこのコンピュータのまたは正常に通信した前回の日時です。
- ステータスの確認: Managerによってただちにハートビート操作が強制実行されて、AgentまたはApplianceのステータスが確認されます。ステータスの確認では、AgentまたはApplianceのセキュリティアップデートは実行されません。ManagerとAgentまたはAppliance間の通信が[Agent/Applianceから開始] に設定されている場合は、[ステータスの確認] ボタンが無効になります。ステータスを確認しても、コンピュータのログはアップデートされません。コンピュータのログをアップデートするには、[処理] タブに進みます。
- 警告/エラーのクリア: このコンピュータに対するアラートまたはエラーを消去します。
- ESXiサーバ: コンピュータがVirtual Applianceによって保護されている仮想マシンの場合は、コンピュータをホストするESXiサーバが表示されます。
- Appliance: コンピュータがVirtual Applianceによって保護されている仮想マシンの場合は、コンピュータを保護するApplianceが表示されます。
- ESXiバージョン: コンピュータがESXiサーバの場合は、ESXiのバージョン番号が表示されます。
- Filter Driverのバージョン: コンピュータがESXiサーバの場合は、Filter Driverのバージョン番号が表示されます。Deep Security Virtual Appliance 10.0以降とESXi 6.0以降を使用している場合は、Filter Driverを使用していないため「なし」と表示されます。
- ゲスト: コンピュータがESXiサーバの場合は、Virtual Applianceとゲストが表示されます。
- Applianceのバージョン: コンピュータがVirtual Applianceの場合は、Applianceのバージョン番号が表示されます。
- ゲストが保護される対象: コンピュータがVirtual Applianceの場合は、ESXiサーバのIPと保護されているゲストが表示されます。

VMware仮想マシンの概要

このセクションには、AgentまたはApplianceが実行される仮想マシンに関するハードウェアとソフトウェアの設定情報の概要が表示されます (VMware仮想マシンのみ)。

[処理] タブ

有効化

新たにインストールされたDeep Security AgentまたはApplianceは、ポリシー、ルール、イベントログの要求などをDeep Security Managerに送信する前に、Deep Security Managerによって「アクティベート」されている必要があります。有効化処理では、Manager (またはそのいずれかのノード) とAgent/Applianceが互いを一意に識別するためのSSLキーが交換されます。Deep Security Managerによってアクティベートされると、Agent/ApplianceはDeep Security Managerをアクティベートしたデバイス(またはそのノードの1つ) とのみ命令を受け入れたり、通信したりします。

非アクティベーションAgentまたはApplianceは、Deep Security Managerによってアクティベートされます。

AgentおよびApplianceは、コンピュータ上でローカルで、またはコンピュータをアクティベートしたDeep Security Managerからのみ非アクティブ化できます。AgentまたはApplianceがすでに有効化されている場合は、このエリアのボタンが[有効化] ではなく[再有効化] と表示されます。再有効化の作用は、有効化と同じです。再有効化すると、AgentまたはApplianceは最初にインストールされたときの状態にリセットされ、新しいSSLキーセットの交換が行われます。

ポリシー

Deep Security Managerを使用してコンピュータ上のAgentまたはApplianceの設定を変更した場合 (新しい侵入防御ルールの適用、ログ設定の変更など) 、Deep Security Managerは新しい情報をAgentまたはApplianceに送信する必要があります。これが「ポリシーの送信」命令です。ポリシーのアップデートは通常ただちに実行されますが、[ポリシーの送信] ボタンをクリックして強制的にアップデートすることもできます。

Agentソフトウェア

ここには、コンピュータ上で現在実行されているAgentまたはApplianceのバージョンが表示されます。AgentまたはApplianceの新しいバージョンがコンピュータのプラットフォームで使用可能な場合は、[Agentのアップグレード] または [Applianceのアップグレード] ボタンをクリックして、AgentまたはApplianceをDeep Security Managerからリモートでアップグレードできます。[管理]→[システム設定]→[アップデート] タブに移動して、いずれかのコンピュータで新しいバージョンのAgentまたはApplianceソフトウェアが実行されている場合に、Deep Security Managerを設定してアラートをトリガできます。

注意: WindowsでDeep Security AgentやRelayをアップデートまたはアンインストールする際は、Agentセルフプロテクションを無効にしておく必要があります。これを実行するには、Deep Security

Managerで、[コンピュータエディタ[1]]→[設定]→[一般]の順に選択します。[Agentセルフプロテクション]で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否]の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。

サポート情報

[診断パッケージの作成]ボタンでは、コンピュータのAgentまたはApplianceの状態に関するスナップショットを作成できます。スナップショットは、サポート担当者がトラブルシューティングの目的で要求することがあります。

コンピュータとの通信が失われた場合は、診断パッケージをローカルに作成できます。詳細については、"診断パッケージの作成" on page 2019を参照してください。

[TPM] タブ

注意: [TPM] タブは、ESXiサーバの [処理] タブの代わりに表示されます。

Trusted Platform Module (TPM) は、ハードウェア認証に使用されるチップの一種です。VMwareは、ESXiハイパーバイザでTPMを使用します。起動シーケンスの間、ESXiは各ハイパーバイザコンポーネントのSHA-1ハッシュを、読み込み時に一連のレジスタに書き込みます。ある起動シーケンスから次の起動シーケンスまでの間、これらの値に想定外の変更が発生した場合は、セキュリティの問題があることを示している可能性があるため、調査することをお勧めします。Deep Securityでは、起動のたびにESXiのTPMを監視し、変更が検出された場合はアラートを発令できます。TPMをサポートしないESXiでTPM監視を有効にするオプションを選択すると、そのオプションは自動的に無効になります。

TPM監視の有効化: 選択すると、TPM監視が有効化されます。

TPM監視が有効なレジスタ値の取得に失敗したときにアラートを生成します。ESXiのブートシーケンス中にTrusted Platform Moduleがハイパーバイザコンポーネントの有効なレジスタ値を取得できなかった場合にDeep Securityでアラートを生成する場合に選択します。

TPMのレジスタデータのインポート: TPMデータがインポートされているかどうかを示します。

前回のTPMチェック: 前回いつTPMがチェックされたかを示します。[今すぐ確認]をクリックすると、TPMチェックを開始できます。

---

[1] コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

注意: TPM監視の最小要件は次のとおりです。

- ESXiにTPM/TXTがインストールされ、有効になっている(詳細についてはVMwareドキュメントを参照)
- Deep Securityの変更監視およびアプリケーションコントロールモジュールの適切なライセンスがある

[システムイベント] タブ

イベントについては、"システムイベント" on page 1342を参照してください。

[除外] タブ

USBデバイスの除外ルール数制限

各コンピュータで現在サポートされているUSBデバイスの除外ルールの数は1000です。

ポリシーエディタの [概要] セクション

ポリシーエディタの [概要] セクションには、次のタブがあります。

- "[一般] タブ" below
- "[このポリシーを使用しているコンピュータ] タブ" on the next page
- "[イベント] タブ" on the next page
- "[除外] タブ" on the next page

[一般] タブ

一般

- 名前:[表示名] 列、およびホスト名の値の横にある丸カッコ内に表示されます。
- 説明: コンピュータの説明です。

継承

現在のポリシーの設定の継承元である親ポリシー(ある場合)を特定します。

モジュール

- 不正プログラム対策: 不正プログラム対策保護がオンとオフのどちらであるか、およびリアルタイム検索または手動検索のどちらについて設定されているかを示します。
- Webレピュテーション: Webレピュテーションがオンとオフのどちらであるかを示します。
- デバイスコントロール: Webレピュテーションがオンとオフのどちらであるかを示します。
- ファイアウォール: ファイアウォールのオン/オフの状態と有効なルールの数を示します。
- 侵入防御: 侵入防御のオン/オフの状態と有効なルールの数を示します。
- 変更監視: 変更監視のオン/オフの状態と有効なルールの数を示します。
- セキュリティログ監視: セキュリティログ監視のオン/オフの状態と有効なルールの数を示します。
- アプリケーションコントロール: アプリケーションコントロールがオンとオフのどちらであるかを示します。

[このポリシーを使用しているコンピュータ] タブ

このポリシーが割り当てられているコンピュータを一覧表示します。

[イベント] タブ

イベントについては、"システムイベント" on page 1342を参照してください。

[除外] タブ

USBデバイス除外ルール数の制限

各コンピュータで現在サポートされているUSBデバイスの除外ルールの数は1000です。

ネットワークエンジン設定

ポリシーまたはコンピュータのネットワークエンジンの設定を編集するには、設定するポリシーまたはコンピュータの**ポリシーエディタ**[1]または**コンピュータエディタ**[2]を開き、[設定]→[詳細]をクリックします。

---

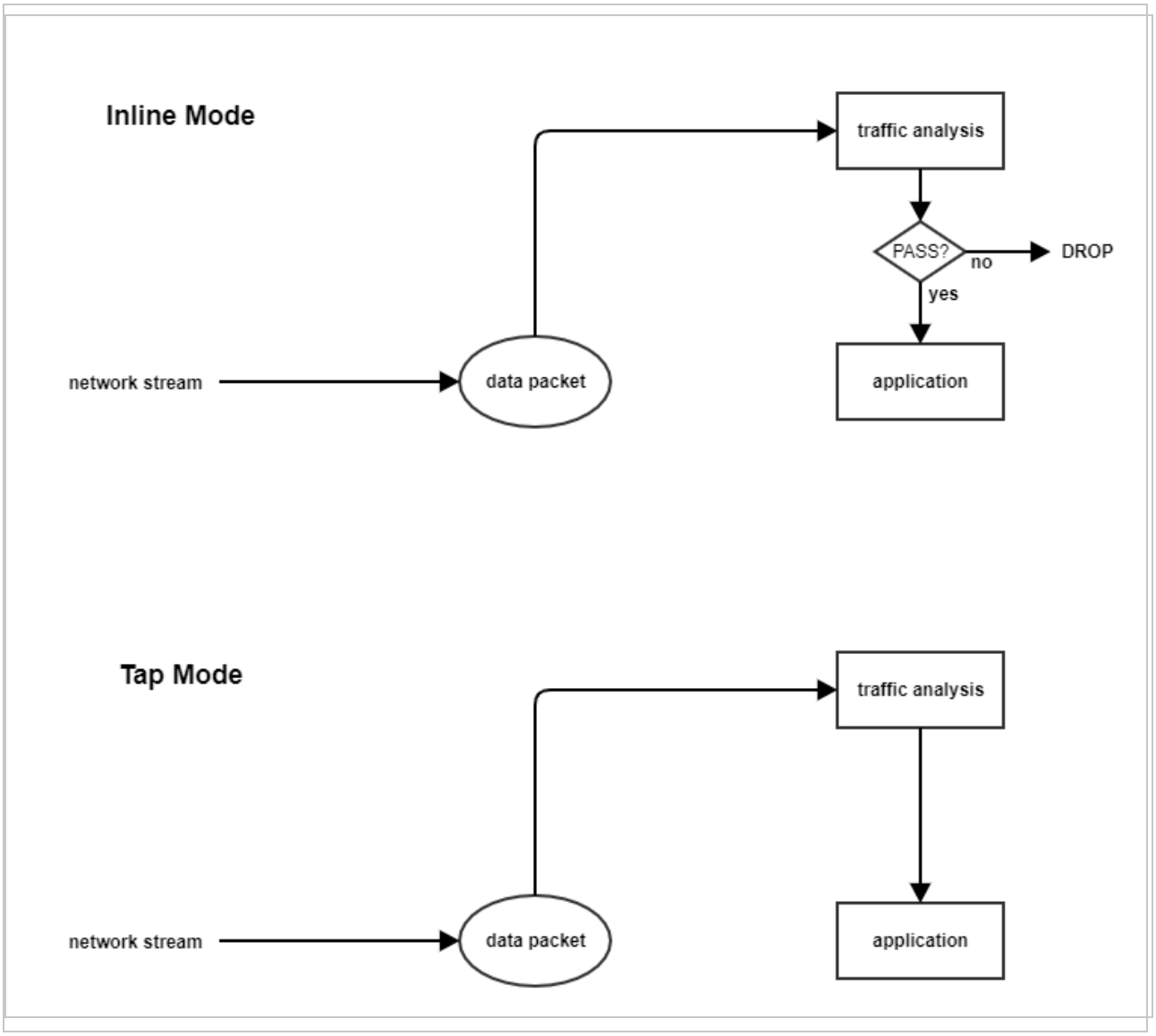
[1] ポリシーエディタを開くには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。

[2] コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

注意: [詳細] タブには、[イベント] 設定もあります。これらの設定については、"ログファイルのサイズを制限する" on page 1156を参照してください。このタブには、[Agentの設定パッケージが最大サイズを超えた場合にアラートを生成する] 設定もあります。この設定を使用して、[Agentの設定パッケージが大きすぎる] 設定の表示を制御します。

以下の設定を使用できます。

- ネットワークエンジンモード: ネットワークエンジンは、パケットをブロックするか許可するかを決定するコンポーネントであり、侵入防御、ファイアウォール、Webレピュテーションの各モジュール内にあります。ファイアウォール および 侵入防御 モジュールの場合、ネットワークエンジンはパケットの健全性チェックを実行し、各パケットが ファイアウォール ルールと侵入防御 ルール(「).に一致するルール」とも呼ばれます) を通過することも確認します。ネットワークエンジンは、インラインモードまたはタップモードで動作できます。インラインで動作している場合、パケットストリームはネットワークエンジンを通過し、設定したルールに基づいて破棄または転送されます。ステートフルテーブルが維持され、ファイアウォール ルールが適用され、侵入防御 ルールとファイアウォール ルールを適用できるようにトラフィックの正規化が実行されます。タップモードで動作している場合、パケットは常に渡されます。ただし、ドライバのフックの問題またはインタフェースの隔離は例外です。タップモードでは、パケット遅延も導入されるため、スループットが低下する可能性があります。



- ネットワークエンジンのステータスチェック: この設定は、エージェントがネットワークエンジンのステータスを監視するかどうかを決定します。これは初期設定で有効になっていますが、無効にすることもできます。関連するイベントについては、「ネットワークエンジンのステータス (Windows OS)」を参照してください。
- エラー発生時の処理: この設定では、不良パケット検出時のネットワークエンジンの動作を決定します。初期設定 (Fail-Closed) では、不良パケットはブロックされますが、後述する理由により、一部の不良パケットを通過させることもできます (Fail-Open)。
  - ネットワークエンジンのシステムエラー: この設定では、メモリ不足エラー、割り当てメモリエラー、ネットワークエンジン (DPI) デコードエラーなど、ネットワークエンジンホストのシステムエラーによって生じる不良パケットを、ネットワークエンジンでブロックするか許可するかを決定し

ます。オプションは次のとおりです。

- Fail-Closed (初期設定): ネットワークエンジンで不良パケットをブロックします。ルールマッチングは実行しません。このオプションを使用すると、最も高いレベルのセキュリティが提供されます。
- Fail-Open: ネットワークエンジンで不良パケットの通過を許可します。ルールマッチングは実行せず、イベントをログに記録します。高負荷やリソース不足によりAgentまたはVirtual Applianceでネットワーク例外が頻繁に発生する場合は、[Fail-Open] の使用を検討してください。

- ネットワークパケットのサニティチェックエラー: この設定では、パケットのサニティチェックでエラーとなるパケットを、ネットワークエンジンでブロックするか許可するかを決定します。健全性チェック失敗の例：ファイアウォール正常性検査の失敗、ネットワーク層2,3、または4属性の確認の失敗、TCPの状態の確認の失敗。オプションは次のとおりです。
  - Fail-Closed (初期設定): ネットワークエンジンでエラーパケットをブロックします。ルールマッチングは実行しません。このオプションを使用すると、最も高いレベルのセキュリティが提供されます。
  - Fail-Open: ネットワークエンジンでエラーパケットの通過を許可します。エラーパケットに対するルールマッチングは実行せず、イベントをログに記録します。ルールマッチング機能を維持しつつ、パケットのサニティチェックを無効にしたい場合は、[Fail-Open] の使用を検討してください。

- 回避技術対策モード: 回避技術対策の設定では、分析を回避しようとする異常なパケットに対するネットワークエンジンによる処理を管理します。詳細については、"回避技術対策の設定" on page 948を参照してください。

- ネットワークエンジンの詳細オプション: [継承] チェックボックスをオフにすると、以下の設定をカスタマイズできます。
  - CLOSEDタイムアウト: ゲートウェイで使用します。ゲートウェイが「ハードクローズ」(RST) を伝えると、RSTを受信したゲートウェイ側は、接続を終了するまで、設定された時間の間、接続をアライブにします。
  - SYN_SENTタイムアウト: 接続を終了するまでSYN_SENT状態になっている時間。
  - SYN_RCVDタイムアウト: 接続を終了するまでSYN_RCVD状態になっている時間。
  - FIN_WAIT1タイムアウト: 接続を終了するまでFIN_WAIT1状態になっている時間。
  - ESTABLISHEDタイムアウト: 接続を終了するまでESTABLISHED状態になっている時間。
  - ERRORタイムアウト: エラー状態で接続を保持する時間(UDP接続の場合、エラーはさまざまなUDPの問題が原因で発生する可能性があります。TCP接続の場合、おそらくパケットがファイアウォールによって破棄されたためです。)

- DISCONNECTタイムアウト: 切断するまで接続がアイドル状態になっている時間。
- CLOSE_WAITタイムアウト: 接続を終了するまでCLOSE_WAIT状態になっている時間。
- CLOSINGタイムアウト: 接続を終了するまでCLOSING状態になっている時間。
- LAST_ACKタイムアウト: 接続を終了するまでLAST_ACK状態になっている時間。
- ACKストームタイムアウト: ACKストーム内で再送されるACK間の最長期間。つまり、ACKが再送される頻度が低く、このタイムアウトが発生した場合、ACKはACKストームの一部とはみなされません。
- ブートスタートタイムアウト: ゲートウェイで使用します。ゲートウェイが再起動されるとき、ゲートウェイを通過している既存の接続が確立している場合があります。このタイムアウトでは、ゲートウェイが再起動される前に、確立された接続の一部である非SYNパケットを許可する時間が定義されます。
- コールドスタートタイムアウト: ステートフル機能が開始される前に、確立された接続に属している非SYNパケットを許可する時間。
- UDPタイムアウト: UDP接続の最大時間。
- ICMPタイムアウト: ICMP接続の最大時間。
- Null IPを許可: 送信元または送信先IPアドレスがないパケットを許可またはブロックします。
- バージョン8以前のAgentとApplianceでIPv6をブロック: バージョン8.0以前のAgentおよびApplianceでIPv6パケットをブロックまたは許可します。

  Deep Security AgentおよびApplianceバージョン8.0以前では、ファイアウォールまたはDPIルールをIPv6ネットワークトラフィックに適用できないため、これらの古いバージョンの初期設定ではIPv6トラフィックをブロックします。

- バージョン9以降のAgentとApplianceでIPv6をブロック: バージョン9.0以降のAgentおよびApplianceでIPv6パケットをブロックまたは許可します。
- 接続クリーンナップタイムアウト: 切断された接続のクリーンナップ時間 (次を参照)。
- 最大接続数 (クリーンナップ単位): 定期的な接続クリーンナップごとに実施するクリーンナップで切断される接続の最大数 (前を参照)。
- 送信元と送信先が同じIPアドレスをブロック: 送信元および送信先IPアドレスが同じパケットをブロックまたは許可します(ループバックインタフェースには適用されません)。
- 最大TCP接続数: 最大TCP同時接続数。
- 最大UDP接続数: 最大UDP同時接続数。
- 最大ICMP接続数: 最大ICMP同時接続数。
- 最大イベント数 (秒単位): 毎秒書き込み可能なイベントの最大数。

- TCP MSSの制限:「TCP MSS」は、TCPセグメントの最大セグメントサイズをバイト単位で定義するTCPヘッダ内のパラメータです。[TCP MSS制限]設定は、TCP MSSパラメータに許可される最小値を定義します。リモート攻撃者が極小の最大セグメントサイズ(MSS)でTCP接続を確立した場合に発生するカーネルパニック攻撃およびサービス拒否(DoS)攻撃を防止できるため、このパラメータの下限値を設定することは重要です。これらの攻撃の詳細については、CVE-2019-11477、CVE-2019-11478、およびCVE-2019-11479を参照してください。「TCP MSS Limit」の初期設定は128バイトで、ほとんどの攻撃サイズに対して保護されます。「No Limit」の値は、下限がなく、TCP MSS値が許可されていることを意味します。

  注意: 10.0アップデート20以降
  のDeep Security Agentの20
  のDeep Security Agentの12.0アップデート1以降
  のDeep Security Agentの11.0アップデート13以降
  のDeep Securityエージェント: TCP MSS制限オプションは、以下のDeep Security Agentのバージョンで動作します

- イベントノードの数: いつでもログとイベントを折りたためるよう、ドライバがそれらを格納するのに使用するカーネルメモリの最大容量。

  イベントの折りたたみは、同じ種類のイベントが連続して多く発生したときに実行されます。このとき、AgentまたはApplianceはすべてのイベントを1つに折りたたみます。

- ステータスコードの無視: このオプションは、特定の種類のイベントを無視します。たとえば、たくさんの「不正なフラグ」が表示される場合は、そのイベントの全インスタンスを無視してかまいません。
- ステータスコードの無視: 同上
- ステータスコードの無視: 同上
- 詳細なログ記録ポリシー:
  - バイパス: イベントをフィルタしません。オーバーライドをIgnore Status Codeやその他の詳細設定より優先させますが、Deep Security Managerで定義されているログ設定は上書きしません。たとえば、Deep Security Managerの[ファイアウォール Stateful Configuration Properties]画面からファイアウォール ステートフル設定ログオプションが設定されても、影響を受けることはありません。
  - 標準: 再送の破棄を除くすべてのイベントがログに記録されます。

- 初期設定: エンジンがタップモードの場合は [タップモード] に切り替わり、インラインモードの場合は、[標準] に切り替わります。
- 下位互換性モード: サポートでのみ使用します。
- 詳細モード:「標準モード」で記録されるログに加え、再送の破棄イベントも記録します。
- ステートフルおよび正規化の抑制:「再送の破棄」、「セッション情報なし」、「不正なフラグ」、「不正なシーケンス」、「不正なACK」、「許可されていないUDP応答」、「許可されていないICMP応答」、および「ポリシーで未許可」を無視します。
- ステートフル、正規化、およびフラグメントの抑制: フラグメンテーション関連のイベントに加え、[ステートフルおよび正規化の抑制] が無視するものすべても無視します。
- ステートフル、フラグメント、および検証機能の抑制: [ステートフル、正規化、およびフラグメントの抑制] が無視するものすべてに加えて、確認に関するイベントも無視します。
- タップモード:「再送の破棄」、「セッション情報なし」、「不正なフラグ」、「不正なシーケンス」、「不正なACK」、「ACK再送の上限」、「切断された接続上のパケット」を無視します。

[ステートフルおよび正規化の抑制]、[ステートフル、正規化、およびフラグメントの抑制]、[ステートフル、フラグメント、および検証機能の抑制]、[タップモード] の各モードで無視されるイベントの包括的なリストについては、"ログに記録するイベントの数を減らす" on page 1167 を参照してください。

- サイレントTCP接続拒否: サイレントTCP接続の破棄がオンの場合、RSTパケットはローカルスタックへのみ送信され、送信元にRSTパケットは送信されません。これにより、潜在的な攻撃者に返す情報量は削減されます。

  [サイレントTCP接続拒否] を有効化する場合、DISCONNECTタイムアウトも調整する必要があります。DISCONNECTタイムアウトの値の範囲は、0秒から10分までの間で設定します。Deep Security エージェントまたはアプライアンスによってアプリケーションが閉じられる前に、接続がアプリケーションによって閉じられるように、この値を設定する必要があります。DISCONNECTタイムアウト値に影響を与える要因としては、OS、接続を確立するアプリケーション、およびネットワークトポロジーが挙げられます。

- デバッグモードを有効にする: デバッグモードの場合、Agent/Applianceは特定のパケット数を取り込みます (下記の [デバッグモードで保持するパケットの数] 内の設定を参照)。ルールがトリガされてデバッグモードがオンになると、Agent/Applianceはルールがトリガされる前に通過した最後のパケット数Xを記録として保持します。これらのパケットは、デバッグイベントとしてManagerに返されます。

> 注意: デバッグモードでは簡単に大量のログが生成されるので、サポート担当者が指示した場合にのみ使用してください。

- デバッグモードで保持するパケットの数: デバッグモードがオンのとき、維持してログするパケット数。
- すべてのパケットデータをログに記録:特定のイベントに関連付けられていないイベントのパケットデータを記録します。ファイアウォールまたは侵入防御ルールつまり、「再送の破棄」や「不正なACK」などのイベントのパケットデータを記録します。

> 注意: イベントの集約によってまとめられたイベントのパケットデータは保存できません

- 期間内で1つのパケットデータのみをログに記録する: このオプションを有効にして[すべてのパケットデータをログに記録する] を有効にしない場合、ほとんどのログにはヘッダデータのみが含まれます。パケット全体は、[1つのパケットデータのみをログに記録する期間] の指定に従って定期的に記録されます。
- 1つのパケットデータのみをログに記録する期間: [1つのパケットデータのみをログに記録する期間] を有効にした場合、この設定にログにパケット全体のデータを含める頻度を指定できます。
- パケットデータがキャプチャされたときに格納する最大データサイズ: ログに追加されるヘッダデータまたはパケットデータの最大サイズ。
- TCP用接続イベントの生成:TCP接続が確立されるたびに、ファイアウォール イベントを生成します。
- ICMP接続イベントの生成:ICMP接続が確立されるたびに、ファイアウォール イベントが生成されます。
- UDPの接続イベントを生成する:UDP接続が確立されるたびに、ファイアウォール イベントを生成します。
- Cisco WAAS接続のバイパス: このモードでは、専用のCISCO WAAS TCPオプションを選択して開始された接続に対して、TCPシーケンス番号のステートフル分析をバイパスします。このプロトコルは、ステートフル ファイアウォール チェックに干渉する無効なTCPシーケンス番号およびACK番号の余分な情報を保持します。CISCO WAASを使用していて、ファイアウォール ログに無効なSEQまたは無効なACKが表示されている場合にのみ、このオプションを有効にしてください。このオプションを選択すると、WAASが有効化されていない接続に対してもTCPステートフルシーケンス番号の確認が実行されます。
- 回避再送の破棄: 処理済みのデータを含む受信パケットは、回避再送の攻撃を避けるため、破棄されます。

- TCPチェックサムの確認: セグメントのチェックサムフィールドのデータは、セグメントの整合性を評価するために使用されます。
- 最小フラグメントオフセット: 許容可能な最小のIPフラグメントオフセットを定義します。オフセットがこの値未満のパケットは、「最小オフセット値以下のIPフラグメント」という理由で破棄されます。0を設定すると制限がなくなります。初期設定は60です。
- 最小フラグメントサイズ: 許容可能な最小のIPフラグメントサイズを定義します。この値より小さいフラグメント化されたパケットは、「最初のフラグメントが最小サイズ未満」という不正の可能性により破棄されます。初期設定は120です。
- SSLセッションのサイズ: SSLセッションキーに保持されるSSLセッションエントリの最大数を設定します。
- SSLセッションの時間: SSLセッション更新キーの有効期間を設定します。
- フィルタIPv4トンネル: Deep Securityのこのバージョンでは使用されません。
- フィルタIPv6トンネル: Deep Securityのこのバージョンでは使用されません。
- Strict Teredo Port Check: Deep Securityのこのバージョンでは使用されません。
- Drop Teredo Anomalies: Deep Securityのこのバージョンでは使用されません。
- 最大トンネルの深さ: このバージョンのDeep Securityでは使用されません。
- 最大トンネルの超過が発生した場合の処理: このバージョンのDeep Securityでは使用されません。
- ドロップIPv6拡張子の種類0: このバージョンのDeep Securityでは使用されません。
- 最小MTU未満のIPv6フラグメントのドロップ: IETF RFC 2460によって規定された最小MTUサイズに満たないIPv6フラグメントがドロップされます。
- IPv6予約済みアドレスのドロップ: 次の予約済みアドレスをドロップします。
  - IETFによって予約済み 0000::/8
  - IETFによって予約済み 0100::/8
  - IETFによって予約済み 0200::/7
  - IETFによって予約済み 0400::/6
  - IETFによって予約済み 0800::/5
  - IETFによって予約済み 1000::/4
  - IETFによって予約済み 4000::/2
  - IETFによって予約済み 8000::/2
  - IETFによって予約済み C000::/3
  - IETFによって予約済み E000::/4

- IETFによって予約済み F000::/5
- IETFによって予約済み F800::/6

許可されるIPv6アドレスは次のとおりです。

- 64:ff9b::/96 - RFC 6052に従って、IPv4アドレスとIPv6アドレスの間のアルゴリズムマッピングで使用される既知のプレフィックス。
- 64:ff9b:1::/48 - RFC 8215に従って、ローカル使用IPv4/IPv6変換用に予約されたプレフィックス。

詳細については、インターネットプロトコルバージョン6のアドレス空間を参照してください。

- IPv6サイトローカルアドレスのドロップ: サイトローカルアドレスFEC0::/1をドロップします。
- IPv6 Bogonアドレスのドロップ: 次のアドレスをドロップします。
  - 「ループバック」::1
  - IPv4互換アドレス::/96
  - IPv4にマッピングされたアドレス::FFFF:0.0.0.0/96
  - IPv4にマッピングされたアドレス::/8
  - OSI NSAP用プレフィックス(RFC4048非推奨) 0200::/7
  - 6bone (非推奨) 3ffe::/16
  - 文書記述用アドレスプレフィックス2001:db8::/32
- 6to4 Bogonアドレスのドロップ: 次のアドレスをドロップします。
  - 6to4 IPv4マルチキャスト2002:e000:: /20
  - 6to4 IPv4ループバック2002:7f00:: /24
  - 6to4 IPv4初期設定 2002:0000:: /24
  - 6to4 IPv4無効 2002:ff00:: /24
  - 6to4 IPv4 10.0.0.0/8 2002:0a00:: /24
  - 6to4 IPv4 172.16.0.0/12 2002:ac10:: /28
  - 6to4 IPv4 192.168.0.0/16 2002:c0a8:: /32
- ゼロペイロードのIPパケットのドロップ: ゼロ長ペイロードのIPパケットをドロップします。
- 不明なSSLプロトコルを削除：不正なプロトコルでDeep Security Managerに接続しようとすると、接続を切断します。初期設定では、プロトコルがhttp/1.1以外であるとエラーになります。

- Allow DHCP DNS: 次のファイアウォールルールが有効かどうかを制御します。

ルールの種類	優先度	方向	プロトコル	送信元ポート	送信先ポート
強制的に許可	4	送信	DNS	任意	53
強制的に許可	4	送信	DHCP	68	67
強制的に許可	4	受信	DHCP	67	68

ルールを有効にすると、Agentコンピュータは表示されているプロトコルとポートを使用してManagerに接続できます。このプロパティには、以下の値を使用できます。

- 継承: ポリシーから設定を継承します。
- ルールをオフにする: ルールを無効にします。この設定によって、Agentコンピュータがオフラインで表示されることがあります。
- DNSクエリを許可: DNS関連のルールのみを有効にします。
- DNSクエリとDHCPクライアントを許可: 3つすべてのルールを有効にします。

- 強制ICMPタイプ3コード4: 次の非表示のファイアウォールルールが有効かどうかを制御します。

ルールの種類	優先度	方向	プロトコル	種類	コード
強制的に許可	4	受信	ICMP	3	4

有効にすると、これらのルールによって、RelayコンピュータをManagerに接続してRelayのハートビートが送信されるようになります。以下の値を使用できます。

- 継承: ポリシーから設定を継承します。
- ルールをオフにする: ルールを無効にします。この値によって、接続がタイムアウトするか、「送信先に到達できません」という応答が発生する可能性があります。
- ICMP type3 code4の「強制的に許可」ルールの追加: このルールを有効にします。

- フラグメントタイムアウト: このように設定されている場合、侵入防御ルールは、パケット(またはパケットフラグメント)の内容が不審と判断された場合、その内容を検査します。この設定では、検査後、パケットを破棄するまで残りのパケットフラグメントを待機する時間が定義されます。

- 保存するフラグメントIPパケットの最大数：Deep Securityで保持する断片化パケットの最大数を指定します。
- フラグメント化されたパケットのタイムアウトを超過したことを示すためにICMPを送信する: この設定を有効にした場合、フラグメントのタイムアウトを過ぎるとICMPパケットがリモートコンピュータに送信されます。
- ホストに属さないMACアドレスのバイパス: 送信先MACアドレスがホストに属していない受信パケットをバイパスします。このオプションを有効にすると、バージョン10.2以降のAgentおよびAppliance上で、NICチーミングまたはプロミスキャスモードのNICのために作成されるパケットの取得によって発生するネットワークイベントの数が減少します。

ユーザーモードソリューション

ユーザーモードは、不正プログラム対策のイベント生成と基本機能をドライバ要件なしで提供します。このソリューションは、カーネルモードで実行するために必要なドライバサポートがないシステムに対して、ある程度の保護を提供し、任意の時点で利用可能な最良の保護を自動的に有効にするオプションを提供します。

基本機能の詳細については、不正プログラム対策エンジンには基本機能のみがありますをご覧ください。

利用可能なモード

以下のモードを使用できます

- カーネルモードはイベントを生成し、完全な不正プログラム対策機能を提供しますが、必要なドライバーサポートがあるシステムでのみ有効にできます。
- ユーザーモードはイベントを生成し、不正プログラム対策の基本機能をドライバなしで有効にします。このモードは、システムがカーネルモードで動作するために必要なドライバをサポートしている場合でも、ドライバを使用せずにシステムで実行するために有効にすることができます。
- オートモードは、カーネルモードとユーザーモードを切り替えて、任意の時点で利用可能な最良の保護を提供します。カーネルモードが優先されますが、カーネルモードの動作を妨げるドライバーサポートのギャップがある場合、Deep Security Agentは自動的にユーザーモードに切り替わります。後にカーネルモードで動作するために必要なドライバーを取得したシステム (例えば、システム更新から) は、エージェントが自動的にカーネルモードを使用するように切り替え、不正プログラム対策からシステムを完全に保護します。

システム保護のためのドライバーの使用

システム保護にドライバーを使用する場合、ドライバーモードを次のように設定できます:

1. コンピューター(またはポリシー) > システム > 一般 > システム保護のためにドライバーを使用するかどうかを選択
2. メニューから自動、カーネルモード、またはユーザモードを選択してください。
3. [保存] をクリックします。

サポートされているエージェント

オペレーティングシステム	ユーザーモードでの機能サポート
	不正プログラム対策
AlmaLinux 9 (64-bit)	✓
Amazon Linux (64ビット)	
Amazon Linux 2 (64ビット)	✓
Amazon Linux 2 (AWS ArmベースGraviton 2)	
Amazon Linux 2 (AWS ArmベースGraviton 3)	
Amazon Linux 2023 (64ビット)	✓
Debian 8 (64ビット)	
Debian 9 (64ビット)	
Debian 10 (64-bit)	✓
Debian 11 (64-bit)	✓
Debian 12 (64ビット)	✓
Oracle Linux 6 (32ビット)	
Oracle Linux 6 (64ビット)	
Oracle Linux 7 (64ビット)	

オペレーティングシステム	ユーザーモードでの機能サポート
	不正プログラム対策
Oracle Linux 8 (64ビット)	✓
Oracle Linux 9 (64ビット)	✓
Red Hat Enterprise Linux 6 (32ビット)	
Red Hat Enterprise Linux 6 (64ビット)	
Red Hat Enterprise Linux 7 (64ビット)	
Red Hat Enterprise Linux 8 (64ビット)	
Red Hat Enterprise Linux 8(AWS ARMベースのGraviton 2)	
Red Hat Enterprise Linux 8.6 (PowerPC little-endian)	
Red Hat Enterprise Linux 9 (64ビット)	✓
Red Hat Enterprise Linux Workstation 7 (64-bit)	
SUSE Linux Enterprise Server 12 (64ビット)	
SUSE Linux Enterprise Server 12 (PowerPCリトルエンディアン)	
SUSE Linux Enterprise Server 15 (64ビット)	✓
SUSE Linux Enterprise Server 15 (PowerPCリトルエンディアン)	
Ubuntu 16.04 (64ビット)	
Ubuntu 18.04 (64ビット)	
Ubuntu 18.04 (AWS ARMベースのGraviton 2)	
Ubuntu 20.04 (64ビット)	✓
Ubuntu 20.04 (AWS ARMベースのGraviton 2)	
Ubuntu 22.04 (64ビット)	✓

オペレーティングシステム	ユーザーモードでの機能サポート
	不正プログラム対策
Ubuntu 22.04 (AWS ARMベースのGraviton 2)	

ポリシーのルール、リスト、およびその他の共通オブジェクトの定義

共通オブジェクトについて

Common Objectsページ(Deep Security Managerの[Policies]→[Common Objects]の下) には、さまざまなポリシーやルールを再利用できるようにオブジェクトを一度定義する方法が用意されています。作成した共通オブジェクトをポリシーエディタまたはコンピュータエディタで使用する際には、オブジェクトの設定をそのポリシーまたはコンピュータ向けにオーバーライドできます。ポリシーまたはコンピュータレベルで共通オブジェクトのプロパティを継承またはオーバーライドする方法については、"ポリシー、継承、およびオーバーライド" on page 724を参照してください。

ルール

一部の保護モジュールはルールを利用します。

- "ファイアウォールルールの作成" on page 967
- ポリシーで使用する侵入防御ルールの設定
- "変更監視 ルールの作成" on page 1012
- "ポリシーで使用するセキュリティログ監視 ルールを定義する" on page 1070

リスト

- "ポリシーで使用するディレクトリリストの作成" on page 804
- "ポリシーで使用するファイル拡張子リストの作成" on page 807
- "ポリシーで使用するファイルリストの作成" on page 808
- "ポリシーで使用するIPアドレスリストの作成" on page 811
- "ポリシーで使用するMACアドレスリストの作成" on page 813
- "ポリシーで使用するポートリストの作成" on page 812

その他

- "ポリシーで使用するコンテキストの定義" on page 814
- "ステートフルファイアウォールの設定の定義" on page 993
- "不正プログラム検索と除外の設定" on page 832
- "ルールに適用するスケジュールの定義" on page 820

ファイアウォールルールの作成

ファイアウォールルールは、個々のパケットの制御情報を確認し、定義された条件に従ってブロックまたは許可します。ファイアウォールルールは、ポリシー、または直接コンピュータに割り当てることができます。

注意: ここでは、ファイアウォールルールの作成方法を具体的に説明します。ファイアウォールモジュールの設定方法については、"Deep Securityファイアウォールの設定" on page 954を参照してください。

新しいファイアウォールルールを作成するには、次の手順を実行する必要があります。

1. "新しいルールを追加する" below。
2. "ルールの動作とプロトコルを選択する" on the next page。
3. "パケットの送信元と送信先を選択する" on page 765。

ファイアウォールルールを作成したら、次の方法も学習できます。

- "ルールイベントとアラートを設定する" on page 766
- "ルールのスケジュールを設定する" on page 767
- "ルールが割り当てられているポリシーとコンピュータを確認する" on page 767
- "ルールにコンテキストを割り当てる" on page 767

新しいルールを追加する

[ポリシー]→[共通オブジェクト]→[ルール]→[ファイアウォールルール] ページで新しいファイアウォールルールを追加する方法は3つあります。次の手順を実行します。

- 新しいルールを作成します。[新規]→[新規ファイアウォールルール] の順にクリックします。
- XMLファイルからルールをインポートします。[新規]→[ファイルからインポート] をクリックします。

- 既存のルールをコピーして変更します。[ファイアウォールルール] リストで、該当のルールを右クリックし、[複製] をクリックします。新しいルールを編集するには、そのルールを選択し、[プロパティ] をクリックします。

ルールの動作とプロトコルを選択する

1. ルールの [名前] と[説明] を入力します。

   ヒント: ファイアウォールルールへの変更をそのルールの [説明] フィールドに記録することを推奨します。ファイアウォールのメンテナンスを簡単にするため、ルールを作成または削除した日付とその理由を記録してください。

2. ルールがパケットに対して実行する[処理] を選択します。次の5つの処理のいずれかを選択できます。

   注意: 1つのパケットに適用されるのは、1つのルール処理だけです。同じ優先度のルールが複数ある場合は、下記の優先順序で適用されます。

   - トラフィックにファイアウォールのバイパスを許可できます。バイパスルールにより、トラフィックはファイアウォールと侵入防御エンジンを可能な限り早く通過できます。バイパスルールは、フィルタリングを望まないマルチメディア系プロトコルを使用するトラフィックや、信頼済みソースからのトラフィックに対して使用します。

     ヒント: ポリシーで信頼済みソース用のバイパスルールを作成して使用する方法の例については、"信頼済みトラフィックに対するファイアウォールのバイパス許可" on page 973を参照してください。

     注意: バイパスルールは単一方向です。トラフィックの各方向に対して明確なルールが必要です。

     ヒント: 次の設定を使用して、バイパスルールで最大のスループットパフォーマンスを達成できます。
     - 優先度: 最高
     - フレームの種類: IP
     - プロトコル: TCP、UDP、またはその他のIPプロトコル(「任意」オプションは使用しないでください)
     - 送信元および送信先のIPおよびMAC: すべて「任意」

- プロトコルがTCPまたはUDPでトラフィックの方向が「受信」の場合は、送信先ポートを「任意」ではなく1つ以上指定する必要があり、送信元ポートを「任意」にする必要があります。
- プロトコルがTCPまたはUDPでトラフィックの方向が「送信」の場合は、送信元ポートを「任意」ではなく1つ以上指定する必要があり、送信先ポートを「任意」にする必要があります。
- スケジュール: なし

- ログ記録のみが可能です。この処理では、ログにエントリは作成されますが、トラフィックは処理されません。
- 定義済みのトラフィックを強制的に許可できます (他のトラフィックを除外することなく、このルールによって定義されたトラフィックを許可できます)。
- トラフィックの拒否が可能です (このルールによって定義されたトラフィックを拒否します)。
- トラフィックの許可が可能です (このフィルタによって定義されたトラフィックを例外的に許可します)。

注意: コンピュータに有効な許可ルールがない場合、拒否ルールでブロックされていないかぎり、すべてのトラフィックが許可されます。許可ルールを1つ作成したら、許可ルールの条件を満たしていないかぎり、その他すべてのトラフィックがブロックされます。ただし、1つだけ例外があります。ICMPv6トラフィックは、拒否ルールで明確にブロックされていない限り、常に許可されます。

3. ルールの [優先度] を選択します。優先度により、ルールが適用される順序を決定します。ルール処理に「強制的に許可」、「拒否」、または「バイパス」を選択した場合は、0 (最低) から4 (最高) の優先度を設定できます。優先度を設定すると、ルール処理を組み合わせて、階層型のルール効果を実現できます。

   注意: ログのみルールでの優先度は4のみ設定でき、許可ルールでは0のみが設定できます。

   注意: 優先度の低いルールよりも優先度の高いルールが優先的に適用されます。たとえば、ポート80の受信を強制的に許可する優先度2のルールが適用されるより前に、ポート80の受信を拒否する優先度3のルールが適用され、パケットを破棄します。

   処理と優先度の関係の詳細については、"ファイアウォールルールの処理と優先度" on page 975を参照してください。

4. [パケットの方向] を選択します。このルールを受信 (ネットワークからコンピュータ) または送信 (コンピュータからネットワーク) トラフィックのどちらに適用するかを選択します。

   注意: 個々のファイアウォールルールは、単一のトラフィック方向にのみ適用されます。特定の種類のトラフィックに対しては、受信および送信ファイアウォールルールをペアで作成する必要があります。

5. イーサネットの [フレームの種類] を選択します。「フレーム」とはイーサネットフレームを指し、フレームで送信されるデータは、使用可能なプロトコルによって指定されます。フレームの種類として「その他」を選択する場合は、フレーム番号を指定する必要があります。

6. 注意: [IP] は、IPv4とIPv6両方をサポートしています。[IPv4] または [IPv6] を個別に選択することもできます。

   注意: Solarisでは、Deep Security AgentはIPフレームタイプのパケットのみを検査し、Linuxエージェントは IPタイプまたはARPフレームタイプのパケットのみを調べます。その他のフレームの種類のパケットは許可されます。Virtual Applianceにはこのような制限事項はありません。保護する仮想マシンのOSに関係なく、すべてのフレームの種類を確認できます。

   フレームの種類としてインターネットプロトコル (IP) を選択した場合は、トランスポートの [プロトコル] を選択する必要があります。プロトコルとして「その他」を選択する場合は、プロトコル番号も指定する必要があります。

パケットの送信元と送信先を選択する

[IP] アドレスと[MAC] アドレスの組み合わせを選択し、フレームの種類で使用できる場合は、パケット送信元およびパケット送信先の [ポート] および [指定フラグ] を選択します。

ヒント: 以前に作成したIP、MAC、またはポートリストを使用できます。

サポートされているIPベースのフレームの種類は次のとおりです。

	IP	MAC	ポート	フラグ
任意	✓	✓		
ICMP	✓	✓		✓
ICMPV6	✓	✓		✓

	IP	MAC	ポート	フラグ
IGMP	✓	✓		
GGP	✓	✓		
TCP	✓	✓	✓	✓
PUP	✓	✓		
UDP	✓	✓	✓	
IDP	✓	✓		
ND	✓	✓		
RAW	✓	✓		
TCP+UDP	✓	✓	✓	✓

注意: ARPおよびREVARPのフレームの種類では、パケットの送信元と送信先としてMACアドレスの使用のみがサポートされています。

[任意のフラグ] を選択することも、以下のフラグを個別に選択することもできます。

- URG
- ACK
- PSH
- RST
- SYN
- FIN

ルールイベントとアラートを設定する

ファイアウォールルールがトリガされると、Deep Security Managerにイベントが記録され、パケットデータが記録されます。

注意: 「許可」、「強制的に許可」、および「バイパス」処理を使用するルールは、イベントのログを記録しません。

アラート

イベントのログを記録した場合に、アラートもトリガするようにルールを設定できます。アラートを設定するには、ルールのプロパティを開き、[オプション] をクリックしてから、[このルールによってイベントが記録された場合にアラート] を選択します。

注意: アラートをトリガするように設定できるのは、処理が [拒否] または [ログ記録のみ] に設定されているファイアウォールルールのみです

ルールのスケジュールを設定する

予約された時間のみファイアウォールルールを有効化するかどうかを選択します。

その方法の詳細については、"ルールに適用するスケジュールの定義" on page 820を参照してください。

ルールにコンテキストを割り当てる

ルールコンテキストを使用すると、さまざまなネットワーク環境に独自のファイアウォールルールを設定できます。コンテキストは一般的に、オンサイトとオフサイトのノートパソコンで異なるルールを有効にするために使用されます。

コンテキストの作成方法については、"ポリシーで使用するコンテキストの定義" on page 814を参照してください。

ヒント: コンテキストを使用してファイアウォールルールを実装するポリシーの例については、「Windows Mobile ラップトップ」ポリシーのプロパティを参照してください。

ルールが割り当てられているポリシーとコンピュータを確認する

ファイアウォールルールに割り当てられているポリシーとコンピュータは、[割り当て対象] タブで確認できます。リスト内のポリシーまたはコンピュータをクリックすると、そのプロパティが表示されます。

ルールをエクスポートする

すべてのファイアウォールルールを、.csv または .xml ファイルにエクスポートするには、[エクスポート] をクリックし、リストから対応するエクスポート処理を選択します。特定のルールを選択し、[エクスポート] をクリックして、リストから該当するエクスポート処理を選択すると、特定のルールをエクスポートすることもできます。

ルールを削除する

ルールを削除するには、[ファイアウォールルール] リストで該当のルールを右クリックしてから、[削除]→[OK] の順にクリックします。

注意: 1台以上のコンピュータに割り当てられたファイアウォールルール、またはポリシーの一部であるファイアウォールルールは削除できません。

侵入防御ルールの設定

次のタスクを実行して、侵入防御ルールを設定および使用します。

- "侵入防御ルールのリストを表示する" below
- "侵入防御ルールに関する情報を表示する" on the next page
- "関連付けられている脆弱性に関する情報を表示する(トレンドマイクロのルールのみ)" on page 770
- "ルールを割り当てる/ルールの割り当てを解除する" on page 771
- "アップデートされた必須ルールを自動割り当てする" on page 771
- "ルールにイベントログを設定する" on page 772
- "アラートを生成する" on page 773
- "設定オプションを設定する(トレンドマイクロのルールのみ)" on page 773
- "有効な時間を予約する" on page 774
- "推奨設定から除外する" on page 774
- "ルールのコンテキストを設定する" on page 774
- "ルールの動作モードをオーバーライドする" on page 775
- "ルールおよびアプリケーションの種類の設定をオーバーライドする" on page 775
- "ルールをエクスポート/インポートする" on page 776
- "SQLインジェクション防御ルールの設定" on page 923

侵入防御モジュールの概要については、"侵入防御" on page 904を参照してください。

侵入防御ルールのリストを表示する

[ポリシー] 画面には侵入防御ルールのリストが表示されます。侵入防御ルールを検索し、ルールのプロパティを開いて編集できます。このリストでは、ルールはアプリケーションの種類で分類されており、ルールのプロパティは列にそれぞれ表示されます。

ヒント: [TippingPoint] 列には、対応するTrend Micro TippingPointルールIDが含まれます。侵入防御ルールの [詳細検索] では、TippingPointルールIDを検索できます。ポリシーおよびコンピュータエディタの割り当てられた侵入防御ルールのリストでもTippingPointルールIDを表示できます。

リストを確認するには、[ポリシー] をクリックして、[共通オブジェクト/ルール] の下の [侵入防御ルール] をクリックします。

侵入防御ルールに関する情報を表示する

侵入防御ルールのプロパティには、ルールおよび防御対象の攻撃コードに関する情報が含まれます。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。

一般情報

- 名前:侵入防御ルールの名前。
- 説明:侵入防御ルールの説明。
- 最小エージェント/アプライアンスバージョン: この侵入防御ルールをサポートするために必要なDeep Security Agentまたはアプライアンス[1] の最小バージョンです。

詳細

[新規] ( ) または [プロパティ] ( ) をクリックして、[侵入防御ルールプロパティ] 画面を表示します。

注意: [設定] タブを確認します。トレンドマイクロの侵入防御ルールは、Deep Security Managerで直接編集できません。その代わり、侵入防御ルールに設定が必要な場合や設定が可能な場合は、[設定] タブの設定オプションを使用します。ユーザ自身で作成したカスタム侵入防御ルールは、[ルール] タブが表示され、直接編集可能です。

侵入防御ルールのリストを表示する

[ポリシー] 画面には侵入防御ルールのリストが表示されます。侵入防御ルールを検索し、ルールのプロパティを開いて編集できます。このリストでは、ルールはアプリケーションの種類で分類されており、ルールのプロパティは列にそれぞれ表示されます。

---

[1]Deep Security AgentとDeep Security Virtual Applianceは、ユーザが定義したDeep Securityポリシーを適用するためのコンポーネントです。Agentはコンピュータに直接インストールされ、ApplianceはAgentレスの保護を提供するためにVMware vSphere環境で使用されます。どちらもDeep Security as a Serviceでは使用できません。

ヒント: [TippingPoint] 列には、対応するTrend Micro TippingPointルールIDが含まれます。侵入防御ルールの [詳細検索] では、TippingPointルールIDを検索できます。ポリシーおよびコンピュータエディタの割り当てられた侵入防御ルールのリストでもTippingPointルールIDを表示できます。

リストを確認するには、[ポリシー] をクリックして、[共通オブジェクト/ルール] の下の [侵入防御ルール] をクリックします。

一般情報

- アプリケーションの種類: この侵入防御ルールが分類されているアプリケーションの種類。

  ヒント: このパネルでアプリケーションの種類を編集できます。ここでアプリケーションの種類を編集すると、そのアプリケーションの種類を使用するすべてのセキュリティコンポーネントに対して変更内容が適用されます。

- 優先度: ルールの優先度。優先度の低いルールよりも優先度の高いルールが優先的に適用されます。
- 重要度:ルールの重要度の設定は、ルールの実装および適用方法に影響しません。重要度レベルは、侵入防御ルールのリストを表示するときにソート条件として使用できます。それぞれの重要度レベルは重要度の値と関連付けられます。この値にコンピュータの資産評価を掛けたものが、イベントのランク付けを決定します([管理]→[システム設定]→[ランク付け] を参照してください)。
- CVSSスコア:脆弱性情報データベースに基づいた、脆弱性の重要度の基準。

ID (トレンドマイクロのルールのみ)

- 種類:[スマート] (1つ以上の既知または不明なゼロデイの脆弱性)、[攻撃コード] (通常、署名ベースの攻撃コード) または [脆弱性] (1つ以上の攻撃コードが存在する可能性のある特定の脆弱性) のいずれかになります。
- 発行日: ルールがリリースされた日付。ダウンロードされた日付ではありません。
- 前回のアップデート: ローカルで、またはセキュリティアップデートのダウンロード中に、ルールが変更された前回の日時。
- 識別子: ルールに一意のIDタグ。

関連付けられている脆弱性に関する情報を表示する (トレンドマイクロのルールのみ)

トレンドマイクロが提供するルールには、ルールが守る脆弱性に関する情報を含めることができます。適用可能な場合は、共通脆弱性評価システム (CVSS) が表示されます(この評価システムの詳細

は、脆弱性情報データベースのCVSSページを参照してください)。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して[プロパティ] をクリックします。
3. [脆弱性] タブをクリックします。

ルールを割り当てる/ルールの割り当てを解除する

Agent検索時に侵入防御ルールを適用するには、該当するポリシーとコンピュータに割り当てます。脆弱性にパッチが適用されたため、ルールが必要でなくなった場合は、ルールを割り当て解除できます。

コンピュータエディタ[1]で侵入防御ルールの割り当てを解除できない場合、そのルールがポリシーに割り当てられている可能性があります。ポリシーレベルで割り当てられたルールを削除するには**ポリシーエディタ**[2]を使用する必要があり、コンピュータレベルでは削除できません。

ポリシーに対する変更は、そのポリシーを使用するすべてのコンピュータに反映されます。たとえば、ポリシーからルールを割り当て解除すると、そのポリシーで保護しているすべてのコンピュータからルールが削除されます。継続してこのルールを他のコンピュータに適用するには、そのグループのコンピュータ用に新しいポリシーを作成します。("ポリシー、継承、およびオーバーライド" on page 724を参照してください)。

ヒント: ルールが割り当てられたポリシーとコンピュータを確認するには、ルールプロパティの [割り当て対象] タブをご覧ください。

1. [ポリシー] 画面に移動し、設定するポリシーを右クリックして[詳細] をクリックします。
2. [侵入防御]→[一般] の順にクリックします。
   ポリシーに割り当てられているルールのリストは、[現在割り当てられている侵入防御ルール] リストに表示されます。
3. [現在割り当てられている侵入防御ルール] で、[割り当て/割り当て解除] をクリックします。
4. ルールを割り当てるには、ルールの横にあるチェックボックスをオンにします。
5. ルールの割り当てを解除するには、ルールの横にあるチェックボックスをオフにします。
6. [OK] をクリックします。

アップデートされた必須ルールを自動割り当てする

セキュリティアップデートには、セカンダリ侵入防御ルールの割り当てが必要な新規またはアップデートされたアプリケーションの種類および侵入防御ルールが含まれている場合があります。Deep Security

---

[1] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。

[2] ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。

は、必要に応じてこれらのルールを自動的に割り当てることができます。ポリシーまたはコンピュータプロパティで、次のように自動割り当てを有効化できます。

1. [ポリシー] 画面に移動し、設定するポリシーを右クリックして [詳細] をクリックします。
2. [侵入防御]→[詳細] を順にクリックします。
3. 自動割り当てを有効にするには、[ルールアップデート] 領域で [はい] を選択します。
4. [OK] をクリックします。

ルールにイベントログを設定する

ルールのイベントをログに記録するかどうか、ログにパケットデータを含めるかどうかを設定します。

注意: Deep Securityは、X-Forwarded-Forヘッダがパケットデータで利用可能な場合に侵入防御イベントに表示できます。この情報は、Deep Security Agentがロードバランサまたはプロキシの背後にある場合に役立ちます。X-Forwarded-Forヘッダデータは、イベントの [プロパティ] 画面に表示されます。ヘッダデータを含めるには、ログにパケットデータを追加します。また、ルール1006540 [X-Forwarded-For HTTPヘッダのログを有効にする] も割り当てる必要があります。

それは、すべてのパケットデータルールはイベントをトリガするたびに記録することは非現実的ですので、のDeep Securityは、データにイベントは、指定された期間内で発生初回のみを記録します。初期設定時間は5分ですが、ポリシーの [ネットワークエンジンの詳細設定] の [1つのパケットデータのみをログに記録する期間] プロパティを使用して期間を変更できます。(「ネットワークエンジンの詳細オプション」を参照してください)。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" on page 775を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [一般] タブで、[イベント] 領域に移動し、次のように必要なオプションを選択します。
   - ルールのログを無効化するには、[イベントログの無効化] を選択します。
   - パケットが破棄またはブロックされた場合にイベントのログを記録するには、[パケット破棄時にイベントを生成] を選択します。
   - ログエントリにパケットデータを含めるには、[常にパケットデータを含める] を選択します。
   - ルールで検出されたパケットの前後のパケットをログに記録するには、[デバッグモードを有効にする] を選択します。サポート担当者から指示があった場合のみデバッグモードを使用します。

また、ログにパケットデータを含めるには、ルールを割り当てるポリシーで次のように、ルールによるパケットデータの取得を許可する必要があります。

1. [ポリシー] 画面で、ルールを割り当てたポリシーを開きます。
2. [侵入防御]→[詳細] を順にクリックします。
3. [イベントデータ] 領域で [はい] を選択します。

アラートを生成する

侵入防御ルールがイベントをトリガした場合にアラートを生成します。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" on page 775を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [オプション] タブをクリックして [アラート] 領域で [オン] を選択します。
4. [OK] をクリックします。

設定オプションを設定する(トレンドマイクロのルールのみ)

トレンドマイクロが提供する侵入防御ルールの中には、ヘッダ長、HTTPの許可される拡張子、Cookieの長さなど、1つ以上の設定オプションがあります。オプションには設定が必要なものもあります。必要なオプションを設定せずにルールを割り当てると、アラートが生成され、必要なオプションについての情報が表示されます。(これは、セキュリティアップデートによってダウンロードされ自動的に適用されたルールにも適用されます)。

設定オプションのある侵入防御ルールは、[侵入防御ルール] リストでルールのアイコンに小さなギアマークが付きます  。

> 注意: 独自のカスタム侵入防御ルールには、[ルール] タブがあり、ルールを編集できます。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" on page 775を参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [設定] タブをクリックします。
4. プロパティを設定して [OK] をクリックします。

有効な時間を予約する

侵入防御ルールが有効な時間を予約します。予約された時間のみ有効になる侵入防御ルールは、[侵入防御ルール] 画面でルールのアイコンに小さな時計マークが付きます。

注意: Agentベースの保護では、スケジュールで保護対象のエンドポイントと同じタイムゾーンが使用されます。Agentレスによる保護では、Deep Security Virtual Applianceと同じタイムゾーンが使用されます。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" on the next pageを参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [オプション] タブをクリックします。
4. [スケジュール] 領域で [新規] を選択するか、頻度を選択します。
5. 必要に応じてスケジュールを編集します。
6. [OK] をクリックします。

推奨設定から除外する

推奨設定検索のルール推奨設定から侵入防御ルールを除外します。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" on the next pageを参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [オプション] タブをクリックします。
4. [推奨設定オプション] 領域で [推奨設定から除外] を選択します。
5. [OK] をクリックします。

ルールのコンテキストを設定する

ルールが適用されるコンテキストを設定します。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" on the next pageを参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [オプション] タブをクリックします。
4. [コンテキスト] 領域で [新規] を選択するか、コンテキストを選択します。
5. 必要に応じてコンテキストを編集します。
6. [OK] をクリックします。

ルールの動作モードをオーバーライドする

新しいルールをテストする場合は、侵入防御ルールの動作モードを [検出] に設定します。[検出] モードでは、ルールは「検出のみ:」という言葉で始まるログエントリを作成しますが、トラフィックに干渉しません。侵入防御ルールには [検出] モードでのみ動作するものがあります。これらのルールについては、動作モードを変更できません。

> 注意: ルールのログを無効にすると、動作モードに関係なく、ルールのアクティビティはログに記録されません。

動作モードの詳細については、"動作モードを使用してルールをテストする" on page 905を参照してください。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" belowを参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [検出のみ] を選択します。

ルールおよびアプリケーションの種類の設定をオーバーライドする

コンピュータエディタとポリシーエディタ[1]で、侵入防御ルールを編集して、ポリシーまたはコンピュータのコンテキストのみで変更を適用できます。グローバルに変更が適用されるようにルールを編集して、ルールが割り当てられた他のポリシーおよびコンピュータで変更を有効にすることもできます。同様に、1つのポリシー/コンピュータ、またはグローバルにアプリケーションの種類を設定できます。

1. [ポリシー] 画面に移動し、設定するポリシーを右クリックして [詳細] をクリックします。
2. [侵入防御] をクリックします。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

3. ルールを編集するには、ルールを右クリックして、次のコマンドのいずれかを選択します。
   - プロパティ: そのポリシーのみのルールを編集します。
   - プロパティ(グローバル): グローバルに (すべてのポリシーとコンピュータに対して) ルールを編集します。
4. ルールのアプリケーションの種類を編集するには、ルールを右クリックして、次のコマンドのいずれかを選択します。
   - アプリケーションの種類プロパティ: そのポリシーのみのアプリケーションの種類を編集します。
   - アプリケーションの種類プロパティ(グローバル): グローバルに (すべてのポリシーとコンピュータに対して) アプリケーションの種類を編集します。
5. [OK] をクリックします。

ヒント: ルールを選択して [プロパティ] をクリックした場合は、編集中のポリシーのみでルールを編集します。

注意: 1つのポートを割り当てできるアプリケーションの種類は8個までです。9個以上割り当てると、そのルールは該当するポートで機能しません。

ルールをエクスポート/インポートする

1つ以上の侵入防御ルールをXMLまたはCSVファイルにエクスポートしたり、XMLファイルからルールをインポートできます。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. 1つ以上のルールをエクスポートするには、[エクスポート]→[選択したアイテムをCSV形式でエクスポート] または [エクスポート]→[選択したアイテムをXML形式でエクスポート] を順にクリックします。
3. すべてのルールをエクスポートするには、[エクスポート]→[CSV形式でエクスポート] または [エクスポート]→[XML形式でエクスポート] を順にクリックします。
4. ルールをインポートするには、[新規]→[ファイルからインポート] を順にクリックして、ウィザードの指示に従います。

変更監視 ルールの作成

変更監視 ルールは、Deep Security Agentがコンピュータのファイル、ディレクトリ、レジストリキーと値の変更、およびインストールされているソフトウェア、プロセス、待機ポート、および実行中のサービスの変更を検索および検出する方法を示します。変更監視ルールは、コンピュータに直接割り当てることも、ポリシーの一部にすることもできます。

注意: ここでは、変更監視ルールの作成方法を具体的に説明します。変更監視モジュールの設定方法については、"変更監視の設定" on page 1004を参照してください。

変更監視ルールには、ユーザ自身が作成したルールとトレンドマイクロが発行するルールの2種類があります。トレンドマイクロが発行するルールの設定方法については、"トレンドマイクロが発行する変更監視ルールを設定する" on page 779セクションを参照してください。

新しい変更監視ルールを作成するには、次の手順を実行する必要があります。

1. "新しいルールを追加する" below。
2. "変更監視ルール情報を入力する" below。
3. "ルールテンプレートを選択し、ルールの属性を定義する" on the next page。

変更監視ルールを作成したら、次の方法も学習できます。

- "ルールイベントとアラートを設定する" on page 780
- "ルールが割り当てられているポリシーとコンピュータを確認する" on page 780
- "ルールをエクスポートする" on page 780
- "ルールを削除する" on page 780

新しいルールを追加する

[ポリシー]→[共通オブジェクト]→[ルール]→[変更監視ルール] ページで、新しい変更監視ルールを追加する方法は3つあります。次の手順を実行します。

- 新しいルールを作成します。[新規]→[新しい変更監視ルール] の順にクリックします。
- XMLファイルからルールをインポートします。[新規]→[ファイルからインポート] をクリックします。
- 既存のルールをコピーして変更します。[変更監視ルール] リストで、該当のルールを右クリックし、[複製] をクリックします。新しいルールを編集するには、そのルールを選択し、[プロパティ] をクリックします。

変更監視ルール情報を入力する

1. ルールの [名前] と[説明] を入力します。

   ヒント: すべての変更監視ルールへの変更をルールの [説明] フィールドに記録することを推奨します。メンテナンスを簡単にするため、ルールを作成または削除した日付とその理由を記録してください。

2. ルールの [重要度] を設定します。

> 注意: ルールの重要度の設定は、ルールの実装および適用方法に影響しません。重要度レベルは、変更監視ルールのリストを表示するときに条件をソートする際に役立ちます。それぞれの重要度レベルは重要度の値と関連付けられます。この値にコンピュータの資産評価を掛けたものが、イベントのランク付けを決定します([管理]→[システム設定]→[ランク付け] を参照してください)。

ルールテンプレートを選択し、ルールの属性を定義する

[コンテンツ] タブに移動し、次の3つのテンプレートのいずれかを選択します。

レジストリ値テンプレート

特にレジストリ値への変更を監視する変更監視ルールを作成します。

> 注意: レジストリ値テンプレートは、Windowsベースコンピュータでのみ使用できます。

1. 監視する[基本キー]、およびサブキーのコンテンツを監視するかどうかを選択します。
2. 含まれる、または除外される[値の名前] が一覧表示されます。ワイルドカード文字として「?」および「*」を使用できます。
3. 監視する[属性] を入力します。「STANDARD」と入力すると、レジストリサイズ、コンテンツ、種類への変更が監視されます。レジストリ値テンプレートの属性の詳細については、"RegistryValueSet" on page 1049ドキュメントを参照してください。

ファイルテンプレート

特にファイルへの変更を監視する変更監視ルールを作成します。

1. ルールの [基本ディレクトリ] を入力します (例: `C:\Program Files\MySQL`)。基本ディレクトリに関連するすべてのサブディレクトリのコンテンツも含めるには、[サブディレクトリも含む] を選択します。ベースディレクトリではワイルドカードはサポートされていません。

2. 特定のファイルを含める、または除外するには、[ファイル名] フィールドを使用します。ワイルドカード(「`?`」を任意の1文字として、「`*`」を0個以上の文字として) 使用できます。

   > 注意: [ファイル名] フィールドを空白のままにすると、基本ディレクトリ内のすべてのファイルが監視されます。この場合、基本ディレクトリに多数のファイルが含まれていると、大量のシステムリソースが消費されます。

3. 監視する[属性] を入力します。「STANDARD」と入力すると、ファイル作成日、最終更新日、権限、所有者、サイズ、コンテンツ、フラグ (Windows)、SymLinkPath (Linux) が監視されます。

ファイルテンプレートの属性の詳細については、"FileSet" on page 1032ドキュメントを参照してください。

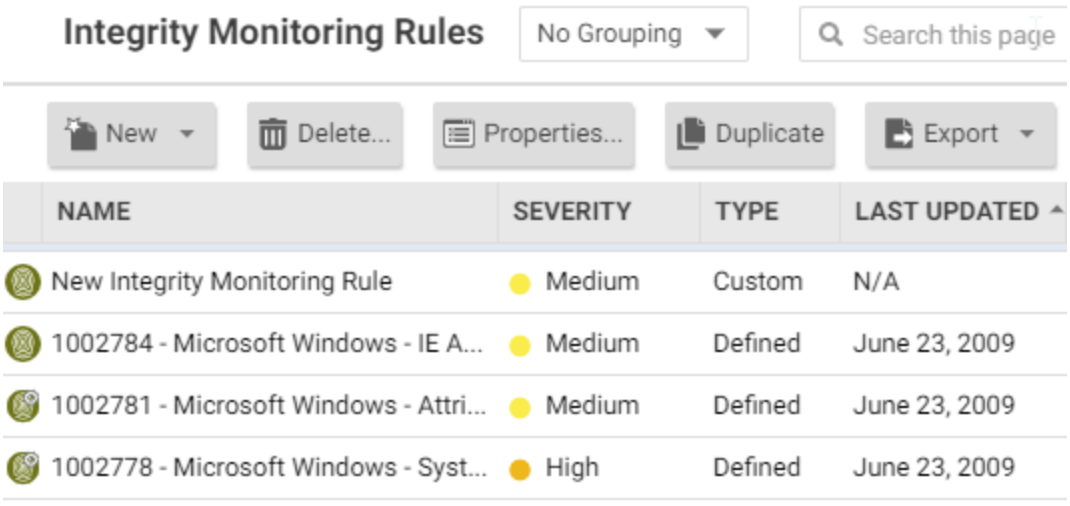
カスタム (XML) テンプレート

カスタム変更監視, レジストリ値, レジストリキー, サービス, プロセス, インストールされたソフトウェア, ポート、グループ, ユーザ, ファイル、およびDeep Security XMLベースの "変更監視 rules languages" on page 1017。

ヒント: 希望するテキストエディタを使用してルールを作成し、完成したルールを[コンテンツ] フィールドに貼り付けることができます。

トレンドマイクロが発行する変更監視ルールを設定する

トレンドマイクロが発行する変更監視ルールは、作成したカスタムルールと同じ方法では編集できません。トレンドマイクロのルールには、まったく変更できないものと、限定的な設定オプションが提供されているものがあります。いずれのルールも「種類」列に「定義済み」として表示されますが、設定可能なルールは変更監視アイコンに歯車 ( ) が表示されます。



ルールの設定オプションにアクセスするには、ルールのプロパティを開き、[設定] タブをクリックします。

トレンドマイクロが発行するルールには、[一般] タブの下に補足情報も表示されます。

- ルールがはじめて発行された日付と、最後に更新された日付、およびルールの一意のID。
- ルールの機能に必要なAgentおよびDeep Security Managerの最小バージョン。

トレンドマイクロが発行するルールは編集できませんが、複製した後にそのコピーを編集することはできます。

ルールイベントとアラートを設定する

変更監視 ルールによって検出された変更は、Deep Security Managerにイベントとして記録されます。

リアルタイムのイベント監視

初期設定では、イベントは発生時にログに記録されます。変更の検索を手動で実行している場合にのみイベントをログに記録するには、[リアルタイム監視を許可] の選択を解除します。

アラート

イベントのログを記録したときに、アラートもトリガするようにルールを設定できます。アラートを設定するには、ルールのプロパティを開き、[オプション] をクリックしてから、[このルールによってイベントが記録された場合にアラート] を選択します。

ルールが割り当てられているポリシーとコンピュータを確認する

変更監視ルールに割り当てられているポリシーとコンピュータは、[割り当て対象] タブで確認できます。リスト内のポリシーまたはコンピュータをクリックすると、そのプロパティが表示されます。

ルールをエクスポートする

すべての変更監視ルールを、.csvまたは.xmlファイルにエクスポートするには、[エクスポート] をクリックし、リストから対応するエクスポート処理を選択します。特定のルールを選択し、[エクスポート] をクリックして、リストから該当するエクスポート処理を選択すると、特定のルールをエクスポートすることもできます。

ルールを削除する

ルールを削除するには、[変更監視ルール] リストで該当のルールを右クリックしてから、[削除]→[OK] の順にクリックします。

注意: 1台以上のコンピュータに現在割り当てられている変更監視ルール、またはポリシーの一部である変更監視ルールは削除できません。

ポリシーで使用するセキュリティログ監視 ルールを定義する

OSSEC セキュリティログ監視 エンジンはDeep Security Agentに統合されており、Deep Securityは、コンピュータ上で実行されているオペレーティングシステムおよびアプリケーションによって生成されたログおよびイベントを検査できます。Deep Security Managerには、コンピュータまたはポリシーに割り当てることができるOSSEC セキュリティログ監視 ルールの標準セットが付属しています。要件に合う既存ルールが存在しない場合は、カスタムルールを作成することもできます。

トレンドマイクロが発行したセキュリティログ監視ルールを変更することはできませんが、それらを複製してから変更することはできます。

1台以上のコンピュータに割り当てられているか、ポリシーの一部であるセキュリティログ監視ルールは削除できません。

セキュリティログ監視 ルールを作成するには、次の基本手順を実行します。

- "新しい セキュリティログ監視 ルールを作成します。" below
- "デコーダ" on page 783
- "サブルール" on page 784
- "例" on page 791
- "セキュリティログ監視 ルールの重大度レベルと推奨される使用" on page 797
- "strftime () 変換指定子" on page 799
- "セキュリティログ監視 ルールを調べる" on page 799

セキュリティログ監視 モジュールの概要については、"セキュリティログ監視" on page 1065を参照してください。

新しい セキュリティログ監視 ルールを作成します。

1. Deep Security Managerで、[ポリシー]→[共通オブジェクト]→[ルール]→[セキュリティログ監視 ルール] に進みます。
2. [新規]→[新しいセキュリティログ監視ルール] をクリックします。
3. [一般] タブで、ルールの名前と説明を入力します (説明は省略できます)。
4. [コンテンツ] タブで、ルールを定義します。ルールを定義する一番簡単な方法は、[基本ルール] を選択し、表示されるオプションを使用してルールを定義する方法です。さらにカスタマイズが必要な場合は、[カスタム (XML)] を選択し、定義しているルールをXMLビューに切り替えることができます。

   カスタム (XML) ビューで行った変更は、基本ルールビューに戻すと失われます。

XMLベースの言語を使用して独自のセキュリティログ監視ルールを作成する場合は、OSSECのドキュメントを参照するか、サポートプロバイダにお問い合わせください。

基本ルールテンプレートでは以下のオプションを使用できます。

- ルールID: ルールIDはルールの一意の識別子です。OSSECは100000 - 109999をユーザ定義ルールのスペースとして定義しています。Deep Security Managerは新しい一意のルールIDでフィールドを事前に入力します。
- レベル: ルールにレベルを割り当てます。ゼロ(0)は、ルールによってイベントが記録されないことを示しますが、このルールを監視する他のルールが発生する可能性があります
- グループ: 1つ以上のカンマ区切りのグループにルールを割り当てます。これが便利なのは、ある1つのルールの発生時に発生する複数のルール、または特定のグループに属するルールを作成した後に依存関係が使用されるときです。
- ルールの説明: ルールの説明。

- パターンマッチング: これはルールがログ内で探すパターンです。ルールは一致時にトリガーされます。パターンマッチングは正規表現またはより単純な文字列パターンをサポートします。文字列パターンのパターンタイプは正規表現よりも高速ですが、3つの特殊操作のみをサポートします。
  - ^ (カレット): テキストの先頭を指定します。
  - $ (ドル記号): テキストの末尾を指定します。
  - | (パイプ): 複数のパターン間に「OR」を作成します。

  セキュリティログ監視モジュールで使用される正規表現の構文については、https://www.ossec.net/docs/syntax/regex.htmlを参照してください。

- 依存関係: 別のルールに依存関係を設定すると、この領域で指定されたルールがトリガーされた場合にのみ、イベントが記録されます。
- [頻度] は、ルールがトリガされるまでの特定の期間内にルールを照合する必要のある回数です。

- [期間] は、イベントを記録するためにルールを特定の回数 (上記の頻度) トリガするまでの期間 (秒数) です。

  コンテンツタブは、ユーザー自身が作成したセキュリティログ監視ルールにのみ表示されます。トレンドマイクロによって発行されたセキュリティログ監視ルールには、代わりに構成タブが表示され、セキュリティログ監視ルールの構成オプションが表示されます (存在する場合)。

5. ファイルタブで、ルールでモニタしたいファイルのフルパスを入力し、ファイルの種類を指定してください。

   グロブ文字はファイル名で使用される場合にサポートされています。グロブ文字はパスのディレクトリ部分で使用される場合も2回までサポートされています。例えば、/home/user1/testlog*.txt、/home/*/testlog1.txt、/home/*/testlog*.txt、/home/*/user*/testlog*.txtはすべて有効ですが、/home/*/demo*/user*/testlog1.txtは無効です。

6. [オプション] タブの [アラート] セクションで、このルールでアラートをトリガするかどうかを選択します。

   最小のアラート重要度 は、基本ルールまたはカスタム(XML) テンプレートを使用してルールに対してアラートをトリガする最小の重大度レベルを設定します。

   基本ルールテンプレートは、一度に1つのルールを作成します。1つのテンプレートに複数のルールを書き込むには、カスタム(XML) テンプレートを使用できます。カスタム(XML) テンプレート内でレベルが異なる複数のルールを作成する場合は、[最小のアラート重要度]設定を使用して、そのテンプレート内のすべてのルールに対するアラートをトリガする最小の重要度を選択できます。

7. [割り当て対象 に割り当てられました]タブには、この セキュリティログ監視 ルールを使用しているポリシーとコンピュータが表示されます。新しいルールは作成中であるため、まだ割り当てられていません。
8. [OK] をクリックします。このルールをポリシーとコンピュータに割り当てる準備ができました。

デコーダ

A セキュリティログ監視 ルールは、変更を監視するファイルのリストと、ルールがトリガする条件のセットで構成されます。セキュリティログ監視 エンジンが監視対象ログファイルの変更を検出すると、その変更はデコーダによって解析されます。デコーダは、rawログエントリを解析して次のフィールドを生成します。

- log: イベントのメッセージセクション
- full_log: イベント全体
- location: ログの生成元
- hostname: イベント発生元のホスト名
- program_name: イベントのSyslogヘッダで使用されるプログラム名
- srcip: イベント内の送信元のIPアドレス
- dstip: イベント内の送信先のIPアドレス
- srcport: イベント内の送信元のポート番号

- dstport: イベント内の送信先のポート番号
- protocol: イベント内のプロトコル
- action: イベント内で実行された処理
- srcuser: イベント内の送信元のユーザ
- dstuser: イベント内の送信先のユーザ
- id: イベントからのIDとしてデコードされたID
- status: イベント内のデコードされたステータス
- command: イベント内で呼び出されるコマンド
- url: イベント内のURL
- data: イベントから抽出される追加データ
- systemname: イベント内のシステム名

ルールは、このデコードされたデータを確認して、ルールで定義された条件に一致する情報を検索します。

一致する項目の重要度レベルが十分に高い場合は、次のいずれかの処理を実行できます。

- アラートを発生させることができます。セキュリティログ監視ルールのプロパティウィンドウのオプションタブで設定可能です。
- イベントは syslog に書き込むことができます。管理 > システム設定 > イベント転送 タブの SIEM エリアで設定可能です。
- イベントはDeep Security Managerに送信できます。ポリシーまたはコンピュータエディタ> 設定 > イベント転送 タブのセキュリティログ監視Syslog設定で設定可能です。

サブルール

1つの セキュリティログ監視 ルールに複数のサブルールを含めることができます。これらのサブルールには、アトミックとコンポジットという2つの種類があります。アトミックルールは1つのイベントを評価し、コンポジットルールは複数のイベントを確認して、頻度、繰り返し、およびイベント間の相関関係を評価できます。

グループ

各ルールまたはルールのグループは、<group></group>要素内で定義する必要があります。属性名には、このグループに含めたいルールを含める必要があります。次の例では、グループにsyslogとSSHDのルールが含まれていることを示しています。

```
<group name="syslog,sshd,"> </group>
```

グループ名の末尾のコンマに注意してください。<if_group></if_group>タグを使用してこのサブルールに別のサブルールを条件付きで追加する場合、末尾のコンマが必要です。

セキュリティログ監視ルールのセットがエージェントに送信されると、エージェント上のセキュリティログ監視エンジンは、各割り当てられたルールからXMLデータを取得し、それを1つの長いセキュリティログ監視ルールに組み立てます。トレンドマイクロによって作成されたすべてのセキュリティログ監視ルールには共通のグループ定義があります。このため、トレンドマイクロはこれらのグループを定義するDefault Rules Configurationというルールを含めており、他のトレンドマイクロのルールと一緒に常に割り当てられます。ルールを割り当てる際にDefault Rules Configurationルールを選択しない場合、そのルールが自動的に割り当てられることを通知するメッセージが表示されます。独自のセキュリティログ監視ルールを作成し、トレンドマイクロ作成のルールを割り当てずにコンピュータに割り当てる場合は、Default Rules Configurationルールの内容を新しいルールにコピーするか、またはDefault Rules Configurationルールをコンピュータに割り当てるために選択する必要があります。

ルール、ID、およびレベル

グループには必要なだけのルールを含めることができます。ルールは<rule></rule>要素を使用して定義され、少なくとも2つの属性、idとlevelを持たなければなりません。idはそのシグネチャの一意の識別子であり、levelはアラートの重大度です。次の例では、異なるルールIDとレベルを持つ2つのルールが作成されています。

```
<group name="syslog,sshd,"> <rule id="100120" level="5"> </rule> <rule id="100121" level="6"> </rule> </group>
```

カスタムルールには、100,000以上のID値を指定する必要があります。

親グループ内に<group></group>タグを使用して追加のサブグループを定義できます。このサブグループは、以下の表に記載されているグループのいずれかを参照することができます。

グループの種類	グループ名	説明
攻撃の予兆	connection_attempt web_scan recon	接続の試行 Web検索 一般的な検索
認証制御	authentication_success authentication_failed invalid_login login_denied authentication_failures adduser account_changed	成功 失敗 無効 ログイン拒否 複数の失敗 ユーザアカウントの追加 ユーザアカウントの変更または削除
攻撃/悪用	automatic_attack exploit_attempt invalid_access spam	ワーム (対象を指定しない攻撃) 攻撃コードのパターン 無効なアクセス スパム

グループの種類	グループ名	説明
	multiple_spam sql_injection attack virus	複数のスパムメッセージ SQLインジェクション 一般的な攻撃 ウイルスの検出
アクセス管理	access_denied access_allowed unknown_resource firewall_drop multiple_drops client_misconfig client_error	アクセス拒否 アクセス許可 存在しないリソースへのアクセス ファイアウォールによるドロップ 複数のファイアウォールによるドロップ クライアントの誤った設定 クライアントエラー
ネットワーク制御	new_host ip_spoof	新しいコンピュータの検出 ARPスプーフィングの疑い
システム監視	service_start system_error system_shutdown logs_cleared invalid_request promisc policy_changed config_changed low_diskspace time_changed	サービスの開始 システムエラー シャットダウン ログのクリア 無効な要求 インタフェースのプロミスキャスモードへの切り替え ポリシーの変更 設定の変更 ディスク容量が少ない 時刻の変更

イベントの自動タグ付けが有効になっている場合、イベントはグループ名でラベル付けされます。トレンドマイクロが提供するセキュリティログ監視ルールは、グループをよりユーザーフレンドリーなバージョンに変更する変換テーブルを使用します。例えば、login_deniedはLogin Deniedとして表示されます。カスタムルールは、ルールに表示されるグループ名で一覧表示されます。

説明

<description></description>タグを含めます。ルールがトリガーされた場合、説明テキストがイベントに表示されます。

```
<group name="syslog,sshd,"> <rule id="100120" level="5"> <group>authentication_success</group>
<description>SSHD testing authentication success</description> </rule> <rule id="100121" level="6">
<description>SSHD rule testing 2</description> </rule> </group>
```

デコード形式

<decoded_as></decoded_as>タグは、指定されたデコーダーがログをデコードした場合にのみルールを適用するようにセキュリティログ監視エンジンに指示します。

```
<rule id="100123" level="5"> <decoded_as>sshd</decoded_as> <description>Logging every decoded sshd message</description> </rule>
```

使用可能なデコーダを表示するには、[セキュリティログ監視ルール] 画面で [デコーダ] をクリックします。[1002791-Default Log Decoders] を右クリックして、[プロパティ] を選択します。[設定] タブに進み、[デコーダの表示] をクリックします。

一致項目

ログ内で特定の文字列を探すには、<match></match>を使用します。こちらはLinuxのsshd失敗パスワードログです。

```
Jan 1 12:34:56 linux_server sshd[1231]: Failed password for invalid user jsmith from 192.168.1.123 port 1799 ssh2
```

「Failed password」という文字列を検索するには、<match></match> タグを使用します。

```
<rule id="100124" level="5"> <decoded_as>sshd</decoded_as> <match>^Failed password</match> <description>Failed SSHD password attempt</description> </rule>
```

正規表現のキャレット(^) は文字列の先頭を示しています。「Failed password」はログの先頭には表示されませんが、セキュリティログ監視デコーダーはログをセクションに分割します。参照 "デコーダ" on page 783 詳細情報については、「log」はログのメッセージ部分であり、「full_log」はログ全体であるセクションの1つです。

次の表は、サポートされている正規表現の構文一覧です。

正規表現の構文	説明
\w	A ~ Z、a ~ z、0 ~ 9の英数字1文字
\d	0 ~ 9の数字1文字
\s	単一のスペース(空白文字)
\t	単一のタブ
\p	()*+,-.:;<=>?[]
\W	\w以外
\D	\d以外
\S	\s以外
\.	任意の文字
+	上記のいずれかの1つ以上に一致 (たとえば、\w+、\d+)
*	上記のいずれかの0個以上に一致 (たとえば、\w*、\d*)
^	文字列の先頭 (^<任意の文字列>)
$	文字列の末尾 (<任意の文字列>$)
|	複数の文字列間の「OR」

条件文

ルールの評価は、他のルールが真と評価された場合に条件付きで行うことができます。<if_sid></if_sid>タグは、タグで識別されたルールが真と評価された場合にのみ、このサブルールを評価するようにセキュリティログ監視エンジンに指示します。次の例では、3つのルールを示しています: 100123、100124、および100125。ルール100124と100125は、<if_sid></if_sid>タグを使用して100123ルールの子として変更されています。

```
<group name="syslog,sshd,"> <rule id="100123" level="2"> <decoded_as>sshd</decoded_as> <description>すべてのデコードされたsshdメッセージを記録</description> </rule> <rule id="100124" level="7"> <if_sid>100123</if_sid> <match>^Failed password</match> <group>authentication_failure</group> <description>SSHDパスワード試行失敗</description> </rule> <rule id="100125" level="3"> <if_sid>100123</if_sid> <match>^Accepted password</match> <group>authentication_success</group> <description>SSHDパスワード試行成功</description> </rule> </group>
```

評価の階層

<if_sid></if_sid>タグは本質的に階層的なルールセットを作成します。つまり、ルールに<if_sid></if_sid>タグを含めることで、そのルールは<if_sid></if_sid>タグで参照されるルールの子ルールとなります。ログにルールを適用する前に、セキュリティログ監視エンジンは<if_sid></if_sid>タグを評価し、親ルールと子ルールの階層を構築します。

階層的な親子構造を使用することで、ルールの効率を向上させることができます。親ルールが真と評価されない場合、セキュリティログ監視エンジンはその親の子ルールを無視します。

<if_sid></if_sid>タグは、まったく異なるセキュリティログ監視ルール内のサブルールを参照するために使用できますが、後でルールを確認するのが非常に難しくなるため、これを避けるべきです。

次の表は、使用可能なアトミックルールの条件指定のオプションを一覧表示しています。

タグ	説明	備考
match	パターン	イベント(ログ)に対して照合される任意の文字列。
regex	正規表現	イベント(ログ)に対して一致する正規表現。
decoded_as	文字列	事前一致する任意の文字列。
srcip	送信元のIPアドレス	ソースIPアドレスとしてデコードされたIPアドレス。IPアドレスを否定するには!を使用します。
dstip	送信先のIPアドレス	宛先IPアドレスとしてデコードされたIPアドレス。IPアドレスを否定するには!を使用します。
srcport	送信元のポート番号	任意の送信元のポート(形式の一致)。
dstport	送信先のポート番号	任意の送信先のポート(形式の一致)。
user	ユーザ名	ユーザ名としてデコードされる任意のユーザ名。

タグ	説明	備考
program_name	プログラム名	Syslogプロセス名からデコードされる任意のプログラム名。
hostname	システムのホスト名	Syslogのホスト名としてデコードされる任意のホスト名。
time	次の形式の時刻の範囲 hh:mm - hh:mmまたは hh:mm am - hh:mm pm	トリガするルールに対してイベントが発生する必要のある時刻の範囲。
weekday	平日 (日曜日、月曜日、火曜日など)	トリガするルールに対してイベントが発生する必要のある曜日。
id	ID	イベントからデコードされる任意のID。
url	URL	イベントからデコードされる任意のURL。

このルールを100125ルールに依存させるには、<if_sid>100125</if_sid>タグを使用します。このルールは、すでに成功したログインルールに一致したSSHDメッセージに対してのみチェックされます。

```
<rule id="100127" level="10"> <if_sid>100125</if_sid> <time>6 pm - 8:30 am</time> <description>Login outside business hours.</description> <group>policy_violation</group> </rule>
```

ログエントリのサイズに関する制限

次の例では、前の例にmaxsize属性を追加し、セキュリティログ監視エンジンに対して、最大サイズの文字数未満のルールのみを評価するように指示します。

```
<rule id="100127" level="10" maxsize="2000"> <if_sid>100125</if_sid> <time>6 pm - 8:30 am</time> <description>Login outside business hours.</description> <group>policy_violation</group> </rule>
```

次の表は、使用可能なアトミックルールのツリーベースのオプションを一覧表示しています。

タグ	説明	備考
if_sid	ルールID	指定された署名IDに一致するルールの子ルールとしてこのルールを追加します。
if_group	グループID	指定されたグループに一致するルールの子ルールとしてこのルールを追加します。
if_level	ルールレベル	指定された重要度レベルに一致するルールの子ルールとしてこのルールを追加します。
説明	文字列	ルールの説明。
info	文字列	ルールの追加情報。
cve	CVE番号	ルールに関連付ける任意のCommon Vulnerabilities and Exposures (CVE) 番号。
options	alert_by_email no_email_	アラートの処理としてメール生成 (alert_by_email)、メール生成なし (no_email_alert)、またはログへの記録なし (no_log) のいずれかを指定する追加のルールオプション。

タグ	説明	備考
	alert no_log	

コンポジットルール

単一のログエントリを検査するのがアトミックルールです。複数のエントリを関連付けるには、コンポジットルールを使用する必要があります。コンポジットルールは、現在のログを既に受信したものと一致させることを目的としています。コンポジットルールには2つの追加オプションが必要です: frequencyオプションは、ルールがアラートを生成する前にイベントまたはパターンが何回発生する必要があるかを指定し、timeframeオプションは、セキュリティログ監視エンジンが過去のログを何秒前まで遡って検索するかを指示します。すべてのコンポジットルールは次の構造を持っています:

```
<rule id="100130" level="10" frequency="x" timeframe="y"> </rule>
```

例えば、10分間に5回のパスワード失敗があった場合に高い重大度のアラートを作成する複合ルールを作成することができます。<if_matched_sid></if_matched_sid>タグを使用して、新しいルールがアラートを作成するために必要な頻度と時間枠内でどのルールを確認する必要があるかを示すことができます。次の例では、frequency属性はイベントが5回発生したときにトリガーされるように設定され、timeframe属性は時間枠を600秒として指定するように設定されています。

<if_matched_sid></if_matched_sid>タグは、複合ルールが監視する他のルールを定義するために使用されます。

```
<rule id="100130" level="10" frequency="5" timeframe="600"> <if_matched_sid>100124</if_matched_
sid> <description>5 Failed passwords within 10 minutes</description> </rule>
```

より詳細なコンポジットルールを作成するのに使用できるタグが他にもいくつかあります。このようなルールを使用すると、次の表に示すように、イベントの特定の部分が同じになるように指定できます。これにより、コンポジットルールを調整して誤判定を減らすことができます。

タグ	説明
same_source_ip	送信元のIPアドレスが同じになるように指定します。
same_dest_ip	送信先のIPアドレスが同じになるように指定します。
same_dst_port	送信先のポートが同じになるように指定します。
same_location	場所 (ホスト名またはAgent名) が同じになるように指定します。
same_user	デコードされるユーザ名が同じになるように指定します。
same_id	デコードされるIDが同じになるように指定します。

複合ルールが特定のルールIDではなく、すべての認証失敗に対してアラートを出すようにしたい場合、<if_matched_sid></if_matched_sid>タグを<if_matched_ group></if_matched_ group>タグに置き換える

ことができます。これにより、authentication_ failureのようなカテゴリを指定して、インフラ全体で認証失敗を検索することができます。

```
<rule id="100130" level="10" frequency="5" timeframe="600"> <if_matched_group>authentication_ failure</if_matched_group> <same_source_ip /> <description>5 Failed passwords within 10 minutes</description> </rule>
```

<if_matched_sid></if_matched_sid>タグと<if_matched_group></if_matched_ group>タグに加えて、<if_matched_regex></if_matched_regex>タグを使用して、受信したログを検索するための正規表現を指定することもできます。

```
<rule id="100130" level="10" frequency="5" timeframe="600"> <if_matched_regex>^Failed password</if_matched_regex> <same_source_ip /> <description>10分以内に5回のパスワード失敗 </description> </rule>
```

例

Deep Securityには、数多くの一般的なアプリケーションおよび一般的なアプリケーションの セキュリティログ監視 初期設定ルールが多数含まれています。新しいルールは、セキュリティアップデートを使用して定期的に追加できます。 セキュリティログ監視 ルールでサポートされるアプリケーションのリストが増加しているにもかかわらず、サポートされていないアプリケーションまたは カスタムアプリケーションのカスタムルールを作成する必要が生じる場合があります。

次の例では、Microsoft Windowsサーバー上でIISとNetプラットフォームを使用してホストされるカスタムCMS (コンテンツ管理システム) を作成し、データリポジトリとしてMicrosoft SQLサーバーデータベースを使用します。

最初に、次に示すアプリケーションログの属性を特定します。

1. アプリケーションログを記録する場所
2. どの セキュリティログ監視 デコーダを使用してログファイルを復号できますか?
3. ログファイル メッセージの一般的な形式

CMSの例について、回答は以下の通りです。

1. Windowsイベントビューア
2. Windowsイベントログ (eventlog)
3. Windowsイベントログ形式 (次のコア属性を使用)
    - ソース: CMS
    - カテゴリ: なし
    - イベント:<Application Event ID>

次に、アプリケーションの機能別にログイベントのカテゴリを特定し、そのカテゴリを監視用のカスケードグループの階層に分類します。監視対象のすべてのグループでイベントを発生させる必要はなく、一致する項目を条件文として使用できます。各グループについて、ルールで照合条件として使用できるログ形式の属性を特定します。これは、すべてのアプリケーションログの、ログイベントのパターンおよび論理分類を調べて実行することもできます。

例えば、CMSアプリケーションは以下の機能をサポートしており、それに対してセキュリティログ監視ルールが作成されています。

- CMSアプリケーションログ (ソース: CMS)
  - 認証 (イベント: 100 ~ 119)
    - ユーザログインの成功 (イベント: 100)
    - ユーザログインの失敗 (イベント: 101)
    - 管理者ログインの成功 (イベント: 105)
    - 管理者ログインの失敗 (イベント: 106)
  - 一般エラー (種類: エラー)
    - データベースエラー (イベント: 200 ~ 205)
    - ランタイムエラー (イベント: 206 ~ 249)
  - アプリケーション監査 (種類: 情報)
    - コンテンツ
      - 新しいコンテンツの追加 (イベント: 450 ~ 459)
      - 既存のコンテンツの変更 (イベント: 460 ~ 469)
      - 既存のコンテンツの削除 (イベント: 470 ~ 479)
    - 管理
      - User
        - 新しいユーザの作成 (イベント: 445 ~ 446)
        - 既存のユーザの削除 (イベント: 447 ~ 449)

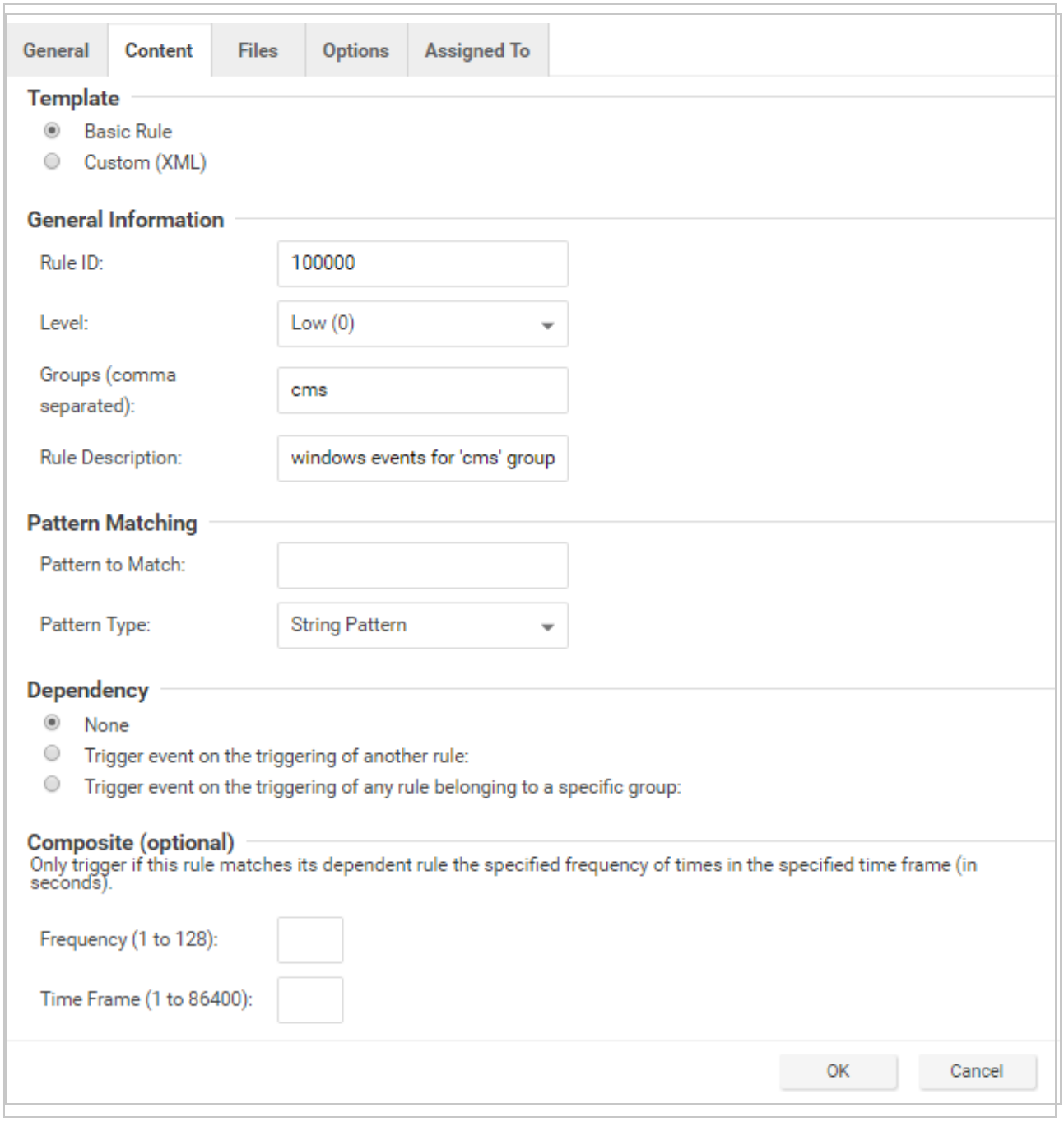
この構造は、ルール作成のための良い基盤を提供します。これで、Deep Security Managerで新しいセキュリティログ監視ルールを作成できます。

新しいCMSセキュリティログ監視ルールを作成するには

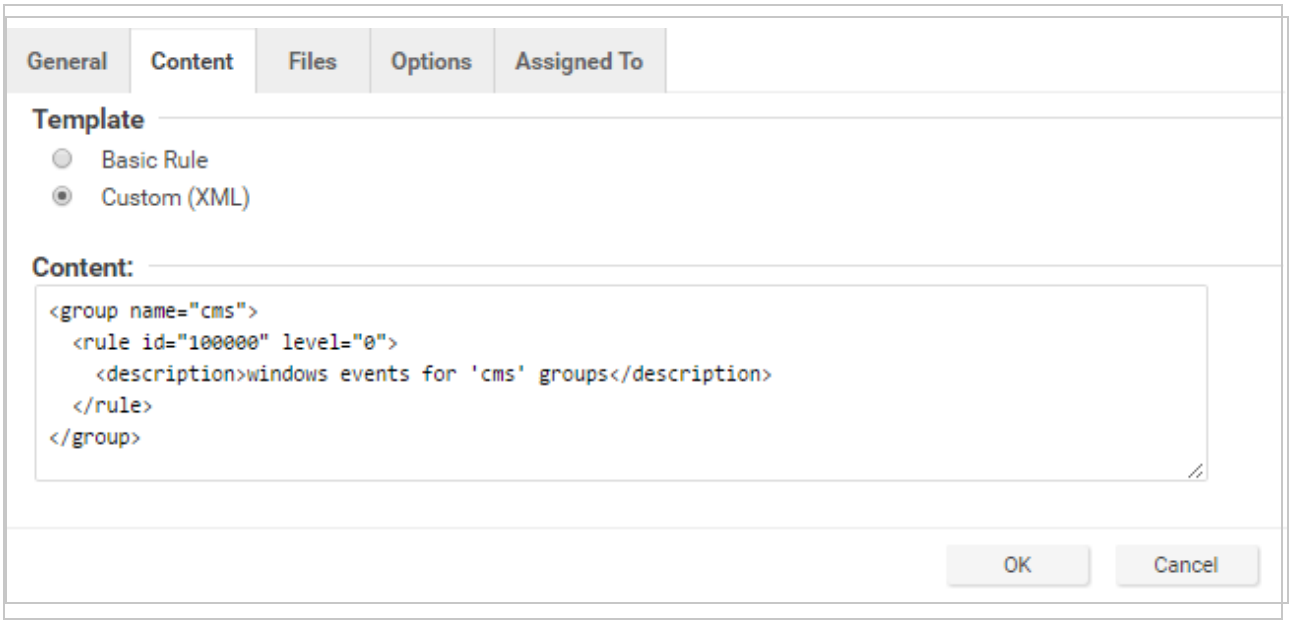
1. Deep Security Managerで、ポリシー > 共通オブジェクト > ルール > セキュリティログ監視ルールに移動し、新規をクリックして新規セキュリティログ監視ルールのプロパティウィンドウを表示します。

2. 新しいルールに名前と説明を付けて、コンテンツタブを選択してください。
3. 基本ルールを選択します。新しいカスタムルールを作成する最も簡単な方法は、基本ルールテンプレートから始めることです。
4. ルールIDフィールドには、カスタムルール用に予約された100,000以上の未使用ID番号が自動的に入力されます。
5. [レベル] を [低 (0)] に設定します。
6. ルールに適切なグループ名を指定します。ここでは「cms」とします。

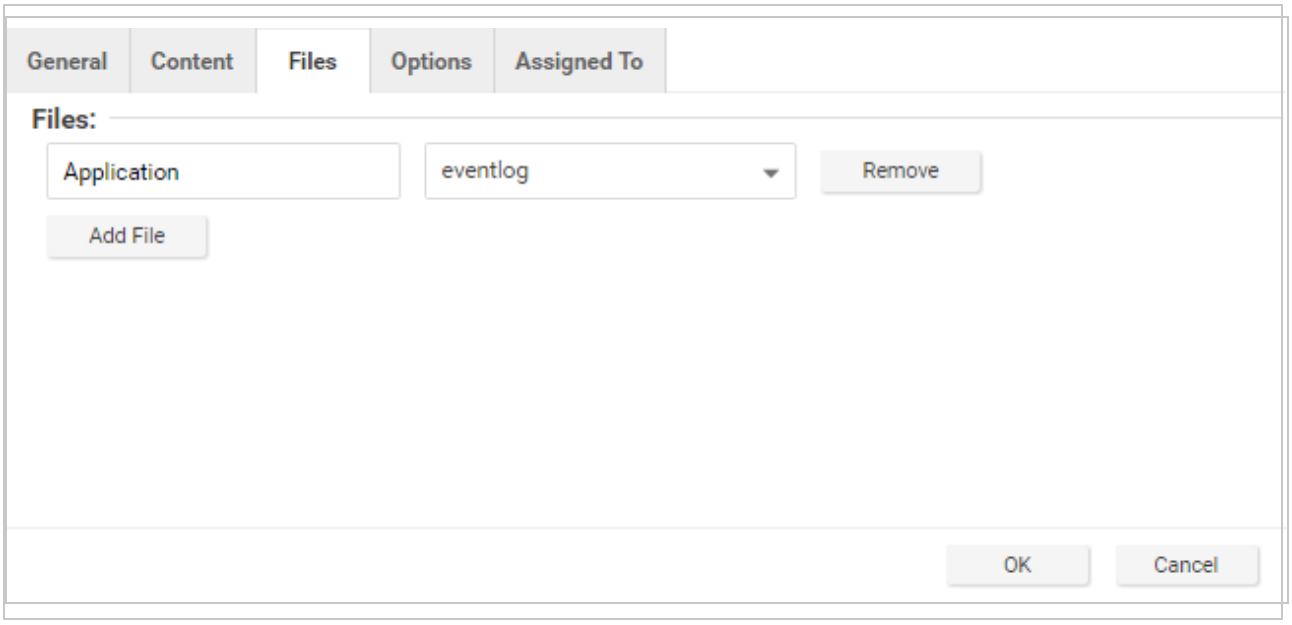
7. ルールの簡単な説明を入力します。



8. カスタム (XML)を選択します。基本ルールで選択したオプションがXMLに変換されます。



9. ファイルタブを選択し、ファイルを追加をクリックして、ルールを適用するアプリケーションログファイルとログタイプを追加します。この場合、ファイルタイプとしてアプリケーションとeventlogを選択します。



EventlogはDeep Securityにおけるユニークなファイルタイプです。なぜなら、ログファイルの場所やファイル名を指定する必要がないからです。代わりに、Windowsイベントビューアに表示されるログ名を入力するだけで十分です。Eventlogファイルタイプの他のログ名には、Security、

System、Internet Explorer、またはWindowsイベントビューアにリストされている他のセクションが含まれることがあります。他のファイルタイプでは、ログファイルの場所とファイル名が必要です。C/C++のstrftime () 変換指定子は、ファイル名の一致に利用可能です。より便利なもののリストについては、表を参照してください。

10. [OK] をクリックして基本ルールを保存します。
11. 基本ルールCustom (XML) を作成したら、以前に特定されたロググループに基づいてグループに新しいルールを追加し始めることができます。基本ルールの基準を初期ルールに設定する必要があります。次の例では、CMS基本ルールがCMSのSource属性を持つWindowsイベントログを特定しています。

    ```
    <group name="cms"> <rule id="100000" level="0"> <category>windows</category> <extra_data>^CMS</extra_data> <description>Windows events from source 'CMS' group messages.</description> </rule>
    ```

12. 識別されたロググループから後続のルールを構築して進めます。次の例では、認証とログインの成功および失敗をイベントIDで識別し、ログに記録します。

    ```
    <rule id="100001" level="0"> <if_sid>100000</if_sid> <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id> <group>authentication</group> <description>CMS認証イベント。</description> </rule> <rule id="100002" level="0"> <if_group>authentication</if_group> <id>100</id> <description>CMSユーザーログイン成功イベント。</description> </rule> <rule id="100003" level="4"> <if_group>authentication</if_group> <id>101</id> <group>authentication_failure</group> <description>CMSユーザーログイン失敗イベント。</description> </rule> <rule id="100004" level="0"> <if_group>authentication</if_group> <id>105</id> <description>CMS管理者ログイン成功イベント。</description> </rule> <rule id="100005" level="4"> <if_group>authentication</if_group> <id>106</id> <group>authentication_failure</group> <description>CMS管理者ログイン失敗イベント。</description> </rule>
    ```

13. 確立されたルールを使用して、任意の複合または相関ルールを追加します。次の例は、10秒間に5回のログイン失敗が発生した場合に適用される高重大度の複合ルールを示しています。

    ```
    <rule id="100006" level="10" frequency="5" timeframe="10"> <if_matched_group>authentication_failure</if_matched_group> <description>CMS繰り返し認証ログイン失敗イベント。</description> </rule>
    ```

14. すべてのルールの重要度レベルが適切かどうかを確認します。たとえば、エラーログの重要度はレベル5以上でなければなりません。情報ルールの重要度は低くなります。
15. 新しく作成したルールを開き、Configurationタブを選択し、カスタムルールのXMLをルールフィールドにコピーします。適用またはOKをクリックして変更を保存します。

ルールがポリシーまたはコンピュータに割り当てられると、セキュリティログ監視 エンジンは、指定されたログファイルの検査をただちに開始します。

完成したカスタムCMSセキュリティログ監視ルール:

```
<group name="cms">
 <rule id="100000" level="0"> <category>windows</category> <extra_data>^CMS</extra_data>
<description>Windows events from source 'CMS' group messages.</description> </rule>
 <rule id="100001" level="0"> <if_sid>100000</if_sid>
<id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id> <group>authentication</group>
<description>CMS Authentication event.</description> </rule> <rule id="100002" level="0"> <if_
group>authentication</if_group> <id>100</id> <description>CMS User Login success
event.</description> </rule> <rule id="100003" level="4"> <if_group>authentication</if_group>
<id>101</id> <group>authentication_failure</group> <description>CMS User Login failure
event.</description> </rule> <rule id="100004" level="0"> <if_group>authentication</if_group>
<id>105</id> <description>CMS Administrator Login success event.</description> </rule> <rule
id="100005" level="4"> <if_group>authentication</if_group> <id>106</id> <group>authentication_
failure</group> <description>CMS Administrator Login failure event.</description> </rule> <rule
id="100006" level="10" frequency="5" timeframe="10"> <if_matched_group>authentication_failure</if_
matched_group> <description>CMS Repeated Authentication Login failure event.</description> </rule>
<rule id="100007" level="5"> <if_sid>100000</if_sid> <status>^ERROR</status> <description>CMS
General error event.</description> <group>cms_error</group> </rule> <rule id="100008" level="10">
<if_group>cms_error</if_group> <id>^200|^201|^202|^203|^204|^205</id> <description>CMS Database
error event.</description> </rule> <rule id="100009" level="10"> <if_group>cms_error</if_group>
<id>^206|^207|^208|^209|^230|^231|^232|^233|^234|^235|^236|^237|^238|
^239^|240|^241|^242|^243|^244|^245|^246|^247|^248|^249</id> <description>CMS Runtime error
event.</description> </rule> <rule id="100010" level="0"> <if_sid>100000</if_sid>
<status>^INFORMATION</status> <description>CMS General informational event.</description>
<group>cms_information</group> </rule> <rule id="100011" level="5"> <if_group>cms_information</if_
group> <id>^450|^451|^452|^453|^454|^455|^456|^457|^458|^459</id> <description>CMS New Content
added event.</description> </rule> <rule id="100012" level="5"> <if_group>cms_information</if_group>
<id>^460|^461|^462|^463|^464|^465|^466|^467|^468|^469</id> <description>CMS Existing Content
modified event.</description> </rule> <rule id="100013" level="5"> <if_group>cms_information</if_
group> <id>^470|^471|^472|^473|^474|^475|^476|^477|^478|^479</id> <description>CMS Existing
Content deleted event.</description> </rule> <rule id="100014" level="5"> <if_group>cms_
information</if_group> <id>^445|^446</id> <description>CMS User created event.</description> </rule>
<rule id="100015" level="5"> <if_group>cms_information</if_group> <id>^447|449</id>
<description>CMS User deleted event.</description> </rule> </group>
```

セキュリティログ監視 ルールの重大度レベルと推奨される使用

レベル	説明	備考
レベル	無視され、	主に誤判定を回避するために使用されます。これらのルールは、他のすべての

レベル	説明	備考
0	処理は行われない	ルールより先に検索され、セキュリティとは無関係のイベントが含まれます。
レベル 1	事前定義された使用法はなし	
レベル 2	システムの優先度の低い通知	セキュリティとは無関係のシステム通知またはステータスメッセージ。
レベル 3	成功した/承認されたイベント	成功したログイン試行、ファイアウォール許可イベントなど。
レベル 4	システムの優先度の低いエラー	不正な設定または未使用のデバイス/アプリケーションに関連するエラー。セキュリティとは無関係であり、通常は初期設定のインストールまたはソフトウェアのテストが原因で発生します。
レベル 5	ユーザによって生成されたエラー	パスワードの見落とし、アクションの拒否など。これらのメッセージは通常、セキュリティに関連しません。
レベル 6	関連性の低い攻撃	システムに脅威を及ぼさないワームまたはウイルスを示します (Linuxサーバを攻撃するWindowsワームなど)。また、頻繁にトリガされるIDSイベントおよび一般的なエラーイベントも含まれます。
レベル 7	事前定義された使用法はなし	
レベル 8	事前定義された使用法はなし	
レベル 9	無効なソースからのエラー	不明なユーザとしてのログインの試行または無効なソースからのログインの試行が含まれます。特にこのメッセージが繰り返される場合は、セキュリティとの関連性がある可能性があります。また、adminまたはrootアカウントに関するエラーも含まれます。
レベル 10	ユーザによって生成された複数のエラー	複数の不正なパスワードや複数のログイン失敗などを含めてください。それらは攻撃を示している可能性もありますし、単にユーザが資格情報を忘れた可能性もあります。
レベル 11	事前定義された使用法はなし	
レベル 12	重要度の高いイベント	システムやカーネルなどからのエラーまたは警告メッセージを含めます。これらは特定のアプリケーションに対する攻撃を示している可能性があります。
レベル 13	通常と異なるエラー (重要度: 高)	バッファオーバーフローの試行などの一般的な攻撃パターン、通常のSyslogメッセージ長の超過、または通常のURL文字列長の超過。
レベル 14	重要度の高いセキュリ	通常、複数の攻撃ルールと攻撃の兆候が組み合わさったもの。

レベル	説明	備考
	ティイベント	
レベル 15	攻撃の成功	誤判定の可能性はほとんどありません。すぐに対処が必要です。

strftime () 変換指定子

指定子	説明
%a	省略された曜日名 (例: 木)
%A	曜日の完全な名前 (例: 木曜日)
%b	省略された月名 (例: Aug)
%B	月の完全な名前 (例: 8月)
%c	日付と時刻の表記 (例: Thu Sep 22 12:23:45 2007)
%d	月の日 (01 - 31) (例: 20)
%H	24時間形式の時刻 (00 - 23) (例: 13)
%I	12時間形式の時 (01 - 12)(例: 02)
%j	年の日数 (001 - 366) (例: 235)
%m	月を10進数で表したもの (01 - 12)(例: 02)
%M	分 (00 - 59) (例えば、12)
%p	午前または午後の指定 (例: AM)
%S	秒 (00 - 61) (例: 55)
%U	最初の日曜日を週の初日とする週番号 (00 - 53) (例: 52)
%w	日曜日を0とする10進数の曜日 (0 - 6) (例: 2)
%W	最初の月曜日を週の初日とする週番号 (00 - 53) (例: 21)
%x	日付表記 (例: 02/24/79)
%X	時間表記 (例: 04:12:51)
%y	年、西暦の下2桁 (00 - 99)(例: 76)
%Y	年 (例: 2008)
%Z	タイムゾーン名または略語 (例: EST)
%%	% 記号 (例えば、%)

詳細については、以下を参照してください。

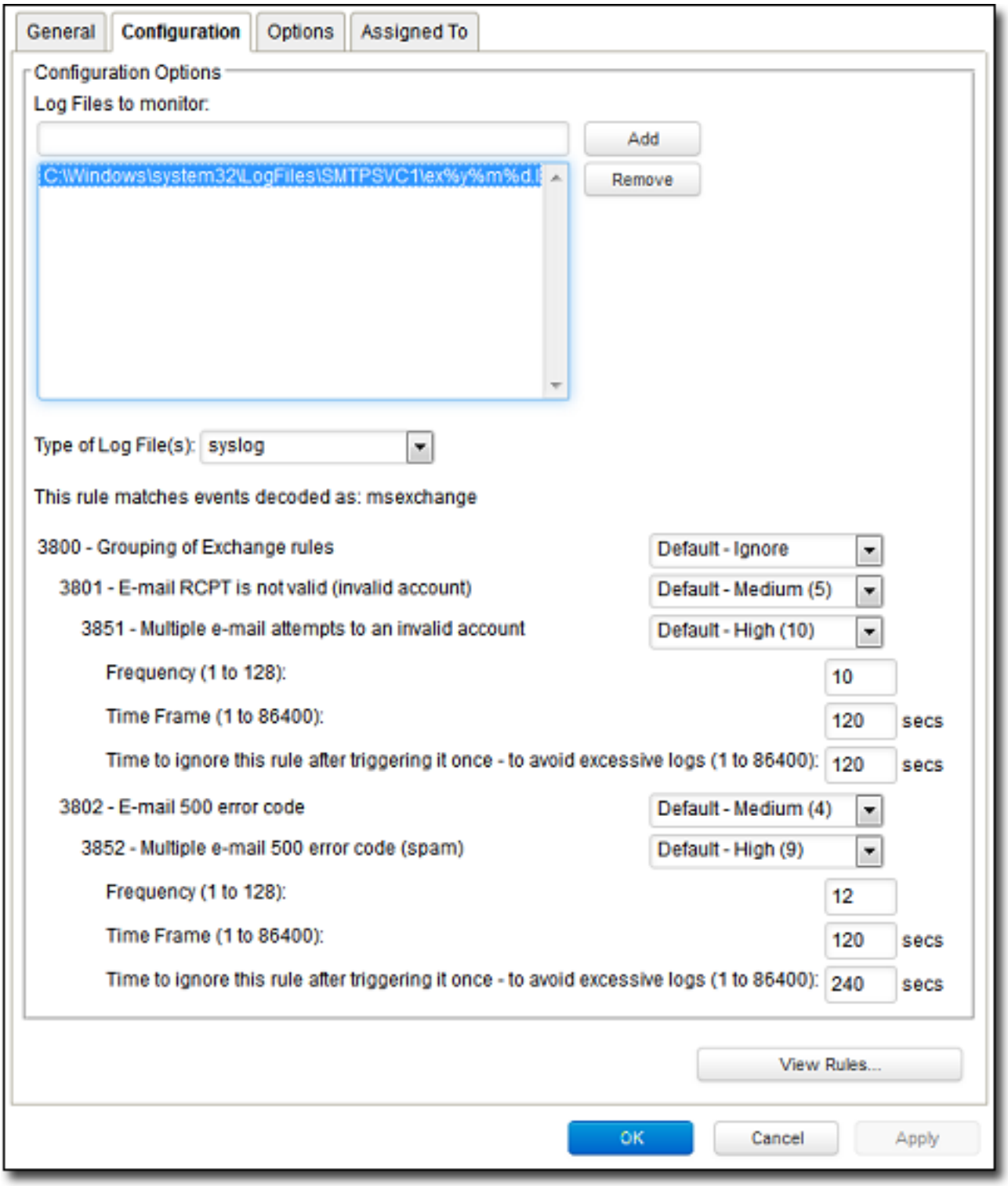
- https://www.php.net/manual/en/function.strftime.php
- www.cplusplus.com/reference/clibrary/ctime/

セキュリティログ監視 ルールを調べる

セキュリティログ監視ルールは、Deep Security Managerのポリシー > 共通オブジェクト > ルール > セキュリティログ監視ルールにあります。

セキュリティログ監視 のルール構造とイベント照合プロセス

次の図は、Microsoft Exchangeセキュリティログ監視ルールのプロパティウィンドウの構成タブの内容を示しています。


General
Configuration
Options
Assigned To
Configuration Options
Log Files to monitor:
Add
Remove
C:\Windows\system32\LogFiles\SMTPSVC1\ex%y%m%d.l
Type of Log File(s): syslog
This rule matches events decoded as: msexchange
3800 - Grouping of Exchange rules
Default - Ignore
3801 - E-mail RCPT is not valid (invalid account)
Default - Medium (5)
3851 - Multiple e-mail attempts to an invalid account
Default - High (10)
Frequency (1 to 128): 10
Time Frame (1 to 86400): 120 secs
Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400): 120 secs
3802 - E-mail 500 error code
Default - Medium (4)
3852 - Multiple e-mail 500 error code (spam)
Default - High (9)
Frequency (1 to 128): 12
Time Frame (1 to 86400): 120 secs
Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400): 240 secs
View Rules...
OK
Cancel
Apply

以下はルール構造です:

- 3800 - Grouping of Exchange Rules - Default - ignore
  - 3801 - Email rcpt is not valid (invalid account) - Default - Medium (5)
    - 3851 - Multiple email attempts to an invalid account - Default - High (10)
      - Frequency (1 to 128) - 10
      - Time Frame (1 to 86400) - 120
      - Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400) - 120
  - 3802 - Email 500 error code - Default - Medium (4)
    - 3852 - Email 500 error code (spam) - Default - High (9)
      - Frequency (1 to 128) - 12
      - Time Frame (1 to 86400) - 120
      - Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400) - 240

セキュリティログ監視エンジンはログイベントをこの構造に適用し、一致があるかどうかを確認します。例えば、Exchangeイベントが発生し、このイベントが無効なアカウントへのメール受信である場合、イベントは行3800と一致します (これはExchangeイベントであるためです)。その後、イベントは行3800のサブルール3801および3802に適用されます。

これ以上の一致がない場合、この一致のカスケードは3800で停止します。3800は無視の重大度レベルであるため、セキュリティログ監視イベントは記録されません。

しかし、無効なアカウントへのメール受信は3800のサブルールの1つ、サブルール3801に一致します。サブルール3801の重大度レベルは中 (4) です。ここで一致が停止した場合、重大度レベルが中 (4) のセキュリティログ監視イベントが記録されます。

しかし、イベントに適用される別のサブルールがあります: サブルール3851です。サブルール3851は、3つの属性を持ち、同じイベントが過去120秒以内に10回発生した場合に一致します。その場合、セキュリティログ監視イベントが重大度高 (9) で記録されます。無視属性は、次の120秒間、サブルール3801に一致する個々のイベントを無視するようにサブルール3851に指示します。これはノイズを減らすのに役立ちます。

サブルール3851のパラメータが一致したと仮定すると、セキュリティログ監視イベントが重大度高 (9) で記録されました。

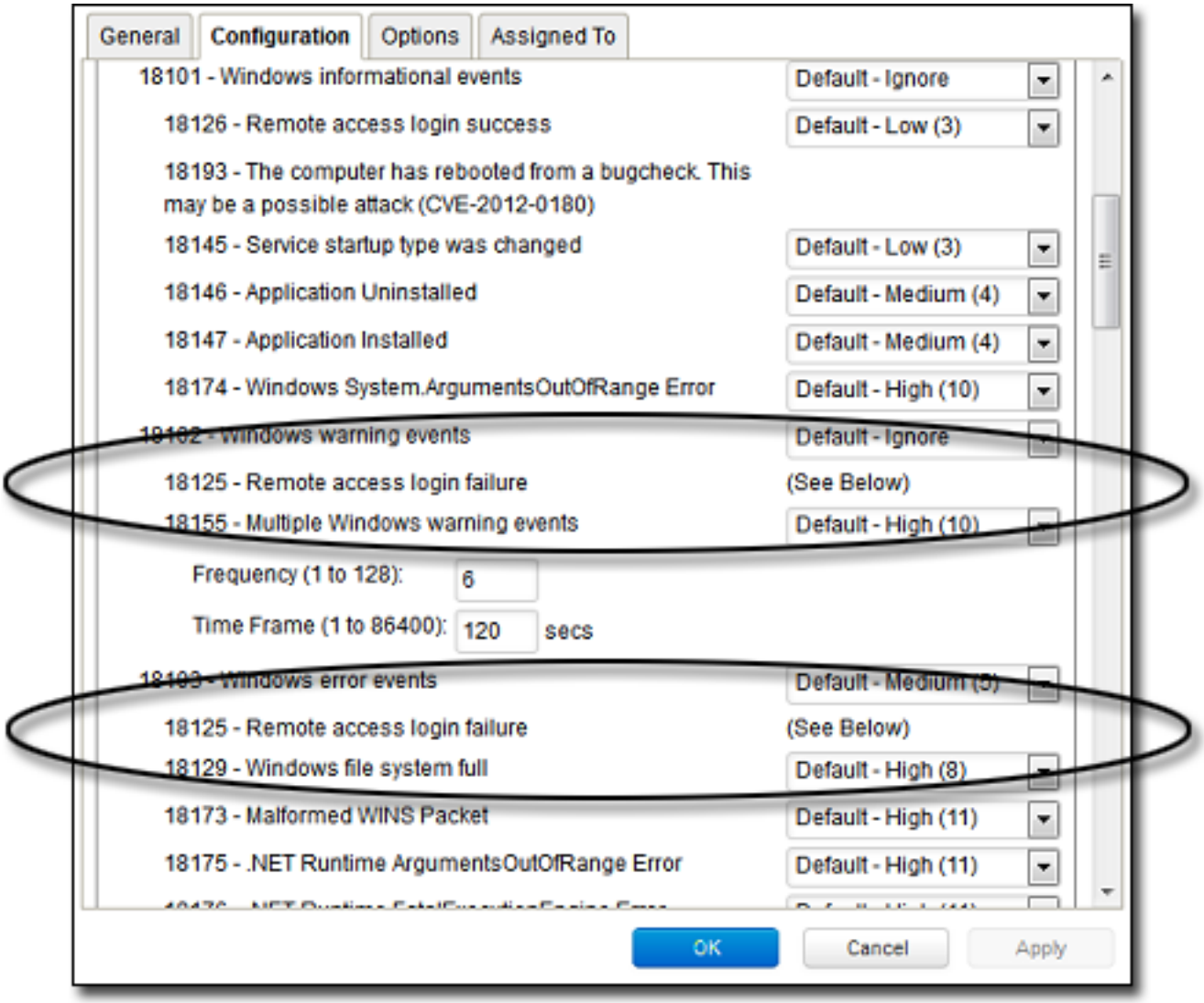
Microsoft Exchangeルールのオプションタブを確認すると、Deep Security Managerは重大度レベルが中 (4) のサブルールが一致した場合にアラートを発することがわかります。この例ではその通りなので、

アラートが発せられます(このルールがイベントを記録したときにアラートを出すが選択されている場合)。

重複するサブルール

一部のセキュリティログ監視ルールには重複するサブルールがあります。例を見るには、Microsoft Windows Eventsルールを開き、設定タブを選択してください。サブルール18125(リモートアクセスログイン失敗)がサブルール18102と18103の下に表示されることに注意してください。また、どちらの場合もサブルール18125には重大度の値がなく、「以下を参照」とだけ表示されることに注意してください。

重複して表示されるのではなく、ルール18125は、[設定]画面の下部に1回だけ表示されています。



ポリシーで使用するディレクトリリストの作成

複数のポリシーで使用するディレクトリパスのリストを作成します。異なるポリシーごとに同じリストを作成するよりも、単一のリストを管理する方が簡単です。これらのリストの最も一般的な使用例は、不正プログラム対策スキャンの対象ファイルの指定または除外です。詳細については、"検索対象ファイルを指定する" on page 838を参照してください。

既存のリストに類似するディレクトリリストを作成するには、既存のリストを複製して編集します。

次の表は、ディレクトリリスト項目を定義するための構文を説明しています。WindowsおよびLinuxの規則に従って、スラッシュとバックスラッシュの両方がサポートされています。

ディレクトリ	形式	説明	例
ディレクトリ	DIRECTORY	指定したディレクトリとそのすべてのサブディレクトリにあるファイルをすべて含めます。	C:\Program Files\ Program Filesディレクトリとそのすべてのサブディレクトリにあるファイルをすべて含めます。
ネットワークリソース	\\NETWORK RESOURCE	対象コンピュータのネットワークリソースに含まれている、コンピュータ上のファイルを含めます。	*12.34.56.78*\ *some-comp-name*\ IPまたはホスト名を使用して識別されたネットワークリソース(およびそのサブフォルダ)上のすべてのファイルが含まれます。 *12.34.56.78**somefolder*\ *some-comp-name**somefolder*\ IPまたはホスト名を使用して識別されたネットワークリソース上のフォルダsomefolderおよびそのサブフォルダ内のすべてのファイルが含まれます。
ワイルドカード(*)を使用したディレクトリ	DIRECTORY*\	任意のサブディレクトリ名を持つすべてのサブディレクトリを含めます。ただし、指定したディレクトリにあるファイルは含めません。	*C:**abc**\ abcのすべてのサブディレクトリ内のすべてのファイルを含みますが、abcディレクトリ内のファイルは含みません。 *C:**abc**wx**z*\ *一致する:* C:\abc\wxz\ C:\abc\wx123z\ *一致しない:* C:\abc\wxz C:\abc\wx123z

ディレクトリ	形式	説明	例
			*C:\abc*wx* *一致する:* C:\abc\wx\ C:\abc\123wx\ *一致しない:* C:\abc\wx C:\abc\123wx
ワイルドカード(*)を使用したディレクトリ	DIRECTORY*	名前が一致する任意のサブディレクトリを含めます。ただし、そのディレクトリにあるファイルおよび任意のサブディレクトリは含めません。	*C:\abc** *対象:* C:\abc\ C:\abc\1 C:\abc\123 *対象外:* C:\abc C:\abc\123\ C:\abc\123\456 C:\abx\ C:\xyz\ *C:\abc*wx* *対象::* C:\abc\wx C:\abc\123wx *対象外::* C:\abc\wx\ C:\abc\123wx\ *C:\abc\wx*z* *対象:* C:\abc\wxz C:\abc\wx123z *対象外::* C:\abc\wxz\ C:\abc\wx123z\ *C:\abc\wx** *対象::* C:\abc\wx C:\abc\wx\ C:\abc\wx12 C:\abc\wx12\345\ C:\abc\wxz\ *対象外::* C:\abc\wx123z\
環境変数	${ENV VAR}	環境変数 ${ENV VAR} の形式で定義されたすべてのファイルおよびサブディレク	*${windir}* 変数がc:\windowsに変換された

ディレクトリ	形式	説明	例
		トリが含まれます。windir、programfilesなどのWindowsの一般的な環境変数がサポートされています。 Virtual Applianceおよび Linuxの場合、環境変数の値のペアはポリシーまたはコンピュータエディタ> 設定 > 一般 > 環境変数オーバーライドで定義する必要があります	場合、c:\windowsとそのすべてのサブディレクトリにあるファイルをすべて含めます。
コメント	DIRECTORY # コメント	対象の定義にコメントを追加できます。	*c:\abc #abcディレクトリを含めます*

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ディレクトリリスト] の順にクリックします。
2. [新規]→[新しいディレクトリリスト] の順にクリックします。
3. 名前を入力し、必要に応じて説明を入力します。
4. [ディレクトリ] リストで、ディレクトリパスを1行に1つずつ追加します。
5. [OK] をクリックします。

ディレクトリリストをインポート/エクスポートする

1つ以上のディレクトリリストをXMLファイルまたはCSVファイルにエクスポートできます。また、XMLファイルからディレクトリリストをインポートできます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ディレクトリリスト] の順にクリックします。
2. 1つ以上のリストをエクスポートするには、リストを選択し、[エクスポート]→[選択したアイテムをCSV形式でエクスポート]、または [エクスポート]→[選択したアイテムをXML形式でエクスポート] をクリックします。
3. すべてのリストをエクスポートするには、[エクスポート]→[CSV形式でエクスポート]、または [エクスポート]→[XML形式でエクスポート] をクリックします。
4. リストをインポートするには、[新規]→[ファイルからインポート] をクリックし、ウィザードの指示に従います。

ディレクトリリストを使用するポリシーを表示

ディレクトリリストを使用するポリシーを確認すると、変更によって影響を受けるポリシーを把握できるので便利です。たとえば、ポリシーによって使用されていないことを確認してから、ディレクトリリストを削除できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ディレクトリリスト] の順にクリックします。
2. ディレクトリリストを選択し、[プロパティ] をクリックします。
3. [割り当て対象] タブをクリックします。

ポリシーで使用するファイル拡張子リストの作成

複数の不正プログラム検索設定で使用できるように、ファイル拡張子のリストを作成します。異なるルールごとに作成された複数の同じリストよりも、単一のリストの方が容易に管理できます。たとえば、検索に含めるファイルとして、あるファイル拡張子リストを複数の不正プログラム検索設定で使用できます。また、検索から除外するファイルとして、別のファイル拡張子リストを複数の不正プログラム検索設定で使用できます。

ヒント: 既存のリストに類似するファイル拡張子リストを作成するには、既存のリストを複製して編集します。

テキストの先頭にナンバー記号 (「#」) を付けたコメントをリストに挿入できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ファイル拡張子リスト] の順にクリックします。
2. [新規]→[新規ファイル拡張子リスト] の順にクリックします。
3. 名前を入力し、必要に応じて説明を入力します。
4. [ファイル拡張子] リストで、拡張子を1行に1つずつ追加します。
5. [OK] をクリックします。

ファイル拡張子リストをインポート/エクスポートする

1つ以上のファイル拡張子リストをXMLファイルまたはCSVファイルにエクスポートできます。また、XMLファイルからリストをインポートできます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ファイル拡張子リスト] の順にクリックします。
2. 1つ以上のリストをエクスポートするには、リストを選択し、[エクスポート]→[選択したアイテムをCSV形式でエクスポート]、または [エクスポート]→[選択したアイテムをXML形式でエクスポート] をクリックします。
3. すべてのリストをエクスポートするには、[エクスポート]→[CSV形式でエクスポート]、または [エクスポート]→[XML形式でエクスポート] をクリックします。
4. リストをインポートするには、[新規]→[ファイルからインポート] をクリックし、ウィザードの指示に従います。

ファイル拡張子リストを使用する不正プログラム検索設定を確認する

ファイル拡張子リストを使用する不正プログラム検索設定を確認すると、変更によって影響を受けるルールを把握できるので便利です。たとえば、検索設定によって使用されていないことを確認してから、ファイル拡張子リストを削除できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ファイル拡張子リスト] の順にクリックします。
2. リストを選択し、[プロパティ] をクリックします。

3. [割り当て対象] タブをクリックします。

ポリシーで使用するファイルリストの作成

複数のポリシーで使用するファイルパスのリストを作成します。単一のリストは、異なるポリシーでそれぞれ作成された複数の同一リストを管理するよりも簡単です。これらのリストの最も一般的な使用例は、不正プログラム対策スキャンの対象ファイルの追加または除外です。詳細については、"検索対象ファイルを指定する" on page 838を参照してください。

既存のリストに類似するファイルリストを作成するには、既存のリストを複製して編集します。

次の表は、ファイルリスト項目を定義するための構文を示しています。スラッシュとバックスラッシュの使用は、WindowsとLinuxの両方の規則でサポートされています。

対象	形式	説明	例
ファイル	FILE	場所やディレクトリに関係なく、指定したファイル名を持つすべてのファイルを含めます。	*abc.doc* すべてのディレクトリにある"abc.doc"という名前のすべてのファイルが含まれます。abc.exeは含まれません。
ファイルパス	FILEPATH	ファイルパスで指定された単一のファイルを含めます。	*C:\Documents\abc.doc* Documentsディレクトリのabc.docという名前のファイルのみ含めます。
ワイルドカード(*)を使用したファイルパス	FILEPATH	ファイルパスで指定されたすべてのファイルを除外します。	*C:\Documents\abc.co** (Windowsエージェントプラットフォームのみ) Documentsディレクトリにある、ファイル名がabcで拡張子が.coで始まるファイルを除外します。
ファイル名がワイルドカード(*)	FILEPATH*	パス配下のすべてのファイルを除外しますが、指定されていないサブディレクトリ内のファイルは含まれません。	*C:\Documents** ディレクトリC:\Documents\以下のすべてのファイルを除外します *C:\Documents\SubDirName*** フォルダ名がSubDirNameで始まるサブディレクトリ内のすべてのファイルを除外します。C:\Documents\または他のサブディレクトリ以下のすべてのファイルは除外しません。 *C:\Documents*** C:\Documents以下のすべてのdirectサブディレクトリ内のすべてのファイルを除外します。後続のサブディレクトリ内のファイルは除外しません。

対象	形式	説明	例
ワイルドカード(*)を使用したファイル	FILE*	パターンに一致するファイル名を持つすべてのファイルを含めます。	*abc*.exe* abcのプレフィックスと.exeの拡張子を持つファイルを含みます。 **.db* *一致する:* 123.db abc.db *一致しない:* 123db 123.abd cbc.dba **db* *一致する:* 123.db 123db ac.db acdb db *一致しない:* db123 *wxy*.db* *一致する:* wxy.db wxy123.db *一致しない:* wxydb
ワイルドカード(*)を使用したファイル	FILE.EXT*	パターンに一致するファイルの拡張子を持つすべてのファイルを含めます。	*abc.v** ファイル名が"abc"で拡張子が.vで始まるファイルを含みます。 *abc.*pp* *一致する:* abc.pp abc.app *一致しない:* wxy.app *abc.a*p* *一致する:* abc.ap abc.a123p *一致しない:* abc.pp

対象	形式	説明	例
			*abc.** *一致する:* abc.123 abc.xyz *一致しない:* wxy.123
ワイルドカード(*)を使用したファイル	FILE*.EXT*	パターンに一致するファイル名と拡張子を持つすべてのファイルを含めます。	*a*c.a*p* 対象: ac.ap a123c.ap ac.a456p a123c.a456p 対象外: ad.aa
環境変数	${ENV VAR}	環境変数 ${ENV VAR} の形式で指定されたファイルを含みます。windir、programfilesなどの Windows の一般的な環境変数がサポートされています。 Virtual Appliance および Linux の場合、環境変数の値のペアはポリシーまたはコンピュータエディタ> 設定 > 一般 > 環境変数オーバーライドで定義する必要があります	${myDBFile} myDBFileファイルを含めます。
コメント	FILEPATH #コメント	対象の定義にコメントを追加できます。	*C:\Documents\abc.doc #これはコメントです*

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ファイルリスト] の順にクリックします。
2. [新規]→[新規ファイルリスト] の順にクリックします。
3. 名前を入力し、必要に応じて説明を入力します。
4. [ファイル] リストで、ファイルパスを1行に1つずつ追加します。
5. [OK] をクリックします。

ファイルリストをインポート/エクスポートする

1つ以上のファイルリストをXMLファイルまたはCSVファイルにエクスポートできます。また、XMLファイルからリストをインポートできます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ファイルリスト] の順にクリックします。
2. 1つ以上のリストをエクスポートするには、リストを選択し、[エクスポート]→[選択したアイテムをCSV形式でエクスポート]、または [エクスポート]→[選択したアイテムをXML形式でエクスポート] をクリックします。
3. すべてのリストをエクスポートするには、[エクスポート]→[CSV形式でエクスポート]、または [エクスポート]→[XML形式でエクスポート] をクリックします。
4. リストをインポートするには、[新規]→[ファイルからインポート] をクリックし、ウィザードの指示に従います。

ファイルリストを使用するポリシーを確認する

ファイルリストを使用するポリシーを確認すると、変更によって影響を受けるポリシーを把握できるので便利です。たとえば、ポリシーによって使用されていないことを確認してから、ファイルリストを削除できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ファイルリスト] の順にクリックします。
2. ファイルリストを選択し、[プロパティ] をクリックします。
3. [割り当て対象] タブをクリックします。

ポリシーで使用するIPアドレスリストの作成

複数のファイアウォールルールで使用できるように、IPアドレスのリストを作成します。異なるルールごとに定義された複数の同じリストよりも、単一のリストの方が容易に管理できます。

ヒント: 既存のリストに類似するIPリストを作成するには、既存のリストを複製して編集します。

個々のIPアドレスだけでなく、IP範囲とマスクされているIPも入力できます。テキストの先頭にナンバー記号 (「#」) を付けたコメントもIPリストに挿入できます。

マスクされているIPの例は、192.168.0/24、192.168.2.0/255.255.255.0、IPV6の場合は2001:0DB8::CD30:0:0:0:0/ffff:ffff:fff0::です。IP範囲の例は、192.168.0.2 - 192.168.0.125、IPV6の場合はFF01::101 - FF01::102です。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト] の順にクリックします。
2. [新規]→[新規IPリスト] の順にクリックします。
3. 名前を入力し、必要に応じて説明を入力します。
4. [IP] リストで、IPアドレス、マスクされたIPアドレス、またはIP範囲 (1行ごとに1つ) を追加します。
5. [OK] をクリックします。

IPリストをインポート/エクスポートする

1つ以上のIPリストをXMLファイルまたはCSVファイルにエクスポートできます。また、XMLファイルからリストをインポートできます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト] の順にクリックします。
2. 1つ以上のリストをエクスポートするには、リストを選択し、[エクスポート]→[選択したアイテムをCSV形式でエクスポート]、または [エクスポート]→[選択したアイテムをXML形式でエクスポート] をクリックします。
3. すべてのリストをエクスポートするには、[エクスポート]→[CSV形式でエクスポート]、または [エクスポート]→[XML形式でエクスポート] をクリックします。

4. リストをインポートするには、[新規]→[ファイルからインポート] をクリックし、ウィザードの指示に従います。

IPリストを使用するルールを確認する

IPリストを使用するファイアウォールルールを確認すると、変更によって影響を受けるルールを把握できるので便利です。たとえば、ファイアウォールルールによって使用されていないことを確認してから、IPリストを削除できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト] の順にクリックします。
2. IPリストを選択し、[プロパティ] をクリックします。
3. [割り当て対象] タブをクリックします。

ポリシーで使用するポートリストの作成

複数のルールで使用できるように、ポート番号のリストを作成します。異なるルールごとに作成された複数の同じリストよりも、単一のリストの方が容易に管理できます。

ヒント: 既存のリストに類似するポートリストを作成するには、既存のリストを複製して編集します。

個々のポートおよびポート範囲をリストに含めることができます (例: 80、20-21)。テキストの先頭にナンバー記号 (「#」) を付けたコメントをポートリストに挿入できます。

注意: 一般的に受け入れられているポート番号割り当てのリストについては、Internet Assigned Numbers Authority (IANA) を参照してください。Deep Security Manager、Relay、またはAgentで使用されるポート番号のリストについては、"ポート番号、URL、およびIPアドレス" on page 428を参照してください。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ポートリスト] の順にクリックします。
2. [新規]→[新規ポートリスト] の順にクリックします。
3. 名前を入力し、必要に応じて説明を入力します。
4. [ポート] リストで、ポート番号を1行に1つずつ追加します。
5. [OK] をクリックします。

ポートリストをインポート/エクスポートする

1つ以上のポートリストをXMLファイルまたはCSVファイルにエクスポートできます。また、XMLファイルからリストをインポートできます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ポートリスト] の順にクリックします。
2. 1つ以上のリストをエクスポートするには、リストを選択し、[エクスポート]→[選択したアイテムをCSV形式でエクスポート]、または [エクスポート]→[選択したアイテムをXML形式でエクスポート] をクリックします。
3. すべてのリストをエクスポートするには、[エクスポート]→[CSV形式でエクスポート]、または [エクスポート]→[XML形式でエクスポート] をクリックします。
4. リストをインポートするには、[新規]→[ファイルからインポート] をクリックし、ウィザードの指示に従います。

ポートリストを使用するルールを確認する

ポートリストを使用するルールを確認すると、変更によって影響を受けるルールを把握できるので便利です。たとえば、ルールによって使用されていないことを確認してから、ポートリストを削除できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ポートリスト] の順にクリックします。
2. ポートリストを選択し、[プロパティ] をクリックします。
3. [割り当て対象] タブをクリックします。

ポリシーで使用するMACアドレスリストの作成

複数のポリシーで使用できるように、MACアドレスのリストを作成します。異なるポリシーごとに作成された複数の同じリストよりも、単一のリストの方が容易に管理できます。

ヒント: 既存のリストに類似するMACリストを作成するには、既存のリストを複製して編集します。

MACリストは、ハイフン区切りおよびコロン区切り両方の形式のMACアドレスをサポートしています (例: 0A-0F-FF-F0-A0-AF、0A:0F:FF:F0:A0:AF)。テキストの先頭にナンバー記号 (「#」) を付けたコメントをMACリストに挿入できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[MACリスト] の順にクリックします。
2. [新規]→[新規MACリスト] の順にクリックします。
3. 名前を入力し、必要に応じて説明を入力します。
4. [MAC] リストで、MACアドレスを1行に1つずつ追加します。
5. [OK] をクリックします。

MACリストをインポート/エクスポートする

1つ以上のMACリストをXMLファイルまたはCSVファイルにエクスポートできます。また、XMLファイルからリストをインポートできます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[MACリスト] の順にクリックします。
2. 1つ以上のリストをエクスポートするには、リストを選択し、[エクスポート]→[選択したアイテムをCSV形式でエクスポート]、または [エクスポート]→[選択したアイテムをXML形式でエクスポート] をクリックします。
3. すべてのリストをエクスポートするには、[エクスポート]→[CSV形式でエクスポート]、または [エクスポート]→[XML形式でエクスポート] をクリックします。
4. リストをインポートするには、[新規]→[ファイルからインポート] をクリックし、ウィザードの指示に従います。

MACリストを使用するポリシーを確認する

MACリストを使用するポリシーを確認すると、変更によって影響を受けるポリシーを把握できるので便利です。たとえば、ポリシーによって使用されていないことを確認してから、MACリストを削除できます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[MACリスト] の順にクリックします。
2. MACリストを選択し、[プロパティ] をクリックします。
3. [割り当て対象] タブをクリックします。

ポリシーで使用するコンテキストの定義

コンテキストは、コンピュータのネットワーク環境に応じてさまざまなセキュリティポリシーを実装する有効な方法です。

コンテキストは、ファイアウォールルールおよび侵入防御ルールと関連付けられるよう設計されています。ルールに関連付けられたコンテキストの定義条件に一致した場合、ルールは適用されます。

コンピュータがインターネットに接続されているかどうかを判別するオプションを設定する

1. Deep Security Managerで、[管理]→[システム設定]→[コンテキスト]の順に選択します。
2. [インターネットの接続テスト用URL] ボックスに、インターネットの接続をテストするために送信されるHTTP要求の宛先URLを入力します(「http://」を含める)。
3. [接続確認用の応答コンテンツの正規表現] ボックスに、HTTP通信が成功したことを確認する応答コンテンツに適用する正規表現を入力します(応答コンテンツがわかっている場合は、単純な文字列を使用できます)。
4. [テスト間隔] リストで、接続テストの間隔を選択します。

たとえば、インターネット接続をテストするには、「http://www.example.com」というURLと、そのURLのサーバから返される「This domain is established to be used for illustrative examples in documents」という文字列を使用できます。

コンテキストを定義する

1. Deep Security Managerで、[Policies]→[Common Objects]→[Other]→[Contexts]の順に選択し、[New]→[New Context]の順にクリックします。
2. [一般情報] エリアで、コンテキストルールの名前と説明を入力します。また、ルールに対応するDeep Security Agentの最も古いバージョンも表示されます。
3. [オプション] エリアで、コンテキストが適用されるタイミングを指定します。
   - 接続が次の場合にコンテキストを適用: このオプションは、コンピュータがドメインコントローラに接続する場合、またはインターネット接続に接続する場合、ファイアウォールルールを有効にするかどうかを決定します。インターネット接続テストの条件は [管理]→[システム設定]→[コンテキスト] で設定できます。

     ドメインコントローラへICMP経由で直接接続できる場合は、「ローカル」接続になります。VPN経由でのみ接続できる場合は、「リモート」接続になります。

     ドメインコントローラ接続のテスト間隔はインターネット接続のテスト間隔と同じで、[管理]→[システム設定]→[コンテキスト] で設定できます。インターネット接続テストは、コンピュータがドメインコントローラに接続できない場合にのみ実行されます。

   - コンテキストをインタフェース制限に適用: このコンテキストは、インタフェース制限のためにトラフィックが制限されているネットワークインタフェースに適用されます。これは主に「許可」または「強制的に許可」ファイアウォールルールで使用されます。"コンピュータで使用可能なインタフェースの検出と設定" on page 739を参照してください。

コンテキストをルールに割り当てると、コンテキストの [割り当て対象] タブにそのルールが表示されます(コンテキストにセキュリティルールを関連付けるには、セキュリティルールの [プロパティ] 画面の [オプション] タブに移動し、[コンテキスト] リストからコンテキストを選択します)。

ステートフルファイアウォールの設定の定義

Deep Securityのステートフルなファイアウォール設定メカニズムは、トラフィック履歴、TCPおよびIPヘッダ値の正確さ、およびTCP接続状態の遷移のコンテキストで各パケットを分析します。UDPやICMPなどのステートレスプロトコルの場合、履歴トラフィック分析に基づいた擬似ステートフルメカニズムが実装されます。パケットは、ステートフルメカニズムによって次のように処理されます。

1. 静的ファイアウォールルール条件によってパケットの通過が許可された場合、パケットはステートフルルーチンに渡されます。
2. パケットを調べて、既存の接続に属しているかどうかが判断されます。
3. TCPヘッダの正当性 (シーケンス番号、フラグの組み合わせなど) が調査されます。

新しいステートフル設定を作成するには、次の手順に従います。

1. "ステートフル設定を追加する" below
2. "ステートフル設定情報を入力する" below。
3. "パケットインスペクションオプションを選択する" below。

ステートフル設定の後は、次の操作について説明します。

- "ステートフル設定が割り当てられたポリシーとコンピュータを表示する" on page 820
- "ステートフル設定をエクスポートする" on page 820
- "ステートフル設定を削除する" on page 820

ステートフル設定を追加する

[ポリシー]→[共通オブジェクト]→[その他]→[ファイアウォールステートフル設定] でステートフル設定を定義する方法には次の3つがあります。

- 新しい設定を作成します。[新規]→[新規ファイアウォールステートフル設定] の順にクリックします。
- XMLファイルから設定をインポートします。[新規]→[ファイルからインポート] をクリックします。
- 既存の設定をコピーして変更します。[ファイアウォールステートフル設定] リストの設定を右クリックして、[複製] をクリックします。新しい設定を編集するには、その設定を選択し、[プロパティ] をクリックします。

ステートフル設定情報を入力する

設定の [名前] と[説明] を入力します。

パケットインスペクションオプションを選択する

IP、TCP、UDPおよびICMPパケットインスペクションのオプションを定義し、アクティブまたはパッシブFTPを有効化できます。

IPパケットインスペクション

[一般] タブで [フラグメント化されたすべての受信パケットを拒否する] を選択し、フラグメント化されたパケットをすべて破棄します。破棄されたパケットはフラグメント化分析をバイパスして、「IP fragmented packet」というログエントリが生成されます。全長がIPヘッダの長さよりも短いパケットはログに記録されずに破棄されます。

警告: 攻撃者は、ファイアウォールルールをバイパスするために、フラグメント化されたパケットを作成して送信する場合があります。

注意: 初期設定では、ファイアウォールエンジンは、フラグメント化されたパケットに対して一連のチェックを実行します。これは初期設定の動作で、変更することはできません。次のような特徴を持つパケットは、破棄されます。

- フラグメントのフラグ/オフセットが無効: IPヘッダ内のDFフラグまたはMFフラグのいずれかが1に設定されている、またはヘッダ内に含まれるDFフラグが1に設定されており、オフセット値が0以外に設定されているとき、パケットは破棄されます。
- 最初のフラグメントが最小サイズ未満: MFフラグが1に設定されていて、オフセット値が0、合計の長さが (最大組み合わせヘッダ長である) 120バイトよりも短い場合、パケットは破棄されます。
- IPフラグメントが範囲を超えている: 合計パケット長と組み合わされたオフセットフラグの値が最大データグラム長である65,535バイトを超えた場合、パケットは破棄されます。
- IPフラグメントのオフセットが小さすぎる: 60バイトよりも小さい値を持つ0以外のオフセットフラグがある場合、パケットは破棄されます。

TCPパケットインスペクション

[TCP] タブで有効化するオプションを次の中から選択します。

- CWR、ECEフラグを含むTCPパケットを拒否する: これらのフラグは、ネットワーク輻輳時に設定されます。

  注意: RFC 3168では、ECN (Explicit Congestion Notification) に使用する予約済みフィールドの6ビットのうち2ビットを、次のように定義しています。
  - ビット8から15: CWR-ECE-URG-ACK-PSH-RST-SYN-FIN
  - TCPヘッダフラグのビット名参照:
    - ビット8: CWR (Congestion Window Reduced) [RFC3168]
    - ビット9: ECE (ECN-Echo) [RFC3168]

  警告: パケットの自動転送 (特にDoS攻撃によって生成されたものなど) によって、これらのフラグが設定されたパケットが作成されることがよくあります。

- TCPステートフルインスペクションを有効にする: TCPレベルでのステートフルインスペクションを有効にします。ステートフルTCPインスペクションを有効にすると、次のオプションが利用可能です。
  - TCPステートフルログを有効にする: TCPステートフルインスペクションイベントがログに記録されます。

- 単一コンピュータからの受信接続数の上限: 単一コンピュータからの接続数を制限すると、DoS攻撃の影響を低減できます。
- 単一コンピュータへの送信接続数の上限: 単一コンピュータへの送信接続数を制限すると、Nimdaなどのワームの影響を大幅に低減できます。
- 単一コンピュータからのハーフオープン接続数の上限: この制限を設定すると、SYNフラッドなどのDoS攻撃から保護できます。ほとんどのサーバでは、ハーフオープン接続を終了するためにタイムアウトが設定されています。この値を設定することにより、ハーフオープン接続が重大な問題にならないようにします。SYN-SENT (リモート) エントリが指定された制限に達した場合、その特定のコンピュータからの後続のTCPパケットは破棄されます。

  注意: 単一コンピュータからのオープン接続を許可する数を決定する際に、使用している種類のプロトコルで妥当と考えられる単一コンピュータからのハーフオープン接続数と、輻輳を引き起こすことなくシステムが維持できる単一コンピュータからのハーフオープン接続数との間の数を選択します。

- すでに確認されたパケット数が次を超過したときにACKストーム防御を有効にする: このオプションを設定して、ACKストーム攻撃が発生した場合のイベントを記録します。
  - ACKストームが検出されたときに接続を中断する: このオプションを設定して、攻撃が検出された場合に接続を切断するようにします。

  注意: ACKストーム保護オプションはDeep Security Agent 8.0以前でのみ使用可能です。

FTPオプション

[FTPオプション] タブで次のオプションを有効化できます。

注意: 以下のFTPオプションはDeep Security Agent 8.0以前で使用可能です。

- アクティブFTP
  - 受信を許可する: このコンピュータがサーバとして動作しているときにアクティブFTPを許可します。
  - 送信を許可する: このコンピュータがクライアントとして動作しているときにアクティブFTPを許可します。
- パッシブFTP
  - 受信を許可する: このコンピュータがサーバとして動作しているときにパッシブFTPを許可します。

- 送信を許可する: このコンピュータがクライアントとして動作しているときにパッシブFTPを許可します。

UDPパケットインスペクション

[UDP] タブで次のオプションを有効化できます。

- UDPステートフルインスペクションを有効にする: UDPトラフィックのステートフルインスペクションを有効にする場合はオンにします。

  注意: UDPステートフル機能は、未承諾の受信UDPパケットを破棄します。送信UDPパケットごとに、ルールがそのUDP「ステートフル」テーブルをアップデートし、要求に対して60秒以内にUDP応答が発生した場合のみ、UDP応答を許可します。特定の受信UDPトラフィックを許可する場合は、強制的に許可ルールを作成する必要があります。たとえば、DNSサーバを実行している場合、送信先のポート53に受信UDPパケットを許可するには、強制的に許可ルールを作成する必要があります。

  警告: UDPトラフィックのステートフルインスペクションがない場合、攻撃者はDNSサーバになりすまして、未承諾のUDP「応答」を送信元のポート53からファイアウォールの内側にあるコンピュータに送信する可能性があります。

  - UDPステートフルログを有効にする: このオプションを選択すると、UDPステートフルインスペクションイベントのログを記録できるようになります。

ICMPパケットインスペクション

[ICMP] タブで次のオプションを有効にできます。

注意: ICMPステートフルインスペクションは、Deep Security Agent 8.0以前で使用できます。

- ICMPステートフルインスペクションを有効にする: ICMPトラフィックのステートフルインスペクションを有効にする場合はオンにします。

  注意: ICMP (擬似) ステートフル機能は、未承諾の受信ICMPパケットを破棄します。送信ICMPパケットごとに、ルールがそのICMP「ステートフル」テーブルを作成またはアップデートし、要求に対して60秒以内にICMP応答が発生した場合のみ、ICMP応答を許可します(サポートするICMPペアの種類は、タイプ0と8、13と14、15と16、17と18です)。

警告: たとえば、ステートフルICMPインスペクションを有効にすると、エコー要求が送信された場合にICMPエコー応答を許可できます。要求されていないエコー応答は、Smurf増幅攻撃、マスターとデーモン間のトライブフラッドネットワーク通信、Loki2バックドアなど、さまざまな種類の攻撃の予兆である可能性があります。

- ICMPステートフルログを有効にする: このオプションを選択すると、ICMPステートフルインスペクションイベントのログを記録できるようになります。

ステートフル設定をエクスポートする

[エクスポート] をクリックし、リストから該当するエクスポート処理を選択すると、すべてのステートフル設定を.csvまたは.xmlファイルにエクスポートできます。ステートフル設定を選択し、[エクスポート] をクリックして、リストから該当するエクスポート処理を選択すると、特定のステートフル設定をエクスポートすることもできます。

ステートフル設定を削除する

ステートフル設定を削除するには、[ファイアウォールステートフル設定] リスト内の設定を右クリックして、[削除] をクリックした後、[OK] をクリックします。

注意: 1台以上のコンピュータに割り当てられたステートフル設定、またはポリシーの一部であるステートフル設定は削除できません。

ステートフル設定が割り当てられたポリシーとコンピュータを表示する

ステートフルインスペクション設定に割り当てられたポリシーとコンピュータは、[割り当て対象] タブに表示できます。リスト内のポリシーまたはコンピュータをクリックすると、そのプロパティが表示されます。

ルールに適用するスケジュールの定義

スケジュールは、ルール、Agentのアップグレードなどに割り当てることのできる再利用可能なタイムテーブルです。

1. Deep Security Managerで、[Policies]→[Common Objects]→[Other]→[Schedules]の順に選択します。
2. [新規]→[新規スケジュール] の順にクリックします。
3. [一般情報] エリアで、スケジュールを識別するための名前と説明を入力します。
4. グリッドからある時間枠をクリックするとその時間枠が選択されます。選択を解除するには、Shiftキーを押しながらその時間枠をクリックします。スケジュール期間は、1時間の時間枠で定義します。

スケジュールをルールに割り当てると、スケジュールの [割り当て対象] タブにそのルールが表示されます スケジュールにセキュリティルールを関連付けるには、セキュリティルールの [プロパティ] 画面の [オプション] タブに移動し、[スケジュール] リストからスケジュールを選択します。

注意: Agentベースの保護では、スケジュールで保護対象のコンピュータのOSと同じタイムゾーンが使用されます。Agentレスによる保護では、Deep Security Virtual Applianceと同じタイムゾーンが使用されます。

保護モジュールの設定

不正プログラム対策を設定する

不正プログラム対策について

ヒント: 不正プログラム対策機能の紹介や推奨設定方法についての情報は、次のWebサイトでまとめて確認できます。環境の構築を始める前に参照すると、動作不調のリスク軽減および安定性の向上に役立てることができます。
https://success.trendmicro.com/dcx/s/solution/000286756?language=ja

Deep Security不正プログラム対策モジュールには、不正プログラム、ウイルス、トロイの木馬、スパイウェアなどのファイルベースの脅威からリアルタイムに保護する機能と、管理者の要求に応じて保護する機能があります。この不正プログラム対策モジュールでは、脅威を特定するために、ローカルハードドライブ上のファイルを包括的な脅威データベースに対して照合します。また、圧縮や既知の攻撃コードなど、特定の特性がないかについても確認します。

脅威データベースの一部はトレンドマイクロのサーバ上にホストされているか、ローカルでパターンとして保存されています。Deep Security Agentは、最新の脅威から保護するために、定期的に不正プログラム対策パターンファイルとアップデートをダウンロードします。

注意: Deep Security Agentを新規にインストールした場合、アップデートサーバに接続して不正プログラム対策パターンファイルとアップデートをダウンロードするまで、不正プログラム対策保護は有効になりません。Deep Security Agentのインストール後に、Deep Security Relayまたはトレンドマイクロのアップデートサーバと通信できることを確認してください。

不正プログラム対策モジュールでは、脅威を排除しつつ、システムパフォーマンスへの影響は最小限に抑えます。不正なファイルは、駆除、削除、または隔離できます。特定した脅威に関連付けられているプロセスを終了したり、他のシステムオブジェクトを削除することもできます。

不正プログラム対策モジュールをオンにして設定するには、"不正プログラム対策を有効化して設定する" on page 828を参照してください。

- "不正プログラム検索の種類" below
- "不正プログラム検索設定" on page 824
- "不正プログラムイベント" on page 824
- "スマートスキャン" on page 824
- "機械学習型検索" on page 825
- "脅威インテリジェンス" on page 825
- "不正プログラム検索の種類" below

不正プログラム検索の種類

不正プログラム対策モジュールでは、さまざまな種類の検索を実行します。"実行するスキャンの種類を選択" on page 829も参照してください。

リアルタイム検索

受信、開く、ダウンロード、コピー、編集などの処理が行われるたびに、そのファイルにセキュリティ上のリスクがないかどうかが検索されます。セキュリティ上のリスクが検出されなかった場合、ファイルは現在の場所にそのまま残され、ユーザはファイルにアクセスできます。セキュリティ上のリスクが検出された場合、感染ファイルの名前と具体的なセキュリティ上のリスクの内容を示す通知メッセージが表示されます。

リアルタイム検索は、[スケジュール] オプションで別の期間を設定した場合を除き、継続的に有効になります。

> ヒント: リアルタイム検索は、ファイルサーバでファイルのバックアップが予約されているときなど、パフォーマンスへの影響が大きいときを避けて実行するように設定できます。

この検索は、不正プログラム対策モジュールでサポートされるすべてのプラットフォームで実行できます。

手動検索

コンピュータ上のすべてのプロセスとファイルを対象にフルシステム検索が実行されます。検索に要する時間は、検索するファイル数と、コンピュータのハードウェアリソースに応じて異なります。手動検索はク

イック検索より時間がかかります。

手動検索は、[不正プログラムのフル検索] をクリックしたときに実行されます。

この検索は、不正プログラム対策モジュールでサポートされるすべてのプラットフォームで実行できます。

予約検索

設定した日時に自動的に実行されます。予約検索を使用して日々の検索を自動化することで、検索をより効率的に管理できます。

予約検索は、予約タスク("Deep Security予約タスクの設定" on page 1826を参照) を使用して [コンピュータの不正プログラムを検索] タスクを作成したときに指定した日時に実行されます。

この検索は、不正プログラム対策モジュールでサポートされるすべてのプラットフォームで実行できます。

クイック検索

コンピュータの重大なシステム領域で、現在アクティブな脅威の検索のみが実行されます。クイック検索では、現在アクティブな不正プログラムが検索されますが、活動のない、または保存されている感染ファイルを検索するためにファイルが詳細に検索されることはありません。大容量のドライブでは、フル検索よりも短時間で終了します。クイック検索は設定できません。

クイック検索は、[不正プログラムのクイック検索] をクリックしたときに実行されます。

注意: クイック検索を実行できるのは、Windowsコンピュータのみです。

検索されるオブジェクトと順序

次の表は、検索の種類ごとに、検索されるオブジェクトと検索の順序を示しています。

対象	フル検索 (手動または予約)	クイック検索
ドライバ	1	1
トロイの木馬	2	2
プロセスイメージ	3	3
メモリ	4	4
ブートセクタ	5	-
ファイル	6	5

対象	フル検索 (手動または予約)	クイック検索
スパイウェア	7	6

不正プログラム検索設定

不正プログラム検索設定は、不正プログラム検索の動作を制御する一連のオプションです。ポリシーを使用して不正プログラム対策を設定したり、特定のコンピュータに対して不正プログラム対策を設定するときは、使用する不正プログラム検索設定を選択します。不正プログラム検索設定は複数作成でき、コンピュータグループによって検索要件が異なる場合はポリシーの異なる設定を使用できます。

リアルタイム検索、手動検索、および予約検索では、すべて不正プログラム検索設定を使用します。Deep Securityは、検索の種類ごとに初期設定の不正プログラム検索の設定を提供します。これらの検索設定は、セキュリティポリシーの初期設定に使用されます。検索の初期設定をそのまま使用することも、変更することも、独自の設定を作成することもできます。

注意: クイック検索は設定できないため、不正プログラム検索設定を使用しません。

検索の対象または対象外となるファイルやディレクトリ、またコンピュータで不正プログラムが検出された場合の処理 (駆除、隔離、削除など) を指定できます。

詳細については、"不正プログラム検索と除外の設定" on page 832を参照してください。

不正プログラムイベント

Deep Securityが不正プログラムを検出すると、イベントログにイベントが記録されます。イベントログでは、イベントに関する情報を確認したり、誤判定の場合のファイルの例外を作成したりできます。また、実際には安全なファイルを復元することもできます。

詳細については、次のセクションを参照してください。

- "不正プログラム対策イベント" on page 1402
- "検出した不正プログラムの確認と復元" on page 884
- "高度な攻撃コードの除外を設定する" on page 891

スマートスキャン

スマートスキャンでは、トレンドマイクロのサーバに保存されている脅威シグニチャが使用されます。スマートスキャンには次のメリットがあります。

- セキュリティステータスの検索をクラウドベースで高速かつリアルタイムに実行
- 脅威からの保護にかかる合計時間を削減
- パターンファイルのアップデート時に使用されるネットワーク帯域幅を削減 (パターン定義のアップデートの大半は、クラウドで保持され、多数のコンピュータへの配信は不要)
- 企業全体へのパターン展開のコストとオーバーヘッドを削減
- コンピュータにおけるカーネルのメモリ消費を削減 (メモリ消費量の増加を最小限に抑制)

スマートスキャンを使用すると、まず、ローカルで保持しているパターンファイルにより検索が行われます。そこでファイルの危険性を評価できなかった場合は、ローカルのSmart Protection Serverに接続します。ローカルのSmart Protection Serverでも危険性を評価できなかった場合は、トレンドマイクロのGlobal Smart Protectionサービスに接続します。この機能の詳細については、"Deep Securityの Smart Protection" on page 881を参照してください。

機械学習型検索

Deep Securityは、機械学習型検索により、未知の脅威とゼロデイ攻撃に対する不正プログラム対策保護を強化します。トレンドマイクロの機械学習型検索では、デジタルDNAフィンガープリント、APIマッピング、その他のファイル機能を使用して、高度な機械学習技術により脅威情報を関連付け、詳細なファイル分析を実行することで新たなセキュリティリスクを検出します。

機械学習型検索は、フィッシングやスピアフィッシングなどの手法を用いた標的型攻撃によるセキュリティ侵害に対する保護に効果的です。これらのケースでは、特定の環境を標的に設計された不正プログラムが従来の不正プログラム検索の手法をすり抜ける場合があります。

Deep Securityはリアルタイムスキャン中に不明なファイルや感染率の低いファイルを検出すると、高度な脅威検索エンジン(ATSE)を使用してファイルを検索し、ファイルの機能を抽出します。このレポートは、Trend Micro Smart Protection Networkの機械学習型検索エンジンに送信されます。機械学習型検索は、不正プログラムモデリングを使用してサンプルを不正プログラムモデルと比較し、脅威の可能性スコアを割り当て、ファイルに含まれる可能性がある不正プログラムの種類を特定します。

ファイルが脅威として認識された場合、Deep Securityはファイルからの脅威の駆除、ファイルの隔離、またはファイルの削除を実行し、脅威がネットワーク全体に広がり続けることを防ぎます。

機械学習型検索の使用方法の詳細については、"機械学習型検索を使用した脅威の検出" on page 859を参照してください。

脅威インテリジェンス

脅威インテリジェンス(旧称「Connected Threat Defense」)は、Deep Securityとトレンドマイクロのサンドボックス技術との接続を確立することで、新たに出現した脅威に対する不正プログラム対策を強

化します。詳細については、「"脅威インテリジェンスを使用した新たな脅威の検出" on page 861」を参照してください。

不正プログラムの種類

不正プログラム対策モジュールは、多数のファイルベースの脅威から保護します。"特定の種類の不正プログラムを検索する" on page 835と"不正プログラムの処理を設定する" on page 846も参照してください。

ウイルス

ウイルスは、ファイルに不正コードを挿入することによって感染します。通常は、感染したファイルを開くと不正なコードが自動的に実行され、他のファイルを感染させるだけでなく、ペイロードが配信されます。次に、一般的なウイルスをいくつか示します。

- COMおよびEXE感染型ウイルス: 一般的に.COMや.EXEの拡張子が付いている、DOSおよびWindows実行可能ファイルに感染します。
- マクロウイルス: 不正マクロを挿入することで、Microsoft Officeファイルを感染させます。
- システム領域感染型ウイルス: OSを起動させるために必要な情報が格納されているハードディスクドライブの領域に感染します。

不正プログラム対策モジュールでは、感染ファイルを特定して駆除するために、さまざまな技術を使用しています。最もよく行われる方法は、ファイルの感染に使用される実際の不正コードを検出し、感染ファイルからこのコードを取り除くことです。その他にも、感染する可能性のあるファイルへの変更を規制する方法や、不審な変更が適用される場合にファイルをバックアップする方法などがあります。

トロイの木馬

一部の不正プログラムは、その他のファイルにコードを挿入することによって拡散する方法を採りません。代わりに別の方法を採ったり、別の影響を及ぼします。

- トロイの木馬: トロイの木馬の神話のように、ファイルを開いたときに実行されてシステムに感染する不正プログラムファイル。
- バックドア:ポート番号を開いて権限のないリモートユーザに感染システムへのアクセスを許可する不正プログラムアプリケーション。
- ワーム: ネットワークを使用してシステム間で伝播する不正プログラム。ワームは人目を引くメールメッセージ、インスタントメッセージ、または共有ファイルを介したソーシャルエンジニアリングを利用して伝播します。また、アクセス可能なネットワーク共有に自身をコピーし、脆弱性を突いて別のコンピュータに広がります。

- ネットワークウイルス: ファイルベースではない、メモリまたはパケット上のみに存在する不正プログラム。不正プログラム対策ではネットワークウイルスを検出または削除できません。
- ルートキット: OSのコンポーネントの呼び出しを操作するファイルベースの不正プログラム。監視やセキュリティソフトウェアなどのアプリケーションでは、ファイルのリスト作成や実行中のプロセスの特定など、非常に基本的な機能を呼び出す必要があります。これらの呼び出しを操作することによって、ルートキットは自身の存在や、その他の不正プログラムの存在を隠すことができます。

パッカー

パッカーは圧縮され暗号化された実行可能プログラムです。不正プログラムの作者は、検出を免れるために、既存の不正プログラムを何重にも圧縮または暗号化することがあります。不正プログラム対策は、実行可能ファイル内に不正プログラムに関連付けられた圧縮パターンがないか検索します。

スパイウェア/グレーウェア

スパイウェアおよびグレーウェアは、別のシステムに送信するための情報や、別のアプリケーションで収集された情報を収集するアプリケーションおよびコンポーネントです。スパイウェア/グレーウェアの検出では、不正と思われる動作だけでなく、リモート監視のような合法的な目的に使用されるアプリケーションまで検出されることがあります。スパイウェア/グレーウェアアプリケーションの中で、既知の不正プログラムチャネルを通して配布されるものなど、もともと不正な性質を帯びているものは、一般にスパイウェア/グレーウェアではなく「トロイの木馬」として検出されます。

スパイウェアおよびグレーウェアアプリケーションは、通常、次のように分類されます。

- スパイウェア: 個人情報を収集および送信する目的でコンピュータにインストールされたソフトウェア。
- ダイヤラー: 不正プログラムであるダイヤラーは、接続の設定先を変更して、ユーザの予期しない料金を発生させるように設計されています。ダイヤラーの中には、個人情報を送信したらり、不正プログラムソフトウェアをダウンロードしたりするものもあります。
- ハッキングツール: コンピュータシステムへの不正アクセスを支援するために設計されたプログラムまたはプログラムのセット。
- アドウェア: 広告を自動的に再生、表示、またはダウンロードするソフトウェアパッケージ。
- Cookie: Webブラウザによって保存されるテキストファイル。Cookieには認証情報やサイトの設定など、Webサイトに関するデータが含まれています。Cookieは実行可能ファイルではないため感染することはありませんが、スパイウェアとして使用される可能性があります。合法的なWebサイトから送信されたCookieも、不正な目的に使用されることがあります。
- キーロガー: ユーザのキー入力を記録して、パスワードやその他の秘密情報を盗むソフトウェア。キーロガーの中には、リモートシステムにログを送信するものがあります。

グレーウェアの定義

スパイウェアのようなアプリケーションの中には、押しつけがましい動作を示すものの、不正ではないとみなされるものがあります。たとえば、市販のリモート制御および監視アプリケーションの中には、システムイベントを追跡および収集して、これらのイベントに関する情報を別のシステムに送信するものがあります。システム管理者などのユーザが自ら、これらの合法的なアプリケーションをインストールしている場合があります。これらのアプリケーションを「グレーウェア」と言います。

不正プログラム対策モジュールでは、グレーウェアの不正使用を防止するためにグレーウェアを検出します。ただし、検出されたアプリケーションを「承認」して、実行を許可することができます。

Cookie

Cookieは、Webブラウザに保存されるテキストファイルで、HTTP要求のたびにWebサーバに返されます。Cookieには認証情報や設定が保存されていますが、感染サーバがからの持続型攻撃の場合、それらに紛れてSQLインジェクションやXSSなどの攻撃コードが含まれている可能性があります。

その他の脅威

その他の脅威は、どのタイプにも分類されない不正プログラムなどです。このカテゴリには、偽の通知を表示したり、画面の動作を操作したりする、一般に実害のないジョークプログラムが含まれます。

潜在的な不正プログラム

潜在的な不正プログラムとは、疑わしいが、特定の不正プログラムの変異形として分類できないファイルのことです。トレンドマイクロでは、ファイルの詳細な分析についてサポート担当者にお問い合わせいただくことをお勧めします。初期設定では、これらの検出がログに記録され、ファイルは保護された方法でトレンドマイクロに送信されて分析されます。

不正プログラム対策を設定する

不正プログラム対策を有効化して設定する

ヒント: 不正プログラム対策機能の紹介や推奨設定方法についての情報は、次のWebサイトでまとめて確認できます。環境の構築を始める前に参照すると、動作不調のリスク軽減および安定性の向上に役立てることができます。
https://success.trendmicro.com/dcx/s/solution/000286756?language=ja

Deep Security不正プログラム対策モジュールを使用するには、次の操作を行います。

1. "不正プログラム対策モジュールを有効にする" on the next page。
2. "実行するスキャンの種類を選択" on the next page。
3. "検索除外を設定する" on page 830

4. "複数の検索リストの除外と含める設定" on the next page
5. "最新の脅威についてDeep Securityを更新する" on page 831
6. "不正プログラム検索と除外の設定" on page 832で提供された情報を確認し、アンチ不正プログラム検索の動作を改善してください

ほとんどの不正プログラム対策設定は、各コンピュータごとに設定するか、複数のコンピュータに適用されるポリシー(例: すべてのWindows 2008サーバーに適用されるポリシー) で設定する必要があります。管理を効率化するために、可能な限りポリシー内で設定を構成してください (個別のコンピュータではなく)。詳細については、"ポリシー、継承、およびオーバーライド" on page 724を参照してください。

不正プログラム対策の設定によって、CPUとRAMの使用率は変化します。Deep Security Agentで不正プログラム対策のパフォーマンスを最適化するには、"不正プログラム対策のパフォーマンスを向上させる" on page 850を参照してください。

詳細については、"不正プログラム対策について" on page 821を参照してください。

不正プログラム対策モジュールを有効にする

1. [ポリシー] に移動します。
2. 不正プログラム対策を有効にしたいポリシーをダブルクリックしてください。
3. [不正プログラム対策]→[一般] の順に選択します。
4. [不正プログラム対策のステータス] で、[オン] を選択します。
5. [保存] をクリックします。

実行するスキャンの種類を選択

不正プログラム対策を有効にした場合、Deep Securityに実行すべきスキャンの種類を通知するには、次の手順を実行します ("不正プログラム検索の種類" on page 822を参照)。

1. [ポリシー] に移動します。
2. 設定するポリシーをダブルクリックします。
3. [不正プログラム対策]>[一般] の順にクリックします。
4. 検索の各種類を有効または無効にします。
   a. 初期設定を使用して検索を実行するには、[初期設定] を選択します。
   b. カスタマイズ可能な不正プログラム検索設定を使用して検索を実行するには、不正プログラム検索設定を選択します。
   c. 検索を無効にするには、不正プログラム検索設定で [設定なし] を選択します。
5. [保存] をクリックします。

トレンドマイクロは、すべての保護されたサーバーで毎週のスケジュールスキャンを実行するようにDeep Securityを設定することを推奨します。これはスケジュールタスクを使用して行うことができます。"Deep Security予約タスクの設定" on page 1826を参照してください。

検索除外を設定する

Deep Securityの不正プログラム検索では、検索時間を短縮してコンピューティングリソースの使用を最小限に抑えるために、すべての種類の検索から除外するフォルダ、ファイル、およびファイルの種類を指定することができます。また、Windowsサーバで実行するリアルタイムの不正プログラム検索からプロセスイメージファイルを除外することもできます。

これらの除外は、不正プログラム検索設定エディターの除外タブで除外リストを選択することによって指定されます。"検索対象ファイルを指定する" on page 838を参照してください。

Deep Securityの不正プログラム対策保護が有効になっているときにパフォーマンス関連の問題が発生した場合、特定のフォルダやファイルをスキャンから除外することで、これらの問題のトラブルシューティングを支援するために除外を使用できます。

複数の検索リストの除外と含める設定

不正プログラム検索設定のプロパティを使用して、特定のリストタイプのリストに対する検索の除外と含めを設定した後、追加の設定を行うことができます。つまり、Deep Securityでは、ポリシーレベルで複数の検索リストの除外と含めを設定できます。これは、不正プログラム検索設定で指定されたリストに拡張されます。複数の検索リストを使用する前に、不正プログラム検索設定で検索リストタイプのリストを有効にして設定する必要があることに注意してください。

すべてのディレクトリ設定は、ディレクトリリストをマルチリスト検索の対象から除外します。すべてのファイルおよびIntelliScanによって識別されるファイルタイプ設定は、ファイル拡張子リストをマルチリスト検索の対象から除外します。

1. ポリシーに移動します。
2. ポリシーをダブルクリックして設定します。
3. 不正プログラム対策 > 除外に移動します。
4. 除外を追加したい検索の種類を選択してください: リアルタイム、スケジュール、または手動。これらの検索タイプに対して次のリストを構成できます:
   a. ファイルリスト
   b. ディレクトリリスト
   c. ファイル拡張子リスト
   d. プロセスイメージファイルリスト(リアルタイム検索のみ)
5. リストを追加、作成、または削除するには、次の手順を実行してください。
   a. すべての継承リストを追加するには、継承リストを使用を選択してください。
   b. 非継承リストを追加するには、リストを選択して追加をクリックしてください。
   c. 新しいリストを作成するには、新規を選択します。詳細については、"ポリシーで使用するファイルリストの作成" on page 808を参照してください。

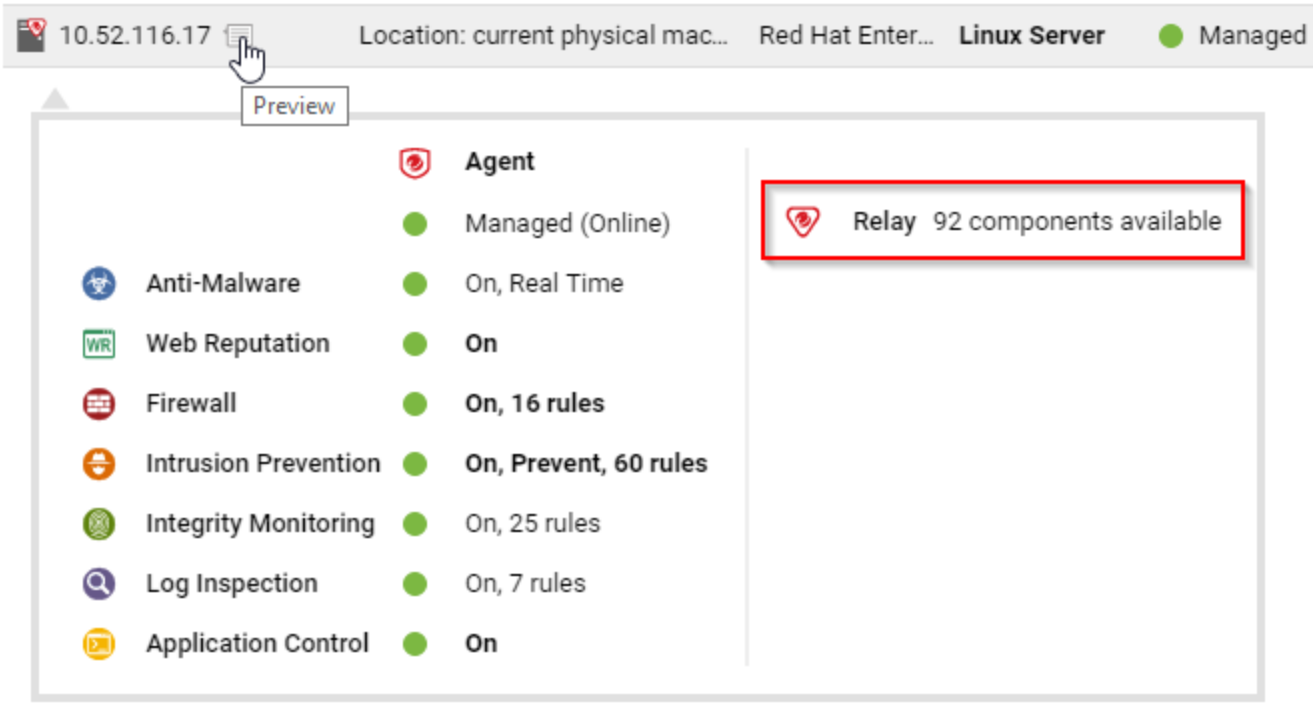
d. 非継承リストを削除するには、そのゴミ箱アイコンを選択します。継承リストを削除するには、継承リストを使用するの選択を解除する必要があります。
6. 保存をクリック。

完了すると、検索リストの包含または除外は、追加された検索リスト、コンピュータまたはポリシーからの追加されたファイルリスト、ディレクトリリスト、ファイル拡張子リストと組み合わされます。リスト間の重複は、包含と除外の動作に影響を与えません。

最新の脅威についてDeep Securityを更新する

新しいウイルスや不正利用に対して有効なままにするには、のDeep Securityエージェントは、独自のRelayから、間接的にトレンドマイクロやから最新のソフトウェアおよびセキュリティ更新プログラムパッケージをダウンロードできるようにする必要があります。これらのパッケージには、脅威の定義とパターンファイルが含まれています。トレンドマイクロからセキュリティアップデートを取得し、他のAgentおよびApplianceに配布する場合は、Relay有効化済みAgentを使用します。Relay有効化済みAgentを使用します。Relay有効化済みAgentはRelayグループに編成されていて、Relayグループの管理および設定はDeep Security Managerで行います。

1. [管理]→[システム設定]→[アップデート] の順に選択します。
2. Deep Securityがトレンドマイクロからセキュリティアップデートを取得できるように設定します。
   Relay有効化済みAgentが少なくとも1つあり、該当するAgentおよびApplianceに割り当てられていることを確認します。
   Deep Security AgentがRelayかどうかを判断するには、コンピュータの横の [プレビュー] をクリックします。



3. [管理]→[予約タスク]の順に選択します。
4. 利用可能なセキュリティアップデートとソフトウェアアップデートの両方を定期的にダウンロードする予約タスクがあることを確認します。

不正プログラム検索と除外の設定

ヒント: 不正プログラム対策機能の紹介や推奨設定方法についての情報は、次のWebサイトでまとめて確認できます。環境の構築を始める前に参照すると、動作不調のリスク軽減および安定性の向上に役立てることができます。
https://success.trendmicro.com/dcx/s/solution/000286756?language=ja

不正プログラム検索設定は保存して再利用可能な設定で、ポリシーまたはコンピュータに不正プログラム対策を設定する場合に適用できます。不正プログラム検索設定では、Deep Securityが検索する不正プログラムの種類と、検索するファイルの種類を指定します。一部のポリシーのプロパティも、不正プログラム検索の動作に影響を与えます。次の操作を実行できます。

- "不正プログラム検索設定を作成または変更する" on the next page
- "特定の種類の不正プログラムを検索する" on page 835
- "検索対象ファイルを指定する" on page 838

- "リアルタイム検索を実行するタイミングを指定する" on page 846
- "不正プログラムの処理を設定する" on page 846
- "ファイルのハッシュダイジェストにより不正プログラムファイルを特定する" on page 849
- "コンピュータで通知を設定する" on page 850

Deep Security ベストプラクティスガイド では、不正プログラム検索の設定に関する推奨事項もいくつか提供しています。

CPU使用率とRAM使用率は不正プログラム対策の設定によって異なります。Deep Securityエージェントで不正プログラム対策のパフォーマンスを最適化する方法については、"不正プログラム対策のパフォーマンスを向上させる" on page 850をご覧ください。

不正プログラム検索設定を作成または変更する

1つ以上の不正プログラム検索設定を作成または変更して、リアルタイム検索、手動検索、または予約検索の動作を制御できます。詳細については、"不正プログラム検索設定" on page 824を参照してください。

- 作成した不正プログラム検索設定は、ポリシーまたはコンピュータの検索と関連付けることができます。詳細については、"実行するスキャンの種類を選択" on page 829を参照してください。
- ポリシーまたはコンピュータが使用している不正プログラム検索設定を編集すると、この変更は設定に関連付けられている検索に影響します。

既存の設定に類似する不正プログラム検索設定を作成するには、既存の設定を複製して編集します。

制御する検索の種類に応じて、2種類の不正プログラム検索設定を作成できます ("不正プログラム検索の種類" on page 822を参照してください)。

- リアルタイム検索の設定: リアルタイム検索を制御します。[アクセス拒否] などの一部の処理は、リアルタイム検索の設定でのみ使用可能です
- 手動/予約検索の設定: 手動検索と予約検索を制御します。[CPU使用率] などの一部のオプションは、手動および予約検索の設定でのみ使用可能です。

Deep Securityは、検索の種類ごとに初期設定の不正プログラム検索の設定を提供します。この設定は次のように使用できます。

1. [ポリシー]→[共通オブジェクト]→[その他]→[不正プログラム検索設定] に移動します。
2. 検索設定を作成するには、[新規]、[新規の不正プログラムのリアルタイム検索設定] または [新規の不正プログラムの手動/予約検索設定] をクリックし、次の手順に従います

a. 検索設定を識別する名前を入力します。この名前は、ポリシーで不正プログラム検索を設定するときにリストに表示されます。
b. オプションで、設定の使用例を説明する説明を入力します。

3. 既存の検索設定を表示して編集するには、その検索設定を選択して[プロパティ]をクリックします。
4. 検索設定を複製するには、その検索設定を選択して[複製]をクリックします。

不正プログラム検索設定を使用するポリシーとコンピュータを確認するには、プロパティの 割り当て対象 タブをご覧ください。

不正プログラム検索をテストする

不正プログラム対策の設定手順に進む前に、スキャンをテストし、それらが正しく動作することを確認します。

リアルタイム検索をテストするには:

1. リアルタイム検索が有効で、設定が選択されていることを確認します。
2. EICARサイトに移動し、不正プログラム対策のテストファイルをダウンロードします。この標準化されたファイルはリアルタイム検索のアンチウイルス機能をテストします。ファイルは隔離される必要があります。
3. Deep Security Managerで、[イベントとレポート]→[不正プログラム対策イベント]の順に選択し、EICARファイルの検出が記録されていることを確認します。検出が記録されていれば、不正プログラム対策のリアルタイム検索は正常に機能しています。

手動検索または予約検索をテストするには:

1. リアルタイム検索が無効になっていることを確認してください。
2. [管理]を選択します。
3. [予定タスク]→[新規]の順にクリックします。
4. メニューからコンピュータの不正プログラムをスキャンを選択し、頻度を選択します。希望する仕様でスキャン設定を完了してください。
5. EICARサイトにアクセスして、不正プログラム対策テストファイルをダウンロードしてください。この標準化されたファイルは、手動または予約検索のウイルス対策機能をテストします。
6. 予約検索を選択して、[今すぐタスクを実行]をクリックします。このテストファイルが隔離されればテストは成功です。
7. Deep Security Managerで、[イベントとレポート]→[不正プログラム対策イベント]の順に選択し、EICARファイルの検出が記録されていることを確認します。検出が記録されていれば、不正プログラム対策の手動および予約検索は正常に機能しています。

特定の種類の不正プログラムを検索する

- "Windows AMSI保護を有効にする(リアルタイム検索のみ) " below
- "スパイウェア/グレーウェアを検索する" below
- "圧縮済み実行可能ファイルを検索する(リアルタイム検索のみ)" on the next page
- "プロセスメモリを検索する" on the next page
- "圧縮ファイルを検索する" on the next page
- "埋め込みのMicrosoft Officeオブジェクトを検索する" on page 837

関連項目:

- "挙動監視による不正プログラム/ランサムウェア検索の強化" on page 873
- "脅威インテリジェンスを使用した新たな脅威の検出" on page 861

Windows AMSI保護を有効にする(リアルタイム検索のみ)

Windows Antimalware Scan Interface (AMSI) は、MicrosoftがWindows 10以降で提供しているインタフェースです。Deep Securityは、AMSIを利用して不正なスクリプトを検出します。初期設定では、Deep Securityの不正プログラム検索設定でこのオプションが有効になっています。

1. 不正プログラム検索設定のプロパティを開きます。
2. [一般]タブで、[AMSI保護を有効にする]を選択します。
3. [OK] をクリックします。

スパイウェア/グレーウェアを検索する

スパイウェアおよびグレーウェア対策を有効にすると、不審なファイルの検出時に、スパイウェア検索エンジンによってこれらのファイルが隔離されます。

1. 不正プログラム検索設定のプロパティを開きます。
2. [一般] タブで、[スパイウェア/グレーウェア対策を有効にする] を選択します。
3. [OK] をクリックします。

スパイウェア検索エンジンで無視する必要があるファイルを特定するには、"高度な攻撃コードの除外を設定する" on page 891を参照してください。

圧縮済み実行可能ファイルを検索する(リアルタイム検索のみ)

ウイルスは、リアルタイム圧縮アルゴリズムを使用して、ウイルスフィルタを回避しようとすることがあります。IntelliTrap機能は、リアルタイムの圧縮済み実行可能ファイルを遮断し、他の不正プログラムの特性とファイルを組み合わせます。

IntelliTrapはそのようなファイルをセキュリティリスクとして識別し、安全なファイルを誤ってブロックする可能性があるため、IntelliTrapを有効にする場合はファイルを削除やクリーンではなく隔離することを検討してください。詳細については、"不正プログラムの処理を設定する" on page 846を参照してください。リアルタイムで圧縮された実行可能ファイルの交換が定期的に行われる場合は、IntelliTrapを無効にしてください。IntelliTrapはウイルス検索エンジン、IntelliTrapパターンファイル、およびIntelliTrap除外パターンファイルを使用します。

1. 不正プログラム検索設定のプロパティを開きます。
2. [一般] タブで、[IntelliTrapを有効にする] を選択します。
3. [OK] をクリックします。

プロセスメモリを検索する

プロセスメモリをモニタし、トレンドマイクロSmart Protection Networkを使用して、疑わしいプロセスが悪意のあるものであるかどうかを確認するための追加チェックを実行します。プロセスが悪意のあるものである場合、Deep Securityはプロセスを終了します。詳細については、"Deep SecurityのSmart Protection" on page 881を参照してください

1. 不正プログラム検索設定のプロパティを開きます。
2. [一般] タブで、[プロセスメモリ内の不正プログラムを検索する] を選択します。
3. [OK] をクリックします。

Deep Security Agentバージョン20.0.1-12510以降では、実行するアクションを使用して、Deep Securityが不正プログラムを検出したときに実行する修復アクションを選択できます。推奨値はActiveActionです。または、Passを選択することもできます。詳細については、"トレンドマイクロの推奨処理" on page 848および"不正プログラム修復処理をカスタマイズする" on page 847を参照してください

圧縮ファイルを検索する

圧縮ファイルを解凍し、コンテンツに不正プログラムが含まれていないか検索します。検索を有効にするときに、解凍するファイルの最大サイズと最大数を指定します(大きなファイルはパフォーマンスに影響を及ぼすことがあります)。また、圧縮ファイル内に存在する圧縮ファイルを検索できるように、検査する圧縮レベルも指定します。圧縮レベル1は、単一の圧縮ファイルです。レベル2は、ファイル内の圧縮

ファイルです。最大6の圧縮レベルを検索できますが、レベルが高くなるとパフォーマンスに影響を及ぼす可能性があります。

1. 不正プログラム検索設定のプロパティを開きます。
2. [詳細] タブで、[圧縮ファイルの検索] を選択します。
3. 解凍するコンテンツファイルの最大サイズ (MB)、検索する圧縮レベル、解凍する最大ファイル数を指定します。
4. [OK] をクリックします。

埋め込みのMicrosoft Officeオブジェクトを検索する

Microsoft Officeの特定のバージョンでは、Object Linking and Embedding (OLE) を使用してOfficeファイルにファイルやその他のオブジェクトを挿入します。これらの埋め込みオブジェクトには、不正なコードが含まれている場合があります。

圧縮ファイルの"圧縮ファイルを検索する" on the previous pageを有効にした後、他のオブジェクトに埋め込まれたオブジェクトを検出するために検索するOLEレイヤーの数を指定できます。パフォーマンスへの影響を軽減するために、各ファイル内の埋め込みオブジェクトのレイヤーを少数のみ検索することができます。

1. 不正プログラム検索設定のプロパティを開きます。
2. [詳細] タブで、[埋め込みのMicrosoft Officeオブジェクトを検索する] を選択します。
3. 検索するOLE層の数を指定します。
4. [OK] をクリックします。

Windows OSでNotifierの手動検索を有効にする

Notifierを使用した手動検索の有効化は、Deep Security Agent 20.0.0-7476以降でサポートされています。

この検索は初期設定では無効になっています。次の手順で有効化およびトリガできます:

1. [コンピュータ] エディタまたは [ポリシー] エディタで、[不正プログラム対策]→[一般] の順に選択します。
2. [手動検索] で、[Agentによる手動検索の実行またはキャンセルを許可する] を選択します。

Agentレスによる検索はサポートされないことに注意してください。

Linux OSでの手動検索の有効化

手動検索の有効化は、Deep Security Agent 20.0.0-7476以降でサポートされています。

この検索は初期設定では無効になっています。次の方法で有効にできます。

1. コンピュータエディタまたはポリシーエディタで、[不正プログラム対策]→[一般] の順に選択します。
2. [手動検索] で、[Agentによる手動検索の実行またはキャンセルを許可する] を選択します。

Agentレスによる検索はサポートされないことに注意してください。

検索対象ファイルを指定する

検索に含めるファイルとディレクトリを特定し、それらのファイルとディレクトリからの除外を特定します。ネットワークディレクトリを検索することもできます。

- "検索対象" below
- "検索除外" on the next page
- "ネットワークディレクトリを検索する(リアルタイム検索のみ)" on page 846

検索対象

検索するディレクトリと、ディレクトリ内の検索するファイルも指定します。

ディレクトリをスキャンするために、すべてのディレクトリまたはディレクトリのリストを指定できます。ディレクトリリストは、特定の構文を使用してスキャンするディレクトリを識別します。詳細については、"ディレクトリリストの構文" on page 840を参照してください。

検索するファイルを指定するには、次のいずれかのオプションを使用します。

- すべてのファイル
- IntelliScanで判別されるファイルタイプ。IntelliScanは、.zipや.exeなど、感染しやすいファイルタイプのみを検索します。検索対象のファイルタイプは、ファイル拡張子からではなく、ファイルのヘッダや内容を読み取って判別されます。すべてのファイルを検索する場合に比べて、IntelliScanを使用すると検索するファイルの数が減り、パフォーマンスが向上します。
- 指定されたリストに含まれるファイル名拡張子を持つファイル: ファイル拡張子リストは特定の構文を使用したパターンを使用します。詳細については、"ファイル拡張子リストの構文" on page 844を参照してください。

1. 不正プログラム検索設定のプロパティを開きます。
2. [検索対象] タブをクリックします。
3. 検索するディレクトリを指定するには、[すべてのディレクトリ] または [ディレクトリリスト] を選択します。
4. [ディレクトリリスト] を選択した場合は、ドロップダウンメニューから既存のリストを選択するか、[新規] を選択して新しいリストを作成します。

5. 検索するファイルを指定するには、[すべてのファイル]、[トレンドマイクロの推奨設定で検索されるファイルタイプ]、または [ファイル拡張子リスト] のいずれかを選択します。
6. [ファイル拡張子リスト] を選択した場合は、メニューから既存のリストを選択するか、[新規] を選択して新しいリストを作成します。
7. [OK] をクリックします。

検索除外

検索対象からディレクトリ、ファイル、およびファイル拡張子を除外します。リアルタイム検索の場合 (Deep Security Virtual Applianceによって実行される場合を除く)、プロセスイメージファイルも検索から除外できます。

以下は除外するファイルとフォルダーの例です:

- Microsoft Exchangeサーバの不正プログラム検索設定を作成する場合は、SMEX隔離フォルダを除外して、不正プログラムであることがすでに確認されているファイルの再検索を回避する必要があります。
- Deep Security Managerで使用されているデータベースサーバ上で不正プログラム検索を実行する場合は、データディレクトリを除外します。Deep Security Managerでウイルスが含まれている可能性のある侵入防御データを取り込み、格納する際に、Deep Security Agentによる隔離が実行され、データベースの破損を引き起こす場合があります。
- サイズの大きいVMwareイメージがある場合は、パフォーマンスの問題が発生した場合は、これらのイメージが格納されているディレクトリを除外します。

信頼できるデジタル証明書で署名されたファイルは、不正プログラム対策のスキャンから除外することもできます。この種の除外は、ポリシーまたはコンピュータの設定で定義されます。詳細については、"信頼された証明書で署名されたファイルを除外する" on page 896を参照してください。

除外するパターンのリストを作成して、ディレクトリ、ファイル、およびプロセスイメージファイルを除外する

1. 不正プログラム検索設定のプロパティを開きます。
2. [検索除外] タブをクリックします。
3. 検索から除外するディレクトリを指定します。
   a. [ディレクトリリスト] を選択します。
   b. ディレクトリリストを選択するか、新規を選択して作成してください。詳細については、"ディレクトリリストの構文" on the next pageを参照してください。
   c. ディレクトリリストを作成した場合は、ディレクトリリストで選択します。

4. 同様に、除外するファイルリスト、ファイル拡張子リスト、およびプロセスイメージファイルリストを指定します。詳細については、"ファイルリストの構文" on page 842、"ファイル拡張子リストの構文" on page 844、および"プロセスイメージファイルリストの構文" on page 844を参照してください
5. [OK] をクリックします。

Deep Security Agentが対象ファイルの種類を特定できない場合、不正プログラム対策 エンジンはそのファイルをメモリにロードし、自己解凍型ファイルであるかどうかを識別します。多数の大きなファイルがメモリにロードされると、検索エンジンのパフォーマンスに影響する可能性があります。特定のサイズを超えるファイルを除外するには、次のDeep Security Managerコマンドを使用します。

```
dsm_c -action changesetting -name
com.trendmicro.ds.antimalware:settings.configuration.maxSelfExtractRTScanSizeMB -value 512
```

この例では、ターゲットファイルの読み込みに対するファイルサイズの制限が512 MBに設定されています。検索エンジンは、設定された値より大きいファイルをメモリに追加せず、直接スキャンします。この設定を展開するには、Deep Security Managerでコマンドを実行した後、ポリシーをターゲットのDeep Securityエージェントに送信する必要があることに注意してください。

ファイル除外のテスト

以降の不正プログラム対策の設定手順に進む前に、ファイル除外をテストし、それらが正しく動作していることを確認します

1. リアルタイム検索が有効で、設定が選択されていることを確認してください。
2. [ポリシー]→[共通オブジェクト]→[その他]→[不正プログラム検索設定] に移動します。
3. [新規]→[新規の不正プログラムのリアルタイム検索設定] の順にクリックします。
4. [検索除外] タブに移動し、ディレクトリリストから[新規] を選択します。
5. ディレクトリリストに名前を付けます。
6. ディレクトリの下でスキャンから除外したいディレクトリのパスを指定します。例えば、`c:\Test Folder\`。
7. [OK] をクリックします。
8. [一般] タブで、手動検索に名前を付け、[OK] をクリックします。
9. EICARサイトに移動し、不正プログラム対策のテストファイルをダウンロードします。前の手順で指定したフォルダにファイルを保存します。このファイルが不正プログラム対策モジュールによって検出されずにそのまま保存されればテストは成功です。

ディレクトリリストの構文

ディレクトリリスト項目では、WindowsとLinuxの両方の命名規則をサポートするため、スラッシュとバックスラッシュの区別はありません。

検索除外	形式	説明	例
ディレクトリ	DIRECTORY\	指定したディレクトリとそのすべてのサブディレクトリにあるファイルをすべて除外します。	C:\Program Files\ Program Filesディレクトリとそのすべてのサブディレクトリにあるファイルをすべて除外します。
ワイルドカード(*)を使用したディレクトリ	DIRECTORY*\	指定されたサブディレクトリと、そこに含まれるファイルを除き、すべてのサブディレクトリを除外します。	*C:\abc** abcのすべてのサブディレクトリ内のすべてのファイルを除外しますが、abcディレクトリ内のファイルは除外しません。 *C:\abc\wx*z* *一致する:* C:\abc\wxz\ C:\abc\wx123z\ *一致しない:* C:\abc\wxz C:\abc\wx123z *C:\abc*wx* *一致する:* C:\abc\wx\ C:\abc\123wx\ *一致しない:* C:\abc\wx C:\abc\123wx
ワイルドカード(*)を使用したディレクトリ	DIRECTORY*\	一致する名前を持つ任意のサブディレクトリを除外します。ただし、そのディレクトリにあるファイルおよび任意のサブディレクトリは除外しません。	*C:\Program Files\SubDirName** SubDirNameで始まるフォルダ名を持つサブディレクトリを除外します。C:\Program Files\以下のすべてのファイルや他のサブディレクトリは除外しません。
環境変数	${ENV VAR}	環境変数 ${ENV VAR} の形式で定義されたすべてのファイルおよびサブディレクトリを除外します。windir、programfilesなどの Windows の一般的な環境変数がサポートされています。 Virtual Appliance および Linux の場合、環境変数の値のペアはポリシーまたはコンピュータエディタ> 設定 > 一般 > 環境変数オーバーライドで定義する必要があります	${windir} 変数がc:\windowsに変換された場合、c:\windowsとそのすべてのサブディレクトリにあるファイルをすべて除外します。

検索除外	形式	説明	例
コメント	DIRECTORY #コメント	除外の定義にコメントを追加します。	c:\abc #Exclude the abc directory

ファイルリストの構文

検索除外	形式	説明	例
ファイル	FILE	場所やディレクトリに関係なく、指定したファイル名を持つすべてのファイルを除外します。	*abc.doc* すべてのディレクトリでabc.docという名前のファイルをすべて除外します。abc.exeは除外しません。
ファイルパス	FILEPATH	ファイルパスで指定された単一のファイルを除外します。	*C:\Documents\abc.doc* Documentsディレクトリのabc.docという名前のファイルのみ除外します。
ワイルドカード(*)を使用したファイルパス	FILEPATH	ファイルパスで指定されたすべてのファイルを除外します。	C:\Documents\abc.co* (Windows Agentプラットフォームのみ) Documentsディレクトリにある、ファイル名がabcで拡張子が.coで始まるファイルを除外します。
ファイル名はワイルドカード(*) です	FILEPATH*	パス内のすべてのファイルを除外しますが、指定されていないサブディレクトリ内のファイルは除外します	*C:\Documents** ディレクトリC:\Documents\にあるすべてのファイルを除外します。 *C:\Documents\SubDirName*** フォルダ名がSubDirNameで始まるサブディレクトリ内のすべてのファイルを除外します。C:\Documents\またはその他のサブディレクトリにあるすべてのファイルを除外しません。 *C:\Documents*** C:\Documents下のすべての直接サブディレクトリ内のすべてのファイルを除外します。以降のサブディレクトリにあるファイルは除外しません。
ワイルドカード(*)を使用したファイル	FILE*	ファイル名のパターンに一致するすべてのファイルを除外します。	*abc*.exe* abcという接頭辞とexeという拡張子を持つファイルを除外します。 **.db*

検索除外	形式	説明	例
			一致する: 123.db abc.db *一致しない:* 123db 123.abd cbc.dba **db* *一致する:* 123.db 123db ac.db acdb db *一致しない:* db123 *wxy*.db* *一致する:* wxy.db wxy123.db *一致しない:* wxydb
ワイルドカード(*)を使用したファイル	FILE.EXT*	ファイルの拡張子のパターンに一致するすべてのファイルを除外します。	*abc.v** ファイル名がabcで拡張子が.vで始まるファイルを除外します。 *abc.*pp* *対象:* abc.pp abc.app *対象外:* wxy.app *abc.a*p* *対象:* abc.ap abc.a123p *対象外:* abc.pp *abc.** *対象:* abc.123 abc.xyz *対象外:*

検索除外	形式	説明	例
			wxy.123
ワイルドカード(*)を使用したファイル	FILE*.EXT*	ファイル名と拡張子のパターンに一致するすべてのファイルを除外します。	*a*c.a*p* *対象:* ac.ap a123c.ap ac.a456p a123c.a456p *対象外:* ad.aa
環境変数	${ENV VAR}	環境変数${ENV VAR}の形式で指定されたファイルを除外します。 windir、programfilesなどのWindows共通環境変数がサポートされています。 Virtual ApplianceおよびLinuxの場合、環境変数の値のペアはポリシーまたはコンピュータエディタ> 設定 > 一般 > 環境変数オーバーライドで定義する必要があります	*${myDBFile}* myDBFileファイルを除外します。
コメント	FILEPATH #コメント	除外の定義にコメントを追加します。	C:\Documents\abc.doc #This is a comment

ファイル拡張子リストの構文

検索除外	形式	説明	例
ファイル拡張子	EXT	一致する拡張子を持つすべてのファイルと一致します。	doc すべてのディレクトリの.docという拡張子を持つすべてのファイルと一致します。
コメント	EXT #コメント	除外の定義にコメントを追加します。	doc #This a comment

プロセスイメージファイルリストの構文

検索除外	形式	説明	例
ファイルパス	C:\DIR\FILE.EXT	ファイルパスで指定したプロセスイメージファイルを除外します。	C:\abc\file.exe abcディレクトリのfile.exeという名前のファイルのみ除外します。
ワイルドカード	C:\DIR*\FILE.EXT	ワイルドカードはディレクトリ名を置	C:\abc*\file.exe

検索除外	形式	説明	例
(*) を含むディレクトリ		き換えます。	一致する: C:\abc\file.exe C:\abc1\file.exe C:\abc1\abc2\file.exe C:\abc**\file.exe 一致する: C:\abc1\abc2\file.exe 一致しない: C:\abc\file.exe C:\abc1\file.exe
ワイルドカード (*) を使用したファイル名	C:\DIR\FILE*.EXT C:\DIR\FILE.EXT* C:\DIR\FILE*.EXT*	ワイルドカードはファイル名を置き換えます。	C:\abc\file*.exe 一致する: C:\abc\file.exe C:\abc\file123.exe 一致しない: C:\abc\file.exe123 C:\abc\file123.exe123 C:\abc\file.exe* 一致する: C:\abc\file.exe C:\abc\file.exe123 一致しない: C:\abc\file123.exe C:\abc\file123.exe123 C:\abc\file*.exe* 一致する: C:\abc\file.exe C:\abc\file.exe123 C:\abc\file123.exe C:\abc\file123.exe123
ワイルドカード (*) を使用したドライブ名	*:\DIR\FILE.EXT	ワイルドカードはドライブ名を置き換えます。	*:\abc\file.exe 一致: C:\abc\file.exe
ワイルドカード (*) を使用した特殊文字	C:\DIR\FILE*EXT C:\DIR\DIR2*FILE.EXT	ワイルドカードは、コロン (:)、バックスラッシュ (\)、スラッシュ (/)、ピリオド (.) などの特殊文字を置き換えます。	C:\abc\file*exe 一致する: C:\abc\file.exe 一致しない: C:\abc\abc2\file.exe C:\abc\abc2\abc3\file.exe

検索除外	形式	説明	例
			C:\abc\abc2*file.exe 一致する: C:\abc\abc2\file.exe C:\abc\abc2\abc3\file.exe 一致しない: C:\abc\file.exe

ネットワークディレクトリを検索する(リアルタイム検索のみ)

Network File System (NFS)、Server Message Block (SMB)、またはCommon Internet File System (CIFS) に存在するネットワーク共有内およびマッピングされているネットワークドライブ内のファイルやフォルダを検索する場合は、[ネットワークディレクトリ検索を有効にする] を選択します。このオプションはリアルタイム検索でのみ使用できます。

GVFS (GNOMEデスクトップで利用できる仮想ファイルシステム) を通じて「~/.gvfs」でアクセスされるリソースは、ネットワークドライブではなくローカルリソースとして扱われます。

ネットワークフォルダをWindowsでスキャン中にウイルスが検出された場合、エージェントは一部のクリーン失敗 (削除失敗)イベントを表示することがあります。

リアルタイム検索を実行するタイミングを指定する

ファイルの読み取り時、書き込み時、またはそのどちらでもファイルを検索するかを選択します。

1. 不正プログラム検索設定のプロパティを開きます。
2. [詳細] タブで、[リアルタイム検索] プロパティのオプションを1つ選択します。
3. [OK] をクリックします。

不正プログラムの処理を設定する

不正プログラムが検出された場合のDeep Securityの動作を設定します。

- "不正プログラム修復処理をカスタマイズする" on the next page
- "不正プログラム検出のアラートを生成する" on page 849
- "NSXセキュリティタグを適用する" on page 849

不正プログラム修復処理をカスタマイズする

Deep Securityは不正プログラムを検出すると、ファイルを処理する修復処理を実行します。Deep Securityが不正プログラムに遭遇した場合に実行できる処理には、次の5つがあります。

- [放置]: ファイルに対して何もせずに感染したファイルへの完全なアクセスを許可します。不正プログラム対策イベントは引き続き記録されます。修復処理の[放置]は、潜在的なウイルスに対しては絶対に使用しないでください。
- クリーン: 感染したファイルを完全にアクセスできるようにする前にクリーンします。ファイルをクリーンできない場合は、隔離されます。
- 削除: Linuxでは、感染したファイルはバックアップなしで削除されます。Windowsでは、感染したファイルはバックアップされてから削除されます。Windowsのバックアップファイルはイベントとレポート> イベント> 不正プログラム対策イベント> 検出されたファイルで表示および復元できます。
- アクセス拒否: この検索アクションはリアルタイム検索中にのみ実行できます。Deep Securityが感染ファイルを開いたり実行しようとする試みを検出すると、直ちに操作をブロックします。感染ファイルは変更されません。アクセス拒否アクションがトリガーされると、感染ファイルは元の場所に留まります。リアルタイム検索が書き込み時に設定されている場合は、修復アクションアクセス拒否を使用しないでください。書き込み時が選択されている場合、ファイルは書き込み時に検索され、アクション[アクセス拒否]は効果がありません。
- 隔離: 感染したファイルをコンピュータまたはVirtual Applianceの隔離ディレクトリに移動します。隔離されたファイルはイベント& レポート> イベント> 不正プログラム対策イベント> 検出されたファイルで表示および復元できます。

  同じ不正プログラムであっても、Linuxでは「隔離」とマークされ、Windowsでは「削除」とマークされる場合があります。どちらの場合でも、[イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[検出ファイル] でファイルを表示および復元できます。

  Windowsでは、感染した非圧縮ファイル (例えば、.txtファイル) は隔離され、感染した圧縮ファイル (例えば、.zipファイル) は削除されます。Windowsでは、隔離ファイルと削除ファイル両方のバックアップがあり、[イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[検出ファイル] でそれらを表示および復元できます。Linuxでは、圧縮ファイルであれ非圧縮ファイルであれ、すべての感染ファイルは隔離され、[イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[検出ファイル] で表示および復元できます。

不正プログラム検索設定の修復処理は、ほとんどの状況に対応できるように初期設定されています。ただし、Deep Securityが不正プログラムを検出したときに実行する処理をカスタマイズできます。トレンドマイクロの推奨処理を使用することも、脆弱性の種類ごとに処理を指定することもできます。

トレンドマイクロの推奨処理は、不正プログラムの各カテゴリ用に最適化された一連の定義済みのクリーンナップ処理です。個々の検出を適切に処理するため、トレンドマイクロの推奨処理での処理は随時調整されます。"トレンドマイクロの推奨処理" belowを参照してください。

1. 不正プログラム検索設定のプロパティを開きます。
2. [詳細] タブで、[修復処理] に対して [カスタム] を選択します。
3. 実行する処理を指定します。
   a. トレンドマイクロ推奨の修復処理から実行する処理を決定するには、[トレンドマイクロの推奨処理を使用] を選択します。
   b. 脆弱性の種類ごとに処理を指定するには、[カスタム処理を使用] を選択してから、使用する処理を選択します。
4. 潜在的な不正プログラムに対して実行する処理を指定します。
5. [OK] をクリックします。

トレンドマイクロの推奨処理

次の表は、トレンドマイクロの推奨処理を選択した場合に実行される処理の一覧です。

不正プログラムの種類	処理
"ウイルス" on page 826	クリーン。ウイルスがクリーンできない場合、(Windowsでは) 削除され、(Linuxまたは Solarisでは) 隔離されます。この動作には除外があります。LinuxまたはSolarisエージェントでTest Virusタイプのウイルスが見つかった場合、感染したファイルへのアクセスが拒否されます。
"トロイの木馬" on page 826	隔離
"パッカー" on page 827	隔離
"スパイウェア/グレーウェア" on page 827	隔離
CVE攻撃コード	隔離
アグレッシブ検出ルール	放置 この設定では、より多くの問題が検出されますが、誤判定も増えるため、初期設定の処理はイベントの発生です。
"Cookie" on page 828	削除 リアルタイム検索には適用されません
"その他の脅威" on page 828	駆除 脅威を駆除できない場合は、次のように処理されます。

不正プログラムの種類	処理
	• Windowsでは、感染ファイルは削除されますが、必要に応じて、確認および復元することができます。 • Linuxでは、感染ファイルへのアクセスは拒否されます。 また、Linux Agentでは、「ジョーク」に分類されるウイルスが検出されると、直ちに隔離されます。駆除は行われません。
"潜在的な不正プログラム" on page 828	トレンドマイクロの推奨処理

Agentでアップデートサーバまたは Relayからウイルスパターンファイルのアップデートをダウンロードすると、それに応じてトレンドマイクロの推奨処理が変わることがあります。

CVE攻撃コードおよびアグレッシブ検出ルールの詳細については、"脅威インテリジェンスで使用する不正プログラム検索設定を作成する" on page 868を参照してください。

不正プログラム検出のアラートを生成する

Deep Securityが不正プログラムを検出すると、アラートを生成できます:

1. 不正プログラム検索設定のプロパティを開きます。
2. [一般] タブで、[アラート] に対して [この不正プログラム検索設定でイベントが記録されたときにアラートを発令する] を選択します。
3. [OK] をクリックします。

NSXセキュリティタグを適用する

Deep Securityでは、不正プログラムの脅威が検出された際に、保護対象の仮想マシンにNSXセキュリティタグを適用できます。詳細については、"NSXセキュリティタグを適用するように不正プログラム対策を設定する" on page 648を参照してください。

ファイルのハッシュダイジェストにより不正プログラムファイルを特定する

Deep Securityは不正プログラムファイルのハッシュ値を計算し、[イベントとレポート]→[イベント]→[不正プログラム対策イベント]画面に表示できます。一部の不正プログラムには複数の異なる名前が使用されていることがあるため、不正プログラムを一意に識別するハッシュ値が役立ちます。ハッシュ値は、他のソースでその不正プログラムに関する情報を確認する場合に使用できます。

1. 設定するポリシーエディタまたはコンピュータエディタを開きます。
2. [不正プログラム対策]→[詳細] の順にクリックします。
3. ファイルハッシュ計算の下で、デフォルトまたは継承チェックボックスをクリアします。デフォルトはルートポリシーに表示され、継承は子ポリシーに表示されます。

   [継承] チェックボックスがオンになっている場合、ファイルハッシュ設定は現在のポリシーの親ポリシーから継承されます。

   Defaultが選択されている場合、Deep Securityはハッシュ値を計算しません。

4. [すべての不正プログラム対策イベントのハッシュ値を計算する(SHA1は初期設定で計算)] を選択します。
5. 初期設定では、Deep SecurityはSHA-1ハッシュ値を生成します。追加のハッシュ値を生成するには、[MD5]または [SHA256]、あるいはその両方を選択します。
6. ハッシュ値を計算する不正プログラムファイルの最大サイズを変更することもできます。初期設定では128MBを超えるファイルはスキップされますが、この値を64 ~ 512MBの任意の値に変更できます。

コンピュータで通知を設定する

Windowsベースのエージェントでは、不正プログラム対策およびWebレピュテーションモジュールに関連するDeep Securityのアクションを実行するために、画面上に通知メッセージが表示されることがあります。例えば、不正プログラム対策のクリーンアップタスクには再起動が必要ですというメッセージが表示されることがあります。このダイアログボックスを閉じるには、OKをクリックする必要があります。

このような通知を表示しないようにするには、次のように設定します。

1. コンピュータエディタまたはポリシーエディタ[1]に移動します。
2. 左側にある[設定] をクリックします。
3. [一般] タブで、[通知] セクションまでスクロールします。
4. [ホストのすべてのポップアップ通知を抑制] を[はい] に設定します。メッセージは引き続きDeep Security Managerでアラートまたはイベントとして表示されます。Notifierの詳細については、"Deep Security Notifier" on page 1531を参照してください。

不正プログラム対策のパフォーマンスを向上させる

Deep Security Agentによるシステムリソースの使用を改善するには、パフォーマンスに関連する設定をベストプラクティスに従って最適化します。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。

関連項目:

- "高度な攻撃コードの除外を設定する" on page 891
- "ファイルのハッシュダイジェストにより不正プログラムファイルを特定する" on page 849
- "NSXセキュリティタグの設定" on page 647

ディスク使用量を最小限に抑える

検出した不正プログラムファイルを保存するために適切なディスク容量を確保します。確保した容量は、物理コンピュータ、仮想マシン、Deep Security Virtual Applianceを含むすべてのコンピュータにグローバルに適用されます。この設定は、ポリシーレベルおよびコンピュータレベルでオーバーライドできます。

1. 設定するポリシーエディタまたはコンピュータエディタを開きます。
2. [不正プログラム対策]→[詳細] の順にクリックします。
3. [検出ファイル] の [初期設定] をクリアします。
4. 検出ファイルの保存に使用される最大ディスク容量 フィールドに使用するディスク容量を指定します。
5. [保存] をクリックします。

検出ファイルを保存するための十分な空き領域がない場合は、アラートが発令されます。

Deep Security Virtual Applianceを使用して仮想マシンを保護している場合は、保護対象の仮想マシンからのすべての検出ファイルがVirtual Applianceに格納されます。そのため、Virtual Appliance上で検出ファイル用のディスク容量を増やす必要があります。

"Virtual Applianceの検索キャッシュ" on page 1062も参照してください。

CPU使用率を最適化する

- データベース、Microsoft Exchange検出ファイル、ネットワーク共有など、通常は安全であるがI/Oが高いファイルをリアルタイム検索から除外します (Windowsの場合は、procmonを使用してI/Oの高いファイルを検出できます)。"検索除外" on page 839を参照してください。
- ネットワークディレクトリを検索しないでください。"ネットワークディレクトリを検索する (リアルタイム検索のみ)" on page 846を参照してください。
- コンピュータがトレンドマイクロSmart Protection NetworkまたはSmart Protection Serverへの信頼できるネットワーク接続を持っていない場合、スマートスキャンを使用しないでください。"Deep SecurityのSmart Protection" on page 881を参照してください。
- CPU使用率 を中 (推奨、ファイル検索の間に一時停止) または 低 (ファイル検索の間に中よりも長い時間一時停止) に設定して、不正プログラム検索がCPUに与える影響を軽減します

a. 不正プログラム検索設定のプロパティを開きます。
b. [詳細] タブで、検索を実行中の [CPU使用率] を選択します。
c. [OK] をクリックします。

- CPUリソースに空きが出た場合に検索を実行する予約タスクを作成します。"Deep Security予約タスクの設定" on page 1826を参照してください。
- VM検索キャッシュで、リアルタイム検索キャッシュの構成を選択します。検索が頻繁でない場合は、有効期限を延長してください (繰り返し検索を避けるため)。"Virtual Applianceの検索キャッシュ" on page 1062を参照してください。
- Agentレスデプロイメントを使用すると、CPU使用率がすべてのコンピュータではなく、集中管理されたVirtual Applianceに集約されます。"Agentレスによる保護またはコンバインモードの保護の選択" on page 569をご覧ください。

- [検索するファイルの最大サイズ]、[ファイルを解凍する最大圧縮レイヤ]、[解凍した個別ファイルの最大サイズ]、[解凍するファイルの最大数]、および [検索するOLE層] の値を引き下げるか、低い初期設定値のままにします。"特定の種類の不正プログラムを検索する" on page 835を参照してください。

  警告: ほとんどの不正プログラムは小さく、ネストされた圧縮は不正プログラムを示します。しかし、大きなファイルをスキャンしない場合、不正プログラム対策が一部の不正プログラムを検出しないリスクがあります。このリスクは、変更監視などの他の機能を使用することで軽減できます。"変更監視の設定" on page 1004をご覧ください

マルチスレッド処理を有効にする

手動検索と予約検索に対してマルチスレッド処理を有効にすることができます。リアルタイム検索はデフォルトでマルチスレッド処理を使用します。マルチスレッド処理は、この機能をサポートするシステムでのみ有効です。この設定を適用するには、それを有効にしてからコンピュータを再起動してください。

リソースが限られている場合 (例えば、CPUに依存するタスク) や、リソースを一度に一人のオペレーターだけが保持しなければならない場合 (例えば、IOに依存するタスク) には、マルチスレッド処理を有効にしないでください。

マルチスレッド処理を有効にすると、CPU使用率に次のような影響を与える可能性があります。

- コンピュータの他のプロセスに利用可能なCPUコアの数を減少させる可能性があります。
- Linuxでは、[不正プログラム検索用のリソース割り当て]が有効になっている場合、[中]または[低]に設定されていても、CPU使用率の設定は無視されます。

マルチスレッド処理を有効にするには:

1. ポリシーを選択します。
2. マルチスレッド処理を有効にするポリシーをダブルクリックして開きます。
3. [不正プログラム対策]→[詳細]の順にクリックします。
4. 不正プログラムスキャンのリソース割り当てセクションで、不正プログラムスキャンにマルチスレッド処理を使用するに対してはいを選択し、保存をクリックします。

   Linuxでは、この設定は再起動を必要とせずに有効になります。Linux以外のプラットフォームでは、再起動が必要です。

5. Linux以外のプラットフォームを使用している場合、次のいずれかの方法でソリューションプラットフォームサービスを再起動してください。
   - services.mscウィンドウで、Trend Microソリューションプラットフォームサービスを選択し、再起動をクリックします。
   - コマンドプロンプトで、次のコマンドを入力してください。

     ```
     sc stop amsp
     ```

     ```
     sc start amsp
     ```

   - マルチスレッド処理を有効にしたコンピュータを再起動して、この設定を有効にします。

RAM使用率を最適化する

- [検索するファイルの最大サイズ]、[ファイルを解凍する最大圧縮レイヤ]、[解凍した個別ファイルの最大サイズ]、[解凍するファイルの最大数]、および[検索するOLE層]の値を引き下げるか、低い初期設定値のままにします。"特定の種類の不正プログラムを検索する" on page 835を参照してください。

  警告: ほとんどの不正プログラムは小さく、ネストされた圧縮は不正プログラムを示します。しかし、大きなファイルをスキャンしない場合、不正プログラム対策が一部の不正プログラムを検出しないリスクがあります。このリスクは、変更監視などの他の機能を使用することで軽減できます。"変更監視の設定" on page 1004をご覧ください

- Agentレスの配信を使用します(すべてのコンピュータではなく1台のVirtual ApplianceのRAMだけが消費されます)。"Agentレスによる保護またはコンバインモードの保護の選択" on page 569を参照してください。

Deep Security AgentとMicrosoft Defender ウイルス対策の共存

Microsoft Defender Antivirus は、Microsoft Windows Server 2016 以降および Windows 10 以降に自動的にインストールされます。Deep Security Agent (DSA) は、Trend Micro Deep Security によって保護されているすべてのオペレーティング システム レベルで、Microsoft Defender Antivirus のパッシブ モードで共存できます。以下は、Microsoft Defender Antivirus、Windows Server およびデスクトップ、ならびに DSA の互換バージョンです:

- Microsoft Defender Antivirus 製品およびエンジンのバージョン:
  - AMProductVersion: 4.18.2202.4
  - AMEngineVersion: 1.1.18900.3

- Windows Server およびデスクトップバージョン:
  - Windows Server 2016以降
  - Windows 10 x64 RS5 以降

- Deep Security Agent:
  - Deep Security Agent 20.0.0-4416 (20 LTS 更新 2022-04-28) 以降

Windows 10またはWindows 11デスクトップに不正プログラム対策を有効にしたDeep Securityをインストールすると、Microsoft Defender Antivirusは自動的にパッシブモードに設定されます。Windows サーバでは、Microsoft Defender Antivirusをパッシブモードにするために不正プログラム対策ポリシーを再度有効にする必要があります。

これらのイベントをまとめた表を以下に示します。

プラットフォーム	処理	説明
Windows 10 および11デスクトップ	不正プログラム対策が有効なDeep Security	Windowsは、Deep Security Agentの不正プログラム対策が有効になると、自動的にMicrosoft Defender Antivirusをパッシブモードに設定します。
Windowsサーバ2016以降	不正プログラム対策ポリシーを再有効化	Deep Security AgentはMicrosoft Defender Antivirusをパッシブモードに自動的に設定します。

DSAの不正プログラム対策を無効にするか、無効化またはアンインストールする場合、Microsoft Defender AntivirusのDisableAntiSpywareおよびForceDefenderPassiveModeレジストリの両方が削除されます

- DisableAntiSpyware レジストリキーは、Microsoft Defender Antivirus を無効にするかどうかを指定します。DisableAntiSpyware を削除すると、無効化キーが削除され、Microsoft Defender Antivirus が有効になります。Microsoft Defender Antivirus を手動で有効にして、アクティブモードにする必要があるかもしれません。
- ForceDefenderPassiveMode レジストリキーは Microsoft Defender Antivirus をパッシブモードに設定します。このキーを削除すると、Microsoft Defender Antivirus はアクティブモードに設定されます。

Windows ServerでDeep Security Agentの不正プログラム対策を有効にすると、Windows Securityのウイルスと脅威の保護サービスが「アクティブなウイルス対策プロバイダがありません。デバイスが脆弱です」というメッセージを表示することがあります。トレンドマイクロはこのケースをテストし、Microsoft Defender Antivirusが無効になっているときにこのメッセージが表示されることを確認しました。これはDeep Securityではなく、Windows Serverの動作です。

Microsoft Defender AntivirusとDeep Security Agentの不正プログラム対策の両方が有効になっている場合、パフォーマンスに影響があることが確認されています。そのため、Microsoft Defender Antivirusをパッシブモードにすることをお勧めします。パッシブモードが不可能な場合の代替アプローチとして、除外リストを使用することが推奨されます。ただし、除外リストは影響を軽減することはできますが、パフォーマンスへの影響を完全に排除することはできない可能性があります。

DSAの除外リストのMicrosoft Defenderウイルス対策アプリケーションファイル

Microsoft Defender Antivirusがパッシブモードに切り替えられない場合、パフォーマンスへの影響を軽減するために、Microsoft Defender Antivirus for EndpointをDeep Security Agentの除外リストに追加する必要があります。詳細については、非Microsoftエンドポイント保護からMicrosoft Defender Antivirus for Endpointへの切り替えを参照してください。

Microsoft Defenderウイルス対策の実行可能ファイルの場所は次のとおりです。

- %Program Files%\Windows Defender\
- %ProgramData%\Microsoft\Windows Defender\Platform\4.18.2201.10-0*\

Microsoft Defenderウイルス対策除外リストのDSAフォルダとプロセス

Deep Security エージェントのフォルダとプロセスを Microsoft Defender ウイルス対策の除外リストに追加する必要があります。

フォルダ:

- C:\Program Files\Trend Micro\AMSP
- C:\Program Files\Trend Micro\Deep Security Agent

プロセス:

- C:\Program Files\Trend Micro\AMSP\coreServiceShell.exe
- C:\Program Files\Trend Micro\AMSP\coreFrameworkHost.exe
- C:\Program Files\Trend Micro\Deep Security Agent\dsa.exe
- C:\Program Files\Trend Micro\Deep Security Agent\Notifier.exe

改ざん防止

Microsoft Defender ウイルス対策の改ざん防止を有効にすると、この特定のウイルス対策がパッシブモードに転送されないように保護されます。複数のウイルス対策製品を導入している場合は、1つのウイルス対策製品の不正プログラム対策コンポーネントを1つだけ保持するのが妥当です。

サポートされている環境の詳細については、「Microsoft Defender ウイルス対策と他のセキュリティ製品との互換性」を参照してください。

Microsoft Defender Antivirus エンドポイント検出と応答 (EDR) のブロックモード

エンドポイントのブロックモードでMicrosoft Defenderウイルス対策のEDRを有効にしないでください。この推奨事項は、ブロックモードのEDRが有効な場合に互換性の問題が検出されたというテストの結果に基づいています。

Virtual Applianceの検索キャッシュ

検索キャッシュは、仮想マシンの不正プログラム対策および変更監視の検索を最大限に効率化する目的で、Virtual Applianceによって使用されます。検索キャッシュによって、大規模なVMware環境で、複数の仮想マシンから同じ内容を検索する必要性がなくなるため、検索の効率が向上します。検索キャッシュには、Deep Security保護モジュールによって検索されたファイルおよびその他の検索対象のリストが含まれます。仮想マシン上の検索対象と過去の検索対象が同じであることが確認された場合、その対象はVirtual Applianceによって再度検索されません。エンティティが同じであるかどうかを確認するために使用される属性は、作成時刻、変更時刻、ファイルサイズ、およびファイル名です。リアルタイム検索キャッシュの場合、Deep Securityはファイルの一部の内容を読み取り、2つのファイルが同一であるかどうかを判断します。ファイルの更新シーケンス番号 (USN、Windowsのみ) を使用するオプション設定もありますが、その設定はクローン作成された仮想マシン以外には使用しないでください。

検索キャッシュによって、クローン作成された仮想マシン間または類似した仮想マシン間で検索結果が共有されるため、変更監視が効率化されます。

後続の検索の速度が向上するため、クローン作成された仮想マシンまたは類似した仮想マシンでの不正プログラムの検索が効率化されます。

また、クローン作成された仮想マシンまたは類似した仮想マシンの起動プロセス検索とアプリケーションアクセス検索の速度が向上するため、不正プログラムのリアルタイム検索が強化されます。

検索キャッシュ設定

検索キャッシュ設定は、有効期限、更新シーケンス番号 (USN)、除外するファイル、含めるファイルなどを指定する設定の集まりです。

注意: 同じ検索キャッシュ設定を使用する仮想マシン間では、同じ検索キャッシュが共有されます。

既存の検索キャッシュ設定のリストを表示するには、[管理]→[システム設定]→[詳細]→[検索キャッシュ設定] の順に進み、[検索キャッシュ設定の表示] をクリックします。Deep Securityには、事前設定された初期設定の検索キャッシュ設定がいくつか付属しています。これらの設定は、保護する仮想マシンのプロパティと実行する検索の種類に応じて、Virtual Applianceによって自動的に実装されます。

[期限] では、個々のエントリを検索キャッシュに保存する期間を指定します。推奨される初期設定は、手動/予約による不正プログラム検索で1日、不正プログラムのリアルタイム検索で15分、変更監視の検索で1日です。

[USNの使用 (Windowsのみ)] では、Windows NTFSの更新シーケンス番号を使用するかどうかを指定します。更新シーケンス番号は、個々のファイルへの変更を記録するための番号です。このオプションは、クローン作成された仮想マシンにのみ設定してください。

[含めるファイル] と[除外するファイル] では、検索キャッシュに含める、または検索キャッシュから除外するファイルの正規表現パターンとリストを指定します。検索対象のファイルは、まず含めるリストに対して照合されます。

個々のファイルとフォルダは名前で識別できます。また、ワイルドカード(「*」および「?」) を使用して、1つの正規表現で複数のファイルや場所を参照することもできます(ゼロ個以上の任意の文字を表すには「*」を、任意の1文字を表すには「?」を使用します)。

注意: 含めるリストと除外リストによって、ファイルの検索に検索キャッシュを使用するかどうかが決まります。ただし、これらのリストを使用することによって、ファイルを従来の方法で検索できなくなるわけではありません。

不正プログラム検索のキャッシュ設定

仮想マシンで使用する検索キャッシュ設定を選択するには、**コンピュータエディタまたはポリシーエディタ**[1]を開き、[不正プログラム対策]→[詳細]→[仮想マシンの検索キャッシュ] の順に進みます。ここで、不正プログラムのリアルタイム検索に使用する検索キャッシュ設定と、手動/予約検索に使用する検索キャッシュ設定を選択できます。

変更監視の検索のキャッシュ設定

仮想マシンで使用する検索キャッシュ設定を選択するには、**コンピュータエディタまたはポリシーエディタ**[2]を開き、[変更監視]→[詳細]→[仮想マシンの検索キャッシュ] の順に進みます。

検索キャッシュの管理設定

検索キャッシュの管理設定では、検索キャッシュの実行に関する設定ではなく、Virtual Applianceによる検索キャッシュの管理方法を指定します。そのため、検索キャッシュの管理設定は、検索キャッシュ設定と別になっています。検索キャッシュの管理設定は、ポリシーレベルで制御されます。検索キャッシュの管理設定を表示するには、**ポリシーエディタ**[3]を開き、[設定]→[一般]→[Virtual Appliance] の順に進みます。

同時検索の最大数: Virtual Applianceによって同時に実行される検索の数を指定します。推奨される数は5です。この数が10を超えると、検索のパフォーマンスが低下する可能性があります。検索要求はVirtual Applianceで処理待ちの状態となり、到着順に実行されます。この設定は、手動/予約検索にのみ適用されます。

不正プログラムの手動検索キャッシュの最大エントリ数: 不正プログラムの手動検索または予約検索を実行したときに保持するファイルやその他の検索可能な内容を特定するレコードの最大数を指定します。エントリが100万件の場合、使用されるメモリは約100 MBです。

不正プログラムのリアルタイム検索キャッシュの最大エントリ数: 不正プログラムのリアルタイム検索を実行したときに保持するファイルやその他の検索可能な内容を特定するレコードの最大数を指定します。エントリが100万件の場合、使用されるメモリは約100MBです。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。

[2] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。

[3] ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。

変更監視の検索キャッシュの最大エントリ数: 変更監視のベースラインデータに含めるエンティティの最大数を指定します。エンティティが20万個の場合、使用されるメモリは約100MBです。

初期設定を変更する場合の考慮事項

検索キャッシュは、同じファイルを再度検索しないことを目的としています。Deep Securityは、すべてのファイルの内容全体を調べてファイルが同一であるかどうかを判断しません。そうするように設定されている場合、Deep SecurityはファイルのUSN値を確認できますが、リアルタイム検索ではファイルの一部の内容が読み取られますが、通常はファイル属性を調べてファイルが同一であるかどうかを判断します。不正プログラムがファイルに変更を加えた後、それらのファイル属性を変更前の状態に復元することは困難ですが、不可能ではありません。

Deep Securityは、この初期設定のキャッシュ期限を短く設定することで、この潜在的な脆弱性を制限します。セキュリティを強化するために、キャッシュの有効期限をさらに短くしたり、USNを使用することもできますが、これによってパフォーマンスの向上率が低下したり、より大きなキャッシュの設定が必要になることがあります。特定の仮想マシンに最高レベルのセキュリティを提供し、他から切り離して検索結果を共有しないようにするには、該当する仮想マシン専用のポリシーを作成して、それらが別のゾーンで管理されるようにします。この方法は、異なる部門または組織間で同じインフラストラクチャを共有する場合に適しています(マルチテナントのDeep Security Managerを使用している場合は、この設定が自動的に各テナントに適用されます)。

VDI環境など、ESXiホストあたりのゲスト仮想マシン数が非常に多い場合は、検索中のディスクI/OとCPU使用率を監視してください。検索に時間がかかりすぎる場合は、キャッシュのサイズを増やすか、パフォーマンスが改善されるまで検索キャッシュの管理設定を調整します。キャッシュのサイズを増やす場合は、Deep Security Virtual Applianceシステムメモリの調整も必要になることがあります。

機械学習型検索を使用した脅威の検出

注意: 機械学習型検索はDeep Security Agent 11.0以降でサポートされています。この機能をサポートするプラットフォームの詳細については、"各プラットフォームでサポートされている機能" on page 417を参照してください。

機械学習型検索を使用して、不明または感染率の低い不正プログラムを検出します(詳細については、"機械学習型検索" on page 825参照してください)。

機械学習型検索では、高度な脅威検索エンジン(ATSE)を使用して、ファイルの特徴を抽出し、Trend Micro Smart Protection Network上の機械学習型検索エンジンにレポートを送信します。機械学習型検索を有効にするには、次の手順を実行します。

1. "インターネットに接続されていることを確認する" below
2. "機械学習型検索を有効にする" below

すべての不正プログラム検出と同様に、機械学習型検索では不正プログラムが検出されると、イベントがログに記録されます("Deep Securityイベントログについて" on page 1150を参照してください)。誤検出の場合の例外も作成できます("高度な攻撃コードの除外を設定する" on page 891を参照してください)。

インターネットに接続されていることを確認する

機械学習型検索では、Global Censusサービス、Good File Reputationサービス、および機械学習型検索サービスにアクセスする必要があります。これらのサービスは、Trend Micro Smart Protection Networkでホストされています。Deep Security AgentまたはVirtual Applianceが直接インターネットにアクセスできない場合は、回避策として"インターネットにアクセスできないAgentを設定する" on page 1504) を参照してください。

機械学習型検索を有効にする

機械学習型検索は、ポリシーまたは個々のコンピュータに適用されるリアルタイム検索設定の一環として設定されます("不正プログラム検索と除外の設定" on page 832を参照してください)。検索設定を行ったら、ポリシーまたはコンピュータに適用します。

注意: 機械学習型検索では、リアルタイム検索で検索対象に設定されたファイルおよびディレクトリのみが保護されます。"検索対象ファイルを指定する" on page 838を参照してください。

これらの設定は、リアルタイム検索の設定にのみ適用できます。

1. [ポリシー]→[共通オブジェクト]→[その他]→[不正プログラム検索設定] に移動します。
2. 設定するリアルタイム検索設定を選択して、[詳細] をクリックします。

   必要に応じて、新しいリアルタイム検索設定も作成できます。

3. [一般]タブの[機械学習型検索]で、[機械学習型検索を有効にするを選択します。[Action to take]リストで、不正プログラムを検出した場合にDeep Securityで実行する修復処理を選択します。
   - 隔離(推奨):) 感染ファイルを保護されたコンピュータの隔離ディレクトリに移動します。隔離されたファイルは、[イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[識別されたファイル]で表示および復元できます。
   - 放置: 感染ファイルに何も行わず、そのファイルへのフルアクセスを許可する(不正プログラム対策イベントは依然として記録されます。)

- 削除：Linuxでは、感染ファイルはバックアップせずに削除されます。Windowsでは、感染ファイルがバックアップされてから削除されます。Windowsのバックアップファイルは、[イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[識別されたファイル]で表示および復元できます。

4. [OK] をクリックします。
5. 検索設定を適用するポリシーまたはコンピュータのエディタを開いて、[不正プログラム対策]→[一般] の順に選択します。
6. [不正プログラム対策のステータス] が [オン] または [継承 (オン)] になっていることを確認します。
7. [リアルタイム検索] セクションで、不正プログラム検索設定を選択します。
8. [保存] をクリックします。

脅威インテリジェンスを使用した新たな脅威の検出

ヒント: 脅威インテリジェンス機能は、以前は Connected Threat Defense と呼ばれていました。以前に Connected Threat Defense を使用していた場合は、「"Connected Threat Defense から脅威インテリジェンスへの移行" on page 872への移行」を参照してください。

今日のデータセンターでは、フィッシングやスピアフィッシングなどの手法を用いた標的型攻撃によるセキュリティ侵害が増えています。これらのケースでは、不正プログラム作成者は特定の環境を標的にした不正プログラムを作成することによって、従来の不正プログラムScannerを回避します。Deep Securityは、脅威インテリジェンス機能により、新しい脅威に対する強化された不正プログラム対策を提供します。

注意: FIPSモードが有効な場合、脅威インテリジェンスは使用できません。"FIPS 140のサポート" on page 1870を参照してください。

このトピックの内容:

- "脅威インテリジェンスの仕組み" on the next page
- "脅威インテリジェンスの前提条件を確認する" on page 863
- "Trend Micro Vision Oneへの接続を設定する" on page 863
- "Deep Discovery Analyzerへの接続を設定する" on page 864
- "Trend Micro Apex Centralへの接続の設定 " on page 866
- "脅威インテリジェンスで使用する不正プログラム検索設定を作成する" on page 868
- "コンピュータで脅威インテリジェンスを有効にする" on page 869
- "サンドボックス分析にファイルを手動で送信する" on page 869

- "誤ったアラームを引き起こしたファイルを許可する" on page 869
- "不審なファイルに対する検索処理を設定する" on page 870
- "Deep Securityで不審オブジェクトリストをアップデートする" on page 870
- "マルチテナント環境での脅威インテリジェンスの設定" on page 871
- "サポートされているファイルタイプ" on page 871
- "Connected Threat Defense から脅威インテリジェンスへの移行" on page 872への移行

不正プログラム対策 モジュールの概要については、"不正プログラム対策について" on page 821についてを参照してください。

脅威インテリジェンスの仕組み

1. すべてのコンポーネントが適切に設定されると、Deep Security Agentはヒューリスティック検出を使用して保護対象コンピュータ上のファイルを分析し、不審なファイルかどうかを判断します。
2. 必要に応じて、不審なファイルをDeep SecurityからTrend Micro Vision One または Deep Discovery Analyzerに手動または自動で送信できます。これにより、不審なファイルがサンドボックス(安全な隔離された仮想環境)で実行され、監視されます。
3. Deep Security Managerは、Trend Micro Vision One または Deep Discovery Analyzerからサンドボックス分析結果を取得します。

   注意: サンドボックス分析レポートは保護を提供しません。Trend Micro Vision One または Deep Discovery分析に関する情報が提供されるだけです。完全に保護するには、Trend Micro Vision One またはTrend Micro Apex Centralへの接続が必要です。レポートは、15分ごとに Trend Micro Vision One または Deep Discovery Analyzer から取得されます。

4. 不審なファイルを他のサービスに送信してさらに分析するようにDeep Securityを設定できます。不審なファイルをTrend Micro Vision Oneに送信すると、分析結果は Trend Micro Vision One 脅威インテリジェンスに転送されます。不審なファイルをDeep Discovery Analyzerに送信すると、分析結果がTrend Micro Apex Centralにプッシュされ、分析に基づいてファイルに対する処理を指定できます。処理が指定されると、「不審オブジェクトリスト」と呼ばれる新しい脅威のリストが作成またはアップデートされます。Deep Discovery InspectorやDeep Discovery Email Inspectorなどの他のトレンドマイクロ製品も、Trend Micro Vision One またはTrend Micro Apex Central に接続して、リストをアップデートできます。
5. オプションで、Trend Micro Vision One またはTrend Micro Apex Central から不審オブジェクトのリストを受信し、不審オブジェクトのリストをDeep Security Agentに送信するようにDeep Security Managerを設定できます。

脅威インテリジェンスの前提条件を確認する

Deep SecurityをDeep Discoveryに接続する前に、環境が次の要件を満たしていることを確認してください。

- Deep Security Managerがインストールされ、コンピュータを保護するDeep Security Agentが設定されている。

オプション:

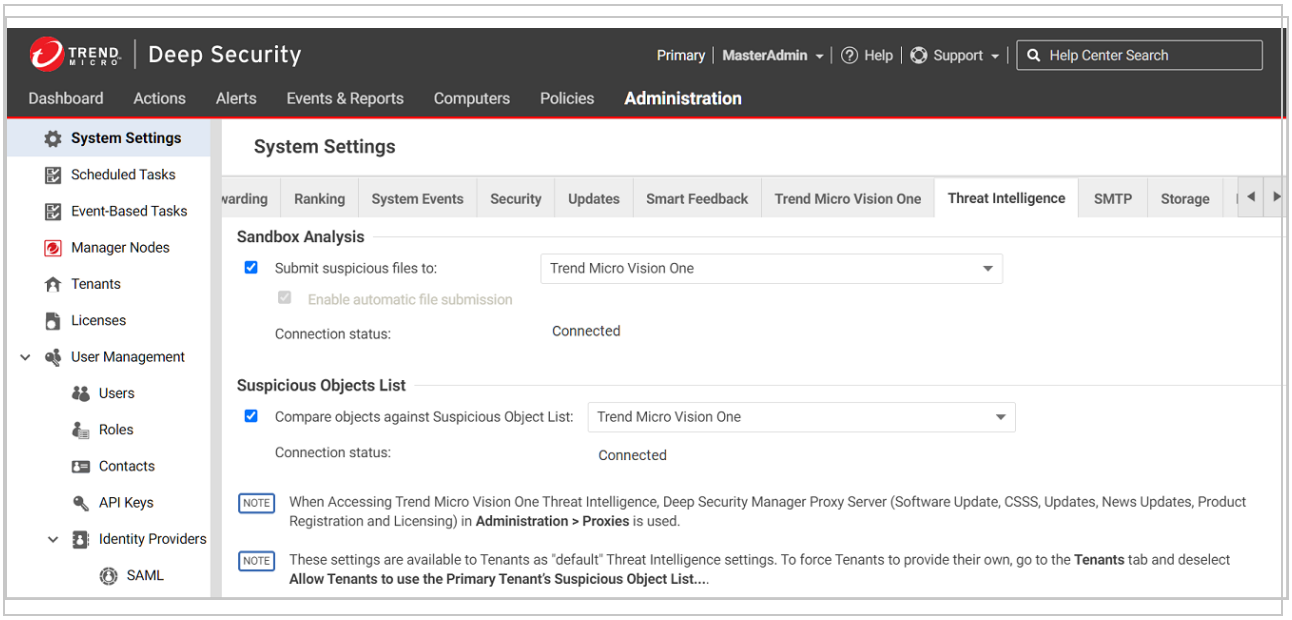
- Trend Micro Vision One (XDR) に接続するには
  - "Trend Vision One (XDR) と統合する" on page 1967と統合します。
  - Trend Micro Vision Oneに不審なファイルを送信するには、「Deep Security : Sandbox as a Service」ライセンスを購入してください。
- Deep Discovery Analyzerに接続するには、Deep Discovery Analyzer 5.5がインストールされ、サンドボックス仮想マシンが準備されていることを確認します。
- Trend Micro Apex Centralに接続するには、Apex Central 2019以降がインストールされている必要があります。
- Deep Discovery Analyzer をTrend Micro Apex Central 管理下のサーバに追加します。詳細については、Apex Centralのドキュメントを参照してください。

Trend Micro Vision Oneへの接続を設定する

不審ファイルを送信して不審オブジェクトリストをTrend Micro Vision Oneから取得し、保護対象のコンピュータと共有して、ローカルオブジェクトをTrend Micro Vision One 脅威インテリジェンス不審オブジェクトリストと比較するようにDeep Securityを設定できます。

1. Deep Security Managerで、[管理]> [システム設定]> [脅威インテリジェンス]に移動します。
2. [不審なファイルを送信する]を選択し、次に[Trend Micro Vision One]を選択します。
3. [オブジェクトを不審オブジェクトリストと比較する]を選択し、次に[Trend Micro Vision One]を

選択します。

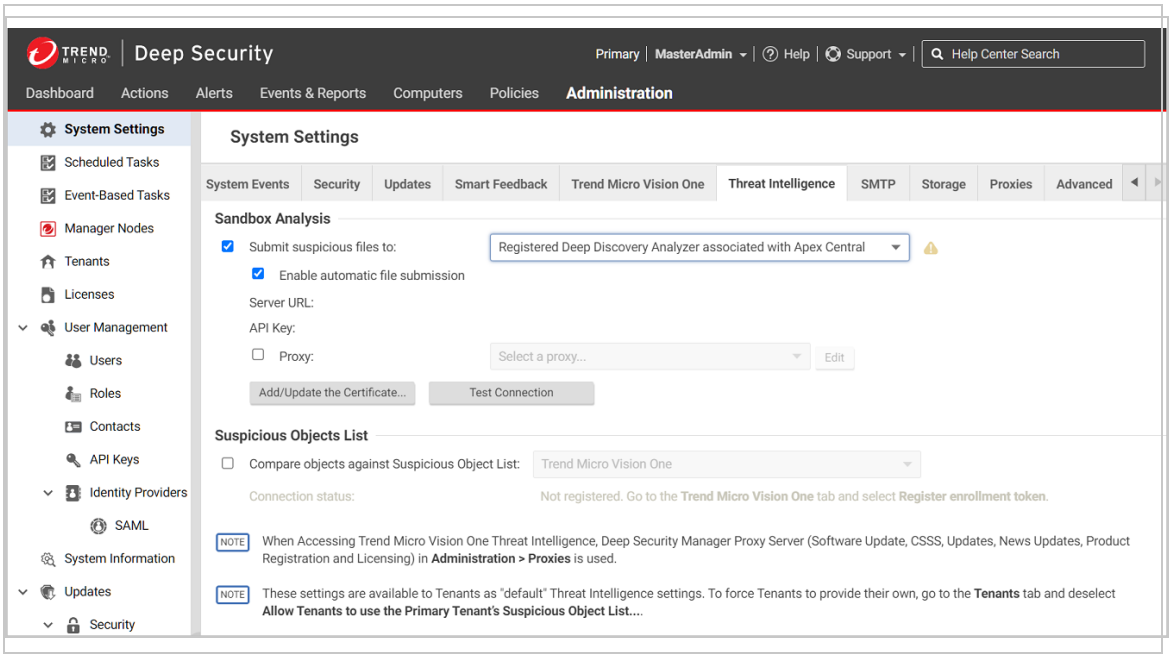


Deep Discovery Analyzerへの接続を設定する

Deep Security Managerから不審なファイルをDeep Discovery Analyzer に送信して分析する場合は、接続を設定する必要があります。

Trend Micro Apex Central がすでにDeep Securityを管理している場合

1. Deep Security Managerで、[管理]> [システム設定]> [脅威インテリジェンス]に移動します。
2. 選択不審ファイルを登録済みDeep Discovery Analyzerに関連付けられたApex Central 。



3. Deep Security Managerでファイルを自動的にDeep Discovery Analyzerに送信するには、[自動ファイル送信を有効にする] を選択します。

   注意: Deep Discovery Analyzer への自動送信は15分ごとに実行され、送信ごとに最大100ファイルが送信されます。

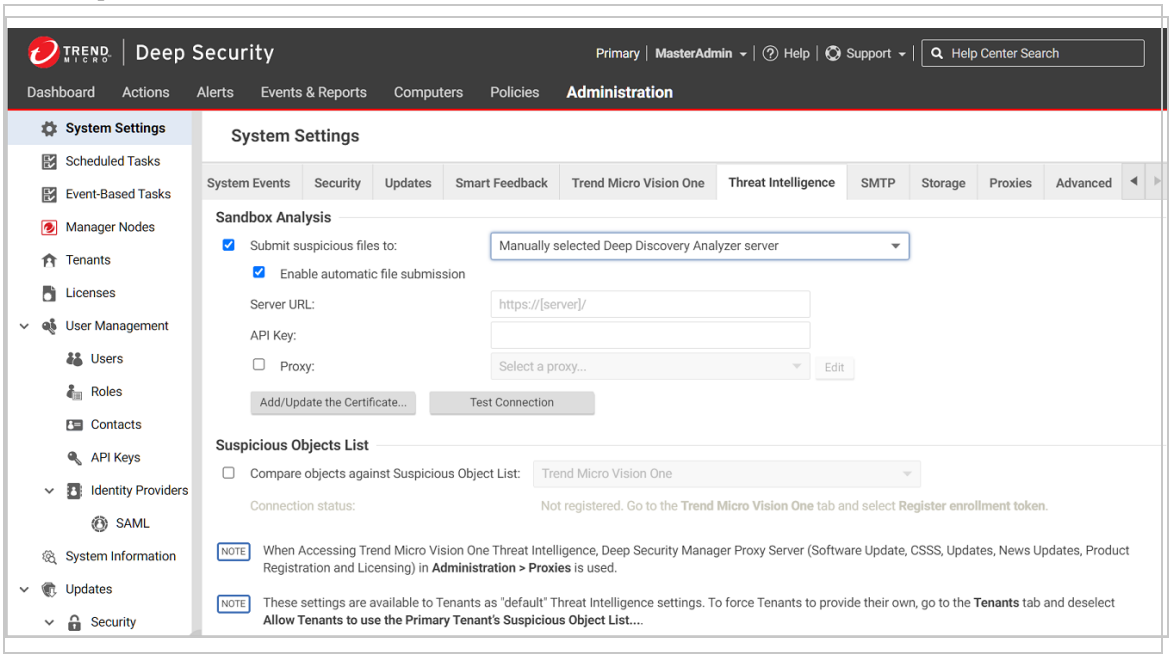
4. [接続テスト]を選択します。証明書が見つからないか無効であるためにDeep Securityが接続できないというエラーが表示された場合は、[証明書の追加/アップデート]を選択して、正しい Deep Discovery Analyzer 証明書にアップデートします。
5. [Save]を選択します。

Trend Micro Apex Central がまだDeep Securityを管理していない場合

1. Deep Discovery Analyzerで、[ヘルプ]→[バージョン情報] に進み、サーバURLとAPIキーを確認します。これらの値は後で必要になるため、テキストファイルにコピーしてください。
2. Deep Security Managerで、[管理]> [システム設定]> [脅威インテリジェンス]に移動します。

---

3. [不審なファイルを送信する]を選択し、[手動で選択したDeep Discovery Analyzerサーバ]を選択します。



4. Deep Security Managerでファイルを自動的にDeep Discovery Analyzerに送信するには、[自動ファイル送信を有効にする] を選択します。

   注意: Deep Discovery Analyzerへの自動送信は15分ごとに発生し、1回の送信で最大100個のファイルが送信されます。

5. 手順1で確認したサーバURL およびAPIキーを入力します。
6. [接続テスト]を選択します。証明書が見つからないか無効であるためにDeep Securityが接続できないというエラーが表示された場合は、[証明書の追加/アップデート]を選択して、正しいDeep Discovery Analyzer証明書にアップデートします。
7. [Save]を選択します。

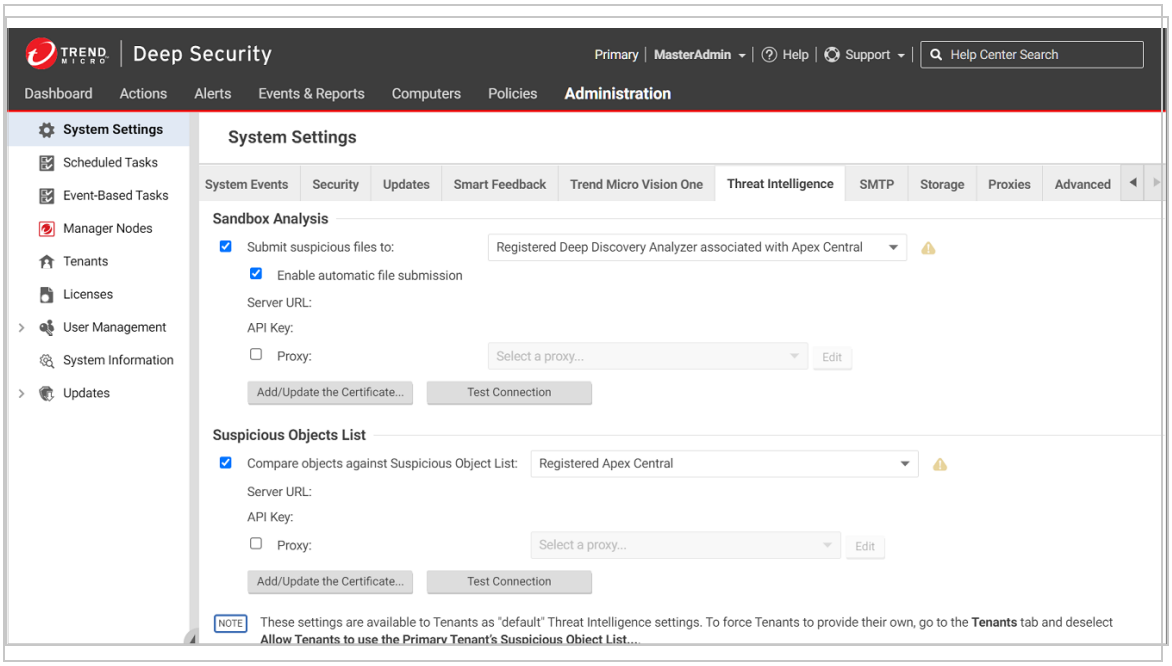
Trend Micro Apex Centralへの接続の設定

以下の設定を行うと、Deep Security ManagerでApex Centralから不審オブジェクトリストを取得し、保護されているコンピュータで共有して、ローカルオブジェクトをApex Centralの不審オブジェクトリストと照合できるようになります。

Trend Micro Apex Central がすでにDeep Securityを管理している場合

1. Deep Security Managerで、[管理]> [システム設定]> [脅威インテリジェンス]に移動します。
2. [オブジェクトを不審オブジェクトリストと比較する]を選択し、次に[Registered Apex Central]を選択します。

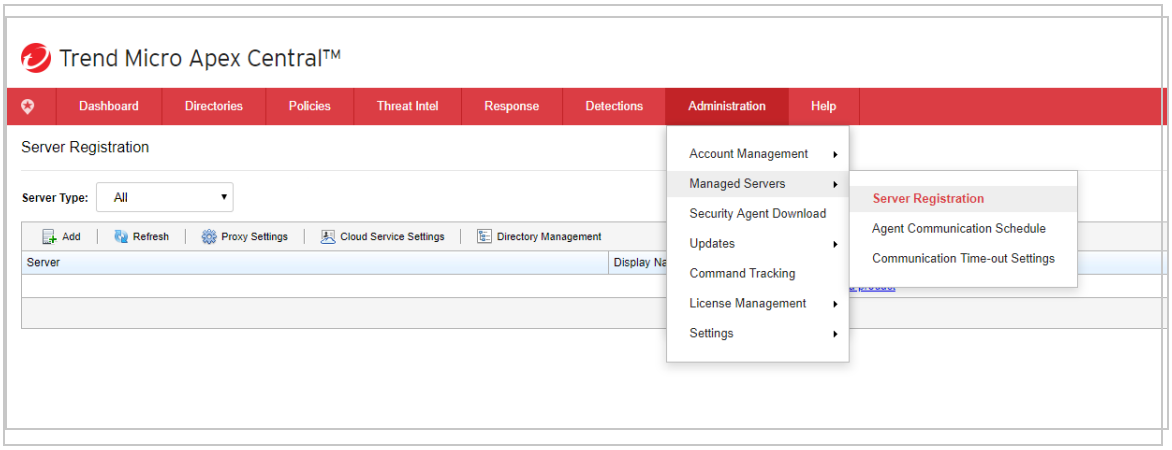
   ヒント: このオプションが利用できない場合、それはApex Centralはまだ Deep Securityを管理していないため、代わりに「Trend Micro Apex Centralがまだ Deep Securityを管理していない場合」(下記)の手順に従ってください。。



3. [接続テスト]を選択します。証明書が見つからないか無効であるためにDeep Securityで接続できないというエラーが表示された場合は、[証明書の追加/アップデート]を選択して、正しいトレンドマイクロの Apex Central 証明書にアップデートします。
4. [Save]を選択します。

Trend Micro Apex Central がまだDeep Securityを管理していない場合

1. Trend Micro Apex Centralから、[管理]→[管理下のサーバ]→[サーバの登録]に移動します。



2. [サーバの種類]ドロップダウンメニューで、[Deep Security]を選択します。
3. [Add]を選択して、Deep SecurityをApex Central サーバに登録します。

> 注意: Apex Centralは、Deep Securityを管理下の製品として追加してから10分以内に、Deep Securityの登録に必要なサービスURLとAPIキーを自動的に転送します。

脅威インテリジェンスで使用する不正プログラム検索設定を作成する

次の設定では、Deep Securityで不審ファイルを検出し、不審ファイルをバックアップして、サンドボックス分析 に送信して詳細な分析を依頼できます。

1. Deep Security Managerで、[Policies]→[共通オブジェクト]→[その他]→[不正プログラム検索設定] の順に選択します。
2. 新しい検索設定を作成するか、または既存の設定を編集します。
3. [一般] タブの [ドキュメントの脆弱性対策] で、[ドキュメントの脆弱性を突いた攻撃コードを検索する] を選択し、次のいずれかのオプションを選択します。
   - 既知の脆弱性に対する攻撃コードのみを検索する: 既知の重大な脆弱性のみを検出します。CVE 攻撃コード脆弱性タイプがこのオプションに関連付けられています(「"不正プログラム修復処理をカスタマイズする" on page 847」を参照してください) 。
   - 既知の脆弱性に対する攻撃に加え、未知の攻撃コードも積極的に検索する: より多くの問題が検出されますが、誤判定も増えます。不審ファイルを検出してTrend Micro Vision One または Deep Discovery Analyzerに送信する場合は、このオプションを選択する必要があります。アグレッシブ検出ルールの脆弱性タイプはこのオプションに関連付けられています(「"不正プログラム修復処理をカスタマイズする" on page 847」を参照してください) 。
4. 「"不正プログラム検索と除外の設定" on page 832」の説明に従って、その他の不正プログラム検索を設定します。

コンピュータで脅威インテリジェンスを有効にする

脅威インテリジェンスは、ポリシーまたは個々のコンピュータで有効にできます。

1. **コンピュータエディタまたはポリシーエディタ**[1]で、[不正プログラム対策]→[一般] の順に選択します。
2. 不正プログラム対策のステータスがオン または 継承 (オン) であることを確認します。
3. [一般] タブには、リアルタイム検索、手動検索、予約検索 の各セクションがあります。(検索の種類については、「"不正プログラム対策を有効化して設定する" on page 828を有効にして設定する」を参照してください) 。該当するセクションで、不正プログラム検索設定 リストから上記の手順で作成した検索設定を選択します。
4. [脅威インテリジェンス] タブに移動し、必要に応じて次の設定を調整します。
   - Deep Securityから不審なファイルをTrend Micro Vision OneまたはDeep Discovery Analyzerに送信する場合は、[サンドボックス分析] のオプションを [はい] または [継承 (はい)] に設定します。
   - Deep SecurityとTrend Micro Apex Central間の接続を設定済みで、Apex Centralの不審オブジェクトリストを使用して不正なファイルを検出する場合は、[不審オブジェクトリスト] の [不審オブジェクトリストを使用] を [はい] または [継承 (はい)] に設定します。
5. [Save]を選択します。

サンドボックス分析にファイルを手動で送信する

[イベントとレポート]→[イベント]→[不正プログラム対策イベント]→[検出ファイル] 画面に表示されるファイルを手動で送信できます。

1. 送信するファイルを選択し、[Analyze] ボタンを選択します。
2. 表示されるウィザードの手順に従います。
3. ファイルが送信された後に、[検出ファイル] 画面の [送信ステータス] 列で分析の進捗状況を確認できます。
4. 分析が完了すると、[送信ステータス] 列が「レポートの準備完了」になります。Results Ready リンクを選択すると、詳細を表示できます。

誤ったアラームを引き起こしたファイルを許可する

イベント&レポート>イベント> 不正プログラム対策 イベント>識別ファイル ページでファイルがマルウェアとして識別されているが、マルウェアではないことがわかっている場合は、そのファイルを、**コンピュータまた**

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

はポリシーエディタ[1]の不正プログラム対策 > [詳細] タブにあるドキュメントの脆弱性対策ルール例外 リストに追加できます。

ファイルを許可するには、そのファイルを右クリックして[Allow]を選択し、表示されるウィザードの手順に従います。

不審なファイルに対する検索処理を設定する

Trend Micro Vision One またはTrend Micro Apex Central コンソールで不審オブジェクトリストを表示し、不審オブジェクトが検出された場合の処理 (ログ、ブロック、または隔離) を設定できます。(処理の設定の詳細については、Trend Micro Vision One または Apex Centralのヘルプを参照してください) 。Trend Micro Vision One または Apex Centralから不審オブジェクトリストを取得するようにDeep Security Managerを設定している場合、不審オブジェクトが検出されると、Deep Securityは指定された処理を実行します。

注意: Deep Securityでは、ファイルが不審なオブジェクトがサポートされます。Webレピュテーション保護モジュールがTrend Micro Smart Protection Serverを使用するように設定されている場合、URL不審オブジェクトもサポートされます。IPが不審なオブジェクトとドメインが不審なオブジェクトはサポートされません。

Deep Securityで不審オブジェクトリストをアップデートする

不審オブジェクトの分析が完了し、ファイルに対する処理がTrend Micro Vision One またはTrend Micro Apex Centralで設定されている場合、Deep Securityでは、Trend Micro Vision Oneの不審オブジェクトリストを使用できます。 または Apex Central を使用してコンピュータを保護します。Deep Security Managerで手動で不審ファイルリストをアップデートするには、[管理]→[アップデート]→[セキュリティ] に進み、[不審オブジェクトリストのアップデート] 列の項目を使用して最新のリストを取得し、保護されたコンピュータに送信します。アップデートされたリストがないかを定期的に確認する予約タスクを作成することもできます ("Deep Security予約タスクの設定" on page 1826を参照してください)。

注意: Apex Centralにおける不審オブジェクトの初期設定は「ログ」です。この初期設定は、必要に応じて「隔離」または「ブロック」に変更できます。

[Trend Micro Vision One 脅威インテリジェンス不審オブジェクトManagement]では、右上隅で[Default Settings]を選択し、各リスクレベルでさまざまな種類のオブジェクトに対して実行する初期設

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (または ポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (または コンピュータを選択して [詳細] をクリック) します。

定の処理と、オブジェクト。Apex Centralにおける不審オブジェクトの初期設定は「ログ」です。この初期設定は、必要に応じて「隔離」または「ブロック」に変更できます。

Deep Securityで不審オブジェクトリストが更新され、指定された処理でコンピュータポリシーが更新されると、Deep Security Agentは影響を受けたコンピュータをチェックし、保護されたコンピュータでこのファイルが再び検出されるたびにこの処理を使用します。

マルチテナント環境での脅威インテリジェンスの設定

マルチテナント環境では、プライマリテナント(t0) のDeep Discovery AnalyzerおよびApex Centralの設定を他のテナントと共有するかどうかを選択できます。この動作を制御する設定は、管理>システム設定>テナント>プライマリテナントの不審オブジェクトリストとサンドボックス分析設定の使用をテナントに許可 です。

- 設定を有効にして、テナントが[管理]> [システム設定]> [脅威インテリジェンス]に移動すると、追加の[デフォルトのサーバー設定を使用する]チェックボックスが表示されます。このチェックボックスをオンにすると、プライマリテナントの設定が使用されます。デフォルトのサーバー設定を使用するが選択されていない場合、テナントは独自の脅威インテリジェンス設定を構成できます。

- プライマリテナントがTrend Micro Vision Oneを選択して不審ファイルを送信し、不審オブジェクトリストに対してオブジェクトを比較すると、テナントは、プライマリテナントのTrend Micro Vision Oneアカウントではなく、独自のTrend Micro Vision Oneアカウントに接続します。テナントがTrend Micro Vision One登録を完了していることを確認してください。

- この設定が有効になっていない場合、脅威インテリジェンスを使用するテナントは、独自のTrend Micro Vision One、またはTrend Micro Apex Central とDeep Discovery Analyzerを使用する必要があります。

サポートされているファイルタイプ

Deep Securityでは、次のファイルタイプをDeep Discovery Analyzerに送信できます。

- doc - Microsoft Word文書
- docx - Microsoft Office Word 2007文書
- gul - JungUm Global文書
- hwp - Hancom Hangul Word Processor (HWP) 文書
- hwpx - Hancom Hangul Word Processor 2014 (HWPX) 文書
- jar - JavaアプレットJavaアプリケーション
- js - JavaScriptファイル

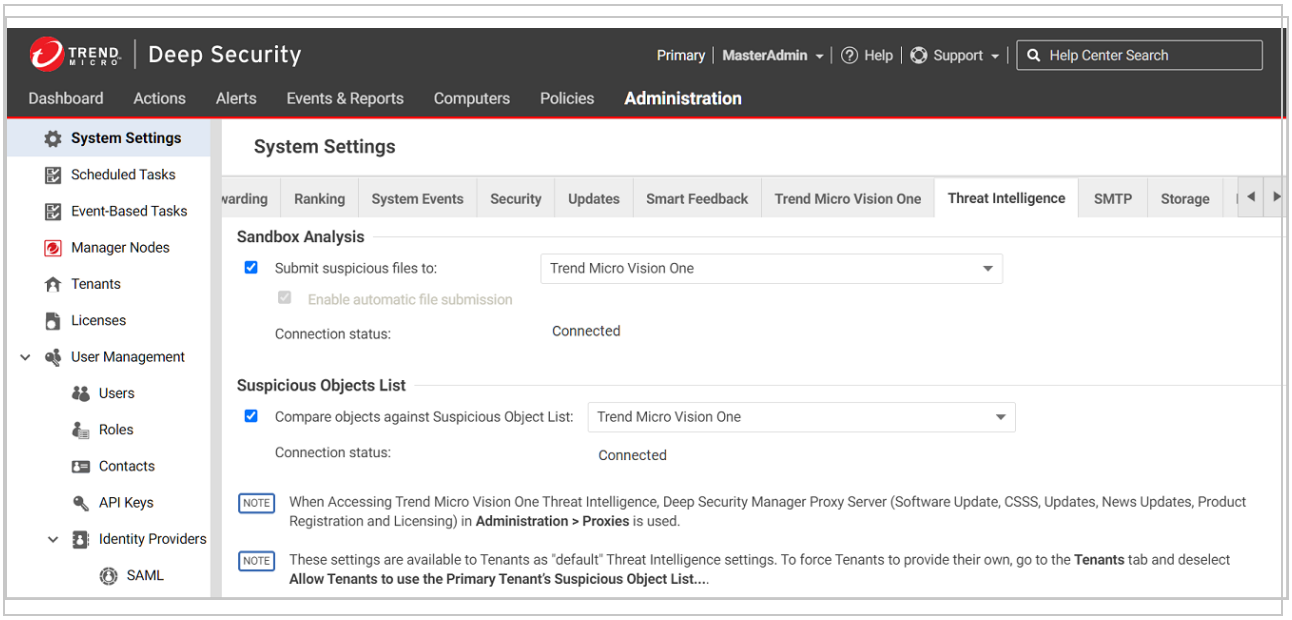
- jse - JavaScriptエンコード済みスクリプトファイル
- jtd - JustSystems一太郎ドキュメント
- lnk - Microsoft Windowsシェルバイナリ形式リンクショートカット
- mov - Apple QuickTimeメディア
- pdf - Adobeポータブルドキュメントフォーマット(PDF)
- ppt - Microsoft PowerPointプレゼンテーション
- pptx - Microsoft Office PowerPoint 2007プレゼンテーション
- ps1 - Microsoft Windows PowerShellスクリプトファイル
- rtf - Microsoftリッチテキスト形式(RTF)文書
- swf - Adobe Shockwave Flashファイル
- vbe - Visual Basicエンコード済みスクリプトファイル
- vbs - Visual Basicスクリプトファイル
- xls - Microsoft Excel表計算ファイル
- xlsx - Microsoft Office Excel 2007表計算ファイル
- xml - Microsoft Office 2003 XMLファイル

Connected Threat Defense から脅威インテリジェンスへの移行

脅威インテリジェンスは、Deep Security Manager 20.0.503(20 LTS Update 2021-09-23) で導入されました。ここでは、Connected Threat Defense がインストールされた以前のバージョンのDeep Security Managerから脅威インテリジェンスがインストールされた新しいバージョンにアップグレードする方法と、Trend Micro Vision One (XDR) への接続を設定する方法について説明します。

1. Deep Security Managerがに[Trend Micro Vision One(XDR) に登録されて]いることを確認します。
2. Deep Security Managerで、[管理]> [システム設定]> [脅威インテリジェンス]に移動します。
3. [不審なファイルを送信する]を選択し、次に[Trend Micro Vision One]を選択します。
4. [オブジェクトを不審オブジェクトリストと比較する]を選択し、次に[Trend Micro Vision One]を選択します。

5. [Save]を選択します。接続ステータスが15分以内に「接続済み」に変わります。



6. Deep Security Managerからファイルサンプルが送信されると、分析の概要がTrend Micro Vision Oneの[脅威インテリジェンス]→[サンドボックス分析]に表示されます。詳細については、Trend Micro Vision One ヘルプを参照してください。
7. 不審オブジェクトが検出された場合、生成された不審オブジェクトのリストは、[Trend Micro Vision One]の[脅威インテリジェンス]→[不審オブジェクトManagement]で確認できます。詳細については、Trend Micro Vision One ヘルプを参照してください。

マルチテナントの移行

マルチテナント環境でConnected Threat Defenseから脅威インテリジェンスに移行する場合:

- プライマリテナントでは、[管理]→[システム設定]→[テナント]→[プライマリテナントの不審オブジェクトリストとサンドボックス分析の設定の使用をテナントに許可]オプションを有効にしないでください。
- アップグレード後、他のすべてのテナントでDeep Security Managerを開き、に移動します。[管理]→[システム設定]→Trend Micro Vision Oneをクリックし、Deep Security ManagerがTrend Micro Vision One (XDR) に登録されていることを確認します。テナントは、管理>システム設定>脅威インテリジェンスで独自の脅威インテリジェンス設定を構成できます。

挙動監視による不正プログラム/ランサムウェア検索の強化

Deep Securityは、Deep Securityエージェントによって保護されているWindowsおよびLinuxマシンに適用できるセキュリティ設定を提供し、不正プログラムやランサムウェアの検出およびクリーン率を向上さ

せます。これらの設定により、不正プログラムのパターンマッチングを超えて、まだ不正プログラム対策パターンに追加されていない新たな不正プログラムを含む可能性のある疑わしいファイルを特定することができます (ゼロデイ攻撃として知られています)。

このページの内容:

- "強化された検索保護" below
- "強化された検索を有効にする" on the next page
- "強化スキャンで検出された問題に対処する" on page 876
- "Agentをインターネットに直接接続できない場合の対処" on page 881

不正プログラム対策モジュールの概要については、"不正プログラム対策について" on page 821を参照してください。

強化された検索保護

脅威の検出: 検出を回避するために、一部の不正プログラムはシステムファイルや既知のインストール済みソフトウェアに関連するファイルを変更しようとします。このような変更は、不正プログラムが正当なファイルの代わりをするため、見逃されることがよくあります。Deep Securityはシステムファイルやインストール済みソフトウェアをモニタし、不正な変更を検出して防止することができます。

アンチ攻撃コード: 不正プログラムの作成者は、信頼されたプロセスに特権アクセスを得て不正な活動を隠すために、ユーザーモードプロセスにフックする悪意のあるコードを使用することができます。不正プログラムの作成者は、昇格された特権を持つAPIを呼び出すDLLインジェクションを通じてユーザプロセスにコードを注入します。また、悪意のあるペイロードを供給してメモリ内でコード実行を引き起こすことにより、ソフトウェア攻撃コードへの攻撃を引き起こすこともできます。Deep Securityでは、アンチ攻撃コード機能が特定のプロセスによって通常行われないアクションを実行している可能性のあるプロセスを監視します。データ実行防止 (DEP)、構造化例外処理オーバーライト保護 (SEHOP)、およびヒープスプレー防止などの多くのメカニズムを使用して、Deep Securityはプロセスが侵害されたかどうかを判断し、その後さらなる感染を防ぐためにプロセスを終了させることができます。

拡張ランサムウェア対策: ランサムウェアはますます高度化し、標的型になっています。ほとんどの組織は、エンドポイントに不正プログラム対策を含むセキュリティポリシーを持っており、既知のランサムウェアの変種に対する一定の保護を提供します。しかし、新しい変種の発生を検出して防ぐには不十分な場合があります。Deep Securityが提供するランサムウェア対策は、文書の無許可の暗号化や変更から保護します。Deep Securityには、暗号化されているファイルのコピーを作成するオプションのデータ復旧エンジンも組み込まれており、ランサムウェアプロセスによって暗号化されたファイルを回復するための追加の機会をユーザに提供します。

強化された検索を有効にする

強化スキャンは、ポリシーまたは個々のコンピュータに適用される不正プログラム対策設定の一部として構成されています。不正プログラム対策の構成に関する情報については、"不正プログラム対策を有効化して設定する" on page 828を参照してください。

これらの設定は、Deep Security Agentで保護されているWindowsコンピュータおよびLinuxコンピュータにのみ適用できます。

注意: 強化スキャンは、負荷の高いアプリケーションを実行しているエージェントコンピュータのパフォーマンスに影響を与える可能性があります。強化スキャンを有効にしてDeep Securityエージェントを展開する前に、"不正プログラム対策のパフォーマンスを向上させる" on page 850を確認してください。

最初に、不正プログラムのリアルタイム検索設定で、強化された検索を有効にします。

1. Deep Security Managerで、[ポリシー]→[共通オブジェクト]→[その他]→[不正プログラム検索設定] の順に選択します。
2. 既存のリアルタイム検索設定をダブルクリックして編集します。不正プログラム検索設定の詳細については、"不正プログラム検索と除外の設定" on page 832を参照してください。
3. 一般タブの挙動監視で、挙動監視の有効化を選択します。
4. 実行するアクションを使用して、Deep Securityが不正プログラムを検出したときに実行する修復アクションを選択します
   - ActiveAction (推奨): ActiveActionが決定するアクションを使用します。ActiveActionは、各不正プログラムカテゴリに最適化された事前定義のクリーンアップアクションのグループです。トレンドマイクロは、個々の検出が適切に処理されるように、ActiveActionのアクションを継続的に調整しています。詳細については、"トレンドマイクロの推奨処理" on page 848を参照してください。
   - 許可: 感染ファイルに対して何もせずに完全なアクセスを許可します。不正プログラム対策イベントは引き続き記録されます。
5. 必要に応じて、ランサムウェアで暗号化されたファイルのバックアップと復元を選択します。このオプションを選択すると、Deep Securityはファイルがランサムウェアプロセスによって暗号化されている場合に備えて、暗号化されているファイルのバックアップコピーを作成します。このオプションは、Windowsを実行しているコンピュータにのみ適用されます。
6. [OK] をクリックします。

デフォルトでは、リアルタイムスキャンはすべてのディレクトリをスキャンするように設定されています。スキャン設定を変更してディレクトリリストをスキャンするように設定した場合、強化されたスキャンが期待通りに機能しない可能性があります。たとえば、[検索対象ディレクトリ] をFolder1に設定した場合に

Folder1でランサムウェアが発生すると、Folder1の外部にあるファイルがランサムウェアによって暗号化された場合、ランサムウェアが検出されない可能性があります。

次に、不正プログラム検索設定をポリシーまたは個々のコンピュータに適用します。

1. コンピュータエディタまたはポリシーエディタ[1]で、[不正プログラム対策]→[一般] の順に選択します。
2. 不正プログラム対策のステータスがオンまたは継承 (オン) に設定されていることを確認します。
3. 一般タブには、リアルタイム検索、手動検索、および予約検索のセクションが含まれています。適切なセクションで、不正プログラム検索設定を使用して作成した検索設定を選択します。
4. [保存] をクリックします。

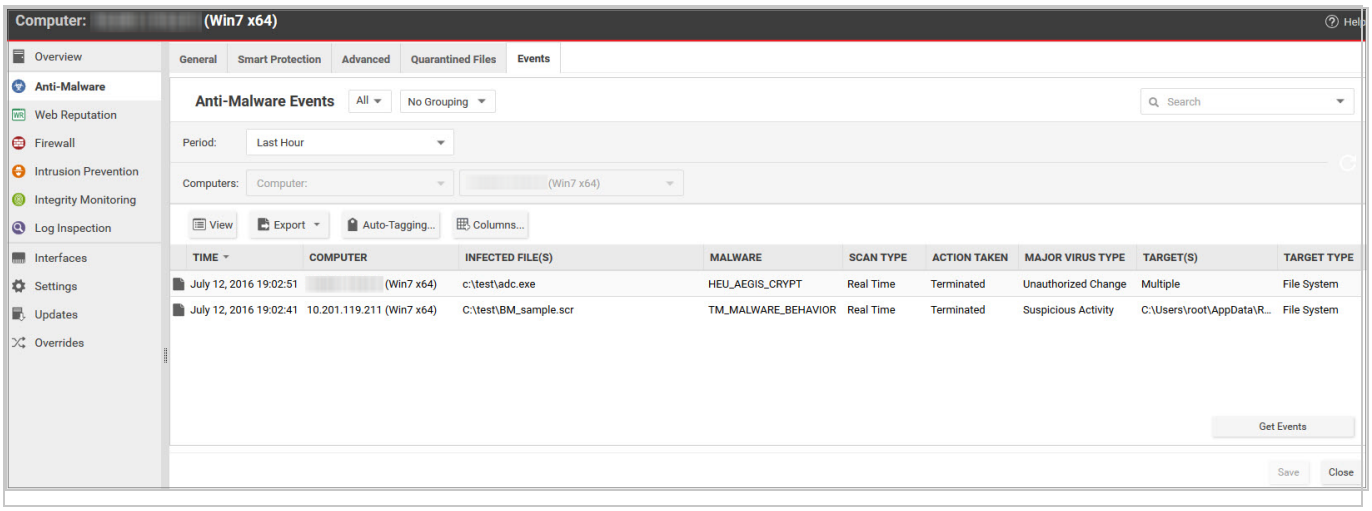
強化スキャンで検出された問題に対処する

Deep Securityが有効にした拡張スキャン設定に一致するアクティビティやファイルを検出すると、イベントを記録します。イベントの一覧を表示するには、イベント& レポート> イベント> 不正プログラム対策イベントに移動して確認できます。イベントは主要ウイルスタイプ列で疑わしいアクティビティまたは不正な変更として識別され、詳細はターゲットおよびターゲットタイプ列に表示されます。

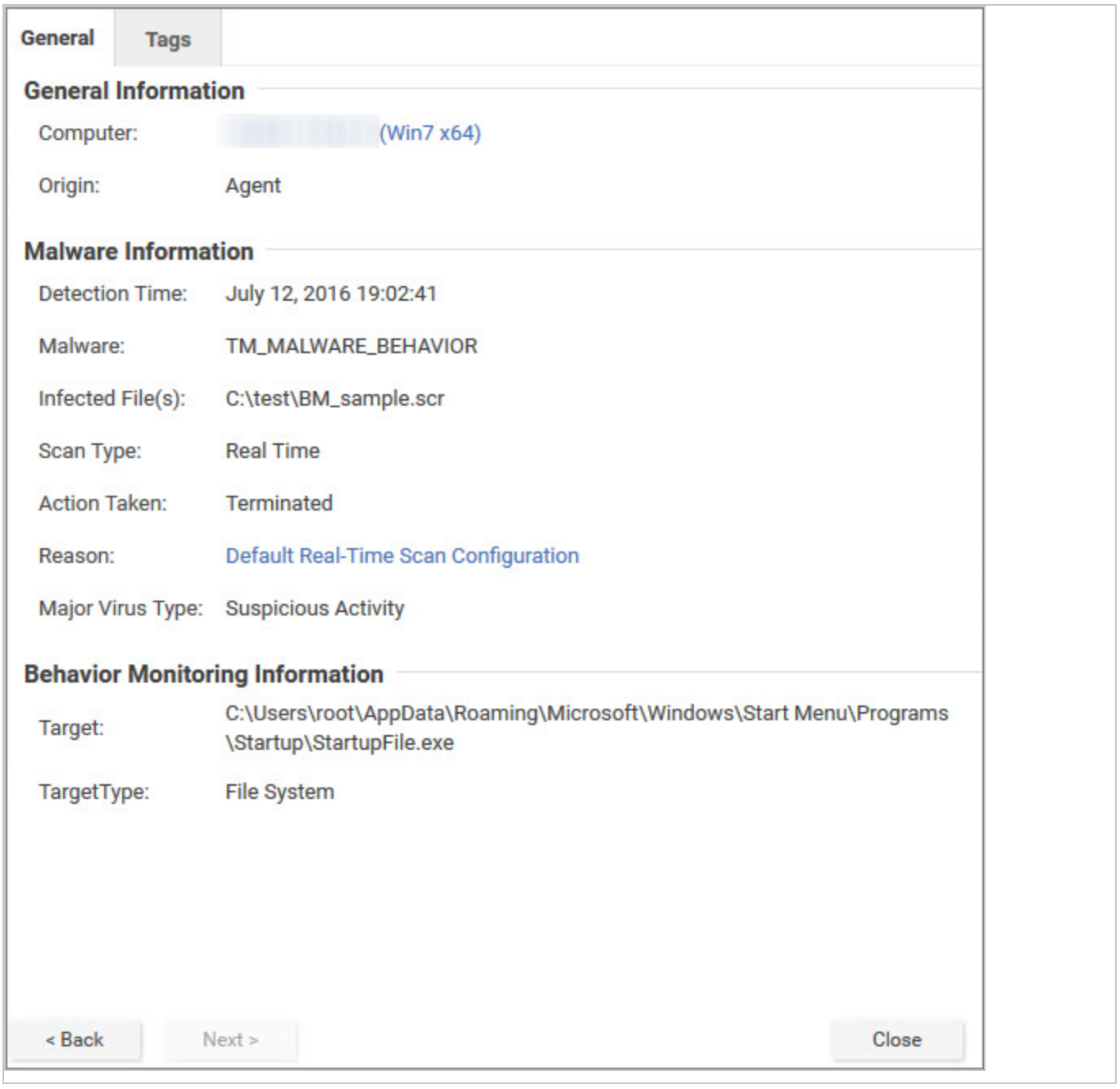
Deep Securityは、強化スキャン設定に関連する多くの種類のチェックを実行し、問題を発見したチェックの種類に応じてアクションを実行します。Deep Securityは、不審オブジェクトに対してアクセス拒否、終了、またはクリーンのいずれかのアクションを実行する場合があります。これらのアクションはDeep Securityによって決定され、クリーンアクションを除いて設定変更はできません

- アクセスを拒否: 不審なファイルをオープンまたは実行しようとする挙動を検知すると、ただちにその操作をブロックして不正プログラム対策イベントを記録します。
- [終了]: Deep Securityは、不審な操作を実行したプロセスを終了し、不正プログラム対策イベントを記録します。
- クリーン: Deep Securityは不正プログラム検索の設定を確認し、アクションタブで指定されたトロイの木馬に対するアクションを実行します。トロイの木馬ファイルに対して実行されたアクションに関連する1つ以上の追加イベントが生成されます。

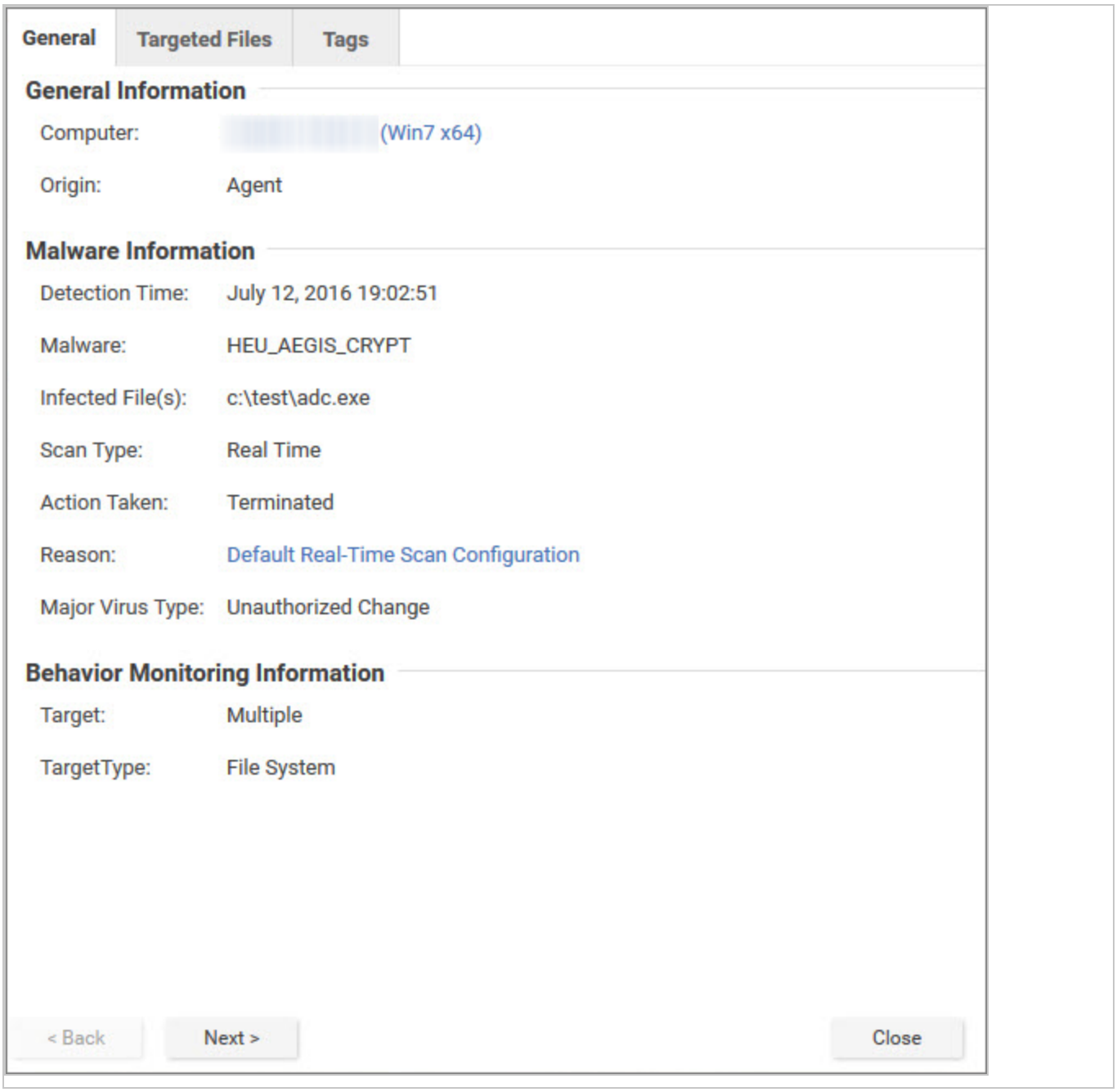
[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

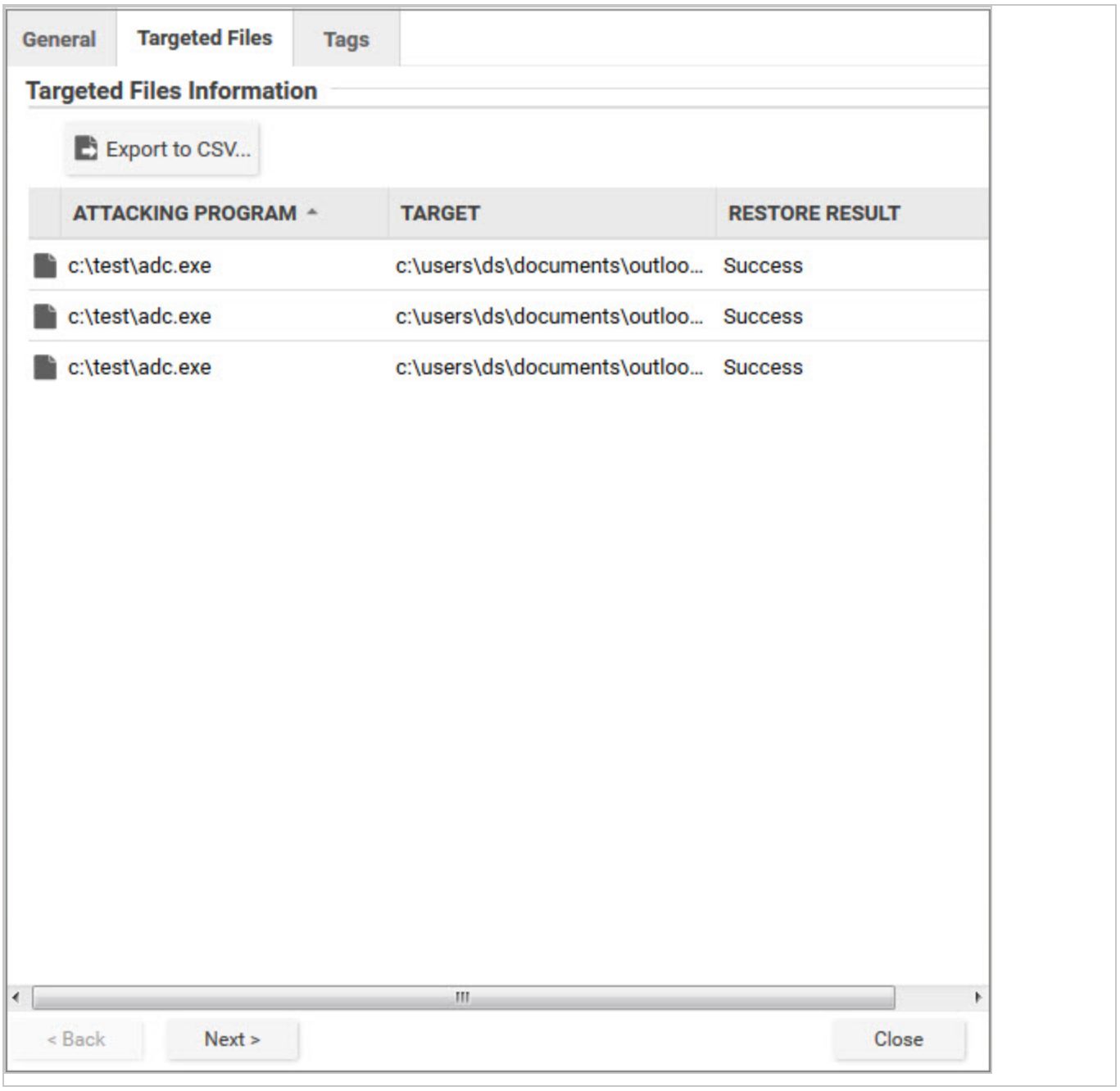


イベントをダブルクリックすると詳細が表示されます。



ランサムウェアに関連するイベントの場合は、[対象ファイル] タブが追加で表示されます。


General
Targeted Files
Tags
General Information
Computer:
(Win7 x64)
Origin:
Agent
Malware Information
Detection Time:
July 12, 2016 19:02:51
Malware:
HEU_AEGIS_CRYPT
Infected File(s):
c:\test\adc.exe
Scan Type:
Real Time
Action Taken:
Terminated
Reason:
Default Real-Time Scan Configuration
Major Virus Type:
Unauthorized Change
Behavior Monitoring Information
Target:
Multiple
TargetType:
File System
< Back
Next >
Close



特定されたファイルを調べて無害であることが判明した場合は、イベントを右クリックして[許可]をクリックし、コンピュータまたはポリシーの検索除外リストにそのファイルを追加します。検索除外リストは、ポリシーエディタまたはコンピュータエディタで[不正プログラム対策]→[詳細]→[挙動監視保護の例外]の順に選択して確認できます。

Agentをインターネットに直接接続できない場合の対処

このトピックで説明した強化された検索機能は、Global Census ServerとGood File Reputation Serviceでファイルをチェックするため、インターネットへのアクセスを必要とします。Deep Security Agentがインターネットに直接アクセスできない場合は、"インターネットにアクセスできないAgentを設定する" on page 1504で回避策について参照してください。

Deep SecurityのSmart Protection

Smart Protection Networkの統合は、不正プログラム対策およびWebレピュテーションモジュールを通じて、コンピュータとワークロードで利用可能です。システムレベルで設定されるスマートフィードバックにより、Smart Protection Networkに継続的なフィードバックを提供できます。

トレンドマイクロのSmart Protection Networkの詳細については、「Smart Protection Network」を参照してください。

このトピックの内容:

- "不正プログラム対策とSmart Protection" below
- "Webレピュテーションとスマートフィードバック" on page 883
- "スマートフィードバック" on page 884

Smart Protection Serverのドキュメントを参照してください。

不正プログラム対策とSmart Protection

- スマートスキャンの利点
- "スマートスキャンを有効にする" on the next page
- "ファイルレピュテーションサービス用のSmart Protection Server" on page 883

スマートスキャンの利点

スマートスキャンには、次の機能と利点があります。

- クラウドでのリアルタイムのセキュリティステータス検索機能を提供します。
- 新たな脅威に対する保護の提供にかかる全体的な時間を短縮します。
- パターンファイルのアップデート中に消費されるネットワーク帯域幅を削減します。パターン定義のアップデートの大部分はクラウドに配信するだけでよく、多くのエンドポイントに配信する必要はあ

りません。

- 企業全体のパターン配信に関連するコストとオーバーヘッドを削減します。

スマートスキャンを有効にする

スマートスキャンは、不正プログラム対策モジュールで使用できます。トレンドマイクロのSmart Protection Networkを利用して、ローカルのパターンファイルを小さくし、エージェントおよびアプライアンスに必要なアップデートのサイズと数を削減します。スマートスキャンを有効にすると、エージェントはトレンドマイクロのアップデートサーバから不正プログラムパターンの小さいバージョンをダウンロードします。この小さいパターンは、*ファイルを確認済みの安全または危険の可能性あり*として迅速に識別できます。危険の可能性のあるファイルは、トレンドマイクロのSmart Protection Serverに保存されている、より大きい完全なパターンファイルと照合され、危険性があるかどうかを確実に判断します。

スマートスキャンが有効でない場合、Relayエージェントはトレンドマイクロのアップデートサーバから完全な不正プログラムパターンをダウンロードし、エージェントでローカルに使用する必要があります。パターンは、スケジュールされたセキュリティアップデートが処理されるときにのみ更新されます。パターンは通常、エージェントがダウンロードするために1日1回更新され、約120 MBです。

コンピュータがグローバルなトレンドマイクロSmart Protection NetworkのURLに確実に接続できることを確認してください。詳細については、"ポート番号、URL、およびIPアドレス" on page 428を参照してください。接続がファイアウォール、プロキシ、またはAWSセキュリティグループによってブロックされている場合、または接続が不安定な場合、不正プログラム対策のパフォーマンスが低下します。

1. [ポリシー] に移動します。
2. ポリシーをダブルクリックします。
3. [不正プログラム対策]→[Smart Protection] の順に選択します。
4. [スマートスキャン] セクションで、次のいずれかを実行します。
   - [継承] を選択します (親ポリシーでスマートスキャンが有効になっている場合)。
   - [継承] の選択を解除し、[オン] または Deep Security Agentの場合は [オン]、Virtual Applianceの場合は [オフ] を選択します。
5. [保存] をクリックします。

注意: スマートスキャンを使用するように設定されているコンピュータでは、完全な不正プログラム対策パターンがローカルにダウンロードされません。したがって、コンピュータがスマートスキャンを使用するように設定されている間に不正プログラム対策ライセンスの有効期限が切れた場合、スマートスキャンをオフにしても、不正プログラムの検索にローカルパターンは使用されません。これは、不正プログラム対策パターンがローカルに存在しないためです。

ファイルレピュテーションサービス用のSmart Protection Server

ファイルレピュテーションサービス用のSmart Protection Serverは不正プログラム対策モジュールで利用可能です。これはスマートスキャンに必要なファイルレピュテーション情報を提供します。

Smart Protection Server for File Reputation Serviceは次のように編集します。

1. [コンピュータ] または [ポリシー]→[不正プログラム対策]→[Smart Protection] の順に選択します。
2. トレンドマイクロのSmart Protection Serverに直接接続するか、ローカルにインストールされた1つ以上のSmart Protection Serverに接続するかを選択します。
3. エージェントとSmart Protection Network間の通信にプロキシを使用する場合は、Smart Protection Network専用のプロキシサーバを作成する必要があります。使用可能なプロキシのリストは、[管理]→[システム設定]画面の [プロキシ] タブで表示および編集できます。プロキシプロトコルの詳細については、「"サポートされるプロキシプロトコル" on page 1456」を参照してください。
4. ドメイン外の場合、グローバルSmart Protectionサービスに接続する(Windowsのみ) オプションを選択して、コンピュータがドメイン外の場合にグローバルSmart Protectionサービスを使用します。コンピュータがドメインコントローラに接続できない場合、ドメイン外と見なされます(このオプションはWindowsエージェントのみ対象です) 。
5. コンピュータからSmart Protection Serverへの接続が失われたときにエラーイベントとアラートを生成するには、[Smart Protection Server接続の警告]を設定します。

WebレピュテーションとSmart Protection

WebレピュテーションサービスのSmart Protection ServerはWebレピュテーションモジュールに必要なWebレピュテーション情報を提供します。

Smart Protection Server for Webレピュテーションサービスは次のように編集します。

1. [コンピュータ] または[ポリシー]→[不正プログラム対策]→[Smart Protection] の順に選択します。
2. トレンドマイクロのSmart Protection Serverに直接接続するか、ローカルにインストールされた1つ以上のSmart Protection Serverに接続するかを選択します。
3. エージェントとSmart Protection Network間の通信にプロキシを使用する場合は、Smart Protection Network専用のプロキシサーバを作成する必要があります。使用可能なプロキシのリストは、[管理]→[システム設定]画面の [プロキシ] タブで表示および編集できます。プロキシプロトコルの詳細については、「"サポートされるプロキシプロトコル" on page 1456」を参照してください。
4. コンピュータがドメイン外の場合にグローバルSmart Protection Serviceを使用するには、[ドメイン外の場合はグローバルSmart Protection Serviceに接続する(Windowsのみ)]を選択します。コンピュータがドメインコントローラに接続できない場合、そのコンピュータはドメイン外であると見なされます (このオプションはWindowsエージェント専用です)。

5. コンピュータからSmart Protection Serverへの接続が失われたときにエラーイベントとアラートを生成するには、[Smart Protection Server接続の警告]を設定します。

スマートフィードバック

トレンドマイクロスマートフィードバックは、トレンドマイクロ製品と、24時間体制の脅威リサーチセンターおよび技術部門との間に継続的な通信を提供します。スマートフィードバックでは、脅威に関する膨大なデータの共有とリアルタイム分析を行うTrend Micro Smart Protection Networkの一部として製品が機能します。この相互接続により、毎日発生する何千もの新しい脅威とその変種/亜種の分析、特定、および阻止を、これまでにない速さで実行できます。

トレンドマイクロスマートフィードバックは、Deep Security Managerのシステム設定として有効にできます。スマートフィードバックを有効にすると、保護された脅威情報がSmart Protection Networkと共有されるため、トレンドマイクロは新しい脅威を迅速に特定し、対処することができます。初期設定では、スマートフィードバックは有効になっています。[管理]→[システム設定]→[スマートフィードバック]に移動すると、この設定を無効にしたり、調整したりできます。

スマートフィードバックでは、[管理]→[アップデート]→[Relay管理]の順に選択して、Relayグループのプロパティ領域にあるアップデート元プロキシを使用します。詳細については、「プロキシ経由でプライマリセキュリティアップデート元に接続する」を参照してください。

不正プログラムの処理

検出した不正プログラムの確認と復元

特定されたファイルとは、不正プログラムまたは不正プログラムを含むことが検出されたため、暗号化され、保護対象コンピュータの特別なフォルダに移動されたファイルです。感染ファイルを表示および復元できるかどうかは、不正プログラム対策の設定とファイルが検出されたオペレーティングシステムによって異なります。

- Windows Agentでは、"不正プログラム修復処理をカスタマイズする" on page 847されたファイルを表示して復元できます。
- Linux Agentでは、隔離されたファイルのみを表示して復元できます。

このページのトピック:

- "検出ファイルのリストを参照する" on the next page
- "検出ファイルを処理する" on page 886
- "検出ファイルを検索する" on page 887

- "検出ファイルを復元する" on page 888
- "検出ファイルを手動で復元する" on page 891

不正プログラム検出時に生成されるイベントの詳細については、"不正プログラム対策イベント" on page 1402を参照してください。

検出ファイルのリストを参照する

[イベントとレポート] 画面には、特定されたファイルのリストが表示されます。そこから、これらのファイルの詳細を確認できます。

1. [イベントとレポート] →[イベント]→[不正プログラム対策イベント] →[検出ファイル] の順にクリックします。
2. ファイルの詳細を確認するには、ファイルを選択して [表示] をクリックします。

検出ファイルのリストには、次の情報が表示されます。

- 感染ファイル: 感染ファイルの名前と特定のセキュリティ上のリスクを表示します。
- 不正プログラム: 感染した不正プログラムを表示します。
- コンピュータ: 感染の疑いがあるコンピュータ名を表示します。
- ファイルステータス: ファイルをダウンロードする準備ができているかどうかを示します。

[詳細] 画面には次の情報が表示されます。

- 検出時刻: 感染コンピュータで感染が検出された日時。
- 感染ファイル: 感染ファイルの名前。
- ファイルのSHA-1: ファイルのSHA-1ハッシュ。
- 不正プログラム: 検出された不正プログラムの名前。
- 検索の種類: 不正プログラムを検出した検索の種類 (リアルタイム検索、予約検索、または手動検索のいずれか)。
- 実行された処理: 不正プログラムが検出されたときにDeep Securityが実行した処理の結果。
- コンピュータ: このファイルが検出されたコンピュータ(コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- コンテナ名: 不正プログラムが検出されたDockerコンテナの名前。
- コンテナID: 不正プログラムが検出されたDockerコンテナのID。
- コンテナイメージ名: 不正プログラムが検出されたDockerコンテナのイメージ名。

検出ファイルを処理する

[識別されたファイル]ページでは、識別されたファイルに関連するタスクを管理できます。メニューバーまたはコンテキストメニューを使用して、次の操作を実行できます。

- 特定されたファイルを元の場所と状態に復元します。ホストがAgent/Applianceからの通信を使用している場合は、この処理を実行できないことに注意してください。
- ダウンロード検出ファイルをコンピュータまたはVirtual Applianceから任意の場所にダウンロードする。ファイルをダウンロードするには：
  a. ダウンロードするファイルを選択します。
  b. ダウンロード>ダウンロードのリクエストに移動します。ファイルステータス列は、ダウンロードが保留中であることを示します。
  c. ファイルのダウンロード準備が完了すると、[ファイルのステータス]列が[ダウンロードの準備完了]に変わり、システムイベント[検出ファイルのダウンロードの準備完了]が表示されます。
  d. ダウンロードする準備ができている識別されたファイルを選択します。
  e. ダウンロード>ダウンロードに移動します。

  ファイルをダウンロードする準備ができたら、24時間以内にファイルを選択した場所にダウンロードできます。

- 分析 コンピュータまたはVirtual Applianceからの検出ファイルを分析する。
- 特定された1つ以上のファイルをコンピュータまたはVirtual Applianceから削除します。ホストがAgent/Applianceからの通信を使用している場合は、この処理を実行できないことに注意してください。
- 特定されたファイル(ファイル自体ではありません)に関する情報をCSVファイルにエクスポートします。
- 表示 検出ファイルの詳細を表示する。
- コンピュータの詳細 不正プログラムが検出されたコンピュータの画面を表示する。
- 不正プログラム対策イベントの表示 この検出ファイルに関連する不正プログラム対策イベントを表示する。

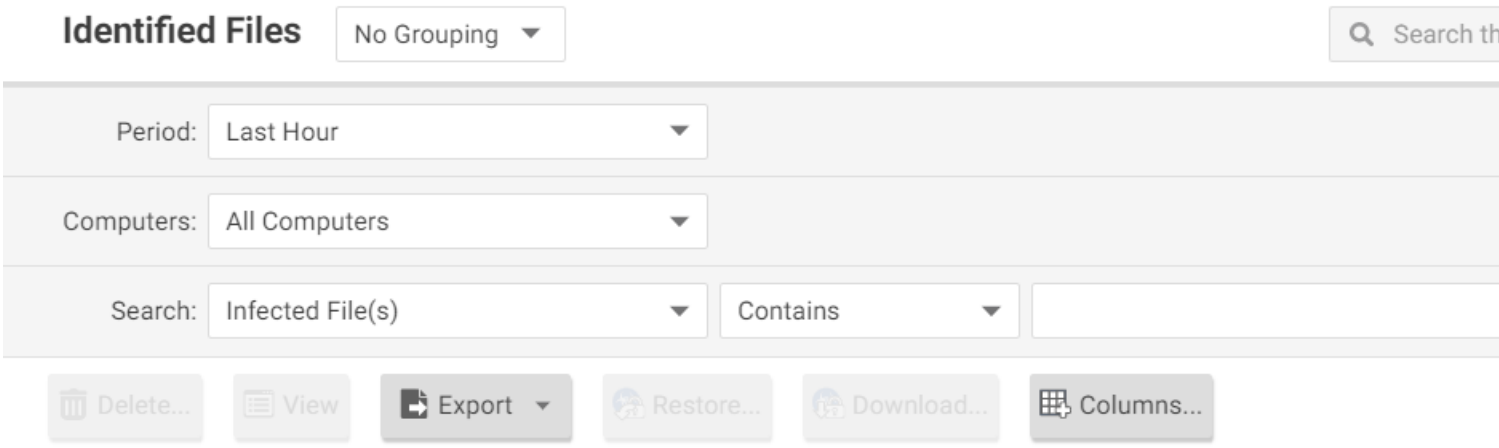
- 列の追加/削除 [追加]/[削除] をクリックして列を追加または削除する。
- 検索 特定の検出ファイルを検索する。

検出されたファイルは、次の場合にDeep Security Virtual Applianceから自動的に削除されます。

- 仮想マシンがvMotionによって別のESXiホストに移動されました。その仮想マシンに関連付けられている特定のファイルが仮想アプライアンスから削除されます。
- Deep Security Managerから仮想マシンが非アクティブ化されました。その仮想マシンに関連付けられている特定のファイルが仮想アプライアンスから削除されます。
- Deep Security Virtual ApplianceがDeep Security Managerから無効化されています。その仮想アプライアンスに保存されている特定されたファイルがすべて削除されます。
- Deep Security Virtual ApplianceがvCenterから削除されます。その仮想アプライアンスに保存されている、識別されたすべてのファイルが削除されます。

検出ファイルを検索する

- [期間] ドロップダウンメニューを使用すると、特定の期間内で検出されたファイルのみを表示できます。
- [コンピュータ] ドロップダウンメニューを使用すると、コンピュータグループまたはコンピュータポリシー別にファイルを表示できます。
- [このページを検索]→[詳細検索を開く] をクリックすると、詳細検索オプションの表示を切り替えることができます。



詳細検索には、検出ファイルのフィルタリングに使用する検索条件が1つ以上含まれます。各条件は、次の項目から構成される論理文になります。

- ファイルの種類 (感染ファイルまたは不正プログラム) や感染したコンピュータなど、フィルタ対象の検出ファイルの特性
- 演算子:
  - 次の文字列を含む: 選択した列の入力内容に検索文字列が含まれる。
  - 次の文字列を含まない: 選択した列の入力内容に検索文字列が含まれない。
  - 次の文字列に等しい: 選択した列の入力内容と検索文字列が完全に一致する。
  - 次の文字列に等しくない: 選択した列の入力内容が検索文字列と一致しない。
  - 次のリストに含まれる: 選択した列の入力内容がカンマ区切りで入力された検索文字列1つと完全に一致する。
  - 次のリストに含まれない: 選択した列の入力内容がカンマ区切りで入力されたどの検索文字列とも一致しない。
- 値

条件を追加するには、最上部の条件の右側にある「プラス」ボタン (+) をクリックします。検索するには、検索ボタン (環状矢印) をクリックします。

注意: 検索では大文字と小文字は区別されません。

検出ファイルを復元する

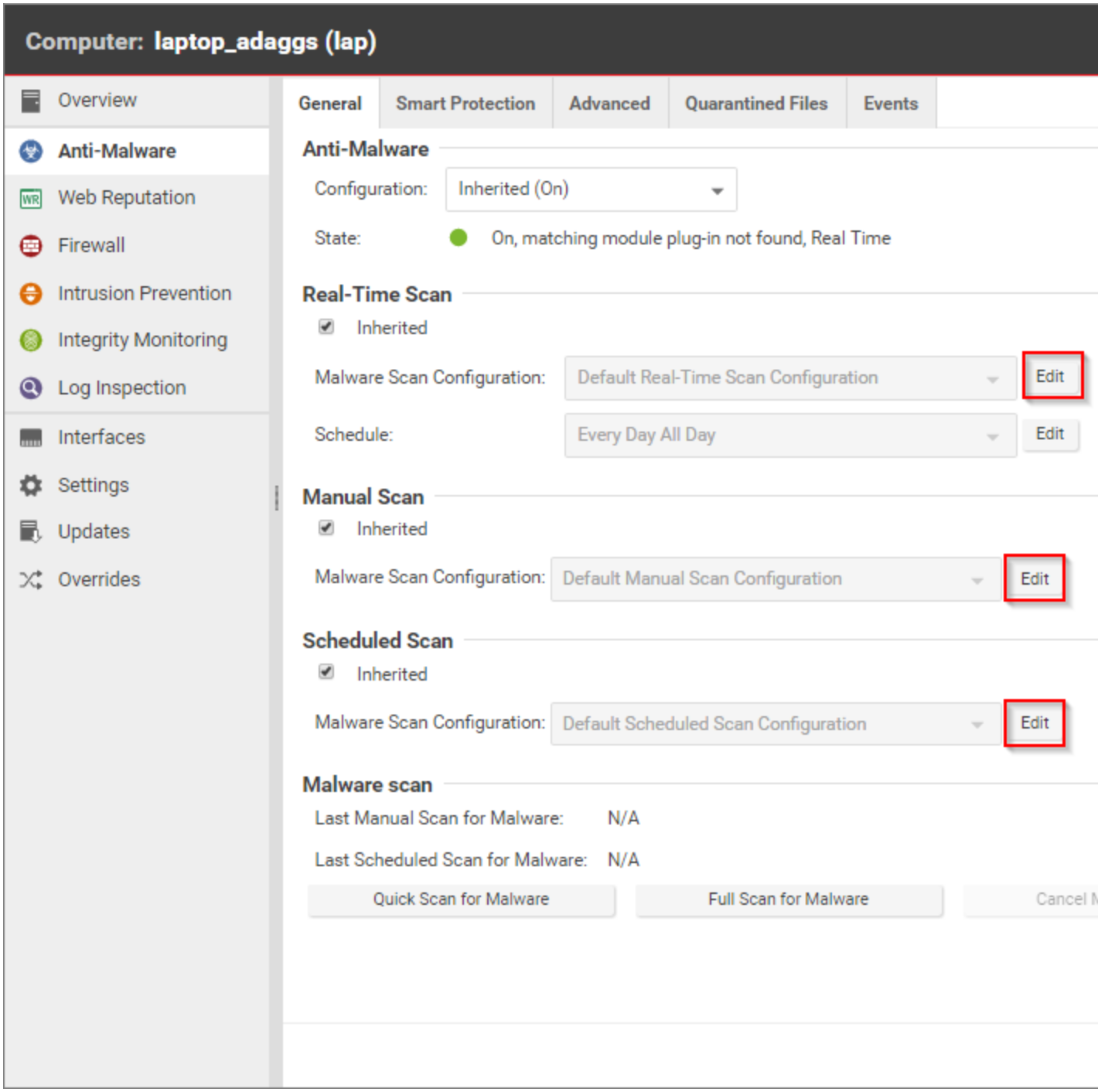
ファイルの検索除外を作成する

ファイルを元の場所に復元する前に、検索除外を作成して、そのファイルがコンピュータに復元されたときにDeep Securityによってただちに再検出されないようにする必要があります。

注意: 以下の手順は個々のコンピュータ上でファイルの検索除外を作成する方法を示していますが、同じ設定変更をポリシーレベルで行うこともできます。

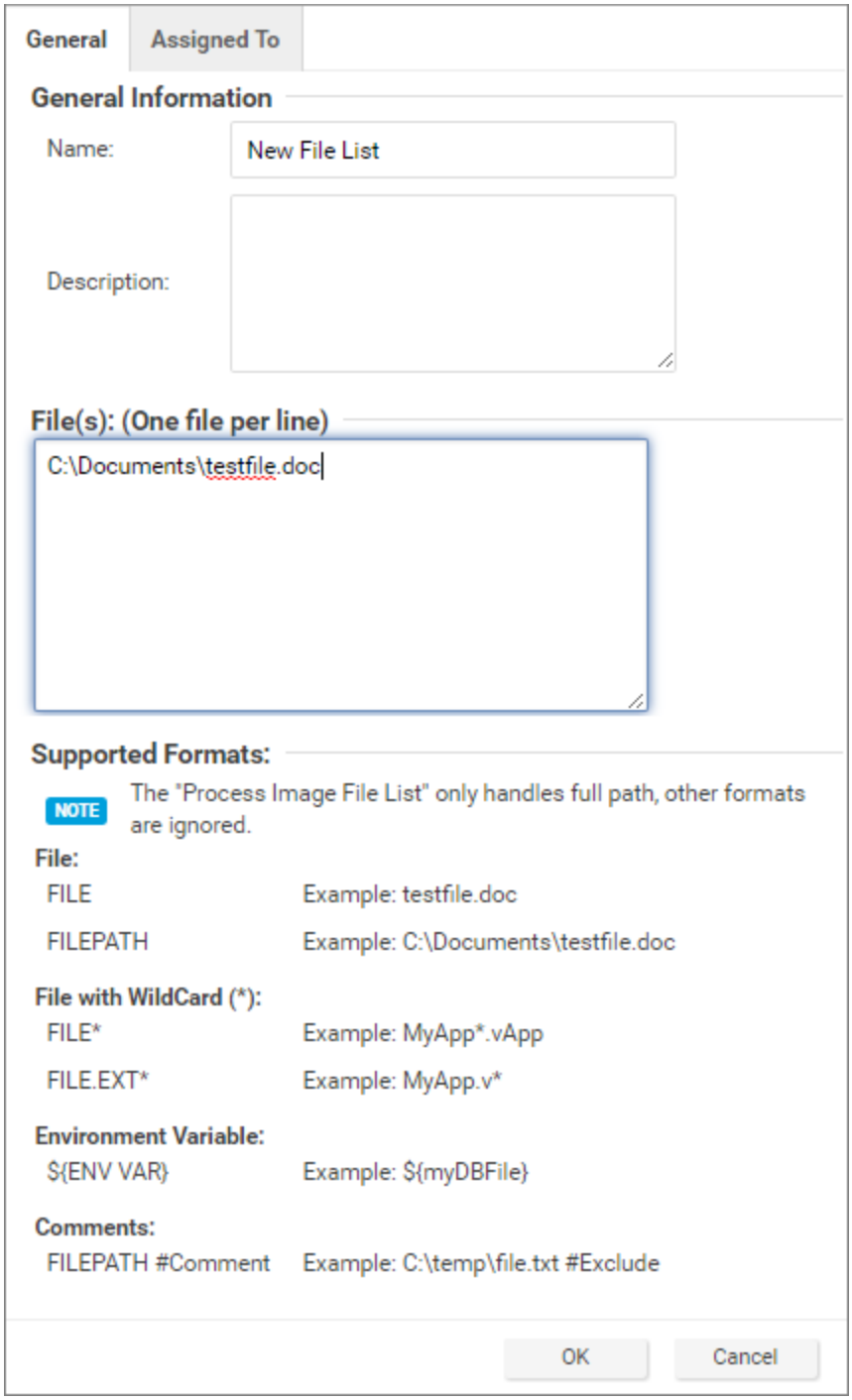
1. [コンピュータ] 画面を開き、[不正プログラム対策]→[検出ファイル] に進み、検出ファイルをダブルクリックしてそのプロパティを表示します。
2. ファイルの正確な名前と元の場所を書き留めます。
3. [コンピュータ] 画面を表示したまま、[不正プログラム対策]→[一般] に進み、有効になっている各不正プログラム検索の横にある [編集] ボタンをクリックし、[不正プログラム検索設定] プロパティ

画面を開きます。



4. [不正プログラム検索設定]プロパティ画面で、[検索除外]タブをクリックします。
5. [検索除外]エリアで、[ファイルリスト]を選択します。次に、[編集]をクリック(ファイルリストがすでに選択されている場合)するか、メニューから[新規]を選択します(新しいファイルリストを作成する場合)。

6. [ファイルリスト] プロパティ画面で、復元するファイルのパスと名前を入力します。[OK] をクリックして [ファイルリスト] プロパティ画面を閉じます。



7. [OK] をクリックして [不正プログラム検索設定] プロパティ画面を閉じます。
8. すべての [不正プログラム検索設定] の編集が終わった後、[コンピュータ] 画面で [保存] をクリックし、変更を保存します。これでファイルを復元する準備ができました。

ファイルを復元する

1. [コンピュータ] 画面を表示したまま、[不正プログラム対策]→[検出ファイル] タブに進みます。
2. 検出ファイルを右クリックして [処理]→[復元] を選択し、ウィザードの手順に従います。

これでファイルが元の場所に復元されます。

検出ファイルを手動で復元する

検出ファイルを手動で復元するには、そのファイルをコンピュータにダウンロードします。[検出ファイル] ウィザードに、管理ユーティリティへのリンクが表示されます。このユーティリティを使用して、ファイルの復号、検査、および復元を行うことができます。検出ファイル復号ユーティリティを使用してファイルを復号し、元の場所に戻します。

復号ユーティリティは、a zipファイル QFAdminUtil_win32.zip内にあります。このファイルは、Deep Security Managerのルートディレクトリにある「util」フォルダにあります。圧縮ファイルには、同じ機能を持つ2つのユーティリティが含まれています。QDecrypt.exeとQDecrypt.comです。QDecrypt.exeを実行するとファイルを開くウィンドウが呼び出され、復号するファイルを選択できます。QDecrypt.comは次のオプションを持つコマンドラインユーティリティです。

- /h, --help: このヘルプメッセージを表示
- --verbose: 詳細なログメッセージを生成
- /i, --in=<str>:復号する検出ファイル。<str>は検出ファイルの名前です。
- /o, --out=<str>:復号したファイルの出力。<str>は復号されたファイルに付けられる名前です。

注意: このユーティリティは、Windows 32ビットシステムおよびWindows 64ビットシステムでサポートされています。

高度な攻撃コードの除外を設定する

不正プログラムと同じ特徴があると、不正ではないファイルが不正プログラムに誤って識別される場合があります。安全なことがわかっていて、不正プログラムに識別されてしまう場合は、そのファイルの例外を作成できます。例外が作成されると、ファイルはDeep Securityがファイルを検索する際にイベントをトリガしません。

不正プログラム対策モジュールの概要については、"不正プログラム対策について" on page 821を参照してください。

リアルタイム検索、手動検索、および予約検索からファイルを除外することもできます。詳細については、「"検索対象ファイルを指定する" on page 838」を参照してください。

次の不正プログラムおよび不正プログラム検索の種類について、例外を作成できます。

- 機械学習型検索。詳細については、「"機械学習型検索を使用した脅威の検出" on page 859」を参照してください。
- ドキュメントの攻撃コード対策検索。詳細については、「"脅威インテリジェンスを使用した新たな脅威の検出" on page 861」を参照してください。
- スパイウェアとグレーウェアを検索します。詳細については、「"スパイウェア/グレーウェアを検索する" on page 835」を参照してください。
- 挙動監視保護。詳細については、「"挙動監視による不正プログラム/ランサムウェア検索の強化" on page 873」を参照してください。

信頼された証明書で署名されているファイルは、不正プログラム対策から除外することもできます。この機能は、WindowsのDeep Security Agent 20.0.0-3445以降でサポートされています。詳細については、「"信頼された証明書で署名されたファイルを除外する" on page 896」を参照してください。

Deep Securityは、ポリシーおよびコンピュータの各プロパティで検索される不正プログラムの種類ごとに除外リストを保持します。

1. 例外のリストを表示するには、ポリシーまたはコンピュータのエディタを開きます。
2. [不正プログラム対策]→[詳細]の順にクリックします。
   例外は、[許可するスパイウェア/グレーウェア]、[ドキュメントの脆弱性対策ルールの例外]、[機械学習型検索の検出除外対象]、[挙動監視保護の例外]、と[信頼された証明書の検出の除外]セクション。

"検索除外の推奨設定" on page 896も参照してください。

不正プログラム対策イベントから例外を作成する

ファイルが不正プログラムとして識別されると、不正プログラムDeep Securityイベントが生成されます。ファイルが無害であることがわかっている場合は、次の手順に従って、イベントレポートからファイルの除外を作成できます。

1. [イベントとレポート]→[イベント]→[不正プログラム対策イベント]の順にクリックして、不正プログラム検出イベントを特定します。
2. 該当するイベントを右クリックします。
3. [許可]を選択します。

不正プログラム対策の例外を手動で作成する

スパイウェア/グレーウェア、ドキュメントの脆弱性対策ルール、機械学習型検索、および挙動監視の例外について、不正プログラム対策の例外を手動で作成できます。例外を追加するには、検索によって生成された不正プログラム対策イベントの特定の情報が必要です。不正プログラムまたは検索の種類によって、次の情報が必要になります。

- スパイウェアまたはグレーウェア: [MALWARE] フィールドの値 (例: SPY_CCFR_CPP_TEST.A)
- ドキュメントの脆弱性対策ルール: [MALWARE] フィールドの値 (HEUR_OLEP.EXEなど)
- 機械学習型検索: FILE SHA-1フィールドのファイルのSHA1ダイジェスト(例: 3395856CE81F2B7382DEE72602F798B642F14140)
- 挙動監視: プロセスイメージパス(C:\test.exeなど)

1. [イベントとレポート]→[イベント]→[不正プログラム対策イベント] の順にクリックして、不正プログラムの識別に必要なフィールド値をコピーします。
2. 例外を作成するポリシーまたはコンピュータのエディタを開きます。
3. [不正プログラム対策]→[詳細] の順にクリックします。
4. [許可するスパイウェア/グレーウェア]、[ドキュメントの脆弱性対策ルールの例外]、[機械学習型検索の検出除外対象]、または [挙動監視保護の例外] セクションのテキストボックスにイベントの情報を入力します。
5. [追加] をクリックします。

除外リストのワイルドカードのサポート

挙動監視保護の除外 リストでは、ファイルパス、ファイル名、およびファイル拡張子の除外の種類を定義するときに、ワイルドカード文字を使用できます。次の表を使用して除外リストを適切にフォーマットし、正しいファイルとフォルダが検索から除外されるようにします。

サポートされるワイルドカード文字:

- アスタリスク(*) : 任意の文字または文字列を表します。

挙動監視保護の除外リストでは、ワイルドカード文字を使用してシステムドライブの指定を置き換えたり、UNC (Universal Naming Convention) アドレス内でワイルドカード文字を使用することはできません。

除外の種類	ワイルドカードの使用	一致	一致しません
ディレクトリ	`C:\*` 指定したドライブ上のすべてのファイルとフォルダを除外します。	• C:\sample.exe • C:\folder\test.doc	• D:\sample.exe • E:\folder\test.doc
特定のフォルダレベルにある特定	`C:\*\Sample.exe` Sample.exe ファイルが	• C:\files\Sample.exe • C:\temp\files\Sample.e	• C:\sample.exe

除外の種類	ワイルドカードの使用	一致	一致しません
のファイル	C:\ ディレクトリの任意のサブフォルダにある場合のみ除外します。	xe	
UNC (Universal Naming Convention) パス	`\\<UNC path>\*\Sample.exe` Sample.exe ファイルが、指定されたUNCパスのサブフォルダにある場合にのみ除外します。	• \\<UNC path>\files\Sample.exe • \\<UNC path>\temp\files\Sample.exe	• R:\files\Sample.exe 理由:マップされたドライブはサポートされていません。 • \\<UNC path>\Sample.exe 理由:ファイルがUNCパスのサブフォルダ内に存在しません。
ファイル名と拡張子	`C:\*.*` C:\ ディレクトリのすべてのフォルダおよびサブフォルダにある拡張子のあるすべてのファイルを除外します。	• C:\Sample.exe • C:\temp\Sample.exe • C:\test.doc	• D:\sample.exe • C:\Sample 注意: C:\Sample にはファイル拡張子がないため、例外とは一致しません。
ファイル名	`C:\*.exe` C:\ ディレクトリのすべてのフォルダおよびサブフォルダにある、.exe 拡張子を持つすべてのファイルを除外します。	• C:\Sample.exe • C:\temp\test.exe	• C:\Sample.doc • C:\temp\test.bat • C:\Sample 注意: C:\Sample にはファイル拡張子がないため、例外と

除外の種類	ワイルドカードの使用	一致	一致しません
			は一致しません。
ファイル拡張子	`C:\Sample.*` Sample という名前と C:\ ディレクトリ内の任意の拡張子を持つすべてのファイルを除外します。	• C:\Sample.exe	• C:\Sample1.doc • C:\temp\Sample.bat • C:\Sample 注意: C:\Sample にはファイル拡張子がないため、例外とは一致しません。
特定のディレクトリ構造内のファイル	`C:\*\*\Sample.exe` C:\ ディレクトリの2番目のサブフォルダレベル以降のサブフォルダ内にあり、ファイル名と拡張子が Sample.exe であるすべてのファイルを除外します。	• C:\files\temp\Sample.exe • C:\files\temp\test\Sample.exe	• C:\Sample.exe • C:\temp\Sample.exe • C:\files\temp\Sample.doc

スパイウェア/グレーウェアの例外の処理方法

スパイウェアが検出されると、検索を制御する不正プログラム検索設定に応じて、不正プログラムの駆除、隔離、または削除をすぐに実行できます。スパイウェアイベントまたはグレーウェアイベントの除外を作成した後で、ファイルの復元が必要になる場合があります。詳細については、「"検出ファイルを復元する" on page 888」を参照してください。

または、処理を[パス]に設定して一時的にスパイウェアおよびグレーウェアを検索し、すべてのスパイウェアおよびグレーウェアの検出を[不正プログラム対策イベント]画面に記録しますが、駆除、隔離、または削除は行いません。その後、検出されたスパイウェアおよびグレーウェアの除外を作成できます。除外リストが堅牢な場合は、処理を[駆除]、[隔離]、または[削除]のいずれかのモードに設定できます。

処理の設定の詳細については、"不正プログラムの処理を設定する" on page 846を参照してください。

検索除外の推奨設定

検索除外については、トレンドマイクロやその他のベンダが包括的な詳しい情報を提供しています。ここでは、検索除外の推奨設定の一部について、その概要を紹介します。

- 不正プログラムであることがすでに確認されているファイルが再検索されないように、隔離フォルダ (Microsoft Windows Exchange ServerのSMEXなど) を除外します。
- 検索を実行するとデータベースのパフォーマンスに影響することがあるため、大規模なデータベースやデータベースファイル (dsm.mdfやdsm.ldfなど) を除外します。データベースファイルを検索する必要がある場合は、ピーク時を避けてデータベースを検索する予約タスクを作成します。Microsoft SQL Serverデータベースは動的であるため、ディレクトリおよびバックアップフォルダを検索リストから除外します。

  Windowsの場合:

  ```
  ${ProgramFiles}\Microsoft SQL Server\MSSQL\Data\
  ${Windir}\WINNT\Cluster\ # if using SQL Clustering
  Q:\ # if using SQL Clustering
  ```

  Linuxの場合:

  ```
  /var/lib/mysql/ # if path is set to this Data Location of MySQL in the machine.
  /mnt/volume-mysql/ # if path is set to this Data Location of MySQL in the machine.
  ```

推奨される検索除外のリストについては、トレンドマイクロ推奨検索除外リストを参照してください。Microsoft もアンチウイルス除外リストを維持しており、Windows サーバー上のファイルを検索から除外するためのレファレンス/参照情報として使用できます。

信頼された証明書で署名されたファイルを除外する

署名付きアプリケーションがあり、それらのプロセスのすべてのアクティビティをリアルタイム不正プログラム対策検索 (ファイル検索、動作監視、予測型機械学習など) から除外する場合は、次のように、Deep Security Managerの信頼できる証明書リストにそのデジタル証明書を追加します。

1. ポリシーエディタまたはコンピュータエディタで、[不正プログラム対策] →[Advanced]に移動します。
2. 信頼された証明書の検出除外セクションで、信頼された証明書を持つファイルを除外を「はい」または「継承(はい) 」に設定してください。

3. [Manage Certificate List]を選択します。
4. [信頼された証明書]画面には、インポートした証明書が表示されます。[Import From File]を選択して、検索除外に別の項目を追加します。
5. 証明書ファイルを選択し、[Next]を選択します。
6. 表示される証明書の概要を確認し、この証明書を信頼するをスキャン除外に設定します。次へを選択します。
7. サマリーページには、インポートが成功したかどうかが表示されます。閉じるを選択してください。

注意: この種類の除外は、WindowsのDeep Security Agent 20.0.0-3445以降でサポートされています。

インポートされた証明書が[信頼された証明書]リストに表示され、[目的]が[例外]と表示されます。

ヒント: Deep Securityは、プロセスの開始時に除外リストを確認します。除外を設定する前にプロセスが実行されていた場合、そのプロセスは再起動されるまで除外リストに追加されません。

保護対象のLinuxインスタンスにおける不正プログラム対策のデバッグログレベルの引き上げ

Linuxオペレーティングシステムを使用している場合、不正プログラム対策 (AM) に関連した問題を診断するために使用するAMデバッグログのレベルを変更することができます。

不正プログラム対策のデバッグログは、テクニカルサポート向けの診断パッケージに自動的に追加されます。

診断パッケージの作成については、"診断パッケージの作成" on page 2019を参照してください。

不正プログラム対策のデバッグログレベルを上げるには、Linuxインスタンスのシェルでスーパーユーザとして次のコマンドを入力します。

```
killall -USR1 ds_am
```

このコマンドはレベルを1つ上げます。初期設定のレベルは6、最大レベルは8です。

不正プログラム対策のデバッグログレベルを下げるには、Linuxインスタンスのシェルでスーパーユーザとして次のコマンドを入力します。

```
killall -USR2 ds_am
```

このコマンドはレベルを1つ下げます。最小レベルは0です。

注意: Linuxディストリビューションでkillallを使用していない場合は、pkillコマンドを代わりに使用できます。

Webレピュテーションを設定する

Webレピュテーションモジュールは、悪意のあるURLへのアクセスをブロックすることにより、Webからの脅威から保護します。Deep Securityは、Smart Protection Networkのソースからトレンドマイクロのセキュリティデータベースを使用して、ユーザがアクセスしようとしているウェブサイトのレピュテーションを確認します。ウェブサイトのレピュテーションは、コンピュータで適用されている特定のWebレピュテーションポリシーと関連付けられています。適用されているセキュリティレベルに応じて、Deep SecurityはURLへのアクセスをブロックするか許可します。

Webレピュテーションがサポートされているオペレーティングシステムのリストについては、"各プラットフォームでサポートされている機能" on page 417を参照してください。

WebレピュテーションモジュールはHTTPSトラフィックをサポートしています。詳細については、TLSトラフィックの検査を参照してください。

Webレピュテーションを有効にして設定するには、次の手順を実行します。

1. "Webレピュテーションモジュールを有効にする" below
2. "Trend ツールバーを有効にする" on the next page
3. "インラインモードとタップモードを切り替える" on the next page
4. "セキュリティレベルを適用する" on page 900
5. "例外設定を作成する" on page 901
6. "Smart Protection Serverを設定する" on page 902
7. "詳細設定を編集する" on page 903
8. "Webレピュテーションをテストする" on page 903

Agentコンピュータのユーザにメッセージが表示されないようにする方法については、"コンピュータで通知を設定する" on page 850を参照してください。

Webレピュテーションモジュールを有効にする

1. [ポリシー] に移動します。
2. Webレピュテーションを有効にするポリシーをダブルクリックします。
3. [Webレピュテーション]→[一般] をクリックします。
4. [Webレピュテーションのステータス] を [オン] にします。
5. [保存] をクリックします。

Trend ツールバーを有効にする

Trend ツールバーを有効にした後、Webブラウザを使用して危険なWebサイト、非常に不審なWebサイト、または不審なWebサイトにアクセスすると、Webブラウザのメインウィンドウにブロックページが表示され、Windowsの通知にポップアップメッセージが表示されます。エリア。さらに、危険、非常に不審、または不審と評価されたURLへのアクセス試行は、Workload SecurityのWebレピュテーションイベントタブに記録されます。

ブラウザー拡張機能にトレンドマイクロTrend ツールバーが含まれている場合、ブラウザーに小さなトレンドマイクロのロゴが表示されます。Chrome とFirefox では、ロゴはウェブサイトアドレスフィールドの右側に表示されます。

Windows用 ツールバーをインストールする

Trend ツールバー拡張機能は、特定のWindowsプラットフォームでのみサポートされます。現在、ChromeおよびMicrosoft Edgeブラウザでサポートされています。詳細については、"各プラットフォームでサポートされている機能" on page 417を参照してください。

Trend ツールバー(Windows版) は、Webレピュテーションモジュールを有効にすると自動的にダウンロードされ、次回Webブラウザを再起動したときにインストールされます。

インラインモードとタップモードを切り替える

Webレピュテーションは、Deep Securityのネットワークエンジンを使用します。このエンジンは、次のいずれかのモードで動作します。

- インライン: パケットストリームがDeep Securityネットワークエンジンを直接流れます。すべてのルールは、プロトコルスタックの上位に伝わる前にネットワークトラフィックに適用されます。
- タップモード: パケットストリームは変更されません。トラフィックは Webレピュテーションによって処理されます(有効な場合)。ただし、問題が検出されてもパケットや接続が拒否されることはありません。タップモードでは、Deep Securityはイベントのレコードを提供する以外の保護は提供しません。

タップモードでは、実際のストリームは変更されません。すべての処理は複製されたストリーム上で行われます。タップモードでは、Deep Securityはイベントのレコードを提供する以外の保護は提供しません。

インラインモードとタップモードを切り替えるには、**コンピュータエディタまたはポリシーエディタ**[1]を開き、[設定]→[詳細]→[ネットワークエンジンモード]の順に選択します。

ネットワークエンジンの詳細については、"ファイアウォールルールを配信前にテストする" on page 955を参照してください。

セキュリティレベルを適用する

既知の不正なWebアドレスまたはその疑いがあるWebアドレスには、次のリスクレベルが割り当てられます。

- 危険: 不正、または脅威の既知の発信源であると確認されたWebアドレス
- 非常に不審: 不正または脅威の発信源である可能性が疑われたWebアドレス
- 不審: スパムメールに関連付けられている、または感染している可能性のあるWebアドレス

セキュリティレベルは、関連付けられたリスクレベルに基づいて、Deep SecurityがURLへのアクセスを許可するかブロックするかを決定します。たとえば、セキュリティレベルを[低]に設定すると、Deep SecurityはWebの脅威であることが判明済みのURLのみをブロックします。セキュリティレベルを上げるほど、Webの脅威の検出率が向上しますが、誤判定の可能性も増加します。

セキュリティレベルを設定するには、次の手順に従います。

1. [ポリシー]に移動します。
2. 編集するポリシーをダブルクリックします。
3. [Webレピュテーション]→[一般]をクリックします。
4. 次のセキュリティレベルのいずれかを選択します。
    - 高: ブロック対象のページ:
        - 危険
        - 非常に不審
        - 不審
    - 中: ブロック対象のページ:
        - 危険
        - 非常に不審

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

- 低: ブロック対象のページ:
  - 危険

5. [保存] をクリックします。

例外設定を作成する

独自のブロックまたは許可するURLのリストで、Trend Micro Smart Protection Networkの評価に基づくブロック/許可の動作をオーバーライドできます。

注意: [許可] リストは [ブロック] リストよりも優先されます。[許可] リスト内のエントリと一致するURLは、[ブロック] リストと照合されません。

URL例外設定を作成するには、次の手順に従います。

1. [ポリシー] に移動します。
2. 編集するポリシーをダブルクリックします。
3. [Webレピュテーション]→[例外] をクリックします。
4. URLを許可するには、次の手順に従います。
   a. [許可] セクションに移動します。
   b. [許可リストに追加するURL (1行に1つずつ)] の下の空白に必要なURLを入力します。一度に複数のURLを追加できますが、その場合は改行で区切る必要があります。
   c. 次のいずれかを選択します。
      - ドメインからのURLを許可:指定されたドメインからのすべてのページが許可されます。サブドメインもサポートされています。エントリにはドメイン(およびオプションでサブドメイン)のみを含めてください。例えば、「testdomain.com」や「another.testdomain.com」は有効なエントリです。
      - URLを許可する: 指定されたURLが許可されます。ワイルドカードがサポートされています。例えば、「testdomain.com/shopping/coats.html」や「testdomain.com/shopping/*」は有効なエントリです。
   d. [追加] をクリックします。

   URLをブロックするには、次の手順に従います。

   a. [ブロック] セクションに移動します。
   b. [ブロックリストに追加するURL (1行に1つずつ)] の下の空白に必要なURLを入力します。一度に複数のURLまたはキーワードを追加できますが、その場合は改行で区切る必要があります。

c. 次のいずれかを選択します。
   - ドメインからのURLをブロック:指定されたドメインからのすべてのページがブロックされます。サブドメインもサポートされています。エントリにはドメイン(およびオプションでサブドメイン) のみを含めてください。例えば、「testdomain.com」や「another.testdomain.com」は有効なエントリです。
   - URLをブロック: 指定されたURLはブロックされます。ワイルドカードがサポートされています。例えば、「testdomain.com/shopping/coats.html」や「testdomain.com/shopping/*」は有効なエントリです。URLに疑問符(?) が含まれている場合は、バックスラッシュ(\) を前に付ける必要があります。例えば、「testdomain.com/shopping.com/?testQuery=test」は「testdomain.com/shopping/\?testQuery=test」と入力する必要があります。
   - このキーワードを含むURLをブロック: 指定されたキーワードを含むURLはブロックされます。

d. [追加] をクリックします。

5. [保存] をクリックします。

Smart Protection Serverを設定する

Webレピュテーション用のSmart Protectionサービスは、Webレピュテーションモジュールに必要なWeb情報を提供します。詳細については、「Smart Protection Network - Global Threat Intelligence」を参照してください。

Smart Protection Serverを設定するには、次の手順に従います。

1. [ポリシー] に移動します。
2. 編集するポリシーをダブルクリックします。
3. [Webレピュテーション]→[Smart Protection] の順にクリックします。
4. トレンドマイクロの Smart Protection サービスに直接接続するかどうかを選択します。
   a. [Global Smart Protectionサービスへの直接接続] を選択します。
   b. オプションで [Global Smart Protectionサービスへのアクセス時にプロキシを使用する] を選択します。[新規] を選択して、希望するプロキシを入力します。

   1台または複数のローカルにインストールされたSmart Protection Serverに接続するには、次の手順に従います

   a. [ローカルにインストールされたSmart Protection Serverの使用。例: "http://[server]:5274"]
   b. フィールドにSmart Protection ServerのURLを入力し、追加をクリックします。Smart Protection ServerのURLを見つけるには、Smart Protection Serverにログインし、メインペインでリアルタイムステータスを確認します。Smart Protection ServerのHTTPおよびHTTPSのURLは、Webレピュテーション行に表示されます。HTTPSのURLは、Deep

Securityエージェントバージョン11.0以降でのみサポートされています。バージョン10.3以前のエージェントを使用している場合は、HTTPのURLを使用してください。

c. 必要に応じて、Windowsのみの場合は ドメインに参加していない場合はGlobal Smart Protectionサービスに接続。

5. [保存] をクリックします。

Smart Protection Serverへの接続の警告

このオプションは、コンピュータのSmart Protection Serverへの接続が切断されたときに、エラーイベントを生成してアラートを発令するかどうかを指定します。[はい] または [いいえ] を選択して [保存] をクリックします。

Smart Protection Serverをローカルにインストールしている場合、Smart Protection Server自体に問題が発生した場合に通知が表示されるよう、少なくとも1台のコンピュータでこのオプションを [はい] に設定する必要があります。

詳細設定を編集する

ブロックページ

ユーザがブロック対象のURLにアクセスしようとすると、ブロックページに転送されます。[リンク] の空欄に、ブロックされたURLへのアクセスを要求するためにユーザが使用できるリンクを指定します。

アラート

[はい] または [いいえ] を選択して、Webレピュテーションイベントがログに記録された場合にアラートを出すかとうかを決定します。

ポート

[有害な可能性のあるWebページを監視するポート] の横にあるドロップダウンリストから、有害な可能性のあるWebページで監視する特定のポートを選択します。

Webレピュテーションをテストする

続行する前に、Webレピュテーションが正常に動作しているかどうかをテストします。

1. Webレピュテーションが有効になっていることを確認します。
2. コンピュータエディタまたはポリシーエディタで、[Webレピュテーション]→[除外] の順に選択します。
3. [ブロック] の下に「*http://www.speedtest.net*」と入力し、[追加] をクリックします。

4. [保存] をクリックします。
5. ブラウザを開いてこのWebサイトへのアクセスを試みます。アクセスを拒否するメッセージが表示されます。
6. [イベントとレポート]→[Webレピュテーション] の順に選択し、Webアクセスが拒否されたことが記録されているかどうかを確認します。検出が記録されていれば、Webレピュテーションモジュールは正常に動作しています。

侵入防御(IPS)を設定する

侵入防御

侵入防御 モジュールは、SQLインジェクション攻撃、クロスサイトスクリプティング攻撃、およびその他のWebアプリケーションの脆弱性に対する脆弱性攻撃からコンピュータを保護します。

アプリケーションまたはOSの既知の脆弱性に対してパッチが利用できない場合、侵入防御 ルールは、この脆弱性を悪用しようとしているトラフィックをインターセプトできます。また、ネットワークにアクセスする不正なソフトウェアを特定し、ネットワークにアクセスするアプリケーションに対する可視性および制御性を向上します。このため、脆弱性を修正するパッチがリリースされ、テストされて配信されるまでコンピュータが保護されます。

ファイル共有やSkypeなどのメッセージングソフトウェアだけでなく、SQLインジェクションやクロスサイトスクリプティング(XSS)などの脆弱性を持つWebアプリケーションに対しても、保護が利用可能です。このように、侵入防御は軽量なWebアプリケーションファイアウォール(WAF)としても使用できます。

侵入防御を有効にして設定するには、"侵入防御の設定" on page 908を参照してください。

侵入防御 ルール

侵入防御ルールは、ネットワークパケットのペイロードセッションおよびアプリケーション層 (DNS、HTTP、SSL、SMTPなど)、およびこれら上位層のプロトコルに従ってパケットのシーケンスと比較される条件のセットを定義します。

ヒント: ファイアウォールルールはパケットのネットワーク層とトランスポート層 (IP、TCP、UDPなど) を確認します。

Deep Security Agentがネットワークトラフィックを検索し、そのトラフィックがルールの一致条件を満たしている場合、エージェントはそのルールを使用して攻撃の可能性があるか確認し、ルールに応じて次のいずれかの処理を実行します。

- パケットの完全な破棄
- 接続のリセット

侵入防御 ルールはポリシーとコンピュータに割り当てられます。このため、使用するポリシーに基づいてコンピュータのグループにルールセットを適用し、必要に応じてポリシーをオーバーライドできます("ポリシー、継承、およびオーバーライド" on page 724を参照してください)。

ルールの機能に影響を与える方法については、"侵入防御ルールの設定" on page 914。

アプリケーションの種類

アプリケーションの種類では、関連付けられているアプリケーションごとにルールを整理します。また、通信に使用されるプロトコルやポート番号などのように必要に応じてルールが参照できるプロパティ値を格納できます。一部のアプリケーションの種類には、設定可能なプロパティがあります。たとえば、Database Microsoft SQLのアプリケーションの種類には、Microsoft SQL Serverに関連付けられているルールが含まれます。このアプリケーションの種類を設定すると、データベースへの接続に使用するポートを指定できます。

詳細については、"アプリケーションの種類" on page 935を参照してください。

ルールアップデート

トレンドマイクロは、侵入防御 ルールを作成し、アプリケーションの脆弱性を検出します。セキュリティアップデートには、新しいルールまたはアップデートされたルール、およびアプリケーションの種類を含めることができます。ルールがすでにポリシーに割り当てられていて、割り当てられたルールが依存するルールがアップデートに含まれる場合は、アップデートされたルールを自動的に割り当てるように選択できます。

ヒント: 侵入防御 ルールには、保護対象となる脆弱性に関する情報が含まれています。

侵入防御 ルールはDeep Security Managerで直接編集できません。ただし、一部のルールは設定可能であり、設定が必要なルールもあります ("設定オプションを設定する(トレンドマイクロのルールのみ)" on page 920参照してください)。

推奨設定の検索

推奨検索を使用して、ポリシーとコンピュータに割り当てる侵入防御 ルールを検出できます。("推奨設定の検索の管理と実行" on page 728を参照してください)。

動作モードを使用してルールをテストする

侵入防御 は、[検出]または[防御]モードで動作します。

- 検出：侵入防御 では、一致するトラフィックを検出してイベントを生成するためにルールを使用しますが、トラフィックはブロックしません。検出モードは、侵入防御 ルールが正規のトラフィックに干渉しないことをテストする場合に便利です。
- Prevent: 侵入防御 では、ルールを使用して一致するトラフィックを検出し、イベントを生成し、トラフィックをブロックして攻撃を防止します。

新しい侵入防御 ルールを最初に適用する場合は、Detectモードを使用して、誤って通常のトラフィックをブロックしないことを確認します(誤検出).誤判定が発生しないことを確認できた時点で、防御モードを使用して、ルールを適用して攻撃をブロックできます ("検出モードで 侵入防御 を有効にする" on page 908 および "予防 モードに切り替える" on page 913 .)

ヒント: 検出モードで 侵入防御 を使用するのと同様に、Deep Securityネットワークエンジンはテスト目的でタップモードで実行できます。タップモードでは、侵入防御 はルールマッチングトラフィックを検出してイベントを生成しますが、トラフィックはブロックしません。また、タップモードは、ファイアウォールおよびWebレピュテーション モジュールにも影響します。検出モードを使用すると、侵入防御 ルールを個別にテストできます。
タップモードを ファイアウォール ルールのテストに使用するのと同じ方法で、侵入防御 でタップモードを使用します。See"ファイアウォールルールを配信前にテストする" on page 955。

ルールの動作 モードをオーバーライドする

個々のルールに対して[検出]モードを選択することで、コンピュータまたはポリシーレベルで[防止 モード]の動作を選択して優先させることができます。ポリシーまたはコンピュータに適用される新しい侵入防御 ルールをテストする場合に便利です。たとえば、防御モードで 侵入防御 が機能するようにポリシーが設定されている場合、ルールを[検出]モードに設定することで、個々のルールの防御モードの動作を回避できます。そのルールの場合にのみ、侵入防御 はトラフィックをログに記録し、ポリシーの動作モードをオーバーライドしない他のルールを適用します。("ルールの動作 モードをオーバーライドする" on page 922を参照してください)。

注意: コンピュータまたはポリシーレベルでの防御モードは、矛盾するルール設定で上書きできますが、[検出]モードにはできません。コンピュータまたはポリシーレベルで[検出]モードを選択すると、ルール設定に関係なく検出モードの動作が適用されます。

トレンドマイクロが用意している一部のルールは、初期設定で検出モードを使用します。たとえば、メールクライアントルールでは、一般的に[検出]モードが使用されます。これは、予防モードでは、すべてのメールのダウンロードがブロックされるためです。一部のルールは、条件が多数回、または一定期間中に一定回数発生した場合にのみアラートをトリガします。これらのルールは、条件が再度発生した場

合にのみ、不審な挙動を示すトラフィックに適用され、その条件が1回発生しただけでは異常とはみなされません。

警告:
設定が必要なルールは、正規のトラフィックをブロックしたりネットワークサービスを中断することがないようにするには、設定が完了するまで検出モードのままにします。ルールを防御モードに切り替えるのは、設定とテストの完了後にします。

侵入防御 イベント

初期設定では、Deep Security Managerは ファイアウォール および 侵入防御 イベントログを、Deep Security エージェントおよびアプライアンス[1] から収集します。Deep Security Managerによって収集されたイベントログは、設定可能な期間保存されます。初期設定値は1週間です ("ログとイベントの保存に関するベストプラクティス" on page 1154を参照してください)。必要に応じて、個々のルールにイベントログを設定できます ("ルールにイベントログを設定する" on page 919を参照してください)。

イベントにタグを付けると、イベントをソートしやすくなります。イベントには、手動でタグを付けることも、自動でタグを付けることもできます。また、自動タグ付け機能を使用し、複数のイベントをグループ化してラベルを付けることもできます。イベントのタグ付けの詳細については、"イベントを識別およびグループ化するためのタグの適用" on page 1161を参照してください。

安全な接続のサポート

侵入防御モジュールでは、セキュリティで保護された接続でパケットを検査できます。"TLS トラフィックの検査" on page 936を参照してください。

コンテキスト

コンテキストは、コンピュータのネットワーク環境に応じてさまざまなセキュリティポリシーを実装する有効な方法です。一般的には、コンテキストが使用されるポリシーを作成して、さまざまな ファイアウォール ルールと侵入防御 ルールをコンピュータ(通常はモバイルラップトップ) に適用します。このルールは、そのコンピュータが社内にあるか離れているかによって異なります。

コンピュータの場所を決定するには、コンピュータがどのようにドメインコントローラと接続されているかコンテキストで検証します。詳細については、"ポリシーで使用するコンテキストの定義" on page 814を参照してください。

---

[1]Deep Security AgentとDeep Security Virtual Applianceは、ユーザが定義したDeep Securityポリシーを適用するためのコンポーネントです。Agentはコンピュータに直接インストールされ、ApplianceはAgentレスの保護を提供するためにVMware vSphere環境で使用されます。どちらもDeep Security as a Serviceでは使用できません。

インタフェースのタグ付け

ファイアウォール または 侵入防御 ルールを特定のインタフェースに割り当てる必要がある場合にインタフェースの種類を使用できます。複数のネットワークインタフェースがあるコンピュータの場合初期設定では、ファイアウォールルールと侵入防御ルールはコンピュータ上のすべてのインタフェースに割り当てられます。たとえば、ワイヤレスネットワークインタフェースにのみ特別なルールを適用する場合、インタフェースの種類を使用します。詳細については、"複数のインタフェースに対してポリシーを設定する" on page 739を参照してください。

侵入防御の設定

侵入防御 モジュールを有効にし、[Detect]モードを使用してネットワークトラフィックの攻撃を監視します。侵入防御 ルールの割り当て方法に満足したら、防御モードに切り替えてください。

1. "検出モードで 侵入防御 を有効にする" below
2. "侵入防御のテスト侵入防御" on page 910
3. "推奨ルールを適用する" on page 911
4. "システムを監視する" on page 912
5. "パケットまたはシステムのエラーに対して「Fail-Open」を有効にする" on page 913
6. "予防モードに切り替える" on page 913
7. "個々のルールについてのベストプラクティスを実装する" on page 913
8. "NSXセキュリティタグを適用する" on page 914

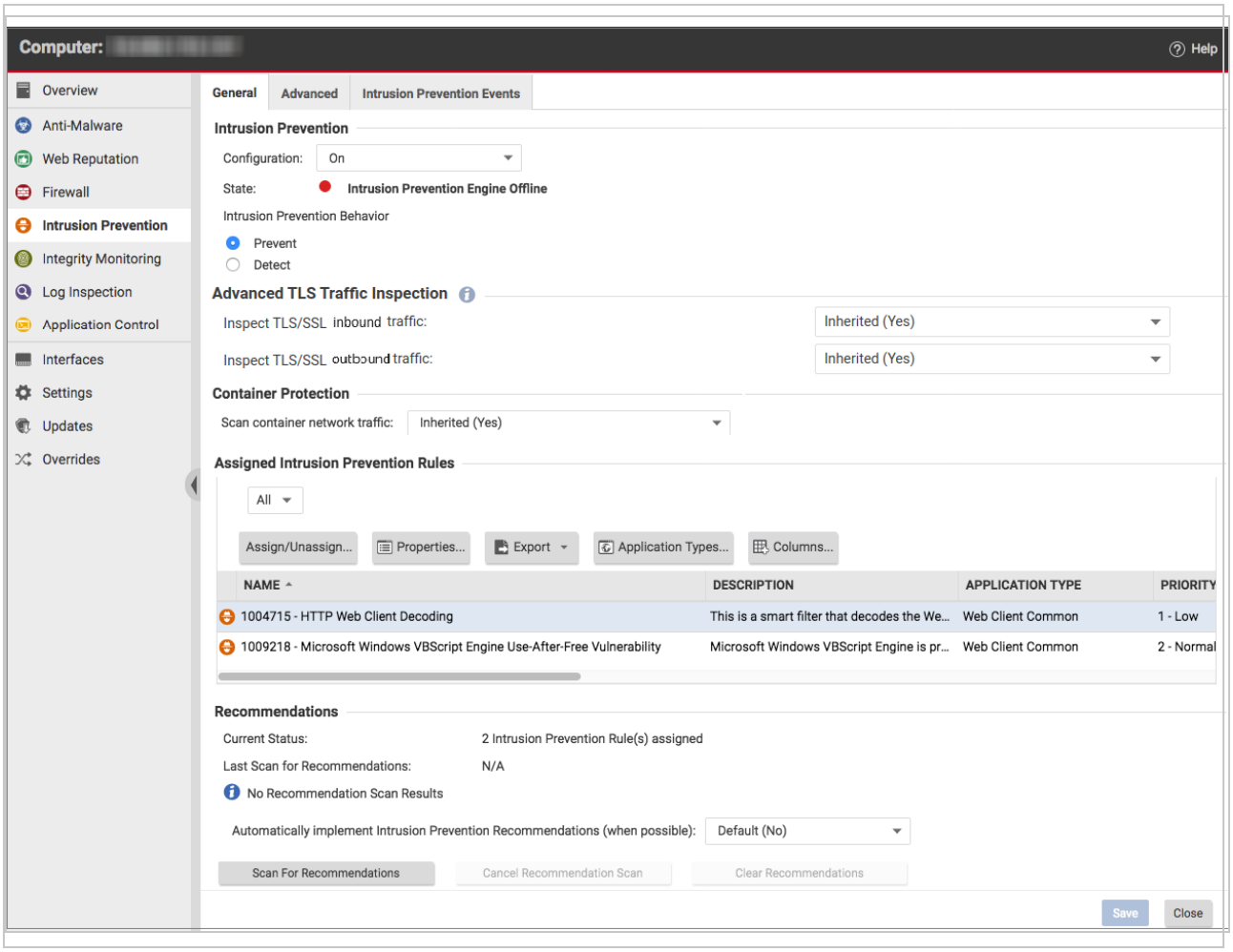
注意: IPSの設定によって、CPUとRAMの使用率は変化します。Deep Security AgentでIPSのパフォーマンスを最適化するには、"侵入防御のパフォーマンスに関するヒント" on page 951のパフォーマンスに関するヒントを参照してください。

侵入防御 モジュールの概要については、"侵入防御" on page 904を参照してください。

検出モードで 侵入防御 を有効にする

侵入防御 を有効にし、[検出]モードを使用して監視します。適切なポリシーを使用して、対象コンピュータに影響を与える侵入防御 を設定します。個々のコンピュータを設定することもできます。

1. コンピュータエディタまたはポリシーエディタ[1]で、[侵入防御]→[一般]に進みます。
2. [設定]で、[オン]または[継承(オン)]を選択します。



3. [侵入防御の動作]では、[検出]を選択します。
4. Deep Security Agent 11.1以前では、ホストコンピュータのネットワークインタフェースを通過してコンテナに向かうトラフィックが侵入防御モジュールによって監視されます。Deep Security Agent 11.2以降では、コンテナ間のトラフィックを監視することもできます。[コンテナのネットワークトラフィックの検索]設定が[はい]に設定されている場合、コンテナとホストの両方を通過するトラフィックがDeep Securityによって検索されます。[いいえ]に設定されている場合、Deep Securityで検索されるのは、ホストネットワークインタフェースを通過するトラフィックだけです。
5. [保存]をクリックします。

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

ヒント: 動作を設定できない場合は、[ネットワークエンジンモード] が [タップ] に設定されている可能性があります("ファイアウォールルールを配信前にテストする" on page 955)を参照してください。

より細かい制御を行うには、侵入防御ルールを割り当てるときに、グローバル動作モードをオーバーライドして、防止または検出のいずれかに特定のルールを設定できます ("ルールの動作モードをオーバーライドする" on page 922を参照してください)。

侵入防御のテスト侵入防御

続行する前に、次の手順を実行して、侵入防御モジュールが正常に動作していることを確認する必要があります。

1. Agentベースの配信がある場合は、コンピュータのAgentが実行中であることを確認します。エージェントレスの配置の場合は、Deep Security Virtual Applianceが正常に動作していることを確認してください。
2. Webレピュテーションモジュールを無効にします。Deep Security Managerで、[Computers]をクリックし、侵入防御をテストするコンピュータをダブルクリックします。コンピュータのダイアログボックスで [Webレピュテーション] をクリックし、[オフ] を選択します。Webレピュテーションは現在無効になっており、侵入防御機能に干渉しません。
3. 不正なトラフィックがブロックされることを確認します。引き続き、コンピュータのダイアログボックスで [侵入防御] をクリックし、[一般] タブで [防御] を選択します(影付き表示されている場合は、[設定] ドロップダウンリストを [継承 (オン)] に設定します)。
4. EICARテストポリシーを割り当てます。引き続き、コンピュータのダイアログボックスで [侵入防御] をクリックします。[割り当て/割り当て解除] をクリックします。1005924を検索します。[1005924 - Restrict Download of EICAR Test File Over HTTP] ポリシーが表示されます。チェックボックスをオンにして、[OK] をクリックします。これで、ポリシーがコンピュータに割り当てられました。
5. EICARファイルをダウンロードしてください(できない場合、侵入防御が適切に実行されている場合は。)を実行できません。Windowsの場合は、: http://files.trendmicro.com/products/eicar-file/eicar.comのリンクをクリックしてください。Linuxの場合は次のコマンドを入力します。curl -O http://files.trendmicro.com/products/eicar-file/eicar.com
6. コンピュータの侵入防御イベントを確認します。引き続き、コンピュータのダイアログボックスで [侵入防御]→[侵入防御イベント] をクリックします。[イベントの取得] をクリックすると、前回のハートビート以降に発生したイベントが表示されます。[理由] が [1005924 - Restrict Download of EICAR Test File Over HTTP] となっているイベントが表示されます。このイベントの存在は、侵入防御が機能していることを示しています。
7. 変更を元に戻し、システムを以前の状態に戻します。Webレピュテーションモジュールをオンにし(オフにした場合)、[防御] または [検出] オプションをリセットして、コンピュータからEICARポリシーを削除します。

推奨ルールを適用する

パフォーマンスを最大化するには、ポリシーとコンピュータで必要な侵入防御ルールのみを割り当てます。推奨検索を使用して、適切なルールのリストを取得できます。

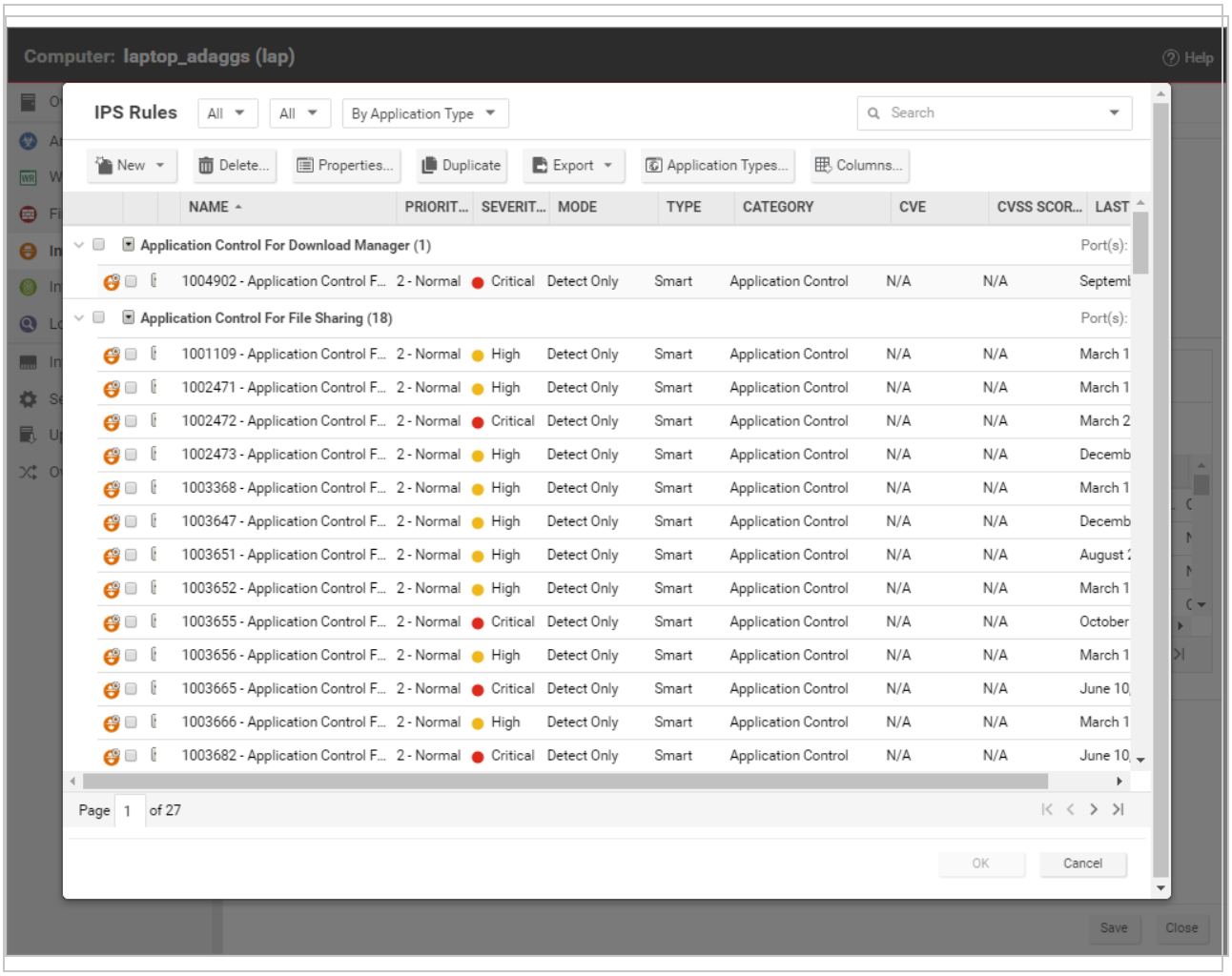
推奨設定の検索は特定のコンピュータに対して実行されますが、この推奨設定はコンピュータが使用するポリシーに割り当てることができます。

詳細については、"推奨設定の検索の管理と実行" on page 728を参照してください。

1. 検索するコンピュータのプロパティを開きます。"推奨設定の検索を手動で実行する" on page 733の説明に従って推奨設定の検索を実行します。

   注意: Deep Securityを"推奨設定を自動的に適用する" on page 734検索結果を自動的に実装します。

2. ルールを割り当てるポリシーを開き、"検索結果を確認して手動でルールを割り当てる" on page 735の説明に従ってルールの割り当てを実行します。



ヒント: 割り当てられた侵入防御 ルールを自動的かつ定期的に微調整するために、推奨検索のスケジュールを設定できます。"Deep Security予約タスクの設定" on page 1826を参照してください。

システムを監視する

侵入防御 ルールを適用した後、システムパフォーマンスと侵入防御 イベントログを監視します。

システムパフォーマンスを監視する

CPU、RAM、およびネットワークの使用量を監視して、システムのパフォーマンスが許容範囲に収まっていることを確認します。パフォーマンスが許容範囲を超えて低下している場合は、パフォーマンスを改善するために一部の設定や環境を変更します("侵入防御のパフォーマンスに関するヒント" on page 951を参照してください)。

侵入防御イベントを確認する

侵入防御 イベントを監視して、ルールが正規のネットワークトラフィックに一致しないようにします。ルールで誤判定が発生している場合は、ルールの割り当てを解除できます("ルールを割り当てる/ルールの割り当てを解除する" on page 918を参照してください)。

侵入防御 イベントを表示するには、[イベントとレポート]→[侵入防御イベント]の順にクリックします。

パケットまたはシステムのエラーに対して「Fail-Open」を有効にする

侵入防御 モジュールには、侵入防御 ルールを適用する前にパケットをブロックするネットワークエンジンが含まれています。これにより、サービスおよびアプリケーションでダウンタイムやパフォーマンスの問題が発生することがあります。この動作を変更し、システムまたは内部パケットエラーの発生時にパケットの通過を許可できます。詳細については、"「Fail-Open」の動作を有効にする" on page 957を参照してください。

予防モードに切り替える

侵入防御で誤検出が検出されないことを確認したら、次のように、侵入防御を防御モードで使用するようにポリシーを設定し、ルールが適用され、関連するイベントがログに記録されるようにします。

1. コンピュータエディタまたはポリシーエディタ[1]で、[侵入防御]→[一般] に進みます。
2. [侵入防御の動作] では、[防御] を選択します。
3. [保存] をクリックします。

個々のルールについてのベストプラクティスを実装する

HTTPプロトコルデコードルール

HTTPプロトコルデコードルールは、アプリケーションの種類「Web Server Common」の中で最も重要なルールです。このルールは、他のルールによってHTTPトラフィックが検査される前にHTTPトラフィックをデコードします。また、このルールを使用して、デコードプロセスの各種のコンポーネントを制御することもできます。

このルールは、このルールを必要とするいずれかの「Web Application Common」ルールまたは「Web Server Common」ルールを使用する場合には必須です。Deep Security Managerは、他のルールでルールが必要な場合に自動的にこのルールを割り当てます。Webアプリケーションは1つ1つ異なるた

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。

め、設定変更が必要かどうかを判断するために、このルールを使用するポリシーは一定期間検出モードで実行してから保護モードに切り替える必要があります。

無効な文字のリストは、しばしば変更が必要です。

詳細については次を参照してください。

- Deep SecurityでのHTTPプロトコルデコード
- Deep Security Agentが不正と見なすURI文字のリストを変更する
- Deep SecurityでURIの不正文字エラーが表示されます

クロスサイトスクリプティングルールと汎用的なSQLインジェクションルール

アプリケーション層への攻撃として最も代表的なものに、SQLインジェクションとクロスサイトスクリプティング (XSS) があります。クロスサイトスクリプティングルールとSQLインジェクションルールは初期設定で攻撃の大半を阻止しますが、特定のリソースが誤判定を引き起こす場合はその破棄のしきい値の調整が必要になることがあります。

この2つのルールは、どちらもWebサーバに合わせてカスタム設定が必要なスマートフィルタです。Webアプリケーション脆弱性Scannerからの情報がある場合は、保護を適用する際に利用することをお勧めします。たとえば、login.aspページのユーザ名フィールドがSQLインジェクションに対して脆弱な場合は、破棄のしきい値を低くしてそのパラメータを監視するようにSQLインジェクションルールを設定してください。

詳細については、Generic SQL Injection Preventionルールを理解するを参照してください。

NSXセキュリティタグを適用する

NSXセキュリティタグを適用する

Deep Securityでは、侵入防御ルールがトリガされた際に、保護対象の仮想マシンにNSXセキュリティタグを適用できます。詳細については、"NSXセキュリティタグを適用するように侵入防御を設定する" on page 649を参照してください。

侵入防御ルールの設定

次のタスクを実行して、侵入防御ルールを設定および使用します。

- "侵入防御ルールのリストを表示する" on the next page
- "侵入防御ルールに関する情報を表示する" on the next page

- "関連付けられている脆弱性に関する情報を表示する(トレンドマイクロのルールのみ)" on page 917
- "ルールを割り当てる/ルールの割り当てを解除する" on page 918
- "アップデートされた必須ルールを自動割り当てする" on page 918
- "ルールにイベントログを設定する" on page 919
- "アラートを生成する" on page 920
- "設定オプションを設定する(トレンドマイクロのルールのみ)" on page 920
- "有効な時間を予約する" on page 920
- "推奨設定から除外する" on page 921
- "ルールのコンテキストを設定する" on page 921
- "ルールの動作モードをオーバーライドする" on page 922
- "ルールおよびアプリケーションの種類の設定をオーバーライドする" on page 922
- "ルールをエクスポート/インポートする" on page 923
- "SQLインジェクション防御ルールの設定" on page 923

侵入防御モジュールの概要については、"侵入防御" on page 904を参照してください。

侵入防御ルールのリストを表示する

[ポリシー] 画面には侵入防御ルールのリストが表示されます。侵入防御ルールを検索し、ルールのプロパティを開いて編集できます。このリストでは、ルールはアプリケーションの種類で分類されており、ルールのプロパティは列にそれぞれ表示されます。

ヒント: [TippingPoint] 列には、対応するTrend Micro TippingPointルールIDが含まれます。侵入防御ルールの [詳細検索] では、TippingPointルールIDを検索できます。ポリシーおよびコンピュータエディタの割り当てられた侵入防御ルールのリストでもTippingPointルールIDを表示できます。

リストを確認するには、[ポリシー] をクリックして、[共通オブジェクト/ルール] の下の [侵入防御ルール] をクリックします。

侵入防御ルールに関する情報を表示する

侵入防御ルールのプロパティには、ルールおよび防御対象の攻撃コードに関する情報が含まれます。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。

一般情報

- 名前:侵入防御ルールの名前。
- 説明:侵入防御ルールの説明。
- 最小エージェント/アプライアンスバージョン: この侵入防御ルールをサポートするために必要な Deep Security Agentまたはアプライアンス[1] の最小バージョンです。

詳細

[新規] () または [プロパティ] () をクリックして、[侵入防御ルールプロパティ] 画面を表示します。

注意: [設定] タブを確認します。トレンドマイクロの侵入防御ルールは、Deep Security Manager で直接編集できません。その代わり、侵入防御ルールに設定が必要な場合や設定が可能な場合は、[設定] タブの設定オプションを使用します。ユーザ自身で作成したカスタム侵入防御ルールは、[ルール] タブが表示され、直接編集可能です。

侵入防御ルールのリストを表示する

[ポリシー] 画面には侵入防御ルールのリストが表示されます。侵入防御ルールを検索し、ルールのプロパティを開いて編集できます。このリストでは、ルールはアプリケーションの種類で分類されており、ルールのプロパティは列にそれぞれ表示されます。

ヒント: [TippingPoint] 列には、対応するTrend Micro TippingPointルールIDが含まれます。侵入防御ルールの [詳細検索] では、TippingPointルールIDを検索できます。ポリシーおよびコンピュータエディタの割り当てられた侵入防御ルールのリストでもTippingPointルールIDを表示できます。

リストを確認するには、[ポリシー] をクリックして、[共通オブジェクト/ルール] の下の [侵入防御ルール] をクリックします。

[1]Deep Security AgentとDeep Security Virtual Applianceは、ユーザが定義したDeep Securityポリシーを適用するためのコンポーネントです。Agentはコンピュータに直接インストールされ、ApplianceはAgentレスの保護を提供するためにVMware vSphere環境で使用されます。どちらもDeep Security as a Serviceでは使用できません。

一般情報

- アプリケーションの種類:この侵入防御ルールが分類されているアプリケーションの種類。

  ヒント: このパネルでアプリケーションの種類を編集できます。ここでアプリケーションの種類を編集すると、そのアプリケーションの種類を使用するすべてのセキュリティコンポーネントに対して変更内容が適用されます。

- 優先度: ルールの優先度。優先度の低いルールよりも優先度の高いルールが優先的に適用されます。
- 重要度:ルールの重要度の設定は、ルールの実装および適用方法に影響しません。重要度レベルは、侵入防御ルールのリストを表示するときにソート条件として使用できます。それぞれの重要度レベルは重要度の値と関連付けられます。この値にコンピュータの資産評価を掛けたものが、イベントのランク付けを決定します([管理]→[システム設定]→[ランク付け] を参照してください)。
- CVSSスコア:脆弱性情報データベースに基づいた、脆弱性の重要度の基準。

ID (トレンドマイクロのルールのみ)

- 種類:[スマート] (1つ以上の既知または不明なゼロデイの脆弱性)、[攻撃コード] (通常、署名ベースの攻撃コード) または [脆弱性] (1つ以上の攻撃コードが存在する可能性のある特定の脆弱性) のいずれかになります。
- 発行日: ルールがリリースされた日付。ダウンロードされた日付ではありません。
- 前回のアップデート: ローカルで、またはセキュリティアップデートのダウンロード中に、ルールが変更された前回の日時。
- 識別子: ルールに一意のIDタグ。

関連付けられている脆弱性に関する情報を表示する(トレンドマイクロのルールのみ)

トレンドマイクロが提供するルールには、ルールが守る脆弱性に関する情報を含めることができます。適用可能な場合は、共通脆弱性評価システム (CVSS) が表示されます(この評価システムの詳細は、脆弱性情報データベースのCVSSページを参照してください)。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して [プロパティ] をクリックします。
3. [脆弱性] タブをクリックします。

ルールを割り当てる/ルールの割り当てを解除する

Agent検索時に侵入防御ルールを適用するには、該当するポリシーとコンピュータに割り当てます。脆弱性にパッチが適用されたため、ルールが必要でなくなった場合は、ルールを割り当て解除できます。

コンピュータエディタ[1]で侵入防御ルールの割り当てを解除できない場合、そのルールがポリシーに割り当てられている可能性があります。ポリシーレベルで割り当てられたルールを削除するには**ポリシーエディタ**[2]を使用する必要があり、コンピュータレベルでは削除できません。

ポリシーに対する変更は、そのポリシーを使用するすべてのコンピュータに反映されます。たとえば、ポリシーからルールを割り当て解除すると、そのポリシーで保護しているすべてのコンピュータからルールが削除されます。継続してこのルールを他のコンピュータに適用するには、そのグループのコンピュータ用に新しいポリシーを作成します。("ポリシー、継承、およびオーバーライド" on page 724を参照してください)。

ヒント: ルールが割り当てられたポリシーとコンピュータを確認するには、ルールプロパティの [割り当て対象] タブをご覧ください。

1. [ポリシー] 画面に移動し、設定するポリシーを右クリックして [詳細] をクリックします。
2. [侵入防御]→[一般] の順にクリックします。
   ポリシーに割り当てられているルールのリストは、[現在割り当てられている侵入防御ルール] リストに表示されます。
3. [現在割り当てられている侵入防御ルール] で、[割り当て/割り当て解除] をクリックします。
4. ルールを割り当てるには、ルールの横にあるチェックボックスをオンにします。
5. ルールの割り当てを解除するには、ルールの横にあるチェックボックスをオフにします。
6. [OK] をクリックします。

アップデートされた必須ルールを自動割り当てする

セキュリティアップデートには、セカンダリ侵入防御ルールの割り当てが必要な新規またはアップデートされたアプリケーションの種類および侵入防御ルールが含まれている場合があります。Deep Security は、必要に応じてこれらのルールを自動的に割り当てることができます。ポリシーまたはコンピュータプロパティで、次のように自動割り当てを有効化できます。

1. [ポリシー] 画面に移動し、設定するポリシーを右クリックして [詳細] をクリックします。
2. [侵入防御]→[詳細] を順にクリックします。
3. 自動割り当てを有効にするには、[ルールアップデート] 領域で [はい] を選択します。
4. [OK] をクリックします。

---

[1] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック)します。

[2] ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック)します。

ルールにイベントログを設定する

ルールのイベントをログに記録するかどうか、ログにパケットデータを含めるかどうかを設定します。

注意: Deep Securityは、X-Forwarded-Forヘッダがパケットデータで利用可能な場合に侵入防御イベントに表示できます。この情報は、Deep Security Agentがロードバランサまたはプロキシの背後にある場合に役立ちます。X-Forwarded-Forヘッダデータは、イベントの[プロパティ]画面に表示されます。ヘッダデータを含めるには、ログにパケットデータを追加します。また、ルール1006540 [X-Forwarded-For HTTPヘッダのログを有効にする]も割り当てる必要があります。

それは、すべてのパケットデータルールはイベントをトリガするたびに記録することは非現実的ですので、のDeep Securityは、データにイベントは、指定された期間内で発生初回のみを記録します。初期設定時間は5分ですが、ポリシーの[ネットワークエンジンの詳細設定]の[1つのパケットデータのみをログに記録する期間]プロパティを使用して期間を変更できます。(「ネットワークエンジンの詳細オプション」を参照してください)。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" on page 922を参照してください。

1. [ポリシー]→[侵入防御ルール]の順にクリックします。
2. ルールを選択して[プロパティ]をクリックします。
3. [一般]タブで、[イベント]領域に移動し、次のように必要なオプションを選択します。
   - ルールのログを無効化するには、[イベントログの無効化]を選択します。
   - パケットが破棄またはブロックされた場合にイベントのログを記録するには、[パケット破棄時にイベントを生成]を選択します。
   - ログエントリにパケットデータを含めるには、[常にパケットデータを含める]を選択します。
   - ルールで検出されたパケットの前後のパケットをログに記録するには、[デバッグモードを有効にする]を選択します。サポート担当者から指示があった場合のみデバッグモードを使用します。

また、ログにパケットデータを含めるには、ルールを割り当てるポリシーで次のように、ルールによるパケットデータの取得を許可する必要があります。

1. [ポリシー]画面で、ルールを割り当てたポリシーを開きます。
2. [侵入防御]→[詳細]を順にクリックします。
3. [イベントデータ]領域で[はい]を選択します。

アラートを生成する

侵入防御ルールがイベントをトリガした場合にアラートを生成します。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" on page 922を参照してください。

1. [ポリシー]→[侵入防御ルール]の順にクリックします。
2. ルールを選択して[プロパティ]をクリックします。
3. [オプション]タブをクリックして[アラート]領域で[オン]を選択します。
4. [OK]をクリックします。

設定オプションを設定する(トレンドマイクロのルールのみ)

トレンドマイクロが提供する侵入防御ルールの中には、ヘッダ長、HTTPの許可される拡張子、Cookieの長さなど、1つ以上の設定オプションがあります。オプションには設定が必要なものもあります。必要なオプションを設定せずにルールを割り当てると、アラートが生成され、必要なオプションについての情報が表示されます。(これは、セキュリティアップデートによってダウンロードされ自動的に適用されたルールにも適用されます)。

設定オプションのある侵入防御ルールは、[侵入防御ルール]リストでルールのアイコンに小さなギアマークが付きます  。

> 注意: 独自のカスタム侵入防御ルールには、[ルール]タブがあり、ルールを編集できます。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" on page 922を参照してください。

1. [ポリシー]→[侵入防御ルール]の順にクリックします。
2. ルールを選択して[プロパティ]をクリックします。
3. [設定]タブをクリックします。
4. プロパティを設定して[OK]をクリックします。

有効な時間を予約する

侵入防御ルールが有効な時間を予約します。予約された時間のみ有効になる侵入防御ルールは、[侵入防御ルール]画面でルールのアイコンに小さな時計マークが付きます  。

注意: Agentベースの保護では、スケジュールで保護対象のエンドポイントと同じタイムゾーンが使用されます。Agentレスによる保護では、Deep Security Virtual Applianceと同じタイムゾーンが使用されます。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" on the next pageを参照してください。

1. [ポリシー]→[侵入防御ルール]の順にクリックします。
2. ルールを選択して[プロパティ]をクリックします。
3. [オプション]タブをクリックします。
4. [スケジュール]領域で[新規]を選択するか、頻度を選択します。
5. 必要に応じてスケジュールを編集します。
6. [OK]をクリックします。

推奨設定から除外する

推奨設定検索のルール推奨設定から侵入防御ルールを除外します。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" on the next pageを参照してください。

1. [ポリシー]→[侵入防御ルール]の順にクリックします。
2. ルールを選択して[プロパティ]をクリックします。
3. [オプション]タブをクリックします。
4. [推奨設定オプション]領域で[推奨設定から除外]を選択します。
5. [OK]をクリックします。

ルールのコンテキストを設定する

ルールが適用されるコンテキストを設定します。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" on the next pageを参照してください。

1. [ポリシー]→[侵入防御ルール]の順にクリックします。
2. ルールを選択して[プロパティ]をクリックします。
3. [オプション]タブをクリックします。
4. [コンテキスト]領域で[新規]を選択するか、コンテキストを選択します。

5. 必要に応じてコンテキストを編集します。
6. [OK] をクリックします。

ルールの動作モードをオーバーライドする

新しいルールをテストする場合は、侵入防御ルールの動作モードを[検出] に設定します。[検出] モードでは、ルールは「検出のみ:」という言葉で始まるログエントリを作成しますが、トラフィックに干渉しません。侵入防御ルールには [検出] モードでのみ動作するものがあります。これらのルールについては、動作モードを変更できません。

> 注意: ルールのログを無効にすると、動作モードに関係なく、ルールのアクティビティはログに記録されません。

動作モードの詳細については、"動作モードを使用してルールをテストする" on page 905を参照してください。

次の手順で設定を実行すると、すべてのポリシーが影響を受けます。ポリシーごとに1つのルールを設定する場合の詳細については、"ルールおよびアプリケーションの種類の設定をオーバーライドする" belowを参照してください。

1. [ポリシー]→[侵入防御ルール] の順にクリックします。
2. ルールを選択して[プロパティ] をクリックします。
3. [検出のみ] を選択します。

ルールおよびアプリケーションの種類の設定をオーバーライドする

コンピュータエディタとポリシーエディタ[1]で、侵入防御ルールを編集して、ポリシーまたはコンピュータのコンテキストのみで変更を適用できます。グローバルに変更が適用されるようにルールを編集して、ルールが割り当てられた他のポリシーおよびコンピュータで変更を有効にすることもできます。同様に、1つのポリシー/コンピュータ、またはグローバルにアプリケーションの種類を設定できます。

1. [ポリシー] 画面に移動し、設定するポリシーを右クリックして [詳細] をクリックします。
2. [侵入防御] をクリックします。
3. ルールを編集するには、ルールを右クリックして、次のコマンドのいずれかを選択します。
   - プロパティ: そのポリシーのみのルールを編集します。
   - プロパティ(グローバル): グローバルに (すべてのポリシーとコンピュータに対して) ルールを編集します。

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

4. ルールのアプリケーションの種類を編集するには、ルールを右クリックして、次のコマンドのいずれかを選択します。
   - アプリケーションの種類プロパティ: そのポリシーのみのアプリケーションの種類を編集します。
   - アプリケーションの種類プロパティ(グローバル): グローバルに(すべてのポリシーとコンピュータに対して)アプリケーションの種類を編集します。
5. [OK] をクリックします。

ヒント: ルールを選択して[プロパティ]をクリックした場合は、編集中のポリシーのみでルールを編集します。

注意: 1つのポートを割り当てできるアプリケーションの種類は8個までです。9個以上割り当てると、そのルールは該当するポートで機能しません。

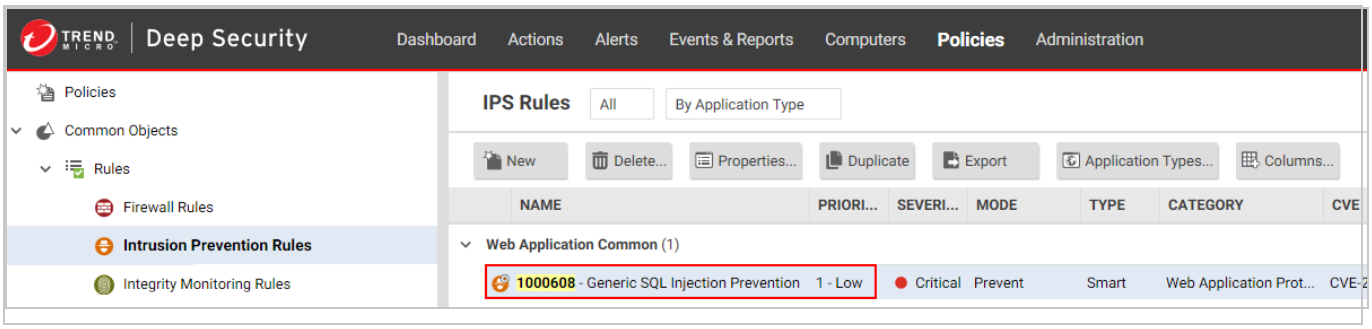
ルールをエクスポート/インポートする

1つ以上の侵入防御ルールをXMLまたはCSVファイルにエクスポートしたり、XMLファイルからルールをインポートできます。

1. [ポリシー]→[侵入防御ルール]の順にクリックします。
2. 1つ以上のルールをエクスポートするには、[エクスポート]→[選択したアイテムをCSV形式でエクスポート]または[エクスポート]→[選択したアイテムをXML形式でエクスポート]を順にクリックします。
3. すべてのルールをエクスポートするには、[エクスポート]→[CSV形式でエクスポート]または[エクスポート]→[XML形式でエクスポート]を順にクリックします。
4. ルールをインポートするには、[新規]→[ファイルからインポート]を順にクリックして、ウィザードの指示に従います。

SQLインジェクション防御ルールの設定

Deep Securityの侵入防御モジュールには、SQLインジェクション攻撃を検出して接続を破棄したり、特性に応じてログを記録するビルトインルールが含まれています。このルールは[1000608 - Generic SQL Injection Prevention]と呼ばれており、組織のニーズに合うように設定できます。たとえば、ルールの感度を変更するには、破棄のしきい値を変更します。



この記事のトピック:

- "SQLインジェクション攻撃とは" below
- "SQLインジェクション攻撃に共通する文字および文字列" below
- "Generic SQL Injection Preventionルールの仕組み" on page 926
- "ルールおよび評価システムの実例" on page 928
- "Generic SQL Injection Preventionルールを設定する" on page 930
- "文字エンコードのガイドライン" on page 933

SQLインジェクション攻撃とは

SQLインジェクション攻撃 (またはSQLフィッシング攻撃) はデータ駆動型アプリケーションの攻撃方法で、攻撃者の入力フィールドにはSQL文が分割して含まれます。新規に生成された不正なSQLコマンドがWebサイトからデータベースに渡され、実行されます。このコマンドによって、攻撃者はデータベース内の情報の読み取り、追加、削除、または変更ができます。

SQLインジェクション攻撃に共通する文字および文字列

以下は一般的に使用される文字および文字列の例です。このリストは一部です。

- ('
- %27
- \x22
- %22
- char
- ;
- ascii
- %3B
- %2B

- --
- %2D%2D
- /*
- %2F%2A
- */
- %2A%2F
- substring
- drop table
- drop+table
- insert into
- insert+into
- version(
- values
- group by
- group+by
- create table
- create+table
- delete
- update
- bulk insert
- bulk+insert
- load_file
- shutdown
- union
- having
- select
- declare
- exec
- and
- or
- like

- @@hostname
- @@tmpdir
- is null
- is+null
- is not null
- is+not+null
- %3D
- CONCAT
- %40%40basedir
- version%28,user(
- user%28,system_user(
- (,%28,)
- %29
- @
- %40
- cast

Generic SQL Injection Preventionルールの仕組み

Generic SQL Injection Preventionルールは、評価システムを使用してSQLインジェクション攻撃を検出します。ルールは次のように動作します。

1. アプリケーションからのパケットは、分析のためにDeep Security Agentに到着します。
2. Generic SQL Injection Preventionルールでは、パケットを検査して以下の表に示す文字列があるかどうかを確認します。文字列はカンマで区切られ、10個のグループに分類されています。
3. 文字列が見つかった場合、スコアが次のように計算されます。
   - 1つの文字列が見つかった場合は、そのグループのスコアが合計スコアになります。
   - 複数の文字列が異なるグループで見つかった場合は、それらのグループのスコアが合計されます。
   - 複数の文字列が同じグループに見つかった場合、そのグループのスコアは1度だけ加算されます。
     詳細については、"ルールおよび評価システムの実例" on page 928を参照してください。
4. 合計スコアを使用して、Deep Securityは接続を削除するかログに記録するかを決定します。合計スコアが破棄のしきい値スコアを超えた場合、接続は中断されます。ログしきい値スコアを超えた場合は、ログに記録されます。

注意: トレンドマイクロではルールが頻繁に更新されるため、次の表の文字列がDeep Security Managerの文字列と正確に一致しないことがあります。

注意: この表内の「\W」は、「この後に英数字以外の文字が続く」ことを示します。

グループ	スコア
drop table,drop+table,insert into,insert+into,values\W,create table,create+table,delete\W,update\W,bulk insert,bulk+insert,shutdown\W,from\W	2
declare\W,select\W	2
cast\W,exec\W,load_file	2
union\W,group by,group+by,order by,order+by,having\W	2
and\W,or\W,like\W,is null,is+null,is not null,is+not+null,where\W	1
--,%2D%2D,/*,%2F%2A,*/,%2A%2F	1
',%27,\x22,%22,char\W	1
;,%3B	1
%2B,CONCAT\W	1
%3D	1
(,%28,),%29,@,%40	1
ascii,substring	1
version(,version%28,user(,user%28,system_user(,system_user%28,database(,database%28,@@hostname,%40%40hostname,@@basedir,%40%40basedir,@@tmpdir,%40%40tmpdir, @@datadir,%40%40datadir	2

ルールおよび評価システムの実例

次に、スコアの集計方法とシナリオごとの処理方法の例を示します。

例1: トラフィックのログ記録と破棄が発生

次のルール設定 (グループのスコアはコロン(「:」) の後にあります) を使用すると仮定します。

```
drop table,drop+table,insert into,insert+into,values\W,create table,create+table,delete\W,update\W,bulk
insert,bulk+insert,shutdown\W,from\W:2
declare\W,select\W:2
cast\W,exec\W,load_file:2
union\W,group by,group+by,order by,order+by,having\W:2
and\W,or\W,like\W,is null,is+null,is not null,is+not+null,where\W:1
--,%2D%2D,/*,%2F%2A,*/,%2A%2F:1
',%27,\x22,%22,char\W:1
;,%3B:1
%2B,CONCAT\W:1
%3D:1
(,%28,),%29,@,%40:1
ascii,substring:1
version(,version%28,user(,user%28,system_user(,system_user%28,databas
(,database%28,@@hostname,%40%40hostname,@@basedir,%40%40basedir,@@tmpdir,%40%40t
mpdir,@@datadir,
%40%40datadir:2

Log Threshold: 3
Drop Threshold: 4
```

ここで、次の攻撃文字列が発生したとします。

`productID=BB10735166+UNION/**/+SELECT+FROM+user`

次の集計をして、合計スコアは5 (2+1+0+2) になります。

- 文字列`UNION/`は4番目のグループに一致するためスコアは2。
- 文字列`/*`は6番目のグループに一致するためスコアは1。
- 文字列`*/`は6番目のグループに一致するためスコアは0 (6番目のグループのスコアは加算済み)。
- 文字列`SELECT+`は2番目のグループに一致するためスコアは2。

合計スコアは5で、ログが生成され、トラフィックは破棄されます。

例2: トラフィックのログ/破棄が発生しない

次のルール設定 (`select\W`文字列は、`union\W`と同じ行に変更しました) を使用すると仮定します。

```
drop table,drop+table,insert into,insert+into,values\W,create table,create+table,delete\W,update\W,bulk
insert,bulk+insert,shutdown\W,from\W:2
declare\W:2
cast\W,exec\W,load_file:2
union\W,select\W,group by,group+by,order by,order+by,having\W:2
and\W,or\W,like\W,is null,is+null,is not null,is+not+null,where\W:1
--,%2D%2D,/*,%2F%2A,*/,%2A%2F:1
',%27,\x22,%22,char\W:1
;,%3B:1
%2B,CONCAT\W:1
%3D:1
(,%28,),%29,@,%40:1
ascii,substring:1
version(,version%28,user(,user%28,system_user(,system_user%28,databas
(,database%28,@@hostname,%40%40hostname,@@basedir,%40%40basedir,@@tmpdir,
%40%40tmpdir,@@datadir,%40%40datadir:2

Log Threshold: 3
Drop Threshold: 4
```

ここで、次の攻撃文字列が発生したとします。

```
productID=BB10735166+UNION/**/+SELECT+FROM+user
```

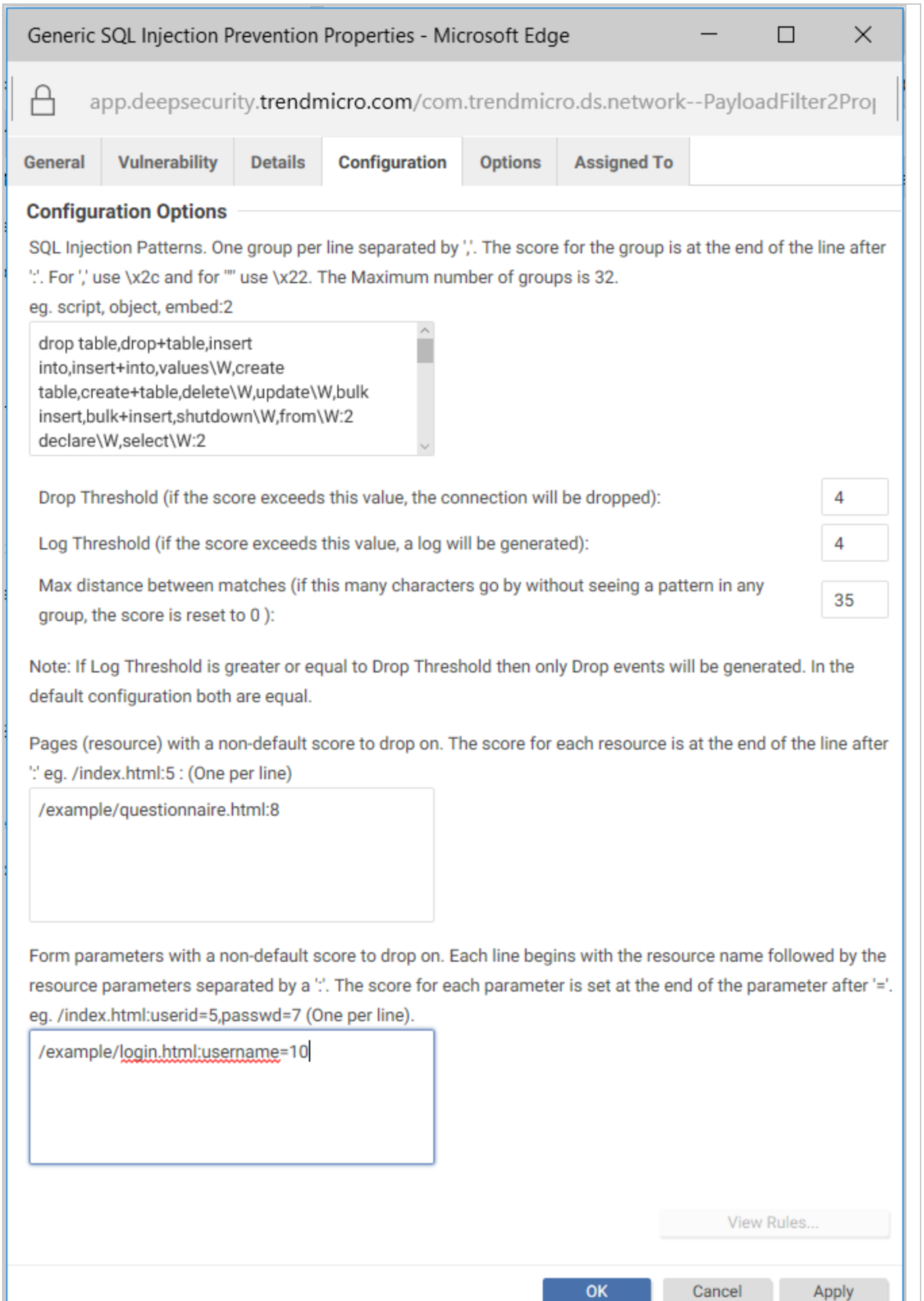
次の集計をして、合計スコアは3 (2+1+0+0) になります。

- 文字列`UNION/`は4番目のグループに一致するためスコアは2。
- 文字列`/*`は6番目のグループに一致するためスコアは1。
- 文字列`*/`は6番目のグループに一致するためスコアは0 (6番目のグループのスコアは加算済み)。
- 文字列`SELECT+`は4番目のグループに一致するためスコアは0 (4番目のグループのスコアは加算済み)。

合計スコアは3で、ログは生成されず、トラフィックは破棄されません。ログや破棄が発生するには、スコアがしきい値を超える必要があります。

Generic SQL Injection Preventionルールを設定する

Generic SQL Injection Preventionルールを組織のニーズに合うように設定できます。設定可能なオプションを次の図に示します。


Generic SQL Injection Prevention Properties - Microsoft Edge
app.deepsecurity.trendmicro.com/com.trendmicro.ds.network--PayloadFilter2Pro
General
Vulnerability
Details
Configuration
Options
Assigned To
Configuration Options
SQL Injection Patterns. One group per line separated by ','. The score for the group is at the end of the line after ':'. For ',' use \x2c and for '"' use \x22. The Maximum number of groups is 32.
eg. script, object, embed:2
drop table,drop+table,insert into,insert+into,values\W,create table,create+table,delete\W,update\W,bulk insert,bulk+insert,shutdown\W,from\W:2 declare\W,select\W:2
Drop Threshold (if the score exceeds this value, the connection will be dropped):
4
Log Threshold (if the score exceeds this value, a log will be generated):
4
Max distance between matches (if this many characters go by without seeing a pattern in any group, the score is reset to 0):
35
Note: If Log Threshold is greater or equal to Drop Threshold then only Drop events will be generated. In the default configuration both are equal.
Pages (resource) with a non-default score to drop on. The score for each resource is at the end of the line after ':' eg. /index.html:5 : (One per line)
/example/questionnaire.html:8
Form parameters with a non-default score to drop on. Each line begins with the resource name followed by the resource parameters separated by a ':'. The score for each parameter is set at the end of the parameter after '='. eg. /index.html:userid=5,passwd=7 (One per line).
/example/login.html:username=10
View Rules...
OK
Cancel
Apply

ルールを設定するには、次の手順に従います。

1. Deep Security Managerにログインします。
2. 画面上部の[ポリシー]をクリックします。
3. 右側にある検索ボックスにGeneric SQL Injection Preventionの番号IDの「1000608」を入力します。Enterキーを押します。メイン画面にルールが表示されます。
4. ルールをダブルクリックします。
5. [設定]タブをクリックします。画面上部のテキストボックスにSQLインジェクションパターンが表示されます。
6. カスタマイズをまだしていない場合は、このSQLインジェクションパターンを最新のバージョンにアップデートします。最新のパターンにアップデートするには、[詳細]タブに移動し、[Default SQL Pattern]見出しの下のテキストをコピーし、[設定]タブの[SQL Injection Patterns]テキストボックスに貼り付けます。現在、トレンドマイクロから最新のパターンファイルを使用して作業しています。
7. 次のようにフィールドを編集します。
   - SQL Injection Patterns: SQLインジェクション攻撃に使用する文字と文字列のリストを指定します。文字と文字列はグループ化されており、スコアが割り当てられています。文字列を追加または変更する場合は、適切なエンコードを使用してください。詳細については、以下の"文字エンコードのガイドライン" on the next pageを参照してください。
   - Drop Threshold: 破棄スコアを指定します。このしきい値をスコアが超えると、接続は中断されます。(スコアがDrop Thresholdと一致した場合、接続は維持されます)。初期設定は4です。
   - Log Threshold: ログスコアを指定します。このしきい値をスコアが超えると、接続のログが記録されます(スコアがLog Thresholdと一致した場合、ログは記録されません)。初期設定は4です。
   - Max distance between matches: スコアを0にリセットする場合の一致の最大間隔をバイト数で指定します。初期設定は35です。
   - 注意: 通常のしきい値では超過してしまう可能性があるページやフィールドのオーバーライドを作成する場合は、次の2つのオプションの使用を検討します。
   - Pages (resource) with a non-default score to drop on: 特定のリソースについては[Drop Threshold]をオーバーライドできます。たとえば、[Drop Threshold]は4ですが、アンケートページでは破棄スコアを8にする場合は、/example/questionnaire.html:8を指定します。この設定では、接続が中断される場合、/example/questionnaire.htmlには8より高いスコアが必要になりますが、その他すべてのリソースでは4より高いスコアで中断されます。リソースは1行に1つ指定します。

- Form parameters with a non-default score to drop on: [Drop Threshold] または [Pages (resources)with a non-default score to drop on] フィールドで定義したしきい値を特定のフォームフィールドについてはオーバーライドできます。たとえば、[Drop Threshold] スコアは4ですが、ユーザ名フィールドについては破棄スコアを高くして10にする場合は、/example/login.html:username=10を指定します。ここで、/example/login.htmlはユーザ名フィールドが表示されるページのパスと名前に置き換え、usernameはアプリケーションで使用するユーザ名フィールドに置き換えます。この設定では、接続が中断される場合、ユーザ名フィールドではスコアが10より高くなる必要がありますが、ページ自体では4を超えると中断されます。フォームフィールドは1行に1つ指定します。

  注意: [Log Threshold] は、[Pages (resources) with a non-default score to drop on] や [Form parameters with a non-default score to drop on] フィールドによる接続の中断時には有効になりません。たとえば、Form parametersフィールドを/example/login.html:username=10に設定していて、usernameフィールドのスコアが11の場合は、接続は中断されますが、このイベントのログは記録されません。

8. [OK] をクリックします。

これでGeneric SQL Injection Preventionルールの設定が完了しました。

文字エンコードのガイドライン

Generic SQL Injection Preventionルールに文字列の変更または追加をする場合は、適切にエンコードする必要があります。たとえば、パターン内で引用符'を使用する場合は、\x22を入力する必要があります。

以下の表に、文字とそのエンコード後の値、および拡張パターンを表現する場合に使用する文字クラスを示します。

入力する文字列	エンコードする文字
\a \A	英字 (a ~ z A ~ Z) 英字以外の文字 例: delete\aは「「delete」の後に英字が続く」ことを意味します
\w \W	英数字 (a ~ z A ~ Z 0 ~ 9) 英数字以外の文字

入力する文字列	エンコードする文字
	例：delete\W とは、「単語「削除」、その後に英数字以外の文字が続くこと」を意味します。
\d \D	数字 (0 ~ 9) 数字以外の文字 例：delete\dは「「delete」の後に数字 (0 ~ 9) が続く」ことを意味します
\s \S	空白文字 空白文字以外の文字 [\r,\n,\t,0x32] 例：delete\Sは「「delete」の後に空白以外の文字が続く」ことを意味します
\p \P	句読文字、上記以外の印字可能なASCII文字 句読文字以外の文字 例：delete\pは「「delete」の後に句読文字または印字可能なASCII文字が続く」ことを意味します
\c \C	制御文字 (ASCIIの32番より前または127番以降、空白文字は含まない) 制御文字以外の文字 制御文字の詳細については、ここを参照してください。
\.	任意
\xDD	16進数のバイト0xDD
\x2c	カンマ文字 (,)
\x22	2重引用符 (")
\\	エスケープされたバックスラッシュ (\)
|	エスケープされたパイプ (|)

入力する文字列	エンコードする文字
|xx xx xx...|	16進数パイプ(バイトシーケンス)

アプリケーションの種類

アプリケーションの種類で定義されるアプリケーションは、トラフィックの方向、使用しているプロトコル、およびトラフィックが通過するポート番号によって識別されます。アプリケーションの種類は、共通の目的がある侵入防御ルールをグループ化する場合に役立ちます。ルールグループによって、侵入防御ルールセットを選択してコンピュータに割り当てる処理が簡略化されます。たとえば、Oracle Report ServerへのHTTPトラフィックの保護に必要な侵入防御ルールセットを検討してみます。「Web Server Common」および「Web Server Oracle Report Server」のアプリケーションの種類でルールを選択して、IISサーバ専用のルールをなど、必要のないルールを除外するだけです。

アプリケーションの種類のリストを表示する

アプリケーションの種類のリストを開きます。ここでは、既存のアプリケーションの種類のプロパティ表示の他、設定、エクスポート、および複製ができます。XMLまたはCSVファイルにエクスポートできます。XMLファイルをインポートできます。アプリケーションの種類の作成と削除もできます。

1. [ポリシー]→[侵入防御ルール]の順にクリックします。
2. [アプリケーションの種類]をクリックします。
3. コマンドをアプリケーションの種類に適用するには、種類を選択して、該当するボタンをクリックします。

ヒント: 設定可能なプロパティがあるアプリケーションの種類にはギアアイコンが表示されます。

"ルールおよびアプリケーションの種類の設定をオーバーライドする" on page 922も参照してください。

一般情報

アプリケーションの種類の名前と説明です。「最小エージェント/アプライアンスバージョン」では、このアプリケーションタイプをサポートするためにDeep Security エージェントまたは アプライアンス[1] のどのバージョ

[1]Deep Security AgentとDeep Security Virtual Applianceは、ユーザが定義したDeep Securityポリシーを適用するためのコンポーネントです。Agentはコンピュータに直接インストールされ、ApplianceはAgentレスの保護を提供するためにVMware vSphere環境で使用されます。どちらもDeep Security as a Serviceでは使用できません。

ンが必要かを示しています。

接続

- 方向: 通信を開始する方向。つまり、2つのコンピュータ間で接続を確立する最初のパケットの方向です。たとえば、Webブラウザのアプリケーションの種類を定義する場合、これは通信を確立するための最初のパケットをサーバに送信するWebブラウザであるため、[送信] を選択します(サーバからブラウザに流れるトラフィックを調査する場合も同じです)。特定のアプリケーションの種類に関連付けられた侵入防御ルールは、いずれかの方向に流れる個々のパケットを調査するために作成できます。
- プロトコル: このアプリケーションの種類に適用されるプロトコル。
- ポート: このアプリケーションの種類が監視するポートトラフィックが例外的に許可されているポートは含まれません)。

設定

[設定] タブには、アプリケーションの種類に関連付けられた侵入防御ルールの処理を制御するオプションが表示されます。たとえば、種類が「Web Server Common」のアプリケーションには「Monitor responses from Web Server」オプションがあります。このオプションの選択を解除すると、アプリケーションの種類に関連付けられた侵入防御ルールでは、応答トラフィックが検査されません。

オプション

[オプション] [ ]タブの項目は、Deep Security Managerがアプリケーションの種類を使用および適用する方法を制御します。たとえば、ほとんどのアプリケーションの種類には、そのアプリケーションを推奨設定の検索から除外するためのオプションがあります。つまり、[推奨設定から除外] オプションを選択すると、推奨設定の検索では、対象のアプリケーションが検出された場合でも、このアプリケーションの種類およびアプリケーションの種類に関連付けられた侵入防御ルールがコンピュータに推奨されません。

割り当て対象

[割り当て対象] タブには、アプリケーションの種類に関連付けられた侵入防御ルールが一覧表示されます。

TLSトラフィックの検査

侵入防御モジュールに対して、高度なTLSトラフィック検査を有効にすることができます。

高度なTLSトラフィック検査とSSL検査は、圧縮されたトラフィックに対応していません。

このページの内容:

- 高度なTLSトラフィック検査の有効化
- 高度なTLSトラフィック監視を使用する
- "SSLインスペクションを設定する(レガシー)" on the next page
- "ポート設定を変更する" on page 939
- "トラフィックがPerfect Forward Secrecy (PFS)で暗号化されている場合に侵入防御を使用する" on page 939
- サポートされている暗号化スイート
- "サポートされているプロトコル" on page 947

高度なTLSトラフィック検査の有効化

高度なTLSトラフィック検査には、従来のSSL検査の実装に比べて次のような利点があります。

- これにより、TLS資格情報を手動で設定する必要がなくなります。
- PFS (Perfect Forward Secrecy) 暗号など、SSL検査よりも多くの暗号がサポートされています。詳細については、「サポートされている暗号化スイート」を参照してください。

侵入防御モジュールが有効になっている場合、インバウンドおよびアウトバウンドトラフィックに対してデフォルトで高度なTLSトラフィック検査が適用されます

- インバウンドTLS/SSLトラフィックの検査は、インバウンドトラフィックに対してデフォルトで有効になっています。
- 送信TLS/SSLトラフィックの検査はデフォルトで送信トラフィックに対して有効になっており、Deep Security Agentリリース20.0.1-12510(20 LTSアップデート2024-06-19)以降でサポートされています。

これらの設定を確認または調整し、アウトバウンドトラフィックの構成手順に関するガイダンスを取得するには、ポリシー>侵入防御>一般>高度なTLSトラフィック検査に移動してください。

受信トラフィックと送信トラフィックに高度なTLSトラフィック検査を使用する

高度なTLSトラフィック検査を有効にして、WindowsおよびLinuxプラットフォームの受信トラフィックと送信トラフィックに使用できます(「プラットフォームごとにサポートされる機能」を参照)。

Windowsでは、Advanced TLS Traffic InspectionはWindowsネイティブのTLS通信チャネル(Secure Channelを参照)を使用するトラフィックのみをサポートします。例えば、IIS、Microsoft Exchange、およびRemote Desktop Protocol (RDP)によって生成されるトラフィックが検査されます。Advanced TLS Traffic Inspectionが有効になると、TMExtractorというコンポーネントがアクティブになり、必要な検査を

実行します。DSAをアンインストールした後もTMExtractorファイルは残りますが、再起動後に自動的に削除されます。

Linuxでは、Advanced TLS Traffic InspectionはNGINX、Apache HTTP Server、HAProxy、およびTomcatサーバなどの一般的なWebアプリケーションによるトラフィックのみをサポートします。なお、TomcatサーバはLinux (64ビット) 上のOpenJDK 8のみをサポートし、コンテナなしで実行されます。

高度なTLSトラフィック検査でサポートされていないTLSトラフィック、または他のオペレーティングシステムのTLSトラフィックを検査する必要がある場合は、代わりに従来のSSL検査を設定できます。

SSLインスペクションを設定する(レガシー)

保護対象のコンピュータの1つ以上のインタフェースで、特定の資格情報とポートのペアに対してSSLインスペクションを設定できます。

資格情報は、PKCS#12またはPEM形式でインポートできます。資格情報ファイルには、秘密鍵が含まれている必要があります。Windowsコンピュータでは、CryptoAPIを直接使用できます。

1. Deep Security Managerで、設定するコンピュータを選択し、[詳細]をクリックしてコンピュータエディタを開きます。
2. コンピュータエディタの左側の画面で、[侵入防御]→[詳細]→[SSL設定の表示] の順にクリックし、[SSL設定の表示] をクリックして [SSL設定] 画面を開きます。
3. [新規] をクリックして、SSL設定ウィザードを開きます。
4. このコンピュータで設定を適用するインタフェースを指定します。
   - このコンピュータのすべてのインタフェースに適用するには、[すべてのインタフェース] を選択します。
   - 特定のインタフェースに適用するには、[特定のインタフェース] を選択します。
5. [ポート] または [ポートリスト] を選択してリストを選択し、[次へ] をクリックします。
6. [IP選択] 画面で、[すべてのIP] を選択するか、SSLインスペクションを実行する [特定のIP] を指定し、[次へ] をクリックします。
7. [資格情報] 画面で、資格情報を指定する方法を選択します。
   - 今すぐ資格情報をアップロードします
   - 資格情報はコンピュータにあります

   > 注意: 資格情報ファイルには、秘密鍵が含まれている必要があります。
8. 今すぐ資格情報をアップロードするオプションを選択する場合、資格情報の種類、格納場所、および必要に応じてパスフレーズを入力します。

   資格情報がコンピュータにある場合は、[資格情報の詳細] を入力します。

- コンピュータに格納されているPEMまたはPKCS#12資格情報形式を使用する場合は、その資格情報ファイルの格納場所と必要に応じてファイルのパスフレーズを入力します。
- Windows CryptoAPI資格情報を使用する場合は、コンピュータで見つかった資格情報のリストから対象の資格情報を選択します。

9. この設定の名前と説明を入力します。
10. 概要を確認して、SSL設定ウィザードを閉じます。設定操作の概要を読んで、[完了] をクリックしてウィザードを閉じます。

ポート設定を変更する

コンピュータのポート設定を変更して、クライアントがSSL対応ポートで適切な侵入防御 フィルタを実行していることを確認します。加えた変更は、Agentコンピュータ上の特定のアプリケーションの種類(Webサーバ共通など) に適用されます。この変更は、他のコンピュータ上のアプリケーションの種類には影響しません。

1. このコンピュータに適用されている侵入防御 ルールのリストを表示するには、コンピュータの[詳細]画面の[侵入防御ルール]の順に選択します。
2. ルールを[アプリケーションの種類] 別にソートし、「Webサーバ共通」のアプリケーションの種類を探します(同様のアプリケーションの種類に対しても、これらの変更を加えることができます)。
3. アプリケーションの種類のルールを右クリックし、[アプリケーションの種類プロパティ] をクリックします。
4. 継承された「HTTP」ポートリストをオーバーライドして、SSLの設定時に定義したポートとポート80をこのポートリストに追加します。ポートはカンマ区切りの値として入力します。たとえば、SSLの設定でポート9090を使用する場合は、「9090, 80」と入力します。
5. パフォーマンスを向上させるために、[設定] タブで、[継承] と[Webサーバからの応答を監視] の選択を解除します。
6. [OK] をクリックして画面を閉じます。

トラフィックがPerfect Forward Secrecy (PFS)で暗号化されている場合に侵入防御を使用する

Perfect Forward Secrecy (PFS) を使用することで、仮に後でサーバの秘密鍵が侵害された場合に復号できない通信チャネルを作成できます。Perfect Forward Secrecyの目的はセッション終了後の復号化を防ぐことであるため、侵入防御モジュールがSSLインスペクションでトラフィックを確認することも防止します。

注意:
高度なTLSトラフィック検査を使用すると、侵入防御モジュールは、追加の設定を行わなくても、PFS暗号で暗号化されたトラフィックを分析できます。

代わりにSSLインスペクションでPFS暗号を使用するには、次の手順を実行します。

1. インターネットとロードバランサまたはリバースプロキシ間のTLSトラフィックには、Perfect Forward Secrecyを使用します。
2. ロードバランサまたはリバースプロキシでPerfect Forward Secrecyセッションを終了します。
3. ロードバランサ(またはリバースプロキシ)とWebサーバまたはアプリケーションサーバの間のトラフィックには、非PFS暗号化スイート(後述の"サポートされている暗号化スイート" on the next page を参照)を使用して、サーバ上の侵入防御モジュールがTLSセッションを復号して検査できるようにします。
4. Perfect Forward Secrecyを使用しないアプリケーションサーバポートのトラフィックをWebサーバに制限します。

SSL Inspectionを使用する場合のDiffie-Hellman暗号に関する特別な考慮事項

Perfect Forward Secrecyは、Diffie-Hellman鍵交換アルゴリズムに依存しています。初期設定でDiffie-Hellmanが使用されるWebサーバでは、SSLインスペクションが正常に動作しない場足があります。そのため、サーバの設定ファイルを確認して、Webサーバとロードバランサ(またはリバースプロキシ)の間のTLSトラフィックに対してDiffie-Hellman暗号化を無効にすることが重要です。ApacheサーバでDiffie-Hellmanを無効にするには、次の手順を実行します。

1. サーバの設定ファイルを開きます。Webサーバ設定ファイルのファイル名と場所は、OSおよびディストリビューションによって異なります。たとえば、次のようなパスになります。
   - RHEL4の初期インストールの場合: `/etc/httpd/conf.d/ssl.conf`
   - Red Hat Linux上のApache 2.2.2の場合: `/apache2/conf/extra/httpd-ssl.conf`
2. ファイル内で「`SSLCipherSuite`」変数を見つけます。
3. 「`!DH:!EDH:!ADH:`」をこれらのフィールドに追加します(この文字列がまだ表示されていない場合)。(「`!`」: この暗号化をApacheで「使用しない」ように指定するものです)。
4. たとえば、Apache設定ファイルの暗号化スイートを次のように編集します。

```
SSLCipherSuite
!DH:!EDH:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
```

SSL Inspectionを使用する場合に限り、前述の情報が適用されます。Advanced TLS Traffic Inspectionを使用する場合は適用されません。

詳細については、Apacheドキュメント「`SSLCipherSuite`: http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite」を参照してください。

サポートされている暗号化スイート

16進値	OpenSSL名	IANA名	NSS名	高度なTLS検査	SSLインスペクション(レガシー)
0x00,0x04	RC4-MD5	TLS_RSA_WITH_RC4_128_MD5	SSL_RSA_WITH_RC4_128_MD5	✓	✓
0x00,0x05	RC4-SHA	TLS_RSA_WITH_RC4_128_SHA	SSL_RSA_WITH_RC4_128_SHA	✓	✓
0x00,0x09	DES-CBC-SHA	TLS_RSA_WITH_DES_CBC_SHA	SSL_RSA_WITH_DES_CBC_SHA	✓	✓
0x00,0x0A	DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA	SSL_RSA_WITH_3DES_EDE_CBC_SHA	✓	✓
0x00,0x2F	AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA	TLS_RSA_WITH_AES_128_CBC_SHA	✓	✓
0x00,0x33	DHE-RSA-AES128-SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	✓	
0x00,0x35	AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA	TLS_RSA_WITH_AES_256_CBC_SHA	✓	✓
0x00,0x39	DHE-RSA-	TLS_DHE_	TLS_DHE_	✓	

16進値	OpenSSL名	IANA名	NSS名	高度なTLS検査	SSLインスペクション(レガシー)
	AES256-SHA	RSA_WITH_AES_256_CBC_SHA	RSA_WITH_AES_256_CBC_SHA		
0x00,0x3C	AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256	✓	✓
0x00,0x3D	AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256	✓	✓
0x00,0x41	CAMELLIA128-SHA	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	✓	✓
0x00,0x67	DHE-RSA-AES128-SHA256	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	✓	
0x00,0x6b	DHE-RSA-AES256-SHA256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	✓	
0x00,0x84	CAMELLIA256-SHA	TLS_RSA_WITH_CAMELLIA_	TLS_RSA_WITH_CAMELLIA_	✓	✓

16進値	OpenSSL名	IANA名	NSS名	高度なTLS検査	SSLインスペクション(レガシー)
		256_CBC_SHA	256_CBC_SHA		
0x00,0x9c	AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256	✓	✓
0x00,0x9d	AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384	✓	✓
0x00,0x9e	DHE-RSA-AES128-GCM-SHA256	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	✓	
0x00,0x9f	DHE-RSA-AES256-GCM-SHA384	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	✓	
0x00,0xBA	CAMELLIA128-SHA256	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	✓	✓
0x00,0xC0	CAMELLIA256-SHA256	TLS_RSA_WITH_CAMELLIA_256_CBC_	TLS_RSA_WITH_CAMELLIA_256_CBC_	✓	✓

16進値	OpenSSL名	IANA名	NSS名	高度なTLS検査	SSLインスペクション(レガシー)
		SHA256	SHA256		
0xc0,0x09	ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	✓	
0xC0,0x0A	ECDHE-ECDSA-AES256-SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	✓	
0xc0,0x13	ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	✓	
0xc0,0x14	ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	✓	
0xc0,0x23	ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	✓	
0xc0,0x24	ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	✓	

16進値	OpenSSL名	IANA名	NSS名	高度なTLS検査	SSLインスペクション(レガシー)
0xc0,0x27	ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	✓	
0xc0,0x28	ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	✓	
0xc0,0x2b	ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	✓	
0xc0,0x2c	ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	✓	
0xc0,0x2f	ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	✓	
0xc0,0x30	ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	✓	
0xC0,0x9C	AES128-CCM	TLS_RSA_WITH_AES_	TLS_RSA_WITH_AES_	✓	✓

16進値	OpenSSL名	IANA名	NSS名	高度なTLS検査	SSLインスペクション(レガシー)
		128_CCM	128_CCM		
0xC0,0x9D	AES256-CCM	TLS_RSA_WITH_AES_256_CCM	TLS_RSA_WITH_AES_256_CCM	✓	✓
0xC0,0xA0	AES128-CCM8	TLS_RSA_WITH_AES_128_CCM_8	TLS_RSA_WITH_AES_128_CCM_8	✓	✓
0xC0,0xA1	AES256-CCM8	TLS_RSA_WITH_AES_256_CCM_8	TLS_RSA_WITH_AES_256_CCM_8	✓	✓
0xcc,0xa8	ECDHE-RSA-CHACHA20-POLY1305	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	✓	
0xcc,0xa9	ECDHE-ECDSA-CHACHA20-POLY1305	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	✓	
0xcc,0xaa	DHE-RSA-CHACHA20-POLY1305	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	✓	

サポートされているプロトコル

次のプロトコルがサポートされます。

- TLS 1.0
- TLS 1.1
- TLS 1.2
- TLS 1.3 (Linuxのみ)

SSL 3.0 の検査はサポートされておらず、デフォルトでブロックされています。

TLSインスペクションのサポート

- Deep Security Agent 20 TLSインスペクションのサポート

TLS検査サポートパッケージのアップデートの管理

この機能では、サポートされているプラットフォームのTLS検査サポートパッケージが常にアップデートされますが、その他の不要なアップデートは無効にできます。

この機能には次のものが必要です。

- Deep Security Manager 20.0.665+
- サポートされるプラットフォーム上のDeep Security Agent 20.0.0.5512+。AIXまたはSolarisではサポートされていません。

高度なTLSトラフィック監視機能でサポートされるプラットフォームのリストについては、"各プラットフォームでサポートされている機能" on page 417を参照してください。

1つのエージェントでTLS検査サポートパッケージのアップデートを無効にする

1. Deep Security Managerで、[コンピュータ]画面に進みます。
2. 更新を無効にするコンピューターをダブルクリックします(または、コンピューターを選択してから、[詳細]ボタンを選択します) 。
3. [設定]を選択します。[高度なTLSトラフィック検査のTLS検査パッケージを自動的にアップデートする]を[いいえ]に変更します。
4. 変更を保存します。

ポリシーによるTLS検査サポートパッケージのアップデートの無効化

この方法では、同じポリシーで保護されているすべてのコンピュータのTLS検査サポートパッケージのアップデートが無効になります。

1. Deep Security Managerで、[ポリシー] ページに移動します。
2. 更新を無効にするポリシーをダブルクリックします(またはポリシーを選択してから、[詳細]ボタンを選択します) 。既存のポリシーをアップデートする代わりに、新しいポリシーを作成することもできます。
3. [設定]を選択します。[高度なTLSトラフィック検査のTLS検査パッケージを自動的にアップデートする]を[いいえ]に変更します。
4. 変更を保存します。

回避技術対策の設定

回避技術対策の設定では、分析を回避しようとする異常なパケットに対するネットワークエンジンによる処理を管理します。回避技術対策の設定は、ポリシーまたは個々のコンピュータで設定されます。セキュリティモード設定は、侵入防御がパケットをどの程度厳密に分析するかを管理し、次のいずれかの値に設定できます。

- 標準: 誤検出が発生しないように侵入防御ルールの回避を防ぎます。これが初期設定値です。
- 厳格: 標準モードよりも厳密なチェックが行われますが、誤検出が発生する場合があります。厳密モードは侵入テストに役立ちますが、通常の状況下では有効にしないでください。
- Custom: Customを選択した場合、Deep Securityがパケットの問題を処理する方法を指定できる追加設定が使用可能になります。これらの設定の場合(TCPタイムスタンプPAWS Window), を除き、オプションは を許可します(Deep Securityはシステムにパケットを送信します)), ログのみ(許可と同じ動作ですが、イベントがログに記録されます)), 拒否 (Deep Securityでパケットが破棄され、イベントが記録される), または 拒否サイレント(拒否と同じ動作が、ログに記録されないイベント)):

> 注意: Deep Security 10.1以前のバージョンでモードを「カスタム」に変更した場合は、回避技術対策設定のすべての初期設定値が「拒否」に設定されていました。これにより、ブロックイベントが大幅に増加しました。Deep Security 10.2では、初期設定のカスタム値が次の表のように変更されています。

設定	説明	標準値	厳格値	初期設定のカスタム値(10.2より前)	初期設定のカスタム値(10.2以降)
無効なTCPタイムスタンプ	TCPタイムスタンプが古い場合の処理	無視とログ(ログのみと同じ機能)	拒否(ログに記録)	拒否(ログに記録)	無視とログ(ログのみと同じ機能)
TCP PAWS ウィンドウ	パケットにはタイムスタンプが付加されている場合があります。パケットのタイムスタンプが、それ以前に受信したタイムスタンプよりも古い場合、不審なタイムスタンプが使用されている可能性があります。タイムスタンプの差異についての許容度は、OSによって異なります。Windowsシステムの場合、0を選択してください(パケットのタイムスタンプが、それ以前のパケットと同じ、もしくは新しい場合、システムがパケットを受容します)。Linuxシステムの場合は、1を選択してください(パケットのタイムスタンプの古さが、それ以前のパケットより最大で1秒未満の場合、システムがパケットを受容します)。	Linux Agentの場合は1、それ以外の場合は0	Linux Agentの場合は1、それ以外の場合は0	0	Linux Agentの場合は1、それ以外の場合は0
TCPタイムスタンプ(PAWS: Protection Against Wrapped Sequence)の値がゼロ	TCPタイムスタンプがゼロの場合の処理	Linux AgentまたはNDIS5の場合は拒否、それ以外の場合は許可	Linux AgentまたはNDIS5の場合は拒否、それ以外の場合は許可	拒否(ログに記録)	Linux AgentまたはNDIS5の場合は拒否、それ以外の場合は許可
フラグメント化されたパケット	パケットがフラグメント化されている場合の処理	許可	許可	拒否(ログに記録)	許可

設定	説明	標準値	厳格値	初期設定のカスタム値(10.2より前)	初期設定のカスタム値(10.2以降)
TCPゼロフラグ	パケットにゼロフラグが設定されている場合の処理	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)
TCP輻輳フラグ	パケットに輻輳フラグが設定されている場合の処理	許可	許可	拒否 (ログに記録)	許可
TCP緊急フラグ	パケットに緊急フラグが設定されている場合の処理	許可	拒否 (ログに記録)	拒否 (ログに記録)	許可
TCP SYN FINフラグ	パケットにSYNおよびFINフラグが設定されている場合の処理	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)
TCP SYN RSTフラグ	パケットにSYNおよびRSTフラグが設定されている場合の処理	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)
TCP RST FINフラグ	パケットにRSTおよびFINフラグが設定されている場合の処理	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)
TCP SYNパケット(データあり)	パケットにSYNフラグが設定されていて、かつデータが含まれる場合の処理	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)
TCP Split Handshake	SYNへの応答として、SYN-ACKの代わりにSYNが受信されたときに実行する処理です。	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)	拒否 (ログに記録)
識別できないTCPセッション上のRSTパケット	識別できないTCPセッション上のRSTパケットに対する処理	許可	拒否 (ログに記録)	拒否 (ログに記録)	許可
識別できない	識別できないTCPセッション	許可	拒否 (ロ	拒否	許可

設定	説明	標準値	厳格値	初期設定のカスタム値(10.2より前)	初期設定のカスタム値(10.2以降)
TCPセッション上のFINパケット	上のFINパケットに対する処理		グに記録)	(ログに記録)	
識別できないTCPセッション上の送信パケット	識別できないTCPセッション上の送信パケットに対する処理	許可	拒否(ログに記録)	拒否(ログに記録)	許可
回避再送	複製または重複したデータを含むパケットに対する処理	許可	拒否(ログに記録)	拒否(ログに記録)	許可
TCPチェックサム	無効なチェックサムを含むパケットに対する処理	許可	拒否(ログに記録)	拒否(ログに記録)	許可

侵入防御のパフォーマンスに関するヒント

Deep Security Agentでシステムリソースの使用率を向上させるには、特定のパフォーマンス関連設定を最適化します。

侵入防御モジュールの概要については、"侵入防御" on page 904を参照してください。

システムリソース	パフォーマンスに影響する設定
CPU使用率	• パケットが破棄またブロックされたときにイベントがログに記録されます。パケットの変更をログに記録すると、多くのログエントリが作成される可能性があります。("ルールにイベントログを設定する" on page 919を参照してください)。 • トラブルシューティング中にのみイベントログにパケットデータを含めます("ルールにイベントログを設定する" on page 919を参照してください)。 • コンピュータのOSとアプリケーションに適用される侵入防御ルールを割り当てます。該当する脆弱性およびルールを検出するための推奨設定の検索の使用については、"推奨設定の検索の管理と実行" on page 728を参照してくださ

システムリソース	パフォーマンスに影響する設定
	い。 • 割り当てるルールの数を300以下にします。
ネットワーク使用量またはスループット	• パケットが破棄またブロックされたときにイベントがログに記録されます。パケットの変更をログに記録すると、多くのログエントリが作成される可能性があります。("ルールにイベントログを設定する" on page 919を参照してください)。 • トラブルシューティング中にのみイベントログにパケットデータを含めます("ルールにイベントログを設定する" on page 919を参照してください)。 • 特にポリシーに多数の署名が適用されている場合はWebサーバから応答を監視しないでください。 a. [ポリシー]→[侵入防御ルール]の順にクリックします。 b. アプリケーションの種類「Web Server Common」のルールを右クリックし、[アプリケーションの種類プロパティ]をクリックします。 c. [設定]タブで、[継承]と[Webサーバからの応答を監視]の選択を解除します。
ディスク使用量	• トラブルシューティング中にのみイベントログにパケットデータを含めます("ルールにイベントログを設定する" on page 919を参照してください)。

設定パッケージの最大サイズ

Agentに大量の侵入防御ルールを割り当てている場合、設定パッケージのサイズが最大許容サイズを超えることがあります。許容サイズを超えると、Agentのステータスが「Agentの設定パッケージが大きすぎる」に変わり、イベントメッセージ「設定パッケージが大きすぎる」が表示されます。

注意: 32ビットのWindowsプラットフォームでは、使用できるカーネルメモリが小さいため、設定制限が20MBまでになっています。他のプラットフォームでは、制限は32MBです。

パフォーマンス上の理由から、1台のコンピュータに割り当てる侵入防御ルールは350未満にしてください。必要なルールの数を最小限にするために、コンピュータのOSとインストールされているサードパーティのソフトウェアに、使用可能なすべてのパッチが適用されていることを確認してください。

1. 使用可能なパッチをコンピュータのOSに適用します。
2. 使用可能なパッチをインストールされているすべてのサードパーティのソフトウェアに適用します。

3. 推奨設定の検索で推奨されている侵入防御ルールのみを適用します。コンピュータからすべてのルール、または割り当ての解除が推奨されている割り当て済みポリシーを削除します("推奨設定の検索の管理と実行" on page 728を参照してください)。
4. ポリシーレベルで侵入防御を管理していて、設定パッケージがまだ大きすぎる場合は、次のいずれかの方法で侵入防御を設定します。
   - ポリシー内のすべてのサーバが同じOSとアプリケーションを持つように、ポリシーを細分化します。
   - コンピュータのルールが自動的に追加および削除されるように、侵入防御をサーバレベルで管理します。

侵入防御をサーバレベルで管理するには、次の手順に従います。

1. コンピュータに割り当てられているポリシーをエディタで開きます。
2. [侵入防御]→[一般] の順にクリックします。
3. [推奨設定] セクションで、[侵入防御の推奨設定を自動的に適用 (可能な場合)] を [はい] に設定します。
4. ポリシーからすべての侵入防御ルールを削除します。
5. コンピュータで推奨設定の検索を実行します。

ファイアウォール設定

ファイアウォールについて

ファイアウォールモジュールは、受信/送信トラフィックの双方向のステートフルインスペクションを提供します。ファイアウォールルールでは、そのトラフィックの個々のパケットに対して実行する処理を定義します。パケットは、すべてのIPベースのプロトコルとフレームタイプで、IPアドレスとMACアドレス、ポートとパケットフラグを使ってフィルタできます。ファイアウォールモジュールはまた、DoS攻撃を防ぎ、攻撃の予兆検索を検出して防ぐのにも役立ちます。

ファイアウォールを有効にして設定するには、"Deep Securityファイアウォールの設定" on the next pageを参照してください。

ファイアウォールルール

ファイアウォールルールでは、優先度の順に示した次のいずれかの処理によってトラフィックを処理できます。

- バイパス
- ログ記録のみ

- 強制的に許可
- 拒否 (ログに記録)
- 許可

また、ルールには4 (優先度が最も高い) ~ 0 (優先度が最も低い) の優先度があります。特定の優先度内では、上記のルール処理の種類における優先度に基づいた順序で処理されます。つまり、他のファイアウォールを設定する際に経験したこととは異なり、Deep Securityファイアウォールはルールを割り当て順序とは別に処理します。

ルールの優先度と処理で処理順序が決まる仕組みの詳細については、「"ファイアウォールルールの処理と優先度" on page 975」を参照してください。

ファイアウォールルールの作成方法の詳細については、"ファイアウォールルールの作成" on page 967を参照してください。

注意: ルールを作成するときは、配信する前に、ファイアウォールモジュールのタップモードとインラインモードを使用して必ずテストしてください。この方法の詳細については、"Deep Securityファイアウォールの設定" belowの「ファイアウォールルールを配信前にテストする」セクションを参照してください。

Deep Securityファイアウォールの設定

Deep Security ファイアウォールは、非常に柔軟なファイアウォールで、制限または許可するように設定できます。侵入防御やWebレピュテーションモジュールと同様に、ファイアウォールモジュールもインラインまたはタップモードの2つのモードで実行できます。ファイアウォールルールをタップモードでテストし、すべてが正しく動作することを確認してからインラインモードに切り替えることを推奨します。

ファイアウォールの設定と管理は慎重に行う必要があり、すべての環境に合うルールセットは存在しません。ルールの作成を開始する前にファイアウォールの処理と優先度を理解しておく必要があります。許可ルールを作成する場合、定義されていない対象がすべて黙示的に拒否されるため、特に注意が必要です。

このトピックの内容:

- "ファイアウォールルールを配信前にテストする" on the next page
- "「Fail-Open」の動作を有効にする" on page 957
- "ファイアウォールをオンにする" on page 958
- "初期設定のファイアウォールルール" on page 958
- "厳格または寛容なファイアウォール設計" on page 960

- "ファイアウォールルールの処理" on page 960
- "ファイアウォールルールの優先度" on page 961
- "推奨されるファイアウォールポリシールール" on page 962
- "ファイアウォールルールをテストする" on page 963
- "攻撃の予兆検索" on page 964
- "ステートフルインスペクション" on page 965
- "例" on page 965
- "重要事項" on page 966

ファイアウォールルールを配信前にテストする

ファイアウォールモジュール(および侵入防御およびWebレピュテーションモジュール)には、パケットをブロックするか、またはパケットを許可するかを決定するDeep Securityネットワークエンジンが含まれています。ファイアウォールモジュールと侵入防御モジュールの場合、ネットワークエンジンはパケットのサニティチェックを実行し、ファイアウォールと侵入防御のルールを各パケットが通過することも確認します。ネットワークエンジンは次の2つのモードで動作します。

- タップモード: パケットストリームは変更されません。ファイアウォールまたは侵入防御モジュールが有効になっている場合、トラフィックはこれらによって処理されます。ただし、問題が検出されてもパケットや接続が拒否されることはありません。タップモードでは、Deep Securityはイベントのレコードを提供する以外の保護は提供しません。
- インラインモード: パケットストリームはDeep Securityネットワークエンジンを直接通過します。すべてのルールは、プロトコルスタックの上位に伝わる前にネットワークトラフィックに適用されます。

配信前はルールの処理を[ログ記録のみ]に設定し、タップモードかインラインモードのいずれかでファイアウォールルールをテストすることが重要です。これにより、トラフィックに対するルールの影響を、処理を実行することなくプレビューできます。配信前にルールをテストしない場合、トラフィックがすべてブロックされ、コンピュータにアクセスできなくなる可能性があります。

タップモードでテストする

タップモードでは、トラフィックのフローを妨げることなくファイアウォールルールをテストできます。

1. Deep Security Managerの Computers または Policies に移動します。
2. コンピュータ(またはポリシー) を右クリックして [詳細] を選択し、**コンピュータエディタまたはポリシーエディタ**[1]を開きます。
3. [設定]→[詳細]→[ネットワークエンジンモード] の順に選択します。
4. リストから[タップ] を選択し、[保存] をクリックします。
5. ルールを作成し、[OK] をクリックします。ルールを確認するには、[イベントとレポート]→[イベント]→[ファイアウォールイベント] に移動します。

注意: タップモードではルールの処理を[ログ記録のみ] に設定する必要はありません。

ファイアウォールルールの結果に問題がない場合は、**コンピュータエディタまたはポリシーエディタ**[2]に戻ってドロップダウンリストから[インライン] を選択し、[保存] をクリックします。

インラインモードでテストする

多くの場合、トラフィックを妨げることなくファイアウォールルールをテストするにはタップモードが良い方法となります。しかし、ルールの処理を[ログ記録のみ] に設定すると、インラインモードでもルールをテストできます。この方法ではトラフィック分析の実際のプロセスが発生し、パケットのブロックや拒否などの処理を実行する必要がありません。

1. Deep Security Managerの Computers または Policies に移動します。
2. コンピュータ(またはポリシー) を右クリックして [詳細] を選択し、**コンピュータエディタまたはポリシーエディタ**[3]を開きます。
3. [設定]→[詳細]→[ネットワークエンジンモード] の順に選択します。
4. ドロップダウンメニューから[インライン] を選択し、[保存] をクリックします。
5. ルールを作成するときは、処理を[ログ記録のみ] に設定しておきます。
6. ルールを確認するには、[イベントとレポート]→[イベント]→[ファイアウォールイベント] に移動します。

ファイアウォールルールの結果に問題がない場合は、処理を[ログ記録のみ] から任意の処理に変更し、[OK] をクリックします。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

[2] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

[3] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

「Fail-Open」の動作を有効にする

ケースによっては、ファイアウォールルール(または侵入防御ルール)を適用する前にネットワークエンジンがパケットをブロックすることがあります。初期設定では、ネットワークエンジンは次の場合にパケットをブロックします。

- AgentまたはVirtual Applianceにメモリ不足などのシステム上の問題がある。
- パケットのサニティチェックでエラーが発生する。

この「Fail-Closed」動作により、高度なセキュリティが提供されます。AgentまたはVirtual Applianceが正常に機能していないときもサイバー攻撃がネットワークに侵入することはできず、不正と思われるパケットから保護できます。「Fail-Closed」の問題は、AgentまたはVirtual Applianceの問題によってサービスおよびアプリケーションが利用できなくなる場合があることです。また、パケットのサニティチェックの誤判定が多いために大量のパケットが必要以上にドロップされ、パフォーマンスの問題が発生することもあります。

サービス可用性に関して懸念がある場合は、以下の手順に従って、システムエラーやパケットチェックエラーの場合にもパケットの通過を許可する(「Fail-Open」にする)ように初期設定の動作を変更できます。

1. Deep Security Managerの Computers または Policies に移動します。
2. コンピュータ(またはポリシー)を右クリックして[詳細]を選択し、**コンピュータエディタまたはポリシーエディタ**[1]を開きます。
3. 左側にある[設定]をクリックします。
4. [詳細]タブをクリックします。
5. [ネットワークエンジン設定]で、[エラー発生時の処理]を次のように設定します。
6. Deep Securityネットワークエンジンで問題が発生した場合(メモリ不足エラー、割り当てメモリエラー、ネットワークエンジンの Deep Packet Inspection (DPI) デコードエラーなど)のパケットの通過を許可するには、[ネットワークエンジンのシステムエラー]を[Fail-Open]に設定します。ここで、Fail-Openの使用を検討するのは、高負荷やリソース不足によりAgentまたはVirtual Appliance でネットワーク例外が頻繁に発生する場合です。フェイルオープンの場合、ネットワークエンジンはパケットを通過させ、侵入防御ルールチェックを実行せず、イベントをログに記録します。AgentまたはVirtual Applianceに問題がある場合でも、サービスとアプリケーションは利用し続けることができます。
7. ネットワークエンジンのパケットのサニティチェックでエラーとなるパケットの通過を許可するには、[ネットワークパケットのサニティチェックエラー]を[Fail-Open]に設定します。パケットのサニティ

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

チェックの例としては、ファイアウォールのサニティチェック、ネットワーク層2、3、または4の属性チェック、TCP状態チェックなどがあります。侵入防御ルールを実行する場合は、健全性チェックに合格する「良好な」パケットのみをチェックする場合は、ここでフェイルオープンを使用することを検討してください。フェイルオープンの場合、ネットワークエンジンは失敗したパケットを通過させ、侵入防御ルールのチェックを実行せず、イベントをログに記録します。

8. [保存] をクリックします。

これで、システムまたはパケットチェックエラーに対するFail-Open動作が有効になります。

ファイアウォールをオンにする

コンピュータでファイアウォール機能を有効にするには、次の手順に従います。

1. コンピュータエディタまたはポリシーエディタ[1]で、[ファイアウォール]→[一般] の順に選択します。
2. Deep Security Agent 11.1以前では、ホストコンピュータのネットワークインタフェースを通過してコンテナに向かうトラフィックがファイアウォールモジュールによって監視されます。Deep Security Agent 11.2以降では、コンテナ間のトラフィックを監視することもできます。[コンテナのネットワークトラフィックの検索] 設定が [はい] に設定されている場合、コンテナとホストの両方を通過するトラフィックがDeep Securityによって検索されます。[いいえ] に設定されている場合、Deep Securityで検索されるのは、ホストネットワークインタフェースを通過するトラフィックだけです。
3. [オン] を選択し、[保存] をクリックします。

注意: 少なくとも1つのファイアウォールルールでDeep Security ファイアウォールを有効にすると、Agentは競合を回避するためにWindows ファイアウォールを自動的に無効にします。

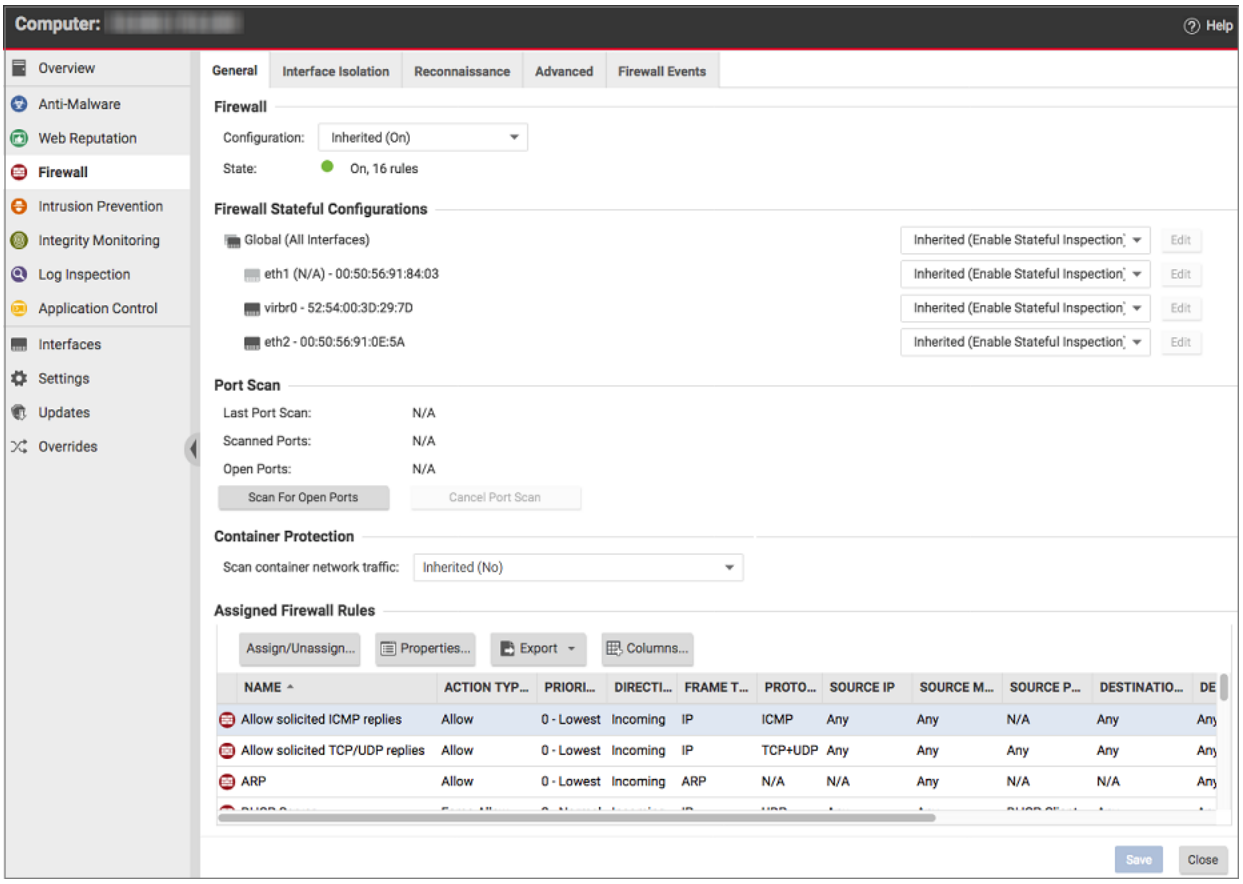
初期設定のファイアウォールルール

初期設定ではDeep Securityに付属するポリシーには送信ルールは割り当てられませんが、いくつかの推奨受信ルールがあります。各ポリシーに割り当てられた初期設定の受信ルールは、該当するオペレーティングシステムポリシーで [ファイアウォール] タブを選択して確認できます。次の例は、Windows 10 Desktopポリシーに初期設定で割り当てられているファイアウォールルールを示しています。これらのファイアウォールルールは環境のニーズに合わせて設定できますが、すぐに始められるようにいくつかの初期設定ルールがあらかじめ用意されています。

ヒント: システムパフォーマンスへの影響を最小限に抑えるには、300件より多くファイアウォールルールを割り当てないようにします。また、ファイアウォールルールへの変更をそのルールの [説明] フィールドに

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

記録することも推奨します。より簡単にファイアウォールをメンテナンスするために、ルールを作成または削除した日付とその理由を記録してください。



デフォルトのバイパスルール(Deep Security Managerトラフィック用)

Deep Security Managerは、Priority 4 Bypass Ruleを自動的に実装します。このルールは、Deep Security Agentを実行しているコンピュータ上でハートビートのエージェントの待機ポート番号を開きます。このルールは優先度4なので、他の拒否ルールよりも先に適用されます。また、バイパスルールなので、トラフィックの障害が発生することはありません。なお、このバイパスルールは内部的に作成されるため、ファイアウォールルールの一覧には明示的に表示されません。

ただし、このルールでは、任意のIPアドレスと任意のMACアドレスからのトラフィックが許可されます。Deep Security Agentの待機ポートを強化するには、このポートに対して代替バイパスルールを作成することもできます。次の設定が適用されている場合、エージェントは初期設定のDeep Security Managerトラフィックルールを新しいカスタムルールで上書きします。

- 優先度: 4 (最高)
- パケット方向: 受信

- フレームの種類: IP
- プロトコル: TCP
- パケット送信先ポート: Agentのハートビートの待機ポート

初期設定のルールをカスタムルールに置き換えるには、カスタムルールに上記のパラメータが必要です。理想的には、実際のDeep Security ManagerのIPアドレスまたはMACアドレスをルールのパケット送信元として使用する必要があります。

厳格または寛容なファイアウォール設計

一般に、ファイアウォールポリシーは、2つの設計戦略のどちらかに基づいています。つまり、明示的に拒否されていないかぎりすべてのサービスを許可するか、明示的に許可されていないかぎりすべてのサービスを拒否するかのいずれかです。どちらのタイプのファイアウォールを実装するか決定しておくことを推奨します。これにより、ルールの作成とメンテナンスにかかる管理の手間を削減できます。

厳格なファイアウォール

厳格なファイアウォールは、セキュリティの観点から推奨されます。初期設定ではすべてのトラフィックがブロックされ、明示的に許可されたトラフィックだけが許可されます。計画しているファイアウォールの主な目的が不正なアクセスをブロックすることであれば、接続を許可するのではなく制限することを重視する必要があります。厳格なファイアウォールはメンテナンスが比較的容易であり、安全性にも優れています。許可ルールを使用して、ファイアウォールを通過する特定のトラフィックだけを許可し、他はすべて拒否します。

注意: 送信の許可ルールを1つ割り当てると同時に、送信ファイアウォールが制限モードで稼働します。これは受信ファイアウォールの場合も同じです。受信の許可ルールを1つ割り当てると同時に、受信ファイアウォールが制限モードで稼働します。

寛容なファイアウォール

寛容なファイアウォールは、初期設定ですべてのトラフィックを許可し、設定されている拒否ファイアウォールルールに基づいて既知の不正なポート/プロトコルのみをブロックします。寛容なファイアウォールは実装は容易ですが、提供されるセキュリティは最小限であり、複雑なルールが必要です。拒否ルールを使用して、トラフィックを明示的にブロックします。

ファイアウォールルールの処理

ファイアウォールは、以下の処理を実行するように設定できます。

警告: 受信ルールのみを割り当てると、送信トラフィックはすべて許可されます。送信許可ルールを1つ割り当てると、送信ファイアウォールは制限モードで稼働します。ただし、1つだけ例外があります。ICMPv6トラフィックは、拒否ルールで明確にブロックされていないかぎり、常に許可されます。

許可	ルールと一致するトラフィックの通過を明示的に許可し、その他のトラフィックは黙示的に拒否します。 注意: [許可]の処理は定義されていないトラフィックをすべて黙示的に拒否するため、この処理は慎重に使用する必要があります。関連するルールを正しく定義せずに許可ルールを作成すると、許可ルールで許可したトラフィックを除き、すべてのトラフィックがブロックされる可能性があります。許可ルールで明示的に許可されていないトラフィックは破棄され、ポリシーで「未許可」のファイアウォールイベントとして記録されます。
バイパス	ファイアウォールと侵入防御分析の両方のバイパスをトラフィックに許可します。バイパスルールは常にペアで(受信トラフィックと送信トラフィックの両方に対して)作成する必要があります。バイパスルールは、IP、ポート、トラフィックの方向、プロトコルに基づいて設定できます。 バイパスルールは、ネットワーク負荷の高いプロトコルや、信頼済みソースからのトラフィックのために設計されたものです。
拒否	ルールと一致するトラフィックを明示的にブロックします。
強制的に許可	強制的に許可ルールに一致したパケットは通過しますが、この場合でも侵入防御によるフィルタリングは行われます。イベントはログに記録されません。 UDPおよびICMPトラフィックには、この種類のファイアウォールルール処理を使用する必要があります。
ログのみ	トラフィックがルールに一致した場合、ログに記録されます。その他の処理は実行されません。

ファイアウォールルールの作成方法の詳細については、「"ファイアウォールルールの作成" on page 967」を参照してください。

ファイアウォールルールの優先度

ルールの優先度によって、フィルタが適用される順序が決定します。優先度の低いルールよりも優先度の高いルールが優先的に適用されます。同じ優先度の処理が複数存在する場合のルールの優先度は、「バイパス」、「強制的に許可」、「拒否」の順になります。ただし、より高い優先度が適用された

拒否処理は、より低い優先度が適用されたバイパス処理よりも優先されます。ルールの優先度と処理で処理順序が決まる仕組みの詳細については、「"ファイアウォールルールの処理と優先度" on page 975」を参照してください。

ファイアウォールルールの管理を簡略化するには、特定の処理に対して所定の優先度を固定します。たとえば、バイパスを使用するルールには初期設定の優先度3を、強制的に許可ルールには優先度2を、拒否ルールには優先度1を適用します。こうすることで、ルールの競合を削減できます。

許可ルール

許可ルールに適用できる優先度は0のみです。これは、より高い優先度の強制的に許可ルールおよび拒否ルールがすべて適用された後で許可ルールが処理されるようにするためです。許可ルールを使用してトラフィックを黙示的に拒否するときにはこの点に注意してください (許可ルールに一致しないトラフィックはすべて拒否されます)。こうすることで、拒否ルールを割り当てると、割り当てられている既存のすべての許可ルールよりも拒否ルールが優先されます。

強制的に許可ルール

強制的に許可ルールは、常に許可する必要があるトラフィック (アドレス解決プロトコル (ARP) など) に推奨されるルールで、同じまたはより高い優先度の拒否ルールに対してのみ機能します。たとえば、10.0.0.0/8サブネットから許可ポート番号へのアクセスを禁止する優先度3の拒否ルールがあり、ホスト10.102.12.56にこのポート番号へのアクセスを許可したいとします。この場合、優先度3の拒否ルールに対して優先度3または4の強制的に許可ルールを作成する必要があります。あるパケットがこのルールに該当するとそのアクセスはただちに許可され、優先度の低いルールは以降このアクセスを処理できなくなります。

バイパスルール

バイパスルールは、ファイアウォールエンジンとDeep Packet Inspection (DPI) エンジンの両方をバイパスすることをパケットに許可する特別なルールです。このルールは優先度4に設定し、ペアで作成する必要があります (各トラフィック方向に対して1つ)。

推奨されるファイアウォールポリシールール

すべてのファイアウォールポリシーに対して以下のルールを必須にすることを推奨します。

- ARP: コンピュータへの受信ARP要求を許可し、コンピュータがMACアドレスのクエリに応答できるようにします。このルールを割り当てないと、ネットワーク上のデバイスはホストにMACアドレスで照会できず、ホストにネットワークからアクセスできなくなります。

- Allow solicited TCP/UDP replies: コンピュータが、送信したTCP接続やUDPのメッセージへの応答を受信できるようにします。これは、TCPとUDPのステートフルファイアウォール設定と連携します。
- Allow solicited ICMP replies: コンピュータが、送信したICMPメッセージへの応答を受信できるようにします。これは、ICMPのステートフルファイアウォール設定と連携します。
- DNS Server: DNSサーバが受信DNSクエリを受け取ることができるようにします。
- Remote Access RDP: コンピュータがリモートデスクトップ接続を受け入れることができるようにします。
- Remote Access SSH: コンピュータがSSH接続を受け入れることができるようにします。

ファイアウォールルールをテストする

以降のファイアウォール設定手順に進む前に、推奨されるファイアウォールルールをテストし、それらが正しく動作することを確認します。

次の手順でRemote Access SSHルールをテストします。

1. コンピュータに対するSSH接続の確立を試みます。ファイアウォールが有効でも、Remote Access SSHルールが有効になっていないと、接続は拒否されます。[イベントとレポート]→[ファイアウォールイベント] の順に選択し、拒否されたイベントを表示します。
2. コンピュータエディタまたはポリシーエディタ[1]で [ファイアウォール] に移動します。[割り当てられたファイアウォールルール] で [割り当て/割り当て解除] をクリックします。
3. Remote Access SSHを検索してそのルールを有効にします。[OK] をクリックし、[保存] をクリックします。
4. コンピュータに対するSSH接続の確立を試みます。接続が許可されます。

次の手順でRemote Access RDPルールをテストします。

1. コンピュータに対するRDP接続の確立を試みます。ファイアウォールが有効でも、Remote Access RDPルールが有効になっていないと、接続は拒否されます。[イベントとレポート]→[ファイアウォール] イベントの順に選択し、拒否されたイベントを表示します。
2. コンピュータエディタまたはポリシーエディタ[2]で [ファイアウォール] に移動します。[割り当てられたファイアウォールルール] で [割り当て/割り当て解除] をクリックします。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

[2] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

3. Remote Access RDPを検索してそのルールを有効にします。[OK] をクリックし、[保存] をクリックします。
4. コンピュータに対するRDP接続の確立を試みます。接続が許可されます。

攻撃の予兆検索

攻撃の予兆検索を検出するようにファイアウォールを設定し、一時的に送信元IPからのトラフィックをブロックして攻撃の防止を図ることができます。攻撃が検出されると、一時的に送信元IPからのトラフィックをAgentおよびApplianceでブロックするように設定できます。ポリシーまたはコンピュータエディタの [ファイアウォール]→[攻撃の予兆] タブにある [トラフィックのブロック] リストを使用し、時間 (分数) を設定してください。

- OSのフィンガープリント調査: AgentまたはApplianceはコンピュータのOSを見つけようとする動作を検出します。
- ネットワークまたはポートの検索: AgentまたはApplianceは、リモートIPがポートに対して異常な割合のIPでアクセスしていることを検出した場合、ネットワークまたはポート検索をレポートします。通常、AgentまたはApplianceのコンピュータは、コンピュータ自身宛てのトラフィックのみを監視するため、ポート検索が最も一般的に検出されます。コンピュータまたはポート検索の検出で使用される統計的な分析方法は「TAPS」アルゴリズムから導出されたもので、2006年にIPCCCで発表された「Connectionless Port Scan Detection on the Backbone」で提案されました。
- TCP Null検索: AgentまたはApplianceはフラグが付いていないパッケージを検出します。
- TCP SYNFIN検索: AgentまたはApplianceはSYNフラグおよびFINフラグの付いたパケットのみ検出します。
- TCP Xmas検索: AgentまたはApplianceは、FINフラグ、URGフラグ、およびPSHフラグの付いたパケット、または値0xFF (想定されるすべてのフラグ) を含むパケットを検出します。

エージェントまたはアプライアンスは、攻撃の種類ごとに、[DSMにただちに通知]オプションを選択して、アラートが送信されるDeep Security Managerに情報を送信するように指示できます。このオプションを機能させるには、エージェントとアプライアンスは ポリシー/ コンピュータエディタ>設定>一般>通信方向のエージェントまたはアプライアンスが開始したか、双方向通信用に設定する必要があります。有効にすると、エージェントまたはアプライアンスは攻撃またはプローブの検出時にただちにDeep Security Managerに対するハートビートを開始します。

注意: 攻撃の予兆の保護を有効にする場合は、ポリシーまたはコンピュータエディタの [ファイアウォール]→[一般] タブで、ファイアウォールおよびステートフルインスペクションも有効にする必要があります。また、ポリシーまたはコンピュータエディタの [ファイアウォール]→[詳細] タブで、[「ポリシーの許可外」の

パケットのファイアウォールイベントを生成]設定も有効にする必要があります。これにより、攻撃の予兆に必要なファイアウォールイベントが生成されるようになります。

注意: 攻撃の予兆の検出では、1つ以上のアクティブなファイアウォールルールがAgentのポリシーに割り当てられている必要があります。

攻撃の予兆警告に対応する方法の詳細については、"警告: 攻撃の予兆の検出" on page 1453を参照してください。

ステートフルインスペクション

Deep Security ファイアウォールステートフル設定メカニズムは、ファイアウォールがオンの場合に有効にする必要があります。このメカニズムでは、トラフィック履歴との関連における各パケット、TCPおよびIPヘッダ値の正当性、およびTCP接続状態の推移が分析されます。UDPやICMPなどのステートレスプロトコルの場合、履歴トラフィック分析に基づいた擬似ステートフルメカニズムが実装されます。

パケットは、ステートフルメカニズムによって次のように処理されます。

1. 静的ファイアウォールルール条件によってパケットの通過が許可された場合、パケットはステートフルルーチンに渡されます。
2. パケットを調べて、既存の接続に属しているかどうかが判断されます。
3. TCPヘッダの正当性 (シーケンス番号、フラグの組み合わせなど) が調査されます。

Deep Security ファイアウォールステートフル設定を使用すると、Stateful TCP、ICMP、またはUDPプロトコルを使用する初期設定が有効で、要求された応答のみが許可されている場合に、サービス拒否などの攻撃から保護することができます。UDPステートフルオプションが有効な場合は、UDPサーバ (DHCPなど) の実行時に強制的に許可を使用する必要があります。Deep Security Agent用にDNSサーバまたはWINSサーバが設定されていない場合、NetBIOSでは[受信UDPポートを強制的に許可する]ルールが必要になることがあります。

ステートフルログは、ICMPまたはUDPプロトコルで必要でない限り無効にする必要があります。

例

Webサーバ用の単純なファイアウォールポリシーを作成する方法の例を示します。

1. オプションが有効になっているグローバルなファイアウォールステートフル設定を使用して、TCP、UDP、およびICMPのステートフルインスペクションを有効にします。
2. ワークステーションからの要求に対するTCPおよびUDPの応答を許可するファイアウォールルールを追加します。そのためには、受信許可ルールを作成し、プロトコルセットを[TCP+UDP]に設定し、[指定フラグ]の下にある[選択以外]と[SYN]をオンにします。この時点で、ワークステーショ

ンのユーザからの要求に応答するTCPとUDPのパケットだけがポリシーによって許可されます。たとえば、手順1で有効にしたステートフル分析オプションと連動してこのルールを使用すると、コンピュータのユーザはDNS検索 (UDP経由) やHTTP (TCP) 経由のWeb閲覧ができるようになります。

3. ワークステーションからの要求にICMP応答を許可するファイアウォールルールを追加します。そのためには、プロトコルを [ICMP] に設定した受信許可ルールを作成し、[任意のフラグ] チェックボックスをオンにします。このコンピュータのユーザは別のワークステーションにpingを送信して応答を受信できますが、他のユーザはこのコンピュータにpingを送信できなくなります。

4. [指定フラグ] セクションの [SYN] チェックボックスをオンにして、受信TCPトラフィックをポート80およびポート443に対して許可するファイアウォールルールを追加します。外部ユーザがこのコンピュータのWebサーバにアクセスできるようになります。

   この時点で、他の受信トラフィックをすべて拒否するコンピュータで、承諾されたTCP、UDP、およびICMP応答とWebサーバへの外部アクセスを許可する基本的なファイアウォールポリシーが設定されます。

   拒否ルールおよび強制的に許可ルールの処理を使用してこのポリシーをさらに詳細に定義する方法の例について、ネットワーク内の他のコンピュータからのトラフィックを制限する方法を考察します。たとえば、内部ユーザに対してはこのコンピュータのWebサーバへのアクセスを許可し、DMZにあるコンピュータからのアクセスは拒否するものとします。この場合、DMZのIP範囲にあるサーバからのアクセスを禁止する拒否ルールを追加することによって設定が可能になります。

5. 送信元IP 10.0.0.0/24 (DMZ内のコンピュータに割り当てられたIP範囲) を使用して、受信TCPトラフィック用に拒否ルールを追加します。このルールでは、DMZ内にあるコンピュータからこのコンピュータへのトラフィックをすべて拒否します。

   ただし、このポリシーをさらに詳細に定義するとDMZ内にあるメールサーバからの受信トラフィックを許可できます。

6. 送信元IP 10.0.0.100からの受信TCPトラフィックに強制的に許可ルールを使用します。この強制的に許可ルールは、前の手順で作成した拒否ルールをオーバーライドして、DMZ内にあるコンピュータからのトラフィックを許可します。

重要事項

- すべてのトラフィックは、まずファイアウォールルールと照合されてからステートフルインスペクションエンジンで分析されます。トラフィックがファイアウォールルールを通過した場合は、ステートフルインスペクションエンジンによって分析されます (ステートフルインスペクションがファイアウォールステートフル設定で有効になっているものとします)。

- 許可ルールは暗黙の拒否ルールを含んでいます。許可ルールで指定されていないトラフィックは自動的に破棄されます。このルールには他の種類のフレームのトラフィックが含まれるため、他のフレームの種類の必要なトラフィックを許可するルールを含める必要があります。たとえば、静的ARPテーブルを使用していない場合にはARPトラフィックを許可するルールを忘れずに含める必要があります。
- UDPのステートフルインスペクションが有効になっている場合は、強制的に許可ルールを使用して未承諾のUDPトラフィックを許可する必要があります。たとえば、UDPステートフルインスペクションがDNSサーバで有効になっている場合に、サーバが受信DNS要求を受け入れるように、強制的に許可ルールをポート53に設定する必要があります。
- ICMPのステートフルインスペクションが有効になっている場合は、強制的に許可ルールを使用して未承諾のICMPトラフィックを許可する必要があります。たとえば、外部のping要求を許可する場合は、ICMPタイプ3 (エコー要求) を強制的に許可するルールが必要です。
- 強制的に許可の処理は、同じ優先度のコンテキスト内でのみ切り札として機能します。
- テスト環境でよく見られるようにDNSまたはWINSサーバが設定されていない場合は、受信のUDPポート137を強制的に許可するルールがNetBIOS (Windows共有) に必要となることがあります。

注意: 新しいファイアウォールポリシーのトラブルシューティング時には、まずAgentまたはAppliance[1]にあるファイアウォールルールのログを確認してください。ファイアウォールルールのログには、拒否されているトラフィックを判断するために必要な情報がすべて含まれており、必要に応じてポリシーをさらに詳細に設定できます。

ファイアウォールルールの作成

ファイアウォールルールは、個々のパケットの制御情報を確認し、定義された条件に従ってブロックまたは許可します。ファイアウォールルールは、ポリシー、または直接コンピュータに割り当てることができます。

注意: ここでは、ファイアウォールルールの作成方法を具体的に説明します。ファイアウォールモジュールの設定方法については、"Deep Securityファイアウォールの設定" on page 954を参照してください。

新しいファイアウォールルールを作成するには、次の手順を実行する必要があります。

---

[1]Deep Security AgentとDeep Security Virtual Applianceは、ユーザが定義したDeep Securityポリシーを適用するためのコンポーネントです。Agentはコンピュータに直接インストールされ、ApplianceはAgentレスの保護を提供するためにVMware vSphere環境で使用されます。どちらもDeep Security as a Serviceでは使用できません。

1. "新しいルールを追加する" below。
2. "ルールの動作とプロトコルを選択する" below。
3. "パケットの送信元と送信先を選択する" on page 971。

ファイアウォールルールを作成したら、次の方法も学習できます。

- "ルールイベントとアラートを設定する" on page 972
- "ルールのスケジュールを設定する" on page 972
- "ルールが割り当てられているポリシーとコンピュータを確認する" on page 973
- "ルールにコンテキストを割り当てる" on page 972

新しいルールを追加する

[ポリシー]→[共通オブジェクト]→[ルール]→[ファイアウォールルール] ページで新しいファイアウォールルールを追加する方法は3つあります。次の手順を実行します。

- 新しいルールを作成します。[新規]→[新規ファイアウォールルール] の順にクリックします。
- XMLファイルからルールをインポートします。[新規]→[ファイルからインポート] をクリックします。
- 既存のルールをコピーして変更します。[ファイアウォールルール] リストで、該当のルールを右クリックし、[複製] をクリックします。新しいルールを編集するには、そのルールを選択し、[プロパティ] をクリックします。

ルールの動作とプロトコルを選択する

1. ルールの [名前] と[説明] を入力します。

   ヒント: ファイアウォールルールへの変更をそのルールの [説明] フィールドに記録することを推奨します。ファイアウォールのメンテナンスを簡単にするため、ルールを作成または削除した日付とその理由を記録してください。

2. ルールがパケットに対して実行する[処理] を選択します。次の5つの処理のいずれかを選択できます。

   注意: 1つのパケットに適用されるのは、1つのルール処理だけです。同じ優先度のルールが複数ある場合は、下記の優先順序で適用されます。

   - トラフィックにファイアウォールのバイパスを許可できます。バイパスルールにより、トラフィックはファイアウォールと侵入防御エンジンを可能な限り早く通過できます。バイパスルールは、フィ

ルタリングを望まないマルチメディア系プロトコルを使用するトラフィックや、信頼済みソースからのトラフィックに対して使用します。

ヒント: ポリシーで信頼済みソース用のバイパスルールを作成して使用する方法の例については、"信頼済みトラフィックに対するファイアウォールのバイパス許可" on page 973を参照してください。

注意: バイパスルールは単一方向です。トラフィックの各方向に対して明確なルールが必要です。

ヒント: 次の設定を使用して、バイパスルールで最大のスループットパフォーマンスを達成できます。

- 優先度: 最高
- フレームの種類: IP
- プロトコル: TCP、UDP、またはその他のIPプロトコル(「任意」オプションは使用しないでください)
- 送信元および送信先のIPおよびMAC: すべて「任意」
- プロトコルがTCPまたはUDPでトラフィックの方向が「受信」の場合は、送信先ポートを「任意」ではなく1つ以上指定する必要があり、送信元ポートを「任意」にする必要があります。
- プロトコルがTCPまたはUDPでトラフィックの方向が「送信」の場合は、送信元ポートを「任意」ではなく1つ以上指定する必要があり、送信先ポートを「任意」にする必要があります。
- スケジュール: なし

- ログ記録のみが可能です。この処理では、ログにエントリは作成されますが、トラフィックは処理されません。
- 定義済みのトラフィックを強制的に許可できます(他のトラフィックを除外することなく、このルールによって定義されたトラフィックを許可できます)。
- トラフィックの拒否が可能です(このルールによって定義されたトラフィックを拒否します)。
- トラフィックの許可が可能です(このフィルタによって定義されたトラフィックを例外的に許可します)。

注意: コンピュータに有効な許可ルールがない場合、拒否ルールでブロックされていないかぎり、すべてのトラフィックが許可されます。許可ルールを1つ作成したら、許可ルールの条件を満

たしていないかぎり、その他すべてのトラフィックがブロックされます。ただし、1つだけ例外があります。ICMPv6トラフィックは、拒否ルールで明確にブロックされていない限り、常に許可されます。

3. ルールの[優先度]を選択します。優先度により、ルールが適用される順序を決定します。ルール処理に「強制的に許可」、「拒否」、または「バイパス」を選択した場合は、0(最低)から4(最高)の優先度を設定できます。優先度を設定すると、ルール処理を組み合わせて、階層型のルール効果を実現できます。

   注意: ログのみルールでの優先度は4のみ設定でき、許可ルールでは0のみが設定できます。

   注意: 優先度の低いルールよりも優先度の高いルールが優先的に適用されます。たとえば、ポート80の受信を強制的に許可する優先度2のルールが適用されるより前に、ポート80の受信を拒否する優先度3のルールが適用され、パケットを破棄します。

   処理と優先度の関係の詳細については、"ファイアウォールルールの処理と優先度" on page 975を参照してください。

4. [パケットの方向]を選択します。このルールを受信(ネットワークからコンピュータ)または送信(コンピュータからネットワーク)トラフィックのどちらに適用するかを選択します。

   注意: 個々のファイアウォールルールは、単一のトラフィック方向にのみ適用されます。特定の種類のトラフィックに対しては、受信および送信ファイアウォールルールをペアで作成する必要があります。

5. イーサネットの[フレームの種類]を選択します。「フレーム」とはイーサネットフレームを指し、フレームで送信されるデータは、使用可能なプロトコルによって指定されます。フレームの種類として「その他」を選択する場合は、フレーム番号を指定する必要があります。

6. 注意: [IP]は、IPv4とIPv6両方をサポートしています。[IPv4]または[IPv6]を個別に選択することもできます。

   注意: Solarisでは、Deep Security AgentはIPフレームタイプのパケットのみを検査し、Linuxエージェントは IPタイプまたはARPフレームタイプのパケットのみを調べます。その他のフレームの種類のパケットは許可されます。Virtual Applianceにはこのような制限事項はありません。保護する仮想マシンのOSに関係なく、すべてのフレームの種類を確認できます。

フレームの種類としてインターネットプロトコル (IP) を選択した場合は、トランスポートの [プロトコル] を選択する必要があります。プロトコルとして「その他」を選択する場合は、プロトコル番号も指定する必要があります。

パケットの送信元と送信先を選択する

[IP] アドレスと[MAC] アドレスの組み合わせを選択し、フレームの種類で使用できる場合は、パケット送信元およびパケット送信先の [ポート] および [指定フラグ] を選択します。

ヒント: 以前に作成したIP、MAC、またはポートリストを使用できます。

サポートされているIPベースのフレームの種類は次のとおりです。

	IP	MAC	ポート	フラグ
任意	✓	✓		
ICMP	✓	✓		✓
ICMPV6	✓	✓		✓
IGMP	✓	✓		
GGP	✓	✓		
TCP	✓	✓	✓	✓
PUP	✓	✓		
UDP	✓	✓	✓	
IDP	✓	✓		
ND	✓	✓		
RAW	✓	✓		
TCP+UDP	✓	✓	✓	✓

注意: ARPおよびREVARPのフレームの種類では、パケットの送信元と送信先としてMACアドレスの使用のみがサポートされています。

[任意のフラグ] を選択することも、以下のフラグを個別に選択することもできます。

- URG
- ACK
- PSH
- RST
- SYN
- FIN

ルールイベントとアラートを設定する

ファイアウォールルールがトリガされると、Deep Security Managerにイベントが記録され、パケットデータが記録されます。

> 注意:「許可」、「強制的に許可」、および「バイパス」処理を使用するルールは、イベントのログを記録しません。

アラート

イベントのログを記録した場合に、アラートもトリガするようにルールを設定できます。アラートを設定するには、ルールのプロパティを開き、[オプション] をクリックしてから、[このルールによってイベントが記録された場合にアラート] を選択します。

> 注意: アラートをトリガするように設定できるのは、処理が [拒否] または [ログ記録のみ] に設定されているファイアウォールルールのみです

ルールのスケジュールを設定する

予約された時間のみファイアウォールルールを有効化するかどうかを選択します。

その方法の詳細については、"ルールに適用するスケジュールの定義" on page 820を参照してください。

ルールにコンテキストを割り当てる

ルールコンテキストを使用すると、さまざまなネットワーク環境に独自のファイアウォールルールを設定できます。コンテキストは一般的に、オンサイトとオフサイトのノートパソコンで異なるルールを有効にするために使用されます。

コンテキストの作成方法については、"ポリシーで使用するコンテキストの定義" on page 814を参照してください。

ヒント: コンテキストを使用してファイアウォールルールを実装するポリシーの例については、「Windows Mobile ラップトップ」ポリシーのプロパティを参照してください。

ルールが割り当てられているポリシーとコンピュータを確認する

ファイアウォールルールに割り当てられているポリシーとコンピュータは、[割り当て対象] タブで確認できます。リスト内のポリシーまたはコンピュータをクリックすると、そのプロパティが表示されます。

ルールをエクスポートする

すべてのファイアウォールルールを、.csv または .xml ファイルにエクスポートするには、[エクスポート] をクリックし、リストから対応するエクスポート処理を選択します。特定のルールを選択し、[エクスポート] をクリックして、リストから該当するエクスポート処理を選択すると、特定のルールをエクスポートすることもできます。

ルールを削除する

ルールを削除するには、[ファイアウォールルール] リストで該当のルールを右クリックしてから、[削除]→[OK] の順にクリックします。

注意: 1台以上のコンピュータに割り当てられたファイアウォールルール、またはポリシーの一部であるファイアウォールルールは削除できません。

信頼済みトラフィックに対するファイアウォールのバイパス許可

Deep Security を設定して、信頼されたトラフィックがファイアウォールをバイパスできるようにすることができます。

この設定の基本手順は次のとおりです。

1. "信頼済みトラフィックのソースの新しいIPリストを作成する" on the next page
2. "IPリストを使用して信頼済みトラフィックの受信用と送信用のファイアウォールルールを作成する" on the next page
3. "信頼済みトラフィックが通過するコンピュータで使用されているポリシーにファイアウォールルールを割り当てる" on the next page

ファイアウォールルールがポリシーに割り当てられると、Deep Security は IP リスト内の信頼された送信元からのトラフィックを許可し、ステートフルな問題または脆弱性についてトラフィックを検索しません。

信頼済みトラフィックのソースの新しいIPリストを作成する

1. [ポリシー] をクリックします。
2. 左側の画面で [リスト]→[IPリスト] の順にクリックします。
3. [新規]→[新規IPリスト] の順にクリックします。
4. IPリストの名前を入力します。
5. 信頼済みソースのIPアドレスを、1行に1つずつ [IP] ボックスに貼り付けます。
6. [OK] をクリックします。

IPリストを使用して信頼済みトラフィックの受信用と送信用のファイアウォールルールを作成する

1. [ポリシー] をクリックします。
2. 左側の画面で [ルール] をクリックします。
3. [ファイアウォールルール]→[新規]→[新規ファイアウォールルール] の順にクリックします。
4. 次の値を使用して、信頼済みトラフィックの受信用のファイアウォールルールを作成します。

名前:	信頼済みトラフィック名 - 受信方向のバイパス
処理:	バイパス
プロトコル:	任意
パケット送信元:	IPリスト(前の手順で作成したIPリストを選択)

5. 次の値を使用して、信頼済みトラフィックの送信用のファイアウォールルールを作成します。

名前:	信頼済みトラフィック名 - 送信方向のバイパス
処理:	バイパス
プロトコル:	任意
パケット送信先:	IPリスト(前の手順で作成したIPリストを選択)

信頼済みトラフィックが通過するコンピュータで使用されているポリシーにファイアウォールルールを割り当てる

1. [ポリシー] をクリックします。
2. 左側の画面で [ポリシー] をクリックします。
3. ポリシーをダブルクリックしてプロパティ画面を開きます。
4. ポリシーのプロパティの左側の画面で [ファイアウォール] をクリックします。
5. [割り当て/割り当て解除] をクリックします。
6. 左上のリストにすべてのファイアウォールルールが表示されていることを確認します。
7. 検索ウィンドウを使用し、作成したルールを探して選択します。
8. [OK] をクリックします。
9. 信頼済みトラフィックが通過する各コンピュータについて上記の手順を繰り返します。

ファイアウォールルールの処理と優先度

このトピックの内容:

- "ファイアウォールルールの処理" below
- "ファイアウォールルールのシーケンス" on page 977
- "各ファイアウォールルールの関係" on page 979
- "ルール優先度" on page 981
- "ルール処理およびルール優先度を集約する" on page 981

ファイアウォールルールの処理

ファイアウォールルールでは、次の処理が可能です。

- 許可: ルールと一致するトラフィックの通過を明示的に許可し、その他のトラフィックは黙示的に拒否します。
- バイパス: ファイアウォールと侵入防御分析の両方のバイパスをトラフィックに許可します。この設定は、ネットワーク負荷の高いプロトコルや信頼済みソースからのトラフィックに対して使用します。バイパスルールは、IP、ポート、トラフィックの方向、プロトコルに基づいて設定できます。
- 拒否: ルールと一致するトラフィックを明示的にブロックします。
- 強制的に許可: 他のルールで拒否されるトラフィックを強制的に許可します。

  注意: 強制的に許可ルールで許可されるトラフィックは、侵入防御モジュールによる分析の対象となります。

- ログ記録のみ: トラフィックはログに記録されるだけです。その他の処理は実行されません。

許可ルールの詳細

許可ルールには、次の2つの機能があります。

1. 明示的に許可されているトラフィックを許可
2. その他のトラフィックを黙示的に拒否

注意: 許可ルールで明示的に許可されていないトラフィックは破棄され、「ポリシーで未許可」のファイアウォールイベントとして記録されます。

一般的に適用される許可ルールは、次のとおりです。

- ARP:受信ARPトラフィックを許可します。
- Allow solicited TCP/UDP replies:コンピュータが、送信したTCPやUDPのメッセージへの応答を受信できるようにします。これは、TCPとUDPのステートフル設定と連携します。
- Allow solicited ICMP replies:コンピュータが、送信したICMPメッセージへの応答を受信できるようにします。これは、ICMPのステートフル設定と連携します。

バイパスルールの詳細

バイパスルールは、ネットワーク負荷の高いプロトコルや信頼済みソースからのトラフィック対象に設計されています。ファイアウォールや侵入防御モジュールによるフィルタリングが必要とされず、望まれてもいないためです。

バイパスルールの条件と一致するパケットは、次のように処理されます。

- ステートフル設定の条件の対象にならない。
- ファイアウォールと侵入防御分析の両方をバイパスする。

バイパスされるトラフィックにはステートフルインスペクションが適用されないので、一方向のトラフィックがバイパスされても、逆方向の応答は自動的にはバイパスされません。受信トラフィック用と送信トラフィック用のバイパスルールは、必ずペアで作成および適用する必要があります。

注意:バイパスルールのイベントは記録されません。この動作は変更できません。

ヒント:Deep Security ManagerがDeep Security Agentで保護されているリモートデータベースを使用している場合、Deep Security Managerが侵入防御ルールをデータベースに保存すると、侵入防御に関連する誤ったアラームが発生することがあります。これは、ルール自体の内容が誤って攻撃と認識されることが原因です。このための回避策の1つは、Deep Security Managerからデータベースへのトラフィックのバイパスルールを作成することです。

Deep Security Managerのトラフィックに関するバイパスルールの初期設定

Deep Security Managerは、優先度4のバイパスルールを自動的に実装します。このルールは、Deep Security Agentが実行されているコンピュータ上で、ハートビート(ハートビートの設定には "ハートビートを設定する" on page 1499 の受信者のTCP待機トラフィックを開きます。このルールは優先度4なので、他の拒否ルールよりも先に適用されます。また、バイパスルールなので、トラフィックの障害が発生することはありません。なお、このバイパスルールは内部的に作成されるため、ファイアウォールルールの一覧には明示的に表示されません。

ただし、このルールでは、任意のIPアドレスと任意のMACアドレスからのトラフィックが許可されます。このポートでのAgentのセキュリティを強化するには、このポート用に、より厳しいバイパスルールを作成します。エージェントは、次の特性を備えている場合は、新しいカスタムルールを優先して、初期設定のDeep Security Managerトラフィックルールを実際に無効にします。

- 優先度:4 (最高)
- パケット方向: 受信
- フレームの種類: IP
- プロトコル: TCP
- パケット送信先ポート: Managerからのハートビートを待機するAgentのポート番号

初期設定のルールをカスタムルールに置き換えるには、カスタムルールに上記のパラメータが必要です。理想的には、実際のDeep Security ManagerのIPアドレスまたはMACアドレスをルールのパケット送信元として使用する必要があります。

強制的に許可ルールの詳細

強制的に許可オプションでは、拒否処理の対象となるトラフィックの一部を除外します。他の処理との関係を下に示します。強制的に許可ルールは、バイパスルールと同じ効果があります。ただし、バイパスルールとは異なり、この処理によってファイアウォールを通過するトラフィックは侵入防御モジュールによる監視の対象となります。強制的に許可ルールの処理は、基本的なネットワークサービスがDSAコンピュータとの通信を確保するのに便利です。一般に、強制的に許可ルールは、許可ルールと一緒に使用して、許可および拒否ルールで禁止されているトラフィックの一部を許可します。また、ICMPおよびUDPステートフルが有効になっている際に、未承諾のICMPおよびUDPトラフィックを許可するように強制的に許可ルールを設定する必要があります。

注意: マルチノード配置で複数のDeep Security Managerを使用する場合は、これらのサーバのIPリストを定義してから、そのリストを使用してDeep Security Managerのカスタムトラフィックルールを作成すると便利です。

ファイアウォールルールのシーケンス

コンピュータに届くパケットは、ファイアウォールルール、ファイアウォールステートフル設定条件、および侵入防御ルールの順に処理されます。

受信および送信でファイアウォールルールが適用される順序は次のとおりです。

1. 優先度4 (最高) のファイアウォールルール
   a. バイパス
   b. ログ記録のみ (ログ記録のみルールは優先度4 (最高) にのみ割り当て可能)

    c. 強制的に許可
    d. 拒否
2. 優先度3 (高) のファイアウォールルール
    a. バイパス
    b. 強制的に許可
    c. 拒否 (ログに記録)
3. 優先度2 (標準) のファイアウォールルール
    a. バイパス
    b. 強制的に許可
    c. 拒否 (ログに記録)
4. 優先度1 (低) のファイアウォールルール
    a. バイパス
    b. 強制的に許可
    c. 拒否 (ログに記録)
5. 優先度0 (最低) のファイアウォールルール
    a. バイパス
    b. 強制的に許可
    c. 拒否 (ログに記録)
    d. 許可 (許可ルールは優先度0 (最低) にのみ割り当て可能)

注意: コンピュータに有効な許可ルールがない場合、拒否ルールでブロックされていないかぎり、すべてのトラフィックが許可されます。許可ルールを1つ作成したら、許可ルールの条件を満たしていないかぎり、その他すべてのトラフィックがブロックされます。ただし、1つだけ例外があります。ICMPv6トラフィックは、拒否ルールで明確にブロックされていないかぎり、常に許可されます。

同じ優先度のコンテキスト内では、拒否ルールが許可ルールをオーバーライドし、強制的に許可ルールが拒否ルールをオーバーライドします。ルールの優先度システムを使用すると、優先度の低い強制的に許可ルールを、優先度の高い拒否ルールでオーバーライドできます。

強制的に許可ルールを使用して受信DNSクエリをすべて許可するDNSサーバ用のポリシーを例に考えてみます。強制的に許可ルールよりも優先度の高い拒否ルールを作成し、この公開サーバへのアクセスを禁止する必要がある特定範囲のIPアドレスを指定します。

優先度に基づいたルール設定によって、ルールを適用する順序を設定できます。拒否ルールに最も高い優先度を設定し、同じ優先度の強制的に許可ルールがない場合、拒否ルールに一致するパケットはすべて自動的に破棄されて残りのルールは無視されます。反対に、強制的に許可ルールに最も高い優先度が設定されている場合、強制的に許可ルールに一致する受信パケットは他のルールに対して確認されることなくすべて自動的に許可されます。

ログに関する注意

バイパスルールはイベントを生成しません。この設定は変更できません。

ログのみルールは、対象のパケットが、次のいずれかのルールによって、それ以降に停止されない場合にのみイベントを生成します。

- 拒否ルール
- そのパケットを除外する許可ルール

この2つのルールのいずれかがパケットを停止する場合は、ログのみルールではなくこれらのルールによって、イベントが生成されます。以降のルールでパケットを停止しない場合は、ログのみルールがエントリを生成します。

各ファイアウォールルールの関係

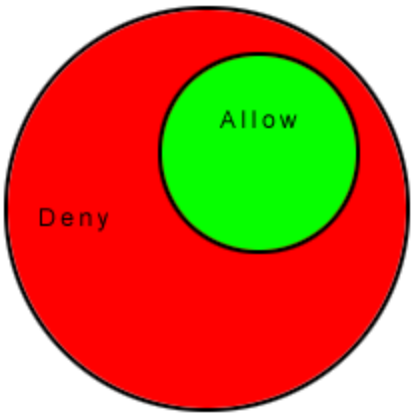
Deep Securityのファイアウォールルールには、ルール処理とルール優先度があります。この2つのプロパティを同時に使用することによって、非常に柔軟で強力なルール設定を作成できます。他のファイアウォールで使用されるルールセットとは異なり、ルールの実行順にルールを定義する必要がある場合もありますが、Deep Security ファイアウォール ルールは、ルール処理とルール優先順位に基づいて決定的な順序で実行されます。それらが定義または割り当てられる順序に依存しません。

ルール処理

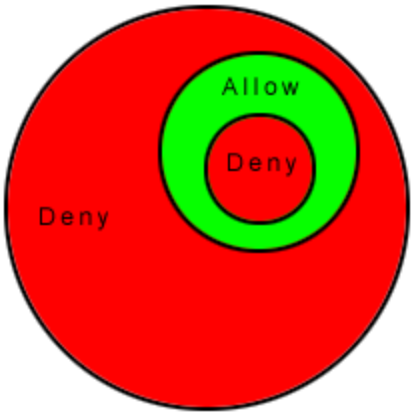
各ルールには、以下の5つのルール処理のいずれかを設定できます。

1. バイパス: パケットがバイパスルールに一致した場合は、同じ優先度の他のルールにかかわらずファイアウォールと侵入防御エンジンを通過します。
2. ログ記録のみ: パケットがログ記録のみルールに一致した場合は、通過してイベントがログ記録されます。
3. 強制的に許可: パケットが強制的に許可ルールに一致した場合は、同じ優先度の他のルールにかかわらず通過します。
4. 拒否: パケットが拒否ルールに一致した場合は、破棄されます。
5. 許可: パケットが許可ルールに一致した場合は、通過します。許可ルールのいずれにも一致していないトラフィックはすべて拒否されます。

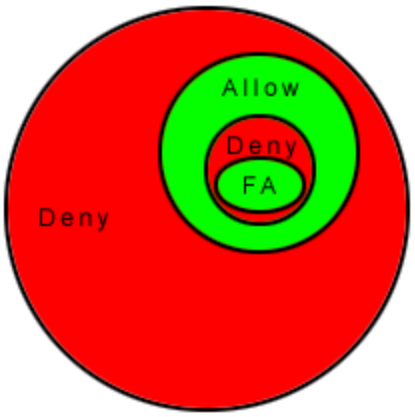
許可ルールを実装すると、許可ルールに一致しないその他すべてのトラフィックが拒否されます。



拒否ルールを許可ルールに優先して適用すると、特定の種類のトラフィックをブロックすることができます。



強制的に許可ルールを拒否トラフィックに適用すると、例外のみ通過させることができます。



ルール優先度

拒否および強制的に許可のルール処理を5つの優先度のいずれかで定義できます。これにより、許可されるトラフィックを許可ルールのセットでさらに細かく定義できます。ルールは、最高 (優先度4) から最低 (優先度0) の順に実行されます。特定の優先度内では、ルール処理 (強制的に許可、拒否、許可、ログのみ) に基づいた順序で処理されます。

優先度のコンテキストによって、ユーザは拒否および強制的に許可の組み合わせを使用してトラフィック管理をさらに詳細に定義することが可能になります。同じ優先度のコンテキスト内では、拒否ルールによって許可ルールを無効にし、また、強制的に許可ルールによって拒否ルールを無効にすることもできます。

> 注意: 許可のルール処理は優先度0でのみ動作し、ログのみのルール処理は優先度4でのみ動作します。

ルール処理およびルール優先度を集約する

ルールは、最高 (優先度4) から最低 (優先度0) の順に実行されます。特定の優先度内では、ルール処理に基づいた順序で処理されます。同じ優先度のルールが処理される順序は次のとおりです。

- バイパス
- ログのみ
- 強制的に許可
- 拒否
- 許可

注意: 許可のルール処理は優先度0でのみ動作し、ログのみのルール処理は優先度4でのみ動作します。

注意: 強制的に許可ルールと拒否ルールが同等の優先度の場合、強制的に許可ルールが拒否ルールよりも優先されるので、強制的に許可ルールと一致するトラフィックが許可されます。

ファイアウォールの設定

[ファイアウォール] モジュールは、双方向のステートフルなファイアウォール保護を提供します。DoS攻撃を阻止し、すべてのIPベースのプロトコルとフレームタイプに対応するほか、ポート、IPアドレス、およびMACアドレスをフィルタリングします。

コンピュータエディタとポリシーエディタ[1]の [ファイアウォール] セクションには、タブで区切られた次のセクションがあります。

- "一般" below
- "インタフェース制限" on the next page
- "攻撃の予兆" on page 984
- "詳細" on page 987
- "ファイアウォールイベント" on page 987

一般

ファイアウォール

ファイアウォールのオン/オフ状態を親ポリシーから継承したり、設定をローカルでロックするようにこのポリシーまたはコンピュータを設定できます。

ファイアウォールステートフル設定

このポリシーに適用するファイアウォールステートフル設定を選択します。上記のポリシーに対して複数のインタフェースを定義した場合は、各インタフェースに対して個別に設定することができます。ステートフル設定作成の詳細については、"ステートフルファイアウォールの設定の定義" on page 993を参照してください。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

ポート検索 (コンピュータエディタのみ)

前回のポート検索 : このコンピュータでDeep Security Managerがポート検索を最後に実行した時刻。

検索されたポート: 直近のポート検索で検索されたポート。

オープンポート: ローカルコンピュータのIPアドレスの下に、オープンポートのリストが表示されます。

[オープンポートの検索] ボタンと[ポート検索のキャンセル] ボタンを使用して、このコンピュータのポート検索を開始またはキャンセルできます。Deep Security Managerは、**コンピュータまたはポリシーエディタ**[1] > [設定]> [一般]> [ポートを開く]> [を検索するポート]で定義された範囲のポートを検索します。

注意: 検索対象のポートに関係なく、Deep Security Managerは常に検索を実行します。Managerからのハートビート接続のエージェントまたはアプライアンスの待機ポート番号。

割り当てられたファイアウォールルール

このポリシーまたはコンピュータで有効になっているファイアウォールルールを表示します。ファイアウォールルールを追加または削除するには、[割り当て/割り当て解除] をクリックします。使用可能なすべてのファイアウォールルールが表示され、ルールを選択したり選択を解除したりできます。

コンピュータエディタまたはポリシーエディタ[2]画面では、ファイアウォールルールを編集して、編集中のルールにのみローカルに適用することも、そのルールを使用しているすべての他のポリシーおよびコンピュータに変更内容をグローバルに適用することもできます。

ルールをローカルに編集するには、ルールを右クリックして [プロパティ] をクリックします。

ルールをグローバルに編集するには、ルールを右クリックして [プロパティ(グローバル)] をクリックします。

ファイアウォールルール作成については、"ファイアウォールルールの作成" on page 967を参照してください。

インタフェース制限

---

1 これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

2 これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

インタフェース制限

インタフェース制限の有効/無効状態を親ポリシーから継承したり、設定をローカルでロックするようにこのポリシーまたはコンピュータを設定できます。

警告: インタフェース制限を有効にする前に、インタフェースパターンを適切な順序で設定し、必要な文字列パターンをすべて追加し、不要なパターンは削除してください。優先度が最も高いパターンのインタフェースのみが、トラフィックの転送を許可されます。それ以外のインタフェース(リスト内にある残りのパターンのいずれかと一致するインタフェース)は、「制限」されます。制限されたインタフェースは、ファイアウォールの [許可] ルールを使用して特定のトラフィックを許可しないかぎり、すべてのトラフィックをブロックします。

インタフェース制限 ポリシーを設定するには

1. [インタフェース制限] タブで、インタフェース制限の有効化を選択します。
2. インタフェースパターンを設定します。(下記参照)
3. [保存] をクリックします。

インタフェースパターン

インタフェース制限が有効な場合、ファイアウォールでは、ローカルコンピュータのインタフェース名が、正規表現パターンと照合されます。

注意: Deep Securityは、POSIX基本正規表現を使用してインタフェース名を照合します。基本的なPOSIX正規表現の詳細については、https://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap09.html#tag_09_03を参照してください。

優先度が最も高いパターンのインタフェースのみが、トラフィックの転送を許可されます。それ以外のインタフェース(リスト内にある残りのパターンのいずれかと一致するインタフェース)は、「制限」されます。制限されたインタフェースは、ファイアウォールの [許可] ルールを使用して特定のトラフィックを許可しないかぎり、すべてのトラフィックをブロックします。

[1つのアクティブインタフェースに制限] を選択すると、優先度が最も高いパターンのインタフェースが複数見つかった場合でも、1つのインタフェースからのトラフィックのみ許可されます。

攻撃の予兆

攻撃の予兆検索

[攻撃の予兆] 画面では、コンピュータのトラフィック分析を有効にして設定することができます。この機能により、標的型攻撃の前段階として脆弱性を見つけるために使用されることの多い「予兆」を特検出することができます。

注意: 攻撃の予兆検索は、TAPモードでは機能しません。攻撃の予兆検索は、IPv4トラフィックでしか検出できません。

偵察の保護を有効にするには、**コンピュータエディタまたはポリシーエディタ**[1] → [ファイアウォール] → [一般] タブで、ファイアウォールおよびステートフルインスペクションも有効にする必要があります。また、**コンピュータエディタまたはポリシーエディタ**[2] → [ファイアウォール] → [詳細] タブで、[「ポリシーの許可外」のパケットのファイアウォールイベントを生成] 設定も有効にする必要があります。これにより、攻撃の予兆に必要なファイアウォールイベントが生成されるようになります。

攻撃の予兆を設定する場合、次のオプションがあります。

- 攻撃の予兆の検出の有効化: 攻撃の予兆の検出のオン/オフを切り替えできます。初期設定では、すべての検索が通知付きのレポートモードで有効になっています。通知をオフにするか、レポートをさらに一時的なブロックモードに切り替える場合は、ドロップリストからはいを選択して、変更を加えます。
- 検出を実行するコンピュータ/ネットワーク: 保護するIPをリストから選択します。既存のIPリストから選択します(このIPリストは、[ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト] 画面を使用して作成できます)。
- 検出を実行しないIPリスト: 無視するコンピュータとネットワークをIPリストセットから選択します(上で述べたように、このIPリストは、[ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト] 画面を使用して作成できます)。

攻撃の種類ごとに、エージェントまたはアプライアンスに対して、アラートが実行されるDeep Security Managerに情報を送信するように指示することができます。アラートが発生したときに通知を送信するようDeep Security Managerを設定できます。詳細については、[管理]→[システム設定]→[アラート]を参照してください。このオプションには [DSMにただちに通知] を選択してください。

---

1 これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。

2 これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。

注意: [DSMにただちに通知] オプションを動作させるには、AgentおよびApplianceの通信方法を[Agent/Applianceから開始] または [双方向] に設定する必要があります (**コンピュータエディタまたはポリシーエディタ**[1]の [設定]→[一般])。有効にすると、エージェントまたはアプライアンスは攻撃またはプローブの検出時にただちにDeep Security Managerに対するハートビートを開始します。

攻撃が検出されると、一時的に送信元IPからのトラフィックをAgentおよびApplianceでブロックするように設定できます。[トラフィックのブロック]ドロップダウンリストを使用して分数を設定します。

アラートは次のとおりです。

- OSのフィンガープリント調査: AgentまたはApplianceは、コンピュータOSを検出しようとする動作を検出します。
- ネットワークまたはポートの検索: AgentまたはApplianceは、リモートIPがポートに対して異常な割合のIPでアクセスしていることを検出した場合、ネットワークまたはポート検索をレポートします。通常、AgentまたはApplianceのコンピュータは、コンピュータ自身宛てのトラフィックのみを監視するため、ポート検索が最も一般的に検出されます。コンピュータまたはポート検索の検出で使用される統計的な分析方法は「TAPS」アルゴリズムから導出されたもので、2006年にIPCCCで発表された「Connectionless Port Scan Detection on the Backbone」で提案されました。
- TCP Null検索: AgentまたはApplianceはフラグが付いていないパッケージを検出します。
- TCP SYNFIN検索: AgentまたはApplianceはSYNフラグおよびFINフラグの付いたパケットのみ検出します。
- TCP Xmas検索: AgentまたはApplianceは、FINフラグ、URGフラグ、およびPSHフラグの付いたパケット、または値0xFF (想定されるすべてのフラグ) を含むパケットを検出します。

注意: それは、単一のパケットによって認識され、一定の期間のトラフィックを監視するのDeep Securityを必要とすることができないという点で、偵察の他の種類の「ネットワークまたはポートスキャン」異なります。
AgentまたはApplianceは、リモートIPがポートに対して異常な割合のIPでアクセスしていることを検出した場合、コンピュータまたはポート検索をレポートします。ポートスキャンがはるかに検出されたプローブの最も一般的なタイプですので、通常はエージェントまたはアプライアンスのコンピュータは、自身宛てのトラフィックが表示されます。ただし、コンピュータがルータまたはブリッジとして動作している場合は、多数の他のコンピュータ宛てのトラフィックを監視して、AgentまたはApplianceがコンピュータ

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

検索 (サブネット全体でポート80が開いているコンピュータを検索するなど) を検出できます。
こうした検索を検出するには数分かかります。これは、AgentまたはApplianceが接続の失敗を追跡して、比較的短い期間に単一のコンピュータからの異常な数の接続の失敗があることを確認する必要があるためです。

注意: ブラウザアプリケーションを使用してWindowsコンピュータで実行されているDeep Security Agentは、閉じられた接続から到着するトラフィックが残っているため、偽陽性の偵察検索を報告することがあります。

攻撃の予兆警告に対応する方法の詳細については、"警告: 攻撃の予兆の検出" on page 1453を参照してください。

詳細

イベント

「ポリシーで未許可」のパケットに対して、イベントを生成するかどうかを設定します。これらは、[許可] ファイアウォールルールで明確に許可されていないため、ブロックされているパケットです。このオプションを[はい] に設定すると、有効なファイアウォールルールに応じて、大量のイベントが生成される場合があります。

ファイアウォールイベント

ファイアウォール イベントは、このポリシーまたは特定のコンピュータに関連するイベントのみが表示される点を除き、Deep Security Managerのメイン画面と同じ方法で表示されます。

Oracle RACでのファイアウォール設定

Deep Securityは、Oracle RACをサポートしています。Oracle RACのサポート対象バージョンのリストについては、"ソフトウェア要件" on page 453を参照してください。

初期設定のLinux Server Deep Securityポリシーは Oracle RAC環境に対応していますが、ファイアウォールの設定だけは例外です。RACノード間の通信チャネルが複雑であるため、ファイアウォールが原因でRACノードが仮想NICの作成やNICの検索に失敗することがあります。このため、一部のノードでOracle Clusterwareが起動しなくなります。ファイアウォールを無効にするか、ファイアウォールの設定をカスタマイズすることができます。

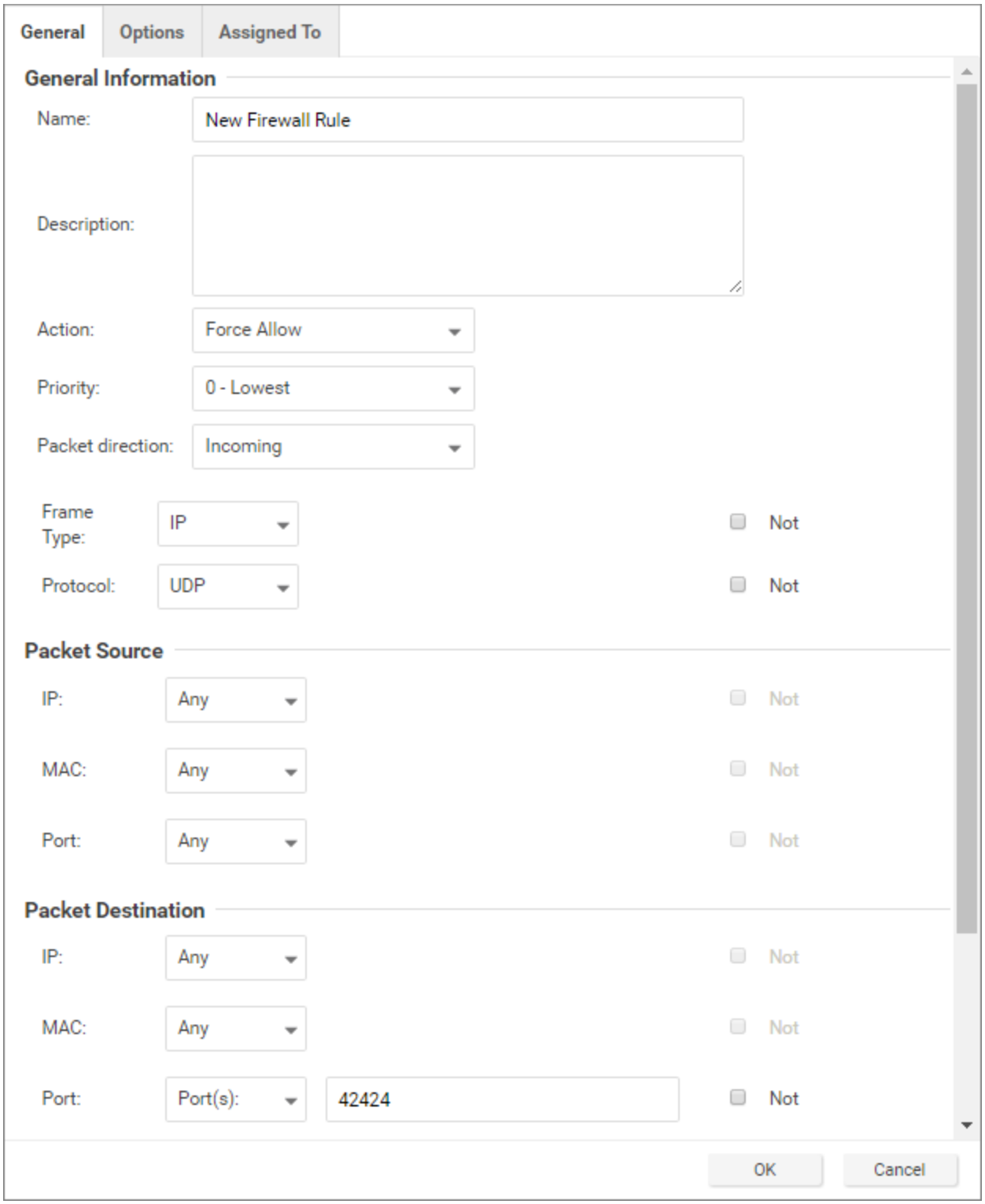
ノード間の接続を許可するルールを追加する

1. Deep Security Managerで、[ポリシー] タブに進みます。
2. [Linux Server] ポリシーを右クリックし、[複製] をクリックします。
3. 新しく作成された[Linux Server_2] ポリシーをクリックし、[詳細] をクリックします。
4. このポリシーに新しい名前 (「Oracle RAC」など) を付け、[保存] をクリックします。
5. [ファイアウォール] をクリックします。
6. [割り当て/割り当て解除] をクリックします。
7. [新規]→[新規ファイアウォールルール] の順にクリックします。
8. [一般情報] で、[名前] に「Oracleノードとの通信を許可」などのわかりやすい名前を指定します。[処理] を「強制的に許可」に設定し、[プロトコル] を「任意」に設定します。
9. [パケット送信元] で、[MAC] を「MACリスト」に設定します。表示された[MACリストの選択] 画面で、[新規] を選択します。[新規MACリストのプロパティ] ダイアログボックスが表示されます。
10. MACリストに「Oracle RAC MACリスト」などの名前を付けます。[MAC: (1行あたり1つのMAC)] に、すべてのOracleノードが使用しているすべてのMACアドレスを追加します (プライベートNICとパブリックNIC両方のMACを含む)。追加したら[OK] をクリックします。
11. [パケット送信先] で、[MAC] を「MACリスト」に設定します。表示された[MACリストの選択] 画面で、手順10で作成したMACリストを選択し、[OK] をクリックします。
12. ポリシーの [ファイアウォールルール] リストで、新しいルールが選択されていることを確認して [OK] をクリックし、[保存] をクリックします。

UDPポート42424を許可するルールを追加する

上記の手順に従って、UDPポート42424を許可する新しいルールを追加します。このポート番号は、Cluster Synchronization Serviceデーモン (CSSD)、Oracle Grid Interprocess Communicationデーモン (GIPCD)、およびOracle HA Servicesデーモン (OHASD) で使用されます。

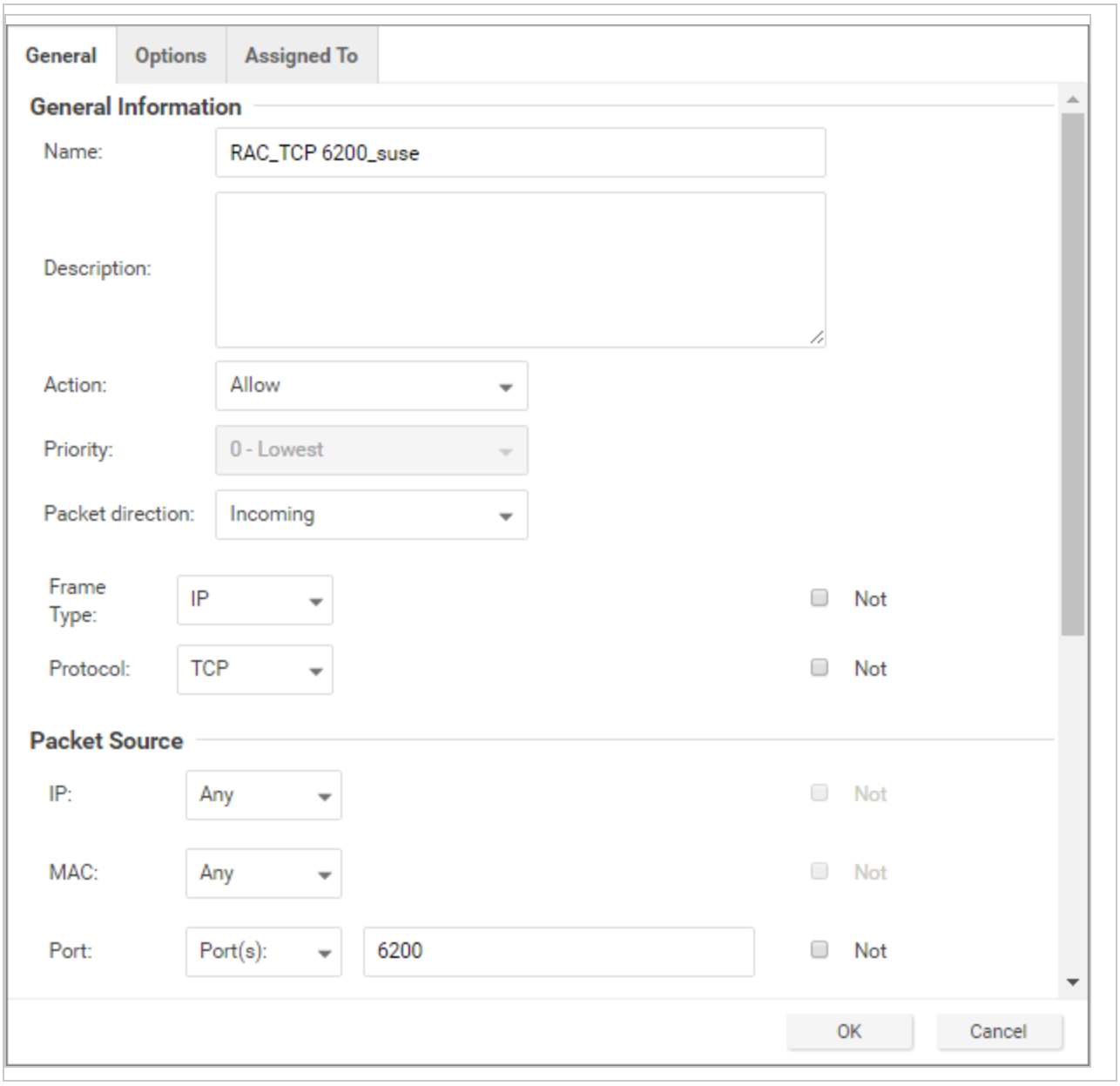
注意: 上記の手順で作成したMACリストでは、このルールに対応できない可能性があります。Oracle RACにはこのルールが必要です。


General
Options
Assigned To
General Information
Name:
New Firewall Rule
Description:
Action:
Force Allow
Priority:
0 - Lowest
Packet direction:
Incoming
Frame Type:
IP
Not
Protocol:
UDP
Not
Packet Source
IP:
Any
Not
MAC:
Any
Not
Port:
Any
Not
Packet Destination
IP:
Any
Not
MAC:
Any
Not
Port:
Port(s):
42424
Not
OK
Cancel

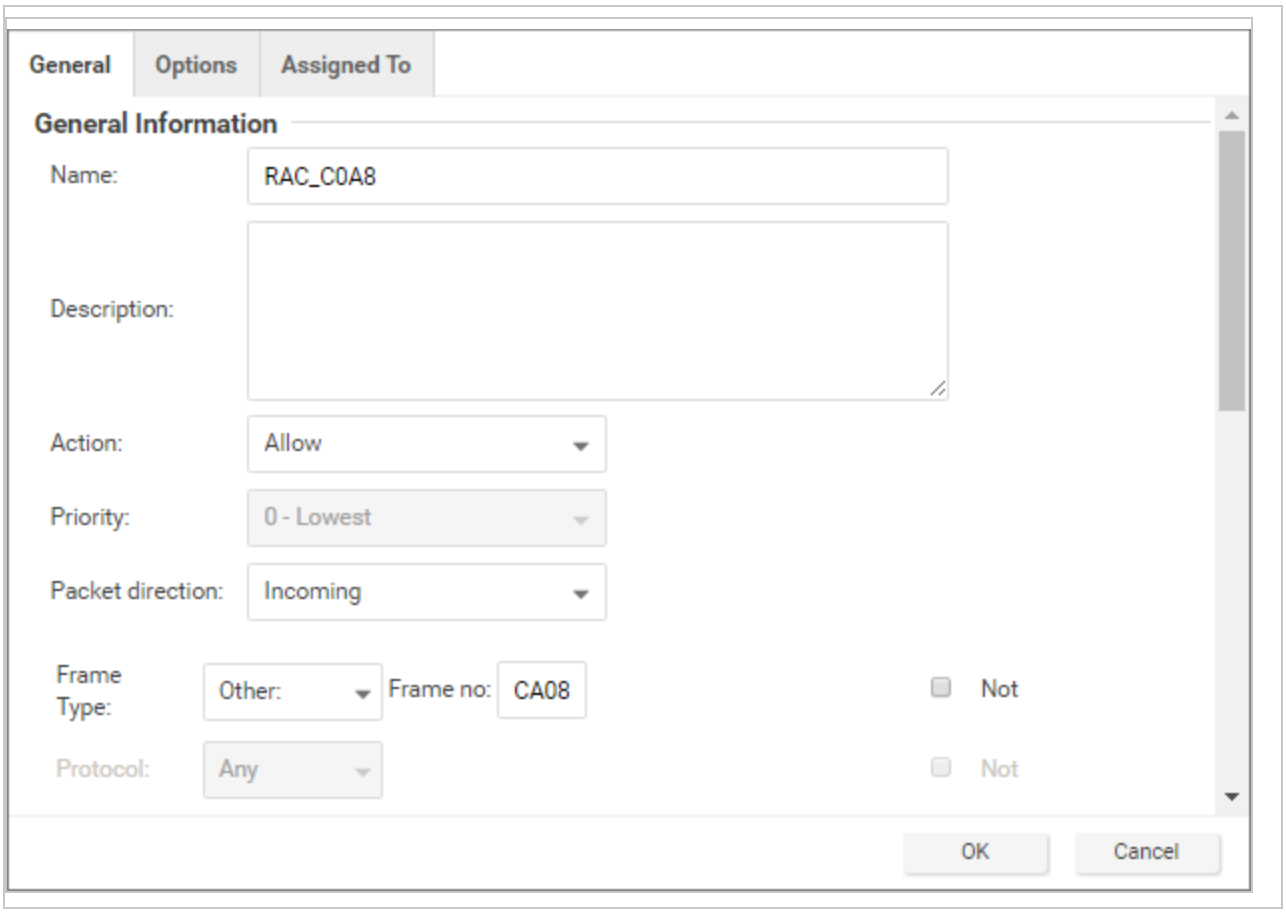
その他のRAC関連パケットを許可する

Oracle RACは、フレームの種類がC08Aおよび0ACBのパケットを大量に送信します。これらのパケットをブロックすると、予期しない動作が発生する可能性があります。

- TCPポート6200を許可する: [パケット送信元] および [パケット送信先] の [IP] フィールドにRACノードのパブリックIPアドレスを追加し、送信先ポートを6200に設定します。このポート番号は、Oracle Notification Services (ONS) で使用されます。このポートは設定可能です。システムで6200以外のポートに設定されている場合は、正しいポート番号を設定してください。

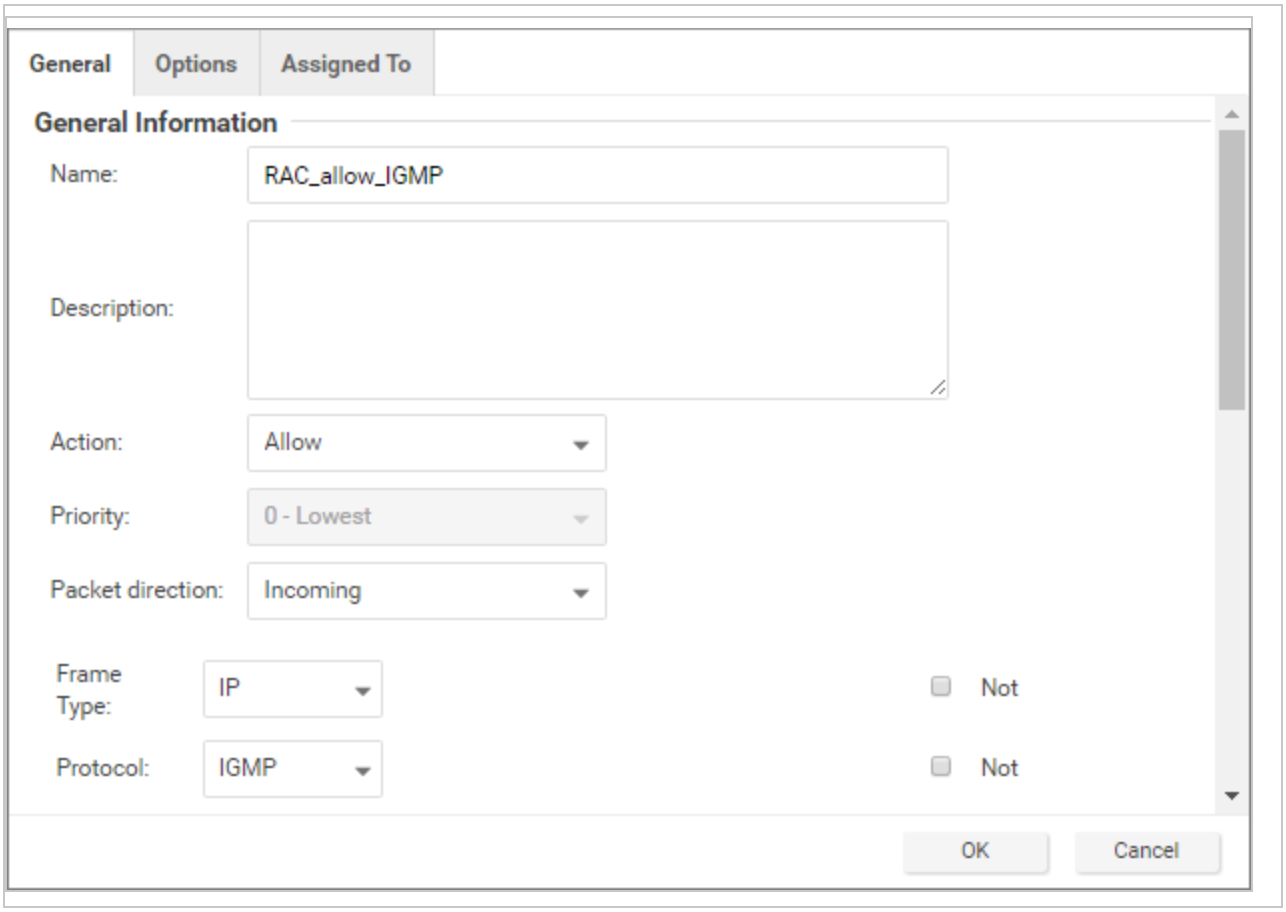


- フレームの種類C0A8を許可する: [フレームの種類] を「その他」、[フレーム番号] を「C0A8」に設定したルールを追加します。



- フレームの種類0ACBを許可する: [フレームの種類] を「その他」、[フレーム番号] を「0ACB」に設定したルールを追加します。
- フレームの種類0AC9を許可する: [フレームの種類] を「その他」、[フレーム番号] を「0AC9」に設定したルールを追加します。

- IGMPプロトコルを許可する: [プロトコル] を「IGMP」に設定したルールを追加します。



特定のポートを許可するファイアウォールルールを追加する必要があるRAC関連コンポーネントがシステムに含まれているかどうかは、次のリンクで確認してください。

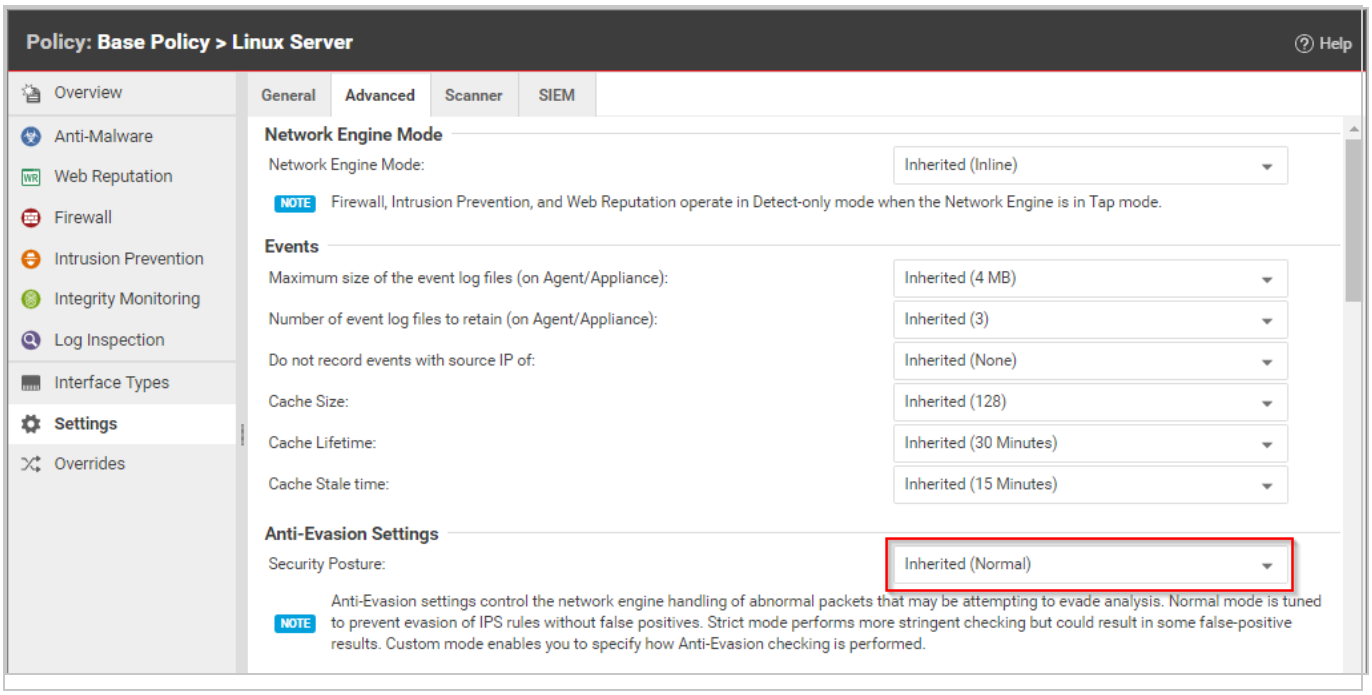
https://docs.oracle.com/database/121/RILIN/ports.htm#RILIN1178

Oracle SQL Serverルールが割り当てられていることを確認する

Linux Serverポリシーに「Oracle SQL Server」ファイアウォールルールが割り当てられていることを確認します。このルールは、Deep Securityで事前に定義されている、ポート1521を許可するファイアウォールルールです。

回避技術対策の設定が「標準」に設定されていることを確認する

Linux Serverポリシーのプロパティでは、[設定]→[ネットワークエンジン]→[回避技術対策の設定] は初期設定で「標準」に設定されています。この設定が「厳格」に設定されていると、RACデータベースの応答が非常に遅くなります。



ステートフルファイアウォールの設定の定義

Deep Securityのステートフルなファイアウォール設定メカニズムは、トラフィック履歴、TCPおよびIPヘッダ値の正確さ、およびTCP接続状態の遷移のコンテキストで各パケットを分析します。UDPやICMPなどのステートレスプロトコルの場合、履歴トラフィック分析に基づいた擬似ステートフルメカニズムが実装されます。パケットは、ステートフルメカニズムによって次のように処理されます。

1. 静的ファイアウォールルール条件によってパケットの通過が許可された場合、パケットはステートフルルーチンに渡されます。
2. パケットを調べて、既存の接続に属しているかどうかが判断されます。
3. TCPヘッダの正当性 (シーケンス番号、フラグの組み合わせなど) が調査されます。

新しいステートフル設定を作成するには、次の手順に従います。

1. "ステートフル設定を追加する" on the next page
2. "ステートフル設定情報を入力する" on the next page。
3. "パケットインスペクションオプションを選択する" on the next page。

ステートフル設定の後は、次の操作について説明します。

- "ステートフル設定が割り当てられたポリシーとコンピュータを表示する" on page 998
- "ステートフル設定をエクスポートする" on page 998
- "ステートフル設定を削除する" on page 998

ステートフル設定を追加する

[ポリシー]→[共通オブジェクト]→[その他]→[ファイアウォールステートフル設定] でステートフル設定を定義する方法には次の3つがあります。

- 新しい設定を作成します。[新規]→[新規ファイアウォールステートフル設定] の順にクリックします。
- XMLファイルから設定をインポートします。[新規]→[ファイルからインポート] をクリックします。
- 既存の設定をコピーして変更します。[ファイアウォールステートフル設定] リストの設定を右クリックして、[複製] をクリックします。新しい設定を編集するには、その設定を選択し、[プロパティ] をクリックします。

ステートフル設定情報を入力する

設定の [名前] と[説明] を入力します。

パケットインスペクションオプションを選択する

IP、TCP、UDPおよびICMPパケットインスペクションのオプションを定義し、アクティブまたはパッシブFTPを有効化できます。

IPパケットインスペクション

[一般] タブで [フラグメント化されたすべての受信パケットを拒否する] を選択し、フラグメント化されたパケットをすべて破棄します。破棄されたパケットはフラグメント化分析をバイパスして、「IP fragmented packet」というログエントリが生成されます。全長がIPヘッダの長さよりも短いパケットはログに記録されずに破棄されます。

警告: 攻撃者は、ファイアウォールルールをバイパスするために、フラグメント化されたパケットを作成して送信する場合があります。

注意: 初期設定では、ファイアウォールエンジンは、フラグメント化されたパケットに対して一連のチェックを実行します。これは初期設定の動作で、変更することはできません。次のような特徴を持つパケットは、破棄されます。

- フラグメントのフラグ/オフセットが無効: IPヘッダ内のDFフラグまたはMFフラグのいずれかが1に設定されている、またはヘッダ内に含まれるDFフラグが1に設定されており、オフセット値が0以外に設定されているとき、パケットは破棄されます。

- 最初のフラグメントが最小サイズ未満: MFフラグが1に設定されていて、オフセット値が0、合計の長さが(最大組み合わせヘッダ長である)120バイトよりも短い場合、パケットは破棄されます。
- IPフラグメントが範囲を超えている: 合計パケット長と組み合わされたオフセットフラグの値が最大データグラム長である65,535バイトを超えた場合、パケットは破棄されます。
- IPフラグメントのオフセットが小さすぎる: 60バイトよりも小さい値を持つ0以外のオフセットフラグがある場合、パケットは破棄されます。

TCPパケットインスペクション

[TCP] タブで有効化するオプションを次の中から選択します。

- CWR、ECEフラグを含むTCPパケットを拒否する: これらのフラグは、ネットワーク輻輳時に設定されます。

  注意: RFC 3168では、ECN (Explicit Congestion Notification) に使用する予約済みフィールドの6ビットのうち2ビットを、次のように定義しています。
  - ビット8から15: CWR-ECE-URG-ACK-PSH-RST-SYN-FIN
  - TCPヘッダフラグのビット名参照:
    - ビット8: CWR (Congestion Window Reduced) [RFC3168]
    - ビット9: ECE (ECN-Echo) [RFC3168]

  警告: パケットの自動転送 (特にDoS攻撃によって生成されたものなど) によって、これらのフラグが設定されたパケットが作成されることがよくあります。

- TCPステートフルインスペクションを有効にする: TCPレベルでのステートフルインスペクションを有効にします。ステートフルTCPインスペクションを有効にすると、次のオプションが利用可能です。
  - TCPステートフルログを有効にする: TCPステートフルインスペクションイベントがログに記録されます。
  - 単一コンピュータからの受信接続数の上限: 単一コンピュータからの接続数を制限すると、DoS攻撃の影響を低減できます。
  - 単一コンピュータへの送信接続数の上限: 単一コンピュータへの送信接続数を制限すると、Nimdaなどのワームの影響を大幅に低減できます。
  - 単一コンピュータからのハーフオープン接続数の上限: この制限を設定すると、SYNフラッドなどのDoS攻撃から保護できます。ほとんどのサーバでは、ハーフオープン接続を終了する

ためにタイムアウトが設定されています。この値を設定することにより、ハーフオープン接続が重大な問題にならないようにします。SYN-SENT (リモート) エントリが指定された制限に達した場合、その特定のコンピュータからの後続のTCPパケットは破棄されます。

注意: 単一コンピュータからのオープン接続を許可する数を決定する際に、使用している種類のプロトコルで妥当と考えられる単一コンピュータからのハーフオープン接続数と、輻輳を引き起こすことなくシステムが維持できる単一コンピュータからのハーフオープン接続数との間の数を選択します。

- すでに確認されたパケット数が次を超過したときにACKストーム防御を有効にする: このオプションを設定して、ACKストーム攻撃が発生した場合のイベントを記録します。
  - ACKストームが検出されたときに接続を中断する: このオプションを設定して、攻撃が検出された場合に接続を切断するようにします。

注意: ACKストーム保護オプションはDeep Security Agent 8.0以前でのみ使用可能です。

FTPオプション

[FTPオプション] タブで次のオプションを有効化できます。

注意: 以下のFTPオプションはDeep Security Agent 8.0以前で使用可能です。

- アクティブFTP
  - 受信を許可する: このコンピュータがサーバとして動作しているときにアクティブFTPを許可します。
  - 送信を許可する: このコンピュータがクライアントとして動作しているときにアクティブFTPを許可します。
- パッシブFTP
  - 受信を許可する: このコンピュータがサーバとして動作しているときにパッシブFTPを許可します。
  - 送信を許可する: このコンピュータがクライアントとして動作しているときにパッシブFTPを許可します。

UDPパケットインスペクション

[UDP] タブで次のオプションを有効化できます。

- UDPステートフルインスペクションを有効にする: UDPトラフィックのステートフルインスペクションを有効にする場合はオンにします。

  注意: UDPステートフル機能は、未承諾の受信UDPパケットを破棄します。送信UDPパケットごとに、ルールがそのUDP「ステートフル」テーブルをアップデートし、要求に対して60秒以内にUDP応答が発生した場合のみ、UDP応答を許可します。特定の受信UDPトラフィックを許可する場合は、強制的に許可ルールを作成する必要があります。たとえば、DNSサーバを実行している場合、送信先のポート53に受信UDPパケットを許可するには、強制的に許可ルールを作成する必要があります。

  警告: UDPトラフィックのステートフルインスペクションがない場合、攻撃者はDNSサーバになりすまして、未承諾のUDP「応答」を送信元のポート53からファイアウォールの内側にあるコンピュータに送信する可能性があります。

  - UDPステートフルログを有効にする: このオプションを選択すると、UDPステートフルインスペクションイベントのログを記録できるようになります。

ICMPパケットインスペクション

[ICMP] タブで次のオプションを有効にできます。

注意: ICMPステートフルインスペクションは、Deep Security Agent 8.0以前で使用できます。

- ICMPステートフルインスペクションを有効にする: ICMPトラフィックのステートフルインスペクションを有効にする場合はオンにします。

  注意: ICMP (擬似) ステートフル機能は、未承諾の受信ICMPパケットを破棄します。送信ICMPパケットごとに、ルールがそのICMP「ステートフル」テーブルを作成またはアップデートし、要求に対して60秒以内にICMP応答が発生した場合のみ、ICMP応答を許可します(サポートするICMPペアの種類は、タイプ0と8、13と14、15と16、17と18です)。

  警告: たとえば、ステートフルICMPインスペクションを有効にすると、エコー要求が送信された場合にICMPエコー応答を許可できます。要求されていないエコー応答は、Smurf増幅攻撃、マスターとデーモン間のトライブフラッドネットワーク通信、Loki2バックドアなど、さまざまな種類の攻撃の予兆である可能性があります。

- ICMPステートフルログを有効にする: このオプションを選択すると、ICMPステートフルインスペクションイベントのログを記録できるようになります。

ステートフル設定をエクスポートする

[エクスポート] をクリックし、リストから該当するエクスポート処理を選択すると、すべてのステートフル設定を.csvまたは.xmlファイルにエクスポートできます。ステートフル設定を選択し、[エクスポート] をクリックして、リストから該当するエクスポート処理を選択すると、特定のステートフル設定をエクスポートすることもできます。

ステートフル設定を削除する

ステートフル設定を削除するには、[ファイアウォールステートフル設定] リスト内の設定を右クリックして、[削除] をクリックした後、[OK] をクリックします。

注意: 1台以上のコンピュータに割り当てられたステートフル設定、またはポリシーの一部であるステートフル設定は削除できません。

ステートフル設定が割り当てられたポリシーとコンピュータを表示する

ステートフルインスペクション設定に割り当てられたポリシーとコンピュータは、[割り当て対象] タブに表示できます。リスト内のポリシーまたはコンピュータをクリックすると、そのプロパティが表示されます。

オープンポートの検索

Deep Security Managerに次のことを指示できます。コンピュータで開いているポートを検索するコンピュータを右クリックして[処理]→[検索するポート]の順に選択するか、または[開く]→[ポートの検索]ボタンをクリックします。ファイアウォールのページ**コンピュータエディタ**[1](最新の検索結果が表示されます) 。

この他、Managerの [コンピュータ] 画面で既存のコンピュータを右クリックして、[オープンポートの検索] を選択する方法もあります。また、[予約タスク] を作成して、コンピュータのリストに対して定期的にポート検索を実行する方法もあります。

初期設定では、検索対象のポート範囲は「ウェルノウンポート」と言われる1 ~ 1024の範囲ですが、別のポートセットを検索するよう定義できます。

[1] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

注意: Managerからの受信ハートビート接続を待機するAgentのポート番号は、ポート範囲の設定に関係なく常に検索されます。このポートは、Managerによって開始された通信が送信されるコンピュータ上のポートです。ただし、コンピュータに対して通信方向を[Agent/Applianceから開始](コンピュータエディタまたはポリシーエディタ[1]の[設定]→[一般])に設定すると、このポート番号は閉じられます。

1. [ポリシー]→[共通オブジェクト]→[リスト]→[ポートリスト]に進み、メニューバーの[新規]をクリックします。[新規ポートリスト]画面が表示されます。
2. [ポート]で、許容される形式を使用して新しいポートリストの名前と説明を入力してから、ポートを定義します(たとえば、ポート100、105、および110 ~ 120を検索するには、1行目に「100」、2行目に「105」、および3行目に「110-120」と入力します)。[OK]をクリックします。
3. コンピュータエディタまたはポリシーエディタ[2]の[設定]→[一般]に進み、[検索するポート]メニューをクリックします。新しく定義したポートリストが1つの選択肢として表示されます。

コンテナのファイアウォールルール

オーバーレイネットワークを使用するコンテナの保護にDeep Security Agent 11.2以降を利用している場合、初期設定のファイアウォールルールではSwarmまたはKubernetesサービスのネットワークトラフィックがブロックされるため、それらのトラフィックを許可するファイアウォールルールの追加が必要になる場合があります。

Kubernetesファイアウォールルール

Kubernetesを使用している場合、ファイアウォールでk8s通信トラフィックを通過させてサービストラフィックを送受信できるようにするには、次のルールを追加します。

名前	処理の種類	優先度	方向	フレームの種類	プロトコル	送信元IP	送信元ポート	送信先IP	送信先ポート
HTTP受信TCP 80送信先ポート	強制的に許可	0 - 最低	受信	IP	TCP	任意	該当なし	任意	80
HTTP送信TCP 80送信元ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	80	任意	任意

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

[2] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

名前	処理の種類	優先度	方向	フレームの種類	プロトコル	送信元IP	送信元ポート	送信先IP	送信先ポート
K8s受信TCP 10054ポート	強制的に許可	0 - 最低	受信	IP	TCP	任意	任意	任意	10054
K8s送信TCP 10054ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	任意	任意	10054
K8s送信TCP 443ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	任意	任意	443
K8s送信TCP 6443ポート	強制的に許可	0 - 最低	受信	IP	TCP	任意	任意	任意	6443
K8s送信TCP 6443ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	任意	任意	6443
K8s送信TCP 8081ポート	強制的に許可	0 - 最低	受信	IP	TCP	任意	任意	任意	8081
K8s送信TCP 8081ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	任意	任意	8081
K8s送信UDP 8472ポート	強制的に許可	0 - 最低	送信	IP	UDP	任意	任意	任意	8472
K8s送信UDP 8285ポート	強制的に許可	0 - 最低	送信	IP	UDP	任意	任意	任意	8285
K8s送信UDP 8285ポート	強制的に許可	0 - 最低	受信	IP	UDP	任意	任意	任意	8285

Swarmファイアウォールルール

Swarmを使用している場合、ファイアウォールでk8s通信トラフィックを通過させてサービストラフィックを送受信できるようにするには、次のルールを追加します。

名前	処理の種類	優先度	方向	フレームの種類	プロトコル	送信元IP	送信元ポート	送信先IP	送信先ポート
HTTP受信TCP 80送信先ポート	強制的に許可	0 - 最低	受信	IP	TCP	任意	該当なし	任意	80
HTTP送信TCP 80送信元ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	80	任意	任意
Swarm送信TCP 443ポート	強制的に許可	0 - 最低	送信	IP	TCP	任意	任意	任意	443
Swarm受信TCP 2377、4789、7946、60012ポート	強制的に許可	0 - 最低	受信	IP	TCP+UDP	任意	任意	任意	2377、4789、7946、60012
Swarm送信TCP	強制的に許	0 - 最低	送信	IP	TCP+UDP	任意	2377、	任意	任意

名前	処理の種類	優先度	方向	フレームの種類	プロトコル	送信元IP	送信元ポート	送信先IP	送信先ポート
2377、4789、7946、60012ポート	可						4789、7946、60012		

デバイスコントロールの設定

デバイスコントロールについて

デバイスコントロールモジュールは、コンピュータに接続されている外部ストレージデバイスへのアクセスを制御します。デバイスコントロールは、データ漏えいの防止に役立ちます。また、ファイル検索と組み合わせることで、セキュリティリスクからの保護に役立ちます。

デバイスコントロールの施行設定 (ポリシーまたはコンピュータの [デバイスコントロール] タブ) は、サポートされているデバイスの種類ごとに、無制限から制限付きまで、「フルアクセス」、「読み取り専用」、および「ブロック」の3つのオプションを設定できます。

特定の種類のデバイスが保護対象のエンドポイントに接続されると、その種類のデバイスに対して処理が実行されます。ユーザの処理によって違反が発生した場合、デバイスコントロールイベントがDeep Security Consoleに送信されます ([イベントとレポート]→[イベント]→[デバイスコントロールイベント])。

ポリシーまたはコンピュータ(コンピュータの[デバイス制御] タブ→ [除外]) に除外を追加して、処理が [読み取り専用] または [ブロック] に設定されている場合でも、デバイスへのフルアクセスを許可することができます。

デバイスコントロールを有効にして設定するには、「デバイスコントロールの設定」を参照してください。

デバイスコントロールプロトコル

デバイスの種類に対する処理

デバイスコントロールを有効にすると、デバイスの種類ごとに「プロトコル」が割り当てられます。プロトコルとは、ユーザがデバイスにアクセスしたときに持つ権限です。

プロトコル	読む	コピー	Exclude	書き込み	削除
フルアクセス	✓	✓	✓	✓	✓
読み取り専用	✓	✓	✗	✗	✗
ブロック	✗	✗	✗	✗	✗

USB自動実行

デバイスコントロールを使用すると、USBデバイスがコンピュータに接続されているときにUSB自動実行が実行されないようにすることができます。

デバイスコントロールの設定

1. [ポリシー] に移動します。(または、特定のコンピュータで有効にするには、コンピュータの [デバイスコントロール] タブに移動します)。
2. デバイスコントロールを有効にするポリシーをダブルクリックします。
3. [デバイスコントロール] →[一般] の順に選択します。
4. [デバイスコントロールのステータス] で [オン] を選択します。
5. [Save]を選択します。

プロトコルの設定

次の表は、各デバイスタイプで使用可能な処理設定を示しています。

	使用可能な設定	説明
USB大容量ストレージ 注意: この機能は、Windows用Deep Security Agent 20.0.0 ~ 4959以降でサポートされています。	• Full Access • Read Only • ブロック	USBデバイスのアクセスポリシーの設定
USB自動実行機能	• 許可	USBデバイスの自動実行を許可またはブロックする

	使用可能な設定	説明
	• ブロック	
モバイル (MTP/PTP) 注意: これは現在、Windows Server Coreエージェントではサポートされていません。	• 許可 • ブロック	USBモバイルデバイスのアクセスポリシーの設定

USBデバイスの例外を設定

新しいデバイスを作成

USBマスストレージがブロックまたは読み取り専用に設定されている場合に特定のUSBデバイスへのアクセスを許可するには、除外ルールを設定します。

各除外ルールごとに名前を入力し、次にベンダー、モデル、およびシリアル番号を指定します。

アクセス違反は、アクセスが除外ルールのベンダー、モデル、およびシリアル番号と一致する場合にバイパスされます。USBデバイスに関する情報については、デバイスコントロールでUSBストレージデバイスおよび携帯電話を除外するを参照してください。

既存のデバイスの選択

既存のデバイスは複数のポリシーに表示できます。既存のデバイスをポリシーに含めるには、[リスト内の既存のデバイスを選択] をクリックし、関連するデバイスを選択します。

デバイスコントロールイベントのタグ付け

デバイスコントロールモジュールで生成されたイベントは、Deep Securityコンソールの[イベントとレポート]→[デバイスコントロールイベント] に表示されます。イベントのタグ付けを使用すると、イベントをソートし、さらに調査が必要なイベントと正当なイベントを判断できます。

イベントを右クリックして[タグの追加]をクリックすると、イベントに手動でタグを適用できます。選択したイベントのみにタグを適用するか、類似のデバイスコントロールイベントにタグを適用するかを選択できます。

自動タグ設定機能を使用して、複数のイベントをグループ化してラベルを付けることもできます。Deep Securityコンソールでこの機能を設定するには、[イベントとレポート]→[デバイス制御イベント]→[自動タグ付け]→[新しい信頼できる送信元]の順に選択します。タグ付けの実行に使用できるソースは3つあります。

- 信頼済みのローカルコンピュータ
- トレンドマイクロのソフトウェア安全性評価サービス
- 信頼済みの共通ベースライン。コンピュータグループから収集された、ファイルのステータスのセットです。

イベントのタグ付けの詳細については、「タグを適用してイベントを識別およびグループ化する」を参照してください。

ムーブ監視の設定

変更監視

整合性監視モジュールは、Deep Security Agentのレジストリ値、レジストリキー、サービス、プロセス、インストールされているソフトウェア、ポート、およびファイルに対する予期しない変更を検索します。変更監視モジュールは、ベースラインの安全な状態を参考にして上記の検索を実行し、想定外の変更が検出されると、イベント(およびオプションのアラート)をログに記録します。

変更監視を有効にして設定するには、"変更監視の設定" belowを参照してください。

変更監視ルールの作成の詳細については、"変更監視 ルールの作成" on page 1012を参照してください。ルールは、ファイルまたはレジストリ監視テンプレートから、またはDeep Security XMLベースの"変更監視 rules languages" on page 1017を使用して作成できます。

変更監視の設定

変更監視保護モジュールは、不審なアクティビティを示している可能性があるファイルや重要なシステム領域 (Windowsレジストリなど) への変更を検出します。検出では、現在の状況が、以前に記録されたベースラインの読み取り値と比較されます。Deep Securityには、事前定義された変更監視ルールが付属しています。新しい変更監視ルールは、セキュリティアップデートで提供されます。

変更監視は、システムに加えられた変更を検出しますが、変更を防止したり元に戻したりすることはありません。

変更監視は、次の操作を行うことで、ポリシー内で有効にすることも、コンピュータレベルで有効にすることもできます。

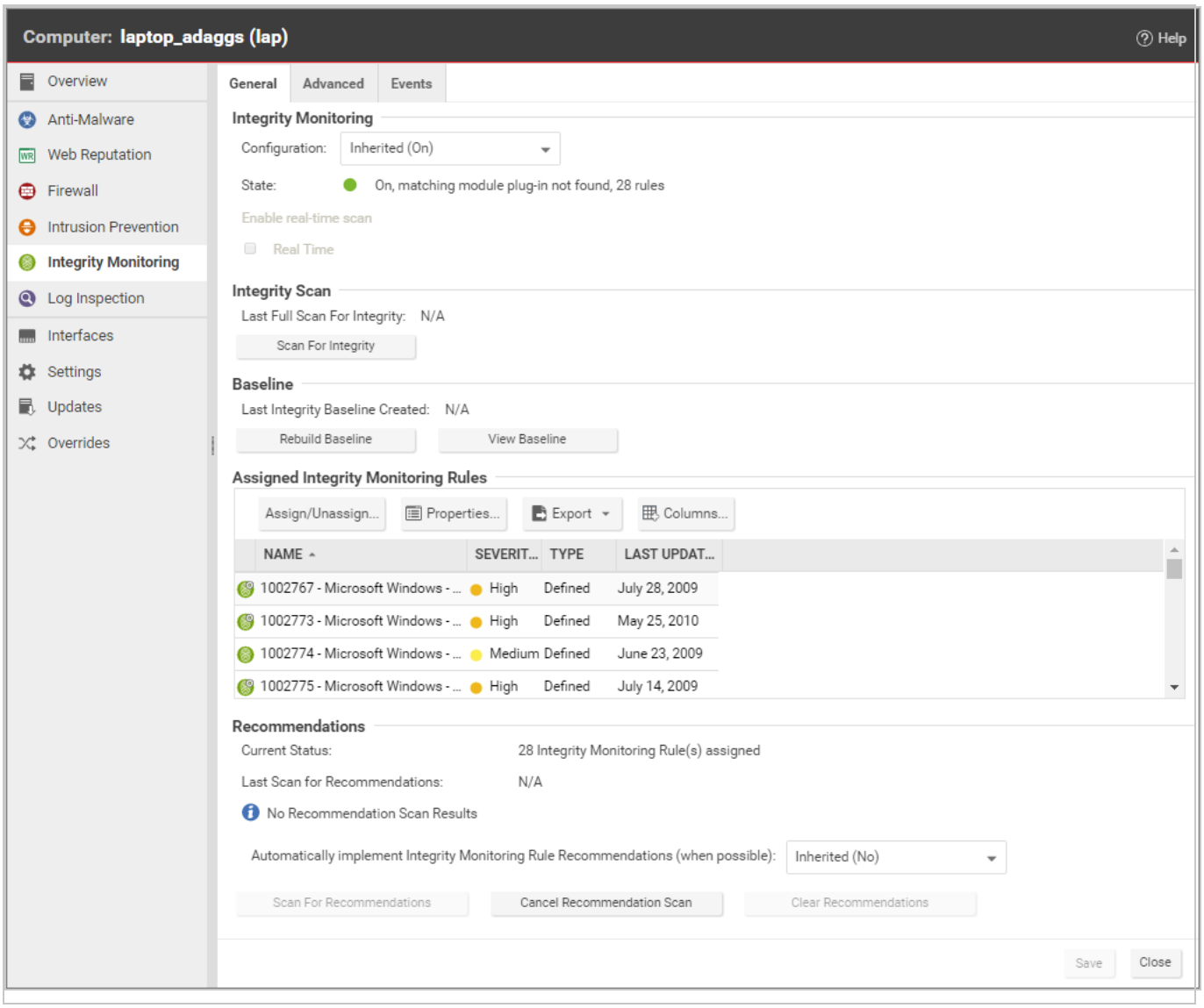
1. "変更監視を有効にする" below
2. "推奨設定の検索を実行する" on the next page
3. "変更監視ルールを適用する" on page 1007
4. "コンピュータのベースラインを構築する" on page 1009
5. "定期的に変更をスキャンする" on page 1009
6. "テスト変更監視" on page 1009

変更監視を有効にしたら、次のトピックに慣れておくとよいでしょう。

- "変更監視スキャンの種類" on page 1010
- "変更監視検索パフォーマンスの設定" on page 1011
- "変更監視イベントのタグ付け" on page 1012

変更監視を有効にする

コンピュータまたはポリシーの設定で変更監視を有効にすることができます。これを行うには、ポリシーまたはコンピュータエディタを開き、変更監視 > 一般に移動します。設定をオンまたは継承 (オン) に設定し、保存をクリックします。



推奨設定の検索を実行する

コンピュータで推奨設定スキャンを実行して、適切なルールに関する推奨設定を取得します。これを行うには、コンピュータエディタを開き、変更監視 > 一般に移動します。推奨設定セクションで、推奨設定のスキャンをクリックします。オプションで、Deep Securityが見つけたルール推奨設定を実装するように指定することもできます。

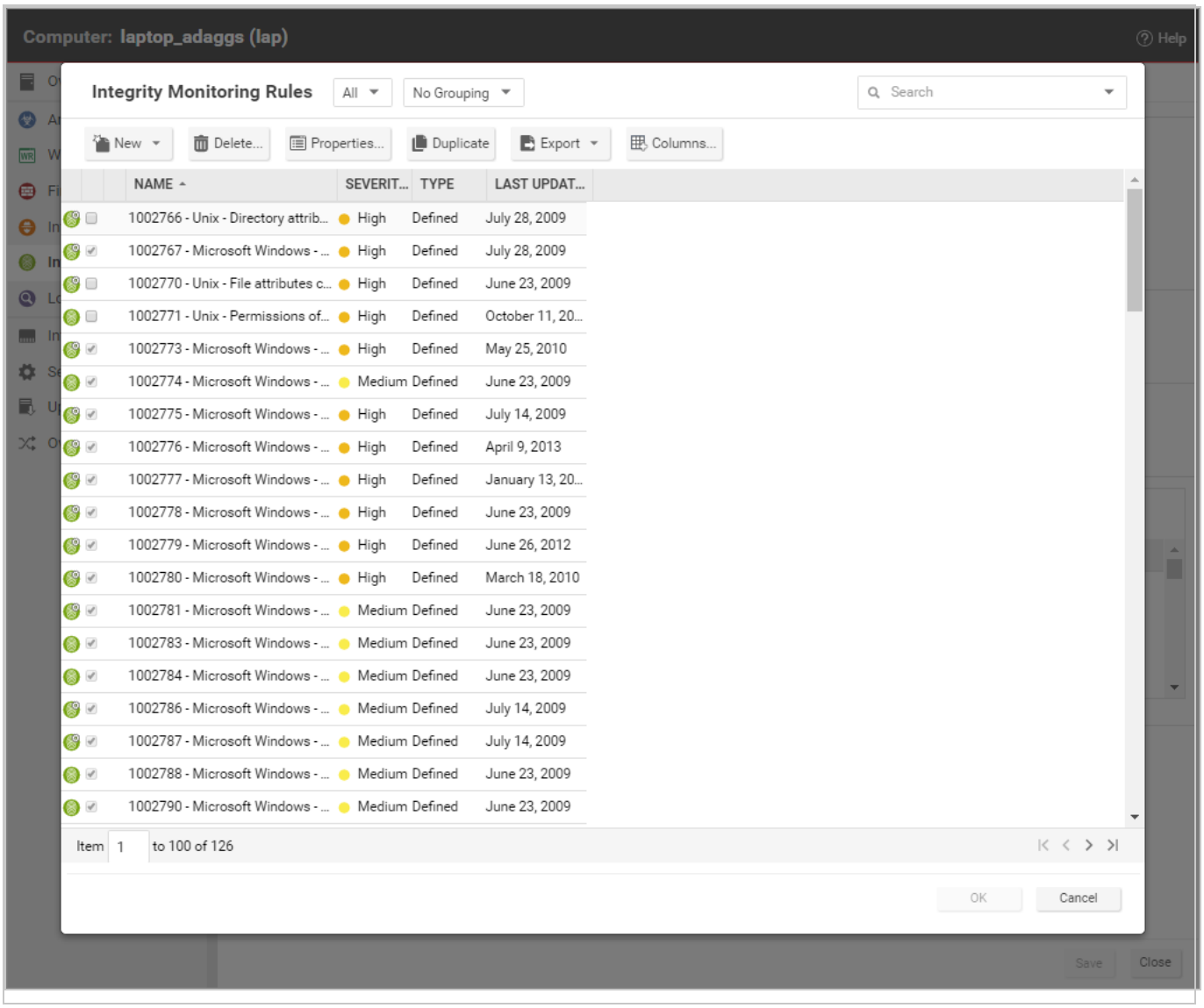
推奨される変更監視ルールを適用すると、監視対象のエンティティと属性が多くなりすぎる可能性があります。重要で監視すべき対象を特定し、カスタムルールを作成するかまたは事前定義されたルールを調整することをお勧めします。頻繁に変更されるプロパティ(プロセスIDや送信元ポート番号など)を監視するルールでは、検出数が多くなりがちなため、調整が必要になることがあるので、注意が必要です。

リアルタイム変更監視スキャンを有効にしていて、一部の推奨ルールが頻繁に変更されるディレクトリを監視しているためにイベントが多すぎると感じた場合は、それらのルールのリアルタイムスキャンを無効にすることができます。ポリシー > 共通オブジェクト > ルール > 変更監視ルールに移動し、ルールをダブルクリックします。オプションタブで、リアルタイム監視を許可の選択を解除します。

変更監視ルールを適用する

推奨設定の検索の実行時に推奨されたルールをDeep Securityで自動的に実装することができます。また、ルールを手動で割り当てることもできます。

コンピュータまたはポリシーエディタで、変更監視 > 一般に移動します。割り当てられた変更監視ルールセクションには、このポリシーまたはコンピュータに適用されているルールが表示されます。変更監視ルールを追加または削除するには、割り当て/割り当て解除をクリックします。これにより、利用可能なすべての変更監視ルールが表示され、ルールを選択または選択解除できます。



トレンドマイクロが作成した変更監視ルールの中には、正しく機能させるためにローカル設定を必要とするものがあります。これらのルールのいずれかをコンピュータに割り当てた場合、またはこれらのルールのいずれかが自動的に割り当てられた場合は、設定が必要であることを通知するアラートが表示されます。

変更監視ルールは、ローカルで編集して編集中のコンピュータまたはポリシーにのみ変更内容を適用することも、グローバルに編集してルールを使用する他のすべてのポリシーまたはコンピュータに変更内容を適用することもできます。ルールをローカルで編集するには、そのルールを右クリックして[プロパティ]をクリックします。ルールをグローバルに編集するには、そのルールを右クリックして[プロパティ(グローバル)]をクリックします。

組織にとって重要な特定の変更 (新しいユーザの追加や新しいソフトウェアのインストールなど) を監視するために、カスタムルールを作成することもできます。カスタムルールの作成方法の詳細については、"変更監視 rules languages" on page 1017を参照してください。

パフォーマンスを向上させ、競合や誤検出を避けるためには、できるだけ具体的な変更監視ルールを作成します。たとえば、ハードドライブ全体を監視するルールは作成しないでください。

コンピュータのベースラインを構築する

ベースラインは、変更の検索の結果を比較するための元の安全な状態です。コンピュータで変更の検索の新しいベースラインを作成するには、コンピュータエディタを開き、変更監視 > 一般に移動して、ベースラインの再構築をクリックします。

現在のベースラインデータを表示するには、[ベースラインの表示] をクリックします。

注意: 大量のベースラインデータに関連するパフォーマンスの問題により、最新バージョンのDeep Security Managerでは、ベースラインの表示が表示されません。詳細については、大量の変更監視ベースラインデータによるデータベースのパフォーマンス問題をご覧ください。

パッチを適用した後は、新しいベースライン検索を実行することをお勧めします。

定期的に変更をスキャンする

定期的に変更をスキャンします。手動検索を実行するには、コンピュータエディタを開き、変更監視 > 一般に移動して整合性をスキャンをクリックします。また、定期的にスキャンを実行する予約タスクを作成することもできます。

テスト変更監視

以降の変更監視設定の手順に進む前に、ルールとベースラインが正常に動作しているかどうかをテストします。

1. 変更監視が有効になっていることを確認します。
2. コンピュータエディタまたはポリシーエディタ[1]で、[変更監視]→[現在割り当てられている変更監視ルール] に移動します。[割り当て/割り当て解除] をクリックします。
3. もしWindowsユーザであれば、1002773 - Microsoft Windows - 'Hosts' ファイルが変更されましたを検索し、ルールを有効にしてください。このルールはC:\windows\system32\drivers\etc\hostsに変

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

更が加えられたときにアラートを発します。

Linuxユーザの場合、1003513 - Unix - /etcの場所でのファイル属性の変更を検索し、ルールを有効にしてください。このルールは、/etc/hostsファイルに変更が加えられたときにアラートを発します。

4. 上記のファイルを変更し、変更を保存します。
5. コンピュータエディタ[1]で、[変更監視]→[一般] に移動し、[変更の検索] をクリックします。
6. [イベントとレポート]→[変更監視イベント] に移動し、ホストファイルの変更が記録されていることを確認します。検出が記録されていれば、変更監視モジュールは正常に動作しています。

変更監視スキャンの種類

変更監視検索を実行するためのオプションは3つあります。

- 手動検索: 手動の変更監視検索は、**コンピュータエディタ**[2]を開いて[変更監視]→[一般] に移動することにより、必要に応じて実行できます。[変更の検索] セクションで、[変更の検索] をクリックします。
- 予約検索: 他のDeep Security操作と同様に、変更監視検索をスケジュールすることができます。Deep Securityは監視対象のエンティティをチェックし、前回の検索以降の変更を特定して記録します。検索間の監視対象エンティティの複数の変更は追跡されず、最後の変更のみが検出されます。エンティティの状態に対する複数の変更を検出して報告するには、予約検索の頻度を増やす (例えば、週次ではなく日次にする) か、頻繁に変更されるエンティティに対してリアルタイム検索を有効にすることを検討してください。予約変更監視検索を有効にするには、管理 > 予約タスク > 新規に移動します。新規予約タスクウィザードで、変更の検索と予約検索の頻度を選択します。新規予約タスクウィザードで要求される情報を希望の仕様で入力してください。予約タスクの詳細については、"Deep Security予約タスクの設定" on page 1826を参照してください。
- リアルタイム検索: リアルタイム検索を有効にすることができます。このオプションを選択すると、Deep Securityはエンティティの変更をリアルタイムで監視し、変更を検出すると変更監視イベントを発生させます。イベントは、次のハートビート通信時にDeep Security Managerに送信されるか、syslogを介してSIEMにリアルタイムで転送されます。リアルタイム検索を有効にするには、**コンピュータまたはポリシーエディタ**[3] > 変更監視 > 一般に移動し、リアルタイムを選択します。64

---

[1] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

[2] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

[3] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

ビットLinuxプラットフォーム上のDeep Securityエージェント11.0以降および64ビットWindowsサーバー上のDeep Securityエージェント11.2以降では、リアルタイム検索結果にファイルを変更したユーザおよびプロセスが表示されます。この機能をサポートするプラットフォームの詳細については、"各プラットフォームでサポートされている機能" on page 417を参照してください。

注意: すべてのファイルの変更に対するディスク全体のリアルタイムモニタは、パフォーマンスに影響を与え、変更監視イベントが多すぎる結果となります。安全策として、ルートドライブ(C:\)をリアルタイムでモニタする場合、Deep Securityは実行可能ファイルとスクリプトのみをモニタします。すべてのファイルをリアルタイムでモニタしたい場合は、ルートドライブ以外のフォルダを指定してください。

変更監視検索パフォーマンスの設定

以下の設定を変更すると、変更監視検索のパフォーマンスを改善できることがあります。

CPUの使用率を制限する

変更監視のシステム検索ではローカルのCPUリソースを消費します。これは、最初に初期ベースラインが作成され、その後のシステム検索時にはシステムの状態がベースラインと照合されるためです。変更監視が予想以上にリソースを消費していることが判明した場合、CPUの使用率を次のレベルに制限することができます。

- 高: 一時停止せずに、ファイルを次々に検索する
- 中: ファイル検索の間に一時停止処理を行い、CPUリソースの消費を抑える
- 低: ファイル検索の間に、「中」よりも長い時間一時停止処理を行う

[変更監視のCPU使用率レベル]設定を変更するには、**コンピュータエディタまたはポリシーエディタ**[1]を開いて[変更監視]→[詳細]に進みます。

コンテンツハッシュアルゴリズムを変更する

変更監視モジュールがベースライン情報を格納するために使用するハッシュアルゴリズムを選択できます。複数のアルゴリズムを選択できますが、パフォーマンスに悪影響を与えるため、お勧めしません。

コンテンツハッシュアルゴリズムを変更できます。

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

仮想マシンの検索キャッシュ設定を有効にする

変更監視に検索キャッシュを使用すると、大規模なVMware環境で複数の仮想マシンから同じ内容を検索する必要性がなくなるため、検索の効率が向上します。仮想マシンで使用する検索キャッシュ設定を選択するには、**コンピュータエディタまたはポリシーエディタ**[1]を開き、[変更監視]→[詳細]→[仮想マシンの検索キャッシュ] の順に進みます。

変更監視の検索キャッシュ設定の詳細については、"Virtual Applianceの検索キャッシュ" on page 1062を参照してください。

変更監視イベントのタグ付け

生成されたイベント変更監視モジュールがDeep Security Managerの下に表示されます。イベント&レポート>変更監視イベント。イベントのタグ付けを行うと、イベントをソートしやすくなり、問題のないイベントと詳細な調査が必要なイベントを判別しやすくなります。

タグは、イベントを右クリックして[タグの追加] をクリックすることにより、手動でイベントに適用できます。タグを選択したイベントにのみ適用するか、同様のすべての変更監視イベントに適用するかを選択できます。

また、自動タグ付け機能を使用し、複数のイベントをグループ化してラベルを付けることもできます。Deep Security Managerでこの機能を設定するには、[イベントとレポート]→[変更監視イベント]→[自動タグ付け]→[新しい信頼済みのソース] に進みます。タグ付けの実行に使用できるソースは3つあります。

- 信頼済みのローカルコンピュータ
- トレンドマイクロのソフトウェア安全性評価サービス
- 信頼済みの共通ベースライン。コンピュータグループから収集された、ファイルのステータスのセットです。

イベントのタグ付けの詳細については、"イベントを識別およびグループ化するためのタグの適用" on page 1161を参照してください。

変更監視 ルールの作成

変更監視 ルールは、Deep Security Agentがコンピュータのファイル、ディレクトリ、レジストリキーと値の変更、およびインストールされているソフトウェア、プロセス、待機ポート、および実行中のサービスの変

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。

更を検索および検出する方法を示します。変更監視ルールは、コンピュータに直接割り当てることも、ポリシーの一部にすることもできます。

注意: ここでは、変更監視ルールの作成方法を具体的に説明します。変更監視モジュールの設定方法については、"変更監視の設定" on page 1004を参照してください。

変更監視ルールには、ユーザ自身が作成したルールとトレンドマイクロが発行するルールの2種類があります。トレンドマイクロが発行するルールの設定方法については、"トレンドマイクロが発行する変更監視ルールを設定する" on page 1015セクションを参照してください。

新しい変更監視ルールを作成するには、次の手順を実行する必要があります。

1. "新しいルールを追加する" below。
2. "変更監視ルール情報を入力する" below。
3. "ルールテンプレートを選択し、ルールの属性を定義する" on the next page。

変更監視ルールを作成したら、次の方法も学習できます。

- "ルールイベントとアラートを設定する" on page 1016
- "ルールが割り当てられているポリシーとコンピュータを確認する" on page 1016
- "ルールをエクスポートする" on page 1016
- "ルールを削除する" on page 1016

新しいルールを追加する

[ポリシー]→[共通オブジェクト]→[ルール]→[変更監視ルール] ページで、新しい変更監視ルールを追加する方法は3つあります。次の手順を実行します。

- 新しいルールを作成します。[新規]→[新しい変更監視ルール] の順にクリックします。
- XMLファイルからルールをインポートします。[新規]→[ファイルからインポート] をクリックします。
- 既存のルールをコピーして変更します。[変更監視ルール] リストで、該当のルールを右クリックし、[複製] をクリックします。新しいルールを編集するには、そのルールを選択し、[プロパティ] をクリックします。

変更監視ルール情報を入力する

1. ルールの [名前] と[説明] を入力します。

ヒント: すべての変更監視ルールへの変更をルールの [説明] フィールドに記録することを推奨します。メンテナンスを簡単にするため、ルールを作成または削除した日付とその理由を記録してください。

2. ルールの [重要度] を設定します。

注意: ルールの重要度の設定は、ルールの実装および適用方法に影響しません。重要度レベルは、変更監視ルールのリストを表示するときに条件をソートする際に役立ちます。それぞれの重要度レベルは重要度の値と関連付けられます。この値にコンピュータの資産評価を掛けたものが、イベントのランク付けを決定します([管理]→[システム設定]→[ランク付け] を参照してください)。

ルールテンプレートを選択し、ルールの属性を定義する

[コンテンツ] タブに移動し、次の3つのテンプレートのいずれかを選択します。

レジストリ値テンプレート

特にレジストリ値への変更を監視する変更監視ルールを作成します。

注意: レジストリ値テンプレートは、Windowsベースコンピュータでのみ使用できます。

1. 監視する [基本キー]、およびサブキーのコンテンツを監視するかどうかを選択します。
2. 含まれる、または除外される [値の名前] が一覧表示されます。ワイルドカード文字として「?」および「*」を使用できます。
3. 監視する [属性] を入力します。「STANDARD」と入力すると、レジストリサイズ、コンテンツ、種類への変更が監視されます。レジストリ値テンプレートの属性の詳細については、"RegistryValueSet" on page 1049 ドキュメントを参照してください。

ファイルテンプレート

特にファイルへの変更を監視する変更監視ルールを作成します。

1. ルールの [基本ディレクトリ] を入力します (例: `C:\Program Files\MySQL`)。基本ディレクトリに関連するすべてのサブディレクトリのコンテンツも含めるには、[サブディレクトリも含む] を選択します。ベースディレクトリではワイルドカードはサポートされていません。

2. 特定のファイルを含める、または除外するには、[ファイル名] フィールドを使用します。ワイルドカード(「`?`」を任意の1文字として、「`*`」を0個以上の文字として) 使用できます。

> 注意: [ファイル名] フィールドを空白のままにすると、基本ディレクトリ内のすべてのファイルが監視されます。この場合、基本ディレクトリに多数のファイルが含まれていると、大量のシステムリソースが消費されます。

3. 監視する[属性] を入力します。「STANDARD」と入力すると、ファイル作成日、最終更新日、権限、所有者、サイズ、コンテンツ、フラグ (Windows)、SymLinkPath (Linux) が監視されます。ファイルテンプレートの属性の詳細については、"FileSet" on page 1032 ドキュメントを参照してください。

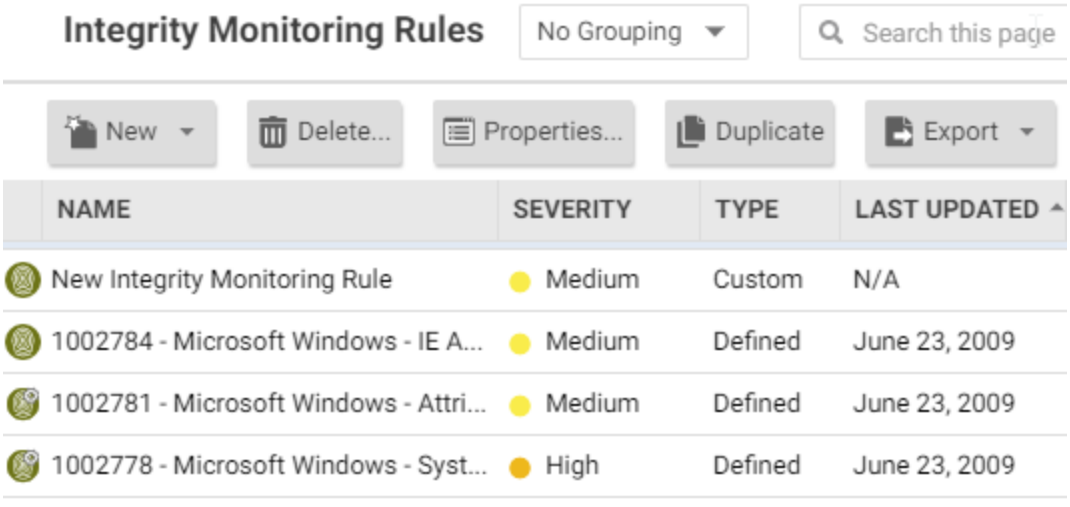
カスタム (XML) テンプレート

カスタム変更監視, レジストリ値, レジストリキー, サービス, プロセス, インストールされたソフトウェア, ポート、グループ, ユーザ, ファイル、およびDeep Security XMLベースの "変更監視 rules languages" on page 1017。

> ヒント: 希望するテキストエディタを使用してルールを作成し、完成したルールを[コンテンツ] フィールドに貼り付けることができます。

トレンドマイクロが発行する変更監視ルールを設定する

トレンドマイクロが発行する変更監視ルールは、作成したカスタムルールと同じ方法では編集できません。トレンドマイクロのルールには、まったく変更できないものと、限定的な設定オプションが提供されているものがあります。いずれのルールも「種類」列に「定義済み」として表示されますが、設定可能なルールは変更監視アイコンに歯車 ( ) が表示されます。



ルールの設定オプションにアクセスするには、ルールのプロパティを開き、[設定] タブをクリックします。

トレンドマイクロが発行するルールには、[一般] タブの下に補足情報も表示されます。

- ルールがはじめて発行された日付と、最後に更新された日付、およびルールの一意のID。
- ルールの機能に必要なAgentおよびDeep Security Managerの最小バージョン。

トレンドマイクロが発行するルールは編集できませんが、複製した後にそのコピーを編集することはできます。

ルールイベントとアラートを設定する

変更監視 ルールによって検出された変更は、Deep Security Managerにイベントとして記録されます。

リアルタイムのイベント監視

初期設定では、イベントは発生時にログに記録されます。変更の検索を手動で実行している場合にのみイベントをログに記録するには、[リアルタイム監視を許可] の選択を解除します。

アラート

イベントのログを記録したときに、アラートもトリガするようにルールを設定できます。アラートを設定するには、ルールのプロパティを開き、[オプション] をクリックしてから、[このルールによってイベントが記録された場合にアラート] を選択します。

ルールが割り当てられているポリシーとコンピュータを確認する

変更監視ルールに割り当てられているポリシーとコンピュータは、[割り当て対象] タブで確認できます。リスト内のポリシーまたはコンピュータをクリックすると、そのプロパティが表示されます。

ルールをエクスポートする

すべての変更監視ルールを、.csvまたは.xmlファイルにエクスポートするには、[エクスポート] をクリックし、リストから対応するエクスポート処理を選択します。特定のルールを選択し、[エクスポート] をクリックして、リストから該当するエクスポート処理を選択すると、特定のルールをエクスポートすることもできます。

ルールを削除する

ルールを削除するには、[変更監視ルール] リストで該当のルールを右クリックしてから、[削除]→[OK] の順にクリックします。

注意: 1台以上のコンピュータに現在割り当てられている変更監視ルール、またはポリシーの一部である変更監視ルールは削除できません。

変更監視ルールのインポート

変更監視 rules languages

変更監視 ルール言語は、宣言XMLベースの言語で、Deep Securityで監視する必要のあるシステムコンポーネントおよび関連する属性を記述します。この言語を使用して、システム内に多数存在するコンポーネントの中から監視の対象外とするものを指定することもできます。

ヒント: ファイルまたはWindowsレジストリへの不正な変更のみを監視する場合は、カスタムテンプレートを作成する代わりにファイルおよびレジストリルールテンプレートを使用できます。これらのテンプレート使用の詳細については、"変更監視 ルールの作成" on page 1012を参照してください。

新しいカスタム変更監視ルールを作成するには、"変更監視 ルールの作成" on page 1012 (テンプレートの種類として [カスタム (XML)] を選択) の手順を開始してから、以下のセクションで説明されているように、変更監視ルール言語に従ってカスタムルールを作成します。

- "エンティティセット" on the next page
- "階層とワイルドカード" on the next page
- "構文とコンセプト" on page 1019
- "includeタグ" on page 1020
- "excludeタグ" on page 1021
- "大文字/小文字の区別" on page 1022
- "エンティティ機能" on page 1022
- "ANDとOR" on page 1024
- "評価の順序" on page 1025
- "エンティティ属性" on page 1025
- "簡略記法属性" on page 1026
- "onChange属性" on page 1027
- "環境変数" on page 1027
- "レジストリ値" on page 1028

- "「..」の使用" on page 1029
- "ベストプラクティス" on page 1029

エンティティセット

変更監視ルールに含めるシステムコンポーネントは、「エンティティ」と呼ばれます。コンポーネントの各種類は、エンティティのクラスを表します。たとえば、ファイル、レジストリキー、プロセスは、それぞれエンティティのクラスです。変更監視ルールの言語には、エンティティの各クラスに対してエンティティのセット(エンティティセット)を記述するためのタグが用意されています。ルールには次の種類のエンティティセットを使用できます。

- "DirectorySet" on page 1030 ディレクトリの変更を検索するルール
- "FileSet" on page 1032 ファイルの変更を検索するルール
- "GroupSet" on page 1037: グループの変更を検索するルール
- "InstalledSoftwareSet" on page 1038 インストールされているソフトウェアの変更を検索するルール
- "PortSet" on page 1041: 待機ポートの変更を検索するルール
- "ProcessSet" on page 1044 プロセスの変更を検索するルール
- "RegistryKeySet" on page 1047 レジストリキーを検索するルール
- "RegistryValueSet" on page 1049 レジストリ値を検索するルール
- "ServiceSet" on page 1051 サービスの変更を検索するルール
- "UserSet" on page 1054: ユーザの変更を検索するルール
- "WQLSet" on page 1057: Windows Management Instrumentation WQLクエリ文の結果の変更を検索するルール

1つの変更監視ルールに複数のエンティティセットを含めることができます。たとえば、複数のファイルとレジストリエントリを監視するルール1つで、アプリケーションを保護できます。

階層とワイルドカード

FileSetやRegistryKeySetなどの階層型のデータの種類を表すエンティティセットでは、セクションベースのパターン照合がサポートされます。

- `/` (スラッシュ): 階層の各レベルに該当する箇所でパターンの各セクションを区切ります
- `**` (2個のアスタリスク): ゼロ個以上のセクションに相当します

次のワイルドカードがサポートされます。

- `?` (疑問符): 1文字に相当します
- `*` (1個のアスタリスク): ゼロ個以上の文字に相当します

次の「エスケープ」文字もサポートされます。

- `\` (バックスラッシュ): 直後の文字をエスケープします

「/」の文字でパターンをセクションに分割します。分割したセクションが一致するかぎり、パターンの各セクションが階層のそれぞれの下位レベルに適用されます。たとえば、次のようなパターンがあります。

```
/a?c/123/*.java
```

これが次のパスに適用された場合

```
/abc/123/test.java
```

次のように判定されます。

- 「a?c」は「abc」に一致
- 「123」は「123」に一致
- 「*.java」は「test.java」に一致

このパターンが次のパスに適用された場合

```
/abc/123456/test.java
```

次のように判定されます。

- 「a?c」は「abc」に一致
- 「123」は「123456」に一致しないため、そこから先はパターン照合は実行されない

「**」の記号パターンは、ゼロ個以上のセクションと照合します。したがって、次のパターンの場合

```
/abc/**/*.java
```

「abc/123/test.java」と「abc/123456/test.java」の両方に一致します。また、「abc/test.java」と「abc/123/456/test.java」にも一致します。

構文とコンセプト

このセクションでは、変更監視ルールの例をいくつか示します。以下の例ではFileSetエンティティセットを使用しますが、説明および使用コンポーネントはすべてのエンティティセットに適用できます。変更監視ルールの最小の形は、次のような構文です。

```
<FileSet base="C:\Program Files\MySQL">
 </FileSet>
```

「base」属性には、FileSetのベースディレクトリを指定します。ルールに関するすべての項目は、このディレクトリを基準とした相対ディレクトリに保存されます。上記のルールを変更しなければ、「base」以下のすべてのもの(サブディレクトリも含む)について変更が監視されます。

注意: ワイルドカード「*」と「?」を「base」属性の文字列に使用できますが、使用できるのはパスの最後のセクションだけです。したがって、次の記述は有効です。

```
base="C:\program files\CompanyName * Web Server"
```

しかし、次のような記述は無効です。

```
base="C:\* files\Microsoft Office"
```

エンティティセット内では、「include」および「exclude」タグを使用してパターン照合を制御できます。これらのタグには、照合するパターンを指定する「key」属性があります。「key」属性の内容はエンティティセットによって異なります。たとえば、ファイルやディレクトリではパスが「key」属性の内容になりますが、ポートの場合は「プロトコル/IP/ポート番号」の組み合わせになります。

注意: includeまたはexcludeルールに記述したパスの構文が無効な場合、Agentによって「変更監視ルールのコンパイルの問題」のイベントが生成され、ルールIDと展開後のパスがイベントのパラメータとして提供されます。C:\test1\D:\test2は無効なパスの例ですが、これは、ファイル名に2つのボリュームIDを含めることができないためです。

includeタグ

includeタグは基本的に許可リストです。includeタグを使用すると、そのincludeタグ(または他のincludeタグ)に一致するエンティティのみが含まれます。includeタグを追加した次のルールは、「C:\Program Files\MySQL」フォルダとそのサブボリュームフォルダ内にある「*.exe」という名前の付いたファイルについてのみ変更を監視します。

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*.exe"/>
 </FileSet>
```

includeタグの構文を組み合わせることができます。次のルールは、「C:\Program Files\MySQL」フォルダとそのサブボリュームフォルダ内にある、「*.exe」と「*.dll」という名前の付いたファイルに対する変更を監視します。

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*.exe"/>
 <include key="**/*.dll"/>
 </FileSet>
```

1つのincludeブロック内に複数の条件を含めることもできます。この場合、あるエンティティが対象となるためにはすべての条件に一致する必要があります。次の「include」タグは、「sample」で始まり「.exe」で終わる名前のエンティティを含めます。この条件はもっと簡潔に記述することもできますが、後述の「機能」のセクションで説明するように、「key」パターンはエンティティの他の機能と組み合わされるため、この構文の方が汎用性があります。

```
<include>
 <key pattern="**/*.exe"/>
 <key pattern="**/sample*"/>
 </include>
```

次の構文は、同じ条件を他の方法で記述したものです。

```
<include key="**/*.exe">
 <key pattern="**/sample*"/>
 </include>
```

excludeタグ

除外タグはブロックリストとして機能し、それ以外の場合に返されるファイルをセットから削除します。次の例は、実際にはありえませんが、tempファイル以外のすべてのファイルを監視対象にします。

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**"/>
 <exclude key="**/*.tmp"/>
 </FileSet>
```

次のルールは、EXEとDLLのファイルセットから「MySQLInstanceConfig.exe」を除外します。

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*.exe"/>
 <include key="**/*.dll" />
 <exclude key="**/MySQLInstanceConfig.exe"/>
 </FileSet>
```

「include」タグと同様、複数の条件を指定する「exclude」タグを記述することができます。次の例に、複数の条件を指定する「exclude」タグを示します。

```
<exclude>
 <key pattern="**/MySQLInstanceConfig*" />
 <key pattern="**/*.exe" />
 </exclude>
```

大文字/小文字の区別

include/excludeタグのパターン照合での大文字/小文字の区別は、「casesensitive」属性で制御できます。この属性は次の3つの値をとります。

- true
- false
- platform

この属性の初期設定は「platform」です。これは、パターンの大文字/小文字の区別を実行中のプラットフォームの大文字/小文字の区別と照合します。次の例の場合、Windowsシステムでは「Sample.txt」と「sample.txt」が返されますが、UNIXシステムで返されるのは「Sample.txt」のみです。

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*Sample*"/>
 </FileSet>
```

次の例では、Windowsの場合もUNIXの場合も「Sample.txt」のみが返されます。

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*Sample*" casesensitive="true"/>
 </FileSet>
```

注意: 大文字/小文字の区別を「true」に設定するのは、Windowsのように、ほとんどのオブジェクト名に対して大文字/小文字の区別をしないプラットフォームに限られます。

エンティティ機能

エンティティの種類によっては、「key」以外の機能に基づいてエンティティをファイルセットに含めたり、除外したりすることができます。エンティティの種類によって、機能のセットは異なります。次の例は、すべての実行可能ファイルを含めます。ファイル拡張子を使用した前述の例のようにファイル拡張子には依存せず、ファイルの最初の数百バイトをチェックして、そのOSで実行可能なファイルかどうかを判定します。

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**" executable="true"/>
 </FileSet>
```

機能属性は「include」または「exclude」タグに指定する必要があります。複数の条件を指定するinclude/excludeの一部として機能属性を使用するには、include/excludeの囲みタグの属性として指定する必要があります。次の例は、ファイル名に「MySQL」の文字列を含むすべての実行可能ファイルを含めます。

```
<include executable="true">
 <key pattern="**/*MySQL*"/>
 </include>
```

上記の例は、次のようにもっと簡潔に記述することができます。

```
<include key="**/*MySQL*" executable="true"/>
```

機能属性によっては、単にエンティティのいずれかの属性の値を照合するだけのものもあります。そのようなときには、「`*`」と「`?`」のワイルドカードで照合できる場合があります。この方法でinclude/excludeルールに使用できる属性について、およびワイルドカード照合と単純な文字列照合のどちらがそれらの属性でサポートされるかについては、各"エンティティセット" on page 1018のヘルプ画面を参照してください。

注意: ワイルドカード照合がサポートされる場合は、属性の文字列の値についての照合になりますが、正規化は行われないので注意が必要です。「**」などのエンティティのキー照合に使用できる構造体やコンポーネントを階層に分ける「/」の使用は適用されません。Windowsのパス名を照合するには、「\」の使用が必要です。これは、チェックの対象となる属性の値にこの文字が含まれているためです。これに対し、UNIXシステムではパスの値に「/」が使われるため、UNIXパスの照合には「/」を使用する必要があります。

次のルールは、「state」属性を使用した機能照合の例です。

```
<ServiceSet>
 <include state="running"/>
 </ServiceSet>
```

注意: state照合ではワイルドカードはサポートされません。

次の例は、バイナリのパスの末尾が「\notepad.exe」となっているプロセスを照合します。

```
<ProcessSet>
 <include path="*\notepad.exe"/>
 </ProcessSet>
```

次の例は、コマンドラインが「/sbin/」から始まるプロセスを照合します。

```
<ProcessSet>
 <include commandLine="/sbin/*"/>
 </ProcessSet>
```

注意: ワイルドカードの使用には注意が必要です。「**」のワイルドカード表現は、「base」以下のすべてのサブディレクトリ内のすべてのファイルを検索します。このような表現のベースラインを構築するには、多くの時間とリソースが必要です。

ANDとOR

複数の条件を指定するinclude/excludeタグと複数のinclude/excludeタグを使用して、論理ANDと論理ORを記述することができます。

複数の条件を指定するincludeまたはexcludeを使用してANDを記述するにはいくつかの方法があります。最も簡単な方法は、複数の条件を1種類の囲みタグで囲む方法です。次の例は、複数の条件を指定する簡単なAND構文です。

```
<include>
 <key pattern="**/*MySQL*" />
 <key pattern="**/*.exe"/>
 </include>
```

また、囲みタグの属性に条件を記述すると、その条件は、複数の条件を指定する要件の一部として囲まれた条件でグループ化されます。次の例は、上記の複数の条件を指定する「include」タグをこのように書き直したものです。

```
<include key="**/*.exe">
 <key pattern="**/*MySQL*" />
 </include>
```

最後の例は、複数の条件をinclude/excludeタグの属性に記述したものですが、これもANDとして扱われます。

```
<include executable="true" key="**/*MySQL*" />
```

ORは、複数のinclude/excludeタグに条件を含めるだけで記述できます。次のコードは、ファイル名に「.exe」または「.dll」を含むファイルを返します。

```
<include key="**/*.dll" />
 <include key="**/*.exe" />
```

評価の順序

ルール内での出現順序にかかわらず、まず、すべての「include」が処理されます。オブジェクト名がいずれかの「include」タグに合致すると、「exclude」タグと照合チェックされます。オブジェクト名がいずれかの「exclude」タグと合致すると、監視対象オブジェクトのセットから除外されます。

エンティティ属性

各エンティティには、監視対象となる属性のセットがあります。エンティティセットに属性が指定されていない (属性のラッパータグがない) 場合は、そのエンティティのSTANDARDセットの属性が使用されます (各"エンティティセット" on page 1018については、「簡略記法属性」セクションを参照してください)。

ただし、エンティティセットによっては、エンティティの特定の属性のみが変更監視の対象となります。たとえば、ログファイルの内容の変更は、通常、変更されることが前提として許可されています。しかし、アクセス許可や所有権の変更はレポートの対象にする必要があります。

エンティティセットの「attributes」タグには、こうしたことを記述できます。「attributes」タグには、監視対象とする属性を列挙したタグのセットを指定します。許可される「attribute」タグのセットの内容は、指定するエンティティセットによって異なります。

注意: 「attributes」タグが存在しても属性が指定されていない場合、ルールで定義されたエンティティが存在するかどうかだけが監視されます。

次の例は、「C:\Program Files\MySQL」ディレクトリ内でファイル名に「SQL」の文字列を含む実行ファイルについて、「last modified」、「permissions」、および「owner」の各属性に関する変更を監視します。

```
<FileSet base="C:\Program Files\MySQL" >
 <include key="**/*SQL*" executable="true"/>
 <attributes>
 <lastModified/>
 <permissions/>
 <owner/>
 </attributes>
 </FileSet>
```

次の例は、「C:\Program Files\MySQL」内のログファイルの「permissions」と「owner」の属性を監視します。

```
<FileSet base="C:\Program Files\MySQL" >
 <attributes>
 <permissions/>
 <owner/>
 </attributes>
 <include key="**/*.log" />
 </FileSet>
```

次の例は、属性のSTANDARDセットを監視します(後述の「簡略記法属性」を参照)。

```
<FileSet base="C:\Program Files\MySQL" >
 <include key="**/*.log" />
 </FileSet>
```

次の例では、監視対象となる属性がありません。エンティティの存在に関する変更のみが監視対象となります。

```
<FileSet base="C:\Program Files\MySQL" >
 <attributes/>
 <include key="**/*.log" />
 </FileSet>
```

簡略記法属性

簡略記法属性を使用すると、上位レベルの属性を1つ指定するだけで属性のグループを指定できます。通常の属性と同じく、許可される値のセットは、指定するエンティティセットによって異なります。

簡略記法属性が役に立つのは、属性のセットが自然にグループ化されている場合、属性のセットをすべて列挙することが煩雑な場合、および上位レベルの属性で表された属性のセットが時間とともにまたはシステム構成によって変わる可能性がある場合などです。各ケースの例を以下に示します。

属性	説明
STANDARD	エンティティセットを監視する属性のセット。これは、エンティティセットの「想定されるすべての属性」とは異なります。たとえば、想定されるすべてのハッシュアルゴリズムが含まれることはなく、必要とみなされる属性だけが含まれます。各"エンティティセット" on page 1018の「STANDARD」属性のリストについては、個々のエンティティセットのセクションを参照してください。
CONTENTS	ファイルの内容のハッシュまたはハッシュのセットを表す簡略記法属性です。SHA-1に初期設定されています。

onChange属性

変更をリアルタイムで監視するように、エンティティセットを設定できます。エンティティセットのonChange属性をtrue (初期設定値) に設定すると、エンティティセットによって返されるエンティティは、変更がリアルタイムで監視されます。変更が検出されると、すぐにそのエンティティがベースラインと比較されます。エンティティセットのonChange属性がfalseに設定されている場合は、ベースラインが作成されたとき、または予約タスク経由で、またはDeep Security Managerの要求に応じてトリガされたときにのみ実行されます。

次の例では、MySQLバイナリをリアルタイムで監視します。

```
<FileSet base="C:\Program Files\MySQL" onChange="true">
 <include key="**/*.exe"/>
 <include key="**/*.dll" />
 </FileSet>
```

環境変数

環境変数は、エンティティセットで使用されるベース値に含めることができます。環境変数は「${}」で囲みます。変数名の先頭に「env.」の文字列が付けられます。

次の例は、FileSetのベースディレクトリを、PROGRAMFILES環境変数に格納されたパスに設定します。

```
<FileSet base="${env.PROGRAMFILES}"/>
```

注意: 参照される環境変数の値は、Agentの起動時にDeep Security Agentによって読み取られ、保存されます。環境変数の値が変更されると、変更内容を登録するためにAgentが再起動されます。

参照先の環境変数が見つからない場合、その環境変数を参照しているエンティティセットは検索も監視もされませんが、それ以外の構成は使用されます。変数が存在しないことを示すアラートがトリガされます。Agentイベント「変更監視ルールのコンパイルの問題」を使用して、Agentが不正な環境変数を報告します。変更監視ルールのIDと環境変数名が、イベントのパラメータとして返されます。

変更監視で使用される初期設定の環境変数を次に示します。

名前	値
ALLUSERSPROFILE	C:\ProgramData
COMMONPROGRAMFILES	C:\Program Files\Common Files
PROGRAMFILES	C:\Program Files
SYSTEMDRIVE	C:

名前	値
SYSTEMROOT	C:\Windows
WINDIR	C:\Windows

環境変数のオーバーライド

Windows OSで非標準的なロケーションを使用するときに環境変数をオーバーライドします。たとえば、Windowsのhostsファイルに対する変更を監視する変更監視ルール「Microsoft Windows - 'Hosts' file modified」は、C:\WINDOWS\system32\drivers\etcフォルダ内のファイルを検索します。ただし、すべてのWindows環境に「C:\WINDOWS\」ディレクトリがあるわけではないため、変更監視ルールではWINDIR環境変数を使用して、このディレクトリを%WINDIR%\system32\drivers\etcと表記します。

注意: 環境変数は、主に、仮想マシンでAgentレスによる変更監視を実行するときにVirtual Applianceによって使用されます。これは、Virtual Applianceでは、特定の仮想マシンのOSが標準のディレクトリロケーションを使用しているかどうかを確認できないためです。

1. 環境変数をオーバーライドするコンピュータまたはポリシーエディタ[1]を開きます。
2. [設定]→[詳細]をクリックします。
3. [環境変数のオーバーライド]セクションで、[環境変数の表示]をクリックして[環境変数のオーバーライド]ページを表示します。
4. メニューバーで[新規]をクリックして新しい名前と値のペア(たとえばWINDIRとD:\Windows)を入力し、[OK]をクリックします。

レジストリ値

レジストリ値は、エンティティセットで使用されるベース値に含めることができます。レジストリ値は「${}」で囲みます。レジストリ値のパスの先頭には「reg.」が付けられます。次の例では、FileSetのベースディレクトリを、「HKLM \ Software \ Trend Micro \ Deep Security Agent \ InstallationFolder」レジストリ値に格納されているパスに設定します。

```
<FileSet base="${reg.HKLM\Software\Trend Micro\Deep Security Agent\InstallationFolder}"/>
```

参照先のレジストリ値は、Agentが新しいルールまたは変更されたルールを受信したときに読み込まれます。また、Agentは起動時にすべてのルールをチェックし、参照先のレジストリ値が変更されていた場合は、影響を受けるルールのベースラインを再構築します。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

参照先のレジストリ値が見つからない場合、その環境変数を参照しているエンティティセットは検索も監視もされませんが、それ以外の構成は使用されます。変数が存在しないことを通知するアラートが発令されます。Agentは、イベント8012を使用して環境変数の不正な変更を報告します。変更監視ルールのIDとレジストリ値のパスが、パラメータとしてイベントに提供されます。

注意: ワイルドカードは、ベース名の構造体の最後のコンポーネントにのみ使用できます。たとえば、「base="HKLM\Software\ATI*"」は有効で、「HKLM\Software\ATI」と「HKLM\Software\ATI Technologies」の両方を検出します。ただし、「base="HKLM*\Software\ATI*」は無効です。

「..」の使用

親ディレクトリへの参照を示す「..」符号は、Agentの現在のすべてのバージョンでサポートされるようになりました。Agentは、FileSetとDirectorySet要素のベースディレクトリ名の正規化を行いますが、このとき、「..」参照を解決し、Windowsの短い名前を長い名前に変換します。たとえば、Windowsの一部の新バージョンでは、次のFileSetのベースディレクトリは「C:\Users」です。以前バージョンのWindowsでは、ベースディレクトリは「C:\Documents and Settings」です。

```
<FileSet base="${env.USERPROFILE}\..">
 <include key="*/Start Menu/Programs/Startup/*"/>
 </FileSet>
```

ベストプラクティス

ルールは、重要なオブジェクトと属性のみを含めるように記述してください。こうすることで、オブジェクトの他の属性が変更されても、イベントは報告されなくなります。たとえば、変更監視ポリシーで「/bin」ディレクトリ内のファイルのアクセス権と所有権を制限することもできます。変更監視ルールは所有者、グループ、およびアクセス権を監視しますが、lastModifiedやハッシュ値などの属性は監視しません。

変更監視ルールを使用して、不正プログラムや不審なアクティビティの検出、サービスの監視、NTFSデータストリームの使用状況の監視、および通常の場所以外のディレクトリ(「/tmp」や「${env.windir}\temp」など) に置かれた実行可能ファイルの監視などを実施します。

ルールに含めるオブジェクトを指定する場合は、必ず、できるだけ詳細に指定してください。ルールに含めるオブジェクトが少ないほど、短期間でベースラインを作成でき、変更の検索にかかる時間も短くなります。変更される可能性のあるオブジェクトは除外し、監視する属性は必要なものだけに絞ります。

ルールを作成するときは、次のことは避けてください。

- **/..」、「C:\」、または「/などのディレクトリ階層の最上位で、「HKLM\Software
- 必要がないのに、データのハッシュの種類を複数使用すること。

- 参照先として、HKEY_CURRENT_USER、${env.USERPROFILE}、または${env.HOME} などのユーザ固有の場所を指定すること。

整合性監視ルール内のこれらの文は、指定されたパターンに一致するようにDeep Security Agentで多くの項目を検索するため、パフォーマンスに問題が発生します。

DirectorySet

注意: 変更監視モジュールは、Deep Security Agent上のディレクトリ、レジストリ値、レジストリキー、サービス、プロセス、インストール済みのソフトウェア、ポート、グループ、ユーザ、ファイル、およびWQLクエリ文に対する想定外の変更を検索します。変更監視を有効にして設定するには、"変更監視の設定" on page 1004を参照してください。

DirectorySetタグは、ディレクトリのセットを記述します。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

属性	説明	必須	初期設定値	設定できる値
base	DirectorySetのベースディレクトリを設定します。タグ内の他のエレメントはすべて、このディレクトリから相対的に位置付けられます。	はい	なし	文字列値は、構文的に有効なパスに変換されます (パスは存在しなくてもかまいません)。注意: UNCパスはWindows Agentで許可されますが、それには、リモートシステムでAgentコンピュータの「LocalSystem」アカウントからのアクセスが許可される必要があります。AgentはWindowsサービスの1つであり、LocalSystem (別名: NT AUTHORITY\SYSTEM) として実行されます。ネットワークリソースにアクセスするとき、LocalSystemは、コンピュータの資格情報であるDOMAIN\MACHINE*DOMAIN\MACHINE*$という名前のアカウントを使用します。リモートコンピュータに表示されるアクセストークンには、そのコンピュータの「Administrators」グループも含まれます。したがってリモート共有は、Agentのコンピュータアカウント、Agentのコンピュータの Administratorsグループ、または「Everyone」のいずれかに読み取り権限を付与する必要があります。UNCパスへのアクセスをテストするには、LocalSystemアカウントでWindowsコマンドプロンプトをサービスとして実行します。これで、ネットワークリソースやローカルリソースにアクセスしたり、LocalSystemアカウントで実行されるその他のアプリケーションを起動したりできます。

属性	説明	必須	初期設定値	設定できる値
				baseの値が構文的に有効でない場合は、FileSetは処理されません。それ以外の設定は評価されます。
onChange	対象のディレクトリをリアルタイムで監視する必要があるかどうかを示します。	いいえ	false	true、false
followLinks	このDirectorySetはシンボリックリンクを追跡します。	いいえ	false	true、false

エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。

- Created: ディレクトリの作成日時のタイムスタンプ
- LastModified: ディレクトリの最終アップデート日時のタイムスタンプ
- LastAccessed: ディレクトリの最終アクセス日時のタイムスタンプ。Windowsの場合、この値はすぐにアップデートされません。また、パフォーマンスを向上させるために、最終アクセス日時のタイムスタンプの記録を無効にすることができます。詳細については、File Timesを参照してください。LastAccessed属性には、ディレクトリ検索を実行するにはAgentがそのディレクトリを開く必要があり、これにより最終アクセス日時のタイムスタンプが変更されるという問題もあります。
- Permissions: Windowsの場合は、ディレクトリのセキュリティ記述子 (SDDL形式)。ACLをサポートするUNIXシステムの場合はPosixスタイルのACL。それ以外の場合は、数値 (8進数) 形式のUNIXスタイルのrwxrwxrwxのファイル権限。
- Owner: ディレクトリ所有者のユーザID (通常、UNIXでは「UID」と呼ばれます)
- Group: ディレクトリ所有者のグループID (通常、UNIXでは「GID」と呼ばれます)
- Flags: Windowsのみ。GetFileAttributes() Win32 APIで返されるフラグ。Windowsエクスプローラでは、これらをファイルの「属性」(読み取り専用、アーカイブ、圧縮など) とみなします。
- SymLinkPath: ディレクトリがシンボリックリンクである場合は、そのリンクのパスがここに格納されます。Windowsでは、SysInternalsの「junction」ユーティリティを使用して、シンボリックリンクに相当するWindows機能を作成します。
- InodeNumber (UNIX/Linuxのみ): ファイルに関連付けられているinodeが格納されるディスクのinode番号

- DeviceNumber(UNIX/Linuxのみ): ディレクトリに関連付けられているinodeが格納されるディスクのデバイス番号

簡略記法による属性

次に、簡略記法による属性と、それらがマッピングされる属性を示します。

- STANDARD:
  - Created
  - LastModified
  - Permissions
  - Owner
  - Group
  - Flags (Windowsのみ)
  - SymLinkPath

「key」の意味

keyは、「dir」で指定されたディレクトリを基準とする相対ディレクトリパスに対して照合されるパターンを指定します。このパターンは、「/」で区切られたパターンのセクションからなる階層型のパターンです。パターン内のセクションは、所定のOSのファイルのセパレータによって区切られたパスのセクションに対して照合されます。

サブエレメント

- Include
- Exclude

これらのエレメントに指定できる属性とサブエレメントの「include」と「exclude」の概要は、"変更監視 rules languages" on page 1017を参照してください。ここでは、このエンティティセットクラスに関連するincludeおよびexcludeに固有の情報のみを記載します。

FileSet

注意: 変更監視モジュールは、Deep Security Agent上のディレクトリ、レジストリ値、レジストリキー、サービス、プロセス、インストール済みのソフトウェア、ポート、グループ、ユーザ、ファイル、およびWQLクエリ文に対する想定外の変更を検索します。変更監視を有効にして設定するには、"変更監視の設定" on page 1004を参照してください。

FileSetタグは、ファイルのセットを記述します。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

属性	説明	必須	初期設定値	設定できる値
base	FileSetのベースディレクトリを設定します。タグ内の他のエレメントはすべて、このディレクトリから相対的に位置付けられます。	はい	なし	文字列値は、構文的に有効なパスに変換されます(パスは存在しなくてもかまいません)。注意: UNCパスはWindows Agentで許可されますが、それには、リモートシステムでAgentコンピュータの「LocalSystem」アカウントからのアクセスが許可される必要があります。AgentはWindowsサービスの1つであり、LocalSystem (別名: NT AUTHORITY\SYSTEM) として実行されます。ネットワークリソースにアクセスするとき、LocalSystemは、コンピュータの資格情報であるDOMAIN\MACHINE*DOMAIN\MACHINE*$という名前のアカウントを使用します。リモートコンピュータに表示されるアクセストークンには、そのコンピュータの「Administrators」グループも含まれます。したがってリモート共有は、Agentのコンピュータアカウント、AgentのコンピュータのAdministratorsグループ、または「Everyone」のいずれかに読み取り権限を付与する必要があります。UNCパスへのアクセスをテストするには、LocalSystemアカウントでWindowsコマンドプロンプトをサービスとして実行します。これで、ネットワークリソースやローカルリソースにアクセスしたり、LocalSystemアカウントで実行されるその他のアプリケーションを起動したりできます。 baseの値が構文的に有効でない場合は、FileSetは処理されません。それ以外の設定は評価されます。
onChange	対象のファイルをリアルタイムで監視する必要があるかどうかを示します。	いいえ	false	true、false
followLinks	このFileSetはシンボリックリンクを追跡し	いいえ	false	true、false

属性	説明	必須	初期設定値	設定できる値
	ます。			

エンティティセットの属性

次に示すFileSetの属性は、変更監視ルールによって監視可能な属性です。

注意: Linux環境のCreated、LastModified、およびLastAccessedの場合、リアルタイム変更監視モジュールは、ファイルの内容が変更された検索を検出しますが、ファイルの変更、ファイルの読み取り、またはその他の変更は検出しません。ファイルが変更された時間などのメタデータのみがアップデートされます。

- Created: ファイルの作成日時のタイムスタンプ
- LastModified: ファイルの最終アップデート日時のタイムスタンプ
- LastAccessed: ファイルの最終アクセス日時のタイムスタンプ。Windowsの場合、この値はすぐにアップデートされません。また、パフォーマンスを向上させるために、最終アクセス日時のタイムスタンプの記録を無効にすることができます。詳細については、File Timesを参照してください。LastAccessed属性には、ファイル検索を実行するにはAgentが対象のディレクトリを開く必要があり、これにより最終アクセス日時のタイムスタンプが変更されるという問題もあります。UNIXの場合、ファイルを開くときにO_NOATIMEフラグが使用可能であれば、Agentはこのフラグを使用します。これにより、最終アクセス日時のタイムスタンプがOSによってアップデートされることがなくなり、検索速度を上げることができます。
- Permissions: Windowsの場合は、ファイルのセキュリティ記述子 (SDDL形式)。ACLをサポートするUNIXシステムの場合はPosixスタイルのACL。それ以外の場合は、数値 (8進数) 形式のUNIXスタイルのrwxrwxrwxのファイル権限。
- Owner: ファイル所有者のユーザID (通常、UNIXでは「UID」と呼ばれます)
- Group: ファイル所有者のグループID (通常、UNIXでは「GID」と呼ばれます)
- Size: ファイルのサイズ
- Sha1: SHA-1ハッシュ
- Sha256: SHA-256ハッシュ
- Md5: MD5ハッシュ(非推奨)
- Flags: Windowsのみ。GetFileAttributes() Win32 APIで返されるフラグ。Windowsエクスプローラでは、これらをファイルの「属性」(読み取り専用、アーカイブ、圧縮など) とみなします。

- SymLinkPath(UNIX/Linuxのみ): ファイルがシンボリックリンクである場合は、そのリンクのパスがここに格納されます。Windows NTFSでは、UNIXライクなシンボリックリンクをサポートしますが、ファイルではなくディレクトリ専用です。Windowsのショートカットオブジェクトは OSでは処理されないため、本当の意味でのシンボリックリンクではありません。Windowsエクスプローラはショートカットファイル (*.lnk) を処理しますが、*.lnkファイルを開くその他のアプリケーションはlnkファイルのコンテンツの表示のみ行います。
- InodeNumber (UNIX/Linuxのみ): ファイルに関連付けられているinodeが格納されるディスクのinode番号
- DeviceNumber (UNIX/Linuxのみ): ファイルに関連付けられているinodeが格納されるディスクのデバイス番号
- BlocksAllocated (Linux/UNIXのみ): ファイルを格納するために割り当てられるブロック数。
- Growing: ファイルのサイズが検索間で同じままか増加する場合、値は「true」で、それ以外の場合は「false」です。これは主に、データが追加されたログファイルに役立ちます。ログファイルをローテーションオーバーすると、この属性が変更されることに注意してください。
- Shrinking: ファイルのサイズが同じであるか、検索間で減少している場合、値は「true」で、それ以外の場合は「false」です。

簡略記法による属性

次に、簡略記法による属性と、それらがマッピングされる属性を示します。

- CONTENTS: コンピュータエディタまたはポリシーエディタの[1] [変更監視]→[詳細] で設定されているコンテンツのハッシュアルゴリズム
- STANDARD: Created、LastModified、Permissions、Owner、Group、Size、Contents、Flags (Windowsのみ)、SymLinkPath (Linux/UNIXのみ)

ディレクトリとしてマウントされたドライブ

ディレクトリとしてマウントされたドライブは他のディレクトリと同様に扱われます。ただし、ネットワークドライブである場合、そのドライブは無視されます。

代替データストリーム

NTFSベースのファイルシステムでは、代替データストリームの概念がサポートされます。この機能が使用される場合には、代替ストリームは概念上、ファイル内のファイルのように動作します。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

注意: この機能のデモを実行するには、コマンドプロンプトに以下のコマンドを入力します。

```
echo plain > sample.txt
echo alternate > sample.txt:s
more < sample.txt
more < sample.txt:s
```

最初の「more」は、テキスト「plain」のみを表示します。これは、メモ帳などの標準のテキストエディタでファイルを開いた場合に表示されるテキストと同じです。2番目の「more」は、sample.txtの「s」ストリームにアクセスして文字列「alternate」を表示します。

FileSetでは、ストリームが指定されていない場合、すべてのストリームが含まれます。各ストリームは、ベースラインの個別のエンティティエントリです。ストリームに対して指定できる属性は次のとおりです。

- size
- Sha1
- Sha256
- Md5 (非推奨)
- Contents

次の例では、前のデモで使用したストリームが両方とも含まれます。

```
<include key="**/sample.txt" />
```

特定のストリームを含めたり除外したりするには、「:」表記を使用します。次の例では、メインのsample.txtストリームではなく、sample.txtの「s」ストリームのみが一致します。

```
<include key="**/sample.txt:s" />
```

パターン照合は、ストリーム表記でもサポートされます。次の例では、sample.txtが含まれますが、その代替ストリームはすべて除外されます。

```
<include key="**/sample.txt" />
 <exclude key="**/sample.txt:*" />
```

「key」の意味

keyは、「base」で指定されたディレクトリを基準とする相対ファイルパスに対して照合されるパターンを指定します。このパターンは、「/」で区切られたパターンのセクションからなる階層型のパターンです。パ

ターン内のセクションは、所定のOSのファイルのセパレータによって区切られたパスのセクションに対して照合されます。

サブエレメント

- Include
- Exclude

これらのエレメントに指定できる属性とサブエレメントの「include」と「exclude」の概要は、"変更監視 rules languages" on page 1017を参照してください。ここでは、FileSetエンティティセットクラスに関連するincludeおよびexcludeに固有の情報のみを記載します。

FileSetのincludeおよびexcludeに固有の属性

executable

ファイルが実行可能かどうかを決定します。これは、ファイルの権限がファイルの実行を許可していることを意味しません。ファイルの内容を確認するのではなく、プラットフォームに応じて、そのファイルが実行可能ファイルであるかどうかを決定します。

注意: これは、Agentがファイルを開き、ファイルの先頭から1KBまたは2KBを検証して有効な実行可能イメージヘッダを探すことが必要になるため、比較的負荷の高い処理です。1つ1つのファイルを開いて読み取ることは、ディレクトリを検索してワイルドカードパターンに基づいてファイル名を照合する処理に比較すると、非常に高い負荷がかかります。結果として、「executable」を使用するincludeおよびexcludeルールでは、この属性を使用しないルールよりも検索に時間がかかります。

GroupSet

注意: 変更監視モジュールは、Deep Security Agent上のディレクトリ、レジストリ値、レジストリキー、サービス、プロセス、インストール済みのソフトウェア、ポート、グループ、ユーザ、ファイル、およびWQLクエリ文に対する想定外の変更を検索します。変更監視を有効にして設定するには、"変更監視の設定" on page 1004を参照してください。

GroupSetはグループのセットを表します。これらはローカルグループのみです。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

属性	説明	必須	初期設定値	設定できる値
onChange	リアルタイムで監視するかどうかを示します。	いいえ	false	true、false

エンティティセットの属性

監視可能なエンティティの属性には次のものがあります。

- Description: (Windowsのみ) グループのテキストによる説明。
- Group: グループのIDと名前。グループ名はエンティティキーの一部ですが、グループの名前を変更した場合やグループに新しいIDを付けた場合に、グループのIDと名前のペアを監視できることが重要になります。通常、OSはIDに基づいてセキュリティを実施します。
- Members: グループメンバーのカンマ区切りのリスト。
- SubGroups: (Windowsのみ) グループのサブグループのカンマ区切りのリスト。

簡略記法による属性

- Standard: グループメンバーのサブグループ

「key」の意味

このkeyはグループの名前です。これは、階層型のエンティティセットではありません。パターンはグループ名のみに適用されます。結果として、「**」パターンは適用できません。次の例は、「Administrators」グループの追加と削除を監視します(「Member」属性はSTANDARDセットの一部であるため黙示的に含まれます。明確にリストされる属性はありません)。

```
<GroupSet>
 <include key="Administrators" />
 </GroupSet>
```

includeとexclude

これらのエレメントに指定できる属性とサブエレメントの「include」と「exclude」の概要は、"変更監視 rules languages" on page 1017を参照してください。

InstalledSoftwareSet

注意: 変更監視モジュールは、Deep Security Agent上のディレクトリ、レジストリ値、レジストリキー、サービス、プロセス、インストール済みのソフトウェア、ポート、グループ、ユーザ、ファイル、およびWQLクエリ文に対する想定外の変更を検索します。変更監視を有効にして設定するには、"変更監視の設定" on page 1004を参照してください。

インストールされたソフトウェアのセットを表します。インストールされたアプリケーションを一意に識別するために使用される「key」はプラットフォームに固有ですが、多くの場合、アプリケーション名の簡略名か一意の数値です。

Windowsでは、このkeyは「FogBugz Screenshot_is1」のように読んで意味のわかる形式か、「{90110409-6000-11D3-8CFE-0150048383C9}」のようなGUIDです。これらの値は、HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstallのサブキーで確認できます。

Linuxでは、このkeyはRPMパッケージ名であり、次のコマンドを入力すると表示されます。

```
rpm -qa --qf "%{NAME}\n"
```

Solarisでは、このkeyはパッケージ名であり、「pkginfo」コマンドを入力すると表示されます。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視が有効になっているコンピュータの属性ではありません。

属性	説明	必須	初期設定値	設定できる値
onChange	リアルタイムで監視するかどうかを示します。	いいえ	false	true、false

エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。エンティティの属性の有無は、プラットフォームとアプリケーション自体の両方に依存します。インストールプログラムが、すべての属性の値を設定する必要はありません。

- Manufacturer: アプリケーションの発行元または製造元
- Name: アプリケーションのフレンドリ名または表示名。Linuxでは使用できません。
- InstalledDate: インストールの日付。これは通常、YYYY-MM-DD [HH:MM:SS],]として返されますが、Windowsの多くのインストーラは日付文字列を別の方法でフォーマットします。この形式は保証されません。(AIX.)では使用できません。
- InstallLocation: アプリケーションがインストールされるディレクトリ。(WindowsおよびSolarisでのみ利用可能です)
- Parent: パッチおよびアップデートの場合、このアイテムの親のkey名を示します。(Windowsでのみ利用可能です。)
- Size: 利用可能な場合、アプリケーションの推定サイズ。Windowsでは、この属性は「HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*」の下の「EstimatedSize」レジストリ値から読み込まれます。その場所の値はKB単位で表されるため、

Agentでは1024を掛けてから値を返します。すべてのWindowsアプリケーションで、レジストリのEstimatedSizeフィールドに値が設定されるわけではありません。(AIX.)では使用できません。

- Version: インストールされたアプリケーションのバージョン。Windowsでは、これは「DisplayVersion」レジストリ値に基づいています。

簡略記法による属性

次に、エンティティの簡略記法による属性と、解釈される属性を示します。

- STANDARD: InstalledDate、Name、Version

「key」の意味

keyは、インストールされたソフトウェアの名前です。階層型のキーではないため、**パターンは適用できません。Windowsでは、多くの場合、このkeyはGUIDです(特に、Windowsインストーラ(別名MSI)を使用してインストールされたソフトウェアの場合)。GUIDではなく表示名に基づいてincludeまたはexcludeを実行する必要がある場合は、name="XXX"機能を使用します。

次の例では、新しいソフトウェアの追加および削除を監視します。

```
<InstalledSoftwareSet>
 <include key="*"/>
 <attributes/>
 </InstalledSoftwareSet>
```

サブエレメント

- Include
- Exclude

これらのエレメントに指定できる属性とサブエレメントの「include」と「exclude」の概要は、"変更監視 rules languages" on page 1017を参照してください。ここでは、このエンティティセットクラスに関連するincludeおよびexcludeに固有の情報のみを記載します。

InstalledSoftwareSetsのincludeおよびexcludeに固有の属性

name (Windowsのみ)

エンティティの「name」属性であるアプリケーション表示名に対して、?および*を使用するワイルドカード照合を実行できます。たとえば、次のとおりです。

```
<InstalledSoftwareSet>
 <include name="Microsoft*"/>
 <InstalledSoftwareSet>
```

コントロールパネルに表示される表示名が、「Microsoft」で始まるインストール済みアプリケーションすべてに一致します。

manufacturer

アプリケーションの発行元または製造元に対して、?および*を使用するワイルドカード照合を実行できます。たとえば、次のとおりです。

```
<InstalledSoftwareSet>
 <include manufacturer="* Company "/>
 <InstalledSoftwareSet>
```

マニファクチャが「 Company 」で終了するインストール済みアプリケーションすべてに一致します。

PortSet

注意: 変更監視モジュールは、Deep Security Agent上のディレクトリ、レジストリ値、レジストリキー、サービス、プロセス、インストール済みのソフトウェア、ポート、グループ、ユーザ、ファイル、およびWQLクエリ文に対する想定外の変更を検索します。変更監視を有効にして設定するには、"変更監視の設定" on page 1004を参照してください。

待機ポートのセットを表します。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

属性	説明	必須	初期設定値	設定できる値
onChange	リアルタイムで監視するかどうかを示します。	いいえ	false	true、false

エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。

- Created: (Windowsのみ - XP SP2以降およびServer 2003 SP1以降)Windows APIのGetExtendedTcpTable() 関数またはGetExtendedUdpTable() 関数によって返されます。このTCPまたはUDPリンクが作成されたバインド処理の発生時刻を示します。

- Listeners: プロトコル、IPアドレス、ポート番号の組み合わせにおけるアクティブなリスナーの数です。指定されたポートにバインドされているソケットと待機中のソケットの数が反映されます。この数は、プロセスがポートに複数のソケットをバインドしている場合、ポートを待機しているプロセスの数より大きくなることがあります。指定されたポートにバインドされているソケットが1つだけの場合、この属性の値はありません。
- パス: (Windowsのみ - XP SP2 +およびServer 2003 SP1 +が必要です) ポートを所有するモジュールのフルパスを示します (存在する場合)。Windowsでは、このパスは、Windows APIのGetOwnerModuleFromXxxEntry() 関数から取得されます。Microsoftのドキュメントでは、接続テーブルエントリを所有者モジュールとして解釈することが推奨されています。
- Process: (Windowsのみ - XP SP2以降およびServer 2003 SP1以降)ポートを所有するモジュールの短い名前を示します (存在する場合)。Windowsでは、このパスは、Windows APIのGetOwnerModuleFromXxxEntry() 関数から取得されます。Microsoftのドキュメントでは、接続テーブルエントリを所有者モジュールとして解釈することが推奨されています。まれに、返された所有者のモジュール名が、「svchost.exe」などのプロセス名、「RPC」などのサービス名、「timer.dll」などのコンポーネント名である場合があります。
- ProcessId: (Windowsのみ - XP SP2以降およびServer 2003 SP1以降)このポートのバインドを発行したプロセスのPIDを示します。
- User: (Linuxのみ)ポートを所有するユーザを示します。

「key」の意味

このkeyは、次の形式をとります。

<PROTOCOL>/<IP ADDRESS>/<PORT>

たとえば、次のとおりです。

```
tcp/172.14.207.94/80
 udp/172.14.207.94/68
```

IPV6

IPアドレスがIPv6である場合、keyも同じ形式になりますが、プロトコルはTCP6またはUDP6です。このIPアドレスは、getnameinfoコマンドによって返される、次のようなIPv6表記となります。

```
tcp6/3ffe:1900:4545:3:200:f8ff:fe21:67cf/80
 udp6/3ffe:1900:4545:3:200:f8ff:fe21:67cf/68
```

「key」の照合

これは、階層型のキーではないため、**は適用できません。*および?を使用するUNIX形式のglob照合は可能です。次のパターンは、72.14.207.90 ~ 72.14.207.99のIPアドレスのポート80に一致します。

```
*/72.14.207.9?/80
```

次のパターンは、72.14.207.2、72.14.207.20 ~ 72.14.207.29および72.14.207.200 ~ 72.14.207.255のIPアドレスのポート80に一致します。

```
*/72.14.207.2*/80
```

次のパターンは、任意のIPアドレスのポート80に一致します。

```
*/80
```

次の例では、待機ポートにおける変更を監視しますが、IPv4およびIPv6のTCPのポート80は無視します。

```
<PortSet>
 <include key="*"/>
 <exclude key="tcp*/*/80"/>
 </PortSet>
```

サブエレメント

- Include
- Exclude

これらのエレメントに指定できる属性とサブエレメントの「include」と「exclude」の概要は、"変更監視 rules languages" on page 1017を参照してください。ここでは、このエンティティセットクラスに関連するincludeおよびexcludeに固有の情報のみを記載します。

PortSetのincludeおよびexcludeに固有の属性

これ以外にも、ポートの各種の属性をincludeおよびexcludeでの監視機能で使用できます。これらの監視では、値とポートの属性値を比較します。各種属性のプラットフォームサポートに注意してください。すべての属性がプラットフォーム間またはプラットフォームリビジョン間で利用可能であるとはかぎりません。したがって、includeおよびexcludeタグを使用したこれらの監視の使用は制限されます。監視機能では、UNIXのglob形式のワイルドカードである「*」および「?」がサポートされ、パスのセパレータまた

はその他の文字の正規化は実行されません。監視機能は、属性の値に対する、単純なglob形式のパターン照合です。

Path

ポートのpath属性に対する、ワイルドカード一致をチェックします。次の例では、メインのIISバイナリを実行するプロセスによって所有されているポートを監視します。

```
<PortSet>
 <include path="*\system32\inetsrv\inetinfo.exe"/>
 </PortSet>
```

Process

ポートのprocess属性に対する、ワイルドカード一致をチェックします。次の例では、svchost.exeまたはoutlook.*バイナリを実行するプロセスによって所有されているポートを監視します。

```
<PortSet>
 <include process="svchost.exe"/>
 <include process="outlook.*"/>
 </PortSet>
```

User

ポートのuser属性に対する、ワイルドカード一致をチェックします。次の例では、スーパーユーザ (root) によって所有されていたUNIXシステム上のポートを監視します。

```
<PortSet>
 <include user="root"/>
 </PortSet>
```

ProcessSet

注意: 変更監視モジュールは、Deep Security Agent上のディレクトリ、レジストリ値、レジストリキー、サービス、プロセス、インストール済みのソフトウェア、ポート、グループ、ユーザ、ファイル、およびWQLクエリ文に対する想定外の変更を検索します。変更監視を有効にして設定するには、"変更監視の設定" on page 1004を参照してください。

プロセスのセットを表します。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

属性	説明	必須	初期設定値	設定できる値
onChange	リアルタイムで監視するかどうかを示します。	いいえ	false	true、false

エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。

- CommandLine:「ps -f」(UNIX)、「ps w」(Linux)、またはProcess Explorer (Windows) によって表示される完全なコマンドライン。
- グループ: プロセスが実行されているグループ。
  - UNIXでは、「有効な」プロセスグループIDです。プロセスグループIDは、共有リソースのアクセス権と、場合によってはファイルのアクセス権を決定します。グループIDは、プロセスの権限喪失や有効なグループの資格情報の変更などで変わる場合があります。たとえば、プログラムでは、ユーザが読み取り専用権限しか持たないディレクトリにインストールファイルをコピーするために、一時的にグループIDを変更し、そのディレクトリへの書き込み権限を取得することができます。
  - Windowsでは、「現在の」プロセスのプライマリグループであり、ログイン時に作成されるユーザ固有のアクセストークンによって確立されます。アクセストークンは、ユーザとユーザが実行するプロセスのアクセス権とリソース権限を設定します。

    注意: Windowsのプロセスには、通常、プライマリグループ以外にも1つ以上のグループ資格情報が関連付けられています。これらの追加のグループ資格情報は、Agentでは監視されません。これらの情報は、Process Explorerにあるプロセスプロパティの「セキュリティ」タブで表示できます。
- Parent: このプロセスを作成したプロセスのPID。
- Path:プロセスのバイナリへのフルパス。Windowsでは、このパスは、GetModuleFileNameEx() APIから取得されます。LinuxおよびSolaris 10では、/proc/{pid}/exe または /proc/{pid}/path/a.out のシンボリックリンクをそれぞれ読むことになります。(Solaris 9およびAIX.)では使用できません。
- Process: プロセスバイナリの短い名前 (パスを含まない名前)。たとえば、「c:\windows\notepad.exe」の場合は「notepad.exe」であり、「/usr/local/bin/httpd」の場合は「httpd」です。
- Threads:プロセス内で現在実行中のスレッドの数。

- User: プロセスが実行されているユーザ。UNIXでは、プロセスの「有効な」ユーザIDです。このユーザIDは、時間とともにプロセスが権限を破棄するか、またはプロセスが有効なユーザ資格情報を切り替えた場合に、変更されることがあります。

簡略記法による属性

- STANDARD: CommandLine、Group、Parent、Path (利用可能な場合)、Process、User

「key」の意味

keyは、実行可能ファイルの短い名前である「Process」属性と、PIDを組み合わせたものです。PIDは、名前とパスのセパレータの後に追加されます。たとえば、Windowsではnotepad.exe\1234、UNIXではhttpd/1234となります。パスのセパレータを使用することで、key="abc/*"のincludeまたはexclude照合が期待どおりに動作するようになります。

サブエレメント

- Include
- Exclude

これらのエレメントに指定できる属性とサブエレメントのincludeの概要は、"変更監視 rules languages" on page 1017を参照してください。ここでは、このエンティティセットクラスに関連するincludeおよびexcludeに固有の情報のみを記載します。

ProcessSetsのincludeおよびexcludeに固有の属性

次の例は、PIDに関係なく、notepad.exeで実行中のプロセスセットを監視します。

```
<ProcessSet>
<include key="notepad.exe\*" />
</ProcessSet>
```

これ以外にも、プロセスの各種の属性をincludeおよびexcludeでの監視機能で使用できます。監視機能では、UNIXのglob形式のワイルドカードである「*」および「?」がサポートされ、パスのセパレータまたはその他の文字の正規化は実行されません。監視機能は、属性の値に対する、単純なglob形式のパターン照合です。

CommandLine

プロセスのcommandLine属性に対する、ワイルドカード一致をチェックします。次の例では、コマンドラインが「*httpd *」に一致するプロセスが監視されます。

```
<ProcessSet>
<include commandLine="*httpd *" />
</ProcessSet>
```

Group

プロセスのgroup属性に対する、ワイルドカード一致をチェックします。数値形式ではなく、テキスト形式のグループ名が使用されます。Linuxでデーモングループをテストするには、「2」ではなく「daemon」を使用します。次の例では、root、daemon、lpのいずれかのグループとして実行されるプロセスを監視します。

```
<ProcessSet>
<include group="root" />
<include group="daemon" />
<include group="lp" />
</ProcessSet>
```

Path

プロセスのpath属性に対する、ワイルドカード一致をチェックします。path属性は、一部のプラットフォームでは使用できません。次の例では、System32の下にバイナリがあるプロセスを監視します。

```
<ProcessSet>
<include path="*\System32\*" />
</ProcessSet>
```

User

プロセスのuser属性に対する、ワイルドカード一致をチェックします。数値形式ではなく、テキスト形式のユーザ名が使用されます。UNIXでスーパーユーザをチェックするには、「0」ではなく「root」を使用します。次の例では、NT AUTHORITY\SYSTEM、NT AUTHORITY\LOCAL SERVICE、NT AUTHORITY\NETWORK SERVICEなど、組み込みのシステムユーザとして実行される任意のプロセスを監視します。

```
<ProcessSet>
<include user="NT AUTHORITY\*" />
</ProcessSet>
```

RegistryKeySet

注意: 変更監視モジュールは、Deep Security Agent上のディレクトリ、レジストリ値、レジストリキー、サービス、プロセス、インストール済みのソフトウェア、ポート、グループ、ユーザ、ファイル、および

WQLクエリ文に対する想定外の変更を検索します。変更監視を有効にして設定するには、"変更監視の設定" on page 1004を参照してください。

RegistryKeySetタグは、レジストリ内のセットキーを記述します(Windowsのみ)。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

属性	説明	必須	初期設定値	設定できる値
base	RegistryKeySetのベースキーを設定します。タグ内の他のエレメントはすべて、このキーから相対的に位置付けられます。ベースは、次のいずれかのレジストリブランチ名で始まる必要があります。 HKEY_CLASSES_ROOT (またはHKCR)、 HKEY_LOCAL_MACHINE (またはHKLM)、 HKEY_USERS (またはHKU)、 HKEY_CURRENT_CONFIG (またはHKCC)	はい	なし	構文的に有効なレジストリキーパスに解釈される文字列値

エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。

- Owner
- Group
- Permissions
- LastModified (Windowsレジストリでは「LastWriteTime」と呼ばれます)
- Class
- SecurityDescriptorSize

簡略記法による属性

- STANDARD: Group、Owner、Permissions、LastModified

「key」の意味

レジストリキーは、ファイルシステム内のディレクトリのように、レジストリ内に階層的に格納されています。この言語では、キーに対する「キーパス」は、ディレクトリに対するパスのようなものだとみなされています。たとえば、エージェントの「Deep Security Agent」キーへの「キーパス」は次のようになります。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\Deep Security Agent
```

このキーパスに対して、RegistryValueSetのincludeおよびexcludeの「キー」値が照合されます。このパターンは、「/」で区切られたパターンのセクションからなる階層型のパターンであり、「/」で区切られたキーパスのセクションに対して照合されます。

サブエレメント

- Include
- Exclude

これらのエレメントに指定できる属性とサブエレメントのincludeの概要は、"変更監視 rules languages" on page 1017を参照してください。

RegistryValueSet

注意: 変更監視モジュールは、Deep Security Agent上のディレクトリ、レジストリ値、レジストリキー、サービス、プロセス、インストール済みのソフトウェア、ポート、グループ、ユーザ、ファイル、およびWQLクエリ文に対する想定外の変更を検索します。変更監視を有効にして設定するには、"変更監視の設定" on page 1004を参照してください。

レジストリ値のセットです (Windowsのみ)。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

属性	説明	必須	初期設定値	設定できる値
base	RegistryValueSetのベースキーを設定します。タグ内の他のエレメントはすべて、このキーから相対的に位置付けられます。ベースは、レジストリブランチ名で始まる必要があります。 HKEY_CLASSES_ROOT (またはHKCR)、 HKEY_LOCAL_MACHINE (またはHKLM)、 HKEY_USERS (またはHKU)、 HKEY_CURRENT_CONFIG (またはHKCC)	はい	なし	構文的に有効なレジストリキーに解釈される文字列値

エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。

- Size
- Type
- Sha1
- Sha256
- Md5 (非推奨)

簡略記法による属性

- CONTENTS: コンピュータエディタまたはポリシーエディタの[1] [変更監視]→[詳細] で設定されているコンテンツのハッシュアルゴリズム
- STANDARD: Size、Type、Contents

「key」の意味

レジストリ値は、レジストリ内のキーに格納されている名前/値のペアです。レジストリ値が格納されているキーは、さらに別のキーに格納されている場合があります。これは、ファイルシステム内でのディレクトリとファイルの関係によく似ています。この表記法では、値に対する「キーパス」は、ファイルに対するパスのようなものです。たとえば、AgentのInstallationFolder値への「キーパス」は、次のようになります。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\Deep Security Agent\InstallationFolder
```

このキーパスに対して、RegistryValueSetのincludeおよびexcludeの「キー」値が照合されます。このパターンは、「/」で区切られたパターンのセクションからなる階層型のパターンであり、「/」で区切られたキーパスのセクションに対して照合されます。

初期設定値

各レジストリキーには、不特定の値 (初期設定値) があります。

パターンの末尾に「/」を使用することで、この値を含める/除外することを明示的に指定できます。たとえば、「**/」は、下位の不特定の値すべてに対して照合され、「*Agent/**/」は、「*Agent」に一致するキーの不特定の値すべてに対して照合されます。

注意: レジストリ値の名前には、引用符、バックスラッシュ、「@」記号など、任意の文字が含まれている可能性があります。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

Agentは、これらの文字がエンティティのキー名に含まれている場合、バックスラッシュをエスケープ記号として使用して対処しますが、この処理によってエスケープされるのはバックスラッシュ自体だけです。このように処理されるのは、バックスラッシュを含む値名と、レジストリパスの一部として使用されているバックスラッシュを区別できるようにするためです。つまり、バックスラッシュで終了する値名は、初期設定/不特定の値に対して一致するように設計されたルールと一致することになります。

次の表に、レジストリ値の名前と生成されるエンティティキーの例を示します。

値	エスケープ形式	例
Hello	Hello	HKLM\Software\Sample\Hello
"Quotes"	"Quotes"	HKLM\Software\Sample\"Quotes"
back\slash	back\\slash	HKLM\Software\Sample\back\\slash
trailing\	trailing\\	HKLM\Software\Sample\trailing\\
		HKLM\Software\Sample\
@	@	HKLM\Software\Sample\@

サブエレメント

- Include
- Exclude

これらのエレメントに指定できる属性とサブエレメントの「include」と「exclude」の概要は、"変更監視 rules languages" on page 1017を参照してください。

ServiceSet

注意: 変更監視モジュールは、Deep Security Agent上のディレクトリ、レジストリ値、レジストリキー、サービス、プロセス、インストール済みのソフトウェア、ポート、グループ、ユーザ、ファイル、およびWQLクエリ文に対する想定外の変更を検索します。変更監視を有効にして設定するには、"変更監視の設定" on page 1004を参照してください。

ServiceSetエレメントは、サービスのセットを表します(Windowsのみ)。サービスは、「サービス名」によって識別されます。このサービス名は、サービスの管理ツールに表示される「name」列の値と同じものではありません。サービス名は、サービスのプロパティで確認することができます。多くの場合、「name」列に表示される値よりも短い名前です(この値は、実際にはサービスの「表示名」です)。たとえば、エージェントのサービス名は「ds_agent」で、表示名は「Trend Micro Deep Security Agent」です。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

属性	説明	必須	初期設定値	設定できる値
onChange	リアルタイムで監視するかどうかを示します。	いいえ	false	true、false

エンティティセットの属性

次に示すエンティティの属性は、変更監視ルールによって監視可能な属性です。

- Permissions: SDDL形式のサービスのセキュリティ記述子
- Owner: サービスの所有者のユーザID
- Group: サービスの所有者のグループID
- BinaryPathName: Windowsがサービスの開始に使用するパスと、省略可能なコマンドライン引数
- DisplayName: サービスの「プロパティ」パネルに表示されるサービスの「表示名」。
- Description: 「サービス」パネルに表示される説明
- State: サービスの現在の状態。次のいずれかです: stopped、starting、stopping、running、continuePending、pausePending、paused
- StartType: サービスの開始方法。次のいずれかです: automatic、disabled、manual
- LogOnAs: サービスプロセスの実行時にサービスプロセスにログオンするアカウントの名前。
- FirstFailure: サービスがはじめて失敗したときに実行される処理。形式は「delayInMsec,action」で、処理はNone、Restart、Reboot、RunCommandのいずれかです。
- SecondFailure: サービスが2回目に失敗したときに実行される処理。形式は「delayInMsec,action」で、処理はNone、Restart、Reboot、RunCommandのいずれかです。
- SubsequentFailures: サービスが3回目以降に失敗したときに実行される処理。形式は「delayInMsec,action」で、処理はNone、Restart、Reboot、RunCommandのいずれかです。
- ResetFailCountAfter: 失敗がない場合に、失敗カウントをゼロにリセットするまでの時間 (秒単位)
- RebootMessage: 「Reboot」サービスコントローラ処理に対する応答として、サーバのユーザにブロードキャスト配信されるメッセージ
- RunProgram: 「RunCommand」サービスコントローラ処理に対する応答として実行されるプロセスの完全なコマンドライン
- DependsOn: サービスが依存しているコンポーネントのカンマ区切りのリスト
- LoadOrderGroup: このサービスが属しているロード順序グループ。システムのスタートアッププログラムは、ロード順序グループを使用して、他のグループに対して指定された順序どおりにサービスのグループをロードします。ロード順序グループは、レジストリ値HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ServiceGroupOrderに含まれています。

- ProcessId: サービスをホストするプロセスの数値ID。1個のWindowsプロセスに多数のサービスが存在する可能性がありますが、独自のプロセスで実行されるサービスについては、この属性を監視することで、サービスの再起動をログに記録することができます。

簡略記法による属性

次に、エンティティの簡略記法による属性と、解釈される属性を示します。

- STANDARD: Permissions、Owner、Group、BinaryPathName、Description、State、StartType、LogOnAs、FirstFailure、SecondFailure、SubsequentFailures、ResetFailCountAfter、RunProgram、DependsOn、LoadOrderGroup、ProcessId

「key」の意味

keyはサービスの名前であり、サービスの管理ツールに表示される「name」列と同じである必要はありません (サービスの管理ツールには、サービスの「表示名」が表示されます)。サービス名は、サービスのプロパティで確認することができます。多くの場合、「name」列に表示される値よりも短い名前です。

注意: これは、階層型のエンティティセットではありません。パターンはサービス名のみに適用されます。結果として、**パターンは適用できません。

サブエレメント

- Include
- Exclude

これらのエレメントに指定できる属性とサブエレメントのincludeの概要は、"変更監視 rules languages" on page 1017を参照してください。ここでは、このエンティティセットクラスに関連するincludeおよびexcludeに固有の情報のみを記載します。

ServiceSetのincludeおよびexcludeに固有の属性

state

サービスの状態である、stopped、starting、stopping、running、continuePending、pausePending、pausedのいずれかに基づいたincludeまたはexclude。次の例では、実行中のサービスセットの変更について監視します。

```
<ServiceSet>
 <include state="running"/>
 </ServiceSet>
```

UserSet

注意: 変更監視モジュールは、Deep Security Agent上のディレクトリ、レジストリ値、レジストリキー、サービス、プロセス、インストール済みのソフトウェア、ポート、グループ、ユーザ、ファイル、およびWQLクエリ文に対する想定外の変更を検索します。変更監視を有効にして設定するには、"変更監視の設定" on page 1004を参照してください。

UserSetエレメントはユーザのセットを表します。Windowsシステムでは、このシステムはローカルのユーザ(「ローカルユーザとグループ」のMMCスナップインによって表示されるユーザと同じユーザ)で動作します。Deep Security Agentがドメインコントローラ以外で実行されている場合にのみ、*ローカル*ユーザであることに注意してください。ドメインコントローラでは、UserSet要素はすべてのドメインユーザを列挙しますが、極端に大きなドメインに対しては推奨されません。

UNIXシステムの場合、監視されるユーザは「getpwent_r()」APIおよび「getspnam_r()」APIで返すように設定されたユーザです。AIXシステムでは、監視対象のユーザは `/etc/passwd` ファイルにリストされています。

タグ属性

次に示すXML属性はタグ自体の属性であり、変更監視ルールによって監視されるエンティティの属性ではありません。

属性	説明	必須	初期設定値	設定できる値
onChange	リアルタイムで監視するかどうかを示します。	いいえ	false	true、false

エンティティセットの属性

監視可能なエンティティの属性には次のものがあります。

一般属性

- cannotChangePassword: ユーザにパスワードの変更が許可されているかどうかをtrueまたはfalseで示す。
- disabled: アカウントが無効になっているかどうかをtrueまたはfalseで示す。Windowsシステムでは、これはユーザの「無効」チェックボックスを反映します。UNIXシステムでは、ユーザのアカウントが期限切れの場合、またはパスワードが期限切れで変更の猶予期間が経過してしまった場合、これはtrueになります。
- fullName: ユーザの表示名。
- groups: ユーザの所属するグループのカンマ区切りのリスト。
- homeFolder: ホームフォルダまたはホームディレクトリへのパス。

- lockedOut: ユーザが明確に、またはパスワードの失敗回数超過によって、ロックされているかどうかをtrueまたはfalseで示す。
- passwordHasExpired: ユーザのパスワードが期限切れかどうかをtrueまたはfalseで示す。Windowsの場合、この属性はWindows XP以降のOSでのみ使用できます
- passwordLastChanged: 前回ユーザのパスワードが変更された日時のタイムスタンプ。これはDeep Security Agentによって、UTC 1970年1月1日以降のミリ秒数として記録されます。Deep Deep Security Managerは、この値に基づいてローカルタイムでタイムスタンプをレンダリングします。Unixプラットフォームでは、この属性の解決は1日であるため、レンダリングされたタイムスタンプの時間コンポーネントは無意味です。(AIXではサポートされていません) 。
- passwordNeverExpires: 期限切れにならないパスワードかどうかをtrueまたはfalseで示す。
- user: OSが認識しているユーザ名。たとえば、「Administrator」や「root」があります。

Windowsのみの属性

- description: ユーザが所属するプライマリグループ。
- homeDriveLetter: ユーザのホームフォルダとしてネットワーク共有がマッピングされているドライブの文字。
- logonScript: ユーザがログインするたびに実行されるスクリプトへのパス。
- profilePath: ローミングまたは必須のWindowsユーザプロファイルが使用されている場合のネットワークパス。

Linux、AIX、およびSolarisの属性

- group: ユーザが所属するプライマリグループ。
- logonShell: ユーザのシェルプロセスへのパス。
- passwordExpiredDaysBeforeDisabled: ユーザのパスワードが期限切れになり、アカウントが無効になってからの日数Solarisでは、この属性は、ユーザが無効になるまでの非アクティブな日数を示します。(AIX.)ではサポートされていません
- passwordExpiry: ユーザのアカウントが期限切れになり、アカウントが無効になる日付。
- passwordExpiryInDays: ユーザのパスワードを変更しなくてはならない日までの残り日数。
- passwordMinDaysBetweenChanges: パスワードを変更してから次に変更するまでの最小日数。
- passwordWarningDays: ユーザのパスワードが期限切れになる前に警告を表示する日付。

簡略記法による属性

- 標準:
  - cannotChangePassword
  - disabled
  - groups
  - homeFolder
  - passwordHasExpired
  - passwordLastChanged
  - passwordNeverExpires
  - user
  - logonScript (Windowsのみ)
  - profilePath (Windowsのみ)
  - group (Linuxのみ)
  - logonShell (Linuxのみ)
  - passwordExpiryInDays (Linuxのみ)
  - passwordMinDaysBetweenChanges (Linuxのみ)

「key」の意味

このkeyはユーザ名です。これは階層型のEntitySetではありません。パターンはユーザ名のみに適用されます。結果として、「**」パターンは適用できません。

次の例は、任意のユーザの作成と削除を監視します(属性は明確に除外されるので、グループメンバーシップは監視対象にはなりません)。

```
<UserSet>
 <Attributes/>
 <include key="*" />
 </UserSet>
```

次の例では、「jsmith」アカウントの追加および削除の監視に加え、アカウントのSTANDARD属性に対する変更の監視も行います(特定の属性リストが含まれていない場合、このEntitySetのSTANDARDセットが自動的に含められるためです)。

```
<UserSet>
 <include key="jsmith" />
 </UserSet>
```

サブエレメント

includeとexclude

これらのエレメントに指定できる属性とサブエレメントのincludeの概要は、"変更監視 rules languages" on page 1017を参照してください。

UserSetのincludeおよびexcludeに固有の属性

これ以外にも、ユーザの各種の属性をincludeおよびexcludeでの監視機能で使用できます。これらの監視では、値とユーザの属性値を比較します。各種属性のプラットフォームサポートに注意してください。すべての属性がプラットフォーム間またはプラットフォームリビジョン間で利用可能であるとはかぎりません。したがって、includeおよびexcludeエレメントを使用したこれらの監視の使用は制限されます。監視機能では、UNIXのglob形式のワイルドカードである「*」および「?」がサポートされ、パスのセパレータまたはその他の文字の正規化は実行されません。監視機能は、属性の値に対する、単純なglob形式のパターン照合です。

- Disabled: ユーザの無効な属性に対する、trueまたはfalse一致。次の例は、プライマリグループに「user」または「daemon」のいずれかがあるユーザを監視します。

```
<UserSet>
 <include disabled="true"/>
 </UserSet>
```

- Group: ユーザのgroup属性に対する、ワイルドカード一致。この監視はUNIXシステムにのみ適用できます。次の例は、プライマリグループに「user」または「daemon」のいずれかがあるユーザを監視します。

```
<UserSet>
 <include group="users"/>
 <include group="daemon"/>
 </UserSet>
```

- LockedOut: ユーザのlockedOut属性に対する、trueまたはfalse一致。
- PasswordHasExpired: ユーザのpasswordHasExpired属性に対する、trueまたはfalse一致。
- PasswordNeverExpires: ユーザのpasswordNeverExpires属性に対する、trueまたはfalse一致。

WQLSet

注意: 変更監視モジュールは、Deep Security Agent上のディレクトリ、レジストリ値、レジストリキー、サービス、プロセス、インストール済みのソフトウェア、ポート、グループ、ユーザ、ファイル、および

WQLクエリ文に対する想定外の変更を検索します。変更監視を有効にして設定するには、"変更監視の設定" on page 1004を参照してください。

WQLSetエレメントは、Windows Management Instrumentation WQLクエリ文の結果セットについて記述します。WQLは、さまざまなオブジェクトクラスに対してSQLに似たクエリを実行し、その結果について、各行にオブジェクト、各列にオブジェクトの特定属性値を格納した表の形式で返します。

注意: WMIクエリの多くは、時間とコンピュータリソースを大量に消費します。完了まで数分かかり何千行もの結果を返すクエリを、不注意で実行してしまうことがあります。WQLSetで使用する前に、すべてのクエリをPowerShellやWMI Explorerなどのプログラムを使用してテストすることを強く推奨します。

属性	説明	必須	初期設定値	設定できる値
namespace	WMIクエリの名前空間を設定します。	はい	なし	有効なWMI名前空間を表す文字列値。 WindowsOSのオブジェクトをテストする場合に最もよく使用される名前空間は「root\cimv2」ですが、「root\directory\LDAP」や「root\Microsoft\SqlServer\ComputerManagement」など、その他の名前空間も使用できます。指定したコンピュータで使用可能なWMI名前空間を列挙する「GetNamespaces.vbs」という短いスクリプトについては、ここを参照してください。
wql	WQLクエリ文字列。	はい	なし	有効なWQL文字列。 クエリは、返されるオブジェクトにそれぞれ__Path属性を含めます。Agentは、レポート結果を保存するときに__Path属性をエンティティキーとして使用します。そのため、返される各WMIオブジェクトには__Pathを含める必要があります。「SELECT * FROM ...」のようなクエリ文字列を使用する場合は__Path属性を使用できますが、「SELECT Name FROM ...」のように選択的なクエリを使用する場合は、クエリを「SELECT __Path,Name FROM ...」のように記述し、__Path属性を明確に含める必要があります。
onChange	対象のファイルをリアルタイムで監視する必要があるかどうかを示	いいえ	false	true、false

属性	説明	必須	初期設定値	設定できる値
	します。			
provider	オプションで、使用する別のWMI名前空間プロバイダを指定します。	いいえ	なし	RsopLoggingModeProvider 現在、これはグループポリシークエリでのみ必要およびサポートされています。サポートされている値は「RsopLoggingModeProvider」のみです。コンピュータ上にあるポリシーデータのスナップショットを作成するときにRsopLoggingModeProviderを使用することが推奨されているため、グループポリシークエリは特別なクエリです。ポリシーデータのスナップショットを作成する場合、ポリシーの更新中にシステムがポリシーを上書きまたは削除する前に、一貫したデータのセットに対してクエリが実行されます。スナップショットの作成は、実際には新しいWMI名前空間を作成することです。そのため、WQLSetでproviderに「RsopLoggingModeProvider」を使用する場合、名前空間の属性には、作成した名前空間に付加する接尾辞を指定します。たとえば、RsopLoggingModeProviderによって作成される一般的な仮の名前空間は「\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010」です。名前空間に「Computer」を指定してクエリを行うと、「\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010\Computer」になります。 仮の名前空間は一時的な値であり、この値がエンティティキーに表示されるため、Agentの変更検出機能の妨げになります。これを回避するため、RsopLoggingModeProviderが使用された場合、返される__Path値の\Rsop\から次のバックスラッシュまでの部分をAgentが削除します。その結果、エンティティキーは「\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010\Computer」ではなく、「\\.\Root\Rsop\Computer」のような接頭辞がつきます。
timeout	行ごとのタイムアウトをミリ秒単位で指定します。	いいえ	5000	1-60000 WMIクエリがsemisynchronousモードで実行されます。このモードでは、結果の行が一度に1つずつ取得され、1つの行を取得するのにタイムアウトがあります。このパラメータが指定されていない場合、タイムアウト値には5000 (5秒) が使用されます。

エンティティセットの属性

WQLクエリによって返される各「行」は、変更監視用にそれぞれ単一のエンティティとして扱われます。返される列は、エンティティの属性を表します。WMI/WQLは変更可能な仕様であるため、有効な属

性やサポートされている属性のセットリストはありません。クエリと、クエリの対象であるWMIオブジェクトのスキーマは、監視対象の属性を決定します。

たとえば、次のWQLSetの場合、

```
<WQLSet namespace="Computer" wql="select * from RSOP_SecuritySettings where precedence=1" provider="RsopLoggingModeProvider" />
```

次の属性を返します。

```
ErrorCode、GPOID、KeyName、SOMID、Setting、Status、id、precedence
```

一方、次のようなネットワークアダプタにクエリ実行するWQLSetは、

```
<WQLSet namespace="root\cimv2" wql="select * from Win32_NetworkAdapter where AdapterTypeId = 0" />
```

次の属性を返します。

```
AdapterType、AdapterTypeId、Availability、Caption、ConfigManagerErrorCode、
ConfigManagerUserConfig、CreationClassName Description、DeviceID、Index、Installed、
MACAddress、Manufacturer、MaxNumberControlled、Name、PNPDeviceID、
PowerManagementSupported、ProductName、ServiceName、SystemCreationClassName、
SystemName、TimeOfLastReset
```

Agentの負荷を減らすため、クエリに「select * ...」を使用する代わりに、監視の必要がある属性のみを明確に含めることをお勧めします。WMIスキーマに属性を追加または削除する変更は、その属性が監視対象のセットの一部でないかぎり、オブジェクトに対する変更であるとレポートされない利点もあります。「select * from Win32_Foobar」を使用すると、Win32_Foobarオブジェクトのクラスに新しい属性を追加するWindowsのパッチが適用された場合、次回の変更の検索で、新しい属性が出現したことによるクラスの各オブジェクトに対する変更がレポートされます。

次に、望ましいWindowsシステムのエンティティを返すWMIクエリの例をいくつか示します。

Windowsにマウントされたストレージデバイスに対するクエリ(*を選択すると、通常、返される属性の80%はnullまたは重複する値になります):

```
<WQLSet namespace="root\cimv2" wql="SELECT __
Path,DeviceID,VolumeName,VolumeSerialNumber,DriveType,FileSystem,Access,MediaType,Size,FreeSpace FROM Win32_LogicalDisk" />
```

前のクエリに追加して、DriveTypeを指定 (「Removable Disk」であるtype2など) することで、特定タイプのマウント済み論理ストレージデバイスを分離できます(リムーバブルUSBストレージドライブなど)。

```
<WQLSet namespace="root\cimv2" wql="SELECT __
Path,DeviceID,VolumeName,VolumeSerialNumber,DriveType,FileSystem,Access,MediaType,Size,Fre
eSpace FROM Win32_LogicalDisk WHERE DriveType=2" />
```

(Win32_LogicalDiskクラスの詳細についてはここを参照してください)

USBストレージデバイスの注意事項: U3 USBデバイスは、type 2の「Removable Disk」デバイスとtype 3の「Compact Disc」デバイスの両方にマウントされます。また、前出のクエリはストレージデバイス専用です。記憶装置ではないUSBデバイスは含まれません。type 1の「No Root Directory」デバイスとしてUSBメモリカードアダプタが表示されることがあります。type 1の「Unknown」デバイスとして、不良またはWindowsと互換性のないUSBストレージデバイスが表示されることがあります。

ドライブが「F:」である既知のシステムディレクトリすべてに対して、関連する属性のクエリを実行します。

```
<WQLSet namespace="root\cimv2" wql="SELECT __
Path,CreationDate,LastAccessed,LastModified,Drive,Path,FileName,Caption,FileType,Readable,Write
able FROM Win32_Directory WHERE Drive='F:'" />
```

ドライブが「F:」である既知のシステムファイルすべてに対して、関連する属性のクエリを実行します。

```
<WQLSet namespace="root\cimv2" wql="SELECT __
Path,CreationDate,LastAccessed,LastModified,Drive,Path,FileName,Name,FileType,Readable,Writeab
le FROM CIM_DataFile WHERE Drive='F:'" />
```

「key」の意味

keyは、返されるWMIオブジェクトの「__Path」属性で、通常は次の形式です。

```
SystemName\Namespace:WmiObjectClass.KeyAttribute=Value[,KeyAttribute=Value]
```

例を挙げます。

```
\\TEST-DESK\root\cimv2:Win32_QuickFixEngineering.HotFixID="KB958215-
IE7",ServicePackInEffect="SP0"
 \\TEST-DESK\ROOT\Rsop\NSF49B36AD_10A3_4F20_9541_B4C471907CE7\Computer:RSOP_
RegistryValue.
Path="MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\LegalNoticeText",p
recedence=1
 \\TEST-DESK\root\cimv2:BRCM_NetworkAdapter.DeviceID="8"
```

include/exclude

これらのエレメントに指定できる属性とサブエレメントの「include」と「exclude」の概要は、"変更監視 rules languages" on page 1017を参照してください。

WQLSetでは通常、「include」サブエレメントと「exclude」サブエレメントは不要です。WQLはAgentおよびコンピュータのWMI実装の両方によって実行される処理の量を制限するため、監視するオブジェクトの正確なセットを指定するためにWQLを使用することが望ましいです。

任意のincludeまたはexcludeサブエレメントを使用すると、クエリによって返されるオブジェクトのセットを減らすことのみ可能です。追加のオブジェクトを返すようにするためには、WQLを変更する必要があります。includeまたはexcludeエレメントを使用してWQLの結果をさらに制限する必要がある場合には、エンティティキーの値に対して一致させる単純なワイルドカードとして「*」および「?」の文字を使用できます。

Virtual Applianceの検索キャッシュ

検索キャッシュは、仮想マシンの不正プログラム対策および変更監視の検索を最大限に効率化する目的で、Virtual Applianceによって使用されます。検索キャッシュによって、大規模なVMware環境で、複数の仮想マシンから同じ内容を検索する必要性がなくなるため、検索の効率が向上します。検索キャッシュには、Deep Security保護モジュールによって検索されたファイルおよびその他の検索対象のリストが含まれます。仮想マシン上の検索対象と過去の検索対象が同じであることが確認された場合、その対象はVirtual Applianceによって再度検索されません。エンティティが同じであるかどうかを確認するために使用される属性は、作成時刻、変更時刻、ファイルサイズ、およびファイル名です。リアルタイム検索キャッシュの場合、Deep Securityはファイルの一部の内容を読み取り、2つのファイルが同一であるかどうかを判断します。ファイルの更新シーケンス番号 (USN、Windowsのみ) を使用するオプション設定もありますが、その設定はクローン作成された仮想マシン以外には使用しないでください。

検索キャッシュによって、クローン作成された仮想マシン間または類似した仮想マシン間で検索結果が共有されるため、変更監視が効率化されます。

後続の検索の速度が向上するため、クローン作成された仮想マシンまたは類似した仮想マシンでの不正プログラムの検索が効率化されます。

また、クローン作成された仮想マシンまたは類似した仮想マシンの起動プロセス検索とアプリケーションアクセス検索の速度が向上するため、不正プログラムのリアルタイム検索が強化されます。

検索キャッシュ設定

検索キャッシュ設定は、有効期限、更新シーケンス番号 (USN)、除外するファイル、含めるファイルなどを指定する設定の集まりです。

注意: 同じ検索キャッシュ設定を使用する仮想マシン間では、同じ検索キャッシュが共有されます。

既存の検索キャッシュ設定のリストを表示するには、[管理]→[システム設定]→[詳細]→[検索キャッシュ設定] の順に進み、[検索キャッシュ設定の表示] をクリックします。Deep Securityには、事前設定された初期設定の検索キャッシュ設定がいくつか付属しています。これらの設定は、保護する仮想マシンのプロパティと実行する検索の種類に応じて、Virtual Applianceによって自動的に実装されます。

[期限] では、個々のエントリを検索キャッシュに保存する期間を指定します。推奨される初期設定は、手動/予約による不正プログラム検索で1日、不正プログラムのリアルタイム検索で15分、変更監視の検索で1日です。

[USNの使用 (Windowsのみ)] では、Windows NTFSの更新シーケンス番号を使用するかどうかを指定します。更新シーケンス番号は、個々のファイルへの変更を記録するための番号です。このオプションは、クローン作成された仮想マシンにのみ設定してください。

[含めるファイル] と[除外するファイル] では、検索キャッシュに含める、または検索キャッシュから除外するファイルの正規表現パターンとリストを指定します。検索対象のファイルは、まず含めるリストに対して照合されます。

個々のファイルとフォルダは名前で識別できます。また、ワイルドカード(「*」および「?」) を使用して、1つの正規表現で複数のファイルや場所を参照することもできます(ゼロ個以上の任意の文字を表すには「*」を、任意の1文字を表すには「?」を使用します)。

注意: 含めるリストと除外リストによって、ファイルの検索に検索キャッシュを使用するかどうかが決まります。ただし、これらのリストを使用することによって、ファイルを従来の方法で検索できなくなるわけではありません。

不正プログラム検索のキャッシュ設定

仮想マシンで使用する検索キャッシュ設定を選択するには、**コンピュータエディタまたはポリシーエディタ**[1]を開き、[不正プログラム対策]→[詳細]→[仮想マシンの検索キャッシュ] の順に進みます。ここで、不正プログラムのリアルタイム検索に使用する検索キャッシュ設定と、手動/予約検索に使用する検索キャッシュ設定を選択できます。

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。

変更監視の検索のキャッシュ設定

仮想マシンで使用する検索キャッシュ設定を選択するには、**コンピュータエディタまたはポリシーエディタ**[1]を開き、[変更監視]→[詳細]→[仮想マシンの検索キャッシュ] の順に進みます。

検索キャッシュの管理設定

検索キャッシュの管理設定では、検索キャッシュの実行に関する設定ではなく、Virtual Applianceによる検索キャッシュの管理方法を指定します。そのため、検索キャッシュの管理設定は、検索キャッシュ設定と別になっています。検索キャッシュの管理設定は、ポリシーレベルで制御されます。検索キャッシュの管理設定を表示するには、**ポリシーエディタ**[2]を開き、[設定]→[一般]→[Virtual Appliance] の順に進みます。

同時検索の最大数: Virtual Applianceによって同時に実行される検索の数を指定します。推奨される数は5です。この数が10を超えると、検索のパフォーマンスが低下する可能性があります。検索要求はVirtual Applianceで処理待ちの状態となり、到着順に実行されます。この設定は、手動/予約検索にのみ適用されます。

不正プログラムの手動検索キャッシュの最大エントリ数: 不正プログラムの手動検索または予約検索を実行したときに保持するファイルやその他の検索可能な内容を特定するレコードの最大数を指定します。エントリが100万件の場合、使用されるメモリは約100 MBです。

不正プログラムのリアルタイム検索キャッシュの最大エントリ数: 不正プログラムのリアルタイム検索を実行したときに保持するファイルやその他の検索可能な内容を特定するレコードの最大数を指定します。エントリが100万件の場合、使用されるメモリは約100MBです。

変更監視の検索キャッシュの最大エントリ数: 変更監視のベースラインデータに含めるエンティティの最大数を指定します。エンティティが20万個の場合、使用されるメモリは約100MBです。

初期設定を変更する場合の考慮事項

検索キャッシュは、同じファイルを再度検索しないことを目的としています。Deep Securityは、すべてのファイルの内容全体を調べてファイルが同一であるかどうかを判断しません。そうするように設定されている場合、Deep SecurityはファイルのUSN値を確認できますが、リアルタイム検索ではファイルの一部の内容が読み取られますが、通常はファイル属性を調べてファイルが同一であるかどうかを判断しま

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。

[2] ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック) します。

す。不正プログラムがファイルに変更を加えた後、それらのファイル属性を変更前の状態に復元することは困難ですが、不可能ではありません。

Deep Securityは、この初期設定のキャッシュ期限を短く設定することで、この潜在的な脆弱性を制限します。セキュリティを強化するために、キャッシュの有効期限をさらに短くしたり、USNを使用することもできますが、これによってパフォーマンスの向上率が低下したり、より大きなキャッシュの設定が必要になることがあります。特定の仮想マシンに最高レベルのセキュリティを提供し、他から切り離して検索結果を共有しないようにするには、該当する仮想マシン専用のポリシーを作成して、それらが別のゾーンで管理されるようにします。この方法は、異なる部門または組織間で同じインフラストラクチャを共有する場合に適しています(マルチテナントのDeep Security Managerを使用している場合は、この設定が自動的に各テナントに適用されます)。

VDI環境など、ESXiホストあたりのゲスト仮想マシン数が非常に多い場合は、検索中のディスクI/OとCPU使用率を監視してください。検索に時間がかかりすぎる場合は、キャッシュのサイズを増やすか、パフォーマンスが改善されるまで検索キャッシュの管理設定を調整します。キャッシュのサイズを増やす場合は、Deep Security Virtual Applianceシステムメモリの調整も必要になることがあります。

ログ検査の設定

セキュリティログ監視

注意: セキュリティログ監視がサポートされるOSのリストについては、"各プラットフォームでサポートされている機能" on page 417を参照してください。

セキュリティログ監視保護モジュールは、OSおよびアプリケーションのログに含まれている可能性のある重要なセキュリティイベントの特定に役立ちます。これらのイベントをセキュリティ情報/イベント管理(SIEM)システムまたは中央のログサーバに送信して、関連付け、レポート、およびアーカイブに使用できます。また、すべてのイベントはDeep Security Managerで安全に収集されます。イベントのログ記録および転送の詳細については、"セキュリティログ監視イベントの転送と保存を設定する" on page 1069を参照してください。

セキュリティログ監視モジュールで実施できる作業は次のとおりです。

- PCI DSSログ監視の要件を満たす。
- 不審な動作を検出する。
- さまざまなOSとアプリケーションを含む異種環境でイベントを収集する。
- エラーなどのイベントや情報イベント(ディスクがいっぱいである、サービスの開始、サービスの停止など)を表示する。

- 管理者のアクティビティ(管理者のログインまたはログアウト、アカウントのロックアウト、ポリシーの変更など) の監査証跡を作成して維持する。

セキュリティログ監視を有効にして設定するには、"セキュリティログ監視" belowを参照してください。

Deep Securityのログ検査機能を使用すると、サードパーティのログファイルをリアルタイムで分析できます。セキュリティログ監視ルールとデコーダは、多種多様なシステムに対して、イベントの解析、分析、ランク付けおよび関連付けを実行するためのフレームワークを提供します。侵入防御および変更監視と同様、セキュリティログ監視の内容は、セキュリティアップデートに含まれているルールのフォームで配信されます。これらのルールによって、分析するアプリケーションとログの選択を高いレベルで選択することができます。セキュリティログ監視ルールを設定して確認するには、"ポリシーで使用するセキュリティログ監視 ルールを定義する" on page 1070を参照してください。

セキュリティログ監視

セキュリティログ監視を使用するには、次の基本手順を実行します。

1. "セキュリティログ監視モジュールをオンにする" below
2. "推奨設定の検索を実行する" below
3. "推奨されるセキュリティログ監視ルールを適用する" on the next page
4. "セキュリティログ監視をテストする" on page 1068
5. "セキュリティログ監視イベントの転送と保存を設定する" on page 1069

セキュリティログ監視モジュールの概要については、"セキュリティログ監視" on the previous pageを参照してください。

セキュリティログ監視モジュールをオンにする

1. [ポリシー] に移動します。
2. セキュリティログ監視を有効にするポリシーをダブルクリックします。
3. [セキュリティログ監視]→[一般] の順にクリックします。
4. [セキュリティログ監視のステータス] で [オン] を選択します。
5. [保存] をクリックします。

推奨設定の検索を実行する

ルールは、要件に関連するセキュリティイベントを収集するように設定する必要があります。設定が適切でないと、大量のログエントリがトリガおよび保存され、Deep Securityデータベースの容量を圧迫する場合があります。コンピュータで推奨設定の検索を実行して、どのルールを適用するのが適切か、推奨設定を取得します。

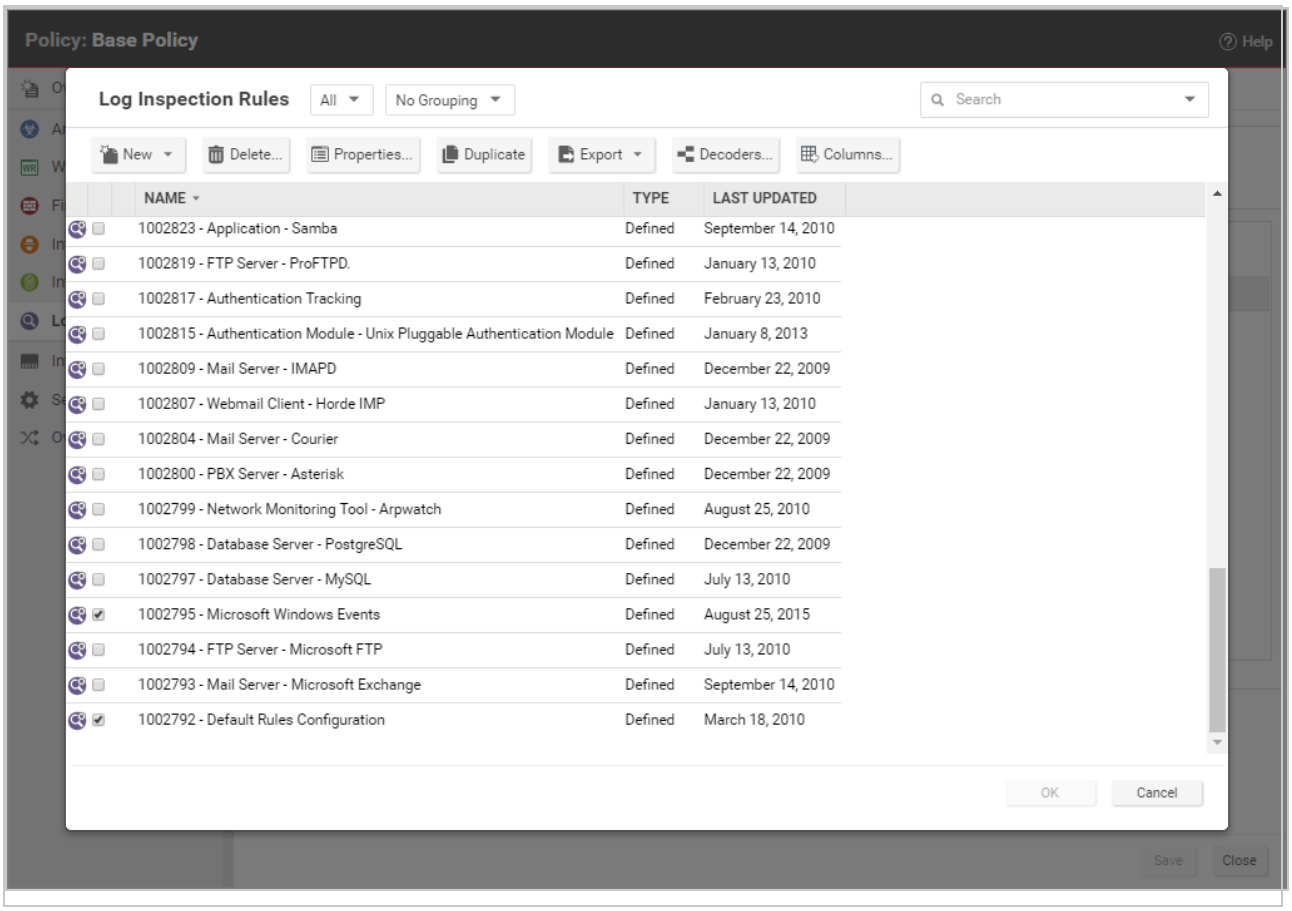
1. [コンピュータ] に移動し、該当するコンピュータをダブルクリックします。
2. [セキュリティログ監視]→[一般] の順にクリックします。
3. [セキュリティログ監視ルールの推奨設定を自動的に適用 (可能な場合)] の設定では、検出されたルールをDeep Securityで実装するかどうかを [はい] または [いいえ] を選択することで決定できます。
4. [推奨設定] セクションで、[推奨設定の検索] をクリックします。トレンドマイクロが提供する一部のセキュリティログ監視ルールは、正常に機能するため、ローカルでの設定を必要とします。このようなルールをコンピュータに割り当てるか、ルールが自動的に割り当てられると、設定が必要であることを通知するアラートが発令されます。

推奨設定の検索の詳細については、"推奨設定の検索の管理と実行" on page 728を参照してください。

推奨されるセキュリティログ監視ルールを適用する

Deep Securityには、さまざまなOSとアプリケーションに対応した、定義済みの多数のルールが用意されています。推奨設定の検索を実行するときは、Deep Securityで推奨設定のルールを自動的に適用することも、次の手順に従ってルールを手動で選択して割り当てることもできます。

1. [ポリシー] に移動します。
2. 設定するポリシーをダブルクリックします。
3. [セキュリティログ監視]→[一般] の順にクリックします。
4. [現在割り当てられているセキュリティログ監視ルール] セクションには、ポリシーで有効になっているルールが表示されます。セキュリティログ監視ルールを追加または削除するには、[割り当て/割り当て解除] をクリックします。



5. 割り当てる、または割り当て解除するルールのチェックボックスをオンまたはオフにします。セキュリティログ監視ルールを編集するには、ルールを右クリックしてて[プロパティ]を選択してルールをローカルで編集する方法と、[プロパティ(グローバル)]を選択してルールを使用しているその他すべてのポリシーに対して変更内容を適用する方法があります。詳細については、"セキュリティログ監視 ルールを調べる" on page 1088を参照してください。
6. [OK]をクリックします。

Deep Securityには多数の一般的なOSおよびアプリケーション用のセキュリティログ監視ルールが用意されていますが、独自のカスタムルールを作成することもできます。カスタムルールを作成する場合は、「基本ルール」テンプレートを使用するか、または新しいルールをXMLで記述できます。カスタムルールの作成方法については、"ポリシーで使用するセキュリティログ監視 ルールを定義する" on page 1070を参照してください。

セキュリティログ監視をテストする

以降のセキュリティログ監視設定の手順に進む前に、ルールが正常に動作しているかどうかをテストします。

1. セキュリティログ監視が有効になっていることを確認します。
2. コンピュータエディタまたはポリシーエディタで、>[セキュリティログ監視]→[詳細] に移動します。[Agent/Applianceイベントが次の重要度以上の場合に、イベントを記録してDSMに送信] を [低 (3)] に変更し、[保存] をクリックします。
3. [一般] タブで、[割り当て/割り当て解除] をクリックします。次の項目を検索して有効にします。
   - [1002792 - Default Rules Configuration] - これは他のすべてのセキュリティログ監視ルールを機能させるために必要なルールです。

   Windowsユーザの場合は次の項目を有効にします。

   - [1002795 - Microsoft Windows Events] - Windowsの監査機能がイベントを登録するたびに、イベントがログに記録されます。

   Linuxユーザの場合は次の項目を有効にします。

   - [1002831 - Unix - Syslog] - syslogに記録されたイベントが検査されます。
4. [OK] をクリックし、[保存] をクリックして、ポリシーにルールを適用します。
5. 存在しないアカウントでサーバーへのログインを試みます。
6. [イベントとレポート]→[セキュリティログ監視イベント] に移動し、ログイン失敗が記録されていることを確認します。検出が記録されていれば、セキュリティログ監視モジュールは正常に動作しています。

セキュリティログ監視イベントの転送と保存を設定する

セキュリティログ監視ルールがトリガされると、イベントがログに記録されます。これらのイベントを表示するには、[イベントとレポート]→[セキュリティログ監視イベント] に移動するか、ポリシーエディタで [セキュリティログ監視]→[セキュリティログ監視イベント] に移動します。セキュリティログ監視イベントの使用に関する詳細については、"セキュリティログ監視イベント" on page 1421を参照してください。

イベントの重要度に応じて、Syslogサーバにイベントを送信したり(この機能を有効にする方法の詳細については"Deep SecurityイベントをSyslogまたはSIEMサーバに転送する" on page 1171を参照)、重要度のクリッピング機能を使用してイベントをデータベースに保存したりすることもできます。

「重要度のクリッピング」では次の2つを設定できます。

- Agent/Applianceイベントが次の重要度以上の場合に、イベントをSyslogに送信: この設定は、Syslogが有効な場合に、ルールによってトリガされたイベントのうちどのイベントがSyslogサーバに送信されるかを決定します
- Agent/Applianceイベントが次の重要度以上の場合に、イベントを記録してDeep Security Managerに送信: この設定は、どのセキュリティログ監視イベントがデータベースに保存され、[セキュリティログ監視イベント] 画面に表示されるかを決定します。

重要度のクリッピングを設定するには、次の手順に従います。

1. [ポリシー] に移動します。
2. 設定するポリシーをダブルクリックします。
3. [セキュリティログ監視]→[詳細] の順にクリックします。
4. [Agent/Applianceイベントが次の重要度以上の場合に、イベントをSyslogに送信] で重要度を[低 (0)] から[重大 (15)] の範囲で選択します。
5. [Agent/Applianceイベントが次の重要度以上の場合に、イベントを記録してDSMに送信] で重要度を[低 (0)] から[重大 (15)] の範囲で選択します。
6. [保存] をクリックします。

ポリシーで使用するセキュリティログ監視 ルールを定義する

OSSEC セキュリティログ監視 エンジンはDeep Security Agentに統合されており、Deep Securityは、コンピュータ上で実行されているオペレーティングシステムおよびアプリケーションによって生成されたログおよびイベントを検査できます。Deep Security Managerには、コンピュータまたはポリシーに割り当てることができるOSSEC セキュリティログ監視 ルールの標準セットが付属しています。要件に合う既存ルールが存在しない場合は、カスタムルールを作成することもできます。

トレンドマイクロが発行したセキュリティログ監視ルールを変更することはできませんが、それらを複製してから変更することはできます。

1台以上のコンピュータに割り当てられているか、ポリシーの一部であるセキュリティログ監視ルールは削除できません。

セキュリティログ監視 ルールを作成するには、次の基本手順を実行します。

- "新しい セキュリティログ監視 ルールを作成します。" on the next page
- "デコーダ" on page 1072
- "サブルール" on page 1074
- "例" on page 1080
- "セキュリティログ監視 ルールの重大度レベルと推奨される使用" on page 1086
- "strftime () 変換指定子" on page 1088
- "セキュリティログ監視 ルールを調べる" on page 1088

セキュリティログ監視 モジュールの概要については、"セキュリティログ監視" on page 1065を参照してください。

新しいセキュリティログ監視ルールを作成します。

1. Deep Security Managerで、[ポリシー]→[共通オブジェクト]→[ルール]→[セキュリティログ監視ルール] に進みます。
2. [新規]→[新しいセキュリティログ監視ルール] をクリックします。
3. [一般] タブで、ルールの名前と説明を入力します (説明は省略できます)。
4. [コンテンツ] タブで、ルールを定義します。ルールを定義する一番簡単な方法は、[基本ルール] を選択し、表示されるオプションを使用してルールを定義する方法です。さらにカスタマイズが必要な場合は、[カスタム (XML)] を選択し、定義しているルールをXMLビューに切り替えることができます。

   カスタム (XML) ビューで行った変更は、基本ルールビューに戻すと失われます。

   XMLベースの言語を使用して独自のセキュリティログ監視ルールを作成する場合は、OSSECのドキュメントを参照するか、サポートプロバイダにお問い合わせください。

   基本ルールテンプレートでは以下のオプションを使用できます。

   - ルールID: ルールIDはルールの一意の識別子です。OSSECは100000 - 109999をユーザ定義ルールのスペースとして定義しています。Deep Security Managerは新しい一意のルールIDでフィールドを事前に入力します。
   - レベル: ルールにレベルを割り当てます。ゼロ (0) は、ルールによってイベントが記録されないことを示しますが、このルールを監視する他のルールが発生する可能性があります
   - グループ: 1つ以上のカンマ区切りのグループにルールを割り当てます。これが便利なのは、ある1つのルールの発生時に発生する複数のルール、または特定のグループに属するルールを作成した後に依存関係が使用されるときです。
   - ルールの説明: ルールの説明。
   - パターンマッチング: これはルールがログ内で探すパターンです。ルールは一致時にトリガーされます。パターンマッチングは正規表現またはより単純な文字列パターンをサポートします。文字列パターンのパターンタイプは正規表現よりも高速ですが、3つの特殊操作のみをサポートします。
     - ^ (カレット): テキストの先頭を指定します。
     - $ (ドル記号): テキストの末尾を指定します。
     - | (パイプ): 複数のパターン間に「OR」を作成します。

     セキュリティログ監視モジュールで使用される正規表現の構文については、https://www.ossec.net/docs/syntax/regex.htmlを参照してください。

- 依存関係: 別のルールに依存関係を設定すると、この領域で指定されたルールがトリガーされた場合にのみ、イベントが記録されます。
- [頻度] は、ルールがトリガされるまでの特定の期間内にルールを照合する必要のある回数です。
- [期間] は、イベントを記録するためにルールを特定の回数 (上記の頻度) トリガするまでの期間 (秒数) です。

  コンテンツタブは、ユーザー自身が作成したセキュリティログ監視ルールにのみ表示されます。トレンドマイクロによって発行されたセキュリティログ監視ルールには、代わりに構成タブが表示され、セキュリティログ監視ルールの構成オプションが表示されます (存在する場合)。

5. ファイルタブで、ルールでモニタしたいファイルのフルパスを入力し、ファイルの種類を指定してください。

   グロブ文字はファイル名で使用される場合にサポートされています。グロブ文字はパスのディレクトリ部分で使用される場合も2回までサポートされています。例えば、/home/user1/testlog*.txt、/home/*/testlog1.txt、/home/*/testlog*.txt、/home/*/user*/testlog*.txtはすべて有効ですが、/home/*/demo*/user*/testlog1.txtは無効です。

6. [オプション] タブの [アラート] セクションで、このルールでアラートをトリガするかどうかを選択します。

   最小のアラート重要度 は、基本ルールまたはカスタム(XML) テンプレートを使用してルールに対してアラートをトリガする最小の重大度レベルを設定します。

   基本ルールテンプレートは、一度に1つのルールを作成します。1つのテンプレートに複数のルールを書き込むには、カスタム(XML) テンプレートを使用できます。カスタム(XML) テンプレート内でレベルが異なる複数のルールを作成する場合は、[最小のアラート重要度]設定を使用して、そのテンプレート内のすべてのルールに対するアラートをトリガする最小の重要度を選択できます。

7. [割り当て対象 に割り当てられました]タブには、この セキュリティログ監視 ルールを使用しているポリシーとコンピュータが表示されます。新しいルールは作成中であるため、まだ割り当てられていません。
8. [OK] をクリックします。このルールをポリシーとコンピュータに割り当てる準備ができました。

デコーダ

A セキュリティログ監視 ルールは、変更を監視するファイルのリストと、ルールがトリガする条件のセットで構成されます。 セキュリティログ監視 エンジンが監視対象ログファイルの変更を検出すると、その変更はデコーダによって解析されます。デコーダは、rawログエントリを解析して次のフィールドを生成します。

- log: イベントのメッセージセクション
- full_log: イベント全体
- location: ログの生成元
- hostname: イベント発生元のホスト名
- program_name: イベントのSyslogヘッダで使用されるプログラム名
- srcip: イベント内の送信元のIPアドレス
- dstip: イベント内の送信先のIPアドレス
- srcport: イベント内の送信元のポート番号
- dstport: イベント内の送信先のポート番号
- protocol: イベント内のプロトコル
- action: イベント内で実行された処理
- srcuser: イベント内の送信元のユーザ
- dstuser: イベント内の送信先のユーザ
- id: イベントからのIDとしてデコードされたID
- status: イベント内のデコードされたステータス
- command: イベント内で呼び出されるコマンド
- url: イベント内のURL
- data: イベントから抽出される追加データ
- systemname: イベント内のシステム名

ルールは、このデコードされたデータを確認して、ルールで定義された条件に一致する情報を検索します。

一致する項目の重要度レベルが十分に高い場合は、次のいずれかの処理を実行できます。

- アラートを発生させることができます。セキュリティログ監視ルールのプロパティウィンドウのオプションタブで設定可能です。
- イベントは syslog に書き込むことができます。管理 > システム設定 > イベント転送 タブの SIEM エリアで設定可能です。
- イベントはDeep Security Managerに送信できます。ポリシーまたはコンピュータエディタ> 設定 > イベント転送 タブのセキュリティログ監視Syslog設定で設定可能です。

サブルール

1つの セキュリティログ監視 ルールに複数のサブルールを含めることができます。これらのサブルールには、アトミックとコンポジットという2つの種類があります。アトミックルールは1つのイベントを評価し、コンポジットルールは複数のイベントを確認して、頻度、繰り返し、およびイベント間の相関関係を評価できます。

グループ

各ルールまたはルールのグループは、<group></group>要素内で定義する必要があります。属性名には、このグループに含めたいルールを含める必要があります。次の例では、グループにsyslogとSSHDのルールが含まれていることを示しています。

```
<group name="syslog,sshd,"> </group>
```

グループ名の末尾のコンマに注意してください。<if_group></if_group>タグを使用してこのサブルールに別のサブルールを条件付きで追加する場合、末尾のコンマが必要です。

セキュリティログ監視ルールのセットがエージェントに送信されると、エージェント上のセキュリティログ監視エンジンは、各割り当てられたルールからXMLデータを取得し、それを1つの長いセキュリティログ監視ルールに組み立てます。トレンドマイクロによって作成されたすべてのセキュリティログ監視ルールには共通のグループ定義があります。このため、トレンドマイクロはこれらのグループを定義するDefault Rules Configurationというルールを含めており、他のトレンドマイクロのルールと一緒に常に割り当てられます。ルールを割り当てる際にDefault Rules Configurationルールを選択しない場合、そのルールが自動的に割り当てられることを通知するメッセージが表示されます。独自のセキュリティログ監視ルールを作成し、トレンドマイクロ作成のルールを割り当てずにコンピュータに割り当てる場合は、Default Rules Configurationルールの内容を新しいルールにコピーするか、またはDefault Rules Configurationルールをコンピュータに割り当てるために選択する必要があります。

ルール、ID、およびレベル

グループには必要なだけのルールを含めることができます。ルールは<rule></rule>要素を使用して定義され、少なくとも2つの属性、idとlevelを持たなければなりません。idはそのシグネチャの一意の識別子であり、levelはアラートの重大度です。次の例では、異なるルールIDとレベルを持つ2つのルールが作成されています。

```
<group name="syslog,sshd,"> <rule id="100120" level="5"> </rule> <rule id="100121" level="6"> </rule> </group>
```

カスタムルールには、100,000以上のID値を指定する必要があります。

親グループ内に<group></group>タグを使用して追加のサブグループを定義できます。このサブグループは、以下の表に記載されているグループのいずれかを参照することができます。

グループの種類	グループ名	説明
攻撃の予兆	connection_attempt web_scan recon	接続の試行 Web検索 一般的な検索
認証制御	authentication_success authentication_failed invalid_login login_denied authentication_failures adduser account_changed	成功 失敗 無効 ログイン拒否 複数の失敗 ユーザアカウントの追加 ユーザアカウントの変更または削除
攻撃/悪用	automatic_attack exploit_attempt invalid_access spam multiple_spam sql_injection attack virus	ワーム(対象を指定しない攻撃) 攻撃コードのパターン 無効なアクセス スパム 複数のスパムメッセージ SQLインジェクション 一般的な攻撃 ウイルスの検出
アクセス管理	access_denied access_allowed unknown_resource firewall_drop multiple_drops client_misconfig client_error	アクセス拒否 アクセス許可 存在しないリソースへのアクセス ファイアウォールによるドロップ 複数のファイアウォールによるドロップ クライアントの誤った設定 クライアントエラー
ネットワーク制御	new_host ip_spoof	新しいコンピュータの検出 ARPスプーフィングの疑い
システム監視	service_start system_error system_shutdown logs_cleared invalid_request promisc policy_changed config_changed low_diskspace time_changed	サービスの開始 システムエラー シャットダウン ログのクリア 無効な要求 インタフェースのプロミスキャスモードへの切り替え ポリシーの変更 設定の変更 ディスク容量が少ない 時刻の変更

イベントの自動タグ付けが有効になっている場合、イベントはグループ名でラベル付けされます。トレンドマイクロが提供するセキュリティログ監視ルールは、グループをよりユーザーフレンドリーなバージョンに変更する変換テーブルを使用します。例えば、login_deniedはLogin Deniedとして表示されます。カスタムルールは、ルールに表示されるグループ名で一覧表示されます。

説明

<description></description>タグを含めます。ルールがトリガーされた場合、説明テキストがイベントに表示されます。

```
<group name="syslog,sshd,"> <rule id="100120" level="5"> <group>authentication_success</group>
<description>SSHD testing authentication success</description> </rule> <rule id="100121" level="6">
<description>SSHD rule testing 2</description> </rule> </group>
```

デコード形式

<decoded_as></decoded_as>タグは、指定されたデコーダーがログをデコードした場合にのみルールを適用するようにセキュリティログ監視エンジンに指示します。

```
<rule id="100123" level="5"> <decoded_as>sshd</decoded_as> <description>Logging every decoded
sshd message</description> </rule>
```

使用可能なデコーダを表示するには、[セキュリティログ監視ルール] 画面で [デコーダ] をクリックします。[1002791-Default Log Decoders] を右クリックして、[プロパティ] を選択します。[設定] タブに進み、[デコーダの表示] をクリックします。

一致項目

ログ内で特定の文字列を探すには、<match></match>を使用します。こちらはLinuxのsshd失敗パスワードログです。

```
Jan 1 12:34:56 linux_server sshd[1231]: Failed password for invalid user jsmith from 192.168.1.123 port
1799 ssh2
```

「Failed password」という文字列を検索するには、<match></match> タグを使用します。

```
<rule id="100124" level="5"> <decoded_as>sshd</decoded_as> <match>^Failed password</match>
<description>Failed SSHD password attempt</description> </rule>
```

正規表現のキャレット(^) は文字列の先頭を示しています。「Failed password」はログの先頭には表示されませんが、セキュリティログ監視デコーダーはログをセクションに分割します。参照 "デコーダ" on page 1072 詳細情報については、「log」はログのメッセージ部分であり、「full_log」はログ全体であるセクションの1つです。

次の表は、サポートされている正規表現の構文一覧です。

正規表現の構文	説明
\w	A ~ Z、a ~ z、0 ~ 9の英数字1文字
\d	0 ~ 9の数字1文字
\s	単一のスペース(空白文字)
\t	単一のタブ
\p	()*+,-.:;<=>?[]
\W	\w以外
\D	\d以外
\S	\s以外
\.	任意の文字
+	上記のいずれかの1つ以上に一致 (たとえば、\w+、\d+)
*	上記のいずれかの0個以上に一致 (たとえば、\w*、\d*)
^	文字列の先頭 (^<任意の文字列>)
$	文字列の末尾 (<任意の文字列>$)
|	複数の文字列間の「OR」

条件文

ルールの評価は、他のルールが真と評価された場合に条件付きで行うことができます。<if_sid></if_sid>タグは、タグで識別されたルールが真と評価された場合にのみ、このサブルールを評価するようにセキュリティログ監視エンジンに指示します。次の例では、3つのルールを示しています: 100123、100124、および100125。ルール100124と100125は、<if_sid></if_sid>タグを使用して100123ルールの子として変更されています。

```
<group name="syslog,sshd,"> <rule id="100123" level="2"> <decoded_as>sshd</decoded_as> <description>すべてのデコードされたsshdメッセージを記録</description> </rule> <rule id="100124" level="7"> <if_sid>100123</if_sid> <match>^Failed password</match> <group>authentication_failure</group> <description>SSHDパスワード試行失敗</description> </rule> <rule id="100125" level="3"> <if_sid>100123</if_sid> <match>^Accepted password</match> <group>authentication_success</group> <description>SSHDパスワード試行成功</description> </rule> </group>
```

評価の階層

<if_sid></if_sid>タグは本質的に階層的なルールセットを作成します。つまり、ルールに<if_sid></if_sid>タグを含めることで、そのルールは<if_sid></if_sid>タグで参照されるルールの子ルールとなります。ログにルールを適用する前に、セキュリティログ監視エンジンは<if_sid></if_sid>タグを評価し、親ルールと子ルールの階層を構築します。

階層的な親子構造を使用することで、ルールの効率を向上させることができます。親ルールが真と評価されない場合、セキュリティログ監視エンジンはその親の子ルールを無視します。

<if_sid></if_sid>タグは、まったく異なるセキュリティログ監視ルール内のサブルールを参照するために使用できますが、後でルールを確認するのが非常に難しくなるため、これを避けるべきです。

次の表は、使用可能なアトミックルールの条件指定のオプションを一覧表示しています。

タグ	説明	備考
match	パターン	イベント(ログ)に対して照合される任意の文字列。
regex	正規表現	イベント(ログ)に対して一致する正規表現。
decoded_as	文字列	事前一致する任意の文字列。
srcip	送信元のIPアドレス	ソースIPアドレスとしてデコードされたIPアドレス。IPアドレスを否定するには!を使用します。
dstip	送信先のIPアドレス	宛先IPアドレスとしてデコードされたIPアドレス。IPアドレスを否定するには!を使用します。
srcport	送信元のポート番号	任意の送信元のポート(形式の一致)。
dstport	送信先のポート番号	任意の送信先のポート(形式の一致)。
user	ユーザ名	ユーザ名としてデコードされる任意のユーザ名。
program_name	プログラム名	Syslogプロセス名からデコードされる任意のプログラム名。
hostname	システムのホスト名	Syslogのホスト名としてデコードされる任意のホスト名。
time	次の形式の時刻の範囲 hh:mm - hh:mmまたは hh:mm am - hh:mm pm	トリガするルールに対してイベントが発生する必要のある時刻の範囲。
weekday	平日 (日曜日、月曜日、火曜日など)	トリガするルールに対してイベントが発生する必要のある曜日。
id	ID	イベントからデコードされる任意のID。
url	URL	イベントからデコードされる任意のURL。

このルールを100125ルールに依存させるには、<if_sid>100125</if_sid>タグを使用します。このルールは、すでに成功したログインルールに一致したSSHDメッセージに対してのみチェックされます。

```
<rule id="100127" level="10"> <if_sid>100125</if_sid> <time>6 pm - 8:30 am</time> <description>Login outside business hours.</description> <group>policy_violation</group> </rule>
```

ログエントリのサイズに関する制限

次の例では、前の例にmaxsize属性を追加し、セキュリティログ監視エンジンに対して、最大サイズの文字数未満のルールのみを評価するように指示します。

```
<rule id="100127" level="10" maxsize="2000"> <if_sid>100125</if_sid> <time>6 pm - 8:30 am</time> <description>Login outside business hours.</description> <group>policy_violation</group> </rule>
```

次の表は、使用可能なアトミックルールのツリーベースのオプションを一覧表示しています。

タグ	説明	備考
if_sid	ルールID	指定された署名IDに一致するルールの子ルールとしてこのルールを追加します。
if_group	グループID	指定されたグループに一致するルールの子ルールとしてこのルールを追加します。
if_level	ルールレベル	指定された重要度レベルに一致するルールの子ルールとしてこのルールを追加します。
説明	文字列	ルールの説明。
info	文字列	ルールの追加情報。
cve	CVE番号	ルールに関連付ける任意のCommon Vulnerabilities and Exposures (CVE) 番号。
options	alert_by_email no_email_alert no_log	アラートの処理としてメール生成 (alert_by_email)、メール生成なし (no_email_alert)、またはログへの記録なし (no_log) のいずれかを指定する追加のルールオプション。

コンポジットルール

単一のログエントリを検査するのがアトミックルールです。複数のエントリを関連付けるには、コンポジットルールを使用する必要があります。コンポジットルールは、現在のログを既に受信したものと一致させることを目的としています。コンポジットルールには2つの追加オプションが必要です: frequencyオプションは、ルールがアラートを生成する前にイベントまたはパターンが何回発生する必要があるかを指定し、timeframeオプションは、セキュリティログ監視エンジンが過去のログを何秒前まで遡って検索するかを指示します。すべてのコンポジットルールは次の構造を持っています:

```
<rule id="100130" level="10" frequency="x" timeframe="y"> </rule>
```

例えば、10分間に5回のパスワード失敗があった場合に高い重大度のアラートを作成する複合ルールを作成することができます。<if_matched_sid></if_matched_sid>タグを使用して、新しいルールがアラートを作成するために必要な頻度と時間枠内でどのルールを確認する必要があるかを示すことができます。次の例では、frequency属性はイベントが5回発生したときにトリガーされるように設定され、timeframe属性は時間枠を600秒として指定するように設定されています。

<if_matched_sid></if_matched_sid>タグは、複合ルールが監視する他のルールを定義するために使用されます。

```
<rule id="100130" level="10" frequency="5" timeframe="600"> <if_matched_sid>100124</if_matched_sid> <description>5 Failed passwords within 10 minutes</description> </rule>
```

より詳細なコンポジットルールを作成するのに使用できるタグが他にもいくつかあります。このようなルールを使用すると、次の表に示すように、イベントの特定の部分が同じになるように指定できます。これにより、コンポジットルールを調整して誤判定を減らすことができます。

タグ	説明
same_source_ip	送信元のIPアドレスが同じになるように指定します。
same_dest_ip	送信先のIPアドレスが同じになるように指定します。
same_dst_port	送信先のポートが同じになるように指定します。
same_location	場所 (ホスト名またはAgent名) が同じになるように指定します。
same_user	デコードされるユーザ名が同じになるように指定します。
same_id	デコードされるIDが同じになるように指定します。

複合ルールが特定のルールIDではなく、すべての認証失敗に対してアラートを出すようにしたい場合、<if_matched_sid></if_matched_sid>タグを<if_matched_ group></if_matched_ group>タグに置き換えることができます。これにより、authentication_ failureのようなカテゴリを指定して、インフラ全体で認証失敗を検索することができます。

```
<rule id="100130" level="10" frequency="5" timeframe="600"> <if_matched_group>authentication_ failure</if_matched_group> <same_source_ip /> <description>5 Failed passwords within 10 minutes</description> </rule>
```

<if_matched_sid></if_matched_sid>タグと<if_matched_group></if_matched_ group>タグに加えて、<if_matched_regex></if_matched_regex>タグを使用して、受信したログを検索するための正規表現を指定することもできます。

```
<rule id="100130" level="10" frequency="5" timeframe="600"> <if_matched_regex>^Failed password</if_matched_regex> <same_source_ip /> <description>10分以内に5回のパスワード失敗 </description> </rule>
```

例

Deep Securityには、数多くの一般的なアプリケーションおよび一般的なアプリケーションの セキュリティログ監視 初期設定ルールが多数含まれています。新しいルールは、セキュリティアップデートを使用して定期的に追加できます。 セキュリティログ監視 ルールでサポートされるアプリケーションのリストが増加しているにもかかわらず、サポートされていないアプリケーションまたはカスタムアプリケーションのカスタムルールを作成する必要が生じる場合があります。

次の例では、Microsoft Windowsサーバー上でIISとNetプラットフォームを使用してホストされるカスタムCMS (コンテンツ管理システム) を作成し、データリポジトリとしてMicrosoft SQLサーバーデータベースを使用します。

最初に、次に示すアプリケーションログの属性を特定します。

1. アプリケーションログを記録する場所
2. どの セキュリティログ監視 デコーダを使用してログファイルを復号できますか?
3. ログファイル メッセージの一般的な形式

CMSの例について、回答は以下の通りです。

1. Windowsイベントビューア
2. Windowsイベントログ (eventlog)
3. Windowsイベントログ形式 (次のコア属性を使用)
    - ソース: CMS
    - カテゴリ: なし
    - イベント:<Application Event ID>

次に、アプリケーションの機能別にログイベントのカテゴリを特定し、そのカテゴリを監視用のカスケードグループの階層に分類します。監視対象のすべてのグループでイベントを発生させる必要はなく、一致する項目を条件文として使用できます。各グループについて、ルールで照合条件として使用できるログ形式の属性を特定します。これは、すべてのアプリケーションログの、ログイベントのパターンおよび論理分類を調べて実行することもできます。

例えば、CMSアプリケーションは以下の機能をサポートしており、それに対してセキュリティログ監視ルールが作成されています。

- CMSアプリケーションログ (ソース: CMS)
    - 認証 (イベント: 100 ~ 119)
        - ユーザログインの成功 (イベント: 100)
        - ユーザログインの失敗 (イベント: 101)
        - 管理者ログインの成功 (イベント: 105)
        - 管理者ログインの失敗 (イベント: 106)
    - 一般エラー (種類: エラー)
        - データベースエラー (イベント: 200 ~ 205)
        - ランタイムエラー (イベント: 206 ~ 249)
    - アプリケーション監査 (種類: 情報)
        - コンテンツ
            - 新しいコンテンツの追加 (イベント: 450 ~ 459)
            - 既存のコンテンツの変更 (イベント: 460 ~ 469)
            - 既存のコンテンツの削除 (イベント: 470 ~ 479)

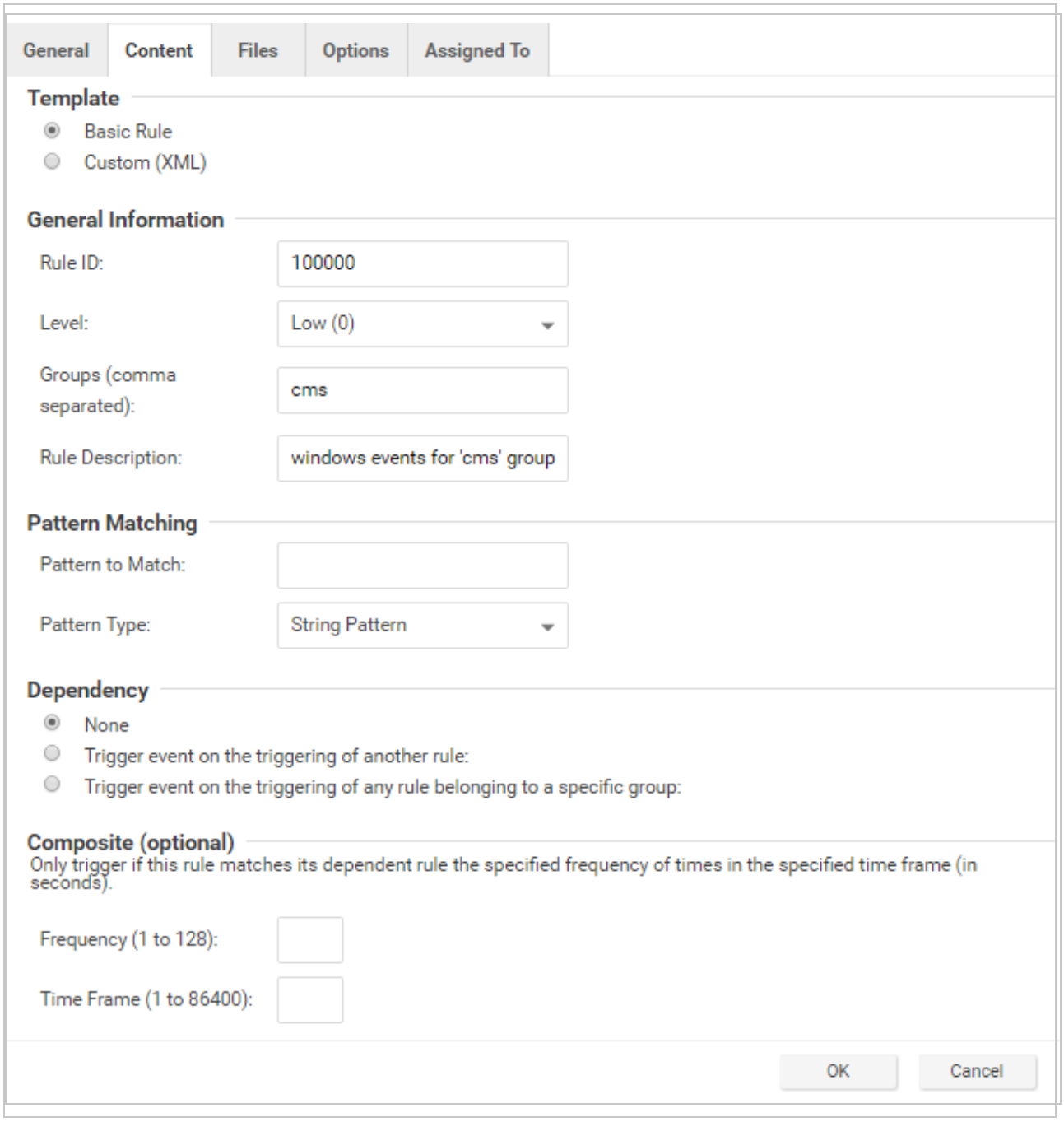
- 管理
  - User
    - 新しいユーザの作成 (イベント: 445 ~ 446)
    - 既存のユーザの削除 (イベント: 447 ~ 449)

この構造は、ルール作成のための良い基盤を提供します。これで、Deep Security Managerで新しいセキュリティログ監視ルールを作成できます。

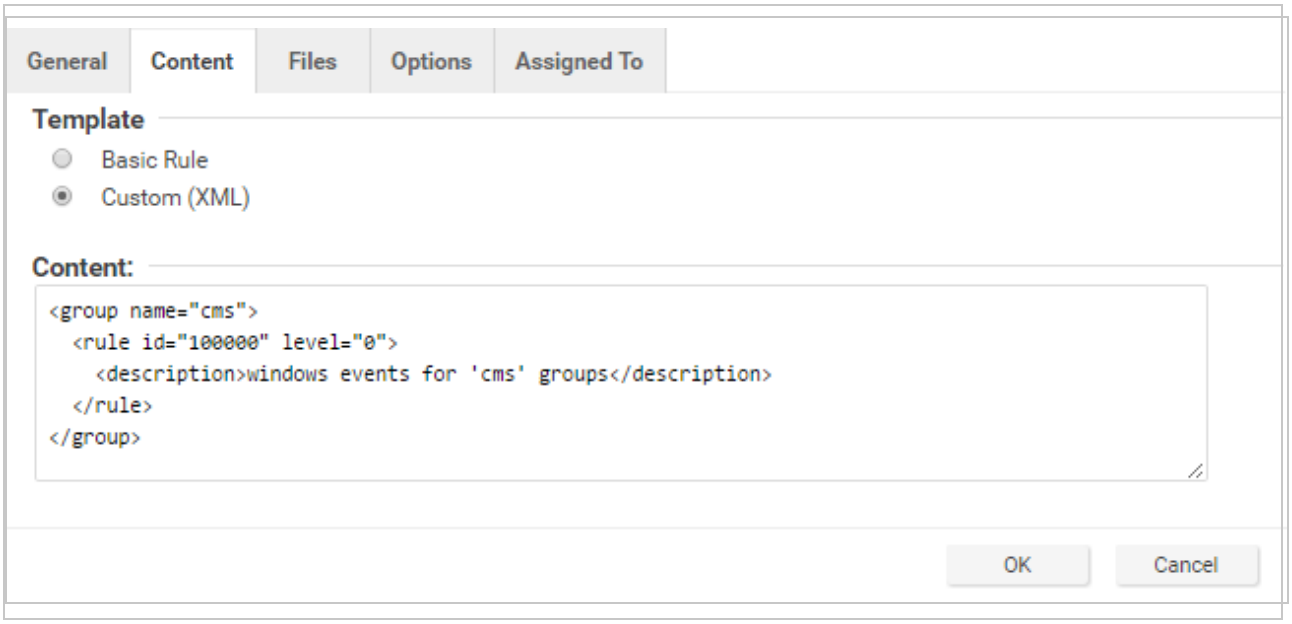
新しいCMSセキュリティログ監視ルールを作成するには

1. Deep Security Managerで、ポリシー > 共通オブジェクト > ルール > セキュリティログ監視ルールに移動し、新規をクリックして新規セキュリティログ監視ルールのプロパティウィンドウを表示します。
2. 新しいルールに名前と説明を付けて、コンテンツタブを選択してください。
3. 基本ルールを選択します。新しいカスタムルールを作成する最も簡単な方法は、基本ルールテンプレートから始めることです。
4. ルールIDフィールドには、カスタムルール用に予約された100,000以上の未使用ID番号が自動的に入力されます。
5. [レベル] を [低 (0)] に設定します。
6. ルールに適切なグループ名を指定します。ここでは「cms」とします。

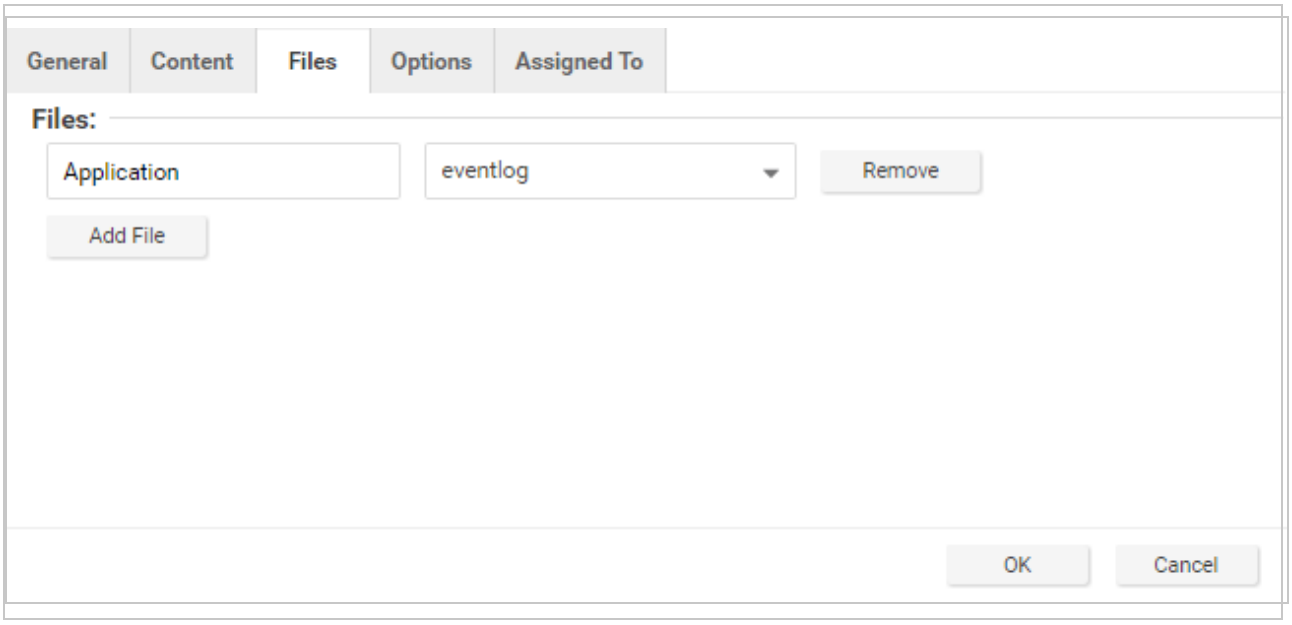
7. ルールの簡単な説明を入力します。



8. カスタム (XML)を選択します。基本ルールで選択したオプションがXMLに変換されます。



9. ファイルタブを選択し、ファイルを追加をクリックして、ルールを適用するアプリケーションログファイルとログタイプを追加します。この場合、ファイルタイプとしてアプリケーションとeventlogを選択します。



EventlogはDeep Securityにおけるユニークなファイルタイプです。なぜなら、ログファイルの場所やファイル名を指定する必要がないからです。代わりに、Windowsイベントビューアに表示されるログ名を入力するだけで十分です。Eventlogファイルタイプの他のログ名には、Security、

System、Internet Explorer、またはWindowsイベントビューアにリストされている他のセクションが含まれることがあります。他のファイルタイプでは、ログファイルの場所とファイル名が必要です。C/C++のstrftime () 変換指定子は、ファイル名の一致に利用可能です。より便利なもののリストについては、表を参照してください。

10. [OK] をクリックして基本ルールを保存します。
11. 基本ルールCustom (XML) を作成したら、以前に特定されたロググループに基づいてグループに新しいルールを追加し始めることができます。基本ルールの基準を初期ルールに設定する必要があります。次の例では、CMS基本ルールがCMSのSource属性を持つWindowsイベントログを特定しています。

    ```
    <group name="cms"> <rule id="100000" level="0"> <category>windows</category> <extra_data>^CMS</extra_data> <description>Windows events from source 'CMS' group messages.</description> </rule>
    ```

12. 識別されたロググループから後続のルールを構築して進めます。次の例では、認証とログインの成功および失敗をイベントIDで識別し、ログに記録します。

    ```
    <rule id="100001" level="0"> <if_sid>100000</if_sid> <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id> <group>authentication</group> <description>CMS認証イベント。</description> </rule> <rule id="100002" level="0"> <if_group>authentication</if_group> <id>100</id> <description>CMSユーザーログイン成功イベント。</description> </rule> <rule id="100003" level="4"> <if_group>authentication</if_group> <id>101</id> <group>authentication_failure</group> <description>CMSユーザーログイン失敗イベント。</description> </rule> <rule id="100004" level="0"> <if_group>authentication</if_group> <id>105</id> <description>CMS管理者ログイン成功イベント。</description> </rule> <rule id="100005" level="4"> <if_group>authentication</if_group> <id>106</id> <group>authentication_failure</group> <description>CMS管理者ログイン失敗イベント。</description> </rule>
    ```

13. 確立されたルールを使用して、任意の複合または相関ルールを追加します。次の例は、10秒間に5回のログイン失敗が発生した場合に適用される高重大度の複合ルールを示しています。

    ```
    <rule id="100006" level="10" frequency="5" timeframe="10"> <if_matched_group>authentication_failure</if_matched_group> <description>CMS繰り返し認証ログイン失敗イベント。</description> </rule>
    ```

14. すべてのルールの重要度レベルが適切かどうかを確認します。たとえば、エラーログの重要度はレベル5以上でなければなりません。情報ルールの重要度は低くなります。
15. 新しく作成したルールを開き、Configurationタブを選択し、カスタムルールのXMLをルールフィールドにコピーします。適用またはOKをクリックして変更を保存します。

ルールがポリシーまたはコンピュータに割り当てられると、セキュリティログ監視 エンジンは、指定されたログファイルの検査をただちに開始します。

完成したカスタムCMSセキュリティログ監視ルール:

```
<group name="cms">
 <rule id="100000" level="0"> <category>windows</category> <extra_data>^CMS</extra_data>
<description>Windows events from source 'CMS' group messages.</description> </rule>
 <rule id="100001" level="0"> <if_sid>100000</if_sid>
<id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id> <group>authentication</group>
<description>CMS Authentication event.</description> </rule> <rule id="100002" level="0"> <if_
group>authentication</if_group> <id>100</id> <description>CMS User Login success
event.</description> </rule> <rule id="100003" level="4"> <if_group>authentication</if_group>
<id>101</id> <group>authentication_failure</group> <description>CMS User Login failure
event.</description> </rule> <rule id="100004" level="0"> <if_group>authentication</if_group>
<id>105</id> <description>CMS Administrator Login success event.</description> </rule> <rule
id="100005" level="4"> <if_group>authentication</if_group> <id>106</id> <group>authentication_
failure</group> <description>CMS Administrator Login failure event.</description> </rule> <rule
id="100006" level="10" frequency="5" timeframe="10"> <if_matched_group>authentication_failure</if_
matched_group> <description>CMS Repeated Authentication Login failure event.</description> </rule>
<rule id="100007" level="5"> <if_sid>100000</if_sid> <status>^ERROR</status> <description>CMS
General error event.</description> <group>cms_error</group> </rule> <rule id="100008" level="10">
<if_group>cms_error</if_group> <id>^200|^201|^202|^203|^204|^205</id> <description>CMS Database
error event.</description> </rule> <rule id="100009" level="10"> <if_group>cms_error</if_group>
<id>^206|^207|^208|^209|^230|^231|^232|^233|^234|^235|^236|^237|^238|
^239^|240|^241|^242|^243|^244|^245|^246|^247|^248|^249</id> <description>CMS Runtime error
event.</description> </rule> <rule id="100010" level="0"> <if_sid>100000</if_sid>
<status>^INFORMATION</status> <description>CMS General informational event.</description>
<group>cms_information</group> </rule> <rule id="100011" level="5"> <if_group>cms_information</if_
group> <id>^450|^451|^452|^453|^454|^455|^456|^457|^458|^459</id> <description>CMS New Content
added event.</description> </rule> <rule id="100012" level="5"> <if_group>cms_information</if_group>
<id>^460|^461|^462|^463|^464|^465|^466|^467|^468|^469</id> <description>CMS Existing Content
modified event.</description> </rule> <rule id="100013" level="5"> <if_group>cms_information</if_
group> <id>^470|^471|^472|^473|^474|^475|^476|^477|^478|^479</id> <description>CMS Existing
Content deleted event.</description> </rule> <rule id="100014" level="5"> <if_group>cms_
information</if_group> <id>^445|^446</id> <description>CMS User created event.</description> </rule>
<rule id="100015" level="5"> <if_group>cms_information</if_group> <id>^447|449</id>
<description>CMS User deleted event.</description> </rule> </group>
```

セキュリティログ監視 ルールの重大度レベルと推奨される使用

レベル	説明	備考
レベル	無視され、	主に誤判定を回避するために使用されます。これらのルールは、他のすべての

レベル	説明	備考
0	処理は行われない	ルールより先に検索され、セキュリティとは無関係のイベントが含まれます。
レベル 1	事前定義された使用法はなし	
レベル 2	システムの優先度の低い通知	セキュリティとは無関係のシステム通知またはステータスメッセージ。
レベル 3	成功した/承認されたイベント	成功したログイン試行、ファイアウォール許可イベントなど。
レベル 4	システムの優先度の低いエラー	不正な設定または未使用のデバイス/アプリケーションに関連するエラー。セキュリティとは無関係であり、通常は初期設定のインストールまたはソフトウェアのテストが原因で発生します。
レベル 5	ユーザによって生成されたエラー	パスワードの見落とし、アクションの拒否など。これらのメッセージは通常、セキュリティに関連しません。
レベル 6	関連性の低い攻撃	システムに脅威を及ぼさないワームまたはウイルスを示します (Linuxサーバを攻撃するWindowsワームなど)。また、頻繁にトリガされるIDSイベントおよび一般的なエラーイベントも含まれます。
レベル 7	事前定義された使用法はなし	
レベル 8	事前定義された使用法はなし	
レベル 9	無効なソースからのエラー	不明なユーザとしてのログインの試行または無効なソースからのログインの試行が含まれます。特にこのメッセージが繰り返される場合は、セキュリティとの関連性がある可能性があります。また、adminまたはrootアカウントに関するエラーも含まれます。
レベル 10	ユーザによって生成された複数のエラー	複数の不正なパスワードや複数のログイン失敗などを含めてください。それらは攻撃を示している可能性もありますし、単にユーザが資格情報を忘れた可能性もあります。
レベル 11	事前定義された使用法はなし	
レベル 12	重要度の高いイベント	システムやカーネルなどからのエラーまたは警告メッセージを含めます。これらは特定のアプリケーションに対する攻撃を示している可能性があります。
レベル 13	通常と異なるエラー (重要度: 高)	バッファオーバーフローの試行などの一般的な攻撃パターン、通常のSyslogメッセージ長の超過、または通常のURL文字列長の超過。
レベル 14	重要度の高いセキュリ	通常、複数の攻撃ルールと攻撃の兆候が組み合わさったもの。

レベル	説明	備考
	ティイベント	
レベル 15	攻撃の成功	誤判定の可能性はほとんどありません。すぐに対処が必要です。

strftime () 変換指定子

指定子	説明
%a	省略された曜日名 (例: 木)
%A	曜日の完全な名前 (例: 木曜日)
%b	省略された月名 (例: Aug)
%B	月の完全な名前 (例: 8月)
%c	日付と時刻の表記 (例: Thu Sep 22 12:23:45 2007)
%d	月の日 (01 - 31) (例: 20)
%H	24時間形式の時刻 (00 - 23) (例: 13)
%I	12時間形式の時 (01 - 12)(例: 02)
%j	年の日数 (001 - 366) (例: 235)
%m	月を10進数で表したもの (01 - 12)(例: 02)
%M	分 (00 - 59) (例えば、12)
%p	午前または午後の指定 (例: AM)
%S	秒 (00 - 61) (例: 55)
%U	最初の日曜日を週の初日とする週番号 (00 - 53) (例: 52)
%w	日曜日を0とする10進数の曜日 (0 - 6) (例: 2)
%W	最初の月曜日を週の初日とする週番号 (00 - 53) (例: 21)
%x	日付表記 (例: 02/24/79)
%X	時間表記 (例: 04:12:51)
%y	年、西暦の下2桁 (00 - 99)(例: 76)
%Y	年 (例: 2008)
%Z	タイムゾーン名または略語 (例: EST)
%%	% 記号 (例えば、%)

詳細については、以下を参照してください。

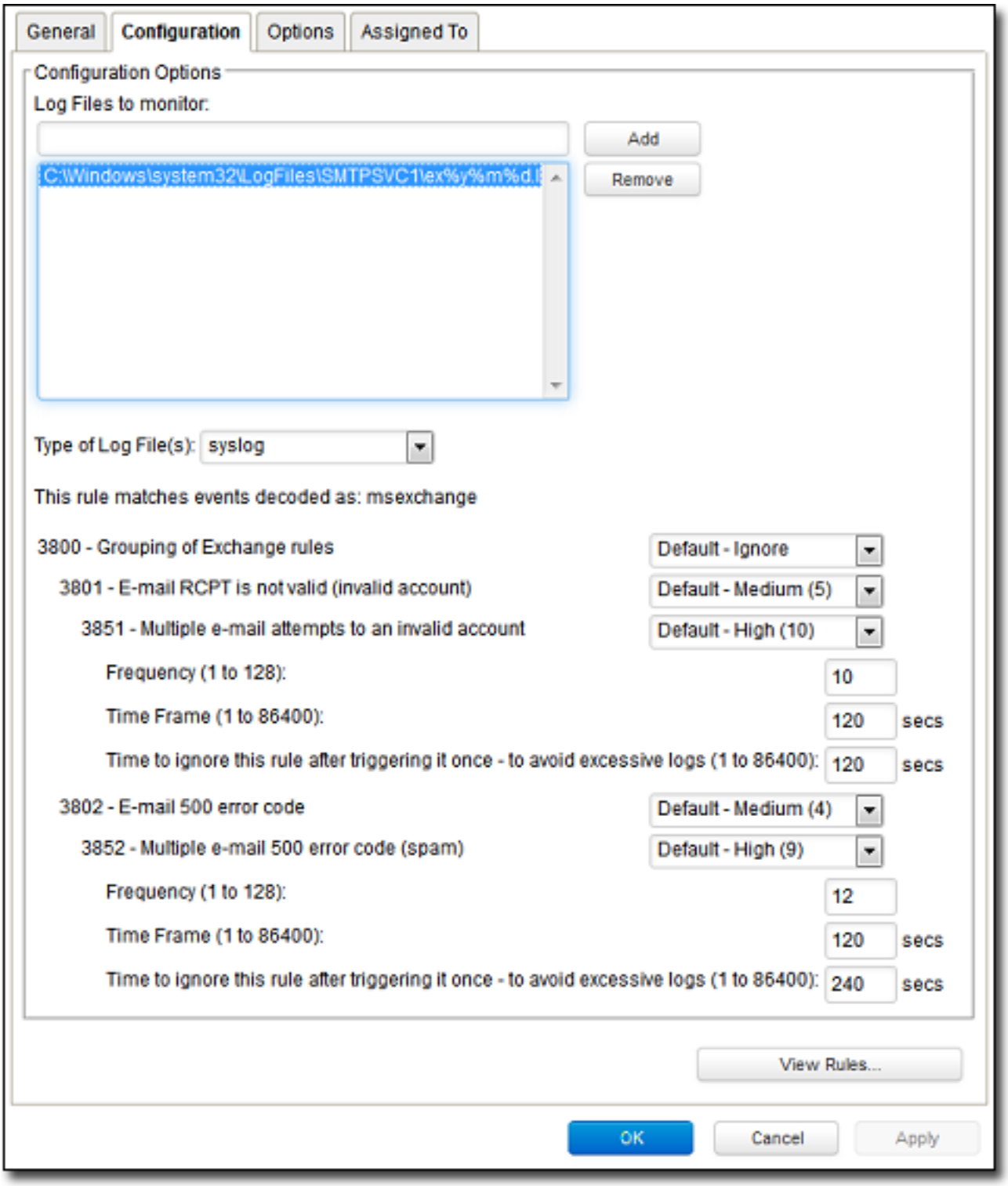
- https://www.php.net/manual/en/function.strftime.php
- www.cplusplus.com/reference/clibrary/ctime/

セキュリティログ監視 ルールを調べる

セキュリティログ監視ルールは、Deep Security Managerのポリシー > 共通オブジェクト > ルール > セキュリティログ監視ルールにあります。

セキュリティログ監視 のルール構造とイベント照合プロセス

次の図は、Microsoft Exchangeセキュリティログ監視ルールのプロパティウィンドウの構成タブの内容を示しています。


General
Configuration
Options
Assigned To
Configuration Options
Log Files to monitor:
Add
Remove
C:\Windows\system32\LogFiles\SMTPSVC1\ex%y%m%d.l
Type of Log File(s): syslog
This rule matches events decoded as: msexchange
3800 - Grouping of Exchange rules
Default - Ignore
3801 - E-mail RCPT is not valid (invalid account)
Default - Medium (5)
3851 - Multiple e-mail attempts to an invalid account
Default - High (10)
Frequency (1 to 128): 10
Time Frame (1 to 86400): 120 secs
Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400): 120 secs
3802 - E-mail 500 error code
Default - Medium (4)
3852 - Multiple e-mail 500 error code (spam)
Default - High (9)
Frequency (1 to 128): 12
Time Frame (1 to 86400): 120 secs
Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400): 240 secs
View Rules...
OK
Cancel
Apply

以下はルール構造です:

- 3800 - Grouping of Exchange Rules - Default - ignore
  - 3801 - Email rcpt is not valid (invalid account) - Default - Medium (5)
    - 3851 - Multiple email attempts to an invalid account - Default - High (10)
      - Frequency (1 to 128) - 10
      - Time Frame (1 to 86400) - 120
      - Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400) - 120
  - 3802 - Email 500 error code - Default - Medium (4)
    - 3852 - Email 500 error code (spam) - Default - High (9)
      - Frequency (1 to 128) - 12
      - Time Frame (1 to 86400) - 120
      - Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400) - 240

セキュリティログ監視エンジンはログイベントをこの構造に適用し、一致があるかどうかを確認します。例えば、Exchangeイベントが発生し、このイベントが無効なアカウントへのメール受信である場合、イベントは行3800と一致します (これはExchangeイベントであるためです)。その後、イベントは行3800のサブルール3801および3802に適用されます。

これ以上の一致がない場合、この一致のカスケードは3800で停止します。3800は無視の重大度レベルであるため、セキュリティログ監視イベントは記録されません。

しかし、無効なアカウントへのメール受信は3800のサブルールの1つ、サブルール3801に一致します。サブルール3801の重大度レベルは中 (4) です。ここで一致が停止した場合、重大度レベルが中 (4) のセキュリティログ監視イベントが記録されます。

しかし、イベントに適用される別のサブルールがあります: サブルール3851です。サブルール3851は、3つの属性を持ち、同じイベントが過去120秒以内に10回発生した場合に一致します。その場合、セキュリティログ監視イベントが重大度高 (9) で記録されます。無視属性は、次の120秒間、サブルール3801に一致する個々のイベントを無視するようにサブルール3851に指示します。これはノイズを減らすのに役立ちます。

サブルール3851のパラメータが一致したと仮定すると、セキュリティログ監視イベントが重大度高 (9) で記録されました。

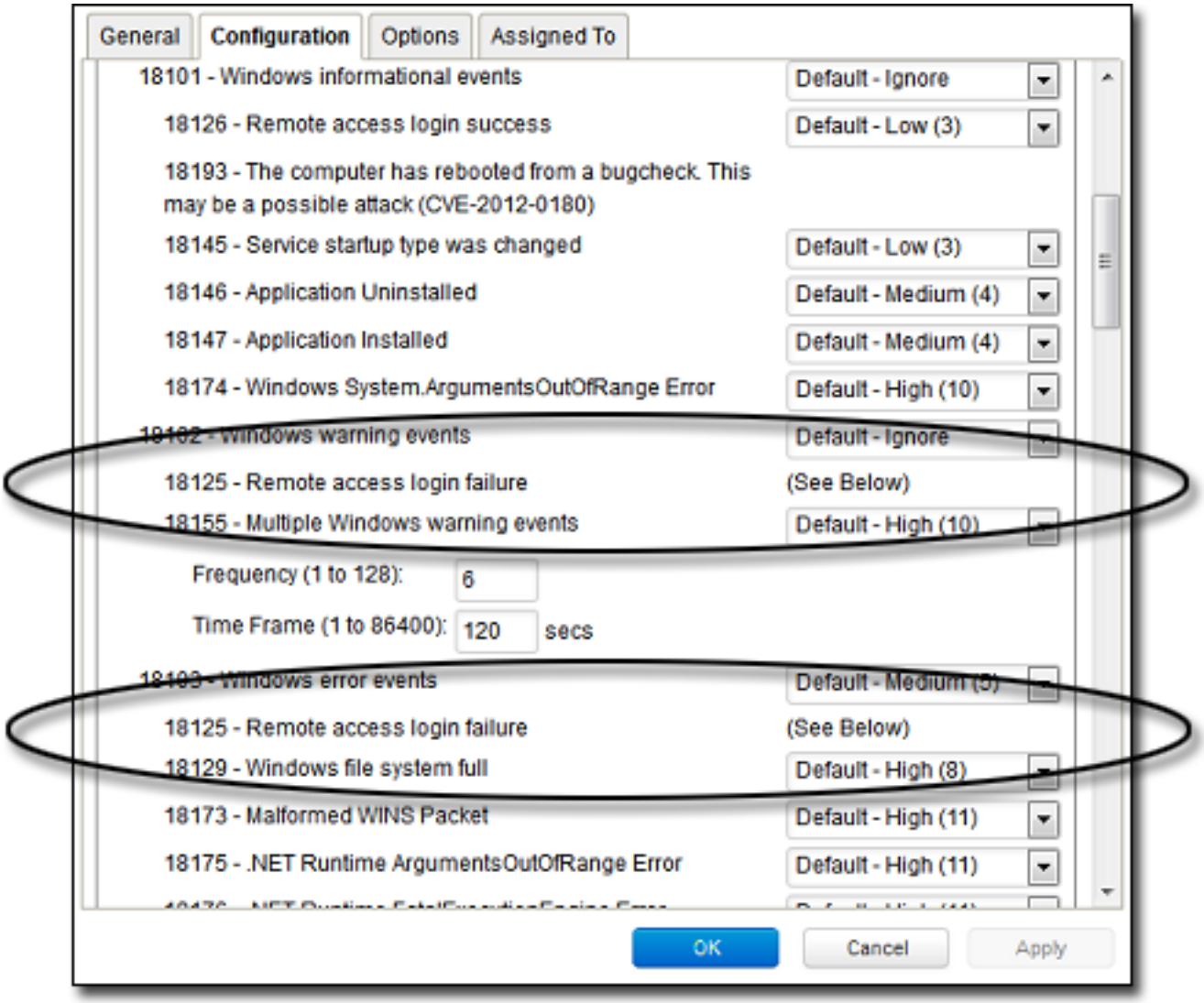
Microsoft Exchangeルールのオプションタブを確認すると、Deep Security Managerは重大度レベルが中 (4) のサブルールが一致した場合にアラートを発することがわかります。この例ではその通りなので、

アラートが発せられます(このルールがイベントを記録したときにアラートを出すが選択されている場合)。

重複するサブルール

一部のセキュリティログ監視ルールには重複するサブルールがあります。例を見るには、Microsoft Windows Eventsルールを開き、設定タブを選択してください。サブルール18125(リモートアクセスログイン失敗)がサブルール18102と18103の下に表示されることに注意してください。また、どちらの場合もサブルール18125には重大度の値がなく、「以下を参照」とだけ表示されることに注意してください。

重複して表示されるのではなく、ルール18125は、[設定]画面の下部に1回だけ表示されています。



アプリケーションコントロールを設定する

アプリケーションコントロール

注意: Deep Security Agent 10.0以上を実行しているコンピュータのアプリケーションコントロールを有効にできます。アプリケーションコントロールがサポートされるOSのリストについては、"各プラットフォームでサポートされている機能" on page 417を参照してください。

アプリケーションコントロールは、保護対象サーバのソフトウェア変更を継続的に監視します。ポリシー設定に基づいて、アプリケーション制御は、許可されていないソフトウェアが明示的に許可されるまで実行されないようにしたり、許可されていないソフトウェアが明示的にブロックされるまで許可したりしないようにします。選択するオプションは、使用環境に必要なコントロールレベルに応じて異なります。

警告: アプリケーションコントロールは、継続的にサーバを監視し、ソフトウェアの変更が生じるたびにイベントをログに記録します。これは、一部のWebサーバやメールサーバなど、自動的に変更されるソフトウェアを使用する環境や通常実行可能ファイルを作成する環境には向いていません。アプリケーションコントロールがお使いの環境に適しているかどうかを確認するには、"アプリケーションコントロールで検出されるソフトウェア変更" on page 1098を参照してください。

ヒント: Deep Security APIを使用してアプリケーションコントロールの作成と構成を自動化できます。詳細については、Deep Security Automation Centerのアプリケーションコントロールの構成ガイドを参照してください。

主な概念

対象となる保護の状態: アプリケーションコントロールの設定時に必要な主な決定事項の1つに、対象となる保護の状態の決定があります。新規または変更されたすべてのソフトウェアについて、許可するように手動で指定するまで実行されないようにしますか。または、明示的にブロックするまで初期設定で実行しますか。はじめてアプリケーションコントロールを有効にしたときに、承認されていないソフトウェアが大量にある場合、承認されていないソフトウェアを最初に許可する方法があります。アプリケーションコントロールルールを追加して、承認されていないソフトウェアの量を減らすと、ブロックモードに切り替えることができます。

アプリケーションコントロールルール: ルールは、特定のコンピュータでのソフトウェアの許可またはブロックを指定します。

インベントリ: コンピュータにインストールされ、実行を許可されたソフトウェアの初期リストです。許可するソフトウェアのみをコンピュータにインストールするようにしてください。アプリケーション制御を有効にす

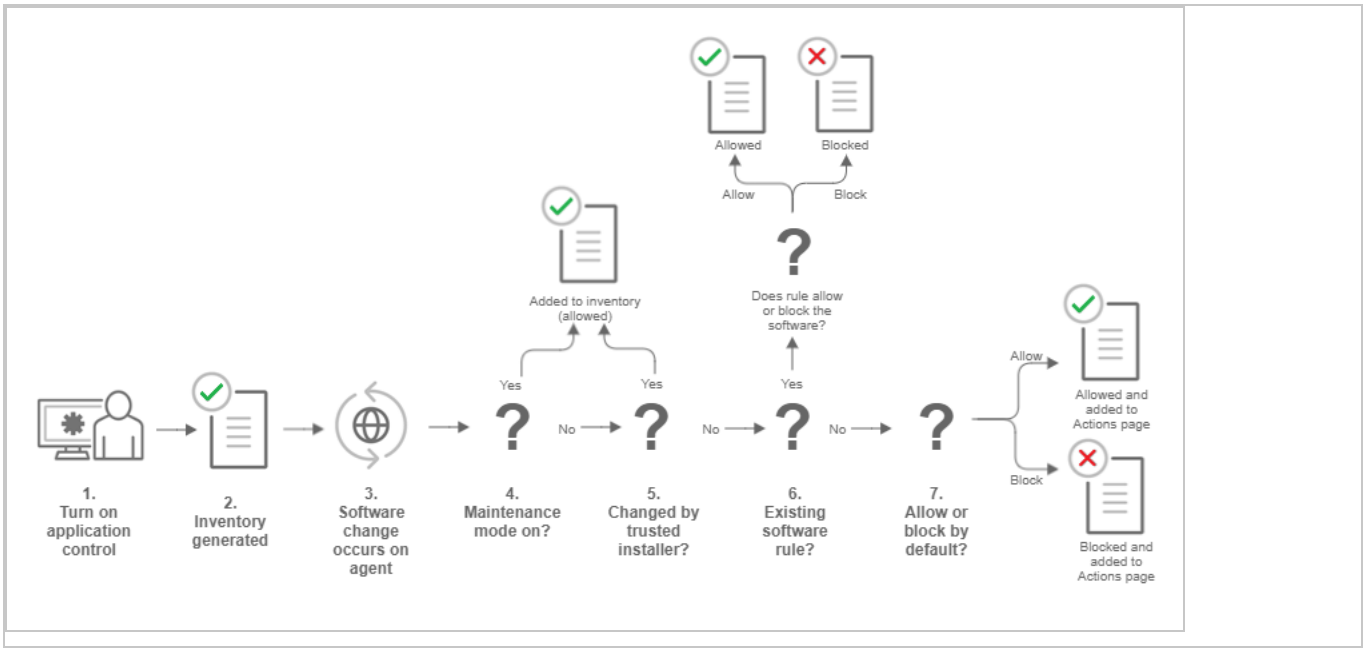
ると、現在インストールされているすべてのソフトウェアがコンピュータのインベントリに追加され、実行が許可されます。コンピュータがメンテナンスモードの場合、コンピュータに対するソフトウェアの変更がコンピュータのインベントリに追加され、実行されるようになります。コンピュータのソフトウェアインベントリはDeep Security Agentに格納されており、Deep Security Managerには表示されません。

認識されないソフトウェア: コンピュータのインベントリに登録されていないソフトウェアで、アプリ制御ルールで保護されていないソフトウェアです。"アプリケーションコントロールで検出されるソフトウェア変更" on page 1098を参照してください。

メンテナンスモード: ソフトウェアのインストールまたはアップデートを予定している場合は、メンテナンスモードをオンにすることをお勧めします。メンテナンスモードでは、アプリケーション制御は引き続きアプリケーションコントロールルールによってブロックされたソフトウェアをブロックしますが、新しいソフトウェアまたはアップデートされたソフトウェアを実行してコンピュータのインベントリに追加することができます。"変更の計画時にメンテナンスモードをオンにする" on page 1104を参照してください。

注意: システム全体のセキュリティを強化するために、インベントリにはリモートファイルシステム上のソフトウェアは含まれず、メンテナンスモードではリモートファイルシステムからの新規またはアップデートされたソフトウェアが自動的に許可されません。リモートファイルシステムのソフトウェアは、インベントリに手動で追加する必要があります。

アプリケーションコントロールの仕組み



1. ポリシーでアプリケーションコントロールを有効にして、Deep Security Agentで保護されているコンピュータにこのポリシーを割り当てます ("アプリケーションコントロールを有効にする" on page 1100

を参照)。

2. エージェントはポリシーを受信すると、コンピュータにインストールされているすべてのソフトウェアのインベントリを作成します。インベントリに記載されているすべてのソフトウェアは安全であるとみなされ、そのコンピュータで実行できるようになります。このインベントリリストはDeep Security Managerからは表示されません。つまり、アプリケーション制御を有効にするコンピュータに適切なソフトウェアのみがインストールされていることを確認する必要があります。
3. インベントリの作成後、アプリケーションコントロールでコンピュータのあらゆるソフトウェア変更が認識されます。ソフトウェア変更により、新しいソフトウェアがコンピュータに表示されたり、既存のソフトウェアに変更が加えられたりします。
4. コンピュータがメンテナンスモードの場合、Deep Security Agentはそのソフトウェアをインベントリリストに追加し、実行を許可します。この変更はDeep Security Managerでは表示できません。"変更の計画時にメンテナンスモードをオンにする" on page 1104を参照してください。
5. 信頼されたインストーラによって変更が行われた場合、Deep Security Agentはそのソフトウェアをインベントリリストに追加して実行します。たとえば、Microsoft Windowsがコンポーネントアップデートを自己始動する場合、数百の新しい実行可能ファイルがインストールされます。アプリケーションコントロールは、既知のWindowsプロセスによって作成された多くのファイル変更を自動認証しますが、Deep Security Managerにはこの変更は表示されません。想定されるソフトウェア変更に関連する「ノイズ」を削除すると、注意が必要な変更を明確に確認できます。

   注意: 信頼済みのインストーラ機能はDeep Security Agent 10.2以上で利用可能です。

6. コンピュータのルールセットに適切なソフトウェアのルールが含まれる場合、ソフトウェアは実行されるルールに従って許可またはブロックされます。"アプリケーションコントロールで検出されるソフトウェア変更" on page 1098を参照してください。
7. ソフトウェアがコンピュータのインベントリにない場合に、既存のルールで保護されていないソフトウェアは、認識されないソフトウェアとみなされます。コンピュータに割り当てられたポリシーでは、承認されていないソフトウェアの処理方法を指定します。ポリシー設定に応じて、実行が許可またはブロックされます。ソフトウェアがブロックされ、OSにエラーメッセージを表示できる場合、そのソフトウェアの実行が許可されない、またはアクセスが拒否されたことを示すエラーメッセージが保護対象のコンピュータに表示されます。

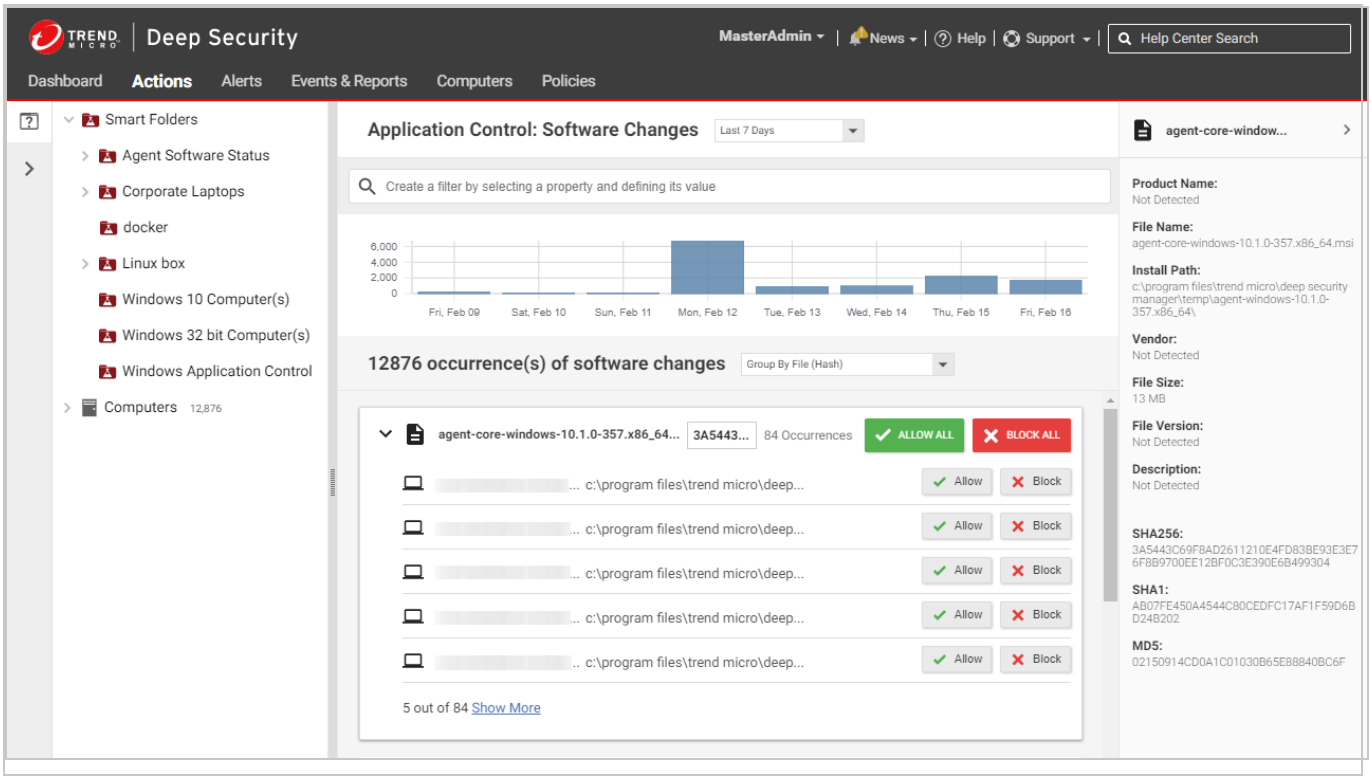
   承認されていないソフトウェアは、Deep Security Managerの [アプリケーションコントロール - ソフトウェア変更] 画面に表示されます。この画面で、管理者は [許可] または [ブロック] をクリックし、特定のコンピュータに対して該当のソフトウェアの許可ルールまたはブロックルールを作成できます。許可ルールまたはブロックルールは、ポリシーで指定された初期設定アクションよりも優先されます。"新規および変更済みソフトウェアを監視する" on page 1101を参照してください。

アプリケーションコントロールインタフェースの紹介

Deep Security Managerには、アプリケーションコントロールに関連する変更を確認できる場所があります。

- "アプリケーションコントロール: ソフトウェア変更 ([処理])" below
- "アプリケーションコントロールルールセット" on the next page
- "セキュリティイベント" on page 1098

アプリケーションコントロール: ソフトウェア変更 ([処理])

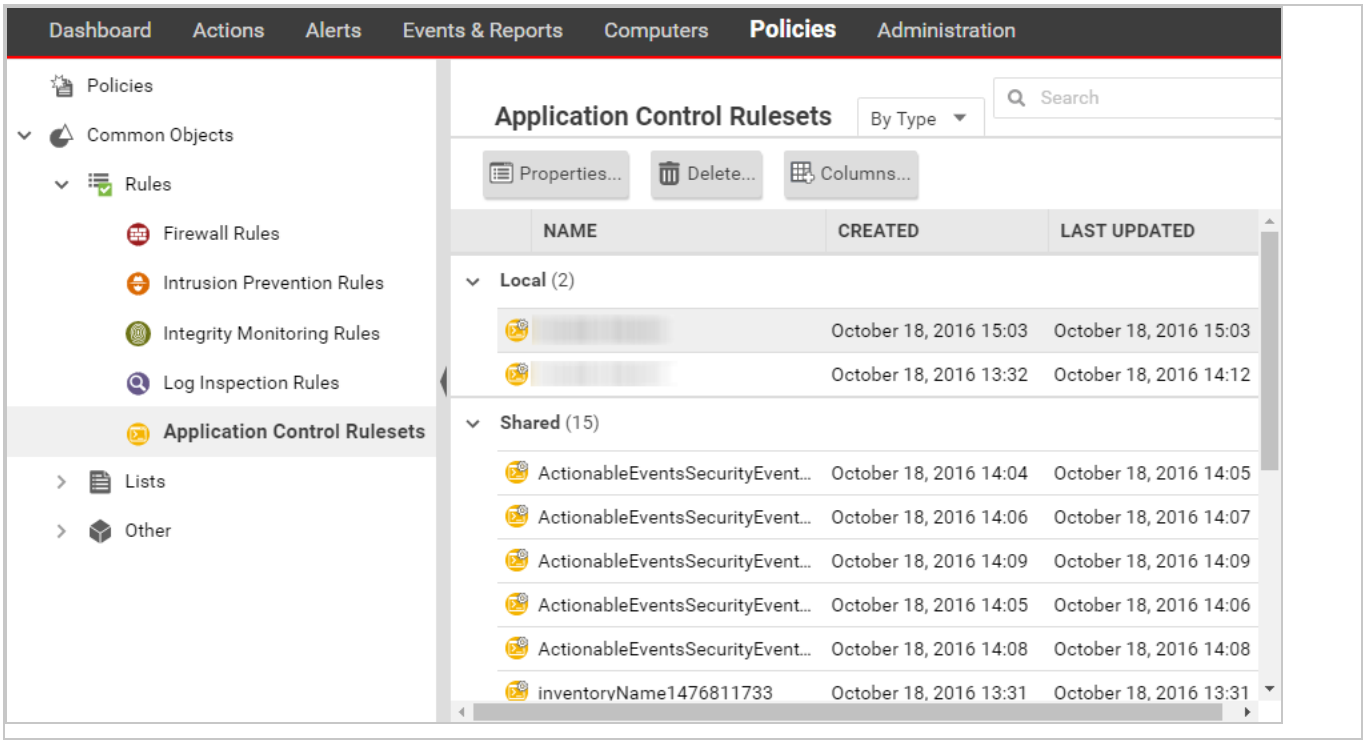


[アプリケーションコントロール: ソフトウェア変更]画面は、Deep Security Managerの [処理] をクリックすると表示されます。すべての認識されないソフトウェア(コンピュータのインベントリにないソフトウェアで、対応するアプリケーション制御ルール).がないソフトウェアが表示されます。ソフトウェア変更はコンピュータレベルで許可またはブロックされるため、特定のソフトウェアを50台のコンピュータにインストールすると、この画面に50回表示されます。ただし、特定のソフトウェアをすべての場所で許可またはブロックする必要がある場合は、[処理] 画面をフィルタしてファイルハッシュ別に変更をソートし、[すべて許可] をクリックしてソフトウェアがインストールされているすべてのコンピュータで許可します。

コンピュータに適用されるポリシーでは、承認されていないソフトウェアの実行を初期設定で許可またはブロックするかを指定しますが、[処理] 画面で [許可] または [ブロック] をクリックするまで、明示的な

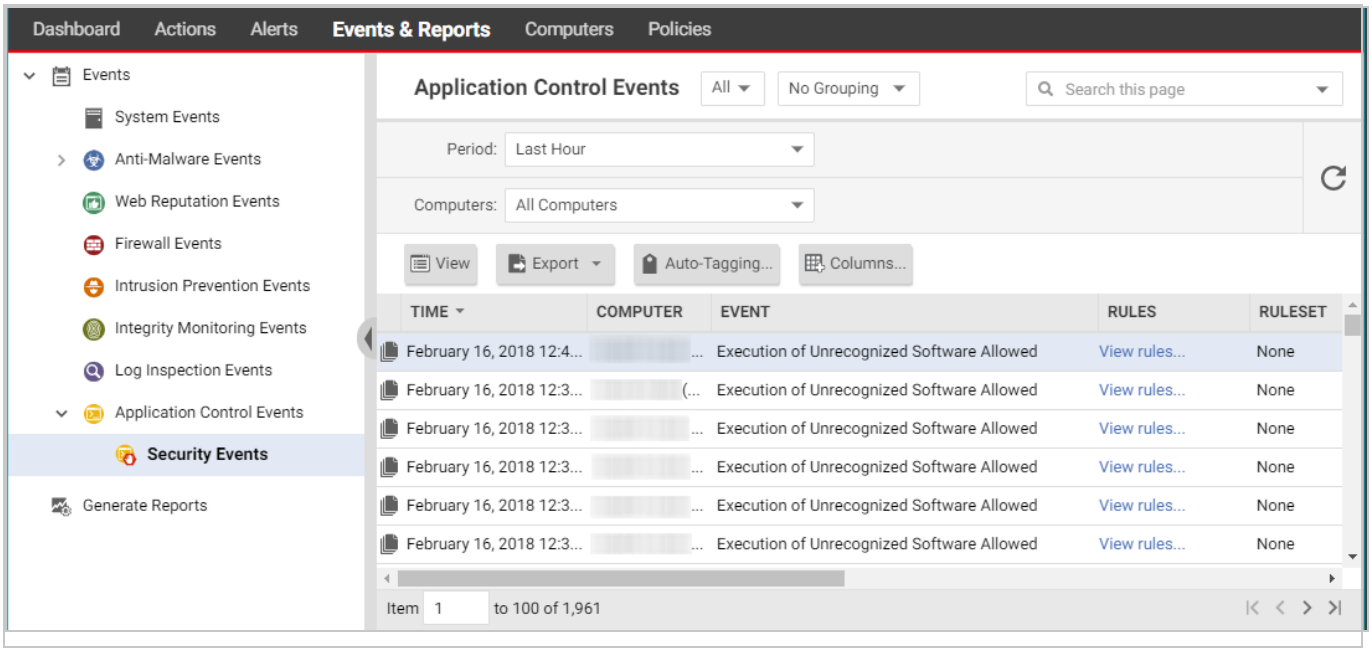
アプリケーションコントロールルールは作成されません。[許可] または [ブロック] をクリックすると、対応するルールがコンピュータのルールセットに表示されます。ルールセットは [アプリケーションコントロールルールセット] 画面に表示されます。

アプリケーションコントロールルールセット



コンピュータのルールセットを確認するには、[ポリシー]→[共通オブジェクト]→[ルール]→[アプリケーションコントロールルールセット] に移動します。ルールセットに含まれるルールを確認するには、ルールセットをダブルクリックして [ルール] タブに移動します。[ルール] タブには、ルールが関連付けられたソフトウェアが表示され、許可ルールをブロックルールに変更したり、ブロックルールを許可ルールに変更したりすることもできます。

セキュリティイベント



[イベント]→[レポート]→[イベント]→[アプリケーションコントロールイベント]→[セキュリティイベント] には、コンピュータで実行された承認されていないソフトウェア、またはブロックルールにより実行されないようにした承認されていないソフトウェアがすべて表示されます。このリストは、期間および他の基準によってフィルタできます。

イベント(集約イベント以外)ごとに、[ルールの表示] をクリックすると、ルールの許可とブロックを切り替えることができます。Deep Security Agent 10.2以上には、同じイベントが繰り返し発生した場合にログの量を減らすためのイベント集約ロジックがあります。

アプリケーションコントロールで検出されるソフトウェア変更

すべてのファイルを監視する変更監視とは異なり、アプリケーションコントロールで初期インストールの調査時と変更の監視時に確認されるのはソフトウェアファイルのみです。

ソフトウェアには次のものも含まれます。

- Windowsアプリケーション(.exe、.com、.dll、.sys)、Linuxライブラリ(.so)、およびその他のコンパイルされたバイナリやライブラリ
- Javaの.jarファイルと.classファイル、およびその他のコンパイルされたバイトコード
- PHP、Python、シェルスクリプト、およびその他の実行時に変換またはコンパイルされるWebアプリやスクリプト

- Windows PowerShellスクリプト、バッチファイル (.bat)、およびその他のWindows専用スクリプト (.wsf、.vbs、.js)

たとえば、WordPressとそのプラグイン、Apache、IIS、nginx、Adobe Acrobat、app.war、/usr/bin/sshは、いずれもソフトウェアとして検出されます。

アプリケーションコントロールは、ファイルの拡張子を確認してスクリプトかどうかを判定します。またLinuxでは、実行権限のあるファイルはスクリプトとみなされます。

注意: Windowsコンピュータでは、アプリケーションコントロールがローカルファイルシステム上の変更を追跡しますが、ネットワーク上の場所、CD/DVDドライブ、USBデバイスの変更は追跡しません。

アプリケーションコントロールはカーネル (Linuxコンピュータ) およびファイルシステムに統合されているため、ルートまたは管理者アカウントでインストールされたソフトウェアを含め、コンピュータ全体を監視する権限があります。監視対象は、ソフトウェアファイルに対するディスク上の書き込みアクティビティとソフトウェアの実行です。

Deep Security Agent 10と11におけるファイルの比較方法の相違点

Deep Security 10 Agentは、新規のソフトウェアやソフトウェアの変更を判定するために、最初にインストールされていたソフトウェアのSHA-256ハッシュ、ファイルサイズ、パス、およびファイル名を比較します (これらには「ファイルベース」のルールセットが使用されています)。Deep Security 11 (およびそれ以降の) Agentは、ファイルのSHA-256ハッシュおよびファイルサイズのみを比較します (これらには「ハッシュベース」のルールセットが使用されています)。Deep Security 11 (およびそれ以降の) Agentで作成されたルールでは、一意のハッシュおよびファイルサイズのみを比較するので、ソフトウェアファイルの名前変更または移動が実行された場合にも、ルールは引き続き適用されます。そのため、Deep Security 11 (およびそれ以降の) Agentを使用すると、処理の必要なソフトウェア変更の数が削減されます。

Deep Security 10 Agentは、Deep Security 11.0以降にアップグレードしない限り、引き続きファイルベースのルールセットを使用します。Agentをバージョン11.0以降にアップグレードすると、そのルールセットはハッシュベースのルールを使用するように変換されます。同じハッシュ値に対するファイルベースのルールが複数ある場合、それらのルールは1つのハッシュベースのルールに統合されます。統合されるルールが相互に競合する場合 (1つのルールがファイルをブロックし、もう1つがそのファイルを許可する場合)、新しいハッシュベースのルールは「許可」ルールになります。

アプリケーションコントロールの設定

警告: アプリケーションコントロールは、継続的にサーバを監視し、ソフトウェアの変更が生じるたびにイベントをログに記録します。これは、一部のWebサーバやメールサーバなど、自動的に変更される

ソフトウェアを使用する環境や通常実行可能ファイルを作成する環境には向いていません。アプリケーションコントロールがお使いの環境に適しているかどうかを確認するには、"アプリケーションコントロールで検出されるソフトウェア変更" on page 1098を参照してください。

アプリケーションコントロールの仕組みについては、"アプリケーションコントロール" on page 1093を参照してください。

アプリケーションコントロールを有効にしてソフトウェア変更を監視するには、次の操作を実行します。

1. "アプリケーションコントロールを有効にする" below
2. "新規および変更済みソフトウェアを監視する" on the next page
3. "変更の計画時にメンテナンスモードをオンにする" on page 1104

この記事では、アプリケーションコントロールを使用する際に注意する必要がある、"アプリケーションコントロールのヒントと注意事項" on page 1105についても説明します。

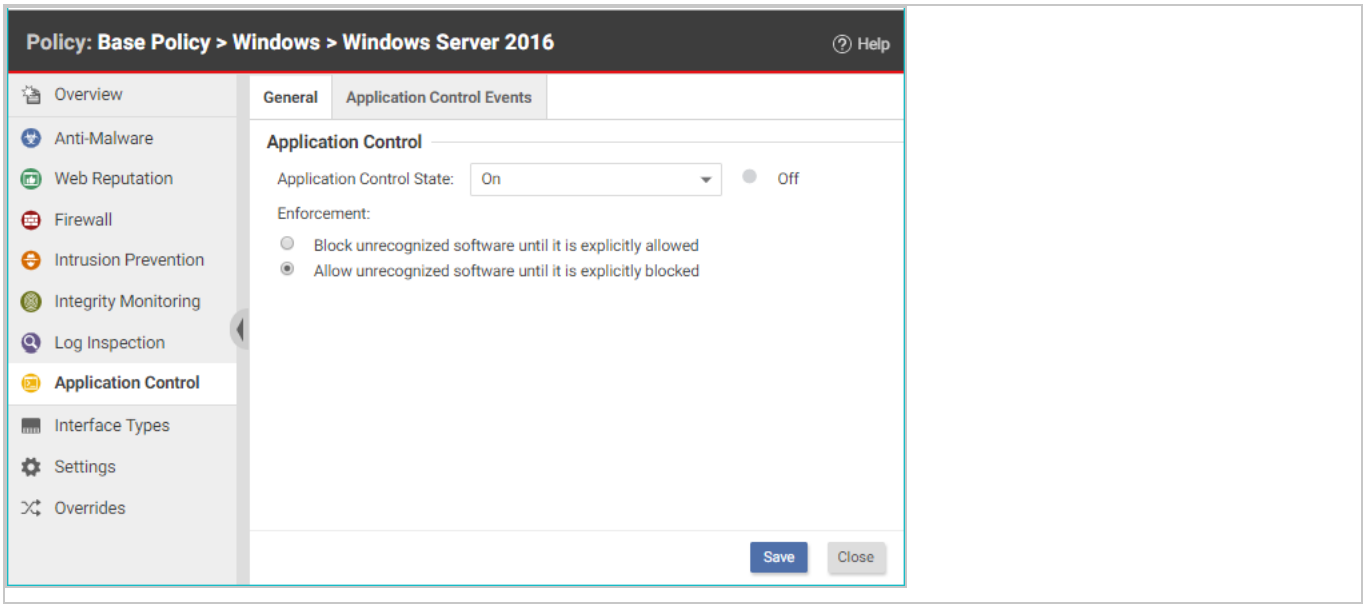
アプリケーションコントロールを有効にした後は、次のことを実行する方法について学ぶこともできます。

- "アプリケーションコントロールルールセットの表示と変更" on page 1110
- "ソフトウェアの変更後にアプリケーションコントロールをリセットする" on page 1141
- "アプリケーションコントロールイベントの監視" on page 1107
- "共有ルールセットとグローバルルールセットを作成するためのAPIの使用" on page 1142

アプリケーションコントロールを有効にする

アプリケーションコントロールは、コンピュータの設定またはポリシーで有効にできます。

1. コンピュータエディタまたはポリシーエディタを開き、[アプリケーションコントロール]→[一般]に移動します。
2. [アプリケーションコントロールの状態]を[オン]または[継承 (オン)]に設定します。
3. [施行]で、対象の保護状態を選択します。
   - 承認されていないソフトウェアを明示的に許可するまでブロック
   - 承認されていないソフトウェアを明示的にブロックするまで許可 (最初にアプリケーションコントロールを設定するときは、このオプションを選択することをお勧めします)
4. [保存]をクリックします。



次回Deep Security Managerとエージェントが接続すると、エージェントはコンピュータ上にインストールされているすべてのソフトウェアを検索してインベントリを生成し、検出されたすべてのソフトウェアを許可するルールを作成します。環境に応じて、この初期インベントリには15分以上かかることがあります。

警告: インベントリを生成する場合、アプリケーションコントロールには、CIFS(Common Internet File System) やNFS(Network File System) などのリモートファイルシステム上のソフトウェアは含まれません。リモートファイルシステム上のソフトウェアは、インベントリに手動で追加する必要があります。

アプリケーションコントロールが予期したとおりに動作していることを確認するには、" アプリケーションコントロール が有効であることを確認します" on page 1106の手順に従います。

新規および変更済みソフトウェアを監視する

保護対象コンピュータでインベントリの作成が完了した後は、追加または変更されたソフトウェアの実行可能ファイルは「ソフトウェア変更」として分類され、Deep Security Managerの [処理] 画面に表示されます。承認されていないソフトウェアが実行されたり、実行の試みがブロックされたりすると、そのイベントは [イベントとレポート]→[イベント]→[アプリケーションコントロールイベント]→[セキュリティイベント] に表示されます。詳細については、"アプリケーションコントロールイベント" on page 1400を参照してください。

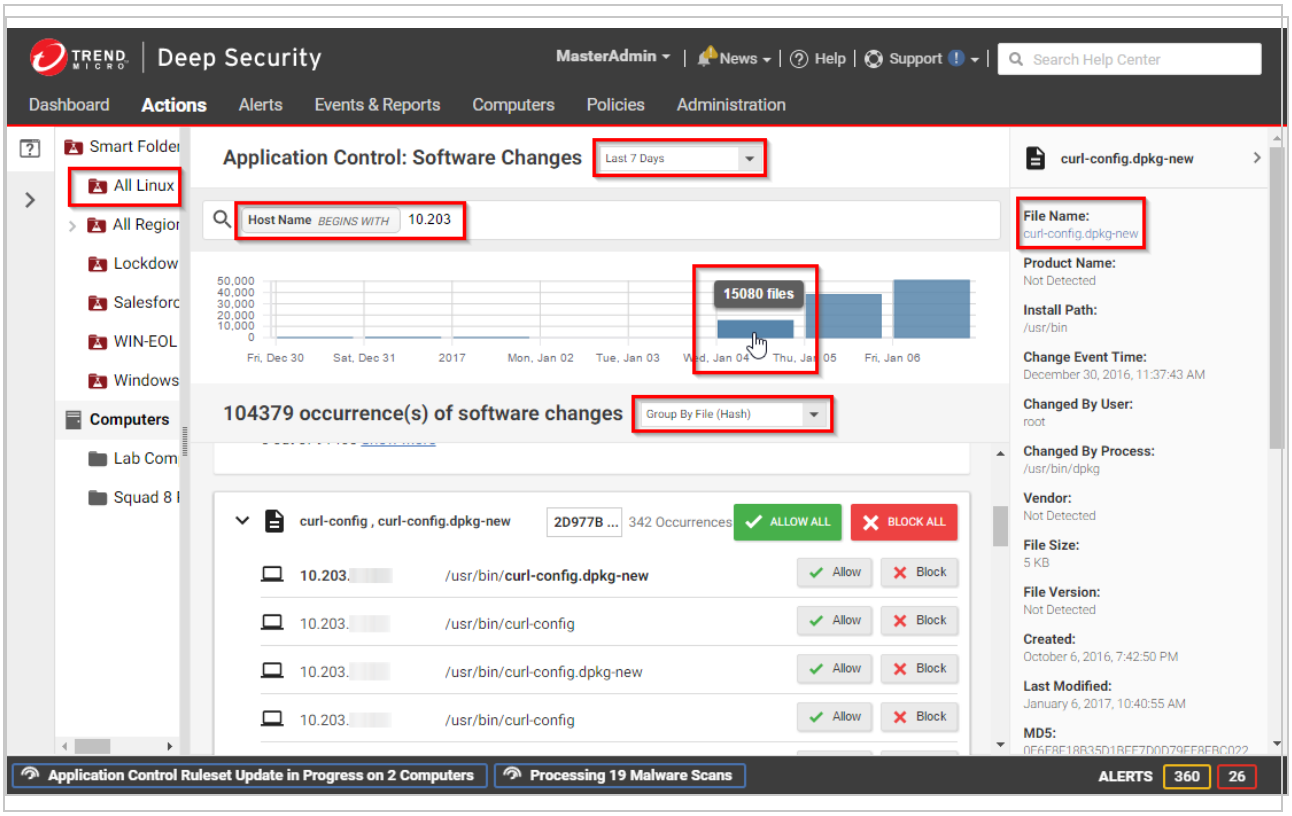
最初にアプリケーションコントロールを有効にした後は、[処理] 画面に多くのソフトウェア変更が表示されることがあります。これは、通常の操作の過程で、許可されたソフトウェアが新しい実行可能ファイルを作成したり、ファイルの名前を変更したり、ファイルを移動した場合に起こります。ルールを追加してアプリケーションコントロールを調整するにつれて、表示されるソフトウェア変更は少なくなります。

すべてのコンピュータのすべてのソフトウェアの変更をすばやく確認し、許可またはブロックルールを作成するには、[処理] タブを使用します。

ヒント: Deep Security APIを使用して、許可またはブロックルールの作成を自動化できます。詳細については、Deep Security Automation Centerの未認識のソフトウェアを許可またはブロックするガイドを参照してください。

1. Deep Security Managerで、[処理] に進みます。
2. 承認されていないソフトウェアの特定の検出情報だけを表示するには、いくつかの方法で情報をフィルタできます。

   ヒント: 各コンピュータの各ソフトウェア変更を個別に評価する代わりに、この後で説明するフィルタを使用して問題のないことが分かっているソフトウェア変更を見つけて、一括で許可します。



表示されるソフトウェア変更の数を減らすには、次の操作を実行します。

- [アプリケーションコントロール: ソフトウェア変更] の横にあるドロップダウンリストから、[過去7日間] などの時間範囲を選択します。画面の上部付近にあるグラフのバーをクリックして、その期間の変更を表示することもできます。

- 左側の画面で、[コンピュータ] をクリックして個別のコンピュータまたはグループを選択するか、[スマートフォルダ] をクリックして特定のスマートフォルダに含まれるコンピュータのみを表示します ("スマートフォルダによるコンピュータの動的なグループ化" on page 1594を参照)。

  注意: [コンピュータ] タブと異なり、[ソフトウェア変更] 画面には通常すべてのコンピュータが表示されることはありません。許可またはブロックルールがないソフトウェア変更がアプリケーションコントロールによって検出されたコンピュータのみが表示されます。

- 検索フィルタフィールドに検索語句と演算子を入力します。プロセスによる変更、ユーザによる変更、ホスト名、インストールパス、MD5、SHA1、SHA256などの属性を検索します。たとえば、信頼する特定のユーザが加えたすべての変更を検索し、[すべて許可] をクリックしてそのユーザのすべての変更を許可できます。または、(メンテナンスモードが有効になっていないときに) 組織全体に特定のソフトウェアアップデートがインストールされた場合は、ファイルのハッシュ値に従って画面をフィルタし、[すべて許可] をクリックして発生したすべての変更を許可します。

  ヒント: ソフトウェア変更に関する詳細が右側の画面に表示されます。詳細のファイル名またはコンピュータ名をクリックして、検索フィルタに追加できます。

- [ファイル (ハッシュ) 別にグループ化] または [コンピュータ別にグループ化] を選択します。

3. [許可] または [ブロック] をクリックして、そのコンピュータに、そのソフトウェア用の許可またはブロックルールを追加します。許可するかブロックするかを判断するために詳細な情報が必要な場合は、ソフトウェア名をクリックし、右側の詳細パネルを使用します。

   次にAgentがDeep Security Managerに接続すると、Agentが新しいルールを受け取ります。

変更の処理のヒント

- ほとんどの環境では、[承認されていないソフトウェアを明示的にブロックするまで許可] オプションを選択して、アプリケーションコントロールを最初に有効にしたときの初期設定でソフトウェア変更を許可し、[処理] 画面に表示された変更の許可およびブロックルールを追加することをお勧めします。最終的に、ソフトウェア変更の頻度が低下します。この時点で、初期設定でソフトウェア変更をブロックし、問題のないことが分かっているソフトウェアの許可ルールを作成することを検討できます。一部の組織では、引き続き初期設定で変更を許可し、ブロックする必要があるソフトウェアを [処理] 画面で監視することが好まれます。
- 承認されていないソフトウェアを最初に処理する代わりに、セキュリティイベントを評価することから始めることもできます。セキュリティイベントは、実行された (または実行が試みられた) 承認されていないソフトウェアを示します。セキュリティイベントの詳細については、"アプリケーションコントロールイベントの監視" on page 1107を参照してください。

- 承認されていないファイルの実行が許可された場合に、そのまま許可を継続するときは、許可ルールを作成します。ファイルの実行が許可されるだけでなく、ファイルに対するイベントが記録されなくなるため、ノイズが低減され、重要なイベントを見つけやすくなります
- 既知のファイルの実行がブロックされた場合は、コンピュータからそのファイルを駆除することを検討します(特に頻繁に発生する場合)。
- ソフトウェア変更は、発生したコンピュータごとに表示されることに注意してください。各コンピュータのソフトウェアを許可またはブロックする必要があります。
- ルールはコンピュータに割り当てられ、ポリシーには割り当てられません。たとえば、3台のコンピュータでhelloworld.pyが検出された場合、[すべて許可] または [すべてブロック] をクリックしても反映されるのはこの3台のコンピュータのみです。他のコンピュータは独自のルールセットを使用しているため、他のコンピュータでその後同じファイルが検出されても選択した処理は適用されません。
- 管理できるソフトウェアアップデートに関連する変更が表示された場合は、そのアップデートを実行するときにメンテナンスモード機能を使用します。"変更の計画時にメンテナンスモードをオンにする" belowを参照してください。

変更の計画時にメンテナンスモードをオンにする

警告: メンテナンスモードが有効な場合、アプリケーションコントロールは、CIFS(Common Internet File System) やNFS(Network File System) などのリモートファイルシステムを検索しません。リモートファイルシステムでのソフトウェアの変更は自動認証できないため、必要に応じて手動でソフトウェアインベントリに追加することをお勧めします。

アプリケーションコントロールはパッチのインストール、ソフトウェアのアップグレード、またはWebアプリケーションの配信も検出します。承認されていないソフトウェアの処理方法の設定によっては、[処理] タブで許可ルールを作成するまでこれらのソフトウェアがブロックされることがあります。

インストールやメンテナンスの実行時に不要なダウンタイムやアラートを回避するには、アプリケーションコントロールをメンテナンス期間用のモードに切り替えます。メンテナンスモードが有効な場合、アプリケーションコントロールは引き続きソフトウェアをブロックするルールを適用しますが、新しいソフトウェアやアップデートされたソフトウェアを実行して自動的にコンピュータのインベントリに追加します。

ヒント: Deep Security APIを使用してメンテナンスモードを自動化できます。詳細については、Deep Security Automation Centerのアップグレード中のメンテナンスモードの設定ガイドを参照してください。

1. Deep Security Managerで、[コンピュータ] に進みます。
2. 1つ以上のコンピュータを選択し、[処理]→[メンテナンスモードをオンにする] をクリックします。

3. メンテナンス期間を選択します。

   予定されているメンテナンス期間が終了した時点で、メンテナンスモードは自動的に無効になります。または、アップデートの完了時に手動でメンテナンスモードを無効にする場合は、[無期限]を選択します。

   [ダッシュボード]の[アプリケーションコントロール - メンテナンスモードのステータス]ウィジェットに、コマンドが成功したかどうかが示されます。

4. ソフトウェアをインストールまたはアップグレードします。
5. メンテナンスモードを手動で無効にするよう選択した場合、ソフトウェアの変更の検出を再び開始するにはメンテナンスモードを忘れずに無効にしてください。

アプリケーションコントロールのヒントと注意事項

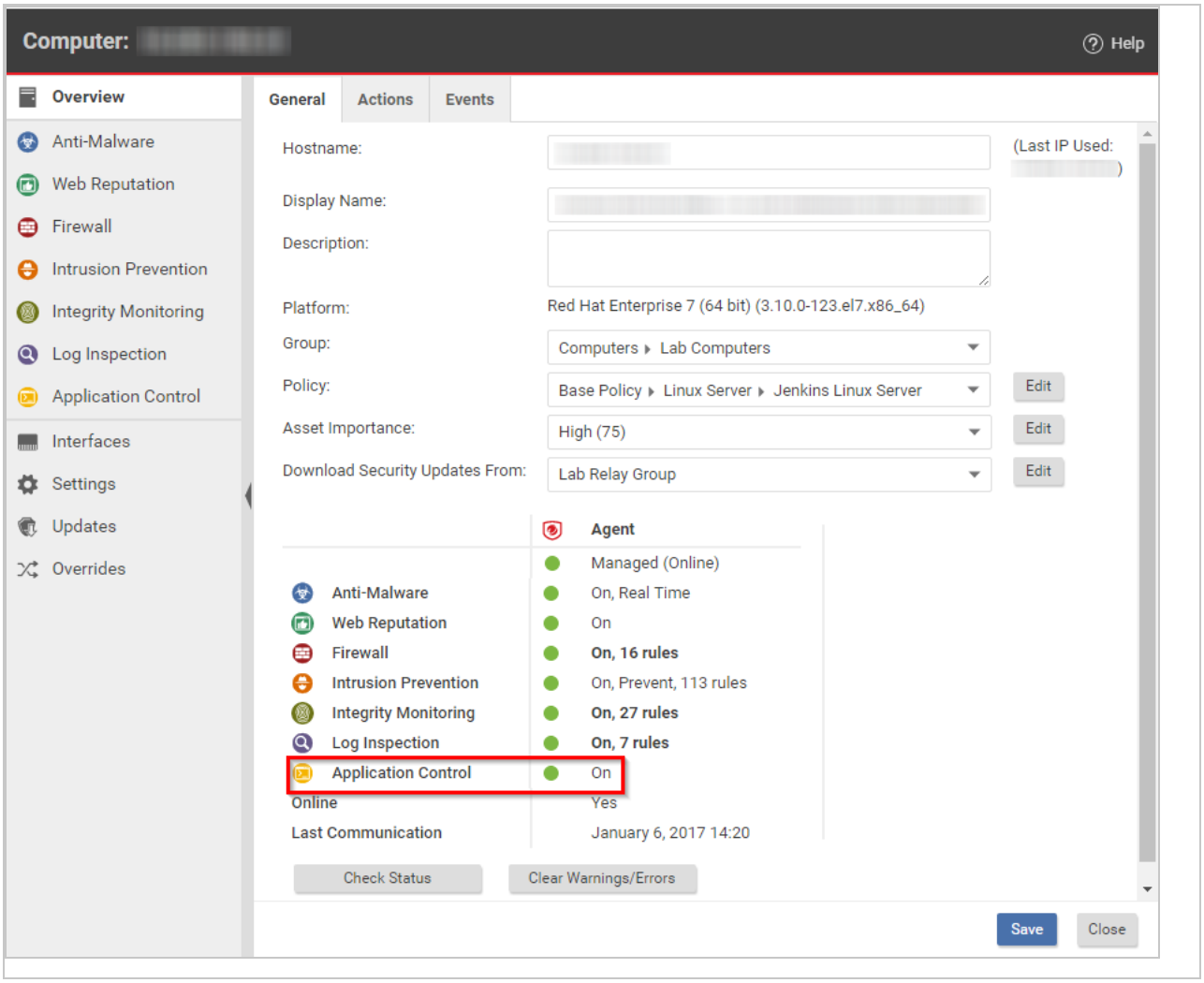
- アプリケーションコントロールのパフォーマンスを向上させるには、Windows DefenderではなくDeep Securityの不正プログラム対策を使用してください。詳細については、"Deep Security AgentとMicrosoft Defender ウイルス対策の共存" on page 854を参照してください。
- バッチファイルまたはPowerShellスクリプトに対するブロックルールを作成する場合は、関連するインタープリタ(PowerShellスクリプトの場合はpowershell.exe、バッチファイルの場合はcmd.exe)の使用時に、このファイルをコピー、移動、または名前変更することはできません。
- 許可またはブロックルールを追加した場合、通常は次にAgentがDeep Security Managerに接続したときに、Agentにルールが送信されます。ルールセットのアップロードに失敗したことを示すエラーが表示された場合は、エージェントとrelayの間のネットワークデバイスがハートビートポート番号または中継ポート番号。
- ブロックルールが機能していることを確認するために、ブロックしたソフトウェアを実行してみます(Deep Security Agentによる変更の検出方法の詳細については、"アプリケーションコントロールで検出されるソフトウェア変更" on page 1098を参照してください)。
- ブロックしたソフトウェアがインストールされたままの場合、アプリケーションコントロールは引き続きソフトウェアの実行をブロックするとアラートを表示し、ログに記録します。コンピュータの権限に関するエラーログを少なくし、攻撃対象領域を縮小するには、アプリケーションコントロールがブロックしているソフトウェアをアンインストールします。その後、関連するアラートを消去するには、[アラート]または[ダッシュボード]へ進み、そのアラートをクリックし、[アラートの消去]をクリックします。ただし、すべてのアラートを消去できるわけではありません。詳細については、"事前定義アラート" on page 1309を参照してください。
- コンピュータでのソフトウェアの変更が多すぎる場合、アプリケーションコントロールは引き続き既存のルールを適用しますが、パフォーマンス上の理由からそれ以上ソフトウェアの変更は検出されず、表示もされなくなります。この問題を解決するには、"ソフトウェアの変更後にアプリケーションコントロールをリセットする" on page 1141を参照してください。

アプリケーションコントロールが有効であることを確認します

アプリケーションコントロールの概要については、"アプリケーションコントロール" on page 1093を参照してください。初期設定の手順については、"アプリケーションコントロールの設定" on page 1099を参照してください。

アプリケーションコントロールが有効で、初期ソフトウェアインベントリ検索が終了した場合：

- [ステータス]が「オン」または「オン、承認されていないソフトウェアをブロック」になります。
- [コンピュータ]の[ステータス]が「アプリケーションコントロールルールセットの構築中」から「管理対象 (オンライン)」に変わります。
- [イベントとレポート]→[イベント]→[システムイベント]に、「アプリケーションコントロールルールセットの作成開始」および「アプリケーションコントロールルールセットの作成完了」が記録されます(ログが表示されない場合は、"ログに記録するアプリケーションコントロールイベントを選択する" on page 1108 .)をログに記録するアプリケーションコントロールイベントの選択



アプリケーションコントロール が機能していることを確認するには

1. コンピュータに実行可能ファイルをコピーするか、プレーンテキストファイルに実行権限を追加して、そのファイルを実行してみます。

   承認されていないソフトウェアに対する設定に応じて、ファイルがブロックまたは許可されます。アプリケーションコントロール が初期許可ルールを作成したり、共有ルールセットをダウンロードしたりしたら、変更が検出された場合は[Actions]タブに表示されます。このルールを使用して許可ルールとブロックルールを作成できます("新規および変更済みソフトウェアを監視する" on page 1101).アラート設定に応じて、認識されないソフトウェアが検出された場合、または アプリケーションコントロール によってソフトウェアの起動がブロックされた場合もアラートが表示されます("アプリケーションコントロールイベントの監視" below).を参照) 。ソフトウェアの変更が存在しなくなるまで、または最も古いデータがデータベースから削除されるまで、イベントは保持されます。

2. テスト用ソフトウェアの許可またはブロックルールを追加して、もう一度実行してみます。今回、アプリケーションコントロール は、許可またはブロックルールを適用する必要があります。

   ヒント: 承認されていないソフトウェアを明示的に許可するまでブロックが明示的に許可されるまでソフトウェアが誤ってブロックされ、ソフトウェアが認識されない場合、アプリケーションコントロール イベントログの Reason 列は、原因のトラブルシューティングに役立ちます。

アプリケーションコントロールイベントの監視

アプリケーションコントロールの概要については、"アプリケーションコントロール" on page 1093を参照してください。初期設定の手順については、"アプリケーションコントロールの設定" on page 1099を参照してください。

初期設定では、アプリケーションコントロールを有効にすると、ソフトウェアの変更が発生したときやアプリケーションコントロールによってソフトウェアの実行がブロックされたときに、この機能によってイベントがログに記録されます。アプリケーションコントロールイベントは、[処理] 画面と[イベントとレポート] 画面に表示されます。設定されている場合は、[アラート] 画面にアラートが表示されます。

どのアプリケーションコントロールイベントログを記録し、どのアプリケーションコントロールイベントログを外部SIEMシステムまたはSyslogサーバに転送するかを設定できます。

コンピュータ上でのソフトウェア変更を監視するには、次の手順に従います。

1. "ログに記録するアプリケーションコントロールイベントを選択する" on the next page
2. "アプリケーションコントロールイベントログを表示する" on the next page
3. "集約されたセキュリティイベントを解釈する" on the next page
4. "アプリケーションコントロールアラートを監視する" on page 1109

ログに記録するアプリケーションコントロールイベントを選択する

1. [管理]→[システム設定]→[システムイベント] に進みます。
2. イベントID 7000「アプリケーションコントロールセキュリティイベントのエクスポート」などのアプリケーションコントロールイベントにスクロールします。
3. そのタイプのイベントのイベントログを記録するには、[記録する] を選択します。

   該当するイベントが発生すると、[イベントとレポート]→[イベント]→[システムイベント] にイベントが表示されます。ログは最大保持期間に達するまで記録されます。詳細については、"Deep Securityイベントログについて" on page 1150を参照してください。

   > 注意: ここで設定するイベントは、[コンピュータ]→[詳細]→[アプリケーションコントロール]→[イベント] に表示されるイベントではありません。ここに表示されるイベントは常に記録されます。

4. イベントログをSIEMまたはSyslogサーバに転送するには、[転送する] を選択します。
5. 外部SIEMを使用する場合は、必要に応じて、対象となるアプリケーションコントロールイベントログのリストをロードし、実行する処理を指定します。アプリケーションコントロールイベントのリストについては、"システムイベント" on page 1342と"アプリケーションコントロールイベント" on page 1400を確認してください。

アプリケーションコントロールイベントログを表示する

アプリケーションコントロールは、システムイベントとセキュリティイベントを生成します。

- システムイベント: 設定変更やソフトウェアアップデートの履歴を提供する監査イベント。システムイベントを確認するには、[イベントとレポート]→[イベント]→[システムイベント] をクリックします。システムイベントの一覧については、"システムイベント" on page 1342を参照してください。
- セキュリティイベント: アプリケーションコントロールで承認されていないソフトウェアがブロックまたは許可されるときや、ブロックルールによってソフトウェアがブロックされるときに、Agentで発生するイベント。セキュリティイベントを確認するには、[イベントとレポート]→[イベント]→[アプリケーションコントロールイベント]→[セキュリティイベント] の順にクリックします。一覧については、"アプリケーションコントロールイベント" on page 1400を参照してください。

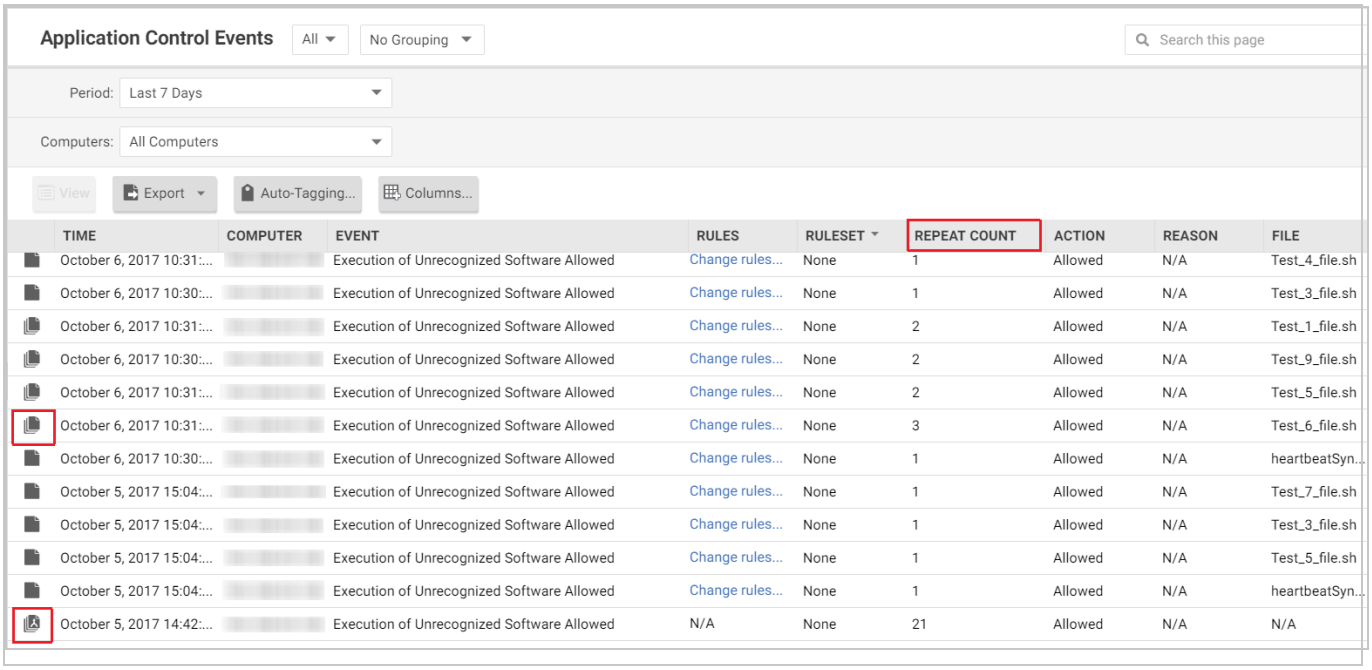
集約されたセキュリティイベントを解釈する

Agentのハートビートに同一のセキュリティイベントの複数のインスタンスが含まれている場合、Deep Securityではセキュリティイベントログのイベントを集約します。イベントの集約によって、ログ内の項目数が減少するため、重要なイベントを見つけやすくなります。

- 一般的なケースとして、同一ファイルにイベントが発生した場合、ログにはファイル名と集約されたイベントが表示されます。たとえば、ハートビートにTest_6_file.shファイルに発生した「承認されていないソフトウェアの実行を許可」イベントの3つのインスタンスが含まれ、このイベントの他のインスタンスが含まれていない場合、Deep SecurityではTest_6_file.shファイルに対するこれらの3つのイベントが集約されます。
- イベントが多くのファイルに対して発生した場合、ログではルールのリンク、パス、ファイル名、およびユーザ名が省略されます。たとえば、ハートビートに複数の異なるファイルに発生した「承認されていないソフトウェアの実行を許可」イベントの21個のインスタンスが含まれている場合、Deep Securityではこの21個のイベントが単一のイベントに集約されますが、ルールのリンク、パス、ファイル名、およびユーザ名は含まれません。

集約されたイベントが複数のファイルに当てはまる場合、これらのイベントの他の発生情報は他のハートビートで報告されている可能性があります。ファイル名がわかっている他のイベントに対処すると、集約されたイベントは発生しなくなる可能性があります。

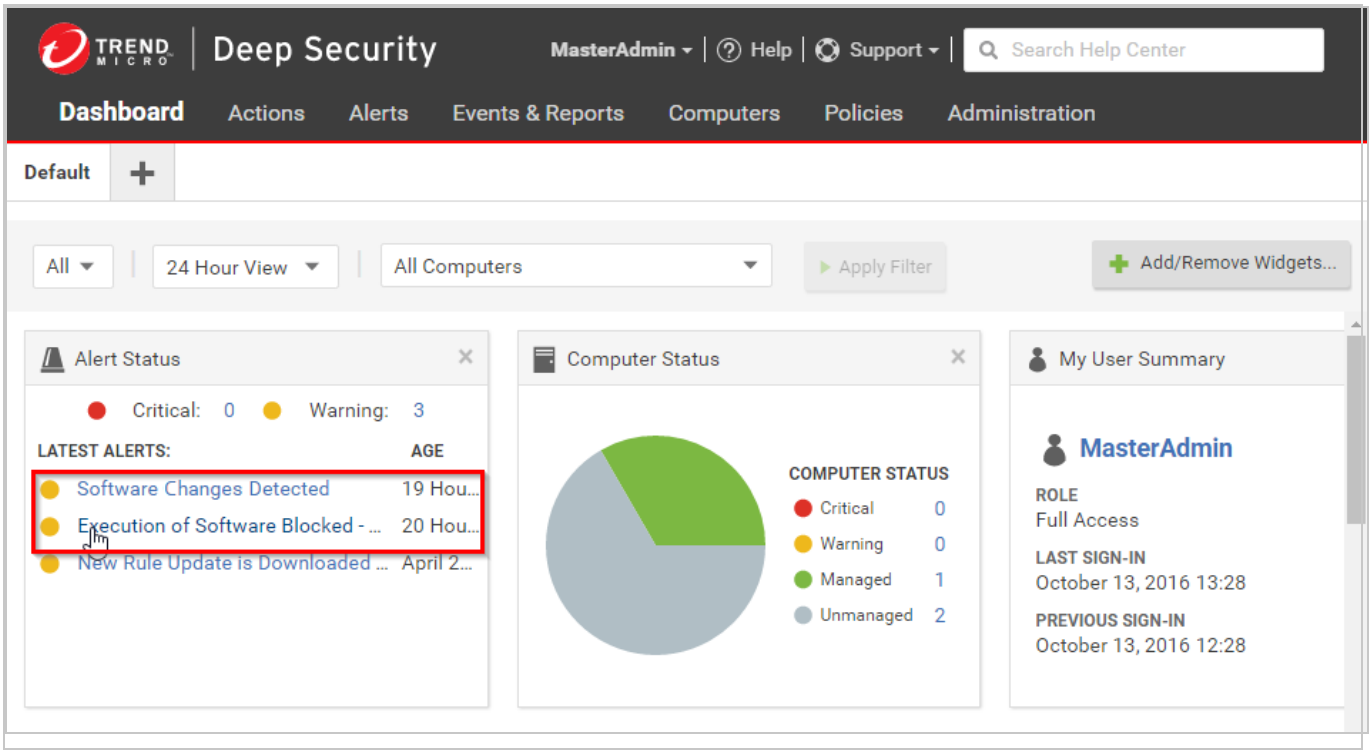
ログでは、集約されたイベントには特別なアイコンが使用され、[繰り返しカウント] 列に集約されたイベント数が表示されます。



アプリケーションコントロールアラートを監視する

どのアプリケーションコントロールイベントまたは重要度でアラートを生成するかを設定するには、[アラート] タブに進み、[アラートの設定] ボタンをクリックし、次にイベントを選択して [プロパティ] をダブルクリックします。詳細については、"アラートの設定" on page 1293を参照してください。

アプリケーションコントロールイベントに対してアラートが有効になっていると、アプリケーションコントロールエンジンによって検出されたソフトウェアの変更と実行がブロックされたソフトウェアがすべて[アラート]タブに表示されます。[アラートステータス]ウィジェットを有効にした場合には、ダッシュボードにもアプリケーションコントロールアラートが表示されます。



どのコンピュータでメンテナンスモードが有効になっているかを監視するには、[ウィジェットの追加/削除]をクリックし、[アプリケーションコントロールメンテナンスモード]ウィジェットを有効にします。このウィジェットには、コンピュータのリストと各コンピュータで予定されているメンテナンス期間が表示されます。

アプリケーションコントロールルールセットの表示と変更

各コンピュータには独自のアプリケーションコントロールルールセットがあります。次の手順を実行します。

- "アプリケーションコントロールルールセットを表示する" on the next pageし、どのルールが含まれているかを確認します。

  ヒント: 最初にコンピュータのアプリケーションコントロールを有効にすると、コンピュータにインストールされているソフトウェアがコンピュータのインベントリに追加され、実行が許可されます。しかし、あなたはそうするのDeep Securityレガシー—REST APIを使用しない限りのDeep Security Managerからの在庫に関連付けられているルールを参照することはできません("共有ルール

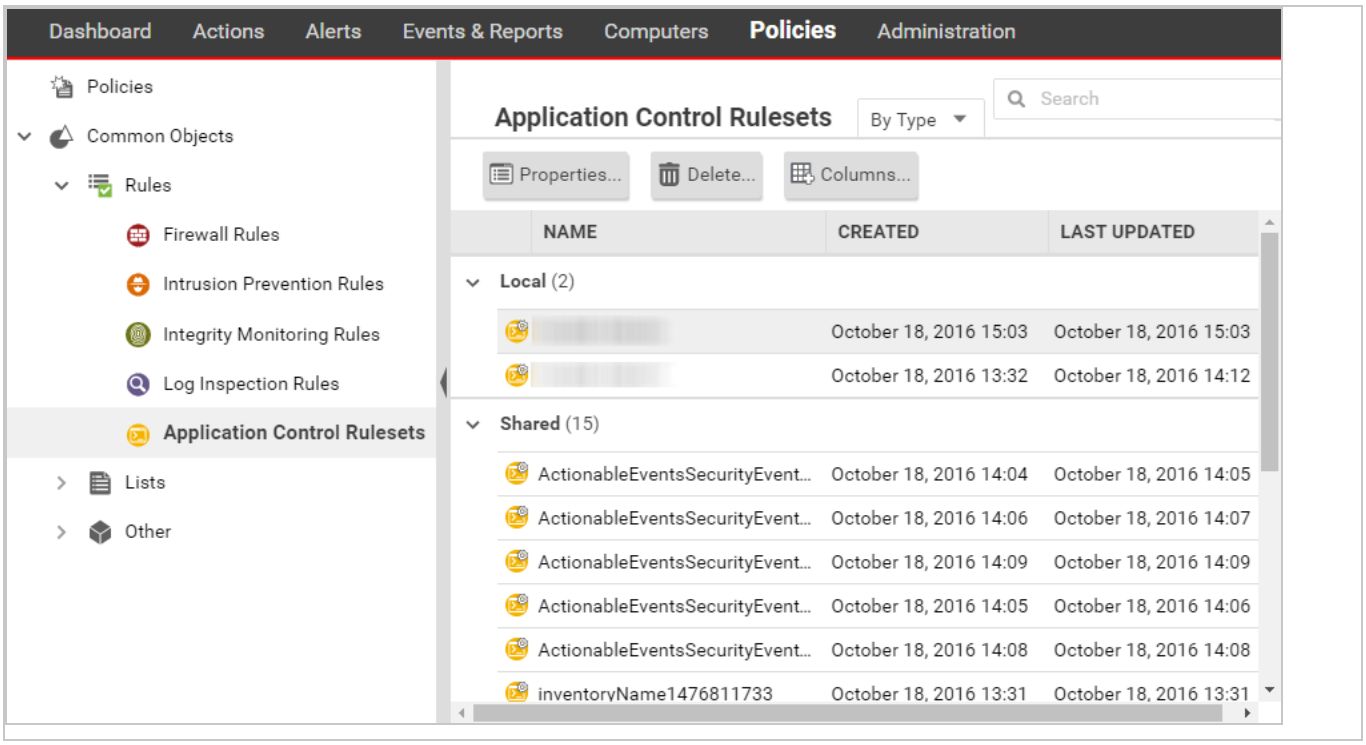
セットとグローバルルールセットを作成するためのAPIの使用" on page 1142を備え進ん)。Deep Security Managerでは、コンピュータの許可ルールまたはブロックルールを作成するまで、コンピュータのルールセットは空です。

- ソフトウェアファイルが許可またはブロックされなくなった場合に、"アプリケーションコントロールルールの処理を変更する" on page 1113ことができます。
- ソフトウェアが削除され、元に戻る可能性が低い場合は、"個々のアプリケーションコントロールルールを削除する" on page 1114ことができます。
- ルールセットに関連付けられたコンピュータが削除されている場合は、"アプリケーションコントロールルールセットを削除する" on page 1114ことができます。

ヒント: 特定のコンピュータで実行する必要のあるソフトウェアがアプリケーションコントロールによってブロックされていることがユーザから報告された場合は、そのコンピュータに対するブロックルールを取り消すことができます。[イベントとレポート]→[アプリケーションコントロールイベント]→[セキュリティイベント]の順に選択して、コンピュータを探して、ブロックイベントを見つけ、[ルールの表示]をクリックします。表示されたポップアップで、ブロックルールを許可ルールに変更できます。

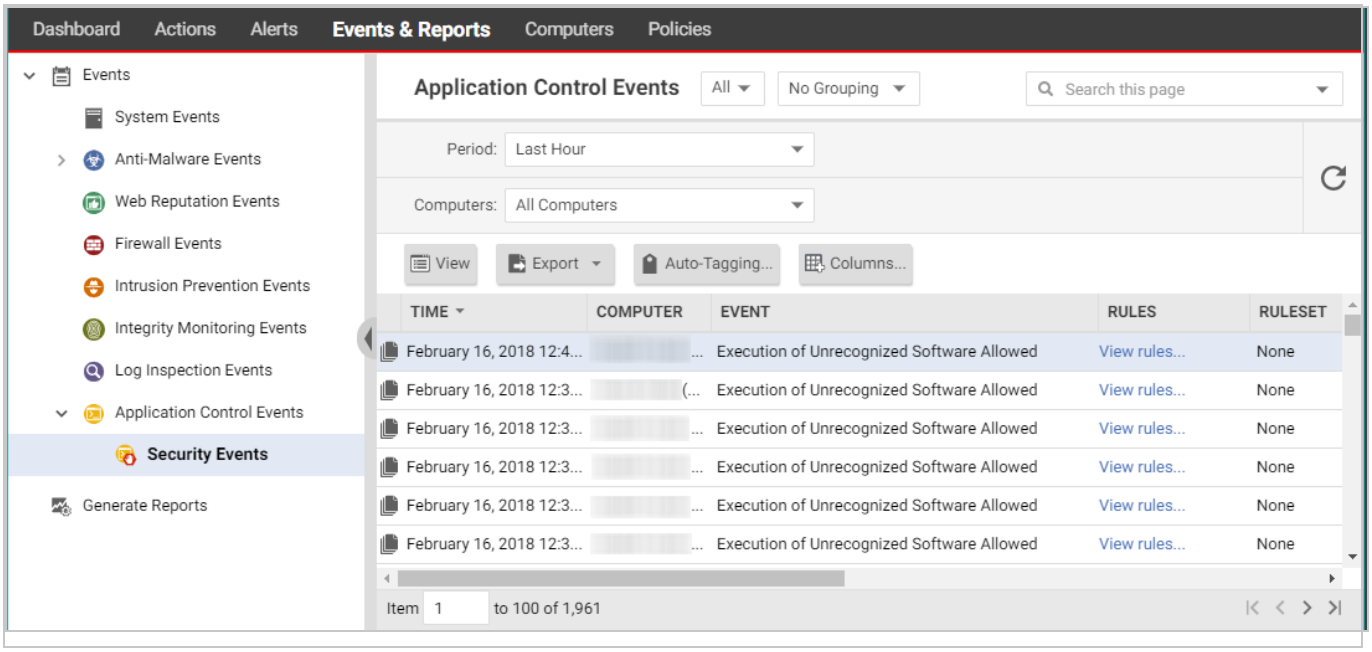
アプリケーションコントロールルールセットを表示する

アプリケーションコントロールルールセットのリストを表示するには、[ポリシー]→[共通オブジェクト]→[ルール]→[アプリケーションコントロールルールセット]に移動します。



ルールセットに含まれるルールを確認するには、ルールセットをダブルクリックして[ルール]タブに移動します。[ルール]タブにはルールが関連付けられているソフトウェアファイルが表示され、許可ルールをブロックルールに変更したり、その逆に変更したりすることもできます("アプリケーションコントロールルールの処理を変更する" on the next pageを参照)。

セキュリティイベント



[イベントとレポート]→[イベント]→[アプリケーションコントロールイベント]→[セキュリティイベント] には、コンピュータ上で実行されているか、アクティブに実行がブロックされているすべての承認されていないソフトウェアが表示されます。このリストは、期間および他の基準によってフィルタできます。詳細については、"アプリケーションコントロールイベント" on page 1400を参照してください。

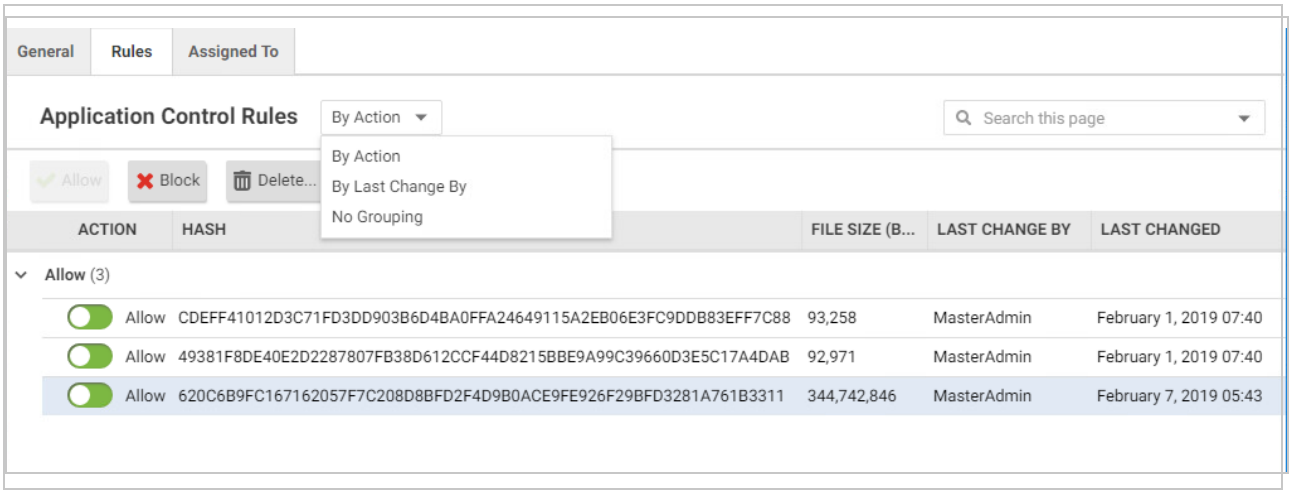
イベント(集約イベント以外) ごとに、[ルールの表示] をクリックすると、ルールの許可とブロックを切り替えることができます。

Deep Security Agent 10.2以上には、同じイベントが繰り返し発生した場合にログの量を減らすためのイベント集約ロジックがあります。("集約されたセキュリティイベントを解釈する" on page 1108を参照してください)。

アプリケーションコントロールルールの処理を変更する

以前にブロックしたソフトウェアを許可 (または以前に許可したソフトウェアをブロック) する場合は、該当するルールの処理を編集します。ソフトウェアがアプリケーションコントロールで認識されないようにルールを取り消す必要がある場合 (処理を変更するだけでなく、ルール自体を削除する場合) は、"個々のアプリケーションコントロールルールを削除する" on the next pageを参照してください。

1. [ポリシー]→[共通オブジェクト]→[ルール]→[アプリケーションコントロールルールセット] の順に選択します。
2. 変更するルールを含むルールセットをダブルクリックして選択します。
3. 表示されたポップアップ画面で、[ルール] タブを選択します。
4. (または), を許可する場合は、アプリケーションコントロールルールの横にあるメニューで、処理別を選択して同様のルールをグループ化します。また、検索を使用してリストをフィルタすることもできます。



ソフトウェアファイルの処理を変更する場合、ファイル名が複数ある場合は、[ファイル名別]を選択して、関連するルールをグループ化します。

5. 許可またはブロックするソフトウェアに対応する行を探します。
6. [処理]列で、許可するかブロックするかの設定を変更し、[OK]をクリックします。

   次回エージェントがDeep Security Managerに接続すると、ルールがアップデートされ、バージョン番号が増加します。

個々のアプリケーションコントロールルールを削除する

作成したルールを取り消す場合は、[ポリシー]→[共通オブジェクト]→[ルール]→[アプリケーションコントロールルールセット]の順に移動し、そのルールを含むルールセットをダブルクリックして、[ルール]タブに移動し、ルールを選択して[削除]をクリックします。

次のことに注意してください。

- ルールが不要になった場合は、それらを削除することでルールセットのサイズを削減することができます。これにより、RAMとCPUの使用量が削減され、パフォーマンスが向上します。
- ルールを削除すると、そのソフトウェアはアプリケーションコントロールで認識されなくなります。ソフトウェアが再度インストールされると、[処理]タブに再び表示されます。
- ソフトウェアアップデートが不安定な場合やダウングレードが必要になる可能性がある場合は、テストが完了するまで前のソフトウェアバージョンへのロールバックを許可するルールを残しておきます。
- 古いルールを確認するには、[ポリシー]→[ルール]→[アプリケーションコントロールルールセット]の順に選択し、[列]をクリックします。[前回の変更日時]を選択して[OK]をクリックし、その列のヘッダをクリックすると、日付順にソートできます。

アプリケーションコントロールルールセットを削除する

ルールセットに関連付けられたコンピュータがもう存在しない場合など、アプリケーションコントロールルールセットがもう使用されていない場合は、削除できます。

ルールセットを削除するには、[ポリシー]→[ルール]→[アプリケーションコントロールルールセット]の順に選択し、ルールセットをクリックして選択してから[削除]をクリックします。

アプリケーションコントロールの信頼エンティティ

信頼エンティティは、"信頼ルールセット" on the next pageに割り当てられた"信頼ルール" on page 1120のプロパティに一致するソフトウェア変更を自動的に承認します。各信頼ルールには、ソフ

トウェア変更の自動承認のパラメータを定義する"信頼ルールのプロパティの種類" on page 1125 が1つ以上含まれています。

信頼エンティティ機能を使用すると、Deep Security Agentでソフトウェア変更を事前に自動認証できるため、Deep Security Managerに送信されるソフトウェア変更イベントの数を減らすことができます。たとえば、OSの定期的なアップデートを実行しているエージェントは、パッチを適用するたびに、いくつかの新しいソフトウェア変更を作成します。適切な信頼ルールを設定してそれらのAgentに適用すると、Agentでソフトウェアの変更を自動承認できるため、Deep Security Managerの[処理]タブから、またはアプリケーションコントロールのセキュリティイベントとして手動で管理する必要がなくなります。

信頼エンティティを使用してソフトウェアの変更を自動承認するには、"信頼ルール" on page 1120を設定し、それらを"信頼ルールセット" belowに割り当て、"信頼ルールセットの割り当てまたは割り当て解除" on page 1117必要があります。

信頼エンティティ機能で自動承認されないソフトウェア変更を許可またはブロックする方法については、「"アプリケーションコントロールルールセットの表示と変更" on page 1110」を参照してください。

このドキュメントでは、*ソース*はソフトウェア変更を作成するプロセスを指し、*ターゲット*はソフトウェア変更自体を指す場合に使用されます。

ヒント: 信頼ルールセットのAPIドキュメントが利用可能です。

現在、一部の信頼ルールプロパティはサポートされるWindowsプラットフォームのエージェントにのみ適用され、Linuxではまだ使用できません。詳細については、"Linuxの信頼ルールプロパティの制限" on page 1141を参照してください。

信頼ルールセット

信頼ルールセットは、1つ以上のユーザ設定の"信頼ルール" on page 1120で構成されます。"信頼ルールセットの割り当てまたは割り当て解除" on page 1117 を割り当てると、そのルールセットに含まれるルールが関連するワークロードに適用され、ルールプロパティの要件を満たすソフトウェアの変更が自動的に承認されます。

信頼ルールセットを作成する

新しい信頼ルールセットを作成するには、次のいずれかを実行します。

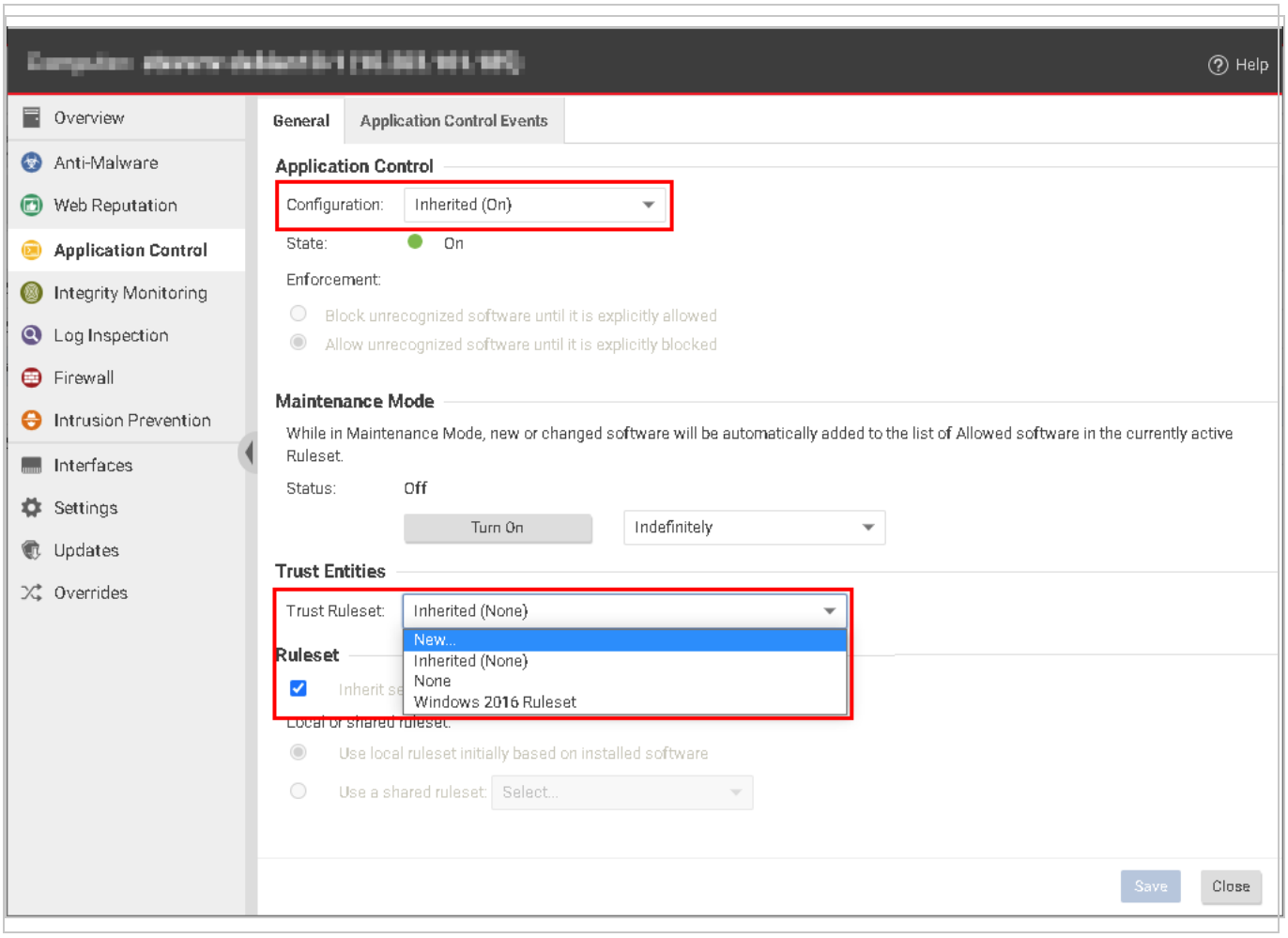
Deep Security Manager Policiesタブで次の操作を実行します。

1. [共通オブジェクト]→[ルール]→[アプリケーションコントロールルール]→[信頼エンティティ]に移動します。
2. [Trust Rulesets]セクションで、[新規]を選択します。
3. [新規ルールセット]ウィンドウで、新しいルールセットの名前と説明(オプション)を入力します。
4. リストから1つ以上の信頼ルールを選択して、信頼ルールセットに割り当てます。

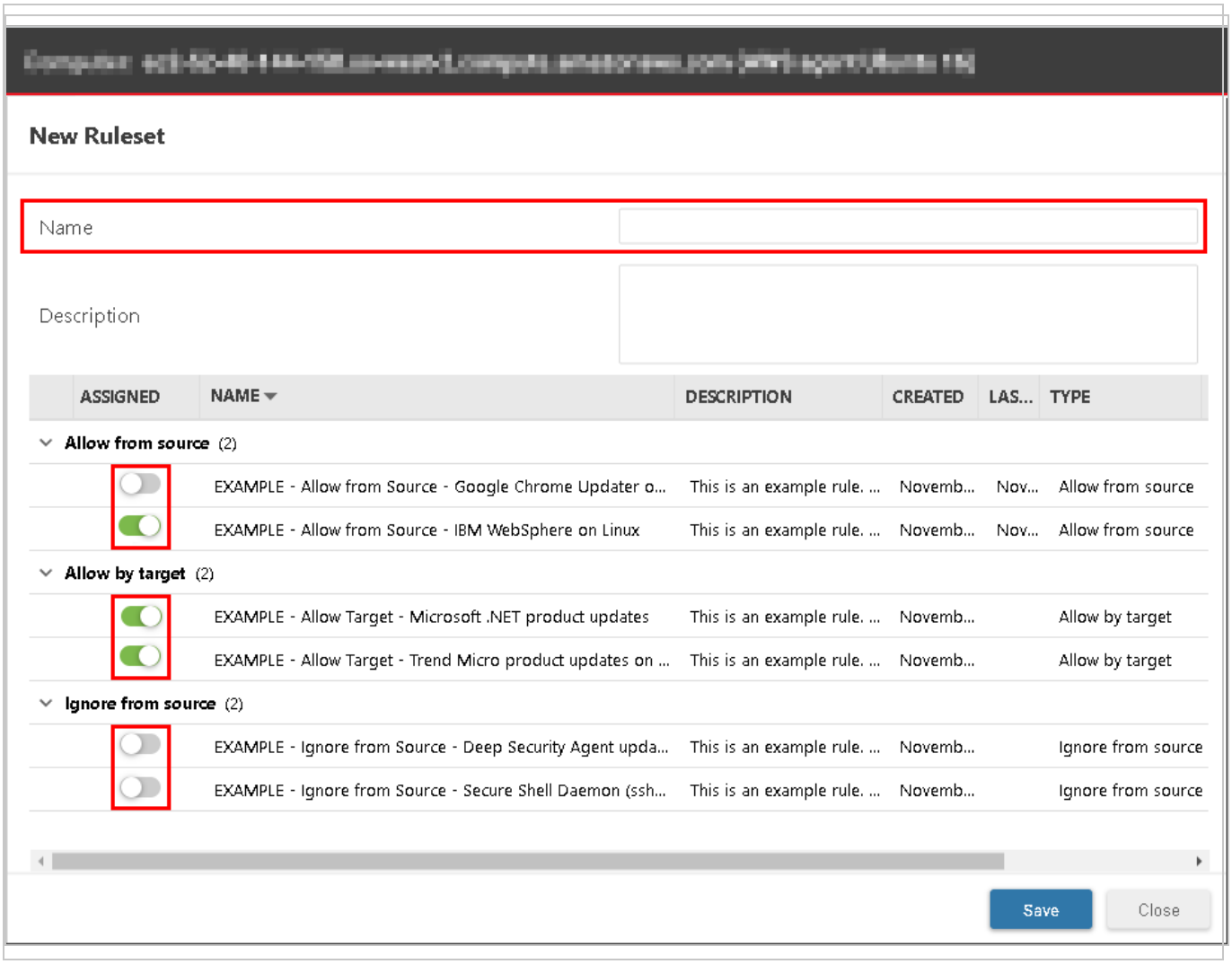


割り当てたルールを含む信頼ルールセットが作成されます。

1. Deep Security Manager Computersまたは[Policies]タブで次の操作を実行します。コンピューターまたはポリシーをダブルクリックします(または右クリックして[詳細]を選択します) 。
2. [アプリケーションコントロール]に移動し、[設定] が [オン] または [継承 (オン)] に設定されていることを確認します。
3. [信頼ルールセット]ドロップダウンリストで、[新規]を選択します。



4. [新規ルールセット]ウィンドウで、新しいルールセットの名前と説明(オプション) を入力します。



5. リストから1つ以上の信頼ルールを選択して信頼ルールセットに割り当て、[保存]を選択して、割り当てたルールを含む信頼ルールセットを作成します。

6. (オプション) 新しい信頼ルールセットをコンピュータまたはポリシーに割り当てるには、[保存]を選択します。

> ヒント: 信頼ルールセットを最初から作成する代わりに、[信頼エンティティの管理] 画面 ([ポリシー]→[共通オブジェクト]→[ルール]→[アプリケーションコントロールルール]→[信頼エンティティ]) の [複製] ボタンを使用して既存のルールセットのコピーを作成し、必要に応じて設定できます。

信頼ルールセットの割り当てまたは割り当て解除

信頼ルールセットを割り当てるには:

1. Deep Security Manager Computers or Policies タブで、コンピュータまたはポリシーをダブルクリックします(または右クリックして[Details]を選択します)。

2. [アプリケーションコントロール]に移動し、[設定]が[オン]または[継承 (オン)]に設定されていることを確認します。

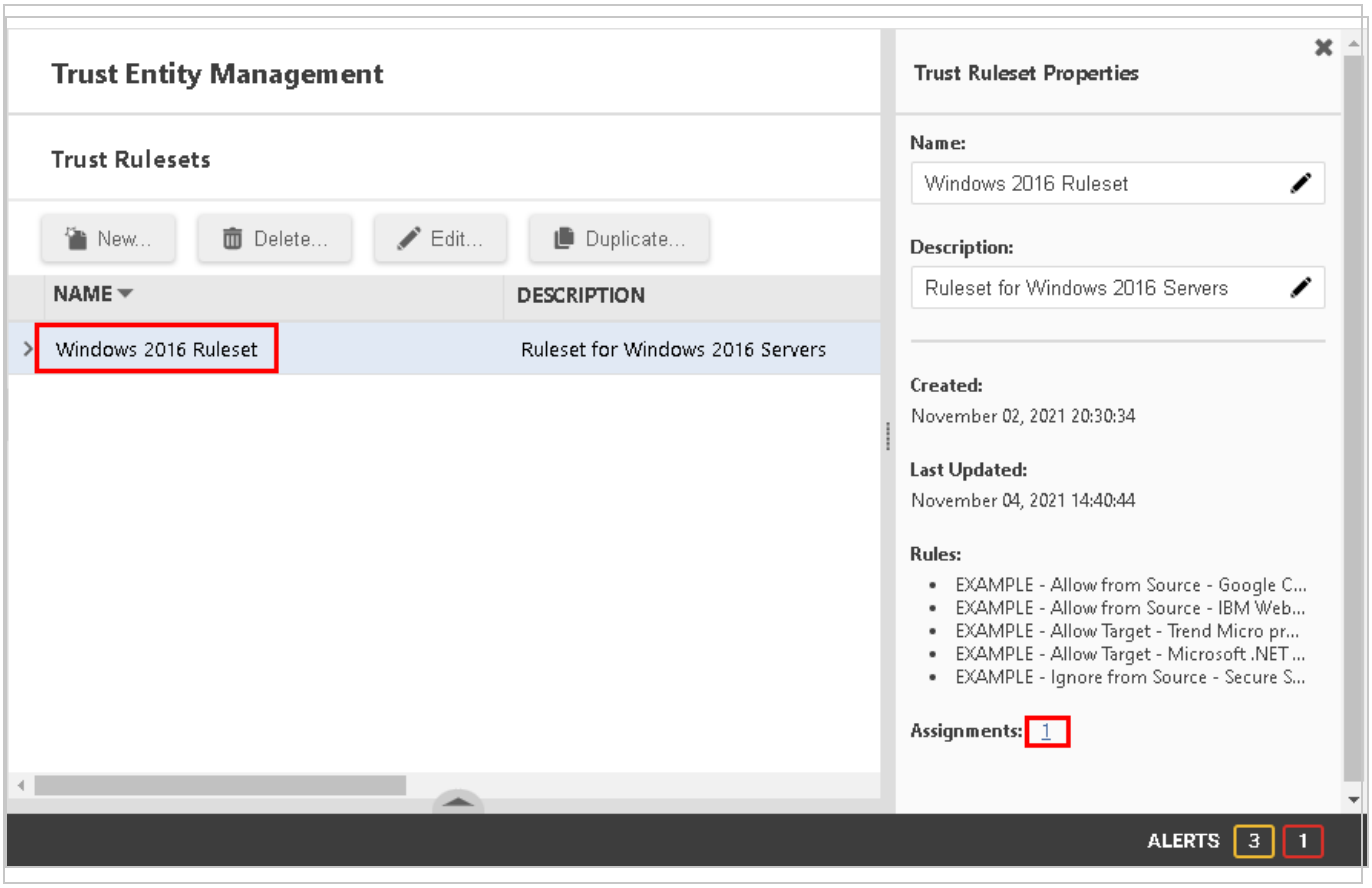
3. ドロップダウンリストから信頼ルールセットを選択します。



これで、選択した信頼ルールセットがコンピュータまたはポリシーに割り当てられました。

信頼ルールセットの割り当てを解除するには：

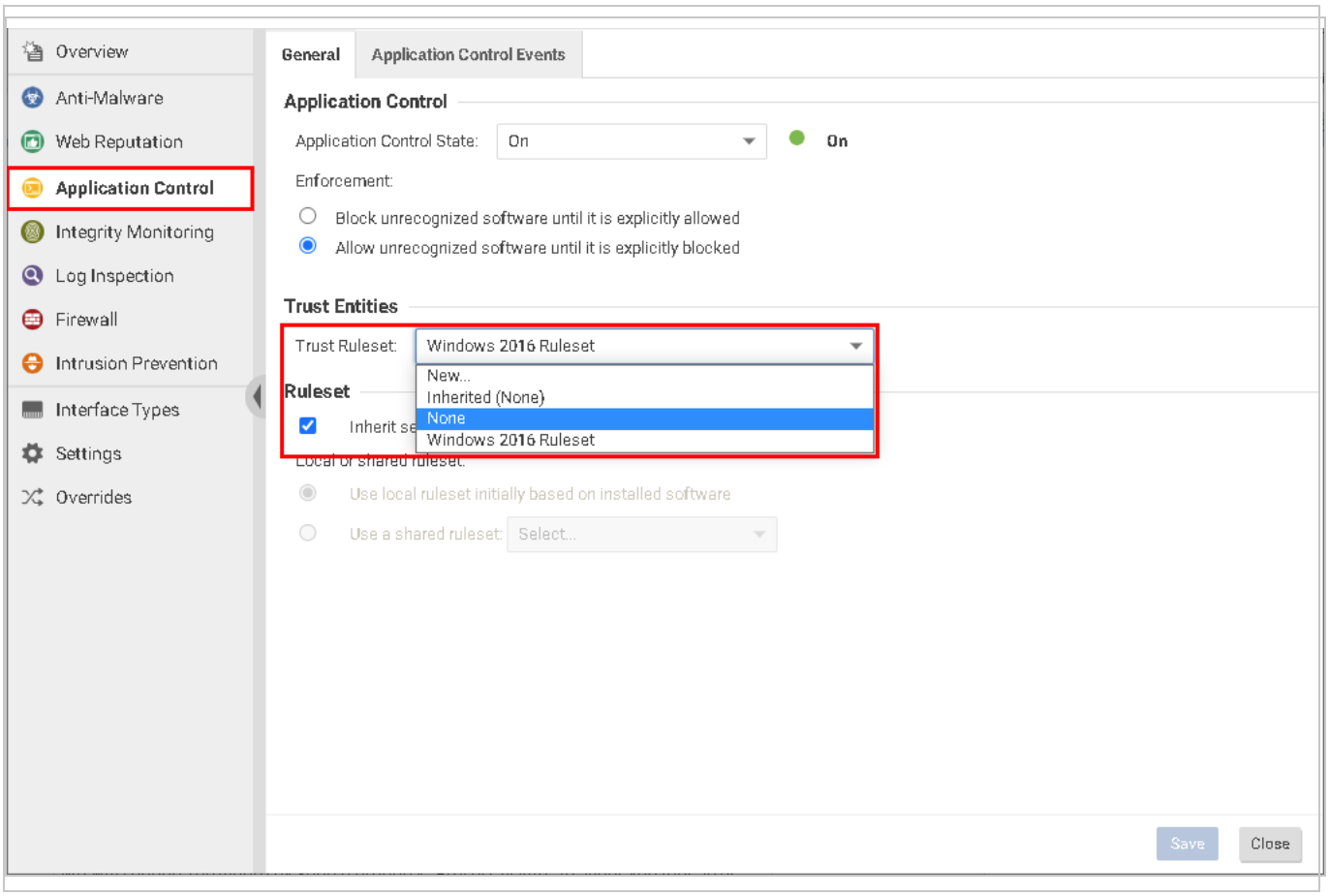
1. [共通オブジェクト]→[ルール]→[アプリケーションコントロールルール]→[信頼エンティティ]の順に選択し、信頼ルールセットを選択します。
2. 右側に表示される[信頼ルールセットのプロパティ]画面で、[割り当て]の横にある数字を選択します。



3. [割り当て先]ウィンドウで、コンピュータまたはポリシーを選択します。



4. コンピュータまたはポリシーウィンドウの[アプリケーションコントロール]タブで、[信頼するルールセット]ドロップダウンリストから[なし]を選択して、ルールセットの割り当てを解除します。



5. [保存]を選択します。

信頼ルールセットがコンピュータまたはポリシーに割り当てられていません。

信頼ルールセットを削除する

1. [共通オブジェクト]→[ルール]→[アプリケーションコントロールルール]→[信頼エンティティ]に移動します。
2. [Trust Rulesets]セクションで、削除するルールセットを選択し、[削除]を選択します。

3. [ルールセットの削除] 確認ウィンドウで、[OK] を選択します。



信頼ルールセットが削除されます。

信頼ルールセットが現在コンピュータまたはポリシーに継承されているか、割り当てられている場合は、信頼ルールセットを削除できないことに注意してください。信頼ルールセットを削除するには、"信頼ルールセットの割り当てまたは割り当て解除" on page 1117必要があります。

信頼ルール

信頼ルールには、アプリケーションコントロールによって自動承認されるソフトウェアの変更を決定する1つ以上のプロパティが含まれます。信頼ルールのプロパティに一致するソフトウェアの変更は自動認証され、Deep Security Managerでイベントが作成されることはありません。

警告: 空の信頼ルールプロパティはすべてワイルドカードとして扱われます。これにより、信頼ルールをカスタマイズする方法が自由になりますが、システムのセキュリティに影響する可能性もあります。システムのセキュリティを最大化し、不要なソフトウェアの変更が許可されないようにするには、信頼ルールを作成するときにできるだけ多くのプロパティを入力してください。信頼ルールがセキュリティに与える影響がよくわからない場合は、システムのセキュリティについて十分な知識がある人に確認するか、信頼ルールセットに追加する前にトレンドマイクロに問い合わせてください。

信頼ルールの種類

- [ソースからの許可]ルールは、信頼されたアップデータまたはインストーラプロセスがシステムに新しいソフトウェアをインストールすることを許可します。信頼できるアップデータによって作成された承認済みの実行可能ファイルは、自動的に承認されます。このルールを使用するには、プロセスやインストーラなどのソースのプロパティをルールで指定する必要があります。さらに、"パス" on page 1126属性を使用して、指定したディレクトリに許可されたソフトウェアのみを作成するようにプロセスを制限する必要があります。このルールを適用すると、[処理] 画面のソフトウェア変更イ

ベントが最小限に抑えられます。[ソースから許可] ルールはソフトウェアの作成時に評価されるため、インストーラを実行する前に設定する必要があります。

- [対象別に許可] ルールは、指定したプロパティに一致する実行可能ファイルの実行を許可します。ルールで指定するプロパティは、実行可能ファイルなど、対象のプロパティと一致する必要があります。このルールは実行時に評価されるため、[アラート] 画面でファイルのセキュリティイベントが検出された後に適用できます。

- 対象ルールでブロックすると、指定したプロパティに一致する実行可能ファイルが実行されなくなります。ルールで指定するプロパティは、実行可能ファイルなど、対象のプロパティと一致する必要があります。このルールは実行時に評価されるため、[アラート] 画面でファイルのセキュリティイベントが検出された後に適用できます。

  注意: [対象別にブロック] ルールは、Deep Security Agent 20.0.0-3288以降でサポートされます。

- [ソースから無視] ルールを使用すると、プロセスの除外が設定されます。これにより、指定されたプロセスは、アプリケーションコントロールによる監視を受けずに、指定されたディレクトリでソフトウェアを実行または作成できます。除外ルールが削除されると、除外はただちに解除されます。[ソースルールで無視] でパスのみを指定した場合は、すべてのプロセスがそれらのディレクトリでソフトウェアを実行または作成できます。この場合、アプリケーションコントロールによる監視は行われません。このオプションは、アプリケーションコントロール検索によって一部のプロセスまたはパスとの互換性の問題 (パフォーマンスの問題や共有違反など) が発生している場合にのみ使用してください。[ソースから無視] ルールは、Workload Security APIを使用して作成されたすべてのグローバルルールよりも優先されます。グローバルルールの詳細については、「"共有ルールセットとグローバルルールセットを作成するためのAPIの使用" on page 1142」を参照してください。

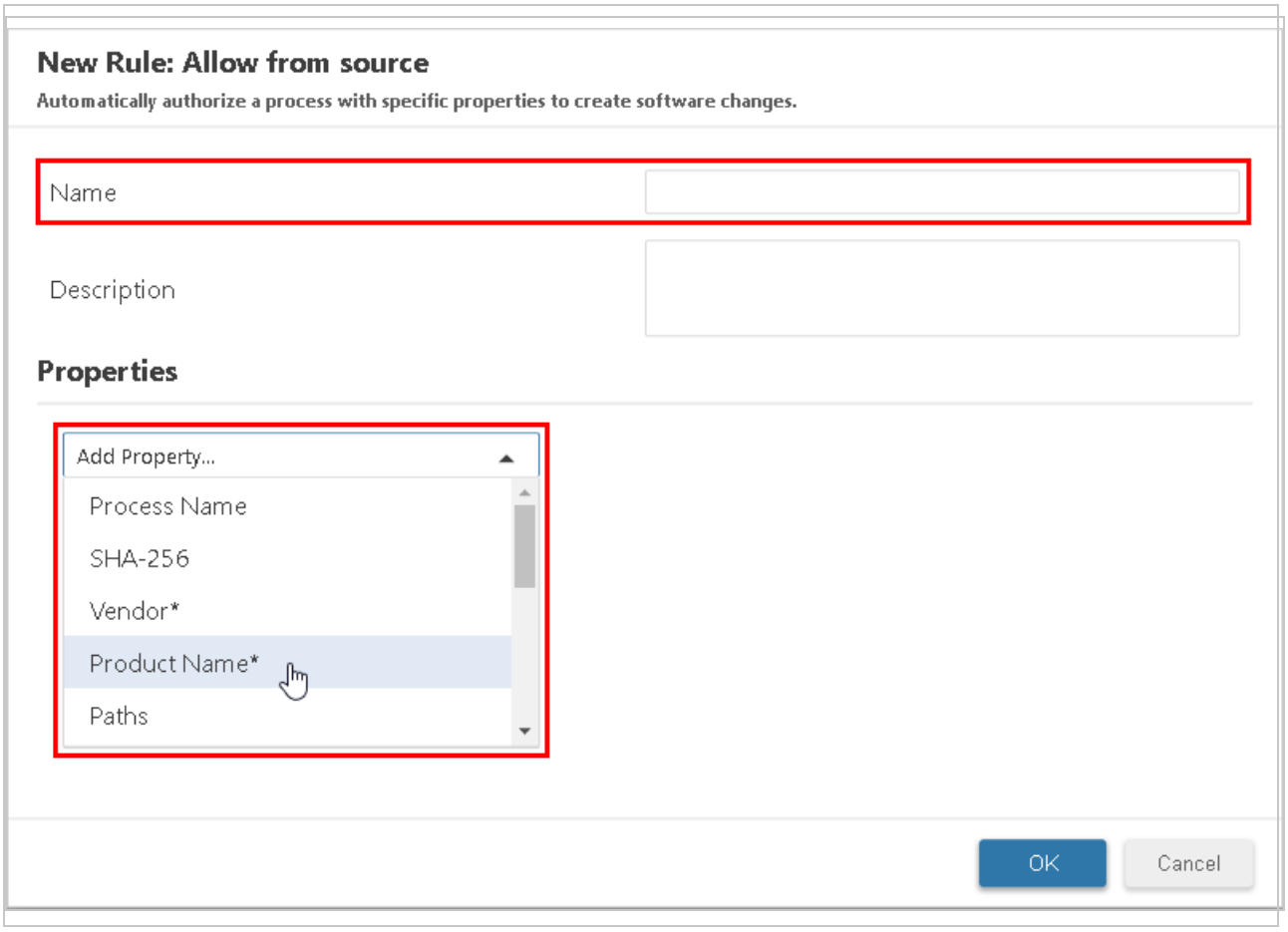
[ソースから許可] ルールによってソフトウェアの変更が自動承認されるたびに、変更が発生したAgentのローカルインベントリにエントリが追加されます。これは、[ソースから無視] ルールでは発生しません。

警告: Ignore by sourceルールで使用する場合、"プロセス名" on page 1126 プロパティは、Deep Security Agent 20.0.0-3165以降でのみサポートされます。

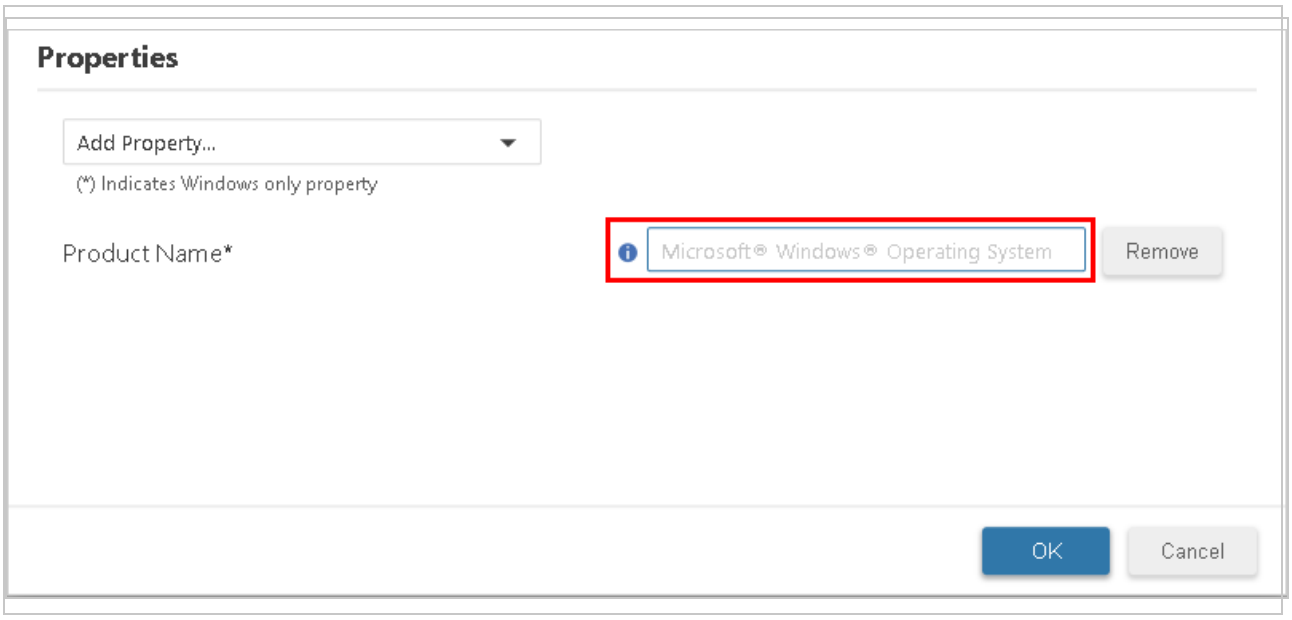
信頼ルールを作成する

1. [共通オブジェクト]→[ルール]→[アプリケーションコントロールルール]→[信頼エンティティ]に移動します。

2. [信頼ルール]セクションで、[新規]を選択し、ドロップダウンリストから"信頼ルールの種類" on page 1120を選択します。
3. [新しいルール]ウィンドウで、新しいルールの名前と説明(オプション)を入力します。
4. [プロパティの追加]ドロップダウンリストからプロパティを選択して、新しいルールに追加します。



5. 表示されたボックスにプロパティの値を入力します。



6. (オプション) この信頼ルールにプロパティを追加するには、手順4と5を繰り返します。
7. [OK] をクリックします。

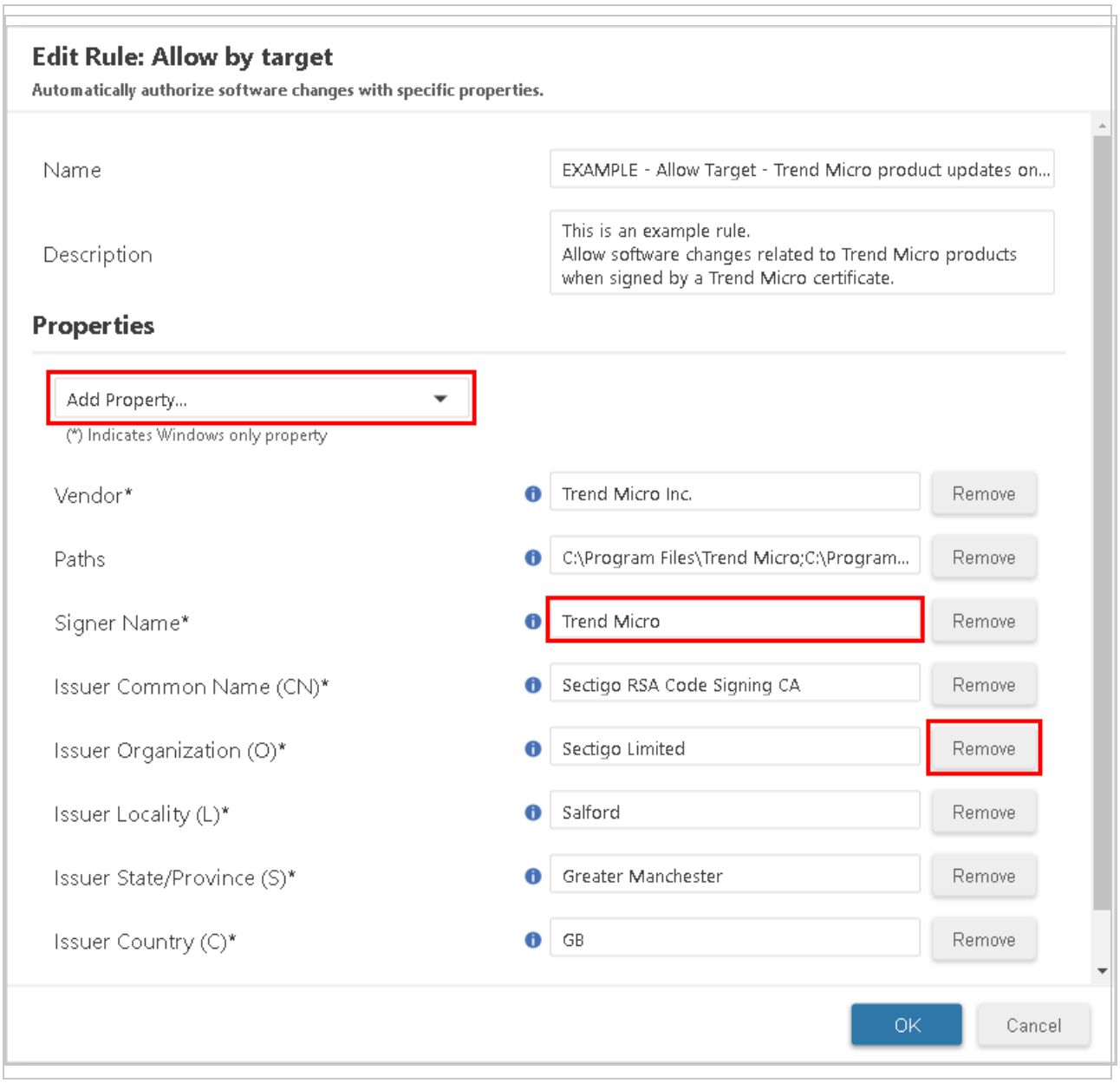
新しい信頼ルールが作成され、信頼ルールセットに割り当てる準備ができました。

ヒント: 信頼ルールのプロパティ値の設定については、「"信頼ルールのプロパティの種類" on page 1125」を参照してください。

ヒント: 信頼ルールを選択し([Policies]→[共通オブジェクト]→[ルール]→[アプリケーションコントロールルール]→[信頼エンティティ]の順に選択)、割り当て/割り当て解除を使用して、どの信頼ルールセットを含めるかを選択します。これは、すばやく割り当てる場合に特に便利です。または、多数のルールセットにまたがる新しいルールの割り当てを解除します。

信頼ルールのプロパティを変更する

1. Deep Security Manager Trust Entities タブ(ポリシー>共通オブジェクト>ルール> アプリケーションコントロール ルール> Trust Entities) から、ルールを選択し、Edit を選択します(またはルールをダブルクリックします)。



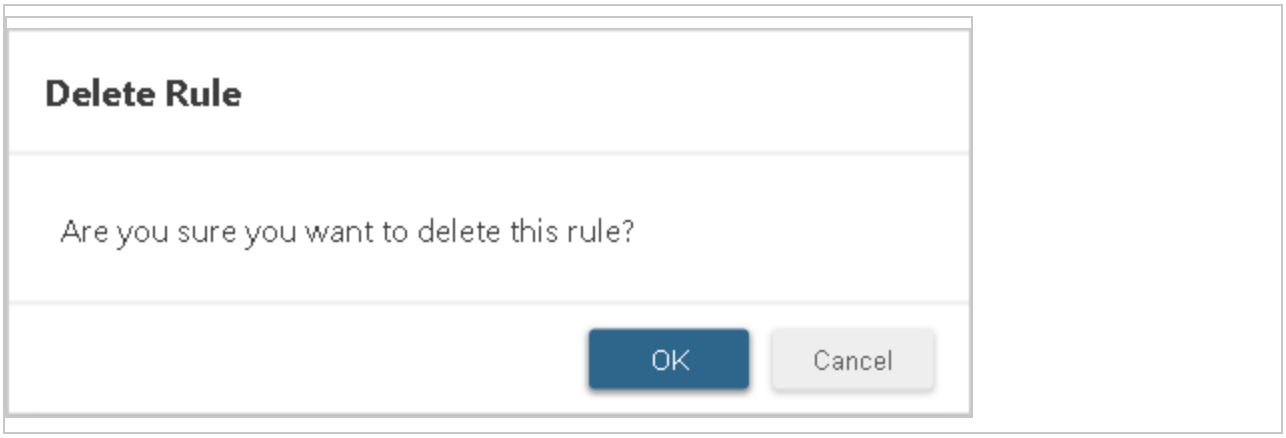
2. [ルールの編集]画面で、次のいずれかを実行します。

   - 新しいプロパティを追加するには、プロパティの追加 ドロップダウンリストからプロパティを選択し、その値を入力します。
   - 既存のプロパティを編集するには、そのテキストフィールドの値を変更します。
   - 既存のプロパティを削除するには、[削除]を選択します。

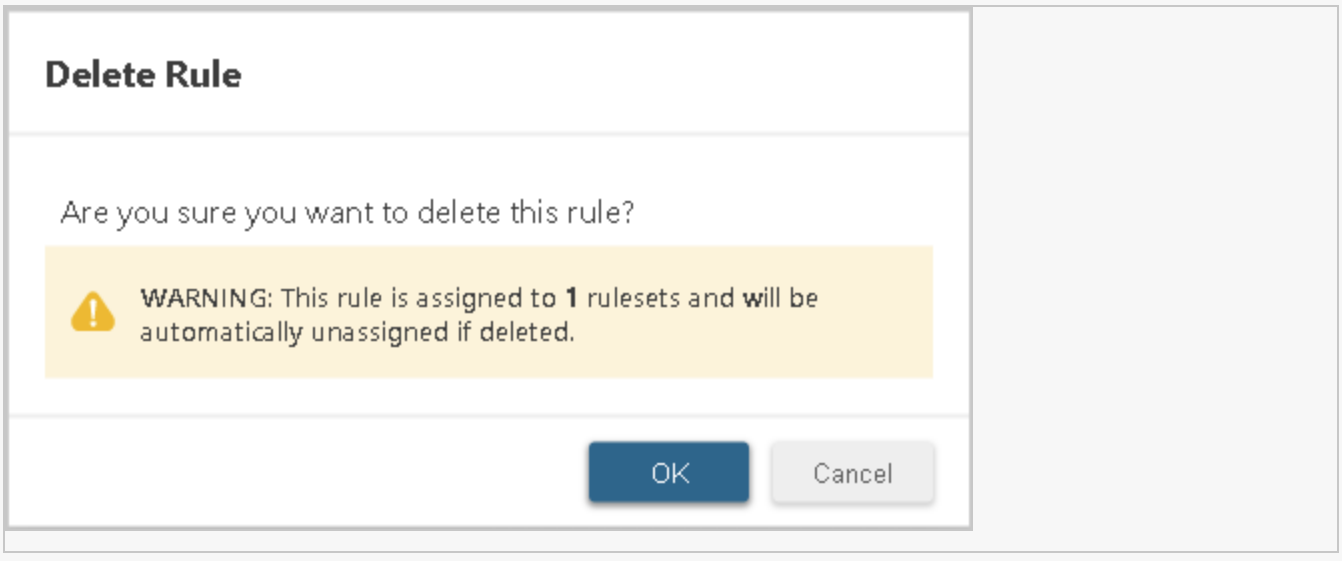
3. [OK] をクリックします。

信頼ルールを削除する

1. Deep Securityから信託団体タブ(ポリシー>共通オブジェクト>ルール>アプリケーションコントロールルール>信頼エンティティ)、ルールを選択して選択します消去。
2. [OK] をクリックして削除を確認します。



注意: いずれかの信頼ルールセットに現在割り当てられている信頼ルールを削除すると、警告メッセージが表示された後、自動的に割り当てが解除されます。



信頼ルールのプロパティの種類

信頼ルールに含まれるプロパティと値は、そのルールによって自動承認されるソフトウェア変更を定義します。次のセクションでは、信頼ルールの設定に使用できる信頼ルールのプロパティの種類について、プロパティ値の設定に必要な情報を見つけるための手順を含めて説明します。

プロセス名

警告: ["信頼ルールの種類" on page 1120] ルールで使用する場合、プロセス名プロパティはDeep Security Agent 20.0.0-3165以降でのみサポートされます。

このプロパティは、ソフトウェア変更を作成するプロセスの名前を指定します。プロセス名には、ファイル名を含むプロセスの絶対パスを使用する必要があります。

ソフトウェア変更のプロセス名を確認するには

1. Deep Security ManagerのActionsタブに移動します。
2. ソフトウェア変更を検索して選択します。

プロセスは、その他の詳細とともに、右側の[変更者プロセス]の下に表示されます。

Deep Security Agentでは、プロセス名にワイルドカードが使用されます。プロセス名にプロセスへのフルパスが含まれる場合:
- パス内のグロブスター**が、プロセス名内の任意の数の追加文字と一致します。- グロブスター**は、プロセス名に含まれる任意の数の追加文字と一致します。- 単一のアスタリスクまたはアスタリスク*は、現在のディレクトリのみの任意の数の追加文字に一致します。- ?単一の文字に一致します。

*文字は、ディレクトリパスの区切り文字 (/および\ ) で検索を停止します。?文字がディレクトリパスの区切り文字と一致しません。ドライブ文字は、ターゲットパス内の他の文字と同じように扱われ、照合に特別な意味はありません。

パス

このプロパティは、信頼ルールに適用される対象パスを指定します。このプロパティに入力されたパス内にソフトウェアの変更が加えられた場合、アプリケーションコントロールは、すべてのサブディレクトリとファイル名を含むソフトウェアの変更を自動的に承認します。セミコロンで区切って複数のパスを設定できます。例: C:\Windows\;C:\Program Files\

パスの値を入力するときは、パスの最後のスラッシュ(\ または /) がどのディレクトリに含まれるかを考慮してください。

- スラッシュで終わるパスは、そのフルパスの下にあるすべてのサブディレクトリに一致します。たとえば、C:\Windows\System\は、Systemディレクトリ内のすべてのサブディレクトリに一致します。
- 最後のスラッシュの後に指定された値は正規表現のワイルドカードとして扱われ、特定のディレクトリ、および同じ値で始まる他のディレクトリと一致します。たとえば、C:\Windows\Systemには、

「C:\Windows\System*」に一致するすべてのディレクトリとサブディレクトリが含まれます。これには、C:\Windows\System\、C:\Windows\System32\、C:\Windows\SystemApps\などがあります。

Deep Security Agentバージョン20.0.0-5137以降では、グロブスター(**) ワイルドカードがサポートされます。パスにグロブスター**を使用すると、現在のディレクトリおよびそのサブディレクトリ内の任意の数の追加文字と一致し、1つのアスタリスク(*)は現在のディレクトリ内の任意の数の追加文字とのみ一致し、疑問符(?)は1つの追加文字と一致します。ドライブ文字またはドライブ区切り文字(/または\)は、ターゲットパス内の他の文字と同じように扱われ、スラッシュ(/)またはバックスラッシュ(\)で停止する*を除き、照合に特別な意味はありません。

SHA-256

ソースからの許可ルールで使用する場合、ソフトウェア変更を作成するソースプロセスのチェックサム(SHA-256)を指定します。[対象による許可]ルールで使用する場合は、ソフトウェア変更自体のチェックサム(SHA-256)になります。

SHA256を見つけるには、次のいずれかを実行します。

Windows PowerShellから(ソースまたはターゲットの場合):
Windows PowerShellコマンドのGet-FileHashの手順に従います。

Deep Security Managerの(ターゲットのみ):
Deep Security ManagerのActionsタブで、ソフトウェア変更を見つけて選択します。

SHA256は、その他の詳細とともに右側のSHA256の下に表示されます。

ベンダ

このプロパティは現在Windowsでのみサポートされており、ソフトウェアのベンダを指定します。

ベンダを見つけるには、次のいずれかを実行します。

ファイルエクスプローラから:
1. プロセスまたはファイルを含むディレクトリから、ファイルエクスプローラーの上部に表示されるプロパティ(名前、変更日など)のいずれかを右クリックし、[詳細]を選択します。
2. [会社名]を選択し、[OK]をクリックします。

ベンダーが[ファイルエクスプローラ]ウィンドウに表示されます。

Deep Securityから:
Deep Security ManagerのActionsタブで、ソフトウェア変更を見つけて選択します。

ベンダーは、その他の詳細とともに、右側の[ベンダー]の下に表示されます。

製品名

このプロパティは、現在Windowsでのみサポートされており、ソフトウェア製品名を指定します。

製品名を確認するには、次のいずれかを実行します。

ファイルのプロパティから:

1. ファイルを含むディレクトリで、プロセスまたはファイルを右クリックし、[プロパティ]を選択します。
2. [詳細] タブで、[製品名] の値を確認します。

ファイルエクスプローラから:

1. ファイルが格納されているディレクトリで、ファイルエクスプローラの上部に表示されるプロパティ(名前、変更日など) のいずれかを右クリックし、[その他] をクリックします。
2. [製品名] を選択し、[OK] をクリックします。

製品名が [製品名] 列に表示されます。

Deep Securityから:

Deep Security ManagerのActionsタブで、ソフトウェア変更を見つけて選択します。

製品名は、その他の詳細とともに [製品名] の右側に表示されます。

署名者名

[ソースから許可] ルールで使用する場合、ソフトウェア変更を作成するソースプロセスの署名者名を指定します。[対象別に許可] ルールで使用する場合は、対象ファイルに署名した証明書の署名者名になります。

このプロパティは現在Windowsでのみサポートされており、ソフトウェア証明書に署名した会社の名前を指定します。

証明書署名者名を確認するには

1. プロセスまたはファイルを右クリックし、プロパティを選択します。
2. [デジタル署名] タブの [署名リスト] で署名者の名前を探します。

[署名者名] に署名者名が表示されます。

ソフトウェア変更イベントまたはセキュリティイベントの最大数を除外するには、署名者名ルールプロパティを使用して、特定の署名者からのすべてのイベントを照合します。

発行者の一般名

このプロパティは現在Windowsでのみサポートされており、署名するソフトウェア証明書の発行者の共通名 (CN) を指定します。

発行者の一般名を確認するには、次の手順に従います。

1. プロセスまたはファイルを右クリックし、[プロパティ] をクリックします。
2. [デジタル署名] タブで、[署名] リストに最初に表示される証明書を選択します。
3. 証明書を選択し、[詳細] をクリックします。
4. [証明書を表示]を選択します。
5. [詳細] タブに移動し、[発行者] を選択します。

証明書に発行者のCNが含まれている場合は、[発行者] の下に表示されます。

発行者の組織単位

このプロパティは現在Windowsでのみサポートされており、ソフトウェア証明書の発行者の組織単位 (OU) を指定します。

発行者の組織単位を見つけるには

1. プロセスまたはファイルを右クリックし、プロパティを選択します。
2. [デジタル署名]タブで、署名リストに表示される最初の証明書を選択します。
3. 証明書を選択し、[詳細] をクリックします。
4. [証明書を表示] をクリックします。
5. [詳細] タブに移動し、[発行者] を選択します。

証明書に含まれている場合は、発行者のOUが表示されます。

発行者の組織

このプロパティは現在Windowsでのみサポートされており、ソフトウェア証明書の発行者組織 (O) を指定します。

発行元の組織を確認するには

1. プロセスまたはファイルを右クリックし、[プロパティ] をクリックします。
2. [デジタル署名]タブで、署名リストに表示される最初の証明書を選択します。
3. 証明書を選択し、[詳細] をクリックします。
4. [証明書を表示] をクリックします。
5. [詳細] タブに移動し、[発行者] を選択します。

証明書に含まれている場合は、発行者Oが表示されます。

発行者の地域

このプロパティは、現在Windowsでのみサポートされており、ソフトウェア証明書の発行者の地域 (L) を指定します。

発行元の場所を確認するには

1. プロセスまたはファイルを右クリックし、[プロパティ] をクリックします。
2. [デジタル署名]タブで、署名リストに表示される最初の証明書を選択します。
3. 証明書を選択し、[詳細] をクリックします。
4. [証明書を表示] をクリックします。
5. [詳細] タブに移動し、[発行者] を選択します。

証明書に含まれている場合は、発行者Lが表示されます。

発行者の都道府県

このプロパティは現在Windowsでのみサポートされており、ソフトウェア証明書の発行者の都道府県 (S) を指定します。

発行者の都道府県を確認するには

1. プロセスまたはファイルを右クリックし、[プロパティ] をクリックします。
2. [デジタル署名]タブで、署名リストに表示される最初の証明書を選択します。
3. 証明書を選択し、[詳細] をクリックします。
4. [証明書を表示] をクリックします。
5. [詳細] タブに移動し、[発行者] を選択します。

証明書に含まれている場合は、発行者Sが表示されます。

発行国

このプロパティは現在Windowsでのみサポートされており、ソフトウェア証明書の発行元の国 (C) を指定します。

発行国を確認するには:

1. プロセスまたはファイルを右クリックし、[プロパティ] をクリックします。
2. [デジタル署名]タブで、署名リストに表示される最初の証明書を選択します。
3. 証明書を選択し、[詳細] をクリックします。
4. [証明書を表示] をクリックします。
5. [詳細] タブに移動し、[発行者] を選択します。

証明書に含まれている場合は、発行者Cが表示されます。

アプリケーションコントロールイベントの集約と分析

サーバ上の動的ソフトウェアアップデートにより、何千ものドリフトイベント([処理] 画面) やセキュリティイベント([アプリケーションコントロールイベント] 画面) が発生する可能性があります。これは、事後に何を承認するかを判断するのが難しいため、アプリケーションコントロールを使用する際の課題となります。Deep Security Agent 20.0.0.5761以降を使用している場合にこの状況を軽減するには、異常なドリフトイベントとセキュリティイベントのみを表示する信頼ルールを作成します。これにより、サーバをロックダウンして、不正なソフトウェアの実行を防ぐこともできます。

ドリフトイベントは、プロセス名とターゲットパスに基づいて集計されます。セキュリティイベントは、SHA256ハッシュと対象パスに基づいて集計されます。たとえば、同じプロセスで同じパスに10,000個のドリフトアイテムが作成された場合、そのドリフトは、processName属性とpaths属性を持つ1つの信頼ルールに集約されます。

エージェントの診断が要求されると、集約されたドリフトイベントとセキュリティイベントが信頼ルール形式でJSONファイルに保存され、診断に含まれます。信頼ルールエディタはこのJSONファイルを使用して、サーバの信頼ルールを追加できます。

ドリフトイベント

JSON形式のドリフトイベントには、次の属性があります。

```
{"time":1615999592250,"eventType":"ApplicationControl","uid":1063,"g
id":1064,"operationType":"create","user":"ribapp","group":"ribapp",
```

"md5":"57579EF7681147B84774F69F44783A67","sha256":"90B0418DCB3B29440EE6F69FEE05BD54265CEE3BCFABDA8ED355E257FECC2939",

"processName":"/opt/IBM/WebSphere/AppServer/java/jre/bin/java","type":4,"rdev":0,"lastModificationTime":1615999090000,"mode":33188,"size":3984617,

"sha1":"B226BDB9DB39AD38C4BEB6FE4F1C1C7151207848","nlink":1,"procUser":"ribapp","isAuthorized":1,"pid":10223,"fileExtension":"jar",

"operationDate":1615999591534,"procUid":1063,"procGroup":"ribapp","path":"/opt/IBM/WebSphere/AppServer/profiles/devmiesAppSrv/installedApps/devdmrhx01-cell02/IESHSRIDEVM.ear/","fileName":"DC.jar","recordTime":1615999592215,"fileSystemType":"ext4","procGid":1063,"dev":64775,"source":4,"ino":3801778}

- processNameは、対象ファイルを作成またはアップデートしたプロセスの名前です。前の例では、/opt/IBM/WebSphere/AppServer/java/jre/bin/javaに設定されています。
- pathは、プロセスが実行可能ファイルをアップデートまたは作成した場所です。前述の例では、/opt/IBM/WebSphere/AppServer/profiles/devmiesAppSrv/installedApps/devdmrhx01-cell02/IESHSRIDEVM.ear/に設定されています。

ドリフトイベントの信頼ルール

イベントのドリフトを自動承認する信頼ルールを作成できます。このルールに対してtrustTypeを1に設定することで、信頼できるアップデータを定義できpaths 。

"trustrules": [{
"trustType":"1",

"processName":"/opt/IBM/WebSphere/AppServer/java/jre/bin/java",

```
"paths":"/opt/IBM/WebSphere/AppServer/profiles/devmiesAppSrv/install
edApps/devdmrhx01-cell02/IESHSRIDEVM.ear/"
        }, ]
```

信頼ルールを作成するためのドリフトイベントの処理は、多対1の操作になる場合があります。たとえば、/opt/IBM/WebSphere/AppServer/java/jre/bin/javaという名前のプロセスがパス/opt/IBM/WebSphere/AppServer/profiles/devmiesAppSrv/installedApps/devdmrhx01-cell02/IESHSRIDEVM.ear/に数千のJARファイルを作成した場合、前述の信頼ルールによってこれらすべてのJARファイルのドリフトが排除されるため、信頼ルールはドリフトを効率的に集計できます。

信頼ルールは、ルールごとに1つの一意のプロセスを含むルールの配列で構成されます。各信頼ルールのpaths属性には、複数のパスを定義できます。たとえば、process1という名前のプロセスが、path1、path2、path3の3つの異なる場所でドリフトを作成した場合、1つの信頼ルールで、次のすべての場所でprocess1によって作成されたすべてのドリフトを取得できます。

```
"trustrules": [{
    "trustType":"1",
    "processName":"process1",
    "paths":"path1;path2;path3"
}, ]
```

プロセスのヒットカウントを目的としたhitcountという追加の属性があります。この属性を使用して、特定の信頼ルールにヒットした回数を確認できます。

拡張子のヒットカウントもあります。拡張子は、プロセスが特定の拡張子を持つファイルを更新するたびに増分することによって追跡されます。

```
"trustrules": [{
    "trustType":"1",
    "processName":"process1",
    "paths":"path1;path2;path3",
    "hitcount":12342,
    ".jar":1234,
    ".py":323,
    ".":456
}, ]
```

前述の例では、JARファイルが1234回、piファイルが323回、拡張子のないファイルが456回更新されたプロセスを示しています。

セキュリティイベント

JSON形式のセキュリティイベントには、次の属性があります。


```
          "
{time":1492100772165,"eventType":"ApplicationControl","sha1":"066A02
D230F3B16439396B049DC

912DB376B96CE","fileName":"svchost.exe","operationType":"detectOnly"
,"blockReason":2,"size":31

1544,"sha256":"62EFB22F6853D73374761A0B8ED2CE40BF09AA401EC7D4AAAA0CE
4D5C3380EEA","type":1,
        "path":"C:\\Windows\System32\\","pid":1832,"operationDate":

1492100772149,"processName":"\\device\\harddiskvolume2\\windows\\sys
tem32\\cmd.exe","md5":
        "5F7B8544F7A20800069107FC93384F0E"},

{"time":1492100772165,"eventType":"ApplicationControl","blockReason"
:2,"sha256":"62EFB22F6

853D73374761A0B8ED2CE40BF09AA401EC7D4AAAA0CE4D5C3380EEA","size":3115
44,"processName":"\\de

vice\\harddiskvolume2\\windows\\system32\\cmd.exe","sha1":"066A02D23
0F3B16439396B049DC912D

B376B96CE","operationType":"detectOnly","pid":1832,"md5":"5F7B8544F7
A20800069107FC93384F0E
```

```
          ","path":"C:\\Program Files\\Trend Micro\\Deep Security
  Agent\\","operationDate":149210077}
```

前の例では、sha256が62EFB22F6853D73374761A0B8ED2CE40BF09AA401EC7D4AAAA0CE4D5C3380EEAに設定され、pathがC:\\Windows\System32\\に設定されています。

セキュリティイベントの信頼ルール

セキュリティイベントのドリフトを自動承認する信頼ルールを作成できます。SHA256ハッシュに基づいて、次のいずれかのpathsで、このルールのtrustTypeを2に設定することで、信頼できる対象を定義できます。

```
          "trustrules": [{
              "trustType":"2",

  "sha256":"62EFB22F6853D73374761A0B8ED2CE40BF09AA401EC7D4AAAA0CE4D5C3
  380EEA",
              "paths":"C:\\Windows\System32\\"
          }, ]
```

セキュリティイベントを処理して信頼ルールを作成する作業は複雑です。信頼ルールは、ルールごとに1つの一意のSHA256を含むルールの配列で構成されます。各信頼ルールのpaths属性には、複数のパスを定義できます。たとえば、異なる場所path1 、path2 、path3からsha256コンテンツハッシュAAAAAAAABBBBBBBBCCCCCCCCDDDDDDDDD を使用してファイルが実行された場合、1つの信頼ルールでこれを次のように表すことができます。

```
          "trustrules": [{
              "trustType":"2",
              "sha256":"AAAAAAAABBBBBBBBCCCCCCCCDDDDDDDDD",
              "paths":"path1;path2;path3"
          }, ]
```

SHA256ヒットカウントを目的としたhitcountという追加の属性があります。この属性を使用して、特定の信頼ルールにヒットした回数を確認できます。

ファイル名のヒット数もあり、異なる名前のファイルが同じSHA256コンテンツハッシュを持つことができます。この属性を使用して、特定の名前のファイルが使用されて同じSHA256が実行された回数をカウントできます。次の例では、SHA256 AAAAAAAABBBBBBBBCCCCCCCCDDDDDDDDEEEEEEEEが12342回実行され、filename1が2342回使用され、filename2が10000回使用されています。filename1とfilename2のコンテンツハッシュは同じです。

異なる名前のプロセスでも同じSHA256コンテンツハッシュを使用して同じターゲットを実行できるため、プロセス名が使用されて同じSHA256が実行された回数もカウントできます。次の例では、SHA256 AAAAAAAABBBBBBBBCCCCCCCCDDDDDDDDEEEEEEEEが12342回実行され、filename1が2342回使用され、filename2が10000回使用されています。filename1とfilename2のコンテンツハッシュは同じです。プロセス名/opt/process1 /process1はターゲットの12000回の実行に使用され、/opt/process2は ターゲットの342回の実行に使用されました。

```
"trustrules": [{
    "trustType":"2",
    "sha256":"AAAAAAAABBBBBBBBCCCCCCCCDDDDDDDDEEEEEEEE",

    "paths":"path1;path2;path3",
    "hitcount":12342,
    "filename1":2342,
    "filename2":10000
    "/opt/process1":12000,
    "/opt/process2":342
}, ]
```

プロセスは絶対パスで表され、ファイル名はいずれかのパスへの相対パスで表されることに注意してください。

イベント分析出力

アプリケーションコントロールのイベント分析出力は、ac_event_analysis.txtというファイルに送信されます。このファイルには、追加のヒットカウント属性と拡張子ヒットカウント属性を含む信頼ルール形式があります。

```
trustrules": [{
    "trustType":"1",
    "processName":"process1",
```

```
        "paths":"path11;path12;path13",
        "hitcount":12342,
        ".jar":12342
    }
    {
        "trustType":"1",
        "processName":"process2",
        "paths":"path21;path22;path23",
        "hitcount":23232,
        ".py":23232
    }
    {
        "trustType":"1",
        "processName":"process3",
        "paths":"path31;path32;path33",
        "hitcount":34332,
        ".exe":34322
    }
    {
        "trustType":"1",
        "processName":"process4",
        "paths":"path41;path42;path43",
        "hitcount":12312,
        ".":12312
    }, ]
```


ファイルの場所は次のとおりです。

- Windowsの場合: C:\ProgramData\Trend Micro\Deep Security Agent\diag\ac_event_analysis.txt
- Linuxの場合: /var/opt/ds_agent/diag/ac_event_analysis.txt
- 診断ファイル: agent/ac/ac_event_analysis.txt

分析は再起動時にこのファイルからロードされるため、Agentの再起動後もその状態が維持されます。アプリケーションコントロールを無効にしてから有効にすると、分析はクリアされます。ac_event_analysis.txtファイルを表示するには、JQまたはオンラインのJSON formatterを使用します。

信頼ルールのデバッグ

信頼ルールは次のようにデバッグできます。

1. Deep Security Managerに新しい信頼ルールを適用します。
2. Deep Security Agentを停止します。
3. ac_event_analysis.txtファイルを削除します。
4. Deep Security Agentを起動します。
5. しばらく待って、ac_event_analysis.txtファイルが再表示されるかどうかを確認します。
   - ファイルが表示されなくなった場合は、信頼ルールが機能しており、イベントの生成が抑制されています。
   - ファイルが引き続き表示される場合は、ac_event_analysis.txtファイルで新しいイベント情報を確認し、必要に応じて新しい信頼ルールを追加します。信頼タイプ1のルールは、ドリフトイベントを自動承認するためのソースルールによる許可であり、信頼タイプ2のルールは、対象ファイルの実行を許可するための対象ルールによる許可です。
6. 新しい信頼ルールを設定するには、手順1からの手順を繰り返します。

信頼ルールがヒットする頻度を確認するには、次のようにAgentでsendCommandを実行します。

- Linux: /opt/ds_agent/sendCommand --get TrustRules
- Windowsの場合: \program files\trend micro\deep security agent\sendCommand --get TrustRules

コンサルト指標

ドリフト分析とイベント分析がアプリケーションコントロールのメトリクスに追加されました。ここでは、ヒット数の多い上位10件のプロセスがdrift_analysisオブジェクトに格納され、SHA256件数の多い上位10件がevent_analysisオブジェクトに格納されます。


```
"AC": {
    "eventReportInQueue":"0",
    "evtPreCreateProcessHandled":"17",
    "acProcessHashCount":"0",
    "acProcessBlockUnrecognized":"0",
    "engFlushDbBufferError":"0",
    "acFileProcessImgPath":"0",
```

```
"evtFilePostClose":"249",
"acFileErrorHash":"0",
"acFileAllowImportingRuleset":"0",
"evtFilePreCreateFromContainer":"0",
"evtFilePostChmodFromContainer":"0",
"engStopError":"0",
"evtFilePreCreateHandled":"0",
"ctrlInterpreterMatched":"0",
"engPurgeDb":"0",
"importCount":"0",
"inventoryAdsVisited":"0",
"engGetInventory":"1",
"acFileAllow":"5",
"acFileAllowBuilding":"0",
"engSetConfigError":"0",
"ctrlMsiInstallationMatched":"0",
"ctrlDropProcessEvtReportQueueFull":"0",
"importFail":"0",
"eventReportDropped":"0",
"evtFilePostChmod":"3",
"acFileBlock":"0",
"acFileDrift":"3",
"engGetMetricsError":"0",
"ctrlDropFileEvtReportQueueFull":"0",
"inventoryFolderVisited":"0",
"engStartError":"0",
"evtFileCloudFileIgnore":"0",
"engSetConfig":"1",
"engFlushDbBuffer":"0",
"engPurgeDbError":"0",
"inventoryBytesInventoried":"433695822",
"evtPreCreateProcessWithCmdLine":"0",
"inventoryDriveVisited":"0",
```

```
            "importSuccess":"0",
            "engSetRuleset":"0",
            "eventReportSent":"3",
            "drift_analysis": [
                {
                "trusttype":"1",
                "processName":"/usr/bin/bash",
                "hitcount":2,
                "paths":"/im1"
                },
                {
                "trusttype":"1",
                "processName":"/usr/bin/cp",
                "hitcount":1,
                "paths":"/im1"
                }
            ],
            "event_analysis": [
                {
                "trusttype":"2",
                "sha256":"AAAAAAAABBBBBBBBCCCCCCCCDDDDDDDDEEEEEEEE",
                "hitcount":2,
                "paths":"/im1"
                },
                {
                "trusttype":"2",

"sha256":"EEEEEEEEDDDDDDDDCCCCCCCCBBBBBBBBAAAAAAAA",
                "hitcount":1,
                "paths":"/im1"
                }
            ],
```

署名者情報の表示

信頼ルールを有効にすると、ドリフトイベント分析の信頼ルールにファイル署名者情報とプロセス署名者情報の両方が含まれます。セキュリティイベント分析のために、ファイルの署名者情報が含まれます。

信頼エンティティルールセットがホストに適用されると、信頼ルールが有効になります(ファイル署名者情報とプロセス署名者情報はac_event_analysis.txtファイルに表示されます)。

Linuxの信頼ルールプロパティの制限

警告: Linuxで現在サポートされていない信頼ルールを追加すると、ルールはソフトウェアの変更に適用されなくなります。

次のトラストルールのプロパティは、現在Linuxではサポートされていません。

- 署名者名
- 製品名
- 発行者の一般名
- 発行者の組織単位
- 発行者の組織
- 発行者の地域
- 発行者の都道府県
- 発行国
- ベンダ

Linuxでは現在、次の信頼ルールのプロパティのみがサポートされています。

- プロセス名
- パス
- SHA-256

ソフトウェアの変更後にアプリケーションコントロールをリセットする

アプリケーションコントロールの概要については、"アプリケーションコントロール" on page 1093を参照してください。

アプリケーションコントロールは頻繁にアップデートされない安定版サーバでの使用を目的としており、多くのソフトウェア変更を受けるワークステーションやサーバには使用できません。

変更が多すぎると、古いルールを削除しないかぎり、大量のルールセットが生成されて多くのRAMが消費されます。承認されたソフトウェアのアップデート時にメンテナンスモードを使用しない場合は、変更が多すぎると、管理者が変更ごとに許可ルールを手動で作成しなければならないため、作業負荷の増加にもつながります。

認識されないソフトウェアの変更が最大値を超えた場合、アプリケーションコントロールは、コンピュータのすべてのソフトウェア変更の検出と表示を停止します。この停止は、ルールセットが大きくなりすぎた場合に発生する可能性のあるメモリ不足やディスク容量のエラーを防ぐことを目的としています。

停止が発生した場合、のDeep Security Managerは(「未解決のソフトウェアの変更の制限に達した」) 警告(「未解決のソフトウェア変更の制限」) およびイベントログを通知します。ソフトウェアの変更の検出を継続するには、問題を解決する必要があります。

1. コンピュータのプロセスとセキュリティイベントを調べ、コンピュータが攻撃を受けていないことを確認します。攻撃を受けていないかどうかがわからない場合や十分な時間がない場合、最も安全かつ迅速な方法は、バックアップまたは仮想マシンスナップショットからシステムを復元することです。

   警告: 不正なソフトウェア(ゼロデイ不正プログラム), アプリケーションコントロールでは、アプリケーションコントロールをリセットする際に、無視されます。それはもはや[処理]タブに表示されず、プロセスがすでに実行されていてRAM上にある場合、コンピュータを再起動するまで アプリケーションコントロールはイベントやアラートをログに記録しません。

2. コンピュータが自動アップデート(ブラウザ、Adobe Reader、yumの自動アップデート), など) を実行している場合は、アプリケーションコントロールの管理モードを有効にした場合にのみ、これらのアップデートが実行されるようにスケジュールまたはスケジュールを設定します("変更の計画時にメンテナンスモードをオンにする" on page 1104).
3. アプリケーションコントロールをリセットします。これを行うには、**コンピュータエディタ**[1]でアプリケーションコントロールを無効にします。エージェントが肯定応答を返し、エラーステータスがクリアされたら、再度アプリケーションコントロールを有効にしてください。エージェントは、新しいソフトウェアインベントリリストを生成します。

共有ルールセットとグローバルルールセットを作成するためのAPIの使用

アプリケーションコントロールの概要については、"アプリケーションコントロール" on page 1093を参照してください。初期設定の手順については、"アプリケーションコントロールの設定" on page 1099を参照して

[1] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。

ください。

Automation CenterでDeep Security Manager APIを使用して、共有ルールセットとグローバルルールを作成できます。1種類のルールセットを使用することも、組み合わせて使用することもできます。詳細については、共有ルールセットの作成およびグローバルルールの追加を参照してください。

- ローカルルールセット:コンピュータのソフトウェアインベントリの一部として、またはメンテナンスモードで追加されたルールは、保護対象コンピュータにのみ保存され、Deep Security Managerでは表示されません。Deep Security Managerで設定するルールの許可またはブロックは、Agentに送信され、両方の場所に保存されます。Agentはインベントリ情報をManagerに転送しないため、ローカルルールセットは共有ルールセットよりも優れたパフォーマンスを発揮します。

  ソフトウェアが新しくなったのか、変更されたのかを判断するために、Deep Security Agent 10は、初期インストールされているソフトウェアのSHA-256ハッシュ、ファイルサイズ、パス、およびファイル名 (「ファイルベース」ローカルのルールセット) を持つファイルと比較します。Deep Security Agent 11以降では、ファイルのSHA-256ハッシュとファイルサイズのみが比較されます (ハッシュベースのローカルルールセット) が使用されます。Deep Security 11 (およびそれ以降の) Agentで作成されたルールでは、一意のハッシュおよびファイルサイズのみを比較するので、ソフトウェアファイルの名前変更または移動が実行された場合にも、ルールは引き続き適用されます。その結果、Deep Security Agent 11以降を使用すると、処理が必要なソフトウェアの変更数が減少します。Deep Security Agent 10は、Deep Security Agent 11.0以上にバージョンアップされるまで、引き続きファイルベースのローカルルールセットを使用します。アップグレードすると、そのローカルルールセットはハッシュベースのルールを使用するように変換されます。

  > 注意:同じハッシュ値に対するファイルベースのルールが複数ある場合、それらのルールは1つのハッシュベースのルールに統合されます。統合されるルールが相互に競合する場合 (1つのルールがファイルをブロックし、もう1つがそのファイルを許可する場合)、新しいハッシュベースのルールは「許可」ルールになります。

- 共有ルールセット:すべてのルールデータをAgentとManagerの両方に同期します (有効な場合はRelayも対象)。これにより、ネットワークとディスクの使用量が増加します。ただし、初期インベントリ検索またはメンテナンスモードのルールを確認する必要がある場合や、設定が同一でなければならない多数のコンピュータで構成されるサーバファームを管理する場合は、共有ルールセットを使用する方が業務を簡素化できることがあります。共有ルールセットは、同じ構成のLAMP Webサーバで構成されるサーバプールや、複数仮想マシンでオートスケーリンググループを構成している場合などに便利です。管理作業の負荷も軽減できます。

警告: [承認されていないソフトウェアを明示的に許可するまでブロック] が有効で、コンピュータが単に類似しているが同一ではない場合は、共有ルールセットを使用しないでください。最初のコンピュータのルールセットに含まれていない他のコンピュータのすべてのソフトウェアがブロックされてしまいます。重要なファイルが含まれている場合、OSが破損する可能性があります。OSが破損すると、再インストール、バックアップの復元、またはOSの復旧モードの使用が必要になる可能性があります。

Deep Security Agent 11.1以降を使用して新しい共有ルールセットを作成する場合、ハッシュベースのルール(ファイルのハッシュとサイズのみを比較するルール) のみを含めることができます。Deep Security Agent 11.0以前を使用して共有ルールセットを作成した場合は、ファイルベースのルール(ファイルの名前、パス、サイズ、およびハッシュを比較するルール) が含まれます。共有ルールセットを使用するすべてのAgentがDeep Security Agent 11.0以降にアップグレードされるまで、古い共有ルールセットでは引き続きファイルベースのルールが使用されます。共有ルールセットは、ハッシュベースのルールを使用するように変換されます。

警告: すべてのエージェントがDeep Security Agent 11.0以上にアップグレードされるまで、新しい共有ルールセットを作成しないでください。新しい共有ルールセットはハッシュベースであり、ファイルベースのルールセットのみをサポートするDeep Security Agent 10.3以前とは互換性がありません。

注意: 同じハッシュ値に対するファイルベースのルールが複数ある場合、それらのルールは1つのハッシュベースのルールに統合されます。統合されるルールが相互に競合する場合 (1つのルールがファイルをブロックし、もう1つがそのファイルを許可する場合)、新しいハッシュベースのルールは「許可」ルールになります。

共有ルールを作成するには、オートメーションセンターの共有ルールセットの作成を参照してください。

- グローバルルール: 共有ルールセットと同様に、グローバルルールはマネージャによってエージェントに配信されます(有効な場合はリレーも含まれます) 。これにより、ネットワークとディスクの使用量が増加します。ただし、これらのルールセットはグローバルであるため、各ポリシーでの選択の手間を省くことができます。グローバルルールは、Deep Security Managerに表示されるルールセットの一部ではありません。グローバルルールにはブロックルールのみを含めることができ、ルールは許可しません。

グローバルルールを使用するには、Deep Security Agent 10.2以降が必要です。Managerは、古いAgentにはグローバルルールを送信しません。グローバルルールは、他のすべてのアプリケーションコントロールルールよりも優先され、アプリケーションコントロールが有効になっているすべてのコンピュータに適用されます。グローバルルールのルールは、ファイルのMD5、SH-1、またはSHA-256ハッシュに基づいています。ソフトウェアファイルのハッシュは一意であるため、ファイルパス、ポリシー、またはコンピュータグループに関係なく、またアプリケーションコントロールが以前にソフトウェアを検出したかどうかに関係なく、特定のソフトウェアをすべての場所でブロックできます。

> 注意: マルチテナント展開では、各テナントにグローバルルールが個別に割り当てられます。すべてのテナントに対してソフトウェアをブロックするには、各テナントに同一のグローバルルールを作成します。

グローバルルールを作成するには、オートメーションセンターの[グローバルルールを追加]を参照してください。

このトピックの内容:

- "共有ルールセットを作成する" below
- "共有許可およびブロックルールからコンピュータ固有の許可およびブロックルールに切り替える" on the next page
- "Relayを介してアプリケーションコントロール共有ルールセットをインストールする" on page 1147
- "共有ルールセットを使用するリレーを使用する場合の考慮事項" on page 1149

共有ルールセットを作成する

APIを使用して、共有の許可ルールまたはブロックルールを作成し、ルールセットを他のコンピュータに適用できます。これは、同一のコンピュータが複数ある場合 (Webサーバファームで負荷を分散している場合など) に便利です。共有ルールセットはインベントリが完全に一致するコンピュータにのみ適用する必要があります。

1. APIを使用してコンピュータの共有許可およびブロックルールを構築します。詳細については、[共有ルールセットの作成]を参照してください。展開する前に共有ルールセットを確認したい場合は、"アプリケーションコントロールルールセットの表示と変更" on page 1110を参照してください。
2. **コンピュータエディタまたはポリシーエディタ**[1]で、[アプリケーションコントロール] に進みます。

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

3. [ルールセット] で、[設定を継承] が選択されていないことを確認してから、[共有ルールセットを使用] を選択します。使用する共有ルールセットを指定します。

   注意: これらの設定は、APIを使用して作成した共有ルールセットがない場合は表示されません。共有ルールセットを作成していない場合、または初期設定をそのまま使用する場合は、各コンピュータには独自の許可およびブロックルールがローカルに使用されます。ローカルルールに対する変更は他のコンピュータには反映されません。

4. [保存] をクリックします。

   次回コンピュータのDeep Security AgentがDeep Security Managerに接続すると、エージェントはそれらのルールを適用します。

   ルールセットのアップロードに失敗したことを示すエラーが表示された場合は、エージェントとマネージャまたはリレー間のネットワークデバイスがハートビートポートまたは ポート番号 の中継を許可することを確認します。

共有許可およびブロックルールからコンピュータ固有の許可およびブロックルールに切り替える

コンピュータで現在API経由で作成された共有ルールが許可されている場合は、ローカルルールを使用するように変更できます。アプリケーションコントロールをはじめて有効にしたときと同様に、ファイルシステムに現在インストールされているすべてのソフトウェアが検索され、初期ルールセットが作成されます。

警告: この手順を開始する前に、適切なソフトウェアのみが現在インストールされていることを確認してください。ルールセットを再構築すると、安全性が確認されていないソフトウェアや不正プログラムも含め、現在インストールされているすべてのソフトウェアが許可されます。インストールされているソフトウェアを把握していない場合は、クリーンインストールを実施し、その後でアプリケーションコントロールを有効にするのが最も安全な方法です。

以下の手順は、特定のコンピュータのAgentでローカルルールセットを使用するように設定する手順です。すべてのコンピュータでローカルルールを使用する場合は、代わりに [ポリシー] タブで設定を編集します。

1. **コンピュータエディタ**[1]で、[アプリケーションコントロール] に進みます。
2. [ルールセット] で、[設定を継承] が選択されている場合は解除し、[最初はインストールされているソフトウェアに基づいてローカルルールセットを使用] を選択します。
3. [保存] をクリックします。

   変更内容を確認するには、次回エージェントとDeep Security Managerが接続するときに、次の項目を確認します。イベントログメッセージのビルドについてアプリケーションコントロールルールセット。

Relayを介してアプリケーションコントロール共有ルールセットをインストールする

アプリケーションコントロールルールセットを作成または変更するたびに、使用するすべてのコンピュータに配布する必要があります。共有ルールセットはローカルルールセットよりも大きくなります。また、共有ルールセットはさまざまなサーバにも適用されることがあります。ルールセットをManagerから同時に直接ダウンロードすると、負荷が大きくなり、パフォーマンスが低下する可能性があります。グローバルルールセットの注意事項も同じです。

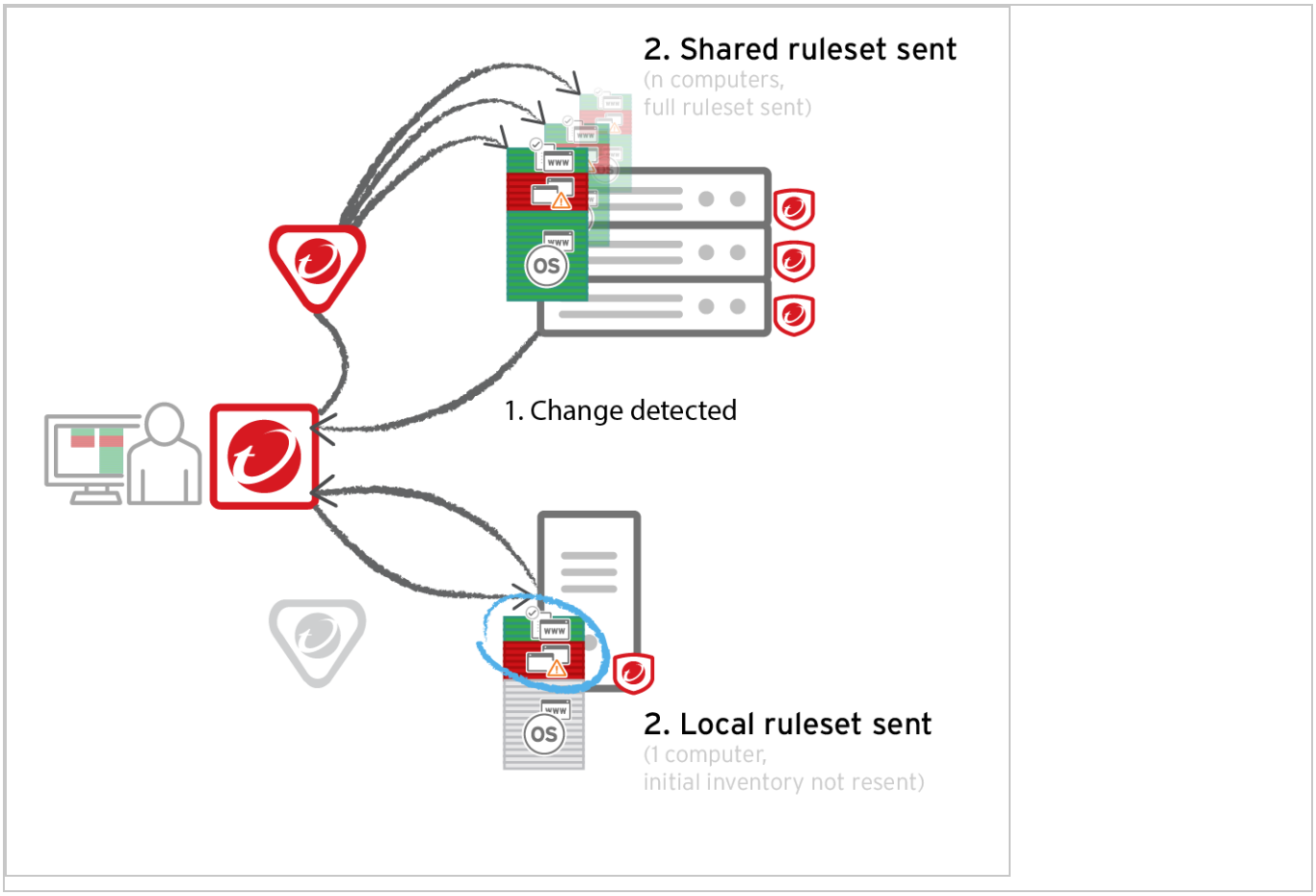
Deep Security Relayを使用すると、この問題を解決できます。(Relayの設定の詳細については、「"追加のリレーを配信する" on page 1467」を参照してください。)

マルチテナント環境を使用しているかどうかによって、手順が異なります。

単一テナント環境

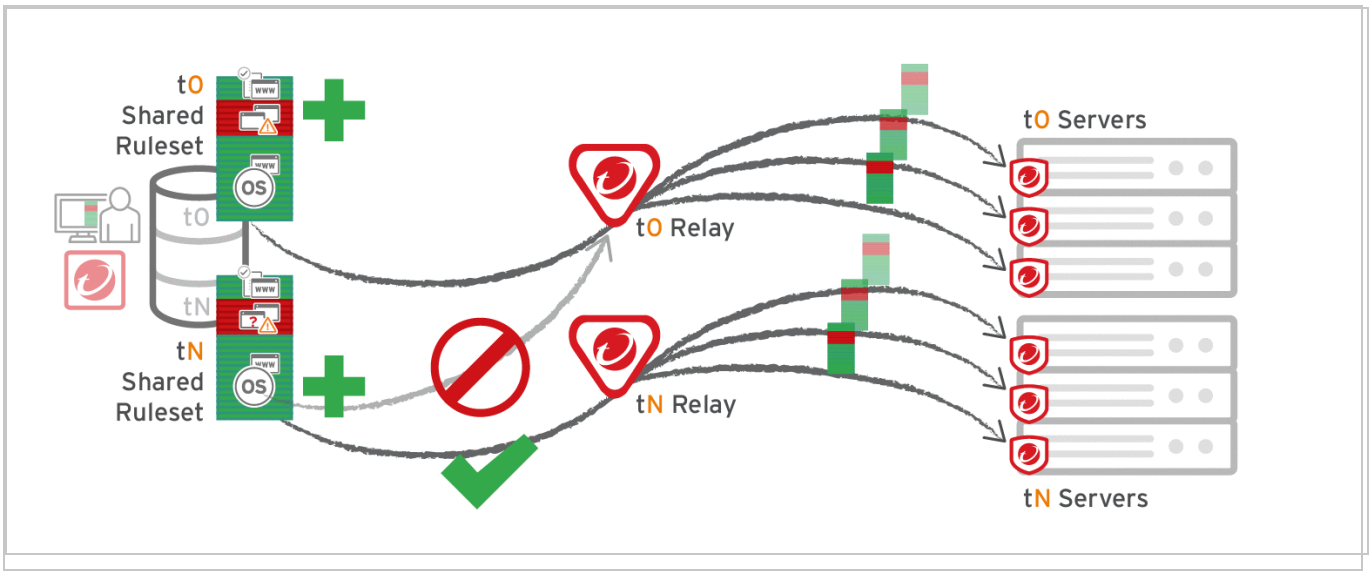
[管理]→[システム設定]→[詳細] の順に選択し、[アプリケーションコントロールルールセットをRelayから提供する] を選択します。

[1] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック) します。



マルチテナント環境

プライマリテナント(t0)は他のテナント(tN)の設定にアクセスできないため、t0 RelayにはtNアプリケーションコントロールルールセットが設定されません。他のテナント(tN)は独自のRelayグループを作成してから[アプリケーションコントロールルールセットをRelayから提供する]を選択する必要があります。



共有ルールセットを使用するリレーを使用する場合の考慮事項

Relayを使用する前に、Relayに使用環境との互換性があることを確認してください。以前にダウンロードされて現在有効になっているルールセットがAgentにない場合、Agentが新しいアプリケーションコントロールルールを受け取らないと、コンピュータがアプリケーションコントロールによって保護されることはありません。アプリケーションコントロールルールセットのダウンロードに失敗した場合は、ルールセットダウンロード失敗イベントが、ManagerおよびAgentで記録されます。

- プロキシを使用してAgentをManagerに接続する場合は、Relayを使用する必要があります。

  注意: Deep Security Agent 10.0以前では、クライアントはプロキシ経由でリレーに接続できませんでした。ルールセットのダウンロードにプロキシが原因で失敗した場合、およびクライアントがリレーまたはマネージャにアクセスするためにプロキシを要求する場合は、次のいずれかを実行する必要があります。

  - アップデートエージェントのソフトウェア、次にがプロキシを設定する
  - プロキシをバイパスする。
  - Relayを追加してから、[アプリケーションコントロールルールセットをRelayから提供する] を選択する。

- 共有ルールセットまたはグローバルルールセットを使用している場合は、Relayを使用するとパフォーマンスが向上します。
- ローカルルールセットを使用している場合は、Relayを使用するとパフォーマンスが低下する可能性があります。

- プライマリ以外のテナント(tN) が初期設定のプライマリ(t0) Relayグループを使用する場合は、マルチテナント設定でRelayを使用しないでください。

イベントとアラートを設定する

Deep Securityイベントログについて

Deep Security Agentは、保護モジュールのルールまたは条件がトリガされたとき(「セキュリティイベント」) に記録されます。AgentおよびDeep Security Managerは、管理イベントやシステム関連のイベントが発生したときにも記録を作成します( ), 、管理者ログイン、アップグレード対象のエージェントソフトウェアなど) 。イベントデータは、Deep Security Managerのさまざまなレポートとグラフを設定するために使用します。

イベントを表示するには、Deep Security Managerの[イベントとレポート]に移動します。

Agentでのイベントログの場所

イベントログの場所はOSによって異なります。Windowsの場合は、次の場所に保存されます。

```
C:\Program Data\Trend Micro\Deep Security Agent\Diag
```

Linuxの場合は、次の場所に保存されます。

```
/var/opt/ds_agent/diag
```

注意: これらの場所には標準レベルのログのみが含まれています。診断デバッグレベルのログは別の場所にあります。パフォーマンス上の理由から、デバッグレベルのログ記録はデフォルトでは有効になっていません。トレンドマイクロのテクニカルサポートと問題を診断する場合にのみデバッグログを有効にし、完了したらデバッグログを無効にするようにしてください。詳細については、Deep Security Agent (DSA) での詳細なログ記録の有効化を参照してください。

イベントがManagerに送信されるタイミング

コンピュータで実行されるほとんどのイベントは、次のハートビート操作中にDeep Security Managerに送信されます。ただし、通信設定でRelay/Agent/ appliance が通信を開始できるようになった場合は、直ちに送信されます。

- スマートスキャンサーバがオフライン
- スマートスキャンサーバがオンライン復帰
- 変更監視検索が完了
- 変更監視のベースライン作成
- 変更監視ルール内に認識できないエレメント
- 変更監視ルールのエレメントがローカルプラットフォームでサポートされていない
- 異常な再起動の検出
- ディスク容量不足の警告
- セキュリティログ監視がオフライン
- セキュリティログ監視がオンライン復帰
- 攻撃の予兆検索の検出 (**コンピュータまたはポリシーエディタ**[1]の [ファイアウォール]→[攻撃の予兆] で、設定が有効になっている場合)

イベントが保持される期間

Deep Security Managerによって収集されたイベントは、[管理]→[システム設定]→[ストレージ] 画面で指定された期間保存されます。詳細については、"ログとイベントの保存に関するベストプラクティス" on page 1154を参照してください。

システムイベント

すべてのDeep Securityシステムイベントが表示され、の[管理]→[システム設定]→[システムイベント] [ ]タブで設定できます。個々のイベントを記録するかどうか、またSIEMシステムに転送するかどうかを設定できます。システムイベントの詳細については、"システムイベント" on page 1342を参照してください。

セキュリティイベント

各保護モジュールでは、ルールがトリガされるか、その他の設定の条件が満たされると、イベントが生成されます。セキュリティイベント生成に関する一部の設定は変更が可能です。特定の種類のセキュリティイベントに関する詳細については、次のトピックを参照してください。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- "不正プログラム対策イベント" on page 1402
- "検出した不正プログラムの確認と復元" on page 884
- "アプリケーションコントロールイベント" on page 1400
- "ファイアウォールイベント" on page 1405
- "変更監視イベント" on page 1419
- "侵入防御イベント" on page 1413
- "セキュリティログ監視イベント" on page 1421
- "Webレピュテーションイベント" on page 1423
- "デバイスコントロールイベント" on page 1404

コンピュータで有効になっているファイアウォールステートフル設定を変更して、TCP、UDP、およびICMPのイベントログを有効または無効にできます。ステートフルファイアウォール設定のプロパティを編集するには、[ポリシー]→[共通オブジェクト]→[その他]→[ファイアウォールステートフル設定] に移動します。ログのオプションは、ファイアウォールステートフル設定の [プロパティ] 画面の [TCP]、[UDP]、[ICMP] の各タブにあります。ファイアウォールイベントの詳細については、"ファイアウォールイベント" on page 1405を参照してください。

ポリシーまたはコンピュータに関連付けられたイベントを確認する

ポリシーエディタ[1]と**コンピュータエディタ**[2]は、どちらも保護モジュールに [イベント] タブがあります。ポリシーエディタには、現在のポリシーに関連付けられたイベントが表示されます。コンピュータエディタには、現在のコンピュータに固有のイベントが表示されます。

イベントの詳細を表示する

イベントの詳細を確認するには、ダブルクリックします。

[一般] タブには次の項目が表示されます。

- 時間 : Deep Security Managerをホストしているコンピュータ上のシステムクロックによる時間。
- レベル: 発生したイベントの重要度。イベントレベルには、情報、警告、エラーが含まれます。
- イベントID: イベントの種類に一意の識別子。
- イベント: イベントIDに関連付けられたイベントの名前。

---

[1] ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。

[2] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- 対象: イベントに関連付けられたシステムオブジェクトは、ここで識別されます。オブジェクトのIDをクリックすると、オブジェクトのプロパティシートが表示されます。
- イベントの起点: イベントが発生したDeep Securityコンポーネントです。
- 処理実行者: イベントをユーザが実行した場合は、そのユーザのユーザ名がここに表示されます。ユーザ名をクリックすると、[ユーザプロパティ] 画面が表示されます。
- Manager: Deep Security Managerコンピュータのホスト名。
- 説明: 必要に応じて、どのような処理が実行されてこのイベントがトリガされたのか、処理の詳細がここに表示されます。

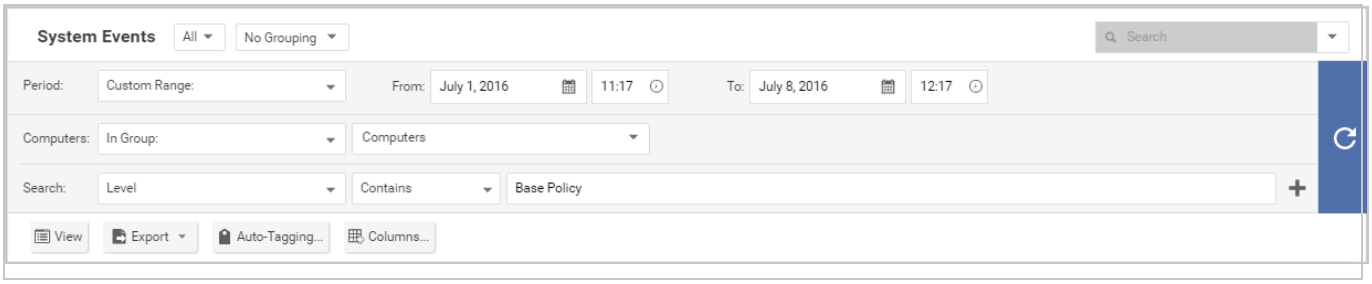
[タグ] タブには、このイベントに関連付けられているタグが表示されます。イベントのタグ付けの詳細については、[ポリシー]→[共通オブジェクト]→[その他]→[タグ]、および"イベントを識別およびグループ化するためのタグの適用" on page 1161を参照してください。

リストをフィルタしてイベントを検索する

[期間] ツールバーでリストをフィルタし、特定の期間内に発生したイベントだけを表示できます。

[コンピュータ] ツールバーで、コンピュータグループ別またはコンピュータポリシー別にイベントログエントリを表示できます。

[検索]→[詳細検索を開く] をクリックすると、詳細検索バーの表示を切り替えることができます。



検索バーの右側にある「検索バーの追加」ボタン (+) をクリックすると、追加の検索バーが表示され、検索に複数のパラメータを適用できます。準備が整ったら、送信ボタン (ツールバーの右側にある上部に右矢印の付いたボタン) をクリックします。

イベントをエクスポートする

表示されたイベントはCSVファイルにエクスポートできます(ページの指定はできません。すべてのページがエクスポートされます)。表示されたリストをエクスポートするか、または選択したアイテムをエクスポートするかを選択できます。

ログのパフォーマンスを向上する

イベント収集のパフォーマンスを最大限にするためのヒントを以下に示します。

- 重要でないコンピュータのログ収集を減らすか、無効にします。
- ファイアウォールステートフル設定の[プロパティ]画面でログオプションの一部を無効にして、ファイアウォールルール処理のログを削減することを検討します。たとえば、UDPログを無効にすると、「許可されていないUDP応答」のログエントリは除外されます。

ログとイベントの保存に関するベストプラクティス

ログおよびイベントのデータストレージのベストプラクティスは、PCIやHIPAAなど、満たす必要があるデータコンプライアンス規制に基づいています。また、データベースを最適に使用できるように考慮する必要があります。保存するデータが多すぎると、データベースのパフォーマンスやサイズの要件に影響する可能性があります。

データベースに保存するデータが多すぎると、次のような症状が発生することがあります。

- データベースの処理が実行されていない可能性を示すエラーメッセージが表示される
- ソフトウェアアップデートをインポートできない
- Deep Securityの一般な低速化

これらの症状を防ぐには、次の手順に従います。

1. 準拠する標準の要件に合わせて、保存するシステムイベントを設定します。
2. システムおよびセキュリティイベントを外部ストレージに転送します。"Deep Securityイベントを SyslogまたはSIEMサーバに転送する" on page 1171を参照してください。これにより、ローカルデータベースでのイベント保持期間を短縮できるようになります。
3. セキュリティログ監視モジュールで、イベントの保存と転送に関するしきい値を設定します。[重要度のクリッピング]を使用すると、セキュリティログ監視ルールの重要度レベルに基づいて、イベントをSyslogサーバ(有効な場合)に送信、またはイベントを保存できます。詳細については、"セキュリティログ監視イベントの転送と保存を設定する" on page 1069を参照してください。

次の表に、ローカルストレージの初期設定を示します。これらの設定を変更するには、[管理]→[システム設定]→[ストレージ]の順に選択します。ソフトウェアバージョンまたは古いルールアップデートを削除するには、[管理]→[アップデート]→[ソフトウェア]→[ローカル]または[管理]→[アップデート]→[セキュリティ]→[ルール]に移動します。

ヒント: データベースのディスク使用量を削減するには、イベントを外部Syslogサーバまたは SIEMに転送し、ローカルのイベント保持期間を短縮します。ローカルではカウンタのみを保持してください。

データタイプの設定	データ削除の初期設定
次の日数を経過した不正プログラム対策イベントを自動的に削除する	7日
次の日数を経過したWebレピュテーションイベントを自動的に削除する:	7日
次の日数を経過したファイアウォールイベントを自動的に削除する:	7日
次の日数を経過した侵入防御イベントを自動的に削除する:	7日
次の日数を経過した変更監視イベントを自動的に削除する:	7日
次の日数を経過したセキュリティログ監視イベントを自動的に削除する:	7日
次の日数を経過したアプリケーションコントロールイベントを自動的に削除する:	7日
次の日数を経過したデバイスコントロールイベントを自動的に削除する:	7日
次の期間を経過したシステムイベントを自動的に削除する:	53週間
次の期間を超過したサーバログを自動的に削除する:	7日
次の期間を経過したカウンタを自動的に削除する:	13週間
プラットフォームごとに保持しておく古いソフトウェアバージョンの数: *	5
保持しておく古いルールアップデートの数:	10

* マルチテナントが有効になっている場合、この設定は使用できません。

注意: PostgreSQLデータベースを使用している場合、古いイベントはただちに削除されない場合があります。古いイベントのデータベースパーティションはPostgreSQLメンテナンスジョブによって定期的に削除されます。削除は次の予約ジョブの実行中に行われます。

イベントは、個々のイベントのレコードです。イベントは [イベント] ページに表示されます。

*カウンタ*は、個々のイベントが発生した回数です。カウンタはダッシュボードのウィジェット(過去7日間のファイアウォールイベントの数など) およびレポートに表示されます。

*サーバのログファイル*は、Deep Security ManagerのWebサーバから取得したログファイルです。ネットワークのWebサーバにインストールされたAgentのイベントログは含まれません。

トラブルシューティング

トラブルシューティングの際にログレベルを上げてイベントをより詳細に記録すると、問題解決に役立つ場合があります。

ログレベルを上げると、ディスク使用量が大幅に増える可能性があります。トラブルシューティングが完了したら、ログレベルを再度下げてください。

1. **コンピュータまたはポリシーエディタ**[1]を開きます。
2. [設定]→[一般]→[ログレベル] の順に選択します。
3. このコンピュータに割り当てられたポリシーからログ記録のオーバーライド設定を継承する場合は [継承]、ログ記録の設定をオーバーライドしない場合は [オーバーライドしない]、トリガされたファイアウォールルールをすべて記録する場合は [完全なファイアウォールイベントのログ記録]、トリガされた侵入防御ルールをすべて記録する場合は [完全な侵入防御イベントのログ記録]、トリガされたルールをすべて記録する場合は [完全なログ記録] を選択します。
4. [保存] をクリックします。

ログファイルのサイズを制限する

個々のログファイルの最大サイズ、および保持される最新ファイルの数を指定できます。イベントログファイルは、最大許容サイズに達するまで書き込まれ、最大サイズに達すると新しいファイルが作成され、そのファイルが最大サイズに達するまで書き込まれます。最大ファイル数に達すると、最も古いファイルが削除され、その後、新しいファイルが作成されます。通常、イベントログエントリのサイズは平均約200バイトであるため、4MBのログファイルには約20,000ログエントリが保持されます。ログファイルがどのぐらいの期間でいっぱいになるかは、実行されるルールの数によって異なります。

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

1. 設定するポリシーの**コンピュータエディタまたは ポリシーエディタ**[1]を開きます。
2. [設定]→[詳細]→[イベント] の順に選択します。
3. 次のプロパティを設定します。

   - イベントログファイルの最大サイズ (Agent/Appliance): ログファイルの最大サイズです。このサイズに達すると、新しいファイルが作成されます。
   - 保管するイベントログファイル数 (Agent/Appliance):保持されるログファイルの最大数です。ログファイルの最大数に達すると、最も古いファイルが削除され、その後、新しいファイルが作成されます。
   - が次の送信元IPを持つイベントを記録しない: Deep Securityが特定の信頼するコンピュータからのトラフィックに対してレコードイベントを作成しないようにする場合に便利です。

     注意: 集約されたイベントは、次の3つの設定で調整します。ディスク容量を節約するために、Deep Security AgentおよびApplianceは同じイベントが複数発生し、それらを1つのエントリに集約し、「repeat count」、「first occurrence」のタイムスタンプ、および「last occurrence」のタイムスタンプを追加します。イベントエントリを集約するには、Deep Security AgentおよびApplianceがメモリ内のエントリをキャッシュしてディスクに書き込む必要があります。

   - キャッシュサイズ: 指定された時間にいくつのイベントの種類を追跡するか決定します。値を10に設定すると、繰り返し回数、初出現、最終出現のタイムスタンプを付けた、10種類のイベントを追跡することになります。新規のイベントの種類が発生すると、最も古い10のイベントは集約され、キャッシュから消去されてディスクに書き込まれます。
   - キャッシュの寿命: ディスクへ書き込まれる前に、どれだけの期間キャッシュに保存するかを決定します。値が10分に設定され、記録をフラッシュする状況が発生しなければ、10分を経過した記録はディスクへ書き込まれます。
   - キャッシュの有効期間: 最近更新されていない繰り返し回数のレコードをどのくらいの期間保持しておくかを決定します。キャッシュの寿命が10分で有効期間が2分の場合、更新されずに2分経過したイベントのレコードはディスクへ書き込まれ、キャッシュから消去されます。

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (または ポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (または コンピュータを選択して [詳細] をクリック) します。

> 注意: 上記の設定に関係なく、キャッシュは、イベントがDeep Security Managerに送信されるたびにフラッシュされます。

4. [保存] をクリックします。

イベントログのヒント

- 重要度が低いコンピュータのログ収集量を変更します。この設定は、**コンピュータエディタまたはポリシーエディタ**[1]の [設定]→[詳細] タブにある、[イベント] エリアおよび [ネットワークエンジンの詳細オプション] エリアで変更できます。
- [ファイアウォールステートフル設定] のログオプションを無効にして、ファイアウォールルール処理のイベントログを削減することを検討します(たとえば、UDPログを無効にすると、未承諾UDPのログエントリが除外されます)。
- 侵入防御ルールの場合、破棄されたパケットのみをログに記録することをお勧めします。パケットの変更をログに記録すると、ログエントリが多くなりすぎることがあります。
- 侵入防御ルールの場合、特定の攻撃の挙動に関する調査が必要なときのみパケットデータを含めます (侵入防御ルールの [プロパティ] 画面のオプション)。すべてのパケットデータを含めることは、ログサイズが大きくなるので推奨されません。

不正プログラム対策 検索の失敗とキャンセル

不正プログラム対策 検索は、推奨される処理が異なるいくつかの理由で失敗またはキャンセルされることがあります。

> 注意: これらのイベントは、手動検索、クイック検索、または予約検索で発生します。

不正プログラム対策 検索失敗イベント

この表は、システムイベント793、795、および1543 (不正プログラム検索失敗) の可能性のある理由を示しています。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

イベントの理由	理由 ID *	説明	推奨処理
空の設定	31	不正プログラム検索を開始できませんでした。これは、不正プログラム検索設定が空であるために発生します。	1. コンピュータまたはポリシーエディタで、[不正プログラム対策]→[一般的な]の順に選択します。 2. 不正プログラム検索の設定が[予約検索]に割り当てられていることを確認してください。 3. 検索を再実行してください。
不正プログラム対策 モジュールがオフになっています	30	不正プログラム検索を開始できませんでした。これは、不正プログラム対策モジュールの電源がオフになっているためです。	1. コンピュータまたはポリシーエディタで、[不正プログラム対策]→[一般的な]の順に選択します。 2. 不正プログラム対策の状態が「オン」または「継承 (オン)」であることを確認してください 3. 検索を再実行してください。
不正プログラム対策 サービスが停止します	7	不正プログラム対策サービスが終了中のため、不正プログラム検索に失敗しました。	1. コンピュータエディタまたはポリシーエディタで、[の概要]→[一般的な]の順に選択し、[ステータスの確認]をクリックします。 2. 不正プログラム対策ステータスが「不正プログラム対策エンジンオフライン」の場合、"エラー: 不正プログラム対策 エンジンオフライン" on page 1429の問題を解決する手順に従ってください。 3. 検索を再実行してください。
不正プログラム対策 エンジンがオフラインです	9	不正プログラム対策エンジンがオフラインであるため、不正プログラム検索に失敗しました。	1. 次の手順に従って"エラー: 不正プログラム対策 エンジンオフライン" on page 1429 問題。 2. 検索を再実行してください。
設定にアクセスできません	-2	不正プログラム検索は、不正プログラム対策の設定にアクセスできないため失敗しました。(これは予期しない内部エラーやタイミングの問題が原因である可能性があります。)	1. [コンピュータ]ページで、対象コンピュータを右クリックし、[処理]→[ポリシーの割り当て]に移動します。 2. 検索を再実行してください。
その他の検索タスクが実行中で	-16	不正プログラム検索は、別の検索タスクが進行中のため失敗しました。(これは予期しない内部エラーやタイミングの	1. [コンピュータ]ページで、別の不正プログラム検索が実行中かどうかを対

イベントの理由	理由 ID *	説明	推奨処理
す。		問題が原因である可能性があります。)	象コンピュータの[タスク]列で確認します。 2. 検出された場合は、現在の検索タスクが完了するまで待機するか、対象コンピュータを右クリックして、[処理]→[不正プログラム検索のキャンセル]の順に選択します. 3. 検索を再実行してください。
エージェントの不明な理由	10	不明な理由により、不正プログラム検索に失敗しました。	1. システムイベント情報を収集し、"診断パッケージの作成" on page 2019をログに記録します。 2. サポート担当者にお問い合わせください。

*IDは、外部のSyslog、SIEMサーバ、またはAmazon SNSに転送されるイベントに含まれます。Deep Security Managerには表示されません。

不正プログラム対策 検索キャンセルイベント

この表は、システムイベント1526、1528、および1540 (不正プログラム検索のキャンセル完了) の可能な理由を示しています。

イベントの理由	理由 ID *	説明	推奨処理
ユーザによるキャンセル	1	不正プログラム対策検索は手動でキャンセルされたか、不正プログラム対策予約検索がタイムアウト制限を超えて終了しました。	検索を再度実行してください。
サーバの再起動	32	不正プログラム対策 検索がキャンセルされました。検索対象のコンピュータがシャットダウンまたは再起動された可能性があります。	コンピュータがオンになっていることを確認し、再度検索を実行してください。
不正プログラム対策 サービスの再起動	7	不正プログラム対策 サービスが再起動されたため、不正プログラム対策 検索がキャンセルされました。	1. コンピュータまたはポリシーエディタで、[不正プログラム対策]→[一般的な]の順に選択します。 2. 不正プログラム対策の状態が「オン」または「継承 (オン)」であることを確認してください 3. 検索を再実行してください。

イベントの理由	理由ID *	説明	推奨処理
Deep Security Agentの再起動	6	エージェントが再起動しているため、不正プログラム対策 検索がキャンセルされました。不正プログラム対策 モジュールがオンラインであることを確認し、再度検索を実行してください。	1. コンピュータまたはポリシーエディタで、[不正プログラム対策]→[一般的な]の順に選択します。 2. 不正プログラム対策の状態が「オン」または「継承 (オン)」であることを確認してください 3. 検索を再実行してください。 また、エージェントのバージョンアップやポリシーの変更がないことを確認してください。これらのタスクによってエージェントが再起動される可能性があるためです。
不明な理由	-1	不明な理由により、不正プログラム検索がキャンセルされました。	1. システムイベント情報を収集し、"診断パッケージの作成" on page 2019をログに記録します。 2. サポート担当者にお問い合わせください。

*IDは、外部のSyslog、SIEMサーバ、またはAmazon SNSに転送されるイベントに含まれます。Deep Security Managerには表示されません。

イベントを識別およびグループ化するためのタグの適用

Deep Securityでは、イベントの識別およびソートに使用できるタグを作成できます。たとえば、タグを使用して、安全なイベントと調査の必要があるイベントを区別できます。また、ダッシュボードのカスタマイズやレポートの作成にも使用できます。

イベントのタグ付けはさまざまな目的に使用できますが、本来の目的はイベント管理の負担を軽減することです。あるイベントを分析して安全であると判断した場合は、コンピュータ(および構成やタスクが類似しているその他のコンピュータ) のイベントログを調べて、類似イベントを検索し、同じラベルを適用できます。こうすると、各イベントを個別に分析する必要がなくなります。

現在使用中のタグを表示するには、[ポリシー]→[共通オブジェクト]→[その他]→[タグ] の順に選択します。

タグによってイベント自体のデータが変更されることや、ユーザにイベントの削除が許可されることはありません。タグはManagerによって指定される追加属性です。

タグ付けを行うには次の方法があります。

- "手動によるタグ付け" below: 必要に応じて特定のイベントをタグ付けできます。
- "自動タグ付け" belowを使用すると、既存のイベントをモデルとして使用して、同じコンピュータまたは他のコンピュータ上の類似イベントに自動タグ付けを行うことができます。タグを適用するために、どのイベント属性がモデルイベント属性と一致する必要があるかを選択して、類似性のパラメータを定義します。
- "信頼済みのソースを使用したタグ付け" on page 1164: 信頼済みのソースの既知のイベントとの類似性に基づいて、変更監視イベントに自動でタグ付けします。

標準のタグ付けと信頼済みのソースを使用したタグ付けには重要な違いがあります。[今すぐ既存のイベントに実行] を実行できるのは、標準のタグ付けのみです。

手動によるタグ付け

1. [イベント]→[レポート]→[イベント] の順に選択し、イベントリストを選択します。イベントを右クリック(または複数のイベントを選択して右クリック) し、[タグを追加] をクリックします。
2. タグの名前を入力します。Deep Security Managerでは、入力時に既存のタグに一致する名前が表示されます。
3. [選択された[イベントの種類] イベント] を選択します。[次へ] をクリックします。
4. 必要に応じてコメントを記入し、[完了] をクリックします。

イベントリストの [タグ] 列にタグが表示されます。

自動タグ付け

Deep Security Managerを使用すると、同じタグを同じようなイベントに自動的に適用するルールを定義できます。保存済みの既存の自動タグ付けルールを表示するには、任意の [イベント] 画面で、メニューバーの [自動タグ付け] を選択します。この画面から、保存済みのルールを手動で実行できます。

1. [イベント]→[レポート]→[イベント] の順に選択し、イベントリストを選択します。ベースにするイベントを右クリックし、[タグの追加] を選択します。
2. タグの名前を入力します。Deep Security Managerでは、入力時に既存のタグに一致する名前が表示されます。
3. [選択されたものと類似の[イベントの種類] イベントに適用] を選択し、[次へ] をクリックします。
4. イベントの自動タグ付けを行うコンピュータを選択し、[次へ] をクリックします。システムイベントへのタグの適用時には、このページはスキップされます。

5. イベントの類似性を判定する基準となる属性を選択します。属性オプションは [イベント] リスト画面の列に表示される情報とほとんど同じです。イベントの選択処理に含めるための属性を選択したら、[次へ] をクリックします。
6. 次の画面で、イベントにタグを付けるタイミングを指定します。[既存の [イベントの種類] イベント] を選択した場合は、[今すぐ自動タグルールを適用する] を選択して自動タグ付けルールをすぐに適用するか、[バックグラウンドで自動タグルールを適用する] を選択し、優先度を下げてバックグラウンドで実行するかを選択できます。今後発生するイベントに自動タグ付けルールを適用するには、[今後の [イベントの種類] イベント] を選択します。また、[自動タグルールの保存] を選択して必要に応じて名前を入力することで、自動タグ付けルールを保存することもできます。[次へ] をクリックします。
7. 自動タグ付けルールの概要を確認し、[完了] をクリックします。

イベントリストで、ベースにしたイベントおよび同様のすべてのイベントにタグが付けられていることを確認できます。

イベントのタグ付けは、エージェントまたはアプライアンスからイベントがDeep Security Managerデータベースに取得された後にのみ発生します。

自動タグ付けルールに優先度を設定する

一度自動タグ付けルールが作成されると、優先度の値を割り当てることができます。自動タグ付けルールが将来のイベントに対して実行されるように設定されている場合、そのルールの優先度は、すべての自動タグ付けルールが受信イベントに適用される順序を決定します。例えば、優先度値が1のルールで、すべてのユーザサインインイベントに「疑わしい」というタグを付け、優先度値が2のルールで、ターゲット (ユーザ) があなたであるすべてのユーザサインインイベントから「疑わしい」タグを削除することができます。これにより、ユーザがあなたでないすべての将来のユーザサインインイベントに「疑わしい」タグが適用されます。

1. イベントリストで、[自動タグ付け] をクリックして、保存済みの自動タグ付けルールのリストを表示します。
2. 自動タグ付けルールを右クリックし、[詳細] をクリックします。
3. [一般] タブで、ルールの [優先度] を選択します。

セキュリティログ監視イベントを自動でタグ付けする

セキュリティログ監視イベントは、ログファイル構造内でのグループに基づいて自動でタグ付けされます。これにより、Deep Security Manager内のログ検査イベントの処理が簡単になり、自動化されます。セキュリティログ監視グループのタグを自動的に付加するには、自動タグ付けを使用します。セキュリティログ監視ルールのグループは、ルールに関連付けられています。次に例を示します。

```
<rule id="18126" level="3">
 <if_sid>18101</if_sid>
 <id>^20158</id>
```

```
<description>Remote access login success</description>
<group>authentication_success,</group>
</rule>

<rule id="18127" level="8">
<if_sid>18104</if_sid>
<id>^646|^647</id>
<description>Computer account changed/deleted</description>
<group>account_changed,</group>
</rule>
```

各グループ名には、それに関連付けられたフレンドリーネーム文字列があります。前述の例では、authentication_successはAuthentication Success、account_changedはAccount Changedとなります。これが有効になると、フレンドリーネームがそのイベントのタグとして自動的に追加されます。複数のルールがトリガーされると、複数のタグがイベントに付加されます。

信頼済みのソースを使用したタグ付け

信頼済みのソースを使用したイベントのタグ付けは、変更監視保護モジュールによって生成されたイベントにのみ使用できます。

変更監視モジュールを使用すると、コンピュータ上のシステムコンポーネントおよび関連属性の変更(作成や削除、編集を含む)をモニタできます。変更をモニタできるコンポーネントには、ファイル、ディレクトリ、グループ、インストールされたソフトウェア、リッスンポート番号、プロセス、レジストリキーなどがあります。

分析の必要があるイベントの数を削減するには、信頼済みのソースを使用したイベントのタグ付けを指定して、許可された変更に関連するイベントが自動識別されるように設定します。

変更監視モジュールでは、類似イベントの自動タグ付けだけでなく、[信頼済みのソース]で検出されたイベントやデータの類似性に基づいてイベントにタグ付けできます。信頼済みのソースには、次のいずれかが含まれます。

- 信頼済みのローカルコンピュータ
- トレンドマイクロの[ソフトウェア安全性評価サービス]
- 信頼済みの共通ベースライン。コンピュータグループから収集された、ファイルのステータスのセットです。

信頼済みのローカルコンピュータ

信頼されたコンピュータとは、無害なイベントのみを生成することができるモデルコンピュータとして使用されるコンピュータです。ターゲットコンピュータとは、不正または予期しない変更を監視しているコンピュータです。自動タグ付けルールは、ターゲットコンピュータ上のイベントを調査し、それらを信頼されたコンピュータのイベントと比較します。もし一致するイベントがあれば、それらは自動タグ付けルールで定義されたタグでタグ付けされます。

保護対象コンピュータのイベントと信頼済みコンピュータのイベントを比較する自動タグルールを設定できます。たとえば、計画されたパッチのロールアウトを信頼済みコンピュータに適用できます。パッチの適用に関連するイベントには、Patch Xのタグを付けることができます。他のシステムで発生した同様のイベントは、自動的にタグ付けされ、許容可能な変更として識別され、フィルタで除外されるため、評価が必要なイベントの数を減らすことができます。

イベントマッチングアルゴリズム

変更監視イベントには、状態の変化に関する情報が含まれています。つまり、イベントにはイベント前およびイベント後の情報が含まれています。イベントを比較すると、自動タグ付けエンジンによってイベント前後の状態が比較されます、2つのイベントでイベント前後の状態が同じ場合、これらのイベントは一致すると判定され、2番目のイベントにタグが適用されます。これは作成および削除イベントにも当てはまります。

信頼済みのソースを使用したイベントのタグ付けに、信頼済みのコンピュータを使用している場合は、変更監視ルールによって生成されたイベントにタグが付けられます。つまり、変更監視ルールを使用して対象コンピュータでイベントを生成している場合は、この変更監視ルールを信頼済みソースのコンピュータでも実行する必要があります。

信頼済みのソースを使用したイベントのタグ付けを適用する前に、信頼済みのソースのコンピュータで不正プログラムを検索する必要があります。

Linuxのprelinkingのような、システムのファイルの中身を定期的に変更するユーティリティは、信頼済みのソースを使用したイベントのタグ付けと干渉することがあります。

信頼済みのローカルコンピュータに基づいてイベントにタグを付ける

1. 信頼済みのコンピュータで不正プログラム対策のフルスキャンを実行し、不正プログラムがないことを確認します。
2. イベントを自動的にタグ付けするコンピュータで、信頼済みソースのコンピュータと同じ(または部分的に同じ)変更監視ルールを実行していることを確認します。
3. Deep Security Managerで、[イベントとレポート]→[変更監視イベント]を選択し、ツールバーの[自動タグ設定]をクリックします。

4. [自動タグルール(変更監視イベント)] 画面で [新しい信頼済みのソース] をクリックし、タグウィザードを表示します。
5. [信頼済みのローカルコンピュータ] を選択して [次へ] をクリックします。
6. リストから信頼済みのソースとして使用するコンピュータを選択し、[次へ] をクリックします。
7. 信頼済みソースコンピュータのイベントに一致した対象コンピュータのイベントに割り当てるタグを、1つ以上指定します。[次へ] をクリックします。

   注意: 新しいタグをテキストで入力するか、既存のタグのリストから選択します。

8. 信頼済みソースとイベントを照合する対象コンピュータを指定します。[次へ] をクリックします。
9. オプションで、ルールの名前を指定し、[完了] をクリックします。

トレンドマイクロのソフトウェア安全性評価サービスに基づいてイベントにタグを付ける

Certified Safe Software Serviceは、トレンドマイクロが管理している既知の正常なファイルの署名の許可リストです。このタイプの信頼済みソースのタグ付けでは、対象コンピュータにファイル関連の変更監視イベントが発生していないかが監視されます。イベントが記録された場合は、変更後のファイルの署名が、信頼できる既知のトレンドマイクロのファイル署名リストと比較されます。一致が見つかると、イベントにタグが付けられます。

1. Deep Security Managerで、[イベントとレポート]→[変更監視イベント]を選択し、ツールバーの[自動タグ設定]をクリックします。
2. [自動タグルール(変更監視イベント)] 画面で [新しい信頼済みのソース] をクリックし、タグウィザードを表示します。
3. ソフトウェア安全性評価サービスを選択して [次へ] をクリックします。
4. ソフトウェア安全性評価サービスに一致した場合に対象コンピュータのイベントに割り当てるタグを、1つ以上指定します。[次へ] をクリックします。
5. ソフトウェア安全性評価サービスとイベントを照合する対象コンピュータを指定します。[次へ] をクリックします。
6. オプションで、ルールの名前を指定し、[完了] をクリックします。

信頼済みの共通ベースラインに基づいてイベントにタグを付ける

信頼済みの共通ベースライン方式では、コンピュータグループ内でイベントを比較します。コンピュータグループが特定されると、グループ内のコンピュータで有効になっている変更監視ルールの監視対象のファイルおよびシステムのステータスに基づいて、共通ベースラインが生成されます。グループ内のあるコンピュータで変更監視イベントが発生した場合、変更後の署名が共通ベースラインと比較されます。ファイルの新しい署名と一致するものが共通ベースライン内にある場合、イベントにタグが付加されます。信頼済みのコンピュータ方式では変更監視イベントの前と後のステータスが比較されますが、信頼済みの共通ベースラインでは、イベント後のステータスだけが比較されます。

この方法では、共通グループ内のすべてのコンピュータが、保護されていて不正プログラムがないことを前提とします。共通ベースラインが生成される前に、グループ内のすべてのコンピュータで不正プログラム対策のフルスキャンを実行してください。

コンピュータの変更監視ベースラインが生成されると、Deep Securityは最初にそのコンピュータが信頼された共通ベースライングループの一部であるかどうかを確認します。もしそうであれば、そのコンピュータのベースラインデータはそのグループの信頼された共通ベースラインに含まれます。このため、信頼された共通ベースラインの自動タグ付けルールは、共通ベースライングループ内のコンピュータに変更監視ルールが適用される前に設定されている必要があります。

1. 信頼済みの共通ベースラインを構成するコンピュータグループに追加するすべてのコンピュータで、不正プログラム対策のフルスキャンを実行し、不正プログラムがないことを確認します。
2. Deep Security Managerで、[イベントとレポート]→[変更監視イベント]を選択し、ツールバーの[自動タグ設定]をクリックします。
3. [自動タグルール(変更監視イベント)]画面で[新しい信頼済みのソース]をクリックし、タグウィザードを表示します。
4. [信頼済みの共通ベースライン]を選択して[次へ]をクリックします。
5. 信頼済みの共通ベースラインに一致した場合にイベントに割り当てるタグを1つ以上指定します。[次へ]をクリックします。
6. 信頼済みの共通ベースラインの生成に使用するグループに含めるコンピュータを特定します。[次へ]をクリックします。
7. オプションで、ルールの名前を指定し、[完了]をクリックします。

注意:大量のベースラインデータに関連するパフォーマンスの問題により、最新バージョンのDeep Security Managerでは、ベースラインの表示がUIに表示されません。詳細については、大量の変更監視ベースラインデータによるデータベースのパフォーマンス問題をご覧ください。

タグを削除する

1. イベントリストで、削除したいタグが付いたイベントを右クリックし、タグを削除を選択します。
2. 選択した[イベントタイプ]イベントまたは選択した類似の[イベントタイプ]イベントに適用から削除したいタグを選択し、次へをクリックしてください。
3. 必要に応じてコメントを追加し、完了をクリックします。

ログに記録するイベントの数を減らす

ログに記録されるイベントの数を減らすために、Deep Security Managerはいくつかの Advanced Logging Policy モードのいずれかで動作するように設定できます。これらのモードは、**コンピュータまたは**

ポリシーエディタ[1]の [設定]→[詳細]→[ネットワークエンジンの詳細設定] エリアで設定できます。

次の表に、詳細なログ記録ポリシーモードのより複雑な4つについて、どのイベントのタイプが無視されるかを示します。

モード	無視するイベント
ステートフルおよび正規化の抑制	セッション情報なし 不正なフラグ 不正なシーケンス 不正なACK 許可されていないUDP応答 許可されていないICMP応答 ポリシーで未許可 再送の破棄
ステートフル、正規化、およびフラグメントの抑制	セッション情報なし 不正なフラグ 不正なシーケンス 不正なACK 許可されていないUDP応答 許可されていないICMP応答 ポリシーで未許可 CEフラグ 不正なIP 不正なIPデータグラム長 フラグメント化 不正なフラグメントオフセット 最初のフラグメントが最小サイズ未満 範囲外のフラグメント 最小オフセット値以下のフラグメント IPv6パケット 受信接続の上限 送信接続の上限 SYN送信の上限 ライセンスの期限切れ 不明なIPバージョン 不正なパケット情報 ACK再送の上限 切断された接続上のパケット 再送の破棄
ステートフル、フラグメント、および検証機能の抑制	セッション情報なし 不正なフラグ 不正なシーケンス

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

モード	無視するイベント
	不正なACK 許可されていないUDP応答 許可されていないICMP応答 ポリシーで未許可 CEフラグ 不正なIP 不正なIPデータグラム長 フラグメント化 不正なフラグメントオフセット 最初のフラグメントが最小サイズ未満 範囲外のフラグメント 最小オフセット値以下のフラグメント IPv6パケット 受信接続の上限 送信接続の上限 SYN送信の上限 ライセンスの期限切れ 不明なIPバージョン 不正なパケット情報 不正なデータオフセット IPヘッダなし 読み取り不能なイーサネットヘッダ 未定義 送信元および送信先IPが同一 不正なTCPヘッダ長 読み取り不能なプロトコルヘッダ 読み取り不能なIPv4ヘッダ 不明なIPバージョン ACK再送の上限 切断された接続上のパケット 再送の破棄
タップモード	セッション情報なし 不正なフラグ 不正なシーケンス 不正なACK ACK再送の上限 切断された接続上のパケット 再送の破棄

イベントのランク付けによる重要度の数値化

ランク付けシステムでは、イベントの重要度を数値化できます。コンピュータに「資産評価」を割り当て、ルールに重要度またはリスクの値を割り当て、これら2つの値を掛け合わせることによって、イベントの重要度 (ランク) が計算されます。これによって、イベントをランクでソートできます。

注意: 不正プログラム対策 では、他のモジュールと異なり、イベントの重要度をランク付けするために資産価値は使用されません。

Webレピュテーション イベントリスク値

Webレピュテーション イベントのリスク値は、Webレピュテーション ページの[General]タブの Webレピュテーション設定で使用される3つのレベルのリスクにリンクされています。

- 危険:「不正、または脅威の既知の発信源であると確認されたURL」に相当
- 非常に不審:「不正または脅威の発信源である可能性が疑われたURL」に相当
- 不審:「スパムメールに関連付けられている、または感染している可能性のあるURL」に相当
- 管理者によるブロック: Webレピュテーションサービスのブロックリストに含まれているURL
- 未評価: リスクレベルが設定されていないURL

ファイアウォールルールの重要度の値

ファイアウォール ルールの重大度の値は、拒否、ログのみ、およびパケット拒否の各処理にリンクされます。(後者は、ファイアウォール ステートフル設定のために拒否されたパケットを参照します。.)このパネルを使用して、コンピュータの資産価値に乗算される重大度値を編集し、ファイアウォール イベントの順位を決定します。(A ファイアウォール ルールの処理は、ルールの プロパティウィンドウ.)で表示および編集できます。

侵入防御 ルールの重要度の値

侵入防御 のルールの重要度の値は、重大度レベル(重大、高、中、低、またはエラー) にリンクされています。このパネルを使用して値を編集します。この値にコンピュータの資産価値を乗算し、侵入防御 イベントの順位を決定します。侵入防御 ルールの重大度設定は、ルールの[プロパティ] [ ]画面で確認できます。

変更監視 ルールの重大度の値

変更監視 のルールの重要度の値は、重要度レベル(重大、高、中、または低) にリンクされます。このパネルを使用して値を編集します。値には、変更監視 イベントのランクを決定するためにコンピュータの資産価値を乗算します。変更監視 ルールの重大度は、ルールの[プロパティ] [ ]画面で確認できます。

セキュリティログ監視 ルール重大度の値

セキュリティログ監視 のルールの重要度の値は、重要度レベル(重大、高、中、低) にリンクされます。セキュリティログ監視 イベントのランクを決定するためにコンピュータの資産価値で乗算される値を編集するには、このパネルを使用します。セキュリティログ監視 ルールの重大度レベルは、ルールの[プロパティ] [ ]画面で表示および編集できます。

資産評価

アセット値は、侵入防御 ルールや ファイアウォール ルールなど、他のプロパティと関連付けられていません。資産評価は、それ自体がプロパティです。コンピュータの資産評価は、コンピュータの [詳細] 画面から表示および編集できます。資産評価の割り当て処理を簡略化するために、コンピュータの最初の [詳細] 画面の [資産の重要度] リストに表示される値の一部を事前定義できます。既存の事前定義されたコンピュータの資産評価を表示するには、このパネルの [資産評価の表示] ボタンをクリックします。[資産評価] 画面に、事前定義された設定が表示されます。これらの値は変更可能で、新しい値を作成できます(新しい設定は、すべてのコンピュータのリストに表示されます)。

イベントをSyslogサーバまたはSIEMサーバに転送する

Deep SecurityイベントをSyslogまたはSIEMサーバに転送する

イベントは、外部のSyslogサーバまたはSecurity Information and Event Management(SIEM) サーバに送信できます。これは、集中管理された監視、カスタムレポート、またはDeep Security Managerのローカルディスクの空き容量の確保に役立ちます。

外部サーバーへのイベント転送を有効にしても、Deep Security Manager はシステムおよびセキュリティイベントをローカルに記録し、レポートやグラフに表示します。したがって、ディスクスペースの使用量を減らす必要がある場合、イベント転送だけでは不十分です。ローカルにイベントを保持する期間も設定する必要があります。

または、イベントをAmazon SNSに公開する場合は、"Amazon Simple Notification Serviceをセットアップする" on page 1238でのイベントのアクセスを参照してください。

基本的な手順には、以下が含まれます

1. "イベント転送 ネットワークトラフィックを許可する" on the next page
2. "クライアント証明書を要求する" on the next page
3. "Syslog設定の定義" on the next page

4. "システムイベントを転送する" on page 1175 and/or "セキュリティイベントを転送する" on page 1175

イベント転送ネットワークトラフィックを許可する

すべてのルータ、ファイアウォール、およびセキュリティグループでは、Deep Security Managerからの受信トラフィック(およびセキュリティイベントの直接転送のために、エージェントからの受信トラフィック) をSyslogサーバに送信する必要があります。"ポート番号、URL、およびIPアドレス" on page 428も参照してください。

クライアント証明書を要求する

イベントを安全に転送したい場合(TLS経由) 、およびSyslogサーバーがクライアント認証を要求する場合は、*クライアント*(サーバーではなく) 証明書署名要求(CSR) を生成する必要があります。Deep Security Managerは、この証明書を使用して、Syslogサーバーにクライアントとして接続する際に自身を識別および認証します。クライアント証明書の要求方法については、証明書発行機関(CA) にお問い合わせください。

一部のSyslogサーバーは自己署名のサーバー証明書(Deep Security Managerのデフォルトなど) を受け入れません。CA署名のクライアント証明書が必要です。

Syslogサーバーが信頼するCA、または信頼されたルートCAによって直接または間接的に署名された中間CAを使用します(これは信頼チェーンまたは署名チェーンとも呼ばれます) 。

CAから署名された証明書を受信すると、CA証明書をDeep Security Managerにアップロードするために、"Syslog設定の定義" belowを続行します。

Syslog設定の定義

Syslog設定では、システムイベントまたはセキュリティイベントの転送時に使用できる宛先と設定を定義します。

2017年1月26日より前にSIEMまたはSyslogを設定した場合、Syslog設定に変換されています。同じ設定がマージされました。

1. [Policies]→[Common Objects]→[Other]→[Syslog Configurations]→[]の順に選択します。
2. [新規]→[新規設定] の順にクリックします。
3. 一般タブで、次の設定を行います:
   - 名前: 設定を識別する一意の名前。
   - 説明: 設定の説明 (オプション)。

- ログのソースID：Deep Security Managerのホスト名の代わりに使用するオプションの識別子。

  Deep Security Managerがマルチノードの場合、各サーバノードのホスト名はそれぞれ異なります。したがって、ログソースIDは異なる場合があります。IDがホスト名に関係なく同じである必要がある場合 (たとえば、フィルタ目的の), では、ここで共有ログソースIDを設定できます。

  この設定は、Deep Security Agentによって直接送信されるイベントには適用されません。このイベントは、ログオン元IDとして常にホスト名が使用されます。

- サーバ名：受信SyslogサーバまたはSIEMサーバのホスト名またはIPアドレス。

- サーバーポート: SIEM または Syslog サーバーのリスニングポート番号。UDP の場合、IANA 標準ポート番号は 514 です。TLS の場合、通常はポート6514 です。"ポート番号、URL、およびIPアドレス" on page 428も参照してください。

- トランスポート: トランスポートプロトコルが安全である(TLS) かどうか(UDP)。

  UDPの場合、Syslogメッセージは64 KBに制限されます。長いメッセージの場合は、データが切り捨てられることがあります。

  TLSの場合、マネージャとSyslogサーバはお互いの証明書を信頼する必要があります。ManagerからSyslogサーバへの接続は、TLS 1.2,1.1、または1.0で暗号化されます。

  TLSを設定するには、[エージェントが次のログを転送する]を設定する必要があります。Via the Deep Security Manager (間接的に) 。エージェントはTLSでの転送をサポートしていません。

- イベントの形式：ログメッセージの形式がLEEF、CEF、またはBasic Syslogのいずれであるか。"syslog メッセージの形式" on page 1177

  LEE形式では、[エージェントは次のログを次のユーザに転送する]を設定する必要があります。Deep Security Managerを介して(間接的に) 。

  基本的なSyslog形式は、Deep Security 不正プログラム対策, Webレピュテーション, 変更監視、および アプリケーションコントロールではサポートされていません。

- イベントにタイムゾーンを含めます。イベントに完全な日付(年と時間帯を含む) を追加するかどうかを指定します。

例 (選択された): 2018-09-14T01:02:17.123+04:00。

例 (選択解除された): Sep 14 01:02:17。

完全な日付を設定するには、[クライアントにログを転送する]を設定する必要があります。Deep Security Managerを介して(間接的に)。

- ファシリティ: イベントが関連付けられるプロセスの種類。Syslogサーバーはログメッセージのファシリティフィールドに基づいて優先順位を付けたりフィルタリングしたりすることがあります。Syslogのファシリティとレベルとは？ も参照してください

- エージェントはログを転送する必要があります: イベントをSyslogサーバに直接送信するか、またはDeep Security Managerを介して(間接的に)。

  ログをSyslogサーバに直接転送する場合、クライアントはクリアテキストUDPを使用します。ログには、セキュリティシステムに関する機密情報が含まれています。インターネットなどの信頼されていないネットワークを介してログを送信する場合は、VPNトンネルなどを追加して偵察や改ざんを防止することを検討してください。

  マネージャー経由でログを転送する場合、Deep Security Managerを設定して含めるようにしない限り、ファイアウォールおよび侵入防御パケットデータは含まれません。手順については、Deep Security Manager (DSM) 経由でパケットデータをsyslogに送信するを参照してください。

4. Syslog または SIEM サーバーが TLS クライアントにクライアント認証(クライアント認証または相互認証とも呼ばれます。"クライアント証明書を要求する" on page 1172を参照) を要求する場合、認証情報 タブで次の設定を行います

   - 秘密鍵: Deep Security Managerのクライアント証明書の秘密鍵を貼り付けます。
   - 証明書: Deep Security ManagerがSyslogサーバへのTLS接続で自身を識別するために使用するクライアントの証明書を貼り付けます。Base64エンコード形式とも呼ばれるPEMを使用します。
   - 証明書チェーン: 中間CAがクライアント証明書に署名したが、SyslogサーバがそのCAを認識して信頼しない場合は、CA証明書を貼り付けて証明書を信頼するルートCAに関連付けます。各CA証明書の間にEnterキーを押します。
5. [Apply] をクリックします。
6. TLS転送メカニズムを選択した場合は、Deep Security ManagerとSyslogサーバの両方が互いの証明書に接続して信頼できることを確認します。

a. [接続テスト] をクリックします。

Deep Security Managerは、ホスト名の解決と接続を試行します。失敗した場合は、エラーメッセージが表示されます。

Deep Security ManagerによってSyslogサーバ証明書またはSIEMサーバ証明書がまだ信頼されていない場合、接続は失敗し、サーバ証明書を受け入れますか? メッセージが表示されます。このメッセージには、Syslogサーバの証明書の内容が表示されます。

b. Syslogサーバの証明書が正しいことを確認してから、[OK]をクリックして認証を受け入れます。

証明書は、の[Administration]→[System Settings]→[Security]で、管理者の信頼された証明書のリストに追加されます。Deep Security Managerでは、自己署名証明書を使用できます。

c. [接続のテスト] [ ]をもう一度クリックします。

今すぐTLS接続が成功する必要があります。

7. イベントを転送するには、選択を続けてください。"システムイベントを転送する" belowおよび/または"セキュリティイベントを転送する" belowを参照してください。

システムイベントを転送する

Deep Security Manager は、管理者のログインやエージェントソフトウェアのアップグレードなどのシステムイベントを生成します。

1. [管理]→[システム設定]→[イベントの転送] に進みます。
2. 設定を使用してリモートコンピュータにシステムイベントを転送する(Syslog経由) から、既存の設定を選択するか、新規 をクリックします。詳細については、"Syslog設定の定義" on page 1172を参照してください。
3. [保存] をクリックします。

Deep Security Managerがマルチノードである場合、システムイベントは1つのノードからのみ送信され、重複が回避されます。

セキュリティイベントを転送する

Deep Security Agent保護機能は、セキュリティイベント(不正プログラムの検出やIPSルールのトリガーなど) を生成します。イベントを次のいずれかに転送できます:

- 直接
- 間接的に、Deep Security Manager経由で

一部のイベント転送オプション では、Deep Security Manager経由で間接的にエージェントイベントを転送する必要があります。

他のポリシー設定と同様、イベント転送の設定も特定のポリシーまたはコンピュータに対してオーバーライドすることができます。"ポリシー、継承、およびオーバーライド" on page 724を参照してください。

1. [ポリシー] に移動します。
2. コンピュータで使用されているポリシーをダブルクリックします。
3. [設定] を選択します。
4. [イベント転送] タブを選択します。
5. イベント送信間隔から、イベント転送の頻度を選択します。
6. 不正プログラム対策 Syslog 設定および他の保護モジュールのコンテキストメニューから、使用するSyslog 設定を選択するか、編集をクリックして変更し、なしを選択して無効にするか、新規をクリックします。詳細については、"Syslog設定の定義" on page 1172を参照してください。
7. [保存] をクリックします。

イベント転送のトラブルシューティング

Syslogメッセージ送信失敗アラート

Syslog設定に問題がある場合は、次のアラートが表示されることがあります。

```
Failed to Send Syslog Message
The Deep Security Manager was unable to forward messages to a Syslog Server.
Unable to forward messages to a Syslog Server
```

アラートには、影響を受けたSyslog設定へのリンクも含まれています。リンクをクリックして設定を開き、[Test Connection]をクリックして詳細な診断情報を取得します。接続が成功したことを示すか、原因に関する詳細が記載されたエラーメッセージが表示されます。

Syslog設定を編集できません

Syslog設定は表示されますが編集できない場合、アカウントに関連付けられている役割に適切な権限がない可能性があります。役割を設定できる管理者は、[管理]→[ユーザ管理]の順に選択して権限を確認できます。ユーザ名を選択して[プロパティ] をクリックします。[その他の権利] [ ]タブで、Syslog Configurations 設定でSyslog設定の編集権限が制御されます。ユーザと役割の詳細については、"ユーザの追加と管理" on page 1537を参照してください。

Deep Security ManagerのSyslog設定セクションが表示されません。

Deep Security ManagerでSyslog設定の画面が表示されない場合は、マルチテナント環境のテナントで、プライマリテナントによってこの機能が無効化または設定されていることが考えられます。

証明書が期限切れのためにSyslogが転送されない

有効な証明書は、TLS経由で安全に接続するために必要です。TLSクライアント認証を設定しても証明書の有効期限が切れた場合、メッセージはSyslogサーバに送信されません。この問題を修正するには、新しい証明書を取得し、Syslog設定を新しい証明書の値でアップデートし、接続をテストしてから設定を保存します。

サーバ証明書が期限切れであるか変更されたためにSyslogが配信されない

有効な証明書は、TLS経由で安全に接続するために必要です。Syslogサーバの証明書が期限切れまたは変更されている場合は、Syslog設定を開き、[接続テストのテスト]をクリックします。新しい証明書を受け入れるように求められます。

互換性

Deep Securityは、次の製品のenterpriseバージョンでテストされています

- IBM QRadar 7.2.8 Patch 3 (TLSプロトコルパッチのPROTOCOL-TLSSyslog-7.2-20170104125004.noarchを適用)
- HP ArcSight 7.2.2 (ArcSight-7.2.2.7742.0-Connectorツールを使用して作成されたTLS Syslog-NGコネクタを使用)

他の標準のSyslogソフトウェアも動作する可能性がありますが、検証されていません。

syslogメッセージの形式

Common Event Format (CEF) とLog Event Extended Format (LEEF) のログメッセージ形式は少し異なります。例えば、UIのSource User列は、CEFではsuserというフィールドに対応しますが、LEEFでは同じフィールドがusrNameと呼ばれます。ログメッセージフィールドは、イベントがDeep Securityエージェントまたは Deep Security Managerのどちらで発生したか、およびどの機能がログメッセージを作成したかによっても異なります。

注意: syslogメッセージが切り捨てられている場合、ユーザデータグラムプロトコル (UDP) を使用していることが原因かもしれません。切り捨てを防ぐには、syslogメッセージをトランスポート層セキュリティ (TLS) 経由で転送してください。TLSへの切り替え手順については、"Syslog設定の定義" on page 1172を参照してください。

不正プログラム対策, Webレピュテーション, 変更監視、および アプリケーションコントロール 保護モジュールでは、基本的なSyslog形式はサポートされていません。

マネージャからsyslogメッセージが送信される場合、いくつかの違いがあります。元のDeep Securityエージェントのホスト名 (イベントの発生元) を保持するために、新しい拡張子 (dvcまたはdvchost) が存在します。ホスト名がIPv4アドレスの場合はdvcが使用され、ホスト名およびIPv6アドレスの場合はdvchostが使用されます。さらに、イベントがタグ付けされている場合は拡張子TrendMicroDsTagsが使用されます。これは、イベントがマネージャによって収集されるときにのみsyslog経由で転送されるため、将来の自動タグ付けにのみ適用されます。マネージャを介して中継されたログの製品名は引き続き「Deep Securityエージェント」と表示されますが、製品バージョンはマネージャのバージョンです。

CEFのsyslogメッセージの形式

すべてのCEFイベントには、イベントの元のDeep Securityエージェントのソースを特定する目的で、dvc=IPv4 Addressまたはdvchost=Hostname(またはIPv6アドレス) が含まれます。この拡張は、Deep Security Virtual Applianceまたはマネージャから送信されたイベントにとって重要です。この場合、メッセージのsyslog送信者はイベントの発信者ではありません。

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

Deep Security ManagerとDeep Security Agentのどちらからのログエントリかを判断するには、デバイス製品 (Device Product) フィールドを確認します。

CEFログエントリのサンプル: Jan 18 11:07:53 dsmhost CEF:0|Trend Micro|Deep Security Manager|<DSM version>|600|Administrator Signed In|4|suser=Master...

> 注意: Virtual Applianceで保護されていて、Agentで保護されていない仮想マシンで発生したイベントも、Agentからのイベントとして識別されます。

イベントをトリガしたルールの種類を判断するには、署名ID (Signature ID) フィールドと名前 (Name) フィールドを確認します。

ログエントリのサンプル: Mar 19 15:19:15 root CEF:0|Trend Micro|Deep Security Agent|<DSA version>|123|Out Of Allowed Policy|5|cn1=1...

署名ID (Signature ID) の値は、トリガされたイベントの種類を示します。

署名ID	説明
10	カスタム侵入防御 (IPS) ルール
20	ログのみのファイアウォールルール
21	ファイアウォールルールの拒否
30	カスタム変更監視ルール
40	カスタムセキュリティログ監視ルール

署名ID	説明
100-7499	システムイベント
100-199	ポリシー ファイアウォール ルールとファイアウォール ステートフル設定
200-299	IPSの内部エラー
300-399	SSL/TLSイベント
500-899	IPSの正規化
1,000,000-1,999,999	トレンドマイクロのIPSルール。署名IDは、IPSルールIDと同一です。
2,000,000-2,999,999	変更監視 ルール。署名IDは、変更監視 ルールID + 1,000,000です。
3,000,000-3,999,999	セキュリティログ監視 ルール。署名IDは、セキュリティログ監視 ルールID + 2,000,000です。
4,000,000-4,999,999	不正プログラム対策 イベント。現在は、以下の署名IDのみが使用されています。 • 4,000,000 - 不正プログラム対策 - リアルタイム検索 • 4,000,001 - 不正プログラム対策 - 手動検索 • 4,000,002 - 不正プログラム対策 - 予約検索 • 4,000,003 - 不正プログラム対策 - クイック検索 • 4,000,010 - スパイウェア対策 - リアルタイム検索 • 4,000,011 - スパイウェア対策 - 手動検索 • 4,000,012 - スパイウェア対策 - 予約検索 • 4,000,013 - スパイウェア対策 - クイック検索 • 4,000,020 - 不審アクティビティ- リアルタイム検索 • 4,000,030 - 不正変更 - リアルタイム検索
5,000,000-5,999,999	Webレピュテーション イベント。現在は、以下の署名IDのみが使用されています。 • 5,000,000 - Webレピュテーション - ブロック済み • 5,000,001 - Webレピュテーション - 検出のみ
6,000,000-6,999,999	アプリケーションコントロール イベント。現在は、以下の署名IDのみが使用されています。 • 6,001,100 - アプリケーションコントロール - ブロックリスト内の検出のみ • 6,001,200 - アプリケーションコントロール - 検出のみ、未許可のリスト • 6,002,100 - アプリケーションコントロール - ブロックリスト(ブロックリスト内) • 6,002,200 - アプリケーションコントロール -許可リストに含まれていないブロック
7,000,000 ~ 7,999,999	デバイスコントロールイベント。現在、次のシグネチャIDのみが使用されていま

署名ID	説明
	す。 • 7,000,000 -デバイスコントロール- 不明なデバイスへのアクセスがブロックされました • 7,000,200 -デバイスコントロール- 不明なデバイスへの書き込みがブロックされました • 7,001,000 -デバイスコントロール- USBデバイスへのアクセスがブロックされました • 7,001,200 -デバイスコントロール- USBデバイスの書き込みがブロックされました • 7,002,000 -デバイスコントロール- モバイルデバイスへのアクセスがブロックされました • 7,002,200 -デバイスコントロール- モバイルデバイスの書き込みがブロックされました

次のイベントログの形式の表に示すすべてのCEF拡張が必ずしも各ログエントリに含まれているわけではありません。また、CEF拡張の順序が常に同じであるとは限りません。正規表現を使用してエントリを解析する場合は、表にある各キーと値のペアがあることを前提としたり、またはその順序に依存したりしないようにしてください。{: .note }

Syslogメッセージは、Syslogプロトコル仕様によって最大64KBに制限されています。長いメッセージの場合は、データが切り捨てられることがあります。Basic Syslog形式は、最大1KBに制限されています。

LEEF 2.0のsyslogメッセージの形式

LEEF 2.0の基本形式: LEEF:2.0|ベンダ(Vendor)|製品 (Product)|バージョン(Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEF 2.0ログエントリのサンプル (DSMシステムイベントログのサンプル): LEEF:2.0|Trend Micro|Deep Security Manager|<DSA version>|192|cat=System name=Alert Ended desc=Alert: CPU Warning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity: Warning sev=3 src=10.201.114.164 usrName=System msg=Alert: CPUWarning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity:Warning TrendMicroDsTenant=Primary

マネージャーから発信されたイベント

システムイベントログの形式

CEFの基本形式: CEF:バージョン(Version)|デバイスベンダ(Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン(Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF:0|Trend Micro|Deep Security Manager|<DSM version>|600|User Signed In|3|src=10.52.116.160 suser=admin target=admin msg=User signed in from 2001:db8::5

LEEF 2.0の基本形式: LEEF:2.0|ベンダ(Vendor)|製品 (Product)|バージョン(Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEF 2.0ログエントリのサンプル: LEEF:2.0|Trend Micro|Deep Security Manager|<DSA version>|192|cat=System name=Alert Ended desc=Alert: CPU Warning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity: Warning sev=3 src=10.201.114.164 usrName=System msg=Alert: CPU Warning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity: Warning TrendMicroDsTenant=Primary

LEEF形式では、重要度を示すsevという予約キーと、名前を示すnameという予約キーが使用されます。

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
src	src	Source IP Address	Deep Security ManagerのIPアドレス。	src=10.52.116.23
suser	usrName	Source User	Deep Security Manager管理者のアカウント。	suser=MasterAdmin
target	target	Target Entity	イベントの件名。Deep Security Managerにログインしている管理者アカウ	target=MasterAdmin target=server01

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			ント、またはコンピュータを指定できます。	
targetID	targetID	Target Entity ID	Managerで追加された識別子。	targetID=1
targetType	targetType	Target Entity Type	イベントの対象のエンティティの種類。	targetType=Host
msg	msg	Details	システムイベントの詳細。イベントの詳細な説明が含まれる場合があります。	msg=User password incorrect for username MasterAdmin on an attempt to sign in from 127.0.0.1 msg=A Scan for Recommendations on computer (localhost) has completed...
TrendMicroDsTags	TrendMicroDsTags	Event Tags	Deep Securityイベントタグがイベントに割り当てられている	TrendMicroDsTags=suspicious
TrendMicroDsTenant	TrendMicroDsTenant	Tenant Name	Deep Securityテナント	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityテナントID	TrendMicroDsTenantId=0
TrendMicroDsReasonId	TrendMicroDsReasonId	イベント理由ID	イベントの説明の理由IDを示します。各イベントには独	TrendMicroDsReasonId = 1

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			自の理由ID定義があります。	
None	sev	Severity	イベントの重要度。重要度は1が最も低く、10が最も高くなります。	sev=3
None	cat	Category	イベントのカテゴリ	cat=System
None	name	名前	イベント名	name=Alert Ended
None	desc	説明	イベントの説明	desc:Alert: CPUの警告しきい値の超過

Agentで発生するイベント

不正プログラム対策 イベントフォーマット

CEFの基本形式: CEF:バージョン(Version)|デバイスベンダ(Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン(Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

サンプルCEFログエントリ: CEF:0|Trend Micro|Deep Security Agent|<DSA version>|4000000|Eicar_test_file|6|cn1=1 cn1Label=Host ID dvchost=hostname cn2=205 cn2Label=Quarantine File Size cs6=ContainerImageName | ContainerName | ContainerID cs6Label=Container filePath=C:\\Users\\trend\\Desktop\\eicar.exe act=Delete result=Delete msg=Realtime TrendMicroDsMalwareTarget=N/A TrendMicroDsMalwareTargetType=N/TrendMicroDsFileMD5=44D88612FEA8A8F36DE82E1278ABB02F TrendMicroDsFileSHA1=3395856CE81F2B7382DEE72602F798B642F14140 TrendMicroDsFileSHA256=275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F TrendMicroDsDetectionConfidence=95 TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_CERBER.C;Ransom_CRYPNISCA.SM

LEEF 2.0の基本形式: LEEF:2.0|ベンダ(Vendor)|製品 (Product)|バージョン(Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEFログエントリのサンプル: LEEF: 2.0|Trend Micro|Deep Security Agent|<DSA version>|4000030|cat=Anti-Malware name=HEU_AEGIS_CRYPT desc=HEU_AEGIS_CRYPT sev=6 cn1=241 cn1Label=Host ID dvc=10.0.0.1 TrendMicroDsTags=FS TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 filePath=C:\\Windows\\System32\\virus.exe act=Terminate msg=Realtime TrendMicroDsMalwareTarget=Multiple TrendMicroDsMalwareTargetType=File System TrendMicroDsFileMD5=1947A1BC0982C5871FA3768CD025453E#011 TrendMicroDsFileSHA1=5AD084DDCD8F80FBF2EE3F0E4F812E812DEE60C1#011 TrendMicroDsFileSHA256=25F231556700749F8F0394CAABDED83C2882317669DA2C01299B45173482FA6E TrendMicroDsDetectionConfidence=95 TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_CERBER.C;Ransom_CRYPNISCA.SM

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=1
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID
cn2	cn2	File Size	検出ファイルのサイズ。	cn2=100
cn2Label	cn2Label	File Size	フィールドcn2の名前ラベル。	cn2Label=Quarantine File Size

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
cs3	cs3	InfectedResource	スパイウェアアイテムのパス。このフィールドはスパイウェア検出イベント専用です。	cs3=C:\test\atse_samples\SPYW_Test_Virus.exe
cs3Label	cs3Label	InfectedResource	フィールドcs3の名前ラベル。このフィールドはスパイウェア検出イベント専用です。	cs3Label=Infected Resource
cs4	cs4	ResourceType	ResourceTypeの値: 10=ファイルとディレクトリ	cs4=10

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			11=システムレジストリ 12=インターネットCookie 13=インターネットURLショートカット 14=メモリ内のプログラム 15=プログラム起動領域 16=ブラウザヘルパーオブジェクト	

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			17=レイヤードサービスプロバイダ 18=hostsファイル 19=Windowsポリシー設定 20=ブラウザ 23=Windowsシェル設定 24=IEでダウンロードしたプログラムファイル	

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			25=プログラムの追加/削除 26=サービス その他=その他 たとえば、システムの再起動後もスパイウェアファイルを存続させるためにレジストリ実行キーを作成するspy.e	

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			xeという名前のスパイウェアファイルがある場合、スパイウェアのレポートには次の2つのアイテムが含まれます。spy.exeのアイテムはcs4=10 (ファイルとディレクトリ)、実行キーの	

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			このフィールドはスパイウェア検出イベント専用です。	
cs4Label	cd4Label	Resource Type	フィールドcs4の名前ラベル。このフィールドはスパイウェア検出イベント専用です。	cs4Label=Resource Type
cs5	cs5	Risk Level	リスクレベルの値: 0=超低 25=低 50=中	cs5=25

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			75=高 100=超高 このフィールドはスパイウェア検出イベント専用です。	
cs5Label	cs5Label	RiskLevel	フィールドcs5の名前ラベル。このフィールドはスパイウェア検出イベント専用です。	cs5Label=Risk Level
cs6	cs6	Container	不正プログラムが検出されたDockerコンテナのイメー	cs6=ContainerImageName | ContainerName | ContainerID

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			ジ名、コンテナ名、コンテナID。	
cs6Label	cs6Label	Container	フィールドcs6の名前ラベル。	cs6Label=Container
cs7	cs7	Flow	このイベントをトリガしたパケットが、侵入防御ルールによって監視されているトラフィックの方向と同じ方向(順方向)または逆方向(逆方向)のどちらで送信された	cs7=FWD

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			かを示します。 Flow値: FWD=接続フロー REV=リバースフロー	
cs7Label	cs7Label	Flow	フィールドcs7の名前ラベル。	cs7Label=Flow
filePath	filePath	FilePath	不正プログラムファイルの場所。	filePath=C:\\Users\\Mei\\Desktop\\virus.exe
act	act	Action	不正プログラム対策エンジンによって実行された処	act=Clean act=Pass

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			理。値には、Deny Access、Quarantine、Delete、Pass、Clean、Terminate、Unspecifiedがあります。	
結果	結果	結果	失敗した不正プログラム対策処理の結果	result=Passed result=Deleted result=Quarantined result=Cleaned result=Access Denied result=Terminated result=Log result=Failed result=Pass Failed result=Delete Failed result=Quarantine Failed result=Clean Failed result=Terminate Failed result=Log Failed result=Scan Failed result=Passed (Scan Failed) result=Quarantined (Scan Failed) result=Quarantine Failed (Scan Failed) result=Deny Access (Scan Failed)
msg	msg	Message	検索の種類。	msg=Realtime msg=Scheduled

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			値には、Realtime、Scheduled、Manualがあります。	
dvc	dvc	Device address	cn1のIPv4アドレス。 送信元がIPv6アドレスまたはホスト名の場合は表示されません(代わりにdvchostを使用します)。	dvc=10.1.144.199
dvchost	dvchost	Device host	cn1のホスト	dvchost=www.example.com dvchost=fe80::f018:a3c6:20f9:afa6%5

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
		name	名またはIPv6アドレス。 送信元がIPv4アドレスの場合は表示されません(代わりにdvcフィールドを使用します)。	
TrendMicroDsBehaviorRuleID	TrendMicroDsBehaviorRuleID	挙動監視ルールID	内部不正プログラムのケース追跡の挙動監視ルールIDです。	BehaviorRuleID = CS913
TrendMicroDsBehaviorType	TrendMicroDsBehaviorType	挙動	検出された	BehaviorType =脅威の検出

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
		監視の種類	挙動監視イベントの種類。	
TrendMicroDsTags	TrendMicroDsTags	Events tags	Deep Securityイベントタグがイベントに割り当てられている	TrendMicroDsTags=suspicious
TrendMicroDsTenant	TrendMicroDsTenant	Tenant name	Deep Securityテナント	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityテナントID	TrendMicroDsTenantId=0
TrendMicroDsMalwareTarget	TrendMicroDsMalwareTarget	Target(s)	不正プログラムが操作を試みた対象のファイル、プロセス、またはレジストリキー	TrendMicroDsMalwareTarget=N/A TrendMicroDsMalwareTarget=C:\\Windows\\System32\\cmd.exe TrendMicroDsMalwareTarget=HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings TrendMicroDsMalwareTarget=Multiple

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			(ある場合)。不正プログラムの対象が複数に及ぶ場合、このフィールドの値は「Multiple」になります。	
TrendMicroDsMalwareTargetCount	TrendMicroDsMalwareTargetCount	ターゲット数	ターゲットファイルの数。	TrendMicroDsMalwareTargetCount = 3
TrendMicroDsMalwareTargetType	TrendMicroDsMalwareTargetType	TargetType	この不正プログラムが操作を試みたシステムリソース	TrendMicroDsMalwareTargetType=N/A TrendMicroDsMalwareTargetType=Exploit TrendMicroDsMalwareTargetType=File System TrendMicroDsMalwareTargetType=Process TrendMicroDsMalwareTargetType=Registry

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			の種類。ファイルシステム、プロセス、Windowsレジストリなどです。	
TrendMicroDsProcess	TrendMicroDsProcess	Process	プロセス名	TrendMicroDsProcess = abc.exe
TrendMicroDsFileMD5	TrendMicroDsFileMD5	FileMD5	ファイルのMD5ハッシュ。	TrendMicroDsFileMD5=1947A1BC0982C5871FA3768CD025453E
TrendMicroDsFileSHA1	TrendMicroDsFileSHA1	FileSHA1	ファイルのSHA1ハッシュ。	TrendMicroDsFileSHA1=5AD084DDCD8F80FBF2EE3F0E4F812E812DEE60C1
TrendMicroDsFileSHA256	TrendMicroDsFileSHA256	FileSHA256	ファイルのSHA256ハッシュ。	TrendMicroDsFileSHA256=25F231556700749F8F0394CAABDED83C2882317669DA2C01299B45173482FA6E
TrendMicroDsDetectionConfidence	TrendMicroDsDetectionConfidence	ThreatProbability	ファイルが不正プログラムモデルと一致する割合(%表	TrendMicroDsDetectionConfidence=95

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			示) を示します。	
TrendMicroDsRelevantDetectionNames	TrendMicroDsRelevantDetectionNames	Probable Threat Type	機械学習検索分析をの他既知の脅威(セミコロン「;」で区切る)と比較したにファイルに含まれる脅威最も可能性高いのい種類をします。	TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_CERBER.C;Ransom_CRYPNISCA.SM
None	sev	Severity	イベントの重要度。重要度が1最も低く、10が最も高くなりま	sev=6

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			す。	
None	cat	Category	Category	cat=Anti-Malware
None	name	Name	イベント名	name=SPYWARE_KEYL_ACTIVE
None	desc	説明	イベントの説明。不正プログラム対策では、イベント名が説明として使用されます。	desc=SPYWARE_KEYL_ACTIVE
TrendMicroDsCommandLine	TrendMicroDsCommandLine	コマンドライン	対象プロセスが実行するコマンド	TrendMicroDsCommandLine = / tmp / orca-testkit-sample / testsys_m64 -u 1000 -g 1000 -U 1000 -G 1000 -e cve_2017_16995 1 -d 4000000
TrendMicroDsCve	TrendMicroDsCve	CVE	Common Vulnerabilities and Exposuresのいずれかでプロセスの動作が特定	TrendMicroDsCve = CVE-2016-5195、CVE-2016-5195、CVE-2016-5195

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
			された場合のCVE情報。	
TrendMicroDsMitre	TrendMicroDsMitre	MITRE	MITER攻撃のシナリオのいずれかでプロセスの動作が特定された場合のMITRE情報。	TrendMicroDsMitre = T1068、T1068、T1068
suser	suser	ユーザ名	このイベントをトリガしたユーザアカウント名	suser=root

アプリケーションコントロール イベント形式

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF: 0|Trend Micro|Deep Security Agent|10.2.229|6001200|AppControl detectOnly|6|cn1=202 cn1Label=Host ID dvc=192.168.33.128 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 fileHash=80D4AC182F97D2AB48EE4310AC51DA5974167C596D133D64A83107B9069745E0 suser=root suid=0 act=detectOnly filePath=/home/user1/Desktop/Directory1//heartbeatSync.sh fsize=20

aggregationType=0 repeatCount=1 cs1=notWhitelisted cs1Label=actionReason cs2=0CC9713BA896193A527213D9C94892D41797EB7C cs2Label=sha1 cs3=7EA8EF10BEB2E9876D4D7F7E5A46CF8D cs3Label=md5

LEEF 2.0の基本形式: LEEF:2.0|ベンダ(Vendor)|製品 (Product)|バージョン(Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEFログエントリのサンプル:LEEF:2.0|Trend Micro|Deep Security Agent|10.0.2883|60|cat=AppControl name=blocked desc=blocked sev=6 cn1=2 cn1Label=Host ID dvc=10.203.156.39 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 fileHash=E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855 suser=root suid=0 act=blocked filePath=/bin/my.jar fsize=123857 aggregationType=0 repeatCount=1 cs1=notWhitelisted cs1Label=actionReason

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=2
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID
cs1	cs1	Reason	アプリケーションコントロールが指定された処理を実行した理由(例: notWhitelisted: ソフトウェアに一致するルールがなく、承認されていないソフト	cs1=notWhitelisted

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			ウェアをブロックするようにアプリケーションコントロールが設定されていた)。	
cs1Label	cs1Label		フィールドcs1の名前ラベル。	cs1Label=actionReason
cs2	cs2		ファイルのSHA-1ハッシュ(計算済みの場合)。	cs2=156F4CB711FDBD668943711F853FB6DA89581AAD
cs2Label	cs2Label		フィールドcs2の名前ラベル。	cs2Label=sha1
cs3	cs3		ファイルのMD5ハッシュ(計算済みの場合)。	cs3=4E8701AC951BC4537F8420FDAC7EFBB5
cs3Label	cs3Label		フィールドcs3の名前ラベル。	cs3Label=md5
act	act	Action	アプリケーションコントロール エンジンによって実行された処理。値には、Blocke	act=blocked

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			d、Allowedがあります。	
dvc	dvc	Device address	cn1のIPv4アドレス。 送信元がIPv6アドレスまたはホスト名の場合は表示されません(代わりにdvchostを使用します)。	dvc=10.1.1.10
dvchost	dvchost	Device host name	cn1のホスト名またはIPv6アドレス。 送信元がIPv4アドレスの場合は表示されません(代わりにdvcフィールドを使用しま	dvchost=www.example.com dvchost=2001:db8::5

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			す)。	
suid	suid	User ID	ユーザ名のアカウントID番号。	suid=0
suser	suser	User Name	保護対象コンピュータにソフトウェアをインストールしたユーザアカウントの名前。	suser=root
TrendMicroDsTenant	TrendMicroDsTenant	Tenant name	Deep Securityテナント名。	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityテナントのID番号。	TrendMicroDsTenantId=0
fileHash	fileHash	File hash	ソフトウェアファイルを識別するSHA 256ハッシュ。	fileHash=E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
filePath	filePath	File Path	不正プログラムファイルの場所。	filePath=/bin/my.jar
fsize	fsize	File Size	ファイルサイズ(バイト)。	fsize=16
aggregationType	aggregationType	AggregationType	イベントの集約方法を	aggregationType=2

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			示す整数: • 0: イベントが集約されません。 • 1: イベントが、ファイル名、パス、イベン	

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			トの種類に応じて集約されます。 • 2: イベントがイベントの種類に応じて集計され	

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			ます。 イベントの集約については、"アプリケーションコントロールイベントログを表示する" on page 1108を参照してください。	
repeatCount	repeatCount	Repeat Count	イベントの発生回数。非集約イベントの値には1を指定します。集約イベントには2以上の値を指定します。	repeatCount=4
None	sev	Severity	イベントの重要度。重要度は1が最も低く、10が最も	sev=6

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			高くなります。	
None	cat	Category	Category	cat=AppControl
None	name	Name	イベント名	name=blocked
None	desc	説明	イベントの説明。アプリケーションコントロールでは、アクションを説明として使用します。	desc=blocked

ファイアウォールイベントログの形式

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF: 0|Trend Micro|Deep Security Agent|<DSA version>|20|Log for TCP Port 80|0|cn1=1 cn1Label=Host ID dvc=hostname act=Log dmac=00:50:56:F5:7F:47 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=192.168.126.150 dst=72.14.204.147 out=1019 cs3=DF MF cs3Label=Fragmentation Bits proto=TCP spt=49617 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 TrendMicroDsPacketData=AFB...

サンプルLEEFログエントリ: LEEF:2.0 |トレンドマイクロ| Deep Security Agent |<DSAバージョン>|21 | cat =ファイアウォール name =リモートドメイン施行(スプリットトンネル) desc =リモートドメイン施行(スプリットトンネル) sev = 5 cn1 = 37 cn1Label =ホストID dvchost = www.example.com TrendMicroDsTenant =プライマリTrendMicroDsTenantId = 0 act =拒否dstMAC = 67:BF:1B:2F:13:EE srcMAC = 78:FD:E7:07:9F:2C TrendMicroDsFrameType = IP src = 10.0.110.221 dst = 105.152.185.81 out = 177 cs3 = cs3Label =フラグメンテーションビットproto = UDP srcPort = 23 dstPort = 445 cnt = 1 TrendMicroDsPacketData = AFB...

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
act	act	Action		act=Log act=Deny

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=113
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID
cnt	cnt	Repeat Count	このイベントが連続して繰り返された回数。	cnt=8
cs2	cs2	TCP Flags		cs2=0x10 ACK cs2=0x14 ACK RST
cs2Label	cs2Label	TCP Flags	フィールドcs2の名前ラベル。	cs2Label=TCP Flags
cs3	cs3	Packet Fragmentation Information		cs3=DF cs3=MF cs3=DF MF
cs3Label	cs3Label	Fragmentation Bits	フィールドcs3の名前ラベル。	cs3Label=Fragmentation Bits
cs4	cs4	ICMP Type and Code	(ICMPプロトコルの場合のみ) ICMPタイプとコード(スペース区切り)。	cs4=11 0 cs4=8 0
cs4Label	cs4Label	ICMP	フィールドcs4の名前ラベル。	cs4Label=ICMP Type and Code
dmac	dstMAC	Destination MAC	送信先コン	dmac= 00:0C:29:2F:09:B3

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
		Address	ピュータのネットワークインタフェースのMACアドレス。	
dpt	dstPort	Destination Port	(TCPプロトコルおよびUDPプロトコルの場合のみ) 送信先コンピュータの接続またはセッションのポート番号。	dpt=80 dpt=135
dst	dst	Destination IP Address	送信先コンピュータのIPアドレス。	dst=192.168.1.102 dst=10.30.128.2
in	in	Inbound Bytes Read	(受信接続の場合のみ) 読み取られた受信バイト数。	in=137 in=21
out	out	Outbound Bytes Read	(送信接続の場合のみ) 読み取られた送信バイト数。	out=216 out=13
proto	proto	Transport protocol	使用するトラン	proto=tcp proto=udp

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			スポートプロトコルの名前。	proto=icmp
smac	srcMAC	Source MAC Address	送信元コンピュータのネットワークインタフェースのMACアドレス。	smac= 00:0E:04:2C:02:B3
spt	srcPort	Source Port	(TCPプロトコルおよびUDPプロトコルの場合のみ)送信元コンピュータの接続またはセッションのポート番号。	spt=1032 spt=443
src	src	Source IP Address	このイベントにおけるパケットの送信元IPアドレス。	src=192.168.1.105 src=10.10.251.231
TrendMicroDsFrameType	TrendMicroDsFrameType	Ethernet frame type	接続のイーサネットフレームの種類。	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
TrendMicroDsPacketData	TrendMicroDsPacketData	Packet data	Base64で表されるパケットデータ。	TrendMicroDsPacketData = AFB...
dvc	dvc	Device address	cn1のIPv4アドレス。 送信元がIPv6アドレスまたはホスト名の場合は表示されません(代わりにdvchostを使用します)。	dvc=10.1.144.199
dvchost	dvchost	Device host name	cn1のホスト名またはIPv6アドレス。 送信元がIPv4アドレスの場合は表示されません(代わりにdvc	dvchost=exch01.example.com dvchost=2001:db8::5

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			フィールドを使用します)。	
TrendMicroDsTags	TrendMicroDsTags	Event Tags	Deep Securityイベントタグがイベントに割り当てられている	TrendMicroDsTags=suspicious
TrendMicroDsTenant	TrendMicroDsTenant	Tenant Name	Deep Securityテナント	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityテナントID	TrendMicroDsTenantId=0
None	sev	Severity	イベントの重要度。重要度は1が最も低く、10が最も高くなります。	sev=5
None	cat	Category	Category	cat=Firewall
None	name	Name	イベント名	name=Remote Domain Enforcement (Split Tunnel)
None	desc	説明	イベントの説明。ファイアウォールイベントでは、イベント名が説明として使用されます。	desc=Remote Domain Enforcement (Split Tunnel)

変更監視 ログイベント形式

CEFの基本形式: CEF:バージョン(Version)|デバイスベンダ(Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン(Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF:0|Trend Micro|Deep Security Agent|<DSA version>|30|New Integrity Monitoring Rule|6|cn1=1 cn1Label=Host ID dvchost=hostname act=updated filePath=c:\\windows\\message.dll suser=admin sproc=C:\\Windows\\System32\\notepad.exe msg=lastModified,sha1,size

LEEF 2.0の基本形式: LEEF:2.0|ベンダ(Vendor)|製品 (Product)|バージョン(Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEFログエントリのサンプル: LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|2002779|cat=Integrity Monitor name=Microsoft Windows - System file modified desc=Microsoft Windows - System file modified sev=8 cn1=37 cn1Label=Host ID dvchost=www.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=updated suser=admin sproc = C:\\Windows\\System32\\notepad.exe

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
act	act	Action	変更監視ルールによって検出される処理。値は、created、updated、deleted、またはrenamedのいずれかです。	act=created act=deleted
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=113
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID
filePath	filePath	Target Entity	変更監視ルールの対象のエンティティ。監視対象のログファイルが含まれます。	filePath=C:\WINDOWS\system32\drivers\etc\hosts
suser	suser	Source	監視対象の	suser=WIN-

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
		User	ファイルを変更したユーザのアカウント。	038M7CQDHIN\Administrator
sproc	sproc	ソースプロセス	イベントのソースプロセスの名前。	sproc = C:\\Windows\\System32\\notepad.exe
msg	msg	Attribute changes	(「renamed」処理の場合のみ) 変更された属性名のリスト。[Manager経由でリレーする] を選択した場合、すべてのイベント処理の種類に完全な説明が含まれます。	msg=lastModified,sha1,size
oldfilePath	oldfilePath	Old target entity	(「renamed」処理の場合のみ) filePathフィールドに記録された新しいエンティティに名前変更された、以前の変更監視ルールの対象のエンティティ。	oldFilePath=C:\WINDOWS\system32\logfiles\ds_agent.log
dvc	dvc	Device address	cn1のIPv4アドレス。 送信元がIPv6アドレスまたはホスト名の場合は表示されません(代わりにdvchostを使用します)。	dvc=10.1.144.199
dvchost	dvchost	Device host name	cn1のホスト名またはIPv6アドレス。	dvchost=www.example.com dvchost=2001:db8::5

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			送信元がIPv4アドレスの場合は表示されません(代わりにdvcフィールドを使用します)。	
TrendMicroDsTags	TrendMicroDsTags	Events tags	Deep Securityイベントタグがイベントに割り当てられている	TrendMicroDsTags=suspicious
TrendMicroDsTenant	TrendMicroDsTenant	Tenant name	Deep Securityテナント	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityテナントID	TrendMicroDsTenantId=0
None	sev	Severity	イベントの重要度。重要度は1が最も低く、10が最も高くなります。	sev=8
None	cat	Category	Category	cat=Integrity Monitor
None	name	Name	イベント名	name=Microsoft Windows - System file modified
None	desc	説明	イベントの説明。変更監視では、イベント名が説明として使用されます。	desc=Microsoft Windows - System file modified
entityType	entityType	EntityType	変更監視イベントが該当するエンティティの種類: Directory、File、Group、InstalledSoftware、Port、Process、RegistryKey、RegistryValue、Service、User、または	entityType=ファイル

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			Wql	

侵入防御 イベントログの形式

CEFの基本形式: CEF:バージョン(Version)|デバイスベンダ(Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン(Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF:0|Trend Micro|Deep Security Agent|<DSA version>|1001111|Test Intrusion Prevention Rule|3|cn1=1 cn1Label=Host ID dvchost=hostname dmac=00:50:56:F5:7F:47 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=192.168.126.150 dst=72.14.204.105 out=1093 cs3=DF MF cs3Label=Fragmentation Bits proto=TCP spt=49786 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 act=IDS:Reset cn3=10 cn3Label=Intrusion Prevention Packet Position cs5=10 cs5Label=Intrusion Prevention Stream Position cs6=8 cs6Label=Intrusion Prevention Flags TrendMicroDsPacketData=R0VUIC9zP3...

LEEF 2.0の基本形式: LEEF:2.0|ベンダ(Vendor)|製品 (Product)|バージョン(Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

サンプルLEEFログエントリ: LEEF:2.0|トレンドマイクロ| Deep Security Agent |<DSAバージョン>|1000940 | cat =侵入防御 name = Sun Java Runtime Environmentのバッファオーバーフローの脆弱性の詳細desc = Sun Java Runtime Environmentの複数のバッファオーバーフローの脆弱性sev = 10 cn1 = 6 cn1Label =ホストID dvchost = exch01 TrendMicroDsTenant =プライマリ TrendMicroDsTenantId = 0 dstMAC = 55:C0:A8:55:FF:41 srcMAC = CA:36:42:B1:78:3D TrendMicroDsFrameType = IP src = 10.0.251.84 dst = 56.19.41.128 out = 166 cs3 = cs3Label =フラグメント化ビット数proto = ICMP srcPort = 0 dstPort = 0 cnt = 1 act = IDS:リセットcn3 = 0 cn3Label = DPIパケットの位置cs5 = 0 cs5Label = DPIストリームの位置cs6 = 0 cs6Label = DPIフラグTrendMicroDsPacketData = R0VUIC9zP3...

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
act	act	Action	(Deep Security バージョン 7.5 SP1 以前に作成された IPSルールでは、Insert、	act=Block

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			Replace、Deleteも実行することができましたが、現在これらの処理は実行されません。これらの処理の実行を試みる古いIPSルールが実行された場合、ルールが検出のみモードで適用されたことを示すイベントが記録されます)。	
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=113
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID
cn3	cn3	Intrusion Prevention Packet Position	イベントをトリガしたデータのパケット内の位置。	cn3=37
cn3Label	cn3Label	Intrusion Prevention Packet Position	フィールドcn3の名前ラベル。	cn3Label=Intrusion Prevention Packet Position
cnt	cnt	Repeat Count	このイベントが連続して繰り返された回数。	cnt=8

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
cs1	cs1	Intrusion Prevention Filter Note	(オプション) DPIルールに関連する短いバイナリまたはテキストによる備考を含めることのできる注記用フィールド。注記用フィールドの値がすべて印刷可能なASCII文字の場合、値はテキストとしてログに記録され、スペース(空白文字)はアンダースコアに変換されます。バイナリデータが含まれる場合は、Base64エンコードを使用してログに記録されます。	cs1=Drop_data
cs1Label	cs1Label	Intrusion Prevention Note	フィールドcs1の名前ラベル。	cs1Label=Intrusion Prevention Note
cs2	cs2	TCP Flags	(TCPプロトコルの場合のみ) TCPフラグバイトの	cs2=0x10 ACK cs2=0x14 ACK RST

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			後には、[URG]、[ACK]、[PSH]、[RST]、[SYN]、[FIN] の各フィールドが続きます。このフラグバイトは、TCP ヘッダが設定されている場合に存在する可能性があります。	
cs2Label	cs2Label	TCP Flags	フィールド cs2の名前 ラベル。	cs2Label=TCP Flags
cs3	cs3	Packet Fragmentation Information		cs3=DF cs3=MF cs3=DF MF
cs3Label	cs3Label	Fragmentation Bits	フィールド cs3の名前 ラベル。	cs3Label=Fragmentation Bits
cs4	cs4	ICMP Type and Code	(ICMPプロトコルの場合のみ) 単一のスペースで区切って個別の順序で格納されている ICMPタイプとコード。	cs4=11 0 cs4=8 0
cs4Label	cs4Label	ICMP	フィールド cs4の名前 ラベル。	cs4Label=ICMP Type and Code
cs5	cs5	Intrusion Prevention Stream	イベントをトリガしたデータのス	cs5=128 cs5=20

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
		Position	トリーム内の位置。	
cs5Label	cs5Label	Intrusion Prevention Stream Position	フィールドcs5の名前ラベル。	cs5Label=Intrusion Prevention Stream Position
cs6	cs6	Intrusion Prevention Filter Flags	フラグの値の合計値。 1 - Data truncated - データをログに記録できませんでした。 2 - Log Overflow - ログがオーバーフローしました。 4 - Suppressed - ログのしきい値が抑制されました。 8 - Have Data - パケットデータが含まれます。 16 - Reference Data - 以前にログに記録されたデータを参照します。	1 (Data truncated) と8 (Have Data) の組み合わせの例: cs6=9
cs6Label	cs6Label	Intrusion Prevention Flags	フィールドcs6の名前ラベル。	cs6=Intrusion Prevention Filter Flags
dmac	dstMAC	Destination MAC Address	送信先コンピュータ	dmac= 00:0C:29:2F:09:B3

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			のネットワークインタフェースMACアドレス。	
dpt	dstPort	Destination Port	(TCPプロトコルおよびUDPプロトコルの場合のみ)送信先コンピュータの接続ポート。	dpt=80 dpt=135
dst	dst	Destination IP Address	送信先コンピュータのIPアドレス。	dst=192.168.1.102 dst=10.30.128.2
xff	xff	X-Forwarded-For	X-Forwarded-Forヘッダ内の最後のハブのIPアドレス。通常は、存在する可能性のあるプロキシを越えた送信元のIPアドレスです。srcフィールドも参照してください。イベントにxffを含めるには、1006540 [X-Forwarded-For HTTPヘッダのログを有効にする] 侵入	xff=192.168.137.1

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			防御ルールを有効にします。	
in	in	Inbound Bytes Read	(受信接続の場合のみ) 読み取られた受信バイト数。	in=137 in=21
out	out	Outbound Bytes Read	(送信接続の場合のみ) 読み取られた送信バイト数。	out=216 out=13
proto	proto	Transport protocol	使用する接続トランスポートプロトコルの名前。	proto=tcp proto=udp proto=icmp
smac	srcMAC	Source MAC Address	送信元コンピュータのネットワークインタフェースMACアドレス。	smac= 00:0E:04:2C:02:B3
spt	srcPort	Source Port	(TCPプロトコルおよびUDPプロトコルの場合のみ) 送信元コンピュータの接続ポート。	spt=1032 spt=443
src	src	Source IP Address	送信元コンピュータのIPアドレス。これは、最後のプロキシサーバ (存在する場合) のIP、またはクライアントIP	src=192.168.1.105 src=10.10.251.231

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			です。xffフィールドも参照してください。	
TrendMicroDsFrameType	TrendMicroDsFrameType	Ethernet frame type	接続のイーサネットフレームの種類。	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI
TrendMicroDsPacketData	TrendMicroDsPacketData	Packet data	Base64で表されるパケットデータ。	TrendMicroDsPacketData = R0VUIC9zP3...
dvc	dvc	Device address	cn1のIPv4アドレス。 送信元がIPv6アドレスまたはホスト名の場合は表示されません(代わりにdvchostを使用します)。	dvc=10.1.144.199
dvchost	dvchost	Device host name	cn1のホスト名またはIPv6アドレス。 送信元がIPv4アドレスの場	dvchost=www.example.com dvchost=2001:db8::5

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			合は表示されません(代わりにdvcフィールドを使用します)。	
TrendMicroDsTags	TrendMicroDsTags	Event tags	Deep Securityイベントタグがイベントに割り当てられている	TrendMicroDsTags=Suspicious
TrendMicroDsTenant	TrendMicroDsTenant	Tenant name	Deep Securityテナント名	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityテナントID	TrendMicroDsTenantId=0
None	sev	Severity	イベントの重要度。重要度は1が最も低く、10が最も高くなります。	sev=10
None	cat	Category	カテゴリ	cat=Intrusion Prevention
None	name	Name	イベント名	name=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities
None	desc	説明	イベントの説明。侵入防御イベントは、イベント名を説明として使用します。	desc=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities

セキュリティログ監視 イベント形式

CEFの基本形式: CEF:バージョン(Version)|デバイスベンダ(Device Vendor)|デバイス製品(Device Product)|デバイスバージョン(Device Version)|署名ID(Signature ID)|名前(Name)|重要度

(Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF:0|Trend Micro|Deep Security Agent|<DSA version>|3002795|Microsoft Windows Events|8|cn1=1 cn1Label=Host ID dvchost=hostname cs1Label=LI Description cs1=Multiple Windows Logon Failures fname=Security src=127.0.0.1 duser=(no user) shost=WIN-RM6HM42G65V msg=WinEvtLog Security: AUDIT_FAILURE (4625): Microsoft-Windows-Security-Auditing: (no user): no domain: WIN-RM6HM42G65V: An account failed to log on.Subject: ..

LEEF 2.0の基本形式: LEEF:2.0|ベンダ (Vendor)|製品 (Product)|バージョン (Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEFログエントリのサンプル: LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|3003486|cat=Log Inspection name=Mail Server - MDaemon desc=Server Shutdown. sev=3 cn1=37 cn1Label=Host ID dvchost=exch01.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 cs1=Server Shutdown. cs1Label=LI Description fname= shost= msg=

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=113
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID
cs1	cs1	Specific Sub-Rule	このイベントをトリガしたセキュリティログ監視のサブルール。	cs1=Multiple Windows audit failure events
cs1Label	cs1Label	LI Description	フィールドcs1の名前ラベル。	cs1Label=LI Description
duser	duser	User Information	(解析可能なユーザ名が存在する場合) ログエントリを記録し	duser=(no user) duser=NETWORK SERVICE

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			た対象ユーザの名前。	
fname	fname	Target entity	セキュリティログ監視ルールの対象エンティティ。監視対象のログファイルが含まれます。	fname=Application fname=C:\Program Files\CMS\logs\server0.log
msg	msg	Details	セキュリティログ監視イベントの詳細。検出されたログイベントの詳細な説明が含まれる場合があります。	msg=WinEvtLog: Application: AUDIT_FAILURE(20187): pgEvent: (no user): no domain: SERVER01: Remote login failure for user 'xyz'
shost	shost	Source Hostname	送信元コンピュータのホスト名。	shost=webserver01.corp.com
src	src	Source IP Address	送信元コンピュータのIPアドレス。	src=192.168.1.105 src=10.10.251.231
dvc	dvc	Device address	cn1のIPv4アドレス。 送信元がIPv6アドレスまたはホス	dvc=10.1.144.199

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			ト名の場合は表示されません(代わりにdvchostを使用します)。	
dvchost	dvchost	Device host name	cn1のホスト名またはIPv6アドレス。 送信元がIPv4アドレスの場合は表示されません(代わりにdvcフィールドを使用します)。	dvchost=www.example.com dvchost=2001:db8::5
TrendMicroDsTags	TrendMicroDsTags	Events tags	Deep Securityイベントタグがイベントに割り当てられている	TrendMicroDsTags=suspicious
TrendMicroDsTenant	TrendMicroDsTenant	Tenant name	Deep Securityテナント	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityテナントID	TrendMicroDsTenantId=0

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
None	sev	Severity	イベントの重要度。重要度は1が最も低く、10が最も高くなります。	sev=3
None	cat	Category	Category	cat=Log Inspection
None	name	Name	イベント名	name=Mail Server - MDaemon
None	desc	説明	イベントの説明。	desc=Server Shutdown

Webレピュテーション イベント形式

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリのサンプル: CEF:0|Trend Micro|Deep Security Agent|<DSA version>|5000000|WebReputation|5|cn1=1 cn1Label=Host ID dvchost=hostname request=example.com msg=Blocked By Admin

LEEF 2.0の基本形式: LEEF:2.0|ベンダ (Vendor)|製品 (Product)|バージョン (Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEFログエントリのサンプル: LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|5000000|cat=Web Reputation name=WebReputation desc=WebReputation sev=6 cn1=3 cn1Label=Host ID dvchost=exch01.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 request=http://yw.olx5x9ny.org.it/HvuauRH/eighgSS.htm msg=Suspicious

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=1
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
request	request	Request	要求のURL。	request=http://www.example.com/index.php
msg	msg	Message	処理の種類。値には、Realtime、Scheduled、Manualがあります。	msg=Realtime msg=Scheduled
dvc	dvc	Device address	cn1のIPv4アドレス。 送信元がIPv6アドレスまたはホスト名の場合は表示されません(代わりにdvchostを使用します)。	dvc=10.1.144.199
dvchost	dvchost	Device host name	cn1のホスト名またはIPv6アドレス。 送信元がIPv4アドレスの場合は表示されません(代わりにdvcフィールドを使用します)。	dvchost=www.example.com dvchost=2001:db8::5
TrendMicroDsTags	TrendMicroDsTags	Events tags	Deep	TrendMicroDsTags=suspicious

CEF拡張フィールド	LEEF拡張フィールド	名前	説明	例
			Securityイベントタグがイベントに割り当てられている	
TrendMicroDsTenant	TrendMicroDsTenant	Tenant name	Deep Securityテナント	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityテナントID	TrendMicroDsTenantId=0
None	sev	Severity	イベントの重要度。重要度は1が最も低く、10が最も高くなります。	sev=6
None	cat	Category	Category	cat=Web Reputation
None	name	Name	イベント名	name=WebReputation
None	desc	説明	イベントの説明。Webレピュテーションでは、イベント名が説明として使用されます。	desc=WebReputation

デバイスコントロールイベントの形式

CEFの基本形式: CEF:バージョン (Version)|デバイスベンダ (Device Vendor)|デバイス製品 (Device Product)|デバイスバージョン (Device Version)|署名ID (Signature ID)|名前 (Name)|重要度 (Severity)|拡張 (Extension)

CEFログエントリの例: CEF:0|Trend Micro|Deep Security Agent|50.0.1063|7000000|Device Control DeviceControl|6|cn1=1 cn1Label=Host ID dvchost=test-hostname TrendMicroDsTenant=tenantName TrendMicroDsTenantId=1 device=deviceName processName=processName1 fileName=/tmp/some_path2 vendor=vendorName serial=aaaa-bbbb-cccc model=modelName computerName=computerName domainName=computerDomain deviceType=0 permission=0

LEEF 2.0の基本形式: LEEF:2.0|ベンダ(Vendor)|製品 (Product)|バージョン(Version)|イベントID (EventID)|(区切り文字、タブの場合は省略可能)|拡張 (Extension)

LEEF Log Entryの例: LEEF:2.0|Trend Micro|Deep Security Agent|50.0.1063|7000000|cat=Device Control name=DeviceControl desc=DeviceControl sev=6 cn1=1 cn1Label=Host ID dvchost=test-hostname TrendMicroDsTenant=tenantName TrendMicroDsTenantId=1 device=deviceName processName=processName1 fileName=/tmp/some_path2 vendor=vendorName serial=aaaa-bbbb-cccc model=modelName computerName=computerName domainName=computerDomain deviceType=0 permission=0

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
cn1	cn1	Host Identifier	Agentコンピュータの一意の内部識別子。	cn1=1
cn1Label	cn1Label	Host ID	フィールドcn1の名前ラベル。	cn1Label=Host ID
dvchost	dvchost	Device host name	cn1のホスト名またはIPv6アドレス。 送信元がIPv4アドレスの場合は表示されません(代わりにdvcフィールドを使用します)。	dvchost=www.example.com dvchost=2001:db8::5
TrendMicroDsTenant	TrendMicroDsTenant	Tenant name	Deep Securityテナント	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep SecurityテナントID	TrendMicroDsTenantId=0
デバイス	デバイス	装置名	アクセスされたデバイス。	device=Sandisk_USB
プロセス名	プロセス名	プロセス名	プロセス名。	processName=someProcess.exe

CEF拡張フィールド	LEEF拡張フィールド	Name	説明	例
ファイル名	ファイル名	ファイル名	アクセスされたファイル名。	fileName=E:\somepath\a.exe
販売代理店	販売代理店	ベンダー名	デバイスのベンダー名。	vendor=sandisk
シリアル	シリアル	シリアル番号	デバイスのシリアル番号。	serial=aaa-bbb-ccc
モデル	モデル	機種,モデル,型,model	デバイスの製品名。	モデル=A270_USB
コンピュータ名	コンピュータ名	コンピュータ名	コンピュータ名。	computerName=Jonh_Computer
domainName	domainName	ドメイン名	ドメイン名。	domainName=CompanyDomain
デバイスの種類	デバイスの種類	デバイスの種類	デバイスのデバイスタイプ USB_STORAGE_DEVICE(1) MOBILE_DEVICE(2)	deviceType=1
Permission	Permission	Permission	アクセスのブロック理由 ブロック(0) READ_ONLY(2)	permission=0

Red Hat Enterprise Linuxでイベントログを受信するように設定する

Red Hat Enterprise Linux 8以降でSyslogを設定する

以下の手順では、Red Hat Enterprise Linux 8以降のバージョンでrsyslogを構成し、Deep Securityからログを受信する方法を説明します。

1. rootとしてログインしてください。

2. 次のコマンドを実行してください:

   ```
   vi /etc/rsyslog.conf
   ```

3. rsyslog.confの上部付近にある次の行のコメントを解除して、

   ```
   #module(load="imudp")
   #input(type="imudp" port="514")

   #module(load="imtcp")
   #input(type="imtcp" port="514")
   ```

   から

   ```
   module(load="imudp")
   input(type="imudp" port="514")

   module(load="imtcp")
   input(type="imtcp" port="514")
   ```

   に変更してください

4. rsyslog.confの末尾に、次の2行を追加します。
   - #Save Deep Security Manager logs to DSM.log
   - Local4.* /var/log/DSM.log

   マネージャの設定によっては、Local4を別の値に置き換える必要があるかもしれません。

5. ファイルを保存して終了します。
6. touch /var/log/DSM.logと入力して、/var/log/DSM.logファイルを作成します。
7. DSMログの権限を設定して、syslogが書き込めるようにします。
8. ファイルを保存して終了します。
9. 次のコマンドを実行してsyslogを再起動してください。

   ```
   systemctl restart rsyslog
   ```

Syslogが機能していると、ログは/var/log/DSM.logに記録されます

Red Hat Enterprise Linux 6または7でSyslogを設定する

以下の手順では、Red Hat Enterprise Linux 6または7でrsyslogを設定してDeep Securityからログを受信する方法について説明します。

1. rootとしてログインしてください。
2. 次のコマンドを実行してください:
   vi /etc/rsyslog.conf
3. rsyslog.confの上部付近にある次の行のコメントを解除して、

   #$ModLoad imudp
   #$UDPServerRun 514

   #$ModLoad imtcp
   #$InputTCPServerRun 514

   から

   $ModLoad imudp
   $UDPServerRun 514

   $ModLoad imtcp
   $InputTCPServerRun 514

   に変更してください
4. rsyslog.confの末尾に、次の2行を追加します。
   - #Save Deep Security Manager logs to DSM.log
   - Local4.* /var/log/DSM.log

   注意: マネージャの設定によっては、Local4を別の値に置き換える必要があるかもしれません。
5. ファイルを保存して終了します。
6. 「touch /var/log/DSM.log」と入力して、/var/log/DSM.logファイルを作成します。
7. DSMログの権限を設定して、syslogが書き込めるようにします。
8. ファイルを保存して終了します。
9. 次のコマンドを実行してsyslogを再起動してください:

   service rsyslog restart

Syslogが機能していると、ログは/var/log/DSM.logに記録されます

Red Hat Enterprise Linux 5でSyslogを設定する

以下の手順は、Deep Securityからのログを受信するためにRed Hat Enterprise Linux 5でSyslogを設定する方法を説明します。

1. rootとしてログインしてください。
2. 次のコマンドを実行してください:
   vi /etc/syslog.conf
3. syslog.confの末尾に、次の2行を追加します。
   - #Save Deep Security Manager logs to DSM.log
   - Local4.* /var/log/DSM.log

   注意: マネージャの設定によっては、Local4を別の値に置き換える必要があるかもしれません。
4. ファイルを保存して終了します。
5. 「touch /var/log/DSM.log」と入力して、/var/log/DSM.logファイルを作成します。
6. DSMログの権限を設定して、syslogが書き込めるようにします。
7. 次のコマンドを実行してください:
   :
   vi /etc/sysconfig/syslog
8. 行 SYSLOGD_OPTIONS を修正し、オプションに -r を追加してください。
9. ファイルを保存して終了します。
10. 次のコマンドを実行してsyslogを再起動してください:

    /etc/init.d/syslog restart

Syslogが機能していると、ログは/var/log/DSM.logに記録されます

Amazon Simple Notification Serviceを設定する

Amazon Simple Notification Serviceをセットアップする

AWSアカウントをお持ちの場合、Amazon Simple Notification Service (SNS)を利用して、Deep Securityイベントに関する通知を発行し、購読者に配信することができます。

Amazon SNSを設定するには、以下の手順を実行してください。

1. "AWS認証を構成する" below。
2. "Amazon SNSトピックを作成する" on page 1240
3. "SNSを有効にする" on page 1240
4. "サブスクリプションを作成する" on page 1241

AWS認証を構成する

Amazon SNSにアクセスするには、Deep SecurityはAWS Identity and Access Management (IAM) ロールまたはAWS Access Keysを通じて認証される必要があります。

IAMロールを使用する

Deep Security ManagerがAWS EC2 Instanceで実行されている場合、認証にIAMロールを使用できます。この方法は自動的な資格情報のローテーションとセキュリティの向上を提供します。

1. AWS IAMコンソールで、SNSの発行権限を持つIAMロールを作成します。
2. 次のポリシーをロールにアタッチしてください:

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                "Action": [
                        "sns:Publish"
                ],
                "Effect": "Allow",
                "Resource": "*"
                }
        ]
}
```

   公開権限を単一のトピックに制限する場合は、"Resource":"*"を"Resource":"TOPIC ARN"に置き換えます。

3. IAMロールをDeep Security ManagerのEC2 Instanceにアタッチしてください。

イベント転送を構成すると、Deep Securityはこのロールを認証に自動的に検出して使用します。

AWS Access Keysを使用する

Deep Security ManagerがAWS EC2上で動作していない場合、またはAccess Keysを使用することを希望する場合は、SNSに適切な権限を持つAWSユーザを作成してください。ユーザのAccess Keyとシークレットキーを保存してください。これらは"SNSを有効にする" on the next page必要です。

AWSユーザは、Deep Securityが公開するすべてのSNSトピックに対してsns:Publish権限が必要です。以下はこの権限を持つポリシーの例です。

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                "Action": [
```

```
                "sns:Publish"
            ],
            "Effect": "Allow",
            "Resource": "*"
            }
        ]
    }
```

単一のトピックに公開権限を制限したい場合は、"Resource":"*"を"Resource":"TOPIC ARN"に置き換えることができます。

詳細については、AWS accountへのユーザアクセスの制御およびAmazon SNS APIの権限: アクションとリソースのレファレンス/参照情報を参照してください。

Amazon SNSトピックを作成する

AWSでイベントが公開されるSNS Topicを作成します。手順については、Amazon SNSトピックの作成を参照してください。SNS Topic ARNを保存してください。"SNSを有効にする" below有効にするために必要です。

SNSを有効にする

1. Deep Security Managerで、管理 > システム設定 > イベント転送に移動します。
2. Amazon SNSセクションで、Amazon Simple Notification Serviceにイベントを公開を選択します。
3. 選択した認証方法に基づいて認証を構成してください。
   - IAMロールが使用された場合、Deep SecurityはEC2 InstanceにアタッチされたIAMロールを自動的に検出します。Access KeyとSecret keyフィールドは空のままにしておくことができます。
   - Access Keysが使用された場合、AWSユーザのAccess keyとSecret keyを入力してください。
4. イベントが送信されるSNS Topic ARNを入力してください。これは以前に保存したARNです。
5. SNSに転送したいイベントの種類を選択してください。これにより、JSON SNS構成が自動的に生成されます。

   IAMロールはEC2デプロイメントに推奨されます。これにより、資格情報の自動ローテーションが提供され、静的Access Keysを管理する必要がなくなり、セキュリティが向上します。

6. 必要に応じて、JSON SNS設定を編集をクリックして、イベントをより詳細にフィルタリングし、各フィルタの転送指示を設定するためにJSON SNS設定を直接編集することもできます。設定言

語の詳細については、"JSON形式でのSNS設定" belowを参照してください。

JSONを編集すると、イベントの選択ができなくなります。イベントを選択または選択解除したい場合は、基本SNS設定に戻すをクリックできますが、JSON SNS設定に対するすべての設定が破棄されます。

7. [保存] をクリックします。

サブスクリプションを作成する

これでSNSが有効になり、イベントがトピックに公開されるようになりました。次に、Amazon SNSコンソールに移動し、トピックにサブスクライブしてイベントにアクセスします。イベントにサブスクライブするには、メール、SMS、Lambdaエンドポイントなど複数の方法があります。

LambdaはすべてのAWS Regionsで利用できるわけではありません。

JSON形式でのSNS設定

Amazon SNSトピックへのイベントの転送を有効にした場合に使用されるJSON設定を編集できます。この設定では、イベントをトピックに公開するために満たさなければならない条件を定義します。設定言語は、AmazonのSNS向けポリシー言語に倣っています。

各フィールドの詳細を以下に示します。基本的なSNS設定は次のような構文で記述されます。

```
{
  "Version": "2014-09-24",
  "Statement": [statement1, statement2, ...]
}
```

例については、"SNS設定の例" on page 1255を参照してください。

Version

Versionエレメントは、設定言語のバージョンを指定します。

注意: 現在有効な「Version」値は、文字列「2014-09-24」のみです。

```
"Version": "2014-09-24",
```

Statement

Statementエレメントは、複数の文の配列です。それぞれの文は、所定の条件を満たした場合にイベントを送信するSNSトピックを示すJSONオブジェクトを指定します。

```
"Statement": [{...}, {...}, ...]
```

それぞれのステートメントの形式は次のとおりです。

```
{
  "Topic": "destination topic",
  "Condition": {conditions event must meet to be published to the
destination topic}
}
```

Topic

Topicエレメントには、発行先のSNSトピックのAmazon Resource Nameを指定する必要があります。

```
"Topic": "arn:aws:sns:us-east-1:012345678901:myTopic"
```

Condition

Conditionエレメントは最も複雑な部分で、イベントをトピックに公開する条件を指定します。

各条件には、トピックに含めるイベントと一致しなければならない(条件の種類によっては一致してはならない)1つ以上のキーと値のペアを指定できます。キーは任意の有効なイベントプロパティです(イベントプロパティについては、"JSON形式のイベント" on page 1256を参照してください)。有効な値はキーによって異なります。キーによっては複数の値がサポートされる場合もあります。

```
"Condition": {
  "ConditionName": {
    "key1": [value1, value2],
    "key2": value3
  },
  "ConditionName2": {
    "key3": [value4]
```

```
    },
    ...
  }
```

有効な条件の名前と構文を以下に示します。

Bool

Bool条件は、ブール値の照合を行います。該当するプロパティがあり、その値が指定したブール値と一致していれば、条件に一致するイベントとみなされます。該当するプロパティがあるものの、その値がブール値でない場合は、次のようにしてプロパティがテストされます。

- 数値0はfalseと評価されます。0以外の数値はtrueと評価されます。
- 空の文字列と文字列「false」および「0」はfalseと評価されます。それ以外の文字列はtrueと評価されます。
- それ以外の値を持つイベントのプロパティについては、値をブール値に変換できず、照合されません。

複数値の使用: ×

次の設定例では、「DetectOnly」プロパティの値がfalseである場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "Bool": {
          "DetectOnly": false
        }
      }
    }
  ]
}
```

Exists

Exists条件は、イベントにプロパティがあるかどうかをテストします。プロパティの値は考慮されません。

複数値の使用: ×

次の設定例では、「Severity」プロパティがあり、かつ「Title」プロパティがない場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "Exists": {
          "Severity": true,
          "Title": false
        }
      }
    }
  ]
}
```

IpAddress

IpAddress条件は、イベントのプロパティの値がCIDR形式で指定したIPアドレス範囲に含まれるかどうか、または単一のIPアドレスに完全に一致するかどうかをテストします。

複数値の使用: ○

次の設定例では、「DestinationIP」プロパティのIPアドレスが10.0.1.0/24の範囲に含まれているか、10.0.0.5と一致する場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
```

```
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "IpAddress": {
          "DestinationIP": ["10.0.1.0/24", "10.0.0.5"]
        }
      }
    }
  ]
}
```

NotIpAddress

NotIpAddress条件は、イベントのプロパティの値が指定したいずれのIPアドレス範囲にも含まれないかどうかをテストします。

複数値の使用: ○

次の設定例では、「DestinationIP」プロパティのIPアドレスが10.0.0.0/8の範囲に含まれていない場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NotIpAddress": {
          "DestinationIP": "10.0.0.0/8"
        }
      }
    }
  ]
}
```

NumericEquals

NumericEquals条件は、イベントのプロパティの数値が指定した1つ以上の値と等しいかどうかをテストします。該当するプロパティがあるものの、その値が数値でない場合は、次のようにしてプロパティがテストされます。

- 文字列は数値に変換されます。数値に変換できない文字列は照合されません。
- それ以外の値を持つイベントのプロパティについては、値を数値に変換できず、照合されません。

複数値の使用: ○

次の設定例では、「Protocol」プロパティの値が6または17である場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericEquals": {
          "Protocol": [6, 17]
        }
      }
    }
  ]
}
```

NumericNotEquals

NumericNotEquals条件は、イベントのプロパティの数値が指定したいずれの値とも等しくないかどうかをテストします。

複数値の使用: ○

次の設定例では、「Protocol」プロパティの値が6以外で、かつ「Risk」プロパティの値が2または3以外である場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericNotEquals": {
          "Protocol": 6,
          "Risk" : [2, 3]
        }
      }
    }
  ]
}
```

NumericGreaterThan

NumericGreaterThan条件は、イベントのプロパティの数値が指定した値よりも大きいかどうかをテストします。該当するプロパティがあるものの、その値が数値でない場合は、前述のNumericEqualsと同じように数値に変換されます。

複数値の使用: ×

次の設定例では、「Protocol」プロパティの値が6よりも大きい場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericGreaterThan": {
          "Protocol": 6
        }
      }
```

```
      }
    ]
  }
```

NumericGreaterThanEquals

NumericGreaterThanEquals条件は、イベントのプロパティの数値が指定した値以上であるかをテストします。該当するプロパティがあるものの、その値が数値でない場合は、前述のNumericEqualsと同じように数値に変換されます。

複数値の使用: ×

次の設定例では、「Number」プロパティの値が600以上の場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericGreaterThanEquals": {
          "Number": 600
        }
      }
    }
  ]
}
```

NumericLessThan

NumericLessThan条件は、イベントのプロパティの数値が指定した値よりも小さいかどうかをテストします。該当するプロパティがあるものの、その値が数値でない場合は、前述のNumericEqualsと同じように数値に変換されます。

複数値の使用: ×

次の設定例では、「Number」プロパティの値が1000よりも小さい場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericLessThan": {
          "Number": 1000
        }
      }
    }
  ]
}
```

NumericLessThanEquals

NumericLessThanEquals条件は、イベントのプロパティの数値が指定した値以下であるかをテストします。該当するプロパティがあるものの、その値が数値でない場合は、前述のNumericEqualsと同じように数値に変換されます。

複数値の使用: ×

次の設定例では、「Number」プロパティの値が500以下の場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericLessThanEquals": {
          "Number": 500
        }
      }
    }
```

```
    ]
}
```

StringEquals

StringEquals条件は、イベントのプロパティの文字列値が指定したいずれかの値と完全に一致するかどうかをテストします。

複数値の使用: ○

次の設定例では、「EventType」プロパティの値が「SystemEvent」と一致し、かつ「TargetType」プロパティの値が「User」または「Role」と一致する場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringEquals": {
          "EventType": ["SystemEvent"],
          "TargetType" : ["User", "Role"]
        }
      }
    }
  ]
}
```

StringNotEquals

StringNotEquals条件は、イベントのプロパティの文字列値が指定したいずれの値にも一致しないかどうかをテストします。

複数値の使用: ○

次の設定例では、「EventType」プロパティの値が「PacketLog」と「IntegrityEvent」のいずれにも一致しない場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringNotEquals": {
          "EventType": ["PacketLog", "IntegrityEvent"]
        }
      }
    }
  ]
}
```

StringEqualsIgnoreCase

StringEqualsIgnoreCase条件は、StringEquals条件と同じ文字列の照合を行いますが、大文字と小文字が区別されません。

StringNotEqualsIgnoreCase

StringNotEqualsIgnoreCase条件は、StringNotEquals条件と同じ文字列の照合を行いますが、大文字と小文字が区別されません。

StringLike

StringLike条件は、イベントのプロパティの文字列値が指定したいずれかの値と一致するかどうかをテストします。この条件では、任意の数の文字と一致する「*」、任意の1文字と一致する「?」をワイルドカードとして使用できます。文字列の比較では大文字と小文字が区別されます。

複数値の使用: ○

次の設定例では、「Title」プロパティの値に「User」または「Role」という文字列が含まれる場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringLike": {
          "Title": ["*User*", "*Role*"]
        }
      }
    }
  ]
}
```

StringNotLike

StringNotLike条件は、イベントのプロパティの文字列値が指定したいずれの値にも一致しないかどうかをテストします。この条件では、任意の数の文字と一致する「*」、任意の1文字と一致する「?」をワイルドカードとして使用できます。文字列の比較では大文字と小文字が区別されます。

複数値の使用: ○

次の設定例では、「システム設定の保存」イベントを除くすべてのイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringNotLike": {
          "Title":"System Settings Saved"
        }
      }
    }
```

```
    ]
}
```

次の設定例では、「Title」プロパティの値の先頭が「User」でなく、かつ末尾が「Created」でない場合にイベントが公開されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringNotLike": {
          "Title": ["User*", "*Created"]
        }
      }
    }
  ]
}
```

複数の文と複数の条件

同じSNSトピックに対して作成した複数の文は、「or」で結合されたものとして評価されます。1つの文に複数の条件が含まれている場合、それらの条件は「and」で結合されたものとして評価されます。

複数の文

間違った設定例を次に示します。最初の文で「System Settings Saved」以外のすべてのイベントを転送するよう指定し、2つ目の文ですべての「System Settings Saved」イベントを転送するよう指定しています。結果は、すべてのイベントが最初の文の条件または2つ目の文の条件に一致するため、すべてのイベントが転送されます。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
```

```
        "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
        "Condition": {
          "StringNotLike" : {
            "Title" : "System Settings Saved"
          }
        }
      },
      {
        "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
        "Condition": {
          "StringLike" : {
            "Title" : "System Settings Saved"
          }
        }
      }
    ]
  }
```

複数の条件

間違った設定例をもう1つ示します。最初の条件で「System Settings Saved」以外のすべてのイベントを転送するよう指定し、2つ目の条件ですべての「System Settings Saved」イベントを転送するよう指定しています。結果は、どのイベントも最初の文の条件および2つ目の文の条件の両方には一致しないため、イベントは転送されません。

```
  {
    "Version": "2014-09-24",
    "Statement": [
      {
        "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
        "Condition": {
          "StringNotLike" : {
            "Title" : "System Settings Saved"
          },
          "StringLike" : {
```

```
            "Title" : "System Settings Saved"
          }
        }
      }
    ]
  }
```

SNS設定の例

以下は、一部の特定シナリオに合ったイベントを送信する設定です。SNSトピックのフィルタとして使用できるイベントプロパティ名および値の詳細については、"JSON形式のイベント" on the next pageを参照してください。

重大なすべての侵入防御イベントをSNSトピックに送信する

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericEquals": {
          "Severity": 4
        },
        "StringEquals" : {
          "EventType" : "PayloadLog"
        }
      }
    }
  ]
}
```

イベントごとに異なるSNSトピックに送信する

この例では、すべてのシステムイベントを1つのトピックに送信し、すべての変更監視イベントを別のトピックに送信します。

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-
1:012345678901:systemEventsTopic",
      "Condition": {
        "StringEquals" : {
          "EventType" : "SystemEvent"
        }
      }
    },
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:integrityTopic",
      "Condition": {
        "StringEquals" : {
          "EventType" : "IntegrityEvent"
        }
      }
    }
  ]
}
```

JSON形式のイベント

Amazon SNSに公開される際、イベントは文字列にエンコードされるJSONオブジェクトの配列として、SNS Messageで送信されます。配列内の各オブジェクトが1つのイベントです。

有効なプロパティはイベントの種類によって異なります。たとえば、MajorVirusTypeはDeep Security不正プログラム対策イベントのみに有効なプロパティであり、システムイベントなどには適用されません。有効なプロパティ値はプロパティごとに異なります。例については、"JSON形式のイベントの例" on page 1289を参照してください。

イベントプロパティ値は、SNSトピックに公開されるイベントをフィルタする際に使用できます。詳細については、"JSON形式でのSNS設定" on page 1241を参照してください。

有効なイベントプロパティ

注意: イベントによっては、その種類のイベントに通常適用されるプロパティの一部を備えていない場合があります。

プロパティ名	データタイプ	説明	適用されるイベントの種類
ACRulesetID	整数	イベントが検出されたコンピュータに適用されたアプリケーションコントロールルールセットの一意の識別子。	アプリケーションコントロールイベント
Action	文字列(列挙)	アプリケーションコントロールイベントに対して実行された処理。「ソフトウェアの実行をルールでブロック」、「承認されていないソフトウェアの実行を許可」(検出のみモードのため)、「承認されていないソフトウェアの実行をブロック」など。	アプリケーションコントロールイベント
Action	整数 (列挙)	ファイアウォールイベントに対して実行された処理。[検出のみ] の値は、ルールが有効になっていた場合に実行されたであろう処理を示します。0=不明、1=拒否、6=ログのみ、0x81=検出のみ: 拒否。	ファイアウォールイベント
Action	整数 (列挙)	侵入防御イベントに対して実行された処理。0=不明、1=拒否、2=リセット、3=挿入、4=削除、5=置換、6=ログのみ、0x81=検出のみ: 拒否、0x82=検出のみ: リセット、0x83=検出のみ: 挿入、0x84=検出のみ: 削除、0x85=検出のみ: 置換。	侵入防御イベント
ActionBy	文字列	イベントを実行したDeep Security Managerユーザの名前。ユーザによって生成されたイベントでない場合は「システム」になります。	システムイベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
ActionReasonDesc	文字列	処理がブロックされた理由。	アプリケーションコントロールイベント
ActionString	文字列	処理の文字列への変換。	ファイアウォールイベント、侵入防御イベント
AdministratorID	整数	処理を実行したDeep Securityユーザの一意の識別子。ユーザではなくシステムによって生成されたイベントには、識別子は割り当てられません。	システムイベント
AggregationType	整数 (列挙)	アプリケーションコントロールイベントが繰り返し発生したかどうか。「AggregationType」が「0」以外の場合、発生回数が「RepeatCount」に入ります。0=未集計、1=ファイル名、パス、およびイベントの種類に基づいた集計、2=イベントの種類に基づいた集計	アプリケーションコントロールイベント
AMTarget	文字列	不正プログラムが操作を試みた対象のファイル、プロセス、またはレジストリキー(ある場合)。不正プログラムの対象が複数に及ぶ場合、このフィールドの値は「Multiple」になります。	不正プログラム対策イベント
AMTargetCount	整数	ターゲットファイルの数。	不正プログラム対策イベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
AMTargetType	整数	この不正プログラムが影響を及ぼそうとしていたシステムリソースの種類の数値コード。説明バージョンについては、「AMTargetTypeString」を参照してください。0 =不明、1 =プロセス、2 =レジストリ、3 =ファイルシステム、4 =起動、5 =攻撃コード、6 = API、7 =メモリ、8 =ネットワーク接続、9 =未分類	不正プログラム対策イベント
AMTargetTypeString	文字列	この不正プログラムが操作を試みたシステムリソースの種類。ファイルシステム、プロセス、Windowsレジストリなどです。	不正プログラム対策イベント
ATSEDDetectionLevel	整数	ドキュメントの脆弱性攻撃からの保護の検出レベル。	不正プログラム対策イベント
ApplicationType	文字列	侵入防御ルールに関連付けられたネットワークアプリケーションの種類の名前 (該当する場合)。	侵入防御イベント
BehaviorRuleId	文字列	内部不正プログラムのケース追跡の挙動監視ルールIDです。	不正プログラム対策イベント
BehaviorType	文字列	検出された挙動監視イベントの種類。	不正プログラム対策イベント
BlockReason	整数 (列挙)	処理に応じた実行理由。0=不明、1=ルールによってブロック、2=承認されていないためブロック	アプリケーションコントロールイベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
Change	整数 (列挙)	変更監視イベントでファイル、プロセス、レジストリキーなどに対して行われた変更の種類。1=作成、2=アップデート、3=削除、4=拡張子変更。	変更監視イベント
ChangeString	文字列	変更監視イベントのファイル、プロセス、レジストリキーなどに加えられた変更の種類:作成、更新、削除、または名前変更	変更監視イベント
CommandLine	文字列	対象プロセスが実行したコマンド。	不正プログラム対策イベント
ContainerID	文字列	イベントが発生したコンテナのIDです。	不正プログラム対策イベント、侵入防御イベント、ファイアウォールイベント
ContainerImageName	文字列	不正プログラムが検出されたDockerコンテナのイメージ名。	不正プログラム対策イベント
ContainerName	文字列	イベントが発生したコンテナの名前。	不正プログラム対策イベント、侵入防御イベント、ファイアウォールイベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
CreationTime	文字列(日付)	感染ファイルの作成日時。	不正プログラム対策イベント
Cve	文字列	Common Vulnerabilities and Exposuresのいずれかでプロセスの動作が特定された場合のCVE情報。	不正プログラム対策イベント
DataIndex	整数	パケットデータの一意のID。	侵入防御イベント
説明	文字列	エンティティに対して行われた変更 (作成、削除、アップデート) の説明と変更された属性に関する詳細。	変更監視イベント
説明	文字列	イベントの内容を示す簡単な説明。	システムイベント
DestinationIP	文字列(IP)	パケットの送信先のIPアドレス。	ファイアウォールイベント、侵入防御イベント
DestinationMAC	文字列(MAC)	パケットの送信先のMACアドレス。	ファイアウォールイベント、侵入防御イベント
DestinationPort	整数	パケットの送信先のネットワークポート番号。	ファイアウォールイベント、侵入防御イベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
DetectionCategory	整数 (列挙)	Webレピュテーションイベントの検出カテゴリ。12=ユーザ定義、13=カスタム、91=グローバル。	Webレピュテーションイベント
DetectOnly	ブール	イベントが返されたときに [検出のみ] フラグがオンだったかどうか。trueの場合、URLへのアクセスが検出されましたが、ブロックはされていません。	Webレピュテーションイベント
Direction	整数 (列挙)	ネットワークパケットの方向。0=受信、1=送信。	ファイアウォールイベント、侵入防御イベント
DirectionString	文字列	方向の文字列への変換。	ファイアウォールイベント、侵入防御イベント
DriverTime	整数	ドライバで記録されたログ生成時刻。	ファイアウォールイベント、侵入防御イベント
EndLogDate	文字列 (日付)	繰り返し発生したイベントについての最終ログ日付。繰り返し発生したイベント以外に対しては表示されません。	ファイアウォールイベント、侵入防御イベント
EngineType	整数	不正プログラム対策エンジンの種類。	不正プログラム対策イベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
EngineVersion	文字列	不正プログラム対策エンジンのバージョン。	不正プログラム対策イベント
EntityType	文字列(列挙)	変更監視イベントが該当するエンティティの種類: Directory、File、Group、InstalledSoftware、Port、Process、RegistryKey、RegistryValue、Service、User、またはWql	変更監視イベント
ErrorCode	整数	不正プログラム検索イベントのエラーコード。0以外の場合、検索に失敗したことを示しており、検索処理および検索結果のフィールドに詳細が表示されます。	不正プログラム対策イベント
EventID	整数	イベントの識別子。識別子は同じ種類のイベントでは一意ですが、種類が異なるイベントでは同じになる場合があります。たとえば、EventTypeがファイアウォールとIPSのイベントのEventIDがどちらも1になることがあります。Deep Securityでイベントを完全かつ一意に識別するには、EventID、EventType、およびTenantIDを組み合わせる必要があります。このプロパティはDeep Security Managerのシステムイベントの「イベントID」プロパティには関連付けられていません。	すべての種類のイベント
EventType	文字列(列挙)	イベントの種類。次のいずれかです:「SystemEvent」、「PacketLog」、「PayloadLog」、「AntiMalwareEvent」、	すべての種類のイベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
		「WebReputationEvent」、「IntegrityEvent」、「LogInspectionEvent」、「AppControlEvent」。	
FileName	文字列	「script.sh」など、許可またはブロックされたソフトウェアのファイル名(フルパスは「Path」内に分けられています)。	アプリケーションコントロールイベント
FileSHA1	文字列	感染ファイルのfilesha1(セキュアハッシュアルゴリズム1の結果)。	不正プログラム対策イベント
FileSHA256	文字列	感染ファイルのfilesha256。	不正プログラム対策イベント
FileSize	整数	許可またはブロックされたソフトウェアのファイルサイズ	アプリケーションコントロールイベント
Flags	文字列	ネットワークパケットから記録されたフラグ(スペース区切りの文字列のリスト)。	ファイアウォールイベント、侵入防御イベント
Flow	整数(列挙)	ネットワーク接続フロー。有効な値: -1=利用不可、0=接続フロー、1=リバースフロー	ファイアウォールイベント、侵入防御イベント
FlowString	文字列	フローの文字列への変換。	ファイアウォールイベント、

プロパティ名	データタイプ	説明	適用されるイベントの種類
			侵入防御イベント
ForwardedSrc	配列(バイト)	転送されたパケットの送信元情報	侵入防御イベント
Frame	整数(列挙)	フレームの種類。-1=不明、2048=IP、2054=ARP、32821=REVARP、33169=NETBEUI、0x86DD=IPv6	ファイアウォールイベント、侵入防御イベント
FrameString	文字列	Frameの内容を示す文字列。	ファイアウォールイベント、侵入防御イベント
GroupID	文字列	「0」など、ソフトウェアを起動しようとしたユーザアカウントのグループID(ある場合)。	アプリケーションコントロールイベント
GroupName	文字列	「root」など、ソフトウェアを起動しようとしたユーザアカウントのグループ名(ある場合)。	アプリケーションコントロールイベント
HostAgentVersion	文字列	イベントが検出されたコンピュータを保護していたDeep Security Agentのバージョン。	アプリケーションコントロールイベント、不正プログラム対策イベント、Webレピュテーション

プロパティ名	データタイプ	説明	適用されるイベントの種類
			イベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント
HostAgentGUID	文字列	Deep Security Managerで有効化された場合のDeep Security Agentのグローバル一意識別子 (GUID)。	不正プログラム対策イベント、アプリケーションコントロールイベント、ファイアウォールイベント、変更監視イベント、侵入防御イベント、セキュリティログ監視イベント、Webレピュテーションイベント
HostAssetValue	整数	イベントが生成された時点のコンピュータの資産評価。	不正プログラム対策イベント、Webレピュテーション

プロパティ名	データタイプ	説明	適用されるイベントの種類
			イベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント、アプリケーションコントロールイベント
HostCloudType	文字列	Deep Security Agentがホストされているクラウドサービスプロバイダ。	不正プログラム対策イベント、アプリケーションコントロールイベント、ファイアウォールイベント、変更監視イベント、侵入防御イベント、セキュリティログ監視イベント、Webレピュテーションイベント
HostGUID	文字列	Deep Security Agentのグローバル一意識別子(GUID)。	不正プログラム対

プロパティ名	データタイプ	説明	適用されるイベントの種類
			策イベント、アプリケーションコントロールイベント、ファイアウォールイベント、変更監視イベント、侵入防御イベント、セキュリティログ監視イベント、Webレピュテーションイベント
HostGroupID	整数	イベントが検出されたコンピュータが属するコンピュータグループの一意の識別子。	アプリケーションコントロールイベント、不正プログラム対策イベント、Webレピュテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
HostGroupName	文字列	イベントが検出されたコンピュータが属するコンピュータグループの名前。コンピュータグループ名は一意とは限らないことに注意してください。	アプリケーションコントロールイベント、不正プログラム対策イベント、Webレピュテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント
HostID	整数	イベントが発生したコンピュータの一意の識別子。	不正プログラム対策イベント、Webレピュテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント、アプリケーションコントロールイ

プロパティ名	データタイプ	説明	適用されるイベントの種類
			ベント
HostInstanceID	文字列	イベントが検出されたコンピュータのクラウドインスタンスID。このプロパティは、クラウドコネクタと同期されたコンピュータに対してのみ設定されます。	アプリケーションコントロールイベント、不正プログラム対策イベント、Webレピュテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント
HostLastIPUsed	文字列(IP)	Deep Security Managerとの通信時にエージェントからアップデートされた最新のIPアドレス。	不正プログラム対策イベント、アプリケーションコントロールイベント、ファイアウォールイベント、変更監視イベント、侵入防御イベント、セキュリティログ監視イベント、

プロパティ名	データタイプ	説明	適用されるイベントの種類
			Webレピュテーションイベント
Hostname	文字列	イベントが生成されたコンピュータのホスト名。	不正プログラム対策イベント、Webレピュテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント、アプリケーションコントロールイベント
HostOS	文字列	イベントが検出されたコンピュータのOS。	不正プログラム対策イベント、Webレピュテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベン

プロパティ名	データタイプ	説明	適用されるイベントの種類
			ト、侵入防御イベント、アプリケーションコントロールイベント
HostOwnerID	文字列	イベントが検出されたコンピュータのクラウドアカウントID。このプロパティは、クラウドコネクタと同期されたコンピュータに対してのみ設定されます。	アプリケーションコントロールイベント、不正プログラム対策イベント、Webレピュテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント
HostSecurityPolicyID	整数	イベントが検出されたコンピュータに適用されているDeep Securityポリシーの一意の識別子。	不正プログラム対策イベント、Webレピュテーションイベント、変更監視イベント、セキュリティログ監視イベ

プロパティ名	データタイプ	説明	適用されるイベントの種類
			ント、ファイアウォールイベント、侵入防御イベント、アプリケーションコントロールイベント
HostSecurityPolicyName	文字列	イベントが検出されたコンピュータに適用されている Deep Security ポリシーの名前。セキュリティポリシー名は一意とは限らないことに注意してください。	不正プログラム対策イベント、Web レピュテーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント、アプリケーションコントロールイベント
HostVCUUID	文字列	イベントが適用されるコンピュータの vCenter UUID (特定された場合)。	アプリケーションコントロールイベント、不正プログラム対策イベント、Web レピュ

プロパティ名	データタイプ	説明	適用されるイベントの種類
			テーションイベント、変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント
ImageDigest	文字列	コンテナイメージの識別に使用されるデータの一意の概要。	侵入防御イベント、ファイアウォールイベント
ImageID	文字列	イベントが発生したDockerコンテナのイメージID	侵入防御イベント
ImageName	文字列	イベントが発生したコンテナの作成に使用されたイメージ名。	侵入防御イベント、ファイアウォールイベント
InfectedFilePath	文字列	不正プログラム検出で見つかった感染ファイルのパス。	不正プログラム対策イベント
InfectionSource	文字列	不正プログラム感染元のコンピュータの名前 (特定された場合)。	不正プログラム対策イベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
Interface	文字列(MAC)	パケットを送信または受信するネットワークインタフェースのMACアドレス。	ファイアウォールイベント、侵入防御イベント
InterfaceType	文字列	コンテナインタフェースの種類。0 =物理インタフェースはDeep Security Managerで個別に制御できるホストに属します.1 =すべての仮想インタフェース、7 =不明なタイプ(通常はホストインタフェース)です。	侵入防御イベント、ファイアウォールイベント
IPDatagramLength	整数	IPデータグラムの長さ。	侵入防御イベント
IsHash	文字列	ファイルの変更後のSHA-1コンテンツハッシュ(16進エンコード)。	変更監視イベント
Key	文字列	整合性イベントが参照しているファイルまたはレジストリキー。	変更監視イベント
LogDate	文字列(日付)	イベントが記録された日時。Deep Security Agentで生成されたイベント(ファイアウォールやIPSなど)の場合は、Deep Security Managerでイベントを受信した日時ではなく、Agentでイベントを記録した日時です。	すべての種類のイベント
MajorVirusType	整数(列挙)	検出された不正プログラムの分類。0=ジョーク、1=トロイの木馬、2=ウイルス、3=テスト、4=スパイウェア、5=パッカー、6=一般的なプログラム、7=その他	不正プログラム対策イベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
MajorVirusTypeString	文字列	MajorVirusTypeの内容を示す文字列。	不正プログラム対策イベント
MalwareName	文字列	検出された不正プログラムの名前。	不正プログラム対策イベント
MalwareType	整数 (列挙)	検出された不正プログラムの種類。1=一般的な不正プログラム、2=スパイウェア。一般的な不正プログラムの場合はInfectedFilePathが表示され、スパイウェアの場合は表示されません。	不正プログラム対策イベント
ManagerNodeID	整数	イベントが生成されたDeep Security Managerノードの一意の識別子。	システムイベント
ManagerNodeName	文字列	イベントが生成されたDeep Security Managerノードの名前。	システムイベント
MD5	文字列	ソフトウェアのMD5チェックサム(ハッシュ) (ある場合)。	アプリケーションコントロールイベント
Mitre	文字列	MITER攻撃のシナリオのいずれかでプロセスの動作が特定された場合のMITRE情報。	不正プログラム対策イベント
ModificationTime	文字列 (日付)	感染ファイルの変更日時。	不正プログラム対策イベント
Note	配列(バ	イベントが発生したパケットに	侵入防

プロパティ名	データタイプ	説明	適用されるイベントの種類
	イト)	関するエンコードされたメモ。	御イベント
Number	整数	システムイベントにイベントを識別する追加IDが指定されています。Deep Security Managerで、このプロパティが「イベントID」として表示されます。	システムイベント
Operation	整数 (列挙)	0=不明、1= 検出のみモードのため許可、2=ブロック	アプリケーションコントロール
OperationDesc	文字列	操作の値を示します。	アプリケーションコントロールイベント
Origin	整数 (列挙)	イベントの生成元。-1=不明、0=Deep Security Agent、1=VMのゲストエージェント、2=Deep Security Appliance、3=Deep Security Manager	すべての種類のイベント
OriginString	文字列	Originの内容を示す判読可能な文字列。	すべての種類のイベント
OSSEC_Action	文字列	OSSECの処理	セキュリティログ監視イベント
OSSEC_Command	文字列	OSSECのコマンド	セキュリティログ監視イベント
OSSEC_Data	文字列	OSSECのデータ	セキュリティログ監視イベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
OSSEC_Description	文字列	OSSECの説明	セキュリティログ監視イベント
OSSEC_DestinationIP	文字列	OSSECの送信先IP	セキュリティログ監視イベント
OSSEC_DestinationPort	文字列	OSSECの送信先ポート	セキュリティログ監視イベント
OSSEC_DestinationUser	文字列	OSSECの送信先ユーザ	セキュリティログ監視イベント
OSSEC_FullLog	文字列	OSSECの完全なログ	セキュリティログ監視イベント
OSSEC_Groups	文字列	OSSECのグループの結果(例: syslog,authentication_failure)	セキュリティログ監視イベント
OSSEC_Hostname	文字列	OSSECのホスト名。これはログエントリから読み取られたホストの名前であり、イベントが生成されたホストの名前と同じとは限りません。	セキュリティログ監視イベント
OSSEC_ID	文字列	OSSECのID	セキュリティログ監視イベント
OSSEC_Level	整数 (列	OSSECのレベル。0 ~ 15の整	セキュリ

プロパティ名	データタイプ	説明	適用されるイベントの種類
	挙)	数。0 ~ 3=重要度: 低、4 ~ 7=重要度: 中、8 ~ 11=重要度: 高、12 ~ 15=重要度: 重大。	ティログ監視イベント
OSSEC_Location	文字列	OSSECの場所	セキュリティログ監視イベント
OSSEC_Log	文字列	OSSECのログ	セキュリティログ監視イベント
OSSEC_ProgramName	文字列	OSSECのプログラム名	セキュリティログ監視イベント
OSSEC_Protocol	文字列	OSSECのプロトコル	セキュリティログ監視イベント
OSSEC_RuleID	整数	OSSECのルールID	セキュリティログ監視イベント
OSSEC_SourceIP	整数	OSSECの送信元IP	セキュリティログ監視イベント
OSSEC_SourcePort	整数	OSSECの送信元ポート	セキュリティログ監視イベント
OSSEC_SourceUser	整数	OSSECの送信元ユーザ	セキュリティログ

プロパティ名	データタイプ	説明	適用されるイベントの種類
			監視イベント
OSSEC_Status	整数	OSSECのステータス	セキュリティログ監視イベント
OSSEC_SystemName	整数	OSSECのシステム名	セキュリティログ監視イベント
OSSEC_URL	整数	OSSECのURL	セキュリティログ監視イベント
PacketData	整数	取り込まれたパケットデータの16進エンコード(パケットデータを取り込むようにルールで設定されている場合)。	侵入防御イベント
PacketSize	整数	ネットワークパケットのサイズ。	ファイアウォールイベント
Path	文字列	「/usr/bin/」など、許可またはブロックされたソフトウェアファイルのディレクトリパス(ファイル名は「FileName」内に分けられています)。	アプリケーションコントロールイベント
PatternVersion	整数 (列挙)	不正プログラム検出パターンファイルのバージョン。	不正プログラム対策イベント
PayloadFlags	整数	侵入防御フィルタフラグ。次のフラグ値を含むビットマスク値: 1 - データ切り捨て - データをログに記録できませんでした。2 -	侵入防御イベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
		ログオーバーフロー - このログの後にログがオーバーフローしました。4 - 抑制 - このログの後にログ数のしきい値が抑制されました。8 - データあり - パケットデータが格納されています。16 - 参照データ - 以前にログに記録されたデータを参照しています。	
PodID	文字列	ポッド一意のID(UID)	侵入防御イベント、ファイアウォールイベント
PosInBuffer	整数	イベントをトリガしたデータのパケット内の位置。	侵入防御イベント
PosInStream	整数	イベントをトリガしたデータのストリーム内の位置。	侵入防御イベント
Process	文字列	イベントを生成したプロセスの名前 (該当する場合)。	変更監視イベント
ProcessID	整数	イベントを生成したプロセスの識別子 (PID) (該当する場合)。	アプリケーションコントロールイベント、侵入防御イベント、ファイアウォールイベント
Process	文字列	検出された挙動監視イベントのプロセス名。	不正プログラム対策イベン

プロパティ名	データタイプ	説明	適用されるイベントの種類
			ト
ProcessName	文字列	「/usr/bin/bash」など、イベントを生成したプロセスの名前 (該当する場合)。	アプリケーションコントロールイベント、侵入防御イベント、ファイアウォールイベント
Protocol	整数 (列挙)	ネットワークプロトコルのID。-1=不明、1=ICMP、2=IGMP、3=GGP、6=TCP、12=PUP、17=UDP、22=IDP、58=ICMPv6、77=ND、255=RAW	ファイアウォールイベント、侵入防御イベント
Protocol	整数	ファイル検索プロトコルの数値。0 = ローカルファイル	不正プログラム対策イベント
ProtocolString	文字列	Protocolの内容を示す文字列。	ファイアウォールイベント、侵入防御イベント
Rank	整数	イベントのランク。コンピュータに割り当てられている資産評価に、この重要度のイベントに対して設定されている重要度の値を掛けた数値です。	変更監視イベント、セキュリティログ監視イベント、ファイアウォールイベント、侵入防御イベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
Reason	文字列	イベントのトリガとなったDeep Securityルールまたは設定オブジェクトの名前。ファイアウォールと侵入防御の場合、ルール以外がトリガとなったイベントではステータスにマッピングされた文字列になります。アプリケーションコントロールでは、「Reason」が「なし」になる場合があります。その場合は、代わりに「BlockReason」を参照してください。	ファイアウォール, 侵入防御, 変更監視, セキュリティログ監視, 不正プログラム対策、およびアプリケーションコントロールイベント
RepeatCount	整数	このイベントが繰り返し発生した回数。1の場合は、イベントが1回だけ確認され、その後に繰り返されていないことを示しています。	ファイアウォールイベント、侵入防御 イベント、アプリケーションコントロール イベント
Risk	整数 (列挙)	アクセスしたURLのリスクレベル: 変換後。2=不審、3=非常に不審、4=危険、5=未評価、6=管理者によるブロック	Webレピュテーションイベント
RiskLevel	整数	URLのリスクレベル: 変換前 (0 ~ 100)。URLがブロックルールによってブロックされた場合は表示されません。	Webレピュテーションイベント
RiskString	文字列	Riskの内容を示す文字列。	Webレピュテーションイベント
ScanAction1	整数	検索処理1。検索処理1と2、	不正プロ

プロパティ名	データタイプ	説明	適用されるイベントの種類
		検索結果処理1と2、およびエラーコードの組み合わせによって1つの「summaryScanResult」が生成されます。	グラム対策イベント
ScanAction2	整数	検索処理2。	不正プログラム対策イベント
ScanResultAction1	整数	検索結果処理1。	不正プログラム対策イベント
ScanResultAction2	整数	検索結果処理2。	不正プログラム対策イベント
ScanResultString	文字列	不正プログラム検索の結果を示す文字列。ScanAction 1と2、ScanActionResult 1と2、およびErrorCodeの組み合わせです。	不正プログラム対策イベント
ScanType	整数 (列挙)	イベントを生成した不正プログラム検索の種類。0=リアルタイム、1=手動、2=予約、3=クイック検索	不正プログラム対策イベント
ScanTypeString	文字列	ScanTypeの内容を示す文字列。	不正プログラム対策イベント
Severity	整数	1=情報、2=警告、3=エラー	システムイベント
Severity	整数 (列挙)	1=低、2=中、3=高、4=重大	変更監視イベン

プロパティ名	データタイプ	説明	適用されるイベントの種類
			ト、侵入防御イベント
SeverityString	文字列	Severityの内容を示す判読可能な文字列。	システムイベント、変更監視イベント、侵入防御イベント
SeverityString	文字列	OSSEC_Levelの内容を示す判読可能な文字列。	セキュリティログ監視イベント
SHA1pacteracontextmathced	文字列	ソフトウェアのSHA-1チェックサム(ハッシュ)(ある場合)。	アプリケーションコントロールイベント
SHA256pacteracontextmathced	文字列	ソフトウェアのSHA-256チェックサム(ハッシュ)(ある場合)。	アプリケーションコントロールイベント
SourceIP	文字列(IP)	パケットの送信元IPアドレス。	ファイアウォールイベント、侵入防御イベント
SourceMAC	文字列(MAC)	パケットの送信元MACアドレス。	ファイアウォールイベント、侵入防御イベント
SourcePort	整数	パケットのネットワーク送信元	ファイア

プロパティ名	データタイプ	説明	適用されるイベントの種類
		ポート番号。	ウォールイベント、侵入防御イベント
Status	整数	このイベントが特定のファイアウォールルールによって生成されたものでない場合は、約50個のハードコードされたルールのうちのいずれかになります。例: 123=ポリシーで未許可	ファイアウォールイベント
Status	整数	このイベントが特定の侵入防御ルールによって生成されたものでない場合は、約50個のハードコードされたルールのうちのいずれかになります。例: -504=無効なUTF8の符号化	侵入防御イベント
Tags	文字列	イベントに適用されているタグのカンマ区切りのリスト。このリストには、イベントの生成時に自動的に適用されるタグのみが含まれます。	すべての種類のイベント
TagSetID	整数	イベントに適用されたタグのグループの識別子。	すべての種類のイベント
TargetID	整数	イベントの対象の一意の識別子。この識別子は、テナント内の同じ種類の対象では一意ですが、異なる種類の対象では同じになる場合があります。たとえば、コンピュータとポリシーの対象IDがどちらも10になることがあります。	システムイベント
TargetIP	文字列(IP)	Webレピュテーションイベントの生成時にアクセスしていたIPアドレス。	Webレピュテーションイベント

プロパティ名	データタイプ	説明	適用されるイベントの種類
TargetName	文字列	イベントの対象の名前。システムイベントの対象は、コンピュータ、ポリシー、ユーザ、ロール、タスクなど、さまざまです。	システムイベント
TargetType	文字列	イベントの対象の種類。	システムイベント
TenantGUID	文字列	イベントに関連付けられたテナントのグローバル一意識別子(GUID)。	すべての種類のイベント
TenantID	整数	イベントに関連付けられたテナントの一意の識別子。	すべての種類のイベント
TenantName	文字列	イベントに関連付けられたテナントの名前。	すべての種類のイベント
ThreadID	文字列	イベントを発生させた(コンテナからの)スレッドのID。	侵入防御イベント、ファイアウォールイベント
Title	文字列	イベントのタイトル。	システムイベント
URL	文字列(URL)	イベントの生成時にアクセスしていたURL。	Webレピュテーションイベント
User	文字列	変更監視イベントの対象となったユーザアカウント(特定された場合)。	変更監視イベント
UserID	文字列	「0」など、ソフトウェアを起動しようとしたユーザアカウントの	アプリケーションコン

プロパティ名	データタイプ	説明	適用されるイベントの種類
		ユーザID (UID) (ある場合)。	トロールイベント
UserName	文字列	不正プログラム対策 イベントの場合、イベントをトリガしたユーザアカウント名です。 アプリケーションコントロールイベントの場合、「root」など、ソフトウェアを起動しようとしたユーザアカウントのユーザ名 (ある場合)。	不正プログラム対策 イベント、アプリケーションコントロール イベント

イベントプロパティのデータタイプ

JSONとして転送されるイベントでは、通常は他のデータタイプのエンコードに文字列が使用されます。

データタイプ	説明
配列(バイト)	バイト値で構成されるJSON array。
ブール	JSON true またはfalse。
整数	JSON int.Deep Securityのイベントでは、浮動小数点数は出力されません。 注意: イベント内の整数は32ビットを超えることがあります。イベント処理用のコードでこの整数を処理できることを確認してください。たとえば、JavaScriptのNumberデータタイプは、32ビットを超える整数を安全に処理できません。
整数 (列挙)	JSON int。一連の列挙値に限定されます。
文字列	JSON string.
文字列 (日付)	JSON string。日時として、YYYY-MM-DDThh:mm:ss.sssZのパターン (ISO 8601) で形式設定されています。「Z」はタイムゾーンです。「sss」は1秒未満の秒数を表す3桁です。W3Cの日付と時刻の形式に関する説明も参照してください。

データタイプ	説明
文字列 (IP)	JSON string。IPv4またはIPv6アドレスとして形式設定されています。
文字列 (MAC)	JSON string。ネットワークMACアドレスとして形式設定されています。
文字列 (URL)	JSON string。URLとして形式設定されています。
文字列 (列挙)	JSON string。一連の列挙値に限定されます。

JSON形式のイベントの例

システムイベント

```
{
  "Type" :             "Notification",
  "MessageId" :        "123abc-123-123-123-123abc",
  "TopicArn" :         "arn:aws:sns:us-west-2:123456789:DS_Events",
  "Message" :          "[
                         {
                           "ActionBy":"System",
                           "Description":"Alert: New Pattern Update
is Downloaded and Available\\nSeverity: Warning\",
                           "EventID":6813,
                           "EventType":"SystemEvent",
                           "LogDate":"2018-12-04T15:54:24.086Z",
                           "ManagerNodeID":123,
                           "ManagerNodeName":"job7-123",
                           "Number":192,
                           "Origin":3,
                           "OriginString":"Manager",
                           "Severity":1,
                           "SeverityString":"Info",
```

```
                            "Tags":"\",
                            "TargetID":1,
                            "TargetName":"ec2-12-123-123-123.us-west-
2.compute.amazonaws.com",
                            "TargetType":"Host",
                            "TenantID":123,
                            "TenantName":"Umbrella Corp.",
                            "Title":"Alert Ended"
                          }
                        ]",
  "Timestamp" :       "2018-12-04T15:54:25.130Z",
  "SignatureVersion" : "1",
  "Signature" :       "500PER10NG5!gnaTURE==",
  "SigningCertURL" :  "https://sns.us-west-
2.amazonaws.com/SimpleNotificationService-abc123.pem",
  "UnsubscribeURL" :  "https://sns.us-west-
2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456:DS_Events:123abc-123-123-123-123abc"
}
```

不正プログラム対策イベント

各SNS Messageに複数のウイルス検出イベントを含めることができます(簡略化のため、次の例では繰り返されるイベントプロパティを省略し、「...」で示しています)。

```
{
  "Type" :            "Notification",
  "MessageId" :       "123abc-123-123-123-123abc",
  "TopicArn" :        "arn:aws:sns:us-west-2:123456789:DS_Events",
  "Message" :         "[
                        {
                          "AMTarget": "VDSO memory",
                          "AMTargetCount": 1,
                          "AMTargetType": 7,
```

```
                            "AMTargetTypeString": "Memory",
                            "ATSEDetectionLevel": 0,
                            "BehaviorRuleId": "DIRTYCOW_MADVISE_EXPL",
                            "BehaviorType": "Exploit_Detection",
                            "CommandLine": "/tmp/demo -f esiv [xxxx]",
                            "Cve": "CVE-2016-5195",
                            "ErrorCode": 0,
                            "EventID": 1179519,
                             "EventType": "AntiMalwareEvent",
                            "FileSHA1":
"CEF4644713633C0864D4283FEFA0CE174D48F115",
                            "HostAgentGUID": "FF8162DF-4CB5-B158-DE42-
EBD52967FCF7",
                            "HostAgentVersion": "20.0.0.1685",
                            "HostGUID": "9089E800-41D3-2CA9-FF0B-
3A30A42ED650",
                            "HostID": 38,
                            "HostLastIPUsed": "172.31.21.47",
                            "HostOS": "Red Hat Enterprise 7 (64 bit)
(3.10.0-957.12.2.el7.x86_64)",
                            "HostSecurityPolicyID": 11,
                            "HostSecurityPolicyName": "Linux_AM_
Sensor",
                            "Hostname": "ec2-3-131-151-239.us-east-
2.compute.amazonaws.com",
                            "InfectedFilePath": "/tmp/demo",
                            "LogDate": "2021-01-07T10:32:11.000Z",
                            "MajorVirusType": 14,
                            "MajorVirusTypeString": "Suspicious
Activity",
                            "MalwareName": "TM_MALWARE_BEHAVIOR",
                            "MalwareType": 4,
                            "Mitre": "T1068",
```

```
                            "Origin": 0,
                            "OriginString": "Agent",
                            "PatternVersion": "1.2.1189",
                            "Process": "testsys_m64",
                            "Protocol": 0,
                            "Reason": "Default Real-Time Scan
Configuration",
                            "ScanAction1": 1,
                            "ScanAction2": 0,
                            "ScanResultAction1": 0,
                            "ScanResultAction2": 0,
                            "ScanResultString": "Passed",
                            "ScanType": 0,
                            "ScanTypeString": "Real Time",
                            "Tags": "",
                            "TenantGUID": "",
                            "TenantID": 0,
                            "TenantName": "Primary",
                            "UserName": "root"
                          }
                        ]",
  "Timestamp" :       "2018-12-04T15:57:50.833Z",
  "SignatureVersion" : "1",
  "Signature" :       "500PER10NG5!gnaTURE==",
  "SigningCertURL" :  "https://sns.us-west-
2.amazonaws.com/SimpleNotificationService-abc123.pem",
  "UnsubscribeURL" :  "https://sns.us-west-
2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456:DS_Events:123abc-123-123-123-123abc"
}
```

リモートコンピュータにSNMP経由でシステムイベントを転送

Deep Securityは、Deep Security Managerからコンピュータへのシステムイベントの転送にSNMPをサポートしています。Windowsの場合、MIBファイル (DeepSecurity.mib) の場所は、\Trend Micro\Deep Security Manager\utilです。Linuxの場合、初期設定の場所は/opt/dsm/utilです。

アラートの設定

アラートは、管理者が実行したコマンドの失敗、ハードディスクの容量不足など、Deep Securityがユーザに注意を促す必要があるときに生成されます。Deep Securityには、あらかじめ定義された一連のアラートが含まれます(リストについては、"事前定義アラート" on page 1309を参照してください) 。また、保護モジュールのルールを作成するときに、ルールがトリガされたときにアラートを生成するように設定できます。

どのアラートがトリガされたのかを確認するには、次の方法があります。

- それらはDeep Security Managerの「アラートステータス」ダッシュボードウィジェットに表示されます。
- Deep Security Managerの [アラート] 画面に表示します ("Deep Security Managerにアラートを表示する" belowを参照)。
- アラートのトリガ時にメール通知を受け取ります ("アラートのメール通知を設定する" on the next pageを参照)。
- アラートレポートを生成します ("アラートやその他のアクティビティに関するレポートの生成" on page 1305を参照)。

セキュリティイベントやシステムイベントと違って、アラートは一定期間後もデータベースから削除されません。手動または自動で消去されないかぎり、アラートは保持されます。

Deep Security Managerにアラートを表示する

Deep Security Managerの[Alerts]画面には、まだ応答されていないすべてのアラートが表示されます。アラートは、同じようなアラートをグループ化した概要ビュー、またはすべてのアラートを個別に一覧表示したリストビューで表示できます。これらの2つのビューを切り替えるには、画面のタイトルの [アラート] の横にあるメニューを使用します。また、時刻または重要度でアラートをソートできます。

概要ビューで、[詳細の表示] をクリックしてアラートパネルを展開すると、その特定のアラートを生成したコンピュータ(またはユーザ) がすべて表示されます。コンピュータをクリックすると、コンピュータの [詳細] 画面が表示されます。アラートが適用されるコンピュータが5台を超える場合、5台目のコンピュータの後ろに省略記号 (「...」)が表示されます。省略記号をクリックすると、リスト全体が表示されます。ア

ラートに対して適切な処理を実行したら、対象のアラートの横にあるチェックボックスをオンにし、[消去]をクリックして、アラートを消去できます(リストビューでは、アラートを右クリックすると、ショートカットメニューにオプションのリストが表示されます)。

「Relayアップデートサービスを利用不可」などの消去できないアラートは、アラートの状態が解消されたときに自動的に消去されます。

注意: 同じコンピュータでアラートが表示されるイベントが複数回発生した場合は、最初に発生したときの時刻がアラートに表示されます。アラートの消去後にまた同じ状態が発生した場合は、消去後に最初に発生したときの時刻が表示されます。

ヒント: [コンピュータ] フィルタバーを使用して、特定のコンピュータグループ内のコンピュータや、特定のポリシーを保持するコンピュータなど、特定のコンピュータに関連するアラートのみを表示できます。

セキュリティイベントやシステムイベントと違って、アラートは一定期間後もデータベースから削除されません。手動または自動で消去されないかぎり、アラートは保持されます。

アラートを設定する

アラートを個別に設定するには、Deep Security Managerの[アラート]画面に移動して、[アラートの設定]をクリックします。これにより、すべてのアラートのリストが表示されます。アラートの横にある緑色のチェックマークは、有効になっていることを意味します。該当する状況が発生した場合は、アラートがトリガされ、Deep Security Managerに表示されます。

アラートを選択して、[プロパティ]をクリックすると、重要度などのその他のアラート設定やメール通知設定を変更できます。

アラートのメール通知を設定する

選択したアラートが発生すると、Deep Security Managerは特定のユーザにメールを送信できます。

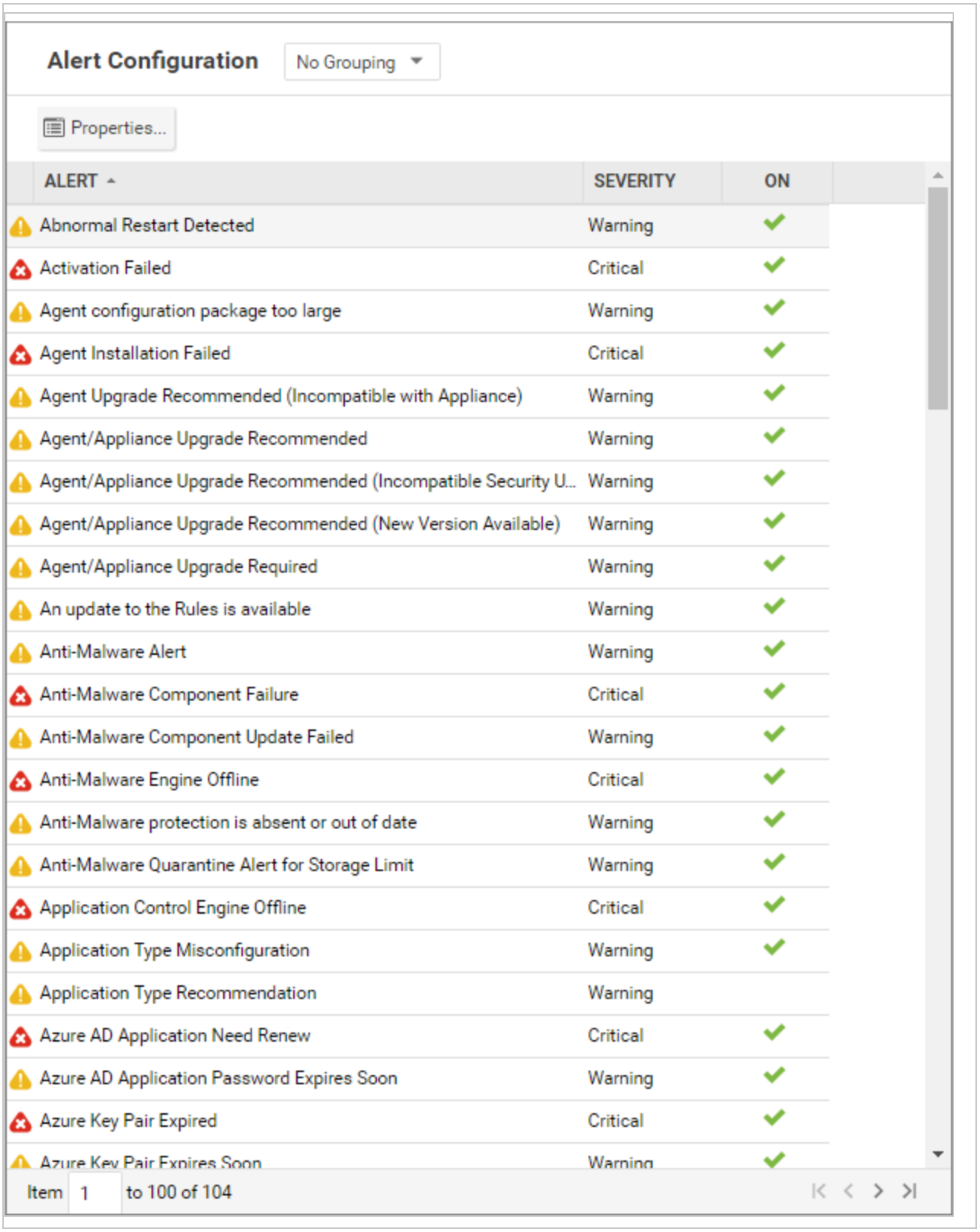
メール通知を有効にするには、次の手順に従います。

1. Deep Security ManagerにSMTPメールサーバへのアクセス権を付与します("メール通知のSMTPの設定" on page 1299を有効にするを参照してください) 。
2. どのアラートでメール通知を送信するかを指定します。たとえば、最も重大なアラートの場合のみメールを送信できます。初期設定では、ほとんどのアラートでメール通知が送信されます("アラートメールのオンとオフを切り替える" on page 1296を参照します)。
3. メール通知の受信者を指定します。アラートメールを受信するようにユーザアカウントを設定できます ("アラートメールを受信するユーザを個別に設定する" on page 1298を参照)。また、アラー

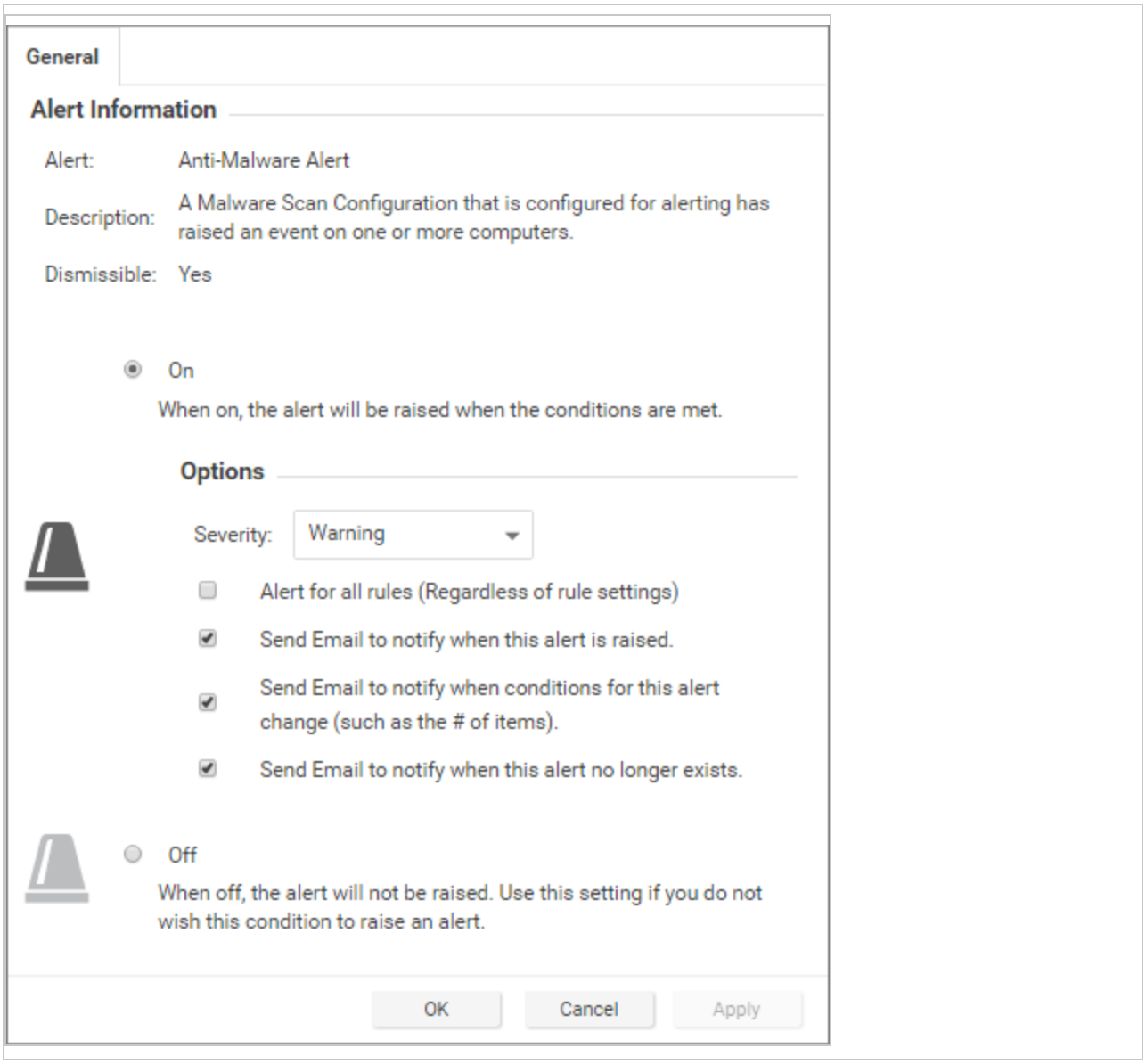
トを設定してユーザのメールアカウントまたは配信リストを指定できます。このオプションを使用すると、ユーザアカウントの設定に関係なく、メールが送信されます ("すべてのアラートメールの受信者を設定する" on page 1299を参照)。

アラートメールのオンとオフを切り替える

1. [アラート] 画面に移動し、[アラートの設定] をクリックしてアラートのリストを表示します。



2. アラートの横にある緑色のチェックマークは、有効になっていることを意味します。該当する状況が発生した場合は、アラートがトリガされ、Deep Security Manager GUIに表示されます。アラートメールも受信する場合は、アラートをダブルクリックして[プロパティ]画面を表示し、[メールの送信]チェックボックスを少なくとも1つオンにします。



アラートメールを受信するユーザを個別に設定する

1. [管理]→[ユーザ管理]→[ユーザ]の順に選択し、ユーザアカウントをダブルクリックして[プロパティ]画面を表示します。
2. [連絡先情報]タブで、メールアドレスを入力し、[アラートメールを受信]を選択します。

すべてのアラートメールの受信者を設定する

注意: 指定したアドレス、またはメール配信リストには、そのユーザアカウントのプロパティでメール通知の受信設定がされていなくても、すべてのアラートメールが送信されます。

1. [管理]→[システム設定]→[アラート]の順に選択します。
2. [アラートメールアドレス - すべてのアラートメールの送信先メールアドレス]で、メールアドレスまたは配信用のメールアドレスリストを指定します。

メール通知のSMTPの設定

Deep Security Managerは、選択されたアラートがトリガーされたときにユーザにメールを送信できます("アラートの設定" on page 1293を参照)。メール通知を設定する前に、Deep Security Managerにシンプル メール トランスファー プロトコル (SMTP) メール サーバーへのアクセスを許可する必要があります

Deep Security 20.0から、Microsoft Exchange Online SMTPにOAuth 2.0認証を使用できます。これにより、基本認証やアプリケーション固有のパスワードを必要とせずに安全なメール配信が可能になります。Microsoft Exchange OnlineのOAuth 2.0を設定するを参照してください。

1. [管理]→[システム設定]→[SMTP]の順に選択します。
2. SMTPメールサーバのIPアドレスまたはホスト名を入力してください。デフォルトのポート番号と異なる場合はポート番号も含めてください。
   AWSは、SMTPのためのインターネット割り当て番号機関 (IANA) 標準ポート番号であるポート25でメールを制限 (レート制限) します。AWS Marketplaceを使用する場合、代わりにStartTLS (Start Transport Layer Security、SMTPの安全なタイプ) を使用すると、より迅速なアラートを受け取ることができます。詳細については、Amazon SES SMTPエンドポイントへの接続を参照してください。
3. メールを送信するメールアドレスを入力するには、Fromフィールドを使用します。Amazon Simple Email Service (SES) を使用している場合、送信者のメールアドレスは確認済みである必要があります。Amazon SESでメールアドレスを確認する方法や、既に確認済みのアドレスのリストを表示する方法については、メールアドレスの確認を参照してください。
4. オプションで、アラートメールを1人以上のユーザに配信できなかった場合に配信ステータス通知 (DSN) を送信するバウンスメールアドレスを入力します。
5. SMTPサーバに基づいて認証を構成する:
   - Microsoft Exchange OnlineでOAuth 2.0を使用する場合、Microsoft Exchange Onlineのメールサーバは OAuth 2.0認証を必要としますを選択し、OAuth 2.0の資格情報を入力してください。Microsoft Exchange OnlineのOAuth 2.0を設定するを参照してください。

- 標準SMTP認証の場合、メールサーバは認証を要求するを選択し、SMTPユーザ名とパスワードを入力してください。

6. SMTPサーバがプロトコルをサポートしている場合は、STARTTLSを選択してください。Deep Security ManagerのFIPSモードは、Deep Security Manager 20 LTS Update 2022-03-22以降でStarTTLSをサポートしています。"FIPS 140のサポート" on page 1870を参照してください。 Microsoft Exchange OnlineでOAuth 2.0認証が有効になっている場合、STARTTLSは自動的に有効になり、OAuth 2.0の要件として無効にすることはできません。
7. 必要な情報を入力したら、[SMTP設定のテスト] をクリックして接続をテストします。

Microsoft Exchange OnlineのOAuth 2.0を構成する

Deep Security 20.0から、Deep Security ManagerはSMTPのためのOAuth 2.0認証をサポートし、基本認証やアプリケーション固有のパスワードを必要とせずにMicrosoft Exchange Onlineを通じて安全なメール配信を可能にします。

前提条件

以下の項目を確認してください:

- Exchange Onlineを含むMicrosoft 365サブスクリプション(ビジネスまたはエンタープライズライセンス)。Exchange Onlineを含まない基本的なOffice 365プランはサポートされていません。
- 管理者ロール:
  - Azure AD構成のためのグローバル管理者またはアプリケーション管理者
  - Exchange管理者またはグローバル管理者 - Exchange Onlineの構成

  必要な管理者権限がない場合は、IT部門またはMicrosoft 365管理者と協力してAzure ADおよびExchange Onlineの構成を完了する必要があります。最終的なDSM構成は、設定更新権限を持つ任意のDSMユーザが実行できます。

Microsoft Entra IDを構成する

Microsoft Entra IDの構成は複数の手順を含むプロセスです。

手順1: Microsoft Entra IDでアプリケーションを登録する

1. Azureポータルにサインインします。
2. Microsoft Entra ID (以前のAzure Active Directory) に移動します。
3. 左側のメニューからアプリ登録を選択します。
4. 新規登録をクリックします。

5. 次の項目を定義してアプリケーションを設定します。
   - 名前: Deep Security Manager SMTPまたはお好みの名前を入力してください。
   - サポートされているアカウントの種類: この組織ディレクトリ内のアカウントのみを選択してください。
   - リダイレクトURI: このフィールドは空白のままにしてください。
6. 登録をクリックしてください。
7. 登録後、概要ページでアプリケーション(クライアント) IDとディレクトリ(テナント) IDの値をメモしておいてください。後で必要になります。

手順2: クライアントシークレットを作成する

1. アプリケーション登録で、左側のメニューから証明書とシークレットを選択してください。
2. クライアントシークレットの下で、新しいクライアントシークレットをクリックします。
3. 次の項目を定義して秘密を設定してください:
   - 説明: DSM SMTPシークレットまたは希望する説明を入力してください。
   - 有効期限: 適切な有効期限を設定してください (例: 24か月)。
4. 追加をクリックします。
5. 値をすぐにコピーして安全な場所に保存してください。これはクライアントシークレットであり、一度しか表示されません。DSMを構成するために必要です。

手順3: APIの権限を構成する

1. アプリケーション登録で、左側のメニューからAPI のアクセス許可を選択します。
2. 権限を追加をクリックします。
3. 組織が使用するAPIを選択してください。
4. Office 365 Exchange Onlineを検索して選択します。
5. アプリケーションのアクセス許可(委任されたアクセス許可ではありません) を選択してください。
6. SMTPセクションを展開し、SMTP.SendAsAppを選択してs権限を追加します。
7. 権限を追加をクリックします。
8. グローバル管理者である場合は、[Your Organization]に管理者の同意を付与をクリックし、次にはいをクリックしてください。
9. ステータスが[Your Organization]に付与済みで緑のチェックマークが付いていることを確認してください。

Office 365 Exchange Online APIをMicrosoft Graphではなく選択することが重要です。APIの権限リストでの権限はSMTP.SendAsAppである必要があります。

Exchange Onlineを構成する

手順4: テナントのSMTP AUTHを有効にする

SMTP AUTHはデフォルトでテナントで無効になっている可能性があります。これを確認し、無効になっている場合は、次の手順で有効にしてください。

1. Exchange管理センターにサインインしてください。
2. 設定 > メールフロー > 受け入れドメインに移動します。
3. ドメインを選択し、SMTPが有効になっていることを確認してください。

   SMTP AUTHが無効になっているというエラーが発生した場合:

   - Exchange管理センターで、設定 > メールフローに移動します。
   - SMTP AUTH設定をクリックします。
   - 組織のために認証済みSMTP (SMTP AUTH)を有効にします。

手順5: メールボックスのSMTP AUTHを有効にする

DSMで使用される特定のメールボックスに対してSMTP AUTHを有効にする必要があります。

オプションA: Exchange Online PowerShellを使用して有効化 (大量操作に推奨)

1. 次のコマンドを実行してExchange Online PowerShellに接続します。

   ```
   Connect-ExchangeOnline -UserPrincipalName admin@yourcompany.com
   ```

2. 次のコマンドを実行して、メールボックスのSMTP AUTHを有効にします。

   ```
   Set-CASMailbox -Identity "dsm-notifications@yourcompany.com" -
   SmtpClientAuthenticationDisabled $false
   ```

3. 次のコマンドを実行して設定を確認してください。

   ```
   Get-CASMailbox -Identity "dsm-notifications@yourcompany.com" |
   Select-Object SmtpClientAuthenticationDisabled
   ```

   値は`False`である必要があります。

オプションB: Exchange管理センターを使用して有効化

1. 受信者 > メールボックスに移動します。
2. メールボックスを選択し、メールアプリ設定を管理をクリックします。
3. 認証済みSMTPが有効になっていることを確認してください。
4. 保存をクリック。

手順6: Exchange Onlineでサービスプリンシパルを登録する

アプリケーションはExchange Onlineでサービスプリンシパルとして登録されている必要があります。

登録するには、PowerShellを使用して次の手順を実行してください(UIオプションは利用できません):

1. 次のコマンドを実行して、Exchange Online PowerShellに接続します(まだ接続されていない場合):

   ```
   Connect-ExchangeOnline -UserPrincipalName admin@yourcompany.com
   ```

2. 次のコマンドを実行してサービスプリンシパルを登録してください。

   ```
   New-ServicePrincipal -AppId <Application (client) ID> -ServiceId
   <Object ID> -DisplayName "Deep Security Manager SMTP"
   ```

   以下の値を置き換えてください。
   - <Application (client) ID>: 手順1のアプリケーション(クライアント)ID。
   - <Object ID>: Azureポータル > アプリ登録 > あなたのアプリ> 概要 > オブジェクトIDのオブジェクトID

3. 次のコマンドを実行して、サービスプリンシパルにメールボックスとしてメールを送信する権限を付与します。

   ```
   Add-MailboxPermission -Identity "dsm-
   notifications@yourcompany.com" -User <Application (client) ID> -
   AccessRights FullAccess
   ```

Deep Security Managerを構成する

手順 7: DSMでSMTP設定を構成する

1. Deep Security Managerコンソールにログインしてください。
2. 管理 > システム設定 > SMTP タブに移動します。
3. 以下を設定してください。
   - SMTP メールサーバアドレス: smtp://smtp.office365.com:587に設定してください
   - 送信元 メールアドレス: dsm-notifications@yourcompany.comに設定します。これは手順5で設定したメールボックスです。
   - バウンスメールアドレス: dsm-notifications@yourcompany.comに設定してください
4. メールサーバーはMicrosoft Exchange OnlineのOAuth 2.0認証を必要としますを選択してください。

5. OAuth 2.0の認証情報を入力してください:
   - ディレクトリ(テナント) ID: 手順1の値を入力してください。
   - アプリケーション(クライアント) ID: 手順1の値を入力してください。
   - クライアントシークレット: 手順2からの値を入力してください。
6. SMTP設定をテストをクリックして、構成を確認します。
7. テストが成功した場合は、保存をクリックしてください。

メールサーバーがMicrosoft Exchange OnlineのOAuth 2.0認証を必要とするを選択した場合、以下が適用されます。

- 標準SMTP認証フィールドのSMTPユーザー名とSMTPパスワードは利用できません。
- STARTTLSは自動的に有効化されており、OAuth 2.0に必要なため無効化することはできません。

トラブルシューティング

以下は、Microsoft Exchange OnlineでOAuth 2.0を使用する際の一般的なエラーとその解決策です。

エラー: "535 5.7.139 認証に失敗しました。SmtpClientAuthenticationが無効です"

原因: テナントまたはメールボックスレベルでSMTP AUTHが無効になっています。

解決策:

1. テナントのSMTP AUTHを有効にする(手順4を参照)。
2. メールボックスのSMTP AUTHを有効にする(手順5を参照)。
3. 変更が反映されるまで5 ~ 10分お待ちください。

エラー: "535 5.7.3 認証に失敗しました"

原因: 次のいずれかが考えられます:

- アプリケーション(クライアント) ID、ディレクトリ(テナント) ID、またはクライアントシークレットが正しくありません。
- Exchange Onlineにサービスプリンシパルが登録されていません。
- API の権限が不足しているか、管理者の同意が得られていません。
- クライアントシークレットの有効期限が切れました。

解決策:

1. DSMですべての認証情報が正しく入力されていることを確認してください。
2. サービスプリンシパルが登録されていることを確認してください(手順6を参照)。
3. SMTP.SendAsAppの権限が管理者の同意を得て付与されていることを確認してください(手順3を参照)。
4. Azureポータルでクライアントシークレットが期限切れになっていないことを確認してください。

エラー: "430 4.2.0 STOREDRV; メールボックスログオン失敗"

原因: サービスプリンシパルがメールボックスにアクセスする権限を持っていません。

解決策:

1. サービスプリンシパルにメールボックスへのFullAccess権限を付与します(手順6を参照)。
2. 権限の変更が反映されるまで15 ~ 30分お待ちください。

詳細については、以下を参照してください。

- IMAP、POP、SMTP接続をOAuthで認証する方法
- Exchange Onlineで認証されたクライアントSMTP送信 (SMTP AUTH) を有効または無効にする

アラートやその他のアクティビティに関するレポートの生成

Deep Security Managerでは、レポートがPDFまたはRTF形式で生成されます。ほとんどのレポートには、期間やコンピュータグループ別のレポートなど、設定可能なパラメータがあります。パラメータオプションは、適用されないレポートでは無効になります。1回限りのレポートを設定するか("単独レポートを設定する" belowを参照)、定期的にレポートを実行するようにスケジュールを設定することができます("予約レポートを設定する" on page 1308を参照)。

単独レポートを設定する

1. Deep Security Managerで、イベントとレポートタブに移動し、左側のペインで[Generate Reports]→[Single Report]の順にクリックします。
2. [レポート]リストで、生成するレポートの種類を選択します。使用している保護モジュールに応じて、次のレポートを使用できます。
   - アラートレポート: 最も一般的なアラートのリスト。
   - 不正プログラム対策レポート: 上位25台の感染コンピュータのリスト。
   - 攻撃レポート: 分析アクティビティを含む概要テーブル(モード別) 。参照攻撃レポートについて。

- AWS Metered Billing Report: AWS Metered Billingの1日あたりの消費量(インスタンスサイズ別)の概要表。
- Azure Metered Billing Report: Azure Metered Billingの1日あたりの消費量(インスタンスサイズ別)の概要表。
- コンピュータレポート: [コンピュータ] タブに表示される各コンピュータの概要。
- 侵入防御ルールの推奨状況レポート: 侵入防御ルールの推奨設定。このレポートは、一度に1つのセキュリティポリシーまたはコンピュータでのみ実行できます。
- ファイアウォールレポート: ファイアウォールルールおよびステートフル設定アクティビティの記録。
- コンピュータフォレンジックス監査レポート: コンピュータ上のAgentの設定
- 変更監視ベースラインレポート1: 特定の時点でのコンピュータのベースラインを示し、タイプ、キー、およびフィンガープリントされた日付を表示します。
- 変更監視の詳細な変更レポート: 検出された変更についての詳細
- 変更変更監視レポート:検出された変更の概要。
- 侵入防御レポート:侵入防御ルールのアクティビティの記録。
- セキュリティログ監視の詳細レポート: 収集されたログデータの詳細。
- セキュリティログ監視レポート: 収集されたログデータの概要。
- 推奨設定レポート: 推奨設定の検索アクティビティの記録。
- セキュリティモジュール使用累計レポート: 保護モジュールの現在のコンピュータ使用状況(累計と100件ごとの合計)。
- セキュリティモジュール使用状況レポート:保護モジュールの現在のコンピュータの使用状況。
- 概要レポート: Deep Securityアクティビティの概要のまとめ。
- 不審なアプリケーション活動レポート: 不審なアクティビティについての情報。
- システムイベントレポート:システム(セキュリティ以外)のアクティビティの記録。
- システムレポート: コンピュータ、連絡先、ユーザの概要。
- テナントレポート: テナント概要。
- ユーザおよび連絡先レポート: ユーザと連絡先の内容およびアクティビティの詳細。
- Webレピュテーションレポート: Webレピュテーションイベントの多いコンピュータのリスト。

3. レポートの形式として、PDFまたはRTFを選択します。セキュリティモジュール使用状況レポートとセキュリティモジュール使用状況の累積レポートは例外で、常にCSVファイルとして出力されます。

4. PDFまたはRTFレポートにオプションの分類を追加することもできます。「空白」、「極秘」、「極秘」、「機密」、「公式使用のみ」、「法規制機密 (LES)」、「限定配布」、「機密扱い」、「内部使用のみ」、「カスタム」。
   [CUSTOM] を指定すると、[名前]フィールドが表示され、カスタム文字列を入力できます。たとえば、「アラートレポートの分類」などです。
5. [タグフィルタ] 領域では、イベントタグを使用してレポートデータをフィルタできます (イベントデータを含むレポートを選択した場合)。すべてのイベントの場合は [すべて] を選択するか、タグなしのイベントのみの場合は [タグなし] を選択します。または、[タグ]を選択してタグを指定し、選択したタグの付いたイベントのみを含めます。
   複数の矛盾するタグを適用すると、タグは結合するのではなく、互いに打ち消し合います。たとえば、[ユーザのサインイン] と[ユーザのサインアウト] を選択した場合、システムイベントは発生しません。

6. 時間フィルタ領域を使用して、レコードが存在する任意の期間に対して時間フィルタを設定できます。これは、セキュリティ監査に役立ちます。時間フィルタのオプションは次のとおりです。
   - 過去24時間:開始時刻から終了時刻までの過去24時間のイベントが含まれます。たとえば、12月5日の午前10時14分にレポートを生成すると、12月4日の午前10時から12月5日の午前10時までに発生したイベントのレポートが生成されます。
   - 過去 7 日間:過去 1 週間のイベントが含まれます。週の開始時刻と終了時刻は午前0時 (00:00) です。たとえば、12月5日の午前10時14分にレポートを生成すると、11月28日の午前0時から12月5日の午前0時までに発生したイベントのレポートが生成されます。
   - 前月: 前月のイベントが含まれます。深夜0時に記録を開始および終了します。たとえば、11月15日にこのオプションを選択すると、10月1日の0時から11月1日の0時までに発生したイベントのレポートが送信されます。
   - カスタム範囲:レポートに独自の日時範囲を指定できます。レポートで、開始日が2日以上前の場合、開始時刻が午前0時に変更されることがあります。
     レポートでは、カウンタに保存されているデータが使用されることに注意してください。カウンタは、イベントから定期的に収集されるデータです。カウンタデータは、過去3日間の1時間ごとに集計されます。現在の時間のデータはレポートに含まれません。3日以上経過したデータは、日次で集計されるカウンタに保存されます。このため、過去3日間のレポート対象期間は時間単位で指定できますが、3日を超える場合は日単位でのみ指定できます。
7. コンピュータフィルタ領域で、レポートにデータを含めるコンピュータを選択します。
   - すべてのコンピュータ: Deep Security Manager内のすべてのコンピュータ。
   - マイコンピュータ:サインインしているユーザが、ユーザの役割の権限設定に基づいてコンピュータへのアクセスを制限している場合、それらのコンピュータは、サインインしているユーザが表示アクセス権を持っています。

- グループ内の: Deep Securityグループ内のコンピュータ。
- 使用ポリシー: 選択したポリシー(およびオプションでそのサブポリシー)を使用しているコンピュータに、レポートの対象を限定できます。
- コンピュータ: 1台のコンピュータ。
  複数のコンピュータグループの特定のコンピュータに関するレポートを生成するには、対象のコンピュータに対する表示権限のみを持つユーザを作成してから、スケジュールタスクを作成してそのユーザの[すべてのコンピュータ]レポートを定期的に生成するか、そのユーザとしてログインして次のコマンドを実行します。[すべてのコンピュータ]レポート。レポートには、そのユーザが表示権限を持つコンピュータのみが含まれます。

8. [暗号化]エリアで、現在ログインしているユーザのパスワードか、レポートごとに設定された新規パスワードでレポートを保護できます。
   - レポートのパスワードの無効化: レポートはパスワードで保護されません。
   - 現在のユーザのレポートのパスワードを使用: 現在のユーザのPDFレポートのパスワードを使用します。ユーザのPDFレポートのパスワードを表示または変更するには、[管理]→[ユーザ管理]→[ユーザ]→[プロパティ]→[設定]→[レポート]に進みます。
   - カスタムレポートのパスワードの使用: このレポートのワンタイムパスワードを作成します。パスワードに複雑さの要件はありません。

予約レポートを設定する

予約レポートは、定期的にレポートを生成し、任意の数のユーザおよび連絡先に配信する予約タスクです。

予約レポートを設定するには、次の手順を実行します。

1. [イベントとレポート]タブの左側のペインで、[レポートの生成] > [スケジュールされたレポート]をクリックします。
2. [新規]をクリックします。[予約タスクの新規作成]ウィザードが開きます。[時間フィルタ]を除き、ほとんどのオプションは単一レポートのオプションと同じです。



- 過去 [N] 時間: [N] に60未満の値を指定した場合、開始時刻と終了時刻は指定した時間の正時となります。[N] に60より大きな値を指定すると、指定した期間の開始時のデータは時間単位で集計されていないため、レポートの開始時刻は開始日の深夜0時 (00:00) に変更されます。
- 過去 [N] 日間: [N] 日前の深夜0時から現在の日付の深夜0時までのデータがレポートされます。
- 過去 [N] 週間: 過去 [N] 週間のイベントがレポートされます。開始および終了時刻は深夜0時 (00:00) です。
- 過去 [N] か月間: 過去 [N] か月間の暦月のイベントがレポートされます。開始および終了時刻は深夜0時 (00:00) です。たとえば、11月15日に「過去1か月間」を選択すると、10月1日の0時から11月1日の0時までに発生したイベントのレポートが送信されます。

レポートでは、カウンタに保存されているデータが使用されます。カウンタは、イベントから定期的に集計されるデータです。カウンタデータは、過去3日間の1時間ごとに集計されます。現在の時間のデータはレポートに含まれません。3日以上経過したデータは、日次で集計されるカウンタに保存されます。このため、過去3日間のレポート対象期間は時間単位で指定できますが、3日を超える場合は日単位でのみ指定できます。

予約タスクの詳細については、"Deep Security予約タスクの設定" on page 1826を参照してください。

脚注:

1

大量のベースラインデータに関連するパフォーマンスの問題により、最新バージョンのDeep Security ManagerではUIからベースラインデータにアクセスすることはできません。詳細については、大量の変更監視ベースラインデータによるデータベースのパフォーマンス問題を参照してください。

イベントとアラートのリスト

事前定義アラート

アラート	初期設定の重要度	消去可能	説明
Deep Security Agentによる保護を有効にするためにコンピュータの再起動が必要	重大	○	Agentソフトウェアのアップデートは正常に完了しましたが、Windows Defenderを無効にしてDeep Security Agentによる保護を有効にするには、コンピュータの再起動が必要です。

アラート	初期設定の重要度	消去可能	説明
Deep Security Relayのセキュリティコンポーネントをダウンロードできません	重大	×	Deep Security Relayがセキュリティコンポーネントを正しくダウンロードできません。ネットワーク接続の問題、またはDeep Security Managerの [管理]→[システム設定]→[アップデート] の下の誤った設定が原因である可能性があります。ネットワーク設定 (Relayグループのプロキシ設定など) と[システム設定] を確認し、[管理]→[アップデート]→[ソフトウェア] 画面の [セキュリティアップデートのダウンロード] オプションを使用して手動でRelayのアップデートを開始してください。
異常な再起動の検出	警告	○	コンピュータで異常な再起動が検出されました。この状況は、さまざまな原因で発生します。Agent/Applianceが根本原因であると疑われる場合は、診断パッケージ ([コンピュータの詳細] 画面の [サポート] セクション) を起動する必要があります。 このアラートは、Deep Security Agentサービスが異常な状態で再起動されたことを示しています。このアラートは消去してもかまいません。アラートが再度発生した場合は、診断パッケージを作成してテクニカルサポートでサポートケースを開いてください。
有効化の失敗	重大	×	Agent/Applianceに問題がある可能性もありますが、Agentセルフプロテクションが有効になっている場合にもこのエラーが発生します。Deep Security Managerで、コンピュータエディタ[1]]→[設定]→[一般]の順に選択します。[Agentセルフプロテクション] で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否] の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。
Agentの設定パッケージが大きすぎる	警告	○	これは通常、割り当てられているファイアウォールルールおよび侵入防御ルールが多すぎることが原因です。安全に割り当てを解除できるルールがあるかどうかを判断するには、コンピュータで推奨設定の検索を実行してください。
Agentハートビートパブリックサーバ証明書の期限切れ	重大	×	AgentハートビートポートでTLSに使用しているパブリックサーバ証明書の期限が切れています。証明書がアップデートされるまで、新しいAgentを有効化することはできません。
Agentハートビートパブリックサーバ証明書がまもなく期限切れ	警告	×	AgentハートビートポートでTLSに使用しているパブリックサーバ証明書がまもなく期限切れになります。Agentの通信が中断されないように、早めに更新してください。
Agentインストールの失敗	重大	○	Agentを1台以上のコンピュータに正常にインストールできませんでし

[1] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

アラート	初期設定の重要度	消去可能	説明
			た。これらのコンピュータは現在保護されていません。コンピュータを再起動し、Agentインストールプログラムを自動的に再起動する必要があります。 Agent/Applianceに問題がある可能性もありますが、Agentセルフプロテクションが有効になっている場合にもこのエラーが発生します。Deep Security Managerで、コンピュータエディタ[1]→[設定]→[一般]の順に選択します。[Agentセルフプロテクション]で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否]の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。
Agentのアップグレード推奨(Applianceと非互換)	警告	×	Deep Security Managerは、アプライアンスと互換性のないバージョンのエージェントを持つコンピュータを検出しました。この構成では、Applianceが常にネットワークトラフィックをフィルタリングするため、保護が冗長になります。(9.5で廃止)
Agent/Applianceのアップグレード推奨	警告	×	Deep Security Managerによって、使用可能なすべての機能をサポートしていない古いバージョンのエージェント/ Applianceが検出されました。Agent/Applianceソフトウェアのアップグレードを推奨します。(9.5で廃止)
Agent/Applianceのアップグレード推奨 (非互換のセキュリティアップデート)	警告	×	Deep Security Managerは、エージェント/ Applianceの1つ以上のセキュリティアップデートと互換性のないバージョンのコンピュータが検出されました。Agent/Applianceソフトウェアのアップグレードを推奨します。
Agent/Applianceのアップグレード推奨 (新しいバージョンが使用可能)	警告	×	Managerにインポートされた最新バージョンより古いバージョンのエージェント/アプライアンスがインストールされているコンピュータがDeep Security Managerで検出されました。Agent/Applianceソフトウェアのアップグレードを推奨します。
Agent/Applianceのアップグレードが必要	警告	×	Deep Security Managerで、このバージョンのManagerと互換性のないバージョンのエージェント/ Applianceがインストールされたコンピュータが検出されました。Agent/Applianceソフトウェアのアップグレードが必要です。
ルールのアップデートが利用可能	警告	×	アップデートされたルールをダウンロード済みですが、ポリシーに適用されていません。ルールを適用するには、[管理]→[アップデート]→[セキュリティ]に移動し、[ルールアップデート]列で[ルールをポリシーに適用]をクリックします。
不正プログラム対	警告	○	1台以上のコンピュータで、アラートを発するように設定された不正

[1] コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

アラート	初期設定の重要度	消去可能	説明
策アラート			プログラム検索設定によってイベントが発生しました。
不正プログラム対策コンポーネントの障害	重大	○	1台以上のコンピュータで不正プログラム対策コンポーネントの障害が発生しました。詳細については各コンピュータのイベントの説明を参照してください。
不正プログラム対策コンポーネントのアップデート失敗	警告	×	1つ以上のAgentまたはRelayで不正プログラム対策コンポーネントをアップデートできませんでした。詳しくは該当するコンポーネントを参照してください。
不正プログラム対策エンジンがオフライン	重大	×	AgentまたはApplianceが、不正プログラム対策エンジンが応答していないことをレポートしました。コンピュータのシステムイベントを確認して、失敗の原因を特定してください。
不正プログラム対策モジュールで検出ファイル保存用の最大ディスク容量を超過	警告	○	検出ファイルの保存に使用する最大ディスク容量に達したため、不正プログラム対策モジュールでファイルを分析または隔離できませんでした。検出ファイルの設定で最大ディスク容量の設定を変更するには、コンピュータエディタまたはポリシーエディタを開き、[不正プログラム対策]→[詳細] タブに移動してください。
不正プログラム対策保護がないか、期限切れ	警告	×	このコンピュータのAgentは、不正プログラム対策保護の初期設定パッケージを受信していないか、不正プログラム対策保護の期限が切れています。Relayが使用可能であること、およびAgentからRelayへの通信が正しく設定されていることを確認してください。Relayおよびその他のアップデートオプションを設定するには、[管理]→[システム設定]→[アップデート] に移動します。
API キーロックアウト	警告	×	APIキーは、手動でロックアウトできます。また、繰り返し認証に失敗した場合にもロックアウトされます。
アプリケーションコントロールエンジンオフライン	重大	×	エージェントは、アプリケーションコントロールエンジンを初期化できませんでした。コンピュータのシステムイベントを確認して、失敗の原因を特定してください。
アプリケーションコントロールルールセットとAgentのバージョンとの間に互換性がありません	重大	×	アプリケーションコントロールルールセットを1台以上のコンピュータに割り当てることができませんでした。これは、インストールされているAgentのバージョンでこのルールセットがサポートされていないためです。通常、ハッシュベースのルールセットが古いDeep Security Agentに割り当てられていることが問題です。ハッシュベースのルールセットと互換性があるのは、Deep Security Agent 11.0以降のみです。Deep Security Agent 10.xでは、ファイルベースのルールセットのみをサポートしています(詳細については、"Deep Security Agent 10と11におけるファイルの比較方法の相違点" on page 1099を参照してください)。この問題を解決するには、Deep Security Agentをバージョン11.0以降にアップグレードしてください。ローカルルールセットを使用している場合は、Agentのアプリケーションコントロールをリセットする方法もあります。また、共有ルールセットを使用している場合は、共有ルールセットを使用するすべてのAgentをDeep Security Agent 11.0以降にアップグレードするまで、Deep Security 10.xで作成した共有ルールセットを使用します。
アプリケーションの	警告	×	アプリケーションの種類が誤って設定されている場合は、セキュリティ

アラート	初期設定の重要度	消去可能	説明
種類の誤った設定			が正しく適用されない可能性があります。
アプリケーションの種類の推奨設定	警告	○	Deep Security Managerは、コンピュータにアプリケーションタイプを割り当てる必要があると判断しました。この理由としては、新しいコンピュータにAgentがインストールされ、脆弱性のあるアプリケーションが検出されたか、以前は安全であると考えられていたインストール済みアプリケーションが新しい脅威として検出されたことが考えられます。コンピュータにアプリケーションの種類を割り当てるには、[コンピュータの詳細] ダイアログボックスを開き、[侵入防御ルール] をクリックし、アプリケーションの種類を割り当てます。
Azureアカウントがリソース情報を読み取る権限がありません	重大	×	Azureアプリケーションはリソースの読み取りを許可されていないため、Azure CloudアカウントはAzure APIからリソース情報を取得できません。Readerロールがアプリケーションに割り当てられていることを確認してください。
Azureアカウントのパスワードが無効	重大	×	Azureアプリケーションのパスワードが無効なため、Azure CloudアカウントはAzure APIからリソース情報を取得できません。
Azureアカウントのシークレットの有効期限切れ	重大	×	Azureアプリケーションの秘密鍵が期限切れになっているため、Azure CloudアカウントはAzure APIからリソース情報を取得できません。
Microsoft Entra IDアプリケーションが見つかりません	重大	×	Azureアプリケーションが見つからないため、Azure CloudアカウントはAzure APIからリソース情報を取得できません。アプリケーションがMicrosoft Entra IDから削除されている可能性があります。
Microsoft Entra IDアプリケーション証明書の期限切れ	重大	×	アプリケーション証明書の有効期限が切れているため、Microsoft Entra IDアプリケーションはクラウドデータを同期できません。Azureアプリケーション証明書を更新します。
Microsoft Entra IDアプリケーション証明書がまもなく期限切れ	警告	×	Microsoft Entra IDアプリケーション証明書の有効期限がまもなく終了します。Azureアプリケーション証明書を更新します。
Microsoft Entra IDアプリケーションの更新が必要	重大	×	Microsoft Entra IDアプリケーションはクラウドデータを同期できません。アプリのパスワードが期限切れになっているか、アプリが削除された可能性があります。アプリケーションを [コンピュータ]→[プロパティ] (対象のグループを右クリックして表示) から更新してください。> [アプリを今すぐ更新]。
Azureキーペアの期限切れ	重大	×	Azureサービスの鍵のペアが期限切れです。このアラートは、Azureサービスのプロパティページでキーペアをアップデートすることで削除できます。
Azureキーペアがまもなく期限切れ	警告	×	Azureサービスのキーペアはまもなく期限切れになります。このアラートは、Azureサービスのプロパティページでキーペアをアップデートすることで削除できます。
Azureサブスクリプションが見つかり	重大	×	Azureサブスクリプションが見つからないため、Azure CloudアカウントはAzure APIからリソース情報を取得できません。

アラート	初期設定の重要度	消去可能	説明
ません			
Cisco ISE pxGrid証明書の有効期限がもうすぐ切れます	警告	○	ルート証明書および/またはクライアント証明書の有効期限が近づいています。このアラートは有効期限の30日前に発生します。Deep Security Managerユーザは Cisco ISEでこれらの証明書を再生成し、マネージャでpxGrid接続証明書をアップロードまたは置換する必要があります。
Cisco ISE pxGrid証明書の有効期限が切れました	重大	はい	ルートまたはクライアント証明書が既に期限切れです。Deep Security Managerユーザはこれらの証明書をCisco ISEで再生成し、マネージャでpxGrid接続証明書をアップロードまたは置換する必要があります。
Census、Good File Reputation、機械学習型検索サービスへの接続解除	警告	はい	Census、Good File Reputation、機械学習型検索サービスへの接続が解除されました。考えられる解決策については、イベントの詳細を参照してください。 トラブルシューティングのヒントについては、"警告: Census、Good File Reputation、機械学習型検索サービスへの接続解除" on page 1451を参照してください。
ソフトウェア安全性評価サービスがオフライン	警告	×	Deep Security Managerノードは、Trend Micro Certified Safe Software Serviceに接続して整合性監視モジュールのファイル署名比較を実行できません。接続が復旧するまで、ローカルにキャッシュされたデータベースを使用します。Managerノードがインターネット接続されていること、およびプロキシ設定 (ある場合) が正しいことを確認してください。
時計の変更の検出	警告	○	コンピュータで時計の変更が検出されました。時計が予期せず変更された場合は、コンピュータに問題がある可能性があり、アラートを消去する前に調査する必要があります。
クラウドコンピュータがクラウドアカウントで管理されていない	警告	○	Deep Securityと同期されていないクラウドアカウント上の1台以上のコンピュータで、Agentが有効化されています。上記の[処理]フィールドのリンクをクリックして、クラウドアカウントをDeep Securityに追加します。コンピュータはこのアカウントに移行され、より低い時間料金にて課金される可能性があります。
通信の問題の検出	警告	○	コンピュータで通信の問題が検出されました。通信に問題があると、ネットワーク設定またはロードの理由により、Deep Security Managerとの通信をコンピュータで開始できません。システムイベントを確認して、コンピュータからDeep Security Managerへの通信が確立されていることを確認してください。アラートを消去する前に、問題の原因を調査する必要があります。
コンピュータがアップデートを受信していない	警告	×	これらのコンピュータではアップデートの受信を停止しています。手動の操作が必要になる可能性があります。
コンピュータの再	重大	○	Agentソフトウェアのアップデートは正常に完了しましたが、インス

アラート	初期設定の重要度	消去可能	説明
起動が必要			トールを完了するにはコンピュータの再起動が必要です。アラートを消去するには、コンピュータを手動でアップデートする必要があります。
不正プログラム対策保護を完了するためにコンピュータの再起動が必要	重大	×	Agentの不正プログラム対策保護が、コンピュータの再起動が必要であることをレポートしました。コンピュータのシステムイベントを確認して、再起動の理由を特定してください。
アプリケーションコントロール保護に必要なコンピュータの再起動	重大	×	Agentのアプリケーションコントロールによる保護機能により、コンピュータを再起動する必要があることが報告されました。コンピュータのシステムイベントを確認して、再起動の理由を特定してください。
変更監視保護のためのコンピュータの再起動が必要	重大	×	エージェントの変更監視保護により、コンピュータを再起動する必要があることが報告されました。コンピュータのシステムイベントを確認して、再起動の理由を特定してください。
設定が必要	警告	×	1台以上のコンピュータで、複数のインタフェースの種類を定義するポリシーを使用していますが、マッピングされていないインタフェースがあります。
Filter Driverとの接続失敗	重大	×	Filter Driverへの接続に失敗したことがApplianceからレポートされました。ESXiで実行されているFilter Driver、またはApplianceに設定上の問題がある可能性があります。ゲストを保護するには、ApplianceをFilter Driverに接続できる必要があります。問題の原因を調査し、解決してください。
CPUの重大しきい値の超過	重大	×	CPUの重大しきい値を超過しました。
CPUの警告しきい値の超過	警告	×	CPUの警告しきい値を超過しました。
メンテナンスジョブで新しいテーブルパーティションを作成中に重大なデータベースエラーが発生しました	重大	×	データベースの定期的なメンテナンス中に重大なエラーが発生しました。メンテナンス時に、新しいデータに対応するために、新しいパーティションがパーティション表に追加されます。最新のメンテナンスジョブの実行中にエラーが発生しました。つまり、一部のテーブルに今後のパーティションがありません。通常、これらのパーティションに書き込まれる新しいデータが失われる可能性があります。 この問題を解決するために、すぐにサポートプロバイダに連絡してください。(プロセスを円滑に進めるために、Deep Security Managerのルートディレクトリにあるサーバログを準備してください)
重複するコンピュータの検出	警告	○	重複するコンピュータが有効化またはインポートされました。必要に応じて、重複するコンピュータを削除し、元のコンピュータを再有効化してください。

アラート	初期設定の重要度	消去可能	説明
重複する一意のIDの検出	警告	×	重複したUUIDが検出されました。重複したUUIDを削除してください。
空のRelayグループの割り当て	重大	×	これらのコンピュータには空のRelayグループが割り当てられています。コンピュータに別のRelayグループを割り当てるか、空のRelayグループにRelayを追加してください。
イベントの抑制	警告	○	Agent/Applianceで予想外に大量のイベントが発生しました。その結果、潜在的なDoS攻撃を防止するために、1つ以上のイベントが記録されませんでした(抑制されました)。ファイアウォールイベントを調べ、抑制原因を確認してください。
イベントの切り捨て	警告	○	データファイルが大きくなりすぎてAgent/Applianceがイベントを保存できなくなったために、一部のイベントが失われました。これは、生成されるイベントの数が予期せず増加したか、エージェント/アプライアンスがDeep Security Managerにデータを送信できないことが原因である可能性があります。詳細については、コンピュータ上の「イベントの切り捨て」システムイベントのプロパティを参照してください。
ソフトウェアの実行をブロック	警告	○	1台以上のコンピュータでソフトウェアの実行がブロックされました。詳細については、次のコンピュータのアプリケーション制御イベントを参照してください。
SNSメッセージの送信に失敗しました	重大	×	Amazon SNSにメッセージを転送できませんでした
Syslogメッセージの送信に失敗	警告	×	1台以上のSyslogサーバにメッセージを転送できませんでした。
ファイルで不正プログラムを検索できませんでした	警告	×	ファイルパスの長さまたはディレクトリの深さが上限を超えているため、ファイルで不正プログラムを検索できませんでした。コンピュータのシステムイベントを確認して、原因を特定してください。
ファイアウォールエンジンがオフライン	重大	×	Agent/Applianceにより、ファイアウォールエンジンがオフラインであることがレポートされました。Agent/Applianceのエンジンのステータスを確認してください。
ファイアウォールルールアラート	警告	○	1台以上のコンピュータで、アラートを発するように選択されているファイアウォールルールに合致しました。
ファイアウォールルールの推奨	警告	○	Deep Security Managerは、ネットワーク上のコンピュータにファイアウォールルールを割り当てる必要があると判断しました。この理由としては、新しいコンピュータにAgentがインストールされ、脆弱性のあるアプリケーションが検出されたか、以前は安全であると考えられていたインストール済みアプリケーションが新しい脅威として検出されたことが考えられます。コンピュータにファイアウォールルールを割り当てるには、[コンピュータの詳細]ダイアログボックスを開き、[ファイアウォールルール]タブをクリックし、ファイアウォールルールを割り当てます。
ハートビートサーバの失敗	警告	×	ハートビートサーバが正常に起動しませんでした。ポート番号の競合が原因である可能性があります。この問題が解決されるまで、Agent/ApplianceはManagerに接続できません。この問題を解決するには、ハートビートサーバ用に確保されているポート番号が別の

アラート	初期設定の重要度	消去可能	説明
			サービスで使用されていないことを確認し、"Deep Security Managerの再起動" on page 1746してください。ハートビートを使用しない場合は、[アラートの設定] セクションでこのアラートをオフにできます。
非互換のAgent/Applianceバージョン	エラー	×	Deep Security Managerは、管理者のこのバージョンと互換性がありませんコンピュータ上のより最近のエージェント/アプライアンスのバージョンを検出しました。Managerソフトウェアのアップグレードをお勧めします。
ディスク容量の不足	警告	○	Agent/Applianceで、古いログファイルを強制的に削除して新しいログファイル用に空きディスク容量を確保したことがレポートされました。侵入防御、ファイアウォール、およびAgent/Applianceのイベントの消失を防ぐため、必要な空きディスク容量をただちに確保してください。"警告:ディスク容量の不足" on page 1453を参照してください。
変更監視エンジンがオフライン	重大	×	Agent/Applianceが、変更監視エンジンが応答していないことをレポートしました。コンピュータのシステムイベントを確認して、失敗の原因を特定してください。
変更監視情報の収集が遅延しています	警告	×	変更監視データ量が増加したため、変更監視情報を収集する速度が一時的に遅延しています。この間、一部のコンピュータでベースラインと整合性イベントの表示が最新ではなくなる可能性があります。変更監視データに遅延がなくなると、このアラートは自動的に消去されます。
変更監視ルールアラート	警告	○	1台以上のコンピュータで、アラートを発するように選択されている変更監視ルールに合致しました。
変更監視ルールのコンパイルエラー	重大	×	コンピュータで変更監視ルールをコンパイルしているときに、エラーが発生しました。その結果、変更監視ルールが予期したとおりに動作しないことがあります。
変更監視ルールの推奨	警告	○	Deep Security Managerは、ネットワーク上のコンピュータに整合性監視ルールを割り当てる必要があると判断しました。コンピュータに変更監視ルールを割り当てるには、[コンピュータの詳細] ダイアログボックスを開き、[変更監視]→[変更監視ルール] ノードをクリックし、変更監視ルールを割り当てます。
変更監視ルールの設定が必要	警告	×	使用前に設定が必要な変更監視ルールが、1台以上のコンピュータに割り当てられています。このルールはコンピュータに送信されません。詳細については、変更監視ルールのプロパティを開き、[設定] タブを選択してください。
変更監視のTPMが無効です	警告	○	TPMが無効になっています。ハードウェアがインストールされていること、およびBIOSの設定が正しいことを確認してください。
変更監視のTPMのレジスタ値が変更されました	警告	○	TPMのレジスタ値が変更されました。ESXiハイパーバイザの設定を変更していない場合は、攻撃を受けた可能性があります。
侵入防御エンジンがオフライン	重大	×	Agent/Applianceにより、侵入防御エンジンがオフラインであることがレポートされました。Agent/Applianceのエンジンのステータスを確認してください。

アラート	初期設定の重要度	消去可能	説明
侵入防御ルールアラート	警告	○	1台以上のコンピュータで、アラートを発するように設定されている侵入防御ルールに合致しました。
侵入防御ルールのコンパイルに失敗しました	重大	○	これは通常、侵入防御ルールの設定が間違っていることが原因です。ルール名はイベントの[プロパティ]画面で確認できます。この問題を解決するには、ルールを特定して割り当て解除するか、トレンドマイクロのサポートにお問い合わせください。
侵入防御ルールの設定が必要	警告	×	使用前に設定が必要な侵入防御ルールが、1台以上のコンピュータに割り当てられています。このルールはコンピュータに送信されません。詳細については、侵入防御ルールのプロパティを開き、[設定]タブを選択してください。
無効なシステム設定を検出	重大	×	Deep Security Managerが1つ以上のシステム設定に対して無効な値を検出しました。
IoTイベントが過負荷です	警告	×	IoTイベントは時間内に処理できません。大量のイベントを生成するコンピュータがあるか、いくつかのルールが誤って設定されている可能性があります。
レガシーのAgentソフトウェアが検出されました	警告	○	バージョンが9.5未満の現在サポートされていないソフトウェアが検出されました。最新のソフトウェアをインポートして置き換えてください。 詳細については、"Deep Security Agentソフトウェアの入手" on page 514を参照してください。
セキュリティログ監視エンジンがオフライン	重大	×	Agent/Applianceにより、セキュリティログ監視エンジンの初期化に失敗したことがレポートされました。コンピュータのシステムイベントを確認して、失敗の原因を特定してください。
セキュリティログ監視ルールアラート	警告	○	1台以上のコンピュータで、アラートを発するように設定されているセキュリティログ監視ルールに合致しました。
セキュリティログ監視ルールの推奨	警告	○	Deep Security Managerは、ネットワーク上のコンピュータにログ検査ルールを割り当てる必要があると判断しました。コンピュータにセキュリティログ監視ルールを割り当てるには、[コンピュータの詳細]ダイアログボックスを開き、[セキュリティログ監視]→[セキュリティログ監視ルール]ノードをクリックし、セキュリティログ監視ルールを割り当てます。
セキュリティログ監視ルールに設定が必要	警告	×	使用前に設定が必要なセキュリティログ監視ルールが、1台以上のコンピュータに割り当てられています。このルールはコンピュータに送信されません。詳細については、セキュリティログ監視ルールのプロパティを開き、[設定]タブを選択してください。
ディスク容量不足	警告	×	Deep Security Managerノードのディスク空き容量が10%未満です。古いファイルや不要なファイルを削除して空き容量を増やすか、ストレージ容量を追加してください。
メンテナンスモード- オン	警告	×	1台以上のコンピュータで、アプリケーションコントロールのメンテナンスモードが有効になっています。このモードを有効にすると、ブロックルールは引き続き適用されますが(承認されていないソフトウェアを

アラート	初期設定の重要度	消去可能	説明
			明示的に許可するまでブロックを選択した場合)、ソフトウェアアップデートは許可され、その後自動的にルールセットのインベントリ部分に追加されます。各コンピュータでソフトウェアのアップデートが終了したら、承認されていないソフトウェアが誤ってルールセットに追加されないように、メンテナンスモードを無効にしてください。
Managerがオフライン	警告	×	Deep Security Managerノードはオフラインです。理由としては、コンピュータでハードウェアまたはソフトウェアの問題が発生したか、単純にネットワーク接続が切断されたことが考えられます。Managerのコンピュータのステータスを確認してください。
Managerの時刻が非同期	重大	×	各Managerノードの時計はデータベースの時計と同期されている必要があります。時計間の時刻の差が30秒を超える場合、Managerノードのタスクは正常に実行されません。Managerノードの時計をデータベースの時計と同期してください。
メモリの重大しきい値の超過	重大	×	メモリの重大しきい値を超過しました。
メモリの警告しきい値の超過	警告	×	メモリの警告しきい値を超過しました。
移行失敗	警告	○	接続に問題があるため、コンピュータはTrend Cloud One - Endpoint & Workload Securityに移動されませんでした。 移動を再試行する前に: • テナント情報、アクティベーショントークン、公開CA証明書、プロキシ設定など、移動に指定されたすべてのパラメータが正しいことを確認します。 • エージェントがTrend Cloud One - Endpoint & Workload Securityにアクセスするのを妨げるネットワーク/ファイアウォール設定がないことを確認します。 • CLIを使用して、失敗した移動に関する情報を含むds_agent.logファイルを含むエージェント診断パッケージを作成します。診断パッケージの作成手順については、「診断パッケージの作成とログ記録」を参照してください。
移行失敗: 応答がありません	警告	○	移動要求がタイムアウトしたため、コンピュータはTrend Cloud One - Endpoint & Workload Securityに移動されませんでした。 Managerからのアクティベーションを使用している場合、Managerがコマンドを開始した後にエージェントからの応答がありませんでした。 Agentからの有効化を使用している場合は、エージェントからの

アラート	初期設定の重要度	消去可能	説明
			ハートビートがありません。 エージェントのステータスを確認して、再度移動してください。
移行失敗: 有効化に失敗しました	警告	○	Trend Cloud One - Endpoint & Workload Security への移行は、アクティベーションの問題が原因で失敗し、ロールバックされました。 移動を再試行する前に: • テナント情報、アクティベーショントークン、公開CA証明書、プロキシ設定など、移動に指定されたすべてのパラメータが正しいことを確認します。 • CLIを使用してエージェント診断パッケージを作成します。このパッケージには、失敗した移動に関する情報を含むdsa_move.logおよびdsa_control.logファイルが含まれます。診断パッケージの作成手順については、「診断パッケージの作成とログ記録」を参照してください。
移行失敗: 非管理対象です	重大	○	Trend Cloud One - Endpoint & Workload Security への移行は、アクティベーションの問題が原因で失敗しました。移行をロールバックできませんでした。コンピュータが管理対象外の状態です。 この問題のトラブルシューティングを行うには、次の手順を実行します。 • 失敗した移動に関する情報を含むdsa_move.logファイルを調べます。 • エージェントを手動で復元するか、エージェントを再有効化してください。詳細については、トラブルシューティングのセクションを参照してください。 移動を再試行する前に: • Workload Security Linkが最新であることを確認します。 • テナント情報、アクティベーショントークン、公開CA証明書、プロキシ設定など、移動に指定されたすべてのパラメータが正しいことを確認します。
ネットワークエンジンモードの非互	警告	×	「ネットワークエンジンモード」を「タップ」に設定できるのは、Agent

アラート	初期設定の重要度	消去可能	説明
換性			バージョン5.2以降のみです。互換性の問題を解決するには、Agentの設定を確認してアップデートするか、Agentをアップグレードしてください。
新しいパターンファイルアップデートがダウンロード済みで利用可能	警告	×	セキュリティアップデートの一部として、新しいパターンファイルを利用できます。パターンファイルはDeep Securityにダウンロードされていますが、まだコンピュータに適用されていません。コンピュータにアップデートを適用するには、[管理]→[アップデート]→[セキュリティ]画面に移動してください。
新しいルールアップデートがダウンロード済みで利用可能	警告	×	セキュリティアップデートの一部として、新しいルールを利用できます。ルールはDeep Securityにダウンロードされていますが、まだポリシーに適用されておらず、コンピュータに送信されていません。アップデートを適用し、更新されたポリシーをコンピュータに送信するには、[管理]→[アップデート]→[セキュリティ]画面に移動してください。
新しいバージョンのDeep Security Managerが利用可能	警告	×	Deep Security Managerの新しいバージョンを使用できます。トレンドマイクロのダウンロードセンター(https://help.deepsecurity.trendmicro.com/ja-jp/software.html)から最新バージョンをダウンロードしてください。
新しいバージョンのソフトウェアが利用可能	警告	×	新しいソフトウェアを利用できます。ダウンロードセンターからソフトウェアをダウンロードできます。
コンピュータ数がデータベースの上限を超過	警告	×	有効化されたコンピュータの数が、組み込みデータベースに対して推奨される上限を超過しています。さらにコンピュータが追加された場合はパフォーマンスの急速な低下が発生するため、現時点で他のデータベースオプション(OracleまたはSQL Server)を検討することを強くお勧めします。
保護モジュールライセンスが期限切れ	警告	○	保護モジュールライセンスが有効期限切れになりました。
保護モジュールライセンスがまもなく期限切れ	警告	×	保護モジュールライセンスはまもなく有効期限切れになります。このアラートは、[管理]→[ライセンス]画面でライセンスを変更すると削除されます。
推奨設定	警告	○	Deep Security Managerは、いずれかのコンピュータのセキュリティ設定をアップデートする必要があると判断しました。推奨されている変更点を確認するには、**コンピュータエディタ**[1]を開き、モジュールの画面で未解決の推奨設定に関する警告を確認してください。割り当て済みのルールのリストで、[割り当て/割り当て解除]をクリックして使用可能なルールのリストを表示してから、[割り当てに推奨される設定の表示]フィルタオプションを使用してフィルタします(安全に割り当てを解除できるルールを表示するには、[割り当て解除に推奨される設定の表示]を選択します)。

[1] コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

アラート	初期設定の重要度	消去可能	説明
攻撃の予兆の検出: OSのフィンガープリント調査	警告	○	AgentまたはApplianceは、「フィンガープリント」調査によってコンピュータのOSを識別しようとする動作を検出しました。これは特定の脆弱性に対する攻撃の前によく見られるアクティビティです。調査の詳細については、コンピュータのイベントを確認し、"警告: 攻撃の予兆の検出" on page 1453を参照してください。
攻撃の予兆の検出: ネットワークまたはポートの検索	警告	○	AgentまたはApplianceが、ネットワークまたはポート検索特有のネットワークアクティビティを検出しました。これは特定の脆弱性に対する攻撃の前によく見られるアクティビティです。調査の詳細については、コンピュータのイベントを確認し、"警告: 攻撃の予兆の検出" on page 1453を参照してください。
攻撃の予兆の検出: TCP Null検索	警告	○	AgentまたはApplianceで、TCP「null」の検索を検出しました。これは特定の脆弱性に対する攻撃の前によく見られるアクティビティです。調査の詳細については、コンピュータのイベントを確認し、"警告: 攻撃の予兆の検出" on page 1453を参照してください。
攻撃の予兆の検出: TCP SYNFIN検索	警告	○	AgentまたはApplianceで、TCP「SYNFIN」の検索を検出しました。これは特定の脆弱性に対する攻撃の前によく見られるアクティビティです。調査の詳細については、コンピュータのイベントを確認し、"警告: 攻撃の予兆の検出" on page 1453を参照してください。
攻撃の予兆の検出: TCP Xmas検索	警告	○	AgentまたはApplianceで、TCP「Xmas」の検索を検出しました。これは特定の脆弱性に対する攻撃の前によく見られるアクティビティです。調査の詳細については、コンピュータのイベントを確認し、"警告: 攻撃の予兆の検出" on page 1453を参照してください。
Agent整合性チェックのためにRelayのアップグレードが必要	警告	×	Agent整合性チェックを有効にするには、Relayをアップグレードしてください。
SAMLアイデンティティプロバイダ証明書の期限が切れました	重大	×	1つ以上のSAML IDプロバイダ証明書の期限が切れました。
SAMLアイデンティティプロバイダ証明書がまもなく期限切れになります	警告	×	1つ以上のSAMLアイデンティティプロバイダ証明書がまもなく期限切れになります。
SAMLサービス証明書の有効期限が切れています	重大	×	SAMLサービスプロバイダ証明書の有効期限が切れています。
SAMLサービス証明書の有効期限が間もなく終了します	警告	×	SAMLサービスプロバイダ証明書がまもなく期限切れになります。
SAPウイルス検	重大	×	Agentにより、SAPウイルス検索アダプタがインストールされていない

アラート	初期設定の重要度	消去可能	説明
索アダプタがインストールされていません			ことがレポートされました。コンピュータのシステムイベントを確認して、失敗の原因を特定してください。
SAPウイルス検索アダプタが最新ではありません	重大	×	Agentにより、SAPウイルス検索アダプタが最新でないことがレポートされました。コンピュータのシステムイベントを確認して、失敗の原因を特定してください。
不正プログラムの予約検索がスキップされました	警告	×	保留中の予約検索タスクがあるコンピュータで、不正プログラムの予約検索が開始されました。検索の頻度が高すぎる可能性があります。検索の頻度を低くするか、予約検索時に検索するコンピュータの台数を減らすことを検討してください。
ポリシー送信の失敗	重大	×	ポリシーを送信できない場合は、Agent/Applianceに問題がある可能性があります。該当するコンピュータを確認してください。
Smart Protection Serverとの接続失敗	警告	○	Smart Protection Serverへの接続に失敗しました。これは、設定の問題またはネットワーク接続が原因である可能性があります。
ソフトウェア変更を検出	警告	×	実行中のファイルシステム監視で、新しいソフトウェアがインストールされたこと、およびそのソフトウェアが設定されている許可またはブロックルールと一致しなかったことが、アプリケーションコントロールによって検出されました。システム管理者がソフトウェアをインストールしておらず、また他のユーザにソフトウェアのインストール権限が与えられていない場合は、セキュリティ侵害の可能性があります。ソフトウェアが起動を試みた場合、実行が許可されるかどうかはその時点でのロックダウン設定によって決まります。
ソフトウェアパッケージが見つからない	重大	×	1台以上のVirtual Applianceで、操作を正常に実行するためにAgentソフトウェアパッケージが必要です。各Applianceに対応するバージョンのRed Hat Enterprise Linux 6 (64ビット) Agentソフトウェアパッケージをインポートしてください。必要なバージョンを入手できない場合は、最新パッケージをインポートし、そのバージョンに合わせてApplianceをアップグレードしてください。
ソフトウェアアップデートをインポート可能	警告	×	新しいソフトウェアを利用できます。新しいソフトウェアをDeep Securityにインポートするには、[管理]→[アップデート]→[ソフトウェア]→[ダウンロードセンター]に移動します。
通信不能	重大	×	Deep Security Managerは、設定された期間内にエージェント/アプライアンスのステータスを検索できませんでした。ネットワーク設定と該当するコンピュータの接続を確認してください。
Agentソフトウェアのアップグレード失敗	警告	○	Deep Security Managerは、コンピュータ上のエージェントソフトウェアをアップグレードできませんでした。 Agent/Applianceに問題がある可能性もありますが、Agentセルフプ

アラート	初期設定の重要度	消去可能	説明
			ロテクションが有効になっている場合にもこのエラーが発生します。Deep Security Managerで、コンピュータエディタ[1]→[設定]→[一般]の順に選択します。[Agentセルフプロテクション] で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否] の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。
未解決のソフトウェア変更数の上限に達しました	重大	×	ファイルシステムで検出されたソフトウェア変更数が上限を超えました。アプリケーションコントロールは引き続き既存のルールを適用しますが、これ以上の変更は記録されず、このコンピュータでのソフトウェアの変更は表示されなくなります。この状況を解決し、大量のソフトウェア変更が発生しないようにする必要があります。
Deep Security Managerソフトウェアのアップグレード推奨 (非互換のセキュリティアップデート)	警告	×	Deep Security Managerは、Deep Security Managerの現在のバージョンと互換性のないセキュリティアップデートを使用しているコンピュータを検出しました。Deep Security Managerソフトウェアのアップグレードをお勧めします。
ユーザのロックアウト	警告	×	ユーザは手動で、不正ログオンが繰り返し試行された場合、ユーザのパスワードの期限が切れた場合、またはインポートされたもののロック解除されていない場合、ロックアウトされることがあります。
ユーザパスワードがまもなく有効期限切れ	警告	×	パスワードの有効期限の設定が有効になっており、7日以内にパスワードが期限切れになるユーザが1人以上います。
Virtual ApplianceとFilter Driverの互換性なし	警告	×	ApplianceがFilter Driverと互換性がありません。両方とも最新バージョンにアップグレードされていることを確認してください。
仮想マシンインタフェースの非同期	警告	×	Deep Security Virtual Applianceによって監視されている1つ以上の仮想マシンで、インタフェースがFilter Driverと同期していないことがレポートされました。これは、Applianceが仮想マシンのインタフェースを適切に監視していない可能性があることを意味しています。問題を解決するには、設定の変更や再起動などの手動操作を仮想マシンで実行しなければならないことがあります。
保護されていないESXiサーバへの仮想マシンの移動	警告	○	有効化されたDeep Security Virtual ApplianceがないESXiサーバに、仮想マシンが移動されました。
別のESXiへの移	警告	○	Applianceで保護されている仮想マシンが、別のESXiへの移動中

[1] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

アラート	初期設定の重要度	消去可能	説明
動後に仮想マシンが保護されていない			または移動後に、保護されていませんでした。移動中にApplianceが再起動したか、電源がオフになったか、あるいは設定に問題がある可能性があります。アラートを消去する前に、問題の原因を調査する必要があります。
VMware Toolsがインストールされていない	重大	○	NSX環境内の保護されている仮想マシンにVMware Toolsがインストールされていない。NSX環境で仮想マシンを保護するにはVMware Toolsが必要です。
Webレピュテーションイベントアラート	警告	○	アラートを発するように設定されている1台以上のコンピュータで、Webレピュテーションイベントが発生しました。
AWSアカウントで無効にされたWorkSpaces	警告	○	Agentが1つ以上のAmazon WorkSpacesで稼働していますが、WorkSpacesが自身のAWSアカウントで無効に設定されています。WorkSpacesを有効にするには、上記の [AWSアカウントの編集] をクリックして、[Amazon WorkSpacesを含める] チェックボックスをオンにします。WorkSpacesがAWSアカウントのWorkSpacesフォルダに移動し。

次の表には、アラートとそれに対応するアラートメールの件名が一覧表示されています。

警告	アラートメール件名
CPUのクリティカルしきい値を超えました	マネージャノード({1}) のCPUクリティカルしきい値が超えました
CPU警告閾値を超えました	マネージャノード({1}) のCPU警告閾値が超えました
DSRU推奨	DSRU 推奨
レガシーエージェントソフトウェアが検出されました	レガシーエージェントソフトウェアが検出されました
ユーザがロックアウトされました	{0}ユーザがロックアウトされました
ユーザパスワードの有効期限が近づいています	{0}人のユーザのパスワードがまもなく期限切れになります
異常な再起動が検出されました	{0}台のコンピュータで異常な再起動が検出されました
時計の変更が検出されました	{0}台のコンピュータで時計の変更が検出されました

警告	アラートメール件名
通信の問題が検出されました	{0}台のコンピュータで通信の問題が検出されました
イベントが切り捨てられました	イベントは{0}台のコンピュータで切り捨てられました
エージェントハートビート公開サーバ証明書の有効期限が切れました	エージェントハートビート公開サーバ証明書の有効期限が切れました
エージェントハートビートパブリックサーバ証明書の有効期限が間もなく切れます	エージェントハートビート公開サーバ証明書の有効期限が間もなく切れます
エージェントのインストールに失敗しました	エージェントのインストールが{0}台のコンピュータで失敗しました
ディスク容量不足	{0}台のコンピュータでディスク容量が不足しています
イベントが抑制されました	{0}台のコンピュータでイベントが抑制されました
通信できません	{0}台のコンピュータと通信できません
Deep Security Relayはセキュリティコンポーネントをダウンロードできません	{0}個のRelayでセキュリティコンポーネントを更新できません
エージェントソフトウェアをアップグレードできません	{0}台のコンピュータでエージェントソフトウェアをアップグレードできません
互換性のないエージェント/アプライアンスバージョン	{0}台のコンピュータで互換性のないエージェント/アプライアンスのバージョンが検出されました
エージェント/アプライアンスのアップグレードを推奨 (新しいバージョンが利用可能)	1台以上のコンピューターでエージェント/アプライアンスソフトウェアのアップグレードを推奨します
エージェントのアップグレードを推奨 (アプライアンスと互換性がありません)	エージェントソフトウェアのアップグレードは、アプライアンスと保護を調整するために{0}台のコンピュータで推奨されます
エージェント/アプライアンスのアップグレードを推奨 (互換性のないセキュリティ更新)	割り当てられたセキュリティアップデートをサポートするために、{0}台のコンピュータでエージェント/アプライアンスソフトウェアのアップグレードを推奨します

警告	アラートメール件名
エージェント/アプライアンスのアップグレードが必要です	{0}台のコンピュータでエージェント/アプライアンスソフトウェアのアップグレードが必要です
エージェント/アプライアンスのアップグレードを推奨	{0}台のコンピュータでエージェント/アプライアンスのアップグレードを推奨します
新しいパターン更新がダウンロードされ、利用可能です	{0}エージェント/アプライアンスの新しいパターン更新が利用可能です
AWSアカウントの移行に失敗しました	AWSアカウントの移行に失敗しました
AWSアカウントのWorkSpacesが無効になっています	AWSアカウントでWorkSpacesが無効になっています
APIキーがロックされました	{0} APIキーがロックされました
フィルタードライバーへの接続失敗	フィルタードライバーへの接続失敗
ソフトウェアパッケージが見つかりません	ソフトウェアパッケージが見つかりません
Microsoft Entra IDアプリケーション証明書の有効期限が切れました	{0}個のAzureサービス用Microsoft Entra IDアプリケーションの有効期限が切れました
Microsoft Entra IDアプリケーション証明書の有効期限が間もなく切れます	{0}Azureサービス用のMicrosoft Entra IDアプリケーション証明書がまもなく期限切れになります
Microsoft Entra IDアプリケーションの更新が必要です	{0}個のAzureサービス用Microsoft Entra IDアプリケーションの更新が必要です
Azureアカウントにリソース情報を読み取る権限がありません	{0}個のAzureクラウドアカウントに対するMicrosoft Entra IDアプリケーションには読み取り権限がありません
Microsoft Entra IDアプリケーションが見つかりません	{0}個のAzureクラウドアカウントに対するMicrosoft Entra IDアプリケーションが見つかりません
Microsoft Entra IDアプリケーションパスワードの有効期限が間もなく切れます	{0}AzureサービスのMicrosoft Entra IDアプリケーションパスワードの有効期限が間もなく切れます

警告	アラートメール件名
Azureアカウントのシークレットが期限切れ	{0}個のAzureクラウドアカウントのMicrosoft Entra IDアプリケーションシークレットキーの有効期限が切れました
Azureアカウントのパスワードが無効です	{0}のAzureクラウドアカウントに対するMicrosoft Entra IDアプリケーションシークレットが無効です
Azureサブスクリプションが見つかりません	{0}個のAzureクラウドアカウントに対するAzureサブスクリプションが見つかりません
Azureキーのペアが期限切れ	{0}のAzureサービスのキーペアの有効期限が切れました
Azureキーのペアがまもなく期限切れ	{0}のAzureサービス用のキーペアがまもなく期限切れになります
Census、ファイルレピュテーション、機械学習型検索サービスが切断されました	Census、ファイルレピュテーション、および機械学習型検索サービスから切断されました
クラウドアカウントの一部として管理されていないクラウドコンピュータ	{0}台のコンピュータはクラウド環境にありますが、クラウドアカウントの一部として管理されていません
重複したコンピュータが検出されました	{0}の重複したコンピュータが検出されました
重複した一意識別子が検出されました	{0}の重複する一意識別子が検出されました
フィルタードライバーのアップグレードを推奨 (新しいバージョンが利用可能)	フィルタードライバーのアップグレードは、最新機能を活用するために{0}台のESXiサーバで推奨されます
ハートビートサーバが失敗しました	ハートビートサーバがマネージャノード ({1}) で起動に失敗しました
構成が必要です	{0}コンピュータでの設定が必要です
コンピュータが更新を受信していません	{0}コンピュータが更新を受信していません
Deep Security Agent保護を有効にするためにコンピュータの再起動が必要	Deep Security Agent保護を有効にするためにコンピュータの再起動が必要

警告	アラートメール件名
無効なシステム設定が検出されました	無効なシステム設定が検出されました
MQTT接続がオフライン	MQTT接続が{0}台のコンピュータでオフラインです
MQTT接続構成に失敗しました	MQTT接続構成が{0}台のコンピュータで失敗しました
保護モジュールのライセンスが期限切れです	{1}のライセンスが期限切れになりました
保護モジュールのライセンスがまもなく期限切れ	{1}のライセンスが ({2}) に期限切れになります
ディスク容量が低	マネージャノード ({1}) のディスク容量が低です
マネージャオフライン	マネージャノード ({1}) はオフラインです
マネージャの時間が同期していません	マネージャノード ({1}) の時計がデータベースの時計と同期していません
Workload Securityマネージャソフトウェアのアップグレードを推奨 (互換性のないセキュリティアップデート)	Workload Securityマネージャソフトウェアのアップグレードをお勧めします。現在のWorkload Securityマネージャバージョンと互換性のないセキュリティアップデートが割り当てられているコンピュータが{0}台あります
メモリの重要な閾値を超えました	マネージャノード ({1}) のメモリクリティカル閾値が超えました
メモリ警告閾値を超えました	マネージャノード ({1}) のメモリ警告閾値が超過しました
仮想マシンが無保護のESXiサーバに移動されました	保護されたESXiサーバから保護されていないESXiサーバに仮想マシンが移動されました
複数のアクティブ化されたアプライアンスが検出されました	複数の有効化されたアプライアンスが検出されました
新しいバージョンのソフトウェアが利用可能です	新しいバージョンのソフトウェアが利用可能です
Workload Securityマネージャの新しいバージョンが利用可能です	Workload Securityマネージャの新しいバージョンが利用可能です

警告	アラートメール件名
コンピュータの数がデータベースの制限を超えています	埋め込みデータベースの推奨制限を超えるコンピュータの数
コンピュータの数がライセンスを超えています	許可されたコンピュータの数を超えています
マネージャノードの数がライセンスを超えています	マネージャノードの数が許可されている{3}ライセンスマネージャを超えています
メンテナンスジョブ中に新しいテーブルパーティションを作成する際に重大なデータベースエラーが発生しました	メンテナンスジョブ中に新しいテーブルパーティションを作成する際に重大なデータベースエラーが発生しました
推奨	{0}台のコンピュータに対して推奨設定が行われました
エージェントの整合性チェックにはRelayのアップグレードが必要です	エージェント整合性チェックを有効にするには、Relayをアップグレードしてください
SAMLアイデンティティプロバイダ証明書の有効期限が切れました	{0} SAMLアイデンティティプロバイダ証明書の有効期限が切れました
SAMLアイデンティティプロバイダ証明書の有効期限が間もなく切れます	{0} SAMLアイデンティティプロバイダ証明書の有効期限が間もなく切れます
SAMLサービスプロバイダ証明書の有効期限が切れました	SAMLサービスプロバイダ証明書の有効期限が切れました
SAMLサービスプロバイダ証明書の有効期限が間もなく切れます	SAMLサービスプロバイダ証明書の有効期限が近づいています
SNSメッセージの送信に失敗しました	Amazon SNSへのメッセージ転送ができません
インポート可能なソフトウェア更新	ソフトウェアの更新がダウンロード可能です
Syslogメッセージの送信に失敗しました	{0} Syslogサーバにメッセージを転送できません

警告	アラートメール件名
アクティベーションに失敗しました	{0}台のコンピュータをアクティベートできませんでした
ポリシーの送信に失敗しました	{0}台のコンピュータへのポリシーの送信に失敗しました
別のESXiに移動後の仮想マシンが未保護	別のESXiに移動後、仮想マシンが保護されていません
VMware Toolsがインストールされていません	VMware Toolsがインストールされていません
ルールの更新が利用可能です	ルールの更新が利用可能です
新しいルールの更新がダウンロードされ、利用可能です	新しいルールの更新が適用されていません
不正プログラム対策アラート	不正プログラム検索設定 ({1}) が{0}台のコンピュータで警告
侵入防御ルールアラート	侵入防御ルール ({1}) が{0}台のコンピュータで警告を発しました
アクティビティ監視でコンピュータの再起動が必要	アクティビティモニタリングでコンピュータの再起動が必要
エージェントは不正プログラム対策の許可が必要です	{0}台のコンピュータ上のエージェントが不正プログラム対策の許可を必要としています
不正プログラム対策エンジンがオフライン	{0}不正プログラム対策エンジンがオフライン
スケジュールされた不正プログラム検索が未実施	スケジュールされた不正プログラム検索が{0}台のコンピュータで実行されませんでした
不正プログラム対策保護が存在しないか、または最新ではありません	{0}台のコンピュータ上のエージェントに最新の不正プログラム対策の更新を適用する
不正プログラム対策モジュールで識別されたファイルを保存するために使用されるディスク容量が最大値を超えました	不正プログラム対策モジュールが識別されたファイルを保存するために使用するディスク容量の上限を超えました
不正プログラム対策保護でコン	不正プログラム対策保護でコンピュータの再起動が必要

警告	アラートメール件名
ピュータの再起動が必要	
ファイルを不正プログラムのスキャンができませんでした	{0}エージェント/アプライアンス上のファイルを不正プログラムのスキャンができませんでした
Smart Protection Server接続失敗	Smart Protection Serverに接続できませんでした
不正プログラム対策コンポーネントの障害	{0}台のコンピュータで不正プログラム対策コンポーネントの障害が発生しました
不正プログラム対策コンポーネントの更新に失敗しました	{0}台のコンピュータで不正プログラム対策コンポーネントの更新に失敗しました
Webレピュテーションイベントアラート	{0}台のコンピュータでWebレピュテーションイベントアラートが発生しました
侵入防御ファイアウォールサーバープラグインライセンスが期限切れになったか、まもなく期限切れになります	侵入防御ファイアウォールサーバープラグインのライセンスが期限切れです ({2})
エージェント/アプライアンスのアップグレードを推奨 (互換性のないコンポーネントの更新)	割り当てられたコンポーネントの更新をサポートするために、{0}台のコンピュータでエージェント/アプライアンスソフトウェアのアップグレードを推奨します
Container Control認証プラグインのリクエスト解析に失敗しました	Container Control認証プラグインはリクエストを解析できませんでした。これはDockerバージョンの非互換性が原因である可能性があります。サポートされているDockerバージョンを使用していることを確認してください。
Container Control認証プラグインのDockerへの接続に失敗しました	Container Control認証プラグインがDockerに接続できません。Container Controlモジュールを一度オフにしてから再度オンにしてみてください。
コンテナコントロール認証プラグインのインストールに失敗しました	Container Control認証プラグインがインストールされていません。Container Controlモジュールを一度オフにしてから再度オンにしてみてください。
Container Control認証プラグインが設定の送信に失敗しました	コンテナコントロール認証プラグインが設定の送信に失敗しました。コンテナコントロールモジュールを一度オフにしてから再度オンにしてみてください。

警告	アラートメール件名
セキュリティログ監視エンジンがオフライン	{0}セキュリティログ監視エンジンがオフラインです
セキュリティログ監視ルールアラート	セキュリティログ監視ルール ({1}) が{0}コンピュータでアラートを発生
セキュリティログ監視ルールは設定が必要です	セキュリティログ監視ルール ({1}) は{0}台のコンピュータでの設定が必要です
セキュリティログ監視ルールの推奨	セキュリティログ監視ルール ({1}) は{0}台のコンピュータで推奨されます
SAPウイルス検索サービスが正しく動作していません	{0} SAPウイルス検索サービスが正しく動作していません
SAPウイルス検索アダプタがインストールされていません	{0} SAPウイルス検索アダプタがインストールされていません
SAPウイルス検索アダプタが最新ではありません	{0} SAPウイルス検索アダプターが最新ではありません
ソフトウェアの実行をブロック	{0}台の{0,choice,1#コンピュータ|2#コンピュータ}でソフトウェアの実行がブロックされました
未解決のソフトウェア変更数の上限に達しました	{0}台の{0,choice,1#コンピュータ|2#コンピュータ}で未解決のソフトウェア変更数の上限に達しました。
アプリケーションコントロールエンジンオフライン	{0}個のアプリケーションコントロール{0,choice,1#エンジン|2#エンジン}がオフラインです
アプリケーションコントロールルールセットとAgentのバージョンとの間に互換性がありません	アプリケーションコントロールルールセットと、{0}{0,choice,1#台のコンピュータ|2#台のコンピュータ}のAgentのバージョンとの間に互換性がありません
メンテナンスモード- オン	{0}台の{0,choice,1#コンピュータ|2#コンピュータ}でメンテナンスモードが有効になっています
アプリケーションコントロール保護でコンピュータの再起動が必要	アプリケーションコントロール保護でコンピュータの再起動が必要
ソフトウェア変更を検出	{0}台の{0,choice,1#コンピュータ

警告	アラートメール件名
AWS契約ライセンス超過	AWS契約ライセンス超過
AWS SaaS課金が正しく構成されていません	AWS SaaS課金が正しく構成されていません
ライセンスの有効期限が切れました	ライセンスの有効期限が切れました
ライセンスの有効期限が近づいています	ライセンスの有効期限が近づいています
ライセンスシートの上限を超えました	ライセンスシートの上限を超えました
ライセンスシートの上限にほぼ達しました	ライセンスシートの上限にほぼ達しました
アカウント残高が不足しています	アカウント残高が不足しています
アカウント残高低	アカウント残高低
変更監視情報の収集が遅れています	変更監視情報の収集が遅れています
変更監視エンジン - オフライン	{0}変更監視エンジンがオフラインです
ソフトウェア安全性評価サービスオフライン	マネージャノード({1})はソフトウェア安全性評価サービスに接続できません
変更監視保護でコンピュータの再起動が必要	変更監視保護でコンピュータの再起動が必要
変更監視ルールアラート	変更監視ルール({1})が{0}台のコンピュータに対して警告を発しました
変更監視ルールコンパイルエラー	{0}台のコンピュータで変更監視ルールのコンパイルエラーが発生しました
変更監視ルールは設定が必要です	変更監視ルール({1})は{0}台のコンピュータでの設定が必要です

警告	アラートメール件名
変更監視のトラステッドプラットフォームモジュールが有効になっていません	変更監視のトラステッドプラットフォームモジュールが有効になっていません
変更監視 トラステッドプラットフォームモジュールのレジスタ値が変更されました	変更監視 トラステッドプラットフォームモジュールのレジスタ値が変更されました
変更監視ルールの推奨	変更監視ルール ({1}) は{0}台のコンピュータで推奨されます
エージェント構成パッケージが大きすぎます	{0}台のコンピュータでエージェント構成パッケージが大きすぎます
侵入防御ルールのコンパイルに失敗しました	侵入防御ルールのコンパイルが{0}台のコンピュータで失敗しました
攻撃の予兆を検出: コンピュータOSフィンガープリントプローブ	攻撃の予兆検出: {0}台のコンピュータでOSフィンガープリントプローブ
攻撃の予兆を検出: TCP Null検索	攻撃の予兆を検出: TCP「Null」検索が{0}台のコンピュータで行われました
攻撃の予兆検出: ネットワークまたはポート検索	攻撃の予兆を検出: ネットワークまたはポート検索が{0}コンピュータで行われました
攻撃の予兆検出: TCP SYNFIN検索	攻撃の予兆検出: TCP "SYNFIN"検索が{0}台のコンピュータで行われました
攻撃の予兆を検出: TCP Xmas検索	攻撃の予兆を検出: TCP "Xmas"検索が{0}台のコンピュータで行われました
アプリケーションタイプの誤設定	{0}台のコンピュータにアプリケーションタイプの誤設定があります
ネットワークエンジンモードの非互換性	{0}エージェントはネットワークエンジンモードを実装できません
ファイアウォールエンジンオフライン	{0}ファイアウォールエンジンがオフライン
ファイアウォールルールアラート	ファイアウォールルール ({1}) が{0}台のコンピュータで警告

警告	アラートメール件名
侵入防御エンジンがオフライン	{0}侵入防御エンジンがオフラインです
侵入防御ルールアラート	侵入防御ルール ({1}) が{0}台のコンピュータで警告を発しました
侵入防御ルールには設定が必要です	侵入防御ルール ({1}) は{0}台のコンピュータでの設定が必要です
アプリケーションタイプの推奨	アプリケーションタイプ ({1}) は{0}台のコンピュータで推奨されます
ファイアウォールルールの推奨	ファイアウォールルール ({1}) は{0}コンピュータで推奨されます
侵入防御ルールの推奨	侵入防御ルール ({1}) は{0}台のコンピュータで推奨されます
侵入防御ルール削除の推奨	侵入防御ルール ({1}) は、{0}台のコンピュータからの削除を推奨します
仮想マシンインターフェイスの同期が取れていません	仮想マシンインターフェイスの同期が取れていません
AWS認証情報が間違っています	{0}アカウントのAWS資格情報が間違っています
Virtual Applianceはフィルタードライバーと互換性がありません	{0}個のVirtual Applianceでフィルタードライバーとの非互換性が検出されました
空のRelayグループが割り当てられました	{0}台のコンピュータが空のRelayグループに割り当てられています
コンピュータの再起動が必要です	{0}台のコンピュータで再起動が必要です

Agentイベント

ID	重要度	イベント	備考
特殊なイベント			
0	エラー	不明なAgent/Applianceイベント	
ドライバ関連のイベント			

ID	重要度	イベント	備考
1000	エラー	エンジンを開けません	
1001	エラー	エンジンコマンドの失敗	
1002	警告	エンジンリストオブジェクトエラー	
1003	警告	オブジェクトの削除失敗	
1004	エラー	ドライバのアップグレードの停止	
1005	警告	ドライバのアップグレード中	
1006	エラー	ドライバのアップグレードで再起動が必要	
1007	警告	ドライバのアップグレード成功	
1008	エラー	サポートされないカーネル	
1010	警告	Trend Micro LightWeight Filter Driverが無効になりました	
1011	情報	Trend Micro LightWeight Filter Driverが再起動されました	
1012	情報	すべてのTrend Micro LightWeight Filter Driverが正常に再起動されました	
1013	警告	すべてのネットワークインタフェースでTrend Micro LightWeight Filter Driverのバインドに失敗しました	
設定関連のイベント			
2000	情報	ポリシー送信	
2001	警告	無効なファイアウォールルール割り当て	
2002	警告	無効なファイアウォールステートフル設定	
2003	エラー	セキュリティ設定の保存失敗	
2004	警告	無効なインタフェース割り当て	
2005	警告	無効なインタフェース割り当て	
2006	警告	無効な処理	
2007	警告	無効なパケット方向	
2008	警告	無効なルール優先度	
2009	警告	認識できないIPアドレスの形式	
2010	警告	無効な送信元IPリスト	
2011	警告	無効な送信元ポートリスト	
2012	警告	無効な送信先IPリスト	
2013	警告	無効な送信先ポートリスト	
2014	警告	無効なスケジュール	
2015	警告	無効な送信元MACリスト	
2016	警告	無効な送信先MACリスト	
2017	警告	無効なスケジュール長	
2018	警告	無効なスケジュール文字列	

ID	重要度	イベント	備考
2019	警告	認識できないIPアドレスの形式	
2020	警告	オブジェクトが見つかりません	
2021	警告	オブジェクトが見つかりません	
2022	警告	無効なルールの割り当て	
2050	警告	ファイアウォールルールが見つかりません	
2075	警告	トラフィックストリームが見つかりません	
2076	警告	侵入防御ルールが見つかりません	
2077	警告	パターンリストが見つかりません	
2078	警告	トラフィックストリーム変換エラー	
2080	警告	条件付きファイアウォールルールが見つかりません	
2081	警告	条件付き侵入防御ルールが見つかりません	
2082	警告	空白の侵入防御ルール	
2083	警告	侵入防御ルールのXMLルール変換エラー	
2085	エラー	セキュリティ設定エラー	
2086	警告	サポートされていないIPマッチタイプ	
2087	警告	サポートされていないMACマッチタイプ	
2088	警告	無効なSSL資格情報	
2089	警告	SSL資格情報がありません	
2090	エラー	セキュリティ設定エラー	
2091	エラー	セキュリティ設定エラー	
ハードウェア関連のイベント			
3000	警告	無効なMACアドレス	
3001	警告	イベントデータの取得失敗	
3002	警告	過剰なインタフェース	
3003	エラー	外部コマンドの実行不能	
3004	エラー	外部コマンド出力の読み取り不能	
3005	エラー	OS呼び出しエラー	
3006	エラー	OS呼び出しエラー	
3007	エラー	ファイルエラー	
3008	エラー	コンピュータ固有のキーエラー	
3009	エラー	Agent/Applianceの予期しないシャットダウン	
3010	エラー	Agent/Applianceデータベースエラー	

ID	重要度	イベント	備考
3300	警告	イベントデータの取得失敗	Linuxエラー。
3302	警告	セキュリティ設定の取得失敗	Linuxエラー。
3303	エラー	ファイルマッピングエラー	Linuxエラー。ファイルタイプエラー。
3600	エラー	Windowsシステムディレクトリの取得失敗	
3601	警告	ローカルデータ読み取りエラー	Windowsエラー。
3602	警告	Windowsサービスエラー	Windowsエラー。
3603	エラー	ファイルマッピングエラー	Windowsエラー。ファイルサイズエラー。
3700	警告	異常な再起動の検出	Windowsエラー。
3701	情報	システムの前回起動時刻の変化	Windowsエラー。
通信関連のイベント			
4000	警告	無効なプロトコルヘッダ	コンテンツ長が範囲外です。
4001	警告	無効なプロトコルヘッダ	コンテンツ長がありません。
4002	情報	コマンドセッションの開始	
4003	情報	設定セッションの開始	
4004	情報	コマンドの受信	
4011	警告	Managerへの接続に失敗しました	
4012	警告	ハートビートの失敗	
Agent関連のイベント			
5000	情報	Agent/Applianceの開始	
5001	エラー	スレッド例外	
5002	エラー	オペレーションタイムアウト	
5003	情報	Agent/Applianceの停止	
5004	警告	時計の変更	
5005	情報	Agent/Applianceの監査開始	
5006	情報	Agent/Applianceの監査停止	
5007	情報	Appliance保護の変更	
5008	警告	Filter Driver接続の失敗	
5009	情報	Filter Driver接続の成功	
5010	警告	Filter Driverの情報イベント	
5100	情報	保護モジュールの配信開始	
5101	情報	保護モジュールの配信成功	
5102	エラー	保護モジュールの配信失敗	
5103	情報	保護モジュールのダウンロード成功	
5104	情報	保護モジュールの無効化開始	
5105	情報	保護モジュールの無効化成功	
5106	エラー	保護モジュールの無効化失敗	
5107	情報	Agentセルフプロテクションの有効化	
5108	情報	Agentセルフプロテクションの無	

ID	重要度	イベント	備考
		効化	
5109	エラー	FIPS検証エラー	
5110	エラー	セキュアブートの公開鍵が未登録	このエラーは、トレンドマイクロのカーネルモジュールで署名を確認するために必要な公開鍵がエージェントコンピュータに正常に登録されていない場合に発生します。 詳細については、"AgentのLinux Secure Bootの設定" on page 520を参照してください。
5111	エラー	セキュアブート'オン'はサポートされていません	Deep Security Agentは、Secure Bootが有効なこのOSをサポートしていません。 詳細については、"AgentのLinux Secure Bootの設定" on page 520を参照してください。
5200	情報	ファイルバックアップ完了	
5201	エラー	ファイルバックアップ失敗	
ログ記録関連のイベント			
6000	情報	ログデバイスオープンエラー	
6001	情報	ログファイルオープンエラー	
6002	情報	ログファイル書き込みエラー	
6003	情報	ログディレクトリ作成エラー	
6004	情報	ログファイル検索エラー	
6005	情報	ログディレクトリオープンエラー	
6006	情報	ログファイル削除エラー	
6007	情報	ログファイルの名前変更エラー	
6008	情報	ログ読み取りエラー	
6009	警告	空き容量不足によるログファイルの削除	
6010	警告	イベントは抑制されました	
6011	警告	イベントの切り捨て	
6012	エラー	ディスク容量の不足	"警告: ディスク容量の不足" on page 1453を参照してください。
6013	警告	Agentの設定パッケージが大きすぎる	
攻撃関連、検索関連、調査関連のイベント			
7000	警告	OSのフィンガープリント調査	
7001	警告	ネットワークまたはポートの検索	
7002	警告	TCP Null検索	
7003	警告	TCP SYNFIN検索	
7004	警告	TCP Xmas検索	
セキュリティアップデートのダウンロードのイベント			

ID	重要度	イベント	備考
9050	情報	Agentでの不正プログラム対策コンポーネントのアップデート成功	
9051	エラー	Agentでの不正プログラム対策コンポーネントのアップデート失敗	
9100	情報	セキュリティアップデート成功	
9101	エラー	セキュリティアップデートの失敗	
9102	エラー	セキュリティアップデートの失敗	エラーメッセージに特定の情報が記録されました。
Relayのイベント			
9103	情報	Relay Webサーバの無効化	
9104	情報	Relay Webサーバの有効化	
9105	エラー	Relay Webサーバの有効化の失敗	
9106	エラー	Relay Webサーバの無効化の失敗	
9107	エラー	Relay Webサーバの失敗	
9108	情報	アップデート元に接続不能	
9109	エラー	コンポーネントのアップデートの失敗	
9110	エラー	不正プログラム対策のライセンスの期限切れ	
9111	情報	セキュリティアップデートのロールバック成功	
9112	エラー	セキュリティアップデートのロールバック失敗	
9113	情報	Relayによるすべてのパッケージの複製	
9114	エラー	Relayによるすべてのパッケージの複製に失敗	
9115	情報	Relay Webサーバからのダウンロードに失敗しました	
変更の検索のステータスに関するイベント			
9201	情報	変更の検索の開始	
9203	情報	変更の検索の異常終了	
9204	情報	変更の検索の一時停止	
9205	情報	変更の検索の再開	
9208	警告	変更の検索の開始失敗	
9209	警告	変更の検索の停止	
Smart Protection Serverのステータスに関するイベント			
9300	警告	Webレピュテーション用のSmart Protection Serverへの接続不能	"「Smart Protection Serverへの接続不能」エラーのトラブルシューティング" on page 1425を参照してください。
9301	情報	Webレピュテーション用のSmart	"「Smart Protection Serverへの接続不能」エラーの

ID	重要度	イベント	備考
		Protection Serverへの接続	トラブルシューティング" on page 1425を参照してください。
9302	警告	Census、Good File Reputation、機械学習型検索サービスへの接続解除	
9303	情報	Census、Good File Reputation、機械学習型検索サービスへの接続	

システムイベント

システムイベントを表示するには、[イベントとレポート]→[イベント] の順に選択します。

システムイベントを設定するには、管理 > システム設定 > システムイベント タブに移動します。このタブでは、個々のイベントを記録するかどうか、またはそれらをSIEMサーバに転送するかどうかを設定できます。記録を選択すると、イベントはデータベースに保存されます。記録を選択解除すると、イベントはイベント& レポートタブ (またはDeep Security Managerのどこにも) に表示されず、転送もされません。

システム構成の変更かセキュリティインシデントかに応じて、各ログはシステムイベントサブメニューまたは不正プログラム対策イベントのようなイベントの保護モジュールに対応するサブメニューに表示されます。

これらのイベントは、時々コンピューターのステータス列にも表示されます。

ID	重要度	イベント	説明または解決策
0	エラー	不明なエラー	
100	情報	Deep Security Managerの開始	
101	情報	ライセンスの変更	
107	情報	ルールアップデートのダウンロードおよび適用	
108	情報	スクリプト実行	
109	エラー	スクリプト実行の失敗	
110	情報	システムイベントのエクスポート	
111	情報	ファイアウォールイベントのエクスポート	
112	情報	侵入防御イベン	

ID	重要度	イベント	説明または解決策
		トのエクスポート	
115	情報	ルールアップデートのダウンロード	
116	情報	ルールアップデートの適用	
117	情報	Deep Security Managerのシャットダウン	
118	警告	オフラインのDeep Security Manager	
119	情報	Deep Security Managerのオンライン復帰	
120	エラー	ハートビートサーバの失敗	受信Agentハートビートを待機するDeep Security Manager内のサーバが起動しませんでした。Managerの受信ハートビートポート番号が、サーバ上の他のアプリケーションによって使用されていないことを確認してください。ポートが確保されると、Managerのハートビートサーバがそのポートにバインドされてエラーが解決します。
121	エラー	スケジューラの失敗	
122	エラー	Managerのメッセージスレッドの失敗	内部スレッドが失敗しました。このエラーの解決策はありません。このエラーが解決しない場合は、カスタマーサポートに問い合わせてください。
123	情報	Deep Security Managerの強制シャットダウン	
124	情報	ルールアップデートの削除	
130	情報	資格情報の生成	
140	情報	コンピュータの検出	
141	警告	コンピュータの検出の失敗	
142	情報	コンピュータの検出の要求	
143	情報	コンピュータの検出のキャンセル	
150	情報	システム設定の保存	
151	情報	ソフトウェアの追加	
152	情報	ソフトウェアの削除	

ID	重要度	イベント	説明または解決策
153	情報	ソフトウェアのアップデート	
154	情報	ソフトウェアのエクスポート	
156	エラー	Agentインストーラのデジタル署名の検証に失敗しました	デジタル署名の確認に失敗したため、「<エージェント>.zip」が削除されました。この失敗は、ファイルが改ざんされている可能性を示しています。詳細: <detailed_message> 詳細については、トレンドマイクロのサポート担当者にお問い合わせください。 詳細については、"ソフトウェアパッケージのデジタル署名の確認" on page 445を参照してください。
160	情報	認証の失敗	
161	情報	ルールアップデートのエクスポート	
162	情報	セキュリティログ監視イベントのエクスポート	
163	情報	不正プログラム対策のイベントのエクスポート	
164	情報	セキュリティアップデート成功	
165	エラー	セキュリティアップデートの失敗	
169	エラー	手動セキュリティアップデートの失敗	
170	エラー	Managerの利用可能ディスク容量の不足	Managerのディスク空き容量が不足しているため、シャットダウンします。ディスク容量を拡張するか、使用していないファイルを削除してディスク容量を確保してから、"Deep Security Managerの再起動" on page 1746をしてください。
171	情報	不正プログラム対策のスパイウェアアイテムのエクスポート	
172	情報	Webレピュテーションイベントのエクスポート	
173	情報	不正プログラム対策の検出ファイル	

ID	重要度	イベント	説明または解決策
		リストのエクスポート	
174	情報	不正プログラム対策の不正変更対象アイテムのエクスポート	
175	情報	ヒープダンプを作成中です	
176	情報	作成されたヒープダンプ	
177	エラー	ヒープダンプを作成できませんでした	
180	情報	アラートの種類のアップデート	
190	情報	アラートの開始	
191	情報	アラートの変更	
192	情報	アラートの終了	
197	情報	アラートメールの送信	
198	警告	アラートメールの失敗	アラートメールを送信できませんでした。SMTP設定が正しく設定されていることを確認してください。
199	エラー	アラート処理の失敗	アラートが完全に処理されていないため、現在のアラートのステータスが正確ではない可能性があります。問題が解決しない場合は、サポート担当者に問い合わせてください。
247	警告	Agent整合性チェックに失敗しました	
248	情報	ソフトウェアアップデート: Relayの無効化要求	
249	情報	ソフトウェアアップデート: Relayの有効化要求	
250	情報	コンピュータの作成	
251	情報	コンピュータの削除	
252	情報	コンピュータのアップデート	
253	情報	コンピュータへのポリシーの割り当て	
254	情報	コンピュータの移動	

ID	重要度	イベント	説明または解決策
255	情報	有効化の要求	
256	情報	ポリシー送信の要求	
257	情報	ロック	
258	情報	ロック解除	
259	情報	無効化の要求	
260	情報	オープンポートの検索	
261	警告	オープンポートの検索の失敗	
262	情報	オープンポートの検索の要求	
263	情報	オープンポートの検索のキャンセル	
264	情報	Agentソフトウェアのアップグレード要求	
265	情報	Agentソフトウェアのアップグレードのキャンセル	
266	情報	警告/エラーのクリア	
267	情報	ステータスの確認の要求	
268	情報	イベントの取得の要求	
269	情報	クラウドコネクタへのコンピュータの追加	
270	エラー	コンピュータの作成の失敗	
271	情報	Agentソフトウェアのアップグレードのタイムアウト	
272	情報	Applianceソフトウェアのアップグレードのタイムアウト	
273	情報	セキュリティアップデート: セキュリティアップデートの確認とダウンロード要求	
274	情報	セキュリティアップデート: セキュリ	

ID	重要度	イベント	説明または解決策
		ティアップデートのロールバック要求	
275	警告	重複するコンピュータ	
276	情報	アップデート: 概要情報	
277	情報	アクティベーションアップグレード(スキップ)	Agentは自動アップグレードの対象になっていましたが、アップグレードは実行されませんでした。詳細については、"Agentを有効化するときに自動的にアップグレードする" on page 1513を参照してください。
278	情報	ソフトウェアアップデート: Agentソフトウェアのアップグレードを完了するには、再起動する必要があります	
280	情報	コンピュータのエクスポート	
281	情報	コンピュータのインポート	
287	情報	コンピュータへのRelayグループの割り当て	
290	情報	グループの追加	
291	情報	グループの削除	
292	情報	グループのアップデート	
293	情報	インタフェース名の変更	
294	情報	コンピュータブリッジ名の変更	
295	情報	インタフェースの削除	
297	情報	推奨設定の検索要求	
298	情報	推奨設定のクリア	
299	情報	コンピュータへの資産評価の割り当て	
300	情報	推奨設定の検索完了	
301	情報	Agentソフトウェアの配信の要求	
302	情報	Agentソフトウェア	

ID	重要度	イベント	説明または解決策
		の削除の要求	
303	情報	コンピュータ名の変更	
304	情報	データセンターへのコンピュータの移動	Deep Security Managerでは、権限の問題によりVMの上位フォルダを特定できなかったため、仮想マシン(VM) がルートデータセンターフォルダに配置されました。Deep Security Managerの正しいフォルダにVMを表示するには、vCenter Server上のVMの権限を確認します。
305	情報	変更の検索の要求	
306	情報	ベースラインの再構築の要求	
307	情報	アップデートの要求のキャンセル	
308	情報	変更監視ルールのコンパイルの問題	
309	情報	変更監視ルールのコンパイルの問題の解決	
310	情報	ディレクトリの追加	
311	情報	ディレクトリの削除	
312	情報	ディレクトリのアップデート	
321	情報	ディレクトリ同期の完了	
322	エラー	ディレクトリ同期の失敗	
323	情報	ディレクトリ同期の要求	
326	情報	ユーザ同期の完了	ユーザアカウントとMicrosoft Active Directoryとの同期が完了しました。
327	エラー	ユーザ同期の失敗	
330	情報	SSL設定の作成	
331	情報	SSL設定の削除	
332	情報	SSL設定のアップデート	
333	情報	ホストのマージ完了	
334	エラー	ホストのマージ失敗	

ID	重要度	イベント	説明または解決策
338	警告	ディレクトリの同期の制限を超えました	Active Directory同期のグループメンバーの合計数に達しました。残りのメンバーをスキップします。システム設定の制限を調整することを検討してください。
350	情報	ポリシーの作成	
351	情報	ポリシーの削除	
352	情報	ポリシーのアップデート	
353	情報	ポリシーのエクスポート	
354	情報	ポリシーのインポート	
355	情報	推奨設定の検索のキャンセル	
356	エラー	セキュアブートの公開鍵が未登録	このエラーは、トレンドマイクロのカーネルモジュールで署名を確認するために必要な公開鍵がエージェントコンピュータに正常に登録されていない場合に発生します。 詳細については、"AgentのLinux Secure Bootの設定" on page 520を参照してください。
357	エラー	セキュアブート'オン'はサポートされていません	Deep Security Agentは、Secure Bootが有効なこのOSをサポートしていません。 詳細については、"AgentのLinux Secure Bootの設定" on page 520を参照してください。
360	情報	VMware vCenterの追加	
361	情報	VMware vCenterの削除	
362	情報	VMware vCenterのアップデート	
363	情報	VMware vCenterの同期	
364	情報	VMware vCenterの同期の完了	
365	エラー	VMware vCenterの同期失敗	
366	情報	VMware vCenterの同期要求	
367	情報	VMware vCenterの同期キャンセル	
368	警告	インタフェースが非同期	Deep Security Virtual ApplianceからレポートされたインタフェースとvCenterからレポートされたインタフェースは異なります。通常、仮想マシンを再起動すると解決します。

ID	重要度	イベント	説明または解決策
369	情報	インタフェースが同期	
370	情報	Filter Driverのインストール完了	
371	情報	Filter Driverの削除完了	VMware ESXiサーバは、Filter Driverソフトウェアがインストールされる前の状態に復元されました。
372	情報	Filter Driverのアップグレード	
373	情報	Virtual Applianceの配置	
374	情報	Virtual Applianceのアップグレード完了	
375	警告	Virtual Applianceのアップグレードの失敗	
376	警告	保護されていないESXiへの仮想マシンの移動	
377	情報	保護されているESXiへの仮想マシンの移動	
378	警告	別のESXiへの移動後に仮想マシンが保護されていない	Deep Security Virtual ApplianceがないESXiに、仮想マシンが移動されました。
379	情報	別のESXiへの移動後に仮想マシンが未保護になる状態が解決	
380	エラー	オフラインのFilter Driver	ESXiサーバのFilter Driverがオフラインです。VMware vCenterコンソールを使用して、ハイパーバイザおよびESXiの問題をトラブルシューティングしてください。
381	情報	Filter Driverのオンライン復帰	
382	情報	Filter Driverのアップグレード要求	
383	情報	Applianceのアップグレード要求	
384	警告	ESXiの準備失敗	
385	警告	Filter Driverのアップグレード失	

ID	重要度	イベント	説明または解決策
		敗	
386	警告	ESXiからのFilter Driver削除の失敗	
387	エラー	Filter Driverとの接続失敗	
388	情報	Filter Driverとの接続成功	
389	エラー	複数の有効化されたApplianceの検出	
390	情報	有効化されたApplianceの複数検出の解決	
391	エラー	ネットワーク設定とvCenterグローバル設定との非同期	
392	情報	ネットワーク設定とvCenterグローバル設定との同期	
393	エラー	不正プログラム対策エンジンがオフライン	不正プログラム対策保護モジュールが機能していません。これは、VMware環境が要件に一致していないことが原因である可能性があります。"システム要件 " on page 400を参照してください。
394	情報	不正プログラム対策エンジンのオンライン復帰	
395	エラー	Virtual ApplianceとFilter Driverの互換性なし	
396	情報	Virtual ApplianceとFilter Driverの互換性がない状態の解決	
397	警告	VMware NSXコールバック認証失敗	
398	エラー	VMware Toolsがインストールされていない	
399	情報	VMware Toolsの未インストール解	

ID	重要度	イベント	説明または解決策
		決	
410	情報	ファイアウォールルールの作成	
411	情報	ファイアウォールルールの削除	
412	情報	ファイアウォールルールのアップデート	
413	情報	ファイアウォールルールのエクスポート	
414	情報	ファイアウォールルールのインポート	
420	情報	ファイアウォールステートフル設定の作成	
421	情報	ファイアウォールステートフル設定の削除	
422	情報	ファイアウォールステートフル設定のアップデート	
423	情報	ファイアウォールステートフル設定のエクスポート	
424	情報	ファイアウォールステートフル設定のインポート	
460	情報	アプリケーションの種類の作成	管理者が新しいIPSネットワークのアプリケーション定義を設定しました。
461	情報	アプリケーションの種類の削除	管理者がIPSネットワークのアプリケーション定義を削除しました。
462	情報	アプリケーションの種類のアップデート	管理者が既存のIPSネットワークのアプリケーション定義を変更しました。
463	情報	アプリケーションの種類のエクスポート	管理者がIPSネットワークのアプリケーション定義をダウンロードしました。
464	情報	アプリケーションの種類のインポート	管理者がIPSネットワークのアプリケーション定義をアップロードしました。
470	情報	侵入防御ルールの作成	
471	情報	侵入防御ルールの削除	

ID	重要度	イベント	説明または解決策
472	情報	侵入防御ルールのアップデート	
473	情報	侵入防御ルールのエクスポート	
474	情報	侵入防御ルールのインポート	
480	情報	変更監視ルールの作成	
481	情報	変更監視ルールの削除	
482	情報	変更監視ルールのアップデート	
483	情報	変更監視ルールのエクスポート	
484	情報	変更監視ルールのインポート	
490	情報	セキュリティログ監視ルールの作成	
491	情報	セキュリティログ監視ルールの削除	
492	情報	セキュリティログ監視ルールのアップデート	
493	情報	セキュリティログ監視ルールのエクスポート	
494	情報	セキュリティログ監視ルールのインポート	
495	情報	セキュリティログ監視デコーダの作成	
496	情報	セキュリティログ監視デコーダの削除	
497	情報	セキュリティログ監視デコーダのアップデート	
498	情報	セキュリティログ監視デコーダのエクスポート	
499	情報	セキュリティログ監視デコーダのインポート	
505	情報	コンテキストの作	

ID	重要度	イベント	説明または解決策
		成	
506	情報	コンテキストの削除	
507	情報	コンテキストのアップデート	
508	情報	コンテキストのエクスポート	
509	情報	コンテキストのインポート	
510	情報	IPリストの作成	
511	情報	IPリストの削除	
512	情報	IPリストのアップデート	
513	情報	IPリストのエクスポート	
514	情報	IPリストのインポート	
520	情報	ポートリストの作成	
521	情報	ポートリストの削除	
522	情報	ポートリストのアップデート	
523	情報	ポートリストのエクスポート	
524	情報	ポートリストのインポート	
525	情報	検索キャッシュ設定の作成	
526	情報	検索キャッシュ設定のエクスポート	
527	情報	検索キャッシュ設定のアップデート	
530	情報	MACリストの作成	
531	情報	MACリストの削除	
532	情報	MACリストのアップデート	
533	情報	MACリストのエクスポート	
534	情報	MACリストのインポート	
540	情報	プロキシの作成	

ID	重要度	イベント	説明または解決策
541	情報	プロキシの削除	
542	情報	プロキシのアップデート	
543	情報	プロキシのエクスポート	
544	情報	プロキシのインポート	
550	情報	スケジュールの作成	
551	情報	スケジュールの削除	
552	情報	スケジュールのアップデート	
553	情報	スケジュールのエクスポート	
554	情報	スケジュールのインポート	
560	情報	予約タスクの作成	
561	情報	予約タスクの削除	
562	情報	予約タスクのアップデート	
563	情報	予約タスクの手動実行	
564	情報	予約タスクの開始	
567	情報	未解決アラートの概要の送信中	
568	警告	未解決アラートの概要の送信失敗	
569	警告	メールの失敗	メール通知を送信できませんでした。SMTP設定が正しく設定されていることを確認してください。
570	情報	レポートの送信中	
571	警告	レポートの送信の失敗	
572	エラー	無効なReport Jar	
573	情報	資産評価の作成	
574	情報	資産評価の削除	

ID	重要度	イベント	説明または解決策
575	情報	資産評価のアップデート	
576	エラー	レポートのアンインストールの失敗	
577	エラー	レポートのアンインストール	
578	警告	設定が必要な変更監視ルール	
580	警告	アプリケーションの種類のポートリストの誤った設定	
581	警告	アプリケーションの種類のポートリストの誤った設定の解決	
582	警告	侵入防御ルールで設定が必要	
583	情報	侵入防御ルールで必要な設定の解決	
584	警告	アプリケーションの種類で設定が必要	IPSルールにはネットワークアプリケーション定義が必要で、定義するまでトラフィックを正しく検索できません。
585	情報	変更監視ルールで必要な設定の解決	
586	警告	セキュリティログ監視ルールで設定が必要	
587	情報	セキュリティログ監視ルールで必要な設定の解決	
588	警告	セキュリティログ監視ルールで必要なログファイル	
589	情報	セキュリティログ監視ルールで必要なログファイルの解決	
590	警告	非推奨の予約タスク	
591	情報	Relayグループの作成	
592	情報	Relayグループのアップデート	

ID	重要度	イベント	説明または解決策
593	情報	Relayグループの削除	
594	情報	イベントベースタスクの作成	
595	情報	イベントベースタスクの削除	
596	情報	イベントベースタスクのアップデート	
597	情報	イベントベースタスクの開始	
600	情報	ユーザのログオン	
601	情報	ユーザのログオフ	
602	情報	ユーザのタイムアウト	
603	情報	ユーザのロックアウト	
604	情報	ユーザのロック解除	
605	情報	ユーザセッションの終了	
608	エラー	ユーザセッションの確認の失敗	Deep Security Managerは、認証が成功した後にセッションが開始されたことを確認できませんでした。ユーザはログインページにリダイレクトされ、再認証を求められます。認証済みのセッションリストがクリアされた場合、これは正常な動作です。
609	エラー	ユーザによる無効な要求	Deep Security Managerは、監査データ(イベント) にアクセスするための無効な要求を受信しました。アクセスは拒否されました。
610	情報	ユーザセッションの有効化	
611	情報	ユーザによるファイアウォールイベントの表示	
613	情報	ユーザによる侵入防御イベントの表示	
615	情報	ユーザによるシステムイベントの表示	
616	情報	ユーザによる変更監視イベントの表示	
617	情報	ユーザによるセキュリティログ監視イベントの表示	
618	情報	ユーザによる検出	

ID	重要度	イベント	説明または解決策
		ファイルの詳細表示	
619	情報	ユーザによる不正プログラム対策イベントの表示	
620	情報	ユーザによるWebレピュテーションイベントの表示	
621	情報	ユーザがテナントとしてログオン	
622	情報	プライマリテナントからのアクセスは有効	
623	情報	プライマリテナントからのアクセスは無効	
624	情報	プライマリテナントからのアクセスを許可	
625	情報	プライマリテナントからのアクセスは取り消し済み	
626	情報	プライマリテナントからのアクセスは期限切れ	
630	情報	Syslog設定の作成	
631	情報	Syslog設定の削除	
632	情報	Syslog設定のアップデート	
633	情報	Syslog設定のエクスポート	
634	情報	Syslog設定のインポート	
650	情報	ユーザの作成	
651	情報	ユーザの削除	
652	情報	ユーザのアップデート	
653	情報	ユーザパスワードの設定	
656	情報	APIキーの作成	
657	情報	APIキーの削除	
658	情報	APIキーのアップデート	

ID	重要度	イベント	説明または解決策
660	情報	役割の作成	
661	情報	役割の削除	
662	情報	役割のアップデート	
670	情報	連絡先の作成	
671	情報	連絡先の削除	
672	情報	連絡先のアップデート	
673	情報	APIキーのロックアウト	
674	情報	APIキーのロック解除	
675	エラー	APIキーセッションの有効化失敗	
678	情報	APIキーの有効期限切れ	
680	情報	マスター暗号化キーの作成	詳細については、masterkeyパラメータを参照してください。
681	情報	マスター暗号化キーのエクスポート	詳細については、masterkeyパラメータを参照してください。
682	情報	マスター暗号化キーのインポート	詳細については、masterkeyパラメータを参照してください。
690	情報	Microservice APIキーが作成されました	
691	情報	マイクロサービス APIキーが削除されました	
692	情報	マイクロサービス APIキーが更新されました	
693	情報	マイクロサービス APIロックアウト	
694	情報	マイクロサービス APIキーのロック解除	
695	エラー	Microservice APIキーセッションの検証に失敗しました	
696	情報	マイクロサービス APIキーの期限切れ	
701	エラー	Agentソフトウェア	

ID	重要度	イベント	説明または解決策
		のインストールの失敗	
702	情報	資格情報の生成	
703	エラー	資格情報の生成の失敗	
704	情報	Agent/Appliance有効化の完了	
705	エラー	Agent/Appliance有効化の失敗	Agentのセルフプロテクションが有効になっている場合に発生することがあります。Deep Security Managerで、**コンピュータエディタ**[1]→[設定]→[一般]の順に選択します。[Agentセルフプロテクション]で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否]の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。
706	情報	ソフトウェアアップデート: Agentソフトウェアのアップグレード	
707	警告	ソフトウェアアップデート: Agentソフトウェアのアップグレードの失敗	アップグレードが失敗した理由の詳細については、イベント詳細を参照してください。
708	情報	Agent/Appliance無効化の完了	
709	エラー	Agent/Appliance無効化の失敗	
710	情報	イベントの取得	
711	情報	Agentソフトウェアの配信	
712	エラー	Agentソフトウェアの配信の失敗	Agentのセルフプロテクションが有効になっている場合に発生することがあります。Deep Security Managerで、**コンピュータエディタ**[2]→[設定]→[一般]の順に選択します。[Agentセルフプロテクション]で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否]の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。
713	情報	Agentソフトウェアの削除	

1 コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

2 コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

ID	重要度	イベント	説明または解決策
714	エラー	Agentソフトウェアの削除の失敗	Agentのセルフプロテクションが有効になっている場合に発生することがあります。Deep Security Managerで、コンピュータエディタ[1]→[設定]→[一般]の順に選択します。[Agentセルフプロテクション]で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否]の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。
715	情報	Agent/Applianceのバージョン変更	
716	情報	不明なAgentの再有効化の試行	Deep Security Managerに認識されていないAgentの再有効化が試行されました。コンピュータは最初のコンピュータにエージェントを削除せずにDeep Security Managerから削除されたとき、これは通常起こります。詳細については、「Agentの設定」の「不明なAgentの再有効化の試行」を参照してください。
720	情報	ポリシー送信	Agent/Applianceがアップデートされました。
721	エラー	ポリシー送信の失敗	
722	警告	インタフェースの取得失敗	
723	情報	インタフェースの取得失敗の解決	
724	警告	ディスク容量の不足	Agentのディスク容量不足が検出されました。コンピュータの空き容量を増やしてください。"警告:ディスク容量の不足" on page 1453 を参照してください。
725	警告	イベントの抑制	
726	警告	Agent/Applianceイベントの取得失敗	マネージャはエージェント/アプライアンスからイベントを取得できませんでした。このエラーは、エージェント/アプライアンス上のデータが失われたことを意味するものではありません。このエラーは通常、イベントが転送されている間のネットワーク中断によって引き起こされます。エラーをクリアし、ステータスを確認して操作を再試行してください。
727	情報	Agent/Applianceイベントの取得失敗の解決	
728	エラー	イベントの取得失敗	マネージャはエージェント/アプライアンスから監査データを取得できませんでした。このエラーは、エージェント/アプライアンス上のデータが失われたことを意味するものではありません。このエラーは通常、イベントが転送されている間のネットワーク中断によって引き起こされます。エラーをクリアし、今すぐイベントを取得を実行して操作を再試行してください。

[1] コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

ID	重要度	イベント	説明または解決策
729	情報	イベントの取得失敗の解決	
730	エラー	オフライン	マネージャはコンピュータと通信できません。しかし通常、オフラインエージェントは最後に設定された設定でコンピュータを保護し続けます。コンピュータとエージェント/アプライアンスのステータスおよび"オフラインエージェント" on page 1986を参照してください。
731	情報	オンラインに復帰	
732	エラー	ファイアウォールエンジンがオフライン	ファイアウォールエンジンがオフラインであるため、トラフィックがフィルタリングされないまま送受信されています。この状態は、通常、ドライバのインストール中または確認中のエラーが原因で発生します。コンピュータのネットワークドライバの状態を調べて、正常に読み込まれていることを確認してください。
733	情報	ファイアウォールエンジンがオンライン復帰	
734	警告	コンピュータの時計の変更	コンピュータエディタまたはポリシーエディタ[1]の [設定]→[一般]→[ハートビート] エリアで指定された最大許容値を超える時計の変更がコンピュータで検出されました。コンピュータの時計が変更された原因を調査してください。
735	警告	誤った設定の検出	Agentの設定が、Managerのレコードで指示されている設定と一致しません。これは通常、最近実行されたManagerまたはAgentバックアップの復元が原因です。設定の不一致が予期しないものである場合、調査する必要があります。
736	情報	ステータス確認の失敗の解決	
737	エラー	ステータスの確認の失敗	"エラー: ステータスの確認の失敗" on page 1433を参照してください。
738	エラー	侵入防御エンジンがオフライン	侵入防御エンジンがオフラインであるため、トラフィックがフィルタリングされないまま送受信されています。この状態は、通常、ドライバのインストール中または確認中のエラーが原因で発生します。コンピュータのネットワークドライバの状態を調べて、正常に読み込まれていることを確認してください。
739	情報	侵入防御エンジンがオンライン復帰	
740	エラー	Agent/Applianceエラー	
741	警告	異常な再起動の検出	
742	警告	通信の問題	AgentからManagerへステータスを送信中に問題が発生しました。

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

ID	重要度	イベント	説明または解決策
			通常、AgentからManagerへの通信で、ネットワークまたは負荷の輻輳が発生していることを示しています。この状態が解決しない場合、詳しい調査が必要です。
743	情報	通信の問題の解決	
745	警告	イベントの切り捨て	
748	エラー	セキュリティログ監視エンジンがオフライン	
749	情報	セキュリティログ監視エンジンのオンライン復帰	
755	情報	Deep Security Managerのバージョン互換性の解決	
756	警告	Deep Security Managerのアップグレード推奨 (非互換のセキュリティアップデート)	各セキュリティモジュールのルール(ファイアウォール、不正プログラム対策など) には、Deep Security Managerの最小バージョンがあります。ルールを実行するために必要です。 現在のDeep Security Managerのバージョンは、サポートされているルールの最小バージョン数を下回っています。Deep Security Managerをアップグレードして警告をクリアし、ルールを実行してください。
760	情報	Agent/Applianceバージョン互換性の解決	
761	警告	Agent/Applianceのアップグレード推奨	
762	警告	Agent/Applianceのアップグレードが必要	現在のDeep Security AgentまたはDeep Security Virtual Applianceのバージョンは、Deep Security Managerのサポートされている最小バージョンより小さいです。Agent/Appliance.のアップグレード
763	エラー	非互換のAgent/Applianceバージョン	現在のDeep Security Managerのバージョンが Deep Security AgentまたはDeep Security Virtual Applianceの最小サポートバージョンより小さい。マネージャーをアップグレードしてください。
764	警告	エージェント/アプライアンスのアップグレードを推奨 (互換性のないセ	各セキュリティモジュールのルール (ファイアウォール、不正プログラム対策など) には、ルールを実行するために必要な特定の最低限のDeep Security AgentまたはDeep Security Virtual Applianceの

ID	重要度	イベント	説明または解決策
		キュリティ更新)	バージョンがあります。 現在のDeep Security AgentまたはDeep Security Virtual Applianceのバージョンが、サポートされているルールの最小バージョン数を下回っています。Deep Security AgentまたはDeep Security Virtual Applianceをアップグレードして、警告をクリアしてルールを実行します。
765	エラー	コンピュータの再起動が必要	
766	警告	ネットワークエンジンモードの設定が非互換	
767	警告	ネットワークエンジンモードのバージョンが非互換	
768	警告	ネットワークエンジンモードの非互換性の解決	
770	警告	Agent/Applianceのハートビートの拒否	
771	警告	認識できないクライアントによる接続	"イベントID 771「認識できないクライアントによる接続」のトラブルシューティング" on page 1424を参照してください。
780	情報	推奨設定の検索失敗の解決	
781	警告	推奨設定の検索失敗	"トラブルシューティング: 推奨設定の検索失敗" on page 738を参照してください。
782	情報	ベースラインの再構築失敗の解決	
783	警告	ベースラインの再構築の失敗	
784	情報	セキュリティアップデート: セキュリティアップデートの確認とダウンロード成功	
785	警告	セキュリティアップデート: セキュリティアップデートの確認とダウンロード失敗	
786	情報	変更の検索失	

ID	重要度	イベント	説明または解決策
		敗の解決	
787	警告	変更の検索の失敗	
790	情報	Agentからのリモート有効化の要求	
791	警告	Agentからのリモート有効化の失敗	
792	情報	不正プログラムの手動検索失敗の解決	
793	警告	不正プログラムの手動検索の失敗	不正プログラム検索に失敗しました。VMware vCenterのコンソールを使用して、検索に失敗した仮想マシンのステータスを確認してください。"不正プログラム対策 検索の失敗とキャンセル" on page 1158も参照してください。
794	情報	不正プログラムの予約検索失敗の解決	
795	警告	不正プログラムの予約検索の失敗	不正プログラムの予約検索に失敗しました。VMware vCenterのコンソールを使用して、検索に失敗した仮想マシンのステータスを確認してください。"不正プログラム対策 検索の失敗とキャンセル" on page 1158も参照してください。
796	警告	不正プログラムの予約検索タスクのスキップ	これは、以前の検索が完了しないうちに、コンピュータ上で不正プログラムの予約検索が開始された場合に発生します。通常、不正プログラムの予約検索の実行間隔が短かすぎることを示しています。
797	情報	不正プログラム検索のキャンセル失敗の解決	
798	警告	不正プログラム検索キャンセルの失敗	不正プログラム検索のキャンセルに失敗しました。VMware vCenterのコンソールを使用して、検索に失敗した仮想マシンのステータスを確認してください。
799	警告	不正プログラム検索の停止	不正プログラム検索が停止しました。VMware vCenterのコンソールを使用して、検索が停止した仮想マシンのステータスを確認してください。
800	情報	アラートの消去	
801	情報	エラーの消去	
803	警告	Agentの設定パッケージが大きすぎる	
804	エラー	侵入防御ルールのコンパイル失敗	
805	エラー	侵入防御ルールのコンパイル失敗	
806	エラー	侵入防御ルール	

ID	重要度	イベント	説明または解決策
		のコンパイル失敗	
850	警告	攻撃の予兆の検出: OSのフィンガープリント調査	"警告: 攻撃の予兆の検出" on page 1453
851	警告	攻撃の予兆の検出: ネットワークまたはポートの検索	"警告: 攻撃の予兆の検出" on page 1453
852	警告	攻撃の予兆の検出: TCP Null検索	"警告: 攻撃の予兆の検出" on page 1453
853	警告	攻撃の予兆の検出: TCP SYNFIN検索	"警告: 攻撃の予兆の検出" on page 1453
854	警告	攻撃の予兆の検出: TCP Xmas検索	"警告: 攻撃の予兆の検出" on page 1453
900	情報	Deep Security Managerの監査の開始	
901	情報	Deep Security Managerの監査のシャットダウン	
902	情報	Deep Security Managerのインストール	
904	情報	診断ログが有効	
905	情報	診断ログの完了	
906	情報	Java Flight Recorderが有効	Java Flight Recorderは、イベントの説明に指定されたパラメーター値で有効になっています。
907	情報	Java Flight Recorderが完了しました	Java Flight Recorderの記録セッションが完了しました。
910	情報	診断パッケージの生成	
911	情報	診断パッケージのエクスポート	
914	情報	検出ファイルの削除の成功	
915	情報	検出ファイルの削除の失敗	
916	情報	検出ファイルのダウンロードの成功	
917	情報	検出ファイルのダウンロードの失敗	

ID	重要度	イベント	説明または解決策
918	情報	検出ファイル管理ユーティリティのダウンロードの成功	
919	情報	検出ファイルが見つかりません	
924	警告	ファイルを分析または隔離できません (検出ファイル保存用のVMの最大ディスク容量を超過)	不正プログラム対策モジュールは、VMの識別されたファイルを保存するための最大ディスク容量に達したため、ファイルを分析または隔離することができませんでした。識別されたファイルの最大ディスク容量設定を変更するには、コンピュータまたはポリシーエディタを開き、不正プログラム対策 > 詳細設定タブに移動してください。
925	警告	識別されたファイルを保存するために使用される最大ディスク容量を超えました。古い識別ファイルが削除されるか、新しく検出されたファイルが分析または隔離されない可能性があります。	識別されたファイルの保存に使用される最大ディスク容量に達しました。その結果、不正プログラム対策モジュールが古い識別ファイルを削除するか、不正プログラム対策モジュールがファイルを分析または隔離できない可能性があります。識別されたファイルの設定の最大ディスク容量を変更するには、コンピュータまたはポリシーエディタを開き、不正プログラム対策 > 詳細タブを選択してください。
926	警告	スマートスキャン用のSmart Protection Serverへの接続不能	"「Smart Protection Serverへの接続不能」エラーのトラブルシューティング" on page 1425を参照してください。
927	情報	スマートスキャン用のSmart Protection Serverへの接続	
928	情報	検出ファイルの復元の成功	
929	警告	検出ファイルの復元の失敗	
930	情報	証明書の承諾	
931	情報	証明書の削除	
932	警告	Webレピュテーション用のSmart Protection Serverへの接続不能	"「Smart Protection Serverへの接続不能」エラーのトラブルシューティング" on page 1425を参照してください。
933	情報	Webレピュテーション用のSmart	

ID	重要度	イベント	説明または解決策
		Protection Serverへの接続	
934	情報	ソフトウェアアップデート: Windowsプラットフォーム用不正プログラム対策のアップデート成功	
935	エラー	ソフトウェアアップデート: Windowsプラットフォーム用不正プログラム対策のアップデート失敗	"Windowsプラットフォーム用不正プログラム対策のアップデート失敗" on page 1992
936	情報	Deep Discovery Analyzerへの検出ファイルの送信に成功しました。	
937	情報	Deep Discovery Analyzerへの検出ファイルの送信に失敗しました。	
938	情報	検出ファイルを送信キューに登録	
940	情報	自動タグルールの作成	
941	情報	自動タグルールの削除	
942	情報	自動タグルールのアップデート	
943	情報	タグの削除	
944	情報	タグの作成	
945	警告	Census、Good File Reputation、機械学習型検索サービスへの接続解除	
946	情報	Census、Good File Reputation、機械学習型検索サービスへの接続	
947	情報	FIPSモード有効	
948	情報	FIPSモード無効	
949	警告	Windowsインス	WindowsインストーラでのDeep Security Agentのインストールを完

ID	重要度	イベント	説明または解決策
		トーラでのDeep Security Agentのインストールを完了するためにコンピュータの再起動が必要	了するためにコンピュータの再起動が必要です。
950	警告	Deep Security Agent保護を有効にするためにコンピュータの再起動が必要	Windows Defenderを無効にしてDeep Security Agent保護を有効にするためにコンピュータの再起動が必要です。
970	情報	コマンドラインユーティリティの開始	
978	情報	コマンドラインユーティリティの失敗	
979	情報	コマンドラインユーティリティのシャットダウン	Deep Security Managerが手動で停止されました。
990	情報	Managerノードの追加	
991	情報	Managerノードの廃止	
992	情報	Managerノードのアップデート	
995	情報	ソフトウェア安全性評価サービスへの接続が復元	
996	警告	ソフトウェア安全性評価サービスに接続不能	
997	エラー	タグ付けエラー	
998	エラー	システムイベント通知エラー	
999	エラー	内部ソフトウェアエラー	
1101	エラー	プラグインのインストールの失敗	
1102	情報	プラグインのインストール	
1103	エラー	プラグインのアップグレードの失敗	
1104	情報	プラグインのアップグレード	
1105	エラー	プラグインの起動の失敗	

ID	重要度	イベント	説明または解決策
1106	エラー	プラグインのアンインストールの失敗	
1107	情報	プラグインのアンインストール	
1108	情報	プラグイン起動	
1109	情報	プラグイン停止	
1110	エラー	ソフトウェアパッケージが見つかりません	エージェントソフトウェアパッケージが見つからないか、新しいパッケージが必要です。
1111	情報	ソフトウェアパッケージが見つかりました	
1112	エラー	サポートされないカーネル	お使いのコンピュータがサポートされていないカーネルにアップグレードされている可能性があるため、Linuxドライバをインストールできません。詳細については、"Linuxカーネルの互換性" on page 400を参照してください。
1204	情報	検出ファイルのダウンロードを要求	ダウンロードリクエストが送信されました。最新のアップデートについては、イベントID1209を確認してください。「ダウンロードの準備ができました」ファイルは24時間利用できます。
1205	情報	検出ファイルのダウンロード要求が失敗	ダウンロード要求を正常に送信できませんでした。
1208	情報	検出ファイルのダウンロード要求のタイムアウト	2日間の制限に達したため、ダウンロード要求がタイムアウトしました。
1209	情報	検出ファイルのダウンロードの準備完了	検出ファイルのダウンロードの準備が完了しました。24時間以内にファイルをダウンロードしてください。
1500	情報	不正プログラム検索設定の作成	
1501	情報	不正プログラム検索設定の削除	
1502	情報	不正プログラム検索設定のアップデート	
1503	情報	不正プログラム検索設定のエクスポート	
1504	情報	不正プログラム検索設定のインポート	
1505	情報	ディレクトリリストの作成	
1506	情報	ディレクトリリストの削除	

ID	重要度	イベント	説明または解決策
1507	情報	ディレクトリリストのアップデート	
1508	情報	ディレクトリリストのエクスポート	
1509	情報	ディレクトリリストのインポート	
1510	情報	ファイル拡張子リストの作成	
1511	情報	ファイル拡張子リストの削除	
1512	情報	ファイル拡張子リストのアップデート	
1513	情報	ファイル拡張子リストのエクスポート	
1514	情報	ファイル拡張子リストのインポート	
1515	情報	ファイルリストの作成	
1516	情報	ファイルリストの削除	
1517	情報	ファイルリストのアップデート	
1518	情報	ファイルリストのエクスポート	
1519	情報	ファイルリストのインポート	
1520	情報	不正プログラムの手動検索の保留中	
1521	情報	不正プログラムの手動検索の開始	
1522	情報	不正プログラムの手動検索の完了	
1523	情報	不正プログラムの予約検索の開始	
1524	情報	不正プログラムの予約検索の完了	
1525	情報	不正プログラムの手動検索キャンセルの実行中	

ID	重要度	イベント	説明または解決策
1526	情報	手動不正プログラム検索キャンセル	このイベントにはいくつか原因があります。"不正プログラム対策 検索の失敗とキャンセル" on page 1158を参照してください。
1527	情報	不正プログラムの予約検索キャンセルの実行中	
1528	情報	不正プログラム検索予約のキャンセル	このイベントにはいくつか原因があります。"不正プログラム対策 検索の失敗とキャンセル" on page 1158を参照してください。
1529	情報	不正プログラムの手動検索の一時停止	
1530	情報	不正プログラムの手動検索の再開	
1531	情報	不正プログラムの予約検索の一時停止	
1532	情報	不正プログラムの予約検索の再開	
1533	情報	不正プログラム対策のクリーンナップまたは復元タスクを完了するためにコンピュータの再起動が必要	不正プログラム対策のクリーンナップまたは復元タスクを完了するには、コンピュータの再起動が必要です。
1534	エラー	不正プログラム対策保護を完了するためにコンピュータの再起動が必要	
1535	情報	不正プログラムのクリーンナップタスクの手動実行が必要	
1536	情報	不正プログラムのクイック検索の保留中	
1537	情報	不正プログラムのクイック検索の開始	
1538	情報	不正プログラムのクイック検索の完了	

ID	重要度	イベント	説明または解決策
1539	情報	不正プログラムのクイック検索キャンセルの実行中	
1540	情報	クイック不正プログラム検索キャンセル	このイベントにはいくつか原因があります。"不正プログラム対策 検索の失敗とキャンセル" on page 1158を参照してください。
1541	情報	不正プログラムのクイック検索の一時停止	
1542	情報	不正プログラムのクイック検索失敗の解決	
1543	警告	不正プログラムのクイック検索の失敗	"不正プログラム対策 検索の失敗とキャンセル" on page 1158を参照してください。
1544	情報	不正プログラムのクイック検索の再開	
1545	情報	ファイルで不正プログラムを検索できませんでした	ファイルパスが最大文字数を超えたため、不正プログラム対策がファイルを検索できませんでした。ファイルパスの最大長はOSとファイルシステムに応じて異なります。この問題を解決するには、ディレクトリパスにファイルを移動して、少ない文字数でファイル名を設定してください。
1546	情報	ファイルで不正プログラムを検索できませんでした	場所がディレクトリの深さの上限を超えたため、不正プログラム対策がファイルを検索できませんでした。この問題を解決するには、ネストするディレクトリの階層数を減らしてください。
1547	情報	不正プログラムの予約検索タスクのキャンセル	
1550	情報	Webレピュテーション設定のアップデート	
1551	情報	不正プログラム検索設定のアップデート	
1552	情報	変更監視設定のアップデート	
1553	情報	セキュリティログ監視設定のアップデート	
1554	情報	ファイアウォールステートフル設定のアップデート	
1555	情報	侵入防御設定のアップデート	

ID	重要度	イベント	説明または解決策
1556	情報	不正プログラム対策検索除外設定のアップデート	
1600	情報	Relayグループのアップデートの要求	
1601	情報	Relayグループのアップデートの成功	
1602	エラー	Relayグループのアップデートの失敗	
1603	情報	セキュリティアップデート: セキュリティアップデートのロールバック成功	
1604	警告	セキュリティアップデート: セキュリティアップデートのロールバック失敗	
1605	情報	ホストへのファイルバックアップコマンドの送信成功	
1606	警告	ホストへのファイルバックアップコマンドの送信失敗	
1607	情報	ファイルバックアップ成功	
1608	エラー	ファイルをバックアップできませんでした	
1650	警告	不正プログラム対策保護がないか、期限切れ	
1651	情報	不正プログラム対策モジュールの準備完了	
1660	情報	ベースラインの再構築の開始	
1661	情報	ベースラインの再構築の一時停止	
1662	情報	ベースラインの再構築の再開	
1663	警告	ベースラインの再	

ID	重要度	イベント	説明または解決策
		構築の失敗	
1664	警告	ベースラインの再構築の停止	
1665	情報	ベースラインの再構築の完了	
1666	情報	変更の検索の開始	
1667	情報	変更の検索の一時停止	
1668	情報	変更の検索の再開	
1669	警告	変更の検索の失敗	
1670	警告	変更の検索の停止	
1671	情報	変更の検索の完了	
1675	エラー	変更監視エンジンがオフライン	
1676	情報	変更監視エンジンのオンライン復帰	
1677	エラー	TPMのエラー	
1678	情報	TPMのレジスタ値の読み込み	
1679	警告	TPMのレジスタ値の変更	
1680	情報	TPMチェックが無効	
1681	情報	TPM情報の信頼性なし	
1700	情報	Agentが検出されない	
1800	エラー	Deep Security Protectionモジュールの障害	
1801	情報	Deep Security Protectionモジュールが正常な状態に復帰	
1900	情報	クラウドアカウントの追加	
1901	情報	クラウドアカウントの削除	
1902	情報	クラウドアカウント	

ID	重要度	イベント	説明または解決策
		のアップデート	
1904	情報	クラウドアカウント同期の完了	
1905	エラー	クラウドアカウント同期の失敗	
1906	情報	クラウドアカウント同期の要求	
1907	情報	クラウドアカウント同期のキャンセル	
1908	情報	AWSアカウントの同期要求	
1909	情報	AWSアカウントの同期完了	
1910	エラー	AWSアカウントの同期失敗	
1911	情報	AWSアカウントの追加	
1912	情報	AWSアカウントの削除	
1913	情報	AWSアカウントのアップデート	
1914	情報	Azureアカウントの追加	
1915	情報	Azureアカウントの削除	
1916	情報	Azureアカウントのアップデート	
1917	情報	Azureアカウントの同期完了	
1918	エラー	Azureアカウントの同期失敗	
1919	情報	Azureアカウントの同期要求	
1920	警告	Azureアカウントの同期完了 (エラーあり)	
1921	情報	vCloudアカウントの追加	
1922	情報	vCloudアカウントの削除	
1923	情報	vCloudアカウントのアップデート	
1924	情報	vCloudアカウントの同期完了	

ID	重要度	イベント	説明または解決策
1925	エラー	vCloudアカウントの同期失敗	
1926	情報	vCloudアカウントの同期要求	
1927	情報	AWSアカウントへのコネクタのアップグレード要求	
1928	警告	AWSアカウントのアップデート失敗	
1929	情報	AWSアカウントへのコネクタのアップグレードの完了	
1930	情報	AWSアカウントの移行要求	
1931	情報	AWS Accountの移行中	
1932	情報	AWSアカウントの移行完了	
1933	警告	AWSアカウントの移行失敗	
1934	情報	GCPアカウントの移行要求	
1935	情報	GCPアカウントの移行が進行中	
1936	情報	GCPアカウントの移行完了	
1937	警告	GCPアカウントの移行失敗	
1938	情報	Azureアカウントの移行要求	
1939	情報	Azureアカウントの移行中	
1940	情報	Azureアカウントの移行完了	
1941	警告	Azureアカウントの移行失敗	
1950	情報	テナントの作成	
1951	情報	テナントの削除	
1952	情報	テナントのアップデート	
1953	情報	テナントのデータベースサーバの作成	
1954	情報	テナントのデータベースサーバの削	

ID	重要度	イベント	説明または解決策
		除	
1955	情報	テナントのデータベースサーバのアップデート	
1956	情報	テナントのエクスポート	
1957	エラー	テナントの初期化失敗	
1958	情報	テナント機能のアップデート	
2000	情報	検索キャッシュ設定オブジェクトの追加	
2001	情報	検索キャッシュ設定オブジェクトの削除	
2002	情報	検索キャッシュ設定オブジェクトのアップデート	
2100	情報	Deep Security as a Serviceサブスクリプションが開始されました	
2101	情報	Deep Security as a Serviceサブスクリプションがキャンセルされました	
2102	情報	クレバーブリッジの数量がアップデートされました	
2103	警告	クレバーブリッジの数量がアップデートされていません	
2104	情報	クレバーブリッジの数量がリセットされました	
2105	警告	クレバーブリッジの数量がリセットされていません	
2106	情報	クレバーブリッジの課金日が設定されました	
2107	警告	クレバーブリッジの課金日が設定さ	

ID	重要度	イベント	説明または解決策
		れていません	
2108	情報	Deep Security as a Serviceサブスクリプションのお支払いを受領しました	
2109	警告	Deep Security as a Serviceサブスクリプションのお支払いを受領していません	
2110	情報	クレバーブリッジから通知を受信しました	
2111	情報	Deep Security as a Serviceサブスクリプションが無効化されました	
2112	情報	アカウント残高がリセットされました	
2113	情報	Agentのインストールの要求	
2114	情報	AWS課金ジョブの開始	
2115	情報	AWS課金ジョブの完了	
2116	エラー	AWS課金エラー	AWS SDKを使用してDeep Security ManagerからAWSに課金使用状況レコードを送信した結果、SDKに例外が返されました。問題が解決しない場合は、サポート担当者に問い合わせてください。
2117	情報	資格の作成	
2118	情報	資格のアップデート	
2119	エラー	AWS Metering課金使用状況データの送信に失敗したためAgentの有効化に失敗	
2120	エラー	AWS課金エラー	AWS課金ジョブの実行中にDeep Security Managerでエラーが発生しました。問題が解決しない場合は、サポート担当者に問い合わせてください。
2123	エラー	Azure Marketplace課金ジョブの失敗	消費ベースの課金のためにホストの使用統計をAzure Marketplaceに送信するために使用されたジョブが失敗しました。このイベントの原因となったエラーの詳細については、イベントの説明を参照してください。

ID	重要度	イベント	説明または解決策
2126	エラー	Event Storage Settings Publish Job Failed	
2200	情報	ソフトウェアアップデート: 不正プログラム対策モジュールのインストール開始	
2201	情報	ソフトウェアアップデート: 不正プログラム対策モジュールのインストール成功	このイベントは、アプリケーションコントロール または 変更監視 をインストールすることによってもトリガされます。これらのイベントは、不正プログラム対策と同じフレームワークを共有するためです。
2202	警告	ソフトウェアアップデート: 不正プログラム対策モジュールのインストール失敗	
2203	情報	ソフトウェアアップデート: 不正プログラム対策モジュールのダウンロード成功	
2204	情報	セキュリティアップデート: Agent/Appliance でのパターンファイルのアップデート成功	
2205	警告	セキュリティアップデート: Agent/Appliance でのパターンファイルのアップデート失敗	
2206	情報	セキュリティアップデート: Agent/Appliance でのパターンファイルアップデートがスキップされました	
2207	警告	サンドボックス分析の1日あたりの送信可能数の上限到達	
2209	警告	不正プログラム対	不正プログラム対策エンジンには、基本的な機能しかありません。

ID	重要度	イベント	説明または解決策
		策エンジン(基本機能)	詳細については、「不正プログラム対策の基本機能のみ」を参照してください。
2210	情報	必要なホスト権限を許可: 不正プログラム対策	
2211	エラー	ホスト権限が必要: 不正プログラム対策	
2300	情報	ソフトウェアアップデート: Webレピュテーションモジュールのインストール開始	
2301	情報	ソフトウェアアップデート: Webレピュテーションモジュールのインストール成功	
2302	警告	ソフトウェアアップデート: Webレピュテーションモジュールのインストール失敗	
2303	情報	ソフトウェアアップデート: Webレピュテーションモジュールのダウンロード成功	
2304	エラー	Webレピュテーションエンジンがオフライン	
2305	情報	Webレピュテーションエンジンがオンライン復帰	
2306	警告	機能が制限された状態でWebレピュテーションエンジンが動作	
2307	情報	すべてのインタフェースでWebレピュテーションエンジンがオンライン復帰	
2308	警告	Webレピュテーションエンジンが無効	

ID	重要度	イベント	説明または解決策
2309	情報	Webレピュテーションエンジンが有効	
2400	情報	ソフトウェアアップデート: ファイアウォールモジュールのインストール開始	
2401	情報	ソフトウェアアップデート: ファイアウォールモジュールのインストール成功	
2402	警告	ソフトウェアアップデート: ファイアウォールモジュールのインストール失敗	
2403	情報	ソフトウェアアップデート: ファイアウォールモジュールのダウンロード成功	
2404	警告	機能が制限された状態でファイアウォールエンジンが動作	
2405	情報	すべてのインタフェースでファイアウォールエンジンがオンライン復帰	
2406	警告	ファイアウォールエンジンが無効	
2407	情報	ファイアウォールエンジンが有効	
2500	情報	ソフトウェアアップデート: 侵入防御モジュールのインストール開始	
2501	情報	ソフトウェアアップデート: 侵入防御モジュールのインストール成功	
2502	警告	ソフトウェアアップデート: 侵入防御モジュールのイ	

ID	重要度	イベント	説明または解決策
		ンストール失敗	
2503	情報	ソフトウェアアップデート: 侵入防御モジュールのダウンロード成功	
2504	警告	機能が制限された状態で侵入防御エンジンが動作	
2505	情報	すべてのインタフェースで侵入防御エンジンがオンライン復帰	
2506	警告	侵入防御エンジンが無効	
2507	情報	侵入防御エンジンが有効	
2600	情報	ソフトウェアアップデート: 変更監視モジュールのインストール開始	
2601	情報	ソフトウェアアップデート: 変更監視モジュールのインストール成功	
2602	警告	ソフトウェアアップデート: 変更監視モジュールのインストール失敗	
2603	情報	ソフトウェアアップデート: 変更監視モジュールのダウンロード成功	
2604	情報	変更監視保護を完了するためにコンピュータの再起動が必要	
2605	情報	Managerがイベント内の変更監視ベースラインのAgentによる送信を要求	
2606	情報	Agentがイベント内の変更監視ベースラインを送信	

ID	重要度	イベント	説明または解決策
2700	情報	ソフトウェアアップデート: セキュリティログ監視モジュールのインストール開始	
2701	情報	ソフトウェアアップデート: セキュリティログ監視モジュールのインストール成功	
2702	警告	ソフトウェアアップデート: セキュリティログ監視モジュールのインストール失敗	
2703	情報	ソフトウェアアップデート: セキュリティログ監視モジュールのダウンロード成功	
2800	情報	ソフトウェアアップデート: ソフトウェアの自動ダウンロード完了	
2801	エラー	ソフトウェアアップデート: ダウンロードセンターのインベントリ取得失敗	
2802	エラー	ソフトウェアアップデート: ダウンロードセンターからのソフトウェアのダウンロード失敗	
2803	情報	オンラインヘルプのアップデート開始	
2804	情報	オンラインヘルプのアップデート完了	
2805	情報	オンラインヘルプのアップデート成功	
2806	警告	オンラインヘルプのアップデート失敗	

ID	重要度	イベント	説明または解決策
2900	情報	ソフトウェアアップデート: Relayモジュールのインストール開始	
2901	情報	ソフトウェアアップデート: Relayモジュールのインストール成功	
2902	警告	ソフトウェアアップデート: Relayモジュールのインストール失敗	
2903	情報	ソフトウェアアップデート: Relayモジュールのダウンロード成功	
2904	情報	VMware NSX同期の完了	
2905	エラー	VMware NSX同期の失敗	
2906	情報	Agentセルフプロテクションの有効化	Deep Security Manager経由でAgentセルフプロテクションが有効化されました。
2907	情報	Agentセルフプロテクションの無効化	
2908	情報	Agentセルフプロテクションの有効化	Deep Security Agentのコマンドラインを使用してAgentセルフプロテクションが有効化されました。
2909	情報	Agentセルフプロテクションの無効化	
2915	情報	データ移行完了	
2916	警告	データ移行完了(エラーあり)	
2920	情報	Deep Discovery Analyzerからのレポートの取得完了	
2921	エラー	Deep Discovery Analyzerからのレポートの取得失敗	
2922	情報	Deep Discovery Analyzerへの送	

ID	重要度	イベント	説明または解決策
		信の処理	
2923	エラー	Deep Discovery Analyzerへのファイル送信の失敗	
2924	情報	セキュリティアップデート: 不審オブジェクトの確認とアップデートに成功	
2925	エラー	セキュリティアップデート: 不審オブジェクトの確認とアップデートに失敗	
2926	警告	Deep Discovery Analyzerへの送信の処理待ち	
2930	情報	ファイルバックアップの保留中	
2931	情報	追加されたスマートフォルダ	
2932	情報	削除されたスマートフォルダ	
2933	情報	更新されたスマートフォルダ	
2934	エラー	Amazon SNSメッセージの送信失敗	
2935	情報	SNSメッセージの送信再開	
2937	情報	SAMLアイデンティティプロバイダの作成	
2938	情報	SAMLアイデンティティプロバイダのアップデート	
2939	情報	SAMLアイデンティティプロバイダの削除	
2940	情報	SAMLサービスプロバイダのアップデート	
2941	エラー	ニュースのアップデートの失敗	このイベントはDeep Security Managerバージョン20.0.313 (20 LTS Update 2021-01-18) 以降では利用できません
2942	情報	パフォーマンスプロ	

ID	重要度	イベント	説明または解決策
		ファイルが作成されました	
2943	情報	パフォーマンスプロファイルがアップデートされました	
2944	情報	パフォーマンスプロファイルが削除されました	
2945	情報	システムのアップグレード開始	
2946	情報	システムのアップデート成功	
2947	エラー	システムのアップグレード失敗	
2948	情報	Managerノードのアップグレード開始	
2949	情報	Managerノードのアップデート成功	
2950	エラー	Managerノードのアップグレード失敗	マルチノード環境のノードがアップグレードに失敗しました。
2951	エラー	TICメッセージを送信できませんでした	管理下の検出および応答イベントを送信できませんでした。
2952	情報	TICメッセージの送信再開	
2953	情報	非アクティブなAgentのクリーンナップが正常に完了しました	非アクティブなエージェントのクリーンアップは、指定された期間のためにオフラインにし、非アクティブになっているコンピュータを削除します。非アクティブなエージェントのクリーンナップの詳細については、"非アクティブなAgentのクリーンナップによるオフラインコンピュータの削除の自動化" on page 1520を参照してください。
2954	警告	記録日時が未来の日時になっているイベントを破棄しました	
2955	情報	パブリックCAチェーンがインポートされました(dsm_cコマンドを使用)	
2656	情報	パブリックCAチェーンが削除されました(dsm_cコマンドを使用)	

ID	重要度	イベント	説明または解決策
2957	情報	管理者の認証局証明書が更新されました(初期設定では自動的に10年ごとに発生します) 。	
2958	情報	初期設定のTLS証明書が更新されました(初期設定では2年ごとに自動的に実行されます) 。	
2960	情報	Appliance (SVM) のアップグレードを要求	Deep Security Managerがアップグレード要求を受信しました。
2961	情報	Appliance (SVM) のアップグレード開始	Deep Security Managerによってアップグレード処理が実行されています。
2962	情報	Appliance (SVM) のアップグレードのキャンセル	Appliance SVMが使用不可のため、アップグレードを実行できませんでした。原因については、システムイベントの説明を参照してください。
2963	情報	Appliance (SVM) のアップグレード完了	Appliance SVMが新しいバージョンにアップグレードされ、正常に有効化されました。Appliance有効化の3分後に、すべてのゲスト仮想マシンが自動で有効化されます。
2964	警告	Appliance (SVM) のアップグレード失敗	Deep Security Managerで1つ以上のエラーが発生し、アップグレードプロセスが失敗しました。詳細については"「Appliance (SVM) のアップグレード失敗」システムイベントのトラブルシューティング" on page 1691を参照してください。
2965	エラー	Appliance (SVM) のアップグレード完了 - 準備未完了	Appliance SVMが新しいバージョンにアップグレードされたものの、まだ有効化されていない状態であるか、Appliance SVMが有効化されたものの、ゲスト仮想マシンがまだ自動で有効化されていない状態です。詳細については、システムイベントの説明を参照してください。Applianceのインストールを確認し、Applianceまたはゲスト仮想マシンの有効化を手動で実行することが必要になる場合があります。
2969	情報	予約タスクのスキップ	
2970	情報	GCPアカウントの追加	GCPアカウント: <GCPアカウント名>が正常に追加されました。 詳細については、"Google Cloud Platformアカウントを追加する" on page 700を参照してください。
2971	情報	GCPアカウントの	GCPアカウント: <GCPアカウント名>が正常に削除されました。

ID	重要度	イベント	説明または解決策
		削除	詳細については、"GCPアカウントを削除する" on page 703を参照してください。
2972	情報	GCPアカウントのアップデート	GCPアカウント: <GCPアカウント名>が正常にアップデートされました。 詳細については、"Google Cloud Platformアカウントを追加する" on page 700を参照してください。
2973	情報	GCPアカウントの同期完了	GCPアカウントの完了したコンピュータを同期: <GCPアカウント名> 詳細については、"GCPアカウントを同期する" on page 704を参照してください。
2974	エラー	GCPアカウントの同期失敗	Deep Security Managerはコンピュータを GCPアカウントと同期できませんでした: <GCPアカウント名> *<detailed_message>* 次に例を示します。 ルートURLは無効です。 詳細については、"GCPアカウントを同期する" on page 704を参照してください。
2975	情報	GCPアカウントの同期要求	コンピュータをGCPアカウントと同期するように要求されました: <GCPアカウント名> 詳細については、"GCPアカウントを同期する" on page 704を参照してください。
2976	警告	GCPアカウントの同期完了 (エラーあり)	GCPアカウント<GCPアカウント名>の同期処理は完了しましたが、次のメッセージで次のホストまたはグループの情報を更新できませんでした。 *<detailed_message>* 次に例を示します。 プロジェクト <GCPprojectname>: 403projects/<GCPprojectname>'の'compute.machineTypes.list'アクセス許可が必要です 詳細については、"GCPアカウントを同期する" on page 704を参照してください。

ID	重要度	イベント	説明または解決策
2990	情報	XDRサービスの登録	
2991	情報	XDRサービスの削除	
2992	警告	VMware NSXのポリシー設定の競合	Deep Security Managerは、次のNSX-Tグループでエンドポイント保護とネットワークイントロスペクション(E-W)に異なるセキュリティポリシーが使用されていることを検出しました: <group_names> NSX-Tに移動し、同じセキュリティポリシーを使用するようにグループを再設定します。 詳細については、「"方法3: Deep SecurityポリシーをNSX-T 3.xと同期する" on page 608」を参照してください。
2993	警告	XDR証明書の期限切れ	
2994	警告	XDR製品コネクタがありません	
2995	情報	XDR証明書がアップデートされました	
2996	警告	XDR証明書のアップデートに失敗しました	
2997	警告	ホストGUIDの取得に失敗しました	
2998	警告	ホストGUIDが無効です	
3000	情報	ソフトウェアアップデート: SAP Scannerのインストール開始	
3001	情報	ソフトウェアアップデート: SAP Scannerのインストール成功	
3002	エラー	ソフトウェアアップデート: SAP Scannerのインストール失敗	
3003	情報	ソフトウェアアップデート: SAP Scannerのダウン	

ID	重要度	イベント	説明または解決策
		ロード成功	
3004	情報	SAP: ウイルス検索アダプタがインストールされています	
3005	エラー	SAP: ウイルス検索アダプタがインストールされていません	
3006	情報	SAP: ウイルス検索アダプタは最新です	
3007	情報	SAP: ウイルス検索アダプタが最新ではありません	
3008	情報	SAP: 不正プログラム対策モジュールの準備が完了しました	
3009	エラー	SAP: 不正プログラム対策モジュールの準備ができていません	
3050	情報	ソフトウェアアップデート: ICAP Scannerのインストール開始	
3051	情報	ソフトウェアアップデート: ICAP Scannerのインストール成功	
3052	警告	ソフトウェアアップデート: ICAP Scannerのインストール失敗	
3053	情報	ソフトウェアアップデート: ICAP Scannerのダウンロード成功	
3100	情報	ソフトウェアアップデート: コンテナコントロールモジュールのインストール開始	
3101	情報	ソフトウェアアップ	

ID	重要度	イベント	説明または解決策
		デート: コンテナコントロールモジュールのインストール成功	
3102	警告	ソフトウェアアップデート: コンテナコントロールモジュールのインストール失敗	
3103	情報	ソフトウェアアップデート: コンテナコントロールモジュールのダウンロード成功	
3104	情報	コンテナコントロール: 認証プラグインのインストール成功	
3105	エラー	コンテナコントロール: 認証プラグインのインストールに失敗しました	
3106	情報	コンテナコントロール: 認証プラグインのDockerへの接続完了	
3107	エラー	コンテナコントロール: 認証プラグインのDockerへの接続失敗	
3108	情報	コンテナコントロール: 認証プラグインの設定の送信成功	
3109	エラー	コンテナコントロール: 認証プラグインの設定の送信失敗	
3110	エラー	コンテナコントロール: 認証プラグインのリクエストの解析失敗	
3111	情報	ユーザによるコンテナコントロールイベントの表示	
3112	情報	コンテナコントロー	

ID	重要度	イベント	説明または解決策
		ルセキュリティイベントのエクスポート	
3113	情報	Registry Scannerの作成	
3114	情報	Registry Scannerの削除	
3115	情報	Registry Scannerのアップデート	
3116	エラー	Registry Scannerの切断	
3300	情報	コンピュータがvCenterアカウントに追加されました	
3301	警告	同じ仮想UUIDを持つ重複するホストが見つかりました	スタンドアロンホストをvCenterに移動できません(<vCenterの名前>)。Deep Securityは同じ仮想UUIDを持つ次のホストを検出しました(<The UUID>):<ホスト>
3400	情報	デバイスコントロールUSBデバイスが作成されました。	
3401	情報	デバイスコントロールUSBデバイスがアップデートされました。	
3402	情報	デバイスコントロールUSBデバイスが削除されました。	
3403	エラー	デバイスコントロールエンジンがオフラインです	デバイスコントロールエンジンがオフラインであるため、デバイスポリシーが機能しておらず、適用されていない可能性があります。これは通常、エンジンの初期化中のエラー、またはプラットフォームがオフラインであることが原因です(プラットフォームは、不正プログラム対策ソリューションプラットフォームまたはAMSPと呼ばれることもあり、トレンドマイクロソリューションプラットフォームと呼ばれることもあります)。コンピュータのプラットフォームのステータスを確認します。
3404	情報	デバイスコントロールエンジンがオンラインに戻りました。	
3405	情報	デバイスコントロールイベントがエクスポートされ	

ID	重要度	イベント	説明または解決策
		ました。	
3406	情報	ユーザがデバイスコントロールイベントを表示しました。	
3500	情報	Service Gatewayの追加	
3501	情報	Service Gatewayの削除	
3502	情報	Service Gatewayのアップデート	
3600	情報	脅威インテリジェンスのステータス公開ジョブの開始	
3601	情報	脅威インテリジェンスのステータス公開ジョブの完了	
3602	エラー	脅威インテリジェンスのステータス公開ジョブの失敗	
7000	情報	アプリケーションコントロールセキュリティイベントのエクスポート	管理者がアプリケーションコントロールイベントログをCSV形式でダウンロードしました。
7007	情報	ユーザがアプリケーションコントロールイベントを確認	管理者がアプリケーションコントロールアラートを消去しました。管理者ログインに成功した侵入者によってシステムが侵害された場合を除いて、これは正常な動作です。
7008	エラー	アプリケーションコントロールエンジンオフライン	Agentのアプリケーションコントロールエンジンをオンラインにできませんでした。このエラーは、カーネルがサポートされていないコンピュータでアプリケーションコントロールを有効にした場合に発生することがあります。
7009	情報	アプリケーションコントロールエンジンのオンライン復帰	Agentのアプリケーションコントロールエンジンが再起動されました。
7010	情報	アプリケーションコントロール設定のアップデート	Deep Security Managerによって、エージェントのアプリケーション制御設定が更新されました。
7011	情報	ソフトウェアアップデート: アプリケー	エージェントは、アプリケーション制御が選択されたDeep Security Managerからポリシーを受信しましたが、アプリケーション制御エンジ

ID	重要度	イベント	説明または解決策
		ションコントロールモジュールのインストール開始	ンがインストールされていないか、またはアップデートが必要であることが検出されてダウンロードが開始されました。コンピュータで初めてアプリケーションコントロールを有効にした場合、またはアプリケーションコントロールエンジンアップデートのリリース中にアプリケーションコントロールが無効にされていた場合、これは正常な動作です。
7012	情報	ソフトウェアアップデート: アプリケーションコントロールモジュールのインストール成功	Agentによってアプリケーションコントロールエンジンがインストールされました。また、アプリケーションコントロールエンジンは、変更監視機能によっても使用されます。
7013	エラー	ソフトウェアアップデート: アプリケーションコントロールモジュールのインストール失敗	Agentでアプリケーションコントロールエンジンをインストールできませんでした。これは正常な動作ではありません。
7014	情報	ソフトウェアアップデート: アプリケーションコントロールモジュールのダウンロード成功	Agentによるアプリケーションコントロールエンジンのダウンロードが完了しました。
7015	情報	アプリケーションコントロールルールセットのルールアップデート	従来のREST APIがソフトウェアの許可またはブロックに使用されました。このメッセージは、管理者がGUIで同じ操作を実行したときには表示されません。
7020	情報	アプリケーションコントロールインベントリの取得	レガシREST API により、コンピュータの初期許可ルールがDeep Security Managerにアップロードされました。
7021	情報	アプリケーションコントロールインベントリ検索の開始	アプリケーションコントロールエンジンが有効化されましたが、そのコンピュータに許可ルールが存在しないことがAgentによって検知されたため、現在インストールされているソフトウェアに基づいて初期ルールの構築が開始されました。これは、アプリケーションコントロールを初めて有効にしたときの正常な動作です。このメッセージは、従来のREST APIを使用して許可ルールを置き換えるときには発生しません。
7022	情報	アプリケーションコントロールインベントリ検索の完了	Agentによるそのコンピュータの初期設定許可ルールの構築が完了しました。以降、許可またはブロックルールに登録されていないソフトウェアが新たに検出された場合は原因とアラート(設定されている場合)の対象になります。
7023	エラー	アプリケーションコントロールインベントリ検索の失敗	Agentはそのコンピュータの初期設定許可ルールを構築できませんでした。これは正常な動作ではありません。
7024	情報	アプリケーションコントロールソフトウェア変更の検出	管理者が[処理]タブでソフトウェアを許可またはブロックしたか、アプリケーションコントロールログメッセージで[ルールの変更]をクリックしてルールを変更しました。このメッセージは、従来のREST APIを使用して許可ルールを置き換えるときには発生しません。

ID	重要度	イベント	説明または解決策
7025	情報	アプリケーションコントロールインベントリ検索の要求	現在のルールを削除し、現在インストールされているソフトウェアに基づいてルールを再構築するように、管理者が手動で要求しました。複数のルールを同時に変更する必要がある場合、これは正常な操作です。
7026	情報	アプリケーションコントロールメンテナンスモードの開始要求	メンテナンスモードを有効にするコマンドが管理者により送信されたか、従来のREST APIにより受信されました。
7027	情報	アプリケーションコントロールメンテナンスモードの停止要求	メンテナンスモードを無効にするコマンドが管理者により送信されたか、従来のREST APIにより受信されました。
7028	情報	アプリケーションコントロールメンテナンスモードの開始	メンテナンスモードが有効化されました。このモードが有効な場合、アップデートまたは新規にインストールされたソフトウェアは、アップデートを許可する既知のソフトウェアとして許可ルールに自動的に追加されます。ブロックルールは、この間も引き続き適用されます。
7029	情報	アプリケーションコントロールメンテナンスモードの停止	メンテナンスモードが無効化されました。メンテナンスモードの停止中は、新規または変更されたソフトウェアが見つかると、明示的に許可またはブロックするまで「承認されていないソフトウェア」として処理されます。
7030	情報	アプリケーションコントロールインベントリ検索のキャンセル	Agentによって初期設定許可ルールの構築が開始されましたが、管理者によってキャンセルされました。
7031	エラー	アプリケーションコントロールルールセットの送信失敗	アプリケーションコントロールの共有ルールセットをAgentにダウンロードできませんでした。ネットワーク接続が切断されたか(AgentとRelay間のファイアウォールやプロキシなど)、Agentの空きディスク容量が十分でない可能性があります。
7032	情報	アプリケーションコントロールルールセットの送信成功	アプリケーションコントロールの共有ルールセットがAgentにダウンロードされました。管理者または従来のREST APIによってソフトウェアが許可またはブロックされた場合や、別の共有ルールセットが適用された場合の正常な動作です。
7033	情報	アプリケーションコントロールルールセットの作成	従来のREST APIによって、アプリケーションコントロールルールセットが作成されました。このメッセージは、管理者がGUIで同じ操作を実行したときには表示されません。
7034	情報	アプリケーションコントロールルールセットのアップデート	従来のREST APIにより、アプリケーションコントロールルールセットに従ってソフトウェアが許可またはブロックされました。このメッセージは、管理者がGUIで同じ操作を実行したときには表示されません。
7035	情報	アプリケーションコントロールルールセットの削除	従来のREST APIにより、アプリケーションコントロールルールセットが削除されました。このメッセージは、管理者がGUIで同じ操作を実行したときには表示されません。
7036	情報	アプリケーションコントロールメンテナンスモードの期間リセット要求	管理者がメンテナンスモードの有効期間を変更しました。

ID	重要度	イベント	説明または解決策
7037	エラー	新しく適用されたルールセットによって、実行中のプロセスの一部は再起動時にブロックされます。	管理者が新しいルールセットを適用しましたが、ブロックルール内に現在実行中のプロセスがいくつか存在します。アプリケーションコントロールはプロセスを終了しますが、設定に応じてこのサービスをリブートまたは再起動すると、アラートが表示されるか、サービスがブロックされてしまいます。プロセスは承認されない場合は、プロセスを手動で終了する必要があります。承認してもプロセスがルールセットに見つからない場合は、プロセスをルールセットに追加する必要があります。
7038	エラー	未解決のソフトウェア変更数の上限に達しました	ファイルシステムで検出されたソフトウェア変更数が上限を超えました。アプリケーションコントロールは引き続き既存のルールを適用しますが、これ以上の変更は記録されず、このコンピュータでのソフトウェアの変更は表示されなくなります。この状況を解決し、大量のソフトウェア変更が発生しないようにする必要があります。
7040	エラー	アプリケーションコントロールルールセットに互換性がありません	アプリケーションコントロールルールセットを1台以上のコンピュータに割り当てることができませんでした。これは、インストールされているAgentのバージョンでこのルールセットがサポートされていないためです。通常、ハッシュベースのルールセットが古いDeep Security Agentに割り当てられていることが問題です。ハッシュベースのルールセットと互換性があるのは、Deep Security Agent 11.0以降のみです。Deep Security Agent 10.xでは、ファイルベースのルールセットのみをサポートしています(詳細については、"Deep Security Agent 10と11におけるファイルの比較方法の相違点" on page 1099を参照してください)。この問題を解決するには、Deep Security Agentをバージョン11.0以降にアップグレードしてください。ローカルルールセットを使用している場合は、Agentのアプリケーションコントロールをリセットする方法もあります。また、共有ルールセットを使用している場合は、共有ルールセットを使用するすべてのAgentをDeep Security Agent 11.0以降にアップグレードするまで、Deep Security 10.xで作成した共有ルールセットを使用します。
7041	情報	アプリケーションコントロールルールセットをアップグレードしました	アプリケーションコントロールのルールセットがファイルベースのルールセットからハッシュベースのルールセットにアップグレードされました。詳細については、"Deep Security Agent 10と11におけるファイルの比較方法の相違点" on page 1099を参照してください。
7042	情報	アプリケーションコントロールソフトウェアインベントリが削除されました	
7043	情報	アプリケーションコントロールの保護を完了するにはコンピュータの再起動が必要です	
7044	情報	アプリケーションコントロール ルールセットを送信しています	Managerがアプリケーションコントロール ルールセットをリモートエージェントに送信しています。

ID	重要度	イベント	説明または解決策
7045	エラー	アプリケーションコントロール ルールセットの送信に失敗しました	Managerが、アプリケーションコントロール ルールセットをリモートエージェントに送信できませんでした。
7046	情報	アプリケーションコントロール信頼ルールが作成されました	
7047	情報	アプリケーションコントロール信頼ルールが更新されました	
7048	情報	アプリケーションコントロール信頼ルールが削除されました	
7049	情報	アプリケーションコントロール信頼ルールセットが作成されました	
7050	情報	アプリケーションコントロール信頼ルールセットが更新されました	
7051	情報	アプリケーションコントロール信頼ルールセットが削除されました	
9100	情報	移行要求済み	
9101	情報	移行中	
9102	警告	移行失敗	"エージェントをTrend Vision One Endpoint Security - Server & Workload Protectionに移行する" on page 1759を参照してください。
9103	警告	移行失敗 (応答がありません)	"エージェントをTrend Vision One Endpoint Security - Server & Workload Protectionに移行する" on page 1759を参照してください。
9104	警告	移行失敗 (有効化に失敗しました)	"エージェントをTrend Vision One Endpoint Security - Server & Workload Protectionに移行する" on page 1759を参照してください。
9105	情報	移行完了	
9106	エラー	移行失敗 (非管理対象です)	"エージェントをTrend Vision One Endpoint Security - Server & Workload Protectionに移行する" on page 1759を参照してください。
9107	情報	Workload Securityリンクを	

ID	重要度	イベント	説明または解決策
		作成	
9108	情報	Workload Securityリンクを更新	
9109	情報	Workload Securityリンクを削除	
9200	警告	サンドボックス分析の1日あたりの送信可能数の上限到達	
9201	情報	Sandbox as a Serviceの登録	
9202	情報	Sandbox as a Serviceの登録更新完了	
9203	警告	Sandbox as a Serviceの登録更新失敗	
9204	情報	Sandbox as a Serviceの削除	
9210	情報	Cisco ANCポリシーが割り当てられました	Cisco ANCポリシーがMACアドレスに正常に割り当てられました。
9211	警告	Cisco ANCポリシーの割り当て失敗	Cisco ANCポリシーをMACアドレスに割り当てることができませんでした。ISEサーバが失敗ステータスを返していました。
9212	警告	Cisco pxGrid接続失敗	Cisco pxGridサーバに接続できません。
9213	警告	Cisco pxGridクライアント証明書の有効期限が切れました	Cisco ISE pxGridルート証明書またはクライアント証明書の有効期限が切れています。
9300	警告	Trend Micro LightWeight Filter Driverが無効になりました	
9301	情報	Trend Micro LightWeight Filter Driverが再起動されました	
9302	情報	すべてのTrend Micro LightWeight Filter Driverが正	

ID	重要度	イベント	説明または解決策
		常に再起動されました	
9303	警告	すべてのネットワークインタフェースでTrend Micro LightWeight Filter Driverのバインドに失敗しました	
10001	情報	AWS課金使用状況データの送信成功	
10002	エラー	AWS課金使用状況データの送信失敗	
10003	情報	AWS Marketplace請求使用データCSVエクスポート	
10004	エラー	AWSマーケットプレイスの請求使用データ送信の失敗によりエージェントのアクティベーションが防止されました	
11000	エラー	Vision One Big Tableへのデータ送信の失敗	
11001	情報	Vision One Big Tableへのデータ送信の再開	

アプリケーションコントロールイベント

イベントに関連する一般的なベストプラクティスについては、"Deep Securityイベントログについて" on page 1150についてを参照してください。

を参照するにはアプリケーションコントロールDeep Securityによってキャプチャされたイベントの場合は、[イベントとレポート→[イベント→[アプリケーションコントロールイベント→[セキュリティイベントます。

アプリケーションコントロールイベントで表示される情報

[アプリケーションコントロールイベント] 画面には次の列が表示されます。[列] をクリックして、表に表示する列を選択することができます。

- 時刻: コンピュータ上でイベントが発生した時刻。
- コンピュータ: このイベントのログが記録されたコンピュータ(コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- イベント: イベントの名前。
- ルール: イベント詳細を表示して、ルールの許可とブロックを切り替えることができます。
- ルールセット: イベントに関連付けられているルールセット。
- 処理: イベントをトリガさせた処理。
- 理由: イベントがトリガされた理由。
- 反復カウント: 集約されるイベントの数。
- タグ: このイベントに関連付けられたイベントのタグ。
- パス: 影響を受けたファイルへのパス。
- ファイル: イベントの影響を受けたファイル。
- ユーザ名: 承認されていないソフトウェアの実行を担当したユーザ。
- イベントの起点: イベントが発生したDeep Securityコンポーネントです。
- MD5: MD5ハッシュ。
- SHA1: SHA-1ハッシュ。
- SHA256: SHA-256ハッシュ。
- グループ: グループの名前。
- グループID: グループのID。
- ユーザID: ファイルの所有者のユーザID。
- プロセスID: 実行処理を実行するプロセスのID。
- プロセス名: 実行処理を実行するプロセス。

アプリケーションコントロールイベント一覧

注意: アプリケーションコントロールに関連するシステムイベントについては、"システムイベント" on page 1342を参照してください。

イベント
承認されていないソフトウェアの実行を許可
承認されていないソフトウェアの実行をブロック
ソフトウェアの実行をルールでブロック

不正プログラム対策イベント

イベントに関する全般的なベストプラクティスについては、"Deep Securityイベントログについて" on page 1150を参照してください。

Deep Securityで検出された不正プログラム対策イベントを表示するには、[イベントとレポート]→[イベント]→[不正プログラム対策イベント]順に選択します。

不正プログラム対策イベントの情報表示

次の列は不正プログラム対策イベントページに表示できます。表示する列を選択するには、列をクリックしてください。

- 時間: イベントがコンピュータで発生した時間。
- コンピュータ: このイベントが記録されたコンピュータ。コンピュータが削除された場合、このエントリは不明なコンピュータと表示されます。
- 感染ファイル: 感染したファイルの場所と名前。
- タグ: このイベントに関連付けられたイベントタグ。
- 不正プログラム: 検出された不正プログラムの名前。
- 実行された処理: イベントに関連付けられた不正プログラム検索設定で指定された処理の結果。
  - クリーン済み: Deep Securityが不正プログラムの種類に応じてプロセスの終了、レジストリ、ファイル、Cookie、ショートカットの削除を成功したことを通知するメッセージ。
  - クリーン失敗: 不正プログラムをクリーンできなかったことを通知するメッセージです。クリーンアクション(限られた種類のウイルスにのみ利用可能)が失敗した場合、次のアクションは隔離です。
  - 削除済み: 感染したファイルが削除されたことを通知するメッセージ。
  - 削除失敗: 感染したファイルが様々な理由で削除できなかったことを通知するメッセージです。例えば、ファイルが他のアプリケーションによってロックされている場合、CD上にある場合、または使用中の場合です。可能であれば、Deep Securityはファイルが解放された後に感染したファイルを削除します。削除アクションが失敗しても、システムやユーザがファイルに対して操作を行ったり実行しようとする試みはリアルタイム検索中に拒否されます。

  - 隔離されました: 感染したファイルが識別されたファイルフォルダに移動されたことを通知するメッセージです。
  - 隔離に失敗しました: 感染したファイルをさまざまな理由で隔離できなかったことを通知するメッセージです。たとえば、ファイルが他のアプリケーションによってロックされている、CD上にある、または使用中である場合です。可能であれば、Deep Securityはファイルが解放された後に感染したファイルを隔離します。また、特定されたファイルを保存するために使用される最大ディスク容量 (ポリシーまたはコンピュータエディタ> 不正プログラム対策 > 詳細設定 タブで指定) が超過している可能性もあります。隔離アクションが失敗した場合でも、リアルタイム検索中にシステムまたはユーザがファイルと対話したり実行したりしようとする試みは拒否されます。
  - アクセス拒否: Deep Securityが感染したファイルのアクセスを防止したことを通知するメッセージであり、ファイルをシステムから削除することなく行われます。
  - 合格: Deep Securityが何も行動を起こさず、不正プログラムの検出をログに記録したことを通知するメッセージ。
- 検索の種類: 不正プログラムを検出した検索の種類 (リアルタイム、スケジュール、または手動)。
- イベント送信元: イベントが発生したDeep Securityシステムのコンポーネントを示します。
- 理由: 不正プログラムが検出された時に有効だった不正プログラム検索の設定。
- 主要なウイルスタイプ: 検出された不正プログラムのタイプ。可能な値は、ジョーク、トロイの木馬、ウイルス、テスト、スパイウェア、パッカー、ジェネリックなどです。これらの不正プログラムのタイプに関する情報は、不正プログラム対策イベントの詳細を参照するか、"不正プログラム対策について" on page 821を参照してください
- ターゲット: 不正プログラムが影響を与えようとしたファイル、プロセス、またはレジストリキー(該当する場合)。不正プログラムが複数に影響を与えようとしていた場合、このフィールドには複数という値が含まれます。
- ターゲットタイプ: この不正プログラムが影響を与えようとしたシステムリソースの種類。ファイルシステム、プロセス、またはWindowsレジストリなど。
- コンテナID: 不正プログラムが発見されたDockerコンテナのID。
- コンテナイメージ名: 不正プログラムが見つかったDockerコンテナのイメージ名。
- コンテナ名: 不正プログラムが見つかったDockerコンテナの名前。
- ファイルMD5: ファイルのMD5ハッシュ。

不正プログラム対策イベントの一覧

次の表は、利用可能なすべての不正プログラム対策イベントの一覧を示しています。

ID	重要度	イベント
9001	情報	不正プログラム検索の開始
9002	情報	不正プログラム検索の完了
9003	情報	不正プログラム検索の異常終了
9004	情報	不正プログラム検索の一時停止
9005	情報	不正プログラム検索の再開
9006	情報	不正プログラム検索のキャンセル
9007	警告	不正プログラム検索キャンセルの失敗
9008	警告	不正プログラム検索開始の失敗
9009	警告	不正プログラム検索の停止
9010	エラー	ファイルを分析または隔離できません(検出ファイル保存用のVMの最大ディスク容量を超過)
9011	エラー	識別されたファイルを保存するために使用されるディスク容量が最大値を超えました。古い識別ファイルが削除されるか、新しく検出されたファイルが分析または隔離されない可能性があります。
9012	警告	スマートスキャン用のSmart Protection Serverへの接続不能
9013	情報	スマートスキャン用のSmart Protection Serverへの接続
9014	警告	不正プログラム対策保護を完了するためにコンピュータの再起動が必要
9016	情報	不正プログラム対策コンポーネントのアップデート成功
9017	エラー	不正プログラム対策コンポーネントのアップデート失敗
9018	エラー	ファイルで不正プログラムを検索できませんでした
9019	エラー	ディレクトリで不正プログラムを検索できませんでした

デバイスコントロールイベント

イベントに関する一般的なベストプラクティスについては、[Workload Securityのイベント](../events)を参照してください。

Workload Securityによって取得されたデバイスコントロールイベントを表示するには、[イベントとレポート]→[イベント]→[デバイスコントロールイベント]→[セキュリティイベント] の順に選択します。

デバイスコントロールイベントについて表示される情報を教えてください。

これらの列は、[デバイスコントロールイベント] 画面に表示できます。[列] をクリックして、テーブルに表示する列を選択できます。

- 時刻: コンピュータでイベントが発生した時刻。
- コンピュータ: このイベントが記録されたコンピュータ。(コンピュータが削除されている場合、このエントリは「不明なコンピュータ」と表示されます)。
- デバイスの種類: イベントを発生させるためにアクセスされたデバイスの種類。例: USB

- 対象: イベントのトリガの原因となったアクセスされたファイルの名前。
- アクセス元: イベントの発生原因となったプロセスの名前。
- 実行された処理:デバイスコントロールで実行された処理。
- ベンダー: デバイスのベンダーの名前。
- モデル: デバイスのモデル名またはモデル番号。
- シリアル番号: デバイスのシリアル番号。
- 製品: イベントを発生させるためにアクセスされたデバイスの名前。
- タグ: このイベントに関連付けられたイベントタグ。
- [イベントの発生元] : イベントの発生元のWorkload Securityコンポーネント。

ファイアウォールイベント

イベントに関する全般的なベストプラクティスについては、"Deep Securityイベントログについて" on page 1150を参照してください。

Deep Securityによってキャプチャされたファイアウォールイベントを表示するには、にアクセスします。イベントとレポート>イベント>ファイアウォールイベント。

ファイアウォールイベントのアイコン:

 単一イベント

 データ付き単一イベント

 折りたたみイベント

 データ付き折りたたみイベント

注意: イベントの折りたたみは、同じ種類のイベントが数回続けて発生したときに実行されます。これによりディスク容量を節約でき、ログメカニズムに負荷をかけるDoS攻撃から防御することができます。

ファイアウォールイベントで表示される情報

[ファイアウォールイベント] 画面には次の列が表示されます。[列] をクリックして、表に表示する列を選択することができます。

- 時刻: コンピュータ上でイベントが発生した時刻。
- コンピュータ: このイベントのログが記録されたコンピュータ(コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- 理由: この画面のログエントリが、ファイアウォールルールによって生成されたか、またはファイアウォールステートフル設定によって生成されたかを示します。エントリがファイアウォールルールによって生成された場合、列エントリには、「ファイアウォールルール:」と表示され、続いてファイアウォールルールの名前が表示されます。それ以外の場合、列エントリには、ログエントリを生成したファイアウォールステートフル設定の内容が表示されます。
- タグ: このイベントに適用されているイベントタグ。
- 処理: ファイアウォールルールまたはファイアウォールステートフル設定によって実行された処理。処理には、許可、拒否、強制的に許可、ログのみがあります。
- ランク: ランク付けシステムでは、侵入防御およびファイアウォールイベントの重要度を数値化できます。コンピュータに「資産評価」を割り当て、侵入防御ルールとファイアウォールルールに「重要度」を割り当て、これら2つの値を掛け合わせることによって、イベントの重要度 (ランク) が計算されます。これによって、侵入防御イベントまたはファイアウォールイベントを表示するときに、イベントをランクでソートできます。
- 方向: パケットの方向 (受信または送信)。
- インタフェース: パケットが経由するインタフェースのMACアドレス。
- フレームの種類: 対象となるパケットのフレームの種類。値は、[IPV4]、[IPV6]、[ARP]、[REVARP]、および [その他: XXXX] (XXXXはフレームの種類を示す4桁の16進コード) のいずれかになります。
- プロトコル: 値は、[ICMP]、[ICMPV6]、[IGMP]、[GGP]、[TCP]、[PUP]、[UDP]、[IDP]、[ND]、[RAW]、[TCP+UDP]、および [その他: nnn] (nnnは、3桁の10進値) のいずれかになります。
- フラグ: パケットに設定されたフラグ。
- 送信元IP: パケットの送信元IP。
- 送信元MAC: パケットの送信元MACアドレス。
- 送信元ポート: パケットの送信元ポート。
- 送信先IP: パケットの送信先IP。
- 送信先MAC: パケットの送信先MACアドレス。
- 送信先ポート: パケットの送信先ポート。
- パケットサイズ: バイト単位のパケットのサイズ。
- 繰り返しカウント: イベントが連続して繰り返された回数。
- 時間 (マイクロ秒): コンピュータ上でイベントが発生した時間 (マイクロ秒)。

- イベントの起点：イベントが発生したDeep Securityコンポーネントです。

次の列も使用できます。Deep Security Agent 12 FR以上で保護されているコンピュータ上のコンテナからトリガされたイベントの情報が表示されます。

- インタフェースの種類：コンテナインタフェースの種類。
- コンテナ名：イベントが発生したコンテナの名前。
- コンテナID：イベントが発生したコンテナのコンテナIDです。
- イメージ名：イベントが発生したコンテナの作成に使用されたイメージ名。
- RepoDigest：コンテナイメージを識別する一意の通知です。
- プロセス名：イベントの原因となった(コンテナからの)プロセスの名前。

注意：ログのみルールは、対象のパケットが、拒否ルールまたはそのパケットを除外する許可ルールによって、それ以降に停止されない場合にログエントリのみを生成します。この2つのルールのいずれかによってパケットが停止される場合は、ログのみルールではなく、これらのルールがログエントリを生成します。以降のルールでパケットを停止しない場合は、ログのみルールがエントリを生成します。

ファイアウォールイベント一覧

ID	イベント	備考
100	セッション情報なし	既存の接続に関連付けられていないパケットを受信しました。
101	不正なフラグ	パケットに設定されたフラグが無効です。このイベントは、現在の接続(存在する場合)のコンテキスト内で意味をなさないフラグ、または無意味な組み合わせのフラグであることを示しています。 接続コンテキストを評価するには「ファイアウォールステートフル設定」がオンになっている必要があります。
102	不正なシーケンス	シーケンス番号が無効なパケットまたはデータサイズが範囲外のパケットが検出されました。
103	不正なACK	確認応答番号が無効なパケットが検出されました。
104	内部エラー	
105	CEフラグ	パケットに輻輳フラグが設定されていたり、ポリシーの回避技術対策でTCP輻輳フラグプロパティがログまたは拒否に設定されているカスタム設定を使用したりしています("回避技術対策の設定" on page 948を参照)。
106	不正なIP	パケットの送信元IPが無効です。
107	不正なIPデータグラム長	IPヘッダで指定されている長さよりも短いIPデータグラム長です。
108	フラグメント化	フラグメント化されたパケットが検出されました。フラグメント化されたパケットは許可されていません。
109	不正なフラグ	

ID	イベント	備考
	メントオフセット	
110	最初のフラグメントが最小サイズ未満	フラグメント化されたパケットが検出されました。最初のフラグメントのサイズがTCPパケット(データなし)のサイズよりも小さくなっています。 パケットヘッダに次の設定が指定されている場合、パケットは破棄されます。 • フラグメントオフセット = 0 (フラグメントはパケットの最初のフラグメントです) • 合計長 (最大組み合わせヘッダ長) < 120バイト(デフォルトの許容最小フラグメントサイズ) このイベントの再発を防止するには、最小フラグメントサイズプロパティの値を低くするようにポリシーのネットワークエンジンの詳細設定を行うか、この監視をオフにするように0に設定します("ネットワークエンジン設定" on page 747の「ネットワークエンジンの詳細オプション」を参照)。
111	範囲外のフラグメント	フラグメント化されたパケットシーケンスに指定されているオフセットが、データグラムの最大サイズ範囲を超えています。
112	最小オフセット値以下のフラグメント	フラグメント化されたパケットが検出されました。フラグメントのサイズがTCPパケット(データなし)のサイズよりも小さくなっています。
113	IPv6パケット	IPv6パケットが検出されました。IPv6ブロックが有効になっています。「ネットワークエンジンの詳細オプション」の「バージョン9以降のAgentとApplianceでIPv6をブロック」プロパティ("ネットワークエンジン設定" on page 747を参照) を参照してください。
114	受信接続の上限	受信接続数が最大許容数を超えました。"TCPパケットインスペクション" on page 995の「TCPステートフルインスペクションを有効にする」プロパティを参照してください。
115	送信接続の上限	送信接続数が最大許容数を超えていました。"TCPパケットインスペクション" on page 995の「TCPステートフルインスペクションを有効にする」プロパティを参照してください。
116	SYN送信の上限	単一コンピュータからのハーフオープン接続数がファイアウォールステートフル設定に指定された数を超えています。"TCPパケットインスペクション" on page 995の「単一コンピュータからのハーフオープン接続数の上限」プロパティを参照してください。
118	不明なIPバージョン	IPv4またはIPv6以外のIPパケットが検出されました。
119	不正なパケット情報	
120	内部エンジンエラー	システムメモリの不足。システムリソースを追加してこの問題を修正します。
121	許可されていないUDP応答	コンピュータに許可されていない受信UDPパケットは拒否されます。
122	許可されてい	ファイアウォールステートフル設定でICMPステートフルが有効になっています。い

ID	イベント	備考
	ないICMP応答	ずれの「強制的に許可」ルールにも一致しない未許可のパケットを受信しました。
123	ポリシーで未許可	パケットはいずれの「許可」ルールまたは「強制的に許可」ルールにも一致しないため黙示的に拒否されます。
124	不正なポートコマンド	FTP制御チャネルのデータストリームで無効なFTPポートコマンドが検出されました。
125	SYN Cookieエラー	SYN Cookieの保護メカニズムでエラーが発生しました。
126	不正なデータオフセット	データオフセットパラメータが無効です。
127	IPヘッダなし	パケットIPヘッダが無効または不完全です。
128	読み取り不能なイーサネットヘッダ	このイーサネットフレームに含まれるデータがイーサネットヘッダよりも少なくなっています。
129	未定義	
130	送信元および送信先IPが同一	送信元IPと送信先IPが同じです。
131	不正なTCPヘッダ長	
132	読み取り不能なプロトコルヘッダ	読み取り不能なTCP、UDP、またはICMPヘッダがパケットに含まれています。
133	読み取り不能なIPv4ヘッダ	読み取り不能なIPv4ヘッダがパケットに含まれています。
134	不明なIPバージョン	IPバージョンを認識できません。
135	不正なアダプタ設定	無効なアダプタ設定を受信しました。
136	重複しているフラグメント	このパケットのフラグメントは以前に送信されたフラグメントと重複しています。
138	切断された接続上のパケット	すでに切断された接続に属するパケットを受信しました。
139	再送の破棄	ネットワークエンジンが、同じTCP接続ですでに受信したデータと重複しているTCPパケットを検出しましたが、すでに受信したデータと一致しません。(ネットワークエンジンは、エンジンの接続バッファ内の処理待ちパケットデータと再送信されたパケットのデータを比較します。) ネットワークエンジンは、処理するTCP接続ごとにデータストリームを順番に再構築します。受信パケットのシーケンス番号と長さにより、このデータストリームの特定の領域が決まります。ログの注記用フィールドは、TCPストリームで変更した次のコンテンツの場所を示します。prev-full、prev-part、next-full、および

ID	イベント	備考
		next-part。 • 「prev-full」と「prev-part」: 変更領域は、順番に整理されたデータストリームの再送信パケットをすぐに処理するパケット内にあります。「prev-full」は、変更領域が順番に整理されたデータストリームの再送信パケットをすぐに処理するパケット内に完全に含まれることを示します。それ以外の場合の注記は「prev-part」です。 • 「next-full」と「next-part」: 変更領域は、順番に整理されたデータストリームの再送信パケットのすぐ後に続くパケット内にあります。「next-full」は、変更領域が順番に整理されたデータストリームの再送信パケットのすぐ後に続くパケット内に完全に含まれることを示します。それ以外の場合の注記は「next-part」です。
140	未定義	
141	ポリシーで未許可 (オープンポート)	
142	新しい接続の開始	
143	無効なチェックサム	
144	無効なフック	
145	IPペイロードがゼロ	
146	IPv6ソースがマルチキャスト	
147	無効なIPv6アドレス	
148	最小サイズ以下のIPv6のフラグメント	
149	無効なトランスポートヘッダ長	
150	メモリ不足	
151	最大TCP接続数	TCP接続の最大数が超えました。"イベント: 最大TCP接続数" on page 1447 を参照してください。
152	最大UDP接続数	
200	リージョンサイズの超過	リージョン (編集リージョン、URIなど) が閉じられずに、バッファの最大許容サイズ (7570バイト) を超えました。これは、通常、データがプロトコルに適合していないために発生します。
201	メモリ不足	リソースがなくなったため、パケットを適切に処理できませんでした。これは、多くの同時接続によってバッファ(最大2,048) や一致リソース (最大128) が一度に

ID	イベント	備考
		要求された場合、1つのIPパケットにおける一致数 (最大2,048) を超過した場合、または単にシステムのメモリが不足した場合に発生することがあります。
202	編集回数の超過	パケットの単一リージョンにおける最大編集回数 (32回) を超えました。
203	編集範囲の超過	リージョンのサイズを最大許容サイズ (8,188バイト) よりも増やそうとする編集が試行されました。
204	パケットの最大一致数を超過	パケット内でパターンに一致する地点が2,048箇所を超えています。この制限に達するパケットは通常ガベージパケットまたは回避パケットであるため、エラーが返されて接続が破棄されます。
205	エンジンのコールスタック数の超過	
206	ランタイムエラー	ランタイムエラーです。
207	パケットの読み込みエラー	パケットデータの読み込み中に発生した低レベルの問題です。
257	Fail-Open: 拒否 (ログに記録)	破棄する必要のあるパケットを記録し、Fail-Open機能がオンでインラインモードの場合には記録しません。
300	サポートされていない暗号化	不明またはサポートされていない暗号化スイートが要求されました。
301	マスターキーの生成エラー	マスターシークレットから、暗号化キー、MACシークレット、および初期化ベクタを生成できません。
302	レコードレイヤメッセージ (準備ができていません)	SSL状態エンジンで、セッションの初期化前にSSLレコードが検出されました。
303	ハンドシェークメッセージ (準備ができていません)	SSL状態エンジンで、ハンドシェークのネゴシエーション後にハンドシェークメッセージが検出されました。
304	ハンドシェークメッセージの障害	適切にフォーマットされたハンドシェークメッセージが、誤った順序で検出されました。
305	メモリの割り当てエラー	リソースがなくなったため、パケットを適切に処理できませんでした。これは、多くの同時接続によってバッファ(最大2,048) や一致リソース(最大128) が一度に要求された場合、1つのIPパケットにおける一致数 (最大2,048) を超過した場合、または単にシステムのメモリが不足した場合に発生することがあります。
306	サポートされていないSSLバージョン	クライアントがSSL V2バージョンのネゴシエーションを試行しました。
307	プレマスターキーの復号時のエラー	ClientKeyExchangeメッセージからプレマスターシークレットを復号できません。
308	クライアントに	クライアントが、ClientHelloメッセージに指定されたバージョンより古いバージョン

ID	イベント	備考
	よるロールバックの試行	のSSLプロトコルへのロールバックを試行しました。
309	更新エラー	キャッシュされたセッションキーでSSLセッションが要求されましたが、該当するセッションキーが見つかりませんでした。
310	鍵の交換エラー	サーバが一時的に生成されたキーを使用してSSLセッションを確立しようとしています。
311	SSLキー交換の上限を超過	キー交換の同時要求数が上限を超えました。
312	鍵サイズの超過	マスターの秘密鍵がプロトコルIDで指定されたサイズを超えています。
313	ハンドシェーク内の不正なパラメータ	ハンドシェークプロトコルのデコード中に無効または不正な値が検出されました。
314	利用可能なセッションなし	
315	未サポートの圧縮方法	
316	サポートされていないアプリケーション層プロトコル	不明、またはサポートされていないSSLアプリケーション層プロトコルが要求されました。
385	Fail-Open: 拒否 (ログに記録)	破棄する必要のあるパケットを記録し、Fail-Open機能がオンでタップモードの場合には記録しません。
500	URIパスの深さが超過	区切り文字「/」が多すぎます。パスの深さは最大100です。
501	無効なトラバーサル	ルートより上位に「../」を使用しようとしました。
502	URIに使用できない文字	URIに無効な文字が使用されています。
503	不完全なUTF8シーケンス	UTF8シーケンスの途中でURIが終了しました。
504	無効なUTF8の符号化	無効または規定外のエンコードが試行されました。
505	無効な16進の符号化	%nnのnnが16進数ではありません。
506	URIパス長の超過	パス長が512文字を超えています。
507	不正な文字の使用	無効な文字を使用しています。
508	二重デコードの攻撃コード	二重デコードの攻撃コードです (%25xx、%25%xxdなど)。
700	不正なBase64コンテ	Base64形式でエンコードされるはずのパケットコンテンツが正しくエンコードされませんでした。

ID	イベント	備考
	ンツ	
710	破損したDeflate/GZIPコンテンツ	Base64形式でエンコードされるはずのパケットコンテンツが正しくエンコードされませんでした。
711	不完全なDeflate/GZIPコンテンツ	不完全なDeflate/GZIPコンテンツです
712	Deflate/GZIPチェックサムエラー	Deflate/GZIPチェックサムエラーです。
713	未サポートのDeflate/GZIP辞書	サポートされていないDeflate/GZIP辞書です。
714	サポートされていないGZIPヘッダ形式/方法	サポートされていないGZIPヘッダ形式または方法です。
801	プロトコルデコード検索の上限を超過	プロトコルデコードルールには検索またはPDUオブジェクトの制限が定義されていますが、オブジェクトを見つける前に制限に達しました。
802	プロトコルデコードの制約エラー	プロトコルデコードルールによってデコードされたデータが、プロトコルコンテンツの制約を満たしていません。
803	プロトコルデコードエンジンの内部エラー	
804	プロトコルデコードの構造の超過	プロトコルデコードルールで、型の最大ネスト深度 (16) を超える型定義とパケットコンテンツが検出されました。
805	プロトコルデコードのスタックエラー	ルールのプログラミングエラーが原因で、反復が発生したか、またはネストされたプロシージャコールが使用されようとしました。
806	データの無限ループエラー	
10002	ゼロシーケンスでリセットされるログの理由	シーケンス番号がゼロのTCPリセット(RST)パケットが複数送信されました。

侵入防御イベント

イベントに関する全般的なベストプラクティスについては、"Deep Securityイベントログについて" on page 1150を参照してください。

Deep Securityでキャプチャされた侵入防御イベントを表示するには、イベントとレポート>イベント>侵入防御イベントにアクセスします。

侵入防御イベントで表示される情報

[侵入防御イベント] 画面には次の列が表示されます。[列] をクリックして、表に表示する列を選択することができます。

- 時刻: コンピュータ上でイベントが発生した時刻。
- コンピュータ: このイベントのログが記録されたコンピュータ(コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- 理由: このイベントに関連付けられた侵入防御ルール。
- タグ: イベントに付けられたタグ。
- アプリケーションの種類: このイベントの原因となった侵入防御ルールに関連付けられたアプリケーションの種類。
- 処理: 侵入防御ルールが実行する処理 (ブロックまたはリセット)。ルールが検出のみモードの場合、処理名の前に「検出のみ:」が付きます。

  注意: Deep Security 7.5 SP1より前に作成された侵入防御ルールでは、挿入、置換、削除処理も実行することができましたが、現在これらの処理は実行されません。これらの処理の実行を試みる古いルールが実行された場合、ルールが検出のみモードで適用されたことを示すイベントが記録されます。

- ランク: ランク付けシステムでは、侵入防御およびファイアウォールイベントの重要度を数値化できます。コンピュータに「資産評価」を割り当て、侵入防御ルールとファイアウォールルールに「重要度」を割り当て、これら2つの値を掛け合わせることによって、イベントの重要度 (ランク) が計算されます。これによって、侵入防御イベントまたはファイアウォールイベントを表示するときに、イベントをランクでソートできます。
- 重要度: 侵入防御ルールの重要度。
- 方向: パケットの方向 (受信または送信)。
- フロー: このイベントを引き起こしたパケットが、侵入防御ルールで監視しているトラフィックと同じ方向に進んでいたか(「接続フロー」)、または反対方向に進んでいたか(「リバースフロー」)。
- インタフェース: パケットが通過したインタフェースのMACアドレス。
- フレームの種類: 対象となるパケットのフレームの種類。値は、[IPV4]、[IPV6]、[ARP]、[REVARP]、および [その他:XXXX] (XXXXはフレームの種類を示す4桁の16進コード) のいずれかになります。

- プロトコル: 値は、[ICMP]、[ICMPV6]、[IGMP]、[GGP]、[TCP]、[PUP]、[UDP]、[IDP]、[ND]、[RAW]、[TCP+UDP]、および [その他: nnn] (nnnは、3桁の10進値) のいずれかになります。
- フラグ: パケットに設定されたフラグ。
- 送信元IP: パケットの送信元IP。
- 送信元MAC: パケットの送信元MACアドレス。
- 送信元ポート: パケットの送信元ポート。
- 送信先IP: パケットの送信先IP。
- 送信先MAC: パケットの送信先MACアドレス。
- 送信先ポート: パケットの送信先ポート。
- パケットサイズ: バイト単位のパケットのサイズ。
- 繰り返しカウント: イベントが連続して繰り返された回数。
- 時間 (マイクロ秒): コンピュータ上でイベントが発生した時間 (マイクロ秒)。
- イベントの起点: イベントが発生したDeep Securityコンポーネントです。

次の列も使用できます。Deep Security Agent 12 FR以上で保護されているコンピュータ上のコンテナからトリガされたイベントの情報が表示されます。

- インタフェースの種類: コンテナインタフェースの種類。
- コンテナ名: イベントが発生したコンテナの名前。
- コンテナID: イベントが発生したコンテナのコンテナIDです。
- イメージ名: イベントが発生したコンテナの作成に使用されたイメージ名。
- RepoDigest: コンテナイメージを識別する一意の通知です。
- プロセス名: イベントの原因となった(コンテナからの) プロセスの名前。

侵入防御 イベントの追加情報を表示する

侵入防御 イベントをエクスポートする場合、エクスポートされたデータには上記のフィールドと、Deep Security Managerコンソールには表示されない追加のフィールドが含まれます。唯一の例外は、Severityフィールドです。このフィールドはCSVファイルでは使用できません。

- Note: CVEコードなど、イベントに意味のある文字列。
- 終了時刻: パケットが最後に確認された時刻。
- バッファ内位置: パケット内の位置。
- ストリーム内の位置: TCP / IPストリーム内のパケットの位置。
- データフラグ: データフラグの値の詳細については、次の表を参照してください。

コード	フラグ	備考
0x01	dataTruncated	データをログに記録できなかったことを示します。
0x02	logOverflow	このエントリの後にログがオーバーフローしました。
0x04	suppressed	このエントリの後にしきい値の抑制が発生したことをログに記録します。
0x08	haveData	パケットデータがログに記録されます。
0x10	refData	DataIdがログに記録されます。パケットペイロードはこのイベントに記録されません。ペイロードは、0x08フラグと同じデータインデックスを持つイベントでのみログに記録されます。
0x20	haveRawPkt	データは完全な生のパケットです。

- Data Index: パケットデータの一意のID(dataId) 。dataIdが同じレコードはすべて同じパケットのものです。
- Data: パケットのペイロード。
- Original IP(XFF) : クライアントの元のIPアドレスを表示します。このフィールドのデータを取得するには、ルール 1006450-Enable X-Forwarded-For HTTP Header Loggingを有効にします。

次のフィールドも使用できます。Deep Security Agent 12 FR以上で保護されているコンピュータ上のコンテナからトリガされたイベントの情報が表示されます。

- プロセスID: コンテナによって報告されたプロセスID。
- スレッドID: コンテナによって報告されたスレッドID。
- Image ID: コンテナイメージのローカルID。
- Pod ID: Pod ID(該当する場合) 。

侵入防御イベント一覧

ID	イベント	備考
200	リージョンサイズの超過	リージョン (編集リージョン、URIなど) が閉じられずに、バッファの最大許容サイズ (7570バイト) を超えました。これは、通常、データがプロトコルに適合していないために発生します。
201	メモリ不足	リソースがなくなったため、パケットを適切に処理できませんでした。これは、多くの同時接続が一度に行われた場合、または単にシステムのメモリが不足した場合に発生することがあります。
202	編集回数の超過	パケットの単一リージョンにおける最大編集回数 (32回) を超えました。
203	編集範囲の超過	リージョンのサイズを最大許容サイズ (8,188バイト) よりも増やそうとする編集が試行されました。
204	パケットの最大一致数を超過	パケット内でパターンに一致する地点が2,048箇所を超えています。この制限に達するパケットは通常ガベージパケットまたは回避パケットであるため、エラーが返されて接続が破棄されます。
205	エンジンのコールスタック数の超過	
206	ランタイムエラー	ランタイムエラーです。

ID	イベント	備考
207	パケットの読み込みエラー	パケットデータの読み込み中に発生した低レベルの問題です。
258	Fail-Open: リセット	リセットする必要のある接続を記録し、Fail-Open機能がオンでインラインモードの場合には記録しません。
300	サポートされていない暗号化	不明またはサポートされていない暗号化スイートが要求されました。
301	マスターキーの生成エラー	マスターシークレットから、暗号化キー、MACシークレット、および初期化ベクタを生成できません。
302	レコードレイヤメッセージ(準備ができていません)	SSL状態エンジンで、セッションの初期化前にSSLレコードが検出されました。
303	ハンドシェークメッセージ(準備ができていません)	SSL状態エンジンで、ハンドシェークのネゴシエーション後にハンドシェークメッセージが検出されました。
304	ハンドシェークメッセージの障害	適切にフォーマットされたハンドシェークメッセージが、誤った順序で検出されました。
305	メモリの割り当てエラー	リソースがなくなったため、パケットを適切に処理できませんでした。これは、多くの同時接続が一度に行われた場合、または単にシステムのメモリが不足した場合に発生することがあります。
306	サポートされていないSSLバージョン	クライアントがSSL V2バージョンのネゴシエーションを試行しました。
307	プレマスターキーの復号時のエラー	ClientKeyExchangeメッセージからプレマスターシークレットを復号できません。
308	クライアントによるロールバックの試行	クライアントが、ClientHelloメッセージに指定されたバージョンより古いバージョンのSSLプロトコルへのロールバックを試行しました。
309	更新エラー	キャッシュされたセッションキーでSSLセッションが要求されましたが、該当するセッションキーが見つかりませんでした。
310	鍵の交換エラー	サーバが一時的に生成されたキーを使用してSSLセッションを確立しようとしています。
311	SSLキー交換の上限を超過	キー交換の同時要求数が上限を超えました。
312	鍵サイズの超過	マスターの秘密鍵がプロトコルIDで指定されたサイズを超えています。
313	ハンドシェーク内の不正なパラメータ	ハンドシェークプロトコルのデコード中に無効または不正な値が検出されました。
314	利用可能なセッションなし	
315	未サポートの圧縮方法	
316	サポートされていないアプリケーション層プロトコル	不明、またはサポートされていないSSLアプリケーション層プロトコルが要求されました。
386	Fail-Open: リセット	リセットする必要のある接続を記録し、Fail-Open機能がオンでタップモードの場合には記録しません。
500	URIパスの深さが超過	区切り文字「/」が多すぎます。パスの深さは最大100です。

ID	イベント	備考
501	無効なトラバーサル	ルートより上位に「../」を使用しようとしました。
502	URIに使用できない文字	URIに無効な文字が使用されています。
503	不完全なUTF8シーケンス	UTF8シーケンスの途中でURIが終了しました。
504	無効なUTF8の符号化	無効または規定外のエンコードが試行されました。
505	無効な16進の符号化	%nnのnnが16進数ではありません。
506	URIパス長の超過	パス長が512文字を超えています。
507	不正な文字の使用	無効な文字を使用しています。
508	二重デコードの攻撃コード	二重デコードの攻撃コードです (%25xx、%25%xxdなど)。
700	不正なBase64コンテンツ	Base64形式でエンコードされるはずのパケットコンテンツが正しくエンコードされませんでした。
710	破損したDeflate/GZIPコンテンツ	Base64形式でエンコードされるはずのパケットコンテンツが正しくエンコードされませんでした。
711	不完全なDeflate/GZIPコンテンツ	不完全なDeflate/GZIPコンテンツです
712	Deflate/GZIPチェックサムエラー	Deflate/GZIPチェックサムエラーです。
713	未サポートのDeflate/GZIP辞書	サポートされていないDeflate/GZIP辞書です。
714	サポートされていないGZIPヘッダ形式/方法	サポートされていないGZIPヘッダ形式または方法です。
801	プロトコルデコード検索の上限を超過	プロトコルデコードルールには検索またはPDUオブジェクトの制限が定義されていますが、オブジェクトを見つける前に制限に達しました。
802	プロトコルデコードの制約エラー	プロトコルデコードルールによってデコードされたデータが、プロトコルコンテンツの制約を満たしていません。
803	プロトコルデコードエンジンの内部エラー	
804	プロトコルデコードの構造の超過	プロトコルデコードルールで、型の最大ネスト深度 (16) を超える型定義とパケットコンテンツが検出されました。
805	プロトコルデコードのスタックエラー	ルールのプログラミングエラーが原因で、反復が発生したか、またはネストされたプロシージャコールが使用されようとしました。
806	データの無限ループエラー	

変更監視イベント

イベントに関する全般的なベストプラクティスについては、"Deep Securityイベントログについて" on page 1150を参照してください。

Deep Securityで取得された整合性監視イベントを表示するには、[イベントとレポートとレポート] →[イベント変更監視イベントます。

変更監視イベントで表示される情報

[変更監視イベント] 画面には次の列が表示されます。[列] をクリックして、表に表示する列を選択することができます。

- 時刻: コンピュータ上でイベントが発生した時刻。
- コンピュータ: このイベントのログが記録されたコンピュータ(コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- 理由:このイベントに関連付けられた変更監視ルール。
- タグ: このイベントに適用されているイベントタグ。
- 変更: 変更監視ルールによって検出された変更。値は、「作成」、「アップデート」、「削除」、または「拡張子変更」のいずれかです。
- ランク: ランク付けシステムでは、イベントの重要度を数値化できます。コンピュータに「資産評価」を、ルールに「重要度」を割り当て、これら2つの値を掛け合わせることによって、イベントの重要度 (ランク) が計算されます。これによって、イベントをランクでソートできます。
- 重要度: 変更監視ルールの重要度
- 種類: イベントの発生元であるエンティティの種類
- キー: イベントの発生元であるパスおよびファイル名またはレジストリキー
- ユーザ: ファイルの所有者のユーザID
- プロセス: イベントの発生元であるプロセス
- イベント送信元: イベントの送信元であるDeep Securityコンポーネント

変更監視イベント一覧

ID	重要度	イベント	備考
8000	情報	完全なベースラインの作成	Agentに対してベースラインを作成するよう要求があった場合、またはAgentの変更監視ルールが0からnになり、その結果ベースラインが作成された場合に作成されます。このイベントには、検索にかかった時間 (ミリ秒) およびカタログ化されたエンティティ数の情報が含まれます。

ID	重要度	イベント	備考
8001	情報	部分的なベースラインの作成	Agentのセキュリティ設定で変更監視ルールが1つ以上変更された場合に作成されます。このイベントには、検索にかかった時間 (ミリ秒) およびカタログ化されたエンティティ数の情報が含まれます。
8002	情報	変更の検索の完了	Agentに対して完全または部分的な手動検索が要求された場合に作成されます。このイベントには、検索にかかった時間 (ミリ秒) およびカタログ化された変更数の情報が含まれます。ファイルシステムドライバまたは通知に基づく変更に対する継続検索では、8002イベントは生成されません。
8003	エラー	変更監視ルール内の不明な環境変数	ルールで ${env.EnvironmentVar} が使用されていて、「EnvironmentVar」が既知の環境変数でない場合に作成されます。このイベントには、該当する変更監視ルールのIDと名前、および不明な環境変数の名前が含まれます。
8004	エラー	変更監視ルール内の不正なベース値	無効な基本ディレクトリまたはキーがルールに含まれる場合に作成されます。たとえば、基本ディレクトリが「c:\foo\d:\bar」のFileSetを指定すると、このイベントが生成されます。または、環境変数の置き換えによって無効な値が生成される場合もあります。このイベントには、該当する変更監視ルールのIDと名前、および無効な基本値が含まれます。
8005	エラー	変更監視ルール内の不明なエンティティ	変更監視ルールで不明なEntitySetが検出された場合に作成されます。このイベントには、該当する変更監視ルールのIDと名前、および検出された不明なEntitySet名のカンマ区切りのリストが含まれます。
8006	エラー	変更監視ルール内のサポートされていないエンティティ	変更監視ルールで既知のサポートされないEntitySetが検出された場合に作成されます。このイベントには、該当する変更監視ルールのIDと名前、および検出されたサポートされないEntitySet名のカンマ区切りのリストが含まれます。RegistryKeySetなどの一部のEntitySetの種類はプラットフォームに固有です。
8007	エラー	変更監視ルール内の不明な機能	変更監視ルールで不明な機能が検出された場合に作成されます。このイベントには、該当する変更監視ルールのIDと名前、エンティティセットの種類 (FileSetなど)、および検出された不明な機能名のカンマ区切りのリストが含まれます。有効な機能値の例は、「whereBaseInOtherSet」、「status」、および「executable」です。
8008	エラー	変更監視ルール内のサポートされていない機能	変更監視ルールで既知のサポートされない機能が検出された場合に作成されます。このイベントには、該当する変更監視ルールのIDと名前、エンティティセットの種類 (FileSetなど)、および検出されたサポートされない機能名のカンマ区切りのリストが含まれます。Windowsサービスの状態を表す「status」などの一部の機能値はプラットフォームに固有です。
8009	エラー	変更監視ルール内の不明な属性	変更監視ルールで不明な属性が検出された場合に作成されます。このイベントには、該当する変更監視ルールのIDと名前、エンティティセットの種類 (FileSetなど)、および検出された不明な属性名のカンマ区切りのリストが含まれます。有効な属性値の例は、「created」、「lastModified」、および「inodeNumber」です。
8010	エラー	変更監視ルール内のサポートされていない属性	変更監視ルールで既知のサポートされない属性が検出された場合に作成されます。このイベントには、該当する変更監視ルールのIDと名前、エンティティセットの種類 (FileSetなど)、および検出されたサポートされない属性名のカンマ区切りのリストが含まれます。

ID	重要度	イベント	備考
			「inodeNumber」などの一部の属性値はプラットフォームに固有です。
8011	エラー	変更監視ルール内のエンティティセットの不明な属性	変更監視ルールで不明なEntitySet XML属性が検出された場合に作成されます。このイベントには、該当する変更監視ルールのIDと名前、エンティティセットの種類 (FileSetなど)、および検出された不明なEntitySet属性名のカンマ区切りのリストが含まれます。<FileSet base="c:\foo"> の代わりに <FileSet dir="c:\foo"> を記述した場合にこのイベントが記録されます。
8012	エラー	変更監視ルール内の不明なレジストリ文字列	ルールが存在しないレジストリキーを参照している場合に作成されます。このイベントには、該当する変更監視ルールのIDと名前、および不明なレジストリ文字列の名前が含まれます。
8013	エラー	WQLSetが無効です。名前空間またはWQLクエリが見つかりませんでした。	変更監視ルールXMLの形式が正しくないため、WQLクエリ内に名前空間が見つからないことを示しています。WQLクエリを使用および監視するカスタム変更監視ルールが使用される、高度な事例でのみ発生します。
8014	エラー	WQLSetが無効です。不明なプロバイダ値が使用されています。	
8015	警告	適用できない変更監視ルール	プラットフォームの不一致、存在しないターゲットディレクトリやファイル、サポートされていない機能など、いくつかの理由によって発生する可能性があります。
8016	警告	2番目に最適な変更監視ルール検出	
8050	エラー	正規表現をコンパイルできませんでした。無効なワイルドカードが使用されています。	

セキュリティログ監視イベント

イベントに関する全般的なベストプラクティスについては、"Deep Securityイベントログについて" on page 1150を参照してください。

Deep Securityで取得されたログ検査イベントを表示するには、[イベントとレポート]→[イベント]→[ログ検査イベント]の順に選択します。

セキュリティログ監視イベントで表示される情報

[セキュリティログ監視イベント] 画面には次の列が表示されます。[列] をクリックして、表に表示する列を選択することができます。

- 時刻: コンピュータ上でイベントが発生した時刻。
- コンピュータ: このイベントのログが記録されたコンピュータ(コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- 理由: このイベントに関連付けられたセキュリティログ監視ルール。
- タグ: イベントに付けられたタグ。
- 説明: ルールの説明。
- ランク: ランク付けシステムでは、イベントの重要度を数値化できます。コンピュータに「資産評価」を、セキュリティログ監視ルールに「重要度」を割り当て、これら2つの値を掛け合わせることによって、イベントの重要度 (ランク) が計算されます。これによって、イベントをランクでソートできます。
- 重要度: セキュリティログ監視ルールの重要度。
- グループ: ルールの所属先グループ。
- プログラム名: プログラム名。イベントのSyslogヘッダから取得されます。
- イベント: イベントの名前。
- 場所: ログの生成元。
- 送信元IP: パケットの送信元IP。
- 送信元ポート: パケットの送信元ポート。
- 送信先IP: パケットの送信先IP。
- 送信先ポート: パケットの送信先ポート。
- プロトコル: 値は、[ICMP]、[ICMPV6]、[IGMP]、[GGP]、[TCP]、[PUP]、[UDP]、[IDP]、[ND]、[RAW]、[TCP+UDP]、および [その他: nnn] (nnnは、3桁の10進値) のいずれかになります。
- 処理: イベント内で実行された処理
- 送信元ユーザ: イベント内の送信元ユーザ。
- 送信先ユーザ: イベント内の送信先ユーザ。
- イベントホスト名: イベント発生元のホスト名。
- ID: イベントからIDとしてデコードされたID。
- ステータス: イベント内のデコードされたステータス。
- コマンド: イベント内で呼び出されるコマンド。

- URL: イベント内のURL。
- データ: イベントから抽出されたその他のデータ。
- システム名: イベント内のシステム名。
- 一致したルール: 一致したルールの数。
- イベントの起点: イベントが発生したDeep Securityコンポーネントです。

セキュリティログ監視のセキュリティイベント一覧

注意: セキュリティログ監視に関連するシステムイベントについては、"システムイベント" on page 1342を参照してください。

ID	重要度	イベント
8100	エラー	セキュリティログ監視エンジンのエラー
8101	警告	セキュリティログ監視エンジンの警告
8102	情報	セキュリティログ監視エンジンの初期化

Webレピュテーションイベント

イベントに関する全般的なベストプラクティスについては、"Deep Securityイベントログについて" on page 1150を参照してください。

Deep SecurityによってキャプチャされたWebレピュテーションイベントを表示するには、[イベントとレポート]→[イベント]→[Webレピュテーションイベント] に移動します。

Webレピュテーションイベントで表示される情報

[Webレピュテーションイベント] 画面には次の列が表示されます。[列] をクリックして、表に表示する列を選択することができます。

- 時刻: コンピュータ上でイベントが発生した時刻。
- コンピュータ: このイベントのログが記録されたコンピュータ(コンピュータが削除されている場合、このエントリは「不明コンピュータ」と表示されます)。
- URL: このイベントをトリガしたURL。
- タグ: このイベントに関連付けられたイベントのタグ。
- リスク: このイベントをトリガしたURLのリスクレベル。「不審」、「非常に不審」、「危険」、「未評価」、「管理者によるブロック」などがあります。
- ランク: イベントの重要度を数値化する手段。コンピュータの資産評価にルールの重要度を乗算

して計算されます("イベントのランク付けによる重要度の数値化" on page 1169を参照)。

- イベント送信元: イベントが発生したDeep Securityシステムのコンポーネントを示します。

許可するURLのリストにURLを追加する

イベントをトリガしたURLを許可するURLのリストに追加するには、イベントを右クリックして [許可リストに追加] を選択します(許可およびブロックのリストを表示または編集するには、メインの [Webレピュテーション] 画面の [除外] タブに進みます)。

共通イベント、アラート、およびエラーのトラブルシューティング

ファイアウォールモジュールが無効であるにも関わらず、ファイアウォールイベントが発生する理由

侵入防御またはWebレピュテーションを有効にしている場合、一部のファイアウォールイベントが表示されることがあります。これは、侵入防御モジュールおよびWebレピュテーションモジュールによる監視でファイアウォールのステートフル設定メカニズムが利用されるためです。

イベントID 771「認識できないクライアントによる接続」のトラブルシューティング

イベントID 771 : 認識できないクライアントによる連絡先がDeep Security Managerに表示されるDeep Security AgentまたはDeep Security Virtual Applianceマネージャに接続しようとしますが、コンピュータの名前がコンピュータ上の保護されたコンピュータのリストに存在しません。

よくある原因は次のとおりです。

- クローン仮想マシンまたはクラウドインスタンス ([クローンAgentの再有効化] を有効にしていない)。
- Deep Security Agentを無効にする前に [コンピュータ] 画面から削除したコンピュータ([不明なAgentの再有効化] を有効にしていない)。Agentソフトウェアは Managerへの接続を定期的に試行し続けるため、ソフトウェアをアンインストールするか、コンピュータを無効にするまでこのイベントが毎回生成されます。
- vCenter、AWS、Azureなど、コネクタの同期の中断。たとえば、VMware ESXiホストが電源障害により正常にシャットダウンされなかった場合、仮想マシンの情報が正確に同期されない可能性があります。

解決策は原因ごとに異なります。

Deep Security Agentをアンインストールする

認識できないコンピュータを保護しない場合は、Deep Security Agentソフトウェアを無効にするか、アンインストールすることでこのイベントを発生しないようにできます。"Deep Securityのアンインストール" on page 1727を参照してください。

コンピュータまたはクローンを再有効化する

コンピュータを保護する場合は、Deep Security Managerでコンピュータを有効化します。再有効化により、Agentの証明書が再確立されるため、Managerが[コンピュータ]のリストで証明書を認証し、コンピュータを認識できるようになります。"エージェント起動アクティベーション(AIA)" on page 1524を参照してください。

VMwareコネクタの同期の中断を修正する

1. Deep Security Managerで、[コンピュータ]に進みます。
2. vCenterコネクタを削除します。
3. VMware vSphereで、Deep Security Virtual Appliance (DSVA)をリセットします。

   これにより、以下から情報が削除されます。

   ```
   /var/opt/ds_agent/guests
   ```

4. Deep Security ManagerにvCenterを再度追加します。
5. 仮想マシンを再度有効化します。

「Smart Protection Serverへの接続不能」エラーのトラブルシューティング

不正プログラム対策またはWebレピュテーションモジュールを使用している場合は、Deep Securityの「Smart Protection Server Disconnected スマートスキャン」または「Smart Protection Server Disffieded for Webレピュテーション」のいずれかのエラーが発生することがあります。マネージャコンソール。エラーを修正するには、次のトラブルシューティングのヒントを試してください。

エラーの詳細を確認する

エラーメッセージをダブルクリックして、サーバが接続するURLなどの詳細情報を表示します。次のようなエラーがあります。

- タイムアウトになる。
- ホスト名を解決できない。

コマンドプロンプトでnslookupを使用して、DNS名がIPアドレスに解決されるかどうかを確認します。URLが解決されない場合は、ローカルサーバでDNSの問題が発生します。

telnetクライアントを使用して、ポート80と443でURLへの接続をテストします。接続できない場合は、すべてのファイアウォールやセキュリティグループなどが、それぞれのポートでURLへの送信トラフィックを許可していることを確認します。

Deep Security Virtual Applianceの問題

Deep Security Virtual Applianceでエラーが発生した場合:

1. Virtual Applianceのインターネット接続を確認します。
2. Virtual Applianceのポート80でインターネットと双方向接続できることを確認します。
3. Virtual Applianceにメモリが十分に割り当てられていることを確認します。メモリ要件の詳細については、"Deep Security Virtual Applianceのサイジング" on page 425を参照してください。

エラー: 有効化に失敗

「有効化に失敗」アラートをトリガするイベントがあります。

- "プロトコルエラー" below
- "ホスト名解決不能" on the next page
- "エージェント/アプライアンスがありません" on the next page
- "ブロックされたポート" on the next page
- "重複するコンピュータ" on page 1428
- "プロキシ経由のエンドポイント" on page 1429
- "再インストールが必要です" on page 1429

プロトコルエラー

通常、このエラーは、Deep Security Managerを使用してDeep Security Agentを有効にする際に、ManagerがAgentと通信できなかった場合に発生します。Agentが使用する通信方向により、このエラーのトラブルシューティングに使用する必要のある方法が決定されます("AgentとManagerの通信" on page 1499を参照)。

Agentから開始

AgentがAgentからの通信を使用するには、AgentコンピュータからAgentを有効にする必要があります("Deep Security Agentの有効化" on page 1805を参照)。

ヒント: コンソールでエージェント起動の有効化を確認してください。[管理]→[システム設定]→[エージェント]の順に選択し、[許可エージェント起動の有効化]を選択します。

双方向の通信

エラーが発生して、Agentが双方向の通信を使用する場合は、次のトラブルシューティング手順を実行します。

1. Agentがコンピュータにインストール済みで稼働していることを確認します。
2. ManagerとAgent間のポートが空いていることを確認します("ポート番号、URL、およびIPアドレス" on page 428と"ファイアウォールルールの作成" on page 967を参照)。

ホスト名解決不能

エラー「有効化に失敗 (ホスト名解決不能)」は、DNSのホスト名が解決不能な場合、またはAgentからのリモート有効化を使用せずに、Deep Security ManagerからAgentを有効化した場合に発生することがあります。

Agentが双方向またはManagerから開始の場合、DNSのホスト名は解決可能です。Deep Security ManagerのDNSがホストを解決できるかどうかを確認します。

お使いのコンピュータがクラウドアカウントを使用している場合は、常にエージェントが開始するアクティベーションを使用することをお勧めします。Agentからの通信用のポリシールールの設定方法、およびインストールスクリプトを使用したAgentのインストール方法については、"Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511を参照してください。

エージェント/アプライアンスがありません

このエラーメッセージは、保護対象のコンピュータにAgentソフトウェアがインストールされていないことを示しています。

"Deep Security Agentソフトウェアの入手" on page 514を参照してください。

ブロックされたポート

ds_agent.logで「有効化に失敗」イベントが次のエラーメッセージとともに記録されている場合、

• 2018-06-25 17:52:14.000000: [Error/1] | CHTTPServer::AcceptSSL(<IP>:<PORT>) - BIO_do_handshake() failed - peer closed connection. | http\HTTPServer.cpp:246:DsaCore::CHTTPServer::AcceptSSL | 1E80:1FEC:ActivateThread

• 2018-06-25 17:52:14.143355: [dsa.Heartbeat/5] | Unable to reach a manager. | .\dsa\Heartbeat.lua:149:(null) | 1E80:1FEC:ActivateThread

• 2018-06-25 17:52:14.000000: [Info/5] | AgentEvent 4012 | common\DomainPrivate.cpp:493:DsaCore::DomPrivateData::AgentEventWriteHaveLock | 1E80:1FEC:ActivateThread

• 2018-06-25 17:52:14.143355: [Cmd/5] | Respond() - sending status line of 'HTTP/1.1 400 OK' | http\HTTPServer.cpp:369:DsaCore::CHTTPServer::Respond | 1E80:1D7C:ConnectionHandlerPool_0011

そして次のメッセージがパケットキャプチャソフトウェア (pcap) に表示される場合、

• [TCP Retransmission] <Ephemeral Port> -> 443 [SYN, ECN, CWR] .....

• [TCP Retransmission] <Ephemeral Port> -> 443 [SYN] .....

Deep Security AgentとManagerが通信を確立する際に使用されたポートがブロックされていた可能性があります。AgentとManagerの間で使用される通信ポートには、たとえば次のものがあります。

AgentとManagerの通信の種類	送信元 / ポート	送信先 / ポート
Agentからの通信	Deep Security Agent / エフェメラルポート	Manager / 4119
Managerからの通信	Deep Security Manager / エフェメラルポート	Agent / 4118

上の表から分かるように、短期ポートはAgentとManagerの間の送信トラフィックの送信元ポートとして使用されます。短期ポートがブロックされている場合は、Agentを有効化できなくなり、ハートビートが機能しなくなります。送信先ポートのいずれかがブロックされている場合も、同様の問題が発生します。

この問題を解決するには、次の手順に従います。

- ネットワーク設定で、クライアントの送信ポート (エフェメラルポート) の制限を削除する。
- Deep Security Managerへのポート4119へのアクセスを許可します。
- Managerからの通信を使用している場合は、ポート4118でDeep Security Agentへの受信アクセスを許可する。

ポートの詳細については、"ポート番号、URL、およびIPアドレス" on page 428を参照してください。

重複するコンピュータ

このエラーは、通常、既存の名前を使用してコンピュータをアクティベートした場合、または別のコネクタですでにアクティブなコンピュータを使用している場合に発生します。

この問題を解決するには、次のいずれかの方法を使用できます。

- 重複しているコンピュータのいずれかを削除し、必要に応じて残りのコンピュータを再度有効にしてください。
- Deep Security Managerから、の[管理]→[システム設定]→[エージェント]の順に選択し、エージェントが開始するアクティベーションの設定を選択します。同じ名前のコンピュータがすでに存在する場合は、既存のコンピュータを再度アクティベートするか、同じ名前の新しいコンピュータをアクティベートするか、またはアクティベーションを許可しないオプションがあります。詳細については、"エージェント起動アクティベーション(AIA) " on page 1524を参照してください。

プロキシ経由のエンドポイント

プロキシを使用している場合は、Deep Security ManagerでSupport> Deployment Scripts に移動し、プロキシでフィールドをアップデートしてから、エージェントを再度有効にします。詳細については、"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849を参照してください。

再インストールが必要です

Deep Security Agentがアクティベートされていない場合は、"Deep Security Agentをアンインストールする" on page 1728をアンインストールしてから、Deep Security Agentを再インストールする必要があります。

エラー: サポートされていないAgentバージョン

「エージェントのバージョンがサポートされていません」というエラーメッセージは、コンピュータに現在インストールされているエージェントのバージョンがDeep Security Managerでサポートされていないことを示しています。

サポートされていないエージェントはまだそれがのDeep Securityマネージャから受信した最後のポリシー設定に基づいてコンピュータを保護しますが、我々はあなたが最新の脅威に迅速に対応できるように、エージェントをアップグレードすることをお勧めします。詳細については、"Deep Security Agentのアップグレード" on page 1676のアップグレードを参照してください。

エラー: 不正プログラム対策 エンジンオフライン

注意: このエラーの一般的な原因は、公開鍵を登録せずにセキュアブートを有効にしていることです。続行する前に、「Linux Secure Boot support for agent」に記載されているように、公開鍵が適切に登録されていることを確認することを検討してください。このエラーが発生し、セキュアブートを使

用しない場合は、このエラーを無効にして、不正プログラム対策エンジンをオンラインに戻すことができます。

このエラーはさまざまな理由で発生します。この問題を解決するには、使用している保護のモードに対応した次の手順に従います。

- "Agentベースの保護" below
- "Agentレスによる保護" on the next page

不正プログラム対策モジュールの概要については、"不正プログラム対策について" on page 821を参照してください。

Agentベースの保護

1. Deep Security Managerで、同じマシンのその他のエラーを確認します。エラーが発生した場合、不正プログラム対策 エンジンがオフラインになっているその他の問題(通信やDeep Security Agentのインストールに失敗したなど)がある可能性があります。
2. エージェントからDeep Security Relay および管理者への通信を確認してください。
3. Deep Security Managerで、問題が発生したAgentの詳細を表示します。不正プログラム対策のポリシーまたは設定が有効になっていること、および各検索の設定(リアルタイム検索、手動検索、予約検索)が有効でアクティブであることを確認します。("不正プログラム対策を有効化して設定する" on page 828 .)を有効にして設定する」を参照してください。
4. Agentを再インストールして再有効化する前に、無効化してアンインストールします。詳細については、"Deep Securityのアンインストール" on page 1727と"Agentの有効化" on page 559を参照してください。
5. Deep Security Managerで、該当コンピュータの[アップデート]セクションに移動します。セキュリティアップデートが存在しており、最新であることを確認します。そうでない場合は、[セキュリティアップデートのダウンロード]をクリックして、アップデートを開始します。
6. 他のウイルス対策製品(例えば、ウイルスバスター コーポレートエディション)との競合がないか確認してください。競合が存在する場合は、他の製品とDeep Security Agentをアンインストールし、再起動してからDeep Security Agentを再インストールしてください。ウイルスバスター コーポレートエディションを削除するには、ウイルスバスター コーポレートエディション(OSCE)でクライアントまたはエージェントを手動でアンインストールするを参照してください。

エージェントがWindowsの場合:

1. 次のサービスが実行されていることを確認します。
   - Trend Micro Deep Security Agent
   - Trend Micro Solution Platform

2. 次のコマンドを実行して、不正プログラム対策関連のドライバがすべて適切に実行されていることを確認します。

   Deep Security Agentのすべてのバージョンの場合:

   - `# sc query AMSP`

   Deep Security Agent 12.5以前の場合は、以下も確認してください。

   - `# sc query tmcomm`
   - `# sc query tmactmon`
   - `# sc query tmevtmgr`

   ドライバが実行されていない場合は、トレンドマイクロのサービスを再起動します。それでも実行されない場合は、次の手順に進んでください。

3. インストール方法を確認します。zipファイルではなく、MSIのみをインストールします。
4. エージェントを手動で削除して再インストールする必要があるかもしれません。詳細については、Trend Micro Deep Security の手動アンインストール手順を参照してください
5. インストールされているComodo証明書が問題の原因である可能性があります。この問題を解決するには、「証明書の問題により、不正プログラム対策機能がオフラインになる」を参照してください。

エージェントがLinuxにインストールされている場合:

1. Agentが実行されていることを確認するには、コマンドラインで次のコマンドを入力します。
   - `service ds_agent status`
2. Linuxサーバーを使用している場合、カーネルがサポートされていない可能性があります。詳細については、"エラー: モジュールのインストール失敗 (Linux)" on page 1442を参照してください。

これらの手順に従っても問題が解決しない場合は、診断パッケージを作成して、サポートにお問い合わせください。詳細については、"診断パッケージの作成" on page 2019を参照してください。

Agentレスによる保護

1. Deep Security Managerで、vCenterとNSXの同期を確認します。[コンピュータ] セクションで、vCenterを右クリックして、[プロパティ] を選択します。[接続テスト] をクリックします。[NSX] タブをクリックして、接続をテストします。証明書が変更されている場合は、[証明書の追加/アップデート] をクリックします。
2. NSXマネージャにログオンし、vCenterと適切に同期していることを確認します。

3. vSphere Clientにログインして、[Network & Security]→[Installation]→[Service Deployments]の順に選択します。Trend Micro Deep SecurityおよびGuest Introspectionのエラーを確認して、検出されたエラーをすべて解決します。
4. vSphere Clientで、[Network & Security]→[Service Composer] の順に選択します。セキュリティポリシーが適切なセキュリティグループに割り当てられていることを確認します。
5. VMware ToolsがDeep Securityと互換性があることを確認してください。詳細については、VMware ToolsとDeep Security Virtual Applianceの組み合わせにおけるトラブル事例を参照してください。
6. File Introspection Driver (vsepflt) がターゲット仮想マシンにインストールされ、実行されていることを確認します。コマンドプロンプトで管理者としてsc query vsepfltを実行します。
7. vCloud Directorのカタログまたはテンプレートから配信されたインスタンスおよび仮想マシンにはすべて同じBIOS UUIDが付与されます。Deep Securityでは、BIOS UUIDによって個々の仮想マシンを識別するため、vCenterに重複した値があると、「不正プログラム対策エンジンがオフライン」エラーが発生します。この問題を解決するには、「VM BIOS UUIDs are not unique when virtual machines are deployed from vApp templates (2002506)」を参照してください。
8. 問題が解決しない場合は、次の情報を含むサポートケースを開きます。
   - 各Deep Security Managerの診断パッケージ詳細については、"診断パッケージの作成" on page 2019を参照してください。
   - Deep Security Virtual Applianceの診断パッケージ
   - 影響を受ける仮想マシンのvCenterサポートバンドル

エラー:デバイスコントロールエンジンがオフラインです

このエラーはさまざまな理由で発生します。問題を解決するには、次の手順に従ってください。

デバイスコントロールモジュールの概要については、「"デバイスコントロールの設定" on page 1001」を参照してください。

1. Deep Security Managerコンソールで、同じコンピュータの他のエラーを確認します。エラーが存在する場合は、通信やAgentのインストールの失敗など、デバイスコントロールエンジンがオフラインになる他の問題が考えられます。
2. AgentからDeep Security RelayおよびDeep Security Managerへの通信を確認します。
3. Deep Security Managerコンソールで、問題のあるAgentの詳細を表示します。デバイスコントロールのポリシーまたは設定が有効になっていることを確認します。
4. Agentを非アクティブ化してアンインストールしてから、再インストールして再度アクティブ化します。詳細については、「"Deep Securityのアンインストール" on page 1727」および「"Agentの有効化" on page 559」を参照してください。

5. Deep Security Managerコンソールで、そのコンピュータの[アップデート]セクションに移動します。セキュリティアップデートが存在し、最新であることを確認します。インストールされていない場合は、[セキュリティアップデートのダウンロード]をクリックしてアップデートを開始します。
6. 別のウイルス対策製品(ウイルスバスター コーポレートエディションなど)との競合がないか確認してください。競合がある場合は、他の製品をアンインストールし、Deep Security Agentを再起動してから再インストールしてください。ウイルスバスター コーポレートエディションを削除するには、ウイルスバスター コーポレートエディションのクライアントおよびエージェントの手動アンインストールに関するトラブルシューティングガイドを参照してください。

AgentがWindowsの場合

1. 次のサービスが実行されていることを確認します。
   - Trend Micro Deep Security Agent
   - Trend Micro Solution Platform

2. 次のコマンドを実行して、デバイスコントロール関連のすべてのドライバが正しく実行されていることを確認します。

   Deep Security Agentのすべてのバージョンの場合:

   - `# sc query AMSP`

   ドライバが実行されていない場合は、トレンドマイクロのサービスを再起動してください。それでも実行されていない場合は、次の手順に進んでください。

3. インストール方法を確認してください。ZIPファイルではなく、MSIのみをインストールしてください。
4. エージェントを手動で削除して再インストールする必要があるかもしれません。詳細については、Trend Micro Deep Security の手動アンインストール手順を参照してください

エラー: ステータスの確認の失敗

Deep Security ManagerコンソールからコンピュータのAgent/Applianceのステータスを確認できます。[コンピュータ]画面でコンピュータを右クリックして、[処理]→[ステータスの確認]の順にクリックします。

「ステータスの確認の失敗」エラーが表示されたら、このエラーメッセージを開いて詳細な説明を確認します。

説明にプロトコルエラーが表示されている場合は、通常、通信問題が原因です。いくつかの原因が考えられます。

- コンピュータ(またはコンピュータに割り当てられたポリシー)がAgentからの通信または双方向の通信用に設定されているかを確認します。エージェントが開始した通信を使用している場合

は、「ステータスの確認」操作は失敗します。

- Deep Security ManagerがAgentと通信できることを確認します。ManagerがAgentにアクセスできる必要があります。"ポート番号、URL、およびIPアドレス" on page 428を参照してください。
- Agentコンピュータのリソースを確認します。メモリ、CPU、またはディスク容量が不足すると、このエラーが発生します。

説明にSQLITE_IOERR_WRITE[778] と表示された場合: ディスクI/Oエラー、Agentコンピュータに問題がある可能性があります。ディスクがいっぱいか、書き込みが制限されていることが最も一般的な問題です。

エラー: 機能「dpi」のインストール失敗: 使用不可: フィルタ

「機能「dpi」のインストール失敗: 使用不可: フィルタ」というエラーメッセージは、OSカーネルバージョンがネットワークドライバでサポートされていないことを示しています。通常、Deep Security Agentがトラフィックを検査するために同時にネットワークドライバをインストールするため、侵入防御, Webレピュテーション、または ファイアウォール のインストール時にこのメッセージが表示されます。同じ状況でエンジンオフラインアラートが生成されることもあります。

アップデートを随時提供できるように、トレンドマイクロでは、さまざまなOSベンダからの新しいカーネルのリリースを常にチェックし、品質保証テストが完了次第、それらのカーネルに対応したアップデートをリリースしています。

対応するOSカーネルバージョン用のアップデートが利用可能になると、必要なモジュールが自動的にインストールされます。

追加情報

これは、侵入防御、Webレピュテーション、およびファイアウォールにのみ影響します。それ以外の保護モジュール (不正プログラム対策、変更監視、およびセキュリティログ監視) はすべて正常に動作します。

サポートされているOSカーネルバージョンを確認するには、「Deep Security 9.6 Supported Linux Kernels」にアクセスし、該当するOSの配信情報を参照してください。

エラー: 仮想マシンを有効化した後に「変更監視エンジンがオフライン」およびその他のエラーが発生する

Deep Security Virtual Applianceで保護される仮想マシンを有効化すると、Deep Security Managerには以下のエラーが表示されます。これらのエラーは、有効化が正常に実行された場合でも表示され

ます。

- 不正プログラム対策エンジンがオフライン
- ベースラインの再構築の失敗 (AgentまたはApplianceのエラー)
- 変更監視エンジンがオフライン

次のトラブルシューティングタスクを実行した場合でも、問題は未解決のままになります。

- vSphere Endpointがインストール済みであることを確認します。
- 最新のVMware Toolsがインストールされていることを確認します。
- VMCIドライバとVSEPFLTドライバが仮想マシンにインストールされていて稼働中であることを確認します。
- DSMコンソールでvCenterを同期します。
- Deep Security Virtual Applianceを無効化してから再度有効化します。
- 問題が発生している特定の仮想マシンを無効にしてから再度有効にします。
- VMware Toolsを再インストールします。

これらのエラーが表示されるのは、仮想マシンのハードウェアがバージョン7以上を実行していないためです。この問題を解決するには、仮想マシンを最新のハードウェアバージョンにアップグレードする必要があります。

エラー: インタフェースが非同期

このエラーは、Deep Security Managerのデータベースに格納されているゲスト仮想マシン(VM)のネットワークインタフェース情報が、Deep Security Virtual Applianceから報告されたインタフェース情報と異なる場合 (たとえば、MACアドレスが異なる場合) に発生します。

この問題の根本原因を確認するには、どの段階で情報が同期されなくなったかを特定する必要があります。

まず、Deep Security Managerのエラーメッセージを確認して、どのVMおよびどのインタフェースに問題があるかを確認します。

仮想マシンのインタフェースを確認する

1. 仮想マシンにログインします。
2. コマンドプロンプトを開きます。
3. コマンドを入力し、すべてのネットワークインタフェースの情報を表示します。たとえば、Windowsでは次のコマンドを入力します。`ipconfig /all`

4. すべてのNICとMACアドレスを検証して、NICに正しいドライバが適用されていて、正常に動作していることを確認します。

vCenterで仮想マシンのインタフェース情報を確認する

vCenter ServerのManaged Object Reference (MoRef) から仮想マシンのインタフェース情報を確認します。

1. https://<VC_SERVER>/mob/?moid=<OBJECT_ID>にアクセスして、仮想マシンのMOBに移動します。

   たとえば、次のようなURLになります。https://192.168.100.100/mob/?moid=vm-1136&doPath=config

   指定する項目は次のとおりです。

   <VC_SERVER> は、vCenter ServerのFQDNまたはIPです。

   =<OBJECT_ID>は、確認するオブジェクトのIDです。

   VC MOBへのアクセスの詳細については、「Looking up Managed Object Reference (MoRef) in vCenter Server」を参照してください。

2. [Config]→[extraConfig["ethernet0.filter0....."]]→[hardware] に移動して、すべてのNICとMACアドレスを確認します。
3. MACアドレスを仮想マシンのOSのMACと比較します。

Deep Security Managerでvmxファイルと仮想マシンのインタフェース情報を確認する

1. vCenter Serverデータストアのブラウザを使用して、仮想マシンのvmxファイルをダウンロードします。
2. メモ帳などのテキストエディタを使用して、vmxファイルを開きます。
3. IP、uuid.bios、およびMACアドレスを確認します。

   次に例を示します。

```
Check virtual computer UUID
- uuid.bios = "42 23 d6 5d f2 d5 22 41-87 41 86 83 ea 2f 23 ac"
Check EPSec Settings
- VFILE.globaloptions = "svmip=169.254.50.39 svmport=8888"
- scsi0:0.filters = "VFILE"
Check DvFilter Settings
- ethernet0.filter0.name = "dvfilter-dsa"
- ethernet0.filter0.onFailure = "failOpen"
```

```
- ethernet0.filter0.param0 = "4223d65d-f2d5-2241-8741-8683ea2f23ac"
- ethernet0.filter0.param2 = "1"
- ethernet0.filter0.param1 = "00:50:56:A3:02:D8"
```

4. Deep Security Managerのダッシュボードに移動し、[VM]→[インタフェース]をダブルクリックして、IPアドレスとMACアドレスを確認します。
5. IPアドレスとMACアドレスを前述の結果と比較します。

Deep Security Virtual Applianceの仮想マシンのインタフェース情報を確認する

1. vCenter Serverデータストアのブラウザを使用して、仮想マシンの該当するvmxファイルをダウンロードします。
2. メモ帳などのテキストエディタを使用して、vmxファイルを開きます。
3. uuid.biosの値を確認します。
4. Deep Security Virtual Applianceのコンソールにログオンし、<Alt>+<F2> キーを押してコマンドモードに切り替え、Deep Security Virtual Applianceのユーザ名とパスワードを入力します。
5. 次のコマンドを実行して、仮想マシンのネットワークインタフェースがDeep Security Virtual Applianceで認識されたかどうかを確認します(注意: $uuidは実際のBIOS UUIDに置き換えます。)

```
cd /var/opt/ds_agent/guests/$uuid
```

```
>/opt/ds_guest_agent/ratt if
```

6. ifconfig -aコマンドを実行して、Deep Security Virtual ApplianceのNIC設定とIPが正しく設定されていることを確認します。
7. IPアドレスとMACアドレスを前述の結果と比較します。

回避策

前述のいずれかの項目が同期されていない場合は、その問題を修正する必要があります。

回避策1

有効化した仮想マシンのクローンをDeep Securityで作成するときに、クローンコンピュータの電源をオンにして有効化すると、「インタフェースが非同期」アラートが表示されることがあります。回避策としては、クローンとして作成したコンピュータの電源をオンにする前にdvfilterの設定を消去します。

- ethernet0.filter0.name = "dvfilter-dsa"
- ethernet0.filter0.onFailure = "failOpen"
- ethernet0.filter0.param0 = "4223d65d-f2d5-2241-8741-8683ea2f23ac"

- ethernet0.filter0.param2 = "1"
- ethernet0.filter0.param1 = "00:50:56:A3:02:D8"

回避策2

1. 仮想マシンを一時停止してから、もう一度電源をオンにします。
2. Deep Security Virtual Applianceを再起動します。
3. 仮想マシンを無効化してから、もう一度有効化します。

回避策3

vMotionで仮想マシンを保護対象のESXiホストに移行して、警告メッセージを消去します。

注意: vCenterは常にDeep Security Managerに接続されている必要があります。そうしないと、インタフェースの同期が失われる問題が繰り返し発生します。

詳細なトラブルシューティング手順

1. IPアドレスとMACアドレスを確認した前述の手順の結果を入力します。"Deep Security Virtual Applianceの仮想マシンのインタフェース情報を確認する" on the previous page
2. 仮想マシンのインタフェースがDeep Security Virtual Applianceによって認識されたことを確認した前述の手順から、rattif.txtファイルを取得します。
3. 次のコマンドからの出力を取得します。

```
$ ls -alR > /home/dsva/ls.txt
$ netstat -an > /home/dsva/netstat.txt
$ ps auxww > /home/dsva/ps.txt
$ lsof > /home/dsva/lsof.txt
$ ifconfig -a > /home/dsva/ifconfig.txt
$ cp /var/log/syslog /home/dsva/syslog.txt
```

4. Deep Security Manager、Deep Security Agent、およびDeep Security Virtual Applianceの診断パッケージを取得します。
5. 次のファイルを収集して、トレンドマイクロのテクニカルサポートに送信します

- rattif.txt
- ls.txt
- netstat.txt
- ps.txt
- lsof.txt

- ifconfig.txt
- syslog.txt

ratt ifコマンドの出力で仮想マシンのMACアドレスを確認できない場合は、次の回避策を実行してください。

1. vCenterでテンプレートから仮想マシンを配置します。
2. 既存のNICを削除します。
3. 仮想マシンの電源をオンにします(ログオンする必要はありません)。
4. 仮想マシンの電源をオフにします。
5. 新しいNICを追加します。
6. 仮想マシンの電源をオンにします。

エラー: 侵入防御ルールのコンパイルに失敗しました

このエラーはさまざまな理由で発生します。次の手順を実行して、エラーが正当なものであることを確認します。

ポリシーを再送信する:

1. Deep Security Managerで[コンピュータ]をクリックします。
2. エラーが発生したコンピュータを右クリックします。
3. [処理]→[ポリシーの送信]の順に選択します。

ステータスを確認する:

1. Deep Security Managerで[コンピュータ]をクリックします。
2. エラーが発生したコンピュータを右クリックします。
3. [処理]→[警告/エラーのクリア]の順に選択します。
4. 警告とエラーがクリアされたら、[処理]→[ステータスの確認]の順に選択します。

上記の手順を実行してもエラーが引き続き発生する場合は、次の解決策を使用して問題のトラブルシューティングを行います。

- "侵入防御のベストプラクティスを適用する" on the next page
- "ルールを管理する" on the next page
- "個々のポートからアプリケーションの種類の割り当てを解除する" on page 1441

これらの方法でもエラーが解決しない場合は、テクニカルサポートに問い合わせてください。

侵入防御のベストプラクティスを適用する

「侵入防御ルールのコンパイルに失敗しました」エラーは、容量、メモリ、CPUなどのリソースがマシンに不足していることが原因で発生する可能性があります。この問題を解決するには、"侵入防御のパフォーマンスに関するヒント" on page 951を参照し、設定を調整します。

ルールを管理する

「侵入防御ルールのコンパイルに失敗しました」エラーは、割り当てられている侵入防御ルールの数が推奨値を超えている場合に発生する可能性があります。エンドポイントに割り当てられている侵入防御ルールの数が400を超えないようにしてください。不要なルールを割り当てないようにするため、推奨設定の検索で推奨される侵入防御ルールのみを適用することをお勧めします。侵入防御ルールを手動で適用する場合は、単一のポートに追加されるアプリケーションの種類が多くなりすぎないように、ポリシーではなくコンピュータにルールを適用します。

この問題を解決するには、次の手順に従って割り当てられているルールの数を減らします。

1. 割り当て方法に応じて、侵入防御ルールにアクセスします。以下のいずれかの方法を実行します。
   - コンピュータレベルでルールが割り当てられている場合は、[コンピュータ] タブに移動し、コンピュータを右クリックして [詳細] を選択します。
   - ポリシーレベルでルールが割り当てられている場合は、[ポリシー] タブに移動し、ポリシーを右クリックして [詳細] を選択します。
2. [侵入防御] に移動し、[推奨設定の検索] をクリックします。
3. 検索が完了したら、[割り当て/割り当て解除] をクリックします。ウィンドウの上部で、[割り当て解除を推奨] を使用してルールを絞り込みます。
4. ルールの割り当てを解除するには、ルール名の横にあるチェックボックスをオンにします。複数のルールの割り当てをまとめて解除するには、ShiftキーまたはControlキーを使用して複数のルールを選択します。
5. 削除する1つまたは複数のルールを右クリックして、[ルールの割り当て解除]→[すべてのインタフェースから] の順に選択し、[OK] をクリックします。ウィンドウを閉じます。
6. [コンピュータ] タブでコンピュータを右クリックし、[処理]→[警告/エラーのクリア] の順に選択します。侵入防御エンジンによって、ルールのコンパイルが自動的に実行されます。このプロセスにかかる時間は、Deep Security ManagerとAgent間のハートビート間隔と通信設定によって異なります。

ヒント: ポリシーを通じて侵入防御ルールを適用していて、どのコンピュータにルールが適用されているのかが不明な場合は、**ポリシーエディタ**[1]を開いて、[概要]→[このポリシーを使用しているコンピュータ]の順に選択します。

個々のポートからアプリケーションの種類の割り当てを解除する

「侵入防御ルールのコンパイルに失敗しました」エラーは、個々のポートに割り当てられているアプリケーションの種類が多すぎる場合に発生する可能性があります。現時点では、1つのポートに割り当てることができるアプリケーションの種類は16個までです。

この問題を解決するには、次の手順に従って、割り当てられたアプリケーションの種類をポートから削除します。

1. 問題が発生しているルールを確認するには、エラーをダブルクリックしてイベント表示ツールを開きます。
2. [コンピュータ] タブに進みます。
3. 侵入防御ルールの設定に問題があるコンピュータを右クリックし、[詳細] を選択します。
4. [侵入防御] に移動します。
5. [割り当て/割り当て解除] をクリックします。設定に問題があるルールの名前を検索バーに入力します。
6. ルールを右クリックし、[アプリケーションの種類プロパティ] を選択します。
7. [継承] チェックボックスをオフにします。
8. ポートを削除し、新しいポートを入力します。
9. [適用]→[OK] の順にクリックします。

エラー: セキュリティログ監視ルールで必要なログファイル

セキュリティログ監視ルールで監視対象のファイルの場所を追加する必要がある場合、または不要なセキュリティログ監視ルールを追加し、監視対象のファイルがマシンに存在しない場合は、**コンピュータエディタ**[2]または**ポリシーエディタ**[3]で次のエラーが発生します。

このエラーを解決するには、次の操作を実行します。

1. [セキュリティログ監視ルールで必要なログファイル] エラーをクリックします。エラーの詳細が含まれるウィンドウが表示されます。[説明] の下に、エラーの原因となったルールの名前が一覧表示されます。

---

[1] ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック)します。

[2] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細] をクリック)します。

[3] ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細] をクリック)します。

2. Deep Security Managerで、[Policies]→[Common Objects]→[Rules]→[Log Inspection Rules]の順に選択し、エラーの原因となっているルールを探します。
3. ルールをダブルクリックします。ルールのプロパティウィンドウが表示されます。
4. [設定] タブに進みます。

ファイルの場所が必要な場合:

1. [監視するログファイル] の下に場所を入力し、[追加] をクリックします。
2. [OK] をクリックします。Agentがポリシーを受け取ると、エラーがクリアされます。

リストされたファイルが保護対象マシンに存在しない場合:

1. **コンピュータエディタ**[1] または **ポリシーエディタ**[2] の [セキュリティログ監視] に進みます。
2. [割り当て/割り当て解除] をクリックします。
3. 不要なルールを見つけて、チェックボックスをオフにします。
4. [OK] をクリックします。Agentがポリシーを受け取ると、エラーがクリアされます。

このエラーを回避するために、推奨ルールの推奨設定の検索を実行するには:

1. Deep Security Managerで、Computersに移動します。
2. 検索するコンピュータを右クリックし、[処理]→[推奨設定の検索] の順にクリックします。
3. **コンピュータエディタ**[3] または **ポリシーエディタ**[4] の保護モジュールの [一般] タブで結果を確認します。

エラー: モジュールのインストール失敗 (Linux)

「モジュールのインストールに失敗しました」というエラーメッセージは、ご使用のOSのカーネルバージョンがDeep Securityネットワークドライバまたはファイルシステムフックでサポートされていないことを示しています。同じ状況でエンジンオフラインアラートが生成されることもあります。互換性のあるネットワークドライバがないことが、このエラーの主な原因です。

侵入防御、Webレピュテーション、またはファイアウォールを適用すると、Deep Security Agentでトラフィックを調査できるようにネットワークドライバがインストールされます。不正プログラム対策および変更監視は、ファイルシステムフックモジュールをインストールします。このモジュールは、ファイルシステムの変

---

1 コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

2 ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。

3 コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

4 ポリシーエディタを開くには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。

更をリアルタイムで監視するために必要です(予約検索には同じファイルシステムフックは必要ありません)。

アップデートが開発中である可能性があります。トレンドマイクロは、多数のベンダの新しいカーネル リリースを常にチェックし、品質保証テストが完了次第、それらのカーネルに対応したアップデートをリリースしています。お使いのカーネルバージョンのサポート予定については、テクニカルサポートにお問い合わせください(ログインして右上の [サポート] をクリック)。

モジュールのサポートアップデートは、利用可能になると自動的にシステムにインストールされます。

サポートされているOSカーネルのバージョンについては、"Linuxカーネルの互換性" on page 400を参照してください。

エラー: このコンピュータに1つ以上のアプリケーションの種類の競合がある

このエラーメッセージは、Deep Security Agentのアップデート時にDeep Security Managerの[DPI Events]タブに表示されます。

このコンピュータには1つ以上のアプリケーションの種類の競合があります。1つのアプリケーションの種類に関連付けられている1つ以上の侵入防御ルールは、他のアプリケーションの種類に関連付けられている1つ以上の侵入防御ルールに依存しています。2つのアプリケーションの種類が異なるポートを使用しているため、この競合が発生しています。

競合しているアプリケーションの種類を以下に示します。

```
[A] "Web Application Tomcat" Ports: [80,8080,4119]

[B] "Web Server Common" Ports: [80,631,8080,7001,7777,7778,7779,7200,7501,8007,
8004,4000,32000,5357,5358,9000]

[A] "Web Server Miscellaneous" Ports: [80,4000,7100,7101,7510,8043,8080,8081,8088,8300,8500,
8800,9000,9060,19300,32000,3612,10001,8093,8094]

[B] "Web Server Common" Ports: [80,631,8080,7001,7777,7778,7779,7200,7501,8007,
8004,4000,32000,5357,5358,9000]"
```

解決方法

競合を解決するには、アプリケーションの種類Bで使用されているポート番号を編集し、アプリケーションの種類Aで使用されているポート番号を追加します。2つのアプリケーションの種類 (Web Application TomcatとWeb Server Miscellaneous) は両方とも、アプリケーションの種類Web Server Commonに依存しています。そのため、この2つのアプリケーションの種類に指定されているポートはWeb Server Commonのポートにも指定されている必要があります。

この3つのアプリケーションの種類のポート番号を統合すると、次のようになります。
80,631,3612,4000,4119,5357,5358,7001,7100,7101,7200,7501,7510,7777,7778,7779,
8004,8007,8043,8080,8081,8088,8093,8094,8300,8500,8800,9000,9060,10001,19300,32000

これをWeb Server Commonのポートリストに追加すると、[イベント] タブに次のメッセージが表示されます。*アプリケーションの種類のポートリストの誤った設定は解決されました。*

ポートを統合する

1. Deep Security Managerにログオンし、[ポリシー]→[ルール]→[侵入防御ルール] に移動します。
2. 検索ボックスでWeb Server Commonを検索し、アプリケーションの種類Web Server Commonをダブルクリックします。
3. [一般]→[詳細]→[アプリケーションの種類]→[編集]→[Web Server Common] に移動します。
4. [一般]→[接続]→[ポート] に移動し、[編集] をクリックして、すべてのポートを次エントリで置き換えます。80,631,3612,4000,4119,5357,5358,7001,7100,7101,7200,
7501,7510,7777,7778,7779,8004,8007,8043,8080,8081,8088,8093,
8094,8300,8500,8800,9000,9060,10001,19300,32000
5. [OK] をクリックします。

継承オプションを無効にする

セキュリティプロファイルで侵入防御の継承オプションを無効にすることをお勧めします。無効にすることで、アプリケーションの種類に対する変更は、現在のセキュリティプロファイルにのみ反映されます。

1. Deep Security Managerにログオンし、[セキュリティプロファイル] に移動します。
2. 右側の画面で、セキュリティプロファイルをダブルクリックします。
3. [DPI] セクションに移動し、[継承] をクリックして選択解除します。
4. [OK] をクリックします。

IPSルール1000128を確認します。

1. [アプリケーションの種類プロパティ] を右クリックします。
2. [継承] をクリックして選択解除します。
3. 現在の継承ポートリストに、Deep Security ManagerのGUIの待機ポート番号が含まれていることを確認します。含まれていない場合は、Web Server Commonのポートグループにこのポートを追加します。
4. [継承] をクリックします。

エラー: クラウドアカウントに接続できない

Amazonクラウドアカウントを追加するときに、「クラウドアカウントに接続できない」というエラーが発生することがあります。これには以下の原因が考えられます。

- キーIDまたはシークレットが無効である
- 権限が正しくない
- ネットワーク接続で障害が発生した

AWSアカウントのアクセスキーIDまたは秘密アクセスキーが無効である

解決方法

入力したセキュリティ資格情報が正しいことを確認します。

Deep Securityで使用するアカウントに間違ったAWS IAMポリシーが適用されている

解決方法

AWSアカウントにアクセスし、そのアカウントのIAMポリシーを確認します。

AWS IAMポリシーで次の権限が割り当てられている必要があります。

- Effect:許可
- AWS Service:Amazon EC2
- [Actions] として次を選択します。
  - DescribeImages
  - DescribeInstances
  - DescribeTags
- Amazon Resource Name (ARN): *

NAT、プロキシ、またはファイアウォールのポートが開いていないか、設定が正しくない

これは、AWS Marketplace上のAMIを使用して新しいDeep Security Managerのインストールを配信する場合など、場合によっては発生します。

Deep Security Managerは [に必要なポート番号](#) で、インターネット、特にAmazon Cloudに接続できる必要があります。

解決方法

次の作業が必要となる場合があります。

- AMIとインターネットの間のファイアウォール/ルータでNATまたはポート転送を設定する
- AMIの外部IPアドレスを取得する

安定したネットワーク接続も必要です。ネットワーク接続が断続的に途切れる場合も、このエラーメッセージが表示されることがあります。

エラー: インスタンスのホスト名を解決できない

「インスタンスのホスト名を解決できない」というエラーメッセージは、Agentからのリモート有効化を使用せずに、Deep Security ManagerからAgentを有効化した場合に発生することがあります。

常に [Agentからのリモート有効化] を使用することを推奨します。Agentからの通信用のポリシールールの設定方法、およびインストールスクリプトを使用したAgentのインストール方法については、"Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511を参照してください。

アラート: 変更監視情報の収集が遅延しています

このアラートは、変更監視情報の収集速度が一時的に遅延していることを示します。遅延は、エージェントからDeep Security Managerに送信されている整合性監視データの量が増加したために発生します。この間、一部のコンピュータでベースラインと変更監視イベントの表示が最新ではなくなる可能性があります。

このアラートは、変更監視データの収集が遅延しなくなったときに自動的に消去されます。

変更監視の詳細については、"変更監視の設定" on page 1004を参照してください。

アラート: Managerの時刻が非同期

Deep Security ManagerのOSのシステム時間は、データベースコンピュータの時間と同期する必要があります。このアラートは、コンピュータの時刻が30秒以上同期していないときに、Managerコンソールの [アラートステータス] ウィジェットに表示されます。

時刻を同期するには、次の設定を適用します。

- データベースとすべてのManagerノードが同じタイムゾーンを使用するように設定します。
- データベースとすべてのManagerノードの時刻が同じタイムソースで同期していることを確認します。
- ManagerがLinuxオペレーティングシステムで稼働している場合は、ntpdデーモンが実行されていることを確認します。

アラート: Managerノードのメモリの警告しきい値を超過しました

メモリの警告しきい値の超過 または メモリの重大しきい値の超過 アラートがDeep Securityに表示され、ホストのメモリ使用量が一定量を超えたことが通知されます。警告アラートは、ホストのメモリの70%が使用されていることを示し、重大なアラートは使用率が85%を超えていることを示します。

この問題を解決するには、予期せず大量のメモリを消費するプロセスがあるかどうかを判断します。

- 検出されたプロセスがDeep Security Managerでない場合は、プロセスをホストから削除するか、または削除します。Deep Security Managerは専用のホストコンピュータで実行する必要があります。
- プロセスがDeep Security Managerの場合は、ホストメモリの量を増やしてください。ガイドラインについては、"サイジング" on page 417 を参照してください。

注意: 初期設定では、Deep Security Managerの最大ヒープサイズは4GBです。つまり、Deep Security Managerは最大4 GBのヒープを割り当てます。ただし、JVMはヒープだけでなく非ヒープも割り当てます。その結果、Deep Security Managerプロセスの最大合計メモリサイズは4GBより大きくなります。

注意: ホストがVMの場合は、そのVMのすべてのゲストメモリを予約することを強くお勧めします。

イベント: 最大TCP接続数

Deep Securityは、保護されているコンピュータに最大数のTCP接続を許可するように設定されています。接続数が最大数を超えた場合は、ネットワークトラフィックが中断し、最大TCP接続数ファイアウォールイベントが発生します。接続が中断しないようにするには、最大TCP接続イベントが発生したコンピュータの最大許容TCP接続数を増やします。

注意: 侵入防御モジュールにより、TCP接続の許容数を適用するネットワークエンジンが有効になります。

1. Deep Security Managerで、[ポリシー] をクリックします。
2. 対象のコンピュータに影響するように設定するポリシーを決定します。"ポリシー、継承、およびオーバーライド" on page 724を参照してください。
3. 設定するポリシーを開くには、ポリシーをダブルクリックします。
4. 左側画面で、[設定] をクリックして、[詳細] タブをクリックします。
5. [ネットワークエンジンの詳細設定] エリアで、[継承] が選択されている場合、チェックボックスをクリアして変更を有効にします。

6. ニーズに応じて、[最大TCP接続数]プロパティの値を10000以上に増やします。
7. [保存]をクリックします。

警告:不正プログラム対策エンジンが提供する基本機能

新しいカーネルバージョンがリリースされると、トレンドマイクロはそれらのカーネルサポートパッケージを作成してリリースします。お使いのカーネルバージョンがLinuxエージェントでサポートされていない場合、Linux不正プログラム対策エンジンはお使いのコンピュータに基本的な保護のみを提供します。不正プログラム対策エンジンは、カーネルのバージョンがサポートされると、基本機能モードから通常のステータスに戻ります。

基本機能

カテゴリ	機能名	サポート
検索/検出	ドキュメントの脆弱性対策	✓
	機械学習型検索	(1)
	挙動監視	
	スパイウェア/グレーウェア	✓
	IntelliTrap	✓
	圧縮ファイルの検索	✓
	スマートスキャン	✓
	Connected Threat Defense	✓

カテゴリ	機能名	サポート
検索対象/除外	ドキュメントの脆弱性対策	✓
	ディレクトリの検索対象	✓
	ファイルの検索対象	✓
	ディレクトリの除外	✓
	ファイルの除外	✓
	ファイル拡張子の除外	✓
	プロセスイメージファイルの除外 (2)	✓
隔離	隔離ファイル	✓
	ファイルを復元	✓
コンテナ	コンテナの保護	(3)

(1) 機械学習型検索：トレンドマイクロがプロセスイメージのパスを取得できる場合は動作することがありますが、信頼性が低いためサポートされません。
(2) プロセスイメージファイルの検索対象からの除外：これはユーザモード一致に移動されます。このモードはパフォーマンスに影響する可能性があります。
(3) コンテナ保護：このモードでは、ランタイムコンテナのワークロードを保護できません。

理由ID

一部の機能が動作している場合、Linuxエージェントが完全に機能するようにするには、理由IDに応じて他の手順を実行する必要があります。理由IDは、外部のSyslog、SIEMサーバ、またはAmazon SNSに転送されるイベントに含まれます。また、Linuxエージェントのイベントの説明にも表示されます(「不正プログラム対策エンジンがオフライン」または「不正プログラム対策エンジン(基本機能)」)。

- 理由ID 7：特定のカーネルバージョンで使用可能なドライバがないため、ドライバオフラインエラーが発生します。この問題を解決するには：特定のカーネル用の最新のカーネルサポートパッケージ(KSP)がリリースされているかどうかを確認します。ケースを送信してKSPのサポートをリクエストします。

- 理由ID 11: Trend Micro公開鍵(SecureBootが有効な場合のシステム上)が存在しないため、ドライバのロードに失敗し、ドライバオフラインエラーが発生しました。これを解決するには: "AgentのLinux Secure Bootの設定" on page 520。
- 理由ID 12: Trend Micro公開鍵(SecureBootが有効な場合のシステム上)が期限切れであるため、ドライバのロードに失敗し、ドライバオフラインエラーが発生しました。これを解決するには: "AgentのLinux Secure Bootの設定" on page 520。
- その他すべての理由IDの場合: "診断パッケージの作成" on page 2019、サポートにお問い合わせください。

理由ID	イベントの理由	説明
1	不明な理由	不明な理由により、不正プログラムの検索に失敗しました。
2	不正プログラム対策が不完全です	不正プログラム対策サービスのインストールが不完全なため、ドライバがオフラインになりました。
3	DSAとAMサービス間のプロセス通信の失敗	Deep Security Agentと不正プログラム対策サービス間のプロセス通信が失敗し、ドライバオフラインエラーが発生していました。
4	再起動のタイムアウト	Windows不正プログラム対策サービス(AMSP)がタイムアウトを再開しました(つまり、署名チェックプロセスがハングしました)。
5	不正プログラム対策サービスを停止しました	不正プログラム対策サービスが予期せず停止し、ドライバオフラインエラーが発生しました。
6	署名チェックに失敗しました	Windowsファイル(バイナリまたはDLL)の署名チェックが予期せず失敗しました。
7	使用できないカーネルバージョン	特定のカーネルバージョンで使用可能なドライバがないため、ドライバオフラインエラーが発生しました。
8	ドライバのロード失敗	tmhookまたはbmhookを介してカーネルにドライバーをロードすることが失敗し、ドライバーオフラインエラーが発生しました。
9	ドライバのアンロードに失敗しました	カーネルからのドライバのアンロードに失敗し、ドライバのオフラインエラーが発生しました。 注意: そのようなシナリオは必要ないため、トレンドマイクロはLinux

理由ID	イベントの理由	説明
		プラットフォーム上のDsspStateでこのコードを報告しません。
10	ドライバデバイスを開けません	ドライバデバイスファイルを開けませんでした。ドライバオフラインエラーが発生しました。
11	トレンドマイクロの公開鍵が見つかりません	SecureBootが有効になっている場合、システムのマシン所有者キーが見つからないため、ドライバのロードに失敗し、ドライバのオフラインエラーが発生していました。
12	期限切れのトレンドマイクロの公開鍵	SecureBootを有効にすると、システムのマシン所有者キーのTrend Micro公開鍵の有効期限が切れてドライバのロードに失敗し、ドライバのオフラインエラーが発生しました。
13	不正な公開鍵で署名されています	ドライバーは不明またはサポートされていない公開鍵で署名されました。
14	構成ファイル無効ドライバー	エージェントは構成INIファイルによってドライバーを読み込まないように設定されています。これにより、ドライバーがオフライン状態になります。
15	ポリシー無効ドライバー	エージェントはDeep Securityポリシーによってドライバーを読み込まないように設定されています。これにより、ドライバーがオフライン状態になります。

警告: Census、Good File Reputation、機械学習型検索サービスへの接続解除

国勢調査、グッドファイルレピュテーション、および機械学習型検索 サービスは、トレンドマイクロのSmart Protection Networkがホストするセキュリティサービスです。これらは、Deep Securityの挙動監視、予測的な機械学習、およびプロセスメモリ検索の機能を正常に実行するために必要です。

サービスと機能が対応する表を次に示します。

サービス名	対象機能
Global Censusサービス	挙動監視、機械学習型検索
Good File Reputationサービス	挙動監視、機械学習型検索、プロセスメモリ検索

サービス名	対象機能
機械学習型検索サービス	機械学習型検索

アラートが表示された場合、

Census、*Good File Reputation*、*機械学習型検索サービス*への接続解除

いくつかの原因が考えられます。

- "原因1: AgentまたはRelay有効化済みAgentがインターネットにアクセスできない" below
- "原因2: プロキシは有効化されているが、適切に設定されていない" below

原因1: AgentまたはRelay有効化済みAgentがインターネットにアクセスできない

AgentまたはRelay有効化済みAgentがインターネットにアクセスできない場合は、上記のサービスにアクセスできません。

解決策:

- ファイアウォールポリシーをチェックして、送信HTTPおよびHTTPSポート(初期設定は80または443)が開いていることを確認します。
- このポートを開くことができない場合、他の解決策については、"インターネットにアクセスできないAgentを設定する" on page 1504を参照してください。

原因2: プロキシは有効化されているが、適切に設定されていない

Census、Good File Reputationサービス、機械学習型検索には、プロキシを使用するとアクセスできます。

プロキシが有効化されているかどうかをチェックして、適切に設定されていることを確認するには、次の手順を実行します。

1. **コンピュータまたはポリシーエディタ**[1]を開きます。
2. 左側で[設定]をクリックします。
3. メイン画面で[一般]タブをクリックします。
4. Census、Good File Reputationサービスおよび機械学習型検索向けのネットワーク設定というタイトルの見出しを探します。

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

5. プロキシが指定されている場合、[編集] をクリックして、[プロキシプロトコル]、[アドレス]、[ポート]、およびオプションの [ユーザ名] と[パスワード] が正しいことを確認します。

警告: ディスク容量の不足

「ディスク容量の不足」警告は、Deep Security AgentまたはApplianceが稼働するコンピュータのディスク容量が少なくなり、イベントをこれ以上保存できない可能性があることを示します。警告を開いてその詳細を表示すると、AgentまたはApplianceの場所、残りの空き容量、AgentまたはApplianceで必要な容量が表示されます。

この問題を修正するには、影響を受けるドライブまたはシステムを確認し、不要なデータを消去します。

注意: AgentまたはApplianceは、ドライブの容量がなくなっても、インスタンスを保護し続けますが、イベントの記録は停止されます。

ヒント

- Deep Security AgentまたはApplianceが原因で警告が発生した場合、同一ファイルシステムを共有する別のプログラムにも容量の問題が発生します。
- Deep Security Agentは、通常の操作中にログファイルを自動的に切り詰めて回転します。(この切り詰めとローテーションは、ディスクの空き容量に関する問題とは関係ありません。)
- Deep Security Agentは自身のログファイルをクリーンナップしますが、他のアプリケーションのログファイルはクリーンナップしません。
- Deep Security Managerは「ディスク容量の不足」警告を自動的に消去しませんが、Deep Security Managerから手動で消去できます。

警告: 攻撃の予兆の検出

攻撃の予兆の検索の検出機能は、潜在的な攻撃またはネットワークの機密情報収集活動の早期警告として機能します。

攻撃の予兆の検出の種類

Deep Securityはいくつかの種類の攻撃の予兆を検出できます。

- OSのフィンガープリント調査:AgentまたはApplianceはコンピュータのOSを見つけようとする動作を検出します。

- ネットワークまたはポートの検索:AgentまたはApplianceは、リモートIPがポートに対して異常な割合のIPでアクセスしていることを検出した場合、ネットワークまたはポート検索をレポートします。通常、AgentまたはApplianceのコンピュータは、コンピュータ自身宛てのトラフィックのみを監視するため、ポート検索が最も一般的に検出されます。コンピュータまたはポート検索の検出で使用される統計的な分析方法は「TAPS」アルゴリズムから導出されたもので、2006年にIPCCCで発表された「Connectionless Port Scan Detection on the Backbone」で提案されました。
- TCP Null検索:AgentまたはApplianceはフラグが付いていないパッケージを検出します。
- TCP SYNFIN検索:AgentまたはApplianceはSYNフラグおよびFINフラグの付いたパケットのみ検出します。
- TCP Xmas検索:AgentまたはApplianceは、FINフラグ、URGフラグ、およびPSHフラグの付いたパケット、または値0xFF (想定されるすべてのフラグ) を含むパケットを検出します。

推奨処理

攻撃の予兆の検出アラートを受信したら、このアラートをダブルクリックして、検出を実行しているIP アドレスなどの詳細を表示します。次に、上記の推奨処理のいずれかを実行できます。

- アラートは不正ではない検索によって発生する場合もあります。アラートに記載されているIPアドレスがわかっており、トラフィックに問題がない場合は、IPアドレスを偵察許可リストに追加できます。
  a. コンピュータまたはポリシーエディタ[1]で、[ファイアウォール]→[攻撃の予兆] の順に選択します。
  b. [検出を実行しないIPリスト] にリスト名を追加する必要があります。リスト名がまだ指定されていない場合は、リスト名を選択します。
  c. [ポリシー]→[共通オブジェクト]→[リスト]→[IPリスト] を選択すると、リストを編集できます。IPアドレスを編集および追加するリストをダブルクリックします。
- 特定の期間、ソースIPからのトラフィックをブロックするようにAgentおよびApplianceに指示できます。分数を設定するには、コンピュータまたはポリシーエディタ[2]で、[ファイアウォール]→[攻撃の予

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

[2] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

兆] の順に選択し、[トラフィックのブロック] の値を適切な検索の種類に変更します。
- ファイアウォールまたはセキュリティグループを使用すると、受信IPアドレスをブロックできます。

注意: Deep Security Managerは「攻撃の予兆の検出」アラートを自動的に消去しませんが、Deep Security Managerから手動で消去できます。

攻撃の予兆の検索に関する詳細については、"ファイアウォールの設定" on page 982を参照してください。

プロキシの設定

プロキシの設定

プロキシは、さまざまなトレンドマイクロのサーバとサービス間で設定できます。

このトピックの内容:

- "管理者にプロキシを登録する" on the next page
- "サポートされるプロキシプロトコル" on the next page
- "プロキシ経由でプライマリセキュリティアップデート元に接続する" on page 1457
- "プロキシ経由でDeep Securityリレーに接続する" on page 1459
- "Deep Security Managerにプロキシ経由で接続する" on page 1458
- "Deep Securityソフトウェアのアップデート、CSSSなどにプロキシ経由で接続する" on page 1460
- "プロキシ経由でクラウドアカウントに接続する" on page 1461
- " Deep Discovery Analyzer にプロキシ経由で接続する" on page 1461
- "プロキシ経由でApex Centralに接続する" on page 1461
- "プロキシを介してSmart Protection Networkする" on page 1462
- "プロキシ経由でWorkload Securityに接続" on page 1463
- "プロキシを削除する" on page 1463

管理者にプロキシを登録する

1. Deep Security Managerで、[管理]→[システム設定]→[プロキシ] の順に選択します。
2. [プロキシサーバ領域で、[新規]→[プロキシサーバの追加] の順にクリックします。

3. 名前 および の説明 フィールドに、プロキシのフレンドリ名と説明を入力します。
4. Proxy Protocolの場合は、[HTTP, SOCKS4]または[SOCKS5]のいずれかを選択します。一部のプロトコルはすべてのコンポーネントでサポートされているわけではありません。詳細については、"サポートされるプロキシプロトコル" below を参照してください。
5. アドレスおよびポートフィールドに、プロキシのIPアドレスまたはURLとそのポートを入力します。デフォルト値は、HTTPの場合は8080または80、Squid HTTPプロキシの場合は3128、SOCKS 4および5の場合は1080です。
6. 以前にHTTPまたはSOCKS 5プロキシがコンポーネントの接続からの認証を要求するように設定している場合は、プロキシで認証資格情報 が必要です。[ユーザ名] および [パスワード] の各フィールドに資格情報を入力します。

サポートされるプロキシプロトコル

次の表に、トレンドマイクロのサービスとクライアントでサポートされるプロキシプロトコルを示します。この情報は、dsa_controlを使用してプロキシを登録および設定するために必要です。

サービス	起点(クライアント)	HTTP	SOCKS4	SOCKS5
Deep Security Manager	Agent/Relay	○	×	×
Deep Security Relay	Agent/Relay	○	○	○
Deep Securityソフトウェア アップデート、ソフトウェア安全性評価サービス(CSSS)、ニュースアップデート、製品登録とライセンス管理	Manager	○	×	×
Deep Securityで保護されている製品の使用状況データの収集	Manager	○	×	×
クラウドアカウント(AWS、Azure、Google Cloud Platform、VMware vCloud)	Manager	○	×	×
Deep Discovery Analyzer	Manager	○	×	×
Apex Central(以前は「Control Manager」)	Manager	○	×	×
Smart Protection Network - 国勢調査、グッドファイルレピュテーション、および機械学習型検索	Agent	○	×	×
Smart Protection Network - グローバルSmart Protectionサービス	Agent	○	×	×
Smart Protection Network - スマートフィードバック	Manager	○	×	○

プロキシ経由でプライマリセキュリティアップデート元に接続する

Agent、、Appliance、、およびRelayをプロキシ経由でプライマリセキュリティアップデート元に接続できます。初期設定では、主要なセキュリティアップデート元はトレンドマイクロのアップデートサーバ (Active Updateとも呼ばれます) です。

エージェントおよびアプライアンスである[1] は、割り当てられたRelayを使用できず、プライマリアップデート元へのアクセス権限が明示的に付与されている場合にのみプロキシを使用することに注意してください。

1. Deep Security Agent 10.0以降を使用していることを確認してください。以前のバージョンではプロキシ経由の接続がサポートされていませんでした。
2. "管理者にプロキシを登録する" on the previous pageにプロキシを登録します。
3. 初期設定のRelayグループにセキュリティアップデートプロキシを設定する場合は、次の手順を実行します。
   - Deep Security Managerで、[管理]→[システム設定]→[プロキシ] タブの順に選択します。
   - プロキシサーバの使用領域で、[クライアント、アプライアンス、およびリレー]で使用するプライマリセキュリティアップデートのプロキシを設定して、新しいプロキシを参照するように設定します。
4. 初期設定以外のRelayグループにセキュリティアップデートプロキシを設定する場合は、次の手順を実行します。
   - Deep Security Managerで、[管理]→[アップデート]→[Relay管理] タブの順に選択します。
   - 対象のRelayグループを選択します。[Relayグループのプロパティ]領域で、[アップデート元のプロキシ]設定を変更して、新しいプロキシを指定します。
5. [Save] をクリックします。
6. エージェントを再起動します。

注意:
プロキシは、セキュリティアップデートの失敗の原因となる可能性があるため、プライマリセキュリティアップデート元との通信に使用するTLS証明書を置き換えないでください。

Deep Security Managerにプロキシ経由で接続する

Agentは、エージェントの有効化およびハートビート時にManagerに接続します。プロキシ経由でエージェントをManagerに接続するには、次の2つの方法があります。

[1] Deep Security AgentとDeep Security Virtual Applianceは、ユーザが定義したDeep Securityポリシーを適用するためのコンポーネントです。Agentはコンピュータに直接インストールされ、ApplianceはAgentレスの保護を提供するためにVMware vSphere環境で使用されます。どちらもDeep Security as a Serviceでは使用できません。

デプロイスクリプトを使用してプロキシ経由でエージェントをマネージャに接続する

1. Deep Security Agent 10.0以降を使用していることを確認してください。以前のバージョンではプロキシ経由の接続がサポートされていませんでした。
2. "管理者にプロキシを登録する" on page 1456にプロキシを登録します。
3. Deep Security Managerの右上にある[サポート]→[配信スクリプト]の順にクリックします。
4. ProxyからDeep Security Managerに接続するには、プロキシを選択します。
5. スクリプトをコピーするか保存します。
6. コンピュータでスクリプトを実行します。スクリプトはエージェントをインストールし、指定されたプロキシ経由でマネージャに接続するようにエージェントを設定します。

---

dsa_controlを使用してプロキシ経由でエージェントをマネージャに接続する

Windowsエージェントの場合:

- 管理者としてコマンドプロンプト(cmd.exe)を開き、次のように入力します。

  ```
  cd C:\Program Files\Trend Micro\Deep Security Agent\

  dsa_control -u myUserName:MTPassw0rd

  dsa_control -x dsm_proxy://squid.example.com:443
  ```

Linuxエージェントの場合:

- 次のように入力します。

  ```
  /opt/ds_agent/dsa_control -u myUserName:MTPassw0rd

  /opt/ds_agent/dsa_control -x dsm_proxy://squid.example.com:443
  ```

エージェントのプラットフォームに関係なく、次の手順を実行します。

- プロキシが"サポートされるプロキシプロトコル" on page 1456のいずれかを使用していることを確認します。
- dsa_control とその -u および -x オプションの詳細については、"dsa_control" on page 1794を参照してください。
- プロキシ経由でマネージャに接続する必要がある各エージェントで、これらのコマンドを繰り返します。

- コマンドを実行して、エージェントのローカル設定を更新します。これらのコマンドを実行しても、Managerでポリシーや設定が変更されることはありません。

プロキシ経由でDeep Securityリレーに接続する

AgentはRelayに接続して、ソフトウェアおよびセキュリティアップデートを入手します。プロキシ経由でエージェントをRelayに接続するには、次の2つの方法があります。

プロキシ経由で中継スクリプトにエージェントを接続する

1. Deep Security Agent 10.0以降を使用していることを確認してください。以前のバージョンではプロキシ経由の接続がサポートされていませんでした。
2. "管理者にプロキシを登録する" on page 1456
3. Deep Security Managerの右上にある[サポート]→[配信スクリプト]の順にクリックします。
4. [Relayへの接続に使用するプロキシ]からプロキシを選択します。
5. スクリプトをコピーするか保存します。
6. コンピュータでスクリプトを実行します。スクリプトはエージェントをインストールし、指定されたプロキシ経由でリレーに接続するようにエージェントを設定します。

エージェントをdsa_controlを使用してプロキシを介してリレーに接続する

Windowsエージェントの場合:

- 管理者としてコマンドプロンプト(cmd.exe)を開き、次のコマンドを入力します。

```
cd C:\Program Files\Trend Micro\Deep Security Agent\

dsa_control -w myUserName:MTPassw0rd

dsa_control -y relay_proxy://squid.example.com:443
```

Linuxエージェントの場合:

- 次のように入力します。

```
/opt/ds_agent/dsa_control -w myUserName:MTPassw0rd

/opt/ds_agent/dsa_control -y relay_proxy://squid.example.com:443
```

エージェントのプラットフォームに関係なく、次の手順を実行します。

- プロキシが"サポートされるプロキシプロトコル" on page 1456のいずれかを使用していることを確認します。
- dsa_control とその -w および -y オプションの詳細については、"dsa_control" on page 1794を参照してください。
- プロキシ経由でマネージャに接続する必要がある各エージェントで、これらのコマンドを繰り返します。
- コマンドを実行して、エージェントのローカル設定を更新します。これらのコマンドを実行しても、Managerでポリシーや設定が変更されることはありません。

Deep Securityソフトウェアのアップデート、CSSSなどにプロキシ経由で接続する

エージェントを次のDeep Securityクラウドベースのサーバおよびサービスにプロキシ経由で接続できます。

- ソフトウェアアップデートサーバ(ダウンロードセンターとも呼ばれます)
- 変更監視モジュールの機能であるソフトウェア安全性評価サービス(CSSS)
- 製品登録サービス
- ライセンスサービス
- Deep Security Protected Product Usage Data Collectionサービス(Telemetryサービスとも呼ばれます)

1. "管理者にプロキシを登録する" on page 1456にプロキシを登録します。
2. Deep Security Managerで、上部の[管理]をクリックします。
3. メインペインで、プロキシタブを選択します。
4. (トレンドマイクロサービスへの接続)の横で、プロキシを選択します。
5. [Save]をクリックします。
6. "Deep Security Managerの再起動" on page 1746 およびすべてのマネージャノードを再起動し、CSSSプロキシ設定が有効になるようにします。

プロキシ経由でクラウドアカウントに接続する

プロキシ経由でAWS、Azure、GCPクラウドアカウントにマネージャを接続できます。これらのアカウントの詳細については、"AWSアカウントの追加について" on page 664, "Deep SecurityへのMicrosoft

Azureアカウントの追加" on page 688にMicrosoft Azureアカウントを追加し、"Google Cloud Platformアカウントを追加する" on page 700を追加してください。

1. "管理者にプロキシを登録する" on page 1456にプロキシを登録します。
2. Deep Security Managerで、上部にある[Administration]をクリックします。
3. メインペインで、[プロキシ] タブを選択します。
4. Deep Security Manager(クラウドアカウント- HTTPプロトコルのみ) の横で、プロキシを選択します。
5. [Save] をクリックします。

Deep Discovery Analyzer にプロキシ経由で接続する

マネージャをDeep Discovery Analyzer にプロキシ経由で接続できます。Deep Discovery Analyzerの詳細については、「 "脅威インテリジェンスを使用した新たな脅威の検出" on page 861」を参照してください。

1. "管理者にプロキシを登録する" on page 1456してください。
2. Deep Security Managerで、上部の[管理]をクリックします。
3. メイン画面で[脅威インテリジェンス]タブを選択します。
4. [サンドボックス分析]セクションで、[プロキシ] を選択し、リストからプロキシを選択します。
5. [Save] をクリックします。

プロキシ経由でApex Centralに接続する

プロキシ経由でマネージャーをApex Centralに接続できます。Apex Centralについては、「 "脅威インテリジェンスを使用した新たな脅威の検出" on page 861を参照してください。

1. "管理者にプロキシを登録する" on page 1456してください。
2. Deep Security Managerで、上部の[管理]をクリックします。
3. メイン画面で、[脅威インテリジェンス]タブを選択します。f
4. [不審オブジェクトList]セクションで、[Proxy]チェックボックスをオンにして、リストでプロキシを選択します。
5. [Save] をクリックします。

プロキシを介してSmart Protection Networkする

エージェントとSmart Protection Network内の次のサービス(世界の国勢調査、良好なファイルレピュテーション、機械学習型検索型検索)、およびSmart Protection Network自体との間にプロキシを設定するには、次の手順を実行します。

1. "管理者にプロキシを登録する" on page 1456してください。
2. Deep Security Managerで、上部の[Policies]をクリックします。
3. メイン画面で、プロキシの背後にあるコンピュータの保護に使用するポリシーをダブルクリックします。
4. 次の手順に従って、Census、Good File Reputationサービス、機械学習型検索にプロキシを設定します。
   a. 左側にある[設定] をクリックします。
   b. メイン画面で[一般] タブをクリックします。
   c. メイン画面で[Census、Good File Reputationサービスおよび機械学習型検索向けのネットワーク設定] セクションを探します。
   d. [継承] チェックボックスがオンになっている場合、プロキシ設定は親ポリシーから継承されます。このポリシーまたはコンピュータでこの設定を変更する場合は、チェックボックスをオフにします。
   e. [グローバルサーバへのアクセス時にプロキシを使用する] を選択し、リストでプロキシを選択するか、[新規] を選択して別のプロキシを指定します。
   f. 設定を保存します。
5. 不正プログラム対策で使用するSmart Protection Networkへのプロキシを設定する:
   a. 左側にある[不正プログラム対策] をクリックします。
   b. メイン画面で、[Smart Protection] タブをクリックします。
   c. [ファイルレピュテーションサービス用のSmart Protection Server] の [継承] チェックボックスがオンになっている場合、プロキシ設定は親ポリシーから継承されます。このポリシーまたはコンピュータでこの設定を変更する場合は、チェックボックスをオフにします。
   d. [Global Smart Protectionサービスへの直接接続] を選択します。
   e. [Global Smart Protectionサービスへのアクセス時にプロキシを使用する] を選択し、リストでプロキシを選択するか、[新規] を選択して別のプロキシを指定します。
   f. プロキシ設定を指定し、[OK] をクリックします。
   g. 設定を保存します。
6. Webレピュテーション:
   a. 左側にある[Webレピュテーション] をクリックします。
   b. メイン画面で、[Smart Protection] タブをクリックします。
   c. 前の手順の[不正プログラム対策] と同じ方法で、[Webレピュテーションサービス用のSmart Protection Server] でプロキシを設定します。
   d. 左側にある[Webレピュテーション] を選択したまま、[詳細] タブをクリックします。
   e. [ポート] で、使用しているプロキシの待機ポート番号を含むポートグループを選択し、[保存] をクリックします。たとえば、Squidプロキシサーバを使用している場合は、[Squid Web Server] を選択します。該当するポートグループがない場合は、[ポリシー]→[共通オブジェクト]→[リスト]→[ポートリスト] の順に選択し、[新規] をクリックして、ポートを設定します。
   f. 設定を保存します。
7. エージェントに新しいポリシーを送信します。"ポリシーの変更を手動で送信する" on page 723。

エージェントはプロキシ経由でSmart Protection Networkに接続します。

プロキシ経由でWorkload Securityに接続

Deep Security Managerをプロキシ経由でTrend Cloud One - Endpoint & Workload Securityに接続できます。詳細については、"Trend Vision One Endpoint Security - Server & Workload Protectionにアップグレード" on page 1749を参照してください。

1. マネージャーでプロキシを登録する。
2. Deep Security Managerで、[管理]→[プロキシ] に移動します。
3. Trend Vision One Endpoint Security Link (HTTP Protocol Only)の横で、プロキシを選択します。
4. 保存 をクリックします。

プロキシを削除する

エージェントとマネージャ、またはエージェントとリレーの間でプロキシを削除するには

- プロキシ設定を含まない新しい配信スクリプトを使用して、クライアントを再配信します。詳細については、「"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849の使用」を参照してください。

  または

- エージェントで次のdsa_controlコマンドを実行します。

  ```
  dsa_control -x ""
  ```

  ```
  dsa_control -y ""
  ```

  これらのコマンドは、エージェントのローカル設定からプロキシ設定を削除します。これらのコマンドを実行した結果、マネージャでポリシーまたは設定の変更が行われません。

  dsa_controlおよび-x/>および-yオプションの詳細については、"dsa_control" on page 1794を参照してください。

他のコンポーネント間のプロキシを削除するには

プロキシを介した接続の手順を実行しますが、プロキシを削除できるように、逆の手順を実行してください。

プロキシ設定

プロキシは、さまざまなTrend Microコンポーネント間で設定できます。詳細については、"プロキシの設定" on page 1455を参照してください。

プロキシサーバを使用する

利用可能なプロキシのリストを表示および編集するには、管理 > システム設定 > プロキシに移動します。次のオプションが利用可能です:

- エージェント、アプライアンス、およびリレーによって使用されるプライマリセキュリティアップデートプロキシ ("プロキシ経由でプライマリセキュリティアップデート元に接続する" on page 1457を参照)
- Deep Security Manager (トレンドマイクロサービスへの接続)(詳細は"Deep Securityソフトウェアのアップデート、CSSSなどにプロキシ経由で接続する" on page 1460を参照)
- Deep Security Manager (Cloud Accounts - HTTPプロトコルのみ) ("プロキシ経由でクラウドアカウントに接続する" on page 1461を参照)
- Trend Vision One Endpoint Security リンク (HTTPプロトコルのみ)(プロキシ経由でWorkload Securityに接続を参照)

Relayの設定

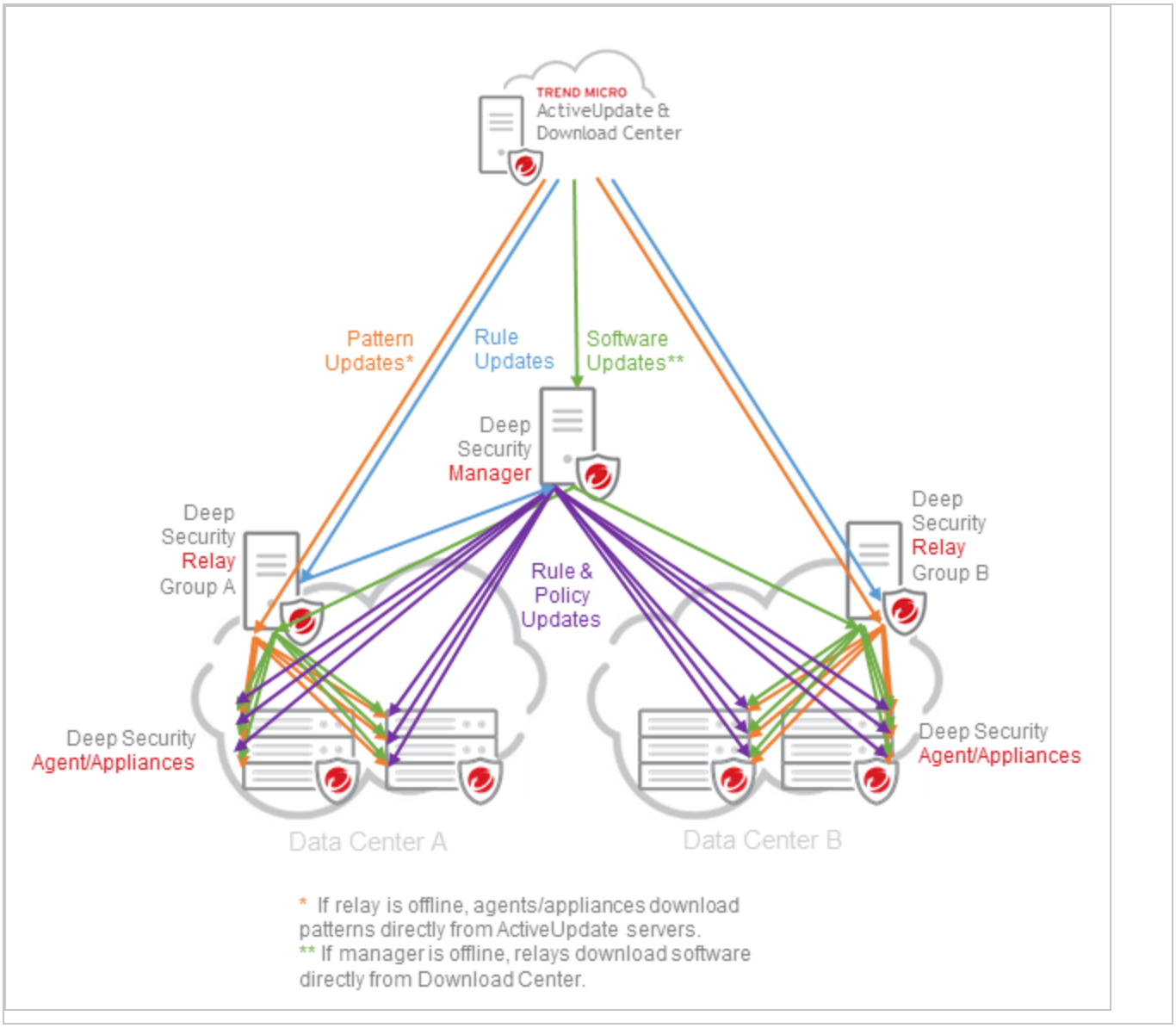
リレーの動作

Relaysでは、ソフトウェアのアップデートとセキュリティ上のアップデートの両方をエージェントおよび仮想アプライアンスに再配信して、展開が適切に機能するように支援します。(または、ソフトウェアアップデートーではなく、セキュリティアップデートーはローカルのミラーWebサーバによって配信される.)Relayには次の機能があります。

- 外部アップデートトラフィックを削減してWAN帯域幅のコストを削減
- 大規模導入におけるアップデート配信の高速化
- アップデートの冗長性を提供する

- 保護されたコンピュータのVMware vMotion中に変更監視データおよびその他の一部のファイルを一時的に保存する

アップデート元は、リレーおよびエージェントのまたは仮想アプライアンスで異なります。アップデート元は、親リレーグループとアップデートの種類に応じて異なります。



エージェントは、割り当てられたリレーグループに対して、ランダムに順序付けられたリレーのリストを取得します。エージェントがアップデートをダウンロードする必要がある場合、エージェントは最初のリレーを試行します。応答がない場合、エージェントはアップデートを正常にダウンロードできるまでリスト内の次のアップデートを試行します。リストはエージェントごとにランダムな値なので、グループのリレー間でアップデート負荷が均等に分散されます。

注意: relays/agentsと仮想アプライアンスがmanager/relay, に接続できない場合、代替アップデート元を使用します。最高のパフォーマンスを得るには、Deep Securityコンポーネント間のネットワーク接続が信頼できるものになっている必要があります。

他のルールのアップデートとは異なり、アプリケーションコントロールのルールはトレンドマイクロからダウンロードされません。ただし、リレーは同様に共有(ローカルではない)アプリケーションコントロールルールセットを再配布できます。「Relayを介したアプリケーションコントロールルールセットのインストール」を参照してください。

Relay階層、コスト、パフォーマンス

Relayグループは階層構造で構成できます.1つ以上の第1レベル(「上位」)リレーグループがマネージャBおよびプライマリセキュリティアップデート元からのアップデート*直接*をダウンロードします(通常はInternet/WAN接続), 経由で、レベル(「子」)のリレーグループは、更新プログラム*を第1レベルのグループ経由で間接的に*( )ダウンロードします。各ローカルネットワーク上に子リレーを配置する場合、通常、クライアントアップデートではローカルネットワーク接続が使用されます。リモート接続はインターネットに接続されません。これにより、外部接続帯域幅(一般的なパフォーマンスのボトルネック)が軽減され、特にネットワークまたはデータセンターの数が多い大規模な環境でのアップデートが高速になります。

パフォーマンスおよび帯域幅使用率は、リレーグループ階層によって影響を受ける可能性があります。階層で指定できる値は次のとおりです。

- 注文のアップデート–子 リレーサブグループが親グループからダウンロードされます。親グループからダウンロードするには、最初に独自のダウンロードを完了する必要があります。したがって、すべてのアップデートがまったく同じ時刻に行われないように、遅延を必要とする場合は一連のサブグループを使用すると便利です。
- 費用 –親リレーグループと子リレーグループの距離が離れている場合は、上位リレーグループ経由で直接ダウンロードするほうが安いかもしれません。
- 速度 –多数のまたは低帯域幅のサブネットが親リレーグループと子リレーグループの間にある場合、直接または親の中継グループ経由ではなく、祖父母経由でのダウンロードが高速になる場合があります。しかし、リレーの数が多すぎると、外部接続の帯域幅が消費され、最終的に速度が低下します。

階層は、リレーグループの作成時に設定されます。詳細については、"Relayグループを作成する" on page 1472を参照してください。

追加のリレーを配信する

最初のDeep Security Relay配信した後は、冗長性と負荷分散のために少なくとも1つ以上を配置する必要があります。展開のサイズと範囲に応じてさらに展開する必要がある場合もあります。

リレーを配置する場合は、次の作業を行う必要があります。

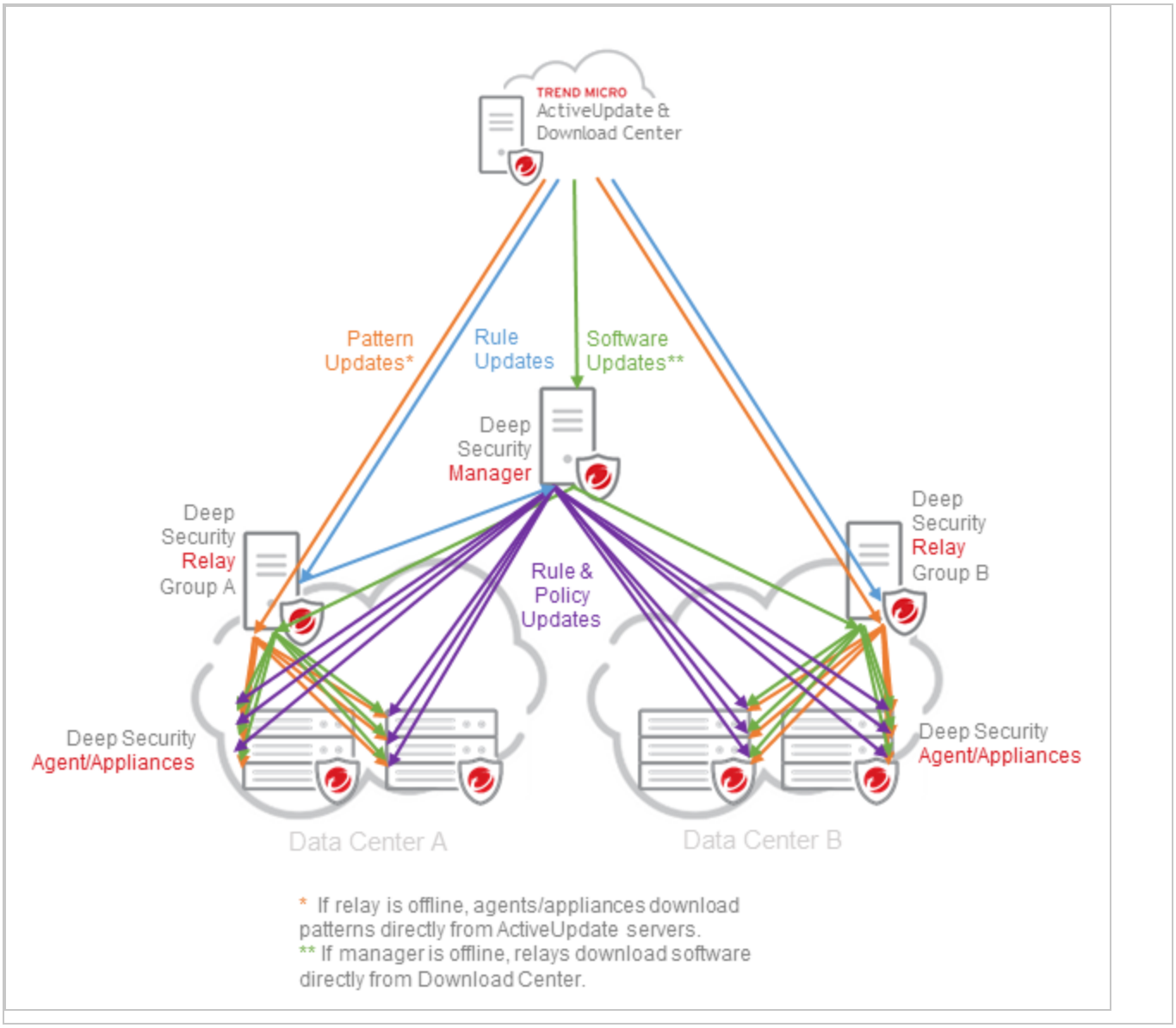
1. "リレーの最適な数と位置を計画する" below
2. "アップデート元を設定する" on page 1470
3. Relayの設定

警告: ネットワーク上のリレーが多すぎるとパフォーマンスが向上しないため、パフォーマンスが低下します。リレーは通常のAgentよりも多くのシステムリソースを使用します。余分なリレーは、外部接続を最小限に抑える代わりに、帯域幅を競合する可能性もあります。必要に応じて、リレーを通常のDeep Security Agentに変換できます。詳細については、「"AgentからRelay機能を削除する" on page 1475」を参照してください。

リレーの最適な数と位置を計画する

リレーの最適な数と配置は次の条件に依存します。

- "地理的地域と距離" on the next page
- "ネットワークアーキテクチャと帯域幅の制限" on the next page
- "エアギャップ環境" on page 1470



地理的地域と距離

理想的には、各地域には少なくとも2つのリレーを持つ独自のリレーグループが必要です。

エージェントは、の同じ地理的地域にローカルリレーを使用する必要があります。長距離およびネットワークの遅延のため、アップデートの再配布が遅くなる可能性があります。他の地域からダウンロードすると、ネットワーク帯域幅および/またはクラウドコストも増加する可能性があります。

ネットワークアーキテクチャと帯域幅の制限

理想的には、帯域幅が制限されたエージェントまたは仮想アプライアンスの各ネットワークセグメントには、少なくとも2つのリレーを持つ独自のリレーグループが必要です。

大量のトラフィック量がネットワーク間を移動する場合、低帯域幅の Internet/WAN 接続、ルータ、ファイアウォール、VPN、VPC、またはプロキシデバイス(ネットワークセグメントをすべて定義できます) がボトルネックになる可能性があります。ボトルネックは、アップデートの再配布を遅くします。したがって、クライアントは、通常、同じネットワークセグメント内のローカルリレーを使用する必要があります。- リレーはボトルネックの外部ネットワークにはありません。

たとえば、リレーグループ階層では、インターネットおよび内部ネットワークの帯域幅の使用を最小限に抑えることができます。1つの「上位」リレーグループのみがインターネット接続を使用できます。サブグループは、ローカルネットワーク接続を介して上位サーバからダウンロードされます。エージェントおよび仮想アプライアンスは、ローカルリレーグループからダウンロードされます。

大規模な導入では、エージェントと仮想アプライアンスの多くが各リレーに接続されている可能性があります。これには、共有サーバにリレーをより多く配置するのではなく、より強力な専用サーバにリレーを配置する必要があります。詳細については、"Deep Security Agent のサイズとリソース消費" on page 420のサイジングを参照してください。

エアギャップ環境

ほとんどの展開はインターネットに接続できます。ただし、インターネット上のトレンドマイクロのアップデートサーバに孤立したネットワーク上に接続できない場合(「Air-Gapped」配信), の場合は、次の手順を実行する必要があります。

1. セキュリティ上のアップデートを取得するために、非武装地帯(インターネットに接続できるDMZ) に別のリレーを追加します。
2. DMZリレーから他の空中ギャップリレーにアップデートをコピーします。

詳細については、"インターネットにアクセスできないAgentを設定する" on page 1504を参照してください。

アップデート元を設定する

リレーを設定する前に、次の手順を実行して、アップデート元を定義し、通常のRelay階層をバイパスしてアップデートを取得するタイミングを定義します。

1. [管理]→[システム設定]→[アップデート] の順に選択します。
2. 必要に応じて、セキュリティアップデート元 とセカンダリソースを設定します。

   初期設定では、プライマリソースは Trend Micro Update Server で、インターネット経由でアクセスします。設定を変更しないでください。サポートプロバイダが、その他のアップデート元を設定す

るよう指示している場合を除きます。代替アップデート元のURLに「http://" 」または「https://".」を含める必要があります。

3. 通常、エージェントおよび仮想アプライアンスは、Deep Security Managerからの指示に従ってセキュリティアップデートを取得するためにリレーに接続します。ただし、およびの十分なインターネット/ WAN帯域幅が利用できる場合、コンピュータが常にマネージャまたはリレー(予約された保守時間など) に接続できない場合は、次のオプションを選択できます。

   - リレーに接続できない場合、セキュリティアップデート元からの直接ダウンロードをAgent/Applianceに許可
   - Deep Security Managerにアクセスできない場合、セキュリティアップデートの自動ダウンロードをAgent/Applianceに許可

   ヒント: ラップトップとポータブルコンピュータを保護する場合、サポートサービスから離れていることがあります。アップデート中に問題の可能性があるセキュリティアップデートのリスクを回避するには、これらのオプションの選択を解除してください。

4. 古いエージェントのセキュリティ更新が必要な場合は、[のサポート対象の8.0および9.0エージェントをにアップデートする]を選択します。これらの薬剤の多くはもはやサポートされているので、デフォルトでは、のDeep Security Managerは、以前のDeep Security Agentの9.0用の更新プログラムをダウンロードしていないとしません。まだサポートされている古いエージェントの詳細については、"Deep Security LTS ライフサイクル日付" on page 121を参照してください。
5. マルチテナントを使用する場合:
   a. 通常、リレーはDeep Security Managerがインストールされた地域 (ロケール) のパターンのみをダウンロードして配信します。これにより、ディスク領域の使用量が最小限に抑えられます。ただし、他の地域にテナントがある場合は、[すべての地域のパターンファイルをダウンロード]を選択します。
   b. 通常、プライマリテナントは、他のテナントとリレーを共有します。これにより、他のテナントが独自のリレーを設定する必要がないため、他のテナントの設定が簡素化されます。これを行わない場合は、[プライマリテナントのリレーグループを初期設定のリレーグループとして使用する(割り当てられていないリレー用)] の選択を解除します。

      注意: このオプションの選択を解除した場合、[管理]→[更新]>>グループ] の順にクリックすると、リレーグループ名は [プライマリテナントのリレーグループ] ではなく、[初期設定のリレーグループ] になります。

6. Deep Security Managerでエージェントアップデートビルドをローカルインベントリに自動インポートする場合は、[ ]を選択して、[インポートされたソフトウェアへのアップデートを自動的にダウンロードします]を実行します。

この設定では、ソフトウェアはDeep Security Managerにインポートされますが、エージェントソフトウェアまたはアプライアンスソフトウェアは自動的にアップデートされません。詳細については、"Deep Security Agentのアップグレード" on page 1676 のアップグレードを参照してください。

7. 通常、リレーはDeep Security Managerに接続してソフトウェアのアップデートを取得し、再配布します。しかし、リレーは常に、このような定期保守時間中として(マネージャと接続できない場合、または企業は、ファイアウォール管理者の間で、リレーのDeep Security Managerがないときは、は、トレンドマイクロのダウンロードセンターからダウンロードソフトウェアアップデートにリレーを許可]を選択することができます), 場合アクセス可能な。リレーは、代わりにダウンロードセンターからソフトウェアのアップデートを取得します。

   ヒント: ハイブリッドクラウド環境では、多くの場合、パブリッククラウド内にいくつかのエージェントとリレーが存在しますが、他のもの(およびマネージャ) はプライベートネットワーク内にあります。プライベートネットワークファイアウォールで ポート番号 を開く危険性を避けるために、またはソフトウェアパッケージをクラウドのリレーに手動でコピーする場合は、このオプションを選択します。

8. 代替ソフトウェアアップデートサーバを設定して、Deep Security Relayを置き換えて、ソフトウェアアップデートの代替ソースを指定します。これにより、セキュリティアップデートが引き続きリレーから送信される必要があることに注意してください。リレーが弾性IPアドレスを持っている場合、を計画している場合にリレーをセキュリティアップデートのみを受信するように設定する場合 (ソフトウェアのアップデートではない),) または ホストソフトウェアをWebサーバ でホストする場合は、効率と可用性の理由から。https://<IP_or_hostname>:<port>/ と入力して、<IP_or_hostname>:<port> を次のいずれかに変更します。
   - 固有IPアドレスを持つリレーのプライベートネットワークIPアドレスとポート
   - Deep Securityソフトウェアをホストするwebサーバおよびポート

Relayの設定

リレーの場所と数、およびリレーで使用するアップデート元を決定したら、次の操作を実行できます。。

1. "Relayグループを作成する" below
2. "リレーを有効にする" on the next page
3. AgentをRelayグループに割り当てる
4. "AgentをRelayのプライベートIPアドレスに接続する" on page 1475

Relayグループを作成する

リレーは、リレーグループに編成する必要があります。リレーグループ自体は、さらに階層構造に編成できます。

Deep Security Managerのインストール時に同じ場所に配置されたリレーをインストールした場合、初期設定のリレーグループが自動的に作成されます。しかし、他の場所にグループを追加する必要がある場合("リレーの最適な数と位置を計画する" on page 1468), では、より多くのグループを作成できます。

1. [管理]→[アップデート]→[Relayの管理] に進みRelay グループのプロパティを開きます。
2. 新しいリレーグループをクリックします。
3. リレーグループの名前を入力します。
4. アップデート元で、セキュリティアップデート元のいずれかを選択するか、サブグループの場合は、, 親リレーグループの名前になります。

   初期設定のRelayグループはアップデート元のリストに含まれていないため、親として設定することはできません。

   コストと速度が最適なアップデート元の選択を検討してください。リレーグループが階層の一部であっても、親リレーグループではなくセキュリティアップデート元からアップデートをダウンロードするほうが安価で高速になる場合があります。
5. この中継グループでセキュリティアップデート元への接続時にプロキシを使用する必要がある場合は、アップデート元プロキシを選択します。詳細については、"プロキシ経由でプライマリセキュリティアップデート元に接続する" on page 1457

   他のリレーグループとは異なり、初期設定のRelayグループでは、[Agent、Appliance、およびRelayで使用されるセキュリティアップデートプロキシを使用します] 設定は、[管理]→[システム設定]→[プロキシ] タブで設定できます。

   このリレーグループが通常は親リレーグループに接続する場合、親リレーグループが使用できず、セキュリティアップデート元を使用するようにフォールバックするように設定されている場合を除き、サブグループはプロキシを使用しません。
6. [コンテンツのアップデート]で、[のセキュリティ]と[ソフトウェアのアップデート] または[のセキュリティのアップデートのみ] []のいずれかを選択します。[Security Updates only]を選択した場合は、別のソフトウェアアップデート元を設定する必要があります。詳細は、"アップデート元を設定する" on page 1470を選択します。

ヒント: 遅延と外部/インターネット帯域幅の使用量を最小限に抑えるには、地域やネットワークセグメント、あるいはその両方に対してRelayグループを作成します。

リレーを有効にする

1. リレーコンピュータが要件を満たしていることを確認してください。"Deep Security Agent のサイズとリソース消費" on page 420および"システム要件 " on page 400を満たしている必要がありま

す。

2. 該当するポート番号のリレーとの間の送受信通信が許可されていることを確認してください。"Deep Securityのポート番号" on page 429を参照してください。
3. リレーがプロキシ経由で接続する必要がある場合は、"プロキシ経由でプライマリセキュリティアップデート元に接続する" on page 1457を参照してください。
4. 選択したコンピュータにエージェントを配信します。"Deep Security Agentソフトウェアの入手" on page 514および"エージェントをインストールする" on page 536を参照してください。
5. エージェントをリレーとして有効にします。
   a. Deep Security Managerにログインします。
   b. 上部の[管理]をクリックします。
   c. 左側のナビゲーションペインで[Relay管理]をクリックします。
   d. リレーを配置するリレーグループを選択します。リレーグループが存在しない場合は、ドメイングループを作成してください。
   e. リレーグループを選択して、リレーを配置するグループを決定します。リレーグループが存在しない場合は、作成してください。Linuxを使用している場合は、ユーザーnobodyとリレーグループnogroupを作成してください。
   f. 使用可能なコンピュータで、配信したばかりのエージェントを選択します。
   g. Relayとグループに追加をクリックします。
   h. Relayとグループに追加をクリックします。

   エージェントはリレーとして有効にされ、リレーアイコン( ) が表示されます。

ヒント: 遅延とインターネット帯域幅の使用量を最小限に抑えるには、同じ地域および同じネットワークセグメントにあるリレーをグループ化します。

ヒント: 検索フィールドを使用してコンピュータのリストをフィルタできます。

AgentをRelayグループに割り当てる

各エージェントが使用するリレーグループを指定する必要があります。各エージェントを手動で中継グループに割り当てるか、イベントベースのタスクを設定して新しいエージェントを自動的に割り当てます。

1. [コンピュータ]に移動します。
2. コンピュータを右クリックし、[Actions]→[Assign Relay Group]の順に選択します。

   複数のコンピュータを割り当てるには、リスト内のコンピュータをShiftキーまたはCtrlキーを押しながらクリックし、[処理]→[Relayグループの割り当て]の順に選択します。
3. コンピュータで使用するリレーグループを選択します。

レイテンシとexternal/Internet の帯域幅使用を最小にするには、同じ地理的地域 and/or ネットワークセグメント内にあるリレーにエージェントを割り当てます。

AgentをRelayのプライベートIPアドレスに接続する

RelayにElastic IPアドレスがある場合、AWS VPC内のAgentはそのIPアドレス経由でRelayにアクセスできない場合があります。その代わりに、Relayグループのプライベート IPアドレスを使用する必要があります。

1. [管理]→[システム設定] の順に選択します。
2. [システム設定] エリアで [アップデート] タブをクリックします。
3. [ソフトウェアアップデート] の [Deep Security Relayの代わりとなるソフトウェアアップデート配信サーバ] で、次のように入力します。

   `https://<IP>:<port>/`

   ここで、`<IP>` はリレーのプライベートネットワークIPアドレス、`<port>` は リレーポート番号
4. [Add] をクリックします。
5. [保存] をクリックします。

Relayグループのプライベート IPが変わった場合は、この設定を手動で更新する必要があります。この設定は自動的には更新されません。

AgentからRelay機能を削除する

次の場合、リレーを通常のDeep Security Agentに戻すことができます。

- 通信遅延の原因となっているリレーが多すぎます
- リレーは、Deep Security Relayになるための最小システム要件を満たしていません。

警告: Deep Securityリレーは、仮想マシン(VM) Deep Security Virtual Applianceで保護されているものをVMware vMotionで移行する場合) にデータを保存します。デプロイメントでvMotionが使用されている場合、リレーを通常のエージェントに戻すと、移行されたVMの保護が失われ、仮想アプライアンスがセキュリティイベントを失う可能性があります。

1. [管理]→[アップデート]→[Relayの管理] に進みます。
2. リレーをエージェントに変換するリレーグループの横にある矢印をクリックします。
3. コンピュータをクリックします。

4. 削除Relayをクリックします。

   Agentのステータスが「無効化しています」に変わり、Relay機能がAgentから削除されます。

   最大15分かかります。エージェントが[無効]状態からこの期間を超えている場合は、エージェントを無効にしてから再有効化して、リレー機能の削除を完了できます。

エージェント(保護されたコンピュータ) の管理

コンピュータおよびAgentのステータス

Deep Security Managerの Computers ページで次の手順を実行します。

- [ステータス] 列にはコンピュータのネットワーク接続の状態が表示され、保護を提供するAgentまたはApplianceが存在する場合は、その状態がカッコ内に表示されます。[ステータス] 列には、システムイベントやAgentイベントも表示されることがあります。"[ステータス] 列 - コンピュータの状態" below および "[ステータス] 列 - AgentまたはApplianceの状態" on the next page
- [タスク] 列にはタスクの状態が表示されます。"[タスク] 列" on page 1478を参照してください。

イベントのリストについては、"Agentイベント" on page 1336と"システムイベント" on page 1342を参照してください。

その他の情報:

- "コンピュータのエラー" on page 1482
- "保護モジュールのステータス" on page 1483
- "コンピュータでその他の処理を実行する" on page 1484
- "コンピュータのアイコン" on page 1487
- "各種コンピュータのステータス情報" on page 1489

[ステータス] 列 - コンピュータの状態

ステータス	説明
有効化済み	AgentまたはApplianceは有効化されています。"コンピュータでその他の処理を実行する" on page 1484を参照してください。
検出済み	検出処理によって、コンピュータがコンピュータリストに追加されました。("コンピュータを検出する" on page 658を参照してください)。
オフライン	ESXiのFilter Driverがオフラインです。

ステータス	説明
のFilter Driver	
管理対象	Agentが存在して有効化されており、保留中の処理やエラーはありません。
複数のエラー	このコンピュータで複数のエラーが発生しています。詳細については、コンピュータのシステムイベントを参照してください。
複数の警告	このコンピュータに複数の警告があります。詳細については、コンピュータのシステムイベントを参照してください。
準備完了	ESXiにVirtual Applianceをインストールする準備ができました(Filter Driverはインストール済みです)。
再有効化が必要	エージェントまたはアプライアンスがインストールされており、Deep Security Managerをリッスンして再アクティベートするのを待機しています。
非管理対象	このコンピュータのエージェントは、アクティベーションされていないため、このDeep Security Managerによって管理されていません。Deep Security Managerは、エージェントをアクティベートするまでエージェントと通信できません。
準備が未完了	ESXiにVirtual Applianceをインストールする準備ができていません (Filter Driverがインストールされていません)。
アップグレード推奨	AgentまたはApplianceの新しいバージョンが使用可能です。ソフトウェアのアップグレードをお勧めします。
Agentのアップグレード中	このコンピュータのAgentソフトウェアを新しいバージョンにアップグレード処理中です。

[ステータス] 列 - AgentまたはApplianceの状態

ステータス	説明
有効化済み	エージェントまたはアプライアンスが正常にアクティベートされ、Deep Security Managerで管理できる状態になりました。
有効化が必要	有効化されていないAgentまたはApplianceが対象のコンピュータで検出されました。Deep Security Managerで管理できるようにするには、アクティベートする必要があります。
無効化が必要	マネージャは、別のDeep Security Managerによってすでにアクティベートされているエージェントまたはアプライアンスをアクティベートしようとしました。元のDeep Security Managerは、エージェントまたはアプライアンスを非アクティブ化してから、新しいマネージャによってアクティブ化される必要があります。
Agent /Appliance なし	コンピュータでAgentまたはApplianceが検出されませんでした。

ステータス	説明
オフライン	**コンピュータエディタまたはポリシーエディタ**[1]→[設定]→[一般]で指定されたハートビート回数でAgentまたはApplianceがManagerに接続されませんでした。 この状態は、ネットワークファイアウォールまたはプロキシ、AWSセキュリティグループ、Agentソフトウェアアップデートによって接続が中断されたり、修復のためにコンピュータの電源がオフになるときに発生します。 ファイアウォール設定で必要なポート番号を許可していることと、コンピュータの電源がオンになっていることを確認してください。
オンライン	AgentまたはApplianceがオンラインで、予期したとおりに動作しています。
不明	AgentまたはApplianceが存在するかどうか判定されていません。
仮想マシン一時停止	仮想マシンが「一時停止」状態です。
仮想マシン停止	仮想マシンが「停止」状態です。

[タスク]列

ステータス	説明
有効化中	ManagerがAgentまたはApplianceを有効化しています。
有効化中(遅延)	関連するイベントベースタスクで指定した時間だけ、Agentまたは Applianceの有効化が遅延します。
有効化の保留中	AgentまたはApplianceを有効化するコマンドが処理待ちになっています。
Agentソフトウェアの配信の保留中	Agentソフトウェアをインストールする命令がコンピュータへの送信処理待ちになっています。
Agentソフトウェアの削除の保留中	Agentソフトウェアを削除する命令がコンピュータへの送信処理待ちになっています。
アプリケーションコントロールのインベントリ検索 - 実行中	アプリケーションコントロールのインベントリ検索が実行中です。
アプリケーションコントロールのインベントリ検索 - 保留中(ハートビート)	アプリケーションコントロールのインベントリ検索を開始する命令は、次回のハートビートでManagerから送信されます。
アプリケーションコントロールのインベントリ検索 - 保留中(オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerがアプリケーションコントロールのインベントリ検索を開始します。
アプリケーションコントロールルールセットのアップデート - 実行中	アプリケーションコントロールルールセットがアップデート中です。

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

ステータス	説明
アプリケーションコントロールルールセットのアップデート - 保留中 (ハートビート)	アプリケーションコントロールルールセットのアップデートを実行する命令は、次回のハートビートでManagerから送信されます。
アプリケーションコントロールルールセットのアップデート - 保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerがアプリケーションコントロールルールセットのアップデートを開始します。
ベースライン再構築の実行中	変更監視エンジンが現在システムベースラインを再構築しています。
ベースライン再構築の一時停止	ベースライン再構築が一時停止になっています。
ベースライン再構築の保留中	変更監視のためにシステムベースラインを再構築する命令が送信処理待ちになっています。
ベースライン再構築の保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。Managerとこのコンピュータ間の通信が再度確立されると、変更監視エンジンがシステムベースラインを再構築します。
ベースライン再構築の処理待ち	ベースライン再構築を実行する命令が処理待ちになっています。
ステータスの確認	Agent/Applianceの状態を確認しています。
無効化の保留中 (ハートビート)	次回のハートビート時にManagerから無効化命令が送信されます。
無効化の実行中	ManagerがAgentまたはApplianceを無効化しています。つまり、エージェントまたはアプライアンスは別のDeep Security Managerによるアクティベーションおよび管理に使用できます。
Agentソフトウェアの配信中	Agentソフトウェアをコンピュータにインストールしています。
ファイルバックアップのキャンセルの実行中	ファイルバックアップがキャンセルされています。
ファイルバックアップのキャンセルの保留中	ファイルバックアップをキャンセルする命令が送信処理待ちになっています。
ファイルバックアップのキャンセルの保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerがファイルバックアップのキャンセルを開始します。
ファイルバックアップの実行中	ファイルバックアップが実行中です。
ファイルバックアップの保留中	ファイルバックアップを開始する命令が送信処理待ちになっています。
ファイルバックアップの保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerがファイルバックアップを開始します。
ファイルバックアップの処理待ち	ファイルバックアップを実行する命令が処理待ちになっています。
イベントの取得	ManagerがAgentまたはApplianceからイベントを取得しています。
変更の検索の実行中	変更の検索が現在処理中です。
変更の検索の一時停止	変更の検索が一時停止になっています。
変更の検索の保留中	変更の検索を開始するコマンドが送信処理待ちになっています。
変更の検索の保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerが変更の検索を開始します。
変更の検索の処理待ち	変更の検索を開始する命令が送信処理待ちになっています。
不正プログラムの手動検索キャンセルの実行中	手動で開始した不正プログラムの検索をキャンセルする命令が送信されました。
不正プログラムの手動検索キャンセルの保留中	手動で開始した不正プログラムの検索をキャンセルするコマンドが送信処理待ちになっています。

ステータス	説明
不正プログラムの手動検索キャンセルの保留中 (オフライン)	Applianceがオフラインです。通信が再度確立されると、手動で開始した不正プログラムの検索をキャンセルする命令が送信されます。
不正プログラムの手動検索の実行中	手動で開始した不正プログラムの検索が処理中です。
不正プログラムの手動検索の一時停止	手動で開始した不正プログラムの検索が一時停止になっています。
不正プログラムの手動検索の保留中	手動で開始した不正プログラムの検索の実行命令がまだ送信されていません。
不正プログラムの手動検索の保留中 (オフライン)	AgentまたはApplianceがオフラインです。通信が再度確立されると、手動で開始した不正プログラムの検索を開始する命令が送信されます。
不正プログラムの手動検索の処理待ち	手動で開始した不正プログラムの検索の実行命令が処理待ちになっています。
不正プログラムの予約検索キャンセルの実行中	不正プログラムの予約検索をキャンセルする命令が送信されました。
不正プログラムの予約検索キャンセルの保留中	不正プログラムの予約検索をキャンセルする命令が送信処理待ちになっています。
不正プログラムの予約検索キャンセルの保留中 (オフライン)	AgentまたはApplianceがオフラインです。通信が再度確立されると、不正プログラムの予約検索をキャンセルする命令が送信されます。
不正プログラムの予約検索の実行中	不正プログラムの予約検索が処理中です。
不正プログラムの予約検索の一時停止	不正プログラムの予約検索が一時停止になっています。
不正プログラムの予約検索の保留中	不正プログラムの予約検索をキャンセルするコマンドがまだ送信されていません。
不正プログラムの予約検索の保留中 (オフライン)	AgentまたはApplianceがオフラインです。通信が再度確立されると、不正プログラムの予約検索を開始する命令が送信されます。
不正プログラムの予約検索の処理待ち	不正プログラムの予約検索をキャンセルする命令が処理待ちになっています。
不正プログラムのクイック検索キャンセルの実行中	不正プログラムのクイック検索がキャンセルされています。
不正プログラムのクイック検索キャンセルの保留中	不正プログラムのクイック検索をキャンセルする命令が送信処理待ちになっています。
不正プログラムのクイック検索キャンセルの保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerが不正プログラムのクイック検索キャンセルを開始します。
不正プログラムのクイック検索の実行中	不正プログラムのクイック検索が実行中です。
不正プログラムのクイック検索の一時停止	不正プログラムのクイック検索が一時停止になっています。
不正プログラムのクイック検索の保留中	不正プログラムのクイック検索を開始する命令が送信処理待ちになっています。
不正プログラムのクイック検索の保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerが不正プログラムのクイック検索を開始します。
不正プログラムのクイック検索の処理待ち	不正プログラムのクイック検索の実行命令が処理待ちになっています。

ステータス	説明
Agentソフトウェアの削除中	Agentソフトウェアをコンピュータから削除しています。
セキュリティアップデートのロールバックの実行中	セキュリティアップデートがロールバックされています。
セキュリティアップデートのロールバックの保留中	セキュリティアップデートをロールバックする命令が送信処理待ちになっています。
セキュリティアップデートのロールバックの保留中 (ハートビート)	セキュリティアップデートをロールバックする命令は、次回のハートビートでManagerから送信されます。
セキュリティアップデートのロールバックの保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerがセキュリティアップデートのロールバックを開始します。
推奨設定の検索の保留中 (ハートビート)	次回のハートビート時にManagerが推奨設定の検索を開始します。
推奨設定の検索の保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerが推奨設定の検索を開始します。
推奨設定の検索の保留中 (仮想マシンがオフライン)	Applianceが現在オフラインです。通信が再度確立されると、Managerが推奨設定の検索を開始します。
オープンポートの検索中	Managerがコンピュータのオープンポートを検索しています。
推奨設定の検索中	推奨設定の検索が進行中です。
セキュリティアップデートの実行中	セキュリティアップデートが実行中です。
セキュリティアップデートの保留中	セキュリティアップデートを実行する命令が送信処理待ちになっています。
セキュリティアップデートの保留中 (ハートビート)	セキュリティアップデートを実行する命令は、次回のハートビートでManagerから送信されます。
セキュリティアップデートの保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerがセキュリティアップデートを開始します。
ポリシー送信中	ポリシーをコンピュータに送信中です。
設定のアップデートの保留中 (ハートビート)	ポリシー変更に対応するために設定をアップデートする命令は、次回のハートビートでManagerから送信されます。
設定のアップデートの保留中 (オフライン)	AgentまたはApplianceが現在オフラインです。通信が再度確立されると、Managerがポリシー変更に対応するための設定のアップデートを開始します。
ソフトウェアをアップグレードしています (実行中)	ソフトウェアアップグレードが実行中です。
ソフトウェアをアップグレードしています (インストールプログラムの送信)	ソフトウェアアップグレードが実行中です。インストールプログラムはコンピュータに送信されています。
ソフトウェアをアップグレードしています (保留中)	ソフトウェアアップグレードを実行する命令が送信処理待ちになっています。
ソフトウェアをアップグレードしています (アップグレードを完了するには再起動する必要があります)	ソフトウェアのアップグレードが要求されましたが、Agentコンピュータが再起動されるまで完了しません。コンピュータは、この状態の場合でも、古いバージョンのDeep Security Agentによって保護されています。
ソフトウェアをアップグレードしています (結果の受信)	ソフトウェアアップグレードが実行中です。結果を受信しています。
ソフトウェアをアップグレードして	コンピュータのアクセススケジュールが許可されると、ソフトウェアアップ

ステータス	説明
います (スケジュール)	グレードが実行されます。

コンピュータのエラー

ステータス	説明
通信エラー	一般的なネットワークエラーです。
コンピュータへのルートなし	通常は、Managerとコンピュータの間のファイアウォールによってブロックされているか、Managerとコンピュータの間のルータが停止しているため、コンピュータに到達できません。
ホスト名解決不能	未解決のソケットアドレスです。
有効化が必要	有効化されていない場合、AgentまたはApplianceに命令が送信されます。
Agent /Applianceとの通信失敗	AgentまたはApplianceとの通信に失敗しました。
プロトコルエラー	IP、TCP、またはHTTP層での通信エラーです。 たとえば、ファイアウォール、ルータ、またはAWSセキュリティグループによって接続がブロックされているためにDeep Security ManagerのIPアドレスに到達できない場合、接続が失敗します。このエラーを解決するには、有効化のポート番号が許可されていること、およびルートが存在することを確認します。
無効化が必要	エージェントまたはアプライアンスは、現在別のDeep Security Managerによってアクティベートされています。
Agent /Appliance なし	ターゲットでAgentまたはApplianceが検出されませんでした。
有効なソフトウェアバージョンなし	要求したプラットフォームおよびバージョンのインストーラが見つからないことを示します。
ソフトウェアの送信失敗	コンピュータへのバイナリパッケージの送信でエラーが発生しました。
内部エラー	内部エラーです。サポート担当者にお問い合わせください。
重複するコンピュータ	Deep Security Managerのコンピュータリスト内の2台のコンピュータが同じIPアドレスを共有しています。
VMware Toolsがインストールされていない	VMware Tools (vShield Endpoint Thin Agent) が、ゲスト仮想マシンにインストールされていません。Deep Security不正プログラム対策および変更監視保護を使用するには、vShield Endpoint Thin Agentが必要です。このエラーステータスは、Deep SecurityがVMware NSX環境に配置されている場合にのみ表示されます。
未解決のソフトウェア変更数の上限に達しました	ファイルシステムで検出されたソフトウェア変更数が上限を超えました。アプリケーションコントロールは引き続き既存のルールを適用しますが、これ以上の変更は記録されず、このコンピュータでのソフトウェアの変更は表示されなくなります。

ステータス	説明
	"ソフトウェアの変更後にアプリケーションコントロールをリセットする" on page 1141を参照してください。

保護モジュールのステータス

[コンピュータ]画面でコンピュータ名の上にマウスを置くと、[プレビュー]アイコン( ) が表示されます。このアイコンをクリックすると、コンピュータの保護モジュールの状態が表示されます。

オンおよびオフの状態:

ステータス	説明
オン	モジュールはDeep Security Managerで設定されており、Deep Security Agentにインストールされ、Deep Security Agentで動作しています。
オフ	モジュールがDeep Security Managerに設定されていないか、Deep Security Agentがインストールされていないか、またはDeep Security Agentで動作していないか、またはその両方です。
不明	保護モジュールでエラーが発生しています。

インストール状態:

ステータス	説明
インストールされていません	モジュールを含むソフトウェアパッケージはDeep Security Managerにダウンロード済みですが、モジュールがDeep Security Managerで有効になっていないか、Agentにインストールされていません。
インストール保留中	モジュールはDeep Security Managerで設定済みですが、Agentにインストールされていません。
インストール実行中	モジュールをAgentにインストール中です。
インストールされています	モジュールはAgentにインストールされています。このステータスは、モジュールの状態が「オフ」の場合にのみ表示されます(状態が「オン」の場合、モジュールはAgentにインストール済みです)。
一致するモジュールプラグインが見つかりません	Deep Security Managerにインポートされた、モジュールを含むソフトウェアパッケージのバージョンが、Agentから報告されたバージョンと一致しません。
サポートされていません/アップデートはサポートされていません	一致するソフトウェアパッケージがAgentに見つかりましたが、プラットフォームでサポートされているモジュールが含まれていません。このモジュールの任意のバージョンがAgentにインストールされているかどうかに応じて、[サポートされていません] または[アップデートはサポートされていません] が表示されます。

コンピュータでその他の処理を実行する

[コンピュータ] 画面の [処理] ボタンには、選択したコンピュータで実行できる処理が多数用意されています。

処理	説明
ステータスの確認	スキャンまたはアクティベーションの試行を実行せずにコンピュータのステータスを確認します。
有効化/再有効化	コンピュータ上のAgentまたはApplianceを有効化/再有効化します。"Agentの有効化" on page 559を参照してください。
無効化	1つのDeep Security Managerインストールから別のDeep Security Managerインストールにコンピュータの制御を転送することができます。その場合は、Agentまたは Applianceを無効にしてから、新しいManagerで再度有効にする必要があります。
ポリシーの割り当て	画面が開き、リストからコンピュータにポリシーを割り当てることができます。コンピュータに割り当てたポリシーの名前は、[コンピュータ] 画面の [ポリシー] 列に表示されます。 注意: ファイアウォールルールの追加やファイアウォールステートフル設定の変更など、他の設定をコンピュータに適用する場合は、ポリシーの名前の横に初期設定が変更されたことがわかるよう太字で表示されます。
ポリシーの送信	Deep Security Managerを使用してコンピュータ上のエージェントまたはアプライアンスの設定を変更する場合(新しい侵入防御ルールの適用、ログ設定の変更など)、Deep Security Managerは新しい情報をエージェントまたはアプライアンスに送信する必要があります。これが「ポリシーの送信」命令です。ポリシーのアップデートは通常ただちに実行されますが、[ポリシーの送信] をクリックして強制的にアップデートすることもできます。
セキュリティアップデートのダウンロード	設定済みのRelayからAgentまたはApplianceに最新のセキュリティアップデートをダウンロードします。"セキュリティ更新プログラムの適用" on page 1661の適用を参照してください。
セキュリティアップデートのロール	AgentまたはApplianceの最新のセキュリティアップデートをロールバックします。

処理	説明
バック	
イベントの取得	通常のイベント取得スケジュール (通常はハートビートごと) をオーバーライドし、コンピュータから今すぐイベントログを取得します。
警告/エラーのクリア	コンピュータのすべての警告とエラーをクリアします。このコマンドは、次の場合に便利です。 • コンピュータのAgentがローカルでリセットされたとき • コンピュータのリストでコンピュータを無効にするかリストから削除する前に、ネットワークからコンピュータが切断されたとき
Agentソフトウェアのアップグレード	エージェントまたはアプライアンスをアップグレードするには、エージェントまたはアプライアンス ソフトウェアパッケージの新しいバージョンをDeep Security Managerにインポートする必要があります("アップグレードについて" on page 1657を参照) 。
推奨設定の検索	Deep Security Managerでは、コンピュータ上のセキュリティルールを検索し、推奨設定を作成できます。推奨設定の検索の結果は、コンピュータの [ルール] 画面の [詳細] 画面に表示されます。"推奨設定の検索の管理と実行" on page 728を参照してください。
推奨設定をクリア	このコンピュータの推奨設定の検索の結果として作成されたルールの推奨をクリアします。また、推奨設定の検索によって生成されたアラートに一覧表示された中から該当するコンピュータを削除します。 注意: この処理では、過去の推奨設定によって割り当てられたルールの割り当ては解除されません。
不正プログラムのフル検索	選択したコンピュータで不正プログラムのフル検索を実行します。フル検索で実行される処理は、このコンピュータで有効になっている不正プログラムの手動検索の設定に応じて変わります。"不正プログラム検索と除外の設定" on page 832を参照してください。
不正プログラムのクイック検索	重要なシステム領域で、現在アクティブな脅威の検索だけが実行されます。クイック検索では、現在アクティブな不正プログラムが検索されますが、活動のない、または保存されている感染ファイルを検索するためにファイルが詳細に検索されることはあり

処理	説明
	ません。大容量のドライブでは、フル検索よりも短時間で終了します。 注意: クイック検索は、手動でのみ実行できます。予約タスクの一部としてクイック検索を予約することはできません。
オープンポートの検索	選択したすべてのコンピュータでポート検索を実行し、コンピュータにインストールされているAgentを確認して、その状態が「無効化が必要」、「有効化が必要」、「再有効化が必要」、または「オンライン」のいずれであるかを判別します。初期設定では、ポート1 ~ 1024が検索されます。この範囲は、**コンピュータエディタまたはポリシーエディタ**[1]→[設定]→[一般] で変更できます。 注意: Agentのハートビートの待機ポート番号は、ポート範囲の設定に関係なく常に検索されます。ManagerはAgentと通信する際、このポート番号を使用して接続します。ただし、コンピュータで通信方向を[Agent/Applianceから開始] (**コンピュータエディタまたはポリシーエディタ**[2]→[設定]→[一般]→[通信方向]) に設定すると、このポート番号は開かれません。使用されるポートのリストについては、"Deep Security のポート番号" on page 429を参照してください。 注意: ネットワーク上の新しいコンピュータは検出されません。新しいコンピュータを検索するには、検出ツールを使用します。
実行中のポート検索をキャンセル	多数のコンピュータまたは広範囲のポートに対して一連のポート検索を開始し、検索に時間がかかりすぎる場合、[実行中のポート検索をキャンセル] オプションを使用して、検索をキャンセルできます。
変更の検索	変更監視では、コンピュータのシステムおよびファイルに対する変更を追跡します。そのためにはベースラインを作成し、定期的に検索してコンピュータの現在の状態とベースラインとを比較します。詳細については、"変更監視の設定" on page 1004を参照

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

[2] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

処理	説明
	してください。
整合性ベースラインの再構築	このコンピュータの変更監視のベースラインを再構築します。
資産評価の割り当て	資産評価を使用すると、コンピュータおよびイベントを重要度別にソートできます。セキュリティルールにはそれぞれ固有の重要度があります。コンピュータでルールがトリガされると、ルールの重要度とコンピュータの資産評価が乗算されます。この値は、重要度の順にイベントにランクを付けるために使用されます。"イベントのランク付けによる重要度の数値化" on page 1169を参照してください。
Relayグループの割り当て	アップデートのダウンロード元となるこのコンピュータのRelayグループを選択するには、コンピュータを右クリックして、[処理]→[Relayグループの割り当て] の順に選択します。

コンピュータのアイコン

 通常のコンピュータ

 Deep Security Relay (Relay対応クライアントがインストールされたコンピュータ)

 Deep Securityスキャナ(検索サービスが有効なエージェントがインストールされたコンピュータ)

 Dockerホスト(物理コンピュータ)

 Dockerがインストールされたマシン

 Dockerがインストールされたマシン

 Dockerがインストールされたマシン

 Scannerがインストールされたマシン

 Scannerがインストールされたマシン(起動済み)

 Scannerがインストールされたマシン(停止)

-  Scannerがインストールされ たAzure仮想マシン(一時停止)
-  Scannerがインストールされ たAmazon EC2
-  Scannerがインストールされ たAmazon EC2 (起動済み)
-  Scannerがインストールされ たAmazon EC2 (停止)
-  Scannerがインストールされ たAmazon EC2 (一時停止)
-  Amazon WorkSpace (起動済み)

vSphere環境のその他のコンピュータアイコン:

-  ESXiサーバ
-  仮想マシン(VMware vCenterによって管理される仮想マシン)
-  仮想マシン(起動済み)
-  仮想マシン(停止)
-  仮想マシン(一時停止)
-  仮想マシン(Relay有効化済み)
-  仮想マシン(起動済み、Relay有効化済み)
-  仮想マシン(停止、Relay有効化済み)
-  仮想マシン(一時停止、Relay有効化済み)
-  仮想マシン(Scanner有効化済み)
-  仮想マシン(起動済み、Scanner有効化済み)
-  仮想マシン(停止、Scanner有効化済み)
-  仮想マシン(一時停止、Scanner有効化済み)
-  Virtual Appliance
-  Virtual Appliance (起動済み)

Virtual Appliance (停止)

Virtual Appliance (一時停止)

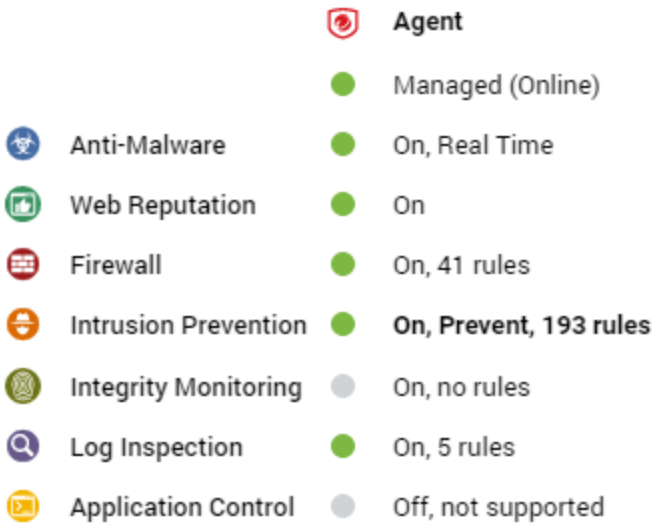
各種コンピュータのステータス情報

円形のアイコンは、エージェントまたはモジュールの全体的なステータスを示します。

- 緑色:問題なし
- 黄色:問題が検出されました
- 赤色:重大な問題が検出されました
- 灰色:問題を検出または確認できません。モジュールがオフになっているか、モジュールがオンになっていてもモジュールに関連付けられたルールがないためにモジュールが結果を報告できない可能性があります。

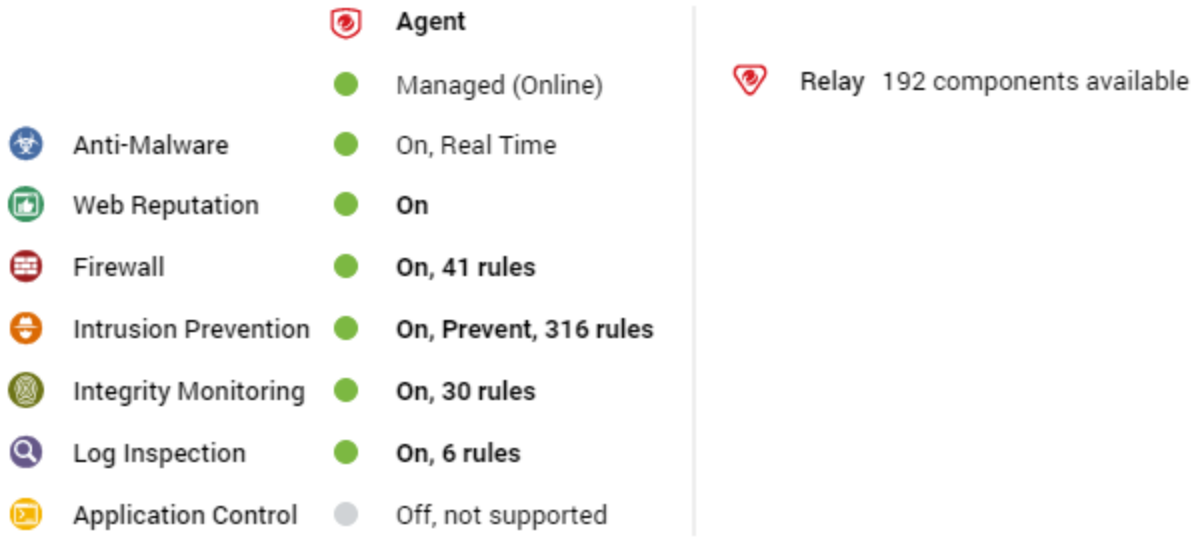
通常のコンピュータ

通常のコンピュータのプレビューペインには、エージェントの有無、ステータス、および保護モジュールのステータスが表示されます。



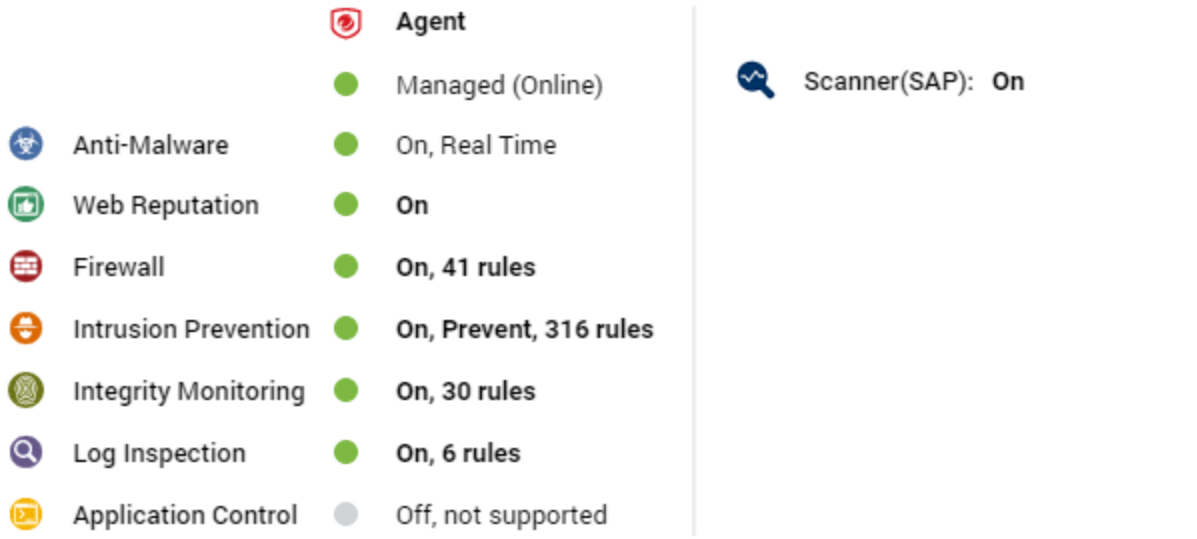
Relay

Deep Securityリレーが有効なエージェントのプレビュー画面には、そのステータス、配信に使用可能なセキュリティアップデートコンポーネントの数、およびDeep Securityエージェントが提供する保護モジュールのステータスが表示されます。



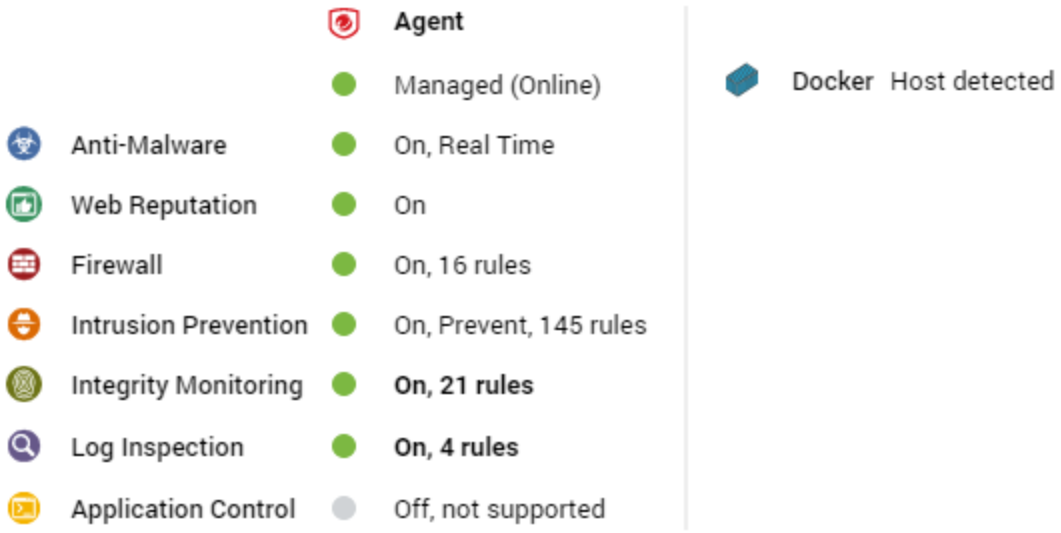
Deep Security Scanner

Deep Security検索ツールのプレビュー画面には、AgentまたはAppliance (コンバインモードの場合はその両方) とそのステータス、保護モジュールのステータス、および検索ツールのステータス (SAP) が表示されます。



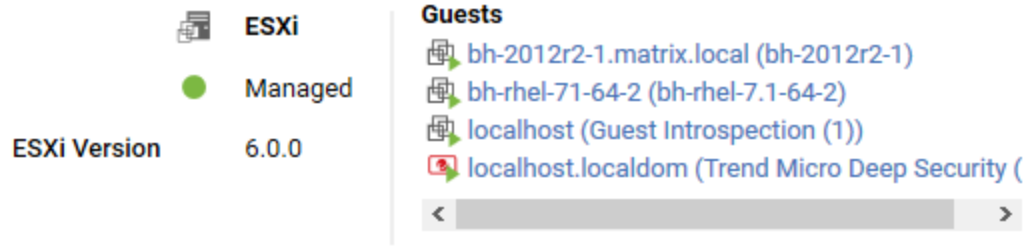
Docker、Podman、およびCRI-Oホスト

ホストのプレビューペインには、エージェントの存在とそのステータス、保護モジュールのステータス、およびホストのステータスが表示されます。



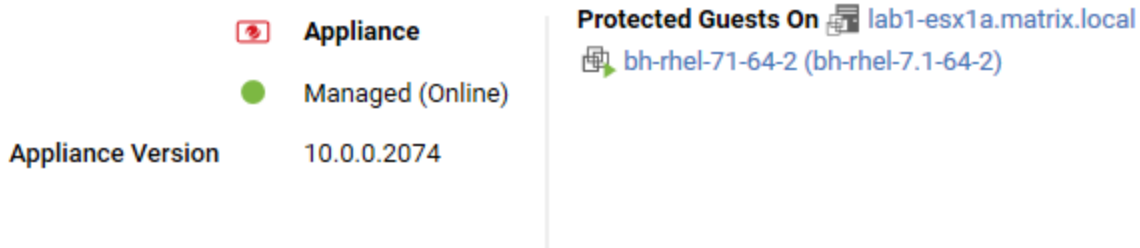
ESXiサーバ

ESXiサーバのプレビュー画面には、ESXiサーバのステータスとESXiソフトウェアのバージョン番号が表示されます。[ゲスト] エリアには、設定されているDeep Security Virtual Applianceと、このホストで実行されている仮想マシンが表示されます。



Virtual Appliance

Virtual Applianceのプレビュー画面には、Applianceのステータスとバージョン番号が表示されます。[ゲストが保護される対象] エリアには、保護されている仮想マシンが表示されます。



仮想マシンをAgentレスで保護する

仮想マシンのプレビュー画面には、仮想マシンがVirtual Applianceまたはゲスト内Agentのいずれかまたは両方で保護されているかが表示されます。また、仮想マシンで実行されているコンポーネントの詳細も表示されます。



エージェントのバージョン管理を設定する

エージェントのバージョン管理は、次の場合に配信されるDeep Security Agentの特定のバージョンを、管理者およびセキュリティ管理チームに制御させる機能です。

- 配置スクリプトを使用する
- アップグレード警告、ボタン、チェックボックス、またはマネージャのその他のウィジェットを使用してエージェントをアップグレードしてください(例外はFAQに記載されています)。
- アクティベーション時のエージェントのアップグレードによるエージェントのバージョンアップ機能

これにより、Deep Security Managerのエージェントのローカルインベントリを管理していないセキュリティオペレーションチームやリレーが、特定の時点でどのエージェントを使用するかを正確に宣言できるようになります。

新しいビジネスセキュリティクライアントがトレンドマイクロによってリリースされると、セキュリティ運用チームは管理下の環境でそれらをテストしてから、バージョン管理設定を変更して新しいビジネスセキュリティクライアントを本番環境の下位アプリケーションチームに公開することができます。

トピック:

- "エージェントのバージョンコントロールを設定する" below
- "エージェントバージョン管理(URL要求あり)" on page 1495
- "エージェントのバージョン管理FAQ" on page 1495

エージェントのバージョンコントロールを設定する

1. 開始する前に、は使用するエージェントのバージョンをインポートします。
2. Deep Security Managerに移動します。
3. 上部の[管理]をクリックします。
4. 左側で、[Updates]→[Software]→[Agent Version Control]の順に展開します。

   すべてのエージェントプラットフォームがメイン画面に表示されます。

5. (オプション)右のShow/Hide Platformsセクションを使用して、表示されているエージェントプラットフォームを制限します。
6. エージェントのバージョンを選択し、[Save]をクリックします。次のガイダンスに従います。

   注意: エージェントバージョン9.0以降のみが表示されます。Solarisの場合は、バージョン11.0以降のみが表示されます。以前のクライアントを配信する場合は、配信スクリプトで使用可能なagentVersion=設定を使用する必要があります。詳細については、「"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849の使用」を参照してください。

列	Description
プラットフォーム	この列には、Deep Security Agentソフトウェアが使用可能なプラットフォームがリスト表示されます。
バージョン	この列では、配信スクリプトなどで使用するエージェントのバージョンを選択します。次のオプションがあります。 • 最新:ローカルのインベントリで提供されている最新のエージェントソフトウェアビルド(長期サポート(LTS)または機能リリース(FR))を使用することを示します。最新のエージェントを決定するロジックは、エージェントのバージョン番号に基づいています。最高のバージョンが使用されます。たとえば、バージョン12.0.0.460のDeep Security 12アップデートエージェントが、Deep Security 12の一般アベイラビリティ(GA)エージェントよりも上位です。ただし、バージョン12.5.0.350のDeep Security 12機能リリースエージェントは、バージョン12.0.0.460のLTSエージェントより遅いと見なされます。要約すると、プラットフォームに最

列	Description
	新のLTSまたはFRエージェントが必要な場合は、[Latest]を選択します。LTSおよびFRリリースの詳細については、"Deep Security 20リリース戦略およびライフサイクルポリシー" on page 116を参照してください。 • Latest LTS : (default) ローカルのインベントリで使用可能な最新の長期サポート(LTS) ソフトウェアビルドを使用することを示します。最新のLTSは元のLTSリリースにすることも、元のLTSリリースにアップデートすることもできます。インベントリ内のすべてのFRは無視されます。LTSビルドバージョンは常にマイナーバージョン番号として「0」を持ちます。LTSおよびFRリリースの詳細については、"Deep Security 20リリース戦略およびライフサイクルポリシー" on page 116を参照してください。 • *<agent_version>* たとえば、11.0.0.760: ローカルインベントリで特定のエージェントバージョンを使用することを示します。インベントリ内の他のエージェントは無視されます。エージェントのバージョンがリストにない場合は、OSに一致するローカルインベントリ内にエージェントが存在しないためです。この問題を解決するには、がエージェントをインベントリにインポートします。 注意: エージェントの最新バージョンは、マネージャ版よりも数リリース遅れていることがあります。たとえば、Windows Server 2003の最新のLTSは、この文書の執筆時点では 10.0.0.3377 です。エージェントの管理下にあるリリースはありますが、[エージェントのバージョン管理]画面に表示されている場合でもサポートされています。詳細については、"Agentプラットフォームサポートポリシー" on page 120を参照してください。
結果エージェント	この列には、VERSION CONTROLの下の選択内容に基づいて配信されるエージェントが表示されます。 列になし(インベントリにAgentがありません) メッセージが表示されるのは、VERSION CONTROLの選択内容に一致するローカルインベントリ内のエージェントがないためです。この問題を解決するには、がエージェントをインベントリにインポートするか、VERSION CONTROLの選択を変更します。

列	Description
	列にN/A(在庫から削除) メッセージが表示された場合、その原因はプライマリテナント(T0)がそのエージェントを配信に適していないと見なして削除したためです。

エージェントバージョン管理(URL要求あり)

Agentのバージョン管理では、エージェントをダウンロードするためのURL要求がDeep Security Managerに送信されたときに、どのエージェントが返されるかを制御できます。詳細については、"エージェントバージョンコントロールを使用して、返されるエージェントバージョンを定義する" on page 1860の定義を参照してください。

エージェントのバージョン管理FAQ

エージェントコントロールとバージョン管理はどのように連携しますか?

エージェントのバージョン管理の導入に先立ち、エージェントのバージョンを制御する主な方法は、あなたが展開したかった自信を持っていたことを選択 輸入 のみのエージェントになりました。エージェントがインポートされると、各プラットフォームの最新のエージェントがリレーに配信されました。その後、upgrade on activation や deployment scriptsなどの機能によって、最新のエージェントがリレーから取得されました。

この機能を継続したい場合(12より前の機能):

1. 前述のように、インベントリに配信するエージェントをインポートし、古いものを削除します。詳細については、"Deep Security Agentソフトウェアの入手" on page 514の入手を参照してください。
2. [エージェントのバージョン管理] [ ]画面に移動し、すべてのプラットフォームが初期設定の最新に設定されていることを確認します。手順については、"エージェントのバージョンコントロールを設定する" on page 1493の設定を参照してください。

   の[最新の]設定は、マネージャに、ローカルインベントリ内の最新のエージェントの使用を続行するように指示します。既存のプロセスを変更せずに引き続き使用できます。

マルチテナントの展開でバージョンコントロールがサポートされていますか?

はい。

プライマリテナントとして(t0), はローカルのインベントリに新しいエージェントバージョンをインポートし、各 エージェントバージョン管理 ページを使用して、各テナントがどのエージェントを配信するかを決定する必要があります。テナントがLTSエージェントのみを使用する場合や特定のエージェントバージョンにロックする場合は、他のテナントから独立して使用できます。

この機能を使用するには、配信スクリプトを更新する必要がありますか?

はい。

配信スクリプトをアップデートするには

1. Deep Security Manager 12以降では、[のサポート]→[展開スクリプト]の順に選択し、新しい配信スクリプトを生成します。手順については、"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849を参照してください。
2. 新しいスクリプトを必要に応じて再配布し、再実行します。

最新の配信スクリプトは、バージョン管理機能が正常に動作するために必要な追加情報をDeep Security Managerに渡します(テナント情報やプラットフォーム情報など) 。

既存の配信スクリプトをアップデートしないとどうなりますか?

エージェントバージョン管理機能が使用可能になる前に生成された既存の配信スクリプトがあり、それらをアップデートするための処理を実行しない場合、初期設定は Latestになります。この初期設定は、エージェントのバージョンコントロールの設定方法に関係なく、すべての古い配信スクリプトに使用されます。古いバージョンの配信スクリプトを新しい配信スクリプトに置き換えて、エージェントのバージョン管理設定で定義した設定を活用します。

エージェントバージョン管理機能が使用可能になった後に生成される配信スクリプトでは、エージェントバージョン管理設定が使用されます。

範囲外の機能(除外)?

設計上、次の機能はエージェントのバージョン管理機能の対象外です。これらの機能には通常、Deep Security Managerの管理者が直接アクセスします。多くの場合、エージェントのバージョンを本番環境に配信する前に、特定のエージェントのバージョンを開発環境またはステージング環境でテストする必要があります。

次の特定のシナリオでアクセス可能なすべてのエージェントバージョンにフルアクセスできます。

- コンピュータの詳細ページ> アップグレードエージェントボタン
- [コンピュータ]→[処理]→[クライアントソフトウェアのアップグレード] ページ

  上記のいずれかのオプションを選択すると、ドロップダウンリストが表示されたウィザードが起動し、バージョンコントロールの設定に関係なく、常に初期設定の[プラットフォーム用の最新バージョンを使用する]に設定されます。詳細については、"[クライアント]ページからエージェントをアップグレードします。" on page 1679から[クライアントのバージョンアップ]を参照してください。

- エージェントのアップグレードはDeep Security Managerから直接開始されません。たとえば、エージェントパッケージをエクスポートしてサーバに転送し、コマンドラインからアップグレードを開始した場合、クライアントバージョンコントロールの設定はこのアップグレードに含まれません。

NICチーミングの設定

「NICチーミング」または「リンク集約」とは、複数のネットワークインタフェースカード(NIC) を使ってコンピュータ上のネットワークリンクを作成することです。総ネットワーク帯域幅を増やしたり、リンクの冗長性を提供する場合に役立ちます。

チーム化されたNICは、WindowsまたはSolaris上でDeep Security Agentと互換性があるように設定できます。

Windows

Windowsでは、NICのチームに参加すると、新しい仮想インタフェースが作成されます。この仮想インタフェースでは、最初にチーム化された物理インタフェースのMACアドレスが使用されます。

初期設定では、Windows Agentはインストール時またはアップグレード時にすべての仮想および物理インタフェースとバインドされます。これには、NICチーミングによって作成された仮想インタフェースが含まれます。ただし、複数のインタフェースで同じMACアドレスが使用されている場合、Deep Security Agentは正常に機能しません。この場合、WindowsではNICチーミングが実行されます。

この問題を回避するには、Agentを物理インタフェースではなく、チーミングした仮想インタフェースにのみバインドします。

警告: インストーラを実行する直前を除き、チーミングしたNICからネットワークインタフェースを追加または削除しないでください。そのような変更を加えると、ネットワーク接続に失敗したり、コンピュータが

Deep Security Managerによって正しく検出されなくなったりすることがあります。Agentのネットワークドライバはインストール時またはアップグレード時にネットワークインタフェースにバインドされ、Agentは以後の変更を継続的に監視することはありません。

Solaris

SolarisのIPMPフェイルオーバ(active-standby)モードでは、2つのNICが同じハードウェア(MAC)アドレスを共有することができます。Deep Security AgentはMACアドレスによってネットワークアダプタを識別するため、このような重複はエージェントが正しく機能しないようにします。

この問題を回避するには、各ネットワークアダプタに一意のMACアドレスを手動で割り当てます。

たとえば、ifconfigを使うと、現在のMACアドレスを確認できます。

```
# ifconfig -a
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
inet 10.20.30.40 netmask 0
ether 8:0:20:f7:c3:f

hme1: flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 8
inet 0.0.0.0 netmask 0
ether 8:0:20:f7:c3:f
```

「ether」行には、アダプタのMACアドレスが表示されます。MACアドレスが同じインタフェースがあり、それらが同じサブネットに接続されている場合は、新しい固有のMACアドレスを手動で設定する必要があります。

```
# ifconfig <interface> ether <new MAC address>
```

MACアドレスが競合する可能性は非常に低いですが、snoopコマンドを使用して、新しいMACアドレスと同じものがないことを確認してください。その後、pingコマンドを使用して、サブネットのブロードキャストアドレスへの接続をテストします。

注意: Solarisでは、同じサブネット上に複数のインタフェースがある場合、任意のインタフェースを経由するようにパケットのルーティングをOSで指定できます。このため、Deep Securityのファイアウォールのステートフルな設定オプションとIPSルールは、すべてのインタフェースに均等に適用する必要があります。

AgentとManagerの通信

Deep Security Managerとエージェントまたはアプライアンスは、相互にサポートされている最新バージョンのTLSを使用して通信します。

この記事のトピック:

- "ハートビートを設定する" below
- "通信方向を設定する" on the next page
- "AgentとManagerの通信でサポートされている暗号化スイート" on page 1502

ハートビートを設定する

ハートビートとは、Deep Security ManagerとDeep Security Agent (またはAppliance)の間の定期的な通信です。ハートビート中に、マネージャーは次の情報を収集します

- ドライバのステータス(オンラインまたはオフライン)
- AgentまたはApplianceのステータス(時刻を含む)
- 前回のハートビート以後のAgentまたはApplianceのログ
- カウンタをアップデートするデータ
- AgentまたはApplianceのセキュリティ設定のフィンガープリント(設定が最新のものかどうか判断するために使用)

ハートビートは、ベースまたは親ポリシー、サブポリシー、あるいは個々のコンピュータで設定できます。

ハートビートは次のプロパティを設定できます。

- ハートビート間隔: ハートビート間の経過時間。
- アラートが発生する前に見逃すことができるハートビートの数: アラートをトリガーする連続して見逃されたハートビートの数。例えば、値が3の場合、4回目の見逃されたハートビートでマネージャーがアラートをトリガーします。

  コンピューターがサーバーである場合、連続して多くのハートビートが失われると、エージェント、アプライアンス、またはコンピューター自体に問題があることを示している可能性があります。ただし、コンピューターがラップトップや接続の持続的な損失が発生しやすい他のシステムである場合、このオプションは無制限に設定する必要があります。

- アラートが発生する前にコンピュータのローカルシステム時間の最大変更(分単位): Windowsでは、システムクロックの変更を検出できるエージェントの場合、これらのイベントはエージェントイベ

ント5004としてマネージャーに報告されます。ここに記載されているクロック変更を超えると、アラートがトリガーされます。この機能をサポートしていないエージェントの場合、マネージャーは各ハートビート操作でエージェントによって報告されたシステム時間を監視し、この設定で指定された許容変更を超える変更を検出するとアラートをトリガーします。

コンピュータの時計の変更アラートがトリガされたら、アラートを手動で消去する必要があることに注意してください。

- 非アクティブな仮想マシンのオフラインエラーを発生させる: 仮想マシンが停止したときにオフラインエラーが発生するかどうかを定義します。

設定を行うには:

1. 設定するポリシーまたはコンピュータの**ポリシーエディタ**[1]または**コンピュータエディタ**[2]を開きます。
2. [設定]→[一般]→[ハートビート]に移動します。
3. 必要に応じてプロパティを変更します。
4. [保存]をクリックします。

通信方向を設定する

注意: 双方向通信は、初期設定で有効になっています。

通信を開始するアーティファクトを定義できます。このアーティファクトは、エージェント、アプライアンス、またはマネージャーである可能性があります。通信にはハートビートおよびその他すべての通信が含まれます。次のオプションが利用可能です:

- 双方向: 通常、エージェントまたはアプライアンスがハートビートを開始し、エージェントのリスニングポート番号でDeep Security Managerからの接続を待ち受けます("Deep Securityのポート番号" on page 429を参照)。マネージャーはエージェントまたはアプライアンスに連絡して必要な操作を実行できます。マネージャーはエージェントまたはアプライアンスのセキュリティ構成に変更を適用できます。

  注意: Deep Security Virtual Applianceは双方向モードでのみ動作します。Virtual Applianceの設定を他のモードに変更すると、機能が中断します。

[1] ポリシーエディタを開くには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。

[2] コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

- マネージャーによる開始: マネージャーはすべての通信をエージェントまたはアプライアンスと開始します。これらの通信には、セキュリティ構成の更新、ハートビート操作、イベントログの要求が含まれます。このオプションを選択する場合は、"Deep Security Agentの保護" on page 1618が既知のDeep Securityマネージャーからの接続のみを受け入れるように保護することを強くお勧めします。
- エージェント/アプライアンス開始: エージェントまたはアプライアンスは、マネージャーからの接続を待ち受けません。代わりに、エージェントはマネージャーがエージェントのハートビートをリッスンするポート番号に接続します("Deep Securityのポート番号" on page 429を参照)。エージェントまたはアプライアンスがマネージャーとのTCP接続を確立すると、すべての通常の通信が行われます。マネージャーは最初にエージェントまたはアプライアンスのステータスとイベントを確認します。これがハートビート操作です。コンピューターで実行する必要がある保留中の操作がある場合(例えば、ポリシーの更新が必要な場合)、これらの操作は接続が閉じられる前に実行されます。マネージャーとエージェントまたはアプライアンス間の通信は、すべてのハートビートでのみ行われます。エージェントまたはアプライアンスのセキュリティ構成が変更された場合、それは次のハートビートまで更新されません。

  注意: Agentからのリモート有効化を設定し、インストールスクリプトを使用してAgentを有効化する方法については、"Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511を参照してください。

マネージャーとエージェントおよびアプライアンス間の通信を有効にするために、マネージャーは自動的に隠しファイアウォールルール(優先度4、バイパス)を実装し、エージェントおよびアプライアンスのハートビート用リスニングポート番号を受信TCP/IPトラフィックに対して開放します。デフォルトでは、任意のIPアドレスおよび任意のMACアドレスからの接続試行を受け入れます。このポートへの受信トラフィックを制限するには、特定のIPまたはMACアドレス、またはその両方からの受信TCP/IPトラフィックのみを許可する新しい優先度4の強制許可またはバイパスファイアウォールルールを作成します。この新しいファイアウォールルールは、設定が次の設定と一致する場合、隠しファイアウォールルールを置き換えます

- アクション: 強制許可またはバイパス
- 優先度: 4 - 最高
- パケットの方向: incoming
- フレームの種類: IP
- プロトコル: TCP
- パケットの宛先ポート: マネージャーからのハートビート接続のためのエージェントのリスニングポート番号、またはポート番号を含むリスト(エージェントのリスニングポート番号を参照)

設定を行うには:

1. 設定するポリシーまたはコンピュータの**ポリシーエディタ**[1]または**コンピュータエディタ**[2]を開きます。
2. [設定]→[一般]→[通信方向]に移動します。
3. Deep Security Managerからエージェント/アプライアンスへの通信の方向 メニューで、次の3つのオプションのいずれかを選択します: Manager Initiated、Agent/appliance Initiated、Bidirectional、またはInheritedを選択します。Inheritedを選択すると、ポリシーまたはコンピュータは親ポリシーから設定を継承します。他のオプションのいずれかを選択すると、Inherited設定がオーバーライドされます。
4. [Save]をクリックします。

エージェントおよびアプライアンスは、マネージャーのホスト名によってネットワーク上のDeep Security Managerを探します。したがって、エージェントまたはアプライアンスが開始する通信または双方向通信が機能するためには、マネージャーのホスト名がローカルDNSに登録されている必要があります。

AgentとManagerの通信でサポートされている暗号化スイート

Deep Security Managerとエージェントまたはアプライアンスは、相互にサポートされている最新バージョンのTLSを使用して通信します。

Deep Security Agent Agentは、Managerとの通信で次の暗号化スイートをサポートしています

- "Deep Security Agent 9.6の暗号化スイート" below
- "Deep Security Agent 10.0の暗号化スイート" on the next page
- "Deep Security Agent 11.0、12.0、および20の暗号化スイート" on the next page

Deep Security Managerがサポートする暗号スイートの詳細については、トレンドマイクロにお問い合わせください。Deep Security Virtual Applianceがサポートする暗号スイートを知る必要がある場合は、アプライアンスに組み込まれているエージェントのバージョンを確認し、そのエージェントをリストで調べてください。

暗号化スイートは、鍵交換非対称アルゴリズム、対称データ暗号化アルゴリズム、およびハッシュ関数で構成されます。

Deep Security Agent 9.6の暗号化スイート

Deep Security Agent 9.6では、以下のTLS 1.0暗号化スイートがサポートされています

---

[1] ポリシーエディタを開くには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。

[2] コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Deep Security Agent 10.0の暗号化スイート

Deep Security Agent 10.0では、以下のTLS 1.2暗号化スイートがそのままの形でサポートされています

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

Deep Security Agent 10.0 Update 16以降では、以下のTLS 1.2暗号化スイートがサポートされています。また、強力な暗号化スイートが有効になっている場合は、サポートされるのは以下のスイートのみです

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Deep Security Agent 11.0、12.0、および20の暗号化スイート

Deep Security Agent 11.0以降では、以下のTLS 1.2暗号化スイートがサポートされています

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

FIPSモードの場合は、以下のTLS 1.2スイートがサポートされています

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

インターネットにアクセスできないAgentを設定する

エージェントまたはリレーがインターネットにアクセスできない場合 (エアギャップエージェント)、トレンドマイクロSmart Protection Networkが提供する一部のセキュリティサービスにアクセスできません。これらのセキュリティサービスは、Deep Security不正プログラム対策およびWebレピュテーションモジュールの完全かつ正常な動作に必要です。

トレンドマイクロSmart Protection Networkセキュリティサービスには以下が含まれます。

サービス名	対象機能
スマートスキャンサービス	スマートスキャン
Webレピュテーションサービス	Webレピュテーション
Global Censusサービス	挙動監視、機械学習型検索
Good File Reputationサービス	挙動監視、機械学習型検索、プロセスメモリ検索
機械学習型検索サービス	機械学習型検索

これらのサービスに加えて、エージェントとRelay有効化済みAgentは、Smart Protection Networkの一部ではないが、トレンドマイクロによってホストされ、インターネット経由でアクセスされるコンポーネントであるトレンドマイクロUpdateサーバ (Active Updateとも呼ばれる) へのアクセスが必要です。

エージェントまたはRelay対応エージェントのいずれかがこれらのサービスに到達できない場合、いくつかの解決策があります。

解決策

- 解決策1:"プロキシを使用する" below
- 解決策2:"Smart Protection Serverをローカルにインストールする" on the next page
- 解決策3: "隔離されたネットワークでアップデートを取得する" on page 1506
- 解決策4:" トレンドマイクロのセキュリティサービスを使用する機能を無効にする" on page 1509

プロキシを使用する

エージェントまたはリレー対応エージェントがインターネットに接続できない場合、接続可能なプロキシをインストールできます。Deep Security AgentとRelayはプロキシに接続し、そのプロキシがSmart

Protection Network内のトレンドマイクロのセキュリティサービスに外向きに接続します。

プロキシを使用すると、各スマートスキャンまたはWebレピュテーションの要求がインターネット経由でTrend Micro Smart Protection Networkに送信されます。代わりにLAN内のSmart Protection Serverを使用して、これらの要求をネットワーク内に保持し、エクストラネットの帯域幅の使用を削減することを検討してください。

プロキシを使用するには、"プロキシの設定" on page 1455を参照してください。

Smart Protection Serverをローカルにインストールする

エージェントとRelay対応エージェントがインターネットに接続できない場合、エージェントとRelay対応エージェントが接続できるローカルエリアネットワーク(LAN)にSmart Protection Serverをインストールできます。ローカルのSmart Protection Serverは、インターネット経由で定期的にSmart Protection Networkに接続し、最新のスマートスキャン不正プログラム対策パターンとWebレピュテーション情報を取得します。この情報はSmart Protection Serverにキャッシュされ、エージェントとRelay対応エージェントによってクエリされます。Smart Protection Serverは、エージェントやRelay対応エージェントに更新をプッシュしません。

このソリューションを使用することに決めた場合、次の点に注意してください。

- 機能が制限されています。ローカルSmart Protection Serverでは、スマートスキャンとWebレピュテーションモジュールのみがサポートされています。
- プロキシソリューションを使用して、挙動監視、機械学習型検索、およびプロセスメモリスキャンを利用してください。詳細は"プロキシを使用する" on the previous pageを参照してください。これらの機能を使用しない場合は、クエリの失敗を防ぎ、パフォーマンスを向上させるために無効にする必要があります。手順については、"トレンドマイクロのセキュリティサービスを使用する機能を無効にする" on page 1509を参照してください

Smart Protection Server をデプロイするには、手動でインストールしてください。詳細については、Smart Protection Server ドキュメントを参照してください。

このシナリオは、エージェントとRelay有効化済みAgentのみがエアギャップされており、Deep Security Managerがインターネットアクセスまたはプロキシアクセスを持っている場合に適用されます。詳細は"ポート番号、URL、およびIPアドレス" on page 428をご参照ください。Deep Security Managerもエアギャップされている場合は、トレンドマイクロActive Updateサーバからセキュリティアップデートを受け取るためにプロキシを使用する必要があります。あるいは、Solution 3 "隔離されたネットワークでアップデートを取得する" on the next pageを使用してください。

隔離されたネットワークでアップデートを取得する

Deep Security Managerがインターネットに接続されていない孤立したネットワークにあり、AgentまたはRelay有効化済みAgentがインターネットに接続できない場合は、インターネットアクセスが可能な非武装地帯 (DMZ)または別のエリアにデータベースとRelay有効化済みAgentを備えた追加のスタンドアロンDeep Security Managerをインストールできます。

すべてのコンポーネントがインストールされたら、DMZ内のRelay有効化済みAgentを構成して、インターネット上のUpdateサーバから最新の不正プログラム検索の更新を自動的に取得できるようにします。これらの更新は.zipファイルに抽出され、その後、手動でエアギャップされたRelayにコピーする必要があります。

このソリューションを使用することに決めた場合、次の点に注意してください。

- .zipファイルには従来の(大規模な)不正プログラムパターンが含まれており、基本的な不正プログラム対策機能を提供します。
- .zipファイルには、侵入防御、変更監視、セキュリティログ監視に使用されるDeep Securityルール更新も含まれています。これらの更新を個別に取得することもできます。"隔離されたネットワークでルールのアップデートを取得する" on page 1508を参照してください。
- 以下の高度な不正プログラム対策機能は利用できません: スマートスキャン、挙動監視、機械学習型検索、プロセスメモリスキャン、およびWebレピュテーション。これらの機能にはトレンドマイクロのセキュリティサービスへのアクセスが必要です。
- 高度な不正プログラム対策機能を無効にする必要があります。これらの機能は使用できません。
- 常に最新の不正プログラムパターンを保持するために、エアギャップされたRelay上の.zipファイルを定期的に更新する計画を立ててください。

このソリューションを展開するには、次の手順に従ってください:

1. Deep Security Managerとその関連データベースをDMZにインストールしてください。これらのインターネットに面したコンポーネントは、DMZマネージャおよびDMZデータベースと呼ぶことができます。
2. DMZにエージェントをインストールし、Relayとして設定します。このエージェントはDMZ Relayと呼ばれます。Relayの設定に関する情報は、"追加のリレーを配信する" on page 1467を参照してください。
   次がインストールされました:
   - DMZマネージャ
   - DMZデータベース
   - DMZ Relay

- エアギャップマネージャ
- エアギャップデータベース
- エアギャップRelay
- 複数のエアギャップAgent

3. DMZ Relayで、このコマンドを実行して最新の不正プログラムパターンを含む.zipファイルを作成してください。

   dsa_control -b
   Command Line出力には、生成された.zipファイルの名前と場所が表示されます。

4. .zipファイルをエアギャップされたRelayにコピーします。ファイルをRelayのインストールディレクトリに配置してください。
   - Windowsでは、デフォルトのディレクトリはC:\Program Files\Trend Micro\Deep Security Agentです。
   - Linuxでは、デフォルトディレクトリは/opt/ds_agentです。

   .zipファイルの名前は変更しないでください。

5. エアギャップManagerで、セキュリティアップデートのダウンロードを開始します。
   a. 上部の[コンピュータ]をクリックします。
   b. コンピュータのリストで、.zipファイルをコピーしたエアギャップRelayを見つけ、右クリックしてセキュリティアップデートをダウンロードを選択します。
      エアギャップRelayは、設定された更新ソース(通常はインターネット上の更新サーバ)を確認します。サーバに接続できないため、インストールディレクトリ内の.zipファイルを確認します。.zipファイルを見つけると、それを抽出して更新をインポートします。更新は、Relayに接続するように設定されたエアギャップエージェントに配信されます。
   c. 更新がエアギャップされたRelayにインポートされた後、.zipファイルを削除してください。
6. 空のギャップのあるリレーを、アップデートサーバではなく自身に接続するように設定します(接続エラーのアラートを防ぐために):
   a. エアギャップManagerにログインします。
   b. 上部の[管理]をクリックします。
   c. 左側で[システム設定]をクリックします。
   d. メインペインで アップデート タブを選択します。
   e. [プライマリセキュリティアップデートサイトのアップデート元]で、[その他のアップデート元]を選択して、https://localhost:[port] と入力します。ここで[port]は、セキュリティアップデートのポート番号(初期設定では4122)です。
   f. [OK]をクリックします。
      エアギャップのあるリレーは、インターネット上のアップデートサーバに接続しようとしなくなりました。

7. オプションとして、パフォーマンスを向上させるために、"トレンドマイクロのセキュリティサービスを使用する機能を無効にする" on the next page。
8. 定期的に、DMZ Relayの最新アップデートをダウンロードし、圧縮して、エアギャップされたRelayにコピーし、Relayでセキュリティアップデートのダウンロードを開始してください。

これで、Deep Security Manager、関連するデータベース、およびリレーがDMZに配置され、不正プログラム検索アップデートを取得できます。

このソリューションをアップグレードするには、次の順序でアップグレードを実行してください:

1. DMZ Manager (データベースソフトウェアのアップグレードも必要な場合はそのデータベースを含む)
2. DMZ Relay
3. エアギャップManager (データベースソフトウェアのアップグレードも必要な場合はそのデータベースを含む)
4. エアギャップRelay
5. エアギャップAgent

警告: リレーを最初にアップグレードしない場合、セキュリティコンポーネントのアップグレードとソフトウェアのアップグレードによりがに失敗することがあります。

アップグレードの詳細については、"Deep Security Managerをインストールする" on page 459、"Deep Security Relay" on page 1675、および"Deep Security Agentのアップグレード" on page 1676を参照してください。

隔離されたネットワークでルールのアップデートを取得する

あなたが作成した.zipファイルには、侵入防御、変更監視、セキュリティログ監視に使用されるDeep Securityルールの更新が含まれています。ただし、それらの更新を個別に取得したい場合は:

1. DMZ Managerで、[管理]→[アップデート]→[セキュリティ]→[ルール]]の順に選択します。
2. ルール更新.dsruファイルをクリックし、エクスポートをクリックします。ファイルはローカルにダウンロードされます。
3. エアギャップマネージャに適用したい各.dsruファイルについてエクスポートを繰り返してください。
4. .dsruファイルをエアギャップマネージャにコピーしてください。
5. Air-Gapped Managerで、[管理]→[アップデート]→[セキュリティ]→[ルール]の順に選択します。
6. インポートをクリックし、.dsruファイルを選択して、次へをクリックします。
7. マネージャーはファイルを検証し、それに含まれるルールの概要を表示します。次へをクリックしてください。

   ルールの更新が正常にインポートされたことを示すメッセージが表示されます。

8. [閉じる] をクリックします。
9. エアギャップマネージャに適用したい各.dsruファイルについてインポートを繰り返してください。

トレンドマイクロのセキュリティサービスを使用する機能を無効にする

トレンドマイクロのセキュリティサービスを使用する機能を無効にすることができます。これにより、エアギャップエージェントがサービスを問い合わせようとしなくなるため、パフォーマンスが向上します。

注意: トレンドマイクロのセキュリティサービスがないと、不正プログラムの検出レベルが大幅に低下し、ランサムウェアがまったく検出されず、プロセスメモリの検索も影響を受けます。したがって、トレンドマイクロのセキュリティサービスへのアクセスを許可するには、他のソリューションの1つを使用することを強くお勧めします。これが不可能な場合は、パフォーマンスを向上するために機能を無効にする必要があります。

- スマートスキャンを無効にするには、次の手順に従います。
  a. **コンピュータまたはポリシーエディタ**[1]を開きます。
  b. 左側で [不正プログラム対策] をクリックします。
  c. メイン画面で [Smart Protection] をクリックします。
  d. スマートスキャンの下で、継承を選択解除 (選択されている場合)、次にオフを選択します。
  e. [保存] をクリックします。
- Webレピュテーションを無効にするには:
  a. **コンピュータまたはポリシーエディタ**[2]を開きます。
  b. 左側で [Webレピュテーション] をクリックします。
  c. メイン画面で [一般] タブが選択されていることを確認します。
  d. 設定リストから、オフを選択します。
  e. [保存] をクリックします。

---

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

[2] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック (またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

- スマートフィードバックを無効にするには、次の手順に従います。
  a. Deep Security Managerで、上部にある[Administration]をクリックします。
  b. 左側にある[システム設定] をクリックします。
  c. メインペインで、スマートフィードバックタブを選択します。
  d. [トレンドマイクロスマートフィードバックを有効にする(推奨)] を選択解除します。
  e. [保存] をクリックします。
- プロセスメモリスキャンを無効にするには:
  a. Deep Security Managerで、上部の [ポリシー] をクリックします。
  b. 左側で共通オブジェクト> その他を展開し、不正プログラム検索の設定をクリックします。
  c. [リアルタイム] の [検索の種類] で不正プログラム検索設定をダブルクリックします。
  d. [一般] タブの [プロセスメモリ検索] で、[プロセスメモリ内の不正プログラムを検索する] を選択解除します。
  e. [OK] をクリックします。
- 機械学習型検索を無効にするには:
  a. 不正プログラムリアルタイム検索設定がまだ開いていることを確認します。
  b. [一般] タブの [機械学習型検索] で、[機械学習型検索の有効化] を選択解除します。
  c. [OK] をクリックします。
- 挙動監視を無効にするには:
  a. 不正プログラムリアルタイム検索設定がまだ開いていることを確認します。
  b. [一般] タブの [挙動監視] で、挙動監視を有効にするの選択を解除します。
  c. [OK] をクリックします。

パフォーマンスを向上させるために、Deep Security Managerでセンサスとグリッド(Goodファイルレピュテーション) クエリを無効にすることができます。それらを有効にしたままにすると、大量の不要なバックグラウンド処理が行われます。

- コマンドラインを使用してセンサス クエリを無効にするには、次のコマンドを実行します:

  ```
  dsm_c -action changesetting -name settings.configuration.enableCensusQuery -value false
  ```

- UIからセンサスクエリを無効にするには:
  a. コンピュータ> 設定 > 一般 > センサス、良好なファイルレピュテーション、および機械学習型検索サービスのネットワーク設定に移動します。
  b. Enable Census queryについては、Noを選択してください。

- コマンドラインを使用してグリッドクエリを無効にするには、次のコマンドを実行してください:

  ```
  dsm_c -action changesetting -name settings.configuration.enableGridQuery -value false
  ```

- UIからグリッドクエリを無効にするには:
  a. コンピュータ> 設定 > 一般 > センサス、良好なファイルレピュテーション、および機械学習型検索サービスのネットワーク設定に移動します。
  b. 良好なファイルレピュテーションのクエリを有効にするには、いいえを選択します。

Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する

エージェントに直接接続するDeep Security Managerではなくエージェント起動の有効化(AIA),) を有効にすると、クライアントはマネージャとの通信を開始し、マネージャのハートビートポート(初期設定では4120) を介して暗号化されたTCP接続を確立します。

AIAを有効にすると、ManagerとAgent間の通信の問題を防ぐことができます。また、インストールスクリプトと共に使用すると、Agentのインストールを簡略化できます。次の場合にAIAを使用することをお勧めします。

- ネットワーク環境により、ManagerからAgentへの接続を開始できない場合。
- 複数のAgentを一度にインストールする必要がある場合。
- クラウドアカウントでコンピュータを保護している場合。

注意: AIAを有効にする前に、AgentがManagerのURLとハートビートのポートに接続できることを確認してください。ManagerのURLとハートビートのポートは、[管理]→[システム情報]→[システムの詳細]→[Managerノード] で確認できます。

Agentからのリモート有効化およびAgentからの通信を有効にする

次の手順を続行します。

1. "Agentからの通信を有効にしたポリシーを作成または変更する" on the next page。
2. "Agentからのリモート有効化を有効にする" on the next page。
3. "Agentにポリシーを割り当てる" on the next page。
4. "インストールスクリプトを使用してAgentを有効にする" on the next page。

Agentからの通信を有効にしたポリシーを作成または変更する

Agentの有効化後に、Managerとの通信を引き続きAgentから開始するには、Agentが使用するポリシーでAgentからの通信を有効にする必要があります。これを行うには、既存のポリシーを変更するか、新しいポリシーを作成してAgentに割り当てます。

ヒント: 既存のポリシーを右クリックして [複製] を選択すると、既存のポリシーから新しいポリシーを簡単に作成できます。

1. [ポリシー] 画面でポリシーをダブルクリックします。
2. [設定]→[一般] に移動します。
3. [通信方向] で [Agent/Applicanceから開始] を選択します。
4. [保存] をクリックします。

Agentからのリモート有効化を有効にする

1. [管理]→[システム設定]→[Agent] の順に選択します。
2. [Agentからのリモート有効化を許可] を選択します。
3. [Agentによるホスト名指定を許可] を選択します。
4. [同じ名前のコンピュータがすでに存在する場合] リストで、[既存のコンピュータの再有効化] を選択します。
5. [保存] をクリックします。

注意: AIAの各設定の詳細な説明については、"Agentの設定" on page 1524の「Agentからのリモート有効化」セクションを参照してください。

Agentにポリシーを割り当てる

インストールスクリプトの設定時にポリシーをAgentに割り当てることも、インストールスクリプトの実行後にイベントベースタスクを使用してポリシーをAgentに割り当てることも可能です。

すべてのAgentで同じポリシーを使用する場合は、次の手順の一環としてインストールスクリプトでポリシーを割り当てることができます。Agentのグループごとに異なるポリシーを使用する必要がある場合は、次の手順に進む前に、ポリシーを割り当てるためにイベントベースタスクを作成してください。

インストールスクリプトを使用してAgentを有効にする

インストールスクリプトを使用してAgentを有効にする方法については、"インストールスクリプトを生成する" on page 1849の「インストールスクリプトを生成する」セクションを参照してください。インストールスクリプトの設定時にポリシーを割り当てる場合は、[セキュリティポリシー] リストから選択します。

Agentを有効化するときに自動的にアップグレードする

「アクティベーション時のアップグレード」は、アクティベーションプロセス中にエージェントのバージョンが確認された場合に、Deep Security Agentを新しいバージョンのソフトウェアに自動的にアップグレードするために使用できる機能です。この機能は、ベーキングプロセスを使用してエージェントを配信する場合に特に便利です("エージェントをAMIまたはWorkSpaceバンドルにインストールする" on page 549).を参照) 。エージェントを焼いた場合、Deep Security Agentの新しいバージョンがリリースされるたびに、「ゴールデン」イメージをアップデートすることは難しい場合があります。この場合は,'のアクティベーション版のアップグレードを使用することができます。このため、古いバージョンのエージェントがベークされたイメージからアクティベーションを実行するたびに、アクティベーションプロセスの一環として指定したバージョンにエージェントをアップグレードするようにDeep Security Managerに指示します。環境を最新に保つ

注意: この機能は、エージェントのバージョン管理 設定に準拠しています。

注意: この機能は現在、LinuxおよびWindowsコンピュータでのみ使用できます。Unixのサポートは、今後のリリースで予定されています。

この機能は次のOSで利用できます。

- Red Hat Enterprise Linux
- Ubuntu
- CentOS
- Debian
- Amazon Linux
- Oracle Linux
- SUSE Linux Enterprise Server
- Cloud Linux
- Windows

Agentの自動アップグレードを有効にする

1. Deep Security Managerで最新のAgentソフトウェアとカーネルサポートパッケージが利用できることを確認します。ソフトウェアアップデートを自動的にダウンロードするか手動でインポートするようにDeep Security Managerを設定できます。詳細については、"Deep Security Agentソフトウェアの入手" on page 514を参照してください。
2. [管理]→[システム設定]→[Agent] の順に選択します。

3. [Agentのアップグレード]で、次のいずれかを選択します. アクティベーション時に自動的にLinuxエージェントをアップグレードする, アクティベーション時にWindowsクライアントを自動的にアップグレードする, アクティベーション時にUnixエージェントを自動的にアップグレードする。
4. [保存] をクリックします。

Agentが正常にアップグレードされたことを確認する

[コンピュータ] 画面の [バージョン] 列には、各コンピュータにインストールされたDeep Security Agentのバージョンが表示されます。

さらに、Agentの自動アップグレードが開始されると、アップグレードのステータスの追跡に使用できる"システムイベント" on page 1342が生成されます。次のシステムイベントを確認できます。

ID	イベント	Description
264	Agentソフトウェアのアップグレード要求	手動かAgentの自動アップグレードによって、Agentソフトウェアのアップグレードが開始されました。
277	アクティベーションアップグレード(スキップ)	Agentは自動アップグレードの対象でしたが、アップグレードは発生しませんでした。 このイベント詳細には、Agentの現行のバージョン、アップグレードが試行されたバージョン、アップグレードが失敗した理由が表示されます。次の理由が考えられます。 • 再起動要求が保留されているため、このコンピュータのアクティベーション時のアップグレードをスキップしました。この問題を解決するには、コンピュータを再起動してください。アップグレード要求は、再起動後の次のアクティベーション時に処理されます。 • アップグレードの対象バージョンがDeep Security Agent 12より前の場合、Windowsサーバでのアクティベーションアップグレードは現在サポートされていません。この機能には、12エージェントに改善が加えられています。アップグレードを成功させるには、エージェントバージョンコントロールの設定 をアップデートして、このプラットフォームに12以降のエージェントを使用するようにしてください。 • 必要なLinuxカーネルサポートファイルが見つからないため、Agentが自動アップグレードされませんでした。Deep Security Managerでは、通常、必要なLinuxカーネルサポートパッケージが自動的にダウン

ID	イベント	Description
		ロードされますが、パッケージを手動でダウンロードしてDeep Security Managerにインポートすることにより、Agentをアップグレードすることもできます。"Deep Security Agentソフトウェアの入手" on page 514を参照してください。 • アクティベーション機能のアップグレードが現在インストールされているOSをサポートしていないため、エージェントは自動的にアップグレードされませんでした。Agentを手動でアップグレードできる場合があります。"エージェントをインストールする" on page 536を参照してください。
706	ソフトウェアアップデート: Agentソフトウェアのアップグレード	アップグレードが成功しました。
707	ソフトウェアアップデート: Agentソフトウェアのアップグレードの失敗	アップグレードに失敗しました。アップグレードに失敗した理由については、イベントの詳細を確認してください。

Deep SecurityでのiptablesのIの使用

Deep Security Agent 10.1以前をLinuxにインストールした場合は、ファイアウォールの競合を避けるために、初期設定でiptablesサービスが無効になっていました(ただし、この変更を防止する設定ファイルが追加されていた場合は例外です)。iptablesサービスはファイアウォール以外にも使用されているため(たとえば、Dockerは通常動作の一貫としてiptablesルールを管理します)、iptablesを無効にすると、悪影響を及ぼすことがありました。

Deep Security 10.2以降 (Deep Security 11を含む) では、iptablesに関連する動作が変更されています。Deep Security Agentによりiptablesが無効化されなくなりました(iptablesが有効な場合は、Agentのインストール後も有効のままです。iptablesが無効な場合は、無効のままです)。ただし、

iptablesサービスが実行されている場合、Deep Security AgentおよびDeep Security Managerでは、以下に説明するように特定のiptablesルールが必要です。

Deep Security Managerの実行に必要なルール

Deep Security Managerがインストールされているコンピュータでiptablesが有効な場合に必要なiptablesルールが2つあります。初期設定では、Deep Security Managerの起動時にこれらのルールが追加され、Managerを停止またはアンインストールするとこれらのルールが削除されます。あるいは、"Deep Securityによるiptablesルールの自動追加を防ぐ" on the next page、手動で次のルールを追加することもできます。

- ポート4119で受信トラフィックを許可します。このルールは、Deep Security ManagerのWeb UIおよびAPIへのアクセスに必要です。
- ポート4120で受信トラフィックを許可します。このルールは、Agentのハートビートの待機に必要です(詳細については、"AgentとManagerの通信" on page 1499を参照してください)。

注意: これらのポート番号は初期設定の番号のため、環境によっては異なるポートが使用されている場合もあります。Deep Securityで使用されるポートの完全なリストについては、"ポート番号、URL、およびIPアドレス" on page 428を参照してください。

Deep Security Agentの実行に必要なルール

Deep Security Agentがインストールされているコンピュータでiptablesが有効な場合は、iptablesルールの追加が必要になる場合があります。初期設定では、Deep Security Agentの起動時にこれらのルールが追加され、Agentを停止またはアンインストールするとこれらのルールが削除されます。あるいは、"Deep Securityによるiptablesルールの自動追加を防ぐ" on the next page、手動で次のルールを追加することもできます。

- ポート4118で受信トラフィックを許可します。このルールは、AgentがManagerからの通信または双方向通信を使用している場合に必要です(詳細については、"AgentとManagerの通信" on page 1499を参照してください)。
- ポート4122で受信トラフィックを許可します。このルールは、AgentがRelayとして機能する場合に、ソフトウェアのアップデートを配信できるようにするために必要です(詳細については、"追加のリレーを配信する" on page 1467を参照してください)。

注意: これらのポート番号は初期設定の番号のため、環境によっては異なるポートが使用されている場合もあります。Deep Securityで使用されるポートの完全なリストについては、"ポート番号、URL、およびIPアドレス" on page 428を参照してください。

Deep SecurityによるiptablesルールのIに追加を防ぐ

必要なルールを手動で追加する場合は、Deep Security ManagerおよびDeep Security Agentでiptablesを変更できないようにできます。iptablesを自動的に変更しないようにするには、Deep Security ManagerおよびDeep Security Agentをインストールするコンピュータに次のファイルを作成します。

/etc/do_not_open_ports_on_iptables

エージェントセルフプロテクションを有効化または無効化する

Deep Securityエージェントセルフプロテクションは、ローカルユーザがエージェントを改ざんするのを防ぎます。有効にすると、ローカルユーザがエージェントを改ざんしようとした場合、「このアプリケーションの削除または変更はセキュリティ設定により禁止されています」というメッセージが表示されます。

エージェントセルフプロテクションはWindowsおよびLinuxでサポートされています。後者にはDeep Security Agentバージョン20.0.0-5953以降が必要です。

Deep Security Agentまたは Relayをアップデートまたはアンインストールする場合、またはコマンドラインからサポート対象の診断パッケージを作成しようとしているローカルユーザの場合診断パッケージとログを作成する、に従ってエージェントの自己保護を一時的に無効にする必要があります。

Windowsでは、不正プログラム対策保護を有効にして、ローカルユーザがエージェントを停止したり、エージェント関連のファイルやWindowsレジストリエントリを変更したりするのを防ぐ必要があります。Linuxでは、次のいずれかを有効にする必要があります: 不正プログラム対策、アプリケーションコントロール、リアルタイムでの変更監視。エージェントのアンインストールを防ぐために自己保護は必要ありません。

Deep Security Agentを停止する前に、問題を回避しスムーズな操作を確保するために、未承認の変更に対する保護機能である自己保護を無効にする必要があります。

エージェントの自己保護は、Deep Security Manager、またはエージェントのコンピュータ上のコマンドラインを使用して設定できます。

Deep Security Managerを介してセルフプロテクションを設定する

1. Agentセルフプロテクションを有効にするコンピュータまたはポリシーエディタ[1]を開きます。
2. [設定]→[一般]を選択します。
3. エージェントセルフプロテクションセクションで、はいを選択して、ローカルユーザがエージェントをアンインストール、停止、またはその他の変更をするのを防ぎます。
4. ローカルオーバーライドにはパスワードが必要ですの場合、はいを選択し、認証パスワードを入力します。認証パスワードは、dsa_controlコマンドの不正使用を防ぐために強く推奨されます。パスワードを指定した後、エージェントでコマンドを実行する際には、dsa_controlコマンドと-pまたは--passwd=オプションを使用して入力する必要があります。パスワードは32文字を超えることはできません。この長さを超えると、パスワードは自動的に切り捨てられます。
5. [保存]をクリックします。
6. 自己防御を無効にするには、いいえを選択し、保存をクリックします。

Command Lineを使用して自己防御を設定する

Command Lineを使用して自己保護を有効または無効にすることができますが、1つの制限があります: 認証パスワードを指定することはできません。そのためにはDeep Security Managerを使用する必要があります ("Deep Security Managerを介してセルフプロテクションを設定する" aboveを参照してください)。

WindowsでCommand Lineを使用する

1. Windows Agentにローカルでログインします。
2. 管理者権限でコマンドプロンプト(cmd.exe)を開きます。
3. 現在のディレクトリをDeep Security Agentのインストールフォルダに変更します。初期設定のインストールフォルダは次のとおりです:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Agent
   ```

4. 次のいずれかのコマンドを入力します。

   Agentセルフプロテクションを有効にするには、次のコマンドを入力します。

   ```
   dsa_control --selfprotect=1
   ```

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

Agentセルフプロテクションを無効にするには、次のコマンドを入力します。

`dsa_control --selfprotect=0 -p <password>`、`-p <password>`の部分には、Deep Security Managerで事前に指定した認証パスワードを入力します。詳細については、「"Deep Security Managerを介してセルフプロテクションを設定する" on the previous page」を参照してください。

LinuxでCommand Lineを使用する

1. 管理者としてコマンドプロンプトを開きます。
2. 現在のディレクトリをDeep Security Agentのインストールフォルダに変更します。以下はデフォルトのインストールフォルダを示しています。

   ```
   cd /opt/ds_agent
   ```

3. 次のコマンドのいずれかを入力してください:

   エージェントセルフプロテクションを有効にするには、次を入力してください:

   ```
   dsa_control --selfprotect=1
   ```

   エージェントセルフプロテクションを無効にするには、次を入力してください:

   `dsa_control --selfprotect=0 -p <password>`、`-p <password>`は以前にDeep Security Managerで指定された認証パスワードです。詳細については、"Deep Security Managerを介してセルフプロテクションを設定する" on the previous pageを参照してください。パスワードは32文字を超えることはできません。この長さを超えると、パスワードは自動的に切り詰められます。

Linuxの制限事項

- システムがシャットダウンまたは再起動しているときにエージェントサービスを停止しないでください。サービスを停止すると、再起動後に正常に動作しない可能性があります。
- エージェントサービスのステータスが不一致になる可能性があります。コマンドstopを実行してエージェントサービスを停止しようとすると、結果は成功と返されますが、エージェントサービスは通常通り動作し続けます。
- システム内でエージェントプロセスと同じ名前の実行中のプロセスがある場合、それは自己保護リストに追加されます。保護されたプロセスは改ざんから保護されます。
- Out-Of-Memory (OOM) が発生した場合、エージェントサービスを終了することはできません。

- Oracle 6 (32-bit) プラットフォームは自己保護をサポートしていません。
- セキュアブートを有効にしていて自己保護が機能していない場合は、マシンのカーネルバージョンを確認してください。カーネルバージョンが5.4以前の場合は、5.4より新しいカーネルバージョンにアップグレードしてください。

トラブルシューティング

サービスの状態を正常に戻すには、次の手順に従ってください。

1. エージェントセルフプロテクションを停止します。
2. エージェントサービスを再起動してください。

エージェントサービスが再起動すると、エージェントセルフプロテクションが再開されます。

オフラインエージェントはDeep Securityによって保護されていますか?

Deep Security Managerでオフラインとして表示されているエージェントは、最後に知られている構成に従って保護されています。ただし、Deep Security Managerとの通信が復旧するまで、ソフトウェア、セキュリティ、ポリシーの更新を受け取ることはできません。

エージェントをオフライン状態から復帰させる方法についての詳細は、"オフラインエージェント" on page 1986を参照してください。

非アクティブなAgentのクリーンナップによるオフラインコンピュータの削除の自動化

Deep SecurityがDeep Security Managerと通信していない多数のオフラインコンピュータを使用している場合は、まずコネクタを使用してみてください("AWSアカウントの追加について" on page 664, "Deep SecurityへのMicrosoft Azureアカウントの追加" on page 688にMicrosoft Azureアカウントを追加する、または "Google Cloud Platformアカウントを追加する" on page 700) 。コネクタを使用すると、コンピュータがライフサイクル全体を通して自動的に管理されるため、クラウドアカウントから削除されたコンピュータはDeep Securityからも自動的に削除されます。環境内でコネクタを使用できない場合は、[非アクティブなAgentのクリーンナップ] を使用して、非アクティブなコンピュータの削除を自動化できます。非アクティブなエージェントのクリーンアップは(2日から12ヶ月まで) 一定の期間のためにオフラインにし、非アクティブにされたコンピュータ1時間ごと確認し、それらを削除します。

注意: 非アクティブなAgentのクリーンナップを使用すると、1時間おきの確認時に最大で1000台のオフラインコンピュータが削除されます。これを上回る数のオフラインコンピュータがある場合は、確認時に1000台ずつ削除され、すべてのオフラインコンピュータが削除されるまでこの動作が繰り返されます。

非アクティブなAgentのクリーンナップを有効にした後には、次のことも行えます。

- "長期間にわたってオフラインになっているコンピュータのDeep Securityによる継続保護" below (任意ですが、有効にしておくことをお勧めします)
- "オーバーライド設定による特定のコンピュータの削除の回避" on the next page (任意)
- "非アクティブなAgentのクリーンナップジョブによって削除されたコンピュータの監査証跡の確認" on the next page

注意: 非アクティブなAgentのクリーンナップでは、クラウドコネクタによって追加されたオフラインコンピュータは削除されません。

非アクティブなAgentのクリーンナップを有効にする

1. [管理] ページに移動します。
2. [システム設定]→[Agent]→[非アクティブなAgentのクリーンナップ] で、[次の期間を超過した非アクティブなAgentを削除する:] を選択します。
3. 非アクティブな期間がどのくらい続いているコンピュータを削除するかをリストから選択します。
4. アクティブではあるものの"長期間にわたってオフラインになっているコンピュータのDeep Securityによる継続保護" below の設定をします (任意ですが、有効にしておくことをお勧めします)。
5. [保存] をクリックします。

長期間にわたってオフラインになっているコンピュータのDeep Securityによる継続保護

あなたがアクティブになっているが、のDeep Security Managerと不規則な通信オフラインのコンピュータを持っている場合、彼らはあなたが定義した非アクティブの期間内に通信できない場合は、非アクティブなエージェントのクリーンアップは、それらを削除します。これらのコンピュータがDeep Security Managerに再接続するようにするには、Agentからのリモート有効化 と不明なAgentの再有効化の両方を有効にすることをお勧めします。これらを有効にするには、[システム設定]→[Agent]→[Agentからのリモート有効化] で、[Agentからのリモート有効化を許可] を選択した後、[不明なAgentの再有効化] を選択します。

注意: 削除されたコンピュータが再接続した場合、ポリシーは割り当てられず、新しいコンピュータとして追加されます。そのコンピュータへの直接リンクは、Deep Security Managerイベントデータからすべて削除されます。

ヒント: イベントベースタスクを使用すると、Agentからのリモート有効化の際に、コンピュータに割り当てられたポリシーを自動的に割り当てることができます。

オーバーライド設定による特定のコンピュータの削除の回避

コンピュータまたはポリシーレベルでオーバーライドを設定すると、非アクティブなAgentのクリーンナップによってコンピュータが削除されるのを明示的に回避できます。

オーバーライドを設定するには、次の手順に従います。

1. オーバーライドを設定するコンピュータやポリシーの**コンピュータエディタまたはポリシーエディタ**[1]を開きます。
2. [設定]→[一般]に移動します。
3. [非アクティブなAgentのクリーンナップのオーバーライド]で、[はい]を選択します。
4. [保存]をクリックします。

非アクティブなAgentのクリーンナップジョブによって削除されたコンピュータの監査証跡の確認

非アクティブなAgentのクリーンナップジョブの実行時には、削除されたコンピュータの追跡に利用できるシステムイベントが生成されます。

次のシステムイベントを確認する必要があります。

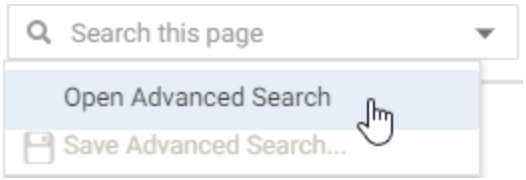
- "2953 - 非アクティブなAgentのクリーンナップが正常に完了しました" on the next page
- "251 - コンピュータの削除" on the next page
- "716 - 不明なAgentの再有効化の試行" on page 1524 ([不明なAgentの再有効化]が有効になっている場合)

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。コンピュータの設定を変更するには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

システムイベントを検索する

非アクティブなAgentのクリーンナップジョブによって生成されたシステムイベントを表示するには、次のように、それらのイベントを表示するためのフィルタ条件を追加した検索を作成する必要があります。

1. [イベントとレポート] ページに移動します。
2. 右上にある検索フィールドのリストをクリックし、[詳細検索を開く] を選択します。



3. [期間] のリストから[カスタム範囲] を選択します。
4. [開始] に、非アクティブなAgentのクリーンナップジョブが最初に実行された時刻の直前にあたる日時を入力します。[終了] に、クリーンナップジョブが完了した時刻の直後にあたる日時を入力します。
5. [検索] で、[イベントID] と[次のリストに含まれる] を選択し、「2953, 251」と入力します。必要に応じて、「716」やコンピュータの再有効化に関連するイベントID (130, 790, 350, 250) を入力することもできます。

これにより、非アクティブなAgentのクリーンナップジョブによって生成されたすべてのシステムイベントが表示されます。時間、イベントID、またはイベント名の列をクリックすると、表示されているイベントをソートできます。その後、イベントをダブルクリックすると、以下で説明するイベントの詳細情報が表示されます。

システムイベントの詳細

2953 - 非アクティブなAgentのクリーンナップが正常に完了しました

このイベントは、非アクティブなAgentのクリーンナップジョブが実行され、コンピュータが正常に削除された場合に生成されます。このイベントの説明には、削除されたコンピュータの数が表示されます。

> 注意: すべてのコンピュータを削除するために複数回の確認が必要な場合は、確認が行われるたびにシステムイベントが生成されます。

251 - コンピュータの削除

「非アクティブなAgentのクリーンナップが正常に完了しました」イベントに加え、コンピュータが1台削除されるたびに「コンピュータの削除」イベントが生成されます。

716 - 不明なAgentの再有効化の試行

未知のエージェントを再アクティベートするが有効な場合、Deep Security Managerに再接続しようとしたときに削除された、アクティベートされたコンピュータに対してこのイベントが生成されます。再有効化されたコンピュータごとに、次のシステムイベントも生成されます。

- 130 - 資格情報の生成
- 790 - Agentからのリモート有効化の要求
- 350 - ポリシーの作成 (ポリシーを割り当てるイベントベースタスクが有効になっている場合)
- 250 - コンピュータの作成
  または
  252 - コンピュータのアップデート

Agentの設定

Deep Security Agentに関連する設定は、の[管理]→[システム設定]→[エージェント] にあります。次のものが含まれます。

ヒント: Deep Security APIを使用してエージェント関連のシステム設定変更を自動化できます。例については、ポリシー、コンピュータ、システム設定の構成を参照してください。

ホスト名

コンピュータをIPで登録していてIPの変更が検出された場合、コンピュータの [ホスト名] を自動的に更新: IPの変更が検出された場合に、コンピュータの [ホスト名] フィールドに表示されるIPアドレスをアップデートします。

注意: Deep Security Managerは、IPアドレスまたはホスト名ではなく、一意のフィンガープリントを使用して保護されたコンピュータを識別します。

エージェント起動アクティベーション(AIA)

Deep Security Managerで新しいエージェントを有効にするには、クラウドコネクタを使用するか、Computersで手動で新しいコンピュータを追加します。また、エージェントが自動的にアクティベートするように設定することもできます。"Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511を使用してエージェントをアクティベートおよび保護します。

許可されたエージェント起動アクティベーション: エージェントが自身にアクティベーションを行うためにマネージャに接続できるようにします。次に、エージェント起動によるアクティベーションを実行できるコンピュータを選択します。

- For Any Computers: すでに Computers に登録されているコンピュータであるかどうか。

  警告: 許可されていないエージェントのアクティベーションを防止するには、インターネットなどの信頼されないネットワークからのDeep Security Managerへの接続がネットワークで許可されている場合は、このオプションを有効にしないでください。同様にDeep Security Agentを不正な管理者から保護するために、では、認証されたマネージャのみでエージェントのアクティベーションを許可します。

- 既存のコンピュータの場合: すでに コンピュータのに登録されているコンピュータのみ。
- 次のIPリストにあるコンピュータの場合: IPアドレスが指定されたIPリストに一致するコンピュータのみ。

また、開始動作を設定します。

- 割り当てるポリシーポリシーがアクティベーションスクリプトによって割り当てられていない場合)): アクティベーション時にコンピュータに割り当てるセキュリティポリシー。この設定は、エージェントのアクティベーションスクリプトまたはAIAイベントベースのタスクでポリシーが指定されていない場合にのみ適用されます。
- エージェントは、ホスト名を指定することができます。エージェントは、起動時にDeep Security Managerにそれを提供することで、そのホスト名を指定することができます。

- 同じ名前のコンピュータがすでに存在する場合: 新しいコンピュータが既存のコンピュータと同じクライアントGUIDまたは証明書を使用しようとした場合に、アクティベーション試行を処理する方法:

  - アクティベーションを許可しない: コンピュータをアクティベートしない。
  - 新しいコンピュータを同じ名前で有効にする: 新しい名前を使用して新しいコンピュータオブジェクトを作成し、コンピュータを有効にします。
  - 既存のコンピュータを再度有効にする: 同じ名前を使用して既存のコンピュータオブジェクトを再利用し、コンピュータを有効にします。

  この設定は、物理コンピュータ、Azure仮想マシン(VM), Google Cloud Platform (GCP) VM、またはVMware VM) にのみ適用されます。(AWSには、すべてのAWSインスタンスを区別するため

にDeep Security Managerが使用する一意のインスタンスIDが用意されているため、これらのコンピュータではこの設定は無視されます。)

- クローン化されたクライアントを再有効化する: 新しいコンピュータとしてクローンを再有効化します。[Policy]で選択したポリシーを[に割り当てるポリシーに割り当てる]チェックボックスをオンにします。これは、すでに有効化されているDeep Security Agentがインストールされた「ゴールドイメージ」を使用して、コンピュータのハードディスクを再イメージングする場合、または新しいVMインスタンスまたはAMIを配信する場合に便利です。これにより、同じソフトウェアイメージをコピーすることによって配置されているにもかかわらず、各コンピュータに一意のエージェントGUIDが確保されます。

  クローンは、最初のアクティベーションの後、最初のハートビート中に検出されます。別のコンピュータで同じエージェントGUIDが使用されている場合、マネージャはクローンを検出してそれらのコンピュータを再度有効化します。

  注意: このオプションを無効にすると、では が自動的に再有効化されません。マネージャを使用して手動でアクティベートするか、アクティベーションスクリプトを使用する必要があります。

  この設定は、AWSインスタンス、Azure仮想マシン(VM), Google Cloud Platform (GCP) VM、または Computersを使用して追加したVMware VM / Add Account)にのみ適用されます。

- 不明なエージェントを再有効化する:削除された(以前にアクティベートされていた)削除されたコンピュータを新しいコンピュータとして再有効化します(再接続した場合)。元のコンピュータの割り当てられたポリシーまたはルールは、初期設定ではコンピュータに再度割り当てられません。手動で再度割り当てたり、次のようなツールを使用する必要があります。イベントベースのタスク自動的に割り当てます。この設定は、非アクティブなエージェントクリーンナップと同時に使用すると便利です。削除された任意のコンピュータが自動的に再アクティベートされることがあります。も参照してください"非アクティブなAgentのクリーンナップによるオフラインコンピュータの削除の自動化" on page 1520。

  以前に知られていたエージェントは、最初のアクティベーション後、次のハートビート中に検出されます。ハートビートにエージェントGUID(アクティベーション前のアクティベーションを示している)があり、そのコンピュータが現在 Computersにリストされていない場合、マネージャはコンピュータを再アクティベーションします。

  注意: 以前のイベントメッセージは引き続き古いコンピュータオブジェクトにリンクされますが、新しいメッセージオブジェクトにリンクされることはありません。

- エージェントのアクティベーショントークン: 任意。エージェントのアクティベーションシークレット指定する場合、エージェントはアクティベーション時に同じ値を指定する必要があります。

  注意: Deep Security Managerがマルチテナントの場合、この設定はプライマリテナントにのみ適用されます。

  これを設定するには、エージェント起動スクリプトの token パラメータを次のように使用します。

  ```
  /opt/ds_agent/dsa_control -a dsm://172.16.0.5:4120/ "token:secret"
  ```

Agentのアップグレード

アクティベーション時にクライアントを自動的にアップグレードする: アクティベーション時に、Deep Security Agentを、Deep Security Managerと互換性のある最新のソフトウェアバージョンにアップグレードします。Linuxコンピュータのみ。"Agentを有効化するときに自動的にアップグレードする" on page 1513。

非アクティブなAgentのクリーンナップ

あなたは(多くのオフラインコンピュータを持っている場合であること、のDeep Security Managerの), と通信していないコンピュータが自動的に非アクティブなエージェントのクリーンアップを使用してコンピュータからそれらを削除することができます。この設定は、現在未知のエージェントを再アクティベートする場合に便利です。"非アクティブなAgentのクリーンナップによるオフラインコンピュータの削除の自動化" on page 1520も参照してください。

非アクティブなエージェントを削除: コンピュータを非アクティブにして削除するまでの時間。

データプライバシー

ネットワークイベントでパケットデータの取り込みを許可する: この設定では、エージェントがDeep Security Managerにパケットデータをキャプチャし、侵入防御およびファイアウォールのイベントを検出します。この設定のオプションは次のとおりです。

- はい(暗号化されたトラフィックを除く):初期設定のオプションです。すべての暗号化されていないパケットデータがDeep Security Managerに送信されます。
- はい (すべてのトラフィック):すべてのパケットデータがDeep Security Managerに送信され、暗号化されたパケットデータが含まれます。暗号化された接続でパケットデータを取得するためのリソース要件は、暗号化されていない接続よりも高くなります。このオプションを選択してワークロー

ドのパフォーマンスに問題が発生した場合は、暗号化されたトラフィックを除外するオプションに切り替えることを検討してください。

- いいえ: パケットデータはエージェントからDeep Security Managerにキャプチャまたは送信されません。規制された環境にいる顧客や、ネットワークコンテンツのDeep Security Managerへの送信を懸念する顧客は、この設定を無効にすることができます。Deep Security Managerに送信されるデータの詳細については、Deep Security 20.0 データ収集通知を参照してください。

注意: この機能は、Deep Security Agent 12.5.0.1001以降でサポートされています。

Agentレスによるvcloud保護

は、vCloudの仮想マシンのアプライアンスの保護を許可：は、VMwareのvCloudの仮想マシンを代わりに(またはそれに加えて) のDeep Securityエージェントの Deep Security仮想アプライアンスによって保護することを可能にします。Deep Security Managerがマルチテナントの場合、テナントはそれらのVMのセキュリティポリシーを設定します。

ユーザーモードソリューション

ユーザーモードは、不正プログラム対策のイベント生成と基本機能をドライバ要件なしで提供します。このソリューションは、カーネルモードで実行するために必要なドライバサポートがないシステムに対して、ある程度の保護を提供し、任意の時点で利用可能な最良の保護を自動的に有効にするオプションを提供します。

基本機能の詳細については、不正プログラム対策エンジンには基本機能のみがありますをご覧ください。

利用可能なモード

以下のモードを使用できます

- カーネルモードはイベントを生成し、完全な不正プログラム対策機能を提供しますが、必要なドライバーサポートがあるシステムでのみ有効にできます。
- ユーザーモードはイベントを生成し、不正プログラム対策の基本機能をドライバなしで有効にします。このモードは、システムがカーネルモードで動作するために必要なドライバをサポートしている場合でも、ドライバを使用せずにシステムで実行するために有効にすることができます。
- オートモードは、カーネルモードとユーザーモードを切り替えて、任意の時点で利用可能な最良の保護を提供します。カーネルモードが優先されますが、カーネルモードの動作を妨げるドライ

バーサポートのギャップがある場合、Deep Security Agentは自動的にユーザーモードに切り替わります。後にカーネルモードで動作するために必要なドライバーを取得したシステム(例えば、システム更新から)は、エージェントが自動的にカーネルモードを使用するように切り替え、不正プログラム対策からシステムを完全に保護します。

システム保護のためのドライバーの使用

システム保護にドライバーを使用する場合、ドライバーモードを次のように設定できます:

1. コンピューター(またはポリシー) > システム > 一般 > システム保護のためにドライバーを使用するかどうかを選択
2. メニューから自動、カーネルモード、またはユーザモードを選択してください。
3. [保存] をクリックします。

サポートされているエージェント

オペレーティングシステム	ユーザーモードでの機能サポート
	不正プログラム対策
AlmaLinux 9 (64-bit)	✓
Amazon Linux (64ビット)	
Amazon Linux 2 (64ビット)	✓
Amazon Linux 2 (AWS ArmベースGraviton 2)	
Amazon Linux 2 (AWS ArmベースGraviton 3)	
Amazon Linux 2023 (64ビット)	✓
Debian 8 (64ビット)	
Debian 9 (64ビット)	
Debian 10 (64-bit)	✓
Debian 11 (64-bit)	✓
Debian 12 (64ビット)	✓

オペレーティングシステム	ユーザーモードでの機能サポート
	不正プログラム対策
Oracle Linux 6 (32ビット)	
Oracle Linux 6 (64ビット)	
Oracle Linux 7 (64ビット)	
Oracle Linux 8 (64ビット)	✓
Oracle Linux 9 (64ビット)	✓
Red Hat Enterprise Linux 6 (32ビット)	
Red Hat Enterprise Linux 6 (64ビット)	
Red Hat Enterprise Linux 7 (64ビット)	
Red Hat Enterprise Linux 8 (64ビット)	
Red Hat Enterprise Linux 8(AWS ARMベースのGraviton 2)	
Red Hat Enterprise Linux 8.6 (PowerPC little-endian)	
Red Hat Enterprise Linux 9 (64ビット)	✓
Red Hat Enterprise Linux Workstation 7 (64-bit)	
SUSE Linux Enterprise Server 12 (64ビット)	
SUSE Linux Enterprise Server 12 (PowerPCリトルエンディアン)	
SUSE Linux Enterprise Server 15 (64ビット)	✓
SUSE Linux Enterprise Server 15 (PowerPCリトルエンディアン)	
Ubuntu 16.04 (64ビット)	
Ubuntu 18.04 (64ビット)	
Ubuntu 18.04 (AWS ARMベースのGraviton 2)	

オペレーティングシステム	ユーザーモードでの機能サポート
	不正プログラム対策
Ubuntu 20.04 (64ビット)	✓
Ubuntu 20.04 (AWS ARMベースのGraviton 2)	
Ubuntu 22.04 (64ビット)	✓
Ubuntu 22.04 (AWS ARMベースのGraviton 2)	

Deep Security Notifier

Deep Security Notifierは、Deep Security AgentおよびDeep Security Relayの状態をクライアントコンピュータに通知するWindowsタスクバーアプリケーションです。Deep Security Agentが不正プログラムをブロックしたり、不正なWebページへのアクセスを防止したりすると、Notifierはタスクバーの通知領域にポップアップユーザ通知を表示します。

Notifierがクライアントマシン上で占有するスペースは小さく、必要なディスク容量は約1MB、メモリの使用容量は約3MBとなります。Notifierの実行中は、タスクバーにNotifierアイコン( ) が表示されます。初期設定では、NotifierはDeep Security Agentと一緒にWindowsコンピュータに自動的にインストールされます。アップグレード用の最新バージョンをインポートするには、[管理]→[アップデート]→[ソフトウェア]→[ローカル] 画面を使用します。

Relay有効化済みAgentを実行しているコンピュータでは、ローカルコンピュータで有効なコンポーネントではなく、AgentまたはApplianceに配布されているコンポーネントがNotifierに表示されます。

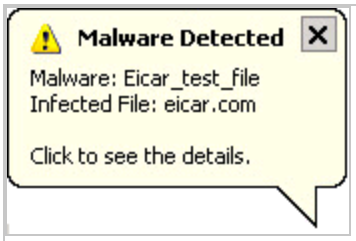
スタンドアロンバージョンのNotifierをダウンロードし、Deep Security Virtual Applianceで保護されている仮想マシンにインストールできます。"Deep Security Notifierを配信する" on page 654を参照してください。

注意: Deep Security Notifierに情報が表示されるためには、Virtual Applianceで保護されている仮想マシンに不正プログラム対策モジュールのライセンスがあり、モジュールが有効になっている必要があります。

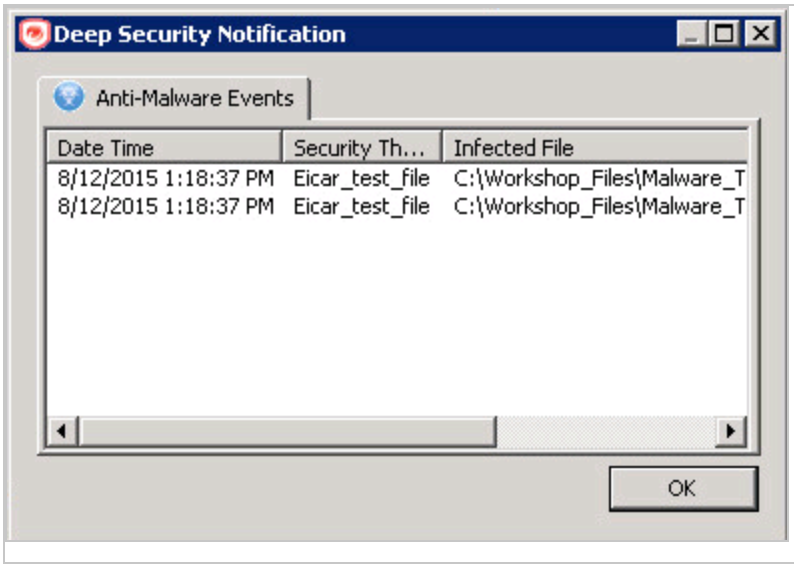
Notifierの仕組み

不正プログラムが検出されるか、不正サイトがブロックされると、Deep Security AgentからNotifierにメッセージが送信され、タスクバーの通知領域にポップアップメッセージが表示されます。

不正プログラムが検出されると、通知領域に次のようなポップアップメッセージが表示されます。



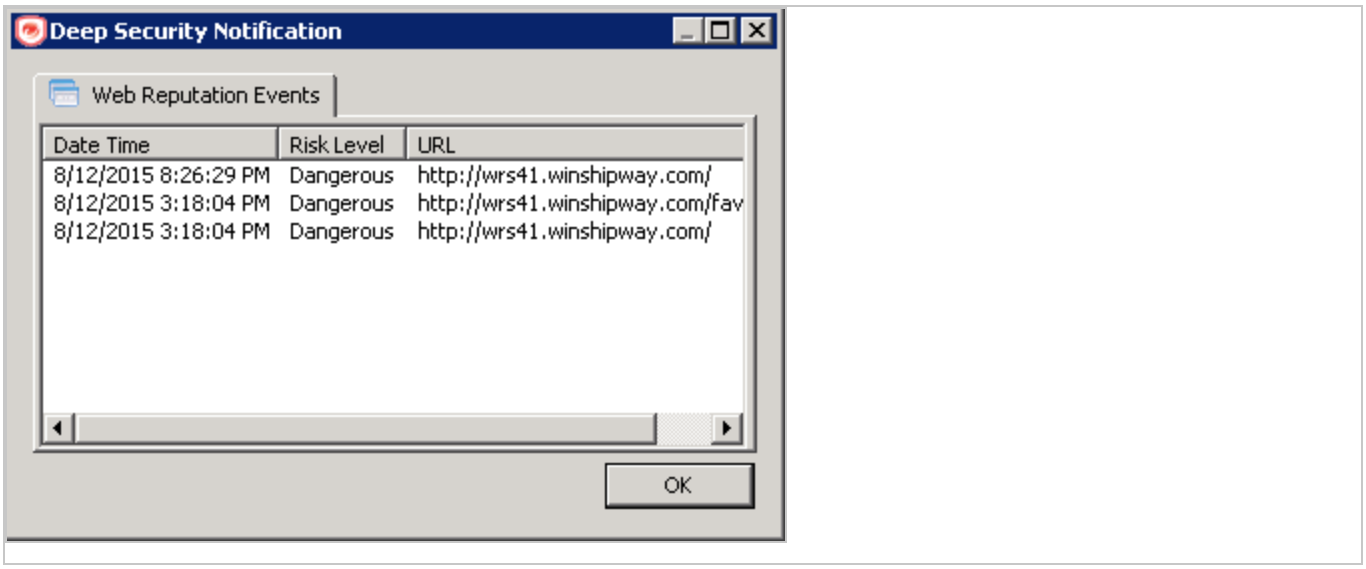
ユーザがメッセージをクリックすると、不正プログラム対策イベントの詳細を示す画面が表示されます。



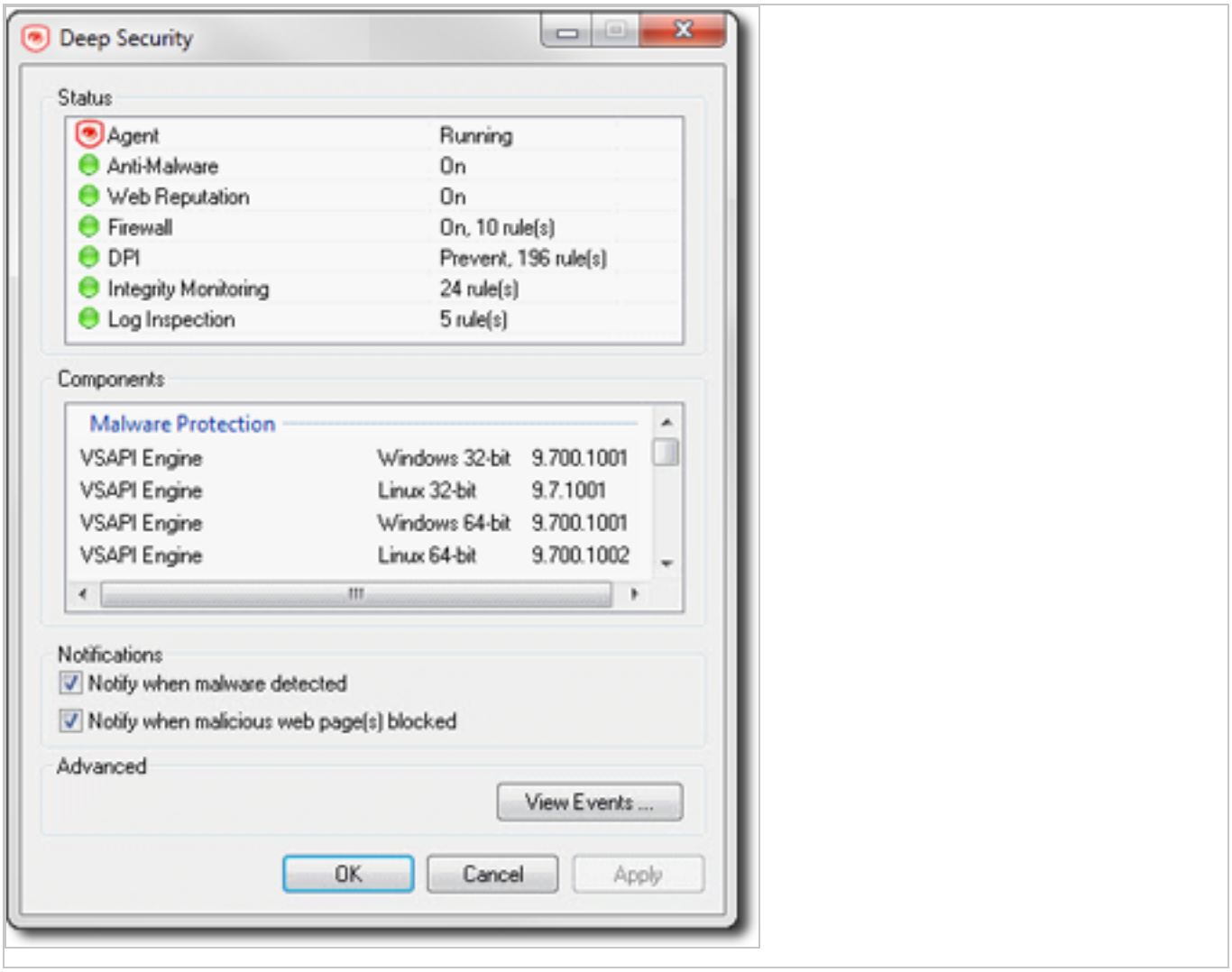
不正なWebページがブロックされると、通知領域に次のようなポップアップメッセージが表示されます。



ユーザがメッセージをクリックすると、Webレピュテーションイベントの詳細を示す画面が表示されます。

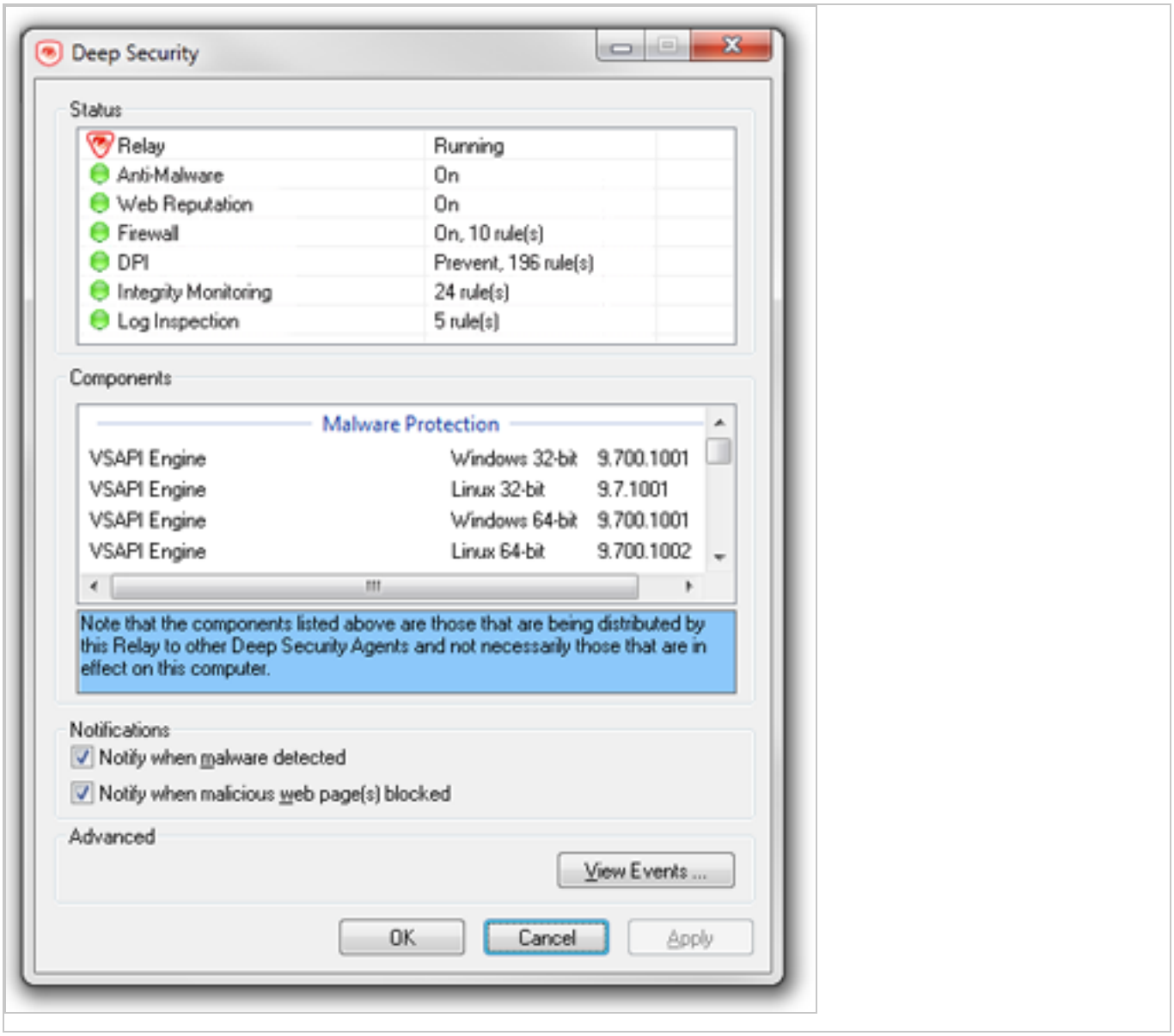


Notifierには、パターンのバージョンなど、現在の保護ステータスやコンポーネント情報を表示するためのコンソールユーティリティもあります。このコンソールユーティリティを使用して、ポップアップ通知のオンとオフを切り替えたり、詳細なイベント情報にアクセスしたりできます。

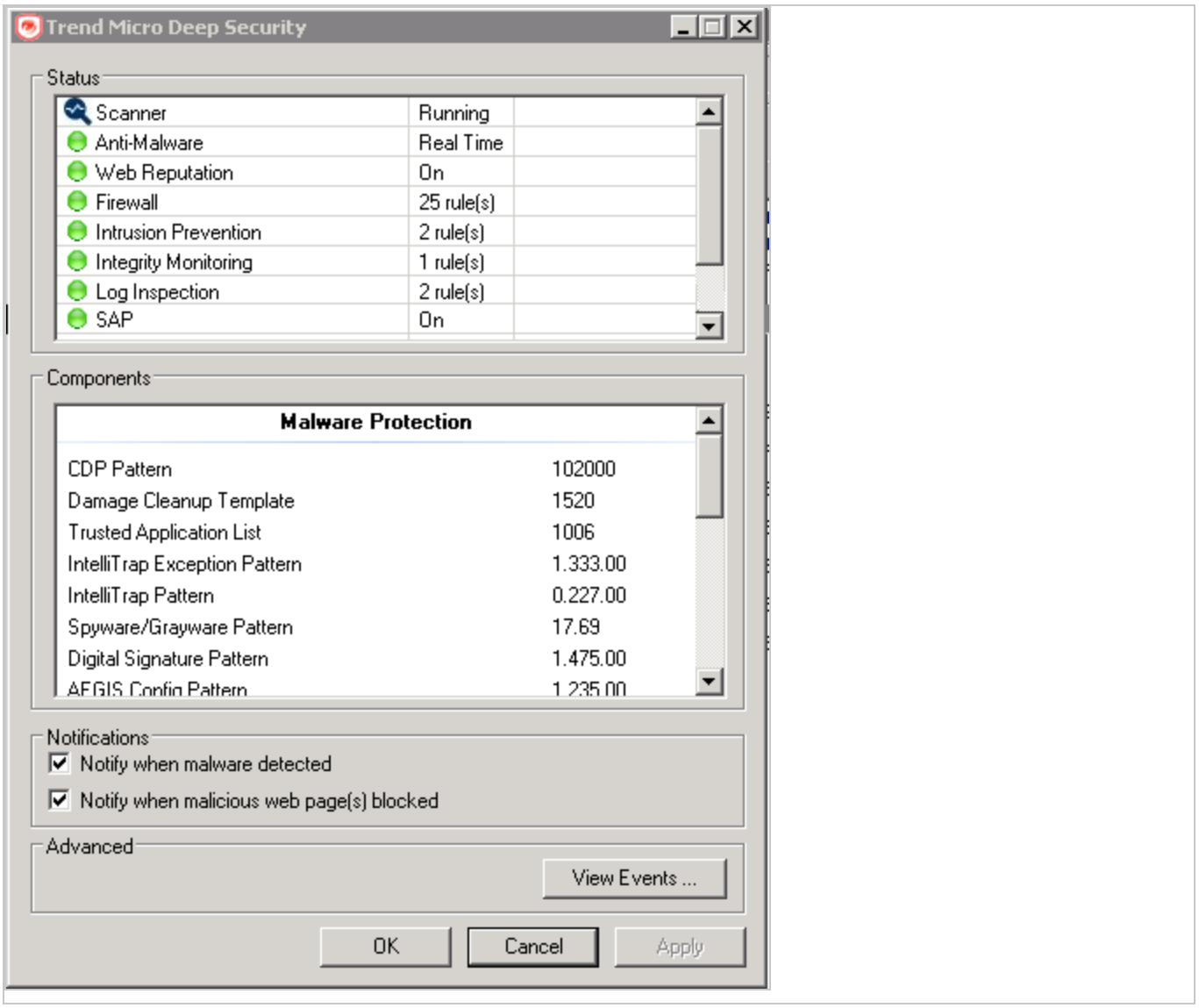


特定のコンピュータまたは特定のポリシーが割り当てられているコンピュータのポップアップ通知をオフにすることもできます(Deep Security Manager の[コンピュータ/ポリシーエディタ]→[設定]→[一般]と設定ホストのすべてのポップアップ通知を抑制 上のすべてのポップアップ通知を抑制する) 。はい。メッセージは引き続きDeep Security Managerでアラートまたはイベントとして表示されます。

NotifierがRelay有効化済みAgentをホストするコンピュータで実行されている場合、Notifierには、コンピュータ上で有効になっているコンポーネントではなく、Relayによって配布されているコンポーネントが表示されます。



Deep Security Scannerをホストしているコンピュータで Notifierが実行されている場合、Notifierはスキャナ機能が有効で、コンピュータをリレーできないことを示します。



Windows OSで手動検索を開始する

AgentがNotifierアプリケーションで手動検索を開始できるようになっている場合は、Notifierコンソールに[検索]というタイトルのパネルが表示されます。Notifierは、コンピュータエディタまたはポリシーエディタ、エディタの[不正プログラム対策]タブ、[一般]水平タブの[手動検索]セクションで割り当てられた検索設定を使用します。詳細については、「不正プログラム検索設定を作成または編集する」を参照してください。

次の場合は検索を開始できません:

- Agentがアップグレード中の場合。
- 実行中のサーバ側検索がすでに実行されている場合。

- 検索設定が空の場合。

Windows OSでAgentによる手動検索を開始するには、

1. [検索] パネルで [検索] をクリックします。
2. 検索するフォルダを選択し、[検索] をクリックします。
    - フル検索の場合は、[このPC] を選択してすべてのファイルの検索を開始します。
    - カスタム検索の場合は、検索を開始するファイルまたはフォルダを1つ以上選択します。

検索が完了すると、[検索結果] に検出された不正プログラムアイテムの数が表示されます。これらの項目の詳細を表示するには、Notifierの [詳細] パネルで [イベントの表示] をクリックします。

実行中の検索は、使用できないコンピュータでトリガーされた場合には停止されます。たとえば、検索の開始後にユーザがコンピュータからログアウトした場合などです。

ユーザを管理する

ユーザの追加と管理

Deep Securityには、の[管理]→[ユーザ管理]で作成および管理できるユーザ、役割、および連絡先があります。

- ユーザは、一意のユーザー名とパスワードでのDeep Security ManagerにサインインすることができますのDeep Securityアカウント所有者です。"Active Directoryとの同期" below または "ユーザを個別に追加または編集する" on the next page
- 役割は、Deep Security Manager内でデータを表示して操作を実行するための権限の集合です。各ユーザには役割が割り当てられます。"ユーザロールの定義" on page 1541を参照してください。
- 連絡先にはユーザアカウントがないため、Deep Security Managerにサインインできませんが、メール通知と予約レポートの受信者として指定できます。"レポートのみを受信できるユーザの追加" on page 1558を参照してください。

Active Directoryとの同期

Active Directoryを使用してユーザを管理する場合、Deep SecurityをActive Directoryと同期してユーザリストを作成できます。ディレクトリに保存されているパスワードを使用してDeep Security Managerにログインできます。

Active DirectoryユーザアカウントをDeep Securityユーザまたは連絡先としてDeep Securityに正常にインポートするには、Active DirectoryユーザアカウントにuserPrincipalName属性値が設定されている必要があります。userPrincipalName属性は、Active Directoryアカウント所有者のユーザログオン名に対応します。

Deep SecurityをFIPSモードで使用している場合は、Directoryと同期する前にActive DirectoryのSSL証明書をインポートする必要があります。"信頼された証明書の管理" on page 1653を参照してください。

1. Deep Security Managerで、[管理]→[ユーザ管理]→[ユーザ]の順に選択します。
2. [ディレクトリと同期] をクリックして [ディレクトリと同期] ダイアログを開きます。
3. ディレクトリサーバのアドレスを入力します。
4. アクセス資格情報を入力します。この資格情報には、少なくともActive Directoryの読み取り権限が必要です。Domain Userグループのメンバには、初期設定で読み取り権限が付与されていることに注意してください。
5. [次へ] をクリックすると、Active Directoryへの接続が試行されます。
6. 次のダイアログで、Active Directoryグループ名またはグループ名の一部を検索フィールドに入力し、Enterキーを押します。[>>] ボタンを使用して、グループを [同期するグループ] ペインに移動します。

インポートされたユーザリストは、初期設定ではDeep Security Managerからロックアウトされます。プロパティを変更して、Deep Security Managerにログインできるようにする必要があります。

Active Directoryとの同期の結果として追加されたDeep Security Managerからユーザを削除し、ディレクトリと再同期した場合、Active Directoryに残っているユーザはユーザリストに再表示されます。

ユーザを個別に追加または編集する

1. Deep Security Managerで、[管理]→[ユーザ管理]→[ユーザ]の順に選択します。
2. [新規] をクリックして新しいユーザを追加するか、既存のユーザアカウントをダブルクリックして設定を編集します。
3. 次を含む、ユーザの一般的なプロパティを指定します。
   - ユーザ名: Deep Security Managerのログイン画面でユーザが入力するユーザ名。
   - パスワードとパスワードの確認入力: ダイアログボックスに表示されるパスワード要件に注意してください。パスワード要件はユーザのセキュリティ設定で設定できます ("ユーザパスワードルールの適用" on page 1647を参照してください)。
   - 名前: (オプション) アカウント所有者の名前。
   - 説明: (オプション) アカウントの説明。

- 役割: リストを使用して、定義済みの役割をこのユーザに割り当てます。また、ユーザを右クリックして [役割の割り当て] をクリックすると、ユーザリストから役割をユーザに割り当てることもできます。

  Deep Security Managerには、フルアクセスと監査者の2つの役割が事前に設定されています。[フルアクセス] の役割では、コンピュータ、コンピュータグループ、ポリシー、ルールなどの作成、編集、削除など、Deep Securityシステムを管理するためのすべての権限がユーザに付与されます。監査者ロールを使用すると、ユーザはDeep Securityシステム内のすべての情報を表示できますが、個人設定 (パスワード、連絡先情報、表示設定など) 以外は変更できません。さまざまなレベルのシステムアクセス権を持つ役割を作成および変更するには、[役割] 画面を使用するか、[役割]リストで [新規] を選択します。

- 言語: ユーザのログイン時にインタフェースに使用される言語。
- タイムゾーン: ユーザのタイムゾーン。このタイムゾーンは、Deep Security Managerで日時を表示する場合に使用します。
- 時間形式 : Deep Security Managerの時間を表示するために使用される時間形式。12時間形式または24時間形式を使用できます。
- パスワードを無期限にする:このオプションを選択すると、ユーザのパスワードは無期限になります。そうしないと、ユーザのセキュリティ設定で指定されたとおりに期限切れになります ("ユーザパスワードルールの適用" on page 1647を参照)。

4. 多要素認証 (MFA) を有効にするには、[多要素認証の有効化] をクリックします。ユーザに対してMFAがすでに有効になっている場合は、[多要素認証の無効化] をクリックすると無効にできます。詳細については、"多要素認証の設定" on page 1649を参照してください。
5. [連絡先情報] タブをクリックし、ユーザの連絡先情報を入力し、そのユーザが主担当者であるかどうかを指定できます。[アラートメールを受信] チェックボックスをオンにして、アラートがトリガされたときにメール通知を受信するユーザのリストにこのユーザを追加することもできます。
6. また、[設定] タブで設定を編集することもできます。ただし、これらの値の一部を増やすと、Deep Security Managerのパフォーマンスに影響します。変更を加えて、その結果に満足できない場合は、[初期設定に戻す] (タブの下部) をクリックして、この画面のすべての設定を初期設定値に戻すことができます。

   モジュール

   - ライセンス許可されていないモジュールを非表示: この設定では、このユーザに対してライセンス許可されていないモジュールをグレー表示ではなく非表示にするかどうかを決定します。このオプションは、[管理]→[システム設定]→[詳細] タブでグローバルに設定できます。

   更新頻度

- ステータスバー: この設定は、コンピュータの検出や検索などのさまざまな処理中にDeep Security Managerのステータスバーが更新される頻度を決定します。
- アラートリスト/概要:リストビューまたは概要ビューの [アラート] ページのデータを最新表示する頻度。
- コンピュータリスト: [コンピュータ]ページのデータを更新する頻度。

  [最終更新] 列の値は、ページを手動で再ロードしない限り再計算されません。

- コンピュータの詳細: 必要に応じて、個々のコンピュータのプロパティページを最新の情報で更新する頻度。

リストビュー

- [各ページの前回のタグフィルタを記憶する]: [イベント] ページでは、表示されるイベントをタグでフィルタできます。[リストビュー] の設定では、[イベント]画面から移動したり戻ったりしたときに、タグフィルタ設定を保持するかどうかを指定します。
- [各ページの前回の記憶フィルタ:][イベント] ページでは、表示されるイベントを期間およびコンピュータ別にフィルタできます。[リストビュー] の設定によって、[イベント] 画面から移動したり戻ったりしたときに、[期間] および [コンピュータ] フィルタの設定を保持するかどうかが決まります。
- [各ページに前回のコンピュータを記憶] フィルタ:]イベント] ページでは、表示されるイベントを期間およびコンピュータ別にフィルタできます。[リストビュー] の設定によって、[イベント] 画面から移動したり戻ったりしたときに、[期間] および [コンピュータ] フィルタの設定を保持するかどうかが決まります。
- [各ページで前回の詳細検索を記憶する]: [イベント] ページで詳細検索を実行したことがある場合に、別のページに移動してからそのページに戻ったときに検索結果を保持するかどうかをこの設定で指定します。
- 1ページに表示するアイテム数:アイテムのリストを表示する画面では、1ページに特定の数のアイテムが表示されます。次のページを表示するには、ページネーションコントロールを使用する必要があります。この設定を使用して、1ページに表示されるリスト項目の数を変更します。
- データベースから取得するアイテムの最大数:この設定では、データベースから取得して表示できるアイテムの数を制限します。これにより、Deep Security Managerでデータベースクエリの結果を大量に表示しようとして処理が停止することがなくなります。クエリでこの数を超える結果が生成されると、結果の一部のみが表示されていることを通知するメッセージが画面の上部に表示されます。

注意: これらの値を大きくすると、Deep Security Managerのパフォーマンスに影響します。

レポート

- PDF暗号化を有効にする:このオプションを選択すると、PDF形式でエクスポートされたレポートは、[レポートパスワード] を使用してパスワードで保護されます。

ユーザのパスワードを変更する

ユーザのパスワードを変更するには、[管理]→[ユーザ管理]→[ユーザ] の順に選択してユーザを右クリックし、[パスワード設定] をクリックします。現在のパスワードと新しいパスワードを入力するように求められます。

ユーザをロックアウトする/ロックアウトをリセットする

ログオン時にユーザが間違ったパスワードを何回も入力すると、自動的にロックされます。この状況を解決して、ユーザがログインできるようにするには、"ロックアウトされたユーザ名のロック解除" on page 1560を参照してください。

ユーザに関連付けられたシステムイベントを表示する

ユーザに関連付けられたシステムイベントを表示するには、[管理]→[ユーザ管理]→[ユーザ] の順に選択してユーザを右クリックし、[システムイベントの表示] をクリックします。

ユーザを削除する

Deep Security Managerからユーザアカウントを削除するには、をクリックします。[管理]→[ユーザ管理]→[ユーザ] 、ユーザーをクリックし、[OK]をクリックします。削除。

Active Directoryとの同期の結果として追加されたDeep Security Managerからユーザを削除し、ディレクトリと再同期した場合、Active Directoryに残っているユーザはユーザリストに再表示されます。

ユーザロールの定義

Deep Securityは、役割ベースのアクセス制御(RBAC) を使用して、Deep Securityの一部に対するユーザ権限を制限します。アクセス権限と編集権限は、ユーザにではなく、役割に関連付けられます。Deep Security Managerをインストールしたら、ユーザごとに個別のアカウントを作成し、各ユーザに役割を割り当てて、そのアクティビティをすべてのアクティビティに限定し、その職務の完了に必要なア

クティビティのみを割り当てる必要があります。個々のユーザのアクセス権限と編集権限を変更するには、ユーザに別の役割を割り当てるか、役割自体を編集する必要があります。

役割がコンピュータとポリシーに対して持つアクセス権限は、コンピュータとポリシーのサブセットに限定することもできます。たとえば、ユーザに対して、既存のすべてのコンピュータの表示は許可するが、特定のグループ内のコンピュータ以外の編集を許可しないようにできます。

Deep Securityには2つの事前構成されたロールがあります。

- フルアクセス: フルアクセスの役割により、コンピュータ、コンピュータグループ、ポリシー、ルール、不正プログラムの検索設定などの作成、編集、削除など、Deep Securityシステムの管理に関するすべての権限がユーザに付与されます。
- 監査担当者: 監査担当者の役割により、Deep Securityシステム内のすべての情報を表示できますが、パスワード、連絡先情報、ダッシュボードのレイアウト設定などの個人設定以外の変更はできません。。

付与されたアクセスレベルに応じて、Deep Security Managerのコントロールは表示および変更可能、表示されるが無効、または非表示 (隠されている) になる場合があります。事前設定された役割で付与される権限の一覧、および新しい役割を作成する際のデフォルトの権限設定については、"Full Access、Auditor、および新規の各役割の初期設定" on page 1549を参照してください。

新しい役割を作成して、特定のコンピュータ、セキュリティルールのプロパティ、またはシステム設定など、Deep Securityオブジェクトの編集や表示を制限できます。

ユーザアカウントを作成する前に、ユーザが担う役割を特定し、その役割がアクセスを必要とするDeep Securityオブジェクトとそのアクセスの性質 (閲覧、編集、作成など) を列挙してください。役割を作成した後、ユーザアカウントを作成し、特定の役割を割り当てることができます。

注意: Full Accessの役割を複製して変更する方法で新しい役割を作成しないでください。新しい役割に目的とする権限のみを確実に付与するには、ツールバーの [新規] をクリックして新しい役割を作成します。新しい役割の権限は、初期設定では最も制限された状態で設定されます。後で必要な権限のみを付与できます。Full Accessの役割を複製してから制限を適用すると、不要な権限を与える危険があります。

新規 () または プロパティ() をクリックすると、ロールプロパティダイアログが表示され、6つのタブがあります: 一般、コンピュータ権限、ポリシー権限、ユーザ権限、その他の権限、および割り当て対象。

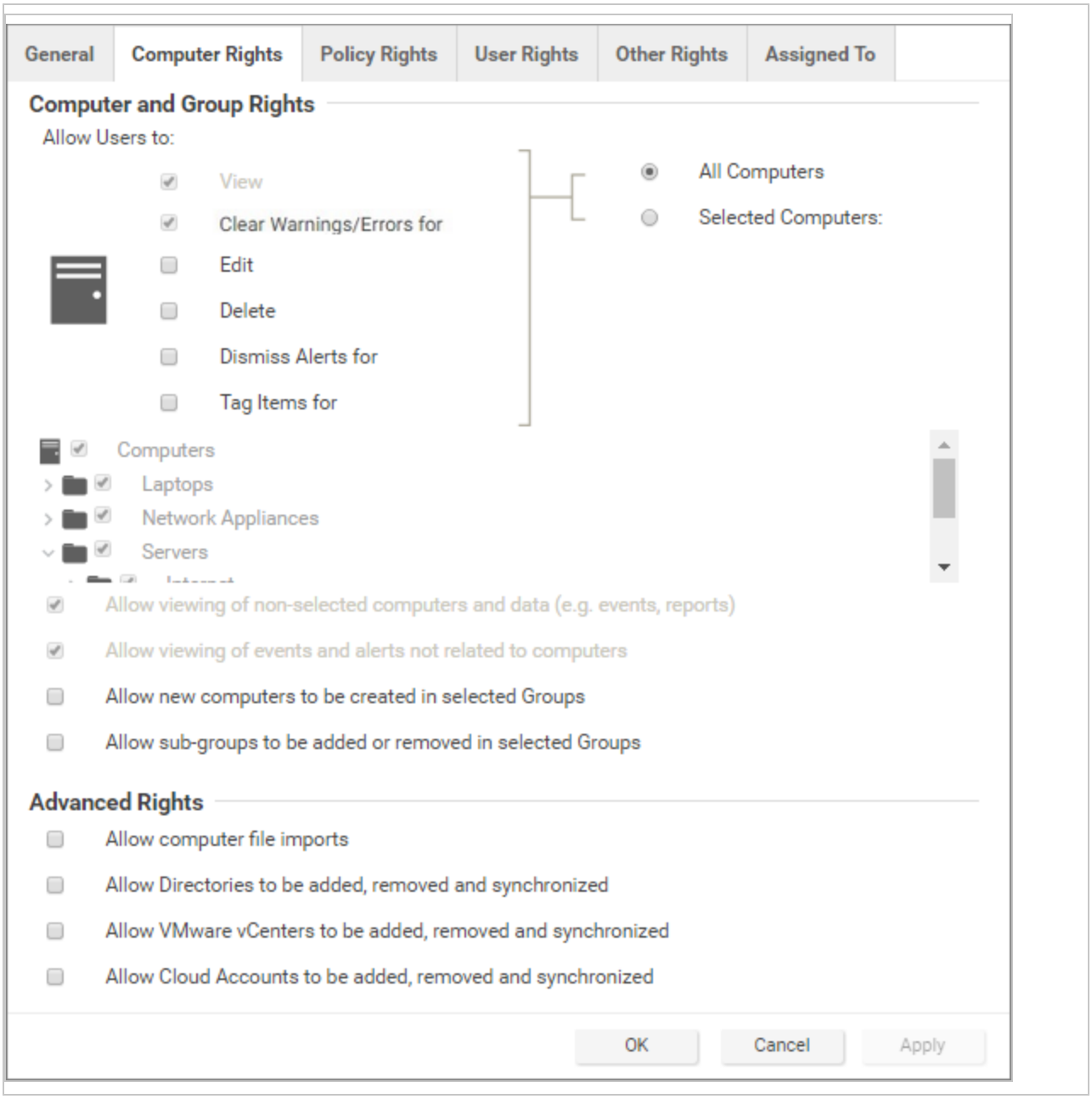
役割を追加または編集する

1. Deep Security Managerで、[管理]>[ユーザ管理]>[ロール] の順に選択します。
2. [新規] をクリックして新しい役割を追加するか、既存の役割をダブルクリックして設定を変更します。
3. 次のような、役割の一般的なプロパティを指定します。
   - 名前: 役割の名前を入力してください。これは役割ページとユーザを追加する際の利用可能な役割のリストに表示されます。
   - 説明: 役割を説明してください (任意)。
   - アクセスの種類: このロールを持つユーザがDeep Security Manager、Deep Security Manager WebサービスAPI (レガシーSOAPおよびREST APIに適用され、管理 > システム設定 > 高度 > SOAP WebサービスAPIで有効にできます) にアクセスするか、またはその両方にアクセスするかを選択します。
   - Trend Vision One Endpoint Securityへの移行: この役割を持つユーザがTrend Vision One Endpoint Securityリンクへのアクセス、移行タスクの処理、またはその両方を行うかどうかを定義します。
   - 認証: このロールを持つユーザが標準またはRADIUSベースの認証方法で認証するかどうかを定義します。後者の場合、ロールに割り当てるRADIUS構成を作成する必要があります。この構成には、名前、通信サーバ名とポート番号、および共有シークレットが定義されている必要があります。

4. [コンピュータの権限] ペインを使用して、役割のユーザに表示、編集、削除、警告とエラーのクリア、アラートの消去、イベントタグ付けの権限を付与します。これらの権限は、すべてのコンピュータおよびコンピュータグループに適用することも、特定のコンピュータに制限することもできます。アクセスを制限するには、ユーザが実行できる処理の種類を選択します。処理を[選択したコンピュータ] にのみ適用する場合は、この役割のユーザがアクセスできるコンピュータグループとコンピュータを選択します。

   これらの権限制限は、Deep Security Managerのコンピュータへのユーザのアクセスに影響するだけでなく、イベントやアラートなど、表示される情報にも影響します。また、メール通知は、ユーザがアクセス権を持っているデータに関連する場合にのみ送信されます。

   警告とエラーをクリアする権限が付与されている場合、その役割は閲覧者ではなく編集者と見なされることに注意してください。



次に示す4つの基本オプションを使用できます。

- 選択されていないコンピュータおよびデータ(イベントやレポートなど)を表示: この役割のユーザの編集、削除、またはアラート消去の権限が制限されている場合でも、このチェックボックスをオンにすることで他のコンピュータに関する情報の表示 (変更は不可) を許可できます。
- コンピュータに関連していないイベントおよびアラートを表示: システムイベント(ユーザがロックされた、新しいファイアウォールルールが作成された、IPリストが削除されたなど)のような、コンピュータ関連以外の情報をこの役割のユーザが表示できるようにするには、このオプション

を設定します。

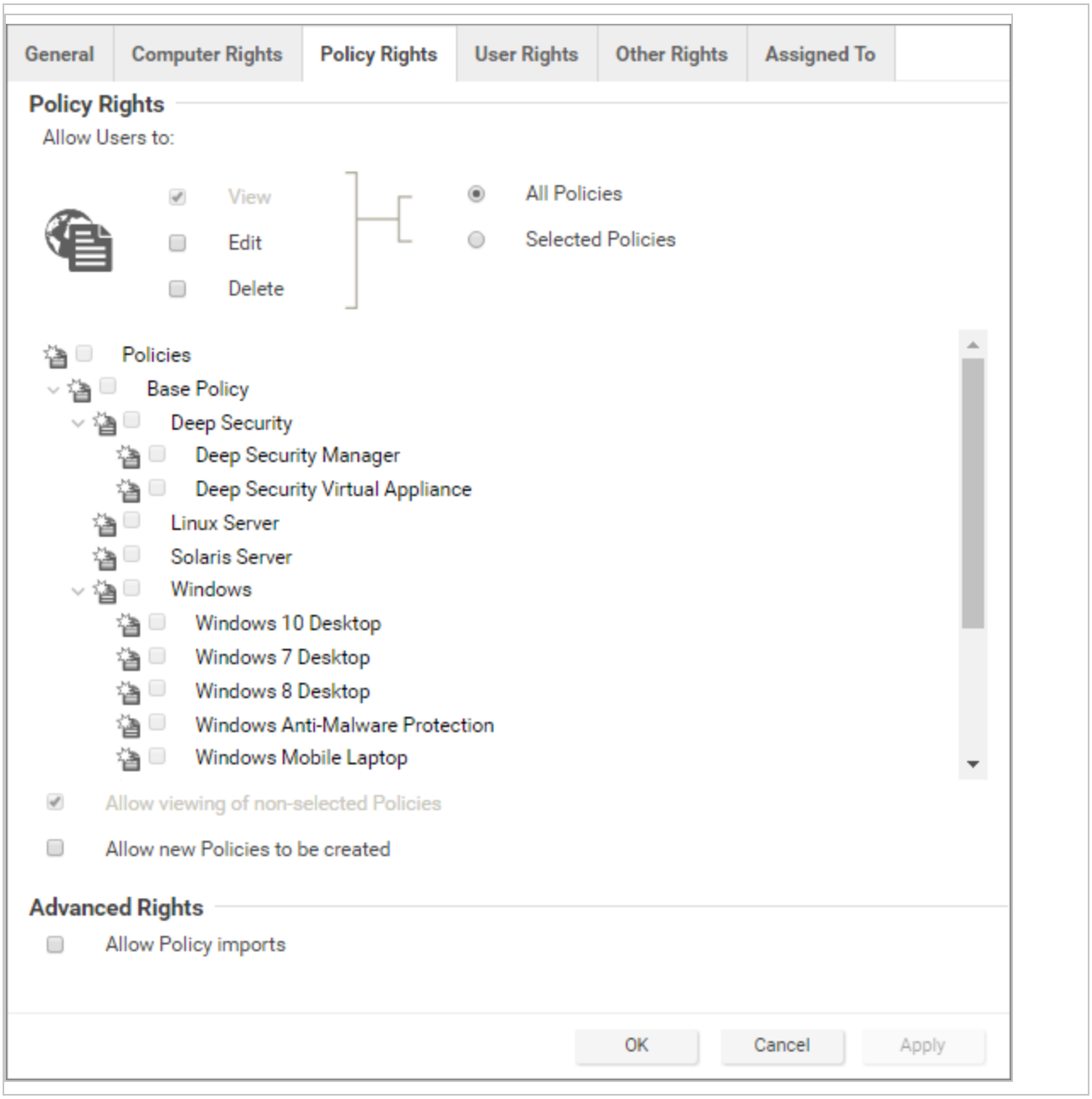
注意: 前述の2つの設定は、ユーザがアクセスできるデータに影響します。この2つの設定は、ユーザがコンピュータに変更を加える機能は制限したまま、アクセス権を持たないコンピュータに関連する情報を表示可能にするかどうかを制御します。それらのコンピュータに関連するメール通知を受信するかどうかも含まれます。

- 選択したグループ内に新しいコンピュータを作成: この役割のユーザが、アクセス可能なコンピュータグループに新しいコンピュータを作成できるようにするには、このオプションを設定します。
- 選択したグループ内にサブグループを追加または削除: このオプションを設定すると、この役割のユーザは、アクセス権のあるコンピュータグループ内でサブグループを作成および削除できます。

[詳細な権限] セクションでこれらを有効にすることもできます。

- コンピュータファイルのインポートを許可する: この役割のユーザは、Deep Security Managerの[Computer Export]オプションを使用して作成されたファイルを使用してコンピュータをインポートできます。
- ディレクトリを追加、削除、および同期: この役割のユーザが、MS Active DirectoryなどのLDAPベースのディレクトリを使用して管理されているコンピュータを追加、削除、および同期できるようにします。
- VMware vCenterを追加、削除、および同期: この役割のユーザが、VMware vCenterを追加、削除、および同期できるようにします。
- クラウドプロバイダの追加、削除、および同期を許可する: この役割のユーザに、クラウドプロバイダの追加、削除、および同期を許可する。

5. ポリシー権限タブを使用して、役割内のユーザに閲覧、編集、および削除の権限を付与します。これらの権限はすべてのポリシーに適用することも、特定のポリシーに制限することもできます。アクセスを制限したい場合は、選択されたポリシーをクリックし、この役割のユーザがアクセスできるポリシーを選択してください。



子ポリシーを持つポリシーに権限を許可すると、ユーザは自動的に子ポリシーへの権限を取得します。

次に示す2つの基本オプションを使用できます。

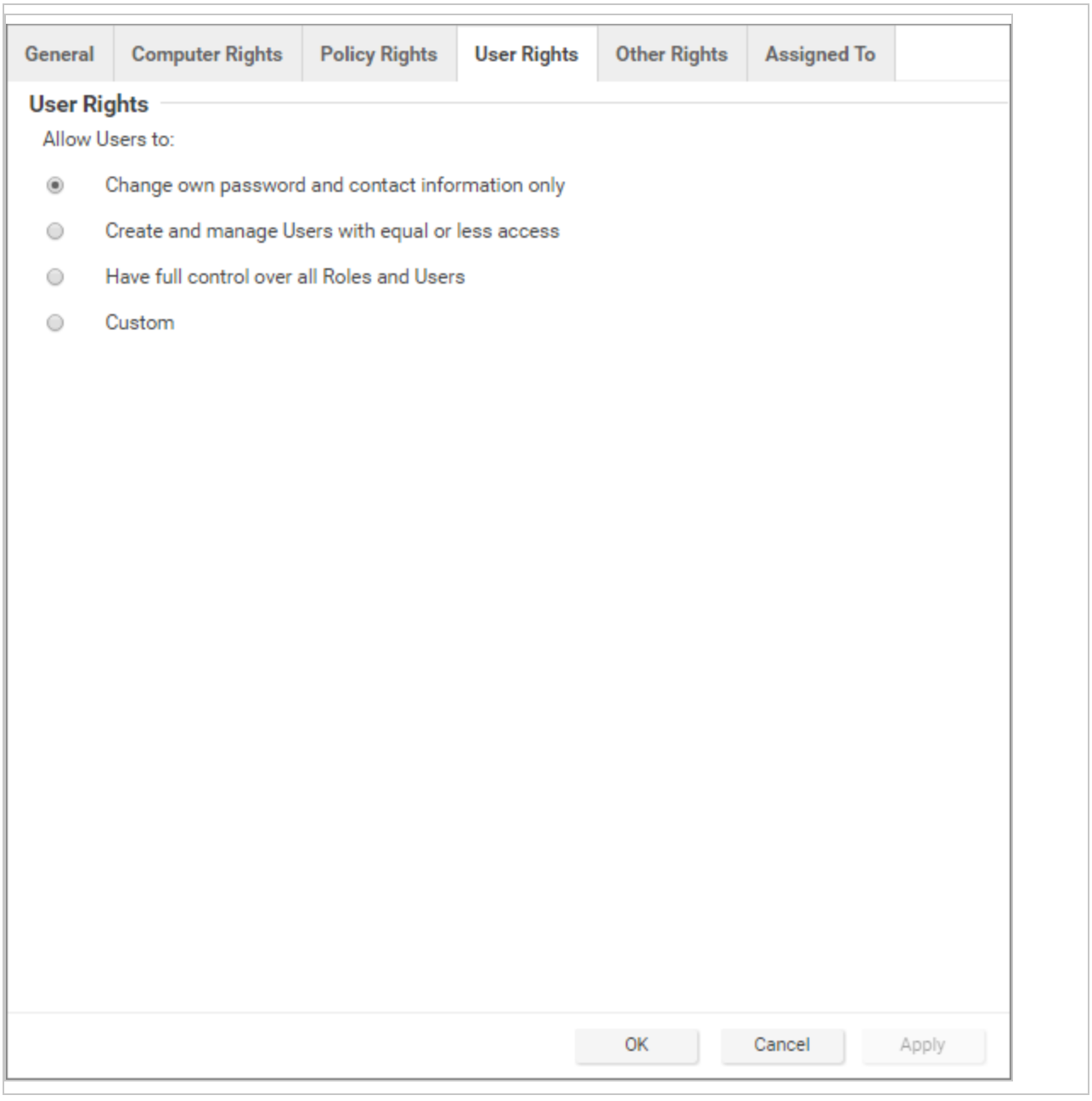
- 選択されていないポリシーの表示を許可: この役割のユーザが編集または削除権限を制限されている場合でも、他のポリシーに関する情報を表示することは許可できますが、変更することはできません。

- 新しいポリシーの作成を許可する: この役割のユーザが新しいポリシーを作成できるようにします。

高度な権限セクションで以下を有効にすることもできます。

- ポリシーのインポートを許可: この役割のユーザに、[Policies]タブのDeep Security Managerの [ポリシー] オプションで作成されたファイルを使用してポリシーをインポートできるようにします。

6. [ユーザ権限] タブのオプションを使用して、管理者アカウントの権限を定義できます。



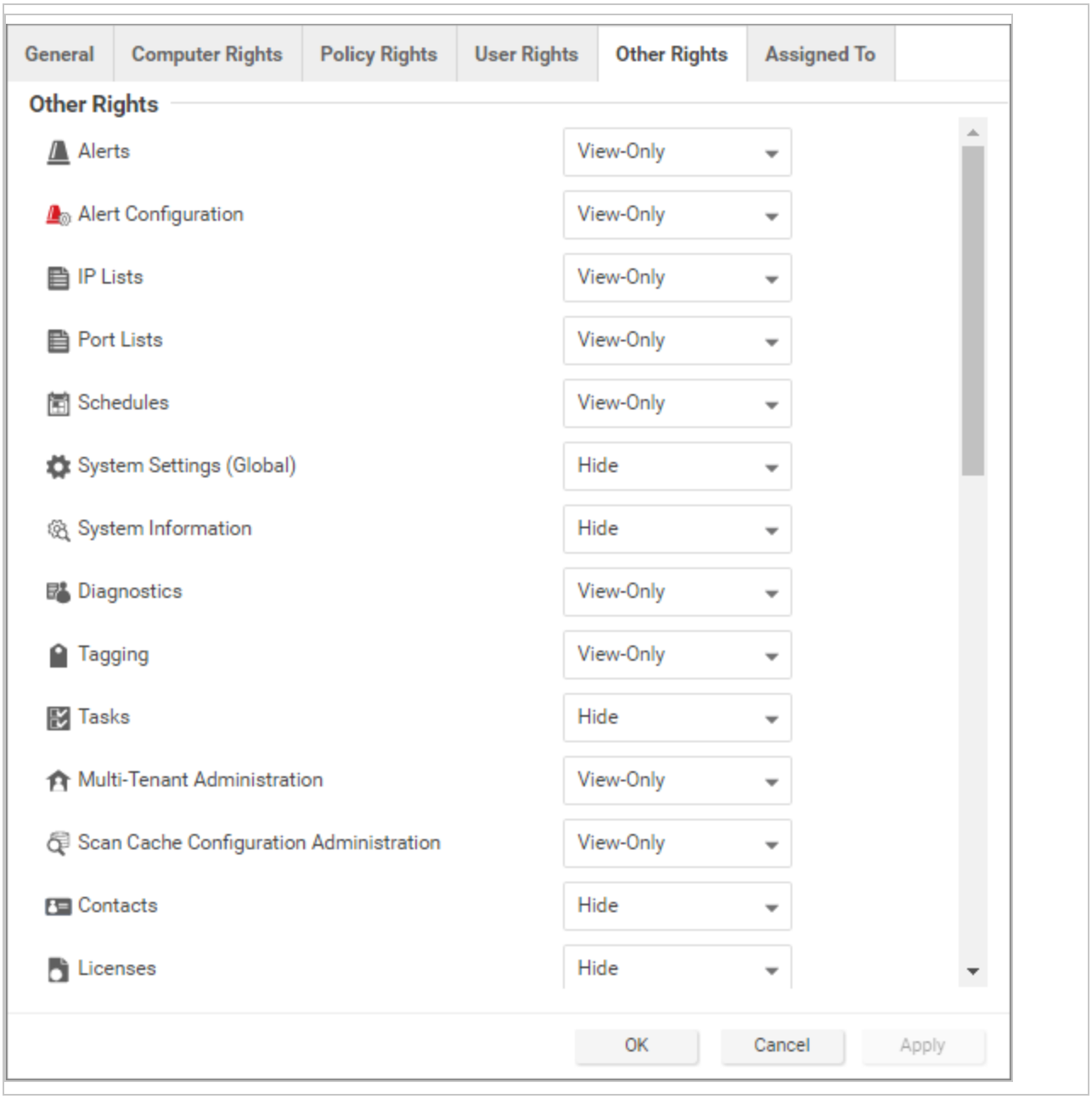
- 自身のパスワードと連絡先情報のみを変更: この役割のユーザは、自身のパスワードと連絡先情報のみを変更できます。
- 同等以下のアクセス権を持つユーザを作成および管理: この役割のユーザは、同等以下のアクセス権を持つユーザを作成および管理できます。この役割を持つユーザの権限を1つでも上回る場合、この役割のユーザはそのユーザを作成または管理できません。
- すべての役割およびユーザを完全に管理: この役割のユーザは、ユーザと役割を制限なしで作成および管理できます。このオプションの使用には、十分な注意が必要です。このロールを役割に割り当てる場合は、制限された権限を持つユーザに対して、Deep Security Managerのすべての側面に対するすべての制限のないアクセス権を持つユーザとして作成してからログインすることができます。
- カスタム: [カスタム] を選択して、[カスタム権限] セクションのオプションを使用すると、ユーザが他のユーザおよび役割を表示、作成、編集、または削除する権限をさらに制限できます。[同等以下の権限を持つユーザのみを操作] オプションを選択すると、特定のユーザに対して一部のオプションが制限される場合があります。

  [同等以下の権限を持つユーザのみを操作] オプションでは、この役割のユーザの権限をさらに制限します。ユーザは、自身と同等または下位の権限を持つユーザに対する変更のみ行うことができます。この役割のユーザは、役割を作成、編集、削除できなくなります。このオプションを選択すると、[カスタム権限] セクションの以下のオプションが制限されます。

  - 新規ユーザを作成できます: 同等または下位の権限を持つユーザの作成のみ可能です。
  - ユーザプロパティを編集できます: 同等または下位の権限を持つユーザの編集、またはパスワードの設定やリセットのみ可能です。
  - ユーザを削除できます: 同等または下位の権限を持つユーザの削除のみ可能です。

7. [その他の権限] タブでは、特定のDeep Securityの機能にのみアクセスできるように、また場合によってはそれらの機能で特定の処理にアクセスできるように、役割の権限を制限できます。たとえば、管理者が複数いる場合、誤って他の管理者の作業内容を上書きすることがないように各管理者の権限を制限できます。初期設定では、各役割は各機能に対して「表示のみ」または「非表示」に設定されています。アクセスを細かく変更またはカスタマイズするには、リストから[カ

スタム] を選択します。



8. [割り当て対象] タブには、この役割が割り当てられたユーザのリストが表示されます。役割が正しく機能していることをテストする場合は、新しいユーザを作成し、そのユーザとしてログインして機能を検証します。

Full Access、Auditor、および新規の各役割の初期設定

次の表は、フルアクセスロールと監査ロールのデフォルト権限設定を示しています。また、ロールページのTrend ツールバーで新規をクリックして新しいロールを作成する際の権限設定も記載されています。

権限	役割別の設定		
一般	Full Accessの役割	Auditorの役割	新規役割の初期設定
DSMユーザインタフェースへのアクセス	許可	許可	許可
WebサービスAPIへのアクセス	許可	許可	不許可
コンピュータの権限	Full Accessの役割	Auditorの役割	新規役割の初期設定
表示	許可、すべてのコンピュータ	許可、すべてのコンピュータ	許可、すべてのコンピュータ
警告/エラーのクリア	許可、すべてのコンピュータ、	不許可、すべてのコンピュータ	不許可、すべてのコンピュータ
編集	許可、すべてのコンピュータ	不許可、すべてのコンピュータ	不許可、すべてのコンピュータ
削除	許可、すべてのコンピュータ	不許可、すべてのコンピュータ	不許可、すべてのコンピュータ
アラートの消去	許可、すべてのコンピュータ	不許可、すべてのコンピュータ	不許可、すべてのコンピュータ
アイテムのタグ付け	許可、すべてのコンピュータ	不許可、すべてのコンピュータ	不許可、すべてのコン

権限	役割別の設定		
			ピュータ
選択されていないコンピュータおよびデータ(イベントやレポートなど)を表示	許可	許可	許可、すべてのコンピュータ
コンピュータに関連していないイベントおよびアラートを表示	許可	許可	許可、すべてのコンピュータ
選択したグループ内に新しいコンピュータを作成	許可	不許可	不許可
選択したグループ内にサブグループを追加または削除	許可	不許可	不許可
コンピュータファイルをインポート	許可	不許可	不許可
クラウドアカウントの追加、削除、および同期を許可	許可	不許可	不許可
ポリシーの権限	Full Accessの役割	Auditorの役割	新規役割の初期設定
表示	許可、すべてのポリシー	許可、すべてのポリシー	許可、すべてのポリシー
編集	許可、すべてのポリシー	不許可、すべてのポリシー	不許可、すべてのポリシー

権限	役割別の設定		
削除	許可、すべてのポリシー	不許可、すべてのポリシー	不許可、すべてのポリシー
選択されていないポリシーの表示	許可	許可	許可
新規ポリシーの作成	許可	不許可	不許可
ポリシーのインポート	許可	不許可	不許可
ユーザ権限 (この後の「ユーザ権限に関する注意」を参照)	Full Accessの役割	Auditorの役割	新規役割の初期設定
ユーザの表示	許可	許可	不許可
ユーザの作成	許可	不許可	不許可
ユーザプロパティの編集	許可	不許可	不許可
ユーザの削除	許可	不許可	不許可
役割の表示	許可	許可	不許可
役割の作成	許可	不許可	不許可
役割のプロパティの編集	許可	不許可	不許可
役割の削除	許可	不許可	不許可
権限の委任	許可	不許可	不許可
その他の権限	Full Accessの役割	Auditorの役割	新規役割の初

権限	役割別の設定		
			期設定
アラート	完全 (グローバルアラートを消去可能)	表示のみ	表示のみ
アラート設定	完全 (アラート設定を編集可能)	表示のみ	表示のみ
IPリスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
ポートリスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
スケジュール	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
システム設定 (グローバル)	完全 (システム設定 (グローバル) を表示、編集可能)	非表示	非表示
診断	完全 (診断パッケージを作成可能)	表示のみ	表示のみ
タグ付け	完全 (タグ付け (コンピュータに属さない項目)、タグ削除、所有していない自動タグルールをアップデート、所有していない自動タグルールを実行、および所有していない自動タグルールを削除可能)	表示のみ	表示のみ
タスク	完全 (タスクを表示、追加、編集、削除、および実行可能)	非表示	非表示
マルチテナントの管理	完全	非表示	非表示
検索キャッシュ設定の管理	完全	表示のみ	表示のみ
連絡先	完全 (連絡先を表示、作成、編集、および削除可能)	非表示	非表示
ライセンス	完全 (ライセンスを表示および変更可能)	非表示	非表示

権限	役割別の設定		
アップデート	完全 (ソフトウェアを追加、編集、および削除可能。コンポーネントのアップデートの表示、ダウンロード、インポート、アップデートコンポーネントの適用、Deep Securityルールのアップデートの削除が可能)	非表示	非表示
資産評価	完全 (資産評価を作成、編集、および削除可能)	表示のみ	表示のみ
証明書	完全 (SSL証明書を作成および削除可能)	表示のみ	表示のみ
Relayグループ	完全	表示のみ	表示のみ
プロキシ	完全	表示のみ	表示のみ
SAML IDプロバイダ	完全	非表示	非表示
不正プログラム検索設定	完全 (不正プログラム検索設定を作成、編集、および削除可能)	表示のみ	表示のみ
検出ファイル	完全 (検出ファイルを削除およびダウンロード可能)	表示のみ	表示のみ
Webレピュテーション設定	完全	表示のみ	表示のみ
アクティビティ監視設定	完全	表示のみ	表示のみ
ディレクトリリスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
ファイルリスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
ファイル拡張子リスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ

権限	役割別の設定		
ファイアウォールルール	完全 (ファイアウォールルールを作成、編集、および削除可能)	表示のみ	表示のみ
ファイアウォールステートフル設定	完全 (ファイアウォールステートフル設定を作成、編集、および削除可能)	表示のみ	表示のみ
侵入防御ルール	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
アプリケーションの種類	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
MACリスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
コンテキスト	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
変更監視ルール	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
セキュリティログ監視ルール	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
セキュリティログ監視デコーダ	完全 (作成、編集、および削除可能)	表示のみ	表示のみ
アプリケーションコントロールルールセット	完全(アプリケーションコントロールのルールセットを作成、表示、編集、または削除できます)	非表示	非表示
アプリケーションコントロールルール	完全(アプリケーションコントロールの作成、表示、編集、または削除のルールを設定できます)	非表示	非表示
アプリケーションコントロールの承認されていないソフトウェア	完全(Can not ViewまたはAllow/Block unrecognizedソフトウェア)	非表示	非表示
アプリケーションコントロールソフトウェアインベントリ	完全(ソフトウェアインベントリを作成、表示、または削除できます)	非表示	非表示

自分のパスワードと連絡先情報のみを変更オプションに対応するカスタム設定は、次の表に一覧されています。

パスワードの変更と連絡先情報のみのオプションのカスタム設定	
ユーザ	
ユーザを表示できます	不許可
新規ユーザを作成できます	不許可
ユーザプロパティを編集できます (ユーザは常に自分のアカウントの選択プロパティを編集できます)	不許可
ユーザを削除できます	不許可
役割	
役割を表示できます	不許可
新規の役割を作成できます	不許可
役割のプロパティを編集できます (警告: この権限を付与すると、この役割を持つユーザが自分の権限を編集できるようになります)	不許可
役割を削除できます	不許可
権限の委任	
同等以下の権限を持つユーザのみを操作	不許可

ユーザの作成と同等またはそれ以下のアクセス権限の管理オプションに対応するカスタム設定は、以下の表に記載されています。

同等またはそれ以下のアクセスオプションを持つユーザの作成と管理のためのカスタム設定	
ユーザ	
ユーザを表示できます	許可
新規ユーザを作成できます	許可

同等またはそれ以下のアクセスオプションを持つユーザの作成と管理のためのカスタム設定	
ユーザプロパティを編集できます (ユーザは常に自分のアカウントの選択プロパティを編集できます)	許可
ユーザを削除できます	許可
役割	
役割を表示できます	不許可
新規の役割を作成できます	不許可
役割のプロパティを編集できます (警告: この権限を付与すると、この役割を持つユーザが自分の権限を編集できるようになります)	不許可
役割を削除できます	不許可
権限の委任	
同等以下の権限を持つユーザのみを操作	許可

すべてのロールとユーザを完全に管理するオプションに対応するカスタム設定は、以下の表に記載されています。

すべてのロールとユーザオプションを完全に制御するためのカスタム設定	
ユーザ	
ユーザを表示できます	許可
新規ユーザを作成できます	許可
ユーザプロパティを編集できます (ユーザは常に自分のアカウントの選択プロパティを編集できます)	許可
ユーザを削除できます	許可
役割	

すべてのロールとユーザオプションを完全に制御するためのカスタム設定	
役割を表示できます	許可
新規の役割を作成できます	許可
役割のプロパティを編集できます (警告: この権限を付与すると、この役割を持つユーザが自分の権限を編集できるようになります)	許可
役割を削除できます	許可
権限の委任	
同等以下の権限を持つユーザのみを操作	該当なし

レポートのみを受信できるユーザの追加

「連絡先」とは、Deep Security Managerにサインインできないユーザですが、(予約タスクを使用して)定期的にレポートを送信できます。連絡先には、既存の役割にマッピングする「アクセス許可」レベルを割り当てることができます。連絡先にレポートが送信される場合、同じレベルのユーザがアクセスできない情報はそのレポートに含まれません。たとえば、3名の連絡先を週次の概要レポートの受信者として指定した場合、各連絡先が使用するコンピュータの権限に応じて、3つのレポートの内容がまったく異なるものになる場合があります。

連絡先を追加または編集する

1. Deep Security Managerで、[管理]→[ユーザ管理]→[連絡先]の順に選択します。
2. 新しい連絡先を追加する場合は [新規] をクリックし、既存の連絡先の設定を編集する場合はその連絡先をダブルクリックします。
3. [一般情報] セクションで、この連絡先の名前、説明、および優先する言語を指定します。
4. [連絡先情報] セクションで、レポート配布リストにこの連絡先が含まれている場合にレポートの送信先となるメールアドレスを入力します(詳細については、[レポートの生成] 画面を参照してください)。
5. [アクセス許可] セクションで役割を指定し、この連絡先が参照できる情報を決定します。たとえば、この連絡先にコンピュータレポートを送信するように予約すると、役割でアクセスが許可されている、コンピュータに関する情報だけがレポートに含まれます。
6. エクスポートされるPDF形式のレポートをパスワードで保護するには、[パスワードで保護されたレポート] セクションで [このユーザが生成したレポートをパスワードで保護する] を選択し、[レポートのパスワード] を指定します。

連絡先を削除する

Deep Security Managerから連絡先を削除するには、[管理]→[ユーザ管理]→[連絡先]の順に選択し、連絡先をクリックしてから[削除]をクリックします。

ユーザ向けのAPIキーの作成

Deep Security Manager APIを使用するには、APIキーが必要です。

注意: APIキーは、Deep Security Manager 11.1以降で使用可能な新しい"Deep Security APIを使用したタスクの自動化" on page 1824でのみ使用できます。

注意: Trend Micro Deep Security ManagerへのAPIアクセスが必要なすべてのユーザに対して、1つのAPIキーを作成することをお勧めします。

ヒント: APIキーの作成は、Deep Security APIを使用して自動化できます。自動化の例については、Deep Security Automation Centerにあるガイド「Create and Manage API Keys」を参照してください。

新しいAPIキーを作成するには、次の手順に従います。

1. [管理]→[ユーザ管理]→[APIキー] の順に移動します。
2. [新規] をクリックします。
3. [プロパティ] ウィンドウで、APIキーの [名前] と[説明] を入力します。
4. [役割] リストをクリックして、役割を選択します。Auditor はAPIを介してDeep Security Managerに読み取り専用アクセスを許可し、Full Access は読み取りアクセスと書き込みアクセスの両方を許可します。より詳細に定義された役割をAPIキーのユーザに割り当てる必要がある場合は、[新規] を選択して役割を定義することもできます。手順の詳細については、"ユーザロールの定義" on page 1541を参照してください。
5. [言語] を選択します。
6. タイムゾーンを選択します。
7. 必要に応じて[有効期限] を選択し、APIキーの有効期限を選択します。
8. [OK] をクリックします。
9. [秘密鍵の値] をコピーします。

   注意: 秘密鍵の値はこのときにしか表示されないため、必ずコピーしておいてください。

既存のAPIキーをロックアウトする

既存のAPIキーが第三者に漏えいした場合は、次の手順でロックアウトすることができます。

1. ロックアウトするAPIキーをダブルクリックします。
2. 必要に応じ、[ロックアウト(認証を拒否)] を選択してAPIキーの使用をブロックします。
3. [OK] をクリックします。

ロックアウトされたユーザ名のロック解除

間違ったパスワードを使用してDeep Security Managerに何回もログオンすると、ユーザアカウントはロックアウトされます。ロックアウトされないログオン試行の許容回数は、[管理]→[システム設定]→[セキュリティ]→[ログオン失敗の許容回数 (ロックアウト前)] で設定します。

次の状況に応じて、ユーザをそれぞれの方法でロック解除できます。

- 管理者ユーザが利用可能な場合、"管理者としてユーザのロックを解除する" belowを参照してください。
- すべての管理ユーザがロックアウトされた場合は、"コマンドラインから管理ユーザのロックを解除する" belowを参照してください。

管理者としてユーザのロックを解除する

1. 作業管理者のユーザ名とパスワードを使用してDeep Security Managerにログインします。
2. [管理]→[ユーザ管理]→[ユーザ] の順に選択します。ロック解除するユーザを選択して右クリックし、[プロパティ] をクリックします。
3. ウィザードで、[一般]→[ログオン資格情報] の順に選択します。[ロックアウト(ログオンを拒否)] チェックボックスの選択を解除します。
4. [保存] をクリックします。

コマンドラインから管理ユーザのロックを解除する

1. ローカルコマンドラインインタフェースに移動します。

   Deep Security ManagerがWindowsの場合、`..\Program Files\Trend Micro\Deep security Manager`ディレクトリに移動します。

   Deep Security ManagerがLinuxの場合、`/opt/dsm`ディレクトリに移動します。

2. 次のコマンドを入力します。

   ```
   dsm_c -action unlockout -username <username>
   ```

SAML シングルサインオン(SSO) を実装する

SAMLシングルサインオン(SSO) について

SAMLシングルサインオンを実装するには、"SAMLシングルサインオンを設定する" on page 1563 または "SAMLシングルサインオンをMicrosoft Entra IDで設定する" on page 1569で設定します。

SAMLとシングルサインオンとは

Security Assertion Markup Language (SAML) は、当事者間でのユーザ識別情報の安全な交換を可能にする、オープンな認証標準です。SAMLは、1回のユーザログインを複数のアプリケーションとサービスにわたって機能させる技術である、シングルサインオンをサポートしています。Deep Securityでは、SAMLシングルサインオンを実装することで、組織のポータルにログオンするユーザが、既存のDeep Securityアカウントなしで Deep Securityにシームレスにログオンできるようになります。

Deep SecurityでのSAMLシングルサインオンの仕組み

信頼関係を確立する

SAMLシングルサインオンでは、両当事者(IDプロバイダとサービスプロバイダ) の間で信頼関係が確立されます。IDプロバイダのディレクトリサーバにはユーザID情報が保存されています。サービスプロバイダ(この場合はDeep Security) は、IDプロバイダのユーザIDを使用して独自の認証とアカウント作成を行います。

IDプロバイダとサービスプロバイダは、SAML メタデータドキュメントを交換することで、信頼を確立します。

> 注意: 現時点では、Deep SecurityはSAML 2.0 IDプロバイダ (IdP) で開始されたログインフローのHTTP POSTバインディングのみをサポートし、サービスプロバイダ (SP) で開始されたログインフローはサポートしません。

ユーザIDからDeep Securityアカウントを作成する

Deep SecurityとIDプロバイダがSAML メタデータドキュメントを交換して信頼関係を確立すると、Deep SecurityはIDプロバイダのディレクトリサーバ上のユーザIDにアクセスできるようになります。ただし、Deep Securityが実際にユーザIDからアカウントを作成する前に、アカウントの種類を定義し、データ形式を

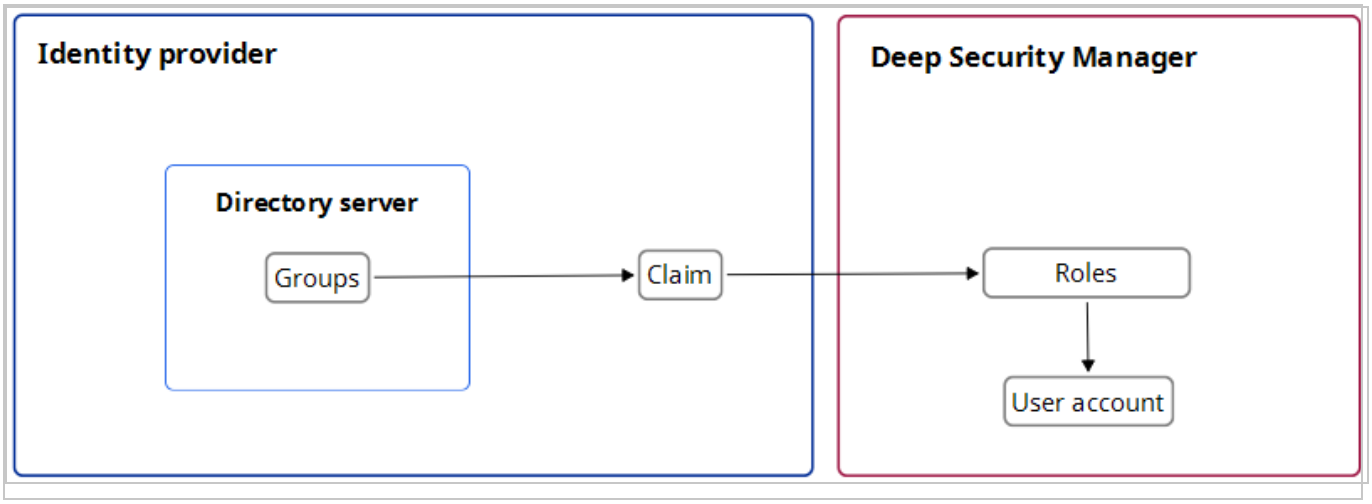
変換するための手順を導入する必要があります。これは、グループ、役割、クレームを使用して実行されます。

グループと役割は、Deep Securityユーザアカウントのテナントとアクセス許可を指定します。グループは、IDプロバイダのディレクトリサーバ上に作成されます。IDプロバイダは、1つ以上のグループにユーザIDを割り当てます。役割はDeep Security Managerで作成されます。各Deep Securityアカウントの種類にはグループと役割の両方が必要で、アクセス許可とテナントの割り当てが一致している必要があります。

各ユーザの種類に一致するグループと役割を用意したら、グループデータ形式をDeep Securityが理解できる形式に変換する必要があります。これは、IDプロバイダによりクレームを使用して実行されます。クレームには、グループデータ形式を一致するDeep Securityの役割に変換するための手順が含まれています。

Deep Securityで必要となる"SAMLクレームの構造" on page 1566について確認してください。

このプロセスを次に示します。



Deep SecurityでSAMLシングルサインオンを実装する

SAMLメタデータドキュメントの交換により、Deep SecurityとIDプロバイダとの間で信頼関係が確立されると、一致するグループと役割が作成され、グループデータを役割に変換するためのクレームが導入されて、Deep SecurityはSAMLシングルサインオンを使用して組織のポータルからログオンするユーザに対してDeep Securityアカウントを自動的に作成できるようになります。

SAMLシングルサインオンの実装の詳細については、"SAMLシングルサインオンを設定する" on the next pageを参照してください。

SAMLシングルサインオンを設定する

Deep SecurityをSAMLシングルサインオン(SSO)で使用するように構成すると、組織のポータルにサインインするユーザは、既存のDeep Securityアカウントなしでシームレスに Deep Securityにサインインできます。SAMLシングルサインオンにより、次のようなユーザ認証アクセス制御機能を実装することも可能になります:

- パスワード強度または変更の強制
- ワンタイムパスワード(OTP)
- 2要素認証 (2FA) または多要素認証 (MFA)

Deep SecurityのSAML標準実装の詳細については、"SAMLシングルサインオン(SSO) について" on page 1561を参照してください。Microsoft Entra IDをIDプロバイダとして使用している場合は、"SAMLシングルサインオンをMicrosoft Entra IDで設定する" on page 1569を使用したSAMLシングルサインオンの設定を参照してください。

注意: 現時点では、Deep SecurityはSAML 2.0 IDプロバイダ(IdP)で開始されたログインフローのHTTP POSTバインディングのみをサポートし、サービスプロバイダ(SP)で開始されたログインフローはサポートしません。

Deep SecurityでSAMLシングルサインオンを使用するには、次の手順を実行する必要があります。

1. "設定前の要件を設定する" below
2. "Deep SecurityをSAMLサービスプロバイダとして設定する" on the next page
3. "Deep SecurityでSAMLを設定する" on the next page
4. "IDプロバイダの管理者に情報を提供する" on page 1565
5. "SAMLクレームの構造" on page 1566
6. "SAMLシングルサインオンをテストする" on page 1568
7. "サービスとIDプロバイダの設定" on page 1569

設定前の要件を設定する

1. Deep Security Managerが正常に動作していることを確認します。
2. IDプロバイダの管理者に次のことを問い合わせます。
   - ディレクトリサーバグループをDeep Securityロールにマッピングするための名前付け規則を設定します。
   - IDプロバイダSAMLメタデータドキュメントを取得します。
   - 必要なユーザ認証アクセス制御機能をポリシーに追加するよう依頼します。

Deep SecurityでのSAMLシングルサインオンの動作がすでにテストされている次のIDプロバイダがサポートされています。

- Active Directoryフェデレーションサービス(ADFS)
- Okta
- PingOne
- Shibboleth
- Microsoft Entra ID

Deep SecurityをSAMLサービスプロバイダとして設定する

まず、Deep Securityをサービスプロバイダとして設定します。

注意: マルチテナントのDeep Securityインストール環境でDeep SecurityをSAMLサービスプロバイダとして設定できるのは、プライマリテナントの管理者だけです。

1. Deep Security Managerで、[管理]→[ユーザ管理]→[IDプロバイダ]→[SAML]の順に選択します。
2. [開始]をクリックします。
3. エンティティID および サービス名を入力し、[ ]をクリックします。[次へ]をクリックします。

   注意: [エンティティID] はSAMLサービスプロバイダの一意の識別子です。SAMLの仕様ではエンティティIDがエンティティのドメイン名を含むURLであることが推奨されており、業界の慣習として、エンティティIDにはSAMLメタデータURLを使用します。SAMLメタデータは、Deep Security Managerの/ samlエンドポイントから配信されるため、例の値はhttps://<DSMServerIP:4119>/samlです。

4. 証明書のオプションを選択し、[次へ]をクリックします。SAMLサービスプロバイダの証明書は現時点では使用されていませんが、サービスプロバイダが開始したログオン機能やシングルサインアウト機能をサポートするために将来使用されます。証明書をインポートするには、PKCS # 12キーストアファイルとパスワードを入力するか、新しい自己署名証明書を作成します。
5. 証明書の詳細の概要が表示されるまで手順を実行し、[完了]をクリックします。

Deep SecurityでSAMLを設定する

IDプロバイダSAMLメタデータドキュメントをインポートする

注意: Deep Securityアカウントには、管理者権限と「SAML IDプロバイダの作成」権限の両方が必要です。

1. [管理] 画面で、[ユーザ管理]→[アイデンティティプロバイダ]→[SAML] に移動します。
2. [開始] をクリックします。
3. [ファイルの選択] をクリックし、IDプロバイダによって提供されたSAMLメタデータドキュメントを選択して、[次へ] をクリックします。
4. IDプロバイダの [名前] を入力し、[完了] をクリックします。

   [役割] 画面が表示されます。

SAMLユーザのDeep Securityの役割を作成する

想定されるユーザの種類ごとに役割を作成する必要があります。各役割は、IDプロバイダのディレクトリサーバに対応するグループがあり、グループのアクセス権限およびテナントの割り当てと一致する必要があります。

IDプロバイダのSAML統合では、グループのメンバーシップをSAMLクレームに変換するメカニズムが用意されます。クレームルールの詳細は、IDプロバイダに付属するドキュメントを確認してください。

役割の作成方法については、"ユーザロールの定義" on page 1541の定義を参照してください。

IDプロバイダの管理者に情報を提供する

Deep Security ManagerサービスプロバイダSAMLメタデータドキュメントをダウンロードする

1. [管理] 画面で、[ユーザ管理]→[アイデンティティプロバイダ]→[SAML] に移動します。
2. SAMLサービスプロバイダの下の [ダウンロード] をクリックします。
   Deep SecurityサービスプロバイダSAMLメタデータドキュメント (ServiceProviderMetadata.xml) がダウンロードされます。

URNおよびDeep Security SAMLメタデータドキュメントをIDプロバイダの管理者に送信する

IDプロバイダの管理者には、Deep SecurityのサービスプロバイダSAMLメタデータドキュメント、IDプロバイダのURN、および作成したDeep Securityの各役割のURNを指定する必要があります。

ヒント:
役割のURNを確認するには、[管理]→[ユーザ管理]→[役割] の順に選択し、[URN] 列を参照します。

IDプロバイダのURNを確認するには、[管理]→[ユーザ管理]→[アイデンティティプロバイダ]→[SAML]→[アイデンティティプロバイダ] の順に選択し、[URN] 列を参照します。

IDプロバイダの管理者が、Deep Securityの役割に対応するグループと、グループメンバーシップをSAMLクレームに変換するために必要なルールを作成していることを確認したら、SAMLシングルサインオンの設定は完了です。

注意: IDプロバイダの管理者には、必要に応じて、Deep Securityが必要とする"SAMLクレームの構造" belowについての情報を提供できます。

SAMLクレームの構造

次のSAML要求はDeep Securityでサポートされています。

- "Deep Securityユーザ名 (必須)" below
- "Deep Securityユーザの役割 (必須)" on the next page
- "最大セッション期間 (オプション)" on the next page
- "言語設定 (オプション)" on page 1568

Deep Securityユーザ名 (必須)

クレームには、Name属性が https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionNameAttributeエレメントと、1つのAttributeValueエレメントが含まれるSAMLアサーションが必要です。Deep Security ManagerはAttributeValueをDeep Securityユーザ名として使用します。

SAMLデータの例 (簡略版)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  <AttributeStatement>
   <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionName">
    <AttributeValue>alice</AttributeValue>
   </Attribute>
  </AttributeStatement>
```

```
 </Assertion>
</samlp:Response>
```

Deep Securityユーザの役割 (必須)

クレームには、Name属性がhttps://deepsecurity.trendmicro.com/SAML/Attributes/RoleAttributeエレメントと、1 ~ 10個のAttributeValueエレメントが含まれるSAMLアサーションが必要です。Deep Security Managerは、この属性値を使用して、ユーザのテナント、IDプロバイダ、役割を確認します。1つのアサーションには複数のテナントの役割が含まれる場合があります。

注意: AttributeValueには、の2つのURNがカンマで区切られています。URNは大文字と小文字が区別されます。

SAMLデータの例 (簡略版)

注意: 読みやすいようにAttributeValueエレメントに改行を入れていますが、クレームでは1行にする必要があります。

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  <AttributeStatement>
   <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/Role">
    <AttributeValue>urn:tmds:identity:[pod ID]:[tenant ID]:saml-provider/[IDP name],
      urn:tmds:identity:[pod ID]:[tenant ID]:role/[role name]</AttributeValue>
   </Attribute>
  </AttributeStatement>
 </Assertion>
</samlp:Response>
```

最大セッション期間 (オプション)

クレームに https://deepsecurity.trendmicro.com/SAML/Attributes/SessionDuration の Name 属性と整数値の AttributeValue 要素を含む Attribute 要素が含まれているSAMLアサーションがある場合、セッションはその時間(秒)が経過すると自動的に終了します。

SAMLデータの例 (簡略版)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  <AttributeStatement>
```

```
    <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/SessionDuration">
     <AttributeValue>28800</AttributeValue>
    </Attribute>
   </AttributeStatement>
  </Assertion>
</samlp:Response>
```

言語設定 (オプション)

要求に https://deepsecurity.trendmicro.com/SAML/attributes/PreferredLanguage というName 属性の Attribute 要素が含まれ、サポートされている言語のいずれかと同じ文字列値の AttributeValue 要素が含まれるSAMLアサーションがある場合、Deep Security Managerはこの値を使用してユーザの優先言語を設定します。

次の言語がサポートされます。

- en-US (米国英語)
- ja-JP (日本語)

SAMLデータの例 (簡略版)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  <AttributeStatement>
   <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/PreferredLanguage">
    <AttributeValue>en-US</AttributeValue>
   </Attribute>
  </AttributeStatement>
 </Assertion>
</samlp:Response>
```

SAMLシングルサインオンをテストする

IDプロバイダサーバのシングルサインオンのログイン画面に移動し、そこからDeep Security Managerにログインします。正しく設定されている場合、Deep Security Managerコンソールにリダイレクトされます。SAMLシングルサインオンが機能していない場合は、次の手順に従います。

設定を確認する

1. "設定前の要件を設定する" on page 1563セクションを確認します。
2. ユーザが正しいディレクトリグループに属していることを確認します。

3. IDプロバイダと役割のURNがIDプロバイダのフェデレーションサービスで正しく設定されていることを確認します。

診断パッケージを作成する

1. [管理]→[システム情報] の順に選択し、[診断ログ] をクリックします。
2. [SAMLに関する問題] を選択し、[保存] をクリックします。
3. ログを生成します。IDプロバイダ経由でDeep Security Managerにログインし、問題を再現します。
4. ログインが失敗したら、[管理]→[システム情報] に移動し、[診断パッケージの作成] をクリックして診断パッケージを生成します。
5. 診断パッケージが作成されたら、*https://success.trendmicro.com/dcx/s/contactus?language=ja*に移動してテクニカルサポートケースを開き、ケースの作成時に診断パッケージをアップロードします。

サービスとIDプロバイダの設定

サーバ証明書とIDプロバイダ証明書の有効期限を事前に通知するタイミングや、SAMLシングルサインオン経由で追加された非アクティブなユーザアカウントを自動的に削除するまでの期間を設定できます。

これらの設定を変更するには、[管理]→[システム設定]→[セキュリティ]→[アイデンティティプロバイダ] に移動します。

SAMLシングルサインオンをMicrosoft Entra IDで設定する

Deep SecurityのSAML標準の実装の詳細については、"SAMLシングルサインオン(SSO) について" on page 1561の実装を参照してください。他のIDプロバイダとの設定手順については、"SAMLシングルサインオンを設定する" on page 1563を参照してください。

注意: 現時点では、Deep SecurityはSAML 2.0 IDプロバイダ (IdP) で開始されたログインフローのHTTP POSTバインディングのみをサポートし、サービスプロバイダ (SP) で開始されたログインフローはサポートしません。

誰がこのプロセスに関与していますか?

通常、Deep Security ManagerでSAMLシングルサインオンにMicrosoft Entra IDを使用するように設定するには、2人必要です(SSO): Deep Security管理者とMicrosoft Entra ID管理者。

Deep Securityの管理者には、SAML IDプロバイダ権限が完全に設定されているか、カスタム(で新しいSAML IDプロバイダの作成可能なが有効) に設定されたDeep Securityの役割が割り当てられている必要があります。

Microsoft Entra IDを使用してDeep SecurityでSAMLシングルサインオンを設定する手順と、各手順を実行する担当者の手順は次のとおりです。

手順	実行者
"Deep SecurityをSAMLサービスプロバイダとして設定する" below	Deep Security管理者
"Deep Securityサービスプロバイダの SAML メタデータドキュメントをダウンロードする" on the next page	Deep Security管理者
"Microsoft Entra IDを設定する" on the next page	Microsoft Entra ID管理者
"Deep SecurityでSAMLを設定する" on page 1572	Deep Security管理者
"Microsoft Entra IDで役割を定義する" on page 1572	Microsoft Entra ID管理者

Deep SecurityをSAMLサービスプロバイダとして設定する

まず、Deep Securityをサービスプロバイダとして設定します。

注意: マルチテナントのDeep Securityインストール環境でDeep SecurityをSAMLサービスプロバイダとして設定できるのは、プライマリテナントの管理者だけです。

1. Deep Security Managerで、[管理]→[ユーザ管理]→[IDプロバイダ]→[SAML]の順に選択します。
2. [開始] をクリックします。
3. エンティティID および サービス名を入力し、[ ]をクリックします。[次へ]をクリックします。

   注意: [エンティティID] はSAMLサービスプロバイダの一意の識別子です。SAMLの仕様ではエンティティIDがエンティティのドメイン名を含むURLであることが推奨されており、業界の慣習として、エンティティIDにはSAML メタデータURLを使用します。SAML メタデータは、Deep Security Managerの/ samlエンドポイントから配信されるため、例の値は https://<DSMServerIP:4119>/samlです。

4. 証明書のオプションを選択し、[次へ] をクリックします。SAMLサービスプロバイダの証明書は現時点では使用されていませんが、サービスプロバイダが開始したログオン機能やシングルサインアウト機能をサポートするために将来使用されます。証明書をインポートするには、PKCS # 12キーストアファイルとパスワードを入力するか、新しい自己署名証明書を作成します。
5. 証明書の詳細の概要が表示されるまで手順を実行し、[完了]をクリックします。

Deep SecurityサービスプロバイダのSAMLメタデータドキュメントをダウンロードする

Deep Security Managerで、管理 > ユーザ管理 > IDプロバイダ > SAMLに移動し、ダウンロードをクリックします。

ファイルはServiceProviderMetadata.xmlとしてダウンロードされます。Microsoft Entra ID管理者に送信してください。

Microsoft Entra IDを設定する

以下の手順はMicrosoft Entra ID管理者によって実行されます。詳細については、Microsoft Entra IDでギャラリー以外のアプリケーションにシングルサインオンを構成するを参照してください。

1. Microsoft Entra IDポータルで、ギャラリー以外の新しいアプリケーションを追加します。
2. アプリケーションのシングルサインオンを設定します。Deep Security Managerからダウンロードした ServiceProviderMetadata.xml メタデータファイルをアップロードする必要があります。あるいは、応答URL (Deep Security ManagerのURL + /saml) を入力することもできます。
3. SAMLクレームを構成します。Deep Securityには次の2つのクレームが必要です:

   - https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionName
     Deep Securityのユーザ名となる一意のユーザIDです。たとえば、User Principal Name (UPN) を使用できます。
   - https://deepsecurity.trendmicro.com/SAML/Attributes/Role
     形式は「IDP URN、役割URN」です。IDPはまだDeep Security Managerに作成されていません。このSAMLクレームは、後で "Microsoft Entra IDで役割を定義する" on the next pageで役割を定義するで設定できます。

   "SAMLクレームの構造" on page 1573で説明されているように、その他の任意のクレームを設定することもできます。
4. フェデレーションメタデータXMLファイルをダウンロードし、Deep Security管理者に送信してください。

Deep Securityで複数の役割が定義されている場合は、これらの手順を繰り返して役割ごとに個別のアプリケーションを作成します。

Deep SecurityでSAMLを設定する

Microsoft Entra IDメタデータドキュメントをインポートする

1. Deep Security Managerで、[管理]→[ユーザ管理]→[IDプロバイダ]→[SAML]の順に選択します。
2. [の開始] または[新規]をクリックします。
3. [ファイルの選択] の順に選択し、Microsoft Entra IDからダウンロードしたフェデレーションメタデータXMLファイルを選択し、[次へ]の順にクリックします。
4. IDプロバイダの [名前] を入力し、[完了] をクリックします。

役割ページに移動します。

SAMLユーザのDeep Securityの役割を作成する

Deep Securityの[管理]→[ユーザ管理]→[役割のの管理]画面に、組織の適切な役割が含まれていることを確認します。ユーザには、自分の業務を職務の遂行に必要なものに限定する役割が割り当てられている必要があります。役割の作成方法については、"ユーザロールの定義" on page 1541の定義を参照してください。Deep Securityの各役割には、対応するMicrosoft Entra IDアプリケーションが必要です。

URNを取得する

Deep Security Managerで次の情報を収集してください。Microsoft Entra IDの管理者に提供する必要があります。

- アイデンティティプロバイダURNIDプロバイダのURNを表示するには、の[管理]→[ユーザ管理]→[IDプロバイダ]→[SAML]→[IDプロバイダ] に移動し、[URN]列を選択します。
- Microsoft Entra IDアプリケーションに関連付けるDeep Securityの役割のURN。ロールURNを表示するには、[管理]→[ユーザ管理]→[ロール] の順に選択し、[URN]列を選択します。複数の役割を持つ場合は、役割ごとにURNが必要になります。役割ごとに個別のAzure Activeアプリケーションが必要なためです。

Microsoft Entra IDで役割を定義する

これはMicrosoft Entra ID管理者によって実行される必要があります。

Microsoft Entra IDでは、前のセクションで識別されたアイデンティティプロバイダURNとロールURNを使用して、エンタープライズアプリケーションのロール属性を定義します。これは「IDP URN,Role URN」の形式でなければなりません。"SAMLクレームの構造" on the next pageセクションの「Deep Securityユーザロール (必須)」を参照してください。

Microsoft Entra IDの[検証]ボタンを使用してセットアップをテストするか、新しいアプリケーションをユーザに割り当ててテストします。

サービスとIDプロバイダの設定

サーバ証明書とIDプロバイダ証明書の有効期限を事前に通知するタイミングや、SAMLシングルサインオン経由で追加された非アクティブなユーザアカウントを自動的に削除するまでの期間を設定できます。

これらの設定を変更するには、[管理]→[システム設定]→[セキュリティ]→[アイデンティティプロバイダ]に移動します。

SAMLクレームの構造

次のSAML要求はDeep Securityでサポートされています。

- "Deep Securityユーザ名 (必須)" below
- "Deep Securityユーザの役割 (必須)" on the next page
- "最大セッション期間 (オプション)" on the next page
- "言語設定 (オプション)" on page 1575

Deep Securityユーザ名 (必須)

クレームには、`Name`属性が`https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionNameAttribute`エレメントと、1つの`AttributeValue`エレメントが含まれるSAMLアサーションが必要です。Deep Security Managerは`AttributeValue`をDeep Securityユーザ名として使用します。

SAMLデータの例 (簡略版)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  <AttributeStatement>
   <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionName">
    <AttributeValue>alice</AttributeValue>
   </Attribute>
  </AttributeStatement>
 </Assertion>
</samlp:Response>
```

Deep Securityユーザの役割 (必須)

クレームには、Name属性がhttps://deepsecurity.trendmicro.com/SAML/Attributes/RoleAttributeエレメントと、1 ~ 10個のAttributeValueエレメントが含まれるSAMLアサーションが必要です。Deep Security Managerは、この属性値を使用して、ユーザのテナント、IDプロバイダ、役割を確認します。1つのアサーションには複数のテナントの役割が含まれる場合があります。

注意: AttributeValueには、の2つのURNがカンマで区切られています。URNは大文字と小文字が区別されます。

SAMLデータの例 (簡略版)

注意: 読みやすいようにAttributeValueエレメントに改行を入れていますが、クレームでは1行にする必要があります。

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  <AttributeStatement>
   <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/Role">
    <AttributeValue>urn:tmds:identity:[pod ID]:[tenant ID]:saml-provider/[IDP name],
      urn:tmds:identity:[pod ID]:[tenant ID]:role/[role name]</AttributeValue>
   </Attribute>
  </AttributeStatement>
 </Assertion>
</samlp:Response>
```

最大セッション期間 (オプション)

クレームにhttps://deepsecurity.trendmicro.com/SAML/Attributes/SessionDurationのName属性と整数値のAttributeValue要素を含むAttribute要素が含まれているSAMLアサーションがある場合、セッションはその時間(秒)が経過すると自動的に終了します。

SAMLデータの例 (簡略版)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  <AttributeStatement>
   <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/SessionDuration">
    <AttributeValue>28800</AttributeValue>
   </Attribute>
```

```
  </AttributeStatement>
 </Assertion>
</samlp:Response>
```

言語設定 (オプション)

要求に https://deepsecurity.trendmicro.com/SAML/attributes/PreferredLanguage というName 属性の Attribute 要素が含まれ、サポートされている言語のいずれかと同じ文字列値の AttributeValue 要素が含まれるSAMLアサーションがある場合、Deep Security Managerはこの値を使用してユーザの優先言語を設定します。

次の言語がサポートされます。

- en-US (米国英語)
- ja-JP (日本語)

SAMLデータの例 (簡略版)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  <AttributeStatement>
   <Attribute Name="https://deepsecurity.trendmicro.com/SAML/Attributes/PreferredLanguage">
    <AttributeValue>en-US</AttributeValue>
   </Attribute>
  </AttributeStatement>
 </Assertion>
</samlp:Response>
```

データベースの管理

データベースの一般的なメンテナンス

Deep Security Managerのパフォーマンスを向上させるには、Deep Securityデータベースでインデックスのメンテナンスを定期的に実行して、過度のフラグメント化を防止することをお勧めします。組織のベストプラクティスに従ってデータベースのインデックスを再作成するか、データベースベンダが提供する以下のドキュメントを参照してください。

- PostgreSQL:PostgreSQLのインデックス再作成コマンドの詳細については、https://www.postgresql.org/docs/10/sql-reindex.htmlを参照してください。
- Microsoft SQL：インデックス管理のベストプラクティスについては、Microsoftのドキュメントを参照してください：https://docs.microsoft.com/en-us/sql/relational-databases/indexes/reorganize-and-rebuild-indexes?view=sql-server-ver15。「保守計画のデータベースバックアップタスク」のオプションも参照してください。
- Oracle Database: インデックスの管理に関するOracleのベストプラクティスに従ってください。たとえば、https://docs.oracle.com/cd/B28359_01/server.111/b28310/indexes002.htm#ADMIN11713を参照してください。

このタスクに役立つスクリプトは、オープンソースのWebサイトでも提供されています。

ヒント: 再インデックスによっていくつかの操作がブロックされる可能性があるため、オフラインで実行することをお勧めします。

PostgreSQLを維持する

次のデータベース管理およびチューニングの推奨事項に従ってください。

1. データベースログのローテーションとパフォーマンス設定を行います。

   ベストプラクティスについては、"ログローテーション" on the next page, "ロック管理" on page 1578, "最大同時接続数" on page 1578, "自動バキューム設定" on page 1580などを参照してください。

   手順は、ディストリビューションや管理対象のホスティングによって異なります。

   - 自己ホスト型データベースの場合:初期設定は、PostgreSQL Core Distributionの汎用値となります。特に大規模環境では、初期設定がデータセンターやカスタマイズされたクラウドインストールに適していないこともあります。

     設定を変更するには、次の手順に従います。

     - プレーンテキストエディタでpostgresql.confファイルを開きます。
     - パラメータを編集します。
     - ファイルを保存します。
     - PostgreSQLサービスを再起動します。

- Amazon RDSの場合:初期設定は、インスタンスのサイズによって異なります。多くの場合、autovacuuming、max_connections、effective_cache_sizeを微調整するだけです。設定を変更するには、データベースパラメータグループを使用し、データベースインスタンスを再起動します。
- Amazon Auroraの場合:初期設定は、インスタンスのサイズによって異なります。多くの場合、autovacuuming、max_connections、effective_cache_sizeを微調整するだけです。設定を変更するには、データベースパラメータグループを使用し、データベースインスタンスを再起動します。

ヒント: パフォーマンスを微調整する場合は、Amazon CloudWatchなどのサービスを使用してデータベースIOPSを監視し、設定を確認してください。

ヒント: 追加の支援が必要な場合は、PostgreSQLからプロフェッショナルサポートが提供されています。

ログローテーション

PostgreSQL Core Distributionの初期設定では、データベースのローカルログファイルに保持期間やファイルサイズの制限がありません。そのため、ログで消費されるディスク容量は徐々に増加していきます。

これを防ぐには、Syslogのlog_destinationへのリモートログ出力またはローカルのログローテーションについてパラメータを設定します。

ログファイルは、保持期間の制限、ファイルサイズの制限、またはその両方 (先に達した方) に基づいてローテーションされます。制限に達した場合は、その時点でファイル名のパターンに一致するログファイルが存在するかどうかに応じて、PostgreSQLでは、新しいファイルが作成されるか、既存のファイルが再利用されます。再利用の場合は、追記するか (保持期間の制限の場合は) 上書きすることができます。

ログローテーションのパラメータは次のとおりです。

- logging_collector:データベースのログ出力を有効にするには、「on」を入力します。
- log_filename:ログファイル名のパターン。ほとんどの場合、パターンではIEEE標準の日時形式が使用されます。
- log_truncate_on_rotation:既存ログファイルに追記する場合は「off」、既存のログファイルを上書きする場合は「on」を入力します。適用されるのは、時間ベースのログローテーションが発生した場合のみです(ファイルサイズベースのログローテーションでは、常に追記されます)。

- log_rotation_age: ログファイルの最大保持期間 (分)。「0」を入力すると、時間ベースのログローテーションが無効になります。
- log_rotation_size: ログファイルの最大サイズ (KB)。「0」を入力すると、ファイルサイズベースのログローテーションが無効になります。

例:日単位のデータベースのログローテーション

以下のパラメータを使用して、ローテーションしたデータベースログファイルを7つ作成します。つまり、ファイルは各曜日に1つずつ作成されます(たとえば、月曜日のファイル名は「postgresql-Mon.log」となります)。

1日 (1440分) ごとに、その曜日の名前が付いたファイルを作成するか (ファイルが存在しない場合)、その前の週で使用されたその曜日のログファイルを上書きします。

負荷が高い状況では、ファイルサイズの制限が無効になるため、ログ出力が「割り当てられたディスク容量を一時的に超過する」ことがあります。ただし、ファイルの数や名前は変更されません。

```
log_collector = on
log_filename = 'postgresql-%a.log'
log_rotation_age = 1440
log_rotation_size = 0
log_truncate_on_rotation = on
```

ロック管理

deadlock_timeoutの値を大きくすると、現在の環境で設定されている通常のトランザクション時間を超過することができます。

クエリによるロックの待機時間がdeadlock_timeoutの値を超えるたびに、PostgreSQLはデッドロック状態を確認し、(設定されている場合は) エラーを記録します。ところが、負荷の高い大規模環境では、多くの場合、待機時間が1秒を超えることは正常です (エラーではありません)。こうした正常なイベントが記録されると、パフォーマンスは低下します。

最大同時接続数

max_connections = 500に引き上げてください。

有効キャッシュサイズ

有効キャッシュサイズ (effective_cache_size) の値を大きくすることを検討してください。この設定は、クエリによりキャッシュの効果を推定するために使用されます。これは、クエリ計画中のコスト見積もりにのみ影響し、RAMの使用量が増加することはありません。

共有バッファ

shared_buffersの値をRAMの25%まで引き上げてください。この設定では、PostgreSQLがデータのキャッシュに使用できるメモリ容量を指定します。これによりパフォーマンスが向上します。

ワークメモリとメンテナンスワークメモリ

work_memの値を大きくしてください。この設定では、一時ディスクファイルへの書き込み前に、内部ソート操作とハッシュテーブルで使用できるRAMのサイズを指定します。複雑なクエリを実行する場合は、多くのメモリが必要になります。

maintenance_work_memの値を大きくすることを検討してください。この設定では、ALTER TABLEなどのメンテナンス操作に使用される最大メモリ容量を決定します。

チェックポイント

チェックポイントの作成頻度を減らしてください。通常は、チェックポイントにより、データファイルへの書き込みのほとんどが行われます。パフォーマンスを最適化するには、大半のチェックポイントを「requested」(使用可能なすべてのWALセグメントを入力することによるトリガ、または明示的なCHECKPOINTコマンドによるトリガ) ではなく、「timed」(checkpoint_timeoutによるトリガ) にする必要があります。

パラメータ名	推奨値
checkpoint_timeout	15min
checkpoint_completion_target	0.9
max_wal_size	16GB

ログ先行書き込み (WAL)

データベース複製を使用する場合は、wal_level = replicaを使用することを検討してください。

自動バキューム設定

PostgreSQLには、「バキューム」と呼ばれる定期的なメンテナンスが必要です。通常、autovacuum_max_workersの初期設定値を変更する必要はありません。

entitys および attribute2s 表で、頻繁な書き込みによって多くの行が頻繁に変更される場合(短時間のクラウドインスタンス), を使用する大規模な配置では、ディスク領域の使用を最小限に抑えてパフォーマンスを維持するために、自動バッファの実行頻度を増やす必要があります) 。パラメータはデータベース全体と特定のテーブルの両方に設定する必要があります。

データベースレベルのパラメータ名	推奨値
autovacuum_work_mem	1GB

テーブルレベルのパラメータ名	推奨値
autovacuum_vacuum_cost_delay	10
autovacuum_vacuum_scale_factor	0.01
autovacuum_analyze_scale_factor	0.005

データベースレベルの設定を変更するには、設定ファイルまたはデータベースパラメータグループを編集し、データベースサーバを再起動する必要があります。データベースが実行されている間、コマンドはその設定を変更できません。

テーブルレベルの設定を変更するには、設定ファイルまたはデータベースパラメータグループを編集するか、次のコマンドを入力します。

```
ALTER TABLE public.entitys SET (autovacuum_enabled = true, autovacuum_vacuum_cost_delay = 10, autovacuum_vacuum_scale_factor = 0.01, autovacuum_analyze_scale_factor = 0.005);
```

```
ALTER TABLE public.attribute2s SET (autovacuum_enabled = true, autovacuum_vacuum_cost_delay = 10, autovacuum_vacuum_scale_factor = 0.01, autovacuum_analyze_scale_factor = 0.005);
```

Linux版PostgreSQL

Transparent huge pages

Transparent Huge Pages (THP) は、RAMのサイズが大きいコンピュータでより大きなメモリページを使用することにより、Translation Lookaside Buffer (TLB) 検索のオーバーヘッドを削減するLinuxのメモリ管理システムです。初期設定ではTHPが有効になっていますが、PostgreSQLデータベースサーバには推奨されていません。この機能を無効にするには、OSベンダのドキュメントを参照してください。

ホストベース認証

ホストベース認証 (HBA) により、許可されたIPアドレスの範囲に含まれていないコンピュータからデータベースへの不正アクセスを防ぐことができます。Linuxの初期設定では、データベースに対するHBAの制限はありません。ただし、通常はセキュリティグループやファイアウォールを使用することをお勧めします。

Microsoft SQL Server Expressの管理

次のデータベース管理の推奨事項に従ってください。

- Deep Security Managerから不要なエージェントソフトウェアパッケージを削除して、データベースのディスク領域を節約してください。
- セキュリティのアップデートとイベントには、データベースに追加の容量が必要です。展開を監視して、Expressデータベースのサイズ制限内に収まるようにしてください。データベース削除の詳細については、"ログとイベントの保存に関するベストプラクティス" on page 1154を参照してください。また、Microsoftのサポートページ「SQL Serverにおける自動拡張および自動圧縮の構成に関する注意事項」に記載されているSQL Server設定を使用することもできます。

Microsoft SQL Server Expressからエンタープライズへの移行

Microsoft SQL Server Expressは非常に限られた環境でのみサポートされます("Microsoft SQL Server Expressに関する注意事項" on page 453 の詳細については、).を参照してください) 。Microsoft SQL Server Expressデータベースを使用していても制限がある場合は、Microsoft SQL Server Enterprise Edition、または でサポートされる別のデータベースに移行できます。

エンタープライズに移行するには

1. Deep Security Managerサービスを終了して、データベースへの書き込みを停止します。

   Deep Security Agentは、マネージャが停止している間も引き続き現在の保護ポリシーを適用します。Deep Security Managerがオンラインに戻ると、イベントは保持され、送信されます。

2. データベースをバックアップします。

3. 次のデータベース接続設定ファイルをバックアップします。

   ```
   [Deep Securityのインストールディレクトリ]/webclient/webapps/ROOT/WEB-INF/dsm.properties
   ```

4. データベースを新しいデータベースエンジンに移動します。バックアップを復元します。

5. 移行後のデータベースに接続するよう、dsm.propertiesを編集します。

   ```
   database.SqlServer.user
   database.name
   database.SqlServer.instance
   database.SqlServer.password
   database.type
   database.SqlServer.server
   ```

   初期設定のインスタンスを使用している場合は、database.SqlServer.instance設定を削除できます。

   database.SqlServer.passwordのプレーンテキストパスワードを入力できます。Deep Security Managerは、サービスの開始時に次のように暗号化します。

   ```
   database.SqlServer.password=!CRYPT!20DE3D96312D6803A53C0D1C691FE6DEB7476104C0A
   ```

6. Deep Security Managerサービスを再起動します。

7. データベースに正常に再接続したことを確認するには、Deep Security Managerにログインします。

   既存の保護対象のコンピュータとイベントログが表示されます。管理者のログインやポリシーの変更などの新しいイベントが発生すると、それらのイベントが追加されます。再接続できない場合は、データベースユーザアカウントに新しいデータベースサーバに対する権限が付与されていることを確認してください。

データベースのバックアップと復元

高可用性やロードバランシングとは別に、ベストプラクティスとして、定期的なデータベースのバックアップや障害復旧プランがあります。バックアップは、重大な障害が発生した場合にデータベースを復元するために使用できます。

データベースをバックアップする

データベースのバックアップ方法については、データベースベンダのドキュメントを参照してください。

ヒント: RDSについては、AWSによって提供されている、データベースをS3バケットにバックアップする手順を参照してください。たとえば、「Amazon RDS for SQL Server - Support for Native Backup/Restore to Amazon S3」を参照してください。

ヒント: PostgreSQLデータベースの場合、pg_dumpやpg_basebackupのような基本的なツールは、エンタープライズ環境でのバックアップと復元には適していません。Barmanなど、別のツールの使用を検討してください。

データベースのみを復元する

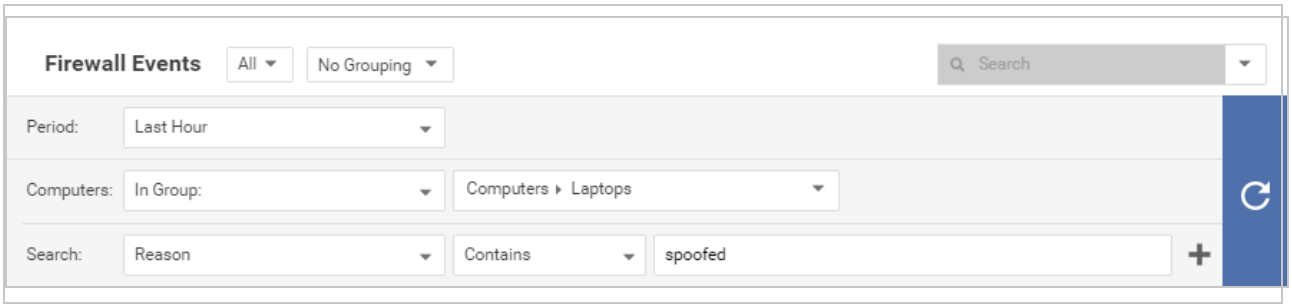
1. Deep Security Managerサービスを停止します。
2. データベースを復元します。
   Deep Security Managerの同じバージョン番号のデータベースである必要があります。
3. Deep Security Managerサービスを開始します。
4. データベースが復元されたことを確認します。
5. 適切な設定が行われるように、すべてのコンピュータをアップデートします。

Deep Security Managerとデータベースの両方を復元します。

1. 紛失または破損したDeep Security Managerの残りをすべて削除します。Deep Security Managerをアンインストールするときは、構成ファイルを保持することを選択しないでください。
2. データベースを復元します。
3. データベースをサポートするDeepSecurity Managerインストーラーのバージョンを見つけて、インストールします。インストール中に、[データベース]オプションで、[新しいマネージャーノードの追加]オプションを選択します。
4. Deep Security Managerを正常にインストールした後、Deep Security Managerコンソールを開き、[管理]> [マネージャーノード]に移動し、古いオフラインマネージャーノードを廃止します。

オブジェクトをXML形式またはCSV形式でエクスポートする

- イベント: いずれかの[イベント]画面に進み、[詳細検索]オプションを使用してイベントデータをフィルタします。たとえば、「理由」列に「spoofed」という語が含まれる、過去1時間以内にログに記録された、「コンピュータ > Laptops」コンピュータグループ内のコンピュータのすべてのファイアウォールイベントを検索できます。



右矢印の付いた送信ボタンをクリックして「クエリ」を実行します。次に、[エクスポート]をクリックして、フィルタしたデータをCSV形式でエクスポートします。表示されているすべてのエントリをエクスポートすることも、選択したデータだけをエクスポートすることもできます。この形式でのログのエクスポートは、主にサードパーティのレポートツールとの統合のために行います。

- コンピュータリスト: コンピュータリストは、[コンピュータ]画面からXML形式またはCSV形式でエクスポートできます。単一のDeep Security Managerから多数のコンピュータを管理しており、2台目のDeep Security Managerを設定してコンピュータの集合を管理することを計画している場合は、この処理を実行することもできます。選択したコンピュータのリストをエクスポートすると、すべてのコンピュータを再検出してグループ分けする手間が省けます。

  注意: ポリシー、ファイアウォールルール、侵入防御ルールの設定は含まれません。ファイアウォールルール、侵入防御ルール、ファイアウォールステートフル設定、およびポリシーをエクスポートしてから、コンピュータに再適用する必要があります。

- ポリシー: XML形式でエクスポートするには、[ポリシー]を選択します。

  注意: 選択したポリシーをXMLにエクスポートすると、子ポリシー(存在する場合)もエクスポートパッケージに追加されます。エクスポートパッケージには、ポリシーに関連する実際のオブジェクトがすべて格納されます。ただし、侵入防御ルール、セキュリティログ監視ルール、変更監視ルール、およびアプリケーションの種類は含まれません。

- ファイアウォールルール: ファイアウォールルールは、上記と同じ検索およびフィルタ方法を使用してXMLファイルまたはCSVファイルにエクスポートできます。
- ファイアウォールステートフル設定: ファイアウォールステートフル設定は、上記と同じ検索およびフィルタ方法を使用してXMLファイルまたはCSVファイルにエクスポートできます。
- 侵入防御ルール: 侵入防御ルールは、上記と同じ検索およびフィルタ方法を使用してXMLファイルまたはCSVファイルにエクスポートできます。
- 変更監視ルール: 変更監視ルールは、上記と同じ検索およびフィルタ方法を使用してXMLファイルまたはCSVファイルにエクスポートできます。
- セキュリティログ監視ルール: セキュリティログ監視ルールは、上記と同じ検索およびフィルタ方法を使用してXMLファイルまたはCSVファイルにエクスポートできます。
- その他の共通オブジェクト: 再利用可能なすべてのコンポーネントの共通オブジェクトは、同じ方法でXMLファイルまたはCSVファイルにエクスポートできます。

CSVにエクスポートする場合、表示されている列のデータのみが含まれます。表示するデータを変更するには、[列] ツールを使用します。グループは無視されるので、データの順序が画面と異なる場合があります。

オブジェクトをインポートする

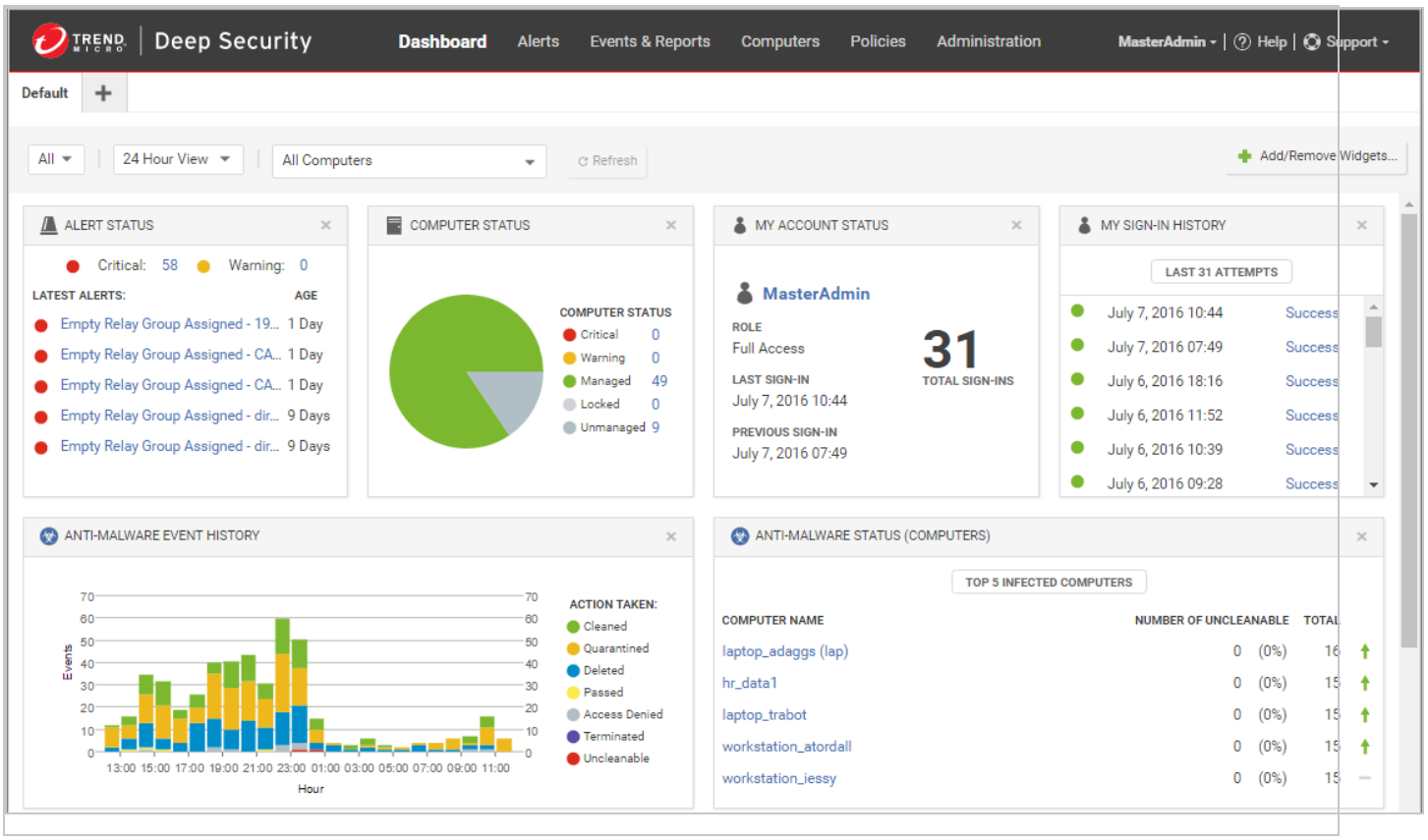
個々のオブジェクトのそれぞれをDeep Securityにインポートするには、オブジェクトページのツールバーで[新規]の横にある[Import From File]を選択します。

Deep Security Managerの移動とカスタマイズ

ダッシュボードのカスタマイズ

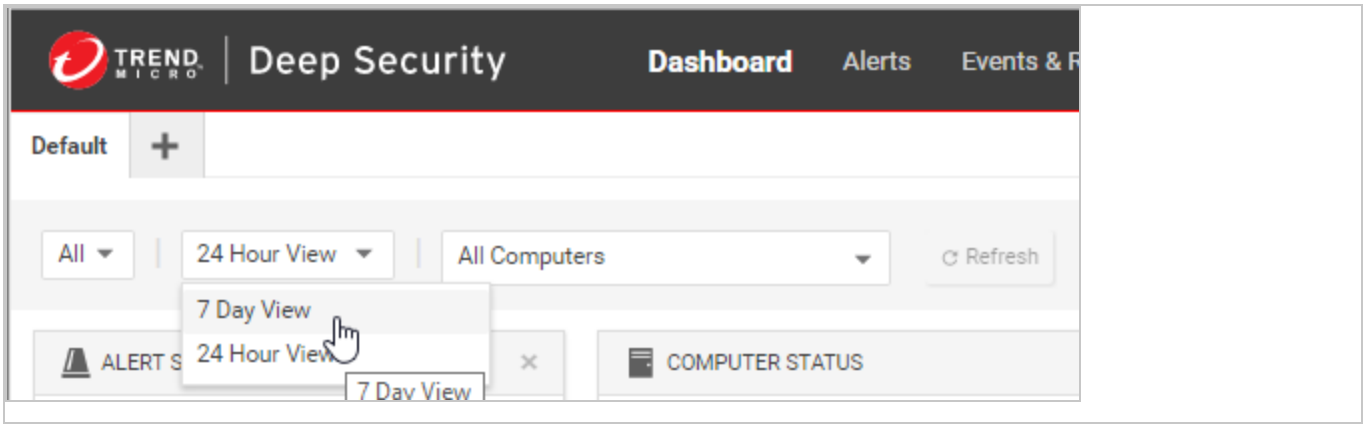
ダッシュボードは、Deep Security Managerにログオンした後に最初に表示されるページです。

ユーザは、ダッシュボードの内容とレイアウトを各自でカスタマイズできます。Deep Security Managerは自動的に設定を保存し、次回ログイン時にダッシュボードを覚えています。データの期間、および表示するコンピュータまたはコンピュータグループのデータも設定できます。



日時の範囲の指定

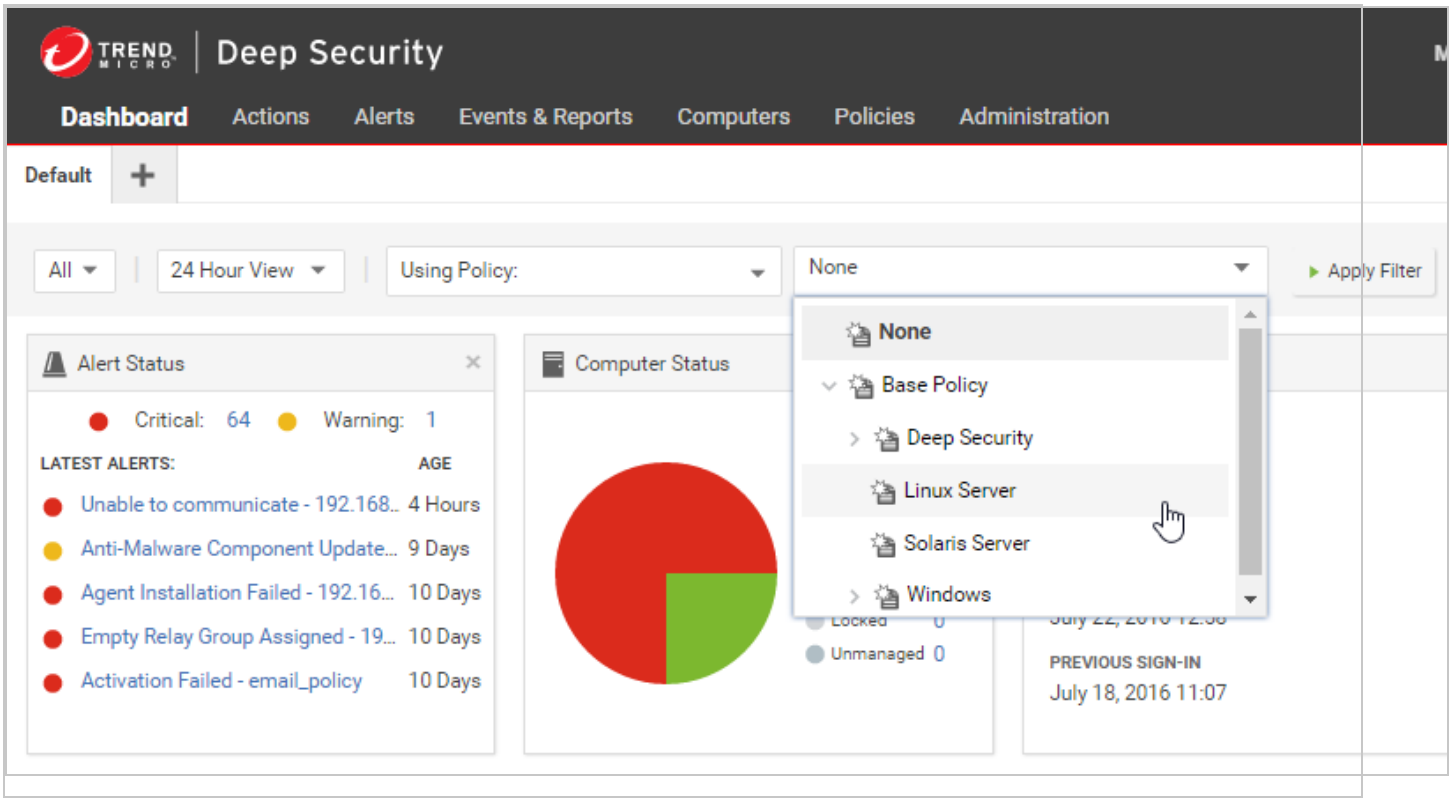
ダッシュボードには、次の図のように過去24時間または7日間のデータを表示できます。



コンピュータおよびコンピュータグループの指定

[コンピュータ] メニューを使用して、特定のコンピュータのデータのみが表示されるように表示データをフィルタします。たとえば、次の図のように「Linux Server」セキュリティポリシーを使用しているコンピュータの

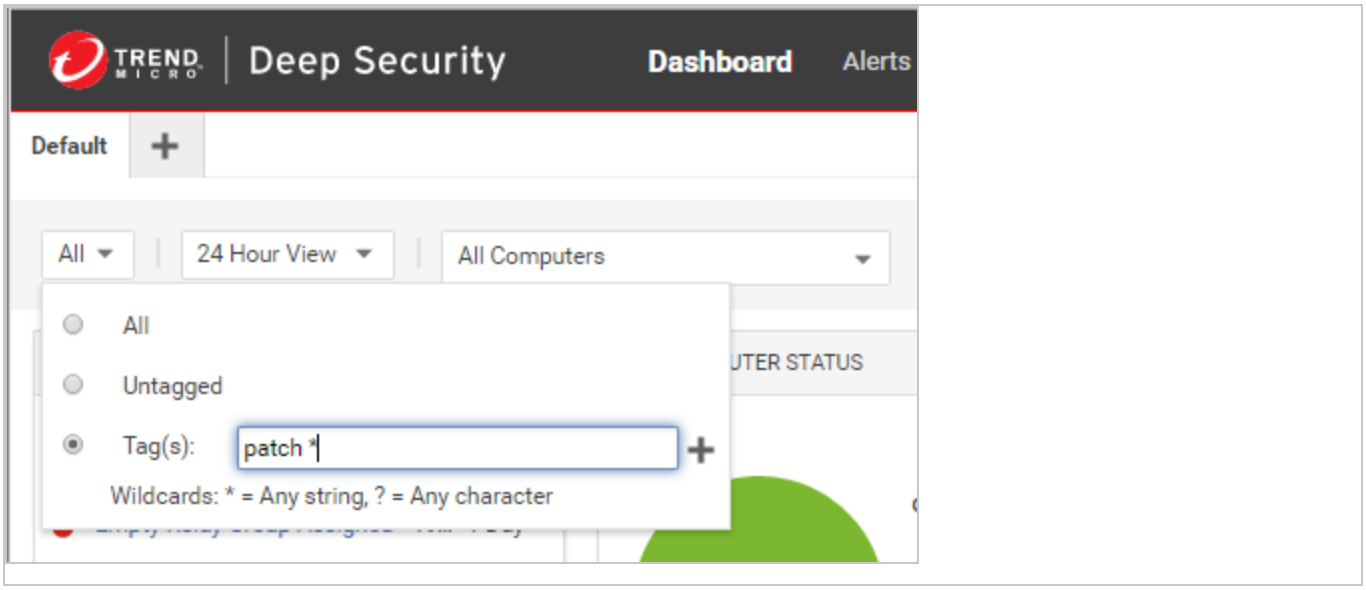
みを表示できます。



タグごとのフィルタ

Deep Securityでは、タグはメタデータの単位で、イベント自体に元々含まれていない追加の属性を作成するためにイベントに適用できます。タグを使用してイベントをフィルタし、イベントの監視と管理のタスクを簡素化できます。タグ付けの一般的な用途は、処理が必要なイベントと、調査の結果無害であることが判明したイベントを区別することです。

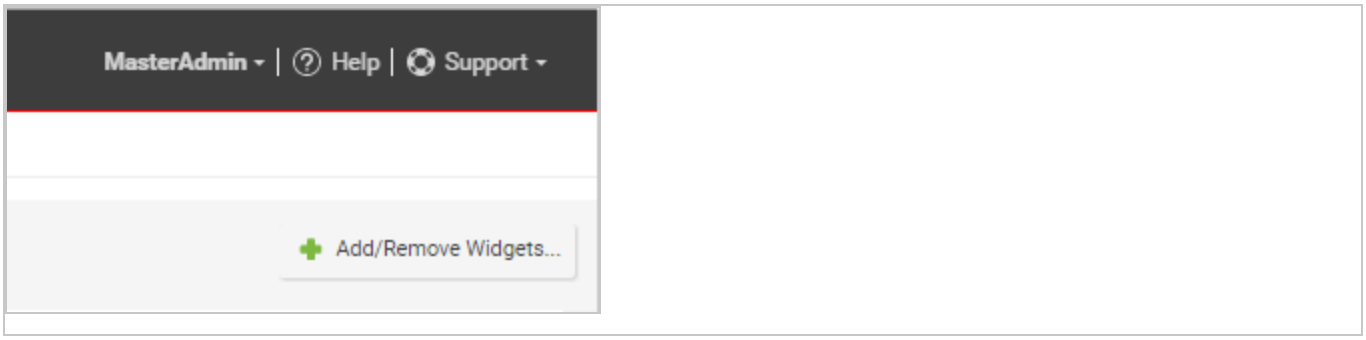
ダッシュボードに表示されるデータは、次の図のようにタグを使ってフィルタできます。



タグ付けの詳細については、"イベントを識別およびグループ化するためのタグの適用" on page 1161を参照してください。

ダッシュボードのウィジェットを選択する

次の図のように[ウィジェットの追加/削除]をクリックし、ウィジェットの選択画面を表示して、表示するウィジェットを選択します。



ウィジェットがダッシュボード上で1x1を超えるより大きなスペースを占める場合は、その寸法が名前の横に表示されます。

以下のウィジェットを使用できます。

監視:

- アクティビティ概要: 保護されている時間数やデータベースのサイズなど、アクティビティの概要。
- アラート履歴 [2x1]: 最近のアラート履歴を、アラートの重要度を含めて表示します。

- アラートステータス: 経過時間や重要度など、アラートの概要。
- コンピュータのステータス: コンピュータが管理対象であるか非管理対象であるかや、警告または重大なアラートがあるかどうかなど、コンピュータの概要。
- Managerノードのステータス [3x1]: Managerノード上の名前、CPU使用率、メモリ、ジョブ、およびシステムイベント。
- セキュリティアップデートのステータス: 最新の状態のコンピュータ、最新でない状態のコンピュータ、および不明なコンピュータの数など、コンピュータのアップデートのステータス。
- テナントのデータベース使用状況: データベースサイズによってランク付けされたテナントトップ5。
- テナントのジョブアクティビティ: ジョブの総数によってランク付けされたテナントトップ5。
- テナントの保護アクティビティ: 保護されている時間数でランク付けされたテナントトップ5。
- テナントのセキュリティイベントアクティビティ: セキュリティイベントの総数によってランク付けされたテナントトップ5。
- テナントのログオンアクティビティ: ログオンアクティビティによってランク付けされたテナントトップ5。
- テナントのシステムイベントアクティビティ: システムイベントの総数によってランク付けされたテナントトップ5。
- テナント: テナント数や保護されている時間数などのテナント情報。

ステータスが「不正プログラム対策設定がオフ」、「不正プログラム対策エンジニアがオフライン」、および「エージェントがオフライン」のコンピュータは、[旧版] カテゴリには含まれないことに注意してください。これらのステータスは、一般的な期限切れの分類とは分けられ、[最新ではありません (不正プログラム対策設定がオフ)] 、[最新ではありません (不正プログラム対策がオフライン)] 、および[最新ではありません (Agentがオフライン)]に個別に分類されます。これらのステータスのコンピュータは、[旧版] の [セキュリティアップデートのステータス] ウィジェットに表示される総数には含まれません。

システム:

- ログオン履歴: 過去50回のログオン試行と、それが成功したかどうか。
- ユーザ情報の概要 [2x1]: 名前、ロール、ログオン情報など、ユーザの概要。
- ソフトウェアアップデート: 最新の状態でないコンピュータ。
- システムイベント履歴 [2x1]: 最近のシステムイベント履歴を、情報、警告、またはエラーとして分類されているイベントの数を含めて表示します。

ランサムウェア:

- ランサムウェアイベント履歴 [3x1]: 最近のランサムウェアのイベント履歴を、イベントの種類を含めて表示します。

- ランサムウェアのステータス: 過去24時間、過去7日間、または過去13週間に発生したランサムウェアイベントの数など、ランサムウェアのステータス。

不正プログラム対策:

- 不正プログラム対策イベント履歴 [2x1]: 最近の不正プログラム対策イベントの履歴を、イベントに対して実行されたアクションを含めて表示します。
- 不正プログラム対策の保護ステータス: コンピュータが保護されているか、保護されていないか、保護不可能かなど、コンピュータに対する不正プログラム対策の保護ステータスの概要。
- 不正プログラム対策のステータス(コンピュータ) [2x1]: 感染コンピュータのトップ5を、駆除できなかったファイルの数と影響を受けたファイルの総数を含めて表示します。
- 不正プログラム対策のステータス(不正プログラム) [2x1]: 検出された不正プログラムのトップ5を、不正プログラムの名前、駆除できなかったファイルの数、およびそれがトリガされた回数を含めて表示します。
- 不正プログラム検索のステータス [2x1]: 不正プログラムの予約検索が不完全だったアプライアンスのトップ5。

Webレピュテーション:

- Webレピュテーションのコンピュータのアクティビティ: Webレピュテーションイベントのあるコンピュータのトップ5を、イベント数を含めて表示します。
- Webレピュテーションイベント履歴 [2x1]: 最近のWebレピュテーションイベント履歴を、イベントの重要度を含めて表示します。
- WebレピュテーションのURLのアクティビティ: WebレピュテーションイベントをトリガしたURLのトップ5を、それらがアクセスされた回数を含めて表示します。

ファイアウォール:

- ファイアウォールのアクティビティ(検出): パケットが検出された理由のトップ5を、回数を含めて表示します。
- ファイアウォールのアクティビティ(防御): パケットが防御された理由のトップ5を、回数を含めて表示します。
- ファイアウォールコンピュータのアクティビティ(検出): 検出されたファイアウォールイベントを生成したコンピュータのトップ5と、イベントの発生回数を表示します。
- ファイアウォールコンピュータのアクティビティ(防御): 防御されたファイアウォールイベントを生成したコンピュータのトップ5と、イベントの発生回数を表示します。

- ファイアウォールイベント履歴 [2x1]: 最近のファイアウォールイベント履歴を、イベントが検出または防御されたかどうかを含めて表示します。
- ファイアウォールIPのアクティビティ(検出): 検出されたファイアウォールイベントを生成した送信元IPのトップ5と、イベントの発生回数を表示します。
- ファイアウォールIPのアクティビティ(防御): 防御されたファイアウォールイベントを生成した送信元IPのトップ5と、イベントの発生回数を表示します。
- ファイアウォールポートのアクティビティ(検出): 検出されたファイアウォールイベントの送信先ポートのトップ5と、イベントの発生回数を表示します。
- ファイアウォールポートのアクティビティ(防御): 防御されたファイアウォールイベントを生成したコンピュータのトップ5と、イベントの発生回数を表示します。
- 攻撃の予兆検索のアクティビティ: 検出された攻撃の予兆検索のトップ5と、検索の発生回数を表示します。
- 攻撃の予兆検索のコンピュータ: 攻撃の予兆検索が発生したコンピュータのトップ5と、検索の発生回数を表示します。
- 攻撃の予兆 検索履歴 [2x1]: 最近実行された偵察検索の履歴を表示します。これには、実行された検索の種類も含まれます。

侵入防御:

- アプリケーションの種類のアクティビティ(検出): 検出されたアプリケーションの種類のトップ5を、トリガされた回数を含めて表示します。
- アプリケーションの種類のアクティビティ(防御): 防御されたアプリケーションの種類のトップ5を、トリガされた回数を含めて表示します。
- アプリケーションの種類のツリーマップ(検出) [2x2]: 検出されたアプリケーションの種類のマップを表示します。ボックスにポインタを合わせると、イベントの重要度、トリガされた回数、および各重要度の割合が表示されます。
- アプリケーションの種類のツリーマップ(防御) [2x2]: 防御されたアプリケーションの種類のマップを表示します。ボックスにポインタを合わせると、イベントの重要度、トリガされた回数、および各重要度の割合が表示されます。
- IPSのアクティビティ(検出): 侵入防御イベントが検出された理由のトップ5を、トリガされた回数を含めて表示します。
- IPSのアクティビティ(防御): 侵入防御イベントが防御された理由のトップ5を、トリガされた回数を含めて表示します。
- IPSコンピュータのアクティビティ(検出): 侵入防御イベントが検出されたコンピュータのトップ5を表示します。

- IPSコンピュータのアクティビティ(防御): 侵入防御イベントが防御されたコンピュータのトップ5を表示します。
- IPSイベント履歴 [2x1]: 最近の侵入防御イベント履歴を、イベントが検出または防御されたかどうかを含めて表示します。
- IPS IPのアクティビティ(検出): 検出された侵入防御イベントを生成した送信元IPのトップ5を表示します。
- IPS IPのアクティビティ(防御): 防御された侵入防御イベントを生成した送信元IPのトップ5を表示します。
- 最新のIPSのアクティビティ(検出): 最新のアップデート以降に侵入防御イベントが検出された理由のトップ5を表示します。
- 最新のIPSのアクティビティ(防御): 最新のアップデート以降に侵入防御イベントが防御された理由のトップ5を表示します。

変更監視:

- 変更監視のアクティビティ: 変更監視イベントが発生した理由のトップ5を、回数を含めて表示します。この場合、理由はトリガされたルールを示しています。
- 変更監視 コンピュータのアクティビティ: 変更監視イベントが発生したコンピュータのトップ5を、イベントの数を含めて表示します。
- 変更監視イベント履歴 [2x1]: 最近の変更監視イベント履歴を、イベントの重要度を含めて表示します。
- 変更監視 キーのアクティビティ: 変更監視イベントのキーのトップ5を表示します。キーのソースは、エンティティセットによって異なります。ファイルとディレクトリの場合はそのパスであり、ポートの場合は一意のプロトコル、IP、ポート番号、またはタプルです。

セキュリティログ監視:

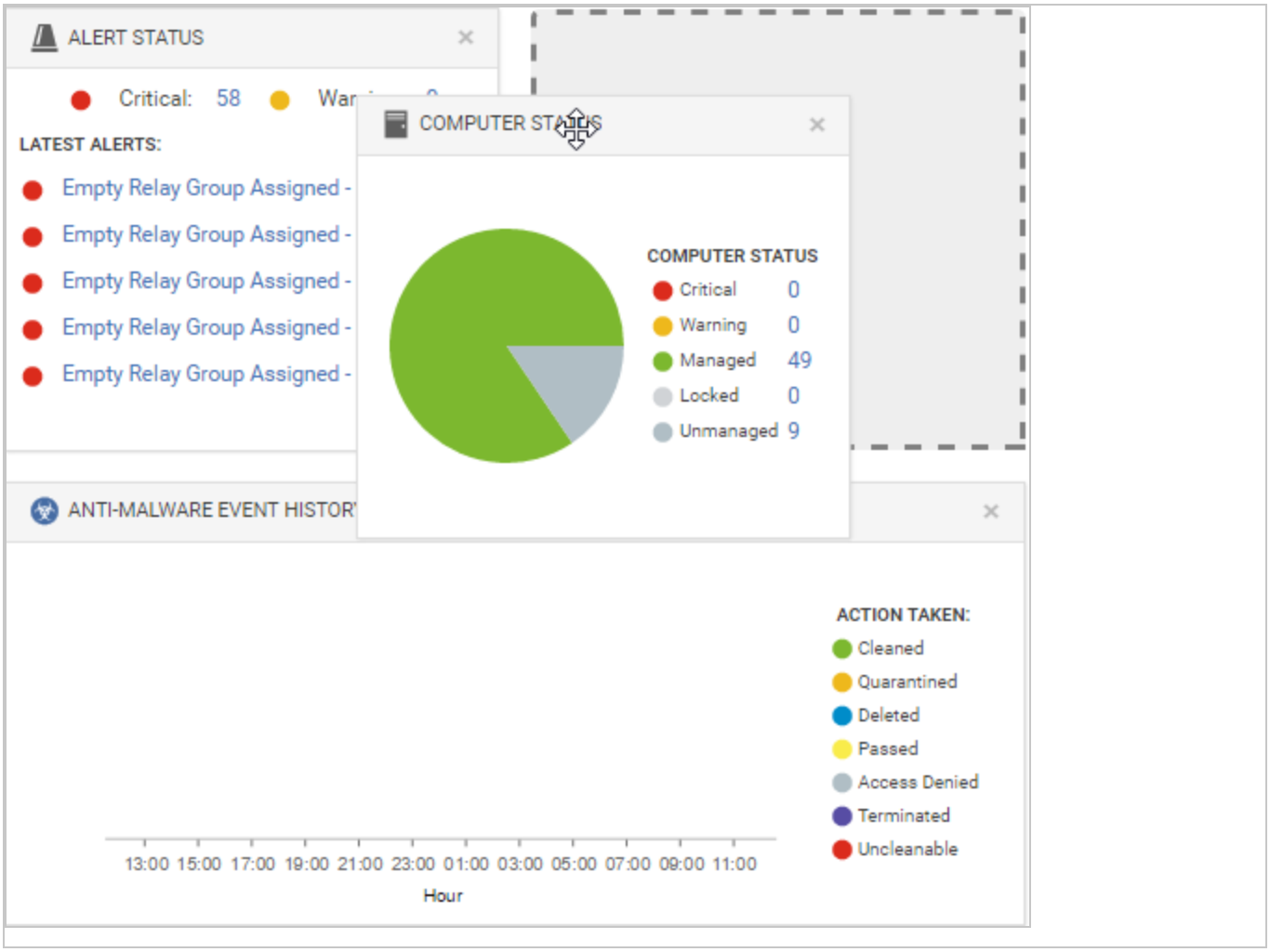
- セキュリティログ監視のアクティビティ: 変更監視イベントが発生した理由のトップ5を、数を含めて表示します。この場合、理由はトリガされたルールを示しています。
- セキュリティログ監視 コンピュータのアクティビティ: セキュリティログ監視イベントが発生したコンピュータのトップ5を、イベントの数を含めて表示します。
- セキュリティログ監視の説明のアクティビティ: セキュリティログ監視イベントの説明のトップ5を、イベントの発生回数を含めて表示します。説明は、トリガされたイベントを示します。
- セキュリティログ監視イベント履歴 [2x1]: 最近のセキュリティログ監視イベント履歴を、イベントの重要度を含めて表示します。

アプリケーションコントロール:

- アプリケーションコントロール メンテナンスモードのステータス [2x1]: メンテナンスモードのコンピュータを、モードの開始および終了時刻を含めて表示します。

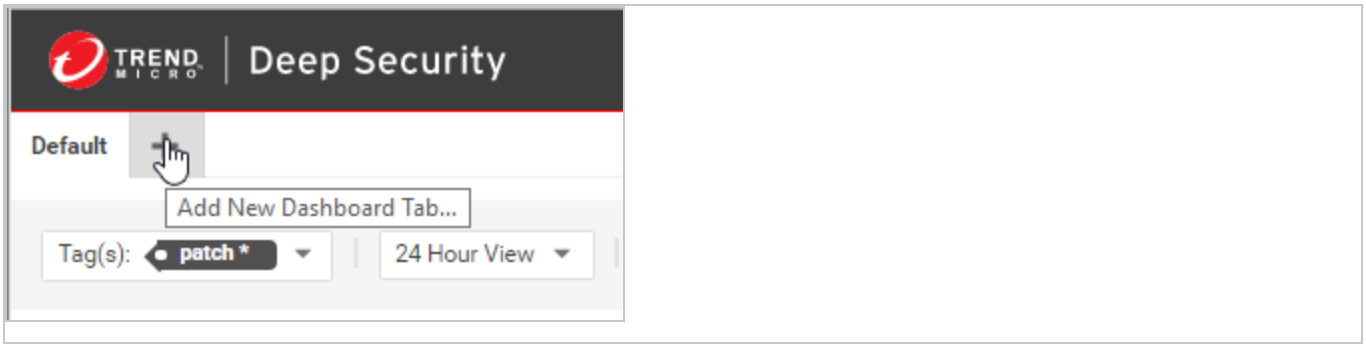
レイアウトを変更する

選択したウィジェットは、そのタイトルバーをドラッグすることによってダッシュボード上を移動できます。既存のウィジェットの上に選択したウィジェットを移動すると、それぞれのウィジェットの場所が入れ替わります (表示しようとしているウィジェットは、一時的にグレー表示になります)。



ダッシュボードのレイアウトを保存/管理する

複数のダッシュボードレイアウトを作成し、それぞれ別のタブとして保存できます。ログオフ後、ダッシュボードの設定とレイアウトを他のユーザが確認することはできません。新しいダッシュボードタブを作成するには、次の図のようにダッシュボードの右端のタブにある「+」記号をクリックします。



スマートフォルダによるコンピュータの動的なグループ化

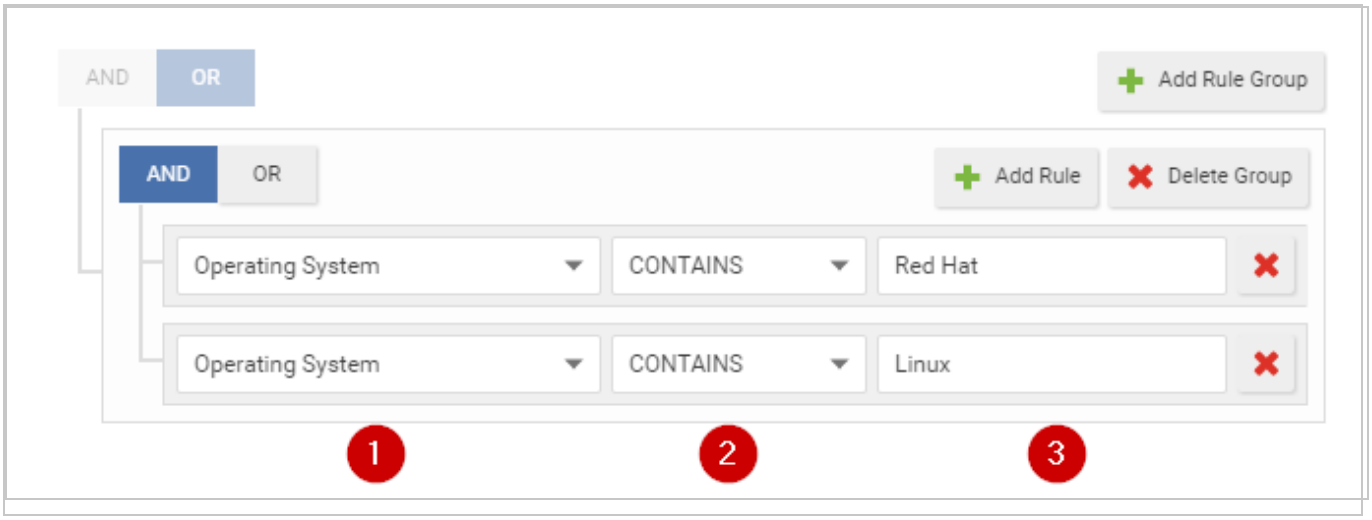
スマートフォルダはコンピュータの動的なグループで、保存した検索クエリで定義します。グループをクリックするたびに、一致するコンピュータが検索されます。コンピュータをOSやAWSプロジェクトタグなどの属性でグループ化して表示したい場合は、スマートフォルダを利用できます。

ヒント: リソースをプログラムで検索することを好む場合、Deep Security APIを使用してリソース検索を自動化できます。例については、Deep Security Automation Centerのリソース検索ガイドを参照してください。

スマートフォルダを作成するには、次の項目を定義します。

1. 検索対象のコンピュータのプロパティ(1)
2. 一致条件を定義する演算子 (2)

3. 検索する値 (3)



スマートフォルダを作成する

1. [コンピュータ]→[スマートフォルダ] の順に選択します。
2. [スマートフォルダの作成] をクリックします。

   初期設定の空の検索条件グループ (ルールグループ) が表示されます。最初にこのグループを設定する必要があります。追加または異なる一致条件を定義する必要がある場合は、後からルールグループを追加できます。
3. スマートフォルダの名前を入力します。
4. 最初のドロップダウンリストで、一致するすべてのコンピュータが持つプロパティ(OS) を選択します。("検索可能なプロパティ" on page 1599を参照)。

   AWS タグ、Azure タグ、またはGCP ラベルを選択した場合は、タグの名前またはラベルキーも入力します。
5. 完全一致、類似、または一致しないコンピュータを選択する演算子を選択します ([次の文字列を含む] など)。

   注意: 一部の演算子はすべてのプロパティには使用できません。
6. 検索語句のすべてまたは一部を入力します。

   注意: ワイルドカード文字はサポートされていません。

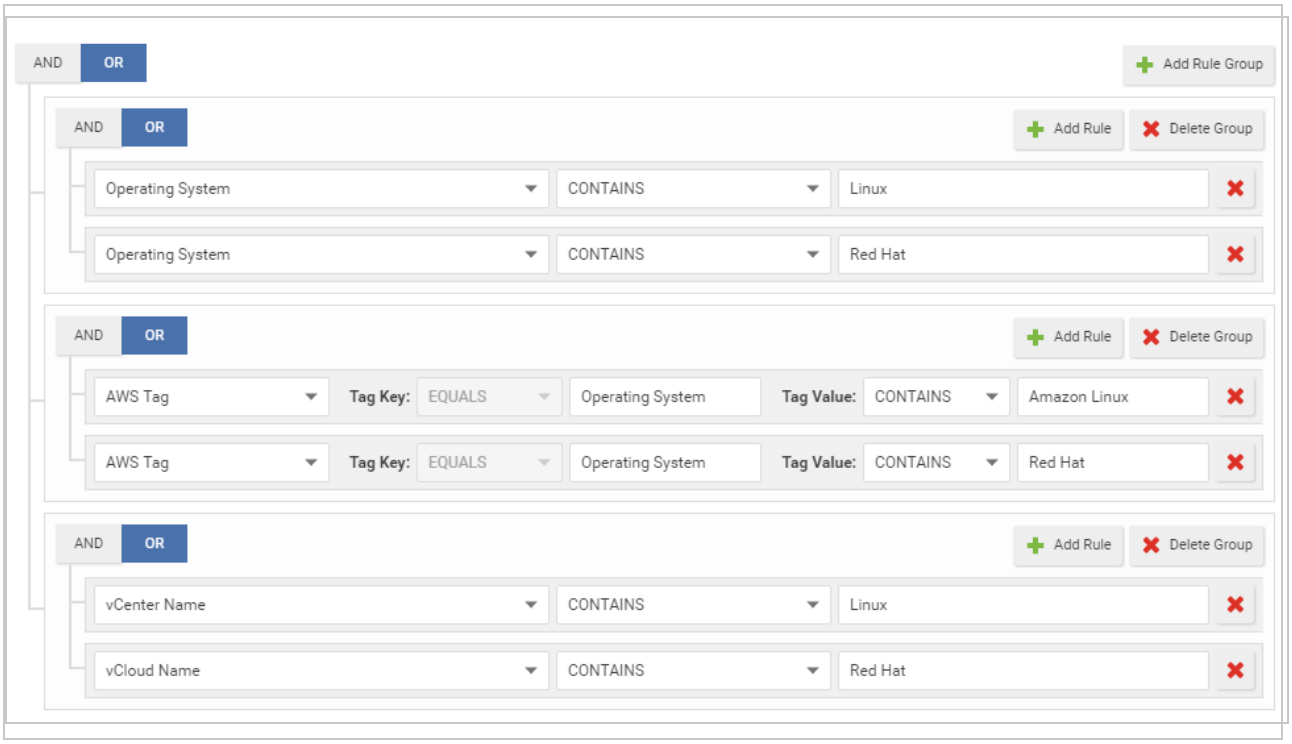
ヒント: 複数の単語を入力した場合、それぞれの単語が個別に比較されるのではなく、*1*つのフレーズとして比較されます。プロパティの値に別の順序の単語が含まれている場合や、一部の単語しか含まれていない場合は、一致しません。
いずれかの単語に一致させるには、[ルールの追加] と[または] をクリックして、別の値を追加します (1つのルールに1つの単語)。

7. コンピュータが複数のプロパティに一致する必要がある場合は、[ルールの追加] と[および] をクリックします。手順4 ~ 6を繰り返します。

   さらに複雑なスマートフォルダを作成するには、複数の検索条件を連結します。[グループの追加] をクリックし、[および] または [または] をクリックします。Repeat steps 4-7.

   たとえば、Linuxコンピュータをオンプレミスと AWSやvCloudなどのクラウドの両方に配置しているとします。次の条件に基づく3つのルールグループを使用して、それらのコンピュータをすべて含むスマートフォルダを作成できます。

   a. ローカルの物理コンピュータのOS
   b. AWSタグ
   c. vCenterまたはvCloud名



ヒント: スマートフォルダを保存する前にクエリの結果をテストするには、[プレビュー] をクリックします。

8. [保存] をクリックします。
9. 確認するため、新しいスマートフォルダをクリックします。想定するコンピュータがすべて含まれていることを確認します。

ヒント: スマートフォルダの処理速度を上げるには、不要なAND演算を削除し、サブフォルダの階層を減らします。クエリが複雑なほどパフォーマンスは低下します。

また、クエリに一致すべきでないコンピュータが除外されていることも確認してください。スマートフォルダのクエリを編集する必要がある場合は、そのスマートフォルダをダブルクリックします。

注意: アカウントの役割に権限がない場合は、一部のコンピュータが表示されないか、またはコンピュータのプロパティを編集できません。詳細については、"ユーザロールの定義" on page 1541を参照してください。

スマートフォルダを編集する

スマートフォルダのクエリを編集する必要がある場合は、そのスマートフォルダをダブルクリックします。

検索条件のルールまたはルールグループを並べ替えるには、ルールまたはグループにカーソルを合わせ、カーソルが✥に変わったら、ルールまたはグループを目的の位置までドラッグします。

スマートフォルダのクローンを作成する

既存のスマートフォルダを新しいスマートフォルダのテンプレートとして複製および変更するには、元のスマートフォルダを右クリックして [スマートフォルダの複製] を選択します。

サブフォルダを使用して検索を絞り込む

サブフォルダを使用して、スマートフォルダの検索結果を絞り込むことができます。

スマートフォルダは、10階層までネストできます。

- スマートフォルダ1
  - サブフォルダ2
    - サブフォルダ3 ...(以下同様)

たとえば、すべてのWindowsコンピュータを対象としたスマートフォルダがあり、32ビットまたは64ビットのWindows 7を実行するコンピュータに絞り込みたいとします。そのためには、親である「Windows」フォルダの下にWindows 7用の子スマートフォルダを作成します。次に、その「Windows 7」フォルダの下に2つの子スマートフォルダ(「32ビット」と「64ビット」)を作成します。



1. スマートフォルダを右クリックし、[子スマートフォルダの作成]を選択します。
2. 子スマートフォルダのクエリグループまたはルールを編集します。[保存]をクリックします。
3. 新しいスマートフォルダをクリックします。想定するコンピュータがすべて含まれていることを確認します。また、クエリに一致すべきでないコンピュータが除外されていることも確認してください。

サブフォルダを自動作成する

注意: AWS、Azure、およびGCPコンピューターにのみ適用されます。

子フォルダーを手動で作成する代わりに、Amazon EC2インスタンス、Amazon Workspace、Azure VM、またはGCP VMインスタンスに割り当てられたAWSタグ、Azureタグ、またはGCPラベルの値ごとにサブフォルダーを自動的に作成できます。コンピューターにタグ/ラベルを適用する方法については、クラウドプロバイダーのドキュメントを参照してください。

- Amazon: AmazonEC2リソースにタグを付ける, タグWorkSpacesリソース
- Azure: タグを使用してAzureリソースと管理階層を整理する
- GCP: ラベリングリソース。

注意: タグ/ラベルベースのサブフォルダーは、親フォルダーの下に手動で作成された既存の子フォルダーを置き換えます。

1. Deep Security Managerで、スマートフォルダを右クリックして、[スマートフォルダのプロパティ]を選択します。
2. メイン画面の下部で、特定のタグまたはラベルキーの値ごとにサブフォルダを自動的に作成するチェックボックスをオンにします。
3. AWS、Azure、またはGCPクラウドベンダーのいずれかを選択します。

4. AWSタグ、Azureタグ、またはGCPラベルキーの名前を入力します。タグまたはラベルの値ごとにサブフォルダーが自動的に作成されます。
5. [Save] をクリックします。

ヒント: タグまたはラベルの値が使用されなくなった場合、空のサブフォルダーが表示されることがあります。これをを削除するには、スマートフォルダを右クリックし、スマートフォルダの同期を選択します。

検索可能なプロパティ

プロパティとは、検索する一部またはすべてのコンピュータが持つ属性です。スマートフォルダには、選択したプロパティがあり、その値が一致するコンピュータが表示されます。

注意: *Deep Security Managerにそのプロパティが表示されたときに正確に*検索を入力します。たとえば、vCenter/AWS/Azure/GCPでは使用できません。値が正確でないとスマートフォルダのクエリは一致しません。
プロパティの正確な値を確認するには、(特に指定のないかぎり) [コンピュータ] に進み、左側のナビゲーションペインを確認します。

一般

プロパティ	説明	データタイプ	例
ホスト名	コンピュータのホスト名です。[コンピュータ]→[詳細] の [ホスト名] に表示されます。	文字列	ca-staging-web1
コンピュータの表示名	Deep Securityでのコンピュータの表示名(存在する場合)です。[コンピュータ]→[詳細] の [表示名] に表示されます。	文字列	nginxTest
フォルダ名	コンピュータに割り当てられているグループです。	文字列	US-East
OS	コンピュータのOSです。[コンピュータ]→[詳細] の [プラットフォーム] に表示されます。	文字列	Microsoft Windows 7 (64ビット) Service Pack 1 Build 7601
IPアドレス	コンピュータのIPアドレスです。 Deep Security ManagerでIPアドレスを見つけることができます。各IPを見つける	IPv4/IPv6アドレス、またはIPv4範囲	172.20.1.5-172.20.1.55 2001:db8:face::5

プロパティ	説明	データタイプ	例
	方法は次のとおりです。 • Add > Add AWS | Azure | GCP Accountを通じてDeep Securityに追加されたAWSインスタンス、GCP VM、またはAzure VM、コンピュータの詳細ページ、および一般タブで、仮想マシンの概要セクションまでスクロールします。AWS IPアドレスは次のフィールドで確認できます。 • プライベートIPアドレス • パブリックIP (PIP) アドレス 注意: AWS、GCP、またはAzureコンピュータをAdd> Add Computersで追加した場合、IPアドレスは物理コンピュータの同じ場所に配置されます。 • 物理コンピュータを選択し、コンピュータの詳細ページに移動し、左側のメニューで[インタフェース]をクリックします。 注意: 静的IPアドレスではなく「DHCP」と表示される場合は、スマートフォルダのクエリに一致しません。 • vCenterまたはvCloud仮想マシン: vCenterコンピュータの詳細画面に移動し、[一般] タブで [仮想マシンの概要] セクションまでスクロールします。vCenterまたはvCloudのIPアドレスは [IPアドレス] フィールドに表		

プロパティ	説明	データタイプ	例
	示されます。		
ポリシー	コンピュータに割り当てられているDeep Securityポリシーです。[コンピュータ]→[詳細] に表示されます。	文字列 (ドロップダウンリストのオプション)	ベースポリシー
有効化済み	コンピュータがDeep Security Managerで有効化されているかどうかを示します。[コンピュータ]→[詳細] に表示されます。	ブール	○
Dockerホスト	コンピュータにDockerがインストールされているかどうかを示します。[コンピュータ]→[詳細] に表示されます。	ブール	×
コンピュータの種類	コンピュータの種類です。: 物理コンピュータ、Amazon EC2インスタンス、Amazon WorkSpace、vCenter VM、Azureインスタンス、Azure ARMインスタンス、GCP VMインスタンスなどがあります。	文字列 (ドロップダウンリストのオプション)	例: 物理コンピュータ、Amazon EC2インスタンス
前回成功した推奨設定の検索	指定した時間内にコンピュータで推奨設定の検索に成功したかどうかを示します。[コンピュータ]→[詳細]→[一般]→[侵入防御] または [変更監視] または [セキュリティログ監視]→[推奨設定] には、前回の推奨設定の検索の日付および結果が表示されます。	日付演算子ドロップダウンリスト、文字列、日付単位ドロップダウンリスト	次の期間より古い、7、日
Agentの前回の通信	指定した期間内にAgentがDeep Security Managerと通信したかどうかを示します。前回の通信日は、[コンピュータ]→[詳細]→[一般]→[前回の通信] に表示されます。	日付演算子ドロップダウンリスト、文字列、日付単位ドロップダウンリスト	次の期間より古い、3、日
オフラインのAgent	Agentがオフラインかどうかを示します。これは、[コンピュータ]→[詳細]→[一般]→[前回の通信] に [管理対象 (オフライン)] または [オフライン] として表示されます。	ブール	○

プロパティ	説明	データタイプ	例
タスク	Computersページのタスクの列に表示されるコンピュータのタスクの状態。考えられるすべてのタスクのリストについては、"コンピュータおよびAgentのステータス" on page 1476を参照してください。	文字列	有効化中
ホスト作成日	そのコンピュータがDeep Security Managerに追加された日付です。	文字列 (日付)	2019/03/15
Version	Deep Security Agentのバージョン。	文字列	12.0.0.1

AWS

プロパティ	説明	データタイプ	例
タグ	コンピュータのAWSタグのキー:値のペアです。[コンピュータ]→[詳細]→[概要]→[一般] の [仮想マシンの概要] の下の [クラウドインスタンスのメタデータ] に表示されます。 タグ名とその値を入力します。大文字と小文字が区別されます。	文字列	タグキー: env タグ値: staging
セキュリティグループ名	コンピュータに関連付けられているAWSセキュリティグループ名です。[コンピュータ]→[詳細]→[概要]→[一般] の [仮想マシンの概要] の下の [セキュリティグループ] に表示されます。	文字列	SecGrp1
セキュリティグループID	コンピュータのAWSセキュリティグループIDです。[コンピュータ]→[詳細]→[概要]→[一般] の [仮想マシンの概要] の下の [セキュリティグループ] に表示されます。	文字列	sg-12345678
AMI ID	コンピュータのAmazon Machine AMI IDです。[コンピュータ]→[詳細]→[概要]→[一般] の [仮想マシンの概要] の下の [AMI ID] に表示されます。	文字列	ami-23c44a56
アカウントID	コンピュータに関連付けられている12桁のAWSアカウントIDです。[コンピュータ] の [Amazonアカウント] を右クリックし、[プロパティ] を選択すると表示されます。	文字列	123456789012

プロパティ	説明	データタイプ	例
	コンピュータはサブフォルダに分けて表示されます。		
アカウント名	コンピュータに関連付けられているAWSアカウントのエイリアスです。[コンピュータ] の [AWSクラウドコネクタ] を右クリックし、[プロパティ] を選択すると表示されます。 コンピュータはサブフォルダに分けて表示されます。	文字列	MyAccount-123
リージョンID	コンピュータのAWSリージョン接尾辞です。 コンピュータはサブフォルダに分けて表示されます。	文字列	us-east-1
リージョン名	コンピュータに関連付けられているAWSリージョン名です。 コンピュータはサブフォルダに分けて表示されます。	文字列	米国東部 (オハイオ)
VPC ID	コンピュータのVirtual Private Cloud (VPC) IDです。 エイリアスがある場合はフォルダ名にはエイリアスが使用され、VPC IDはカッコ内に表示されます。エイリアスがない場合は、VPC IDがフォルダ名になります。 コンピュータはサブフォルダに分けて表示されます。	文字列	vpc-3005e48a
サブネットID	コンピュータに関連付けられているVirtual Private Cloud (VPC) サブネットIDです。 エイリアスがある場合はフォルダ名にはエイリアスが使用されVPCサブネットIDはカッコ内に表示されます。エイリアスがない場合は、VPCサブネットIDがフォルダ名になります。 コンピュータはサブフォルダに分けて表示されます。	文字列	subnet-b1c2e468
ディレクトリID	Amazon WorkSpacesに関連付けられたユーザエントリがあるAWSディレクトリのIDです。ディレクトリIDは [コンピュータ]→[詳細]→[仮想マシンの概要] の [WorkSpaceディレクトリ] フィールドに表示されます。	文字列	d-9367232d89

プロパティ	説明	データタイプ	例
	フィールドの形式は<directory_alias>(<directory_ID>) です。例: myworkspacedir(d-9367232d89)		

Azure

プロパティ	説明	データタイプ	例
サブスクリプション名	注意: Deep Security Manager 12.0以降、Subscription名は収集されなくなりました。情報が以前のバージョンのManagerの。から取得された場合、プロパティのドロップダウンリストに残ります。 コンピュータに関連付けられているAzureサブスクリプションアカウントIDです。[コンピュータ] の [Azure] を右クリックし、[プロパティ] を選択すると表示されます。 コンピュータはサブフォルダに分けて表示されます。	文字列	MyAzureAccount
リソースグループ	コンピュータに関連付けられているリソースグループです。	文字列	MyResourceGroup
地域	コンピューターの場所の名前	文字列	米国東部
タグ	コンピューターのAzureタグのキーと値のペア。コンピューター>詳細>概要> クラウドインスタンスメタデータの仮想マシンの概要の下にある一般的な。 タグ名とその値を入力します。大文字と小文字が区別されます。	文字列	タグキー: env タグ値 : ステージング

GCP

プロパティ	説明	データタイプ	例
ラベル	コンピュータのGCPのラベルキー: 値のペア、クラウドインスタンスのメタデータには、仮想マシンのサマリの下 コンピュータ > 詳細 > 概要 > 一般に見られるように。 ラベルキーとその値を入力します。大文字と小文字が区別されます。	文字列	ラベルキー: env ラベル値 : ステージング
ネットワークタグ	コンピュータのネットワークタグには、コンピュータ>詳細>概要>一般に見られるように仮想マシンの下を概要、クラウドインスタンスのメタデータを参照してください。	文字列	生産

vCenter

プロパティ	説明	データタイプ	例
名前	コンピュータに関連付けられているvCenterです。 コンピュータはサブフォルダに分けて表示されます。	文字列	vCenter - lab13-vc.example.com
データセンター	コンピュータに関連付けられているvCenterデータセンターです。 コンピュータはサブフォルダに分けて表示されます。	文字列	lab13-datacenter
フォルダ	コンピュータのvCenterフォルダです。 コンピュータはサブフォルダに分けて表示されます。	文字列	db_dev
親ESXのホスト名	コンピュータのゲスト仮想マシンが実行されているESXiハイパーバイザのホスト名です。[コンピュータ] に表示されます。	文字列	lab13-esx2.example.com
カスタム属性	コンピュータに割り当てられているvCenterカス	文字列	env, production

プロパティ	説明	データタイプ	例
	タム属性です。[コンピュータ]→[詳細] の [仮想マシンの概要] に表示されます。	(カンマ区切りの属性名と値)	
電源の状態	[VMware仮想マシンの概要] の [コンピュータ]→[詳細] に表示されるコンピュータのvCenterの状態。	文字列 (リストのオプション)	電源オン

vCloud

プロパティ	説明	データタイプ	例
名前	コンピュータに関連付けられているvCloudです。 コンピュータはサブフォルダに分けて表示されます。	文字列	vCloud-lab23
データセンター	コンピュータに関連付けられているvCloudデータセンターです。 コンピュータはサブフォルダに分けて表示されます。	文字列	lab13-datacenter
vApp	コンピュータに関連付けられているvCloudデータセンターフォルダです。 コンピュータはサブフォルダに分けて表示されます。	文字列	db_dev

Active Directory

プロパティ	説明	データタイプ	例
名前	Microsoft Active DirectoryまたはLDAPディレクトリのホスト名です。 コンピュータはサブフォルダに分けて表示されます。	文字列	ad01.example.com
フォルダ	コンピュータのMicrosoft Active DirectoryまたはLDAPフォルダ名です。	文字列	台

プロパティ	説明	データタイプ	例
	コンピュータはサブフォルダに分けて表示されます。		

演算子

スマートフォルダの演算子は、一致するコンピュータが検索語句と同一のプロパティ値、類似のプロパティ値、または異なるプロパティ値を持つかどうかを示します。すべての演算子をすべてのプロパティに使用できるわけではありません。

演算子	説明	使用例
次の文字列に等しい	完全に一致するコンピュータのみが検出されます。	「OS」プロパティで「Windows」を指定した検索クエリでは、「Windows 7」または「Microsoft Windows」のコンピュータは検出されません。
次の文字列に等しくない	一致しないコンピュータがすべて検出されます。	「OS」プロパティで「Amazon Linux (64ビット)」を指定した検索クエリでは、Amazon Linux 64ビット以外のすべてのコンピュータが検出されます。
次の文字列を含む	検索語句を含むコンピュータがすべて検出されます。	「IPアドレス」プロパティで「203.0.113」を指定した検索クエリでは、203.0.113.xxxサブネット上にあるすべてのコンピュータが検出されます。
次の文字列を含まない	検索語句を含まないコンピュータが検出されます。	「OS」プロパティで「Windows」を指定した検索クエリでは、OS名に「Windows」がないコンピュータが検出されます。
任意の値	選択したプロパティのすべてのコンピュータが検出されます。	「グループ名」プロパティの検索クエリでは、そのグループに属するすべてのコンピュータが検出されます。
範囲内	指定した開始範囲と終了範囲の間のすべてのコンピュータが検出されます。	「IPアドレス」プロパティで開始範囲に「10.0.0.0」、終了範囲に「10.255.255.255」を指定した検索クエリでは、IPアドレスが10.0.0.0 ~ 10.255.255.255の範囲にあるすべてのコンピュータが検出されます。

演算子	説明	使用例
範囲外	指定した開始範囲と終了範囲の間にないすべてのコンピュータが検出されます。	「IPアドレス」プロパティで開始範囲に「10.0.0.0」、終了範囲に「10.255.255.255」を指定した検索クエリでは、IPアドレスが10.0.0.0 ~ 10.255.255.255の範囲外のすべてのコンピュータが検出されます。
はい	選択したプロパティのすべてのコンピュータが検出されます。	「Docker」プロパティで「はい」を選択した検索クエリでは、Dockerサービスが実行されているすべてのコンピュータが検出されます。
いいえ	選択したプロパティを持たないすべてのコンピュータが検出されます。	「Docker」プロパティで「いいえ」を選択した検索クエリでは、Dockerサービスが実行されていないすべてのコンピュータが検出されます。
次の期間より古い	プロパティで指定した日付よりも前のすべてのコンピュータが検出されます。 日、週、時間、または分といった演算子と組み合わせて使用します。	[前回成功した推奨設定の検索] プロパティで「次の期間より古い」、「7」、「日」を指定した検索クエリでは、8日以前に推奨設定の検索に成功したコンピュータが検出されます。
次の期間より新しい	プロパティで指定した日付よりも後のすべてのコンピュータが検出されます。 日、週、時間、または分といった演算子と組み合わせて使用します。	[前回成功した推奨設定の検索] プロパティで「次の期間より新しい」、「1」、「月」を指定した検索クエリでは、1か月よりも前に推奨設定の検索に成功したコンピュータが検出されます。
なし	プロパティと一致しないすべてのコンピュータが検出されます。	[前回成功した推奨設定の検索] プロパティで「なし」を指定した検索クエリでは、推奨設定の検索に成功したことのないコンピュータが検出されます。

詳細なシステム設定のカスタマイズ

上級者向けのいくつかの機能は、[管理]→[システム設定]→[詳細] から設定できます。

ヒント: システム設定の変更は、Deep Security APIを使用して自動化できます。例については、Deep Security Automation Centerにあるガイド「Configure Policy, Computer, and System Settings」を参照してください。

プライマリテナントアクセス

初期設定では、プライマリテナントはDeep Security環境にアクセスできます。

ただし、プライマリテナントがお使いの環境で[プライマリテナントアクセス]の設定を有効にしている場合、プライマリテナントがDeep Security環境にアクセスできないようにしたり、一定期間アクセスを許可したりすることはできません。

ロードバランサ

注意: FIPSモードが有効な場合、ロードバランサ設定は使用できません。"FIPS 140のサポート" on page 1870を参照してください。

エージェントには、Deep Security ManagerとDeep Security Relayのリストが設定されています。複数のマネージャとリレーがにがインストールされていない場合、ロードバランサの場合、エージェントは自動的にラウンドロビンシーケンスを使用してマネージャとリレーに接続します。

ネットワークのスケーラビリティを高めるには、ManagerやRelayの手前にロードバランサを配置すると効果的です。ロードバランサのホスト名とポート番号を設定すると、Agentで現在使用されているIPアドレスまたはホスト名とポート番号がオーバーライドされます。

スクリプトジェネレータは、接続しているDeep Security Managerのアドレスを使用します。そのため、いずれかのDeep Security Managerノードで障害が発生した場合やメンテナンスやアップグレードのために停止しているときもスクリプトは機能します。

注意: Agentのハートビートポート番号とのSSLまたはTLSセッションでは相互認証が使用されるため、このセッションがロードバランサで終端しないようにする必要があります。SSLインスペクションが終端する場合 (SSLオフロードを使用する場合など)、セッションが中断します。

マルチテナントモード

1. [マルチテナントモードの有効化] を選択します。
2. 表示されるウィザードで、[マルチテナントのアクティベーションコード] を入力し、[次へ] をクリックします。
3. ライセンスモードとして次のいずれかを選択します。
   - プライマリテナントからライセンスを継承: すべてのテナントでプライマリテナントと同じライセンスを使用します。
   - テナント単位のライセンス: 初回ログイン時にテナント自身がライセンスを入力します。
4. [次へ] をクリックします。

Deep Security Managerプラグイン

プラグインとは、Deep Security Manager用のモジュール、レポート、およびその他のアドオンを指します。トレンドマイクロでは、新規または追加のバージョンのプラグインを必要に応じて生成し、自己インストール型のパッケージとして配布する場合があります。

SOAP WebサービスAPI

従来のSOAP API Webサービスを有効または無効にします。WSDL (Web Services Description Language) には、画面のパネルに表示されるURLからアクセスできます。APIの詳細については、"Deep Security APIを使用したタスクの自動化" on page 1824を参照してください。

注意: WebサービスAPIにアクセスするには、適切なアクセス権限を持つ役割をユーザに割り当てる必要があります。役割を設定するには、[管理]→[ユーザ管理]→[役割] の順に選択し、役割のプロパティを開いて [WebサービスAPIへのアクセスを許可] を選択します。

ステータス監視API

従来のREST APIのステータス監視APIを有効または無効にします。このAPIは、Deep Security Manager (個々のManagerノードを含む) のステータス情報 (CPUやメモリの使用率、処理待ちのジョブ数、データベースの合計サイズおよびテナント固有のデータベースサイズなど) のクエリに使用されます。APIの詳細については、"Deep Security APIを使用したタスクの自動化" on page 1824を参照してください。

エクスポート

エクスポートファイルの文字エンコード: Deep Security Managerからデータファイルをエクスポートする際に使用される文字エンコード。このエンコードは選択した言語の文字をサポートしている必要があります。

エクスポートされた診断パッケージ言語: サポートプロバイダにより、Deep Security診断パッケージが生成され、送信される場合があります。この設定は診断パッケージの言語を指定します。診断パッケージは [管理]→[システム情報] で生成します。

Whois

Whoisは、ログに記録された侵入防御イベントやファイアウォールイベントを確認する際に、IPアドレスに関連付けられたドメイン名の確認に使用できます。検索URLを次のように入力します。[IP] には、検索するIPアドレスを指定します。
例: http://reports.internic.net/cgi/whois?whois_nic=[IP]&type=nameserver

ライセンス

新規ユーザに対してライセンス許可されていないモジュールを非表示: 以降に作成されるユーザに対して、ライセンス許可されていないモジュールをグレー表示ではなく非表示にする場合に指定します。この設定は、[管理]→[ユーザ管理]→[ユーザ]→[プロパティ] 画面の設定でユーザごとに上書きできます。

保存済みの検索キャッシュ設定のリストを表示するには、[検索キャッシュ設定の表示] をクリックします。検索キャッシュ設定は、仮想化された環境における不正プログラム検索および変更の検索の効率を最大化するためにVirtual Applianceで使用される設定です。詳細については、"Virtual Applianceの検索キャッシュ" on page 1062を参照してください。

推奨設定の検索中のCPU使用率

推奨設定の検索に使用するCPUリソース量を制御します。CPU使用率が想定以上に高くなった場合は、設定を下げて状況を改善するようにしてください。その他のパフォーマンス制御については、[管理]→[Managerノード]→[プロパティ]→[パフォーマンスプロファイル] を参照してください。

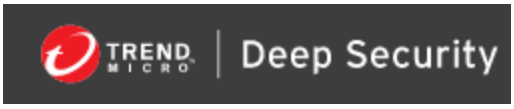
NSX

Deep SecurityがVMware NSX環境の仮想マシンの保護に使用され、複数のDeep Security Managerノードにインストールされている場合に、どのDeep Security ManagerノードがNSX Manager

と通信するかを決定します。Deep SecurityとNSX環境の統合の詳細については、"Deep Security Managerをインストールする" on page 459を参照してください。複数のDeep Security Managerノードの詳細については、"複数のノードにDeep Security Managerをインストールする" on page 505を参照してください。

ロゴ

ログオン画面、Deep Security Manager GUIの右上、およびレポートの上部に表示されるDeep Securityのロゴを置き換えることができます。使用できるのは、幅320ピクセル×高さ35ピクセル、ファイルサイズ1MB未満のPNGファイルです。テンプレートは、Deep Security Managerの `installfiles` ディレクトリにあります。



[ロゴのインポート] をクリックして独自のロゴをインポートするか、または [ロゴのリセット] をクリックして初期設定のロゴにリセットします。

Manager AWS ID

クロスアカウントアクセスを設定できます。次のいずれかを選択します。

- Managerインスタンスロールを使用: クロスアカウントアクセスを設定するためのより安全なオプションです。sts:AssumeRole権限を持つポリシーをDeep Security Managerのインスタンスの役割に関連付けてから、このオプションを選択します。Deep Security Managerにインスタンスの役割がない場合、またはDeep Security ManagerのAzure Marketplaceまたはオンプレミスインストールを使用している場合は表示されません。
- AWSアクセスキーを使用: このオプションを選択する場合は、キーを作成し、sts:AssumeRole権限を設定したポリシーを関連付けておきます。オプションを選択したら、[アクセスキー] と[秘密鍵] を入力します。Deep Security ManagerのAzure Marketplaceまたはオンプレミスインストールを使用している場合は表示されません。

アプリケーションコントロール

アプリケーションコントロールルールセットを作成または変更するたびに、使用するすべてのコンピュータに配布する必要があります。共有ルールセットはローカルルールセットよりも大きくなります。また、共有ルールセットはさまざまなサーバにも適用されることがあります。ルールセットをManagerから同時に直接

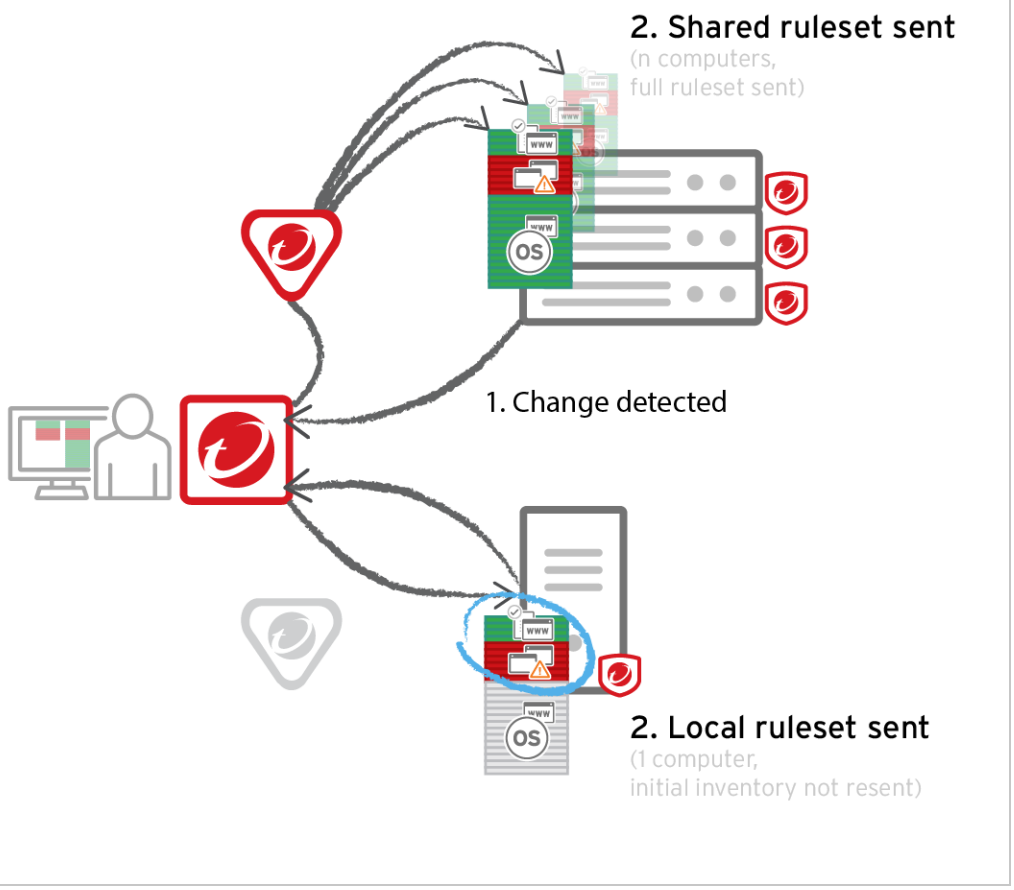
ダウンロードすると、負荷が大きくなり、パフォーマンスが低下する可能性があります。グローバルルールセットの注意事項も同じです。

Deep Security Relayを使用すると、この問題を解決できます。(Relayの設定の詳細については、「"追加のリレーを配信する" on page 1467」を参照してください。)

マルチテナント環境を使用しているかどうかによって、手順が異なります。

単一テナント環境

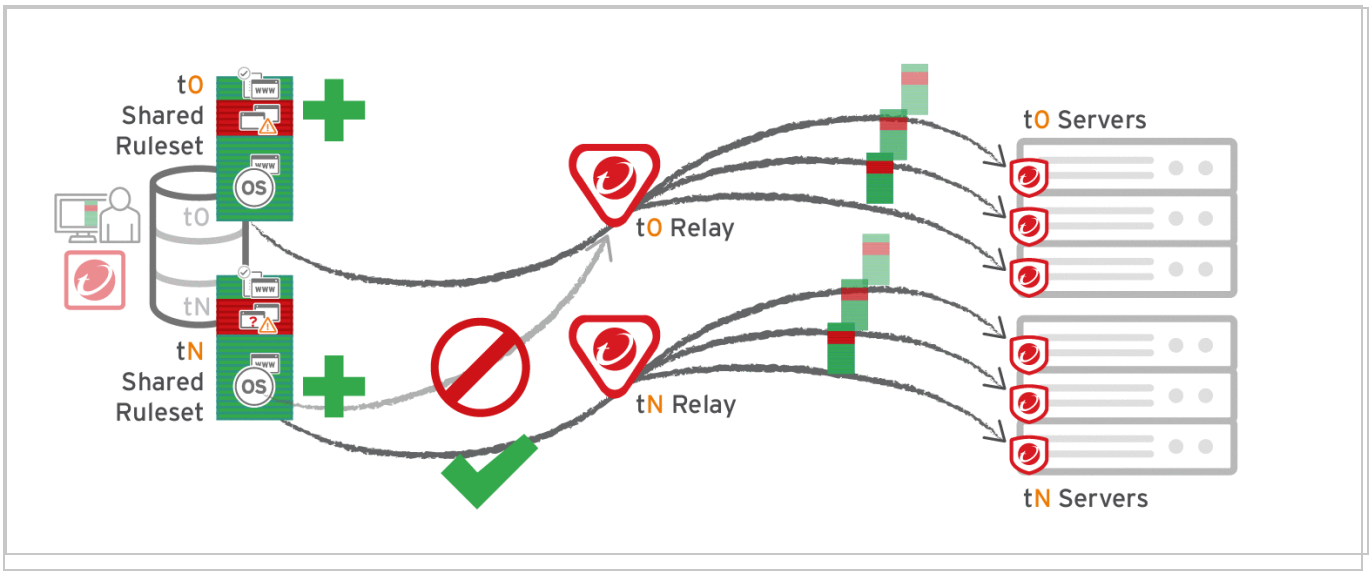
[管理]→[システム設定]→[詳細] の順に選択し、[アプリケーションコントロールルールセットをRelayから提供する] を選択します。



マルチテナント環境

プライマリテナント(t0)は他のテナント(tN)の設定にアクセスできないため、t0 RelayにはtNアプリケーションコントロールルールセットが設定されません。(IPSのような他の機能には、テナントではなくトレンドマイクロのルールセットが設定されるため、この注意事項は関係ありません。)

他のテナント(tN)は独自のRelayグループを作成してから[アプリケーションコントロールルールセットをRelayから提供する]を選択する必要があります。



警告:

Relayの使用前に使用環境との互換性を確認します。以前にダウンロードしたルールセットがAgentに現在適用されていない場合、新しいアプリケーションコントロールルールを受信しないと、コンピュータはアプリケーションコントロールで保護されません。アプリケーションコントロールルールセットのダウンロードに失敗した場合は、ルールセットダウンロード失敗イベントが、Managerおよび Agentで記録されます。

Relayのパフォーマンスが変化したり、アプリケーションコントロールルールセットのダウンロードが中断し、Relayが必要になる場合があります。プロキシの場所、マルチテナント、グローバル/共有ルールセットかローカルルールセットかによって異なります。

必須	パフォーマンス向上	パフォーマンス低下	有効にしない
[Agent]→[プロキシ]→[Manager] 注意: Deep Security Agent 10.0	共有ルールセット グローバルルールセット	ローカルルールセット	プライマリ以外のテナント(tN)が初期設定のプライマリ(t0) Relayグループを使用する場合のマルチテナント設定: • [Agent (tN)]→[DSR (t0)]→[DSM (tN)] • [Agent (tN)]→[プロキシ]→[DSR (t0)]→[DSM (tN)]

必須	パフォーマンス向上	パフォーマンス低下	有効にしない
以前では、プロキシ経由でのRelayへの接続がサポートされていませんでした。ルールセットのダウンロードがプロキシによって に失敗し、クライアントが中継またはマネージャのにアクセスするプロキシを必要とする場合は、次のいずれかを実行する必要があります。 • アップデートエージェントのソフトウェア、次にがプ			

必須	パフォーマンス向上	パフォーマンス低下	有効にしない
ロキシを設定する • プロキシをバイパスする。 • Relayを追加して、[アプリケーションコントロールルールセットをRelayから提供する] を選択する。			

Deep Securityの強化

Deep Securityの強化について

Deep Securityのセキュリティ設定を強化するには、いくつかの方法があります。

- "Agentを使用したDeep Security Managerの保護" below
- "Deep Security Agentの保護" on the next page
- "Deep Security ManagerのTLS証明書を変更します。" on page 1622
- "ロードバランサの証明書のアップデート" on page 1631
- "Deep Security Managerとデータベース間の通信の暗号化" on page 1633
- "Deep Security Managerのデータベースのパスワードの変更" on page 1638
- "HTTPセキュリティヘッダを設定する" on page 1641
- "Deep Securityの暗号化アルゴリズムのアップグレード" on page 1646
- "ユーザパスワードルールの適用" on page 1647
- "多要素認証の設定" on page 1649
- "信頼された証明書の管理" on page 1653
- "SSLの実装と資格情報のプロビジョニング" on page 1656

Agentを使用したDeep Security Managerの保護

Deep Security Managerを保護するには、ManagerのホストコンピュータにAgentをインストールし、Deep Security Managerポリシーを適用します。

1. Managerと同じコンピュータにAgentをインストールします。
2. [コンピュータ] に移動します。
3. Managerのコンピュータを追加します。ポリシーは、まだ適用しないでください。
4. ルールなしで侵入防御 をオンにします。新しいコンピュータをダブルクリックしての[詳細] 画面を表示し、[侵入防御]→[一般] →[設定]→の順に選択します。
5. 侵入防御 がオンになるのを待ちます。
6. [侵入防御]→[詳細]→[SSL設定]の順に選択します。
7. [SSL設定の表示]→[新規作成]をクリックしてウィザードを開始し、新しいSSL設定を作成します。
8. Managerで使用するインタフェースを指定します。[次へ] をクリックします。
9. [Port]画面で、Deep Security Manager GUIのポート番号を保護するかどうかを選択します。(「ポート番号」を参照)。[次へ] をクリックします。
10. SSLの侵入防御分析をこのコンピュータのすべてのIPアドレスで実行するのか、それとも1つのIPアドレスでのみ実行するのかを指定します(この機能は、1つのコンピュータに複数の仮想マシンを設定する場合に使用できます)。
11. [Deep Security Manager内蔵のSSL資格情報を使用します] を選択します (このオプションは、ManagerのコンピュータのSSL設定を作成する場合にのみ表示されます)。[次へ] をクリックします。

12. ウィザードを終了して、[SSL設定] 画面を閉じます。
13. コンピュータの [詳細] 画面に戻ります。Deep Security Managerポリシーを適用します。このポリシーには、Deep Security ManagerのGUIのポート番号を保護するために必要なファイアウォールルールと侵入防御ルールが含まれています。

これでManagerのコンピュータは保護され、ManagerへのSSLを含むトラフィックはフィルタされます。

注意: SSLトラフィックをフィルタするようにAgentを設定すると、Deep Security Agentからいくつかの更新エラーイベントが返されることがあります。これらは、Managerコンピュータで発行された新しいSSL証明書が原因の証明書の更新エラーです。これを修正するには、Webページを更新してから、Deep Security ManagerのGUIに再接続してください。

[Deep Security Manager] ポリシーには、Managerをリモートで利用できるように基本のファイアウォールルールが割り当てられています。Managerのコンピュータを別の目的で使用する場合は、追加でファイアウォールルールを割り当てる必要があります。また、このポリシーには、アプリケーションの種類 [Web Server Common] の侵入防御ルールが含まれます。必要に応じて、侵入防御ルールを追加で割り当てることもできます。

なぜならWebサーバコモンアプリケーションの種類は通常、HTTPポートリストには含まれず、Deep Security Manager GUIのポート番号は含まれていません。ポートの設定に優先されます。侵入防御ポリシーの[ルール]ページ詳細ウィンドウ。 "ポート番号、URL、およびIPアドレス" on page 428を参照)

SSLデータの検査の詳細については、"TLSトラフィックの検査" on page 936を参照してください。

Deep Security Agentの保護

セキュリティを向上させるために、Deep Security Agentを特定のDeep Security Managerにバインドすることができます。手順は、マネージャ開始のアクティベーションを使用するか、エージェント開始のアクティベーションを使用するかによって異なります。

マネージャーによるアクティベーション

エージェント-マネージャ間の通信中、Deep Security Agentはマネージャの身元を認証できます。これは、信頼されたマネージャの証明書を接続しているマネージャの証明書と比較することで行われます。一致しない場合、マネージャの認証は失敗し、エージェントは接続しません。

これは、エージェントが悪意のあるサーバがあなたのDeep Security Managerであると偽装してアクティブ化したり接続したりするのを防ぎます。特に、エージェントがインターネットのような信頼できないネットワークを介して接続する場合に推奨されます。

エージェントを保護するために、エージェントがアクティブ化を試みる前に、各エージェントが認証されたマネージャを認識できるように設定する必要があります。

注意: エージェントをリセットまたは無効にすると、エージェントはDeep Security Managerの証明書を削除します。エージェントを再度有効にするには、これらの手順を繰り返します。

1. Deep Security Managerで、次のコマンドを実行してサーバ証明書をエクスポートします。

   ```
   dsm_c -action exportdsmcert -output ds_agent_dsm.crt [-tenantname TENANTNAME | -tenantid TENANTID]
   ```

   どこ

   - `ds_agent_dsm.crt`はマネージャのサーバ証明書の名前です。この正確なファイル名を使用する必要があります。
   - `-tenantname TENANTNAME`はDeep Securityテナントの名前です。Deep Security Managerがマルチテナントの場合、これまたは`-tenantid`パラメータが必要です。"マルチテナント環境の設定" on page 478も参照してください。
   - `-tenantid TENANTID`テナントのIDです。

   複数のテナントがある場合、最初のテナントの証明書をエクスポートするためにコマンドを実行してください。

   ```
   dsm_c -action exportdsmcert -output ds_agent_dsm.crt -tenantname TENANT1
   ```

   次の手順に進みます。TENANT1の証明書が完了するまで、TENANT2やその他のエクスポートコマンドを再実行しないでください。このコマンドはファイルを上書きするためです。

2. 各エージェントのコンピュータで、`ds_agent_dsm.crt`ファイルを次の場所に配置してください。

- Windows上: *%ProgramData%\Trend Micro\Deep Security Agent\dsa_core*
- LinuxまたはUnixの場合: */var/opt/ds_agent/dsa_core*

複数のテナントがある場合、各テナントの証明書ファイルをそのテナント専用のエージェントにのみコピーしてください。エージェントは他のテナントによってアクティベートされることはできません。

3. マルチテナントのDeep Security Managerをお持ちの場合は、各テナントに対して前の手順を繰り返してください。

最初にこれらの手順を完了すると、エージェントは事前にアクティブ化された状態になります。エージェントが完全にアクティブ化されるまで、他のDeep Security Managerによって開始された操作や、dsa_controlを介してエージェントにコマンドを入力することは機能しません。これは意図的なものであり、アクティブ化されると通常の操作が再開されます。

Agentからのリモート有効化

エージェントのアクティベーション中、Deep Security Agentはマネージャの証明書をエージェントに固定することでDeep Security ManagerのIDを認証できます。これは、接続マネージャの証明書パスを検証し、信頼された認証機関(CA)によって署名されていることを確認することで行います。証明書パスが検証されると、マネージャ認証はエージェントを通過させ、エージェントをアクティベートします。これにより、エージェントがDeep Security Managerであると思われる不正なサーバからのアクティベーションを防ぐことができます。

エージェントを保護するために、エージェントがアクティブ化を試みる前に、各エージェントが認証されたマネージャを認識できるように設定する必要があります。

パブリックCAによって発行されたDeep Security Manager証明書チェーンをインポートする

1. 次の仕様に基づいてchain.pemファイルを準備してください。
   - PKCS＃8形式の秘密鍵です。
   - プライベートキーに対応するX509証明書。
   - 信頼された認証局(CA)ルートへの信頼の連鎖を構築するための他の中間X509証明書。各証明書はそれに直接先行する証明書に署名しなければならないため、順序が重要です。RFCのcertificate_listを参照してください。

---

2. Deep Security Managerで、次のコマンドを実行して証明書チェーンをインポートします。

   ```
   /opt/dsm/dsm_c -action agentHBPublicServerCertificate -set ${path_to_pem_file}
   ```

   ${path_to_pem_file}は絶対パスでなければなりません。

3. 公開CA証明書をコピーして、ds_agent_dsm_public_ca.crtに名前を変更してください。
4. エージェントコンピュータで、ds_agent_dsm_public_ca.crt ファイルを次のいずれかの場所に配置します。
   - Windowsの場合: %ProgramData%\Trend Micro\Deep Security Agent\dsa_core
   - LinuxまたはUnixの場合: /var/opt/ds_agent/dsa_core

注意: Deep Security Manager 20.0.262をインストールし、Deep Security Agent 20.0.1540以降をアクティベートする場合、アクティベーション時に次のエラーメッセージが表示されます。これは、マネージャの証明書をエージェントにピン留めしていないことを示しています。

"[Warning/2] | SSLVerifyCallback () - verify error 20: unable to get local issuer certificate"

信頼できる証明書のピン留めは任意であるため、該当しない場合はこのエラーを無視できます。ただし、信頼できる証明書を使用したい場合は、Deep Security Agentをアクティベートする前に前述の手順に従ってください。

証明書チェーンがインポートされたことを確認するには、次のコマンドを入力してください。

```
/opt/dsm/dsm_c -action agentHBPublicServerCertificate -isSet
```

インポートされた証明書チェーンを削除

パブリックCAによって発行されたDeep Security Managerの証明書チェーンの使用を停止するには、次のコマンドを入力してください。

```
/opt/dsm/dsm_c -action agentHBPublicServerCertificate -delete
```

デフォルトでは、Deep Security Managerは自己署名証明書の使用に戻ります。

Deep Security ManagerのTLS証明書を変更します。

インストール中に、Deep Security Managerは自己署名のX.509証明書を自動的に生成するため、最初にコンソールに接続する際にTLSを使用できます。ウェブブラウザはこの自己署名の証明書認証局 (CA) を認識しないため、証明書の署名を検証できず、自動的に信頼しません。ブラウザはセキュリティ警告を表示し、接続するために証明書を手動で検証するよう求めます。管理者が接続するたびにこれを回避するには、このデフォルトの証明書を信頼できるCAからの証明書に置き換えることができます。

警告: デフォルトの証明書を無効な証明書や不完全な証明書署名チェーンを持つ証明書に置き換えると、修正するまでDeep Security Managerコンソールに接続できなくなります。証明書を置き換える前に、指示を注意深く読んでください。

注意: 証明書は、Deep Security Managerのアップグレード時に保持されます。再度アップロードする必要はありません。

証明書を置き換えるには、次のいずれかを行ってください:

- Deep Security Managerドメイン名の新しい証明書を要求する
  a. FIPSモードが有効になっている場合 (「"FIPS 140のサポート" on page 1870」を参照)、証明書の置き換えを開始する前にFIPSモードを無効にします。
  b. "秘密鍵とJavaキーストアの生成" on the next page。
  c. "署名付き証明書 (CSR) の" on page 1625。
  d. "署名された証明書をキーストアにインポートする" on page 1626します。
  e. "キーストアを使用するためのDeep Security Managerの設定" on page 1628。
  f. 最初の手順でFIPSモードを無効にした場合は、ここでFIPSモードを再度有効にします。

- 既存のJavaキーストアファイルまたは証明書を使用する

  以前のインストールからの証明書ファイルのバックアップがある場合、または複数のドメイン名 (*.example.comなどの ワイルドカード証明書 、または 複数ドメイン/サブジェクト代替名 (SAN) フィールド証明書) である場合は、代わりにそれを使用できます。

  a. FIPSモードが有効になっている場合 (「"FIPS 140のサポート" on page 1870」を参照)、証明書の置き換えを開始する前にFIPSモードを無効にします。
  b. 完全な証明書署名チェーンがあることを確認します。必要に応じて、証明書を発行したCAに問い合わせます。

c. "キーストアを使用するためのDeep Security Managerの設定" on page 1628。
d. 最初の手順でFIPSモードを無効にした場合は、ここでFIPSモードを再度有効にします。

秘密鍵とJavaキーストアの生成

多くの公開CAと秘密CAには、公開鍵と秘密鍵のペアと証明書署名要求 (CSR) を同時に生成できるWebサイトがあります。たとえば、次のことができますMicrosoft Active Directoryでキーペアと CSR を同時に生成するまたはopensslCA、ダウンロードしてPKCS #12 ファイルをインポートする署名済み証明書と秘密鍵の両方をJava キーストアに入れます。

これを行う場合は、次の手順をスキップして"署名付き証明書 (CSR) の" on page 1625、「"署名された証明書をキーストアにインポートする" on page 1626」に進みます。それ以外の場合は、次の手順を使用してファイルをローカルに生成します。

1. Deep Security Managerが実行されているコンピュータで、管理者としてコマンドプロンプトを開きます。
2. コマンドを入力して、新しい秘密鍵とキーストアファイルを生成します。

   次のコマンド例では、新しい秘密鍵のキーストアエントリ(エイリアス) の名前は tomcatです。

   > 注意:
   > 証明書の共通名 (CN) またはサブジェクトの別名 (SAN) のフィールドは、多くの場合、ブラウザのロケーションバーに表示されるドメイン名と異なる必要があります。
   >
   > たとえば、ブラウザのロケーションバーのURLに https://dsm2.infosec.example.com と表示されていても、すべてのDeep Security Managerノードで同じ証明書を使用する場合は、ワイルドカード証明書を共通名 (CN)の *.infosec.example.comで作成します。

   - Linux:

     ```
     cd /opt/dsm/jre/bin
     keytool -genkey \
     -alias tomcat \
     -keystore ~/.keystore \
     -keyalg RSA \
     -validity 365 \
     -keysize 2048 \
     -dname "cn=dsm.example.com, ou=IT, o=Trend Micro, l=Ottawa,
     s=Ontario, c=CA"
     ```

- Windows:

```
cd "C:\Program Files\Trend Micro\Deep Security
Manager\jre\bin"
keytool -genkey ^
-alias tomcat ^
-keystore C:\Users\Administrator\.keystore ^
-keyalg RSA ^
-validity 365 ^
-keysize 2048 ^
-dname "cn=dsm.example.com, ou=IT, o=Trend Micro, l=Ottawa,
s=Ontario, c=CA"
```

> 注意: 例のコマンドでは、コマンドプロンプト(cmd.exe)構文を使用しています。代わりにPowerShellを使用する場合は、キャレット(^)をバッククォート(`)に置き換えます。

keytool コマンドの詳細については、Java keytoolのドキュメントを参照してください。

3. キーストアへのアクセスにDeep Security Managerで使用するパスワードを入力します。コマンド例では、これは YOUR_PASSWORD と表示されます。
4. コマンドを入力して、キーストアをPKCS #12形式でエクスポートします。

   このコマンド例では、エクスポートされるファイルの名前は .YOUR_PKCS12_EXPORTED_KEYSTOREです。

   - Linux:

```
keytool -importkeystore \
-srckeystore ~/.keystore \
-destkeystore ~/.YOUR_PKCS12_EXPORTED_KEYSTORE \
-deststoretype pkcs12
```

   - Windows:

```
keytool -importkeystore ^
-srckeystore C:\Users\Administrator\.keystore ^
-destkeystore "C:\Users\Administrator\.YOUR_PKCS12_EXPORTED_
```

```
KEYSTORE" ^
-deststoretype pkcs12
```

プロンプトが表示されたら、エクスポートされた(宛先)キーストアの新しいパスワードを入力し、次に元の(ソース)キーストアのパスワードを入力します。

5. "署名付き証明書 (CSR) の" belowに進みます。

署名付き証明書 (CSR) の

証明書署名要求 (CSR) ファイルには、署名されていない証明書と公開鍵が含まれています。Webブラウザが信頼するCAに署名を依頼します。証明書に署名するCAは、Webブラウザによって直接信頼されるルートCA、またはルートCAによって直接または間接的に信頼される中間CAのいずれかです。

1. コマンドを入力して、PKCS #12ファイルを使用してCSRファイルを生成します。

   -ext 拡張パラメータの san= フィールドに一致するドメイン名またはIPアドレスを指定することで、複数ドメイン/サブジェクトの別名 (SAN) 証明書を作成できます。SAN証明書が必要ない場合は、-ext パラメータを省略します。

   複数ドメイン/SAN証明書の場合、ブラウザは接続の検証時にCNフィールドを無視する必要があります。代わりに、一致するドメイン名とIPアドレスのカンマ区切りリストを含むSANフィールドを使用します。必要な構文をコマンド例に示します。

   - Linux:

     ```
     keytool -certreq \
     -alias tomcat \
     -keystore ~/.YOUR_PKCS12_EXPORTED_KEYSTORE  \
     -file YOUR_CSR.csr \
     -keyalg RSA \
     -ext san=dns:dsm.example.com,dns:*.example.org,ip:10.10.10.5
     ```

   - Windows:

     ```
     keytool -certreq ^
     -alias tomcat ^
     -keystore C:\Users\Administrator\.YOUR_PKCS12_EXPORTED_
     KEYSTORE ^
     -file YOUR_CSR.csr ^
     ```

```
-keyalg RSA ^
-ext san=dns:dsm.example.com,dns:*.example.org,ip:10.10.10.5
```

2. CSRファイルをCAにアップロードします。要求が処理されたら、署名付き証明書ファイルをダウンロードします。
3. 中間 CA を使用し、証明書がいいえPKCS #7 形式 (署名チェーンは含まれません) で、CA 証明書と、それとルートCA の間にある他のすべての CA (存在する場合) の証明書もダウンロードします。
4. "署名された証明書をキーストアにインポートする" belowに進みます。

署名された証明書をキーストアにインポートする

注意:
ブラウザは、証明書に追加されたCA署名のリスト(署名チェーン/信頼チェーン) を使用して証明書を検証し、接続しても安全かどうかを判断します。各CA証明書を順番に評価します。次の手順に示すように、すべてのCA証明書を正しい順序でインポートする必要があります。

署名のリストが正しくない場合、Webブラウザは証明書を検証できず、修正するまでコンソールへの接続をブロックします。

1. ルートCAがすでにキーストアにある場合は、この手順をスキップしてください。それ以外の場合は、コマンドを入力してインポートします。

   ヒント:
   キーストアの内容がわからない場合は、次のコマンドで内容を確認できます。

   ```
   keytool -list -v
   ```

   このコマンド例では、証明書は.crt形式で、ルートCAのキーストアエントリ(エイリアス) の名前はrootCAです。

   - Linux:

     ```
     keytool -import \
     -alias rootCA \
     -file ~/YOUR_ROOT_CA.crt \
     -keystore ~/.YOUR_PKCS12_EXPORTED_KEYSTORE \
     -storepass YOUR_PASSWORD
     ```

   - Windows:

```
keytool -import ^
-alias rootCA ^
-file c:\Users\Administrator\YOUR_ROOT_CA.crt ^
-keystore c:\Users\Administrator\.YOUR_PKCS12_EXPORTED_
KEYSTORE ^
-storepass YOUR_PASSWORD
```

2. 中間CA (存在する場合) がすでにキーストアにある場合は、この手順をスキップします。それ以外の場合は、コマンドを入力してインポートします。ルートCAによって署名されたもので始まり、証明書に署名されたもので終わります。

   - Linux:

     ```
     keytool -import \
     -alias intermediateCA \
     -trustcacerts \
     -file ~/YOUR_INTERMEDIARY_CA.crt \
     -keystore ~/.YOUR_PKCS12_EXPORTED_KEYSTORE \
     -storepass YOUR_PASSWORD
     ```

   - Windows:

     ```
     keytool -import ^
     -alias intermediateCA ^
     -trustcacerts ^
     -file c:\Users\Administrator\YOUR_INTERMEDIARY_CA.crt ^
     -keystore c:\Users\Administrator\.YOUR_PKCS12_EXPORTED_
     KEYSTORE ^
     -storepass YOUR_PASSWORD
     ```

3. 署名付き証明書をインポートするコマンドを入力します。

   - Linux:

     ```
     keytool -import \
     -alias tomcat \
     -trustcacerts \
     -file ~/YOUR_SIGNED_CERTIFICATE.crt \
     ```

```
-keystore ~/.YOUR_PKCS12_EXPORTED_KEYSTORE \
-storepass YOUR_PASSWORD
```

- Windows:

```
keytool -import ^
-alias tomcat ^
-trustcacerts ^
-file c:\Users\Administrator\YOUR_SIGNED_CERTIFICATE.crt ^
-keystore c:\Users\Administrator\.YOUR_PKCS12_EXPORTED_
KEYSTORE ^
-storepass YOUR_PASSWORD
```

インポートが成功すると、次のメッセージが表示されます。
Certificate reply was installed in keystore

4. "キーストアを使用するためのDeep Security Managerの設定" belowに進みます。

キーストアを使用するためのDeep Security Managerの設定

1. 次のコマンドを入力して、設定ファイルと古いキーストアファイルをバックアップし、キーストアファイルを置き換えてから、キーストアパスワードを更新します。

- Linux:

```
cp /opt/dsm/configuration.properties
/opt/dsm/configuration.properties.bak

cp /opt/dsm/.keystore /opt/dsm/.keystore.bak

cp ~/.YOUR_PKCS12_EXPORTED_KEYSTORE /opt/dsm/.keystore
```

- Windows:

```
copy "C:\Program Files\Trend Micro\Deep Security
Manager\configuration.properties" "C:\Program Files\Trend
Micro\Deep Security Manager\configuration.properties.bak"

copy "C:\Program Files\Trend Micro\Deep Security
Manager\.keystore" "C:\Program Files\Trend Micro\Deep
Security Manager\.keystore.bak"
```

```
copy "c:\Users\Administrator\.YOUR_PKCS12_EXPORTED_KEYSTORE"
"C:\Program Files\Trend Micro\Deep Security
Manager\.keystore"
```

注意: デフォルトのキーストアファイルは、元の場所に上書きする必要があります。新しいファイル名や別の場所を指すようにパスを設定しないでください。Deep Security Managerのアップグレードでは、キーストアパスの変更が保持されないため、変更が元に戻されます。

2. プレーンテキストエディタで configuration.properties ファイルを開き、キーストアのパスワード設定を更新します。

   ```
   keystorePass=YOUR_PASSWORD
   ```

3. Deep Security Managerサービスを再起動します。
4. Managerで新しい証明書が使用されていることを確認するには、Webブラウザを開き、Deep Security Managerコンソールに接続します。ロケーションバーの南京錠アイコンをクリックし、フィンガープリント(SHA-256署名)などの証明書の詳細を確認します。

Deep Security Managerでの自己署名証明書の再生成 (概要)

自己署名証明書を再生成する前に、次のコマンドを実行して古い.keystoreをバックアップする必要があります。

Linux:

```
cp /opt/dsm/configuration.properties /opt/dsm/configuration.properties.bak
```

```
cp /opt/dsm/.keystore /opt/dsm/.keystore.bak
```

Windows:

```
copy "C:\Program Files\Trend Micro\Deep Security Manager\configuration.properties" "C:\Program Files\Trend Micro\Deep Security Manager\configuration.properties.bak"
```

```
copy "C:\Program Files\Trend Micro\Deep Security Manager\.keystore" "C:\Program Files\Trend Micro\Deep Security Manager\.keystore.bak"
```

次のように、新しい.keystoreを作成します。

- Linux:
  a. Deep Security Managerがインストールされているコンピュータで、管理者としてコマンドプロンプトを開き、/opt/dsm/jre/binディレクトリに移動します。

b. cnの値をDeep Security Managerに合わせて置き換えて、次のコマンドを実行します。

```
keytool -genkey -alias tomcat -keystore ~/.keystore -keyalg
RSA -validity 365 -keysize 2048 -dname "cn=dsm.example.com,
ou=IT, o=Trend Micro, l=Ottawa, s=Ontario, c=CA"
```

c. プロンプトが表示されたら、パスワードを入力します。このパスワードは、/opt/dsm/configuration.propertiesファイルのkeystorePassの値に設定します。

d. プロンプトが表示されたら、Tomcatのキーパスワードを入力するか、Enterキーを押してキーストアファイルと同じキーを使用します。

e. 次のコマンドを実行して、新しいキーストアを正しい場所にコピーします。

```
cp ~/.keystore /opt/dsm/.keystore
```

f. /opt/dsm/configuration.propertiesファイルで、keystorePassの値にキーストアのパスワードを設定し、ファイルを保存します。

g. Deep Security Managerを再起動します。

h. ブラウザが証明書を検証できることを確認します。

- Windows:
  a. Deep Security Managerがインストールされているコンピュータで、管理者としてコマンドプロンプトを開き、C:\Program Files\Trend Micro\Deep Security Manager\jre\binディレクトリに移動します。

  b. cnの値をDeep Security Managerに合わせて置き換えて、次のコマンドを実行します。

```
keytool -genkey -alias tomcat -keystore
C:\Users\Administrator\.keystore -keyalg RSA -validity 365 -
keysize 2048 -dname "cn=dsm.example.com, ou=IT, o=Trend
Micro, l=Ottawa, s=Ontario, c=CA"
```

  c. プロンプトが表示されたら、C:\Program Files\Trend Micro\Deep Security Manager\configuration.propertiesファイルのkeystorePassの値に後で設定するパスワードを入力します。

  d. プロンプトが表示されたら、Tomcatのキーパスワードを入力するか、Enterキーを押してキーストアファイルと同じキーを使用します。

e. 次のコマンドを実行して、新しいキーストアを正しい場所にコピーします。

```
copy "c:\Users\Administrator\.keystore" "C:\Program
Files\Trend Micro\Deep Security Manager\.keystore"
```

f. C:\Program Files\Trend Micro\Deep Security Manager\configuration.propertiesファイルで、keystorePassの値にキーストアのパスワードを設定し、ファイルを保存します。

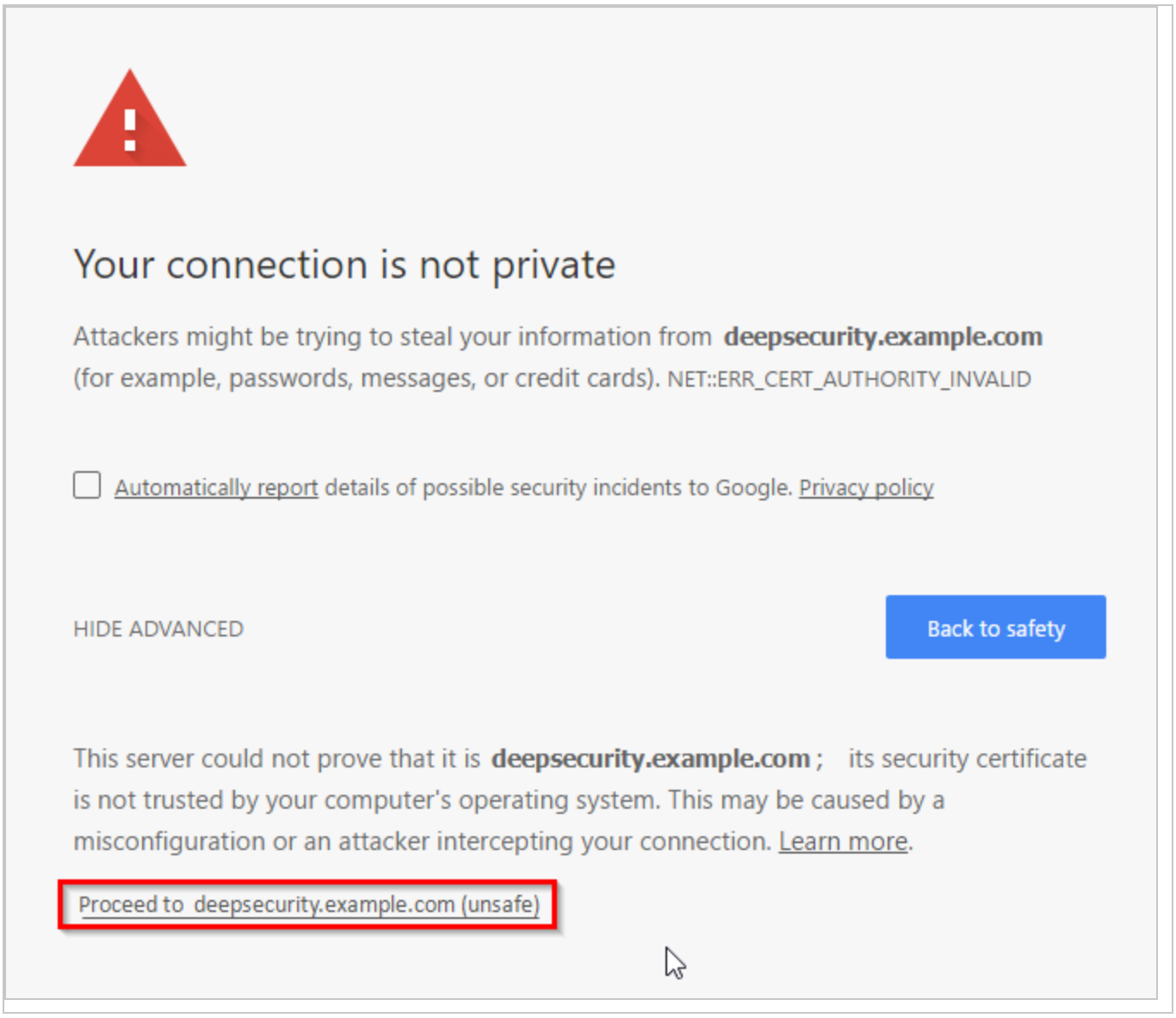
g. Deep Security Managerを再起動します。

h. ブラウザが証明書を検証できることを確認します。

ロードバランサの証明書のアップデート

通常、自己署名証明書を使用してサーバに接続しようとすると、証明書の検証エラーを示す警告がブラウザに表示されます。これは、自己署名証明書の場合、信頼できるサードパーティの認証局(CA)に対して証明書の署名をブラウザが自動的に検証できず、この証明書が攻撃者によって送信されたものかどうかを判別できないためです。インストール時、Deep Security ManagerはHTTPS接続(SSLまたはTLS)に自己署名証明書を使用するように設定されているため、この接続の保護に使用されているサーバ証明書フィンガープリントがお使いのDeep Securityサーバに属していることを手動で確認する必要があります。これは、自己署名証明書をCAによって署名された証明書に置き換えるまで続きます。

AWS Elasticロードバランサ(ELB)または他のロードバランサを使用した場合も同じエラーが発生し、ブラウザに自己署名証明書が表示されます。



警告を無視し続けても、Deep Security Managerにアクセスすることはできます (ブラウザごとに方法が異なります)。ただし、次の操作を行わない限り、接続のたびにこのエラーが発生します。

- コンピュータの信頼された証明書のストアに証明書を追加します (非推奨)。
- ロードバランサの証明書を、信頼できるCAによって署名された証明書に置き換えます (強く推奨)。

1. すべてのHTTPSクライアントに信頼されるCAに、管理者、Relay、およびAgentがDeep Security Managerへの接続に使用する完全修飾ドメイン名 (IPアドレスではない) を登録します。

Deep Security Managerを一意に識別するサブドメインを指定します(deepsecurity.example.comなど)。SSLターミネータロードバランサの背後にあるノードの場合、この証明書は、Deep Security Managerのノードごとではなく、そのロードバランサでブラウザおよび他のHTTPSクライアントに表示されます。

CAが証明書に署名したら、証明書(公開鍵)と秘密鍵の両方をダウンロードします。

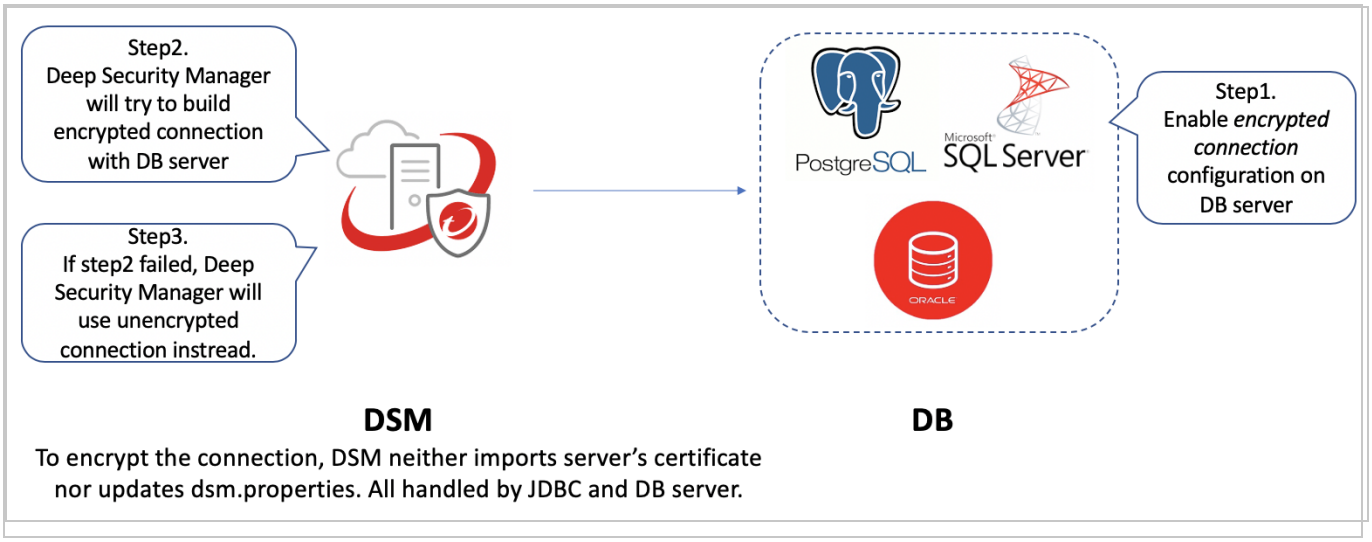
警告: 秘密鍵をセキュアな方法で保存および送信します。ファイル権限または暗号化されていない接続により、第三者による秘密鍵へのアクセスが許可される場合、この証明書と鍵で保護されるすべての接続が危険にさらされます。この証明書を無効にして、鍵を削除し、新しい証明書と鍵を取得する必要があります。

2. 証明書を証明書ストアに追加します(証明書に署名したCAをコンピュータが信頼する場合は任意)。
3. 新規ドメイン名を使用するようにロードバランサのDNS設定をアップデートします。
4. ロードバランサのSSL証明書を置き換えます。

Deep Security Managerとデータベース間の通信の暗号化

Deep Security Managerとデータベース間の通信チャネルが安全でない場合、それらの間の通信を暗号化することができます。現在の設計では、Deep Security Managerは、まずデータベースサーバとの暗号化された接続を確立しようとします。失敗した場合、Deep Security Managerはデータベースサーバとの暗号化されていない接続を使用します。

関連するメカニズムは、Deep Security Managerの基になるデータベースライブラリに組み込まれているため、サーバ証明書をインポートする必要はなく、設定ファイルをアップデートする必要はありません。暗号化されたセッションを有効にするときにパフォーマンスに重大な影響を及ぼすかどうかを判断するには、データベースのベンダーおよびそのサポートドキュメントを参照する必要があります。



この手順は、使用するデータベースによって異なります。

- "Microsoft SQL Serverデータベース" below
- "Oracleデータベース" on the next page
- "PostgreSQL" on the next page

注意: 複数ノードモードでDeep Security Managerを実行している場合は、以下の変更をノードごとに適用する必要があります。

このセクションでは、"データベースサーバでAgentを実行する" on page 1636、"Managerとデータベース間の暗号化を無効にする" on page 1636方法、および"古いDeep Security Managerバージョンからのアップグレード" on page 1638してください。

Managerとデータベースの間の通信を暗号化する

Microsoft SQL Serverデータベース

Deep Security Manager 20がインストールされていない場合は、次の手順を実行します。

1. Microsoft社のMSDNサイトで データベースエンジンへの暗号化された接続を有効にするの手順に従って、Microsoft SQL Serverで暗号化された接続オプションを有効にしてください。
2. Deep Security Managerをインストールします。

初期設定では、Deep Security Manager 20とMicrosoft SQL Server間の通信は暗号化されます。

すでにDeep Security Manager 20がインストールされており、Microsoft SQL Serverで暗号化オプションを有効にしていない場合：

1. Deep Security Managerを停止します20。
2. Microsoft MSDNサイトでデータベースエンジンに対する暗号化された接続を有効にするの手順に従って、Microsoft SQL Serverで暗号化された接続オプションを有効にします。
3. "Deep Security Managerの再起動" on page 1746。

初期設定では、Deep Security Manager 20とMicrosoft SQL Server間の通信は暗号化されます。

注意: SQL Server Manager Studioを使用してMicrosoft SQL Serverに接続できます。Deep Security Managerの暗号化された接続が機能しているかどうかを確認するには、コマンドselect client_net_address,connect_time,net_transport,protocol_type,encrypt_option from sys.dm_exec_connectionsを使用してください。

Oracleデータベース

Deep Security Manager 20がインストールされていない場合は、次の手順を実行します。

1. Oracle Help CenterでData Encryption and Integrityを設定する方法の手順に従って、Oracle Database Server側で暗号化された接続オプションを有効にします。
2. Deep Security Managerをインストールします。

初期設定では、Deep Security Manager 20とOracle Database Serverとの間の通信は暗号化されます。

すでにDeep Security Manager 20がインストールされていて、Oracle Database Serverの暗号化オプションを有効にしていない場合は、すでにインストールされています。

1. Deep Security Managerを停止します20。
2. Oracle Help CenterでData Encryption and Integrityを設定する方法の手順に従って、Oracle Database Server側で暗号化された接続オプションを有効にします。
3. "Deep Security Managerの再起動" on page 1746。

初期設定では、Deep Security Manager 20とOracle Database Serverとの間の通信は暗号化されます。

注意: オラクル社のブログ記事「ネイティブ暗号化と整合性の使用の検証」に従って、暗号化された接続が有効かどうかを確認してください。

PostgreSQL

Deep Security Manager 20をまだインストールしていない場合は、次の手順を実行します。

1. PostgreSQLでSSLを有効にします。オンプレミスのPostgreSQLデータベースについては、Secure TCP/IP SSL接続 を参照してください。Amazon RDS for PostgreSQLの場合、詳細に

ついては、PostgreSQLデータベースインスタンスでのSSLの使用を参照してください。
2. Deep Security Managerをインストールします。

初期設定では、Deep Security Manager 20とPostgreSQL データベースサーバとの間の通信は暗号化されます。

Deep Security Manager 20がすでにインストールされており、PostgreSQL データベースサーバで暗号化オプションが有効になっていない場合:

1. Deep Security Managerを停止します20。
2. PostgreSQLでSSLを有効にします。オンプレミスのPostgreSQLデータベースについては、Secure TCP/IP SSL接続 を参照してください。Amazon RDS for PostgreSQLの場合、詳細については、PostgreSQLデータベースインスタンスでのSSLの使用を参照してください。
3. "Deep Security Managerの再起動" on page 1746。

初期設定では、Deep Security Manager 20とPostgreSQL データベースサーバとの間の通信は暗号化されます。

注意: TLSを使用してマネージャーが接続されていることを確認するには、次のクエリを使用して[SSL]列を確認します。select a.client_addr, a.application_name, a.usename, s.* from pg_stat_ssl s join pg_stat_activity a using (pid) where a.datname='<Deep Security database name>';

データベースサーバでAgentを実行する

Agentを使用してデータベースを保護している場合は、暗号化を有効にする必要があります。セキュリティ更新プログラム( ) を実行すると、次のエラーメッセージが表示されます。Deep Security Managerは、新しい侵入防御ルールをデータベースに格納します。データが暗号化されていないと、Agentによるルールの解析の際に、ルール名が原因である誤判定がほぼ間違いなく発生してしまいます。

Managerとデータベース間の暗号化を無効にする

まれに、Deep Security Managerとデータベース間の暗号化を無効にすることが必要になる場合があります。たとえば、古いバージョンのSQL Serverを使用している場合は、接続エラーを回避するために暗号化を無効にしなければならないことがあります。詳細については、エラー: データベースサーバへの安全な接続を確立できませんでした。

暗号化を無効にするには、データベースの種類に応じた手順に従ってください。

Microsoft SQL Server

1. Deep Security Managerサービスを停止します。
2. SQL Serverで、 データベースエンジンへの暗号化された接続を有効にするで有効にされた[強制暗号化]オプションを無効にします。
3. (オプション) Deep Security Manager 20がDeep Security Manager 12.5またはそれ以前のバージョンからアップグレードされた場合は、dsm.propertiesの暗号化に関連するすべての設定を削除します。

   ```
   database.SqlServer.encrypt=true
   ```

   ```
   database.SqlServer.trustServerCertificate=true
   ```

   注意: Deep Security 10.1またはそれ以前のバージョンからアップグレードした場合、データベースへの接続で名前付きパイプがトランスポートとして使用される場合は、代わりに次の行を削除してください。database.SqlServer.ssl=require
4. 必要に応じてMicrosoft SQL Serverを再起動してください。
5. Deep Security Managerを起動します。

Oracle Database

1. Deep Security Managerサービスを停止します。
2. データの暗号化と整合性を設定する方法 に従って、Oracleサーバで接続暗号化を無効にします。
3. (オプション) Deep Security Manager 20がDeep Security Manager 12.5またはそれ以前のバージョンからアップグレードされた場合は、dsm.propertiesの暗号化に関連するすべての設定を削除します。

   ```
   database.Oracle.oracle.net.encryption_types_client=(AES256)
   ```

   ```
   database.Oracle.oracle.net.encryption_client=REQUIRED
   ```

   ```
   database.Oracle.oracle.net.crypto_checksum_types_client=(SHA1)
   ```

   ```
   database.Oracle.oracle.net.crypto_checksum_client=REQUIRED
   ```
4. Oracleリスナーを再起動します。
5. Deep Security Managerサービスを開始します。

PostgreSQL

1. Deep Security Managerサービスを停止します。
2. TCP/IP Connections with SSL に従って、ssl=on in postgresql.confを削除し、PostgreSQLデータベースで接続暗号化を無効にします。

3. (オプション) Deep Security Manager 20がDeep Security Manager 12.5またはそれ以前のバージョンからアップグレードされた場合は、dsm.propertiesの暗号化に関連するすべての設定を削除します。

   ```
   database.PostgreSQL.connectionParameters=ssl=true
   ```

4. PostgreSQLサービスを再起動します。
5. Deep Security Managerサービスを開始します。

古いDeep Security Managerバージョンからのアップグレード

現在Deep Security Manager 12.5以前を使用しており、次の条件を満たす場合:

- 暗号化された接続が有効になっています。
- PostgreSQLデータベースサーバを使用します。

アップグレードする前に、次の手順に従ってください。

いずれかの条件が満たされない場合は、次のセクションを無視して、Deep Security Manager 20.0に直接アップグレードできます。

Deep Security Managerをアップグレード

PostgreSQL JDBCドライバはバージョンによって動作が異なるため、アップグレードする前に次の手順を実行する必要があります。

1. 証明書をPostgreSQLデータベースサーバからエクスポートします。(これはすでに完了しているはずです。これは、古いDeep Security Managerで接続暗号化を有効にするために証明書が必要になるためです。).
2. 証明書ファイルの名前をroot.crt .と変更します。
3. あらかじめ定義されたDeep Security Manager 20のパスに配置します。

   Linuxでは、root.crtを~/.postgresql/に配置してください。

   Windowsでは、 root.crtを c:\Users\{USERNAME}\AppData\Roaming\postgresql\。

4. アップグレードフローを実行します。Deep Security Manager 20は、アップグレード後に引き続きPostgreSQLサーバとの暗号化された接続を使用します。

Deep Security Managerのデータベースのパスワードの変更

組織のセキュリティポリシーによっては、Deep Security Managerがデータベースへのアクセスに使用するパスワードを定期的に変更する必要がある場合があります。

- "Microsoft SQL Serverのパスワードを変更する" below
- "Oracleのパスワードを変更する" below
- "PostgreSQLのパスワードを変更する" on the next page

Microsoft SQL Serverのパスワードを変更する

1. Windowsでは、各Deep Security Managerインスタンスで Trend Micro Deep Security Manager サービスを停止します。

   Linuxでは、サービスを停止するコマンドは次のとおりです。

   ```
   # service dsm_s stop
   ```

2. SQL Server Management Studioを使用してSQLユーザパスワードを変更します。
3. Deep Security Managerの各インスタンスで、`/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties` ファイルを変更して新しいパスワードを指定します。このファイルを開くと、次のような難読化されたパスワード値が記載されています。

   ```
   database.SqlServer.password=$1$4ec04f9550e0bf378fa6b1bc9698d0bbc59ac010bfef7ea1e6e47f30394800b1a9554fe206a3ee9ba5f774d205ba03bb86c91c0664c7f05f8c467e03e0d8ebbe
   ```

   この値を新しいパスワードで上書きします (新しいパスワードはサービスを再起動したときに難読化されます)。

   ```
   Database.SqlServer.password=NEW PASSWORD GOES HERE
   ```

4. Windowsでは、各Deep Security Managerインスタンスで Trend Micro Deep Security Manager サービスを開始します。

   Linuxでは、サービスを開始するコマンドは次のとおりです。

   ```
   # service dsm_s start
   ```

Oracleのパスワードを変更する

1. Windowsでは、各Deep Security Managerインスタンスで Trend Micro Deep Security Manager サービスを停止します。

   Linuxでは、サービスを停止するコマンドは次のとおりです。

   ```
   # service dsm_s stop
   ```

2. Oracleのツールを使用してパスワードを変更します。

3. Deep Security Managerの各インスタンスで、/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties ファイルを変更して新しいパスワードを指定します。このファイルを開くと、次のような難読化されたパスワード値が記載されています。

   database.Oracle.password=$1$4ec04f9550e0bf378fa6b1bc9698d0bbc59ac010bfef7ea1e6e47f30394800b1a9554fe206a3ee9ba5f774d205ba03bb86c91c0664c7f05f8c467e03e0d8ebbe

   この値を新しいパスワードで上書きします(新しいパスワードはサービスを再起動したときに難読化されます)。

   Database.Oracle.password=NEW PASSWORD GOES HERE

4. Windowsでは、各Deep Security ManagerインスタンスでTrend Micro Deep Security Managerサービスを開始します。

   Linuxでは、サービスを開始するコマンドは次のとおりです。

   # service dsm_s start

PostgreSQLのパスワードを変更する

1. Windowsでは、各Deep Security ManagerインスタンスでTrend Micro Deep Security Managerサービスを停止します。

   Linuxでは、サービスを停止するコマンドは次のとおりです。

   # service dsm_s stop

2. パスワードを変更するには、PostgreSQLドキュメントの手順に従います。
3. Deep Security Managerの各インスタンスで、/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties ファイルを変更して新しいパスワードを指定します。このファイルを開くと、次のような難読化されたパスワード値が記載されています。

   database.PostgreSQL.password=$1$4ec04f9550e0bf378fa6b1bc9698d0bbc59ac010bfef7ea1e6e47f30394800b1a9554fe206a3ee9ba5f774d205ba03bb86c91c0664c7f05f8c467e03e0d8ebbe

   この値を新しいパスワードで上書きします(新しいパスワードはサービスを再起動したときに難読化されます)。

   Database.PostgreSQL.password=NEW PASSWORD GOES HERE

4. Windowsでは、各Deep Security ManagerインスタンスでTrend Micro Deep Security Managerサービスを開始します。

Linuxでは、サービスを開始するコマンドは次のとおりです。

```
# service dsm_s start
```

HTTPセキュリティヘッダを設定する

セキュリティヘッダとは、Webブラウザでのセキュリティ対策を設定するためにWebアプリケーションで使用されるディレクティブです。ブラウザはこれらのディレクティブに基づき、クロスサイトスクリプティングやクリックジャッキングなど、クライアント側の脆弱性を利用するのを困難にすることができます。また、ヘッダを使用すると、有効なTLS通信のみを許可したり、有効な証明書の使用を強制したり、特定のサーバ証明書の使用を強制したりするようにブラウザを設定することもできます。

以降のセクションでは、各種のセキュリティヘッダと、Deep Securityにおける各種ヘッダのサポート状況について詳しく説明します。

- "カスタマイズ可能なセキュリティヘッダ" below
- "強制的に適用されるセキュリティヘッダ" on page 1644
- "サポートされていないセキュリティヘッダ" on page 1645

カスタマイズ可能なセキュリティヘッダ

環境要件によっては、次のヘッダを有効にして設定することができます。

- "HTTPの厳密なトランスポートセキュリティ(HSTS)" below
- "Content Security Policy (CSP)" on the next page
- "HTTP公開鍵ピンニング (HPKP)" on page 1643

注意: プライマリテナントの場合は、Deep Security Managerで"カスタマイズ可能なセキュリティヘッダを有効化する" on page 1643ことや、"設定をリセットする" on page 1644ことができます。

HTTPの厳密なトランスポートセキュリティ(HSTS)

HTTPの厳密なトランスポートセキュリティは、Webアプリケーションと通信する際、常に有効で安全な接続を使用するようにWebブラウザを設定するヘッダです。サーバのTLS証明書が突然期限切れになったり信頼されなくなったりした場合、ブラウザはWebアプリケーションとの接続を行わなくなります。また、ユーザがhttp://で始まるURLを使用してWebアプリケーションにアクセスしようとした場合は、自動的にhttps://に変更されます。これらのセキュリティ対策は、中間者攻撃に加え、セッションハイジャッキングなどの攻撃を防ぐのに役立ちます。

インストール直後のDeep Security Managerコンソールでは、(信頼されていない) 自己署名証明書とHSTSがオフになっています。これは、各組織で、Managerのホスト名と一致する特定の証明書を使用してDeep Security Webアプリケーションを設定する必要があるためです。この設定は、AWS ELB/ALBなどのTLS終端機能を持つロードバランサを設定することで完了することもできます。

有効なTLS設定が行われると、の[管理]→[システム設定]→[セキュリティ]からHTTP Strict Transport Securityヘッダを有効にできます。

HTTPの厳密なトランスポートセキュリティ(HSTS) を有効化する方法については、"カスタマイズ可能なセキュリティヘッダを有効化する" on the next pageを参照してください。

Content Security Policy (CSP)

Content Security Policyには、ブラウザへの読み込みやブラウザでの実行を許可するコンテンツの種類を制限することにより、クロスサイトスクリプティングやクリックハイジャッキングなどのクライアント側攻撃を防止するのに役立つ包括的なディレクティブが含まれています。

注意: CSPを有効にすると、悪影響が生じる場合があります。たとえば、組み込みスクリプトが機能しなくなったり、jQueryなどのサードパーティコンポーネントで必要とされる特定の種類のイメージが読み込まれなくなったりすることがあります。

CSPを有効にする場合は、最初に [Report-only] をオンにしてCSPを実行し、必要なアプリケーション機能で指定したURL関連する違反がレポートされていないか確認することを推奨しています。

Deep Security CSPは、の[管理]→[システム設定]→[セキュリティ]で設定できます。

Deep Securityで推奨される設定は次のとおりです。

```
object-src 'self'
default-src 'self'
script-src 'self' 'unsafe-eval' 'unsafe-inline'
frame-src 'self'
frame-ancestors 'self'
style-src 'self' 'unsafe-inline' blob:
form-action 'self'
img-src 'self' data:
report-uri https://your_report_uri.org/DS_CSP_Violation
```

注意: 初期設定では、[Report-only] チェックボックスがオンになっています。CSPを有効にしても必要なアプリケーション機能に影響しないことを確認できたら、[Report-only] を選択解除してこのポリシーを適用できます。

警告: script-src は現在、「nonce」または「harsh-algorithm」をサポートしていません。クロスサイトスクリプティング(XSS) について懸念がある場合は、侵入防御ルールを有効にする1000552-Generic Cross Site Scripting(XSS) Preventionにしてください。

Content Security Policy (CSP) を有効化する方法については、"カスタマイズ可能なセキュリティヘッダを有効化する" belowを参照してください。

HTTP公開鍵ピンニング (HPKP)

HPKPヘッダを有効にすると、ブラウザは安全な通信を開始する際に、特定の証明書または特定の認証局のみを信頼するようになります。このヘッダを有効にすると、感染した信頼済み認証局やクライアントに不正にインストールされた信頼済み認証局を利用した攻撃を防止できます。

注意: HPKPを有効にすると、ヘッダが変更されずに証明書のみが変更された場合に、ブラウザがサーバと接続できなくなる可能性があります。

HTTP公開鍵ピンニング (HPKP) を有効化する方法については、"カスタマイズ可能なセキュリティヘッダを有効化する" belowを参照してください。

カスタマイズ可能なセキュリティヘッダを有効化する

注意: マルチテナントモードの場合、セキュリティヘッダの設定はプライマリテナントでのみ使用可能です。

1. [管理]→[システム設定]→[セキュリティ] の順に選択します。
2. HTTPの厳密なトランスポートセキュリティ(HSTS)、Content Security Policy (CSP)、またはHTTP公開鍵ピンニング (HPKP)のディレクティブを対応するフィールドに入力します。

   注意: 設定を有効にする前にポリシーをテストするには、[Report-only] オプションを選択し、ポリシー違反レポートの内容に問題がないことを確認します。

   ヒント: 各ポリシーのディレクティブを別々の行に入力できます。
3. 画面下部の [保存] をクリックします。

設定をリセットする

ディレクティブの設定中に問題が発生し、Deep Security Managerで問題を修正できない場合は、ManagerにSSHで接続し、対応するコマンドを実行して設定をリセットします。

HTTPの厳密なトランスポートセキュリティ

```
dsm_c -action changesetting -name settings.configuration.enableHttpStrictTransportSecurity -value ""
```

```
dsm_c -action changesetting -name settings.configuration.enableHttpStrictTransportSecurity -value "false"
```

Content Security Policy (CSP)

```
dsm_c -action changesetting -name settings.configuration.contentSecurityPolicy -value ""
```

```
dsm_c -action changesetting -name settings.configuration.contentSecurityPolicyReportOnly -value "true"
```

Public Key Pinning Policy

```
dsm_c -action changesetting -name settings.configuration.publicKeyPinPolicy -value ""
```

```
dsm_c -action changesetting -name settings.configuration.publicKeyPinPolicyReportOnly -value "true"
```

強制的に適用されるセキュリティヘッダ

次のヘッダは初期設定で強制的に適用され、変更できません。

- "Cache-ControlおよびPragma" below
- "X-XSS-Protection" on the next page
- "X-Frame-Options" on the next page

Cache-ControlおよびPragma

これらのヘッダは、ブラウザでのコンテンツのキャッシュ方法を設定します。認証されたアプリケーションから機密情報を含むコンテンツをキャッシュする場合、複数のユーザが使用するマシンにコンテンツがキャッシュされたり、ユーザがアプリケーションからログアウトした後にロック解除されたマシンへ攻撃者がアクセスできる状態になっていたりすると、セキュリティ上の脆弱性につながる恐れがあります。そのため、Deep Securityでは、no-cacheおよびno-storeの値を強制的に適用することにより、静的でないすべてのコンテンツのキャッシュが無効化されます。

X-XSS-Protection

XSS-Protectionヘッダは、ブラウザのクロスサイトスクリプティング (XSS) ヒューリスティックを強制的に有効にしてXSS攻撃を検出します。Deep Securityの初期設定では、このヘッダがブロックモードで強制的に適用されます。そのため、XSS攻撃の可能性がブラウザで検出されると、ページ全体の読み込みがブロックされます。この方法は、潜在的な不正要素を置き換えることによってページを無害化しようとする他の方法よりも安全です。

注意: XSS-Protectionは、あらゆる種類の攻撃に対して有効なわけではなく、XSSフィルタを備えていないブラウザもあります。

X-Frame-Options

このヘッダは、クリックハイジャッキング攻撃の防止に役立ちます。Deep Security Managerでは、このヘッダのSAMEORIGINという値を強制的に適用することにより、同じドメインでホストされているWebアプリケーションへの組み込みのみが許可されます。

注意: このヘッダの効果は、CSPのframe-ancestorsディレクティブと同じです。frame-ancestorsディレクティブはX-Frame-Optionsヘッダの値よりも優先されます。

サポートされていないセキュリティヘッダ

次の種類のヘッダはサポートされていません。

X-Content-Type-Options

nosniffという値を含むこのヘッダを使用すると、MIMEタイプスニフィングからの保護に役立ちます。MIMEタイプスニフィング攻撃は、ブラウザでテキストコンテンツやバイナリコンテンツがHTMLとして解釈される可能性がある特定のシナリオにおいてのみ影響を及ぼします。たとえば、ユーザがxss.htmlというアバタファイルを読み込み、Webアプリケーションが画像を提供する際にContent-typeヘッダを設定していない場合、ブラウザはコンテンツタイプの判定を試み、xss.htmlをHTMLファイルとして扱う可能性があります。その場合、攻撃者はユーザをxss.htmlに誘導してクロスサイトスクリプティング攻撃を実行することが可能になります。

このヘッダを有効にするとリダイレクトの動作に悪影響を及ぼすことがあります。Deep Securityでは現在、このヘッダを有効にすることはできませんが、これに関連する攻撃のシナリオがManager Webアプリケーションとその基本的な機能に影響する可能性は低いと考えられます。

Deep Securityの暗号化アルゴリズムのアップグレード

Deep Security 9.6 SP1以前では、Deep Security ManagerとDeep Security Agent間の通信を保護するために、RSA-1024およびSHA-1を使用します。初期設定では、Deep Security 10.0以降ではRSA-2048およびSHA-256が使用されます。これは、より安全なアルゴリズムです。

Deep Security 10.0以降の新しいインストールでは、RSA-2048およびSHA-256が使用されますが、以前のバージョンからDeep Security 10.0以降にバージョンアップする場合は、個別にアップグレードする場合を除き、初期の暗号化アルゴリズムが引き続き使用されます。

この記事では、Deep Security 10.0以降にアップグレードした後にアルゴリズムをアップグレードする方法について説明します。この記事の説明に従って設定を変更すると、Deep Security Manager自体および管理下のすべてのエージェント用の新しい証明書が生成されます。エージェントがDeep Security Managerに再度接続すると、マネージャは新しい証明書をエージェントに送信します。

Windowsでアルゴリズムをアップグレードする

1. Microsoft管理コンソールの[サービス]画面を使用して「Trend Micro Deep Security Manager」サービスを停止します。
2. Windowsのコマンドラインで、Deep Security Managerの作業フォルダ(例：`C:\Program Files\Trend Micro\Deep Security Manager`)に移動します。
3. dsm_cコマンドとパラメータを使用して、新しい設定に変更します。次に例を示します。

   ```
   dsm_c -action changesetting -name settings.security.defaultSignatureAlg -value "SHA256withRSA"
   ```

   ```
   dsm_c -action changesetting -name settings.security.defaultKeyLength -value "2048"
   ```

   ```
   dsm_c -action changesetting -name settings.security.forceCertificateUpdate -value "true"
   ```

4. エラーが表示されないことを確認し、Trend Micro Deep Security Managerサービスを再起動します。

Linuxでアルゴリズムをアップグレードする

1. コマンドラインで、Deep Security Managerサービスが実行されているディレクトリに移動し、次のコマンドを実行してサービスを停止します。

   ```
   service dsm_s stop
   ```

2. Linuxのコマンドラインで、Deep Security Managerの作業フォルダ(例：`/opt/dsm`)に移動します。

3. dsm_cコマンドとパラメータを使用して、新しい設定に変更します。次に例を示します。

```
./dsm_c -action changesetting -name settings.security.defaultSignatureAlg -value "SHA256withRSA"
```

```
./dsm_c -action changesetting -name settings.security.defaultKeyLength -value "2048"
```

```
./dsm_c -action changesetting -name settings.security.forceCertificateUpdate -value "true"
```

4. エラーが表示されないことを確認し、Trend Micro Deep Security Managerサービスを再起動します。

複数ノード環境でアルゴリズムをアップグレードする

複数のノードでDeep Security Managerを実行している場合は、いずれかのノードでdsm_cコマンド(前述)を実行し、他の各ノードで「Trend Micro Deep Security Manager」サービスを手動で再起動して変更を有効にします。そこに。

マルチテナント環境でアルゴリズムをアップグレードする

Deep Security 10.0では、アルゴリズム設定はテナントごとに独立しています。そのため、dsm_cコマンドでテナント名(-tenantnameを使用)またはテナントID(-tenantidを使用)を指定して、各テナントについて個別に設定をアップデートする必要があります。テナントIDが5のテナントの設定を変更する例を次に示します。

```
dsm_c -action changesetting -name settings.security.defaultSignatureAlg -value "SHA256withRSA" -tenantid 5
```

```
dsm_c -action changesetting -name settings.security.defaultKeyLength -value "2048" -tenantid 5
```

```
dsm_c -action changesetting -name settings.security.forceCertificateUpdate -value "true" -tenantid 5
```

ユーザパスワードルールの適用

Deep Security Managerのパスワードとユーザ認証に関係するその他の設定に対してパスワード要件を指定できます。

パスワード要件を指定する

注意: セキュリティを強化するため、パスワード要件を厳しく指定することを推奨します。文字数は8文字以上で、英数字の両方を含める、大文字と小文字の両方を含める、英数字以外の文字を含める、期限を設ける、などを組み合わせます。

[管理]→[システム設定]→[セキュリティ] の順に選択します。[ユーザセキュリティ] セクションでは次の設定を変更できます。

- セッションアイドルタイムアウト: ユーザの再ログオンが必要になるまでの期間を指定します。
- 最大セッション期間 : ユーザがDeep Security Managerにログインして再度ログインする必要がある最大時間です。
- ログオン失敗の許容回数 (ロックアウト前): 特定のユーザ名を持つ各ユーザが、間違ったパスワードを使用してログオンを試行できる回数。この回数を超えるとロックされます。ユーザのロックを解除できるのは、「ユーザのプロパティを編集できる」権限を持つユーザのみです ("ユーザロールの定義" on page 1541を参照)。

  注意: ログオンの失敗回数が多すぎるなど、特定の理由でユーザがロックされた場合に、そのアカウントのロックを解除する権限を持つユーザがいないときは、「コマンドラインの使用方法」セクションを参照して、Deep Security Managerのコマンドラインを使用してロック解除を行ってください。

- ユーザごとに許可された同時セッション数: ユーザごとに許可されている同時セッションの最大数。

  注意: 一度に2人のユーザとしてログオンする場合、Firefoxでは、画面ベースではなくプロセスベースでセッションCookieが設定されます。つまり、何らかの理由で同時に2人のユーザとしてログオンする場合は、2つの異なるブラウザ (一方はFirefox) を使用するか、2台の異なるコンピュータからログオンする必要があります。

- 同時セッション制限を超えた場合の処理: 同時セッション数の上限に達した場合の処理を指定します。
- ユーザパスワードの有効期限: パスワードが有効な日数。無期限に設定することもできます。
- ユーザパスワードの最小文字数: パスワードに必要な最小の文字数。
- ユーザパスワードには文字と数字の両方を含めることを要求する: 英字 (a ~ z、A ~ Z) と数字 (0 ~ 9) の両方をパスワードに使用する必要があります。
- ユーザパスワードには大文字と小文字の両方を含めることを要求する: 大文字と小文字の両方を使用する必要があります。
- ユーザパスワードには英数字以外の文字を含めることを要求する: 英数字以外の文字をパスワードに使用する必要があります。
- パスワードの有効期限が近いユーザにメールを送信: ユーザのパスワードの有効期限が切れる前にメールメッセージが送信されます。この機能を使用するには、"メール通知のSMTPの設定" on page 1299を行う必要があります。

ログオンに別のIDプロバイダを使用する

SAMLシングルサインオンを使用するようにDeep Securityを設定することもできます。詳細については、"SAMLシングルサインオンを設定する" on page 1563を参照してください。

Deep Security Managerログオンページにメッセージを追加する

[管理]→[システム設定]→[セキュリティ]画面で[ログオンページのメッセージ]を使用し、Deep Security Managerのサインインページに表示されるテキストを入力します。

ユーザに使用条件を提示する

Deep Security Managerへのログオン時にユーザに使用条件への同意を求めるように設定することができます。

この機能を有効にするには、[管理]→[システム設定]→[セキュリティ]画面で[使用条件へのユーザの同意が必要]を選択します。ユーザがログオンページで[条件を表示]リンクをクリックしたときに表示するタイトルと条件のリストを、該当する2つのテキストボックスに入力します。

その他のセキュリティ設定

[管理]→[システム設定]→[セキュリティ]画面では次の機能も有効にできます。

- "信頼された証明書の管理" on page 1653
- "HTTPセキュリティヘッダを設定する" on page 1641

多要素認証の設定

Deep Security Managerでは、多要素認証 (MFA) を使用することができます。MFAはユーザ名とパスワードの他にも情報を必要とするアクセス管理方式であり、ベストプラクティスとして推奨されています。

このトピックの内容:

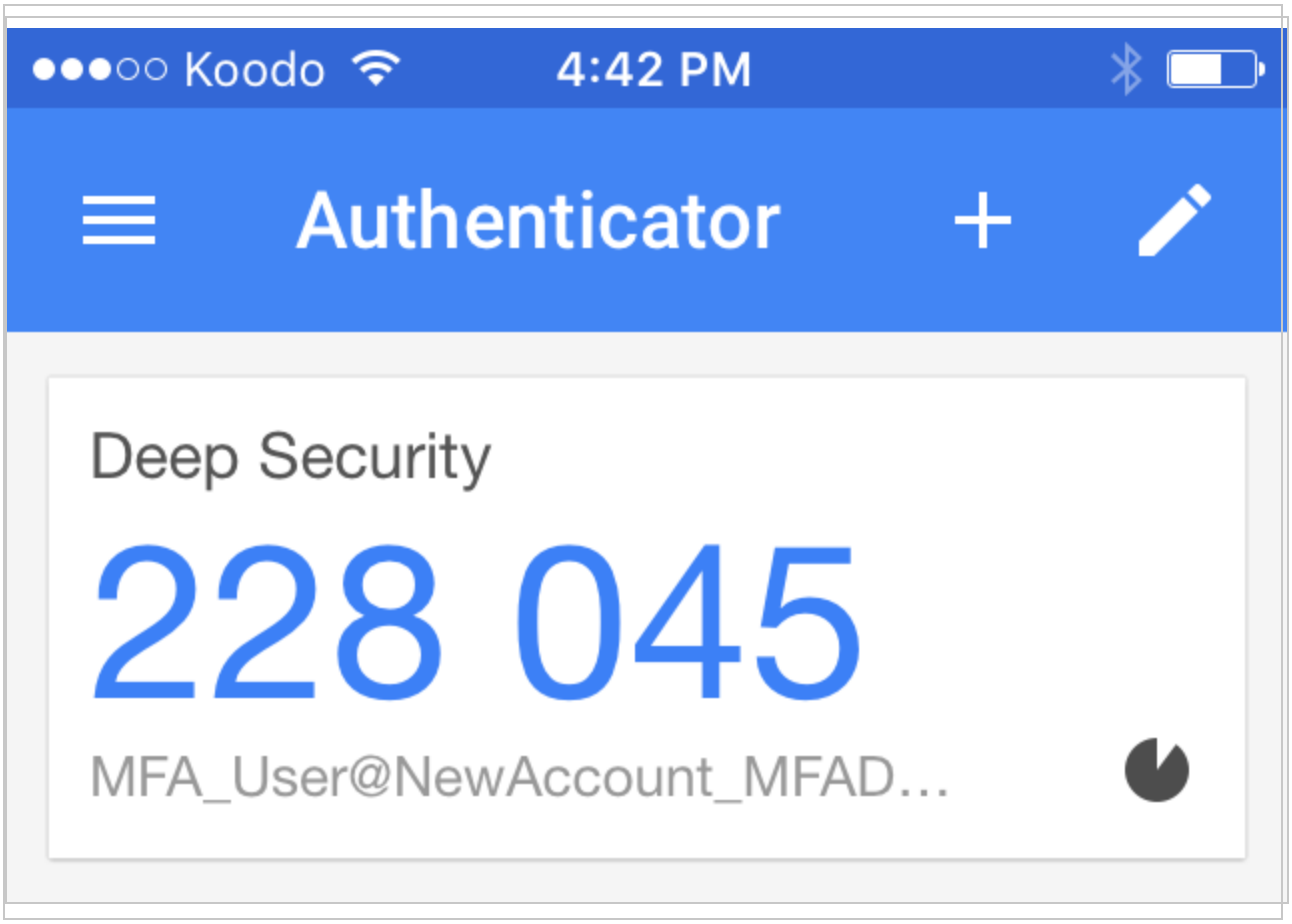
- "多要素認証を有効にする" on the next page
- "多要素認証を無効にする" on page 1652
- "サポートされる多要素認証 (MFA) アプリケーション" on page 1652
- "MFAをトラブルシューティングする" on page 1653

多要素認証を有効にする

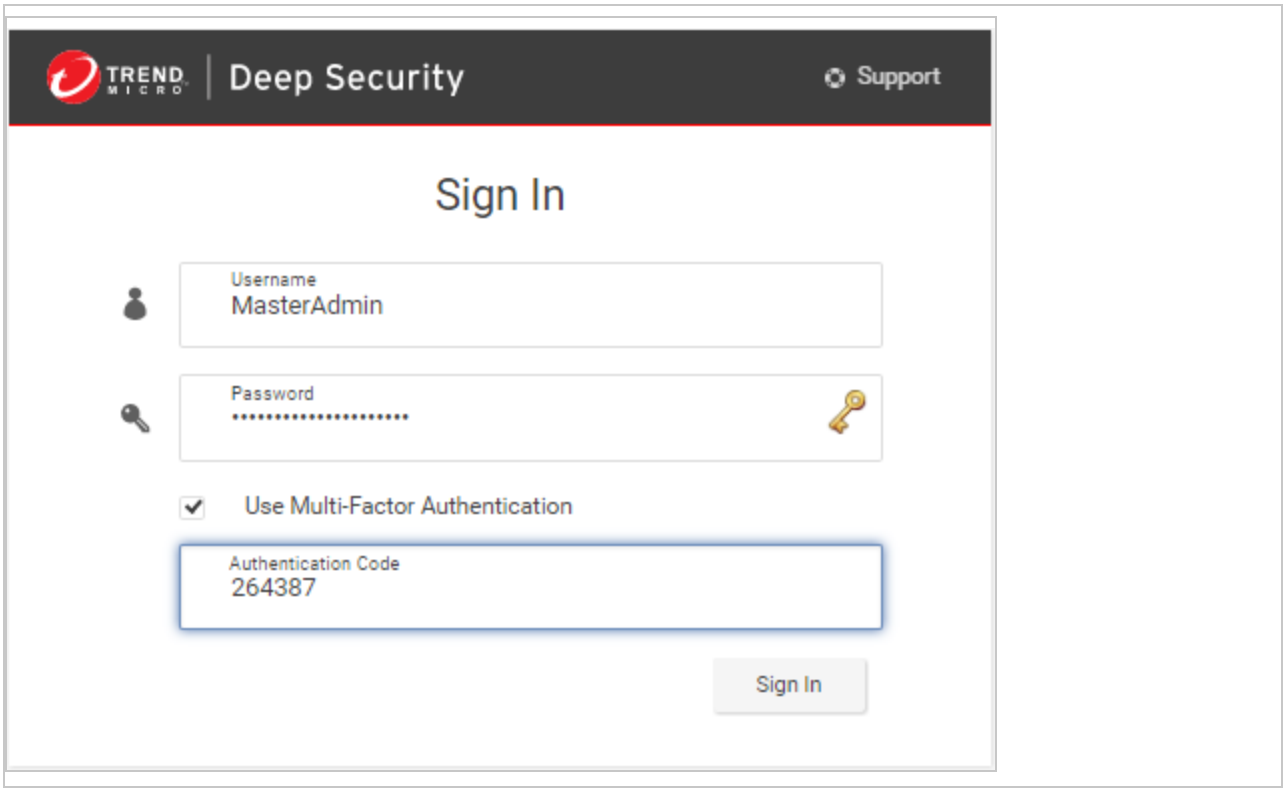
1. Deep Security Managerで、右上に表示されるユーザ名の下のメニューから[ユーザプロパティ] を選択します。
2. [一般] タブで [多要素認証の有効化...] ボタンをクリックします。多要素認証の有効化ウィザードが開くので、ウィザードの指示に従って作業を進めます。
3. ウィザードの最初の画面で、互換性がある仮想MFAアプリケーション (Google Authenticatorなど) をインストールするように求めるメッセージが表示されます。詳細については、この後の"サポートされる多要素認証 (MFA) アプリケーション" on page 1652を参照してください。
4. デバイスがQRコードの読み取りに対応している場合は、カメラで読み取ってMFAアプリケーションを設定し、[次へ] をクリックします。

   対応していない場合は、[QRコードの読み取りに対応していないため、手動設定用の秘密鍵を表示する]を選択します。

5. 認証コードをスペースなしで入力します。例: 228045。



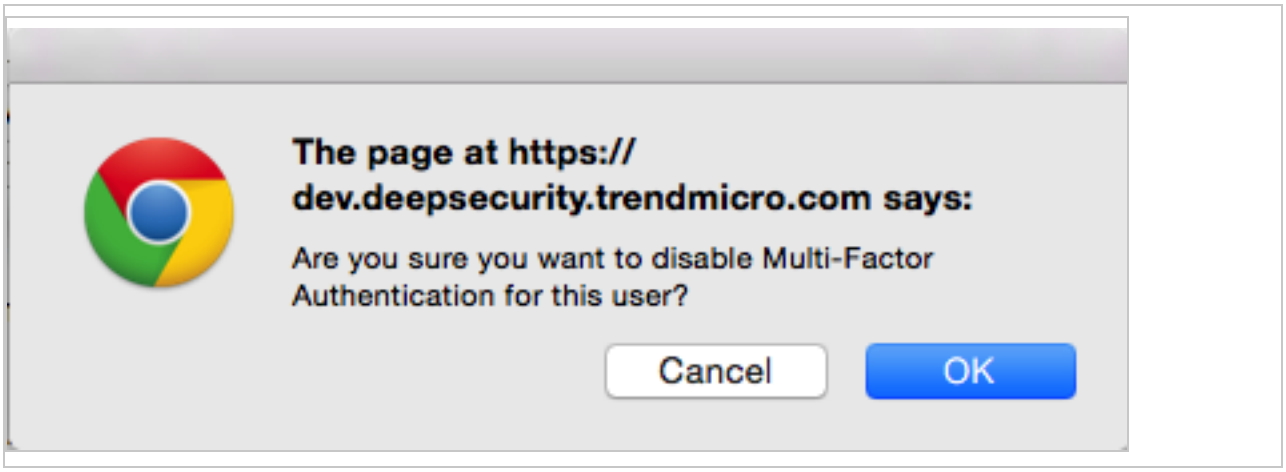
6. 認証コードが正しければアカウントでMFAが有効になり、ログオン時に毎回新しいMFAコードの入力が要求されるようになります。



多要素認証を無効にする

1. Deep Security Managerで、右上に表示されるユーザ名の下のメニューから[ユーザプロパティ]を選択します。

2. [一般] タブで [MFAを無効にする] ボタンをクリックします。
3. 確認画面で [OK] をクリックしてMFAを無効にします。



4. ユーザプロパティ画面に、MFAが変更されたことを示すメッセージが表示されます。[OK] をクリックして画面を閉じます。

サポートされる多要素認証 (MFA) アプリケーション

MFAには以下のスマートフォンとアプリケーションの使用を推奨しますが、RFC 6238準拠のTime-base One-time Password Algorithmを実装するアプリケーションは機能します。

スマートフォン	MFAアプリ
Android	Google Authenticator、Duo
iPhone	Google Authenticator、Duo
Blackberry	Google Authenticator

MFAをトラブルシューティングする

MFAデバイスを有効にしても機能しない場合の対処

MFAログインに関する問題のほとんどは、Deep Security Managerの時間がデバイスと同期していないことが原因で発生します。

選択したOSの以下に示す手順に従って、時間が適切に同期しているかを確認してください。

Deep Security ManagerがLinuxの場合:

コマンドラインに「ntpstat」と入力して、NTPが正常に動作していることを確認します。現在のシステムの時刻と日付を表示するには、「date」と入力します。

Deep Security ManagerがWindowsの場合:

Windowsのタイムサービスが正常に動作していることを確認します。現在のシステムの時刻と日付を表示するには、コマンドラインに「time」および「date」と入力します。

MFAデバイスが紛失または動作停止した場合の対処

MFAデバイスが紛失、破損、あるいは動作を停止した場合は、アカウントのMFAを無効にしてログオンを可能にする必要があります。

1. ログオン資格情報の担当者に連絡し、"多要素認証を無効にする" on the previous pageに記載されている手順を実行してもらいます(これでユーザ名とパスワードだけでログオンできるようになります)。
2. ログオン後、パスワードを変更します。
3. "多要素認証を有効にする" on page 1650に記載されている手順を実行します。

信頼された証明書の管理

信頼できる証明書は、Microsoft Active Directory やVMware vCenterなどの外部サービスへのコード署名とSSL接続に使用されます。また、不正プログラム対策からファイルを除外するためにも使用されます。

信頼された証明書をインポートする

注意: 信頼された証明書をインポートして、Amazon Web Servicesのリージョンと信頼を確立する場合は、dsm_cコマンドラインツールを使用する必要があります。

Deep Security Managerを使用して信頼された証明書をインポートするには

1. Deep Security Managerで、管理 > システム設定 > Securityに移動します。
2. [信頼された証明書]で、[証明書リストを表示]をクリックして、Deep Security Managerで受け入れられたすべてのセキュリティ証明書のリストを表示します。
3. [ファイルからインポート] をクリックして証明書のインポートウィザードを起動します。

dsm_cを使用して信頼された証明書をインポートするには

1. Deep Security Managerサーバで、次のコマンドを実行します。

```
dsm_c -action addcert -purpose PURPOSE -cert CERTFILE
```

パラメータは次のとおりです。

パラメータ	説明	値のサンプル
PURPOSE	証明書を使用する接続の種類。右のいずれかの値を選択する必要があります。	AWS - Amazon Web Services
		DSA - コード署名
		EXCEPTION - 除外
		SSL - SSL接続
CERTFILE	インポートする証明書を含むファイルのユーザ定義の名前。	/path/to/cacert.pem

注意: Linux環境でDeep Security Managerを実行している場合は、dsm_c コマンドをrootユーザとして実行する必要があります。

信頼された証明書を表示する

注意: Amazon Web Services接続に使用する信頼された証明書を表示する場合は、dsm_cコマンドラインツールを使用する必要があります。

Deep Security Managerを使用して信頼された証明書を表示するには

1. Deep Security Managerで、[管理]→[システム設定]→[セキュリティ] の順に選択します。
2. [信頼された証明書] で [証明書リストの表示] をクリックします。

dsm_cを使用して信頼された証明書を表示するには

1. Deep Security Managerサーバで、次のコマンドを実行します。

   ```
   dsm_c -action listcerts [-purpose PURPOSE]
   ```

   「-purpose PURPOSE」はオプションのパラメータで、すべての証明書のリストを表示する場合は省略できます。「PURPOSE」に値を指定した場合は、その目的に使用する証明書だけが表示されます。

パラメータ	説明	値のサンプル
PURPOSE	証明書を使用する接続の種類。	AWS - Amazon Web Services
		DSA - コード署名
		EXCEPTION - 除外
		SSL - SSL接続

注意: Linux環境でDeep Security Managerを実行している場合は、dsm_c コマンドをrootユーザとして実行する必要があります。

信頼された証明書を削除する

注意: Amazon Web Services接続に使用する信頼された証明書を削除する場合は、dsm_cコマンドラインツールを使用する必要があります。

Deep Security Managerを使用して信頼された証明書を削除するには

1. Deep Security Managerで、[管理]→[システム設定]→[セキュリティ]の順に選択します。
2. [信頼された証明書]で[証明書リストの表示]をクリックします。
3. 削除する証明書を選択し、[削除]をクリックします。

dsm_cを使用して信頼された証明書を削除するには

1. Deep Security Managerにログインします。
2. 次のコマンドを実行します。

   ```
   dsm_c -action listcerts [-purpose PURPOSE]
   ```

   「-purpose PURPOSE」はオプションのパラメータで、すべての証明書のリストを表示する場合は省略できます。「PURPOSE」に値を指定した場合は、その目的に使用する証明書だけが表示されます。

パラメータ	説明	値のサンプル
PURPOSE	証明書を使用する接続の種類。	AWS - Amazon Web Services
		DSA - コード署名
		EXCEPTION - 除外
		SSL - SSL接続

3. 削除する証明書のIDをリストから探します。
4. 次のコマンドを実行します。

```
dsm_c -action removecert -id ID
```

「ID」パラメータは必須です。

パラメータ	説明	値のサンプル
ID	削除する証明書に対してDeep Security Managerによって割り当てられたID値。	3

注意: Linux環境でDeep Security Managerを実行している場合は、dsm_c コマンドをrootユーザとして実行する必要があります。

SSLの実装と資格情報のプロビジョニング

Deep Security Agentは、コンピュータオブジェクトが双方向モードで動作するように設定されている場合、Deep Security Managerへの通信を開始するか、マネージャから連絡を受けることがあります。Deep Security Managerは、すべてのエージェントおよびアプライアンスへの接続を同様に扱います。エージェントがアクティベートされていない場合、限られたインタラクションのみが可能です。エージェントがアクティベートされている場合 (管理者によるか、エージェント起動型アクティベーション機能を介して)、完全なインタラクションが有効になります。Deep Security Managerは、TCP接続を形成する際にクライアントであったかどうかに関わらず、すべての場合においてHTTPクライアントとして機能します。エージェントおよびアプライアンスは、データを要求したり、操作を自ら開始したりすることはできません。マネージャは、イベントやステータスなどの情報を要求し、操作を呼び出したり、エージェントに設定をプッシュしたりします。このセキュリティドメインは厳密に管理されており、エージェントおよびアプライアンスがDeep Security Managerやそれが稼働しているコンピュータにアクセスすることはできません。

AgentとManagerの両方で異なる2つのセキュリティコンテンツを使用して、HTTP要求の安全なチャネルを確立します。

1. 有効化の前に、Agentはまずブートストラップ証明書を受け入れてSSLまたはTLSチャネルを確立します。
2. その認証が完了すると、今度は、接続を開始するための相互認証が必要になります。この相互認証を行うために、Managerの証明書がAgentに送信され、Agentの証明書がManagerに送信されます。エージェントは、権限が付与されたアクセスが許可される前に、証明書がDeep Security Managerであることを検証します。

安全なチャネルの確立後は、AgentはHTTP通信のサーバとして機能します。Managerへのアクセスは制限され、要求に対する応答のみが可能です。この安全なチャネルにより、認証性、暗号化による機密性、および整合性が確保されます。相互認証を使用することで、第三者によるSSL通信チャネルの不正なプロキシを防ぎ、中間者 (MiTM) 攻撃から保護することができます。ストリーム内の内部コンテンツにはGZIPが使用され、設定はPKCS #7でさらに暗号化されます。

Deep Security製品間の通信に対するSSL/TLSの復号化は推奨されません。すべてのデバイスやミドルウェアはTLSパススルー用に設定する必要があります。例えば、ファイアウォールがSSL検査を行う場合、通信を復号化してから再暗号化し、その過程で証明書を変更します。この変更により、提供された元の証明書と異なるものになります。その結果、Deep Security AgentからDeep Security Managerに通信が届くと、変更された証明書は許可されていないと見なされます。

Smart Protection Networkの接続を無効にした場合のトレンドマイクロへの情報の送信について

Smart Protection Networkが無効になっている場合、Deep Security Agentからトレンドマイクロに脅威インテリジェンスの情報が送信されることはありません。

Deep Securityのアップグレード

アップグレードについて

Trend Micro Deep Securityのアップデートの種類は次のとおりです。

- ソフトウェアのアップグレード: Deep SecurityManager,Virtual Appliance,Agent および Relayなどの新しいソフトウェア。

- セキュリティアップデート: Deep Security Agent およびVirtual Appliance ソフトウェアが潜在的な脅威を特定するために使用するルールおよび不正プログラムパターンファイル。セキュリティアップデートの種類は次のとおりです。
  - パターンファイルのアップデート: 不正プログラム対策で使用されます。
  - ルールアップデート: Used by:
    - ファイアウォール
    - 侵入防御
    - 変更監視
    - セキュリティログ監視

アプリケーションコントロールルールのアップデートは、コンピュータのソフトウェアに基づいてローカルで作成されます。トレンドマイクロから提供されたものではありません。

エージェントの不正プログラム対策 エンジンおよび仮想アプライアンス ソフトウェアは、最新の脅威に対応するために、個別にアップデートできます。"自動 不正プログラム対策 エンジンのアップデートを有効にする" on page 1665を有効にします。

トレンドマイクロでは、毎週火曜日に新しいルールのアップデートをリリースし、新たな脅威が検出された場合にアップデートを実行します。アップデートに関する情報は、トレンドマイクロの脅威百科事典に掲載されています。

Deep Security Managerによるソフトウェアアップグレードの確認方法

Deep Security Managerは定期的にトレンドマイクロのアップデートサーバに接続し、がDeep Security Managerデータベースにインポートしたソフトウェアのアップデートを確認します。次のようにします。

- Deep Security Agent
- Deep Security Virtual Appliance
- Deep Security Manager

これは、ダウンロードセンターではなく、ローカルインベントリに基づいてチェックされます。(ダウンロードセンターに新しいソフトウェアが見つかった場合は、別途アラートが表示されます)。

注意:
Deep Securityは、マイナーバージョンのアップデートのみを通知します。ソフトウェアのメジャーアップデートは通知しません。

たとえば、Deep Security Agentが9.6.100で、トレンドマイクロのリリースが9.6.200の場合、ソフトウェアアップデートが利用可能であることを示すアラートが表示されます。ただし、10.0.nnn (メジャーバージョンの差分) がリリースされていて、10.0エージェントがない場合は、アラートは表示されません(10.0が9.6.100より新しくても)。

Managerのアラートは、ソフトウェアアップデートが利用可能であることを通知します。[管理]→[アップデート]→[ソフトウェア]の [トレンドマイクロダウンロードセンター] セクションには、利用可能なアップデートがあるかどうかも表示されます。ソフトウェアをDeep Security Managerデータベースにインポート(ダウンロード) すると、配置内のソフトウェアをアップグレードできます。「 "Deep Security Agentのアップグレード" on page 1676 のアップグレード」および「 "Applianceをアップグレードする" on page 1688のアップグレード」を参照してください。

ヒント: ダウンロード可能なすべてのソフトウェアパッケージを表示するには (インポートしたことがない場合でも)、[管理]→[アップデート]→[ソフトウェア]→[ダウンロードセンター] の順に選択します。

最後のチェックがいつ実行されたか、成功したかどうか、手動でアップデートのチェックを開始するには、の[管理]→[アップデート]→[ソフトウェア]の順に選択して、「Deep Security」セクションを表示します。アップデートの確認を実行する予約タスクを設定している場合は、次回の予約確認の日時もここに示されます"Deep Security予約タスクの設定" on page 1826を参照してください。

インポートされたソフトウェアは、Deep Security Managerデータベースに格納されます。インポートされたソフトウェアは定期的にリレーに複製されます。

アップグレードのベストプラクティス

Deep Security AgentまたはDeep Security Virtual Applianceの新しいリリースを配信する場合:

- Deep Security Relaysは、ご使用の環境内のすべてのエージェントおよびアプライアンスと同じか、または新しいバージョンである必要があります。
- Deep Security RelaysはDeep Security Managerと同じバージョンである必要があります。
- Deep Securityソフトウェアのアップグレードを実行する場合、アップグレードの順序は重要です。まずDeep Security Managerをアップグレードし、次にすべてのリレー、エージェント、およびアプライアンスをアップグレードします。

注意: Deep Security 20以降、そのエージェントの最小DSMバージョンより古いDeep Security ManagerでDeep Security Agentを有効化することはできません。DSMの最小バージョンは、Deep Securityソフトウェアのダウンロードページで確認できます。

ヒント: Workload Securityを使用すると、サービスで提供されるManagerとRelayを常に最新の状態に保つことができます。環境に追加のRelayを導入する場合を除き、DSMの最小バージョンは無視して、Relayのバージョンについては考慮しません。

Deep Securityによるアップデートの整合性の検証方法

ソフトウェアアップデートとセキュリティアップデートの両方がデジタル署名されています。自動チェックに加えて、シグネチャまたはチェックサムを手動で検証する場合は、次のような外部ツールを使用できます。

- sha256sum (Linux)
- Checksum Calculator (Windows)
- jarsigner (Java Development Kit(JDK); "ソフトウェアパッケージのデジタル署名の確認" on page 445のデジタル署名をチェックする

デジタル署名

Deep Security Managerデータベースにセキュリティアップデートが表示、使用、またはインポートされた場合 (が手動で に設定されているか、の予約タスク), によって自動的に署名が検証されます) 。デジタル署名が正しいことは、ソフトウェアがトレンドマイクロから認証されており、破損していないことを示しています。デジタル署名が無効な場合、マネージャはファイルを使用しません。server0.logなどのログファイルにも警告が記録されます。

```
WARNING: ThID:85|TID:0|TNAME:Primary|UID:1|UNAME:MasterAdmin|Verifying the signature failed.
```

```
com.thirdbrigade.manager.core.general.exceptions.FileNotSignedValidationException: "corrupted_
rules.zip." has not been digitally signed by Trend Micro and cannot be imported.
```

デジタル署名が無効なセキュリティ更新プログラムパッケージを手動でインポートすると、マネージャにもエラーメッセージが表示されます。

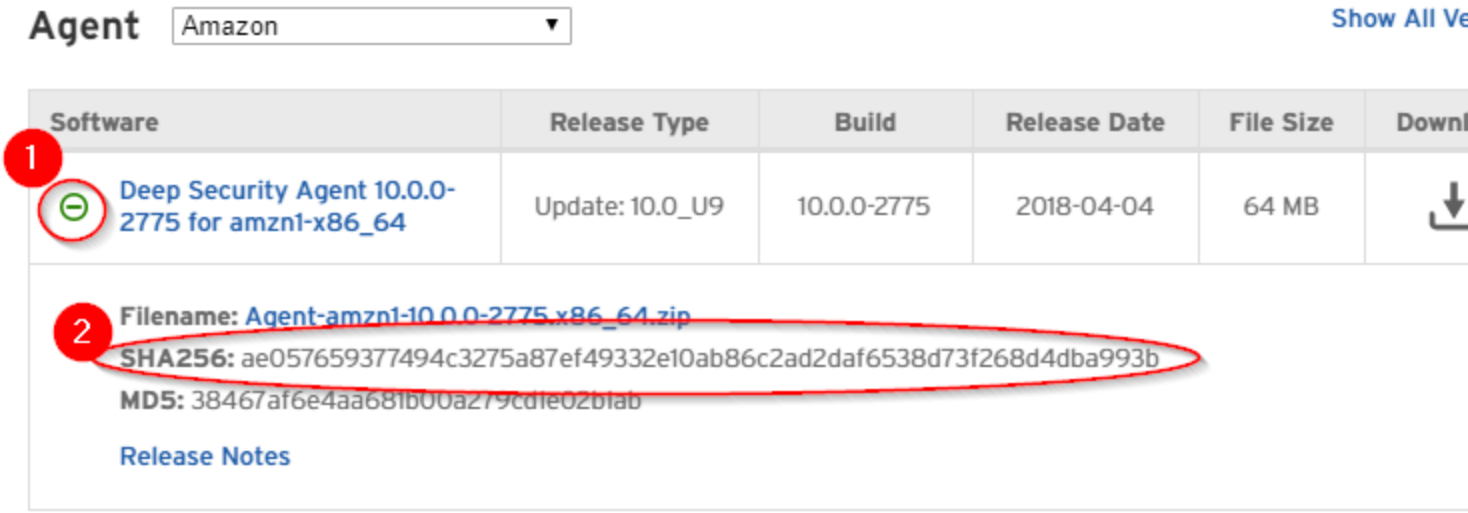
注意: 署名が適用されていない以前のバージョンのDeep Security Managerに正常にインポートされた場合でも、署名されていない古いセキュリティアップデートを使用すると検証に失敗します。保護を強化するには、代わりに新しいセキュリティアップデートを使用してください。ただし、引き続き古

いセキュリティアップデートが必要な場合は、サポートプロバイダに連絡して署名付きファイルを要求し、セキュリティアップデートを手動でインポートできます。

Deep Security Agentは、デジタル署名の妥当性検査、チェックサム(ハッシュまたはフィンガープリントとも呼ばれます) を比較し、その他の公開されていない整合性メソッドも使用します。

チェックサム

ソフトウェアチェックサム(ハッシュまたはフィンガープリントとも呼ばれる) は、ダウンロードセンターに公開されています。SHA-256ハッシュを表示するには、ソフトウェアの名前の横にある+ ボタンをクリックします。



セキュリティ更新プログラムの適用

新たな脅威を特定する上で有効なままにするには、Deep Security AgentおよびVirtual Appliance に定期的なセキュリティアップデートが必要です。

エージェント、仮想アプライアンス、、およびリレーがセキュリティアップデートを受信する前に、それらを配信する方法を定義する必要があります("追加のリレーを配信する" on page 1467 および "アップデート元を設定する" on page 1470)。次に、次のことができます。

- "セキュリティ更新プログラムを起動する" on the next page
- セキュリティアップデートのステータスを確認する
- "パターンファイルのアップデートの詳細を表示" on page 1663

- "ルールのアップデートに関する詳細の復元、インポート、または表示" on the next page
- "セキュリティ更新プログラムを構成する" on page 1664

セキュリティ更新プログラムを起動する

ヒント: アップデートを手動で確認する代わりに、予約アップデートを介してDeep Security Managerでセキュリティアップデートが自動的に確認されるように設定してください。"Deep Security予約タスクの設定" on page 1826を参照してください。

セキュリティ更新は、予約タスクに関係なく、いつでも手動で開始できます。

- すべてのクライアントおよび仮想アプライアンスのセキュリティアップデートを取得するには、[管理]→[アップデート]→[セキュリティ]に移動し、[アップデートとアップデートの確認]をクリックします。
- *の1台の*エージェントまたは仮想アプライアンスでセキュリティアップデートを取得するには、Computersに移動し、エージェントまたは仮想アプライアンスを選択して右クリックし、[Action]→[Security Updateのダウンロード]の順に選択します。

セキュリティアップデートのステータスを確認する

セキュリティ更新プログラムのステータスを表示するには、[管理]→[アップデート]→[セキュリティ]の順に選択します。

- トレンドマイクロのアップデートサーバ: トレンドマイクロのアップデートサーバに接続して最新のセキュリティアップデートを確認できるかどうかを示します。

- Deep Security: 最後に正常にチェックおよびダウンロードが実行された日時、および次回の予約チェックが実行された日時を示します。[すべてのRelayは同じコンポーネントを保持しています]では、すべてのRelayが前回正常にダウンロードされたパターンファイルアップデートを配布していることが示されます。

  ヒント: 同期されていないステータスは通常、リレーがTrend Micro Update Serverに接続できないことを示します。通常、これは正常ではありません。ネットワーク接続の問題を修正する必要があります。ただし、「エアギャップのある」配置では、ネットワークの隔離は意図的に行われます。手動でアップデートを提供する必要があります。

- コンピュータ: いずれかのコンピュータが、*現在リレー上のパターンファイルのアップデートと比較して*古いかどうかを示します。すべてのコンピュータに、割り当てられたリレーから最新のパターンファイ

ルのアップデートを取得するように指示するには、[パターンファイルをコンピュータに送信]をクリックします。

パターンファイルのアップデートの詳細を表示

不正プログラム対策 パターンファイルアップデートのコンポーネントのリストを表示するには、の[管理]→[アップデート]→[セキュリティ]→[パターンファイル]の順に選択します。このページは、Deep Securityに有効なRelayがある場合のみ表示されます。

- コンポーネント: アップデートコンポーネントの種類。
- 使用目的: このコンポーネントが対象とするDeep Security製品。
- プラットフォーム: アップデート対象のOS。
- 現在のバージョン: Deep Securityリレーによって現在配信されているコンポーネントのバージョン。

  ヒント: 保護されたコンピュータで使用されているセキュリティ更新プログラムのコンポーネントのバージョンを確認するには、[Computers]に移動してコンピュータをダブルクリックし、[Updates]を選択します。
- 最終更新日: 現在のセキュリティ更新プログラムがトレンドマイクロからダウンロードされたとき。

ルールのアップデートに関する詳細の復元、インポート、または表示

Deep Security Managerデータベースにダウンロードされた侵入防御, 変更監視 および セキュリティログ監視 ルールのリストを表示するには、の[管理]→[アップデート]→[セキュリティ]→[ルール]に移動します。

そこから、以下を実行できます。

- ルールアップデートの詳細を表示: ルールアップデートを選択し、[の表示]をクリックします。詳細には、アップデートの特定のルールのリストが含まれます。

  ヒント: リレーが配信しているルールアップデートのバージョンを確認するには、Computersに移動し、リレーをダブルクリックして、[Security Updates]を選択します。そのコンピュータで 不正プログラム対策 が有効になっている場合は、コンピュータのパターンファイルも表示されます。

- ルールアップデートをロールバックする: 最近のルールアップデートで問題が発生した場合は、元のルールバージョンに戻すことができます。元に戻すルールのアップデートを選択し、[Rollback]をクリックします。Deep Security Managerはプレビュー変更の概要を生成します。この結果、ファイナライズ前に結果を確認できます。

  注意: 復帰ルールによって影響を受けたすべてのポリシーは、*のすべてのコンピュータでこれらのポリシー*を使用してただちにアップデートされます。

- 現在のルールセットを再度適用します: ✔ は、ルールアップデートが適用されていることを示します。ルールアップデートを保護されたコンピュータに再度適用するには、ルールアップデートを右クリックし、[Reapply]をクリックします。

- ルールアップデートのインポート: 通常、ルールアップデートは で手動で にインポートされるか、自動的に(で予約タスク).によってインポートされます。ただし、配信がインターネット上のトレンドマイクロのアップデートサーバに接続されていない場合(「Air-Gapped」配信), の場合)、またはサポートプロバイダからの要求がある場合は、このボタンをクリックして手動でアップロードおよびインポートを実行できます。セキュリティ更新プログラムパッケージ。

- ルールアップデートをエクスポート: 通常、サポートプロバイダからの問い合わせがない限り、ルールアップデートをエクスポートする必要はありません。

- ルールアップデートを削除: 選択したルールアップデートをDeep Security Managerデータベースから削除します。

  ヒント: Deep Security Managerデータベースに保持されるルールのアップデート数を制限するには、[管理]→[システム設定]→[ストレージ]の順に選択します。

セキュリティ更新プログラムパッケージには有効なデジタル署名が必要です。無効なパッケージを表示しようとするか、), 署名のない古いセキュリティ更新プログラムを使用すると、マネージャにエラーメッセージが表示されます。"Deep Securityによるアップデートの整合性の検証方法" on page 1660。

セキュリティ更新プログラムを構成する

次の設定を行うことができます。

- "ルールの自動パッチを有効にする" on the next page
- "自動 不正プログラム対策 エンジンのアップデートを有効にする" on the next page

- "古いクライアントのセキュリティ更新を有効にする" on the next page
- "最新のセキュリティ更新プログラムの警告のしきい値を変更します。" on the next page

ルールの自動パッチを有効にする

トレンドマイクロでは、既存のDeep Securityルールをアップデートしてパフォーマンスを改善したり、バグを修正することがあります。これらのパッチを自動的に適用するには、[コンピュータ]または[ポリシーエディタ]→[設定]→[一般]の順に選択し、[ポリシーの変更をすぐに送信する]で[ポリシーの変更をコンピュータに自動的に送信する]を選択し、ドロップダウンを[はい]に設定します。選択されていない場合は、ダウンロードしたルールのアップデートをポリシーに手動で適用する必要があります。[管理]→[システム設定]→[アップデート]に移動し、[ルールのアップデートをポリシーに自動的に適用する]をクリックします。

注意: 初期設定では、ポリシーに対する変更は自動的に適用されます。

自動不正プログラム対策エンジンのアップデートを有効にする

初期設定では、Deep Security AgentまたはVirtual Appliance ソフトウェアをアップデートすると、Deep Security 不正プログラム対策 がアップデートされます。頻繁にソフトウェアをアップデートしない場合、不正プログラム対策 エンジンは、頻繁にアップデートする必要がある不正プログラムパターンファイルよりも古いバージョンになる可能性があります。

保護機能を強化するために、エージェントおよび仮想アプライアンスを設定して、ソフトウェアの不正プログラム対策 エンジン部分を自動的に最新の状態に保つことができます。この方法は、使用するセキュリティアップデートと類似しています。

1. [Computers]または[Policies]に移動します。
2. コンピュータまたはポリシーをダブルクリックします。
3. [設定]→[検索エンジンアップデート] の順に選択します。
4. 不正プログラム対策エンジンを自動的にアップデートするを更新する場合は、[はい]を選択します。

   この設定が無効な場合は、の[コンピュータの詳細情報]→[アップデート]→[高度な脅威検索エンジン]で、[は最新のが表示されます]セクションに「N/A".

注意: この設定にかかわらず、リレーには常に最新の不正プログラム対策 エンジンアップデートが送信されます。これにより、同じリレーグループのリレーのローカル保護およびアップデート元が最新の状態に維持されます。そのため、Relay上でエンジンのアップデートを直接有効または無効にすることはできません。

古いクライアントのセキュリティ更新を有効にする

一部のプラットフォームでは、Deep Security Manager20では旧バージョンがサポートされます。Deep Security Agentのプラットフォーム "Deep Security Agentのプラットフォーム" on page 400を参照してください。

初期設定では、ディスク領域を節約するため、Deep Security Relayはこれらの古いエージェントのセキュリティアップデートをダウンロードおよび配信しません。セキュリティアップデートを有効にするには、の[管理]→[システム設定]→[アップデート]の順に選択します。[8.0および9.0のAgentのアップデートを許可] を選択します。

注意: Deep Security Agent 8.0はサポートされなくなりました。このチェックボックスは、9.0エージェントにのみ適用されます。

最新のセキュリティ更新プログラムの警告のしきい値を変更します。

更新プログラムがトレンドマイクロからダウンロードされてしばらく使用可能になっているが、コンピュータがまだアップデートされていない場合、アラートが発生します。ルールのアップデートについては、初期設定では30分です。パターンファイルのアップデートの場合、初期設定では1時間です。

アラートの時間制限を変更する場合は、の[管理]→[システム設定]→[アラート]の順に選択し、アラートを発生させるまでに更新が保留されるまでの時間を設定します。

新しいパターンファイルアップデートアラートのメールの無効化

Deep Security ManagerでDeep Security Managerをダウンロードした1時間後に、セキュリティアップデートがエージェントに適用されていない場合、[New Pattern Update is Downloaded and Available] アラートが表示されます。1時間という期間は変更できません。アラートがデフォルトで発令される場合、このアラートはメールで送信されます。

アップデートの解決に1時間では足りないため、このようなメールアラートを数多く受信する場合は、このアラートのメール通知を無効にできます。その代わり、アラートが発令される時間を設定できるように、「コンピュータがアップデートを受信していない」アラートに関するメールメッセージを受信できます。

1. Deep Security Managerがセキュリティアップデートを自動的にダウンロードするように設定するには、Deep Security Managerで[管理]→[予約タスク]の順にクリックします。
2. 種類が[セキュリティアップデートの確認] の予約タスクがない場合は、そのタスクを作成します("Deep Security予約タスクの設定" on page 1826を参照してください)。
3. [管理]→[システム設定]→[アップデート] の順にクリックします。[セキュリティ更新]の[規則]セクションで、[新しいルールアップデートを自動的にポリシーに適用]が選択されている。
4. [アラート]→[アラートの設定] の順にクリックします。

5. [アラートの設定] 画面で、[新しいパターンファイルアップデートがダウンロード済みで利用可能] アラートをクリックし、[プロパティ] をクリックします。
6. [アラート情報] 画面で、[このアラートの発令時、通知のメールを送信する] を選択解除し、[OK] をクリックします。
7. [コンピュータがアップデートを受信していない] アラートをクリックして、[プロパティ] をクリックします。
8. [このアラートの発令時、通知のメールを送信する] が選択されていることを確認し、[OK] をクリックします。
   アラートはアップデートを7日間保留すると発令されます。
9. アップデートを保留してから任意の時間の経過後にアラートを発令するには、[管理]→[システム設定]→[アラート] をクリックします。
10. [アラート] エリアで、ドロップダウンを使用して時間を選択し、[保存] をクリックします。

ソフトウェアアップデートを配布するWebサーバの使用

Deep Securityソフトウェアのアップデートは、通常、リレーによってホストされ、配信されます。ただし、すでにWebサーバがある場合は、Relayではなく Webサーバ経由でソフトウェアアップデートを提供できます。そのためには、Relayのソフトウェアリポジトリのミラーを Webサーバに作成する必要があります。

注意: Deep Security Agentは ソフトウェアの アップデートをWebサーバからダウンロードできますが、不正プログラム対策やIPSシグネチャなどの セキュリティパッケージのアップデートを配信するには、少なくとも1つのリレーが必要です("セキュリティ更新プログラムの適用" on page 1661を参照) 。

注意: ソフトウェアの配布に独自のWebサーバを使用している場合でも、[管理]→[アップデート]→[ソフトウェア] に移動し、Deep Security Managerのデータベースにソフトウェアをインポートする必要があります。次に、ソフトウェアWebサーバに、Deep Security Managerにインポートされたソフトウェアと同じソフトウェアが含まれていることを確認する必要があります。同じものが格納されていないと、利用可能なアップデートに関する通知を表示するアラートなどのインジケータが正常に機能しません。

Webサーバのシステム要件

ディスク容量: 20 GB

ポート: Webサーバのポートと Relayのポート

フォルダ構造をコピーする

Relay有効化済みAgentのソフトウェアリポジトリフォルダのフォルダ構造のミラーを作成します。方法はプラットフォームおよびネットワークによって異なります。たとえば、Linuxコンピュータおよび SSHを許可す

るネットワークを使用している場合は、SSH経由のrsyncを使用できます。

Windowsの場合、Relay有効化済みAgentのソフトウェアリポジトリフォルダの初期設定の場所は次のとおりです。

```
C:\ProgramData\Trend Micro\Deep Security Agent\relay\www\dsa\
```

Linuxの場合、Relayのソフトウェアリポジトリフォルダの初期設定の場所は次のとおりです。

```
/var/opt/ds_agent/relay/www/dsa/
```

フォルダは次のような構造になっています。

```
|-- dsa
|    |-- <Platform>.<Architecture>
|         |--  <Filename>
|         |--  <Filename>
|         |--  ...
|
|    |--<Platform>.<Architecture>
|         |--  <Filename>
|         |--  <Filename>
|         |--  ...
```

次に例を示します。

```
|-- dsa
|    |--  CentOS_<version>.x86_64
|         |--   Feature-AM-CentOS_<version>.x86_64.dsp
|         |--   Feature-DPI-CentOS_<version>.x86_64.dsp
|         |--   Feature-FW-CentOS_<version>.x86_64.dsp
|         |--   Feature-IM-CentOS_<version>.x86_64.dsp
|         |--  ...
|
|    |--  RedHat_EL6.x86_64
|         |--   Agent-Core-RedHat_<version>.x86_64.rpm
|         |--   Feature-AM-RedHat_<version>.x86_64.dsp
|         |--   Feature-DPI-RedHat_<version>.x86_64.dsp
```

```
|          |--   Feature-FW-RedHat_<version>.x86_64.dsp
|          |--   ...
|          |--   Plugin-Filter_2_6_32_131_0_15_el6_x86_64-RedHat_
<version>.x86_64.dsp
|          |--   Plugin-Filter_2_6_32_131_12_1_el6_x86_64-RedHat_
<version>.x86_64.dsp
|          |--   ...
|
|     |-- Windows.x86_64
|          |--   Agent-Core-Windows-<version>.x86_64.msi
|          |--   Agent-Core-Windows-<version>.x86_64.msi
|          |--   Feature-AM-Windows-<version>.x86_64.dsp
|          |--   Feature-AM-Windows-<version>.x86_64.dsp
|          |--   Feature-DPI-Windows-<version>.x86_64.dsp
|          |--   Feature-DPI-Windows-<version>.x86_64.dsp
|          |--   ...
|          |--   Plugin-Filter-Windows-<version>.x86_64.dsp
|          |--   Plugin-Filter-Windows-<version>.x86_64.dsp
|          |--   ...
```

上記の例では少数のファイルとフォルダしか示されていませんが、完全なdsaフォルダ内には、もっと多くのファイルとフォルダが存在します。ディスク容量や帯域幅を節約する必要がある場合は、そのすべてのミラーを作成する必要はなく、使用しているコンピュータのプラットフォームに適用されるファイルのミラーだけで十分です。

新しいソフトウェアリポジトリを使用するようにAgentを設定する

Webサーバ上のミラーが完了したら、Webサーバからソフトウェアアップデートを取得するようにDeep Security Agentを設定します。

1. Deep Security Managerで、[管理]→[システム設定]→[アップデート]の順に選択します。
2. [ソフトウェアアップデート] セクションで、WebサーバのミラーフォルダのURLを入力します。
3. [保存] をクリックします。

注意: AgentとWebサーバの間の通信が安定していることを確認します。接続がブロックされた場合、Agentは代わりにRelayを使用します。

Deep Security Managerをアップグレード

Deep Security Manager、Deep Security Manager、および仮想アプライアンスをアップグレードする前に、Deep Security Managerをアップグレードしてください。

- "開始前の準備" below
- "マネージャをアップグレードする" on the next pageのバージョンアップ
- "古いバージョンのReleaseが2つ以上ある場合はマネージャをアップグレードしてください" on the next page
- "マルチノード配置でマネージャをアップグレードする" on page 1672
- "マルチテナント環境でマネージャをアップグレードする" on page 1673
- "アップグレードするとどうなりますか? " on page 1673
- "アップグレード後のタスク" on page 1673
- "マネージャのバージョンアップのトラブルシューティング(ログファイル) " on page 1674
- "マネージャのバージョンアップに失敗しました(ロールバック) " on page 1674のアップグレードに失敗しました(ロールバック)

開始前の準備

Managerをアップグレードする前に、次のタスクを完了してください。

1. サポート対象のバージョンからアップグレードしていることを確認してください。サポートされるバージョンの詳細については、「 "サポートされるアップグレードパス" on page 116」を参照してください。
2. 配置をバックアップします。
   - マネージャーをバックアップします。サーバのシステムの復元ポイントまたは仮想マシンのスナップショットを作成します。
   - データベースサーバ上のマネージャのデータベースをバックアップします。アップグレードによってデータベーススキーマが変更される可能性があるため、元のデータベースをバックアップする必要があります。
   - バックアップを検証してください。バックアップがなく、インストーラの処理が何らかの理由で中断された場合、環境を元に戻すことができません。この場合、環境全体の再インストールが必要になることがあります。
3. 新しいマネージャのシステム要件とサイジングのガイドラインを確認する: "システム要件 " on page 400と"サイジング" on page 417を参照してください。a>。

> 注意: Deep Security 20のサイジングガイドラインはDeep Security 12のサイジングガイドラインとは異なります。現在の環境がDeep Security 20のガイドラインを満たしていることを確認してから、バージョンアップしてください。

4. マネージャソフトウェアをダウンロード: https://help.deepsecurity.trendmicro.com/ja-jp/software.htmlから入手できます。
5. マネージャのインストーラファイルのデジタル署名を確認します。"インストーラファイル (EXE、MSI、RPM、またはDEBファイル) の署名の確認" on page 447を参照してください。
6. 準備完了チェックを実行します。"準備チェックを実行する" on page 458。

マネージャをアップグレードする

マネージャをアップグレードするには、"Managerをインストールする" on page 460を参照してください。参照インストール手順は、アップグレードでも同様に機能します。

> 注意:
> Deep Security 11からアップグレードする場合で、Microsoft SQL Serverを使用する場合は、システムイベントを含むさまざまなテーブルのプライマリキーが最大整数値に達しないようにIntegerからBigIntに更新されているため、インストーラにデータ移行手順が追加されています。
>
> 場合によっては、メンテナンス期間を長くする必要があります。所要時間は、データベースの負荷、ネットワーク帯域幅と待ち時間、および移行する既存のシステムイベントの数によって異なります。1分あたりの推定システムイベント数は50,000-150,000です。

古いバージョンのReleaseが2つ以上ある場合はマネージャをアップグレードしてください

管理者のインストーラは、2つのメジャーリリースからのアップグレードのみをサポートしています。そのバージョンよりも古いバージョンのマネージャバージョンを使用している場合は、アップグレードパスに「ホップ数」が表示されます.': 最初のホップが少し前のバージョンに戻ってきます。次のバージョンでは最新バージョンにアップデートされます。

古いマネージャから新しいマネージャにアップグレードする方法については、後者のインストールガイドを参照してください。

他のバージョンのドキュメントを取得する

マルチノード配置でマネージャをアップグレードする

Managerをアップグレードするには

1. 各マネージャノードをバックアップします。サーバのシステムの復元ポイントまたは仮想マシンのスナップショットを作成します。
2. すべてのノードを停止します。
3. 最初のノードでマネージャをアップグレードします。

   警告: 複数のノードで同時にインストーラを実行しないでください。アップグレードを同時に実行すると、データベースが破損する可能性があります。この場合は、データベースのバックアップを復元してから、再度アップグレードを開始する必要があります。
4. 最初のノードのアップグレードが完了すると、そのノードはサービスを開始します。他のノードがアップグレードされるまでは、このノードのソフトウェアだけがデータベースと互換性があるため、最初は唯一利用可能なManagerとなります。このノードがすべてのジョブを実行する必要があるため、この間はパフォーマンスが低下する場合があります。[管理]→[システム情報] の [アクティビティグラフ付きネットワークマップ] に、他のノードがオフラインであり、アップグレードが必要なことが表示されます。
5. 他のノードをアップグレードします。アップグレードすると、オンラインに戻り、再度負荷分散を開始します。
6. カスタムのマスターキーを設定した場合は、masterkeyコマンドを実行して、既存のデータをいずれか*1*つのノードでのみ暗号化します。

マネージャOSをバージョンアップするには

1. 新しいノードを追加して、古いノードをアップグレードする際に使用可能なノードが1つ以上あるようにします。"ノードを追加する" on page 506を参照してください。
2. 古いノードを廃止します。"ノードを削除する" on page 507を参照してください。
3. 廃止されたノードのOSをアップグレードします。
4. 古いノードにDeep Security Managerを再インストールします。これにより、ノードが既存のインストールに再接続されます。

マルチテナント環境でマネージャをアップグレードする

詳細については、"マルチテナント環境のアップグレード" on page 499 のアップグレードを参照してください。

アップグレードするとどうなりますか?

アップグレードすると、インストーラは次の処理を実行します。

- 新しいDeep Securityソフトウェアをインストール
- 既存のコンピュータの詳細、ポリシー、侵入防御ルール、ファイアウォールルールなどを保持します。
- 新しい形式にデータを移行します(必要な場合)。
- 必要に応じてデータベーススキーマを変更します。
- イベントデータの移行を開始します

インストーラを終了すると、アップグレードが続行されます。次の処理が行われます。

1. Managerサービスが再起動します。
2. Managerは、新しいデータベーススキーマへのイベントデータの移行を続行します。

   画面下部のステータスバーに、新しいイベントおよびアラート(エラーが発生した場合)と一緒に進捗状況が表示されます。合計移行時間は、データ量、ディスクの速度、RAM、および処理能力によって異なります。
3. イベントデータの移行中も、新しいイベントデータは通常どおり記録されます。

   > 注意: データベースのアップグレードの移行が完了するまで、古いシステムイベントデータを含む結果が不完全な可能性があります。

追加タスクは、マルチノードまたはマルチテナントのアップグレード時に実行されます。詳細については、"マルチノード配置でマネージャをアップグレードする" on the previous page および "マルチテナント環境でマネージャをアップグレードする" above。

アップグレード後のタスク

アップグレード後、次のタスクを完了することができます:

- サーバ証明書の置き換え: アップグレード後、Deep Security Managerのサーバ証明書は新規インストールを行わない限り保持されます。証明書がSHA-1などの弱い暗号アルゴリズムを使用して作成された場合、証明書の置き換えを検討してください。より強力な暗号化を使用することで、最新の標準に準拠し、最新のエクスプロイトや攻撃に対する保護を強化できます。"Deep Securityの暗号化アルゴリズムのアップグレード" on page 1646および"Deep Security ManagerのTLS証明書を変更します。" on page 1622を参照してください。

- vCenterを削除してから再追加してください

  : NSX-TでDeep Security Virtual Applianceを使用している場合は、NSX-T環境からDeep Securityをアンインストールし、NSX-Tをマネージャに再追加して更新されたサービスを登録してください。登録されるサービスは次のとおりです:

  - E-Wネットワークイントロスペクション
  - エンドポイント保護

マネージャのバージョンアップのトラブルシューティング(ログファイル)

何らかの理由でスキーマの変更が中断された場合、エラーがログに記録されます。

`<install-directory>/DBUpgrade/SchemaUpdate`

初期設定の `<install-directory>` は `/opt/dsm` (Linux)または `C:\Program Files\Trend Micro\Deep Security Manager` (Windows)です。

上記のディレクトリ内には、次の2種類のファイルが作成されます。

- `T-00000-Plan.txt` - このファイルには、インストーラがスキーマのアップデートに使用するすべてのデータ定義言語(DDL) SQL文が含まれています。
- `T-00000-Progress.txt` - このファイルには、スキーマアップデートの進捗ログが含まれています。インストーラが終了すると、ファイル名が `T-00000-Done.txt` (成功アップデート) または `T-00000-Failed.txt` (アップデート失敗)に変更されます。

注意: マルチテナント環境では、ファイル名の「00000」がテナント番号に置き換えられます(テナントt1の場合は「00001」など) 。

マネージャのバージョンアップに失敗しました(ロールバック)

Deep Security Manager 20へのアップグレード時に問題が発生した場合は、次の場合に迅速に機能状態に戻すことができます。

- アップグレード前にデータベースをバックアップしている。
- Agent、Relay、Virtual Applianceをアップグレードしていない(またはアップグレード前に作成した仮想マシンスナップショットやシステムバックアップがある)。

1. Deep Security Managerサービスを停止します。
2. データベースを復元します。
3. すべてのDeep Security Managerサーバノードを復元します。
4. アップグレード中にDeep Security Managerのホスト名、FQDN、またはIPアドレスを変更した場合は、それらを復元します。
5. Agent、Relay、Virtual Applianceを復元します。
6. Deep Security Managerサービスを開始します。
7. Managerとエージェント間の接続を含め、Deep Security Managerへの接続を確認します。

Deep Security Relay

すべてのリレーをアップグレードしてからエージェントをアップグレードしてください(詳細については、"アップグレードのベストプラクティス" on page 1659を参照してください)。リレーをアップグレードするには、次の2つの方法があります。

マネージャからリレーをアップグレードする

1. Deep Security Managerにログインします。
2. Deep Securityリレーを特定します。いずれか:
   - [コンピュータ]に移動します。メイン画面で、Relayアイコン( ) の付いたコンピュータを探します。
   - [管理]を選択します。左側で、[アップデート]→[Relayの管理]をクリックします。メイン画面で、[Relayグループ]を展開します。使用しているRelayがRelayアイコン( ) 付きで表示されます。
3. アップグレードするリレーをダブルクリックします。
4. [処理]タブをクリックします。
5. [Agentのアップグレード]をクリックします。

   表示されるウィザードの手順に従います。手順はDeep Security Agentのアップグレードと似ています。これは、リレーはリレー機能が有効になっているエージェントにすぎないためです。詳細については、"Deep Security Agentのアップグレード" on the next pageのアップグレードを参照してください。

インストーラを手動で実行してリレーをアップグレードする

場合によっては、Deep Security Managerからリレーソフトウェアをアップグレードできないことがあります。このような場合は、リレーを手動でアップグレードできます。詳細な手順については、"エージェントを手動でアップグレードする" on page 1680) を参照してください。参照される手順はエージェント用ですが、リレーでも同様に動作します。

Deep Security Agentのアップグレード

ソフトウェアのアップグレードは、Deep Security Managerまたはサードパーティの配置システムから開始できます。

このトピックの内容:

- "アップグレードを開始する前に" below
- "アラートからAgentをアップグレードする" on page 1678
- "複数のエージェントを一度にアップグレードする" on page 1678
- "[クライアント]ページからエージェントをアップグレードします。" on page 1679
- "アクティベーション時にエージェントをアップグレードする" on page 1679
- "予約タスクからAgentをアップグレードする" on page 1679
- "エージェントを手動でアップグレードする" on page 1680
- "仮想アプライアンスに組み込まれているエージェントを自動的にアップグレードする" on page 1683
- "Agentアップグレードのベストプラクティス" on page 1684

アップグレードを開始する前に

エージェントのアップグレードを開始する前に:

1. サポート対象のバージョンからアップグレードしていることを確認してください。次の場所からDeep Security 20 にアップグレードできます。
   - Deep Security 11 LTS(GAバージョンまたはLTSアップデート)
   - ディープセキュリティ11の機能リリース
   - Deep Security 12 LTS(GAバージョンまたはLTSアップデート)
   - ディープセキュリティ12機能リリース

2. アップグレードするエージェントコンピュータをバックアップします。各エージェントのシステム復元ポイントまたはVMスナップショットを作成します。
3. 新しいエージェントパッケージをマネージャにインポートします。"エージェントソフトウェアのインポート" on page 515を参照してください。
4. すべてのDeep Securityリレーをアップグレードします。「"Deep Security Relay" on page 1675 Relayのアップグレード」を参照してください。

> 警告: エージェントのアップグレードを開始する前に、すべてのリレーをアップグレードする必要があります。そうしないと、アップグレードが失敗する可能性があります。

> 注意: Deep Security Agentをアップグレードすると、Deep Security Agentで署名が検証され、署名後にソフトウェアファイルが変更されていないことが確認されます。詳細については、「"エージェントパッケージの整合性チェック" on page 1863」を参照してください。

次に、以下のプラットフォーム固有の注意事項を確認し、推奨されるタスクを完了します。

Linuxエージェントのアップグレードに関する注意事項

LinuxプラットフォームでDeep Security Agentをアップグレードする前に、エージェントの最新バージョンでOSカーネルがサポートされていることを確認してください。詳細については、"Linuxカーネルの互換性" on page 400

Windowsクライアントのアップグレードに関する注意事項

不正プログラム対策が有効になっているWindowsでDeep Security Agent 12以降をバージョンアップした直後に、不正プログラム対策エンジンが「オフライン'.」として表示されることがあることに注意してください。アップグレード後、最初のハートビートが発生した後、エンジンは「オンライン」に戻ります。

Solarisエージェントのアップグレードに関する注意事項

- Solaris 11でDeep Security Agent 9.0からアップグレードする場合は、Deep Security Agent 9.0.0-5616または9.0以降のAgentにアップグレードしてからDeep Security Agent 11.0にアップグレードする必要があります。それ以前のビルドから直接アップグレードすると、Agentを起動できなくなる可能性があります。この問題が発生した場合は、"Solaris 11でのアップグレードの問題を解決する" on page 1990を参照してください。

- Solarisでのアップグレードには、完了までに5分以上かかることがあります。

AIXエージェントのアップグレードに関する注意事項

この時点では、AIXのアップグレードに関する注意事項はありません。

これで、このトピックで説明するいずれかの方法を使用してエージェントをアップグレードする準備が整いました。

アラートからAgentをアップグレードする

新しいAgentソフトウェアバージョンが利用可能になると、[アラート] にメッセージが表示されます。



1. アラートで [詳細の表示] をクリックし、[旧版のコンピュータをすべて表示] をクリックします。コンピュータが表示され、ソフトウェアアップデートステータスが旧版であるすべてのコンピュータが表示されます。「古い」とみなされるのは、設定したバージョンコントロールルールによって決まります。詳細については、"エージェントのバージョン管理を設定する" on page 1492の設定を参照してください。
2. "[クライアント]ページからエージェントをアップグレードします。" on the next page または "エージェントを手動でアップグレードする" on page 1680。

複数のエージェントを一度にアップグレードする

1. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]の順に選択します。
2. メイン画面で、[Computers]セクションの下を参照して、アップグレードが利用可能なクライアントまたは仮想アプライアンスが実行中であることを確認します。このチェックは、Deep Securityにインポートされたソフトウェアに対してのみ実行され、ダウンロードセンターから入手可能なソフトウェアに対しては実行されません。
3. [Upgrade Agent / Appliance Software]をクリックして、古いコンピュータをすべてアップグレードします。「古い」とみなされるのは、設定したバージョンコントロールルールによって決まります。詳細については、"エージェントのバージョン管理を設定する" on page 1492の設定を参照してください。

[クライアント]ページからエージェントをアップグレードします。

1. Deep Security Managerで、Computersに移動し、次の手順を実行します。
   - アップグレードするコンピュータを右クリックし、[処理]→[クライアントソフトウェアのアップグレード]の順に選択します。

     または

   - アップグレードするコンピュータを選択し、上部のActionsボタンをクリックし、[Upgrade Agent Software]を選択します。

     または

   - アップグレードするコンピュータをダブルクリックし、[コンピュータの詳細]ダイアログボックスで[Upgrade Agent]ボタンをクリックします。

   警告: 失敗を防ぐには、Agentの前にRelayをアップグレードする必要があります。詳細を表示。リレーを識別するには、リレーアイコン( )。
2. 表示されたダイアログボックスで、[Agentバージョン]を選択します。初期設定の[プラットフォーム用の最新バージョンを使用 (X.Y.Z.NNNN)]を選択することをお勧めします。[次へ]をクリックします。

アクティベーション時にエージェントをアップグレードする

Deep Security AgentがLinuxまたはWindows上にインストールされている場合は、自動的にエージェントがアクティブ化または再アクティブ化されたとき、あなたのDeep Security Managerと互換性のある最新のソフトウェアバージョンにエージェントをアップグレードすることもできます。詳細については、"Agentを有効化するときに自動的にアップグレードする" on page 1513を参照してください。

予約タスクからAgentをアップグレードする

予約タスクを作成して、設定したスケジュールでAgentのグループをアップグレードできます。詳細については、Agentアップグレードの予約タスクを参照してください。

エージェントを手動でアップグレードする

Deep Security Managerからエージェントソフトウェアをアップグレードできないことがあります。理由は次のとおりです。

- マネージャとクライアントコンピュータ間の接続に制限があります。
- エージェントソフトウェアが古すぎます。マネージャはサポートを停止しています。
- サードパーティ製のシステムを使用してアップグレードを展開することをお勧めします。

上記のシナリオのいずれかで状況が説明されている場合は、インストーラを手動で実行してエージェントをアップグレードできます。この方法は、OSによって異なります。

Windowsでエージェントをアップグレードする

1. エージェント自己保護を無効にして、インストーラがエージェントを変更できるようにします。自己保護を無効にするには
   a. Deep Security Managerで、**コンピュータエディタ**[1]→[設定]→[一般]の順に選択します。
   b. [Agentセルフプロテクション]で、[ローカルのエンドユーザによるエージェントのアンインストール、停止、または変更を拒否]を選択解除するか、ローカルでオーバーライドするためのパスワードを入力します。
2. 新しいエージェントZIPをマネージャからエクスポートします。手順については、"Agentのインストーラをエクスポートする" on page 517 のエクスポートを参照してください。プラットフォームに複数の新しいエージェントがある場合は、最新のエージェントを選択します。
3. ZIPをエージェントコンピュータにコピーして解凍します。
4. ZIPファイルのルートにあるMSIファイルをダブルクリックします。インストーラによって以前のエージェントが検出され、アップグレードが実行されます。

Linuxでエージェントをアップグレードする

1. インストーラーがエージェントに変更を加えられるようにするために、エージェントセルフプロテクションを無効にします。

[1] コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

2. 新しいエージェントのZIPファイルをマネージャからエクスポートします。手順については"Agentのインストーラをエクスポートする" on page 517を参照してください。プラットフォームに複数の新しいエージェントが利用可能な場合は、最新のものを選択してください。
3. ZIPファイルをエージェントコンピュータにコピーして解凍してください。
4. コンピュータがRPMパッケージマネージャ(Red Hat、CentOS、Amazon Linux、Cloud Linux、SUSE) を使用している場合、次のコマンドを実行してください。

   ```
   rpm -U <new agent installer rpm>
   ```

   -U 引数は、インストーラにアップグレードの実行を指示します。

   dpkgパッケージマネージャ(DebianまたはUbuntu) を使用しているコンピュータの場合は、次のコマンドを入力します。

   ```
   dpkg -i <new agent installer dpkg>
   ```

エージェントをSolaris上でアップグレードする

1. 新しいエージェントZIPをマネージャからエクスポートします。手順については、"Agentのインストーラをエクスポートする" on page 517 のエクスポートを参照してください。プラットフォームに複数の新しいエージェントがある場合は、最新のエージェントを選択します。
2. ZIPをエージェントコンピュータにコピーして解凍します。
3. インストーラを実行します。

- Solaris 11、1つのゾーン(グローバルゾーンで実行):

  x86: `pkg update -g file:///mnt/Agent-Solaris_5.11-9.x.x-xxxx.x86_64/Agent-Core-Solaris_5.11-9.x.x-xxxx.x86_64.p5p pkg:/security/ds-agent`

  SPARC: `pkg update -g file:///mnt/Agent-Solaris_5.11-9.x.x-xxxx.x86_64/Agent-Solaris_5.11-9.x.x-xxxx.sparc.p5p pkg:/security/ds-agent`

- Solaris 11、複数のゾーン(グローバルゾーンで実行):

  ```
  mkdir <path>
  pkgrepo create <path>
  pkgrecv -s file://<dsa core p5p file location> -d <path> '*'
  pkg set-publisher -g <path> trendmicro
  ```

```
pkg update pkg://trendmicro/security/ds-agent
pkg unset-publisher trendmicro
rm -rf <path>
```

- Solaris 10：次の内容の ds_adm.file というインストール設定ファイルを作成し、ルートディレクトリに保存します。次に、以下のコマンドを実行してパッケージをインストールします。

  pkgadd -G -v -a /root/ds_adm.file -d Agent-Core-Solaris_5.10_U7-10.0.0-1783.x86_64.pkg

ds_adm.fileの内容

```
mail=
instance=overwrite
partial=nocheck
runlevel=quit
idepend=nocheck
rdepend=quit
space=quit
setuid=nocheck
conflict=quit
action=nocheck
proxy=
basedir=default\
```

AIX上のエージェントをアップグレードする

1. 新しいエージェントZIPをマネージャからエクスポートします。手順については、"Agentのインストーラをエクスポートする" on page 517 のエクスポートを参照してください。プラットフォームに複数の新しいエージェントがある場合は、最新のエージェントを選択します。

---

2. ZIPをエージェントコンピュータにコピーして解凍します。BFFファイルが使用可能になります。
3. BFFファイルをAIXコンピュータ上の /tmp などの一時フォルダにコピーします。詳細な手順については、"エージェントを手動でインストールする" on page 537) を参照してください。
4. エージェントをアップグレードしてください。次のコマンドを使用します。

   ```
   /tmp> rm -f ./.toc
   ```

   ```
   /tmp> installp -a -d /tmp/<agent_BFF_file_name> ds_agent
   ```

   ここで、<agent_BFF_file_name> は、抽出したBFFインストーラファイルの名前に置き換えられます。

仮想アプライアンスに組み込まれているエージェントを自動的にアップグレードする

Deep Security Virtual Applianceには、Deep Security Agentが組み込まれています。Deep Securityを設定すると、仮想アプライアンスがNSXに配信されているときに、このエージェントを自動的に最新バージョンにアップグレードできます。

注意: 仮想アプライアンスをすでにNSXに配置している場合は、次の代替手順に従って組み込みエージェントをアップグレードする必要があります. "アプライアンスSVMに組み込まれているエージェントをアップグレードします" on page 1699を適用します。

NSXに仮想アプライアンスを配置する際に、組み込みエージェントの自動アップグレードを設定するには、次の手順を実行します。

1. Deep Security Managerで、最新の仮想アプライアンスパッケージをインポートしてください。"アプライアンスを配信する(NSX-T 3.x) " on page 576、または"Applianceのインストール (NSX-V)" on page 611を参照してください
2. 正しい仮想アプライアンスのパッチとエージェントをインポートします。"アプライアンスSVMに組み込まれているエージェントをアップグレードします" on page 1699を適用するを参照してください。これらの手順では、組み込みエージェントがまだ配信されていないため、最後の手順は無視してください。
3. [管理]→[システム設定]→[アップデート] の順に選択します。
4. メインペインで、Virtual Appliance Deployment 見出しを下部に表示します。

5. からDeep Security Virtual Applianceを ドロップダウンリストにアップデートするか、最新のエージェントバージョンを選択するか、または初期設定の最新(推奨)のままにしてください。

   注意: インポート済みのApplianceより前のバージョンのAgentソフトウェアは リストに表示されません。

6. [保存] をクリックします。

   仮想アプライアンスをNSXに配置すると、仮想アプライアンスに組み込まれているエージェントが自動的にアップグレードされるようになりました。配信手順については、"アプライアンスを配信する(NSX-T 3.x)" on page 576または"Applianceのインストール (NSX-V)" on page 611を参照してください。

Agentアップグレードのベストプラクティス

エージェントサーバで重大なワークロードが実行されている場合は、アップグレード時に次のベストプラクティスに従うことをお勧めします。

- コンピュータの使用率が低い場合にアップグレードします。
- 実稼働サーバをアップグレードする前に、準備環境でアップグレード手順をテストします。
- 実稼働サーバをアップグレードする場合、最初の数台については、1台ずつアップグレードします。各サーバのアップグレードは、それぞれ十分な間隔を空けてから行います。
- 特定のOSバージョン(およびアプリケーションの役割、SolarisまたはAIX), の場合は、グループ内の残りのサーバをバージョンアップするための数の本番サーバを個別にバージョンアップした後。
- また、"アップグレードのベストプラクティス" on page 1659も確認してください。

Deep Security Virtual Applianceのバージョンアップ

トレンドマイクロでは、最新のセキュリティパッチ、アップデート、および継続的なサポートを利用できるように、Deep Security Virtual Applianceを最新バージョンにアップグレードすることを推奨しています。

Applianceを構成する次の2つの要素は、個別にアップグレードできます。

- AppliancのService Virtual Machine (SVM)
- Appliance SVMに組み込まれたDeep Security Agent

注意:「Appliance SVM」という用語は、VMwareインフラストラクチャにインストールされているDeep Security Virtual Appliance仮想マシンを指します。

トピック:

- "新しいアプライアンスソフトウェアが使用可能かどうかを確認する" below
- "アプライアンスをバージョンアップする前に" on the next page
- "Applianceをアップグレードする" on page 1688

新しいアプライアンスソフトウェアが使用可能かどうかを確認する

現在実行しているAppliance SVMと組み込みのAgentのバージョンが不明な場合、または新しいバージョンがあるかどうかがわからない場合は、このセクションを参照してください。それ以外の場合は、このセクションをスキップして、直接"Applianceをアップグレードする" on page 1688してください。

アップグレードが必要かどうかを判断するには、以下のセクションを参照してください。

- "現在使用しているAppliance SVMと組み込みのAgentのバージョンを確認する" below
- "新しいAppliance SVMがあるかどうかを確認する" below
- "新しいAgentがあるかどうかを確認する" on the next page

現在使用しているAppliance SVMと組み込みのAgentのバージョンを確認する

1. Deep Security Managerで、[コンピュータ] をクリックします。
2. 画面の右上部にある検索ボックスに、Deep Security Virtual Applianceと入力してAppliance仮想マシンを検索します。
3. Appliance仮想マシンを右クリックして、次の順にメニュー項目をクリックします: [詳細]→[一般]。
   - [Virtual Applianceのバージョン] プロパティに、組み込みのDeep Security Agentのバージョンが表示されます。このAgentはAppliance SVM上にインストールされています。この値を書き留めます。
   - [Appliance (SVM) のバージョン] プロパティ: この仮想マシンをインストールするために使用されるDeep Security Virtual Applianceパッケージのバージョンを示します。この値を書き留めます。

新しいAppliance SVMがあるかどうかを確認する

1. Deep Security Managerで、[管理] をクリックします。
2. 左側で、[アップデート]→[ソフトウェア]→[ダウンロードセンター] の順に展開します。
3. メイン画面で、上部右の検索バーにAppliance-ESXと入力し、<Enter>キーを押します。すべてのAppliance SVMソフトウェアが表示されます。
4. メイン画面で、現在使用しているDeep Security Managerのリリースと一致するLTSリリースを展開します。
5. [バージョン] フィールドに表示されているバージョンが現在インストールされているバージョンよりも

新しいかどうかを確認します。
6. アップグレードが必要な場合は、"Applianceをアップグレードする" on page 1688してください。

新しいAgentがあるかどうかを確認する

1. Deep Security Managerで、[管理] をクリックします。
2. 左側で、[アップデート]→[ソフトウェア]→[ダウンロードセンター] の順に展開します。
3. メイン画面で、上部右の検索バーに、現在インストールされているAppliance SVMと互換性のあるAgentの名前を入力します。詳細については、互換性の表を参照してください。たとえば、検索ボックスにAgent-RedHat_EL7と入力します。互換性のあるAgentのリストが表示されます。
4. メイン画面で最新のリリースを展開し、最新のAgentを表示します。
5. [バージョン] フィールドに表示されているバージョンが現在インストールされているバージョンよりも新しいかどうかを確認します。
6. アップグレードが必要な場合は、"Applianceをアップグレードする" on page 1688してください。

アプライアンスをバージョンアップする前に

Deep Security Virtual Applianceをアップグレードする前に、次のタスクを完了してください。

システム要件とサポートされているNSXのバージョンを確認する

- この表で、サポートされているNSXのライセンスとバージョンを確認します。
- システム要件を確認します。NSX、Deep Security Manager、およびその他の必要なソフトウェアとハードウェアを必要に応じてアップグレードします。

vCenterおよびNSXアカウントのアクセス許可を確認する

以前のアプライアンスの配信時にDeep Security Managerで指定した既存のvCenterアカウントとNSXアカウントに、適切な権限があることを確認してください。必要な権限のリストについては、"VMware vCenterの追加" on page 704を参照してください。

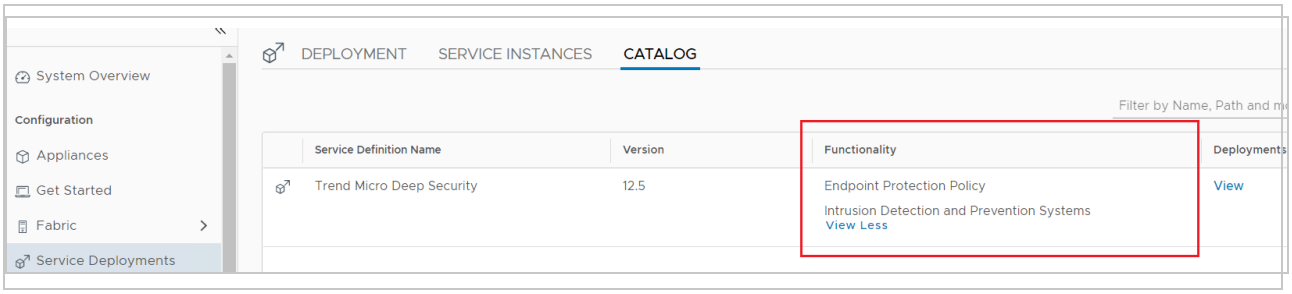
NSX-Tの再登録

NSX-Tを再登録する必要がある場合があります。

NSX-Tを再登録する必要があるかどうかを確認するには

1. NSX-T Managerに移動し、システム>サービス配信>CATALOGをクリックします。
2. エンドポイント保護ポリシーと侵入検知および予防システムの両方が存在することを確認してく

ださい(下の図を参照) 。そうでない場合、再登録が必要であることを意味します。



NSX-Tを再登録するには

1. Deep SecurityをNSX環境からアンインストールします。詳細については、"NSX環境からのDeep Securityのアンインストール" on page 1731を参照してください。
2. マネージャーにNSXを再登録してください。"VMware vCenterの追加" on page 704を参照してください。

新しいアプライアンスZIPをマネージャにインポートします。

新しいアプライアンスZIPをマネージャにインポートする必要があります。

ヒント: アプライアンスのZIPをインポートする代わりに、OVFファイルをURL の場所に配置して、NSXがより高速にダウンロードできるようにすることもできます。詳細については、"アプライアンスのOVFの場所を設定する" on page 650を参照してください。

1. 移動先:

   https://help.deepsecurity.trendmicro.com/ja-jp/software.html

2. Deep Security Virtual Applianceパッケージをダウンロードします。システム要件のバージョン要件を確認してください。

   複数バージョンのアプライアンスをインポートできます。マネージャは、最新のパッケージを選択します。

3. Deep Security Managerで、[管理]→[アップデート]→[ソフトウェア]→[ローカル] に進みます。

4. [インポート] をクリックして、パッケージをDeep Security Managerにアップロードします。

   インポート時、Deep Security Manager は も仮想アプライアンスVMのOSと互換性のあるエージェントを自動的にダウンロードおよびインポートします。このエージェントには、Deep Security Agent for 64ビットRed Hat Enterprise Linuxと同じ保護モジュールがあります。

5. 別の組み込みエージェントを指定する場合は、管理> システム設定> アップデートにアクセスし、仮想アプライアンスの配信。初期設定では、仮想アプライアンスの配信オプションは最新のバージョン(推奨) に設定されています。これは、マネージャに、インポートされた最新の組み込みエージェントを使用するように仮想アプライアンスをアップグレードすることを示します。必要に応じて、この設定を変更します。

次の手順

アップグレード前の手順が完了し、アップグレードを続行する必要があります。シナリオに応じて、次のいずれかのセクションに移動する必要があります。

- NSX-Tを再登録した場合、アプライアンスは削除されました。つまり、新しいアプライアンスを展開する必要があります( ).をバージョンアップしないでください) 。次の手順については、"アプライアンスを配信する(NSX-T 3.x) " on page 576に進んでください。
- NSX-Tを再登録しなかった場合は、アプライアンスをアップグレードする準備が整いました。"Applianceをアップグレードする" belowします。

Applianceをアップグレードする

アップグレード前のタスクが完了したら、アプライアンスをアップグレードする準備が整いました。いくつかのアップグレードオプションがあります:

- 方法1: "既存のAppliance SVMを自動的にアップグレードする" below。
- 方法2: "既存のAppliance SVMを手動でアップグレードする" on page 1692。アップグレード中にゲストVMの保護喪失が*un*のままである場合は、このオプションを使用します。
- オプション3: "アプライアンスSVMに組み込まれているエージェントをアップグレードします" on page 1699。このオプションは、最新のエージェントソフトウェアで提供される最新の保護機能をアプライアンスのSVMバージョンアップを実行せずに実行する場合に使用します。

NSX-Tを使用している場合は、オプション2または3を選択できます。

NSX-Vを使用している場合は、任意のオプションを使用できます。

"NSXライセンスをアップグレードして、利用できるDeep Securityの機能を増やす" on page 1702も参照してください。

既存のAppliance SVMを自動的にアップグレードする

このアップグレード方法では、アップグレードプロセス中にゲスト仮想マシンの保護が失われます。アップグレードプロセスには、VMwareコンポーネントのリソースとネットワークの安定性に応じて5 ~ 15分かか

ります。ゲスト仮想マシンの保護を維持する場合は、代わりに"既存のAppliance SVMを手動でアップグレードする" on page 1692を参照してください。

注意: CPUまたはメモリの拡張、パスワードの変更など、現在のAppliance SVMに対して行ったリソース調整やカスタム設定は、アップグレード後の新しいAppliance SVMに引き継がれません。これらの設定は、アップグレードの完了時に手動で再度適用する必要があります。

アプライアンスSVMを自動的にアップグレードするには、次の手順を実行します。

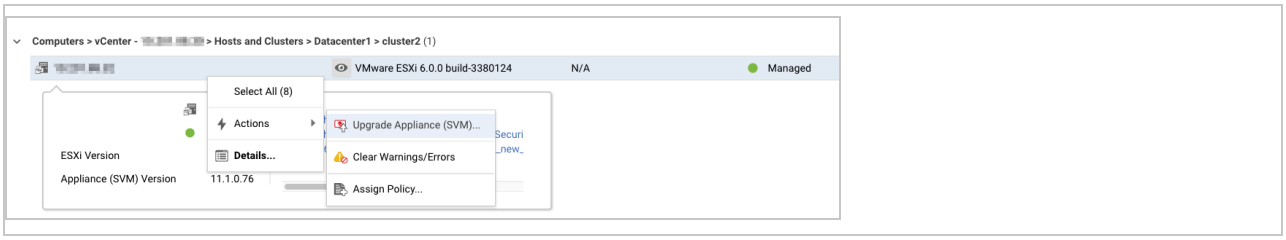
- "手順1: ManagerでAppliance SVMをアップグレードする" below
- "手順2: アップグレードが成功したことを確認します。" on page 1692

手順1: ManagerでAppliance SVMをアップグレードする

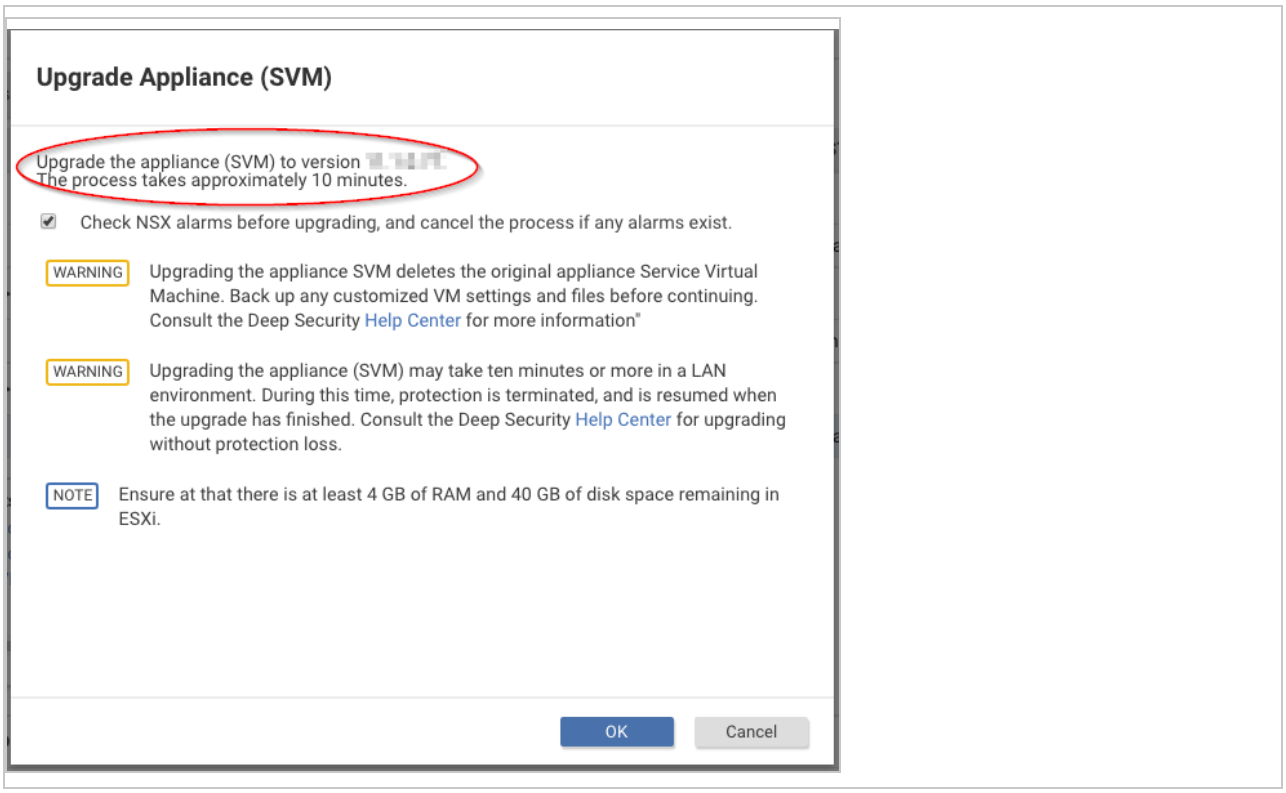
1. Deep Security Managerで、上部の [コンピュータ] をクリックします。
2. 既存のAppliance SVMがインストールされているESXiホストを探します。このESXiホストの [プラットフォーム] 列は VMware ESXi <version_build> に設定されています (下図を参照)(このホストは、[プラットフォーム] にDeep Security Virtual Applianceと表示されているコンピュータでは *ありません*)。
3. ESXiホストを右クリックして、[処理]→[Appliance (SVM) のアップグレード] を選択します。

   ヒント: 一度に複数のESXiホストをアップグレードする場合は、<Shift> キーを押しながら複数のESXiホストをクリックして選択できます。

   注意: [Appliance (SVM) のアップグレード] オプションは、ローカルソフトウェアの最新のVirtual Applianceパッケージが現在使用中のものよりも新しい場合にのみ使用できます。このオプションを使用するには、最新のApplianceパッケージをインポートしてください。この操作を行ってもうまくいかない場合は、すでに最新バージョンのAppliance SVMを使用している可能性があります。これを確認するには、Applianceの仮想マシンのコンピュータの詳細ページで [Appliance (SVM) のバージョン] プロパティを調べます。



チェックボックス、警告、およびメモを含む [Appliance (SVM) のアップグレード] ページが表示されます。



注意: 使用しているvCenterおよびESXのリソースによっては、アップグレード中にAppliance (SVM) が3 ~ 10分間シャットダウンされます。

4. (オプション)アップグレードを開始する前にManagerがNSX Managerからのサービスステータスを確認するよう設定するには、[アップグレードの開始前にNSXアラームを確認し、アラームがある場合は処理をキャンセルしてください] を選択します。この確認をスキップして、アラームが発生した場合もアップグレードを続行するには、チェックボックスをオフにします。
5. ページ上の警告と注意をよく読みます。
6. [OK] をクリックします。

   アップグレード前のサービスステータスの確認 (有効にした場合) を含め、アップグレードプロセスが開始されます。

7. (オプション)引き続きManager内で、[コンピュータ] ページに戻ってESXiホストを見つけ、その [タスク] 列でアップグレードのステータスを確認します。

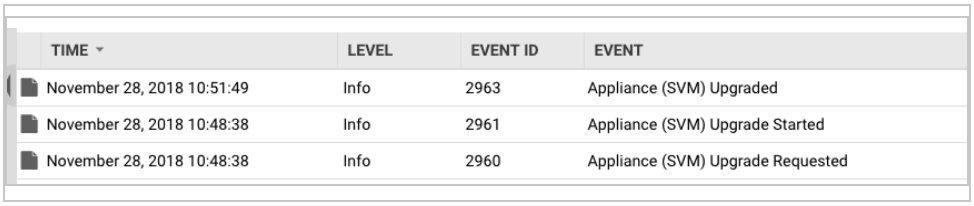
注意: 前の手順で <Shift> キーを押しながら複数のESXiホストをクリックして選択した場合、ESXiホストは1つずつ順番に処理されます。[タスク] 列を見ると、どのサーバが現在処理されているかを確認できます。

[タスク] 列には次のいずれかが表示されます。

- Appliance (SVM) のアップグレード中 (保留中): アップグレード要求がManagerによって受け取られましたが、まだキューに登録されていません。
- Appliance (SVM) のアップグレード中 (処理待ち): プロセスがManagerによってキューに登録され、まもなくアップグレードが開始されます。
- Appliance (SVM) のアップグレード中 (実行中): Managerによってアップグレード処理が実行されています。

8. (オプション)引き続きManager内で、いずれかのESXiホストの [コンピュータの詳細] ページに移動し、[システムイベント] タブをクリックして、アップグレードが正常に実行されていることを確認します。

   アップグレードが成功したときに表示されるシステムイベントの例を次に示します。その他のイベントについては、このAppliance SVMのアップグレードイベントの完全なリストを参照してください。



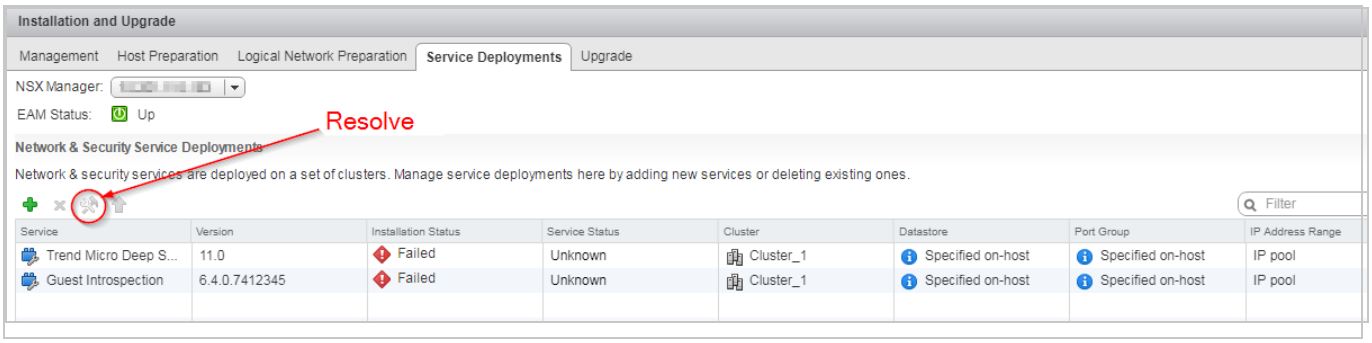
TIME	LEVEL	EVENT ID	EVENT
November 28, 2018 10:51:49	Info	2963	Appliance (SVM) Upgraded
November 28, 2018 10:48:38	Info	2961	Appliance (SVM) Upgrade Started
November 28, 2018 10:48:38	Info	2960	Appliance (SVM) Upgrade Requested

注意: 「Appliance (SVM) のアップグレード失敗」システムイベントが表示された場合は、"「Appliance (SVM) のアップグレード失敗」システムイベントのトラブルシューティング" belowを参照してください。

「Appliance (SVM) のアップグレード失敗」システムイベントのトラブルシューティング

「Appliance (SVM) のアップグレード失敗」システムイベントが表示された場合は、その詳細な説明を読んで、理由と考えられる修正方法を確認します。ワーストケースのシナリオでは、NSX Managerコンソールに移動し、[Resolve] アイコンをクリックします (下の図を参照)。このボタンをクリックすると、手動でアラームを解決し、Applianceを再インストールできます。ゲストVMは、古いDeep Security Virtual Applianceを配置したときにアクティベーションを設定する方法に従ってアクティベートされます。有効化

の設定の詳細については、"Applianceのインストール (NSX-V)" on page 611の有効化に関するセクションを参照してください。



手順2: アップグレードが成功したことを確認します。

Appliance SVMが正常にアップグレードされます。Managerの [コンピュータ] ページに移動し、Appliance SVMとすべてのゲスト仮想マシンが保護ステータス (緑色のドット) に戻っていることを再確認します。

既存のAppliance SVMを手動でアップグレードする

手動アップグレードの場合は、vMotionメカニズムを使用してアップグレード中のゲスト仮想マシンの保護を維持します。

Appliance SVMをアップグレードするには、次の手順に従います。

- "手順1: 検出ファイルを確認または復元する" below
- "手順2: ゲスト仮想マシンを別のESXiホストに移行する" below
- "手順3: 古いAppliance SVMをアップグレードする" on the next page
- "手順4: メンテナンスモードがオフになっていることを確認する" on page 1698
- "手順5: 新しいAppliance SVMが有効化されていることを確認する" on page 1698
- "手順6: 最後の手順" on page 1699

手順1: 検出ファイルを確認または復元する

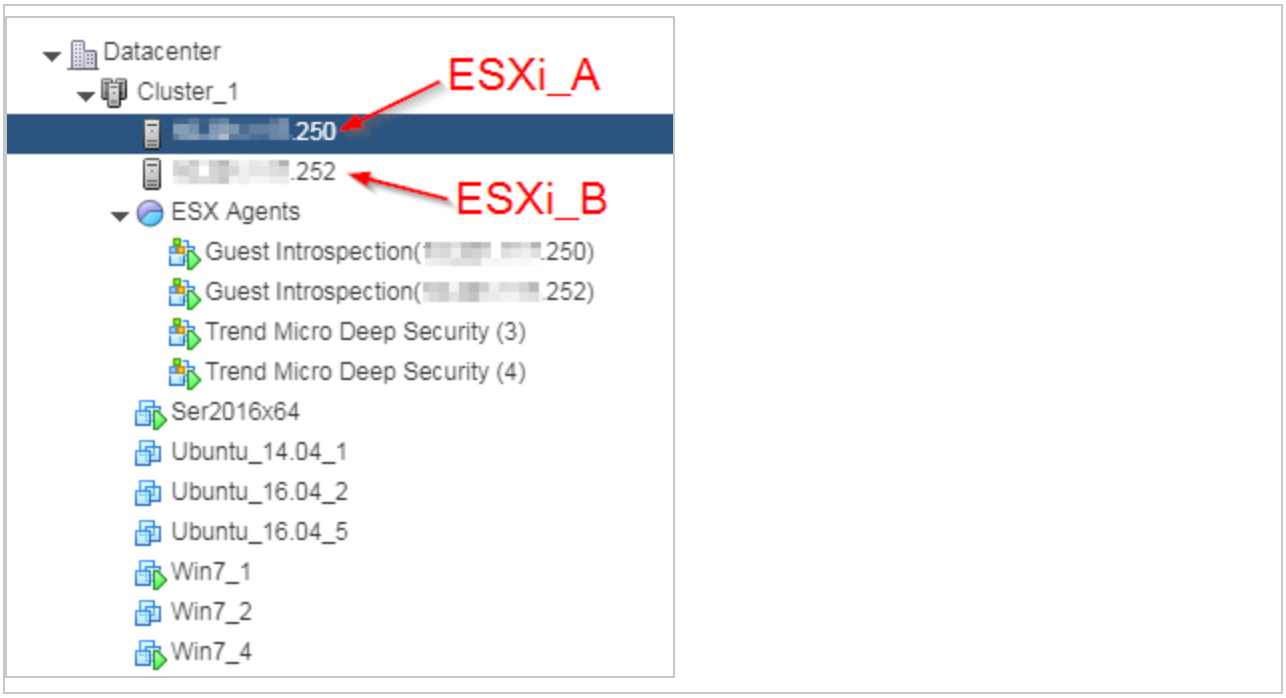
1. VMを移動したりDeep Security Virtual Applianceを削除すると、特定されたファイルが失われるため、必要に応じてファイルを確認または復元してください。

手順2: ゲスト仮想マシンを別のESXiホストに移行する

注意: NSX-T 3.xを使用している場合は、このセクションをスキップしてください。

説明を簡潔にするために、この手順では次の用語を使用します。

- ESXi_Aは、アップグレードするVirtual Applianceを含むESXiサーバです。
- ESXi_Bは、Appliance SVMのアップグレードの実行中にゲスト仮想マシンの移行先となるESXiサーバです。このサーバは、ESXi_Aと同じクラスタにあるものとします。



1. クラスタのDRSを有効にして、DRSの自動化レベルが [Fully Automated] であることを確認します。詳細については、こちらのVMwareの記事を参照してください。
2. ESXi_Aを探して、このESXiサーバをメンテナンスモードに切り替えます。

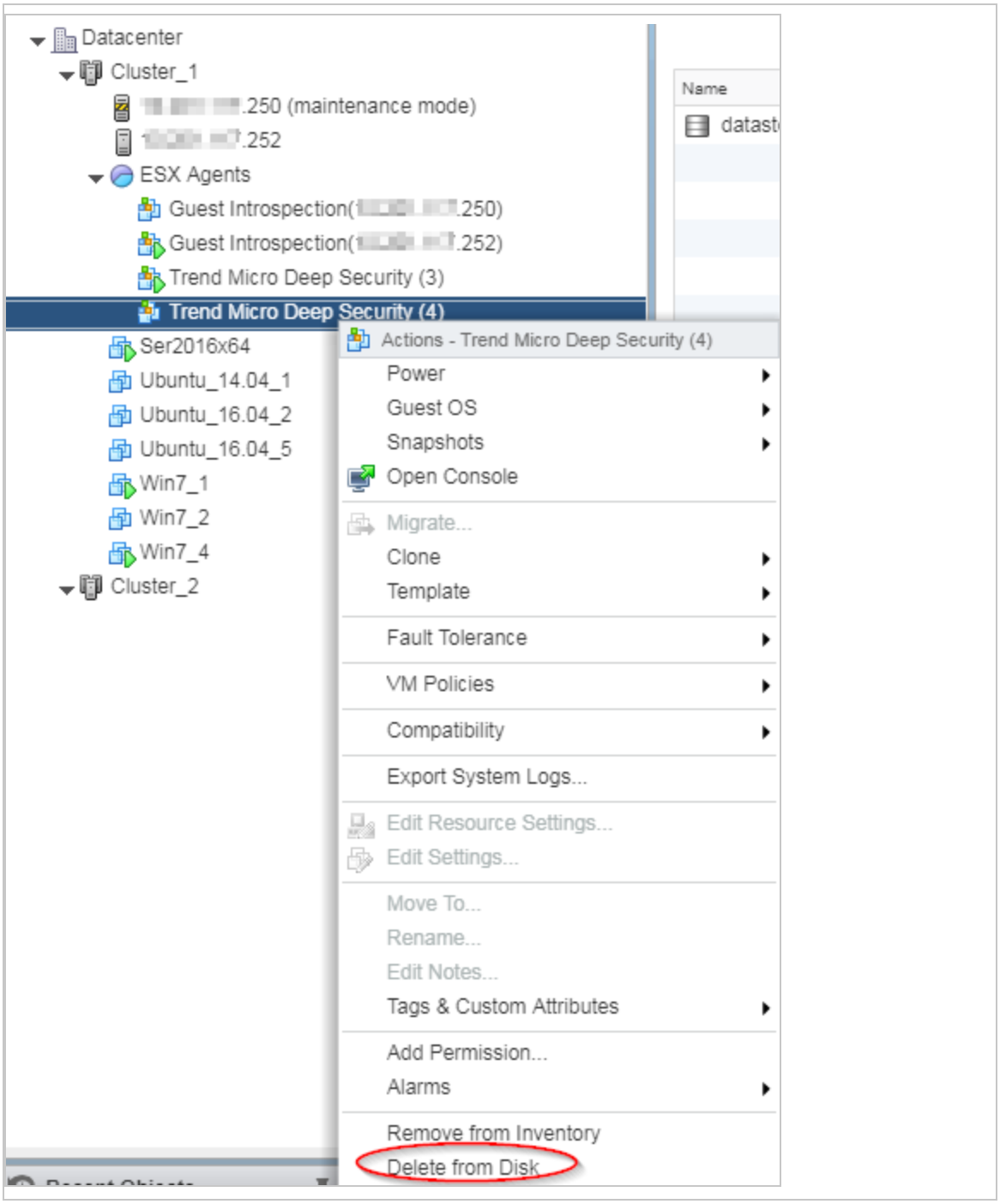
   メンテナンスモードに移行すると、次のようになります。

   - ESXi_Aのゲスト仮想マシンが自動的に (vMotionを使用して) クラスタ内のESXi_Bに移行されます。
   - ESXi_A を保護しているDeep Security Virtual Applianceは自動的にシャットダウンされます。
   - ESXi_Aのメンテナンスモードが終了するまで、ゲスト仮想マシンの電源をオンにできなくなります。

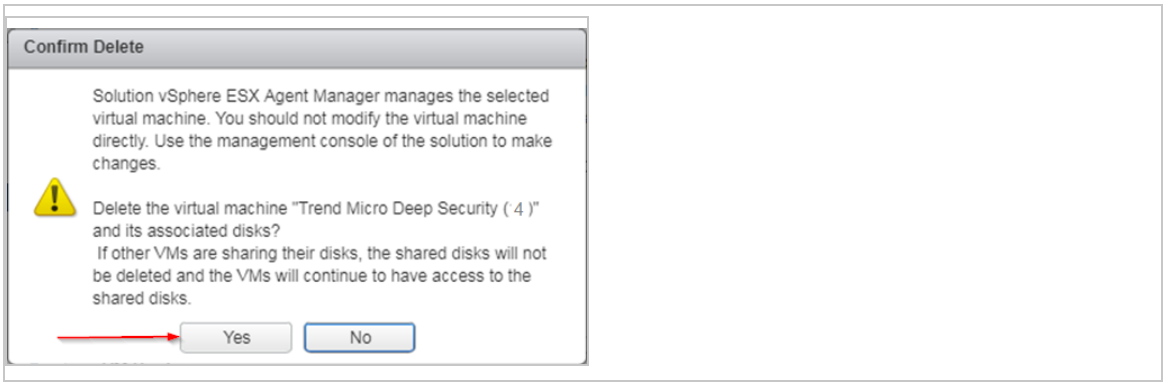
手順3: 古いAppliance SVMをアップグレードする

NSX-V命令

1. VMware vSphere Web Clientの [Hosts and Clusters] に移動します。
2. 電源がオフになっているTrend Micro Deep Security Appliance SVMを見つけます。緑色の矢印が付いていないものです (次の画像を参照)。Appliance SVMは、対応するESXiサーバをメンテナンスモードにしたときに自動的にオフにされています。
3. オフになっている状態のTrend Micro Deep Security Appliance SVMを右クリックし、[Delete from Disk] を選択します。


Datacenter
Cluster_1
.250 (maintenance mode)
.252
ESX Agents
Guest Introspection(.250)
Guest Introspection(.252)
Trend Micro Deep Security (3)
Trend Micro Deep Security (4)
Ser2016x64
Ubuntu_14.04_1
Ubuntu_16.04_2
Ubuntu_16.04_5
Win7_1
Win7_2
Win7_4
Cluster_2
Name
Actions - Trend Micro Deep Security (4)
Power
Guest OS
Snapshots
Open Console
Migrate...
Clone
Template
Fault Tolerance
VM Policies
Compatibility
Export System Logs...
Edit Resource Settings...
Edit Settings...
Move To...
Rename...
Edit Notes...
Tags & Custom Attributes
Add Permission...
Alarms
Remove from Inventory
Delete from Disk

4. [Confirm Delete] メッセージが表示されたら、[Yes] をクリックします。

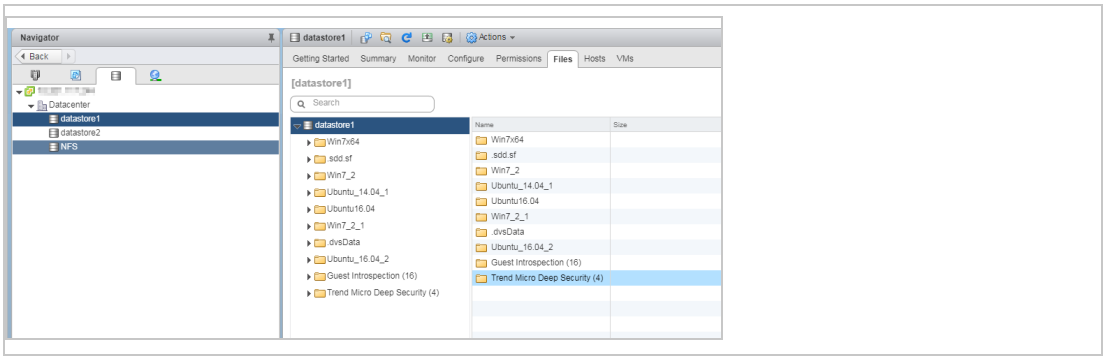


5. 削除に失敗すると、次のメッセージが表示されます。

   This operation not allowed in the current state

   この場合は、次の手順を実行してください。

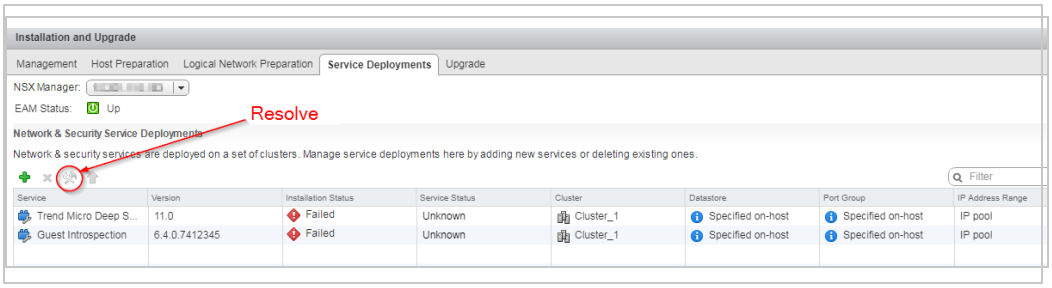
   a. もう一度Trend Micro Deep Security Appliance SVMを右クリックします。今回は [Remove from Inventory] を選択します。これは [Delete from Disk] のすぐ上に表示されます。Appliance SVMは、vCenterからは削除されますが、データストアでは保持されます。
   b. ナビゲーション画面でデータストアのタブを選択し、古いVirtual Applianceがあるデータストアを選択します。
   c. メイン画面で [Files] タブをクリックします。
   d. 古いAppliance SVMフォルダを右クリックし、[Delete File] を選択します。



   e. VMware vSphere Web Clientを開き、[ホーム]→[ネットワークとセキュリティ]→[インストール]→[サービス配信]に移動します。

      以下が表示されます。

- 削除したTrend Micro Deep Security Appliance SVMの [Installation Status] 列に [Failed] と表示されます。
- メンテナンスモードの場合は、Guest Introspectionサービスも [Failed] として表示されます。



f. Guest Introspectionサービスの [Installation Status] が [Failed] になっている場合、そのサービスの [Resolve] ボタンをクリックします。[Failed] ステータスが [Enabling]、[Succeeded] の順に変わります。Guest Introspectionサービスがオンになり、メンテナンスモードが終了します。

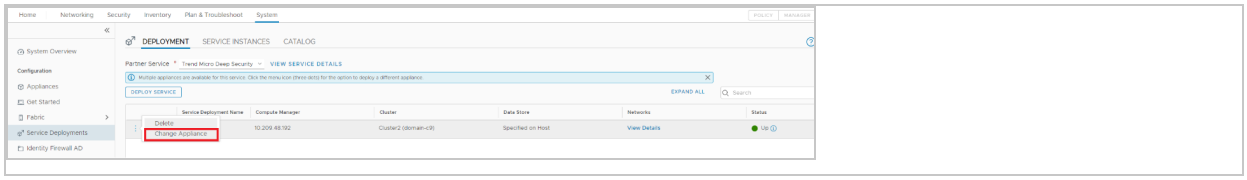
g. [Failed] ステータスのTrend Micro Deep Securityサービスの [Resolve] ボタンをクリックします。[Failed] ステータスが [Enabling]、[Succeeded] の順に変わります。この間には、次の処理が行われます。
   - Trend Micro Deep Securityアプライアンスは、Deep Security Managerにロードした最新のソフトウェアで再配信されました。
   - Appliance SVMが有効化されます。
   - Appliance SVMの組み込みのAgentが初期設定で [ローカルソフトウェア] 内の最新の互換バージョンに自動的にアップグレードされます。

NSX-Vを使用している場合の手順はこれで完了です。"手順4: メンテナンスモードがオフになっていることを確認する" on the next pageに進んでください。

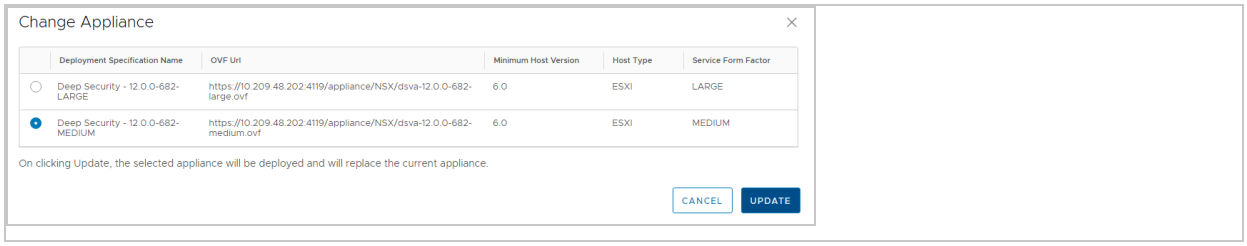
NSX-T 3.x命令

NSX-T Managerで、[System]→[Service Deployments]→[DEPLOYMENT] の順に進みます。

メニューアイコン(3つの点) をクリックします。>変更 アプライアンス。



c。更新するアプライアンスを選択し、アップデートボタンをクリックします。



アップグレードプロセスが完了するのを待ちます。

手順4: メンテナンスモードがオフになっていることを確認する

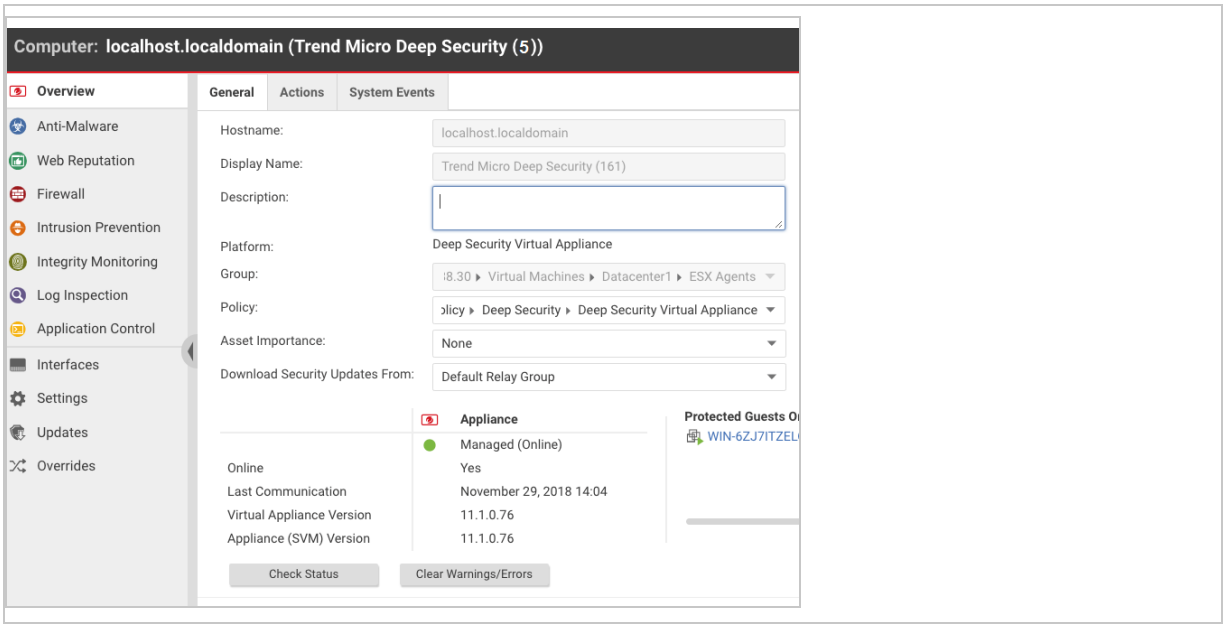
注意: NSX-T 3.xを使用している場合は、このセクションをスキップしてください。

- 以前にメンテナンスモードをオンにした場合は、オフになっていることを確認します。まだオンの場合は、すぐにオフにします。

手順5: 新しいAppliance SVMが有効化されていることを確認する

1. Deep Security Managerの上部にある[Computers]をクリックします。
2. リスト内でTrend Micro Deep Securityを見つけてダブルクリックします。これがApplianceです。
3. 以下を確認します。
   a. ステータスが[管理対象 (オンライン)] に設定されていることを確認します。これは、Agentが正常に有効化されたことを示します。
   b. Virtual Applianceのバージョンが埋め込みDeep Security Agentのバージョンに設定されていることを確認してください。このバージョンは、[管理]→[アップデート]→[ソフトウェア]→[ローカル] で確認できる最新のAgentソフトウェアのバージョン、または [管理]→[システム設定]→[アップデート]→[Virtual Applianceの配置] で設定した特定のバージョンと一致する必要があります。
   c. [Appliance (SVM) のバージョン] が [管理]→[アップデート]→[ソフトウェア]→[ローカル] で確認できる最新のDeep Security Virtual Applianceパッケージのバージョンに設定されているこ

とを確認します。



これで、Appliance SVMがアップグレードされました。

手順6: 最後の手順

1. 置き換える必要がある各Appliance SVMに対して、"手順1: 検出ファイルを確認または復元する" on page 1692から"手順5: 新しいAppliance SVMが有効化されていることを確認する" on the previous pageまで、このセクションのすべての手順を繰り返します。

ゲストVMは、古いDeep Security Virtual Applianceを配置したときにアクティベーションを設定する方法に従ってアクティベートされます。アクティベーションセットアップの詳細については、"アプライアンスを配信する(NSX-T 3.x) " on page 576または "Applianceのインストール (NSX-V)" on page 611。

アプライアンスSVMに組み込まれているエージェントをアップグレードします

アプライアンスのSVMを再デプロイせずにアプライアンスSVMに組み込まれているDeep Security Agentだけをアップグレードできます。

注意: 組み込みエージェントのみをアップグレードすると、アプライアンスのSVM'の元のサポート終了日は有効なままです。詳細については、"Deep Security LTS ライフサイクル日付" on page 121を参照してください。

Appliance SVMに組み込まれているAgentをアップグレードするには、次の手順に従います。

1. "現在使用しているAppliance SVMと組み込みのAgentのバージョンを確認する" on page 1685。この処理の残りの手順を完了するには、次の情報が必要です。
2. 互換性のあるAgentをインポートします。
   a. それでもDeep Security Managerの左側にある[Updates]→[Software]→[Download Center]の順に選択します。
   b. Appliance SVMと互換性のあるAgentソフトウェアを選択します。解説については、この後に表示される互換性の表を参照してください。
   c. エージェントをDeep Security Managerにインポートするには、[今すぐインポート]列のボタンをクリックします。
   d. 左側で、[ローカルソフトウェア] をクリックし、Agentが正しくインポートされていることを確認します。

   アプライアンスのSVMバージョンと互換性のあるDeep Security Agentがインポートされました。アプライアンスSVMでエージェントをアップグレードする準備ができました。

3. アプライアンスのエージェントをアップグレードするSVM:
   a. [コンピュータ] をクリックし、Applianceコンピュータをダブルクリックします。
   b. [処理]→[Applianceのアップグレード] の順にクリックします。
   c. Applianceにインストールするバージョンを選択します。これは先ほどインポートしたAgentです。
   d. [OK] をクリックします。
4. [イベントとレポート] をクリックして710を検索し、アップデートファイルのインストールに関するレポートを確認します。

これで、アプライアンスSVM上のエージェントがアップグレードされました。

互換性テーブル: アプライアンス、エージェント

Appliance SVMのバージョン	イメージのOS	互換性のあるAgentソフトウェア
Appliance-ESX-11.0以降	CentOS 7	Agent-RedHat_EL7-<version>.x86_64.zip <version> の部分はAgentソフトウェアのバージョンです。最新バージョンを選択します。このバージョンのAgentが組み込みのAgentとして使用されます。

データベースのアップグレード

Deep Security Managerからアップグレードする場合は、Deep Securityデータベースのアップグレードも必要になることがあります。の現在サポートされているデータベースのこのリストを確認し、必要に応じて次の手順に従って新しいデータベースに移行します。

アップグレードパス

データベースのアップグレードパスは次のとおりです。

1. データベースソフトウェアを先にアップグレードしてください。
2. Deep Security Managerからアップグレードします。

選択したデータベースは、*の新しいとの現在インストールされているバージョン*のDeep Security Manager)の両方でサポートされる必要があります。次のリストを参照してください。

- Managerの現在のリリースでサポートされているデータベース。
- 以前のバージョンのManagerでサポートされていたデータベース。(隣のリンクをクリックすると、以前のリリースのドキュメントにアクセスできるようになります。ドキュメントをドリルダウンして、データベースサポートを検索できます。.)

データベースのアップグレード

データベースをアップグレードするには、次の手順に従ってください。

警告:データの損失を防ぐには、Deep Security Managerソフトウェア)からアップグレードする前に、データベースの移行を完了してください。

1. Deep Security Managerサービスを停止します。マネージャが停止している間、Deep Security Agentは現在の保護ポリシーを継続します。
2. データベースをバックアップします。
3. データベース接続設定ファイルをバックアップします:[Deep Securityのインストールディレクトリ]/webclient/webapps/ROOT/WEB-INF/dsm.properties
4. 新しいデータベースサーバに移行します。特定の要件については、"データベースの要件" on page 452を参照してください。
5. 移行の際に既存のデータベースが保持されなかった場合は、新しいデータベースエンジンにデータベースのバックアップを読み込みます。
6. 必要に応じて、移行後のデータベースを使用するようにdsm.propertiesを編集します。
7. Deep Security Managerサービスを再起動します。

エラー: データベースサーバへの安全な接続を確立できませんでした

Deep Security Managerのインストールまたはアップグレード時に、Deep Securityデータベースとして Microsoft SQL Serverを使用している場合、次のエラーメッセージが表示されることがあります。

データベースサーバへの安全な接続を確立できませんでした。データベースサーバをアップグレードするか設定して、TLS 1.2の暗号化がサポートされるようにしてください。

Deep Security Managerの java.security ファイルに jdk.tls.disabledAlgorithms= 設定の TLSv1 および TLSv1.1 が含まれていると、初期設定のTLSが無効になり、TLS 1.2のみが許可されます。(java.securityファイルは、TLS 1.2のみが許可されるDeep Security Manager 11.1以降の新規インストールを実行する場合、またはTLS 1.2を強制した後でアップグレードを実行する場合にこのように設定されます)。アップグレード中またはインストール中に、Managerのデータベースドライバは、TLS 1.2を使用してSQL Serverとの通信を試みますが、SQL Serverのバージョンが TLS 1.2をサポートしていない場合は、このエラーが表示されます。

この問題を解決するには、SQL ServerデータベースをTLS 1.2をサポートするバージョンにアップグレードしてから、Deep Security Managerのインストールまたはアップグレードを再度実行する必要があります。TLS 1.2をサポートするSQL Serverバージョンのリストについては、こちらのMicrosoftの記事を参照してください。

NSXライセンスをアップグレードして、利用できるDeep Securityの機能を増やす

Deep Securityの ファイアウォール、侵入防御、またはWebレピュテーションを使用する場合は、a> Deep Security Virtual Applianceの機能を使用するには、VMwareのネットワーク機能をサポートするライセンスを使用する必要があります。ネットワーク機能は、次の種類のライセンスでサポートされます。

- NSX Advanced
- NSX エンタープライズ
- NSX データセンターアドバンス
- NSX Data Center Enterprise Plus
- NSX リモートオフィス支社のデータセンター

別のライセンスタイプを使用している場合は、ライセンスタイプをアップグレードする必要があります。以下を参照してください。

- "NSX-T 3.xライセンスのアップグレード" below
- "NSX-Vライセンスをアップグレードします" belowする

ヒント: NSXライセンスをアップグレードする代わりに、Deep Security AgentをゲストVMに配置して上記の機能を利用することもできます。詳細については、こちらの表のほか、"Agentレスによる保護またはコンバインモードの保護の選択" on page 569を参照してください。

NSX-T 3.xライセンスのアップグレード

1. NSX-T Managerにログインします。
2. システム>ライセンスをクリックします。
3. 追加をクリックし、ライセンスキーを入力して、[追加]をクリックします。
4. NSX-T Managerからログアウトし、再度ログオンしてください。新しいライセンスが適用されます。

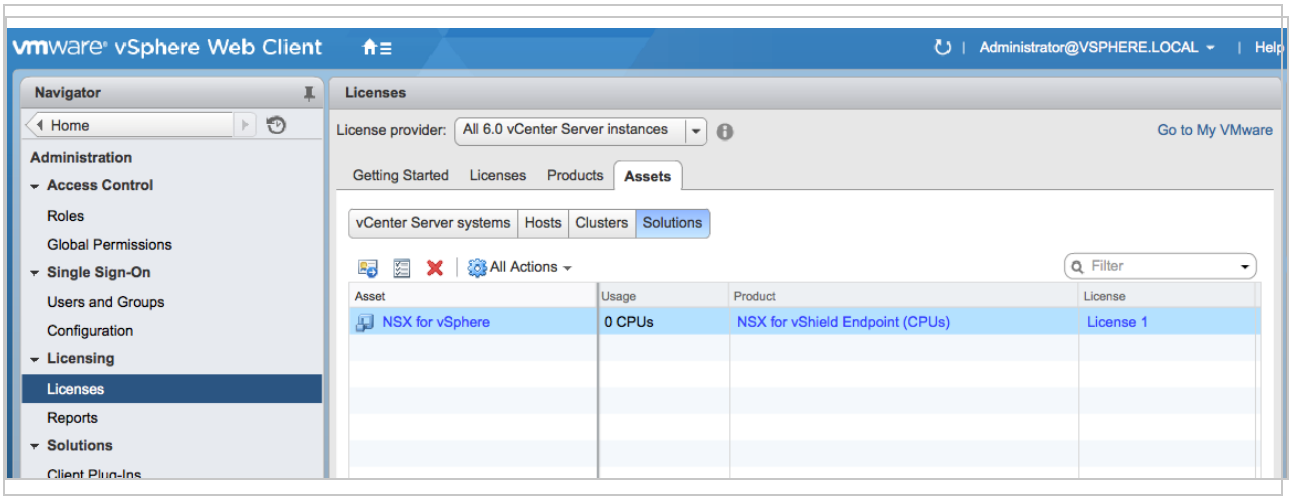
VMwareのネットワーク機能に依存するDeep Securityの機能、つまりファイアウォール、侵入防御、およびWebレピュテーション機能を使用します。今後も引き続き不正プログラム対策および変更監視機能を使用できます。

NSX-Vライセンスをアップグレードします

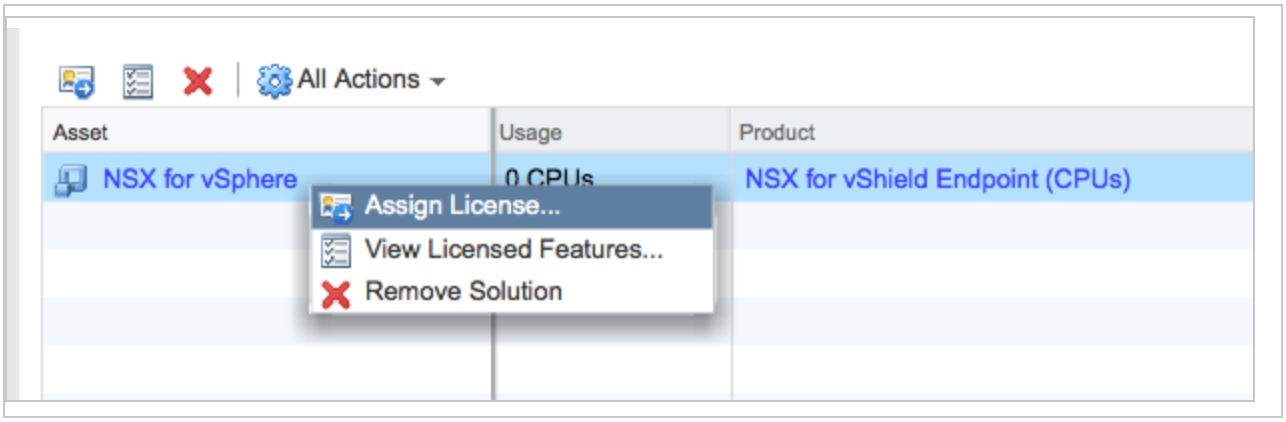
- "手順1: NSXライセンスをアップグレードする" on the next page
- "手順2: Deep SecurityをNSXからすべて削除する" on page 1707
- "手順3: Deep Security Virtual Applianceを再インストールする" on page 1707

手順1: NSXライセンスをアップグレードする

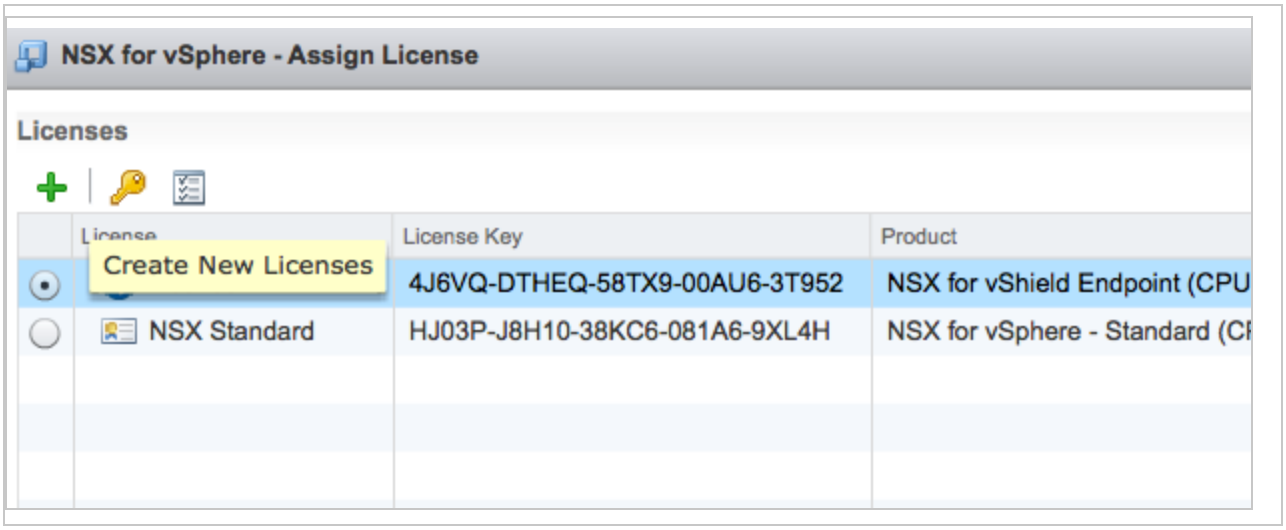
1. vSphere Web Clientで、[Home]→[Administration]→[Licenses] の順に選択します。
2. メイン画面で、[Assets] をクリックして [Solutions]ボタンをクリックします。



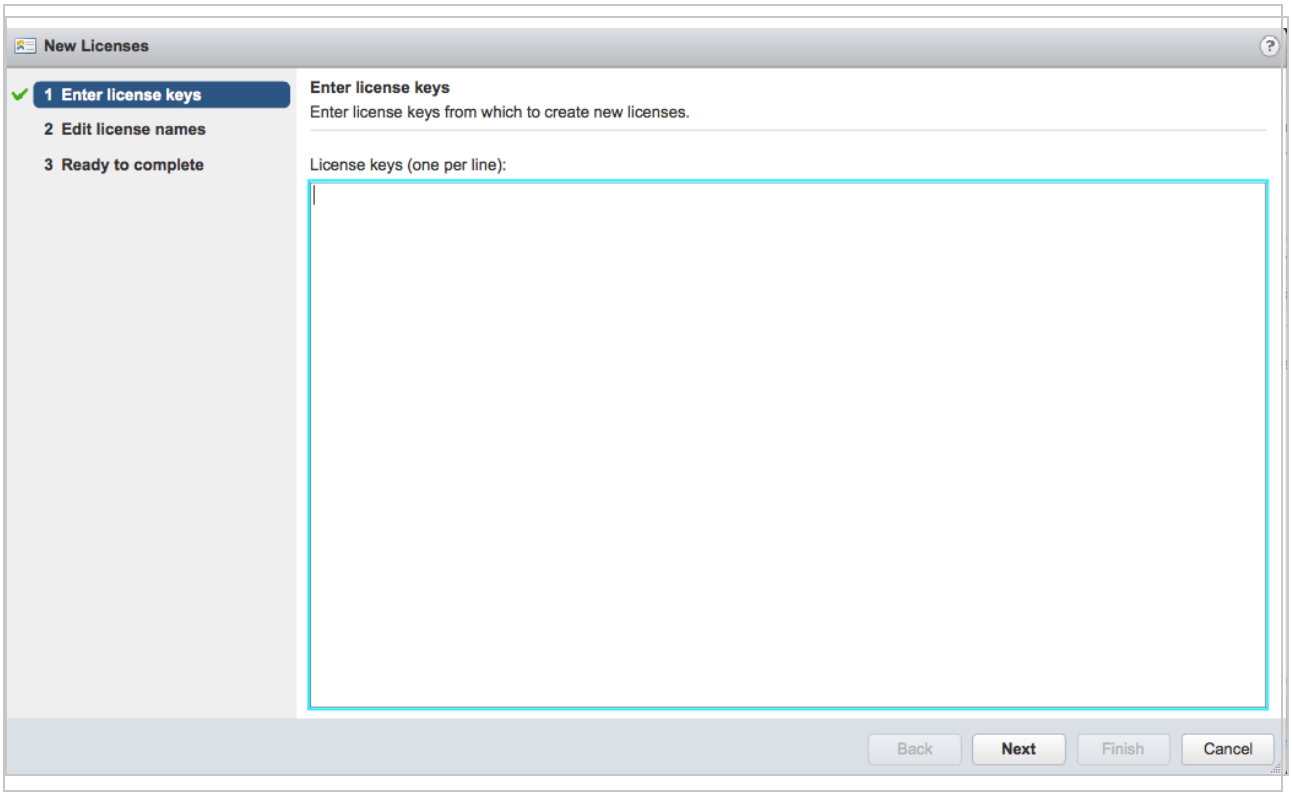
3. [NSX for vSphere] を右クリックし、[Assign License] を選択します。



4. 左側の緑の「+」をクリックし、新しいライセンスを作成します。



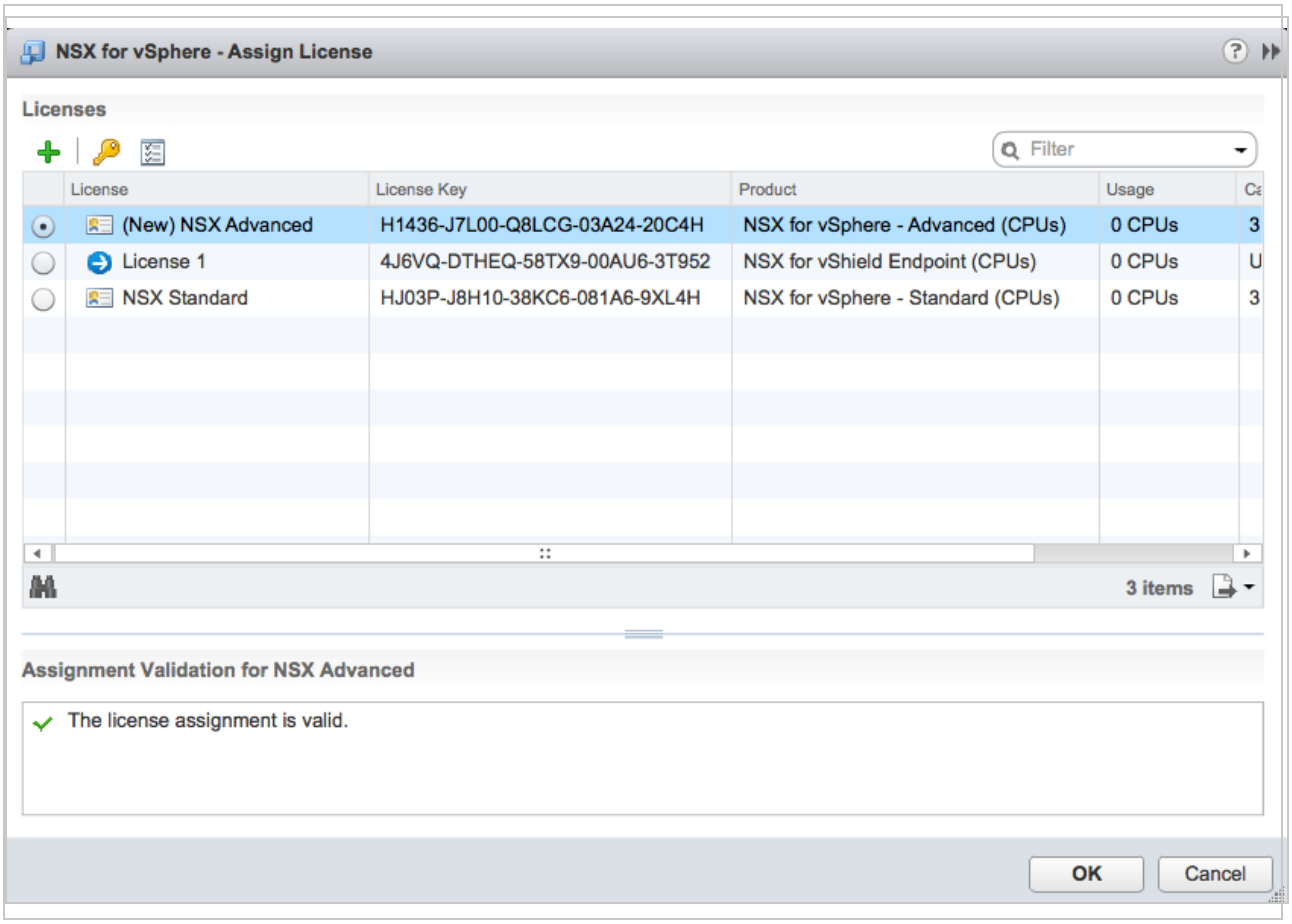
ウィザードが表示され、ライセンスキー追加の手順が示されます。



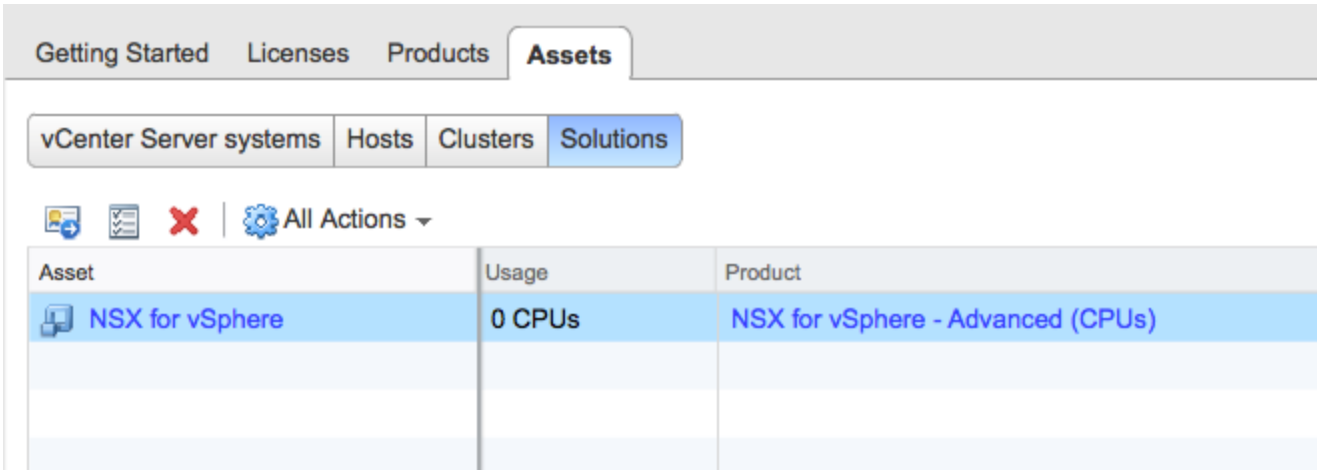
5. ウィザードで、NSX Advanced、NSX Enterprise、NSX Data Center Professional、NSX Data Center Advanced、NSX Data Center Enterprise Plus、またはNSX Data Center for Remote Branch Officeのライセンスキーとライセンス名を入力します。ウィザードの最後で [Finished] をクリックします。

新しいライセンスが [Assign License] 画面のリストに表示されます。

6. 新しいライセンスを選択し、[OK] をクリックします。



新しいNSXライセンスが使用中の状態になります。



手順2: Deep SecurityをNSXからすべて削除する

新しいライセンスを有効にするには、NSXからDeep Securityを完全に削除する必要があります。NSXからDeep Securityを削除するには、"NSX環境からのDeep Securityのアンインストール" on page 1731を参照してください。

手順3: Deep Security Virtual Applianceを再インストールする

NSXからDeep Securityを完全に削除したら、Deep Security Virtual Applianceを再配信する必要があります。再配信するには、"Applianceのインストール (NSX-V)" on page 611に配信します。

これで、ファイアウォール、侵入防御、およびWebレピュテーション機能を使用できるようになります。以前に利用可能だった不正プログラム対策および変更監視機能を引き続き使用できます。

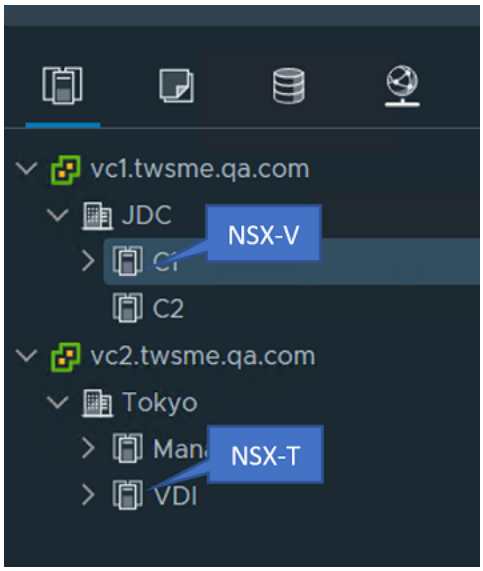
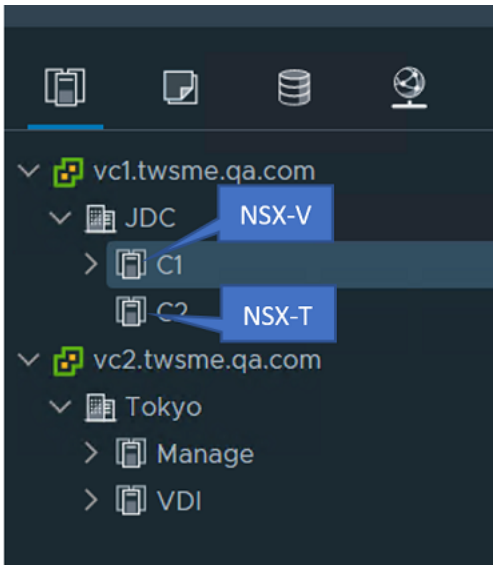
エージェントレスソリューションをNSX-VからNSX-Tに移行する

日本地域向けの製品は、地域固有のポリシーに基づいて取り扱われます。詳細については、Trend Micro Deep Security Virtual Appliance の製品サポート終了に関するご案内をご覧ください。

ここでは、NSX-V環境で既存のエージェントレスソリューションをNSX-T 3.0以上に移行する方法について説明します。

移行手順は、環境の設定方法によって異なります。さまざまな設定の説明については、VMwareドキュメントの NSX for vSphere とNSX-T の共存を参照してください。以下のセクションでは、VMWareドキュメントの[ユースケース1]または[ユースケース2]のいずれかの移行方法について説明します。

	ユースケース1	ユースケース2
地域	VMware NSX-VおよびNSX-Tは、別々のvCenter Serverに登録されています。	VMware NSX-VおよびNSX-Tは、異なるクラスタを保護するため、同じvCenter Serverに登録されています。

	ユースケース1	ユースケース2
例		
移行手順	"移行シナリオ1" below を参照してください。	"移行シナリオ2" on page 1711 を参照してください。

移行シナリオ1

次の手順に従ってください。

- "移行前" below
- "ステップ1: 移行のためのNSX-Tインフラストラクチャの準備" on the next page
- "ステップ2: 新しいアプライアンスをインポートする" on the next page
- "ステップ3: 移行する" on the next page
- "ステップ4: 新しい配信とそのセキュリティ機能を確認する" on page 1710
- "ステップ5: Deep Security ManagerからのNSX-Vのアンインストール" on page 1710からDeep Securityサービスをアンインストールします。

移行前

1. のシステム要件を確認してください。特に:
   - Deep Security Managerは、バージョン20のLTS Update 2020-11-26以上である必要があります。
   - NSX-Tはバージョン3.0以上である必要があります。

- 既存のvCenterコネクタがNSX-V 6.4.xにバインドされたDeep Security Managerがすでにインストールされている必要があります。

2. 別のvCenter Server(VC-2など) を設定してNSX-T Managerに登録するには、VMwareドキュメントのNSX for vSphereとNSX-Tの共存に関するユースケース1を参照してください。
3. VMwareのドキュメントを参照して、NSX-T管理用のESXiホストおよびクラスタを調整してください。
4. NSX-VにEdgeクラスタが含まれている場合は、VMwareドキュメントの NSX Edge Networking Setup を参照して、NSX-Tのエッジクラスタでルーティングまたはブリッジモードを設定してください。
5. 移行プロセスを続行する前に、ネットワーク接続を確認してください。

ステップ1:移行のためのNSX-Tインフラストラクチャの準備

Fabric settings の準備の手順に従って、NSX-Tを設定します。新しいvCenterをNSX-Tにすでに追加している場合(たとえば、前述のセクション), で説明したVC-2の場合は、[Compute Managerの設定] の手順を省略できます。

ステップ2:新しいアプライアンスをインポートする

次に、Deep Security Managerで、が新しいDeep Security Virtual Applianceをインポートします。

ステップ3:移行する

1. Deep Security Managerで、新しいvCenter(上記の例ではVC-2) とNSX-Tを追加します。手順については、新しいvCenterコネクタの追加を参照してください。
2. Deep Security Virtual ApplianceをNSX-Tに配置します。
3. ゲストVMのアクティベーションとセキュリティポリシーの割り当てには、NSX-Vに比べてNSX-Tに追加の要件があります。次のタスクを実行します。
   a. "NSX-Tのセキュリティグループをアップデートする" on page 1715のセキュリティグループを更新します。
   b. "セキュリティポリシーをNSX-VからNSX-Tに移行する" on page 1722に移行する
   c. アクティベーションの準備。

      NSX-V環境を準備する際に方法1または方法2を使用した場合、ゲストVMを自動的にアクティベートするには、既存のイベントベースのタスクの[ポリシーの割り当て]または[条件]を変更する必要があります。

> 注意:NSX-Tでのセキュリティポリシーの移行およびサービスプロファイルの作成を開始すると、NSX-Vクラスタの下のゲストVMが保護機能を失う可能性があります。これは、NSXセキュリ

ティグループのバインドが移行の一部であるためです。NSX-Tの設定が完了したゲストVMがNSX-Tクラスタに移行されると、保護が再開されます。

4. ゲストVMの移行:
   a. 両方のvCenter Serverを同じSSOドメインにリンクして、クロスvCenterの移行をサポートします。Vmwareドキュメントの「vCenter Serverインスタンス間の移行の要件」を参照してください。
   b. vMotionを使用して、ゲストVMを元のvCenterから新しいvCenterに移動します。詳細については、VDS/VSS とNSX-Tスイッチ間のvMotionを参照してください。
   c. NSX-Vでネットワークイントロスペクションを使用していた場合、vMotionの完了後、新しいvCenterがNSX-Tネットワーク上にある場合、ゲストVMは少なくとも1つのNICを論理スイッチ(オーバーレイモード)に接続してネットワークセキュリティを有効にする必要があります。NSX-Tの機能
5. Deep Security Managerで、Computers ページに移動してゲストVMを探し、Deep Security Virtual Applianceがアクティベートされており、初期設定の「Deep Security Virtual Appliance」ポリシーが適用されていることを確認します。

   ゲストVMを有効にし、セキュリティポリシーを自動的に割り当てる必要があります。ゲストVMが期待されるセキュリティポリシーでアクティベートされていない場合は、次の手順を実行してください。
   - [Computers]画面で、vCenterを右クリックして、[Synchronize Now]を選択します。
   - ゲストVMがまだアクティベートされていない場合は、アクティベーションを行い、セキュリティポリシーを手動で割り当ててみてください。

ステップ4:新しい配信とそのセキュリティ機能を確認する

1. 不正プログラム モジュールが正しく動作していることをテストし、イベントをDeep Security Managerに送信してください。"不正プログラム検索をテストする" on page 834を参照してください。
2. ネットワーク保護モジュール(Webレピュテーション, Firewall, Intrusion Prevention)が正しく動作しており、イベントをDeep Security Managerに送信していることをテストします。"Webレピュテーションをテストする" on page 903, "ファイアウォールルールを配信前にテストする" on page 955および"侵入防御のテスト侵入防御" on page 910。

ステップ5:Deep Security ManagerからのNSX-Vのアンインストール

Deep Securityモジュールが正しく機能していることを確認したら、Deep Security ManagerからNSX-Vをアンインストールします。手順については、"NSX-V環境からのDeep Securityの手動アンインストール" on page 1740のアンインストールを参照してください。これで、移行プロセスが完了しました。

移行シナリオ2

次の手順に従ってください。

- "移行前" below
- "ステップ1:NSX-TネットワークとvCenterインフラストラクチャの準備" below
- "ステップ2:新しいアプライアンスをインポートする" below
- "ステップ3:移行する" on the next page
- "ステップ4:新しい配信とそのセキュリティ機能を確認する" on page 1714
- "ステップ5:NSX-Vをクリーンナップする" on page 1715

移行前

1. のシステム要件を確認してください。特に:
   - Deep Security Managerは、バージョン20のLTS Update 2020-11-26以上である必要があります。
   - NSX-Tはバージョン3.0以上である必要があります。
   - 既存のvCenterコネクタがNSX-V 6.4.xにバインドされたDeep Security Managerがすでにインストールされている必要があります。
2. NSX-Tで管理される別のクラスタを設定するには、VMwareドキュメントの「vSphereのNSXとの共存」および「NSX-T の使用例2」を参照してください。
3. VMwareのドキュメントを参照して、NSX-T管理用のESXiホストおよびクラスタを調整してください。
4. NSX-VにEdgeクラスタが含まれている場合は、VMwareドキュメントの NSX Edge Networking Setup を参照して、NSX-Tのエッジクラスタでルーティングまたはブリッジモードを設定してください。
5. 移行プロセスを続行する前に、ネットワーク接続を確認してください。

ステップ1:NSX-TネットワークとvCenterインフラストラクチャの準備

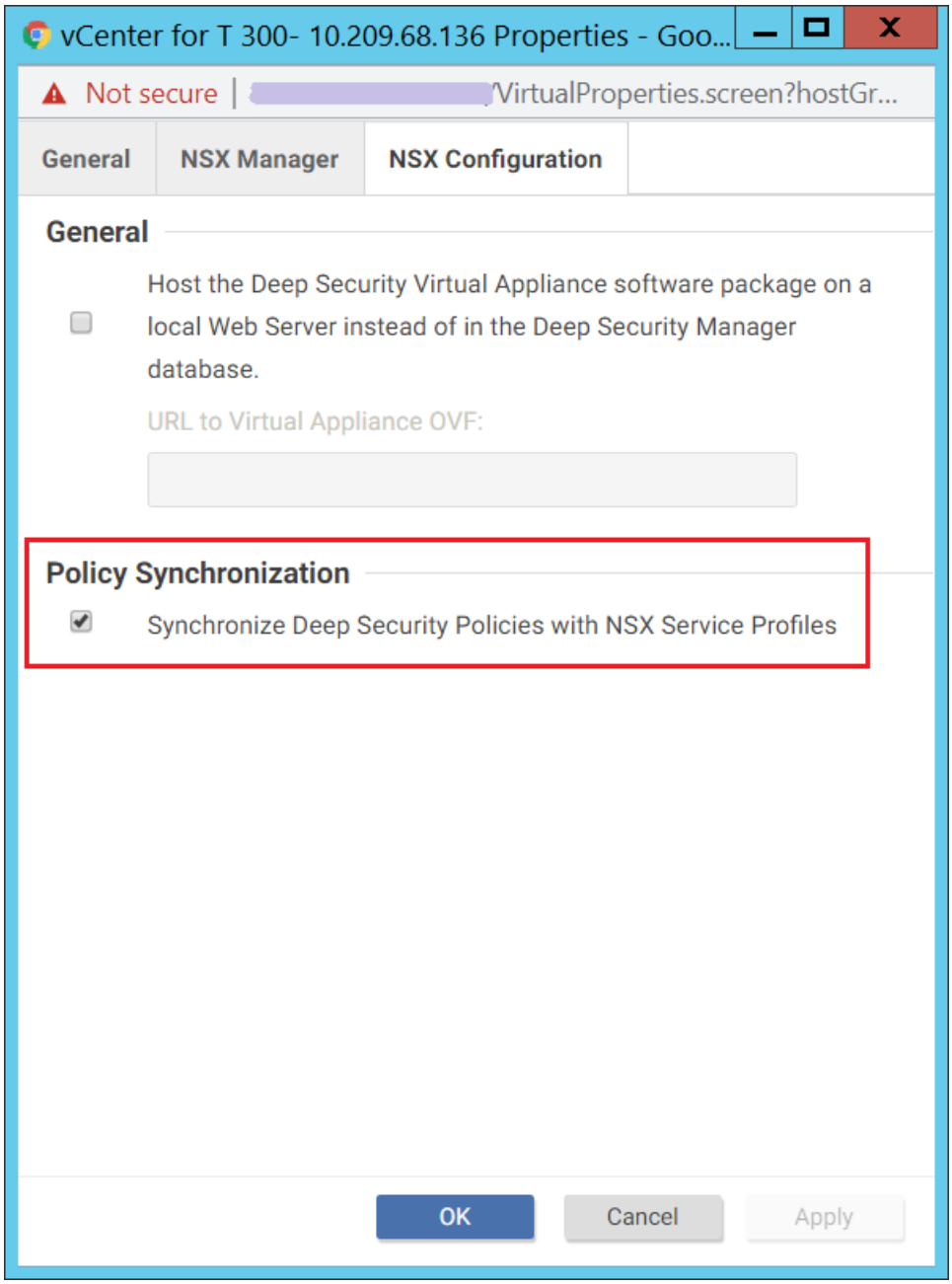
Fabric設定の準備 の手順に従って、NSX-Tで管理するクラスタを設定します。

ステップ2:新しいアプライアンスをインポートする

次に、Deep Security Managerで、が新しいDeep Security Virtual Applianceをインポートします。

ステップ3:移行する

1. 変更をロールバックする必要がある場合に備えて、Deep Security Managerデータベースをバックアップします。
2. Deep Security Managerで、[Computers]画面に移動し、vCenterコネクタを右クリックして、[Properties]を選択します。[NSX Configuration]タブで、[Policy Synchronization]の下のオプションが選択されているかどうかを確認します。この手順の後半でこれを知っておく必要があります。



3. NSX-Vバインディングを削除します。Deep Security Managerで、[Computers]画面に移動し、vCenterコネクタを右クリックして、[Properties]を選択します。[NSX Manager] タブで、[NSX Managerの削除] をクリックします。

   ヒント: Deep Security Managerがシステムイベント397(「VMware NSX Callback Authentication Failed」),) を受信した場合、NSX設定はDeep Security Managerから削除されていますが、NSX-VにはDeep Securityサービスがあります。この問題は、移行が完了し、NSX-Vをシャットダウンまたはアンインストールすると解決されます。

   注意: この手順では、Deep Security ManagerからNSX-Vの設定が削除されますが、NSX-VにはDeep Securityサービスがあるため、VMはまだ保護されています。NSX-V環境からDeep Securityを手動で削除する必要があります(「"NSX-V環境からのDeep Securityの手動アンインストール" on page 1740」を参照) 。

   警告: 移行プロセス中にNSX-Vで管理されるクラスタに配信されるワークロードは変更しないでください。

4. NSX-Tバインディングを追加します。Deep Security Managerで、[Computers]画面に移動し、vCenterコネクタを右クリックして、[Properties]を選択します。NSX Manager タブで次の操作を実行します。
   a. NSX-T Managerのアドレスと資格情報を入力します。
   b. [Add/Update] [証明書]をクリックして、NSX-T SSL証明書を追加します。
   c. [接続のテスト] [ ]をクリックして、Deep Security ManagerがNSX-T Managerに接続できることを確認します。
   d. [OK] をクリックします。
5. [NSX Configuration]タブで、[Policy Synchronization]の下のオプションが手順2での設定であることを確認します。
6. Deep SecurityサービスがNSX-Tに登録されていることを確認してください。NSX-T ManagerのWebコンソールで、[System]→[Service Deployments]の順に選択します。「Trend Micro Deep Security」サービスを登録する必要があります。
7. Deep Security Virtual ApplianceをNSX-Tに配置します。
8. ゲストVMのアクティベーションとNSX-Tのセキュリティポリシーの割り当てには、NSX-Vと比較していくつかの追加のタスクがあります。必要なもの:
   a. "NSX-Tのセキュリティグループをアップデートする" on page 1715のセキュリティグループを更新します。
   b. "セキュリティポリシーをNSX-VからNSX-Tに移行する" on page 1722に移行する

c. アクティベーションの準備。

NSX-V環境を準備する際に方法1または方法2を使用した場合、ゲストVMを自動的にアクティベートするには、既存のイベントベースのタスクの[ポリシーの割り当て]または[条件]を変更する必要があります。

注意: NSX-Tでのセキュリティポリシーの移行およびサービスプロファイルの作成を開始すると、NSX-Vクラスタの下のゲストVMが保護機能を失う可能性があります。これは、NSXセキュリティグループのバインドが移行の一部であるためです。NSX-Tの設定が完了したゲストVMがNSX-Tクラスタに移行されると、保護が再開されます。

9. ゲストVMの移行:
   a. ゲストVMを元のクラスタから新しいVMに移動するには、vMotionを使用します。詳細については、 VDS/VSS とNSX-Tスイッチ間のvMotionを参照してください。
   b. NSX-Vでネットワークイントロスペクションを使用していた場合、vMotionの完了後、新しいvCenterがNSX-Tネットワーク上にある場合、ゲストVMは少なくとも1つのNICを論理スイッチ(オーバーレイモード)に接続してネットワークセキュリティを有効にする必要があります。NSX-Tの機能
10. Deep Security Virtual Applianceおよびゲスト VMがアクティベートされ、セキュリティポリシーが割り当てられていることを確認します。
    a. 初期設定のセキュリティポリシー「Deep Security Virtual Appliance」を使用してアプライアンスをアクティベートします。
    b. ゲストVMを有効にし、セキュリティポリシーを自動的に割り当てる必要があります。ゲストVMが期待されるセキュリティポリシーでアクティベートされていない場合は、次の手順を実行してください。
       - [Computers]画面で、vCenterを右クリックして、[Synchronize Now]を選択します。
       - ゲストVMがまだアクティベートされていない場合は、アクティベーションを行い、セキュリティポリシーを手動で割り当ててみてください。

ステップ4:新しい配信とそのセキュリティ機能を確認する

1. 不正プログラム モジュールが正し く動作していることをテストし、イベントをDeep Security Managerに送信してください。"不正プログラム検索をテストする" on page 834を参照してください。
2. ネットワーク保護モジュール(Webレピュテーション, Firewall, Intrusion Prevention)が正し く動作しており、イベントをDeep Security Managerに送信していることをテストします。"Webレピュテーションをテストする" on page 903, "ファイアウォールルールを配信前にテストする" on page 955および"侵入防御のテスト侵入防御" on page 910。

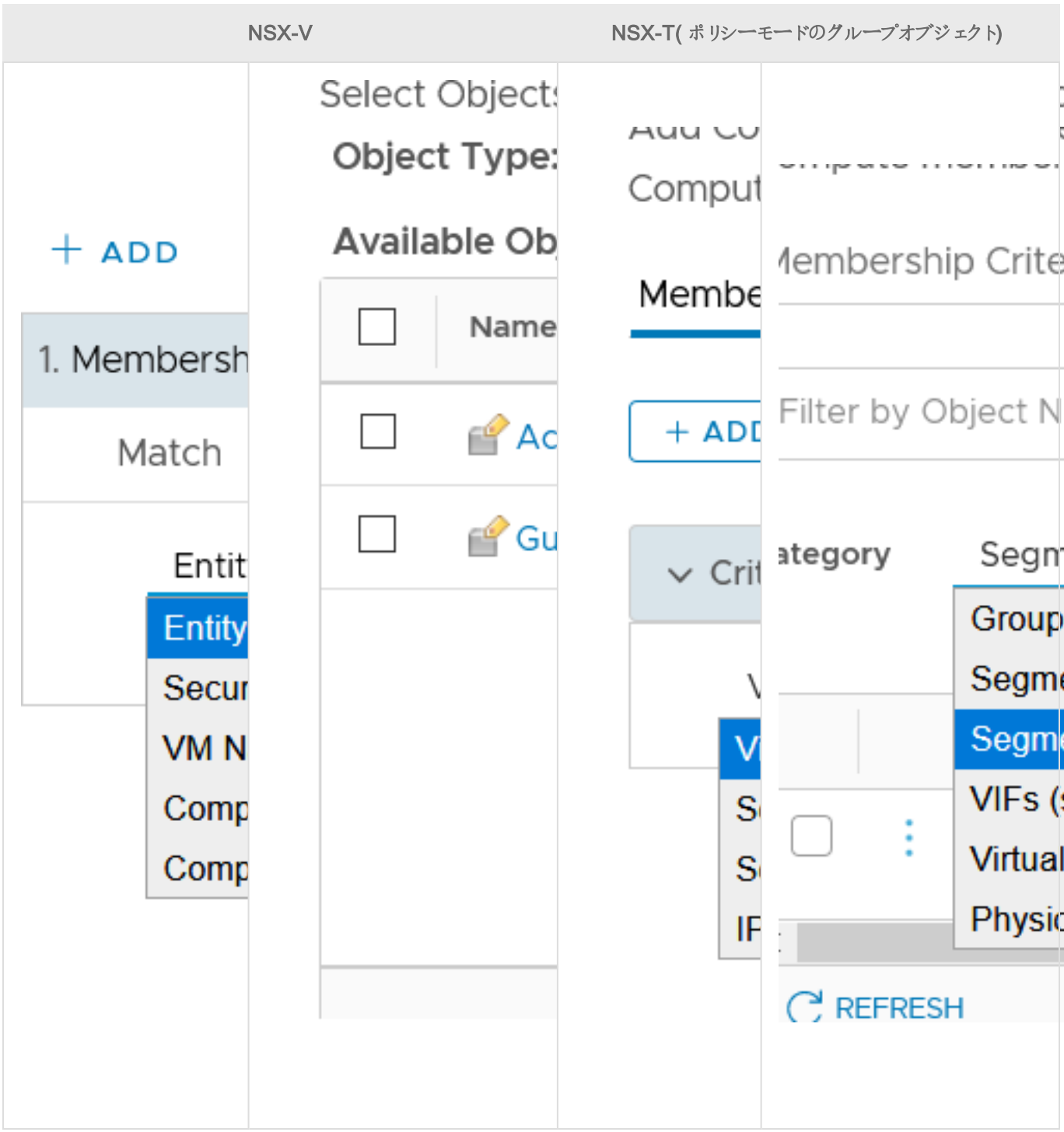
ステップ5:NSX-Vをクリーンナップする

Deep Securityモジュールが正しく機能していることを確認したら、VMwareの指示に従ってNSX-Vをクリーンナップしてください。これで、移行プロセスが完了しました。

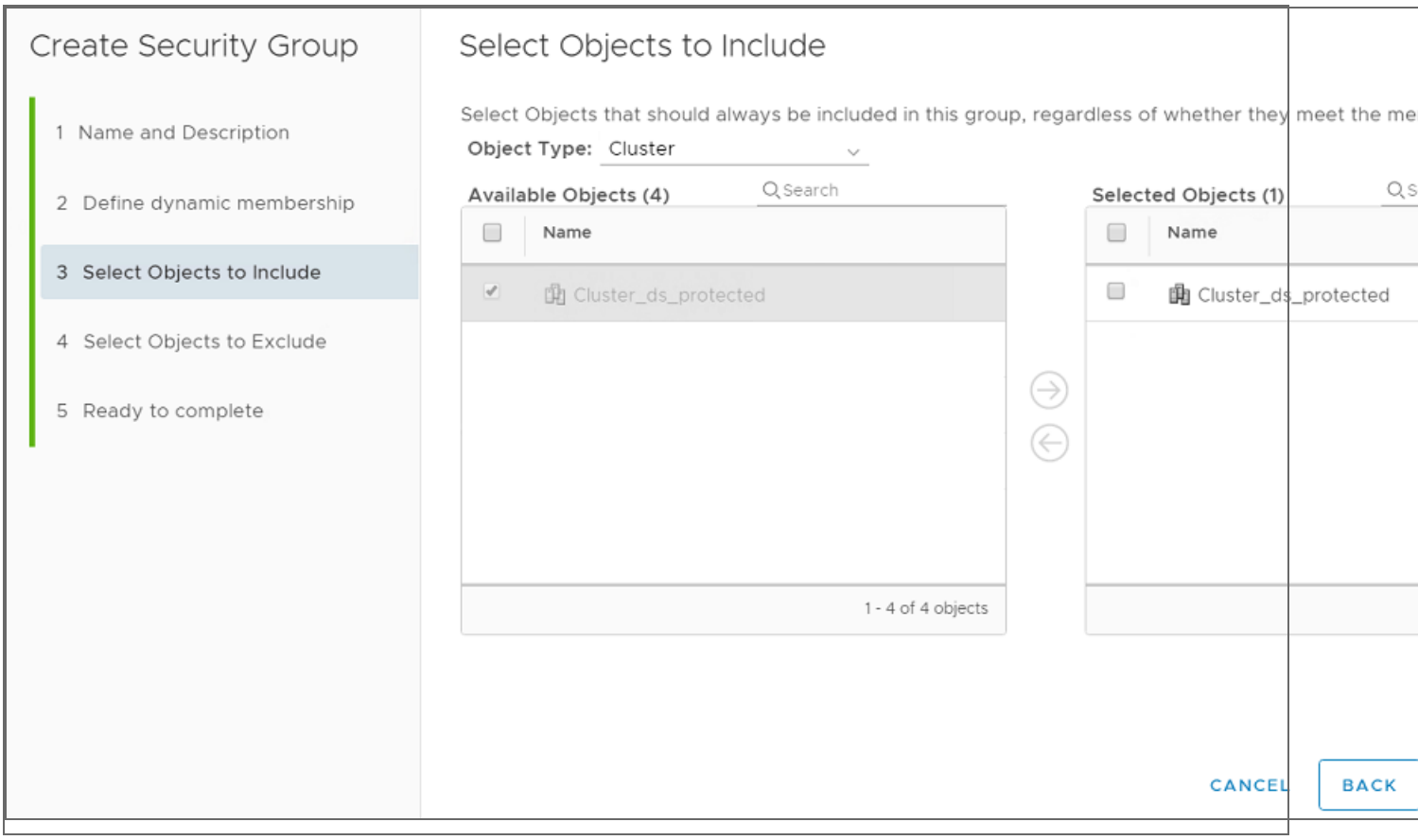
NSX-Tのセキュリティグループをアップデートする

NSX-Tでは、グループ設定のをメンバーシップ基準とNSX-Vとは異なるメンバーカテゴリで提供しています。NSX-Tでセキュリティグループを再作成する必要があります。

NSX-V		NSX-T(ポリシーモードのグループオブジェクト)	
ダイナミックメンバーシップの条件	インクルードまたは除外設定のオブジェクトの種類	ダイナミックメンバーシップの条件	メンバーカテゴリ

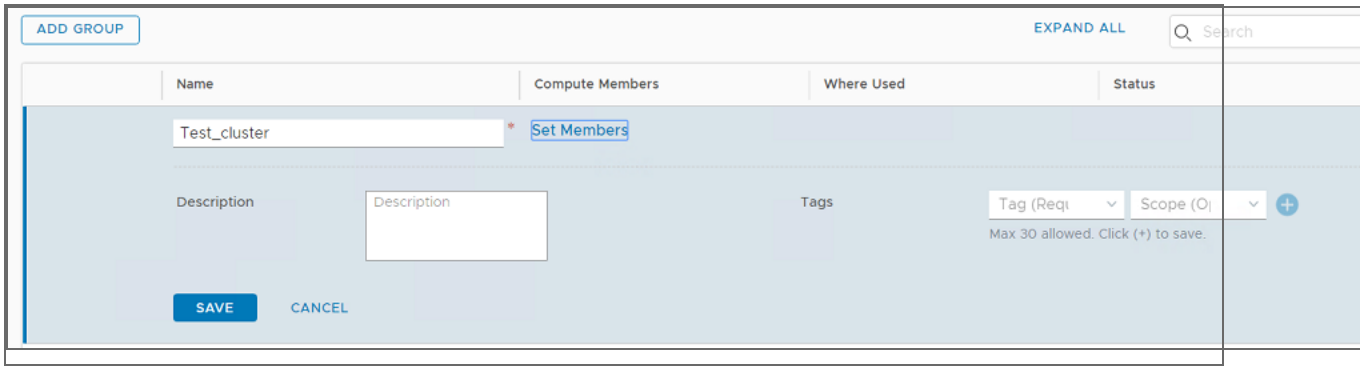


たとえば、「vCenterクラスタ」を使用するセキュリティグループを、NSX-Vのメンバーシップ条件としてNSX-Tに変換する方法があります。

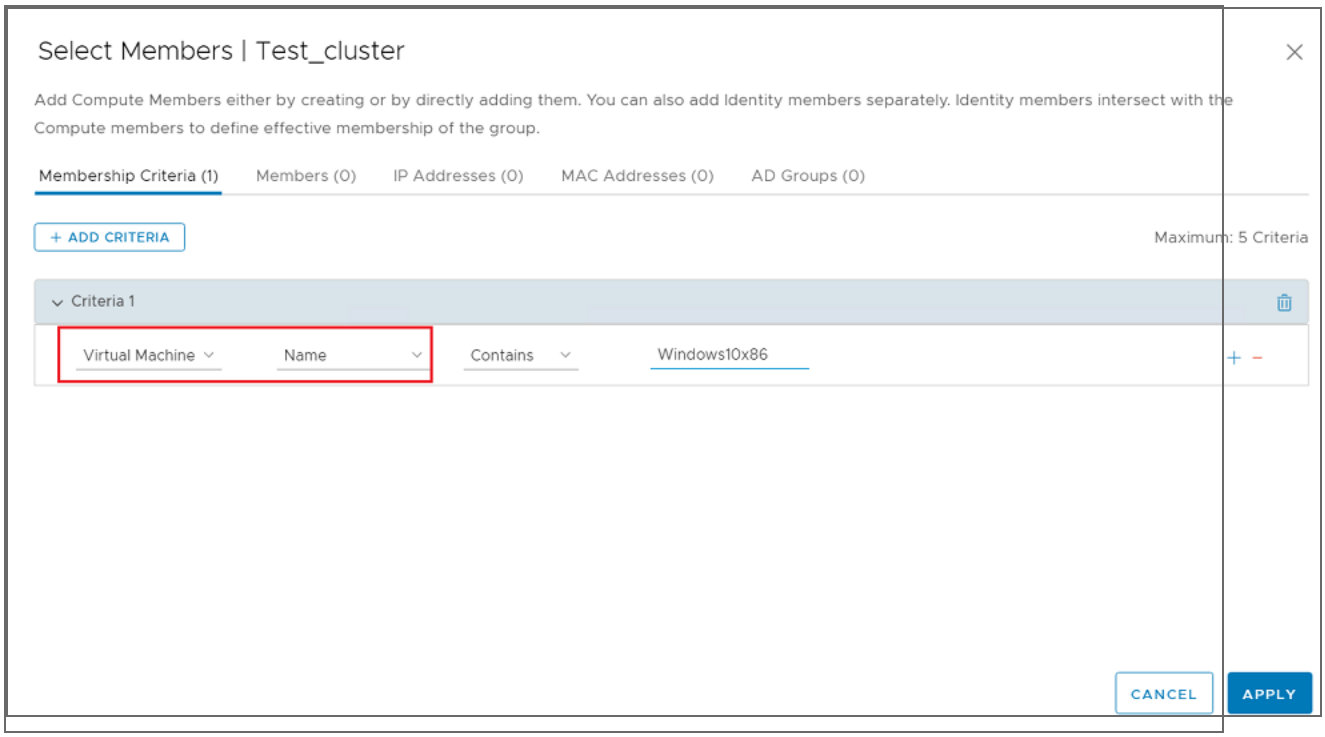


NSX-Tでは、vCenterクラスタオブジェクトはサポートされていません。次の3つの方法では、NSX-Tでサポート対象グループを設定する方法を提案します。ただし、詳細については、VMwareのマニュアルを参照する必要があります。

- 方法1:動的メンバーシップを「VM名」に基づいて定義します。
  a. グループを追加します。NSX-Tで、Inventory> Groups に移動し、[ADD GROUP]をクリックします。

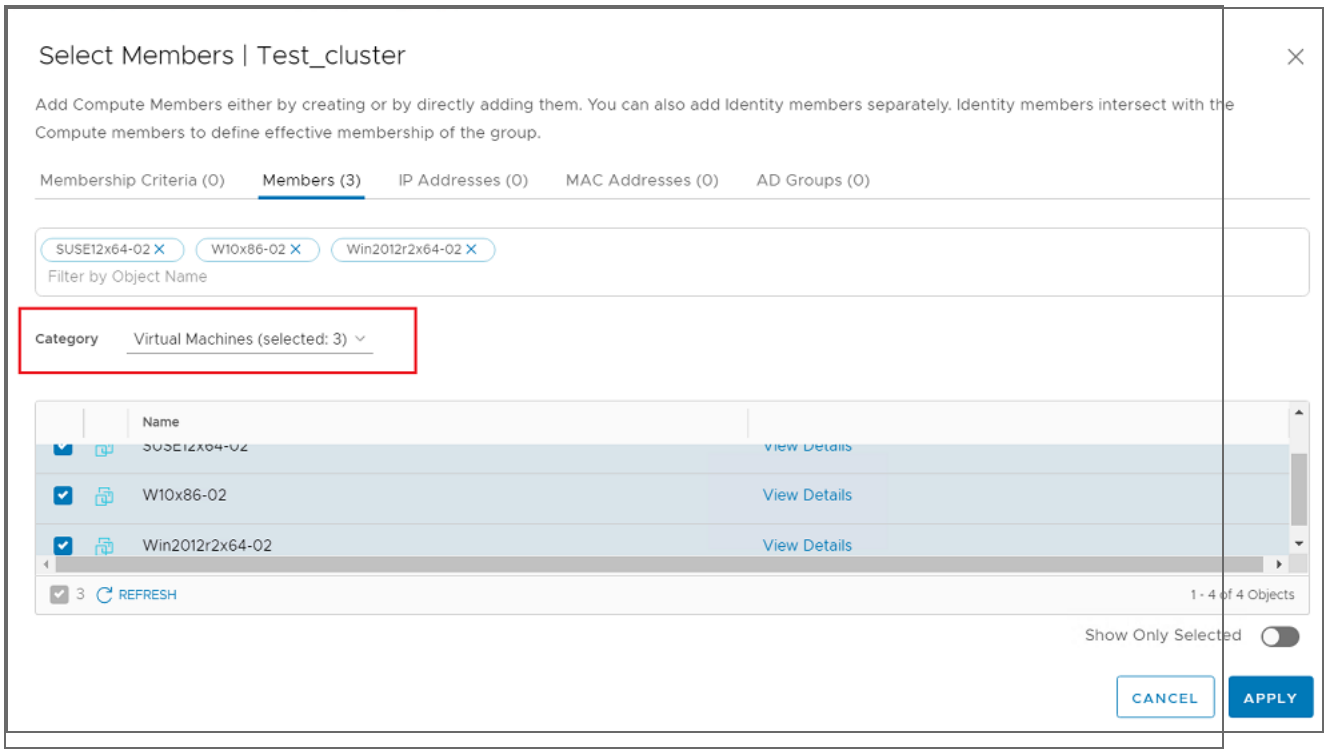


b. [メンバーの設定] []の順に選択し、[Membership Criteria]タブを選択して、[仮想マシン]と[名前]の条件を1つ作成します。

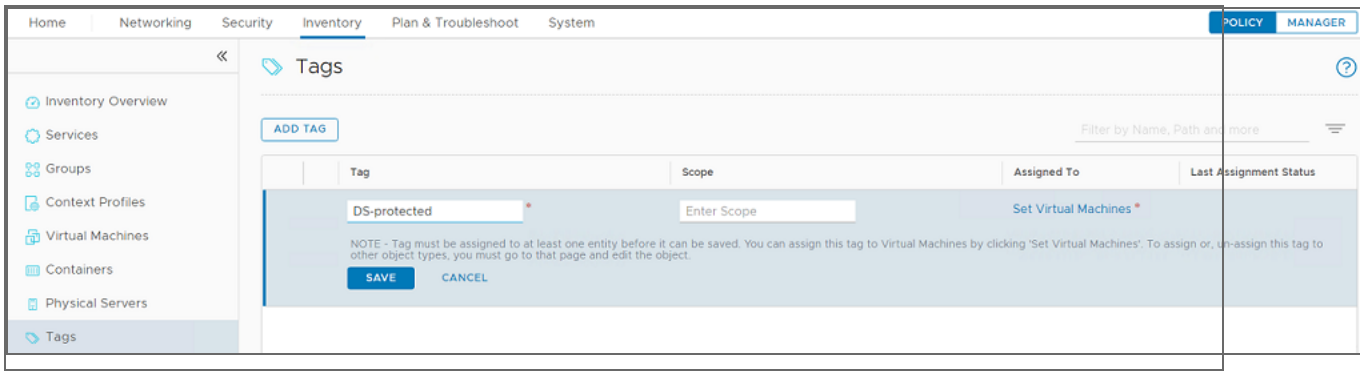


- 方法2:動的メンバーシップを「VM名」に基づいて定義します。
  a. グループを追加します。NSX-Tで、Inventory> Groups に移動し、[ADD GROUP]をクリックします。
  b. [メンバーの設定] [ ]の順に選択し、[メンバー] [ ]タブを選択します。カテゴリで、保護を

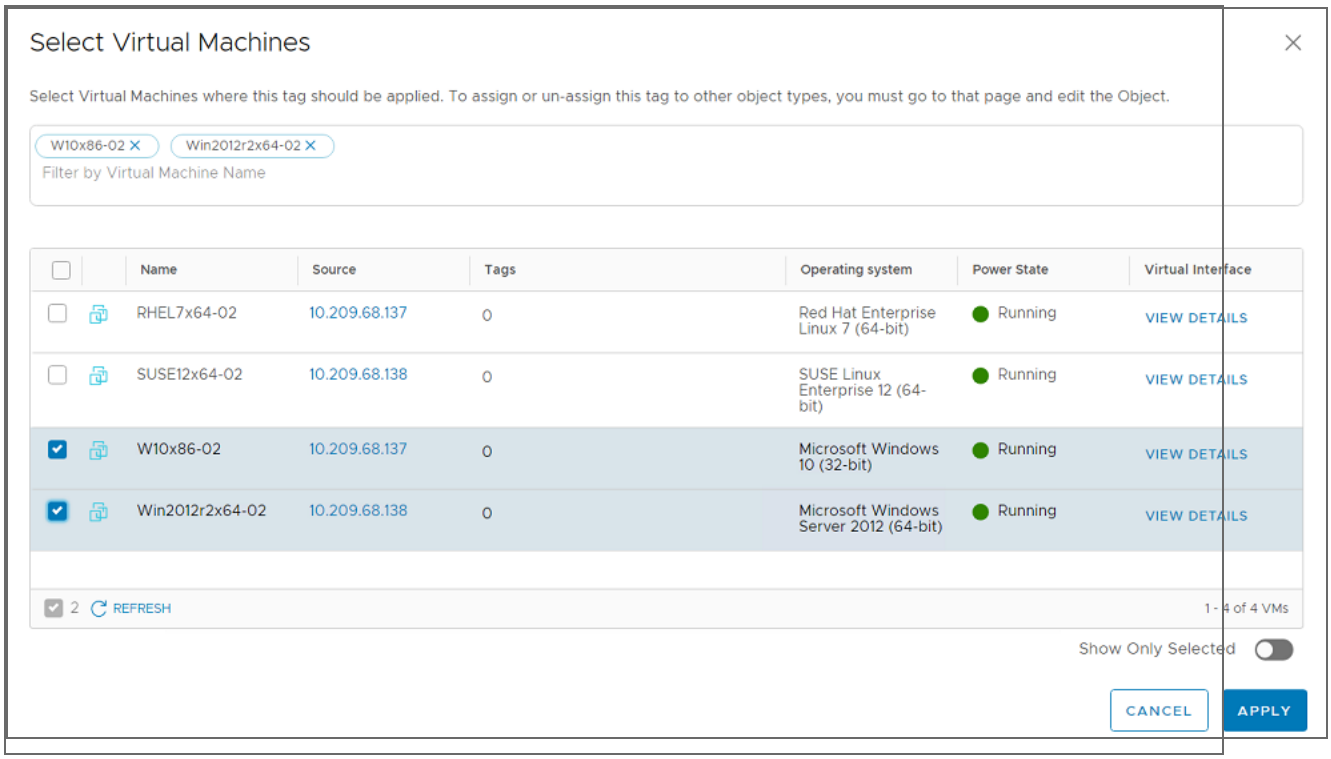
NSX-Tに移行するVMを選択します。



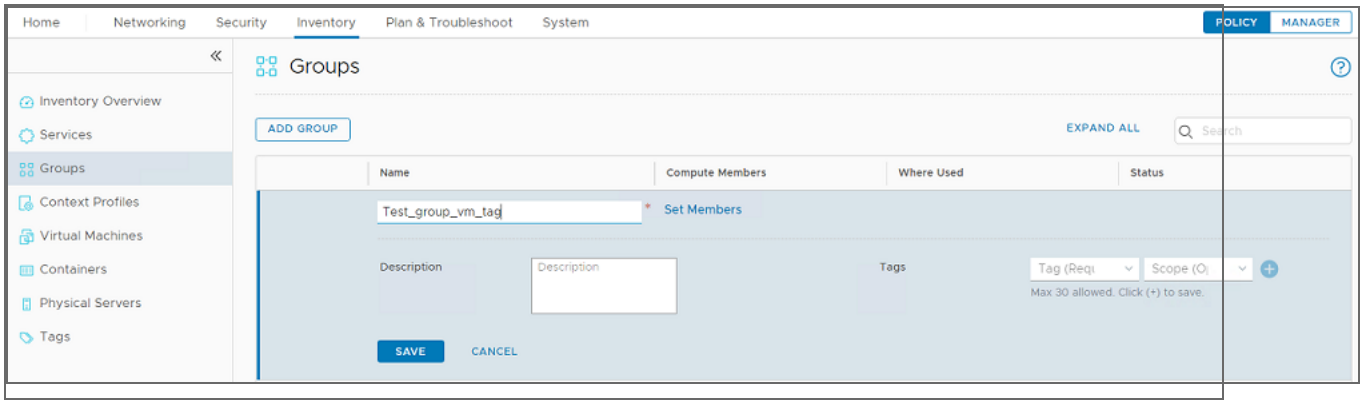
- 方法3: グループメンバーシップのタグを使用する:
  a. NSX-Tで、Inventory> Tag に移動し、タグを作成します。



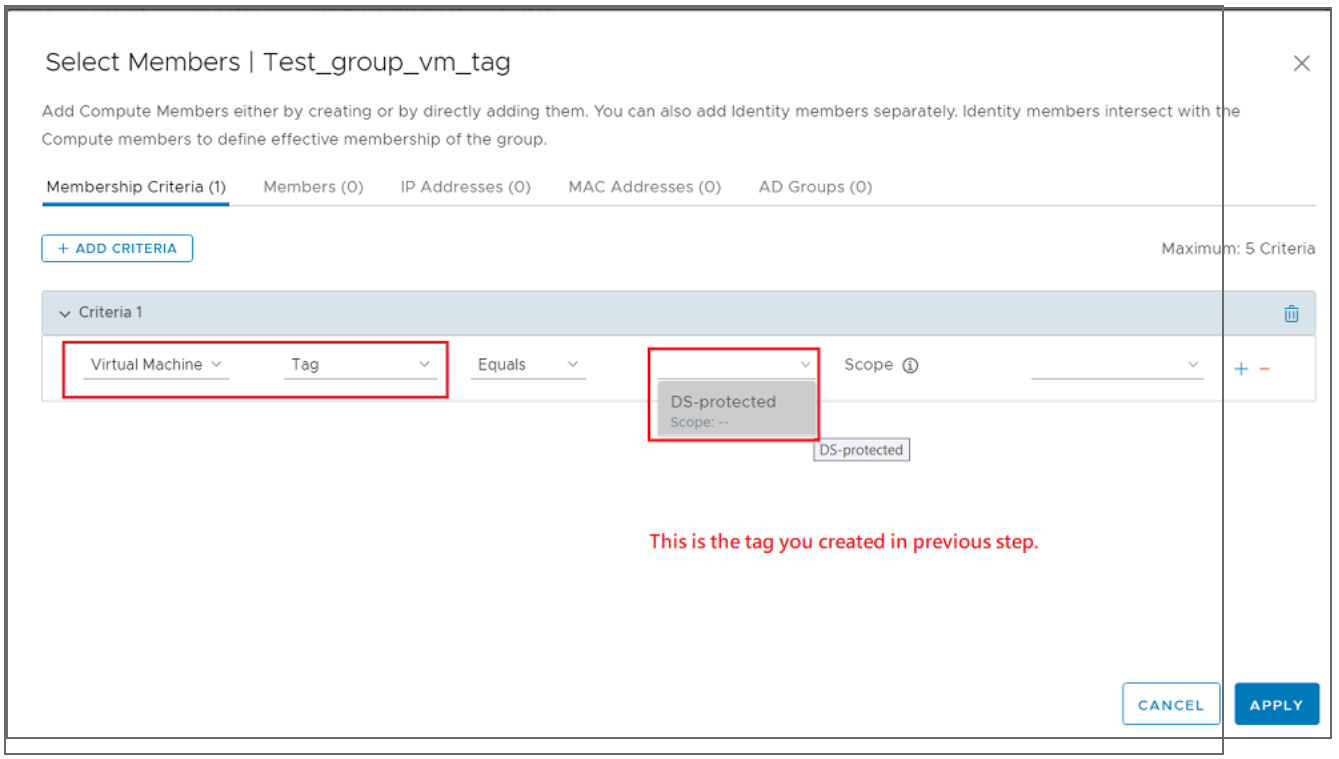
b. [仮想マシンの設定] [ ]をクリックし、VMにタグを割り当てます。



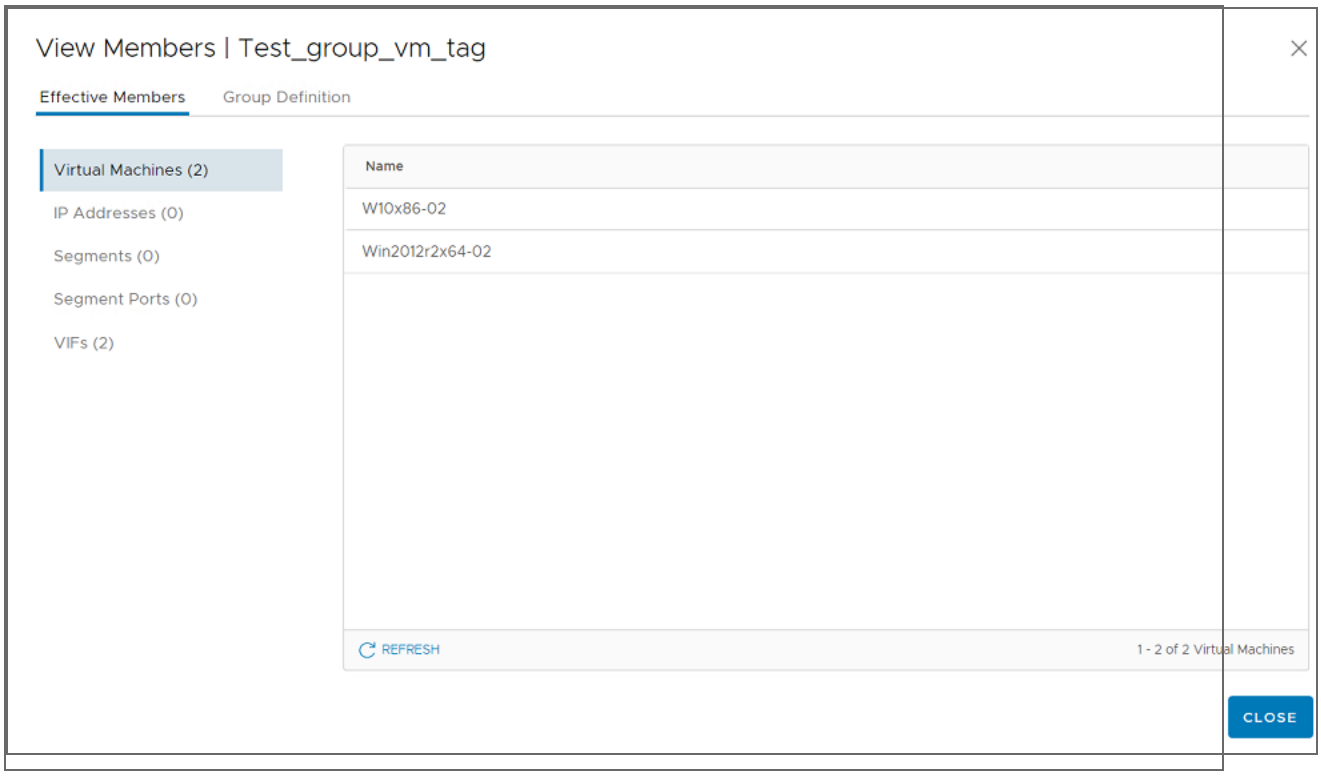
c. [Inventory]→[Groups]の順に選択し、[ADD GROUP]をクリックして新しいセキュリティグループを追加します。



d. [メンバーの設定] [ ]をクリックし、[仮想マシン]および[タグ]条件を追加します。



e. [メンバーの表示] []の順にクリックします。設定されたVMが仮想マシンにリストされている必要があります。



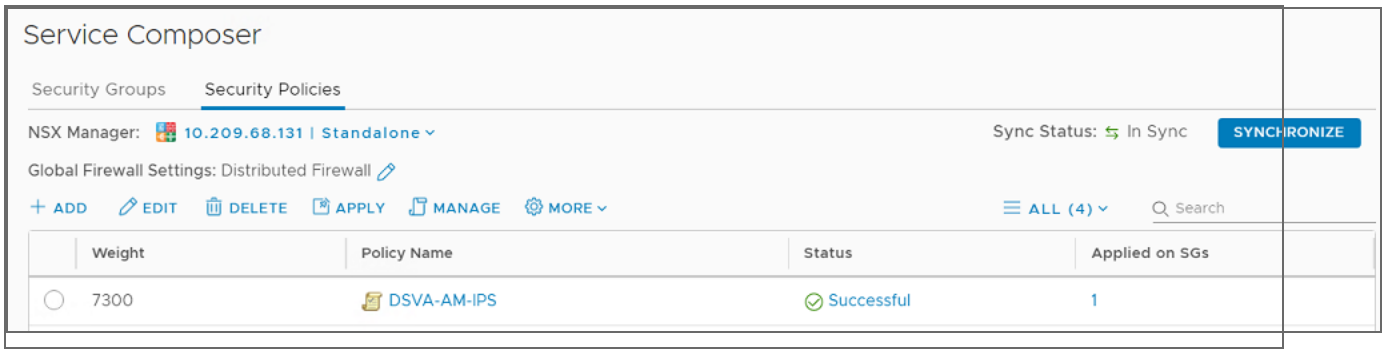
セキュリティポリシーをNSX-VからNSX-Tに移行する

NSX-Vでは、セキュリティポリシーにゲストイントロスペクションサービスとネットワークイントロスペクションサービスの両方の設定が含まれます。NSX-Tの設定を次の手順で再作成する必要があります。

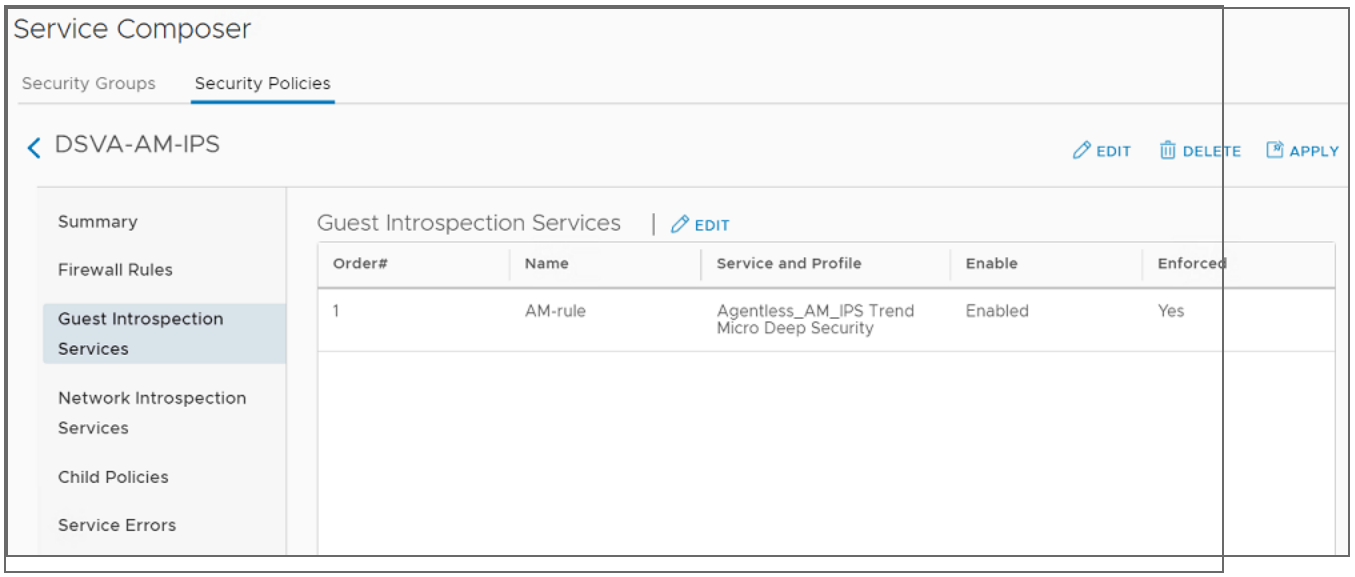
1. "現在のNSX-V設定を確認する" below
2. "NSX-Tのゲストイントロスペクション設定を再作成します" on page 1724のゲストイントロスペクション設定を再作成します
3. "NSX-Tのネットワークイントロスペクション設定を再作成する" on page 1725のネットワークイントロスペクション設定を再作成する

現在のNSX-V設定を確認する

1. vCenterで、[ネットワーク/セキュリティ]→[サービスコンポーザ]→[セキュリティポリシー]に移動します。Deep Securityサービスに対して作成されたポリシーを見つけます。それらは、NSX-T用に再作成する必要があるポリシーです。

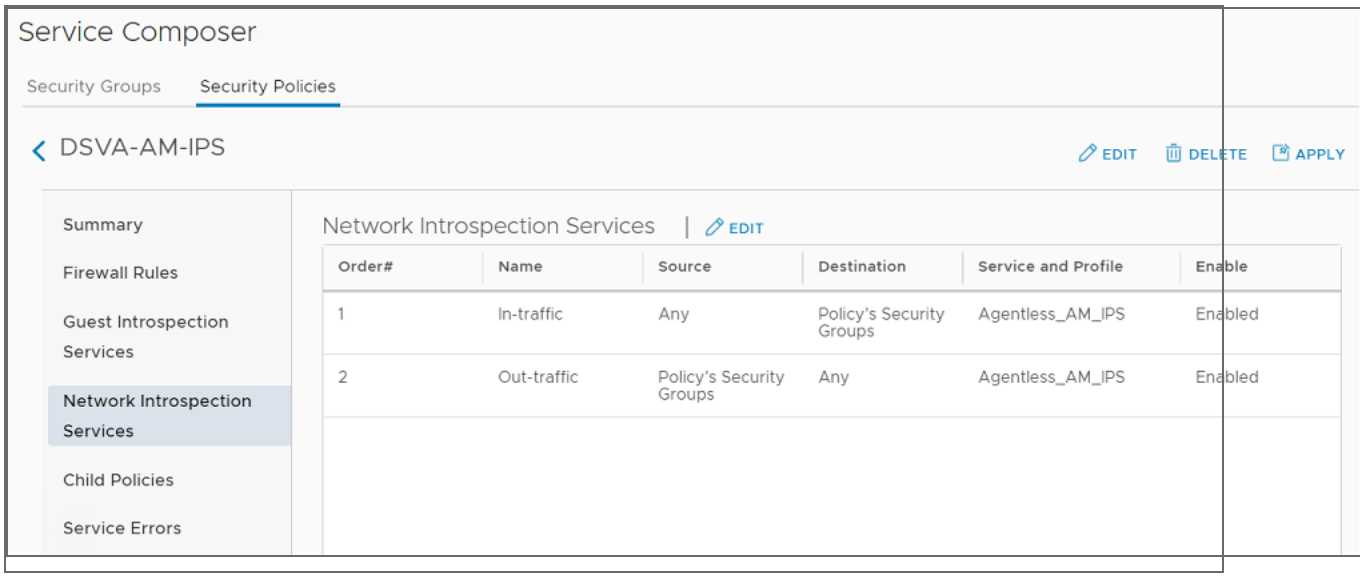


2. セキュリティポリシーごとに:
   a. ポリシーをクリックします。
   b. 左側のペインで[Guest Introspection Services]をクリックします。



   c. サービスおよびプロファイル列の値をメモしておきます。この情報は、NSX-Tのエンドポイント保護ルールとサービスプロファイルを作成する際に必要になります(次のセクションで説明します) 。

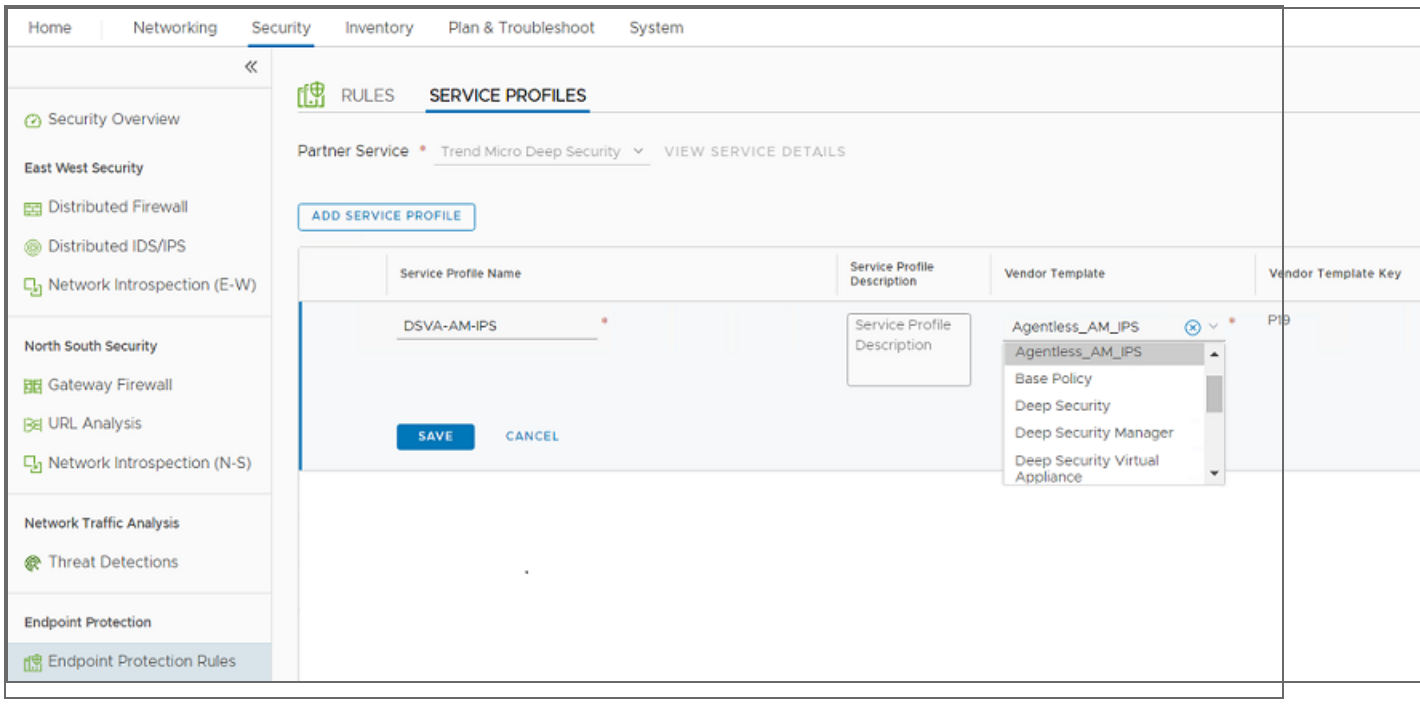
d. 左側のペインで、[Network Introspection Services]をクリックします。



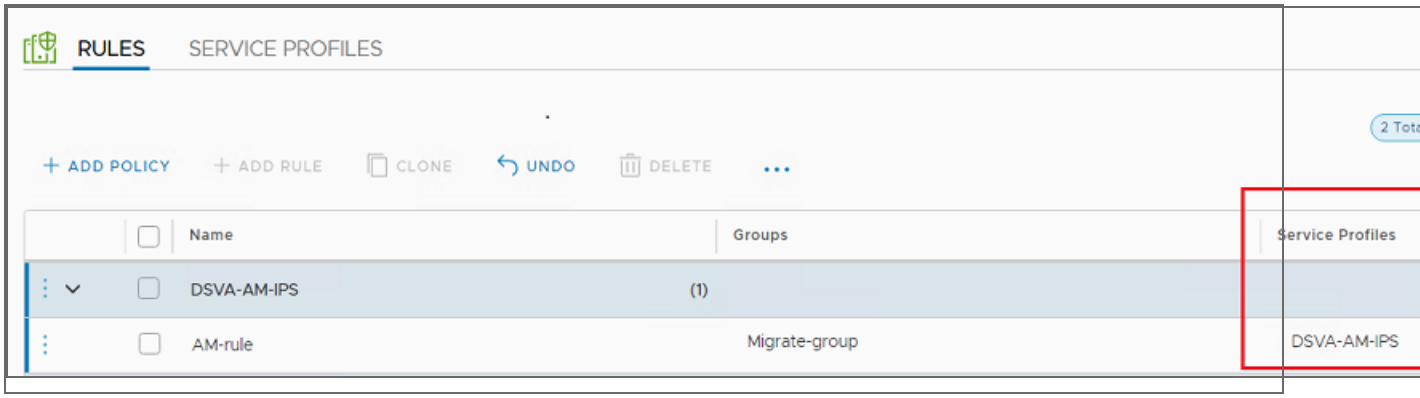
e. この表の値に注意してください。この情報は、Network Introspection Settings for NSX-Tを作成するときに必要になります(後で説明します) 。

NSX-Tのゲストイントロスペクション設定を再作成します

1. NSX-T Webコンソールで、[Security]→[Endpoint Protectionルール]の順に選択します。
2. サービスプロファイルを作成します。NSX-Vの設定(上記の手順2cの Guest Introspection Service の サービスおよびプロファイル 列の値) に基づいて、Vendor Template を選択します。

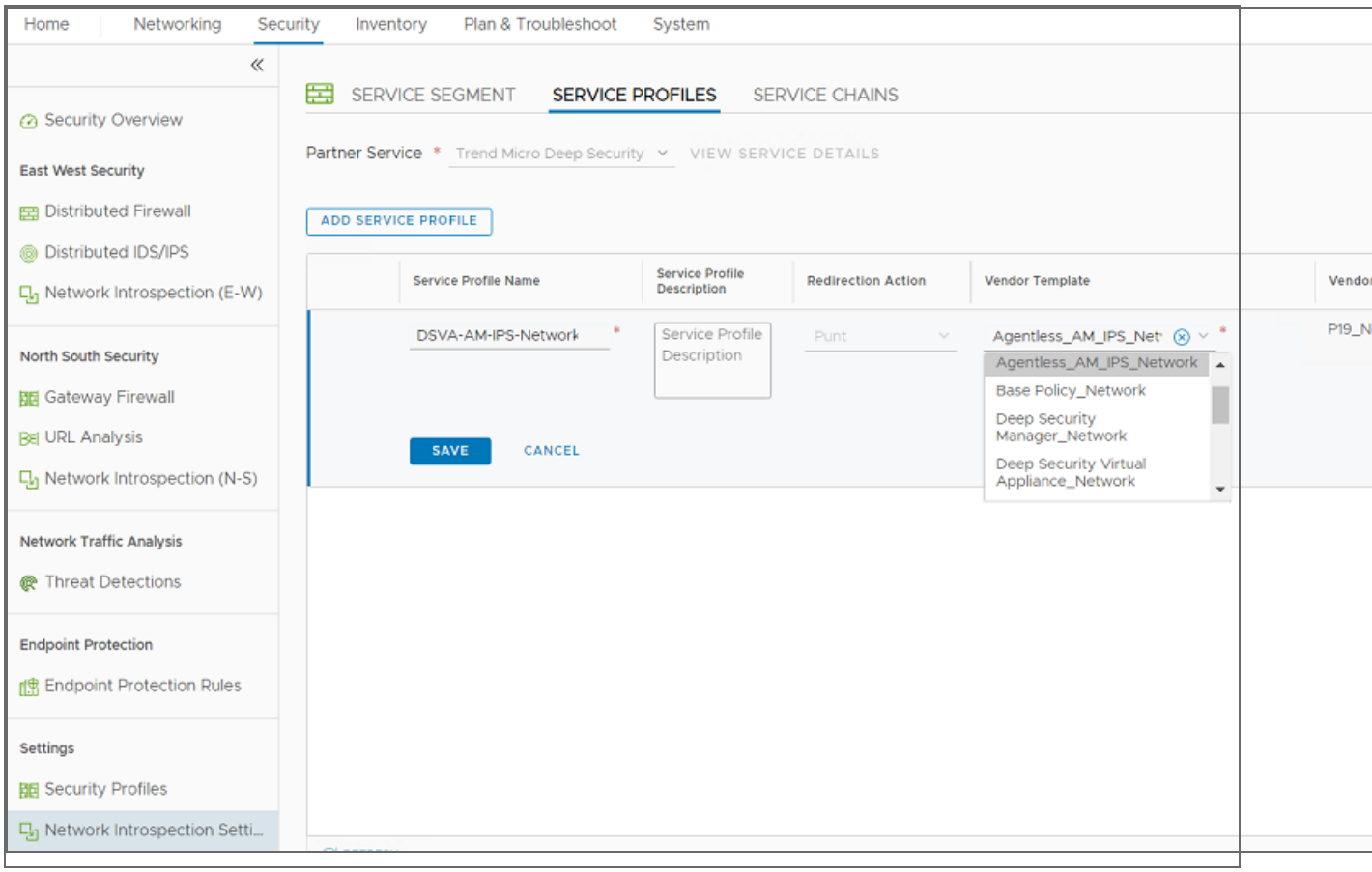


3. 新しいルールを作成して、Guest Introspection Services for NSX-Vで定義された各ルールを置き換えます(上記の手順2cを参照)。新しいルールごとに、前の手順で作成した対応するサービスプロファイル を選択します。

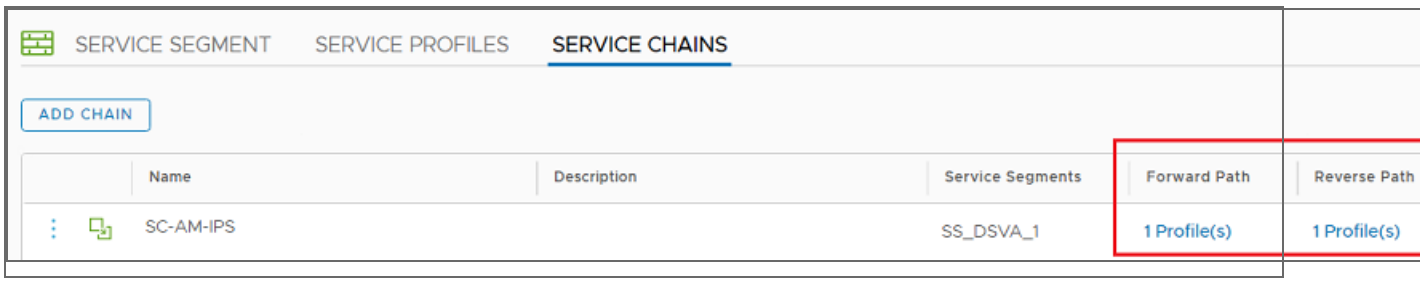


NSX-Tのネットワークイントロスペクション設定を再作成する

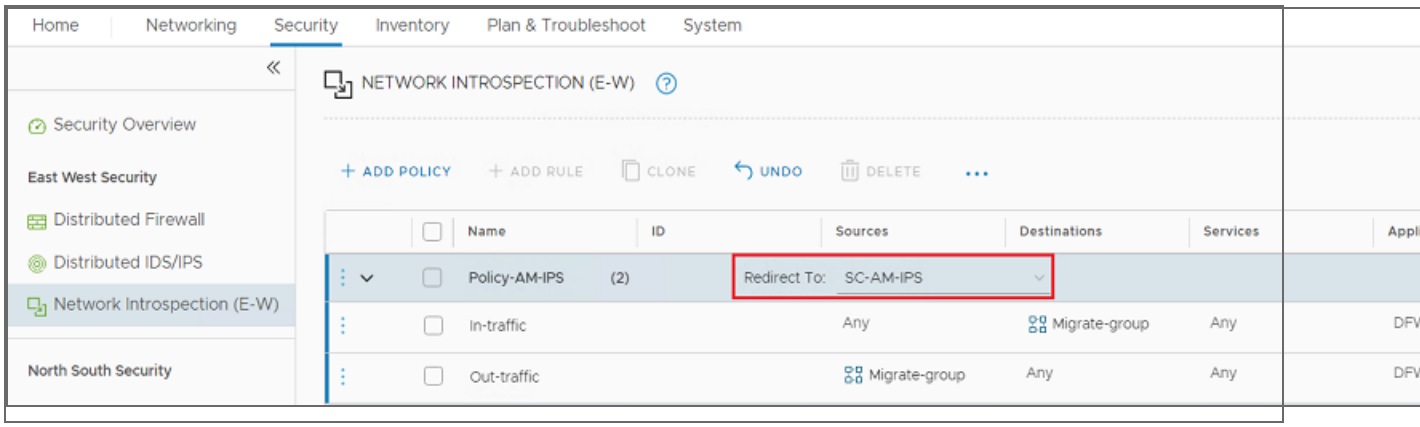
1. NSX-T Webコンソールで、Security> Network Introspection Settings>サービスプロファイルに移動します。
2. サービスプロファイルを作成します。NSX-Vの設定(上記の手順2eの Network Introspection Service の サービスおよびプロファイル 列の値) に基づいて、Vendor Template を選択します。プレフィックス名が同じで、完全名が「same_name」_Networkのベンダーテンプレート名を探します。この例では、「Agentless_AM_IPS_Network」です。



3. Service Chains に移動し、前の手順で作成したサービスプロファイルを選択してサービスチェーンを作成します。[サービスセグメント]フィールドで、Deep Security Virtual ApplianceをNSX-T上に配置したときに作成したセグメントを選択します。



4. Security> Network Introspection(EW) に移動します。
5. Network Inspection Services for NSX-V(上記の手順2eを参照) に現在あるセキュリティポリシーごとに1つのポリシーを追加し、このポリシーにルールを追加します。[へのリダイレクト]ファイルで、手順3で作成したサービスチェーンを選択します。



Deep Securityのアンインストール

Deep Securityのアンインストール

有効化されたDeep Security Agentまたはリレーをコンピュータから手動でアンインストールすると、Deep Security Managerにソフトウェアがアンインストールされたことは通知されません。Deep Security Managerの[コンピュータ]画面では、コンテキストに応じて、コンピュータのステータスが「管理(オフライン)」または類似した状態になります。これを回避するには、Deep Security Managerで次のいずれかを実行します。

- エージェントまたはリレーを無効化してから、アンインストールしてください。
- エージェントをアンインストールしてから、コンピュータをリストから削除します。

Deep Security Relayのアンインストール

Deep Security Relayは、リレー機能が有効なエージェントです。リレーを削除するには、エージェントソフトウェアをアンインストールする必要があります。

WindowsでのRelayのアンインストール

WindowsでDeep Security AgentまたはRelayをアップデートまたはアンインストールする前に、Agentのセルフプロテクションを無効にする必要があります。これを実行するには、Deep Security Managerでコンピュータエディタ[1]>設定>一般。[Agentセルフプロテクション]で、[ローカルエンドユーザによるAgentの

[1] コンピュータエディタを開くには、[コンピュータ]画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

アンインストール、停止、またはその他の変更を禁止する] の選択を解除するか、ローカルオーバーライドのパスワードを入力します。

Windowsの [コントロール パネル] で、[プログラムの追加と削除] を選択します。[Trend Micro Deep Security Agent] をダブルクリックして、[削除] をクリックします。

次のコマンドを使用して、コマンドラインからアンインストールすることもできます。

```
msiexec /x <package name including extension>
```

サイレントアンインストールを実行する場合は前述のコマンドに、/quietを追加します。

LinuxでのRelayアンインストール

Relayと、Red Hatパッケージマネージャ(RPM) を使用するプラットフォーム (CentOS、Amazon Linux、Oracle Linux、SUSE、CloudLinuxなど) に作成された設定ファイルを完全に削除するには、次のコマンドを実行します。

```
# sudo rpm -ev ds_agent
 Stopping ds_agent: [ OK ]
 Unloading dsa_filter module [ OK ]
```

Relay有効化済みAgentのインストール前にiptablesが有効になっていた場合は、Relay有効化済みAgentをアンインストールするときに再度有効になります。

注意: Deep Security Managerの管理対象コンピュータのリストおよびRelayグループから、Relay有効化済みAgentを必ず削除してください。

Deep Security Agentをアンインストールする

WindowsでのAgentアンインストール

WindowsでDeep Security AgentやRelayをアップデートまたはアンインストールする際は、Agentセルフプロテクションを無効にしておく必要があります。これを実行するには、Deep Security Managerで、**コンピュータエディタ**[1]]→[設定]→[一般]の順に選択します。[Agentセルフプロテクション] で、[ローカルのエンドユーザによるAgentのアンインストール、停止、または変更を拒否] の設定をオフにするか、ローカルでオーバーライドするためのパスワードを入力します。

---

1 コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (またはコンピュータを選択して [詳細] をクリック) します。

1. Deep Security Managerを使用してエージェントを無効にするには、[コンピュータ]画面に移動し、コンピュータを右クリックして[処理]→を選択します。
   Deep Security Managerがエージェントと通信できないためにエージェントを非アクティブ化できない場合は、次の手順に進む前に次の手順を実行する必要があります.
   `C:\Program Files\Trend Micro\Deep Security Agent>dsa_control --selfprotect 0`
2. Windowsコントロールパネルを開き[プログラムのアンインストール]を選択します。
3. Trend Micro Deep Security Agentを探して、[アンインストール]を選択します。

次のコマンドを実行して、コマンドラインからアンインストールすることもできます。

```
msiexec /x <拡張子を含むパッケージ名>
```

サイレントアンインストールを実行する場合は、前述のコマンドに`/quiet`を追加します。

LinuxでのAgentアンインストール

Linuxでエージェントをアンインストールする前に、エージェントセルフプロテクションが有効かどうかを確認してください。有効になっている場合は、ポリシーまたはコンピュータレベルで無効にする必要があります。詳細については、エージェントセルフプロテクションの有効化または無効化を参照してください。

Linuxのバージョンでグラフィカルパッケージ管理ツールが用意されている場合は、`ds_agent`パッケージを探して、このツールを使用してパッケージを削除します。それ以外の場合は、以下のコマンドラインの手順を使用します。

Agentと、Red Hatパッケージマネージャ(RPM)を使用するプラットフォーム(CentOS、Amazon Linux、Oracle Linux、SUSE、CloudLinuxなど)に作成された設定ファイルを完全に削除するには、次のコマンドを実行します。

```
# sudo rpm -ev ds_agent
 Stopping ds_agent: [ OK ]
 Unloading dsa_filter module [ OK ]
```

Deep Security Agentのインストール前に、iptablesが有効になっていた場合は、Deep Security Agentをアンインストールするときに再度有効になります。

Debianパッケージマネージャ(dpkg)を使用するプラットフォーム(DebianやUbuntuなど)の場合は、次のコマンドを実行します。

```
$ sudo dpkg -r ds-agent
 Removing ds-agent...
 Stopping ds_agent: .[OK]
```

Solaris 10でのAgentアンインストール

次のコマンドを実行します。

```
pkgrm ds-agent
```

アンインストール後に再起動が必要になる場合があります。

Solaris 11でのAgentアンインストール

次のコマンドを実行します。

```
pkg uninstall ds-agent
```

アンインストール後に再起動が必要になる場合があります。

AIXでのAgentアンインストール

次のコマンドを実行します。

```
installp -u ds_agent
```

Red Hat OpenShiftでのAgentアンインストール

次のコマンドを実行します。

```
helm uninstall ds-agent
```

Deep Security Notifierをアンインストールする

Windowsの [コントロール パネル] を開き、[プログラムの追加と削除] を選択します。[Trend Micro Deep Security Notifier] をダブルクリックして、[削除] をクリックします。

コマンドラインからアンインストールするには、次のコマンドを入力します。

```
msiexec /x <package name including extension>
```

サイレントアンインストールを実行する場合は、前述のコマンドに`/quiet`を追加します。

Deep Security Managerをアンインストールする

WindowsでManagerをアンインストールする

Windowsの [スタート] メニューで、[Trend Micro]→[Trend Micro Deep Security Managerアンインストーラ] の順に移動し、手順に従って、アンインストールを完了します。

コマンドラインから上記と同じWindowsを起動してアンインストールするには、次のコマンドを入力します。

```
<installation folder>\Uninstall.exe
```

コマンドラインからサイレントアンインストールするには、以下のように`-q`オプションを追加します。

```
<installation folder>\Uninstall.exe -q
```

コマンドラインを使用したサイレントアンインストール中は、設定ファイルが保持されるため、再インストール時に既存の設定を使用してエージェントが修復またはアップグレードされます。

LinuxでManagerをアンインストールする

コマンドラインからアンインストールするには、インストールフォルダに移動して次のコマンドを入力します。

```
sudo ./uninstall
```

サイレントアンインストールを実行する場合は、前述のコマンドに`-q`を追加します。

コマンドラインを使用したサイレントアンインストール中、設定ファイルは初期設定で保持されるため、再インストールすると、インストーラは既存の設定を使用してエージェントのアップグレードを修復します。

アンインストール時に設定ファイルを保持せず、後でDeep Security Managerを再インストールする場合は、再インストールする前に手動でクリーンナップを実行してください。Deep Security Managerのインストールディレクトリを削除するには、次のコマンドを実行します。

```
sudo rm -rf <installation location>
```

初期設定のインストール場所は`/opt/dsm`です。

NSX環境からのDeep Securityのアンインストール

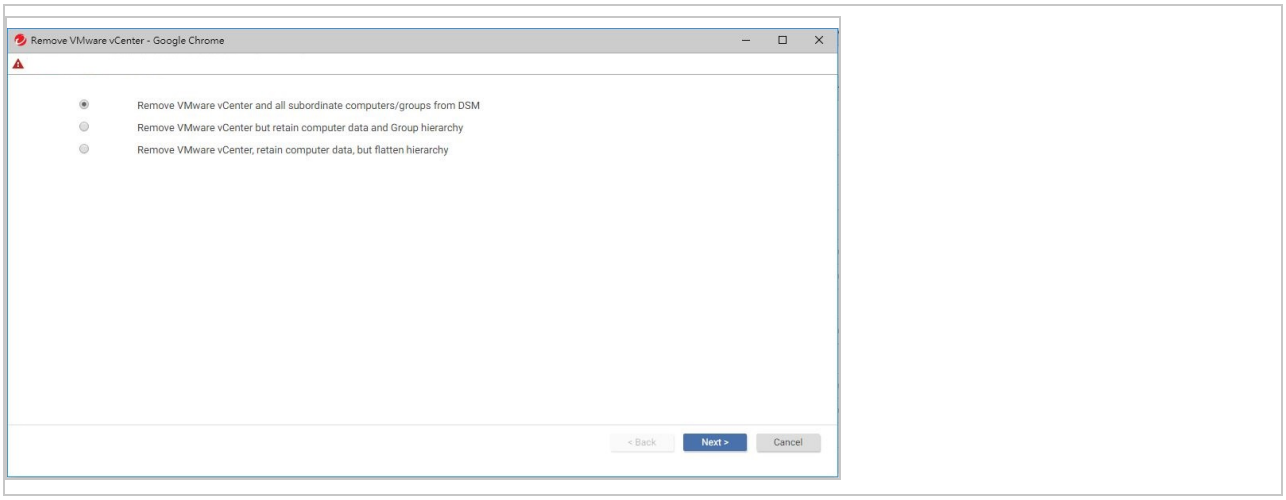
Deep SecurityをNSX環境からアンインストールすると、Deep Security Virtual ApplianceがNSX Data Center for vSphere (NSX-V) またはNSX-Tから削除され、関連するすべての履歴がDeep Security Managerから削除されます。

このページのトピック:

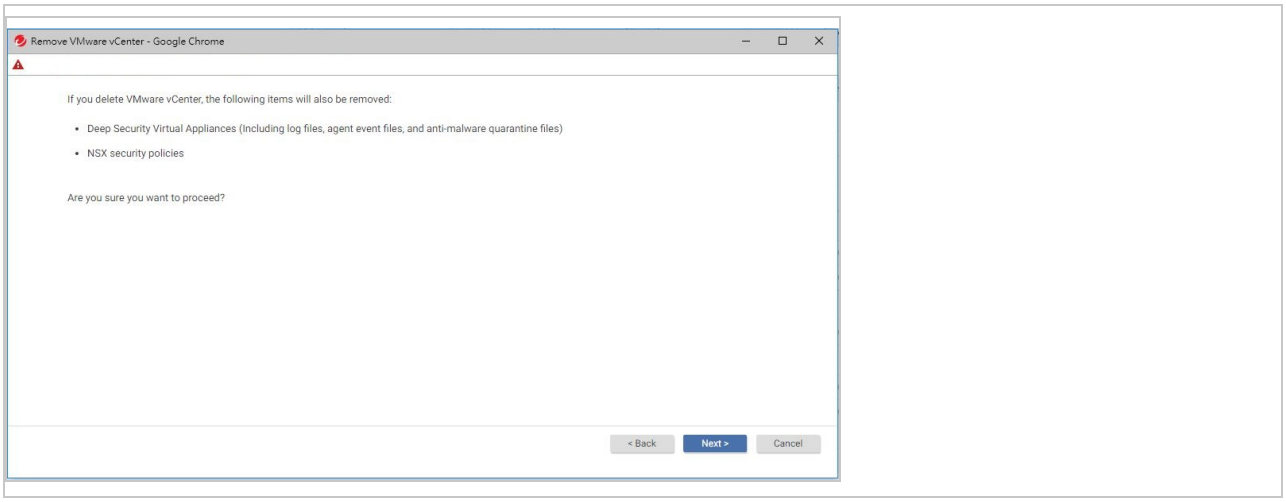
- "Deep Securityを自動的にアンインストールします" below
- "NSX-T 3.xからのDeep Securityの手動アンインストール" on the next page
- "NSX-V環境からのDeep Securityの手動アンインストール" on page 1740

Deep Securityを自動的にアンインストールします

1. Deep Security Managerで、[コンピュータ] に進みます。
2. 左側のナビゲーションツリーでvCenterを右クリックして、[VMware vCenterの削除] を選択します。
3. 次のいずれかのオプションを選択します。
   - VMware vCenterおよびすべての下位コンピュータ/グループをDSMから削除します: vCenterとすべての仮想マシンのレコード(割り当てられているDeep Securityのポリシーとルールを含む) を削除します。
   - VMware vCenterを削除しますが、コンピュータのデータおよびグループの階層は維持します: vCenterを削除しますが、階層構造と仮想マシンのレコード(割り当てられているDeep Securityのポリシーとルールを含む) は維持します。
   - VMware vCenterを削除し、コンピュータのデータを維持しますが、階層はフラット化します: vCenterを削除しますが、仮想マシンのレコード(割り当てられているDeep Securityのポリシーとルールを含む) は維持します。vCenterの階層構造は1つのグループにまとめられます。



4. いずれかのオプションを選択した後、[次へ] をクリックします。



5. もう一度 [次へ] をクリックして、削除を続行します。

   たとえば1番目のオプションである[VMware vCenterおよびすべての下位コンピュータ/グループをDSMから削除します] を選択した場合は、NSX環境からDeep Security Virtual ApplianceおよびNSXのすべてのポリシーが自動的に削除されます。

   「VMware vCenterが正常に削除されました」という処理の成功を通知するメッセージが表示されます。

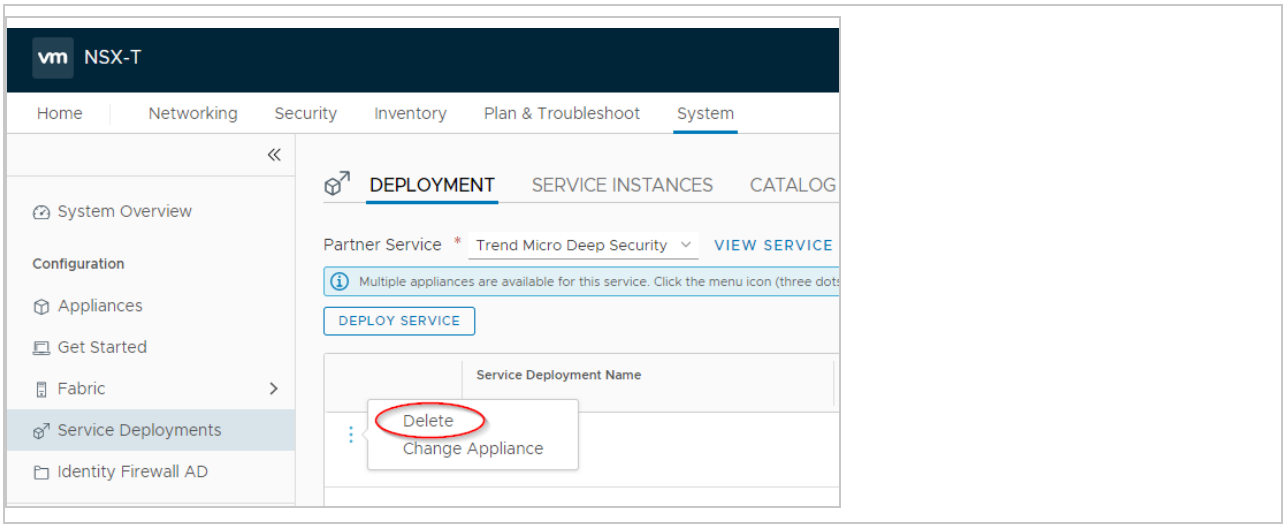
   注意: Deep Security ManagerとNSX Managerの接続が切断されている場合、「VMwareからDeep Securityを削除できません」というエラーが表示されることがあります。このエラーが発生した場合は、NSX ManagerからDeep Securityサービスを手動で削除する必要があります。詳細については、次のセクションを参照してください。

NSX-T 3.xからのDeep Securityの手動アンインストール

注意: NSX-T Managerの右上にあるPOLICYが選択されていることを確認してください。そうすることで、以下の手順で説明するユーザインタフェース要素を確認できます。

最初に、Deep Security Virtual Applianceサービスのインストールを削除します。

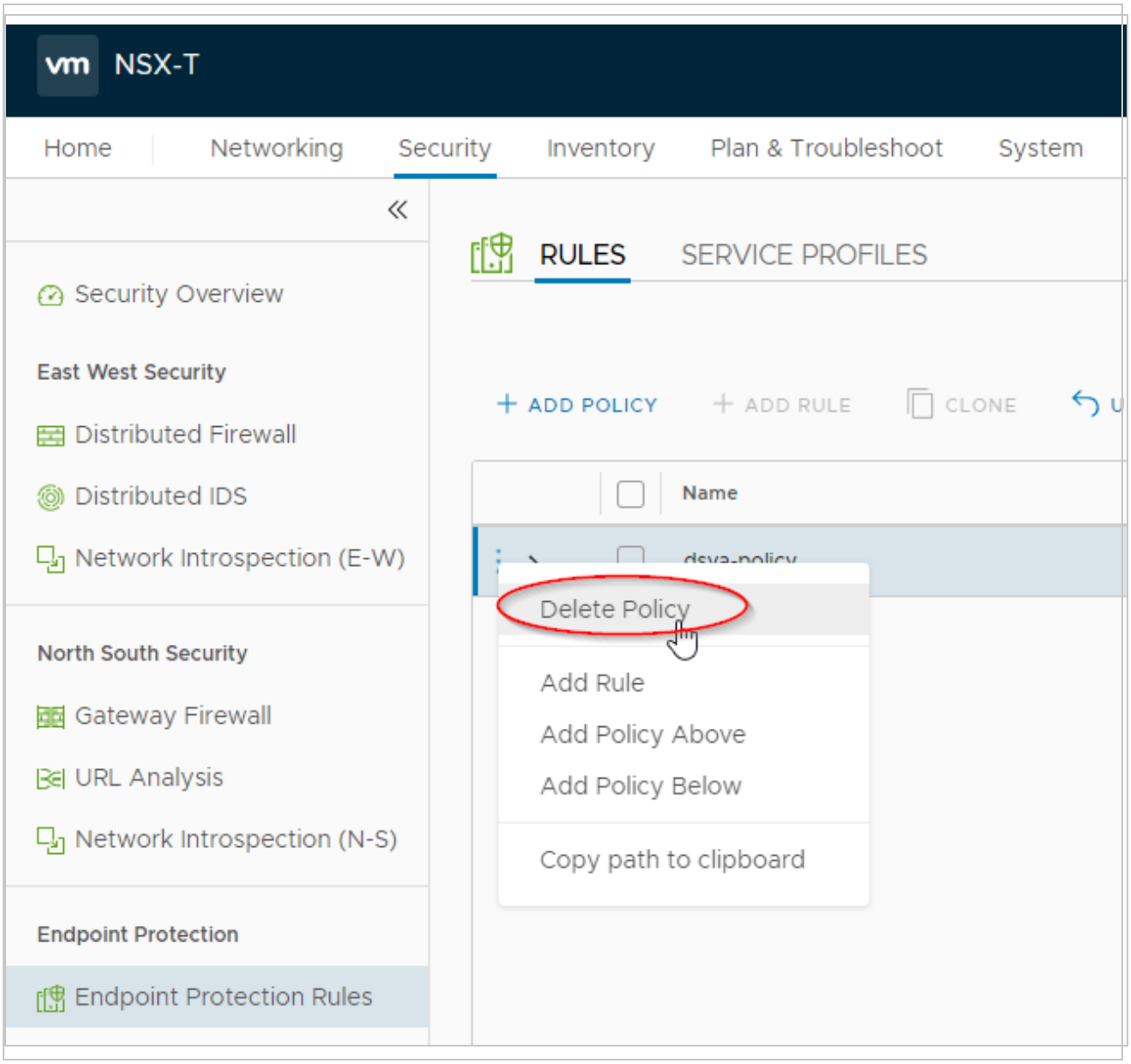
1. NSX-T Managerで、[System]→[Service Deployments]→[DEPLOYMENT] の順に進みます。
2. [Partner Service] ドロップダウンリストから、[Trend Micro Deep Security] を選択します。表示されていなかった場合、サービスのインストールが表示されます。



3. サービスのインストール名の横にある3つのドットをクリックして、[Delete] を選択します。

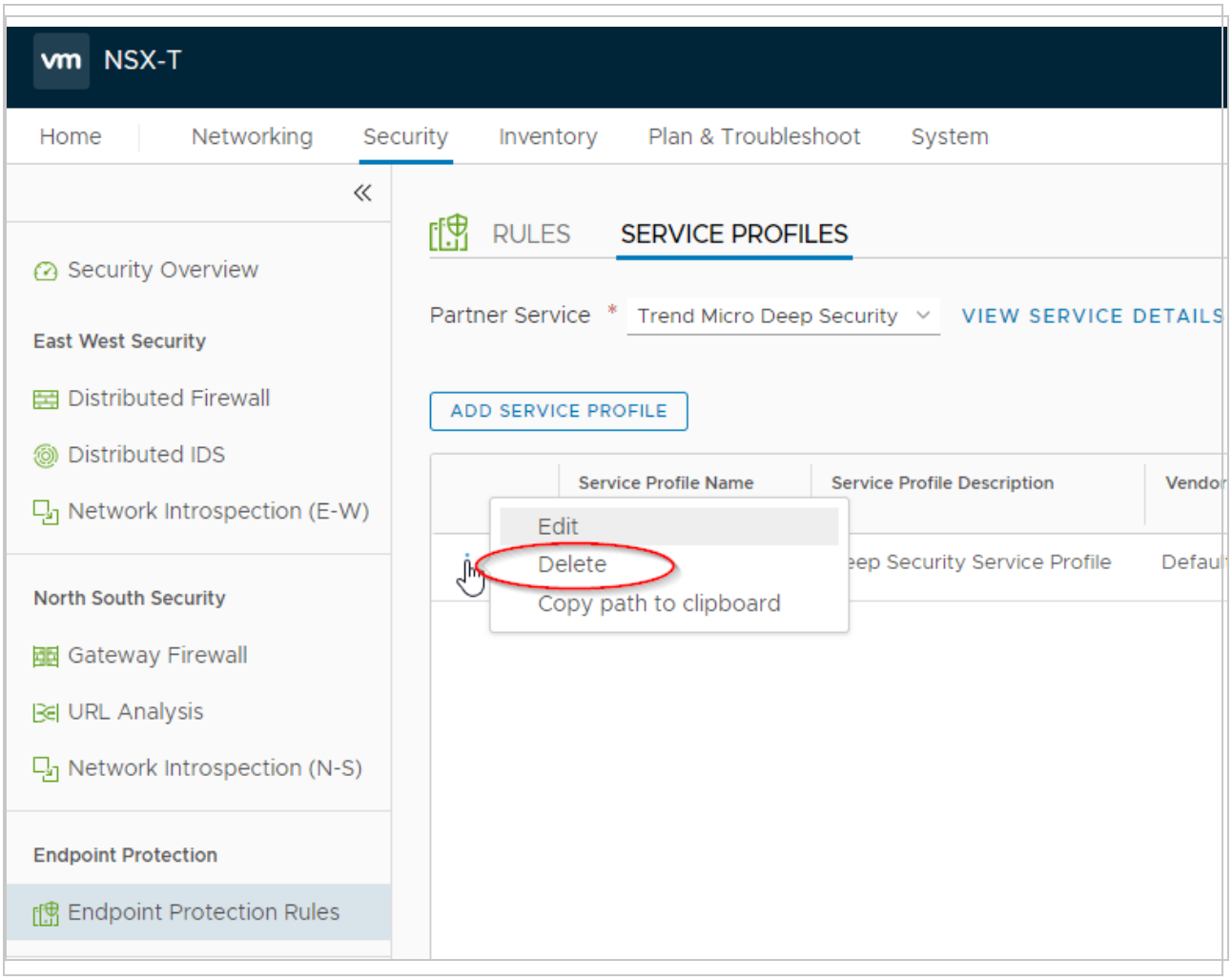
次に、[Endpoint Protection]でDeep Security Virtual Applianceのポリシーとサービスプロファイルを削除します。

1. [セキュリティ>エンドポイント保護>のルール]をクリックします。



2. Deep Security Virtual Appliance ポリシーの横にある3つの点をクリックし、[ポリシーの削除]をクリックします。
3. 変更を反映するには、[Publish] をクリックします。ポリシーと関連するルールが削除されます。

4. システム> エンドポイント保護> をクリックします。サービス160;プロフィール。

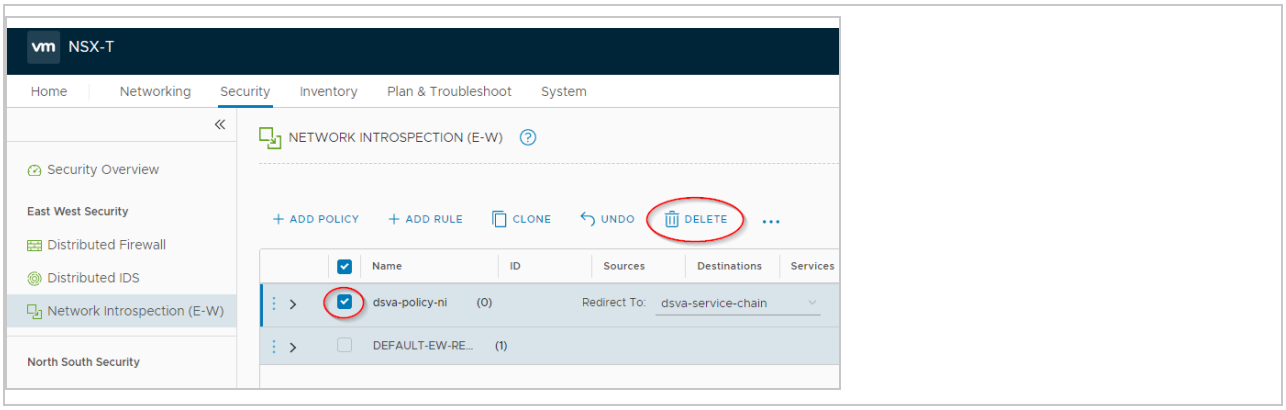


5. サービスプロファイルの横にある3つのドットをクリックして、[Delete] を選択します。

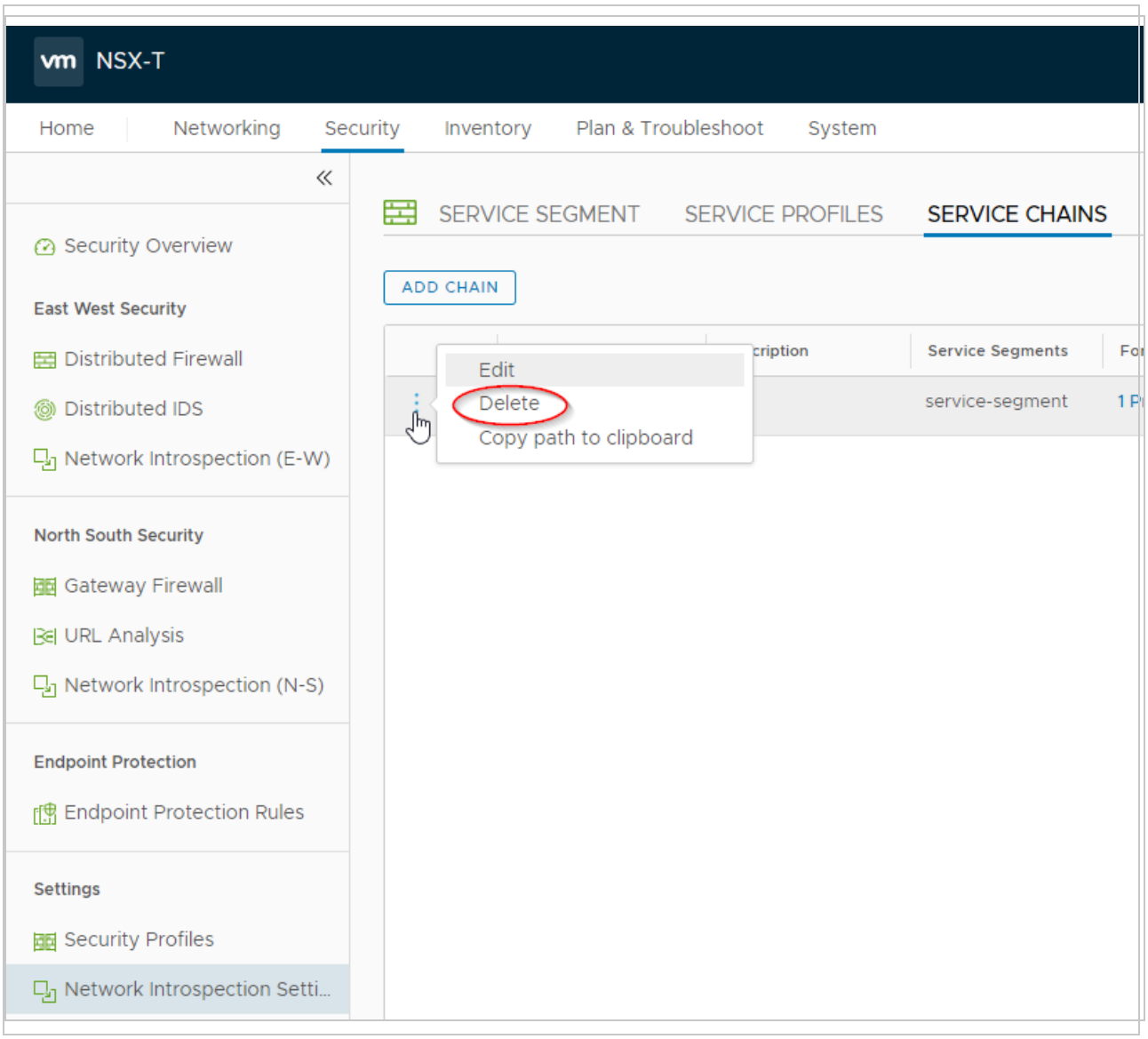
(NSX-T 3.xにのみ適用) 次に、[Network Introspection]の下でDeep Security Virtual Applianceのアーティファクトを削除します。

1. NSX-T Manager 3.xでセキュリティをクリックし、POLICYに切り替え、左側でネットワークイントロスペクション(EW) を参照してください。

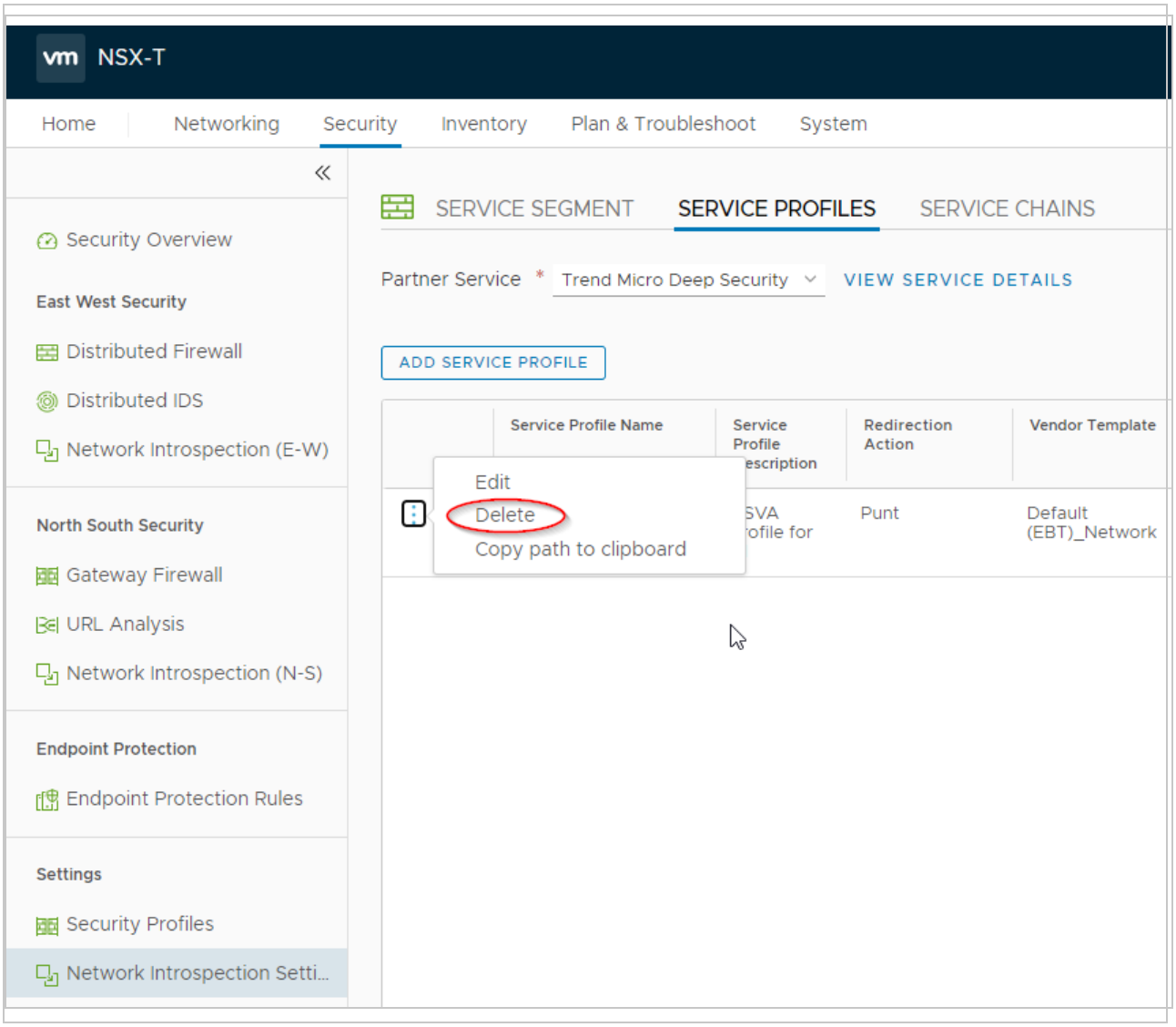
2. Deep Security Virtual Applianceポリシーを選択し、[削除]をクリックします。



3. 変更を有効にするには、[PUBLISH]をクリックしてください。
4. 左側の設定で、ネットワークイントロスペクション設定をクリックします。
5. メイン画面で、[サービスチェーン]をクリックします。
6. Deep Security Virtual Applianceサービスチェーンの横にある3つの点をクリックし、[削除]をクリックします。


NSX-T
Home
Networking
Security
Inventory
Plan & Troubleshoot
System
Security Overview
East West Security
Distributed Firewall
Distributed IDS
Network Introspection (E-W)
North South Security
Gateway Firewall
URL Analysis
Network Introspection (N-S)
Endpoint Protection
Endpoint Protection Rules
Settings
Security Profiles
Network Introspection Setti...
SERVICE SEGMENT
SERVICE PROFILES
SERVICE CHAINS
ADD CHAIN
Service Segments
service-segment
Edit
Delete
Copy path to clipboard

7. メイン画面で、[SERVICE PROFILES] をクリックします。



8. Deep Security Virtual Applianceのサービスプロファイルの横にある3つのドットをクリックし、[削除] を選択します。

   これで、[ネットワークイントロスペクション]でDeep Security Virtual Applianceポリシー、サービスチェーン、およびサービスプロファイルが削除されました。

最後に、Deep Security ManagerからvCenterを削除します。

1. Deep Security Managerで、[コンピュータ] をクリックします。
2. 左側でvCenterを右クリックして [VMware vCenterの削除] をクリックします。

   ウィザードが表示されます。このウィザードのオプションの説明については、"Deep Securityを自動的にアンインストールします" on page 1732を参照してください。

これで、NSX-T環境からDeep Securityを手動で削除することができました。

NSX-V環境からのDeep Securityの手動アンインストール

このセクションが該当するのは、NSX-V環境のみです。NSX-T環境の手順については、"NSX-T 3.xからのDeep Securityの手動アンインストール" on page 1733を参照してください。

"Deep Securityを自動的にアンインストールします" on page 1732の手順に従ってvCenterをDeep Security Managerから削除する際に「VMwareからDeep Securityを削除できません」というエラーが表示された場合は、Deep Security ManagerとNSX Managerの接続が切断されている可能性があります。このエラーが発生した場合は、NSX ManagerからDeep Securityを手動で削除する必要があります。

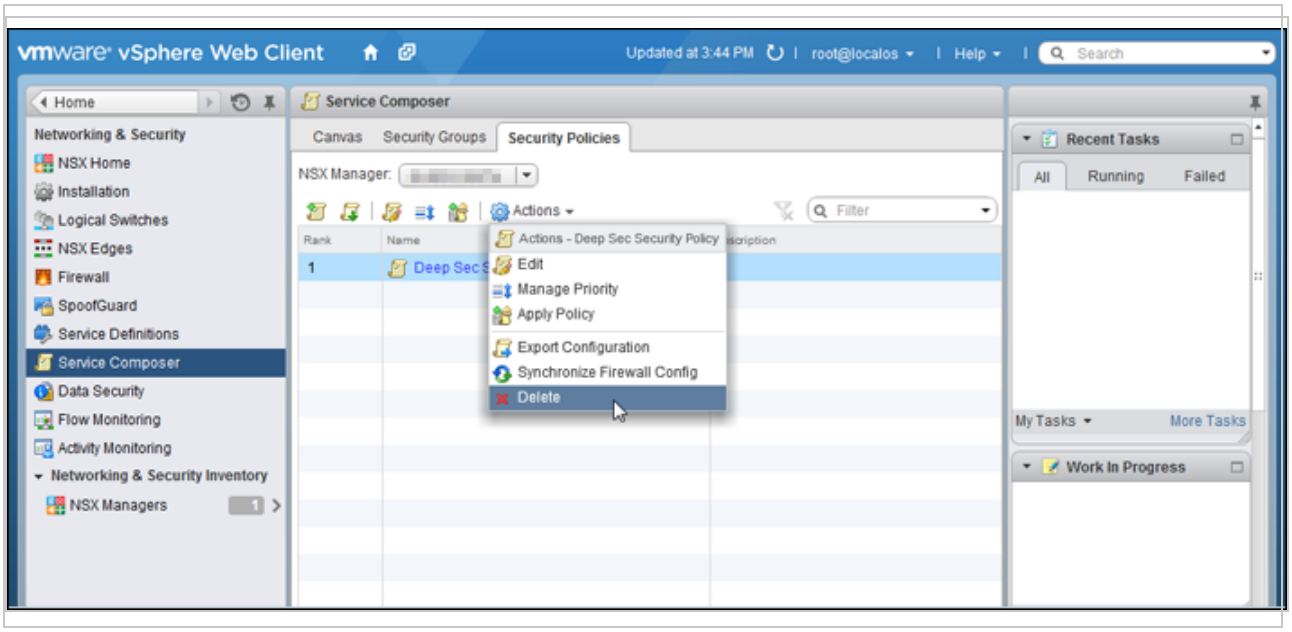
最初に、Deep Security ManagerからNSX Managerを削除します

1. Deep Security Managerで、[コンピュータ] に進みます。
2. 左側のナビゲーションツリーでvCenterを右クリックして、[プロパティ] を選択します。
3. [NSX Manager] タブで、[NSX Managerの削除] をクリックします。
4. [OK] をクリックします。

次に、NSX Managerでトレンドマイクロのサービスを削除します

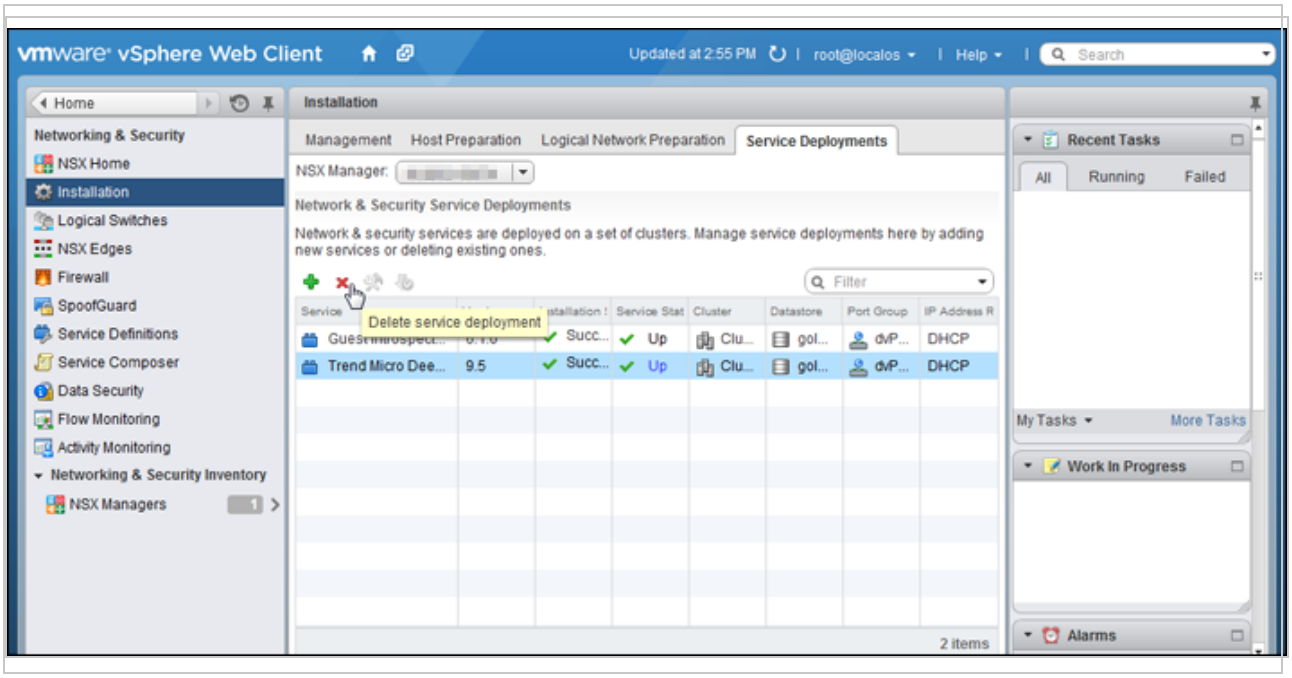
1. vSphere Web Clientで、[Home]→[Networking and Security]→[Service Composer]→[Security Policies] の順に移動します。

   [Deep Security] セキュリティポリシーを削除します。



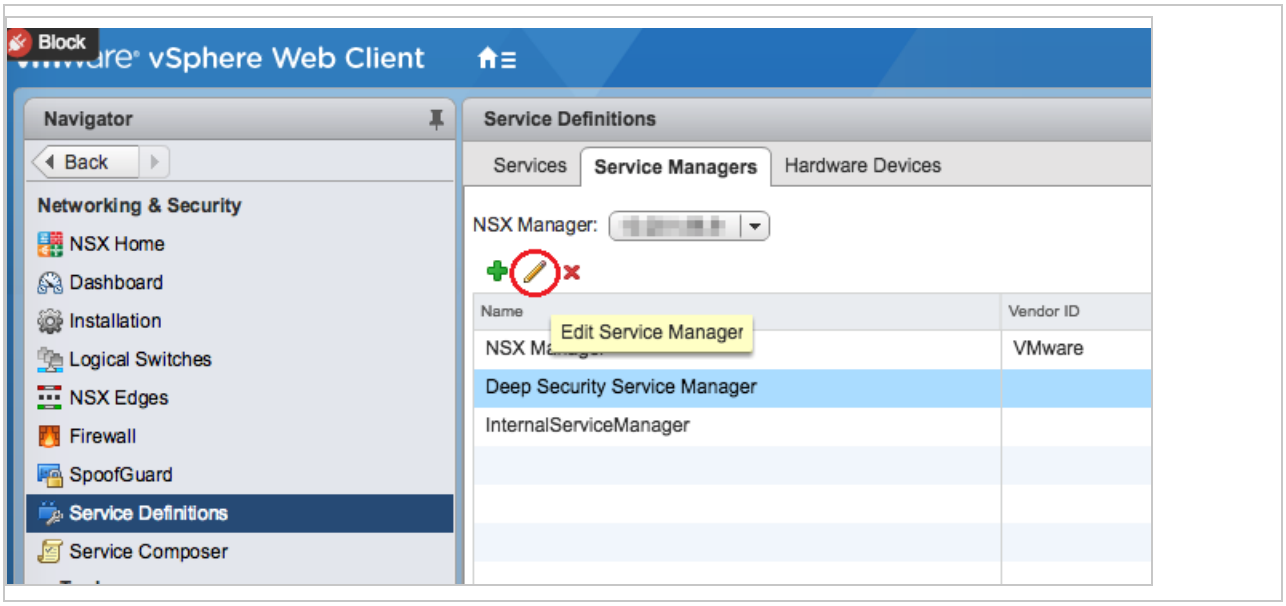
2. [Home]→[Networking and Security]→[Installation]→[Service Deployments] の順に移動します。

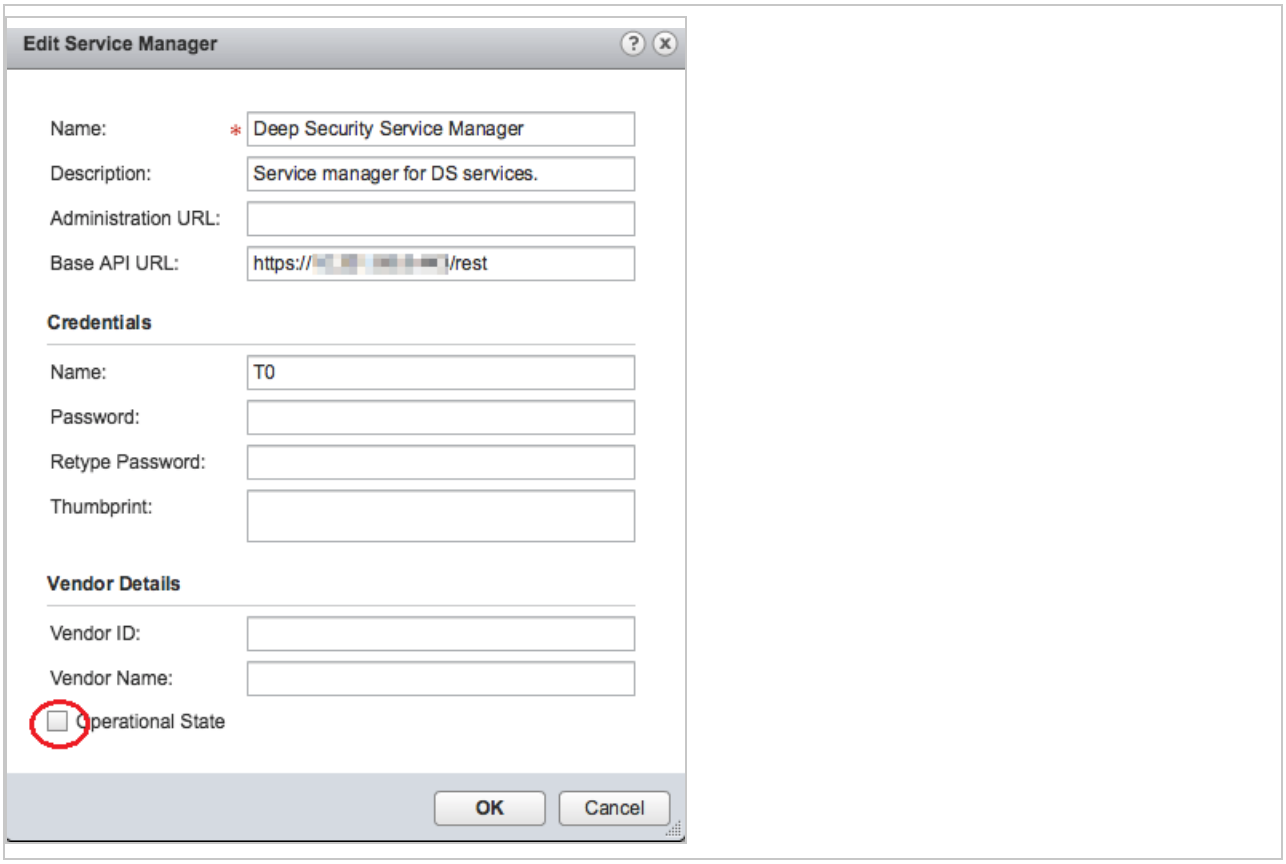
   Trend Micro Deep Security サービスの配信を削除します。



3. [Home]→[Networking and Security]→[Service Definitions]→[Service Managers] の順に移動します。

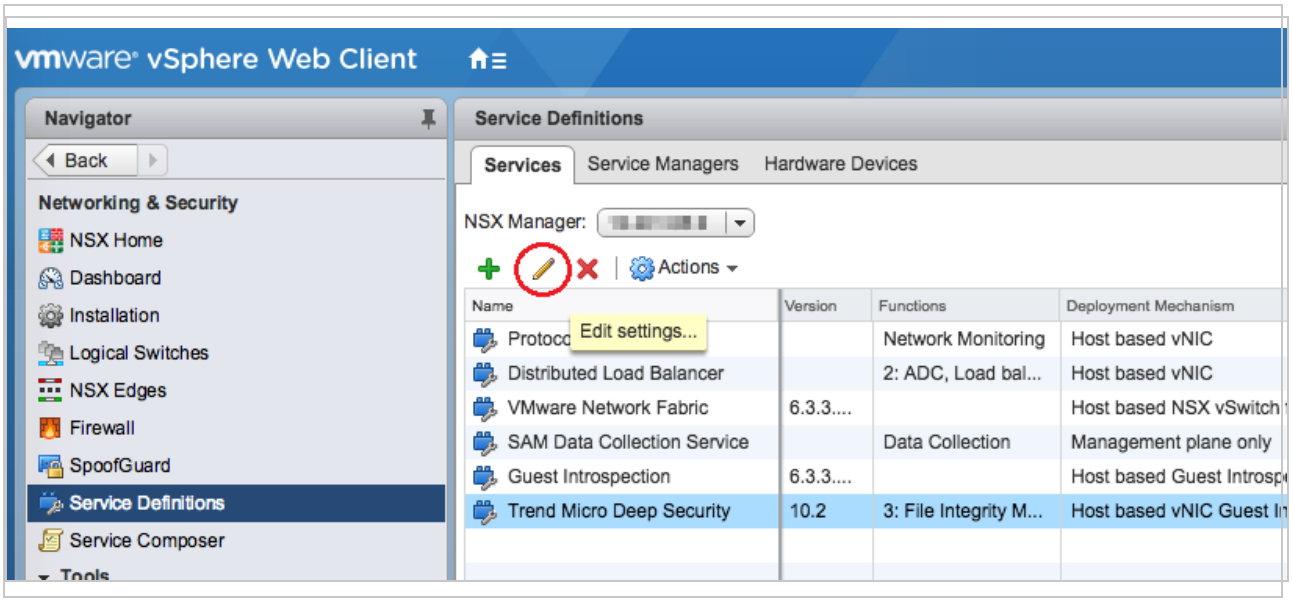
[Deep Security Service Manager] を選択し、鉛筆アイコンをクリックします。[Operational State] を選択解除します。





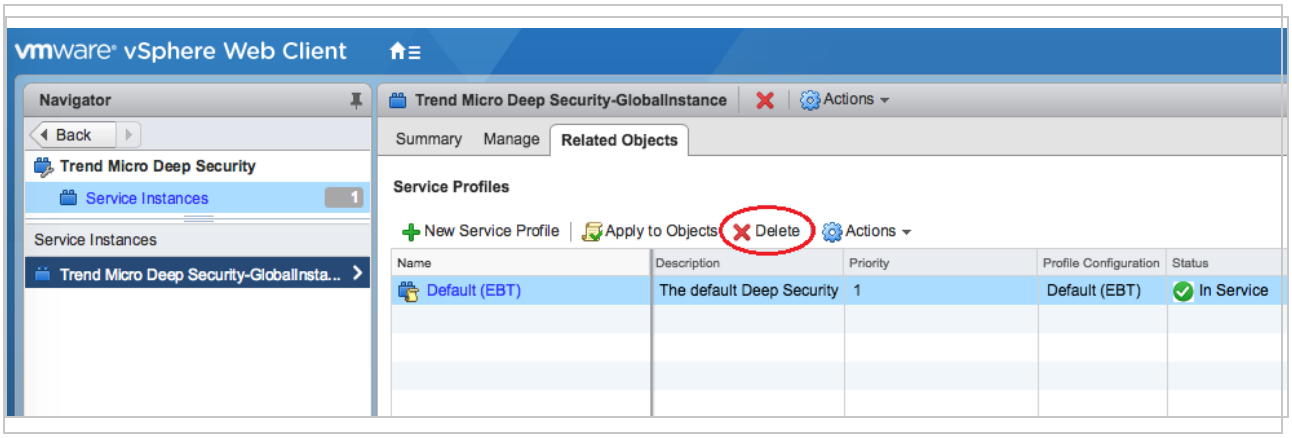
4. [Home]→[Networking and Security]→[Service Definitions]→[Services] の順に移動します。

[Trend Micro Deep Security] をクリックし、鉛筆アイコンをクリックします。



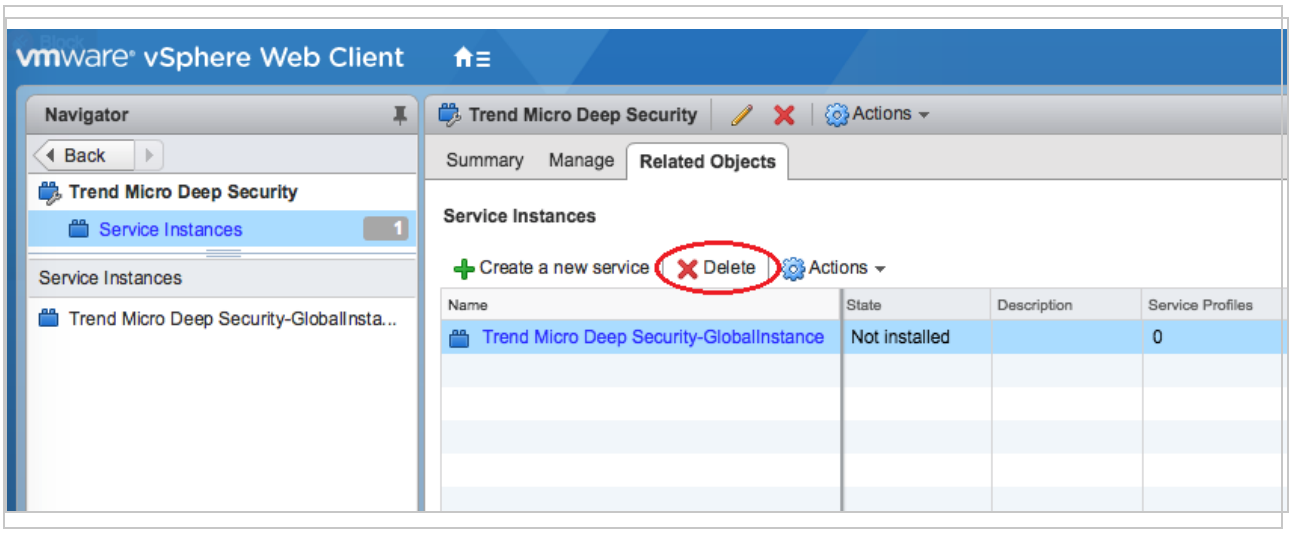
5. 左側のナビゲーション画面で、[Service Instances] をクリックし、左側の [Trend Micro Deep Security-GlobalInstance] をクリックします。

   メイン画面で、[Default (EBT)] を選択し、[Delete] をクリックしてサービスプロファイルを削除します。

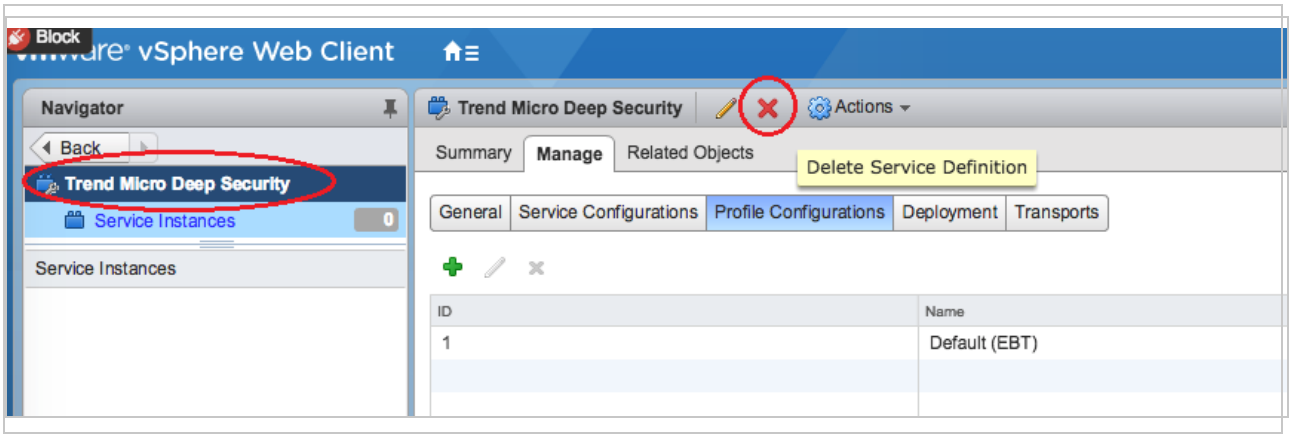


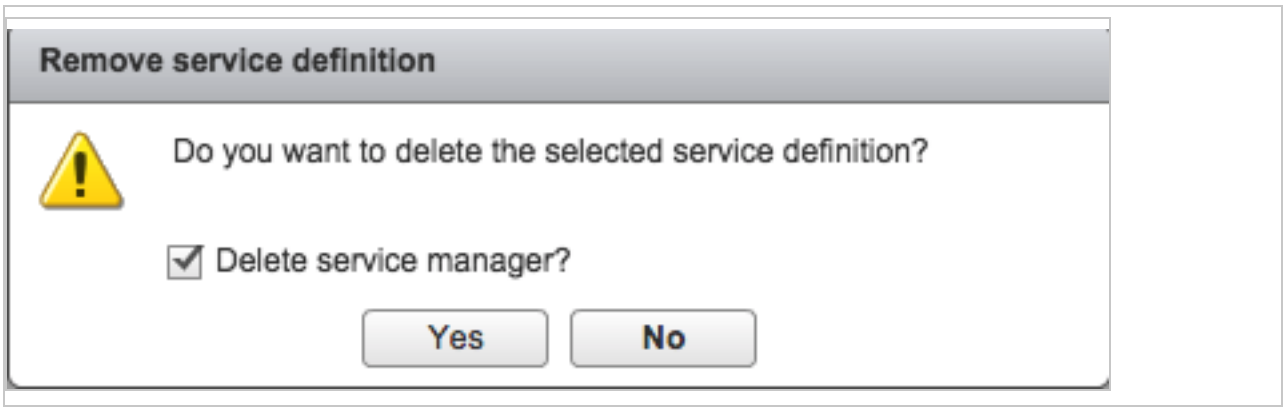
6. 左側のナビゲーション画面で、[Service Instances] をクリックします。

   メイン画面で、[Trend Micro Deep Security-GlobalInstance] を選択し、[Delete] をクリックしてサービスインスタンスを削除します。



7. Trend Micro Deep Security のサービス定義を選択し、最上部の削除アイコンをクリックして削除します。





最後に、Deep Security ManagerからvCenterを削除します。

1. Deep Security Managerで、[コンピュータ] をクリックします。
2. 左側でvCenterを右クリックして [VMware vCenterの削除] をクリックします。

   ウィザードが表示されます。このウィザードのオプションの説明については、"Deep Securityを自動的にアンインストールします" on page 1732を参照してください。

これで、NSX-V環境からDeep Securityを手動で削除することができました。

Deep Security Managerのメモリ使用量を設定する

インストーラーの最大メモリ使用量を設定する

インストーラーはデフォルトで1GBの連続メモリを使用するように設定されています。インストーラーが実行に失敗した場合は、より多くのメモリを使用するようにインストーラーを設定できます。

1. インストーラのあるディレクトリに移動します。
2. インストールプロパティファイルを準備します。例えば、ファイルにinstall.propという名前を付けて、サイレントインストールに使用できます (サンプルプロパティファイルを参照)。
   サイレントインストールを実行する際、インストーラーコマンドに-J-Xmx2gパラメーターを追加して2GBのメモリを確保します。例えば、Manager-Linux-*Version*.x64.sh -q -console -varfile *PropertiesFile* -J-Xmx2g
   異なるメモリ量を確保するには、追加されたパラメーターの値を調整します。例えば、-J-Xmx1024mまたは-J-Xmx4g。

Deep Security Managerの最大メモリ使用量を設定する

Deep Security ManagerのマネージャJVMプロセスに割り当てられるメモリのデフォルト設定は4GBです。この設定を変更することが可能です。

1. Deep Security Managerのインストールディレクトリに移動します。これはDeep Security Managerの実行可能ファイルと同じディレクトリです。
2. 新しいファイルを作成します。プラットフォームに応じて、次のように名前を付けます。
   - Windows: Deep Security Manager.vmoptions
   - Linux: dsm_s.vmoptions
3. 次のような行を追加してファイルを編集してください:
   -Xmx10g
   この例では、10gはDeep Security Managerに10GBのメモリを利用可能にします。

4. ファイルを保存してDeep Security Managerを再起動してください。
5. 新しい設定を確認するには、管理 > システム情報に移動し、システム詳細エリアでマネージャノード> メモリを展開します。最大メモリの値が新しい設定を示しているはずです。

注意:
Deep Security Managerバージョン20.0.313 (20 LTS Update 2021-01-18) 以降をインストールする際、インストーラーが16GB以上のRAMが利用可能であると検出した場合、マネージャJVMプロセスに割り当てられるデフォルトのメモリ量は8GBです。

Deep Security Managerの再起動

Linux

Deep Security Managerを再起動するには、CLIを開いて次のコマンドを実行します。

```
sudo systemctl restart dsm_s
```

Windows

Deep Security Managerを再起動するには、まずDeep Security Managerが実行されているWindowsインスタンスにログインし、"Windowsデスクトップ" below、"コマンドプロンプト" below または "PowerShell" on the next pageの次の手順に従ってください。

Windowsデスクトップ

1. Windowsタスクマネージャーを開きます。
2. [サービス] タブをクリックします。
3. [Trend Micro Deep Security Manager] サービスを右クリックし、[再起動] をクリックします。

コマンドプロンプト

コマンドプロンプト(cmd.exe) を開いて、次のコマンドを実行します。

1. `net stop "Trend Micro Deep Security Manager"`
2. `net start "Trend Micro Deep Security Manager"`

PowerShell

PowerShellを開き、次のコマンドを実行します。

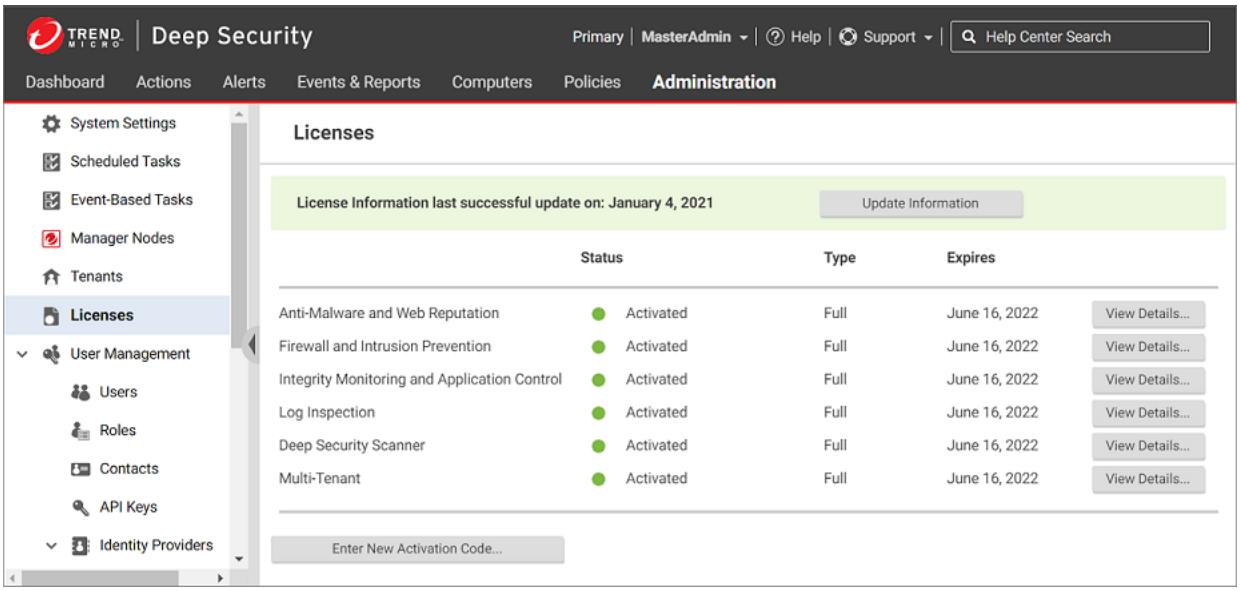
1. `Stop-Service 'Trend Micro Deep Security Manager'`
2. `Start-Service 'Trend Micro Deep Security Manager'`

ライセンス情報の確認

注意: この情報は、上位テナントからライセンスを継承するマルチテナント構成には適用されません。

現在のライセンスを確認する

Trend Micro Deep Security製品ライセンスに関する情報を表示するには、Deep Security Managerコンソールで、[管理]→[Licenses]の順に選択します。



Deep Securityは、6個のモジュールパッケージで構成されています。

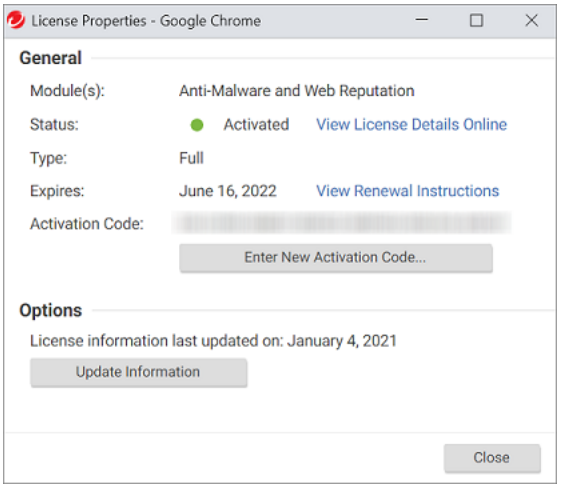
- 不正プログラム対策とWebレピュテーション
- ファイアウォールと侵入防御
- 変更監視とアプリケーションコントロール
- セキュリティログ監視

- Deep Security Scanner
- マルチテナント

モジュールパッケージごとに製品版または体験版のライセンスが必要です。

ライセンスの詳細を表示

[ライセンス]画面で、個々のパッケージのライセンスの横にある[詳細の表示][ ]の順にクリックして、追加情報を表示します。



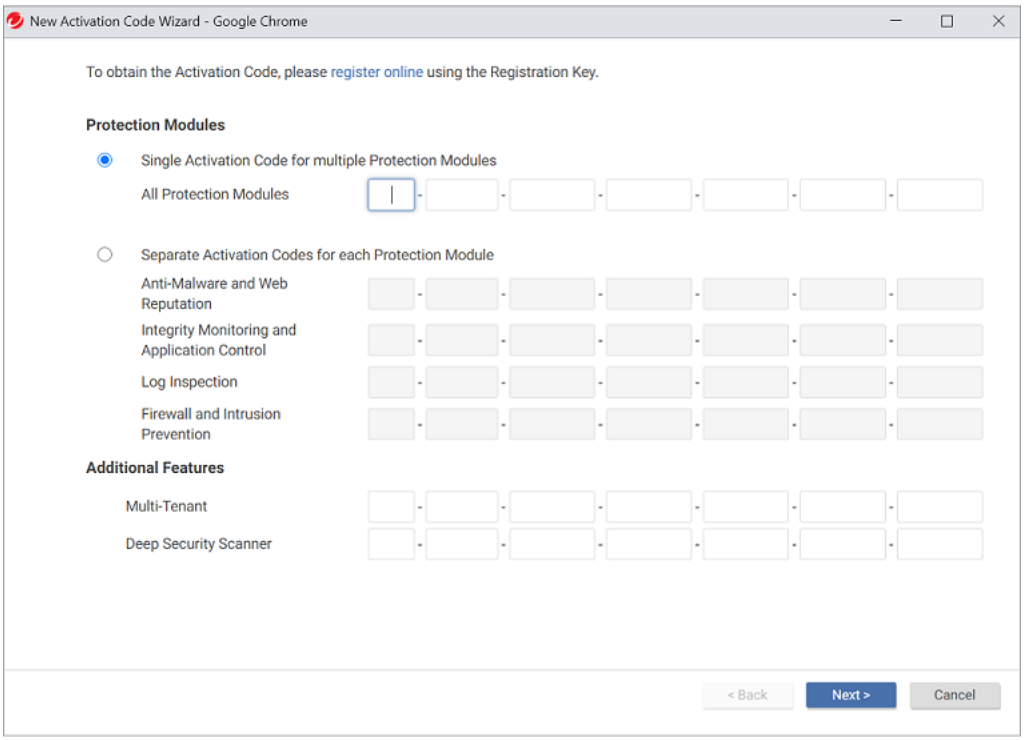
ライセンスに含まれているライセンス数などの詳細情報が必要な場合は、[ライセンス情報の表示 オンライン]をクリックして、Trend Micro Customer Licensing Portalにアクセスしてください。Viewの更新手順 リンクは、Customer Licensing Portalにも移動します。

期限切れが近い、または期限切れになったモジュールがある場合は、ユーザに通知されます。ライセンスの有効期限が切れると、既存の機能は継続されますが、アップデートは配信されなくなります。

ライセンスの追加またはアップグレード

ライセンスを追加またはバージョンアップするには、トレンドマイクロに問い合わせてください。

トレンドマイクロから新しいアクティベーションコードが提供されている場合は、[新しいアクティベーションコードの入力]をクリックし、表示されたウィンドウに入力します。



新たにライセンスされた機能がすぐに利用可能

注意: Trend Micro Deep Securityライセンス種類および価格については、次のサイトをご覧ください。https://www.trendmicro.com/ja_jp/business/products/hybrid-cloud/deep-security-data-center.html?modal=pdf02-c2aa2b

Deep Security を Trend Vision One Endpoint Security - Server & Workload Protection にアップグレード

Trend Vision One Endpoint Security - Server & Workload Protectionにアップグレード

Deep Security 管理者は、Trend Vision One Endpoint Security - Server & Workload Protection へのアップグレードを準備する際に、この記事の指示をロードマップとして使用できます。

お使いの環境は、Deep Security Manager 20.0.513 (20 LTS Update 2021-10-14) 以降である必要があります。

一般的に、成功するアップグレードの操作順序は次のとおりです:

1. "Trend Vision One Endpoint Security - Server & Workload Protectionを構成する" below
2. "APIキーを作成" below
3. Trend Vision One Endpoint Security - Server & Workload Protectionのリージョンを見つける
4. "Trend Vision One Endpoint Security - Server & Workload Protectionへのリンクを準備する" on the next page
5. ポリシーの移行
6. 共通オブジェクトの移行
7. クラウドアカウントを移行する
8. エージェントの移行
9. "その他のDeep Security設定の移行" on page 1752
10. "ネットワークと通信の設定" on page 1754

Trend Vision One Endpoint Security - Server & Workload Protectionを構成する

Trend Vision Oneアカウントを持っていることに加えて、次の操作を行う必要があります:

- Trend Vision One を Foundation Services リリースに更新
- 新しいTrend Vision One Endpoint Security - Server & Workload Protectionインスタンスをプロビジョニングする

APIキーを作成

APIキーを作成するには、次の手順に従ってください:

1. Trend Vision Oneにログインする。
2. エンドポイントセキュリティオペレーション > サーバー & ワークロード保護 に移動します。
3. 管理 > ユーザ管理 > API Keys に移動し、Deep Security Migration の役割を持つ新しい API キーを作成します。
   Deep Security Migration の役割は事前に設定されており、Trend Vision One Endpoint Security - Server & Workload Protection によって管理されており、エージェントとポリシーの移行を実行する権限があります。追加の移行機能が実装されると、関連する権限が将来変更される可能性があることに注意してください。
4. キーを後で使用するために保存してください。

Trend Vision One Endpoint Security - Server & Workload Protectionの地域を決定する

地域を特定するには、次のようにデプロイメントスクリプトでACTIVATIONURLを使用することができます

1. [管理]→[アップデート]→[ソフトウェア]→[ローカル] に進みます。
2. ソフトウェアパッケージを選択し、デプロイメントスクリプトを生成をクリックします。
3. デプロイメントスクリプトダイアログで、ACTIVATIONURLを確認します。以下は、アクティベーションURLとリージョンのマッピングです:

アクティベーションURL	REGION
dsm://agents.workload.jp-1.cloudone.trendmicro.com:443	JP-1
dsm://agents.workload.in-1.cloudone.trendmicro.com:443	IN-1
dsm://agents.workload.gb-1.cloudone.trendmicro.com:443	GB-1
dsm://agents.workload.ca-1.cloudone.trendmicro.com:443	CA-1
dsm://agents.workload.sg-1.cloudone.trendmicro.com:443	SG-1
dsm://agents.workload.au-1.cloudone.trendmicro.com:443	AU-1
dsm://agents.workload.de-1.cloudone.trendmicro.com:443	DE-1
dsm://agents.deepsecurity.trendmicro.com:443	US-1

Trend Vision One Endpoint Security - Server & Workload Protectionへのリンクを準備する

ユーザがTrend Vision One Endpoint Security - Server & Workload Protection Linkを管理するには、Trend Vision One Endpoint Securityの管理を許可するロール権限を割り当てる必要があります。

1. Deep Security Manager コンソールで、サポート> Trend Vision One エンドポイントセキュリティにアップグレードを選択します。
2. Link to Trend Vision One Endpoint Security Account ダイアログを完了してください:
   a. 前のセクションで作成したAPIキーを入力します。
   b. Trend Vision One Endpoint Security - Server & Workload Protection アカウントが所在するリージョンを選択してください。
   c. [Save] をクリックします。

   警告: 以前にDeep SecurityとTrend Vision One Endpoint Security - Server & Workload Protectionの間に接続を設定し、リンクを変更したい場合は、リンクを変更する前に、以前の接続を使用したすべての移行関連タスクが完了していることを確認してください。そうしないと、予期しない動作が発生する可能性があります。

   各Deep Security Managerテナントは、1つのTrend Vision One Endpoint Security - Server & Workload Protectionリンクのみを許可します。

Trend Vision One Endpoint Security - Server & Workload Protectionリンクの作成中に、Deep Security ManagerはTrend Vision One Endpoint Security - Server & Workload Protectionに接続してリンクを認証し、情報を取得します。Deep Security Managerのインストールがあり、Trend Vision One Endpoint Security - Server & Workload Protectionに接続するためにプロキシを必要とする場合は、Trend Vision One Endpoint Security - Server & Workload Protectionのプロキシを構成します。

Trend Vision One Endpoint Security へのアップグレードダイアログが開き、設定の移行 タブが選択されています。

ユーザがすべての移行タスクを処理できるようにするには、Trend Vision One Endpoint Security への移行を許可する役割の権限を割り当てる必要があります。

次に、ポリシーをTrend Vision One Endpoint Security - Server & Workload Protectionに移行します。

その他のDeep Security設定の移行

次のアーティファクトをDeep Security環境で使用している場合は、移行してください:

- "VMwareコネクタとデータセンターゲートウェイ" below
- "コンピュータグループとスマートフォルダ" below
- "プロキシ設定" on the next page
- "イベントとアラートのログ" on the next page
- "追加設定" on the next page

VMwareコネクタとデータセンターゲートウェイ

VMware 環境で実行されている仮想マシンには、他のワークロードと同様に Trend Vision One Endpoint Security - Server & Workload Protection サービスにエージェントを展開してアクティブ化することができます。VM インベントリを取得するために VMware vCenter に接続したい場合、Trend Vision One Endpoint Security - Server & Workload Protection は vCenter と通信する必要があります。これはデータセンターゲートウェイを通じて行われます。データの設定とvCenter インベントリのインポートに関する手順については、Trend Vision One Endpoint Security - Server & Workload Protection に VMware vCenter を追加する を参照してください。

コンピュータグループとスマートフォルダ

コンピュータグループとスマートフォルダには、まだ直接の移行方法がありません。Deep Security と Trend Vision One Endpoint Security - Server & Workload Protection にはコンピュータグループをリス

トおよび作成するための API があるため、大量のグループの移行は適切な API コールをスクリプト化することで自動化できます。

プロキシ設定

現在、Deep Security からTrend Vision One Endpoint Security - Server & Workload Protection へのプロキシ設定を自動的に移行する方法はありません。プロキシの設定の指示に従って、Trend Vision One Endpoint Security - Server & Workload Protection でエージェント通信のプロキシ設定を手動で構成できます。

マネージャーのプロキシを設定する必要はありません。これはTrend Vision One Endpoint Security - Server & Workload Protectionサービスの一部であり、トレンドマイクロによって管理されています。

イベントとアラートのログ

Deep Security とTrend Vision One Endpoint Security - Server & Workload Protection の主な違いは、マネージャ内のイベントおよびアラートデータの保持です。Trend Vision One Endpoint Security - Server & Workload Protection は、セキュリティイベントを4週間、システムイベントを13週間保持します。イベントをより長く保持する必要がある場合は、トレンドマイクロはイベントを SIEM またはログサーバーにエクスポートすることを推奨します。

イベントログが既に使用されている場合、アラートやイベントの受信方法のインフラストラクチャにいくつかの変更が必要になるかもしれません。Deep Security Managerがすべてのアラートとイベントをsyslogを介してローカルのsyslogサーバーに送信する従来のオンプレミス展開では、そのsyslogサーバーはTrend Vision One Endpoint Security - Server & Workload Protectionから直接アクセスできない可能性があります。次の代替案を検討してください:

- Trend Vision One Endpoint Security - Server & Workload Protection サービスからアクセス可能な新しい syslog サーバーを作成するには、Trend Vision One Endpoint Security - Server & Workload Protection イベントを Syslog または SIEM サーバーに転送するに記載されている手順に従ってください。
- エージェントを構成して、マネージャーを介さずにローカルのsyslogサーバーに直接イベントを送信するようにします。syslogでTLS暗号化を使用するには、イベントをTrend Vision One Endpoint Security - Server & Workload Protectionサービスから転送する必要があることに注意してください。エージェントは現在、syslogイベントのTLS暗号化をサポートしていません。
- syslogの代わりにAmazon SNSを使用します。「Amazon SNSを設定する

追加設定

他の項目の設定(システム設定、レポート、イベントベースおよびスケジュールされたタスク、タグ、バージョン管理、API Keysなど) は、現在、自動化された移行機能の一部ではありません。これらはTrend

Vision One Endpoint Security - Server & Workload Protectionで手動で再作成できます。これらの項目の多くは、Deep SecurityおよびTrend Vision One Endpoint Security - Server & Workload ProtectionのAPIで設定可能であり、自動化することができます。

Deep Security を Trend Vision One Endpoint Security - Server & Workload Protection にアップグレードする際、一部のシステム設定がサポートされない、または適用されない場合があります。これらの設定を API コールを通じて自動化する際には注意が必要です。これらの設定に関するガイダンスについては、トレンドマイクロ サポートにお問い合わせください。

ネットワークと通信の設定

以下のアーティファクトを評価してください:

- "必要なポート、プロトコル、およびURL" below
- "プロキシ設定" below
- "検索されたサイズ使用率" below
- "Relay の設定" on the next page

必要なポート、プロトコル、およびURL

Deep Security Agent とTrend Vision One Endpoint Security - Server & Workload Protection 間のネットワーク通信は、エージェントとDeep Security Manager 間の通信とは異なります。アウトバウンドインターネットアクセスが制限されている環境では、特定の URL を許可する必要があります。完全なリストについては、ポート番号、URL、および IP アドレスを参照してください。

プロキシ設定

エージェント通信のためのプロキシの設定に関する情報については、Trend Vision One Endpoint Security - Server & Workload Protection サービスのプロキシの設定 を参照してください。

SOCKS4およびSOCKS5プロキシはエージェント通信に対応していません。エージェント通信にプロキシを使用する必要がある場合は、エージェントがTrend Vision One Endpoint Security - Server & Workload Protectionサービスにアクティベートされる前にHTTPプロキシを実装してください。

検索されたサイズ使用率

Deep Security Agentの配置に関するネットワーク計画を検討する際は、エージェントのダウンロードと有効化、および継続的な操作とセキュリティパターンのアップデートの両方について、エージェントの全体的なライフサイクルを考慮してください。

既存のDeep Securityエージェントを再インストールする必要はなく、Trend Vision One Endpoint Security - Server & Workload Protectionサービスに再アクティブ化するだけで済みます。アクティベーションスクリプトを使用して行われる新しいデプロイメントでは、次の帯域幅使用量が予想されます:

- エージェントのダウンロードとアクティベーション: Linuxで5 MB; Windowsで25 MB
- 初回セキュリティ更新のダウンロード: 50 MB Linux; 102 MB Windows

継続的なエージェントトラフィックは、検出アクティビティ、ポリシー設定、およびモジュールの使用状況によって大きく異なります。次のガイドラインに類似した、管理トラフィックのベースラインの使用を想定します。

- セキュリティアップデート(毎日1回、スマートスキャンオン) : 60MB
- セキュリティアップデート(1日1回、スマートスキャンオフ) : 120MB
- ハートビートのオーバーヘッド: 1回のハートビートにつき40 KB。デフォルトの間隔は10分; エージェント1台あたり1日約5.7 MB

詳細については、Trend Vision One Endpoint Security - Server & Workload ProtectionのSmart Protectionを参照してください。

ベースラインのトラフィックを超えて、エージェントがTrend Vision One Endpoint Security - Server & Workload ProtectionおよびVision Oneサービスと通信するため、検出が発生すると追加の帯域幅消費が発生します。これは予測が難しいですが、検出が少ない場合はエージェントごとに1時間あたり0.1 MB、検出率が高い場合はエージェントごとに1時間あたり最大3 MBの使用量を見込んでください。

Relayの設定

ほとんどの場合、Trend Vision One Endpoint Security - Server & Workload Protectionサービスによって提供されるRelayは十分です。いくつかのシナリオでは、Relayを使用することで操作が改善される場合があります。詳細については、Relayの動作および追加のRelayの展開を参照してください。

Deep SecurityおよびTrend Vision One Endpoint Security - Server & Workload Protection APIを使用してアップグレード

Deep Security ManagerとTrend Vision One Endpoint Security - Server & Workload Protection UIを使用してアップグレードを実行できます

- 一般的な要件とヒントについては、さらにお読みください。
- "APIキーを作成" on page 1750し、APIドキュメントを使用してTrend Vision One Endpoint Security - サーバ&Workload Protectionリンクを作成します。
- Deep Security APIドキュメントを参照して、以下の情報を確認してください
  - ポリシーの移行
  - エージェントの移行
  - 共通オブジェクトの移行
  - AWSコネクタの移行
- HTTP GET 呼び出しを使用して、/policymigrationtasks/{taskID} からステータスを取得し、ポリシー移行ステータスを確認します。詳細については、Automation Center を参照してください。

現在、製品内の移行機能でサポートされていないアーティファクトは、一般的に Deep Security と Trend Vision One Endpoint Security - Server & Workload Protection API を組み合わせて、Deep Security デプロイメントから関連する設定やオブジェクトを読み取り、Trend Vision One Endpoint Security - Server & Workload Protection アカウントに書き込むことで移行できます。

一部のアーティファクトは現在のAPIでは利用できませんが、レガシーRESTおよびSOAP APIを介してアクセス可能です。また、一部の機能はDeep Securityのみに存在し、移行はサポートされていません。

以下はTrend Vision One Endpoint Security - Server & Workload Protectionでサポートされていません:

- Deep Security マルチテナント設定、/tenants API に従います。Trend Cloud One の複数アカウント管理は従来のオンプレミスのマルチテナントを超えており、これらの設定は Trend Vision One Endpoint Security - Server & Workload Protection には適用されません。
- AgentレスVMware環境の保護

現在のAPIには、以下のレガシーREST APIは含まれていません:

- ステータス監視
- SAML設定
- プロキシの設定、制御、および割り当て
- イベントの取得

現在のAPIに含まれていないSOAP APIは次のとおりです:

- プロキシの設定、制御、および割り当て
- イベントの取得
- アクション(アップデートエージェント、スキャンの実行など)
- ルール設定

クラウドアカウントをTrend Vision One Endpoint Security - Server & Workload Protectionに移行する

"Trend Vision One Endpoint Security - Server & Workload Protectionにアップグレード" on page 1749は、複数のステップを要するプロセスです。

クラウドコネクタを使用してDeep Securityにクラウドアカウントを追加した可能性があります。移行ツールまたは移行APIを使用して、保護対象のクラウドアカウントを移行できます。

前提条件

- Deep Security Manager 20.0.635 (20 LTS Update 2022-04-21) 以降を実行していることを確認してください。
- すでに行っていない場合は、"Trend Vision One Endpoint Security - Server & Workload Protectionにアップグレード" on page 1749で説明されている前の手順を完了し、Trend Vision One Endpoint Security - Server & Workload Protectionアカウントの設定、APIキーの作成、およびTrend Vision One Endpoint Security - Server & Workload Protectionへのリンクの準備を行ってください。

AWSアカウントの移行

登録済みのAWSアカウントを移行する手順は、それらが最初にDeep Security Managerに追加された方法に依存します:

- アクセスキーを使用して追加されたAWSアカウントは、移行ツールまたは移行APIを使用して移行できます。詳細については、レガシーAWS接続の更新を参照してください。
- クロスアカウントロールを使用して追加されたAWSアカウントは、Trend Vision One Endpoint Security - Server & Workload Protectionではサポートされていないため、これらのアカウントを移行することはできません。クラウドアカウントを手動で追加する方法については、クラウドアカウントを参照してください。

- マネージャーインスタンスロールを使用して追加されたAWSアカウントは、Trend Vision One Endpoint Security - Server & Workload Protectionではサポートされていません。これらのアカウントの移行はサポートされていません。
- Deep Security Manager 9.6以前で追加された従来のAWSアカウントは、APIエンドポイント `/api/awsconnectors`経由でアクセスできないため、サポートされません。

移行ツールを使用して他のクラウドアカウントを移行する

1. Deep Security Managerコンソールの右上隅で、サポート> Trend Vision Oneエンドポイントセキュリティにアップグレードを選択します。
2. Trend Vision One Endpoint Securityへのアップグレードダイアログが表示されたら、Cloud Accountsタブを選択して、移行をサポートするすべての接続されたクラウドアカウントを表示します。
3. 移行するアカウントを選択し、[選択したものを移行] をクリックします。
4. 移行が開始されたら、更新 をクリックして移行状況を確認してください。考えられるステータスは次のとおりです:
   - 移行が要求されました: クラウドアカウントのTrend Vision One Endpoint Security - Server & Workload Protectionへの移行が要求されましたが、移行はまだ開始されていません。
   - 移行中: クラウドアカウントはTrend Vision One Endpoint Security - Server & Workload Protectionに移行されており、完全な同期が開始されました。このプロセスは完了するまでに時間がかかる場合があります。
   - 移行済み: クラウドアカウントは正常にTrend Vision One Endpoint Security - Server & Workload Protectionに移行されました。
   - 失敗: クラウドアカウントのTrend Vision One Endpoint Security - Server & Workload Protectionへの移行に失敗しました。エラーコードを確認してください:
     - エラーコード900未満: Trend Vision One Endpoint Security - Server & Workload Protectionからの障害があります。応答の詳細については障害システムイベントを参照するか、サポートに連絡してください。
     - エラーコード900以上: Deep Security Managerは Trend Vision One Endpoint Security - Server & Workload Protection との通信に問題があります。Trend Vision One Endpoint Security - Server & Workload Protection リンクが正しく構成されていることを確認するか、詳細については `server0.log` を確認してください。

VMware vCloudアカウントの移行

現在、VMware vCloud アカウントをTrend Vision One Endpoint Security - Server & Workload Protection に自動的に移行することはできません。ただし、Trend Vision One Endpoint Security - Server & Workload Protection アカウントに新しい VMware vCloud コネクタを作成して保護することができます。トレンドマイクロは、ホストを移行する前にコネクタを設定することを推奨します。

Trend Vision One Endpoint Security - Server & Workload Protection でクラウドコネクタを設定する方法については、VMware vCloud にホストされている仮想マシンを追加する を参照してください。

エージェントをTrend Vision One Endpoint Security - Server & Workload Protectionに移行する

"Trend Vision One Endpoint Security - Server & Workload Protectionにアップグレード" on page 1749は、複数のステップを要するプロセスです。

前提条件

- API経由でアップグレードするには、Deep Security Manager 20.0.321 (20 LTS 2021-01-26)以降を使用していることを確認してください。また、Deep Security Managerアップデートツールを使用してアップグレードするには、Deep Security Manager 20.0.513 (20 LTS Update 2021-10-14)以降を使用してください。
- Deep Security Agent 20.0.0-3445 (20 LTS Update 2021-11-24) 以降を使用していることを確認してください。その後、Trend Vision One Endpoint Security - Server & Workload Protection コンソールで、管理 > アップデート > ソフトウェア > ローカル に移動し、アカウントに対応する Deep Security Agent パッケージがあることを確認してください。
- エージェントが移行をサポートするプラットフォームで実行されていることを確認してください:
  - Deep Security Agent プラットフォームサポートテーブルには、Deep Security Manager 20 によってサポートされているエージェントプラットフォームが一覧表示されています。
  - エージェントの移行は現在、Intelアーキテクチャ上のWindowsおよびLinuxプラットフォームでのみ完全に検証されています。
  - Windows 2008 32ビット版ではエージェントの移行はサポートされていません。
- 機能の違いにより、Deep Security Manager とTrend Vision One Endpoint Security - Server & Workload Protection の間で、エージェントを移行する前に以下を無効にしてください
  - FIPS 140: FIPS 140 が有効になっている場合、Deep Security Manager を更新できません。

  - Virtual Appliance: Virtual Appliance (エージェントレスまたはコンバインドモード) によって保護されているコンピュータは更新できません。

- すでに行っていない場合は、"Trend Vision One Endpoint Security - Server & Workload Protectionにアップグレード" on page 1749で説明されている前の手順を完了し、Trend Vision One Endpoint Security - Server & Workload Protectionアカウントの設定、APIキーの作成、およびTrend Vision One Endpoint Security - Server & Workload Protectionへのリンクの準備を行ってください。

移行ツールを使用してエージェントを移行する

1. Deep Security Manager コンソールの右上隅で、サポート> Trend Vision One エンドポイントセキュリティにアップグレードを選択します。
2. Trend Vision One Endpoint Security へのアップグレードダイアログが表示されたら、エージェントタブを選択します。
3. コンピュータを使用して移行を選択すると、Deep Securityのコンピュータページが表示されます。
4. 移行するコンピュータを1台以上選択します。
5. アクション> Trend Vision One エンドポイントセキュリティにアップグレードを選択します。
6. ダイアログが表示されたら、移動するエージェントに適用したい設定を指定し、移行をクリックします
   - セキュリティポリシー: Deep SecurityポリシーをTrend Vision One Endpoint Security - Server & Workload Protectionに移行し、移行されたエージェントに同じポリシーを適用したい場合は、移行されたポリシーを割り当てるを選択します。別のポリシーを割り当てたい場合は、Trend Vision One Endpoint Security - Server & Workload Protectionからポリシーを選択を選択し、新しいポリシーを選択します。
   - コンピュータグループ: エージェントが配置されるコンピュータグループは、Trend Vision One Endpoint Security - Server & Workload Protection にあります。
   - Relayグループ: すべてのエージェントはTrend Vision One Endpoint Security - Server & Workload ProtectionのプライマリRelayグループに割り当てられます。
   - サーバーおよびワークロード保護マネージャーに連絡するためのプロキシ: エージェントがTrend Vision Oneエンドポイントセキュリティ- サーバーおよびワークロード保護に連絡するためにプロキシが必要な場合は、プロキシを選択します。
   - Relayに連絡するためのプロキシ: エージェントがTrend Vision One Endpoint Security - Server & Workload ProtectionのRelayに連絡するためにプロキシが必要な場合、プロキシを選択します。
   - 既存のホスト名、表示名、および説明で移行: このオプションを選択すると、移行されたエージェントに既存のホスト名、表示名、および説明を使用します。

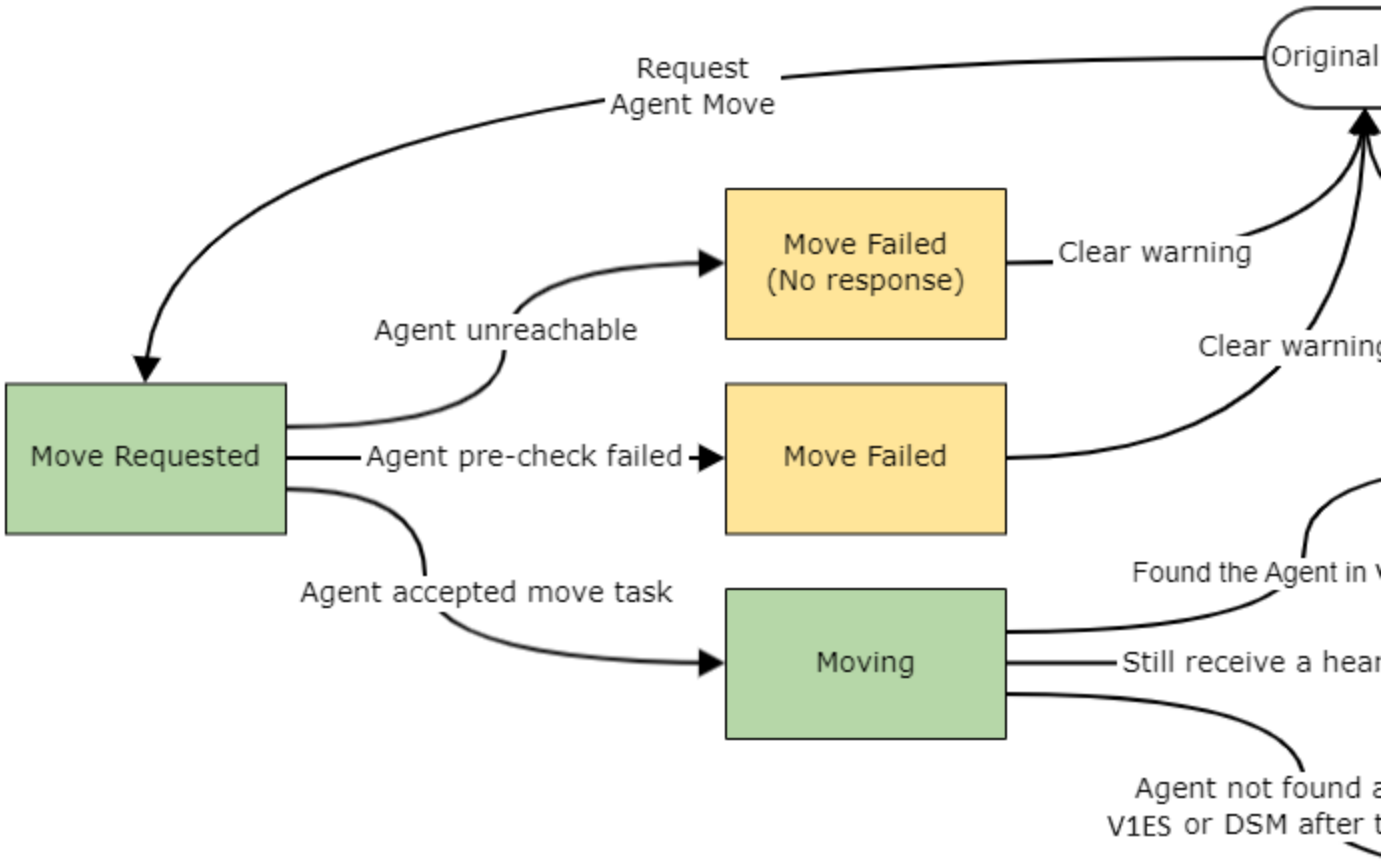
- コンピュータレベルで設定を上書きして移行: コンピュータレベルで上書きされた設定を移行するには、このオプションを選択してください。これにはルールの割り当てや複数の検索リストの除外は含まれません。

7. "移動ステータスを確認する" below を確認します。
8. 問題が発生した場合は、"トラブルシューティング" on page 1766 を参照してください。

移動ステータスを確認する

移動タスクのステータスは、APIレスポンス、コンピュータページ、およびシステムイベントから確認できます。移動ステータスはスマートフォルダの検索条件でもあります。

移動タスクの元の状態は、エージェントがオンプレミスのDeep Security Managerによって管理されている状態です。



Status	説明	元の状態に復元する方法
移行要求済み	Trend Vision One Endpoint Security - Server & Workload Protection への移動タスクが要求されました。 移動タスクはDeep Security Managerによって受け入れられましたが、まだエージェントに送信されていません。	N/A
移行中	コンピュータはTrend Vision One Endpoint Security - Server & Workload Protectionに移動中です。 エージェントは移動タスクを受け入れ、Trend Vision One Endpoint Security - Server & Workload Protection に移動しています。	N/A
移行完了	コンピュータは正常にTrend Vision One Endpoint Security - Server & Workload Protectionに移動されました。 Deep Security Manager は、移動したエージェントが Trend Vision One Endpoint Security - Server & Workload Protection でアクティブ化されていることを識別できます。	エージェントを手動で再有効化してDeep Security Managerに戻します。 エージェントはすでにTrend Vision One Endpoint Security - Server & Workload Protectionの公開証明書を信頼していることに注意してください。エージェントをDeep Security Managerに再度アクティブ化する前に、ds_agent_dsm_public_ca.crtファイルを手動で削除する必要があります。
移行失敗	エージェントからTrend Vision One Endpoint Security - Server & Workload Protectionへの接続の問題により、コンピュータはWorkload Securityに移動されませんでした。 エージェントは事前チェックを行っている間に移動タスクを拒否しました。 移動を再試行する前に: • 移行のために指定されたすべてのパラメータが正しいことを確認してください。アカウント情報、アクティ	コンソールの警告をクリアします。 エージェントは引き続きDeep Security Managerによって管理されます。

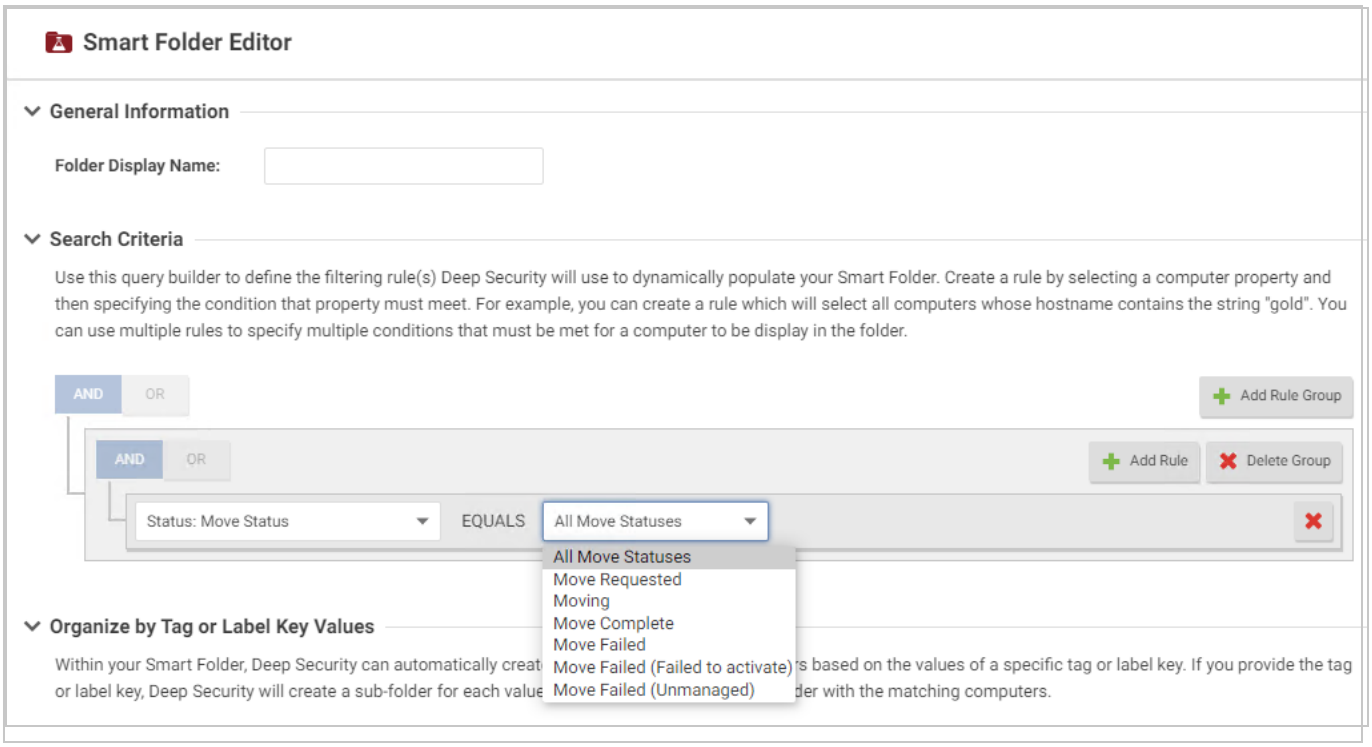
Status	説明	元の状態に復元する方法
	ベーション トークン、公開 CA 証明書、およびプロキシの設定を含みます。 • ネットワークまたはファイアウォールの設定が、エージェントがTrend Vision One Endpoint Security - Server & Workload Protectionに到達するのを妨げていないことを確認してください。 • CLIを使用して、失敗した移動に関する情報を含む ds_agent.log ファイルを含むエージェント診断パッケージを作成します。診断パッケージの作成手順については、「診断パッケージとログの作成」を参照してください。	
移動失敗(応答なし)	コンピュータは、エージェントが移動タスクにタイムリーに応答しなかったため、Trend Vision One Endpoint Security - Server & Workload Protection に移動されませんでした。 移動を再試行する前に: • Agentが実行されていることを確実にする。 • エージェントがDeep Security Managerと適切に通信できることを確認してください。	コンソールの警告をクリアします。 エージェントは引き続きDeep Security Managerによって管理されます。
移動失敗(有効化に失敗)	Trend Vision One Endpoint Security - Server & Workload Protection への移行は、アクティベーションの問題により失敗し、ロールバックされました。 事前チェックは合格しましたが、エージェントはTrend Vision One Endpoint Security - Server & Workload	コンソールの警告をクリアします。 エージェントは引き続きDeep Security Managerによって管理されます。

Status	説明	元の状態に復元する方法
	Protectionをアクティブ化できませんでした。 移動を再試行する前に: • Trend Vision One Endpoint Security - Server & Workload Protection Link が最新であることを確認してください。 • 移行のために指定されたすべてのパラメータが正しいことを確認してください。アカウント情報、アクティベーション トークン、公開 CA 証明書、およびプロキシの設定を含みます。 • CLIを使用して、失敗した移動に関する情報を含む dsa_move.log ファイルとdsa_control.log ファイルを含むエージェント診断パッケージを作成します。診断パッケージの作成手順については、「診断パッケージとログの作成」を参照してください。	
移動に失敗した(管理対象外)	Trend Vision One Endpoint Security - Server & Workload Protection への移行はアクティベーションの問題により失敗し、移行を自動的にロールバックすることができませんでした。コンピュータは管理されていない状態です。 事前チェックは合格しましたが、エージェントはTrend Vision One Endpoint Security - Server & Workload Protectionを有効にできませんでした。 この状態のエージェントは、ロールバック中に不明な問題が発生した可能性があり、エージェントの手動操作が必要で	Deep Security Managerにエージェントを手動で復元します。 エージェントは引き続きホストコンピュータを保護していますが、Deep Security Managerによって管理されていません。 詳細については、トラブルシューティングをご覧ください。

Status	説明	元の状態に復元する方法
	す。 この問題のトラブルシューティング: • dsa_move.log ファイルを調べて、失敗した移動に関する情報を確認してください。 • エージェントを手動で復元するか、エージェントを再有効化してください。詳細については、トラブルシューティングを参照してください。 移動を再試行する前に: • Trend Vision One Endpoint Security - Server & Workload Protection Link が最新であることを確認してください。 • 移動のために指定されたすべてのパラメータが正しいことを確認してください。アカウント情報、アクティベーション トークン、公開 CA 証明書、およびプロキシの設定を含みます。	

スマートフォルダを使用して移動ステータスを表示する

1. スマートフォルダ Editor から、検索条件 を展開します。
2. 最初のリストで、プロパティStatus: Move Status を選択します。
3. 2番目のリストで、移動完了 や移動失敗 などの値を選択します。



トラブルシューティング

管理対象外のエージェントを手動で復元する

dsa_move.log ファイルを調べて、移動失敗の根本原因を特定してください。エージェントの復元が失敗したのは、エージェントが停止に失敗したか、開始に失敗したためかもしれません。

エージェントを停止できなかった場合

エージェントがリストアプロセス中に停止に失敗した場合、次のエラーメッセージがログに表示されます:

```
Unable to stop the agent. Agent restore failed.
```

エージェントを復元するには:

1. エージェントサービスを停止します。
2. エージェントのバックアップを復元します。
   a. エージェントの作業ディレクトリを探します。
      - Windows のエージェント作業ディレクトリ: %ProgramData%\Trend Micro\Deep Security Agent\
      - Linux/Unix のエージェント作業ディレクトリ: /var/opt/ds_agent/

   b. そのディレクトリ内で、バックアップ名は backup_ で始まり、日付で終わります。次に例を示します。backup_2021-05-11_20.11.45
   c. エージェントの作業ディレクトリからdiagおよびbackup_*ディレクトリを除くすべてを削除します。
   d. backup_* ディレクトリからエージェントの作業ディレクトリにすべてをコピーします。
3. エージェントサービスを開始します。
4. dsa_control -mを使用してDeep Security Managerにハートビートを送信する
5. エージェントが正常に復元された(Deep Security Managerで正常に有効化された) 場合は、backup_* ディレクトリを削除します。

エージェントを起動できなかった場合

復元プロセス中にエージェントの起動に失敗した場合、次のエラーメッセージがログに表示されます:

```
Unable to start the agent. Agent restore failed.
```

エージェントを復元するには:

1. エージェントサービスを開始します。
2. dsa_control -mを使用してDeep Security Managerにハートビートを送信する

重複したエンドポイントレコードエラーと不正な保護の管理値エラーを解決する

重複したエンドポイントレコードエラーと不正な保護の管理値エラーが発生した場合は、Deep SecurityからTrend Vision One Endpoint Security - サーバ & Workload Protectionへのエージェント移行時のEndpoint Inventoryの問題の解決を参照して、これらのエラーに対処する方法についての情報を確認してください。

エージェントを移行するその他の方法

環境に十分な自動化ツールが含まれている場合、Trend Vision One Endpoint Security - Server & Workload Protection コンソール内のデプロイスクリプトからアクティベーションコマンドを抽出してエージェントを再アクティベートできます。エージェントがインストールされていない新しいホストは、スクリプト全体を実行する必要があります。既存の最新のエージェントがあるホストは、デプロイスクリプトの最後にコメントとして記載されているdsa_control コマンドを実行できます。プロキシが使用されている場合、このコマンドの前にある数行を確認し、正しい値で実行してからアクティベーションコマンドを実行してください。再アクティベーションには再起動は不要で、プロセス中に保護が失われることはありません。

自動化インフラストラクチャが十分でない環境では、Deep Security MoveAgent API を使用できます。これは、ターゲットの Trend Vision One Endpoint Security - Server & Workload Protection アカウント用に構成された Trend Vision One Endpoint Security - Server & Workload Protection リンクを使

用して、エージェントを自動的に再アクティブ化します。この方法には、Deep Security Manager 20.0.321 (20 LTS 2021-01-26) 以降および Deep Security Agent 20.0.0-3445 (20 LTS Update 2021-11-24) 以降が必要です。手順については、"Deep SecurityおよびTrend Vision One Endpoint Security - Server & Workload Protection APIを使用してアップグレード" on page 1755を参照してください。

Trend Vision One Endpoint Security - Server & Workload Protection のオプションを有効にして、エージェントを自動的にアップグレードして、最新のエージェントで提供される完全なセキュリティ制御を取得する必要があります。各 Trend Vision One Endpoint Security リージョンで利用可能な最小エージェントバージョンは異なります。トレンドマイクロは可能な限り最新のエージェントバージョンを使用することを推奨しますが、アカウントで利用できない古いエージェントバージョンが必要な場合は、トレンドマイクロ サポートに連絡してください。

Deep Security を Trend Cloud One - Endpoint & Workload Security に移行する

Trend Cloud One - Endpoint & Workload Securityに移行

環境をTrend Cloud One - Endpoint & Workload Securityに移行する準備をしているDeep Security管理者は、この記事の手順を使用して、移行を成功させるためのロードマップを作成できます。

> 注意: Deep Security Manager 20.0.513 (20 LTS Update 2021-10-14) 以降である必要があります。

一般的に、成功する移行のための操作順序は次のとおりです:

1. "Workload Security アカウント、ユーザー、ロール、および認証を設定する" on the next page
2. "ロールとAPIキーを作成" on the next page
3. "Workload Securityへのリンクを準備する" on page 1770
4. ポリシーの移行
5. 共通オブジェクトの移行
6. クラウドアカウントを移行する
7. エージェントの移行
8. "その他のDeep Security設定の移行" on page 1770
9. "ネットワークと通信の設定" on page 1772

Workload Security アカウント、ユーザー、ロール、および認証を設定する

Workload Security サービスを使用するには、Trend Cloud One アカウントが必要です。設定、ポリシー、またはコンピュータをサービスに移行する前に、アカウントを設定してください。

SAML は Trend Cloud One で 2 つのサポートレベルがあります: 特に Workload Security の場合と共通レベルの場合です。これらの手順は Deep Security と Workload Security を接続する方法を説明します。

Trend Cloud Oneには、2021年8月4日以降に作成された新しいアカウントと、2021年8月4日より前に作成された従来のアカウントの2種類があります。アカウントの種類がわからない場合は、「Trend Cloud Oneアカウントの変更点」を参照してください。

新しいTrend Cloud Oneアカウントは、新しいアイデンティティおよびアクセス管理システムを使用します。Workload Securityに移行する際にユーザとロールを正しく管理する方法について詳しく理解するために、Trend Cloud Oneアカウントおよびユーザ管理ドキュメントを確認してください。

もしレガシーのTrend Cloud Oneアカウントをお持ちの場合、ユーザおよびロールの権限をDeep Security実装からレガシーアカウントのWorkload Securityに手動で移行する必要があります。レガシーアカウントのユーザおよびロールの構成は、Deep Securityソフトウェア実装とほぼ同一であり、既存の機能を複製します。

SAML を Deep Security Manager で使用している場合は、Workload Security コンソールで SAML を構成し、認証とロールマッピングを実行するアイデンティティプロバイダにエクスポートされた適切なサービスプロバイダメタデータをインポートする必要があります。

注意: ADFS経由でSAML経由で委任されないかぎり、認証のためのActive Directoryとの統合は Workload Security ではサポートされません。

ロールとAPIキーを作成

指示に従って、カスタムロールを定義するでカスタムロールを作成します。事前定義された権限 Deep Security サービス Workload Security の移行をロールに割り当てます。Deep Security 移行権限は事前構成されており、エージェントやポリシーの移行を実行する権利を持つWorkload Security によって管理されています。追加の移行機能が実装されると、関連する権利が将来変更される可能性があります。ロールを作成した後、新しい API キーを作成するの手順に従って、定義されたロールで API キーを作成します。

注意: トレンドマイクロは、APIキーにフルアクセスの役割を割り当てないことを強く推奨します。これによりセキュリティ上の懸念が生じます。

Workload Securityへのリンクを準備する

Trend Vision One Endpoint Security への移行(以前は Workload Security ツールへの移行と呼ばれていました) は、Trend Vision One Endpoint Security - Server & Workload Protection および Trend Cloud One - Endpoint & Workload Security の両方の移行を可能にします。ツール自体に加えて、関連するロール構成も名前が変更されたことに注意してください。

ロール権限Trend Vision One Endpoint Security Linkの管理を許可は、ユーザがTrend Vision One Endpoint Security Linkを管理するために割り当てられる必要があります。

1. Deep Security Manager コンソールで、サポート> Trend Vision One エンドポイントセキュリティに移行 を選択します。
2. Trend Vision One Endpoint Security へのリンクページで:
   a. 前のセクションで作成したAPIキーを入力します。
   b. Workload Security アカウントがあるリージョンを選択します。
   c. [Save] をクリックします。

   警告: 以前にDeep SecurityとWorkload Security の間の接続を設定していて、リンクを変更する場合は、リンクを変更する前に、以前の接続を使用するすべての移行関連タスクが完了していることを確認してください。そうしないと、予期しない動作が発生する可能性があります。

   各Deep Security Managerテナントは、1つのTrend Vision One Endpoint Security Link(旧称 Workload Security Link) のみを許可します。

   Trend Vision One Endpoint Security Link(以前はWorkload Security Linkと呼ばれていました) の作成中に、Deep Security ManagerはWorkload Securityに接続してリンクを認証し、情報を取得します。Deep Security ManagerのインストールがWorkload Securityに接続するためにプロキシを必要とする場合は、Workload Securityのプロキシを構成します。

3. Trend Vision One Endpoint Security への移行 ページが表示され、設定の移行 タブが選択されています。

   ユーザがすべての移行タスクを処理できるようにするには、Trend Vision One Endpoint Security への移行を許可する役割の権限を割り当てる必要があります。

次に、ポリシーを Workload Security

その他のDeep Security設定の移行

次に、Deep Security環境で使用している場合は、次のアーティファクトを移行します:

- "VMwareコネクタとデータセンターゲートウェイ" below
- "コンピュータグループとスマートフォルダ" below
- "プロキシ設定" below
- "イベントとアラートのログ" below
- "追加設定" on the next page
- "Trend Micro Vision One (XDR) 登録" on the next page

VMwareコネクタとデータセンターゲートウェイ

VMware環境で実行されている仮想マシンでは、他のワークロードと同様に、エージェントをWorkload Securityサービスに配信して有効化できます。VMware vCenterに接続して仮想マシンのインベントリを取得する場合は、Workload SecurityがvCenterと通信する必要があります。これは、データセンターゲートウェイを介して実行されます。データの設定とvCenterインベントリのインポートの手順については、「Workload SecurityにVMware vCenterを追加する」を参照してください。

コンピュータグループとスマートフォルダ

コンピュータグループとスマートフォルダには、まだ直接移行する方法はありません。Deep SecurityとWorkload Securityコンピュータグループを一覧表示および作成するためのAPIがあるため、適切なAPI呼び出しをスクリプト化することで、多数のグループの移行を自動化できます。

プロキシ設定

現在、プロキシ設定をDeep SecurityからWorkload Securityに自動的に移行する方法はありません。「プロキシの設定」の手順に従って、Workload Securityでエージェント通信のプロキシ設定を手動で設定できます。

Managerのプロキシは Workload Security サービスの一部であり、トレンドマイクロが管理しているため、プロキシを設定する必要はありません。

イベントとアラートのログ

Deep Security とWorkload Security の主な違いは、マネージャ内のイベントおよびアラートデータの保持です。Workload Security はセキュリティイベントを32日間、システムイベントを91日間保持します。イベントをより長く保持する必要がある場合は、トレンドマイクロはイベントをSIEM またはログサーバーにエクスポートすることを推奨します。

すでにイベントログを使用している場合、アラートやイベントを受信するためにインフラストラクチャの変更が必要になることがあります。Deep Security Managerがすべてのアラートとイベントをsyslogを介し

てローカルのsyslogサーバーに送信する従来のオンプレミス展開では、そのsyslogサーバーがWorkload Securityから直接アクセスできない場合があります。次の代替案を検討してください:

- Workload Security サービスからアクセス可能な新しい syslog サーバーを次の手順に従って作成します: Workload Security イベントを Syslog または SIEM サーバーに転送する。
- Manager経由ではなくローカルのSyslogサーバにイベントを直接送信するようにAgentを設定します。SyslogでTLS暗号化を使用するには、イベントをWorkload Security サービスから転送する必要があります。エージェントは現在、SyslogイベントのTLS暗号化をサポートしていません。
- syslogの代わりにAmazon SNSを使用します。「Amazon SNSを設定する」を参照してください。

追加設定

他のアーティファクトの構成(システム設定、レポート、イベントベースおよびスケジュールされたタスク、タグ、バージョン管理、API Keysなど) は、現在のところ自動化された移行機能の一部ではありません。これらはWorkload Securityで手動で再作成できます。これらのアーティファクトの多くは、Deep SecurityおよびWorkload SecurityのAPIで構成可能であり、自動化することができます。

注意: 一部のシステム設定は、Deep Security からWorkload Security への移行時にサポートされないか、適用されない場合があります。これらの設定をAPI コールを通じて自動化する際には注意が必要です。これらの設定に関するガイダンスについては、トレンドマイクロサポートにお問い合わせください。

Trend Micro Vision One (XDR) 登録

Trend Micro Vision One は Workload Security に含まれていますが、Workload Security コンソールで有効にするには登録トークンが必要です。ポリシーやコンピュータ設定でアクティビティ監視を有効にすることもできます。詳細については、Workload Security とTrend Micro Vision One の統合を参照してください。

ネットワークと通信の設定

次の項目を評価します。

- "必要なポート、プロトコル、およびURL" on the next page
- "プロキシ設定" on the next page
- "検索されたサイズ使用率" on the next page
- "Relay の設定" on page 1774

必要なポート、プロトコル、およびURL

Deep Security Agent とWorkload Security 間のネットワーク通信は、エージェントとDeep Security Manager 間の通信とは異なります。アウトバウンドインターネットアクセスが制限されている環境では、特定の URL を許可する必要があります。完全なリストについては、ポート番号、URL、および IP アドレスを参照してください。

プロキシ設定

Workload Security サービスへのエージェント通信用のプロキシーの構成については、「プロキシの設定」を参照してください。

SOCKS4およびSOCKS5プロキシは、エージェント通信ではサポートされていません。エージェント通信にプロキシを使用する必要がある場合は、エージェントが Workload Security サービスに対して有効化される前に、HTTPプロキシを実装します。

検索されたサイズ使用率

Deep Security Agentの配置に関するネットワーク計画を検討する際は、エージェントのダウンロードと有効化、および継続的な操作とセキュリティパターンのアップデートの両方について、エージェントの全体的なライフサイクルを考慮してください。

既存のDeep Securityエージェントは再インストールする必要はなく、Workload Securityサービスに再アクティブ化するだけです。アクティベーションスクリプトを使用して行われる新しいデプロイメントでは、次の帯域幅使用量が予想されます:

- エージェントのダウンロードとアクティベーション: Linuxで5 MB; Windowsで25 MB
- 初回セキュリティ更新のダウンロード: 50 MB Linux; 102 MB Windows

継続的なエージェントトラフィックは、検出アクティビティ、ポリシー設定、およびモジュールの使用状況によって大きく異なります。次のガイドラインに類似した、管理トラフィックのベースラインの使用を想定します。

- セキュリティアップデート(毎日1回、スマートスキャン オン) : 60MB
- セキュリティアップデート(1日1回、スマートスキャン オフ) : 120MB
- ハートビートのオーバーヘッド: ハートビートごとに40 KB。デフォルトの間隔は10分; エージェントごとに1日約5.7 MB

詳細については、Workload SecurityのSmart Protectionを参照してください。

ベースラインのトラフィックを超えると、エージェントがWorkload SecurityおよびVision Oneサービスと通信するため、検出が追加の帯域幅消費を引き起こします。これは予測が難しいですが、検出が少ない場合はエージェント1つあたり1時間に0.1 MB、検出率が高い場合はエージェント1つあたり1時間に最大3 MBの使用を見込んでください。

Relay の設定

ほとんどの場合、Workload Securityサービスによって提供されるRelayは十分です。いくつかのシナリオでは、Relayを使用することで操作が改善されることがあります。詳細については、Relayの仕組みおよび追加のRelayの展開を参照してください。

Deep Security APIとWorkload Security APIを使用した移行

この記事および関連する記事では、Deep Security ManagerおよびWorkload Security UIを使用して移行を実行する方法について説明します。APIを使用する場合:

- 一般的な要件とヒントについては、こちらの記事を参照してください。
- "ロールとAPIキーを作成" on page 1769
- APIドキュメントに従ってWorkload Securityリンクを作成してください。
- 次の情報については、Deep Security API ドキュメントを参照してください
  - ポリシーの移行
  - エージェントの移行
  - 一般的なオブジェクトの移行
  - AWSコネクタの移行
- ポリシー移行ステータスを確認するには、HTTP GET 呼び出しを使用して `/policymigrationtasks/{taskID}` からステータスを取得します。詳細については、Workload Security Automation Centerを参照してください。

製品内の移行機能で現在サポートされていない項目は、通常、Deep SecurityとWorkload Security APIの組み合わせを使用して移行し、Deep Security配置から関連する設定またはオブジェクトを読み取り、Workload Security アカウントに書き込むことができます。。

いくつかのアーティファクトは現在のAPIでは利用できませんが、従来のRESTおよびSOAP APIを介してアクセス可能です。また、いくつかの機能はDeep Securityのみに存在し、移行はサポートされていません。

Workload Securityでサポートされていない機能:

- Deep Security マルチテナント設定、/tenants API に従います。Trend Cloud One の複数アカウント管理は従来のオンプレミスのマルチテナントを超えており、これらの設定は Workload Security には適用されません。
- VMware環境向けのAgentレス保護

現在のAPIにないレガシーREST APIの機能：

- ステータス監視
- SAML設定
- プロキシの設定、制御、および割り当て
- イベントの取得

現在のAPIにないSOAP APIの機能：

- プロキシの設定、制御、および割り当て
- イベントの取得
- 処理(エージェントのアップデート、検索の実行など)
- ルール設定

ポリシーをTrend Cloud One - Endpoint & Workload Securityに移行する

"Trend Cloud One - Endpoint & Workload Securityに移行" on page 1768は複数のステップを含むプロセスです。

Workload SecurityでDeep Securityと同じポリシーを使用することをお勧めします。ポリシーをWorkload Securityで手動で再作成するか、移行ツールを使用してポリシーの移行を自動化するか、他のポリシー移行方法のいずれかを使用できます。

前提条件

- Deep Security Manager 20.0.513 (20 LTS Update 2021-10-14) 以降を実行していることを確認してください。

  サポートされているDeep Security 20バージョンにアップグレードしてポリシーを移行したくない場合は、ポリシーをXMLにエクスポートし、APIを介してWorkload Securityにインポートする方法については、Deep Security 12のドキュメントを参照してください。

- 最新のDeep Security Rule Updates(DSRU) にアップデートして適用します。Deep Security Managerで、[管理]→[アップデート]→[セキュリティ]→[ルール]に選択します。

  移行がエラー303を引き起こした場合、DSRUを更新しなかった可能性があります。

- まだ行っていない場合は、Trend Cloud Oneアカウントの作成、APIキーの作成、Workload Securityへのリンクの準備を含む、"Trend Cloud One - Endpoint & Workload Securityに移行" on page 1768の前の手順を完了してください。

制限事項

- SAP Scanner モジュール設定を含むポリシーは移行またはインポートできますが、これらの設定は、SAP Scannerに対して Workload Security アカウントのライセンスも付与されていない限り表示されません。
- Workload Securityでは、VMwareエージェントレス設定を含むポリシーはサポートされません。
- アプリケーションコントロール設定は移行されません。
- ネットワークに依存するオブジェクトと設定(プロキシ設定、Syslog設定など) は移行されないことがあります。
- ポリシーで参照されている共通オブジェクトのみが移行されます。移行対象の共通オブジェクトがWorkload Securityの既存の共通オブジェクトと同じ名前である場合は、既存のオブジェクトが移行されたオブジェクトで上書きされます。

一般的なオブジェクトの移行に関する情報については、一般的なオブジェクトをWorkload Securityに移行するを参照してください。

移行ツールを使用してポリシーを移行する

Trend Vision One Endpoint Security ツールへの移行 (以前は Workload Security ツールへの移行と呼ばれていました) は、Trend Vision One Endpoint Security - Server & Workload Protection と Trend Cloud One - Endpoint & Workload Security の両方の移行を可能にします。ツール自体に加えて、関連するロール構成も名前が変更されたことに注意してください。

1. Deep Security Manager コンソールで、サポート> Trend Vision One エンドポイントセキュリティに移行 を選択します。
2. 設定タブが選択された状態で表示されるTrend Vision One Endpoint Security への移行ページで、ポリシーの移行をクリックしてそのセクションを展開します。

最初にTrend Vision One Endpoint Security アカウントへのリンクページが表示された場合、リンクの設定方法については"Workload Securityへのリンクを準備する" on page 1770を参照してください。

3. [移行]を選択します。移行ツールは、Deep Security Managerのすべてのポリシーを対象とします。

   移行ツールがステータスを表示するときは、ポリシーに移動してWorkload Securityでも確認できます。移行されたポリシーはリストに表示され、タイムスタンプとDeep Security Managerのホスト名が表示されます。

   以下は、可能なステータスです

   - 移行が要求されました: Workload Security へのポリシー移行タスクが要求されましたが、ポリシー移行はまだ開始されていません。
   - 移行中: ポリシーがWorkload Securityに移行されています。ステータスが移行中のままの場合、Deep Security ManagerがWorkload Securityからの応答を受信できないことを意味します。ネットワーク構成を確認してください。
   - 移行済み: ポリシーが Workload Securityに正常に移行されました。
   - 失敗: ポリシーが何らかの理由で Workload Security に移行できませんでした。エラーコードを確認します。
     - エラーコード303: 移行中のポリシーは、Workload Securityで使用できない1つ以上のルールを参照しています。Deep Security ManagerとWorkload Security で同じバージョンのルールアップデートを使用していることを確認してください。
     - その他のエラーコード900未満: Workload Securityの障害が発生しました。トレンドマイクロ サポートに連絡してください。
     - エラーコードが900以上: Deep Security Managerで Workload Securityとの通信に問題があります。Workload Security リンクが正しく設定されていることを確認するか、詳細についてserver0.log を確認してください。

次に、共通オブジェクトを Workload Security

ポリシーを移行するその他の方法

移行ツールを使用することに加えて、以下の方法を使用してポリシーをWorkload Securityに移行することができます:

- Deep Securityポリシー移行APIとWorkload Security リンク機能を使用してポリシーを直接移行します。この機能は、Deep Security Manager 20.0.463(20 LTS Update 2021-07-22) 以降

で使用できます。手順については、"Deep Security APIとWorkload Security APIを使用した移行" on page 1774

- Deep Security からポリシーXML をエクスポートし、次に Workload Security ポリシーインポート API を使用します。古いバージョンの Deep Security を使用している場合、または Deep Security から Workload Security への直接接続が不可能な場合は、Deep Security 12 以降からポリシーをエクスポートし、ポリシーインポートAPI を使用して Workload Security にインポートできます。詳細については、Deep Security 12 ヘルプの Workload Security へのポリシーの移行 を参照してください。

共通オブジェクトをTrend Cloud One - Endpoint & Workload Securityに移行する

"Trend Cloud One - Endpoint & Workload Securityに移行" on page 1768は複数のステップを含むプロセスです。

移行ツールを使用して、共通オブジェクト(ルールと不正プログラムの設定を除く)をTrend Cloud One - Endpoint & Workload Securityに移行できます。

前提条件

- Deep Security Manager 20.0.585 (20 LTS Update 2022-01-17) 以降を実行していることを確認してください。
- まだ行っていない場合は、Trend Cloud Oneアカウントの作成、APIキーの作成、Workload Securityへのリンクの準備を含む、"Trend Cloud One - Endpoint & Workload Securityに移行" on page 1768の前の手順を完了してください。

移行ツールを使用して共通オブジェクトを移行する

Trend Vision One Endpoint Security ツールへの移行 (以前は Workload Security ツールへの移行と呼ばれていました) は、Trend Vision One Endpoint Security - Server & Workload Protection と Trend Cloud One - Endpoint & Workload Security の両方の移行を可能にします。さらに、ツール自体に加えて、関連するロール構成も名前が変更されたことに注意してください。

1. Deep Security Manager コンソールで、サポート> Trend Vision One エンドポイントセキュリティに移行 を選択します。
2. Trend Vision One Endpoint Security への移行ページが表示され、設定タブが選択されています。共通オブジェクトの移行をクリックして、そのセクションを展開します。

最初にTrend Vision One Endpoint Security アカウントへのリンクページが表示された場合、リンクの構成方法については"Workload Securityへのリンクを準備する" on page 1770を参照してください。

3. 共通オブジェクトリストで、移行するオブジェクトの種類を選択します。

   警告: 移行されたオブジェクトは、移行される共通オブジェクトが次のいずれかの条件を満たす場合、既存のオブジェクトを上書きします
   - 共通オブジェクトは、Workload Securityに既存の共通オブジェクトと同じ名前です。
   - 共通オブジェクトは、Workload Security内の既存の共通オブジェクトと同じ名前であるかどうかに関係なく、トレンドマイクロによって作成されたデフォルトオブジェクトです。

4. 移行したい共通オブジェクトを選択し、選択したものを移行をクリックします。
5. 移行が開始されたら、移行ステータスを確認するために更新をクリックしてください。考えられるステータスは次のとおりです:
   - リクエスト済み: 共通オブジェクトのWorkload Securityへの移行がリクエストされましたが、移行はまだ開始されていません。
   - 移行中: 共通オブジェクトがWorkload Securityに移行されています。ステータスが移行中のままの場合、Deep Security ManagerがWorkload Securityからの応答を受信できないことを意味します。ネットワーク構成を確認してください。
   - 移行済み: 共通オブジェクトは正常にWorkload Securityに移行されました。
   - 失敗: 一部の共通オブジェクトが何らかの理由でWorkload Securityへの移行に失敗しました。エラーコードを確認してください:
     - エラーコード300: 選択した共通オブジェクトが存在しません。
     - エラーコードが900以上: Deep Security ManagerでWorkload Securityとの通信に問題があります。Workload Securityリンクが正しく設定されていることを確認するか、詳細についてserver0.logを確認してください。

次に、クラウドアカウントとエージェントを移行します。

クラウドアカウントをTrend Cloud One - Endpoint & Workload Securityに移行する

"Trend Cloud One - Endpoint & Workload Securityに移行" on page 1768は複数のステップを含むプロセスです。

クラウドコネクタを使用してDeep Securityにクラウドアカウントを追加した可能性があります。移行ツールまたは移行APIを使用して、保護対象のクラウドアカウントを移行できます。

前提条件

- Deep Security Manager 20.0.635 (20 LTS Update 2022-04-21) 以降を実行していることを確認してください。
- もしまだ行っていない場合は、"Trend Cloud One - Endpoint & Workload Securityに移行" on page 1768の前の手順を完了してください。これには、Trend Cloud One アカウントの作成、APIキーの作成、および Workload Security へのリンクの準備が含まれます。

AWSアカウントを移行する場合

注意: AWS ではないアカウントの移行に関する情報については、"移行ツールを使用して他のクラウドアカウントを移行する" on page 1783を参照してください。

制限事項

登録されたAWSアカウントの移行に使用する手順は、最初にDeep Security Managerに追加された方法によって異なります。

- アクセスキーを使用して追加されたAWSアカウントは、移行ツールまたは移行APIを使用して移行できます。
- クロスアカウントロールを使用して追加されたAWSアカウントは、移行ツールまたは移行APIを使用して移行できます。ただし、これらのクロスアカウントロールは、Deep Security Managerの元のプリンシパルに加えて、Workload Security のAWSプリンシパルを信頼するように設定する必要があります。詳細については、"クロスアカウントロールを使用して追加されたAWSアカウントを移行する" below を使用して追加されたAWSアカウントの移行」を参照してください。
- Managerインスタンスロールを使用して追加されたAWSアカウントは、Workload Securityではサポートされません。これらのアカウントの移行はサポートされていません。
- Deep Security Manager 9.6以前で追加された従来のAWSアカウントは、APIエンドポイント `/api/awsconnectors` 経由でアクセスできないため、サポートされません。

クロスアカウントロールを使用して追加されたAWSアカウントを移行する

AWSアカウントをWorkload Securityに登録する方法は2つあります:

- "新しいクロスアカウントロールを作成する" on the next page を作成します。
- "既存のクロスアカウントロールを再利用する" on the next pageをDeep Security Managerに再利用します。

新しいクロスアカウントロールを作成する

この方法では、移行ツールやAPIを使用する代わりに、Workload Security からAWSアカウントへのアクセスを許可する新しいクロスアカウントロールを追加します。手順については、Workload Security ヘルプの「クロスアカウントロールを使用したAWSアカウントの追加」を参照してください。

既存のクロスアカウントロールを再利用する

この方法では、元のクロスアカウントロールを特定し、Workload Securityとの信頼関係を設定して、移行APIを呼び出します。

1. Deep Security Managerからのアクセスを許可するAWSアカウントのクロスアカウントロールを特定します。

   ARNの役割は、Deep Security Managerコンソールで AWSアカウントを右クリックし、[プロパティ]を選択すると表示されます。

   ロールARNの形式は、arn:aws:iam::<AWSアカウントID>:role/<ロール名>です。

2. Workload Security のAWSアカウントとテナントの外部IDをメモします。アカウントIDと外部IDの取得方法については、Workload Securityヘルプのこの記事を参照してください。
3. AWSアカウントにログインします。
4. AWS コンソールで、IAM サービスに移動します。
5. 左側のナビゲーションペインで [役割] をクリックします。
6. メイン画面で、手順1の役割名を見つけてクリックし、概要ページを開きます。
7. 信頼関係タブで、信頼関係を編集するをクリックします。
8. ポリシードキュメントでは、信頼関係は次のようになります。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::<original Deep Security AWS Account>:root"
   },
   "Action": "sts:AssumeRole",
   "Condition": {
    "StringEquals": {
     "sts:ExternalId": "<original Deep Security External ID>"
    }
   }
```

```
  }
 ]
}
```

9. 上記の Workload Security アカウント(147995105371) と外部IDをポリシードキュメントに追加します(最初の文) 。次のようになります。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::147995105371:root"
   },
   "Action": "sts:AssumeRole",
   "Condition": {
    "StringEquals": {
     "sts:ExternalId": "<Workload Security External ID>"
    }
   }
  },
  {
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::<original Deep Security AWS Account>:root"
   },
   "Action": "sts:AssumeRole",
   "Condition": {
    "StringEquals": {
     "sts:ExternalId": "<original Deep Security External ID>"
    }
   }
  }
 ]
}
```

10. [信頼ポリシーのアップデート]をクリックして変更を保存します。
11. 前述の手順を、Workload Security に移行したい各 AWS アカウントに対して繰り返します。

12. 移行ツールまたは移行APIを使用してAWSアカウントを移行します。

移行ツールを使用して他のクラウドアカウントを移行する

Trend Vision One Endpoint Security ツールへの移行(以前は Workload Security への移行と呼ばれていました)は、Trend Vision One Endpoint Security - Server & Workload Protection とTrend Cloud One - Endpoint & Workload Security の両方の移行を可能にします。さらに、ツール自体に加えて、関連するロール構成も名前が変更されました。

1. Deep Security Manager コンソールで、サポート> Trend Vision One エンドポイントセキュリティに移行 を選択します。
2. Trend Vision One Endpoint Security への移行 ページで、クラウドアカウント タブを選択します。
3. すべての移行をサポートする接続されたクラウドアカウントが表示されたら、移行したいアカウントを選択し、選択したものを移行をクリックします。
4. 移行が開始されたら、更新をクリックして移行状況を確認してください。考えられるステータスは次のとおりです:
   - 移行が要求されました: クラウドアカウントのWorkload Securityへの移行が要求されましたが、移行はまだ開始されていません。
   - 移行中: クラウドアカウントがWorkload Securityに移行され、完全な同期が開始されました。このプロセスは完了するまでに時間がかかる場合があります。
   - 移行済み: クラウドアカウントは正常にWorkload Securityに移行されました。
   - 失敗: 何らかの理由でクラウドアカウントのWorkload Securityへの移行に失敗しました。エラーコードを確認してください:
     - エラーコードが900未満: Workload Securityで障害が発生しました。応答の詳細については失敗システムイベントを参照するか、サポートにお問い合わせください。
     - エラーコード900以上: Deep Security Manager は Workload Security との通信に問題があります。Workload Security のリンクが正しく構成されていることを確認するか、詳細については `server0.log` を確認してください。

VMware vCloudアカウントの移行

現在、VMware vCloud アカウントを Workload Security に自動的に移行することはできません。ただし、Workload Security アカウントに新しい VMware vCloud コネクタを作成して保護することができます。トレンドマイクロは、ホストを移行する前にコネクタを設定することを推奨します。

Workload Security でクラウドコネクタを設定する方法については、VMware vCloud でホストされている仮想マシンを追加する を参照してください。

エージェントをTrend Cloud One - Endpoint & Workload Securityに移行する

"Trend Cloud One - Endpoint & Workload Securityに移行" on page 1768は複数のステップを含むプロセスです。

前提条件

- APIを使用して移行する場合は、Deep Security Manager 20.0.321 (20 LTS 2021-01-26) 以降を使用していることを確認してください。また、Deep Security Manager移行ツールを使用して移行する場合は、Deep Security Manager 20.0.513 (20 LTS Update 2021-10-14) 以降を使用してください。
- Deep Security Agent 20.0.0-3445 (20 LTS Update 2021-11-24) 以降を使用していることを確認してください。その後、Workload Security コンソールで 管理 > アップデート > ソフトウェア > ローカル に移動し、アカウントに対応するDeep Security Agent パッケージがあることを確認してください。
- エージェントが移行をサポートするプラットフォームで実行されていることを確認してください:
  - エージェントプラットフォームサポート表 に、Deep Security Manager 20でサポートされるエージェントプラットフォームを示します。
  - エージェントの移行は、IntelアーキテクチャのWindowsおよびLinuxプラットフォームでのみ検証されています。
  - Windows 2008 32ビット版ではエージェントの移行はサポートされていません。
- Deep Security Manager とWorkload Security の機能の違いにより、エージェントを移行する前に次の項目を無効にしてください:
  - FIPS 140: Deep Security Manager は FIPS 140 が有効になっている場合、移行を拒否します。
  - Virtual Appliance: Virtual Appliance (エージェントレスまたは コンバインモード) で保護されているコンピュータは移行を拒否されます。
- もしまだ行っていない場合は、"Trend Cloud One - Endpoint & Workload Securityに移行" on page 1768で説明されている前の手順を完了してください。これには、Trend Cloud One アカウントの作成、API キーの作成、および Workload Security へのリンクの準備が含まれます。

移行ツールを使用してエージェントを移行する

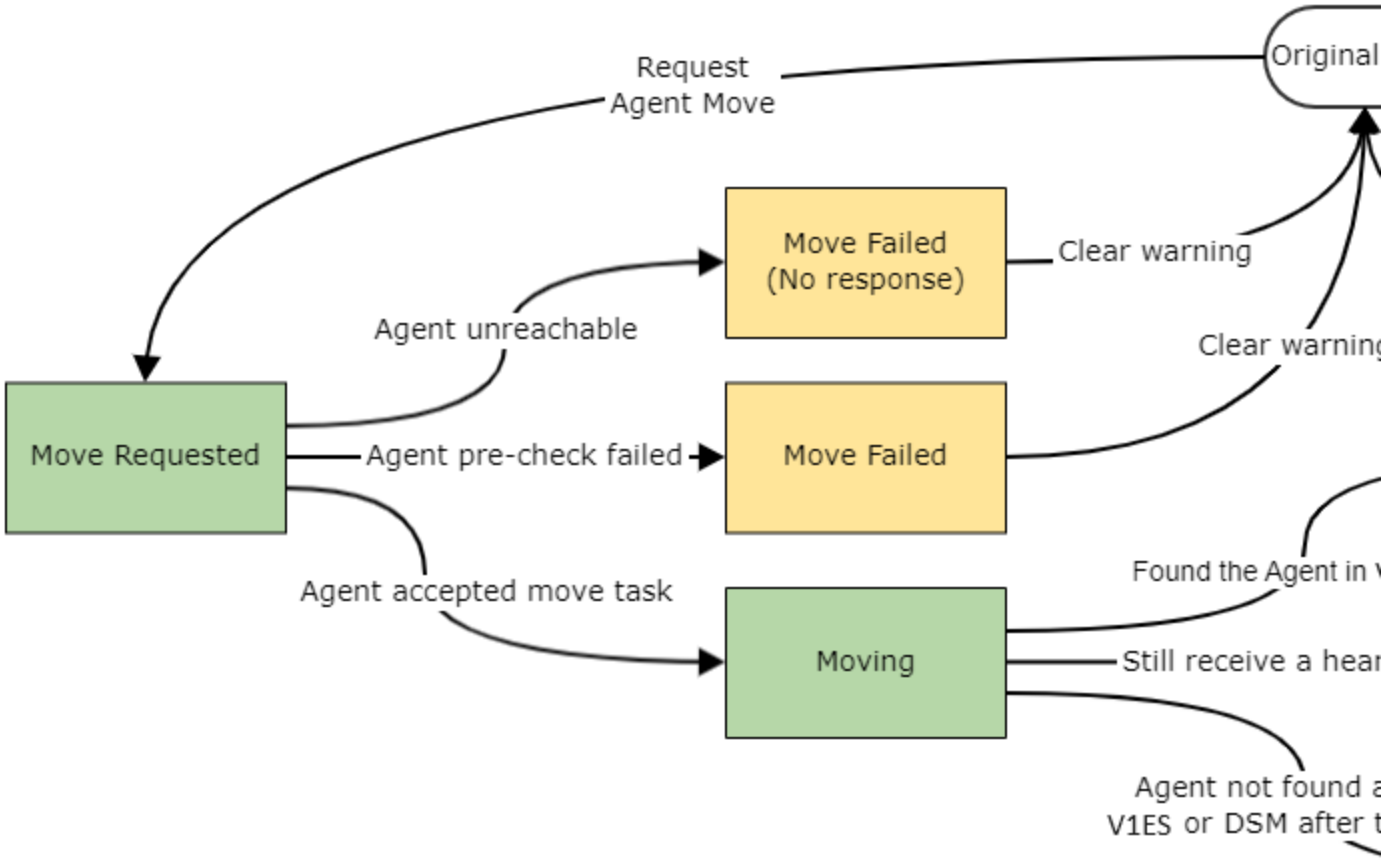
Trend Vision One Endpoint Security への移行ツールは、以前は Workload Security への移行と呼ばれていました。このツールは、Trend Vision One Endpoint Security - Server & Workload Protection とTrend Cloud One - Endpoint & Workload Security の両方の移行を可能にします。さらに、ツール自体に加えて、関連するロール構成も名前が変更されていることに注意してください。

1. Deep Security Manager コンソールで、サポート> Trend Vision One エンドポイントセキュリティに移行 を選択します。
2. Trend Vision One Endpoint Security への移行 ページが表示されたら、エージェント タブを選択します。
3. [[コンピュータ] ページを使用した移行]を選択します。Deep Security [Computers] 画面が表示されます。
4. 移行するコンピュータを1台以上選択します。
5. アクション> Trend Vision One Endpoint Security への移行 を選択します。
6. エージェントを移動する際に適用したい設定を指定し、移行をクリックしてください:
   - セキュリティポリシー: Deep Securityポリシーを Workload Securityに移行し、移行したエージェントに同じポリシーを適用したい場合は、移行ポリシーを割り当てるを選択します。別のポリシーを割り当てたい場合は、Trend Vision One Endpoint Securityからポリシーを選択を選択し、新しいポリシーを選択します。
   - コンピュータグループ: エージェントがWorkload Securityに配置されるコンピュータグループ。
   - Relayグループ: すべてのエージェントは、Workload Securityのプライマリ Relayグループに割り当てられます。
   - サーバーおよびワークロード保護マネージャーに連絡するためのプロキシ: エージェントが Workload Securityに連絡するためにプロキシが必要な場合は、プロキシを選択します。
   - リレーに連絡するためのプロキシ: Workload Security上のリレーに連絡するためにエージェントがプロキシを必要とする場合は、プロキシを選択してください。
   - 既存のホスト名、表示名、および説明を使用して移行:移行したエージェントの既存のホスト名、表示名、および説明を使用する場合に選択します。
   - コンピュータレベルで設定を上書きして移行: コンピュータレベルで上書きされた設定を移行するにはこれを選択します。これにはルールの割り当てや複数の検索リストの除外は含まれません。
7. "移動ステータスを確認する" on the next pageを確認します。
8. 問題が発生した場合は、"トラブルシューティング" on page 1790を確認してください。

移動ステータスを確認する

移動タスクのステータスは、API応答、コンピュータのページ、およびシステムイベントで確認できます。移動ステータスは、スマートフォルダの検索条件でもあります。

移動タスクの元の状態は、エージェントがオンプレミスのDeep Security Managerによって管理されている状態です。



Status	説明	元の状態に復元する方法
移行要求済み	Workload Security への移動タスクが要求されました。 移動タスクはDeep Security Managerによって受け入れられましたが、まだエージェントに送信されていません。	N/A

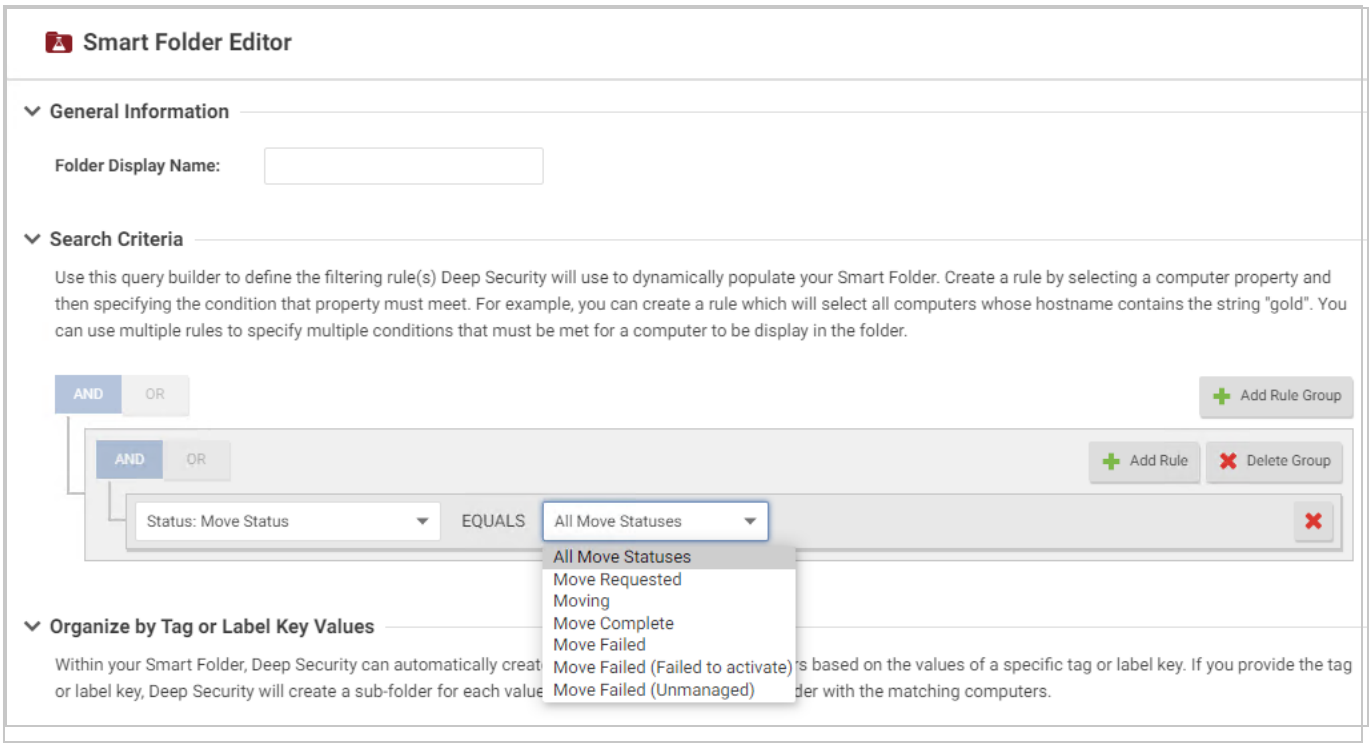
Status	説明	元の状態に復元する方法
移行中	コンピュータをWorkload Securityに移動しています。 エージェントは移動タスクを受け入れ、Workload Securityに移動しています。	N/A
移行完了	コンピュータはWorkload Securityに正常に移動されました。 Deep Security Managerは、移動されたエージェントがWorkload Securityで有効化されていることを識別できます。	エージェントを手動で再有効化してDeep Security Managerに戻します。 エージェントはすでにWorkload Security公開証明書を信頼していることに注意してください。エージェントを有効化してDeep Security Managerに戻す前に、ds_agent_dsm_public_ca.crtファイルを手動で削除する必要があります。
移行失敗	エージェントからWorkload Securityへの接続の問題により、コンピュータはWorkload Securityに移動されませんでした。 エージェントは事前チェックを行っている間に移動タスクを拒否しました。 移動を再試行する前に: • アカウント情報、アクティベーショントークン、パブリックCA証明書、プロキシ設定など、移動に指定したすべてのパラメータが正しいことを確認します。 • ネットワークまたはファイアウォールの設定がエージェントがWorkload Securityに到達するのを妨げていないことを確認してください。 • CLIを使用して、失敗した移動に関する情報を含むds_agent.logファイルを含むエージェント診断パッケージを作成します。診断パッケージの作成手順については、「診断パッケージとログの作成」を参照してください。	コンソールで[警告]をクリアします。 エージェントは引き続きDeep Security Managerによって管理されます。
移動失敗(応答な	エージェントが移動タスクに適切なタイミングで	コンソールの警告をクリアします。

Status	説明	元の状態に復元する方法
し)	応答しなかったため、コンピュータが Workload Security に移動されませんでした。 移動を再試行する前に: • エージェントが稼働中であることを確認します。 • エージェントがDeep Security Managerと適切に通信できることを確認します。	エージェントは引き続きDeep Security Managerによって管理されます。
移動失敗(有効化に失敗)	Workload Security への移動が、アクティベーションの問題により失敗し、ロールバックされました。 事前チェックに成功しましたが、エージェントをWorkload Securityに有効化できませんでした。 移動を再試行する前に: • Trend Vision One Endpoint Security Link(以前はWorkload Security Linkと呼ばれていました) が最新であることを確認してください。 • アカウント情報、アクティベーショントークン、パブリックCA証明書、プロキシ設定など、移動に指定したすべてのパラメータが正しいことを確認します。 • CLIを使用して、失敗した移動に関する情報を含む dsa_move.log ファイルと dsa_control.log ファイルを含むエージェント診断パッケージを作成します。診断パッケージの作成手順については、「診断パッケージとログの作成」を参照してください。	コンソールの警告をクリアします。 エージェントは引き続きDeep Security Managerによって管理されます。
移動に失敗した(管理対象外)	アクティベーションの問題により、Workload Security への移動が失敗し、移動を自動的にロールバックできませんでした。コンピュータが管理対象外の状態です。	Deep Security Managerにエージェントを手動で復元します。 エージェントは引き続きホストコンピュータを

Status	説明	元の状態に復元する方法
	事前チェックは合格しましたが、エージェントはWorkload Securityを有効にできませんでした。 この状態のエージェントは、ロールバック中に不明な問題が発生した可能性があり、エージェントの手動操作が必要です。 この問題のトラブルシューティング: • dsa_move.log ファイルを確認してください。失敗した移動に関する情報が含まれています。 • エージェントを手動で復元するか、エージェントを再有効化してください。詳細については、トラブルシューティングを参照してください。 移動を再試行する前に: • Trend Vision One Endpoint Security Link(以前はWorkload Security Linkと呼ばれていました) が最新であることを確認してください。 • アカウント情報、アクティベーショントークン、パブリックCA証明書、プロキシ設定など、移動に指定したすべてのパラメータが正しいことを確認します。	保護していますが、Deep Security Managerによって管理されていません。 詳細についてはトラブルシューティングを参照してください。

スマートフォルダを使用して移動ステータスを表示する

1. スマートフォルダ Editor から、検索条件 を展開します。
2. 最初のリストで、プロパティStatus: Move Statusを選択します。
3. 2番目のリストで、移動完了や移動失敗などの値を選択します。



トラブルシューティング

管理対象外のエージェントを手動で復元する

dsa_move.log ファイルを確認して、移動の失敗の根本原因を特定します。エージェントの停止または開始に失敗したため、エージェントの復元に失敗した可能性があります。

エージェントを停止できなかった場合

復元プロセス中にエージェントの停止に失敗した場合、ログに次のエラーメッセージが表示されます。

```
Unable to stop the agent. Agent restore failed.
```

エージェントを復元する方法は次のとおりです。

1. エージェントサービスを停止します。
2. エージェントのバックアップを復元します。
   a. エージェントの作業ディレクトリを探します。
      - Windowsのエージェント作業ディレクトリ: %ProgramData%\Trend Micro\Deep Security Agent\
      - Linux / Unixのエージェント作業ディレクトリ: /var/opt/ds_agent/

   b. そのディレクトリ内で、バックアップ名は backup_ で始まり、日付で終わります。次に例を示します。backup_2021-05-11_20.11.45
   c. diag ディレクトリと backup_* ディレクトリを除いて、エージェントの作業ディレクトリからすべてを削除します。
   d. backup_* ディレクトリからエージェントの作業ディレクトリにすべてをコピーします。
3. エージェントサービスを開始します。
4. dsa_control -m を使用して Deep Security Manager にハートビートを送信する
5. エージェントが正常に復元された(Deep Security Manager で正常に有効化された) 場合は、backup_* ディレクトリを削除します。

エージェントを起動できなかった場合

復元プロセス中にエージェントの起動に失敗した場合は、次のエラーメッセージがログに表示されます。

```
Unable to start the agent. Agent restore failed.
```

エージェントを復元する方法は次のとおりです。

1. エージェントサービスを開始します。
2. dsa_control -m を使用して Deep Security Manager にハートビートを送信する

エージェントを移行するその他の方法

環境に十分な自動化ツールが含まれている場合、Workload Security コンソール内のデプロイメントスクリプトからアクティベーションコマンドを抽出してエージェントを再アクティベートできます。エージェントがない新しいホストは、スクリプト全体を実行する必要があります。既存の最新のエージェントがあるホストは、デプロイメントスクリプトの最後にコメントとして記載されている dsa_control コマンドだけを実行すればよいです。プロキシが使用されている場合、このコマンドの前にある数行を確認し、正しい値で実行してからアクティベーションコマンドを実行してください。再アクティベーションには再起動は不要で、プロセス中に保護が失われることもありません。

自動化インフラストラクチャが十分でない環境では、Deep Security MoveAgent API を使用できます。これにより、ターゲットの Workload Security アカウントに構成された Trend Vision One Endpoint Security Link(以前は Workload Security Link と呼ばれていました) を使用してエージェントが自動的に再アクティブ化されます。この方法には、Deep Security Manager 20.0.321 (20 LTS 2021-01-26) 以降および Deep Security Agent 20.0.0-3445 (20 LTS Update 2021-11-24) 以降が必要です。手順については、"Deep Security API と Workload Security API を使用した移行" on page 1774 を参照してください。

トレンドマイクロは、Workload Securityでエージェントをアクティベーション時に自動的にアップグレードするオプションを有効にすることを推奨します。これにより、最新のエージェントで提供される完全なセキュリティコントロールを確保できます。各Trend Cloud Oneリージョンで利用可能な最小エージェントバージョンは異なります。トレンドマイクロは可能な限り最新のエージェントバージョンを使用することを推奨しますが、アカウントで利用できない古いエージェントバージョンが必要な場合は、トレンドマイクロサポートに連絡してください。

DevOps、automation、およびApi

DevOps、自動化、およびAPIについて

管理開発ワークフローをサポートするために、Deep Securityは、リリースのライフサイクル全体にわたってセキュリティを自動化、監視、および管理するためのAPIを提供します("Deep Security APIを使用したタスクの自動化" on page 1824を参照してください)。

Trend Micro Hybrid Cloud Securityコマンドラインインタフェース(THUS) は、APIを簡単にナビゲートするためのツールです。詳細については、https://github.com/trendmicro/thusを参照してください。

Deep SecurityのGitHubリポジトリには、次の役に立つスクリプトが含まれています。

注意: GitHubに公開されているリソースについてのお問い合わせはサポート対象外となります。

- AWSにDeep Security Managerを配置するためのCloudFormationテンプレート。
- 解析ロジック、保存された検索、Splunkを使用したDeep Security監視のためのダッシュボードを含む設定ファイル。
- さまざまなAgentおよびManagerのタスクを自動化する、BashとPowershellのスクリプト。

このAPIの使用を開始するには、Deep Security Automation Centerにあるガイド「First Steps Toward Deep Security Automation」を参照してください。オートメーションセンターには、APIレファレンス/参照情報も含まれています。

Deep Securityには、コンピュータやその他のリソースの保護を迅速化するために、さまざまな方法があります。

- "Deep Security予約タスクの設定" on page 1826
- "コンピュータの追加または変更時にタスクを自動的に実行する(イベントベースのタスク)" on page 1829

- "AWSオートスケーリングとDeep Security" on page 1836
- "インストールスクリプトを使用したコンピュータの追加と保護" on page 1849
- "クラウドプロバイダーのタグ/ラベルを使用してポリシーを自動的に割り当てる" on page 1861
- "コマンドラインの基本" below

さらに、Deep Securityは、Spunk、QRadar、ArcSight、およびAmazon SNSなどのSIEMにイベントを転送する機能を提供します。詳細については、次のセクションを参照してください。

- "Deep SecurityイベントをSyslogまたはSIEMサーバに転送する" on page 1171
- "Amazon Simple Notification Serviceをセットアップする" on page 1238

Trend Micro Hybrid クラウドセキュリティコマンドラインインタフェース(THUS)

Trend Micro Hybrid Cloud Securityコマンドラインインタフェース(THUS) は、Deep Security環境の配信、設定、および管理を支援するツールです。インストールと設定が簡単です(すべて端末から) 。

Trend Micro Hybrid Cloud Securityコマンドラインインタフェースの設定の詳細については、「https://github.com/trendmicro/thus」を参照してください。

コマンドラインの基本

ローカルのコマンドラインインタフェース(CLI) を使用して、Deep Security AgentおよびDeep Security Managerに処理の実行を指示できます。また、CLIを使用して一部の設定を行ったり、システムリソースの使用状況情報を表示したりすることもできます。

さまざまなCLIコマンドをDeep Security APIを使用して自動化できます (Deep Security自動化への最初の手順を参照してください)。

- "dsa_control" on the next page
- "dsa_query" on page 1807
- "dsa_scan" on page 1810
- "dsm_c" on page 1814

dsa_control

dsa_controlを使用すると、Deep Security Agentの一部の設定を行い、有効化、不正プログラム対策検索、ベースラインの再構築などの処理を手動で実行できます。

Windows OSでセルフプロテクションが有効になっている場合、ローカルユーザはDeep Security Agentのアンインストール、アップデート、停止などの操作を行うことができません。また、CLIコマンドの実行時に認証パスワードを指定する必要があります。

dsa_controlは英語の文字列のみをサポートします。Unicodeはサポートされていません。

dsa_controlを使用するには

Windowsの場合:

1. 管理者としてコマンドプロンプトを開きます。
2. Deep Security Agentのインストールディレクトリに移動します。例:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Agent\
   ```

3. dsa_controlコマンドを実行します。

   ```
   dsa_control <option>
   ```

   ここで、<オプション>は、"dsa_control options" on the next pageで説明されているオプションのいずれかに置き換えられます。

Linux、AIX、およびSolarisの場合:

- sudo /opt/ds_agent/dsa_control <option>

  ここで、<option> は、"dsa_control options" on the next page

複数のdsa_controlコマンドを実行すると、新しいコマンドによって以前のコマンドが上書きされることがあります。複数のコマンドを実行する場合は、パラメータを並べて指定する必要があります。例: dsa_control -m "RecommendationScan:true" "UpdateComponent:true"

通常、Deep Security Agentタスクの管理には、[予約タスク] UI ([管理]→[予約タスク]) を使用することをお勧めします。詳細については、"Deep Security予約タスクの設定" on page 1826を参照してください。

dsa_control options

`dsa_control [-a <str>] [-b] [-c <str>] [-d] [-g <str>] [-s <num>] [-m] [-p <str>] [-r] [-R <str>] [-t <num>] [-u <str>:<str>] [-w <str>:<str>] [-x dsm_proxy://<str>] [-y relay_proxy://<str>] [--buildBaseline] [--scanForChanges] [Additional keyword:value data to send to manager during activation or heartbeat...]`

パラメータ	説明
`-a <str>, --activate=<str>`	次の形式で指定されたURLのManagerに対して、Agentを有効化します。 `dsm://<host>:<port>/` 指定する項目は次のとおりです。 • `<host>` にはManagerの完全修飾ドメイン名 (FQDN)、IPv4アドレス、またはIPv6アドレスを入力します。 • `<port>` は、管理者が待機しているポート番号です。 オプションで、引数の後に、アクティベーション時に送信する説明などの設定を指定することもできます。「"Agentからのハートビート有効化コマンド(「dsa_control -m」)" on page 1799」を参照してください。これらは、区切り文字としてコロンを使用して、key:valueのペアとして入力する必要があります。入力できるキーと値のペアの数に制限はありませんが、キーと値のペアはスペースで区切る必要があります。スペースや特殊文字が含まれる場合は、key:valueのペアを引用符で囲む必要があります。
`-b, --bundle`	アップデートバンドルを作成します。
`-c <str>, --cert=<str>`	証明書ファイルを特定します。
`-d, --diag`	エージェントパッケージを生成します。詳細については、「"保護されているコンピュータでCLIを使用してAgentの診断パッケージを作成する" on page 2022」を参照してください。
`-g <str>, --agent=<str>`	AgentのURLです。初期設定: `https://localhost:<port>/` にはManagerの待機ポート番号を入力します。

パラメータ	説明
-m, --heartbeat	Agentを今すぐ強制的にManagerに接続します。
-p <str> or --passwd=<str>	以前にDeep Security Managerで設定した認証パスワード。詳細については、「"Deep Security Managerを介してセルフプロテクションを設定する" on page 1518」を参照してください。パスワードが設定されている場合は、dsa_control -a 、dsa_control -x 、およびdsa_control -yを除くすべてのdsa_controlコマンドにパスワードを含める必要があります。 例: dsa_control -m -p MyPa$$w0rd パスワードは、コマンドラインに直接入力した場合、画面上に表示されます。入力中のパスワードをアスタリスク(*) にして非表示にする場合は、対話形式のコマンド-p *を入力します。この場合、パスワードの入力を求めるプロンプトが表示されます。 例: dsa_control -m -p *
-r, --reset	Agentの設定をリセットします。これにより、Agentから有効化情報が削除され、エージェントが無効化されます。
-R <str>, --restore=<str>	隔離ファイルを復元します。Windows版では、駆除したファイルや削除したファイルも復元できます。
-s <num>, --selfprotect=<num>	Agentの自己保護を有効にします (1: 有効、0: 無効)。自己保護機能により、ローカルのエンドユーザはAgentをアンインストール、停止、または制御できなくなります。詳細については、「"エージェントセルフプロテクションを有効化または無効化する" on page 1517」を参照してください。これはWindowsのみの機能です。 dsa_controlでは自己保護を有効にできますが、関連付けられた認証パスワードを設定することはできません。そのためにはDeep Security Managerが必要です。詳細については、「"Deep Security Managerを介してセルフプロテクションを設定する" on page 1518」を参照してください。設定したら、コマンドラインで-pまたは--passwd=オプションを使用してパスワードを入力する必要があります。 Deep Security 9.0以前では、このオプションは、-H <num>, --

パラメータ	説明
	harden=<num>でした。
-t <num>, --retries=<num>	dsa_controlエージェントサービスに接続して付随する指示を実行できない場合、このパラメータはdsa_controlに<num>回再試行するよう指示します。再試行の間には1秒の一時停止があります。
-u <user>:<password>	プロキシで認証が必要な場合は、-x オプションとともにプロキシのユーザ名とパスワードを指定します。ユーザ名とパスワードは、コロン(:)で区切ります。例：# ./dsa_control -x dsm_proxy://<str> -u <new username>:<new password>。 ユーザ名とパスワードを削除するには、空の文字列("") を入力します。例：# ./dsa_control -x dsm_proxy://<str> -u <existing username>:""。 プロキシのユーザ名のみを変更せずにプロキシのパスワードのみをアップデートする場合は、-xなしで -u オプションを使用できます。例：# ./dsa_control -u <existing username>:<new password>。 基本認証のみ。Digest認証とNTLM認証はサポートされていません。 dsa_control -uの使用は、エージェントのローカル設定にのみ適用されます。このコマンドを実行しても、マネージャのセキュリティポリシーは変更されません。
-w <user>:<password>	プロキシで認証が必要な場合は、-y オプションとともにプロキシのユーザ名とパスワードを指定します。ユーザ名とパスワードは、コロン(:)で区切ります。例：# ./dsa_control -y relay_proxy://<str> -w <new username>:<new password> 。 ユーザ名とパスワードを削除するには、空の文字列("") を入力します。例：# ./dsa_control -y relay_proxy://<str> -w <existing username>:""。 プロキシのユーザ名のみを変更せずにプロキシのパスワードのみをアップデートする場合は、-yなしで -w オプションを使用できます。例：# ./dsa_control -w <existing username>:<new password>。 基本認証のみ。Digest認証とNTLM認証はサポートされていません。 dsa_control -wの使用は、エージェントのローカル設定にのみ適用されることに注意してください。このコマンドを実行しても、マネージャのセキュリ

パラメータ	説明
	ティポリシーは変更されません。
-x dsm_proxy://<str>:<num>	エージェントとマネージャの間にプロキシを設定します。プロキシのIPv4 / IPv6アドレスまたはFQDNおよびポート番号をコロンで区切って指定します。(:).IPv6アドレスは角カッコで囲む必要があります。例：dsa_control -x "dsm_proxy://[fe80::340a:7671:64e7:14cc]:808/"。URLの代わりにアドレスを削除するには、空の文字列 ("").を入力します。 -uオプションも参照してください。 詳細については、"Deep Security Managerにプロキシ経由で接続する" on page 1458。 dsa_control -xの使用は、エージェントのローカル設定にのみ適用されることに注意してください。このコマンドを実行しても、マネージャのセキュリティポリシーは変更されません。
-y relay_proxy://<str>:<num>	エージェントとリレーの間にプロキシを設定します。プロキシのIPアドレスまたはFQDNとポート番号をコロンで区切って指定します。(:).IPv6アドレスは角カッコで囲む必要があります。例：dsa_control -y "relay_proxy://[fe80::340a:7671:64e7:14cc]:808/"。URLの代わりにアドレスを削除するには、空の文字列 ("").を入力します。 -wオプションも参照してください。 詳細については、"プロキシ経由でDeep Securityリレーに接続する" on page 1459) を参照してください。 dsa_control -yの使用は、エージェントのローカル設定にのみ適用されることに注意してください。このコマンドを実行しても、マネージャのセキュリティポリシーは変更されません。
--buildBaseline	変更監視のベースラインを作成します。
--scanForChanges	変更監視の変更を検索します。
--max-dsm-retries	有効化を再試行する最大回数。0から100までの値を入力してください。初期設定値は30です。
--dsm-retry-interval	有効化を再試行する間隔 (秒)。1から3600までの値を入力してください初期設定値は300です。

Agentからのリモート有効化 (「dsa_control -a」)

Agentからのリモート有効化 (AIA) を有効にすると、ManagerとAgent間の通信の問題を防ぐことができます。また、インストールスクリプトと共に使用すると、Agentのインストールを簡略化できます。

AIAを設定し、インストールスクリプトを使用してAgentを有効化する方法については、"Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511を参照してください。

コマンドの形式は次のとおりです。

```
dsa_control -a dsm://<host>:<port>/
```

指定する項目は次のとおりです。

- `<host>` にはManagerの完全修飾ドメイン名 (FQDN)、IPv4アドレス、またはIPv6アドレスを入力します。
- `<port>` は、エージェント間の通信 ポート番号 (初期設定では4120) です。

次に例を示します。

```
dsa_control -a dsm://dsm.example.com:4120/ hostname:www12 "description:Long Description With Spaces"
```

```
dsa_control -a dsm://fe80::ad4a:af37:17cf:8937:4120
```

Agentからのハートビート有効化コマンド(「dsa_control -m」)

AgentからManagerに、ハートビートをただちに強制送信することができます。

有効化コマンドと同様、ハートビート有効化コマンドでも、実行中に設定をManagerに送信することができます。

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
AntiMalwareCancelManualScan	ブール。 コンピュータ上で実行されている手動検索をキャ	"AntiMalwareCancelManualScan:true"	不可	可

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
	ンセルします。			
AntiMalwareManualScan	ブール。 コンピュータに対して手動の不正プログラム検索を開始します。	"AntiMalwareManualScan:true"	不可	可
description	文字列。 コンピュータの説明を設定します。最大2000文字。	"description:Extra information about the host"	可	可
displayname	文字列。 [コンピュータ] のホスト名の横にカッコで囲んで表示される表示名を設定します。最大2000文字。	"displayname:the_name"	可	可
externalid	整数。 externalid値を設定します。この値を使用して、Agentを一意に識別できます。この値には、従来のSOAP Webサービス API を使用してアクセスできます。	"externalid:123"	可	可
group	文字列。	"group:Zone A web servers"	可	可

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
	[コンピュータ] 画面に表示される、コンピュータの属するグループを設定します。1つの階層レベルの1つのグループ名につき最大254文字。 スラッシュ(「/」)はグループの階層を示します。groupパラメータはグループの階層を読み取ったり、作成したりできます。 このパラメータは、メインの「コンピュータ」ルートブランチの下位にある標準のグループにコンピュータを追加する場合にのみ使用できます。ディレクトリ(Microsoft Active Directory)、VMware vCenter、またはクラウドプロバイダのアカウントに所属するグループに			

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
	コンピュータを追加する場合には使用できません。			
groupid	整数。	"groupid:33"	可	可
hostname	文字列。 最大254文字。 ManagerがAgentに接続する際に使用するIPアドレス、ホスト名、またはFQDNを指定します。	"hostname:www1"	可	不可
IntegrityScan	ブール。 コンピュータで変更の検索を開始します。	"IntegrityScan:true"	不可	可
policy	文字列。 最大長は254文字です。 ポリシー名は、大文字と小文字を区別せずにポリシーリストに一致します。ポリシーが見つからない場合、ポリシーは割り当てられていません。	"policy:Policy Name"	可	可

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
	イベントベースのタスクによって割り当てられたポリシーは、Agentからの有効化中に割り当てられたポリシーよりも優先されます。			
policyid	整数。	"policyid:12"	可	可
relaygroup	文字列。 コンピュータを特定のRelayグループにリンクします。最大長は254文字です。 Relayグループ名は、既存のRelayグループ名と大文字と小文字が区別されません。Relayグループが見つからない場合は、初期設定のRelayグループが使用されます。 イベントベースのタスクで割り当てられたRelayグループには影響しません。このオプションまたはイ	"relaygroup:Custom Relay Group"	可	可

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
	ベントベースのタスクのいずれかを使用します。両方を使用することはできません。			
relaygroupid	整数。	"relaygroupid:123"	可	可
relayid	整数。	"relayid:123"	可	可
tenantIDとtoken	文字列。 Agentからのリモート有効化をテナントとして使用する場合は、tenantIDとtokenの両方が必要です。tenantIDとtokenはインストールスクリプト生成ツールから取得できます。	"tenantID:12651ADC-D4D5" and "token:8601626D-56EE"	可	可
RecommendationScan	ブール。 コンピュータで推奨設定の検索を開始します。	"RecommendationScan:true"	不可	可
UpdateComponent	ブール。 セキュリティアップデートの実行をDeep Security Managerに指示します。 Deep Security Agent 12.0以降	"UpdateComponent:true"	不可	可

パラメータ	説明	例	有効化中の使用	ハートビート中の使用
	でUpdateComponentパラメータを使用する場合は、Deep Security Relayもバージョン12.0以降であることを確認してください。詳細を表示。			
RebuildBaseline	ブール。 コンピュータに変更監視ベースラインを再構築します。	"RebuildBaseline:true"	不可	可
UpdateConfiguration	ブール。 「ポリシーの送信」操作を実行するようDeep Security Managerに指示します。	"UpdateConfiguration:true"	不可	可

Deep Security Agentの有効化

Agentをコマンドラインから有効化するには、テナントIDとパスワードが必要です。これらの情報はインストールスクリプトで確認できます。

1. Deep Security Managerの画面右上で、[サポート情報]→[インストールスクリプト] の順にクリックします。
2. プラットフォームを選択します。
3. [インストール後にAgentを自動的に有効化] を選択します。
4. インストールスクリプトで、tenantIDとtokenの文字列を探します。

Windows

PowerShellの場合:

```
& $Env:ProgramFiles"\Trend Micro\Deep Security Agent\dsa_control" -a <manager URL> <tenant ID> <token>
```

cmd.exeの場合:

```
C:\Windows\system32>"\Program Files\Trend Micro\Deep Security Agent\dsa_control" -a <manager URL> <tenant ID> <token>
```

Linux、AIX、およびSolaris

```
/opt/ds_agent/dsa_control -a <manager URL> <tenant ID> <token>
```

Agentからのハートビート有効化コマンド

Windows

PowerShellの場合:

```
& "\Program Files\Trend Micro\Deep Security Agent\dsa_control" -m
```

cmd.exeの場合:

```
C:\Windows\system32>"\Program Files\Trend Micro\Deep Security Agent\dsa_control" -m
```

Linux、AIX、およびSolaris

```
/opt/ds_agent/dsa_control -m
```

不正プログラムの手動検索を開始する

Windows

1. 管理者権限でコマンドプロンプト(cmd.exe)を開きます。
2. 次のコマンドを入力します。

   ```
   cd C:\Program Files\Trend Micro\Deep Security Agent\
   ```

   ```
   dsa_control -m "AntiMalwareManualScan:true"
   ```

Linux、AIX、およびSolaris

```
/opt/ds_agent/dsa_control -m "AntiMalwareManualScan:true"
```

診断パッケージを作成する

Deep Security Agentに関する問題のトラブルシューティングを行う必要がある場合に、コンピュータの診断パッケージを作成して送信するよう、サポート担当者から求められることがあります。詳細な手順については、"保護されているコンピュータでCLIを使用してAgentの診断パッケージを作成する" on page 2022を参照してください。

Deep Security Agentコンピュータの診断パッケージはDeep Security Manager経由で作成できますが、エージェントコンピュータが Agent / Appliance Initiated コミュニケーションを使用するように設定されている場合、Managerは必要なログをすべて収集できません。そのため、テクニカルサポートから診断パッケージを要求された場合は、該当するAgentコンピュータで直接コマンドを実行する必要があります。

Agentをリセットする

このコマンドは、対象エージェントから有効化情報を削除し、対象エージェントを無効化します。

Windows

PowerShellの場合:

```
& "\Program Files\Trend Micro\Deep Security Agent\dsa_control" -r
```

cmd.exeの場合:

```
C:\Windows\system32>"\Program Files\Trend Micro\Deep Security Agent\dsa_control" -r
```

Linux、AIX、およびSolaris

```
/opt/ds_agent/dsa_control -r
```

dsa_query

エージェント情報を表示するには、`dsa_query` コマンドを使用できます。

dsa_queryのオプション

```
dsa_query [-c <str>] [-p <str>] [-r <str]
```

パラメータ	説明
-p,--passwd <string>	オプションのAgentセルフプロテクション機能で使用される認証パスワードです。セルフプロテクションを有効化した際にパスワードを指定した場合は必須となります。 一部のクエリコマンドでは、認証を直接バイパスできます。この場合、パスワードは必要ありません。
-c,--cmd <string>	Agentに対してクエリコマンドを実行します。次のコマンドがサポートされます。 • "GetHostInfo": ハートビート中にManagerに返されるIDを照会します。 • "GetAgentStatus": どの保護モジュールが有効になっているかを検索します. 不正プログラム対策 または 変更監視 検索のステータスおよびその他のその他の情報 • "GetComponentInfo": 不正プログラム対策のパターンおよびエンジンのバージョン情報を照会します。 • "GetPluginVersion": Agentと保護モジュールのバージョン情報を照会します。 • 「GetProxyInfo」: すべてのプロキシタイプのプロキシ情報をクエリします。
-r,--raw <string>	"-c"と同じクエリコマンドの情報を返しますが、サードパーティのソフトウェアで解釈できるように未加工のデータ形式で出力します。
pattern	1. 結果をフィルタするためのワイルドカードのパターンです(オプション)。 例: dsa_query -c "GetComponentInfo" -r "au" "AM*" 1. より詳細なコンテンツを印刷するオプションとして。 例: dsa_query -c GetProxyInfo details=true

CPU使用率とRAM使用量を確認する

Windows

タスクマネージャーまたはprocmonを使用します。

LinuxおよびSolaris

top

AIX

topas

ds_agentプロセスまたはサービスが実行されていることを確認する

Windows

タスクマネージャーまたはprocmonを使用します。

Linux、AIX、およびSolaris

ps -ef|grep ds_agent

LinuxでAgentを再起動する

service ds_agent restart

または

/etc/init.d/ds_agent restart

または

systemctl restart ds_agent

一部の処理には-tenantnameパラメータまたは-tenantidパラメータのいずれかが必要です。テナント名を使用すると実行エラーが発生する場合は、関連付けられたテナントIDを使用してコマンドを再度実行します。

Solarisでエージェントを再起動する

svcadm restart ds_agent

AIXでエージェントを再起動する

stop agent: stopsrc -s ds_agent

start agent: startsrc -s ds_agent

dsa_scan

Windowsの管理者権限またはLinuxのルートアクセス権限を持っている場合は、dsa_scanコマンドを使用して、指定したファイルまたはディレクトリ(サブディレクトリを含む)で検索タスクを実行できます。

dsa_scanでは、最大10個のDeep Security Agentインスタンスを同時に実行できます。

このコマンドは、対象と除外の設定に関するAgentの現在の検索ポリシーを無視します([ポリシー]→[不正プログラム対策]→[対象]→[手動]および[ポリシー]→[不正プログラム対策]→[除外]→[手動])。

dsa_scanを使用するには

Windowsの場合:

1. 管理者としてコマンドプロンプトを開きます。
2. エージェントのインストールディレクトリに移動します。
   cd C:\Program Files\Trend Micro\Deep Security Agent\
3. dsa_scanコマンドを実行します。
   dsa_scan <option>
   どこで<option> "dsa_scanのオプション" below。

Linuxでは、次のコマンドを実行します。

sudo /opt/ds_agent/dsa_scan <option>
どこで<option> "dsa_scanのオプション" below

dsa_scanコマンドは、macOSではサポートされていません。

dsa_scanのオプション

dsa_scan [--target <str>] [--action <str>] [--log <str>]

パラメータ	説明
--target	区切り文字「|」を含むファイルパスまたはディレクトリ入力ファイルの絶対パスとディレクトリを区切ります。 ファイルパスとディレクトリの例: "c:\user data|c:\app\config.exe|c:\workapps" コマンドの例: dsa_scan --target "c:\user data|c:\app\config.exe|c:\workapps"

パラメータ	説明
--action	任意 サポートされている処理は、パス、削除、隔離です。 パラメータ処理が指定されていない場合は、[手動検索設定]の現在のエージェント検索処理が適用されます。 例: dsa_scan --action delete --target "c:\user data|c:\app\config.exe"
--log	任意 出力ログファイルの絶対ファイルパス。 このオプションが指定されていない場合、検索結果はコマンドラインコンソールに出力されます。 出力ファイルの例: "c:\temp\scan.log" コマンドの例: dsa_scan --target "c:\users\" --log "c:\temp\scan.log"
--scanLargeFile	オプション 大きなファイルのスキャンを有効にする。 ウイルスを含む大きなファイルが検出されると、スキャンは[Infected]とパスアクションを返します。 圧縮ファイルに含まれる大きなファイルはスキャンできませんのでご注意ください。 例 コマンド: dsa_scan --target "c:\user data|c:\app\config.exe" --scanLargeFile

dsa_scanの出力

次の表に、dsa_scanコマンドの実行後に表示される検索ステータスラベルを示します。

ラベル	説明
スキップ	検索ファイルのサイズが上限に達しました。

ラベル	説明
感染	ファイルが検索エンジンによって検出され、処理が実行されました。
警告	ファイルは検索エンジンによって検出されましたが、実行された処理で問題が発生しました。 エラーコードを確認してください。

次に、検索出力の例を示します。

```
DSA on-demand scan utility

System date/time: 2023/10/12 16:04:10

trace id: 7acf6855-8547-46fc-a58f-9218d108e727

Scanning...

[Skipped] Path: /home/user1/Documents/oversize.zip

[Skipped] Path: /home/user1/Documents/xxx.big

[Infected] Path: /home/user1/Documents/readme, Action: Passed, Malware Name: EICAR, QuarantineID: 0, Error code: 0

[Infected] Path: /home/user1/Documents/sales.doc, Action: Cleaned, Malware Name: BRAIN.A, QuarantineID: 0, Error code: 0

[Warning] Path: /home/user1/Documents/po.ppt, Action: Quarantine, Malware Name: RANSOM.A, QuarantineID: 0, Error code: 5

[Infected] Path: /home/user1/Documents/shipment.zip(po.exe), Action: Deleted, Spyware Name: BLKFRI.A, QuarantineID: 0, Error code: 0

25 files scanned, 2 skipped in 10 seconds.

4 files out of 25 were infected.

End of Scan.
```

終了コードの検索

`dsa_scan`コマンドの終了コードは、検索の成功または失敗を示します。

成功の終了コード

成功終了コードは、次の表に示すように、dsa_scanユーティリティが問題やウイルスを検出せず、またはファイルをスキップせずに検索タスクを完了したことを示します。

終了コード	説明	解決方法
0	検索が完了し、不正プログラムは検出されませんでした。	不正プログラムが検出されずに検索タスクが完了しました。
1	不正プログラムが1つ以上検出され、検索が完了しました。	出力で[感染]および[警告]のラベルが付いた行を確認します。
2	検索が完了しました。不正プログラムは検出されませんでしたが、一部のファイルがスキップされました。	出力で[スキップ]と表示されている行を確認します。
3	検索は完了しましたが、不正プログラムが検出され、一部のファイルがスキップされました。	出力で「感染」、「警告」、および「スキップ」のラベルが付いた行を確認します。

致命的な終了コード

dsa_scanユーティリティで致命的なエラーが発生した場合、dsa_scanは検索タスクを中断し、次の表に示すエラーコードを表示して終了します。

終了コード	説明	解決方法
246	引数文字列が長すぎます。	文字列のサイズ制限は2048文字です。 対象パラメータを短くして、再度実行してください。
247	Security Platformをシャットダウンしています。	エージェントを停止しています。しばらくしてからもう一度お試しください。
248	インスタンスが多すぎます。	dsa_scanを同時に実行できるインスタンスは10を超えることはできません。 インスタンスの数を減らします。
249	権限がありません。	このコマンドには、Linuxではrootが、WindowsではAdministratorが必要です。 検索ポリシーで、[Agentによる手動検索の開始またはキャンセルを許可する]を有効にします。
250	手動検索設定が設定されていません。	検索ポリシーで手動検索を設定します。

終了コード	説明	解決方法
251	AM機能が有効になっていません。	検索ポリシーでAM機能を有効にします。
252	このプラットフォームはサポートされていません。	dsa_scanは、現在のOSプラットフォームではサポートされていません。
253	Agentが実行されていません。	Deep Security Agentが実行されていません。 エージェントを有効にするか、管理者に問い合わせてください。
254	パラメータが無効です。	入力パラメータが正しくありません。
255	予期しないエラーです。	しばらくしてからもう一度お試しください。問題が解決しない場合は、管理者に問い合わせてください。

dsm_c

dsm_cコマンドを使用して、Managerの一部の設定を行ったり、ユーザアカウントのロックを解除したりできます。

注意: 一部のコマンドを実行すると、Deep Security Managerが再起動することがあります。コマンドの実行後、Deep Security Managerが再起動されていることを確認します。

dsm_cオプション

dsm_c -action *actionname*

コマンドのヘルプを表示するには、-hオプションを使用します。dsm_c -h

一部の処理では、-tenantnameパラメータまたは-tenantidパラメータのいずれかが必要です。テナント名の使用時に問題が発生した場合は、関連付けられたテナントIDを使用してコマンドを実行してください。次の表で括弧で囲まれたパラメータはすべて必須です。

処理名	説明	使用方法
addazureendpoint	Azureエンドポイントを許可されたエ	dsm_c -action addazureendpoint -endpoint ENDPOINT

処理名	説明	使用方法
	ンドポイントリストに追加します。このコマンドには ENDPOINT パラメータが必要です。このパラメータは、https://<fqdn> の形式で指定する必要があります。許可されたエンドポイントリストは、Deep Security ManagerにAzureアカウントを追加する際に指定されたエンドポイントの検証に使用されます。エンドポイントを指定しない場合、初期設定の組み込みエンドポイントのみが許可されます。 Azureアカウントの追加については、"Deep SecurityへのMicrosoft Azureアカウントの追加" on page 688 関連するdsm_cオプション: listazureendpoint removeazureendpoint	

処理名	説明	使用方法
addcert	信頼済み証明書を追加します。	dsm_c -action addcert -purpose PURPOSE -cert CERT
addregion	プライベートクラウドプロバイダのリージョンを追加します。	dsm_c -action addregion -region REGION -display DISPLAY -endpoint ENDPOINT
changesetting	設定を変更します。 コマンドを実行する前に、デプロイメントをバックアップする必要があります。設定の影響を理解していない場合は、このコマンドを使用しないでください。設定に誤りがあると、サービスが使用できなくなったり、データを読み取れなくなったりする可能性があります。通常、このコマンドは、テクニカルサポートプロバイダから変更する設定NAMEを指示された場合にのみ使用します。通常の使用時にこのコマンドが必要になる場合があります。その場合の設定については、masterkeyなど、ドキュメントの	dsm_c -action changesetting -name NAME [-value VALUE | -valuefile FILENAME] [-computerid COMPUTERID] [-computername COMPUTERNAME] [-policyid POLICYID] [-policyname POLICYNAME] [-tenantname TENANTNAME | -tenantid TENANTID]

処理名	説明	使用方法
	該当するセクションで説明されています。	
createinsertstatements	別のデータベースへのエクスポートに使用するinsert文を作成します。	dsm_c -action createinsertstatements [-file FILEPATH] [-generateDDL] [-databaseType sqlserver|oracle] [-maxresultfromdb count] [-tenantname TENANTNAME | -tenantid TENANTID]
diagnostic	システム用の診断パッケージを作成します。 必要に応じて、"詳細な診断パッケージのプロセスメモリを増やす" on page 2024ことができます。	dsm_c -action diagnostic [-verbose 0|1] [-tenantname TENANTNAME | -tenantid TENANTID]
disablefipsmode	FIPSモードを無効にします。	dsm_c -action disablefipsmode
enablefipsmode	FIPSモードを有効にします。	dsm_c -action enablefipsmode
fullaccess	管理者にFull Accessの役割を与えます。	dsm_c -action fullaccess -username USERNAME [-tenantname TENANTNAME | -tenantid TENANTID]
listazureendpoint	許可されているAzureエンドポイントをすべてリストします。 関連するdsm_cオプション: addazureendpoint removeazureendpo	dsm_c -action listazureendpoint

処理名	説明	使用方法
	int	
listcerts	信頼済み証明書を一覧表示します。	dsm_c -action listcerts [-purpose PURPOSE]
listregions	プライベートクラウドプロバイダのリージョンを一覧表示します。	dsm_c -action listregions
masterkey	カスタムのマスターキーを生成、インポート、エクスポート、または使用して、以下を暗号化します。 • データベースのパスワード • Keystoreパスワード • 個人データ カスタムマスターキーが設定されていない場合、Deep Securityではハードコードされたシードが使用されます。	新規インストールの実行中にすでにマスターキーを設定している場合は、このセットアップは完了です。マスターキーの作成をスキップして、今すぐ設定する場合は、手順1のコマンドから開始してください。すべてのコマンドを順に入力します。新しいマスターキーを生成するには、手順1のコマンドから開始し、すべてのコマンドを順に入力します。 マスタ鍵、生成方法、および暗号化の詳細については、"Managerをインストールする" on page 460のインストールを参照してください。 アップグレード時にマスターキーを設定した場合は、データベースとプロパティファイルをバックアップして、手順4のコマンドから開始してください。 1. dsm_c -action masterkey -subaction [generatekmskey -arn AWSARN | generatelocalkey] - Key Management System (KMS) キーのAmazon Resource Name (ARN) か、LOCAL_KEY_SECRETローカル環境変数を使用して、マスターキーを生成します。マルチノードDeep Security Managerでローカル環境変数を使用する場合は、システムレベルのすべてのノードで設定する必要があります (ユーザレベルの), では使用できません。また、最低でも次を含める必要があります。

処理名	説明	使用方法
		• 大文字 • 小文字の手紙 • 数字 • 特殊文字 • 8〜64文字 マスターキーを設定する場合は、Deep Security ManagerでKMSまたはLOCAL_KEY_SECRETへの権限と信頼性の高いネットワークアクセスが必要です。Managerはこれらを使用して、使用時にマスターキーを暗号化および復号化します。一時的にアクセスできない場合、Deep Security Managerは必要なデータを復号化できず、サービスを使用できなくなります。症状には、再起動の失敗やその他のさまざまなエラーに関するイベントログやアラートが断続的に表示されることがあります。 2. dsm_c -action masterkey -subaction export -file FILEPATH - マスターキーをバックアップのために、パスワードで暗号化されたファイルにエクスポートします。パスワードが要求されます。 マスターキーは、安全な場所にエクスポートしてバックアップする必要があります。マスターキーを紛失または破損した場合、バックアップがないと、暗号化されたすべてのデータを読み取ることができなくなります。その場合は、Deep Security Manager、すべてのRelay、およびすべてのAgent/appliancesを再インストールする必要があります。キーが盗まれると、Deep Security環境のセキュリティが危険にさらされます。欧州の一般データ保護規則(GDPR)などの一部のコンプライアンス規制では、個人データの漏えいを72時間以内に法執行機関に通知することが法律で義務付け

処理名	説明	使用方法
		られている場合があり、違反した場合は罰金が科される可能性があります。詳細については、弁護士にご相談ください。 障害復旧を目的にバックアップを検証するには、マスターキーをインポートしてテストします。 `dsm_c -action masterkey -subaction [importkmskey -file FILEPATH -arn AWSARN | importlocalkey -file FILEPATH]` – マスターキーのバックアップをインポートします。これは、破損したキーのディザスタリカバリや、マスターキーを別のKMSに移行する場合に役立ちます。このコマンドを実行する前に、プライマリテナント(T0)データベースから既存のマスターキーを削除する必要があります。 たとえば、以下のSQLコマンドを入力します。 `delete from systemsettings where uniquekey = 'settings.configuration.keyEncryptingKey'` 3. `dsm_c -action masterkey -subaction encryptproperties` – マスター鍵を使用して、dsm.propertiesおよびconfiguration.propertiesのキーストアおよびデータベースのパスワードを暗号化します。この設定を有効にするには、Deep Security Managerを再起動する必要があります。 4. `dsm_c -action masterkey -subaction encrypttenantkey -tenantid [all | TENANTNUM]` – マルチテナント環境の場合は、マスターキーを使用して既存のテナントキーシードを暗号化します。テナントキーシードは、次の手順で使用できるサブキーを派生させます。このコマンドは複数回実行できます(すでに暗号化されているシードに追加の暗号化レイヤは適用されません)。

処理名	説明	使用方法
		必要に応じて、既存の各テナントに段階的にロールアウトしながら、新しいテナントにのみ暗号化を適用するには、次のコマンドを実行します。 `dsm_c -action changesetting -name settings.configuration.encryptTenantKeyForNewTenants -value true` 環境内に(プライマリ)テナントが1つしかない場合、tenantidはallまたは0のいずれかになります。 5. `dsm_c -action masterkey -subaction encryptpii -tenantid [all | TENANTNUM]` – マルチテナント環境の場合は、各テナントのキーを使用して、データベース内の管理者および連絡先の個人データを暗号化します。環境内に(プライマリ)テナントが1つしかない場合、tenantidはallまたは0のいずれかになります。 6. `dsm_c -action masterkey -subaction encryptdsmprivatekey -tenantid [all | TENANTNUM]` – マスターキーを使用して、SSL/TLSを介したアクティベーションおよびAgent/Manager間の通信に使用される秘密鍵を暗号化します。環境内に(プライマリ)テナントが1つしかない場合、tenantidはallまたは0のいずれかになります。 7. `dsm_c -action masterkey -subaction isconfigured` – マスターキーが作成されたかどうかを確認します。
`removeazureendpoint`	許可されたエンドポイントリストからAzureエンドポイントを削除します。 `dsm_c -action`	`dsm_c -action removeazureendpoint -endpoint ENDPOINT`

処理名	説明	使用方法
	addazureendpoint コマンドを使用して追加されたエンドポイントのみを削除できます。初期設定の組み込みエンドポイントは削除できません。 関連するdsm_cオプション: addazureendpoint listazureendpoint	
removecert	信頼済み証明書を削除します。	dsm_c -action removecert -id ID
removeregion	プライベートクラウドプロバイダのリージョンを削除します。	dsm_c -action removeregion -region REGION
resetcounters	カウンタテーブルをリセットして空の状態に戻します。	dsm_c -action resetcounters [-tenantname TENANTNAME | -tenantid TENANTID]
script	スクリプトファイル内にあるdsm_cコマンドのバッチ処理を実行します。	dsm_c -action script -scriptfile FILEPATH [-tenantname TENANTNAME | -tenantid TENANTID]
setports	Deep Security Manager ポートを設定します。	dsm_c -action setports [-managerPort port] [-heartbeatPort port]
trustdirectorycert	ディレクトリの証明書を信頼します。	dsm_c -action trustdirectorycert -directoryaddress DIRECTORYADDRESS -directoryport DIRECTORYPORT [-username USERNAME] [-password PASSWORD] [-tenantname TENANTNAME | -tenantid TENANTID]

処理名	説明	使用方法
unlockout	ユーザアカウントのロックを解除します。	dsm_c -action unlockout -username USERNAME [-newpassword NEWPASSWORD] [-disablemfa][-tenantname TENANTNAME | -tenantid TENANTID]
upgradetasks	インサービスアップグレードの一環として必要になる場合がある、アップグレードタスク処理を実行します。	dsm_c -action upgradetasks [-listtasksets] [-listtasks -taskset UPGRADE_TASK_SET [-force]] [-tenantlist] [-tenantsummary] [-run -taskset UPGRADE_TASK_SET [-force] [-filter REGULAR_EXPRESSION]] [-showrollbackinfo -task TASKNAME] [-purgehistory [-task TASKNAME]] [-showhistory [-task TASKNAME]] [-tenantname TENANTNAME | -tenantid TENANTID] • [-listtasksets]: システム全体またはテナント(-tenantnameで指定)用の一連のタスクを一覧表示します。 • [-listtasks -taskset UPGRADE_TASK_SET [-force]]: 実行する変更内容を一覧表示します。すべてのタスクを表示するには、-forceを指定します。 • [-tenantlist]: 指定したテナントの未解決アップグレード処理のバージョンを表示します。 • [-tenantsummary]: 最新ではないテナントの概要を表示します。 • [-run -taskset UPGRADE_TASK_SET [-force] [-filter REGX]]: 各テナントにアップグレード処理を実行します。実行済みであっても、すべてのタスクを実行する場合は、-forceを含めます。正規表現で処理を制限する場合は、-filterを含めます。 • [-showrollbackinfo -task TASKNAME]: 指定したタスクのロールバック情報を表示します。1つのテナントまたはすべてのテナントを表示できます。 • [-purgehistory [-task TASKNAME]]: 指定したテナントやタスクの履歴を削除します。テナント

処理名	説明	使用方法
		やタスクを指定しないと、すべての項目が対象になります。 • [-showhistory [-task TASKNAME]]: 指定したテナントやタスクの履歴を表示します。テナントやタスクを指定しないと、すべての項目が対象になります。
versionget	現在のソフトウェアバージョン、データベーススキーマバージョン、またはその両方に関する情報を表示します。	dsm_c -action versionget [-software] [-dbschema]
viewsetting	設定値を表示します。	dsm_c -action viewsetting -name NAME [-computerid COMPUTERID] [-computername COMPUTERNAME] [-policyid POLICYID] [-policyname POLICYNAME] [-tenantname TENANTNAME | -tenantid TENANTID]

リターンコード

dsm_cコマンドは、コマンドが正常に実行されたかどうかを示す整数値を返します。次の値が返されます。

- 0 : 正常に実行されました。
- -1 : ソフトウェアのインストールの破損など、原因不明のエラー。
- 1 : データベースに現在アクセスできないなど、実行中にエラーが発生しました。
- 2 : 無効な引数が指定されました。

Deep Security APIを使用したタスクの自動化

Deep Security 11.1以降には、Deep Securityを使用したセキュリティのプロビジョニングとメンテナンスを自動化できる新しいRESTful APIが追加されています。Deep Security Automation Centerにアクセスし、任意の言語でSDKをダウンロードして、APIの使用方法を次の資料で確認します。

- APIリファレンス
- 豊富なコード例が記載されたタスク中心のガイド
- サポートリソース

このAPIは継続的にアップデートされ、新しい機能や改良が加えられています。新しいAPIが自動化のニーズに合っている場合は、新しい自動化プロジェクトを開始する際に、今後も継続的なサポートとメンテナンスを長期にわたって受けられるこのAPIを使用することをお勧めします。

このAPIの使用を開始するには、Deep Security Automation Centerにあるガイド「First Steps Toward Deep Security Automation」を参照してください。

従来のREST APIおよびSOAP API

注意: Deep Security 11.1より前に提供されたREST APIおよびSOAP APIは変更されていません。これらはすでに非推奨となっているため、新しい機能は追加されませんが、既存のAPI機能は引き続き通常どおりに機能します。

Deep Securityには引き続き従来のREST APIおよびSOAP APIも含まれています。これらのAPIの使用方法については、Deep Security Automation Centerにある次のガイドを参照してください。

- Transition from the SOAP API
- Use the Legacy REST API

以降のセクションでは、SOAP APIおよびREST APIの使用に関連するタスクをDeep Security Managerで完了する方法について説明します。どのような場合にこれらのタスクを実行する必要があるかについては、上記のガイドを参照してください。

ステータス監視APIを有効にする(オプション)

従来のREST APIでステータス監視を使用するには、このAPIを有効にする必要があります。このAPIは認証を必要としないため、初期設定では無効になっています。

1. Deep Security Managerで、[管理]→[システム設定]→[高度な]の順に選択します。
2. [ステータス監視API] セクションで、[有効] を選択し、[保存] をクリックします。

Webサービスユーザアカウントを作成する

Webサービスアクセス専用の役割を作成し、新しいユーザに割り当てます。

1. Deep Security Managerで、管理 > ユーザ管理 > ロールに移動します。
2. [新規] をクリックします。
3. [Deep Security Managerユーザインタフェースへのアクセスを許可] チェックボックスをオフにし、[WebサービスAPIへのアクセスを許可] チェックボックスをオンにします。
4. 他の設定がすべて完了したら、[保存] をクリックします。
5. [管理]→[ユーザ管理]→[ユーザ] に進み、[新規] をクリックします。
6. WebサービスAPIでのみ使用する新しいユーザを作成します。先に作成した新しい役割をこのユーザに割り当てます。
   新しいユーザアカウントのユーザ名とパスワードを書き留めてください。

Deep Security予約タスクの設定

Deep Securityには、定期的に自動実行すると便利なタスクが多数あります。予約タスクは、お客様の環境にDeep Securityをインストールする時はもちろん、インストール後にシステムを最新の状態に保ち、スムーズに運用するうえでも便利です。特に、オフピーク時の定期的な検索には予約タスクが役立ちます。

ヒント: Deep Security APIを使用して予約タスクの作成と設定を自動化できます。例については、Deep Security Automation Centerの予約タスクを使用した保護の維持ガイドを参照してください。

予約タスクを作成する

Deep Security Managerで予約タスクをセットアップするには、[管理]→[予約タスク]→[新規] をクリックします。「新規予約タスクウィザード」が表示されます。このウィザードの手順に従って予約タスクを作成できます。

セキュリティアップデートの確認: セキュリティアップデートを定期的に確認し、使用可能なアップデートがある場合、Deep Securityにインポートします。ほとんどの組織にとって、このタスクは毎日1回実行するのが理想的です。

注意: Deep Security 11.0 Update 2以降を使用している場合、[セキュリティアップデートの確認] タスクは、30日以上通信がないオフラインホストを無視します。

ソフトウェアアップデートの確認: Deep Security Agentソフトウェアアップデートを定期的に確認し、使用可能なアップデートがある場合、ダウンロードします。

コンピュータの検出: 検出操作を予約することによって、ネットワーク上の新しいコンピュータを定期的に確認します。確認するIP範囲を入力し、コンピュータの追加先となるコンピュータグループを指定するよう求められます。このタスクは、クラウドコネクタに含まれていないコンピュータを検出するのに便利です。

レポートの生成および送信: レポートを自動生成し、オプションでユーザのリストへ送信します。

コンピュータの変更を検索: Deep Security Managerで変更の検索が実行され、コンピュータの現在の状態とベースラインが比較されます。

コンピュータの不正プログラムを検索: 不正プログラム検索の予定を作成します。検索の設定は、各コンピュータのポリシーエディタまたはコンピュータエディタの[不正プログラム対策]画面で行います。ほとんどの組織にとって、このタスクは週に1回 (または組織のポリシーに従って) 実行するのが理想的です。このタスクを設定する際に、検索のタイムアウト値を指定できます。タイムアウトオプションは、毎日、毎週、毎月、および1回のみの検索に使用できます。毎時の検索には使用できません。予約された不正プログラム検索が実行されているときにタイムアウト制限に達すると、現在実行中または保留中のタスクがキャンセルされます。

ヒント: [コンピュータの不正プログラムを検索] タスクがタイムアウトすると、次の予約検索は (前回の検索が終了したところから再開されるのではなく) 最初から開始されます。検索を完了することが目的であるため、検索が頻繁にタイムアウト値に達する場合は、設定を変更することをお勧めします。不正プログラム検索設定を変更して、例外を追加したり、タイムアウト値を延長したりできます。

コンピュータのオープンポートを検索: 1つ以上のコンピュータに対して定期的なポート検索を予約します。検索対象には、個別のコンピュータまたは特定のコンピュータグループに所属するすべてのコンピュータを指定できます。Deep Security Managerは、[ポリシー]または[コンピュータエディタ]→[設定]画面の[検索]タブで定義されたポート番号を検索します。

コンピュータの推奨設定を検索: Deep Security Managerによって、コンピュータ上の一般的なアプリケーションが検索され、検出結果に基づいた推奨設定が作成されます。定期的に推奨設定の検索を実行すると、関連する最新のルールセットによってコンピュータが保護され、不要になったルールは削除されます。推奨設定の検索をサポートする3つの各保護モジュールに対して「推奨設定を自動的に適用」オプションを設定すると、必要なルールの割り当てと割り当ての解除がDeep Securityによって行われます。特別な注意が必要なルールについては、その内容を通知するアラートが発令されます。ほとんどの組織にとって、このタスクは週に1回実行するのが理想的です。

注意: 推奨設定の検索はCPU負荷が高くなることがあります。このため、推奨設定の検索を予約する場合は、タスクをグループ別に設定し (たとえば、ポリシーごとやコンピュータグループ別、ただしグループあたりのマシン台数が1,000台を超えないようにする)、タスクを各曜日に振り分ける (たとえば、データベースサーバ検索を毎週月曜日に予約し、メールサーバ検索を毎週火曜日に予約するなど)

ことが推奨されます。頻繁に変更されるシステムの場合、より頻繁に推奨設定の検索を実行するように設定してください。

Agentアップグレードの予約タスク: Agentのアップグレードを予約します。Agentアップグレードのベストプラクティス を参照すると、Agentのアップグレードに最適なスケジュールを決定できます。

ヒント: このタスクを設定して、エージェントを最新バージョンにアップグレードすることも、その前の2つのバージョンのいずれかにアップグレードすることもできます。エージェントのアップグレード先の正確なバージョンは、予約タスクの実行時に決定されます。予約タスク設定ウィザードに表示される例は、Red Hat Enterprise Linuxエージェントのバージョンに基づいています。

未解決アラートの概要の送信: すべての未解決アラートをリストしたメールを生成します。

ポリシーの送信: 更新されたポリシーを定期的に確認し、送信します。予約アップデートでは、既存の変更制御プロセスに準拠することができます。例として、マシンのアップデートをメンテナンス期間中や業務時間外などに実行するよう予約タスクを設定できます。

クラウドアカウントの同期: コンピュータのリストと追加したクラウドアカウントを同期します。(Deep Security Managerにクラウドアカウントを追加した場合にのみ使用できます。AzureおよびvCoudアカウントにのみ適用されます。AWSやGoogle Cloud Platform(GCP) などのクラウドアカウントの種類には対応していません。)

ディレクトリの同期: コンピュータのリストと追加のLDAPディレクトリを同期します。LDAPディレクトリをDeep Security Managerに追加した場合のみ使用可能です。

ユーザ/連絡先の同期: ユーザおよび連絡先のリストを、追加されたActive Directoryと同期します。Active DirectoryをDeep Security Managerに追加した場合のみ使用可能です。

VMware vCenterの同期: コンピュータのリストを、追加されたVMware vCenterと同期します。VMware vCenterをDeep Security Managerに追加した場合のみ使用可能です。

予約タスクを有効または無効にする

予約タスクを有効または無効にできます。たとえば、特定の管理作業を実行する間他のアクティビティが発生しないようにするには、予約タスクを一時的に無効にします。予約タスクの有効化または無効化は、該当タスクの [プロパティ] ウィンドウの [一般] タブで設定します。

予約レポートを設定する

予約レポートとは、レポートを定期的に生成してユーザおよび連絡先に配信する予約タスクです(この機能の名前は「定期レポート」です) 。ほとんどのオプションは前述の単独レポートと同じですが、[期間] オプションだけは例外です。

ヒント: 複数のコンピュータグループから特定のコンピュータに関するレポートを生成するには、まず該当するコンピュータのみの閲覧権限があるユーザを作成し、「すべてのコンピュータ」レポートを定期的に生成する予約タスクを作成するか、作成したユーザでログオンして「すべてのコンピュータ」レポートを実行します。レポートには、そのユーザが閲覧できるコンピュータのみが記載されます。

コンピュータの追加または変更時にタスクを自動的に実行する(イベントベースのタスク)

注意: この記事は、Deep Securityオンプレミスソフトウェアインストールにのみ適用される仮想マシンの保護に関するリファレンスです。

イベントベースタスクを使用して、保護対象のコンピュータの特定のイベントを監視し、特定の条件に基づいてタスクを実行できます。

イベントベースタスクを作成する

Deep Security Managerで、[Administration]→[Event-Based Tasks]→[New]の順にクリックします。表示されるウィザードの手順に従って、新しいタスクを作成します。タスクの種類によって、入力を求められる情報が異なります。

既存のイベントベースタスクを編集または停止する

既存のイベントベースタスクのプロパティを変更するには、[管理]→[イベントベースタスク] をクリックします。リストからイベントベースタスクを選択し、[プロパティ] をクリックします。

監視できるイベント

- コンピュータの作成 (システムによる): Active Directoryやクラウドプロバイダのアカウントとの同期中、またはVirtual Applianceを実行する管理対象ESXiサーバ上への仮想マシンの作成中における、Managerへのコンピュータの追加。
- コンピュータの移動 (システムによる): 1台のESXi内のvApp間での仮想マシンの移動。またはデータセンター間、あるいはESXi間 (非管理対象ESXiサーバからVirtual Applianceを実行する管理対象ESXiサーバへの移動を含む) でのESXi上の仮想マシンの移動。
- Agentからのリモート有効化: Agentからのリモート有効化によるAgentの有効化。
- IPアドレスの変更: コンピュータが別のIPの使用を開始した場合。
- NSXセキュリティグループの変更: このイベントは下記の状況で発生します (イベントは影響を受ける各仮想マシン側に記録されます)。
  - NSX Deep Securityサービスプロファイルに間接的に関連付けられたグループに仮想マシンが追加された
  - NSX Deep Securityサービスプロファイルに関連付けられたNSXグループから仮想マシンが削除された
  - NSX Deep Securityサービスプロファイルに関連付けられたNSXポリシーがNSXグループに適用された
  - NSX Deep Securityサービスプロファイルに関連付けられたNSXポリシーがNSXグループから削除された
  - NSXポリシーがNSX Deep Securityサービスプロファイルに関連付けられた
  - NSXポリシーがNSX Deep Securityサービスプロファイルから削除された
  - NSX Deep Securityサービスプロファイルに関連付けられたNSXグループの名前が変更された
- コンピュータの電源オン (システムによる): VMware仮想マシンの電源オンイベントによってユーザが有効化をトリガできるようにします。

  注意: 「コンピュータの電源オン」イベントは、VMWareのESX環境でホストされた仮想マシンでのみ使用できます。このイベントを使用する際は、同時に多数のコンピュータの電源がオンになると処理速度が低下する可能性があることに注意してください。

条件

タスクを実行するために特定の一致条件が満たされるように要求できます。たとえば、コンピュータのアクティベート処理を実行するには、Amazon EC2インスタンスにProductionSystemのAWS「タグ」を含め

る必要があります("処理" on page 1833、下を参照) を実行します。

条件を追加する場合:

- 複数の条件を追加するには、[+]ボタンをクリックします。複数条件のセットアップでは、処理を実行するにはすべての条件を満たす必要があります。
- Javaの正規表現構文を使用する(regex).正規表現の使い方の例を次の表に示します。正規表現の詳細については、https://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.htmlを参照してください。

それぞれの条件と説明のリスト

- クラウドインスタンスのイメージID: AWS クラウドインスタンスAMI ID。

  注意: この一致条件は、Computers> Add>Add AWS Accountを介してマネージャに追加されたAWSインスタンスでのみ使用できます。

- クラウドインスタンスメタデータ: 一致するメタデータは、AWS、Azure、またはGCPインスタンスに追加された AWSタグ、Azureタグ、または GCP ラベル に対応します。

  注意: この一致条件は、Computers> Add>[Add AWS Account, Add Azure Account、または Add GCP Account]を介してマネージャーに追加されたAWSインスタンスおよびAzureまたはGCP VMで使用できます。コンピュータに現在関連付けられているメタデータが、エディタ画面の[概要]画面に表示されます。一致する条件を定義するには、メタデータキーとメタデータ値の2つの情報を提供する必要があります。たとえば、「AlphaFunction」という名前のメタデータキーの値が「DServer」であるコンピュータに一致させるためには、「AlphaFunction」および「DServer」を入力します (括弧は不要)。複数の候補に一致させる場合、正規表現を使用できます。この例では、「AlphaFunction」と「.*Server」、または「AlphaFunction」と「D.*」というように指定できます。

- クラウドインスタンスのセキュリティグループ名: クラウドインスタンスが適用されるセキュリティグループです。

  注意: この一致条件は、AWSクラウドインスタンスに対してのみ使用できます。

- クラウドアカウント名: クラウドアカウントプロパティウィンドウの[表示名]フィールドです。
- Cloud Vendor: インスタンスのクラウド環境ベンダー。この条件は、特定のクラウドベンダーのインスタンスを照合するために使用されます。現在、AWS、Azure、およびGCPのベンダーで一致させることができます。

> 注意: クラウドベンダーは、Computers> Add>[Add AWS Account, Add Azure Account、または Add GCP Account]を介してクラウドインスタンスをマネージャーに追加した場合にのみ機能します。

- コンピュータ名: コンピュータプロパティウィンドウの [ホスト名] フィールドです。
- ESXi名: 仮想マシンコンピュータをホストするESXiサーバの [ホスト名] フィールドです。ESXi名: 仮想マシンコンピュータをホストするESXiサーバの [ホスト名] フィールドです。
- フォルダ名: ローカル環境でコンピュータが配置されているフォルダ名またはディレクトリ名です。

  > 注意: この一致条件は、コンピュータの任意の上位フォルダ(vCenterサーバと統合されている場合はルートデータセンターを含む) の名前を照合します。正規表現の先頭に「*」を追加すると、すべての上位フォルダの名前が条件に一致する必要があります。これは、正規表現の否定構文と組み合わせると特に便利です。たとえば、フォルダ名に「Linux」を含まないフォルダ内のコンピュータを検索するには、「*^((?!Linux).)*$」という正規表現を使用できます。

- GCPネットワークタグ: GCP VMに追加されたネットワークタグ。

  > 注意: GCP VM に複数のGCP ネットワークタグがあり、そのいずれかが*任意のいずれか*に一致する場合、VMは一致したものと見なされます。

- NSXセキュリティグループ名: この条件に適合するグループは、NSX Deep Securityサービスプロファイルの NSXポリシーに関連付けられたNSXグループのみです。仮想マシンは他のNSXグループのメンバーである可能性がありますが、この一致条件では関係ありません。
- プラットフォーム: コンピュータのOSです。
- vCenter名: Deep Security Managerに追加されたコンピュータのvCenterプロパティの[名前] フィールド。

  次の2つの条件は、TrueまたはFalseと一致させる条件です。

- Appliance保護が利用可能: 仮想マシンがホストされているESXi上にDeep Security Virtual Applianceがあり、仮想マシンを保護できます。仮想マシンの状態が有効化済みになっているかどうかは問いません。
- Appliance保護が有効化済み: Deep Security Virtual Applianceを使用して、有効化されている仮想マシンをホストしているESXi上の仮想マシンを保護できます。

  この条件では、IPリスト内のIPに一致するものが検索されます。

- 最後に使用されたIPアドレス: コンピュータの現在または最後に使用された既知のIPアドレスです。

  注意: 新しいコンピュータは、そのソースによって使用可能なフィールドが異なります。たとえば、Active Directoryを使用した同期の結果として追加されたコンピュータの場合、「プラットフォーム」は使用できません。

Java正規表現の例

一致させる値	正規表現
任意の文字列 (空ではない)	.+
空の文字列 (文字なし)	^$
Folder Alpha	Folder\ Alpha
FIN-1234	FIN-\d+ または FIN-.*
RD-ABCD	RD-\w+ または RD-.*
AB または ABC または ABCCCCCCCCCC	ABC*
Microsoft Windows 2003 または Windows XP	.*Windows.*
Red Hat 7 または Some_Linux123	.*Red.*|.*Linux.*|

処理

上記のどのイベントが検出されたかに応じて、次の処理が実行されます。

- コンピュータの有効化: コンピュータでDeep Securityの保護が有効化されます。
  - 有効化の遅延 (分): 指定した時間 (分) の経過後に有効化されます。

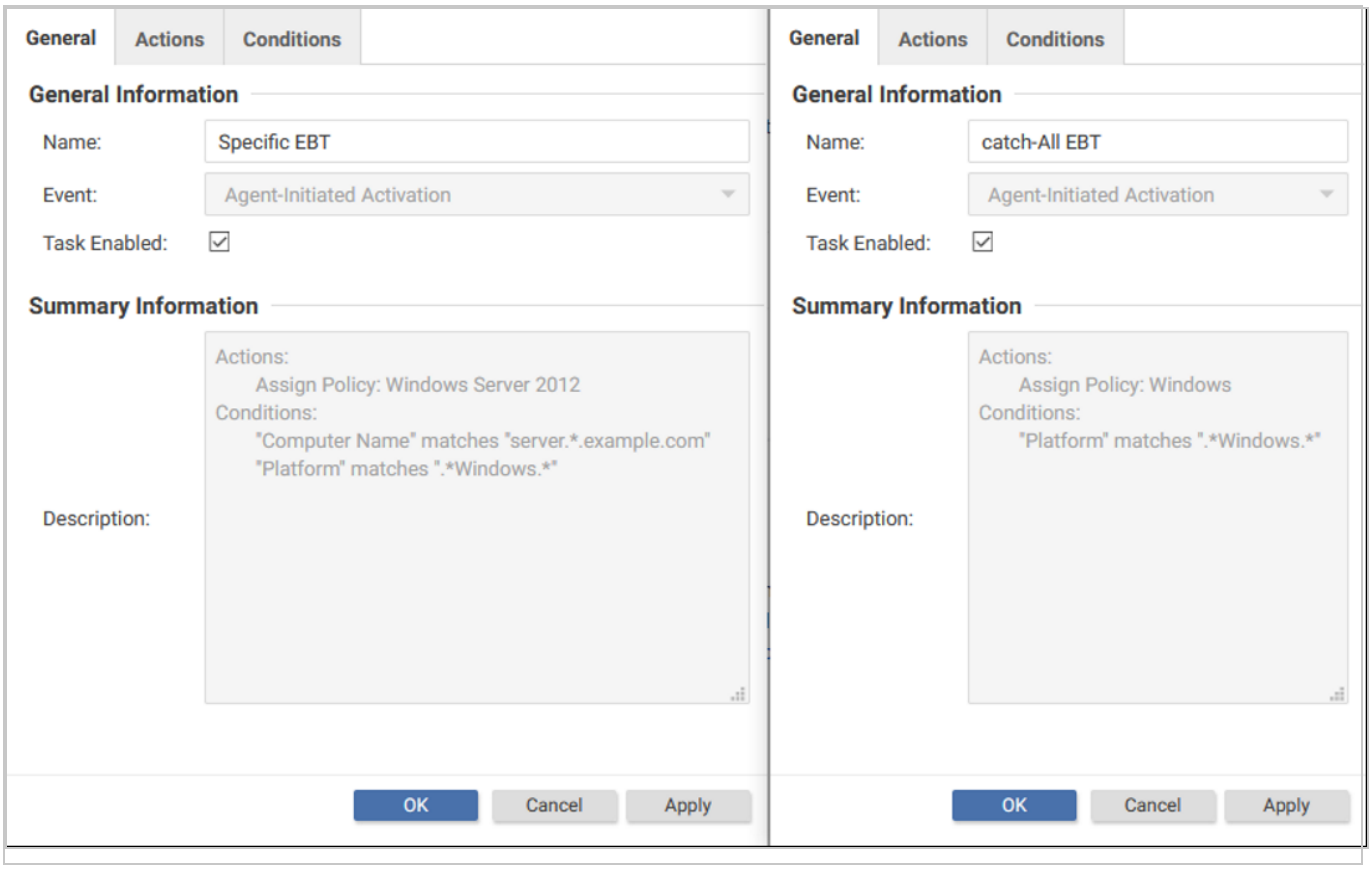
- 注意: イベントベースのタスクによって、Deep Security Virtual Applianceで保護されているESXiにvMotionで移動中の仮想マシンに保護が適用される場合、保留になっているVMware管理タスクを完了できるよう、有効化を遅らせます。遅らせる時間は環境ごとに異なります。

- コンピュータを無効にする: Deep Securityの保護機能がコンピュータで無効になっています。
- ポリシーの割り当て: 新しいコンピュータにポリシーが自動的に割り当てられます。(最初にコンピュータを有効化する必要があります)。
- Relayグループの割り当て: 新しいコンピュータに、セキュリティアップデートを受信するためのRelayグループが自動的に割り当てられます。
- コンピュータグループへの割り当て: [コンピュータ] 画面のいずれかのコンピュータグループにコンピュータが配置されます。

実行順序

イベントベースのタスクを使用する場合は、各タスクに固有の条件を作成して使用する必要があります。これは、同一の条件に遭遇した場合、Deep Securityはそれらを特定の順序で処理するため、この順序では、タスク内の条件の数を考慮しないため、これらのタスクを相互にランク付けします。

たとえば、*Windows Server 2012* プラットフォーム上の *server01.example.com* コンピュータで、次のイベントベースのタスクが発生したとします。



条件の多いイベントベースのタスクは自動的には実行されません。代わりに、「Platform」条件は2回照合され、イベントベースのタスクはタスクの名前とデータベースの種類に基づいて実行されます。

- PostgreSQL:「a task」、「A task」、「b task」、「B task」
- Oracle:「タスク」、「Bタスク」、「aタスク」、「bタスク」(ASCIIBetical の順)
- Microsoft SQL Server: オペレーティングシステムのロケールによって異なります。

ただし、この順序は最初の一致では停止せず、最後に一致した時点で停止します。これは実際には、Oracleを使用している場合、上記の例では、「catch-All EBT」によってポリシーが割り当てられることになります。というのも、ASCIIBetical orderを使用すると、「catch」の「c」が「S」の後に来ることになるからです。「特定」

予期しない結果を回避するには、イベントベースのタスク(CamelCaseなど) に固有の命名規則を使用してください。

注意: タスク名の順序は実際には、データベース内のテーブル「scheduledtasks」の列「name」に使用する照合スキームによって決まります。たとえば、Oracleでは、すべての列に対して初期設定の照合スキームとして照合スキーム「NLS_COMP:BINARY」および「NLS_SORT:BINARY」が使用さ

れ、タスク名文字列はASCII順序でソートされます。

イベントベースタスクを一時的な無効にする

既存のイベントベースタスクが実行されないようにするには、このタスクを右クリックして、[無効] をクリックします。たとえば、特定の管理作業の実行時に他のアクティビティが発生しないようにするには、イベントベースタスクを一時的に無効にします。

イベントベースタスクを再び有効にするには、このタスクを右クリックして、[有効] をクリックします。

AWSオートスケーリングとDeep Security

AWS自動スケーリングで作成された新しいインスタンスに対して、Deep Securityの自動保護を設定できます。

自動スケーリングで作成された各インスタンスには、Deep Securityエージェントがインストールされている必要があります。Agentのインストールには、AMIの作成に使用されたEC2インスタンスにインストール済みのAgentを組み込む方法と、AMIの起動設定にインストールスクリプトを組み込んでAgentをインストールする方法があります。それぞれのオプションにはメリットとデメリットがあります。

- インストール済みAgentを組み込むと、Agentソフトウェアをダウンロードしてインストールする必要がなくなるため、インスタンスが稼働するまでの時間を短縮できます。欠点は、エージェントソフトウェアが最新でない可能性があることです。この問題を回避するには、アクティベーション時のアップグレード機能を有効にします。
- 配信スクリプトを使用してエージェントをインストールする場合は、Deep Security Managerからエージェントソフトウェアの最新バージョンが常に取得されます。

Agentをプレインストールする

Deep Security Agentを設定済みのEC2インスタンスがある場合は、そのインスタンスを使用してオートスケーリング用のAMIを作成できます。AMIを作成する前に、EC2インスタンスのAgentを無効にし、インスタンスを停止する必要があります。

```
dsa_control -r
```

注意: 有効化されたAgentを含むAMIは作成しないでください。各Agentは個別に有効化する必要があります。

オートスケーリングで新規に作成された各EC2インスタンスでAgentを有効にし、ポリシーがまだない場合は適用する必要があります。これには次の2つの方法があります。

- Agentを有効にしてポリシーを適用 (オプション) するインストールスクリプトを作成します。このインストールスクリプトをAWS起動設定に追加して、新しいインスタンスが作成されたときに実行されるようにします。手順については、この後の「インストールスクリプトでAgentをインストールする」を参照してください。ただし、インストールスクリプトの、Agentを取得してインストールするセクションは除外します。必要なのは、スクリプトのdsa_control -aセクションだけです。

  注意: インストールスクリプトが機能するためには、Deep Security ManagerでAgentからの通信を有効にする必要があります。この設定の詳細については、"Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511を参照してください。

- インスタンスの起動時および「コンピュータの作成 (システムによる)」イベント発生時にAgentを有効にしてポリシーを適用する (オプション) イベントベースタスクを、Deep Security Managerで設定することができます。

インストールスクリプトでAgentをインストールする

Deep Securityには、カスタマイズされた配置スクリプトを生成する機能があり、EC2インスタンスの作成時に実行できます。EC2インスタンスにインストール済みAgentが含まれていない場合は、インストールスクリプトでAgentをインストールして有効にし、ポリシーを適用し、オプションでコンピュータをコンピュータグループとRelayグループに割り当てる必要があります。

ヒント: Deep Security APIを使用して、Agentのインストールを自動化するためのインストールスクリプトを生成できます。詳細については、「Generate an agent deployment script」を参照してください。

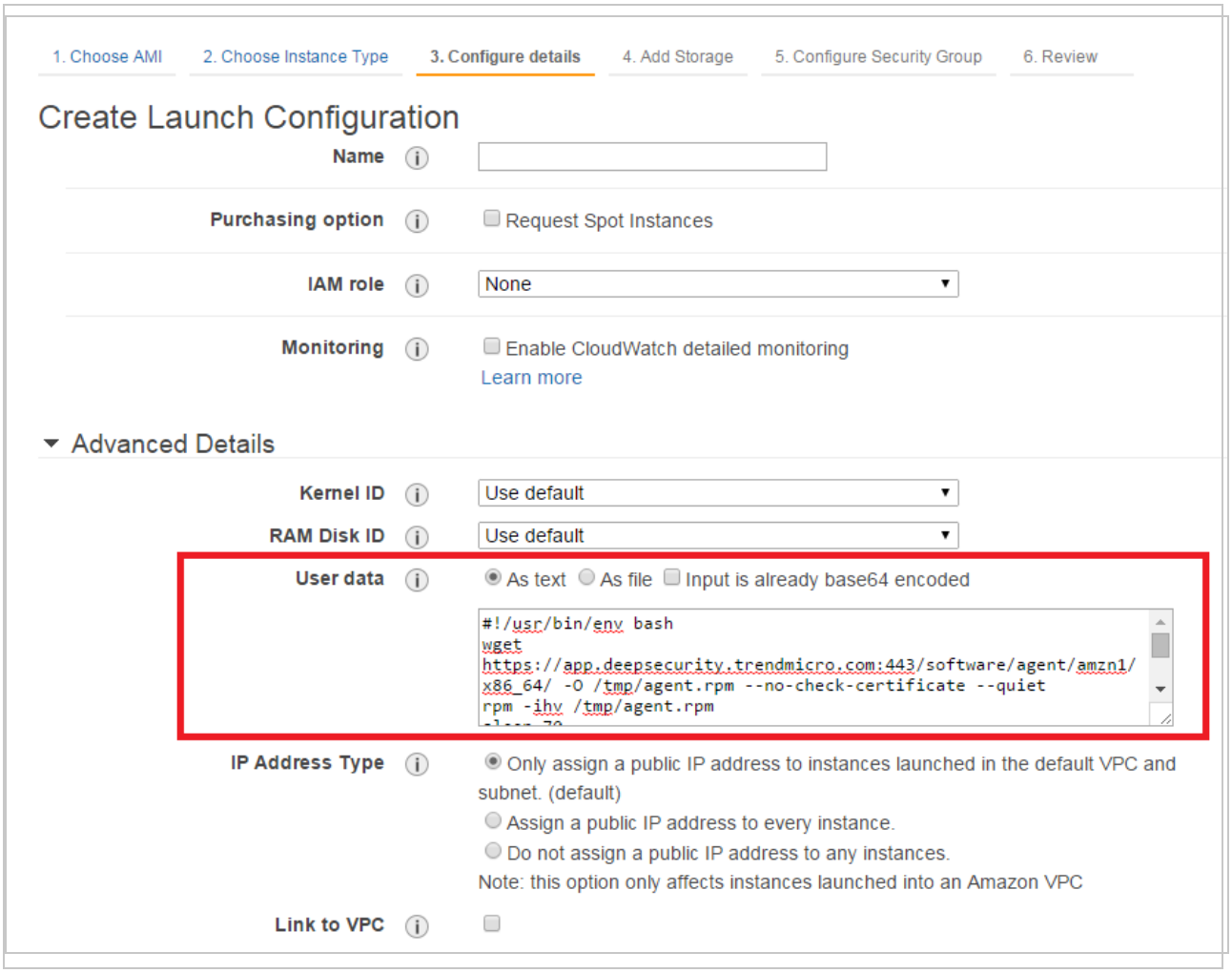
インストールスクリプトが機能するためには、以下の要件を満たす必要があります。

- 停止したコンピュータからAMIを作成する必要があります。
- Deep Security ManagerでAgentからの通信を有効にする必要があります。この設定についての詳細は、"Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511を参照してください。

インストールスクリプトを使用してインスタンスの自動保護を設定するには

1. Deep Security Managerにログオンします。
2. 右上隅のサポートメニューから、配信スクリプトを選択します。
3. プラットフォームを選択します。

4. [インストール後にAgentを自動的に有効化] を選択します。
5. 適切な [セキュリティポリシー]、[コンピュータグループ]、および [Relayグループ] を選択します。
6. [クリップボードにコピー] をクリックします。
7. AWS起動設定に移動し、[Advanced Details] を展開して [User Data] にインストールスクリプトを貼り付けます。



注意: Microsoft WindowsベースのAMIでPowerShellインストールスクリプトを実行する際に問題が発生した場合は、実行中のインスタンスからAMIを作成したことが原因である可能性があります。AWSでは実行中のインスタンスからAMIを作成できますが、そのAMIから作成されるインスタンスで起動時に実行されるEc2Configタスクがすべて無効になります。その結果、インスタンスはPowerShellスクリプトを実行できなくなります。

注意: WindowsにAMIを作成する場合は、ユーザデータ処理を手動で、またはイメージ作成プロセスの一環として、再有効化する必要があります。ユーザデータ処理は、明示的に指定されていない

かぎり、WindowsベースのAMIの最初の起動時にのみ実行される(最初の起動プロセスの実行中に無効になる) ため、カスタムAMIから作成されたインスタンスでは、この機能を再び有効にしないとユーザデータが実行されません。この機能をリセットする方法または最初の起動で無効にならないようにする方法については、「EC2Configサービスを使用したWindowsインスタンスの設定」で詳しく説明されています。EC2Configバージョン2.1.10以降を使用している場合は、<persist>true</persist> をユーザデータに組み込むのが最も簡単な方法です。

オートスケーリングの結果としてDeep Securityからインスタンスを削除する

Deep Security ManagerでAWSアカウントを追加すると、オートスケーリング後にAWSに存在しなくなったインスタンスはDeep Security Managerから自動的に削除されます。

AWSアカウントの追加の詳細については、"AWSアカウントの追加について" on page 664を参照してください。

Azure Virtual Machine Scale SetsとDeep Security

Azure Virtual Machine Scale Sets (VMSS) を使用すると、一連の同一の仮想マシンを配置して管理できます。仮想マシンの数は、設定可能なスケーリングルールに基づいて自動的に増加または減少します。詳細については、「Azure Virtual Machine Scale Sets とは」を参照してください。

Deep Security Agentが事前にインストールされ、事前有効化されている基本VMイメージを含めるようにVMSSを設定できます。VMSSがスケールアップすると、スケールセットの新しい仮想マシンインスタンスにAgentが自動的に含まれます。

AgentをVMSSに追加するには:

- "手順1: (推奨) AzureアカウントをDeep Security Managerに追加する" on the next page
- "手順2: インストールスクリプトを準備する" on the next page
- "手順3: カスタムスクリプト拡張機能を介してAgentをVMSSインスタンスに追加する" on page 1841

手順1: (推奨) AzureアカウントをDeep Security Managerに追加する

Deep Security ManagerにAzureアカウントを追加すると、そのアカウントで作成されたすべてのAzureインスタンスがDeep Security Managerにロードされ、Computersの下に表示されます。インスタンスは、Agentがインストールされているかどうかに関係なく表示されます。Agentを含まないインスタンスの[ステータス] は [Agent/Applianceなし] です。インスタンスにAgentをインストールして有効化したら、[ステータス] は [管理対象 (オンライン)] に変更されます。

Azureアカウントを追加した後でスケールの設定が手動または自動でスケールアップされた場合、Deep Securityは新しいAzureインスタンスを検出し、Computersのリストに追加します。同様に、スケールセットがスケールダウンすると、インスタンスがビューから削除されます。このため、Deep Security Managerは常に、使用可能なAzureインスタンスの現在のリストをスケールセットに表示します。

ただし、AzureアカウントをDeep Security Managerに追加せず、代わりに別の方法を使用して個々のAzureインスタンスを追加すると、Deep Securityはスケールダウンを検出せず、存在しないAzureインスタンスをそのインスタンスから削除しません。リスト。Deep Security ManagerでAzure VMのリストが拡大するのを防ぐため、いつAzureインスタンスが常に使用可能であるかを常に表示するには、AzureアカウントをDeep Security Managerに追加することを強くお勧めします。

Azureアカウントの追加手順については、"Deep SecurityへのMicrosoft Azureアカウントの追加" on page 688を参照してください。

手順2: インストールスクリプトを準備する

Deep Security Managerで、Deep Security ManagerからDeep Securityスクリプトを準備します。手順については、"インストールスクリプトを使用したコンピュータの追加と保護" on page 1849を参照してください。このインストールスクリプトは、次に設定するカスタムスクリプト拡張機能で参照されます。

注意: 次のVMSSスクリプトを使用してカスタムスクリプトを実行するには、Azure Blobストレージに、または有効なURLを介してアクセス可能な場所にスクリプトを保存する必要があります。Azure Blobストレージへファイルをアップロードする手順については、「Azure PowerShellでAzure Blobストレージ操作を実行する」を参照してください。

手順3: カスタムスクリプト拡張機能を介してAgentをVMSSインスタンスに追加する

次に、PowerShellを使用してAgentを追加する方法に関する例を示します。

- 例1では、Agentを含む新しいVMSSを作成する方法を示します。
- 例2では、既存のVMSSにAgentを追加する方法を示します。

両方の例:

- Add-AzureRmVmssExtension cmdletを使用して拡張機能をVMSSに追加します。
- Azure PowerShell 5.1.1を使用します。

注意: PowerShell cmdletを使用して新しいVMSSを作成する手順については、このMicrosoftチュートリアルを参照してください。Linuxプラットフォームについては、https://github.com/Azure/custom-script-extension-linuxを参照してください。

例1: Agentを含む新しいVMSSを作成する

```
$resourceGroupName = <The resource group of the VMSS>
$vmssname = <The name of the VMSS>

# Create ResourceGroup
New-AzureRmResourceGroup -ResourceGroupName $resourceGroupName -Location EastUS

# Create a config object
$vmssConfig = New-AzureRmVmssConfig `
  -Location EastUS `
  -SkuCapacity 2 `
  -SkuName Standard_DS2 `
  -UpgradePolicyMode Automatic
```

```
# Define the script for your Custom Script Extension to run on the Windows Platform
$customConfig = @{
   "fileUris" = ("A URL of your copy of deployment script, ex. deploymentscript.ps1");
   "commandToExecute" = "powershell -ExecutionPolicy Unrestricted -File deploymentscript.ps1"
}

# Define the script for your Custom Script Extension to run on the Linux Platform
#$customConfig = @{
# "fileUris" = ("A URL of your copy of deployment script, ex. deploymentscript.sh");
# "commandToExecute" = "bash deploymentscript.sh"
#}

# The section is required only if deploymentscript has been located within Azure StorageAccount
$storageAccountName = <StorageAccountName if deploymentscript is locate in Azure Storage>
$key = (Get-AzureRmStorageAccountKey -Name $storageAccountName -ResourceGroupName
$resourceGroupName).Value[0]
$protectedConfig = @{
   "storageAccountName" = $storageAccountName;
   "storageAccountKey" = $key
}

# Use Custom Script Extension to install Deep Security Agent (Windows)
Add-AzureRmVmssExtension -VirtualMachineScaleSet $vmssConfig `
   -Name "customScript" `
   -Publisher "Microsoft.Compute" `
   -Type "CustomScriptExtension" `
   -TypeHandlerVersion 1.8 `
   -Setting $customConfig `
```

```
    -ProtectedSetting $protectedConfig

# Use Custom Script Extension to install Deep Security Agent (Linux)
#Add-AzureRmVmssExtension -VirtualMachineScaleSet $vmssConfig `
# -Name "customScript" `
# -Publisher "Microsoft.Azure.Extensions" `
# -Type "customScript" `
# -TypeHandlerVersion 2.0 `
# -Setting $customConfig `
# -ProtectedSetting $protectedConfig

# Create a public IP address
# Create a frontend and backend IP pool
# Create the load balancer
# Create a load balancer health probe on port 80
# Create a load balancer rule to distribute traffic on port 80
# Update the load balancer configuration
# Reference a virtual machine image from the gallery
# Set up information for authenticating with the virtual machine
# Create the virtual network resources
# Attach the virtual network to the config object

# Create the scale set with the config object (this step might take a few minutes)
New-AzureRmVmss `
    -ResourceGroupName $resourceGroupName `
    -Name $vmssname `
    -VirtualMachineScaleSet $vmssConfig
```

例2: 既存のVMSSにAgentを追加する

```
$resourceGroupName = <The resource group of the VMSS>
$vmssname = <The name of the VMSS>

# Get the VMSS model
$vmssobj = Get-AzureRmVmss -ResourceGroupName $resourceGroupName -VMScaleSetName $vmssname

# Show model data if you prefer
# Write-Output $vmssobj

# Define the script for your Custom Script Extension to run on the Windows platform
$customConfig = @{
   "fileUris" = ("A URL of your copy of deployment script, ex. deploymentscript.ps1");
   "commandToExecute" = "powershell -ExecutionPolicy Unrestricted -File deploymentscript.ps1"
}

# Define the script for your Custom Script Extension to run on the Linux platform
#$customConfig = @{
# "fileUris" = ("A URL of your copy of deployment script, ex. deploymentscript.sh");
# "commandToExecute" = "bash deploymentscript.sh"
#}

# The section is required only if deploymentscript has been located within Azure StorageAccount
$storageAccountName = <StorageAccountName if deploymentscript is locate in Azure Storage>
$key= (Get-AzureRmStorageAccountKey -Name $storageAccountName -ResourceGroupName $resourceGroupName).Value[0]
$protectedConfig = @{
```

```
    "storageAccountName" = $storageAccountName;
    "storageAccountKey" = $key
}

# Use Custom Script Extension to install Deep Security Agent (Windows)
$newvmssobj = Add-AzureRmVmssExtension `
    -VirtualMachineScaleSet $vmssobj `
    -Name "customScript" `
    -Publisher "Microsoft.Compute" `
    -Type "CustomScriptExtension" `
    -TypeHandlerVersion 1.8 `
    -Setting $customConfig `
    -ProtectedSetting $protectedConfig

# Use Custom Script Extension to install Deep Security Agent (Linux)
#$newvmssobj = Add-AzureRmVmssExtension `
#    -VirtualMachineScaleSet $vmssobj `
#    -Name "customScript" `
#    -Publisher "Microsoft.Azure.Extensions" `
#    -Type "customScript" `
#    -TypeHandlerVersion 2.0 `
#    -Setting $customConfig `
#    -ProtectedSetting $protectedConfig

# Update the virtual machine scale set model
Update-AzureRmVmss -ResourceGroupName $resourceGroupName -name $vmssname -
VirtualMachineScaleSet $newvmssobj -Verbose
```

```
# Get Instance ID for all instances in this VMSS, and decide which instance you'd like to update
# Get-AzureRmVmssVM -ResourceGroupName $resourceGroupName -VMScaleSetName $vmssname

# Now start updating instances
# If upgradePolicy is Automatic in the VMSS, do NOT execute the next command Update-AzureRmVmssInstance. Azure will auto-update the VMSS.
# There's no PowerShell command to update all instances at once. But you could refer to the output of Update-AzureRmVmss, and loop all instances into this command.
Update-AzureRmVmssInstance -ResourceGroupName $resourceGroupName -VMScaleSetName $vmssname -InstanceId 0
```

GCP自動スケーリングとDeep Security

自動スケーリングをサポートするために、GCP マネージドインスタンスグループ(MIG) を通じて作成された新しいGCP VMインスタンスのDeep Securityで自動保護を設定できます>。

MIGで作成された各GCP VMインスタンスには、Deep Securityエージェントがインストールされている必要があります。これには2通りの方法があります。インスタンステンプレートの作成に使用したGCP VMインスタンスに事前インストールされたエージェントを組み込むことも、インスタンステンプレートに配置スクリプトを組み込んでエージェントをインストールすることもできます。。それぞれのオプションにはメリットとデメリットがあります。

- インストール済みAgentを組み込むと、Agentソフトウェアをダウンロードしてインストールする必要がなくなるため、インスタンスが稼働するまでの時間を短縮できます。欠点は、エージェントソフトウェアが最新でない可能性があることです。この問題を回避するには、アクティベーション時のアップグレード機能を有効にします。
- インストールスクリプトを使用してAgentをインストールする場合、スクリプトはDeep Security Managerから常に最新バージョンのAgentソフトウェアを取得します。

Agentをプレインストールする

Deep Security Agentですでに設定されているGCP VMインスタンスがある場合は、そのインスタンスを使用してMIGのインスタンステンプレートを作成できます。インスタンステンプレートを作成する前に、GCP VMインスタンスでエージェントを無効にしてインスタンスを停止する必要があります。

```
dsa_control -r
```

MIGによって作成された新しいGCP VMインスタンスのそれぞれは、エージェントがアクティベートされ、Policyが適用されている必要があります(ポリシーがすでに適用されている場合) 。これには次の2つの方法があります。

- Agentを有効にしてポリシーを適用 (オプション) するインストールスクリプトを作成します。次に、配置スクリプトをGCPインスタンステンプレートに追加して、新しいインスタンスが作成されたときに実行されるようにします。手順については、"インストールスクリプトでAgentをインストールする" below のセクションを参照してください。ただし、配信スクリプトでエージェントを取得およびインストールするセクションは省略してください。スクリプトのdsa_control -aセクションのみが必要になります。

  注意: インストールスクリプトが機能するためには、Deep Security ManagerでAgentからの通信を有効にする必要があります。この設定についての詳細は、"AgentからのリモートAgent有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511を参照してください。

- エージェントをアクティベートするイベントベースのタスクをDeep Security Managerで設定し、オプションでインスタンスの起動時および「コンピュータによって作成された(システム別) 」イベントが発生したときにポリシーを適用できます。

インストールスクリプトでAgentをインストールする

Deep Securityは、カスタマイズされた配信スクリプトを生成して、GCP VMインスタンスの作成時に実行できるようにします。GCP VMインスタンスに事前インストールされたエージェントが含まれていない場合、配信スクリプトはエージェントをインストールして有効化し、ポリシーを適用し、必要に応じてコンピュータグループと中継グループにコンピュータを割り当てる必要があります。

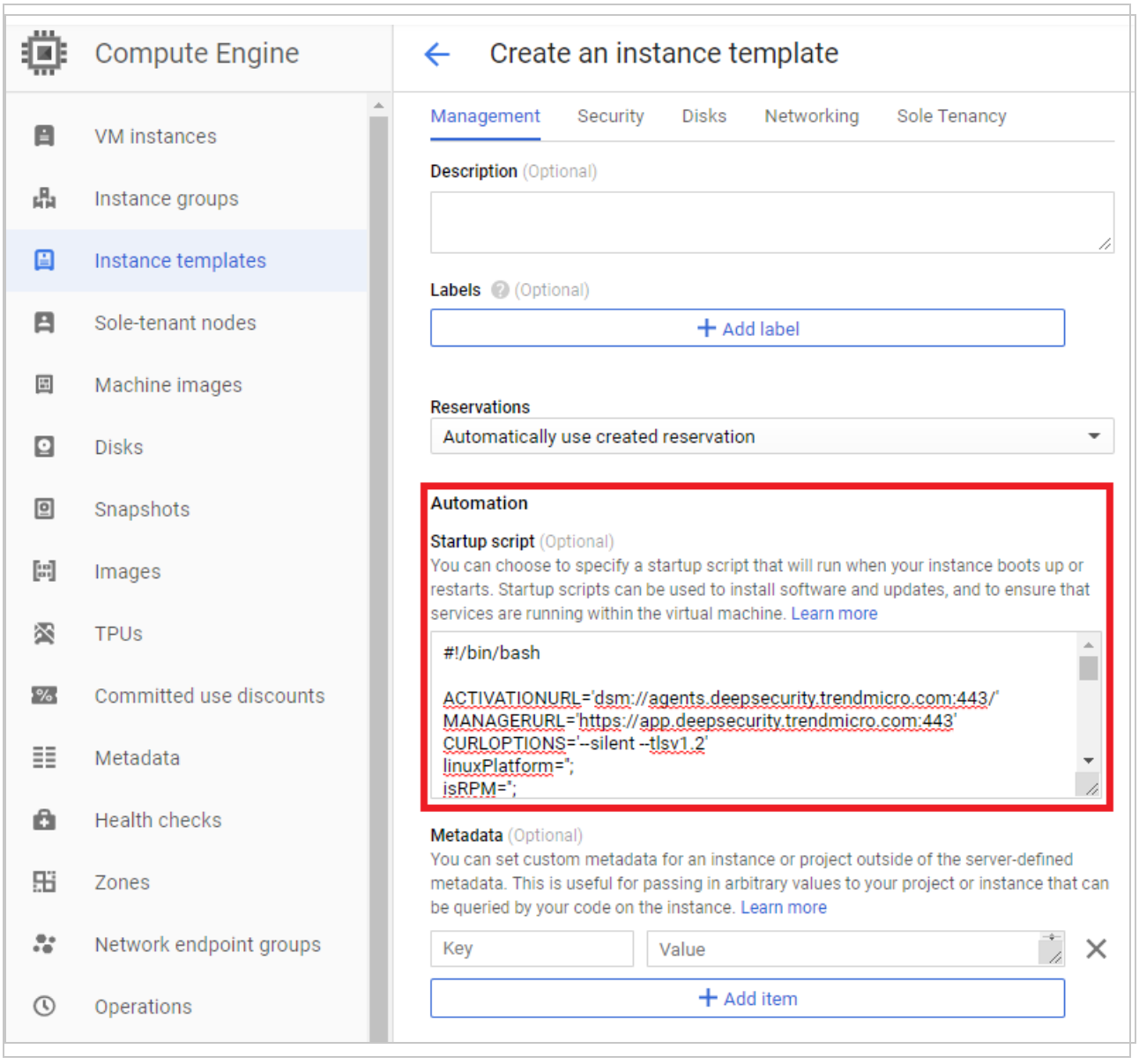
ヒント: Deep Security APIを使用してエージェントのインストールを自動化するためのデプロイメントスクリプトを生成できます。詳細については、エージェントデプロイメントスクリプトの生成を参照してください。

インストールスクリプトが機能するためには、以下の要件を満たす必要があります。

- 停止しているコンピュータからイメージを作成する必要があります。
- Deep Security ManagerでAgentからの通信を有効にする必要があります。この設定についての詳細は、"AgentからのリモートAgent有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511を参照してください。

インストールスクリプトを使用してインスタンスの自動保護を設定するには

1. Deep Security Managerにログオンします。
2. 右上隅のサポートメニューから、配信スクリプトを選択します。
3. プラットフォームを選択します。
4. [インストール後にAgentを自動的に有効化] を選択します。
5. 適切な [セキュリティポリシー]、[コンピュータグループ]、および [Relayグループ] を選択します。
6. クリップボードにコピーをクリックします。
7. GCPインスタンステンプレートに移動し、管理、セキュリティ、ディスク、ネットワーク、借用を展開し、配信スクリプトをスタートアップスクリプトに貼り付けます。。



GCP MIGの結果としてDeep Securityからインスタンスを削除します。

Deep Security ManagerでGCPアカウントを追加すると、管理対象インスタンスグループの結果としてGCPに存在しなくなったインスタンスは、Deep Security Managerから自動的に削除されます。

GCPアカウントの追加については、"Google Cloud Platformアカウントを追加する" on page 700 を参照してください。

インストールスクリプトを使用したコンピュータの追加と保護

Deep Securityの保護されたリソースのリストにコンピュータを追加し、保護を実装することは、複数のステップからなるプロセスです。ほとんどの手順は、コンピュータのコマンドラインから実行できるので、スクリプト化が可能です。Deep Security Managerには、サポート情報メニューからアクセスできる配信スクリプト作成アシスタントが含まれています。

Deep Security Managerによって生成された配信スクリプトは、次の処理を実行します。

- Deep Security Agentを選択したプラットフォームにインストールします。
- エージェントをアクティベートする
- エージェントにポリシーを割り当てる

インストールスクリプトを生成する

1. 開始前の準備:
   a. エージェントソフトウェアがDeep Security Managerにインポートされていることを確認してください。詳細については、"Deep Security Agentソフトウェアの入手" on page 514 の入手を参照してください。
   b. エージェントのバージョン管理設定が必要に応じて設定されていることを確認してください。詳細については、"エージェントのバージョン管理を設定する" on page 1492 の設定を参照してください。
   c. エージェント起動アクティベーション(AIA)が有効になっていることを確認してください。AIAは、インストールスクリプトをインストール後にエージェントを有効にする場合に必要です。"Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511 を使用したエージェントのアクティベートおよび保護を参照してください。
2. Deep Security Managerコンソールの右上隅で、[サポート]→[インストールスクリプト] をクリックします。

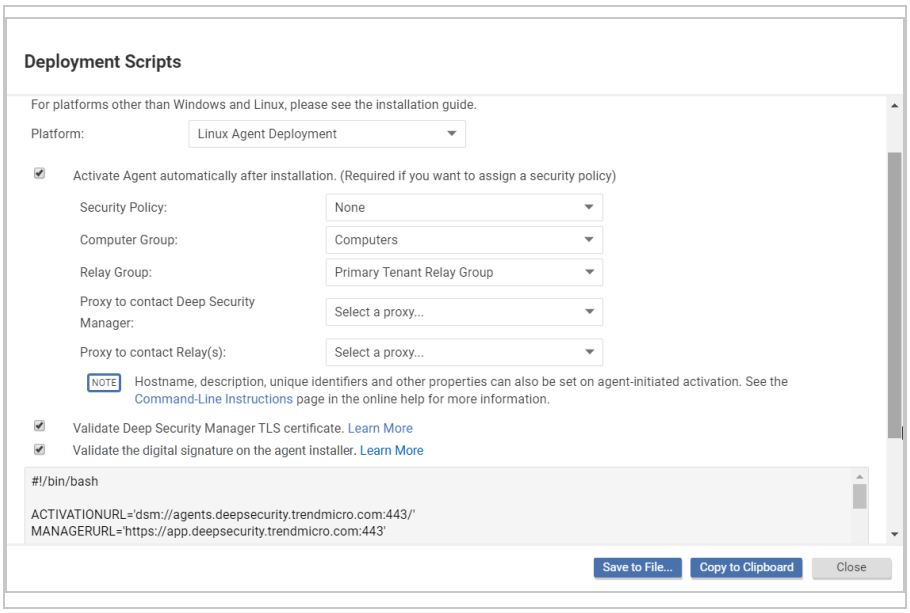
3. ソフトウェアをインストールするプラットフォームを選択します。
4. [インストール後にAgentを自動的に有効化] を選択します。

   Agentはコンピュータを保護するポリシーの適用前に有効にする必要があります。有効化により、最初の通信時にManagerにAgentが登録されます。

5. 必要に応じて、[セキュリティポリシー]、[コンピュータグループ]、[Relayグループ]、[Deep Security Managerへの接続に使用するプロキシ]、[Relayへの接続に使用するプロキシ] を選択します。
6. 必要に応じて (ただし、強くお勧めします)、[Deep Security ManagerのTLS証明書を確認する] を選択します。

   このオプションを選択すると、Agentソフトウェアをダウンロードするときにに Deep Security Managerが信頼できる認証局 (CA) の有効なTLS証明書を使用するため、「中間者」攻撃を回避できます。Deep Security Managerコンソールのブラウザバーで、Deep Security Managerが有効なCA証明書を使用しているかどうかをチェックできます。初期設定では、Deep Security Managerは自己署名証明書を使用するため、[Deep Security Manager TLS証明書の検証] オプションと互換性がありません。Deep Security Managerがロードバランサの背後に配置されていない場合に、初期設定の自己署名証明書と信頼できる認証局の証明書を置き換えるときの手順については、"Deep Security ManagerのTLS証明書を変更します。" on page 1622を参照してください。Managerがロードバランサの背後に配置されている場合は、ロードバランサの証明書を置き換える必要があります。

7. オプションで( ), を強くお勧めします。 を選択してください。エージェントインストーラファイルのデジタル署名チェックを開始するには、エージェントインストーラの署名の妥当性検査を実行します。チェックに成功すると、エージェントのインストールが続行されます。チェックに失敗した場合、エージェントのインストールは中止されます。このオプションを有効にする前に、次の点を理解してください。
   - このオプションはLinuxおよびWindowsインストーラ(RPM、DEB、またはMSIファイルの).のみ) でサポートされます。
   - (Linuxのみ) このオプションでは、公開スクリプトを実行するクライアントコンピュータごとにパブリック署名キーをインポートする必要があります。詳細は、"RPMファイルの署名の確認" on page 448 および "DEBファイルの署名の確認" on page 450の署名を確認します。
8. インストールスクリプトジェネレータにスクリプトが表示されます。[クリップボードにコピー] をクリックして、使用する配信ツールにインストールスクリプトを貼り付けるか、[ファイルに保存] をクリックします。



注意: Deep Security Manager for Windowsエージェントの配信で生成される配信スクリプトには、Windows PowerShell 4.0以上が必要です。PowerShellを管理者として実行する必要があります。スクリプトを実行するには、次のコマンドを実行する必要があります。Set-ExecutionPolicy RemoteSigned

注意: PowerShell 4.0またはcurl 7.34.0を最低限必要とする以前のバージョンのWindowsまたはLinuxにエージェントを配信する場合は、初期のTLSがマネージャおよびリレーで許可されていることを確認してください。詳細については、"TLS 1.2が強制されているかどうかを確認する" on page 1895および"初期のTLS (1.0) を有効にする" on page 1893を参照してください。また、次のように配置スクリプトを編集します。

- Linux: --tls1.2 タグを削除します。
- Windows: #requires -version 4.0 行を削除します。また、初期のTLS(バージョン1.0) がManagerとの通信に使用されるように、[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; 行も削除します。

Amazon Web Servicesを使用していて、新しいAmazon EC2、Amazon WorkSpacesまたはVPCのインスタンスを作成する場合は、生成したスクリプトをコピーして [User Data] フィールドに貼り付けます。このスクリプトによって既存のAmazon Machine Image (AMI) が起動され、Agentが自動的にインストールされて有効化されます。新しいインスタンスは、生成したインストールスクリプトで指定されているURLにアクセスできる必要があります。つまり、Deep Security Managerがインターネットに接続されているか、Amazon Web ServicesにVPN接続または直接接続されているか、またはDeep Security ManagerがAmazon Web Servicesにもインストールされている必要があります。

Linux環境用の [User Data] フィールドにインストールスクリプトをコピーする場合、インストールスクリプトをそのまま [User Data]フィールドにコピーすると、CloudInitによってsudoでスクリプトが実行されます(エラーが発生した場合、*/var/log/cloud-init.log*に記録されます)。

注意: [User Data] フィールドは、CloudFormationなどの他のサービスでも使用します。詳細については次を参照してください。
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-waitcondition.html

トラブルシューティングおよびヒント

- インストールスクリプトを実行しようとして、終了コード2「Agentパッケージダウンロードで TLS証明書の検証に失敗しました。Deep Security Manager TLS証明書が信頼されたルート証明機関によって署名されていることを確認してください。詳細については、Deep Securityのヘルプセンターで「配信スクリプト」を検索してください。「」、「Deep Security Manager TLS証明書のEDC証明書の検証」チェックボックスが選択された配信スクリプトが作成されました。このエラーは、Deep Security ManagerがDeep Security ManagerとそのAgentの間の接続に公的に信頼されていない証明書 (初期設定の自己署名証明書など) を使用している場合、または証明書と信頼済みCAの間の信頼チェーンの証明書が見つからないなど、サードパーティの証明書に問題がある場合に表示されます。証明書の詳細については、"Deep Security ManagerのTLS証明書を変更します。" on page 1622を参照してください。信頼する証明書を置き換える代わりに、配置スクリプトの生成時に [Deep Security Manager TLS証明書の検証] チェックボックスをオフにすることもできます。セキュリティ上の理由から、この方法はお勧めしません。
- PowerShell (x86) を使用してAgentをインストールする場合、次のエラーメッセージが表示されます。`C:\Program Files (x86)\Trend Micro\Deep Security Agent\dsa_control' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.`

  PowerShellスクリプトでは`ProgramFiles`の環境変数が「Program Files (x86)」ではなく、「Program Files」に設定されている必要があります。この問題を解決するには、PowerShell (x86) を終了して、スクリプトをPowerShellで管理者として実行します。

- Windowsコンピュータでは、ローカルOSと同じプロキシ設定を使用してインストールスクリプトが実行されます。ローカルOSがプロキシを使用するように設定されていて、直接接続でしかDeep Security Managerにアクセスできない場合、インストールスクリプトは失敗します。
- 展開スクリプトは `rpm -U`に `rpm -ihv` を変更することで、エージェントの更新の代わりに、新規インストールを実行するように変更することができます。

- 配信スクリプトで使用される特定のエージェントのバージョンを制御する必要がある場合は、次の2つのオプションを使用してこの目標を達成できます。
  - エージェントバージョン管理を使用します。詳細については、"エージェントのバージョン管理を設定する" on page 1492 の設定を参照してください。このアプローチには、各スクリプトにエージェントのバージョン自体をハードコードする必要がないという利点があります。これは、一部の展開ではより柔軟なアプローチになる可能性があります。
  - 展開スクリプトを変更するか、独自のスクリプトを作成して、展開に固有の要件を満たしてください。エージェントをダウンロードするためのURL形式の詳細は、こちらを参照してください。"エージェントのダウンロードURL形式" belowのダウンロードURL形式。
- マネージャによって生成された配信スクリプトを使用する代わりに、独自の自動化メソッドとクライアントダウンロードURLを組み合わせて、クライアントのダウンロードとインストールを自動化できます。詳細については、"エージェントのダウンロードURL形式" belowを参照してください。

エージェントのダウンロードURL形式

Deep Security Agentソフトウェアパッケージは、Deep Security Managerから適切なURL形式でダウンロードできます。

ほとんどの場合、標準配信スクリプトを使用することになります(ただし、このセクションで説明する同じURL形式を使用してエージェントソフトウェアをダウンロードすることもできます)。デプロイ要件の大部分を満たします。

このURL形式は、クライアントのダウンロードとインストールのカスタマイズをさらに必要とする場合に便利です。たとえば、ソフトウェアをダウンロードするために各サーバがマネージャに接続するのではなく、各サーバで実行される配信スクリプトがローカルストレージの場所(AWS S3など)を指すようにする必要がある場合があります。あなたは定期的に、ローカルストレージの場所に新しいエージェントのバージョンをダウンロードするには、独自の自動化を構築するために、このURL形式を使用し、この目的を達成するために、ローカルストレージ・ロケーションに各サーバー上で実行することエージェントの展開スクリプトを指すことができます。

トピック:

- "エージェントのダウンロードURL形式" on the next page
- "<dsm fqdn>パラメータ" on the next page
- "<ファイル名>パラメータ" on the next page

- "<エージェントバージョン>パラメータ" on the next page
  - "<エージェントのバージョン>をスクリプトに明示的に含める必要がありますか? " on the next page
- "<プラットフォーム>,<arch>、および<filename>パラメータ" on page 1856
  - 例
- "下位互換性の除外設定" on page 1860
- "エージェントバージョンコントロールを使用して、返されるエージェントバージョンを定義する" on page 1860
  - 例
  - "<エージェントバージョン>パラメータとエージェントバージョン管理の間の相互作用" on page 1861

エージェントのダウンロードURL形式

エージェントのダウンロードに使用されるURL形式は次のとおりです。

`https://<dsm fqdn>/software/agent/<platform>/<arch>/<agent version>/<filename>`

URL formatを構成するすべてのパラメータは次のとおりです。

<dsm fqdn>パラメータ

`<dsm fqdn>` パラメータは、待機ポート番号を含む、マネージャの完全修飾ドメイン名です。

例:

`example.com:4119`

<ファイル名>パラメータ

`<filename>`パラメータは、エージェントインストーラファイルのファイル名です。ファイル名は、各プラットフォームで使用されるインストールプロセスによって異なります。

プラットフォーム	<ファイル名>
Linux Red Hat Enterprise Linux、CentOS、Oracle、CloudLinux、Amazon Linux、SUSE	`agent.rpm`

プラットフォーム	<ファイル名>
Linux Debian、Ubuntu	agent.deb
Windows	agent.msi
AIX	agent.bff.gz
Solaris 11以上	agent.p5p.gz
Solaris 10以前	agent.pkg.gz

注意: マネージャーは、ファイル名自体を検証しません。ただし、ファイル名を指定した場合は、拡張子は .rpm, .msi, .deb, .gzのいずれかにする必要があります。他のファイル名が指定されている場合、マネージャによって返されるファイル名は常に上記の表の名前の1つになります。

<エージェントバージョン>パラメータ

<agent version>パラメータはオプションです。

このパラメータが指定されていない場合、対象プラットフォームのマネージャのローカルインベントリにある最新のエージェントが返されます。

このパラメータを指定すると、エージェントのバージョン文字列が表示されます。例:「12.0.0.123」

<エージェントのバージョン>をスクリプトに明示的に含める必要がありますか?

特定のバージョンのエージェントを管理下の環境でのみ使用する場合は、URLにエージェントバージョンを明示的に追加することでこの目標を達成できます。

エージェントを大規模に展開する場合は、URLにエージェントのバージョンを追加すると(このエージェントのバージョンを配布するすべてのスクリプトにハードコードする) 、多くのアプリケーションチームにスクリプトを配信するセキュリティ運用チームに課題が発生する可能性があることに注意してください。

新しいバージョンのエージェントを使用するために時間がかかった場合に必要となるプロセスを検討します。<agent version>が配信する各スクリプトでハードコードされている場合は、これらのスクリプトで新しいエージェントバージョンの使用を開始するためのアップデートが必要になります。内部アプリケーション

チームが多数いる場合は、使用中のスクリプトのそれぞれに変更を要求するプロセスが重要になります。

Deep Securityには、次の2つのオプションがあります。

- パスから<agent version>コンポーネントを省略したスクリプトを使用します。

  マネージャのローカルインベントリにある最新のエージェントを使用している場合は、要件を満たすことができます。これは最も簡単なオプションです。

- エージェントバージョン管理を使用する

  エージェントのバージョン管理を使用すると、Deep Security管理者は、マネージャから返されるエージェントのバージョンを、プラットフォームごとに選択できます。エージェントバージョン管理の詳細とスクリプトからこの機能を活用する方法については、"エージェントバージョンコントロールを使用して、返されるエージェントバージョンを定義する" on page 1860を参照してください。

<プラットフォーム>,<arch>、および<filename>パラメータ

<platform>、<arch>、および<filename>パラメータは、次の表に示す文字列で置き換える必要があります。

注意: <platform>および<arch>は大文字と小文字が区別されます。

プラットフォーム	配信	<プラットフォーム>	<アーチ>	<ファイル名>	例
Linux	Amazon 1	amzn1	x86_64	agent.rpm	/software/agent/amzn1/x86_64/agent.rpm
	Amazon 2	amzn2	x86_64	agent.rpm	/software/agent/amzn2/x86_64/agent.rpm
	CloudLinux 6	CloudLinux_6	x86_64	agent.rpm	/software/agent/CloudLinux_6/x86_64/agent.rpm
	CloudLinux 7	CloudLinux_7	x86_64	agent.rpm	/software/agent/CloudLinux_7/x86_64/agent.rpm
	CloudLinux 8	CloudLinux_8	x86_64	agent.rpm	/software/agent/CloudLinux_8/x86_64/agent.rpm
	Debian 7	Debian_7	x86_64	agent.deb	/software/agent/Debian_

プラットフォーム	配信	<プラットフォーム>	<アーチ>	<ファイル名>	例
					7/x86_64/agent.deb
	Debian 8	Debian_8	x86_64	agent.deb	/software/agent/Debian_8/x86_64/agent.deb
	Debian 9	Debian_9	x86_64	agent.deb	/software/agent/Debian_9/x86_64/agent.deb
	Oracle Linux 6	Oracle_OL6	x86_64	agent.rpm	/software/agent/Oracle_OL6/x86_64/agent.rpm
	Oracle Linux 6	Oracle_OL6	i386	agent.rpm	/software/agent/Oracle_OL6/i386/agent.rpm
	Oracle Linux 7	Oracle_OL7	x86_64	agent.rpm	/software/agent/Oracle_OL7/x86_64/agent.rpm
	RedHat 6	RedHat_EL6	x86_64	agent.rpm	/software/agent/RedHat_EL6/x86_64/agent.rpm
	RedHat 6	RedHat_EL6	i386	agent.rpm	/software/agent/RedHat_EL6/i386/agent.rpm
	RedHat 7	RedHat_EL7	x86_64	agent.rpm	/software/agent/RedHat_EL7/x86_64/agent.rpm
	RedHat 8	RedHat_EL8	x86_64	agent.rpm	/software/agent/RedHat_EL8/x86_64/agent.rpm
	SuSE 11	SuSE_11	x86_64	agent.rpm	/software/agent/SuSE_11/x86_64/agent.rpm
	SuSE 11	SuSE_11	i386	agent.rpm	/software/agent/SuSE_11/i386/agent.rpm
	SuSE 12	SuSE_12	x86_64	agent.rpm	/software/agent/SuSE_12/x86_64/agent.rpm
	SuSE 15	SuSE_15	x86_64	エージェント.rpm	/software/agent/SuSE_15/x86_64/agent.rpm

プラットフォーム	配信	<プラットフォーム>	<アーチ>	<ファイル名>	例
	Ubuntu 16.04	Ubuntu_16.04	x86_64	agent.deb	/software/agent/Ubuntu_16.04/x86_64/agent.deb
	Ubuntu 18.04	Ubuntu_18.04	x86_64	agent.deb	/software/agent/Ubuntu_18.04/x86_64/agent.deb
Windows		Windows	x86_64	agent.msi	/software/agent/Windows/x86_64/agent.msi
		Windows	i386	agent.msi	/software/agent/Windows/i386/agent.msi
UNIX	Solaris 10アップデート4-6	Solaris_5.10_U5	x86_64	agent.pkg.gz	/software/agent/Solaris_5.10_U5/x86_64/agent.pkg.gz
		Solaris_5.10_U5	スパーク	agent.pkg.gz	/software/agent/Solaris_5.10_U5/sparc/agent.pkg.gz
	Solaris 10アップデート7-11	Solaris_5.10_U7	x86_64	agent.pkg.gz	/software/agent/Solaris_5.10_U7/x86_64/agent.pkg.gz
		Solaris_5.10_U7	スパーク	agent.pkg.gz	/software/agent/Solaris_5.10_U7/sparc/agent.pkg.gz
	Solaris 11アップデート1-3	Solaris_5.11	x86_64	agent.p5p.gz	/software/agent/Solaris_5.11/x86_64/agent.p5p.gz
		Solaris_5.11	スパーク	agent.p5p.gz	/software/agent/Solaris_5.11/sparc/agent.p5p.gz
	Solaris 11 Update 4	Solaris_5.11_U4	x86_64	agent.p5p.gz	/software/agent/Solaris_5.11_U4/x86_64/agent.p5p.gz
		Solaris_5.11_U4	スパーク	agent.p5p.gz	/software/agent/Solaris_5.11_U4/sparc/agent.p5p.gz
	AIX 5.3	AIX_5.3	power	agent.bff.	/software/agent/AIX_

プラットフォーム	配信	<プラットフォーム>	<アーチ>	<ファイル名>	例
	(Deep Security Agent 9.0)		pc	gz	5.3/powerpc/agent.bff.gz
	AIX 6.1 (Deep Security Agent 9.0)	AIX_6.1	power pc	agent.bff.gz	/software/agent/AIX_6.1/powerpc/agent.bff.gz
	AIX 7.1,2.2 (Deep Security Agent 9.0)	AIX_7.1	power pc	agent.bff.gz	/software/agent/AIX_7.1/powerpc/agent.bff.gz
	AIX 6.1,7.1,7.2(Deep Security Agent 12 以降)	AIX	power pc	agent.bff.gz	/software/agent/AIX/powerpc/agent.bff.gz

例

<agent version>がない場合

- https://example.com:4119/software/agent/RedHat_EL7/x86_64/agent.rpm
- https://example.com:4119/software/agent/Windows/x86_64/agent.msi

<agent version>:

- https://example.com:4119/software/agent/RedHat_EL7/x86_64/12.0.0.481/agent.rpm
- https://example.com:4119/software/agent/Windows/x86_64/12.0.0.481/agent.msi

下位互換性の除外設定

[...]/<platform>/<arch>/の後に<filename>が指定されていない場合、マネージャは前の表の説明に従って、そのプラットフォームのエージェントのダウンロードを返します。

[...]<platform>/<arch>でパスが終了した場合(<agent version>と<filename>の両方が), に指定されていないため、マネージャはそのプラットフォームのエージェントのダウンロードを上記の表に従って返します。

例:

- https://example.come:4119/software/agent/RedHat_EL7/x86_64/
- https://example.come:4119/software/agent/Windows/x86_64

エージェントバージョンコントロールを使用して、返されるエージェントバージョンを定義する

エージェントバージョンコントロールの機能を使用すると、エージェントをダウンロードするためのURL要求がDeep Securityに送信されたときに、どのエージェントが返されるかを制御できます。

エージェントのバージョン管理を有効にするには、URL要求を使用して次のHTTPヘッダを送信します。

Agent-Version-Control: on

エージェントバージョン管理を使用するには、各プラットフォームでも必要な特定のクエリパラメータがあることに注意してください。彼らは次のとおりです。

プラットフォーム	必須のクエリパラメータ	例
Windows	tenantID, windowsVersion, windowsProductType	/software/agent/Windows/x86_64/agent.msi?tenantID=123&windowsVersion=10.0.17134&windowsProductType=3
Linux	テナントID	/software/agent/RedHat_EL7/x86_64/agent.rpm?tenantID=123
Solaris	テナントID	/software/agent/Solaris_5.11_U4/x86_64/agent.p5p.gz?tenantID=123

プラットフォーム	必須のクエリパラメータ	例
AIX	tenantID、aixVersion、aixRelease	/software/agent/AIX/powerpc/agent.bff.gz?tenantID=123&aixVersion=7&aixRelease=1

注意: 上記の表のパラメータは、配信スクリプトによって自動的に生成されます。

例

例については、Managerから生成されたデプロイスクリプトの例を参照してください。初期設定では、マネージャによって生成された配信スクリプトはエージェントバージョン管理を使用し、プラットフォームごとにこれらのパラメータを取得する方法を示します。

<エージェントバージョン>パラメータとエージェントバージョン管理の間の相互作用

エージェントのバージョン管理機能の目的は、どのエージェントのバージョンが返されるかをDeep Security管理者が制御できるようにすることです。また、<agent version>パラメータも含まれるURL要求との自然な競合が発生します。

このため、 Agent-Version-Control: on HTTPヘッダの送信時に <agent version>を要求の一部として指定しないでください。

我々は要求の両方Agent-Version-Control: on HTTPヘッダと<agent version>パラメータが表示されている場合、返されたエージェントのバージョンは、エージェントバージョンコントロールから採取された値によって決定されるであろう設定。(URL<Hの<エージェントバージョン>は無視されます。

クラウドプロバイダーのタグ/ラベルを使用してポリシーを自動的に割り当てる

AWSタグ、Azureタグ、およびGCPラベルを使用すると、メタデータをAWSEC2インスタンス, Azure VM、またはGCPVMインスタンスにキーと値の形式で割り当てることでリソースを分類できます。同様にキーと値のペアでAmazon WorkSpacesのタグ付けもできます。Deep Securityは、このメタデータを使用して、Deep Securityエージェントがアクティブ化されたときに、そのエージェントへのポリシーの自動割り当てをトリガーできます。これは、Deep Securityでイベントベースのタスクを作成し、イベント、ポリ

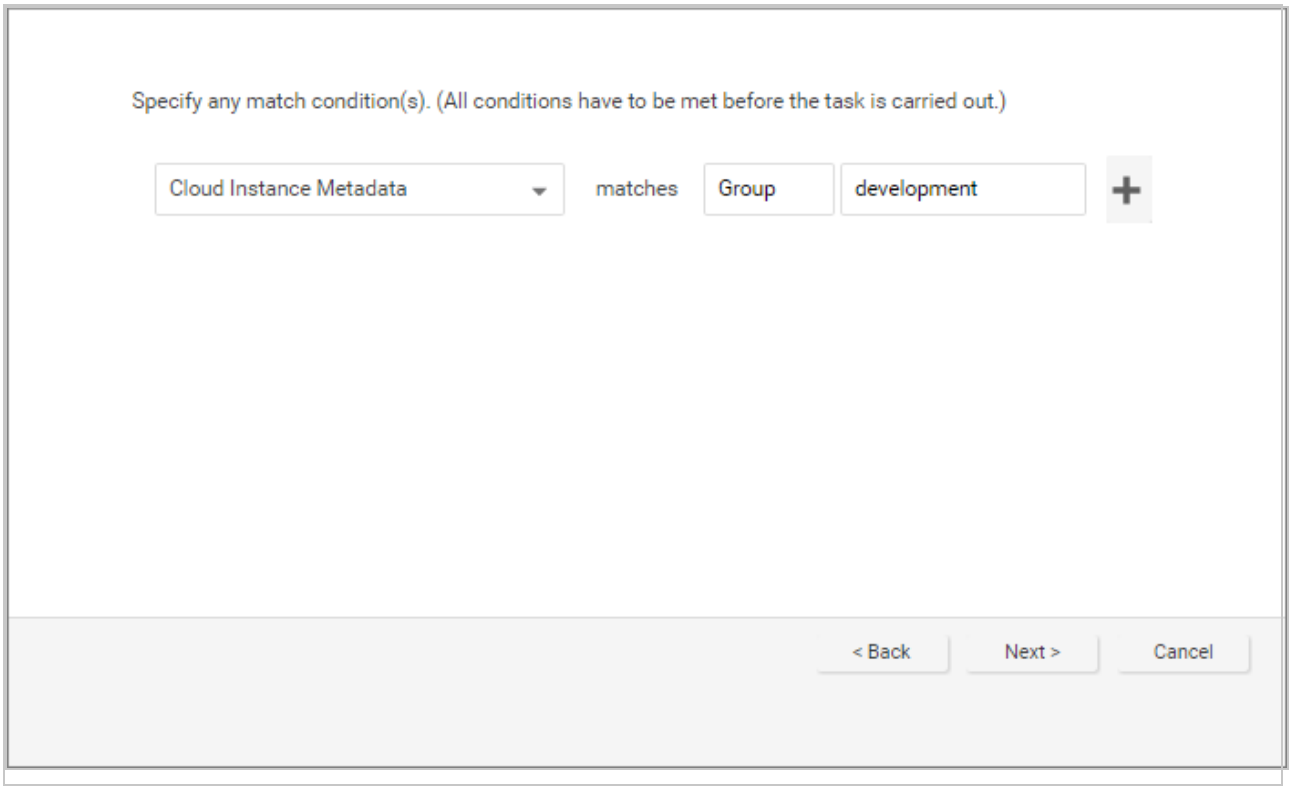
シー、およびメタデータを定義することによって行われます。イベントベースタスクは、特定のイベントについて保護対象リソースを監視し、所定の条件に応じてタスクを実行するために使用します。このケースでは、Agentからのリモート有効化がイベントで、特定のAWSインスタンスタグが条件です。

ここでは、次の例を使用して手順を説明します。

- ポリシー:AIA_Policy
- AWSタグキー: Group
- AWSタグ値: development

注意: 以下の例は、ポリシーAIA_Policyがすでに作成されていることを前提とします。

1. Deep Security Managerコンソールで管理→イベントベースタスクに移動し、新規をクリックします。
2. [イベント] リストから[Agentからのリモート有効化] を選択し、[次へ] をクリックします。
3. [ポリシーの割り当て] チェックボックスを選択し、リストからAIA_Policyを選択し、[次へ] をクリックします。
4. リストからクラウドインスタンスのメタデータを選択し、キーフィールドにグループと入力し、値フィールドに開発と入力します。



5. (オプション) スコープを1つのクラウドベンダーのみに制限するには、リストからクラウドベンダーを選択し、一致基準としてAWS, Azureまたは GCP を選択します。3つすべてにルールを適用する場合は、クラウドベンダーの条件を定義しないでください。
6. Next をクリックします。
7. イベントベースタスクに名前を指定し、[完了] をクリックして保存します。

以上で、キー「Group」と値「development」でタグ付けされたインスタンスでAgentが有効化された時にそのインスタンスにAIA_Policyを適用するイベントベースタスクが作成されました。

信頼とコンプライアンス

コンプライアンスについて

トレンドマイクロは、複数のセキュリティコントロールを1つの製品に統合してコンプライアンスを推進し、包括的な監査とサポートを提供します。詳細については、トレンドマイクのWebサイトにある「Regulatory Compliance」を参照してください。

要件に応じて、次を参照してください。

- "Deep SecurityによるPCI DSS要件への対応" on page 1865
- "コモンクライテリアの設定" on page 1865
- "GDPR" on page 1869
- "FIPS 140のサポート" on page 1870
- AWS Config Rulesの設定
- "Deep Securityでの脆弱性管理検索トラフィックのバイパス" on page 1881
- "Deep SecurityでのTLS 1.2の使用" on page 1883
- "TLS 1.2の強力な暗号化スイートの有効化" on page 1897

エージェントパッケージの整合性チェック

Deep Securityは、ソフトウェア・ファイルが署名時以降に変更されていないことを確実にするためのDeep Security Agentであなたの署名を検証します。整合性チェックは次の場合に実行されます。

1. Deep Security Agentをアップグレードしています。
2. カーネルサポートがアップデートされるように、新しいセキュリティモジュールを有効にしています。

検証が失敗した場合は、プラグインのインストールとエージェントのアップグレードがブロックされています。

トラブルシューティング

ID	イベント	Reason	ソリューション
5302	Agent/Plugin パッケージの署名のダウンロードに失敗しました。	エージェントの整合性チェックに使用されるシグネチャファイルは、アップデート元から入手できません。Deep Security Relayは、必要なバージョンにアップグレードされない可能性があります。	1. アラートページで、「Relayエージェントの整合性チェックに必要なアップグレード」アラートがないかどうかを確認します。アラートが存在する場合は、"サポートされるDeep Security Relayのバージョン" on the next page と"Deep Security Relay" on page 1675。署名ファイルがアップデート元に同期されていることを確認します。 2. 署名ファイルがアップデート元に同期されていることを確認してください。 3. エージェントをアップグレードするか、アップデートしたポリシーを再度送信してください。 4. 問題が解決しない場合は、"診断パッケージの作成" on page 2019、トレンドマイクロのサポートチームに送信してください。
5300	Agent/Plugin パッケージ署名の検証に失敗しました。	エージェントパッケージが改ざんされているか、パッケージに問題がある可能性があります。	1. アップデート元から改ざんされている可能性のあるファイルをバックアップして削除します。 2. Deep Security Managerから対応するエージェントパッケージを削除します。 3. エージェントパッケージをダウンロードセンターから再ダウンロードし、Deep Security Managerにインポートします。 4. パッケージがアップデート元に同期されていることを確認します。 5. エージェントをアップグレードするか、アップデートしたポリシーを再度送信してください。 6. 問題が解決しない場合は、"診断パッケージの作成" on page 2019、トレンドマイクロのサポートチームに送信してください。
5301	Agent/Plugin パッケージの検証に失敗しました。		
5303	Agent/Plugin パッケージのシグネチャがポリシー内のシグネチャと一致しません。		

サポートされるDeep Security Relayのバージョン

次のDeep Security Relay のバージョンがサポートされています。

- Deep Security 20
- Deep Security FR 2020-04-16(12.5.0.834)(Windows)
- Deep Security FR 2020-05-19(12.5.0.936)(Linux)
- Deep Security 12.0 update 8(12.0.0.967)
- Deep Security 11.0 Update 23(11.0.1617)

Deep SecurityによるPCI DSS要件への対応

Payment Card Industry Data Security Standard (PCI DSS) は、カード所有者のデータの安全を促進する情報セキュリティ基準です。Deep Securityを使用すると、PCI DSSに従ってPCIデータを保護できます。

ヒント:
PCI コンプライアンスについては、「AWSでのPCI DSSコンプライアンス」および「"Deep Securityでの TLS 1.2の使用" on page 1883」または「"TLS 1.2の強力な暗号化スイートの有効化" on page 1897」も参照してください。

コモンクライテリアの設定

Common Securityの証明書がDeep Security 20に発行されました。コモンクライテリア は、コンピュータセキュリティ認証の国際標準です。このトピックでは、コモンクライテリア評価保証レベル2以上の認定を受けた構成(CC EAL2 +) でDeep Securityを配置する方法について説明します。*Deep Security 20 Security Target* のドキュメントと組み合わせて使用します。

Deep Security 20の証明書レポートおよびDeep Security 20のセキュリティ対象への直接リンクは、次の場所にあります。

Deep Security 20証明書レポート。

Deep Security 20 Security Target。

注意: コモンクライテリア標準の一部として、Deep Securityの管理者は組織のセキュリティポリシーと手順を十分に理解し、Deep Securityの使用方法に関するトレーニングを受け、このガイドに記載

されたガイダンスに従ってDeep Securityを設定できることが求められます。この記事とDeep Security 20の残りのドキュメントを参照してください。

CC EAL2 +認証済みの設定を配信するには、次の手順に従います。特に明記されていないかぎり、すべての手順が必須です。

- "手順1: Deep Securityのインストール" below
- "手順2: FIPSモードを有効にする" on the next page
- "手順3: 不正アクセスを防ぐためにDeep Securityを強化する" on the next page
- "手順4: 強力なパスワードポリシーを適用する" on page 1868
- "手順5: 従来のAPIを無効にする" on page 1868
- "手順6: アラートのメール通知を設定する" on page 1868
- "次の手順(動作確認済みの設定での運用)" on page 1869

手順1: Deep Securityのインストール

このヘルプセンターの他のセクションの手順に従って、通常どおりにDeep Securityソフトウェアをインストールして設定します。Common Criteria認定の設定で配信するには、Deep Security Download Centerから評価済みのソフトウェアバージョンをダウンロードしてインストールします。

インストール時には、次のことを確認してください。

- Deep Security Manager、そのデータベース、Deep Security Virtual Appliance、ESXiサーバ、vCenter、vShield Manager、およびNSX Managerを格納する施設は、すべて物理的に安全です。
- Deep Security Managerは、他の主要なアプリケーションがインストールされたコンピュータで実行されておらず、組織のベストプラクティスに従って強化されています。
- Deep Security Managerコンピュータは、受信および送信トラフィックが厳格に制御される隔離されたネットワークセグメント内に配置されます。
- Managerコンピュータにアクセスできるのは、正しい管理権限を持つ許可されたユーザのみです。
- エージェントとRelayコンピュータにアクセスできるのは、許可されたユーザのみです。
- この環境は、信頼性が高く安全なドメインネームサーバ(DNS)サービスとネットワークタイムプロトコル(NTP)サービスを提供します。
- VMware仮想インフラストラクチャ(ESXiサーバ、vCenter、vShield Manager、NSX Manager)は十分に強固で、盗難から保護されています。

- Deep Security Virtual Applianceの管理インタフェースは、隔離された内部のみのネットワーク上に存在します(アクセスが制限されます) 。
- Deep Security Virtual Applianceは、不正プログラム対策 のみを提供します。侵入防御 (IPS) などの他のモジュールが必要な場合は、Deep Security AgentとApplianceをコンバインモードで使用します。"Agentレスによる保護 またはコンバインモードの保護の選択" on page 569を参照してください。
- ドメインネームサーバ(DNS) の応答時間は妥当です。Deep Securityには、DNS応答時間が非常に遅い場合に一部の不正プログラムが検出されないという既知の問題があります。

注意: コモンクライテリアの設定では、日本語に対するShift JIS(Shift_JIS) 文字エンコードの使用はサポートされていません。

このトピックの残りの手順では、コモンクライテリアが評価された設定に到達するために、初期インストールおよび設定に対して行う必要のある変更について説明します。

手順2: FIPSモードを有効にする

Deep SecurityがFIPS 140モードで動作するように設定する必要があります。手順については、「"FIPS 140のサポート" on page 1870 」を参照してください。かなりの数の手順、制限、および要件があります。たとえば、Deep Security Scanner (SAP Netweaverとの統合) はサポートされていません。FIPSのすべての手順、制限、および要件が適用されます。

"FIPS 140のサポート" on page 1870 ページに記載されているタスクを完了するほかに、次のことも実行する必要があります。

- SQL ServerでTLSをバージョン1.2に制限します。詳細については、「 KB3135244-TLS 1.2 support for Microsoft SQL Server from Microsoft」を参照してください。
- 保護対象のOSでFIPSモードを有効にします。WindowsでFIPSモードを有効にする手順については、MicrosoftのFIPS 140検証を参照してください。

手順3: 不正アクセスを防ぐためにDeep Securityを強化する

Deep Securityコンポーネントを強化して、脆弱性の影響を軽減し、不正アクセスを防止する必要があります。システムを強化するには、以下のリンクに従ってください。これらのタスクの一部は、FIPSモードの設定時に完了している場合があります。

必須の強化タスク:

- "Deep Security Managerとデータベース間の通信の暗号化" on page 1633
- Deep Securityデータベースの強化¯SQL Serverを使用している場合は、「Microsoft SQL Serverの保護」を参照してください。
- "Deep Security ManagerのTLS証明書を変更します。" on page 1622
- "Agentを使用したDeep Security Managerの保護" on page 1617
- Deep Securityリリースノートを確認して、セキュリティ関連の既知の問題を回避してください。

オプションの強化タスク:

- Deep Security Agentを特定のManagerにバインドする
- "エージェントセルフプロテクションを有効化または無効化する" on page 1517を有効または無効にします(オプションで有効にします)。

手順4:強力なパスワードポリシーを適用する

強力なパスワードポリシーを適用する必要があります。詳細については、"ユーザパスワードルールの適用" on page 1647を参照してください。ポリシーには、少なくとも次の特性が必要です。

- ユーザパスワードの最小文字数は、初期設定の8文字以上である必要があります。
- ログオン失敗の許容回数(ロックアウト前)は初期設定の5回を超えてはなりません。

手順5:従来のAPIを無効にする

次の手順に従って、SOAPおよびステータス監視APIを無効にする必要があります。

1. [Deep Security Manager]で、[管理]→[システム設定]→[詳細]の順にクリックします。
2. [SOAP Webサービス API]セクションで、[無効]を選択します。
3. [ステータス監視API]セクションで、[無効]を選択します。
4. 保存をクリックします。

手順6:アラートのメール通知を設定する

すべての通知の送信先メールアドレスを設定する必要があります。"アラートのメール通知を設定する" on page 1294」を参照してください。初期設定では、アラートごとにDeep Security Managerからメール通知が送信されます。初期設定のアラート通知は無効にしないでください。

次の手順(動作確認済みの設定での運用)

認定された設定でDeep Securityを使用するには、次のことを確認してください。

- 追加ユーザのアカウントを作成する

  管理アカウント(初期設定ではMasterAdmin)は、Deep Security Managerのインストール時に作成されたものです。追加のユーザ用に新しいアカウントを作成し、Deep Securityのインストールを担当する元の管理者のみがMasterAdminアカウントをバックアップとして使用するようにします。その他のアカウントは、継続的な管理および設定タスクに使用します。

- Deep Security Managerのコマンドラインインターフェイス(dsm_c)の使用を停止します

  このインタフェースは、Managerの初期インストールおよび設定では使用できますが、CC EAL2 +認証の設定には含まれていないため、以降は使用しないでください。

- Deep Security Agentのコマンドラインインタフェース(dsa_controlおよびdsa_query)の使用を停止します。

  これらのインタフェースは、エージェントの初期インストール時および設定時に許可されますが、CC EAL2 +認証の設定には含まれないため、その後は使用しないでください。

- 通常の操作中はDeep Security Virtual Applianceをシャットダウンしないでください。

  不明な理由でアプライアンスがオフラインのように見える場合は、常に原因を調査してください。

GDPR

欧州連合(EU)の一般データ保護規則(GDPR)では、EU市民のデータを処理している世界各地の組織に対し、データ処理の管理方法の見直しとデータ保護を強化するための計画の実施が義務付けられています。GDPRとトレンドマイクロの詳細については、トレンドマイクロのGDPRへの準拠に関するWebサイトを参照してください。

Deep Securityでの個人情報データの収集の詳細については、"プライバシーと個人データの収集に関する規定 " on page 1903を参照してください。

FIPS 140のサポート

連邦情報処理規格 (FIPS) は暗号化モジュールのための一連の標準です。詳細については、米国国立標準技術研究所 (NIST) のウェブサイトをご覧ください。Deep Security は、暗号化モジュールが FIPS 140 標準に準拠したモードで動作するようにする設定を提供します。トレンドマイクロは、Java 暗号化モジュールとネイティブ暗号化モジュール (OpenSSL) の認証を取得しています。

現在、Deep Security は FIPS 140-2 標準に対応しています。FIPS-140 の新しいバージョンがリリースされると、トレンドマイクロはそれらの標準をサポートするための認証を取得します。

FIPS以外のモードとFIPSモードで実行するDeep Securityインストールにはいくつかの違いがあります。詳細については、"Deep SecurityをFIPSモードで操作する際の違い" on the next pageを参照してください。

Deep Security Manager SSL証明書を置き換える場合は、FIPSモードを有効にする前に行ってください。FIPSモードの有効化後に証明書を置き換える必要がある場合は、FIPSモードを無効にし、"Deep Security ManagerのTLS証明書を変更します。" on page 1622の手順を実行してから、FIPSモードを再び有効にします。

Deep SecurityをFIPS 140モードで動作させるには、次の手順を実行します。

1. Deep SecurityをFIPSモードで動作させる場合の"Deep SecurityをFIPSモードで操作する際の違い" on the next pageを確認し、FIPS 140モードで動作する場合に必要なDeep Security機能を使用できることを確認します。
2. Deep Security ManagerおよびDeep Security Agentが"FIPSモードのシステム要件" on the next pageに一致していることを確認します。
3. "Deep Security ManagerでFIPSモードを有効にする" on page 1873。
4. Deep Security ManagerはSSLを使用して外部サービス (Active Directory、vCenter、またはNSX Managerなど) に接続する必要がある場合は、"FIPSモードで外部サービスに接続する" on page 1873を参照してください。
5. "保護しているコンピュータのOSのFIPSモードを有効にする" on page 1874。
6. "保護しているコンピュータでDeep Security AgentのFIPSモードを有効にする" on page 1875
7. "Deep Security Virtual ApplianceでFIPSモードを有効にする" on page 1876。
8. Red Hat Enterprise Linux (RHEL) 7.0 GAなど、Linuxカーネルのいくつかのバージョンでは、FIPSモードを有効にするためにSecure Bootを有効にする必要があります。手順については、「"AgentのLinux Secure Bootの設定" on page 520」を参照してください。

"FIPSモードを無効にする" on page 1880こともできます。

Deep SecurityをFIPSモードで操作する際の違い

次の内容はDeep Security Manager 20.0.619 (20 LTS Update 2022-03-22) 以降で利用可能です:

- ロードバランサ設定、[管理]→[システム設定]→[詳細]→[ロードバランサ]からアクセス可能。
- STARTTLS オプションは、[管理]→[システム設定]→[SMTP] からアクセスできます。
- マルチテナント環境。

FIPSモードで操作している場合、次の機能は利用できません:

- "VMware vCloudでホストされる仮想マシンの追加" on page 710の説明に従った、VMware vCloudでホストされた仮想マシンへの接続。また、[管理]→[システム設定]→[Agent]→[Agentレスによるの保護] 設定も使用できません。
- Deep Security Scanner (SAP Netweaverとの統合)。
- 脅威インテリジェンス。

Deep Security ManagerでFIPSモードが有効になっているか確認する

Deep Security ManagerでFIPSモードが有効かどうかを確認するには、管理 > システム情報に移動します。システム詳細の下で、マネージャノードを展開します。FIPSフィールドは、FIPSモードが有効か無効かを示します。

Deep Security ManagerでFIPSが有効になっている場合複数のノードにデプロイ、すべてのマネージャノードで FIPS が有効になっている必要があります。

FIPSモードのシステム要件

Deep Security Managerの要件

FIPSモードを有効にしたDeep Security Managerの要件は、いくつかの例外を除き、「"システム要件 " on page 400」で説明されている要件と同じです。

次のオペレーティングシステムのみがサポートされています。

- Red Hat Enterprise Linux 10 (64-bit)
- Red Hat Enterprise Linux 9 (64ビット)
- Red Hat Enterprise Linux 8 (64ビット)

- Red Hat Enterprise Linux 7 (64ビット)
- Windows Server 2019 (64ビット)
- Windows Server 2016 (64ビット)
- Windows Server 2012または2012 R2 (64ビット)

次のデータベースのみがサポートされます。

- PostgreSQL 17 ("FIPSモードをPostgreSQLデータベースで使用する" on page 1876を参照)
- PostgreSQL 16 ("FIPSモードをPostgreSQLデータベースで使用する" on page 1876を参照)
- PostgreSQL 15 ("FIPSモードをPostgreSQLデータベースで使用する" on page 1876を参照)
- PostgreSQL 14 ("FIPSモードをPostgreSQLデータベースで使用する" on page 1876を参照)
- Microsoft SQL Server 2019 Enterprise Edition ("Microsoft SQL ServerデータベースでFIPSモードを使用する" on page 1879を参照)
- Microsoft SQL Server 2016 Enterprise Edition ("Microsoft SQL ServerデータベースでFIPSモードを使用する" on page 1879を参照)
- Microsoft SQL Server 2014 Enterprise Edition ("Microsoft SQL ServerデータベースでFIPSモードを使用する" on page 1879を参照)
- Microsoft SQL Server 2012 Enterprise Edition ("Microsoft SQL ServerデータベースでFIPSモードを使用する" on page 1879を参照)

SSL接続でFIPSモードを有効にしていても、Oracle Databaseはサポートされません。

Microsoft SQL Serverの名前付きパイプはサポートされません。

AWS MarketplaceはFIPSモードをサポートしていません。

Deep Security Agentの要件

FIPSモードを有効にしたDeep Security Agentは、「"システム要件 " on page 400」で説明されている要件と同じです。FIPSモードは、一部のOSのみでサポートされています。この機能をサポートしているOSについては、"各プラットフォームでサポートされている機能" on page 417を参照してください。

Deep Security Virtual Applianceの要件

Virtual AppliancesでFIPSモードをサポートするための要件は、次のとおりです。

- Deep Security Manager 11.0 Update 3以降。
- Deep Security Virtual Appliance 10.0または11.0以降。

- Deep Security Agent 11.0 for RedHat_EL7以降 (Applianceの組み込みのAgentとして使用されます。)

Applianceのシステム要件の詳細については、"システム要件 " on page 400を参照してください。

Deep Security ManagerでFIPSモードを有効にする

WindowsでDeep Security ManagerのFIPSモードを有効にする

1. Microsoft管理コンソールのサービス画面を使用してTrend Micro Deep Security Managerサービスを停止します。
2. Windowsコマンドラインで、Deep Security Managerの作業用フォルダに移動します。例: `C:\Program Files\Trend Micro\Deep Security Manager`。
3. 次のコマンドを入力して、FIPSモードを有効にします。

   ```
   dsm_c -action enablefipsmode
   ```

4. Deep Security Managerサービスを再起動します。

LinuxでDeep Security ManagerのFIPSモードを有効にする

1. Deep Security Managerコンピュータで、コマンドラインを開き、Deep Security Managerの作業フォルダ(`/opt/dsm`など) に移動します。
2. 次のコマンドを入力して、Deep Security Managerサービスを停止します。

   ```
   service dsm_s stop
   ```

3. 次のコマンドを入力して、FIPSモードを有効にします。

   ```
   dsm_c -action enablefipsmode
   ```

4. 次のコマンドを入力して、Deep Security Managerサービスを再起動します。

   ```
   service dsm_s start
   ```

FIPSモードで外部サービスに接続する

Deep Security ManagerがFIPSモードで動作していて、SSL接続を使用して外部サービス(Active Directory、vCenter、またはNSX Managerなど) に接続する場合は、事前にその外部サービスのSSL

証明書をManagerにインポートする必要があります。それに接続しています。証明書をインポートする手順については、"信頼された証明書の管理" on page 1653を参照してください。

Active Directoryからコンピュータをインポートする手順については、"Active Directoryコンピュータを追加する" on page 659を参照してください。

ユーザ情報とActive Directoryを同期する手順については、"ユーザの追加と管理" on page 1537を参照してください。

Deep Security ManagerにVMware vCenterを追加する手順については、"vCenter - FIPSモードを追加する" on page 709を参照してください。

保護しているコンピュータのOSのFIPSモードを有効にする

サポートされているオペレーティングシステムでFIPSモードを有効にする手順については、オペレーティングシステムのプロバイダが提供する次のドキュメントを参照してください。

- Windows: システム暗号化: Windows XPおよびそれ以降のバージョンのWindowsでの暗号化、ハッシュ化、および署名のセキュリティ設定にFIPS準拠のアルゴリズムを使用する
- RHEL 7またはCentOS 7: 連邦規格および規制 および RHEL 6またはRHEL 7 FIPS 140-2準拠のを作成する方法
- RHEL 8: RHEL 8はFIPS 140-2要件に対応するように設計されています
- RHEL 9: RHELをFIPSモードに切り替える
- RHEL 10: RHELをFIPSモードに切り替える
- Amazon Linux 2: Amazon Linux 2でFIPSモードを有効にする
- Amazon Linux 2023: Amazon Linux 2023でFIPSモードを有効にする
- SUSE Linux Enterprise Server 12: SUSE Linux Enterprise Server 12でFIPSモードを有効にする
- SUSE Linux Enterprise Server 15: SUSE Linux Enterprise Server 15でFIPSモードを有効にする
- Oracle Linux 8: Oracle Linux 8 - システムセキュリティの強化
- Oracle Linux 10: Oracle Linux 10 - システムセキュリティの強化
- Rocky Linux 9: FIPS準拠のLinuxマシンを構成する
- Rocky Linux 10: FIPS準拠のLinuxマシンを構成する
- Miracle Linux 8: RHEL 8ドキュメントを使用したFIPSモードでのシステムのインストール
- Miracle Linux 9: RHEL 9ドキュメントを使用したFIPSモードでのシステムのインストール

- Debian Linux 10: DebianでFIPSモードを有効にする
- Debian Linux 11: DebianでFIPSモードを有効にする
- Debian Linux 13: DebianでのFIPSモードの有効化

保護しているコンピュータでDeep Security AgentのFIPSモードを有効にする

次の情報は、Deep Security ManagerでFIPSモードを有効にした後にインストールするDeep Security 11.0以降のエージェントには適用されません。これらのバージョンでは、エージェントに対してFIPSモードが既に有効になっています。

Windows AgentのFIPSモードを有効にする

1. Windowsシステムのルートフォルダ(C:\Windowsなど)で、ds_agent.iniという名前のファイルを探します。テキストエディタで既存のファイルを開くか、新しいファイルを作成します。
2. ファイルに次の行を追加します。

   ```
   FIPSMode=1
   ```

3. Deep Security Agentサービスを再起動します。

Linux AgentでFIPSモードを有効にする

サポートされているLinuxエージェントは次のとおりです: RHEL 7、RHEL 8、RHEL 9、RHEL 10、CentOS 7、Amazon Linux 2、Amazon Linux 2023、Ubuntu 18、Ubuntu 20、SUSE Linux 12、SUSE Linux 15、Oracle Linux 8、Oracle Linux 10、Rocky Linux 9、Rocky Linux 10、Miracle Linux 8、Miracle Linux 9、Debian Linux 10、Debian Linux 11、Debian Linux 13。

1. /etc/でds_agent.confという名前のファイルを探します。テキストエディタでファイルを開くか、まだファイルがない場合は新しいファイルを作成します。
2. ファイルに次の行を追加します。

   ```
   FIPSMode=1
   ```

3. Deep Security Agentを再起動します。

   SysV initスクリプトの使用：/etc/init.d/ds_agent restart

   systemdコマンドの使用：systemctl restart ds_agent

Ubuntu 18またはUbuntu 20でFIPSモードを有効にする方法の詳細については、「FIPS for Ubuntu」を参照してください。

Deep Security Virtual ApplianceでFIPSモードを有効にする

1. <DSVA_root>/etc/で、ds_agent.confという名前のファイルを探します。テキストエディタで既存のファイルを開くか、新しいファイルを作成します。
2. ファイルに次の行を追加します。

   FIPSMode=1

3. コマンドラインからApplianceを再起動します。

   SysV initスクリプトの使用：/etc/init.d/ds_agent restart

   systemdコマンドの使用：systemctl restart ds_agent

FIPSモードをPostgreSQLデータベースで使用する

Deep Security Managerデータベースとして PostgreSQLを使用している場合は、「"データベースの要件" on page 452」に記載されている要件に加えて、別の要件があります。

FIPSモードでは、キーストアはBCFKSタイプである必要があります。Javaの初期設定のキーストア(C:\Program Files\Trend Micro\ Deep Security Manager\jre\lib\security\cacertsまたは/opt/dsm/jre/lib/security/cacerts)を直接変換する代わりに、初期設定のキーストアを別の場所にコピーして、SSLの初期設定のキーストアとして使用します。接続:

1. PostgreSQL環境を作成します。
2. PostgreSQLサーバからserver.crtファイルをコピーし、<Deep_Security_Manager_install_folder>に貼り付けます。
3. Deep Security Managerをインストールします。
4. "Deep Security ManagerでFIPSモードを有効にする" on page 1873。
5. 初期設定のJava cacertsファイルをDeep Security Managerのルートインストールフォルダにコピーします。

   Windowsの場合:

   ```
   copy "C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\security\cacerts" "C:\Program Files\Trend Micro\Deep Security Manager\cacerts"
   ```

   Linuxの場合:

```
cp "/opt/dsm/jre/lib/security/cacerts" "/opt/dsm/cacerts"
```

6. キーストアファイルをJKSからBCFKSに変換します。次のコマンドは、Deep Security Managerのインストールフォルダにcacerts.bcfksファイルを作成します。

   Windowsの場合:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Manager\jre\scripts
   ```

   ```
   keytool_fips.cmd -importkeystore -srckeystore "C:\Program Files\Trend Micro\Deep Security Manager\cacerts" -srcstoretype JKS -deststoretype BCFKS -destkeystore "C:\Program Files\Trend Micro\Deep Security Manager\cacerts.bcfks" -srcstorepass <changeit> -deststorepass <changeit>
   ```

   *<changeit>*の部分は、適切な値に置き換えてください。

   Linuxの場合:

   ```
   cd /opt/dsm/jre/scripts
   ```

   ```
   keytool_fips.sh -importkeystore -srckeystore "/opt/dsm/cacerts" -srcstoretype JKS -deststoretype BCFKS -destkeystore "/opt/dsm/cacerts.bcfks" -srcstorepass <changeit> -deststorepass <changeit>
   ```

   *<changeit>*の部分は、適切な値に置き換えてください。

7. 証明書をインポートします "Deep_Security_Manager_root_folder/server.crt"

   Windowsの場合:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Manager\jre\scripts
   ```

   ```
   keytool_fips.cmd -import -alias psql -file "C:\Program Files\Trend Micro\Deep Security Manager\server.crt" -keystore "C:\Program Files\Trend Micro\Deep Security Manager\cacerts.bcfks" -storepass <changeit> -storetype BCFKS
   ```

   *<changeit>*の部分は、適切な値に置き換えてください。

   Linuxの場合:

   ```
   cd /opt/dsm/jre/scripts
   ```

   ```
   keytool_fips.sh -import -alias psql -file "/opt/dsm/server.crt" -keystore "/opt/dsm/cacerts.bcfks" -storepass <changeit> -storetype BCFKS
   ```

   *<changeit>*の部分は、適切な値に置き換えてください。

8. Deep Securityインストーラは.vmoptionsファイルを使用してJVMパラメータを割り当てる必要があります

   Windowsの場合、Deep Security Manager.vmoptions という名前のファイルをインストールフォルダに作成し、次のテキストをファイルに追加します。

   ```
   -Djavax.net.ssl.keyStoreProvider=BCFIPS
   -Djavax.net.ssl.trustStore=C:\Program Files\Trend Micro\Deep Security Manager\cacerts.bcfks
   -Djavax.net.ssl.trustStorePassword=<changeit>
   -Djavax.net.ssl.keyStoreType=BCFKS
   -Djavax.net.ssl.trustStoreType=BCFKS
   ```

   *<changeit>*の部分は、適切な値に置き換えてください。

   Linuxの場合、インストールフォルダにdsm_s.vmoptionsという名前のファイルを作成して、そのファイルに次の文字列を追加します。

   ```
   -Djavax.net.ssl.keyStoreProvider=BCFIPS
   -Djavax.net.ssl.trustStore=/opt/dsm/cacerts.bcfks
   -Djavax.net.ssl.trustStorePassword=<changeit>
   -Djavax.net.ssl.keyStoreType=BCFKS
   -Djavax.net.ssl.trustStoreType=BCFKS
   ```

   *<changeit>*の部分は、適切な値に置き換えてください。

9. <Deep Security Managerのディレクトリ>\webclient\webapps\ROOT\WEB-INF\dsm.propertiesファイルをテキストエディタで開いて次の文字列を追加します。

   Windowsの場合:

   ```
   database.PostgreSQL.connectionParameters=sslmode=verify-ca&sslcert=C\:\\Program Files\\Trend Micro\\Deep Security Manager\\server.crt
   ```

   Linuxの場合:

   ```
   database.PostgreSQL.connectionParameters=sslmode=verify-ca&sslcert=/opt/dsm/server.crt
   ```

10. テキストエディタで/opt/postgresql/data/postgresql.confファイルを開いて、次の文字列を追加します

```
ssl= on
ssl_cert_file= 'server.crt'
ssl_ksy_file= 'server.key'
```

11. PostgreSQLを再起動してから、Deep Security Managerサービスを再起動します。
12. 接続を次のように確認します

```
cd /opt/postgresql/bin
./psql -h 127.0.0.1 -Udsm dsm
```

求められたらパスワードを入力してください。次のように表示されます:

```
dsm=> select a.client_addr, a.application_name, a.usename, s.* from pg_stat_ssl s join pg_stat_
activity a using (pid) where a.datname='dsm';
```

Microsoft SQL ServerデータベースでFIPSモードを使用する

Deep Security ManagerデータベースとしてMicrosoft SQL Serverを使用している場合は、FIPSモードを有効にする前に、次の手順に従ってデータベースのSSL暗号化を設定する必要があります。

1. Deep Security Managerサービスを停止します。
2. SQLサーバ証明書を使用してBCFKSキーストアファイルを作成します。`C:\Program Files\Trend Micro\Deep Security Manager\jre\scripts`の`keytool_fips.cmd`を使用できます。
3. 次のコマンドを使用してSQL Server証明書 `C:\sqlserver_cert.cer` を新しいKeystoreファイル `C:\Program Files\Trend Micro\Deep Security Manager\mssql_keystore.bcfks` にインポートします。

   ```
   keytool_fips.cmd -import -alias mssql -file "C:\sqlserver_cert.cer" -keystore "C:\Program Files\Trend Micro\Deep Security Manager\mssql_keystore.bcfks" -storepass <changeit> -storetype BCFKS
   ```

   *<changeit>*の部分は、適切な値に置き換えてください。

   両方の `keytool_fips.cmd` および `keytool_fips.sh` ファイルは、DSM 20.0.970 以降のバージョンでのみ利用可能です。これらのファイルがDSMインストールに含まれていない場合は、トレンドマイクロサポートに連絡してください。

   インポートプロセス中に、[はい] を選択してこの証明書を信頼します。

4. キーストアファイルが正常に作成された場合は、次のコマンドを使用して、キーストアにリストされている証明書を確認できます。

   ```
   keytool_fips.cmd -list -v -keystore "C:\Program Files\Trend Micro\Deep Security Manager\mssql_keystore.bcfks" -storetype BCFKS -storepass <changeit>
   ```

*<changeit>*の部分は、適切な値に置き換えてください。

5. テキストエディタでC:\Program Files\Trend Micro\Deep Security Manager\webclient\webapps\ROOT\WEB-INF\dsm.propertiesファイルを開き、次の行を追加してSSL/TLSおよびFIPS設定を有効にします。

```
database.SqlServer.encrypt=true
database.SqlServer.trustServerCertificate=false
database.SqlServer.fips=true
database.SqlServer.trustStorePassword=<changeit>
database.SqlServer.fipsProvider=BCFIPS
database.SqlServer.trustStoreType=BCFKS
database.SqlServer.trustStore=C\:\\Program Files\\Trend Micro\\Deep Security Manager\\mssql_keystore.bcfks
```

*<changeit>*の部分は、適切な値に置き換えてください。

6. 必要に応じて、SQLサーバとクライアントの接続プロトコルを名前付きパイプからTCP/IPに変更できます。これにより、FIPSのサポートが可能になります。
   a. SQL Server構成マネージャで、[SQL Serverネットワーク構成]→[MSSQLSERVER のプロトコル] を選択し、[TCP/IP] を有効にします。
   b. [SQL Native Client 11.0 の構成]→[クライアントプロトコル] に移動し、[TCP/IP] を有効にします。
   c. Microsoftの指示に従って、SQL Serverデータベースのインスタンスの暗号化接続を有効にします。データベース エンジンへの暗号化接続を有効にするを参照してください。
   d. dsm.propertiesファイルを編集し、database.sqldserver. driver=MSJDBCおよびdatabase.SqlServer.namedPipe=falseを変更します。
7. Deep Security Managerサービスを再起動します。
8. "Deep Security ManagerでFIPSモードを有効にする" on page 1873。

FIPSモードを無効にする

1. Deep Security ManagerのFIPSモードを無効にするには、有効化の際に使用した手順 ("Deep Security ManagerでFIPSモードを有効にする" on page 1873を参照) に従いますが、手順3で次のコマンドを使用します

```
dsm_c -action disablefipsmode
```

2. Deep Security AgentのFIPSモードを無効にするには、有効化の際に使用した手順 ("保護しているコンピュータでDeep Security AgentのFIPSモードを有効にする" on page 1875を参照) に従いますが、`FIPSMode=1`の代わりに`FIPSMode=0`を使用します。

Deep Securityでの脆弱性管理検索トラフィックのバイパス

(PCI準拠等の目的で) QualysやNessusなどの脆弱性管理プロバイダを使用している場合、このプロバイダの検索トラフィックをバイパスし、そのまま許可するようにDeep Securityを設定する必要があります。

- "脆弱性検索プロバイダのIP範囲またはアドレスから新しいIPリストを作成する" below
- "受信および送信検索トラフィック用のファイアウォールルールを作成する" on the next page
- "新規ファイアウォールルールをポリシーに割り当てて、脆弱性検索をバイパスする" on page 1883

これらのファイアウォールルールを新規ポリシーに割り当てると、Deep Security ManagerはIPリストに追加したIPからのトラフィックをすべて無視します。

Deep Securityは、脆弱性管理プロバイダのトラフィックについては、ステートフルの問題または脆弱性の有無を検索せず、そのまま許可します。

脆弱性検索プロバイダのIP範囲またはアドレスから新しいIPリストを作成する

脆弱性検索プロバイダから受け取ったIPアドレスを手元に用意します。

1. Deep Security Managerで、[ポリシー] に進みます。
2. 左側の画面で [リスト]→[IPリスト] の順に展開します。
3. [新規]→[新規IPリスト] の順にクリックします。
4. 「Qualys IP list」など、新規IPリストの [名前] を入力します。
5. 脆弱性管理プロバイダから受け取ったIPアドレスを、1行に1つずつ [IP] ボックスに貼り付けます。
6. [OK] をクリックします。

受信および送信検索トラフィック用のファイアウォールルールを作成する

IPリストの作成後、受信トラフィック用と送信トラフィック用の2つのファイアウォールルールを作成する必要があります。

それぞれ、次のように名前を付けます。
<プロバイダ名> Vulnerability Traffic - Incoming

<プロバイダ名> Vulnerability Traffic - Outgoing

1. メインメニューで [ポリシー] をクリックします。
2. 左側の画面で [ルール] を展開します。
3. [ファイアウォールルール]→[新規]→[新規ファイアウォールルール] の順にクリックします。
4. 脆弱性管理プロバイダとの間で送受信するTCPおよびUDP接続の受信および送信をバイパスする、最初のルールを作成します。

   ヒント: 以下に記載しない設定については、初期設定のままにします。

   名前: (推奨) <プロバイダ名>Vulnerability Traffic - Incoming

   処理: バイパス

   プロトコル: 任意

   パケット送信元: [IPリスト] を選択し、前の手順で作成した新しいIPリストを指定します。

5. 2番目のルールを作成します。

   名前:<プロバイダ名> Vulnerability Traffic - Outgoing

   処理:バイパス

   プロトコル: 任意

   パケット送信先: [IPリスト] を選択し、前の手順で作成した新しいIPリストを指定します。

注意: コンピュータでファイアウォールルールを機能させるには、ファイアウォールの設定を「オン」または「継承(オン)」に設定する必要があります([コンピュータ]→[ファイアウォール]→[一般])。ファイアウォールルールがポリシーで機能するようにするには、ファイアウォール状態を「オン」に設定する必要があります([ポリシー]→[ファイアウォール]→[一般])。

新規ファイアウォールルールをポリシーに割り当てて、脆弱性検索をバイパスする

脆弱性管理プロバイダによって検索されるコンピュータですでに使用されているポリシーを特定します。

ポリシーを個別に編集し、ファイアウォールモジュールでルールを割り当てます。

1. メインメニューで [ポリシー] をクリックします。
2. 左側の画面で [ポリシー] をクリックします。
3. 右側の画面で、各ポリシーをダブルクリックしてポリシー詳細を開きます。
4. 左側の画面のポップアップで [ファイアウォール] をクリックします。
5. [割り当てられたファイアウォールルール] で [割り当て/割り当て解除] をクリックします。
6. 左上のリストにすべてのファイアウォールルールが表示されていることを確認します。
7. 検索ウィンドウを使用し、作成したルールを探して選択します。
8. [OK] をクリックします。

Deep SecurityでのTLS 1.2の使用

Deep Security Manager 11.1以降の新規インストールでは、初期設定でTLS 1.2が強制されます。

対応が必要であるかどうかは、以下の表で確認してください。

注意: TLS 1.2のA+評価の強力な暗号化スイートのみを有効にする場合は、"TLS 1.2の強力な暗号化スイートの有効化" on page 1897」を参照してください。強力な暗号化スイートを使用すると、互換性の問題が発生することがあります。

目的	現在の環境	対応
Deep Security	10.0以降の	なし

目的	現在の環境	対応
Manager 11.1以上の新規インストール	Deep Security Agent、Relay、Virtual Applianceのみ	初期設定で、TLS 1.2は、すべてのコンポーネント間で使用され、ManagerとRelay上で強制されます。
	9.6未満のDeep Security Agent、Relay、Virtual Applianceを含む	(推奨)すべてのコンポーネントを、TLS 1.2をサポートする9.6以上のバージョンにアップグレードしてください。「"TLS 1.2を使用するようにコンポーネントをアップグレードする" on page 1887」を参照してください。お使いの環境のセキュリティを強化するための最良の方法です。 古いコンポーネントとの下位互換性を確保するために、初期のTLS 1.0を有効にすることもできます。「"初期のTLS (1.0)を有効にする" on page 1893」を参照してください。
Deep Security Manager 11.1以上へのアップグレード	10.0以降のDeep Security Agent、Relay、Virtual Applianceのみ	(推奨)環境のセキュリティを強化するためにTLS 1.2の強制を有効にします。「"TLS 1.2を強制する" on page 1889」を参照してください。 何もしないという選択肢もあります。以前の環境にあったTLS設定はすべて維持されます。これまでTLS 1.2を強制する設定になっていた場合は、その設定がアップグレード後も維持されます。逆に、強制する設定を無効にしていた場合も、それらの設定が維持されます。
	9.6未満のDeep Security Agent、Relay、Virtual Applianceを含む	(推奨)すぐに対応する必要はありませんが、古いコンポーネントは、TLS 1.2がサポートされる9.6以上にアップグレードし、TLS 1.2を強制することを検討してください。「"TLS 1.2を使用するようにコンポーネントをアップグレードする" on page 1887」および「"TLS 1.2を強制する" on page 1889」を参照してください。お使いの環境のセキュリティを強化するための最良の方法です。 何もしないという選択肢もあります。以前の環境にあったTLS設定はすべて維持されます。以前TLS 1.0が許可されていた場合は、アップグレード後も許可されます。

このページのトピック:

- "TLS 1.2のアーキテクチャ" below
- "TLS 1.2を使用するようにコンポーネントをアップグレードする" on page 1887
- "TLS 1.2を強制する" on page 1889
- "初期のTLS (1.0) を有効にする" on page 1893
- "TLS 1.2が強制されているかどうかを確認する" on page 1895
- "TLS 1.2の強制後のAgent、Virtual Appliance、Relayのインストールに関するガイドライン" on page 1896

TLS 1.2とDeep Security Agentの互換性

プラットフォームにインストールされているDeep Security Agent 10.0以降は、TLS 1.2を介してDeep Security Managerと通信します。

また、次のプラットフォームにインストールされたDeep Security Agentバージョン9.6は、TLS 1.2を介してDeep Security Managerと通信します。

- Windows 2000
- Linux Debian 6
- SuSE 10。このプラットフォームのDeep Security Agent 9.6のサポート延長は、2021年5月23日に終了しました。
- Ubuntu 12.04

TLS 1.2は、次のプラットフォームのDeep Security Agentsバージョン9.0でもサポートされます。

- AIX。このプラットフォームのDeep Security Agent 9.0のサポート延長は、2020年12月31日に終了しました。
- Solaris。このプラットフォームのDeep Security Agent 9.0のサポート延長は、2019年12月31日に終了しました。

TLS 1.2のアーキテクチャ

下の図は、Deep Securityアーキテクチャにおけるを示しています。TLS通信

図1は、TLS 1.2が強制されているときのを示しています (新しい11.1以上のDeep Security Manager環境では、これが初期設定となります)。図に示されているとおり、バージョン9.5のAgentも古いサードパーティのアプリケーションも、Deep Security Managerと通信できなくなります。TLS通信

図2は、TLS 1.2が強制されていない場合のTLS通信を示しています。図に示されているとおり、Deep Security Agent 9.6以降のAgentはTLS 1.2を介してDeep Security Managerと通信できますが、バージョン9.5のAgentは初期のTLSを介して通信します。同様に、新しいサードパーティのアプリケーションではTLS 1.2が使用されていますが、古いアプリケーションでは初期のTLSが使用されています。

図1: TLS 1.2の強制あり

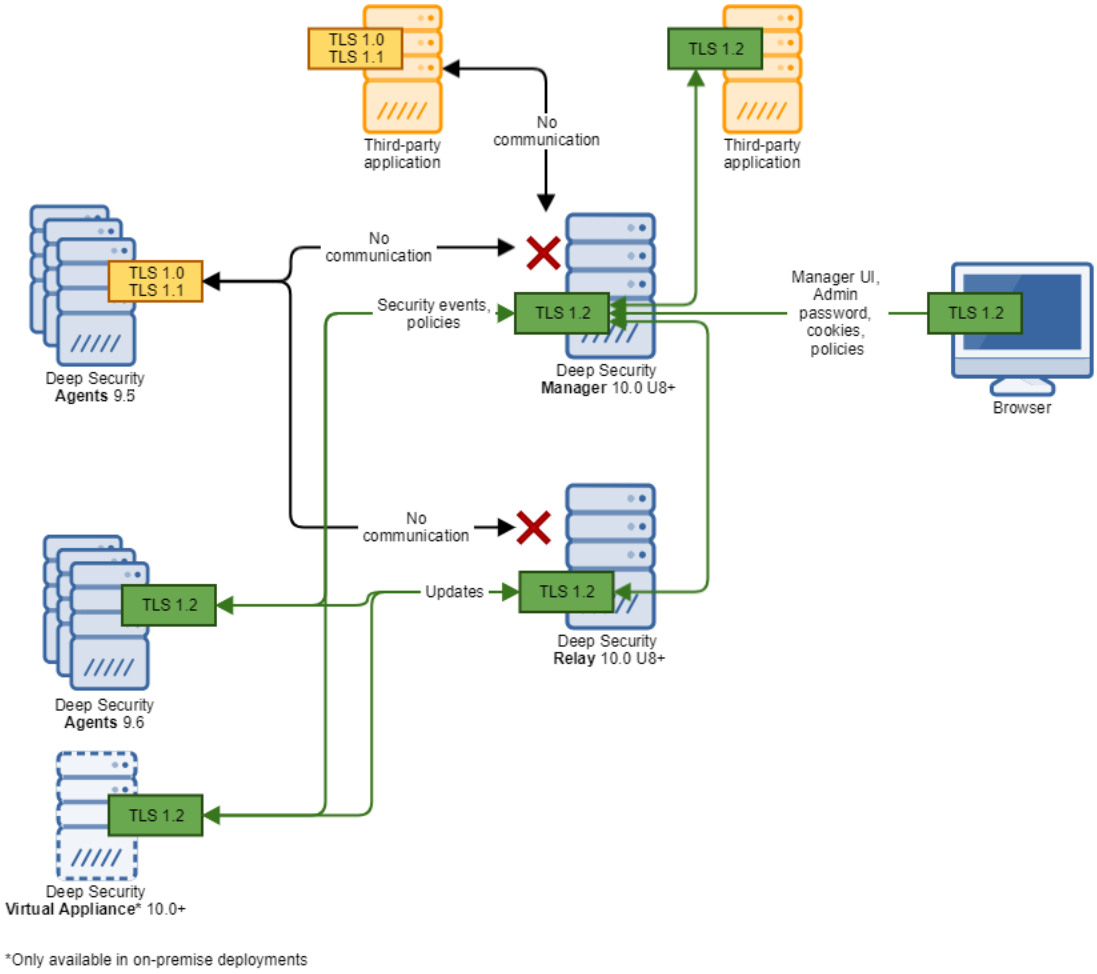
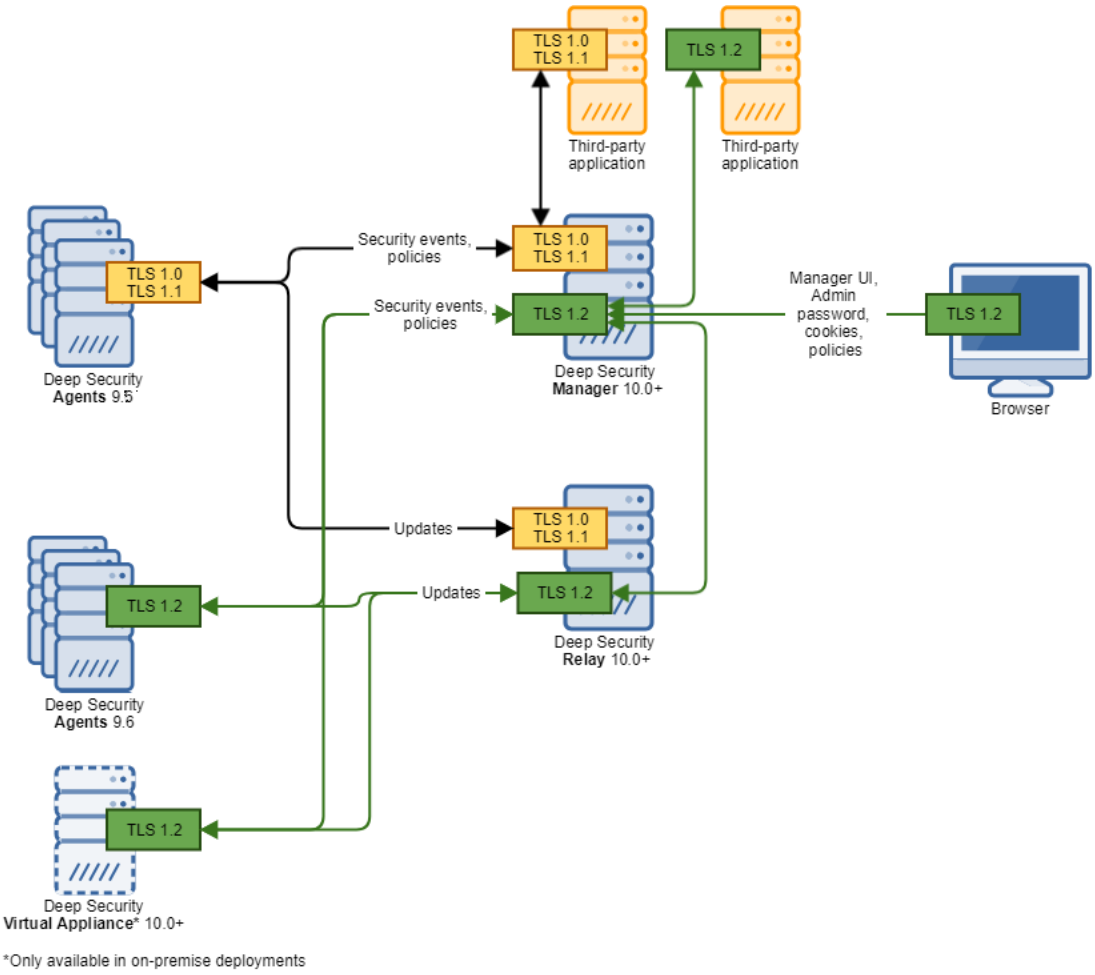


図2: TLS 1.2の強制なし



TLS 1.2を使用するようにコンポーネントをアップグレードする

Deep Securityコンポーネントで TLS 1.2を使用する場合、個々のコンポーネントで TLS 1.2がサポートされていることを確認してください。

以下の手順に従って、Deep Securityのコンポーネントが TLS 1.2をサポートしていることを確認し、必要に応じてそれらをアップグレードします。

注意: TLS 1.2を強制して初期のTLSが使用されないようにするには、「"TLS 1.2を強制する" on page 1889」を参照してください。

Deep Security Managerを確認してアップグレードする

- 次のいずれかのバージョンのDeep Security Managerを使用していることを確認します。別のバージョンを使用している場合はアップグレードしてください。
  - Managerで"TLS 1.2を強制する" on the next page予定がある場合は、Deep Security Manager 10.0 Update 8以降を使用します。TLS 1.2の強制をサポートしているのは、10.0 Update 8以降のManagerのみです。
  - Managerで"TLS 1.2を強制する" on the next page予定がない場合は、Deep Security Manager 10.0以降を使用します。TLS 1.2通信をサポートしているのは、10.0以降のManagerのみです。
- アップグレードの手順については、"Deep Security Managerをアップグレード" on page 1670のアップグレードを参照してください。

Deep Security Managerデータベースを確認する

- Deep Security ManagerデータベースとしてMicrosoft SQL Serverを使用する場合は、データベースでTLS 1.2がサポートされていることを確認し、サポートされていなければ、データベースをアップグレードします。解説については、こちらのMicrosoftのWebサイトを参照してください。
- PostgreSQLデータベースを使用している場合は、TLS 1.2がサポートされているため、何もする必要はありません。
- Oracleデータベースを使用している場合は、データベースとManager間の通信でTLSではなく、Oracleのネイティブの暗号化がサポートされているため、何もする必要はありません。
- 初期設定では、データベース(SQL Server、PostgreSQL、またはOracle)とDeep Security Manager間の通信は暗号化されていません。暗号化は手動で有効にすることができます。

Deep Security Agentを確認する

- 既存のDeep Security Agentがある場合は、バージョンが10.0以降であることを確認します。TLS 1.2をサポートしているのは、10.0以降のAgentのみです。

注意: アップグレードされていないAgent (10.0より以前のAgent) が残っていると、そのAgentは初期のTLSを介して通信するため、初期のTLSを有効にする必要があります。詳細については、「"初期のTLS (1.0) を有効にする" on page 1893」を参照してください。

エージェントをアップグレードするには、"Deep Security Agentのアップグレード" on page 1676を参照してください。

Deep Security Relayを確認する

- 次のいずれかのバージョンのDeep Security Relayを使用していることを確認します。別のバージョンを使用している場合はアップグレードしてください。
  - Relayで"TLS 1.2を強制する" below予定がある場合は、Deep Security Relay 10.0 Update 8以降を使用します。TLS 1.2の強制をサポートしているのは、10.0 Update 8以降のRelayのみです。
  - Relayで"TLS 1.2を強制する" below予定がない場合は、Deep Security Relay 10.0以降を使用します。TLS 1.2通信をサポートしているのは、10.0以降のRelayのみです。

リレーをアップグレードするには、"Deep Security Relay" on page 1675を参照してください。

Deep Security Virtual Applianceを確認する

Deep Security Virtual Appliance 10.0以降を使用していることを確認してください。

Applianceをアップグレードするには

1. 一時的に初期のTLS (1.0) を有効にします。
2. Applianceを10.0以上にアップグレードします(「"既存のAppliance SVMを自動的にアップグレードする" on page 1688」を参照)。新しいVirtual ApplianceではTLS 1.2がサポートされます。
3. アップグレードが完了したら、TLS 1.2の強制を再び有効にします。

注意: Virtual Applianceに必要なvSphereおよびNSXソフトウェアの最小バージョンでは、TLS 1.2はすでにサポートされています。詳細については、"システム要件 " on page 400を参照してください。

TLS 1.2を強制する

このセクションのトピック:

- "TLS 1.2を強制できるコンポーネント" on the next page
- "TLS 1.2を強制した場合の動作" on the next page

- "初期設定でTLS 1.2が強制されるかどうか" below
- "TLS 1.2の強制が可能になる場合の条件" below
- "Deep Security ManagerでTLS 1.2を強制する" on the next page
- "Deep Security RelayでTLS 1.2を強制する" on the next page
- "ManagerのGUIポート(4119)でのみTLS 1.2を強制する" on page 1892
- "TLS 1.2の強制をテストする" on page 1892

TLS 1.2を強制できるコンポーネント

TLS 1.2を強制できるコンポーネントは次のとおりです。

- Deep Security Manager
- Deep Security Relay

TLS 1.2を強制した場合の動作

TLS 1.2を強制すると、ManagerとRelayで初期のTLS接続が許可されなくなり、初期のTLSの使用を試みるアプリケーションは、アクセスが拒否されて正常に機能しなくなります。

TLS 1.2を強制しない場合、ManagerとRelayで初期のTLSに加えてTLS 1.2接続も許可されます。そのため、古いアプリケーションと新しいアプリケーションの両方が接続できます。

初期設定でTLS 1.2が強制されるかどうか

- Deep Security Manager 11.1以上をアップグレードではなく新規インストールした場合、初期設定でTLS 1.2が強制されます。
- 既存のDeep Security Managerを11.1以上にアップグレードした場合は、既存のTLS設定が維持されます。つまり、それまでTLSを強制していなかった場合、アップグレード後も強制されません。逆に、強制していた場合は、引き続き強制されます。

TLS 1.2の強制が可能になる場合の条件

TLS 1.2を強制できるのは、Deep Security Agentすべてが、TLS 1.2がサポートされているバージョンである10.0以降にアップグレードされている場合のみです。

Deep Security ManagerでTLS 1.2を強制する

1. 開始前の準備:
   - Deep Security Managerのバージョンが10.0 Update 8以上であることを確認してください。TLS 1.2を強制するためには、このバージョンが必要です。
   - その他すべてのコンポーネントがTLS 1.2をサポートしていることを確認します。「"TLS 1.2を使用するようにコンポーネントをアップグレードする" on page 1887」を参照してください。
2. Deep Security Managerコンピュータで、次のdsm_cコマンドを実行します。

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol ShowValue
   ```

   TLSのバージョンが表示されます。それが、現在Deep Security Managerで許可される最小のTLSバージョンとなります。
3. 次のdsm_cコマンドを実行します。

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol TLSv1.2
   ```

   このコマンドによって、最小TLSバージョンが1.2に設定されます。これでDeep Security ManagerがTLS 1.2接続を許可し、TLS 1.0接続を禁止するようになりました。

   Deep Security Managerサービスが自動的に再開されます。

Deep Security RelayでTLS 1.2を強制する

1. 開始前の準備:
   - Deep Security Relayのバージョンが10.0 Update 8以上であることを確認してください。TLS 1.2を強制するためには、このバージョンが必要です。
   - すべてのコンポーネントがTLS 1.2をサポートしていることを確認します。「"TLS 1.2を使用するようにコンポーネントをアップグレードする" on page 1887」を参照してください。
   - Deep Security ManagerでTLS 1.2を強制する設定になっていることを確認します。
2. Relayに関連するポリシーを再送信します。
   a. Deep Security Managerで、[Computers]をクリックして、コンピュータのリストでリレーのいずれかを検索します。どのRelayかわからない場合は、上部にある[管理] をクリックします。左側の[アップデート] を展開し、[Relayの管理] をクリックします。メイン画面でRelayグループを展開し、該当するRelayを表示します。
   b. コンピュータのリストでRelayをダブルクリックします。
   c. メイン画面で[処理] タブをクリックします。
   d. [ポリシーの送信] をクリックしてポリシーを再送信します。
   e. 各Relayにポリシーを再送信します。

ManagerのGUIポート(4119) でのみTLS 1.2を強制する

"Deep Security ManagerでTLS 1.2を強制する" on the previous pageおよび"Deep Security RelayでTLS 1.2を強制する" on the previous pageで説明したとおり、Deep Security ManagerおよびRelayで完全な強制が不可能な場合にのみ、このセクションを読んでください。

このセクションでは、ポート4119の最小TLSバージョンをTLS 1.2に設定する方法について説明します。ポート4119に接続するアプリケーションは、通常、WebブラウザとDeep Security APIクライアントです。TLS 1.2をサポートしていない古いDeep Securityコンポーネントは引き続き、TLS 1.0を使用してManagerに接続できます (初期設定ではポート4120を使用)。

1. Deep Security Managerで次のdsm_cコマンドを実行してTLS 1.0を有効にします。

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol TLSv1
   ```

   Deep Security Managerが、古いAgentやアプリケーションからのTLS 1.0接続を許可するようになりました。

2. ManagerのGUIポート(4119) で初期のTLSを無効にします (すでに無効になっている可能性があります)。
   a. Deep Security Managerのインストールディレクトリのルートにあるconfiguration.propertiesファイルを開きます。
   b. serviceName=の下にあるprotocols=設定を探します。

      この設定では、WebブラウザおよびDeep Security APIクライアントのサーバとして動作している場合に、Deep Security Managerに接続するために使用できるプロトコルを定義します。

   c. protocols=設定がある場合は、ポート4119でTLS 1.2のみが許可されるように、この設定を削除します。
   d. ファイルを保存します。
3. Deep Security Managerサービスを再起動します。

TLS 1.2の強制をテストする

1. 初期TLS 1.2を強制したDeep Securityコンポーネントで、次のnmapコマンドを実行します。

   ```
   nmap --script ssl-enum-ciphers <ds_host> -p <ds_port> -Pn
   ```

   指定する項目は次のとおりです。
   - <ds_host>は、ManagerまたはRelayのIPアドレスまたはホスト名に置き換えます。

- <ds_port>は、TLSが使用されている待機ポートに置き換えます。Managerの場合は4119、Relayの場合は4122、Agentの場合は4118です(Managerからの有効化を使用した場合)。

この応答ではTLS 1.2のみが表示されます。応答の例は次のとおりです。

```
PORT STATE SERVICE
443/tcp open https
| ssl-enum-ciphers:
| | TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
| TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
| TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
| compressors:
```

初期のTLS (1.0) を有効にする

初期設定では、初期のTLS (1.0) が無効になっています。Deep Security Manager 11.1以上をアップグレードではなく新規インストールした場合で、かつ以下に該当する場合は、自分で有効にする必要があります。

- 10.0より前のAgentを使用している。この場合、サポートされるのは初期のTLSだけです。お使いのOSで10.0以上のAgentが利用できるかどうかについては、こちらを参照してください。

- 古いサードパーティコンポーネントを使用していて、Deep Security Managerとの通信に初期のTLSを使用する必要がある。
- 現在サポート対象外となっている、10.0より前のバージョンのDeep Security Virtual Applianceを使用している。

初期のTLS (1.0) を有効にするには、以下の手順に従います。

Deep Security ManagerとDeep Security RelayでTLS 1.0を有効にする

1. Deep Security Managerコンピュータで、次のdsm_cコマンドを実行します。

   `dsm_c -action settlsprotocol -MinimumTLSProtocol ShowValue`

   TLSのバージョンが表示されます。それが、現在Deep Security Managerで許可される最小のTLSバージョンとなります。

2. 次のdsm_cコマンドを実行します。

   `dsm_c -action settlsprotocol -MinimumTLSProtocol TLSv1`

   このコマンドによって、最小TLSバージョンが1.0に設定されます。

   Deep Security ManagerでTLS 1.0が再び有効になりました。

   Deep Security Managerサービスが自動的に再開されます。

3. Relayに関連するポリシーを再送信します。
   a. Deep Security Managerで、[Computers]をクリックして、コンピュータのリストでリレーのいずれかを検索します。どのRelayかわからない場合は、上部にある[管理] をクリックします。左側の [アップデート] を展開し、[Relayの管理] をクリックします。メイン画面でRelayグループを展開し、該当するRelayを表示します。
   b. コンピュータのリストでRelayをダブルクリックします。
   c. メイン画面で [処理] タブをクリックします。
   d. [ポリシーの送信] をクリックしてポリシーを再送信します。
   e. 各Relayにポリシーを再送信します。

   RelayでTLS 1.0が再び有効になりました。

ManagerのGUIポートでTLS 1.0を有効にする (4119)

以前ManagerのGUIポート (4119) でのみTLS 1.2を強制しており、今後はそのポートで初期のTLS 1.0を再び有効にしたい場合は、このセクションをお読みください。

1. 「"Deep Security ManagerとDeep Security RelayでTLS 1.0を有効にする" on the previous page」の手順に従ってください。これにより、GUIポート(4119) でTLS 1.0が再び有効になります。

インストールスクリプトでTLS 1.0を有効にする

Deep Security AgentとDeep Security Relayは、インストールスクリプトを使用してインストールできます。これらのスクリプトに次のように変更を加える必要があります。

1. インストール先がWindows XP、2003、2008のいずれかである場合は、インストールスクリプトから次の行を削除します。

   ```
   #requires -version 4.0
   ```

   ```
   [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;
   ```

   TLS 1.2ではPowerShell 4.0が必要ですが、Windows XP、2003、2008ではPowerShell 4.0がサポートされません。

2. インストール先がRed Hat Enterprise Linux 6である場合は、インストールスクリプトから次のタグを削除します。

   ```
   --tls1.2
   ```

   Red Hat Enterprise Linux 6の初期設定では、TLS 1.2をサポートしないcurl 7.19が使用されます。

3. それ以外のサポート対象のOSがインストール先である場合は、インストールスクリプトをそのままにしてください。

TLS 1.2が強制されているかどうかを確認する

Deep Security ManagerでTLS 1.2が強制されているかどうかわからない場合は、以下の手順に従って確認してください。

1. Deep Security Managerコンピュータでコマンドプロンプトを開き、次のdsm_cコマンドを実行します。

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol ShowValue
   ```

   Managerで許可される最小バージョンのTLSプロトコルが表示されます。TLS 1.2と表示された場合は、TLS 1.2が強制されています。TLS 1.0と表示された場合、初期のTLSは許可されていますが、TLS 1.2は強制されていません。

RelayでTLS 1.2が強制されているかどうかを確認するのは、もっと難しくなります。「"Deep Security RelayでTLS 1.2を強制する" on page 1891」または「"Deep Security ManagerとDeep Security RelayでTLS 1.0を有効にする" on page 1894」に従い、お使いのTLS設定をポリシーを通じてRelayに強制した場合、それらのTLS設定がRelayに適用されます。ポリシーを通じてTLS設定を強制しなかった場合は、Relayの初期設定のTLS設定が適用されます。Relayの初期設定は、そのバージョンによって異なります。11.1以上のRelayを使用している場合は、初期設定でTLS 1.2が強制されます。11.1より前のRelayの初期設定では、TLS 1.2が強制されません。

TLS 1.2の強制後のAgent、Virtual Appliance、Relayのインストールに関するガイドライン

このセクションでは、TLS 1.2を強制した後でAgent、Virtual Appliance、およびRelayをインストールする場合の特別な注意事項について説明します。初期のTLS (1.0) を有効にした場合、特に注意事項はないため、このセクションを読む必要はありません。

このセクションのトピック:

- "TLS 1.2が強制されているときのAgent、Virtual Appliance、およびRelayのインストールに関するガイドライン" below
- "TLS 1.2の強制後にインストールスクリプトを使用する場合のガイドライン" below

TLS 1.2が強制されているときのAgent、Virtual Appliance、およびRelayのインストールに関するガイドライン

- 10.0以上のAgent、Virtual Appliance、およびRelayをインストールする必要があります。TLS 1.2をサポートしているのは、10.0以上のAgentとRelayのみです。
- 9.6以前のAgentまたはRelayをインストールする必要がある場合は、初期のTLS (1.0) を有効にする必要があります。

TLS 1.2の強制後にインストールスクリプトを使用する場合のガイドライン

TLS 1.2が強制されている場合、インストールスクリプトを使用して、10.0以上のAgentとRelayをインストールできます。ここでは、インストールスクリプトを確実に機能させるためのガイドラインを示します。

1. WindowsコンピュータにAgentまたはRelayをインストールする場合は、TLS 1.2をサポートしているPowerShell 4.0以降を使用します。

2. LinuxにAgentまたはRelayをインストールする場合は、TLS 1.2をサポートしているcurl 7.34.0以降を使用します。
3. インストール先がWindows XP、2003、2008のいずれかである場合

   または

   インストール先がRed Hat Enterprise Linux 6である場合

   これらのOSはTLS 1.2をサポートしていないため、"初期のTLS (1.0) を有効にする" on page 1893にしたうえで、インストールスクリプトに変更を加える必要があります。

TLS 1.2の強力な暗号化スイートの有効化

強力な暗号化スイートを有効にすることで、Deep Securityコンポーネントとのすべての通信を安全に行えるようになります。悪意のあるユーザーが、弱い暗号化スイートを使用した通信チャネルを介してシステムへの接続を作成できると、その暗号化スイートの既知の脆弱性を悪用して、システムや情報の安全性を脅かすことになります。

このページでは、TLS 1.2の強力な暗号化スイートを使用するように、Deep Security Manager、Deep Security Agent、およびDeep Security Relayをアップデートする方法について説明します。これらの暗号スイートには+ (A+) の詳細評価があり、このページの表にリストされています。

手順1: "環境を確認する" below

手順2: "Deep Securityコンポーネントをアップデートする" on the next page

手順3: "TLS 1.2の強力な暗号化スイートを有効にするためのスクリプトを実行する" on the next page

手順4: "スクリプトの動作を確認する" on page 1899

"TLS 1.2の強力な暗号化スイートを無効にする" on page 1902

環境を確認する

強力な暗号化スイートを有効にせず、代わりにDeep SecurityでTLS 1.2を使用する必要がある場合があります。

- FIPSモードを使用している場合。

- 環境内のいずれかのコンピュータで、強力な暗号化スイートをサポートしていないWindows Server 2012 R2以前を実行している場合。これらのコンピュータを、強力な暗号化スイートをサポートするWindows Server 2016にアップグレードすることを検討してください。
- すべてのDeep Securityコンポーネントを12.0以降にアップグレードできない場合。たとえば、12.0エージェントを使用できないOSを使用している場合です。

Deep Securityコンポーネントをアップデートする

すべてのコンポーネントを次の順序でアップデートしてください。そうしないと、AgentはRelayおよびManagerと通信できません。

1. すべてのManagerインスタンスを12.0以降のバージョンにアップデートします。アップグレード手順については、"Deep Security Managerをインストールする" on page 459を参照してください。
2. すべてのRelayを12.0以降にアップデートします。Relayをアップグレードするには、Agentのアップグレードと同じ手順に従います。
   a. Managerに最新のRelayソフトウェアを手動または自動でインポートします。詳細については、"エージェントソフトウェアのインポート" on page 515 を参照してください。
   b. リレーをアップグレードします。"Deep Security Relay" on page 1675のアップグレードを参照してください。
3. すべてのAgentを12.0以降にアップデートします。Agentをアップグレードするには
   a. Managerに最新のAgentソフトウェアを手動または自動でインポートします。詳細については、"エージェントソフトウェアのインポート" on page 515 を参照してください。
   b. Deep Security Agentをアップグレードします。"Deep Security Agentのアップグレード" on page 1676を参照してください。

TLS 1.2の強力な暗号化スイートを有効にするためのスクリプトを実行する

1. https://github.com/deep-security/ops-tools/tree/master/deepsecurity/managerにあるEnableStrongCiphers12.scriptファイルを以下の場所にコピーします。
   - Windowsの場合: `<Manager_root>\Scripts`
   - Linuxの場合: `<Manager_root>/Scripts`

   この場合、`<Manager_root>`は、Managerのインストールディレクトリのパスに置き換えます。初期設定では次のようになっています。

- C:\Program Files\Trend Micro\Deep Security Manager (Windows)
- /opt/dsm/ (Linux)

注意: \Scripts ディレクトリが表示されない場合は、作成してください。

2. Managerにログインします。
3. 上部の[管理]をクリックします。
4. 左側で、[予約タスク] をクリックします。
5. メイン画面で、[新規] をクリックします。
6. [新規予約タスクウィザード] が表示されます。
7. [種類] リストで [スクリプトの実行] を選択します。[1回のみ] を選択します。[次へ] をクリックします。
8. 日付、時刻、およびタイムゾーンの初期設定を受け入れ、[次へ] をクリックします。
9. [スクリプト] で、[EnableStrongCiphers.script] を選択します。[次へ] をクリックします。
10. [名前] には、スクリプトの名前 (たとえば、Enable Strong Cipher Suites) を入力します。[タスクの有効化] が選択されていることを確認します。[[完了] でタスクを実行] をクリックします。[完了] をクリックします。

    スクリプトが実行されます。

11. Deep Security Managerサービスを再起動します。

    Agent、Relay、およびManagerは、TLS 1.2の強力な暗号化スイートのみを使用して相互に通信を行うようになりました。

スクリプトの動作を確認する

スクリプトの動作と、TLS 1.2の強力な暗号化スイートのみが許可されていることを確認するには、一連のnmapコマンドを実行する必要があります。

- "nmapを使用してManagerを確認する" below
- "nmapを使用してRelayを確認する" on the next page
- "nmapを使用してAgentを確認する" on page 1901

nmapを使用してManagerを確認する

次のコマンドを実行します。

```
nmap --script ssl-enum-ciphers -p 4119 <Manager_FQDN>
```

出力は次のようになります。強力な暗号化スイートは中段付近で確認できます。

```
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-14 09:51 EST
Nmap scan report for <DSM FQDN> (X.X.X.X)
Host is up (0.0049s latency).
PORT STATE SERVICE
4119/tcp open assuria-slm
| ssl-enum-ciphers:
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256k1) - A
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256k1) - A
| compressors:
| NULL
| cipher preference: client
|_ least strength: A
Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds
```

nmapを使用してRelayを確認する

次のコマンドを実行します。

```
nmap --script ssl-enum-ciphers -p 4122 <Relay_FQDN>
```

出力は次のようになります。強力な暗号化スイートは中段付近に記述されています。

```
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-14 09:49 EST
Nmap scan report for <DSR FQDN> (X.X.X.X)
Host is up (0.0045s latency).
PORT STATE SERVICE
4122/tcp open unknown
| ssl-enum-ciphers:
| TLSv1.2:
```

```
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
| compressors:
| NULL
| cipher preference: server
|_ least strength: A
Nmap done: 1 IP address (1 host up) scanned in 31.02 seconds
```

nmapを使用してAgentを確認する

次のコマンドを実行します。

```
nmap --script ssl-enum-ciphers -p 4118 <Agent_FQDN>
```

出力は次のようになります。

```
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-14 09:50 EST
Nmap scan report for <DSA FQDN> (X.X.X.X)
Host is up (0.0048s latency).
PORT STATE SERVICE
4118/tcp open netscript
| ssl-enum-ciphers:
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
| compressors:
| NULL
| cipher preference: server
|_ least strength: A
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
```

TLS 1.2の強力な暗号化スイートを無効にする

すべてのAgent、Relay、およびManagerをアップグレードする前に誤ってスクリプトを実行してしまった場合には、次の手順に従って以前の状態に戻すことができます。

1. <Manager_root>にあるconfiguration.propertiesファイルを開き、ciphersで始まる行を削除します。次のような行です。

   ciphers=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

2. protocols フィールドに値TLSv1とTLSv1.1を追加します。プロパティは最終的には次のようになります。

   protocols = TLSv1, TLSv1.1, TLSv1.2

3. ファイルを保存して、閉じます。
4. <Manager_root>\jre\lib\security\にあるjava.securityファイルを開き、jdk.tls.disabledAlgorithms から次の2つのプロトコルを削除します。

   TLSv1, TLSv1.1

5. Deep Security Managerで、次のdsm_cコマンドを実行します。

   ```
   dsm_c -action changesetting -name settings.configuration.restrictRelayMinimumTLSProtocol -value TLSv1
   ```

   ```
   dsm_c -action changesetting -name settings.configuration.enableStrongCiphers -value false
   ```

   システムが再度通信できるようになります。TLS 1.2の強力な暗号化スイートを有効にする必要がある場合は、すべてのコンポーネントをアップグレードしてからスクリプトを実行するようにしてください。

Deep Security Managerとの通信の問題が解決しない場合は、次の追加のdsm_cコマンドを実行します。

```
dsm_c -action changesetting -name settings.configuration.MinimumTLSProtocolNewNode -value TLSv1
```

法的開示

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

Deep Securityにより収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

https://www.go-tm.jp/data-collection-disclosure

※重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。Deep Securityにおける無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー(Globaly Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

Deep Security製品使用状況データ収集

トレンドマイクロは、Deep Security Managerの向上に役立つ保護対象のパフォーマンスおよび機能の使用状況データを収集します。トレンドマイクロでは、製品の改善のために収集されたデータのみを内部的に使用します。外部者と共有されることはなく、個人を特定できる情報は含まれません。

トレンドマイクロがDeep Securityをより効果的にサポートできるようにするために、データ収集を有効にしておくことをお勧めします。ただし、Deep Security Managerでこのデータを収集しない場合は、データ収集を無効にできます。

データ収集を無効にするには、[システム設定]→[詳細]→[製品使用状況データ収集]の順に選択し、[製品使用状況データ収集]の選択を解除します。

法律上の免責事項

以下は、次のリリースに関する免責事項です。

- "Hot Fix" below
- "メジャーリリース、アップデート、パッチ、Service Pack" below

Hot Fix

本HotFixは、お客さまの使用環境で実際に発生している不具合を修正するために提供いたします。トレンドマイクロでは、発生している不具合に関する動作テストのみ実施していますので、本HotFixの適用によりその他の不具合が発生する可能性があることをご理解いただき、本HotFixをご利用いただきますようお願いいたします。

■ 保証および責任の限定 ■
1. トレンドマイクロ株式会社は、本HotFixに関して一切の保証を行いません。またトレンドマイクロ株式会社は、本ソフトウェアの機能がお客さまの特定の目的に適合することを保証するものではなく、本HotFixの物理的な紛失、盗難、事故および誤用等に起因するお客さまの損害につき一切の補償をいたしません。
2. お客さまが期待する成果を得るためのソフトウェアプログラム (本HotFixを含むがこれに限られない) の選択、導入、使用および使用結果につきましては、お客さまの責任とさせていただきます。本HotFixの使用に起因してお客さままたはその他の第三者に生じた結果的損害、付随的損害および逸失利益に関してトレンドマイクロ株式会社は一切の責任を負いません。

メジャーリリース、アップデート、パッチ、Service Pack

プログラムの仕様は予告なしに変更される場合があります。あらかじめご了承ください。また、本製品をご利用いただく前に、使用許諾契約に同意していただく必要があります。
製品の最新情報については、弊社ホームページをご覧ください。
URL: https://www.trendmicro.com

本製品を体験版としてお使いの場合には、30日以内に製品版を購入していただき、製品版にアップグレードしていただくことをお勧めします。製品版の購入については、トレンドマイクロの営業部または販売代理店にお問い合わせください。

統合

AWS Control Towerとの統合

Deep SecurityとAWS Control Towerを統合して、Control Towerアカウントファクトリを介して追加されたすべてのアカウントがDeep Securityで自動的にプロビジョニングされるようにします。各アカウントに配置されたEC2インスタンスのセキュリティ状況を一元的に把握できます。ポリシーと課金の自動化の基盤となります。

概要

Lifecycle HookソリューションではCloudFormationテンプレートが提供され、Control Tower Master Accountで起動するとAWSインフラストラクチャが配置され、Deep Securityが各Account Factory AWSアカウントを自動的に監視できるようになります。このソリューションは、2つのラムダ関数で構成されます。1つはMcAfeeの役割を管理し、Deep Securityにはアクセスし、もう1つはLambdaのライフサイクルを管理するためのものです。AWS Secrets ManagerはDeep SecurityのAPIキーをMasterアカウントに格納するために利用され、CloudWatch Eventsルールは、Control Towerアカウントが正常に配信されたときにカスタマイズLambdaを実行するように設定されています。

Deep SecurityがAWS Control Towerと統合されると、Deep Securityは次の方法で実装されます。

1. スタックの起動時に、Control Tower Master、Audit、およびLogアカウントを含む既存のControl Towerアカウントごとにライフサイクルが実行されます。
2. 起動後、CloudWatchイベントルールによって、成功したControl Towerの[CreateManagedAccount]イベントごとにライフサイクルラムダがトリガされます。
3. ライフサイクルラムダ関数は、AWS Secrets ManagerからDeep Security APIキーを取得し、組織の外部IDをDeep Security APIから取得します。
4. ラムダ関数は、対象の管理下のアカウントでControlTowerExecutionの役割を引き継ぎ、必要なクロスアカウントの役割と関連するポリシーを作成します。
5. Deep Security APIが呼び出され、この管理対象アカウントがテナントに追加されます。

AWS Control Towerとの統合

1. Deep Security ManagerをAWS Control Towerの共有セキュリティアカウントに配置します。Deep Security クイックスタートをControl Towerのセキュリティアカウントに配信し、クイックスタートの配信で一般公開されているELBを利用して、ワークロード管理下のアカウントとDeep Security Manager間の接続を作成することをお勧めします。

2. CloudFormationスタックが正常に起動したら、最上位CloudFormationテンプレートのDeepSecurityConsole値を記録します。このURLは、コンソールにサインインしてマルチアカウントの統合を設定するために必要になります。
3. Deep Security Managerで、管理>ユーザ管理>APIキーにアクセスし、新規をクリックします。キーの名前とフルアクセスの役割を選択します。キーは後で検索できないので、必ず保存してください。このキーは、AWS Control Tower MasterからコンソールAPIへの自動化の認証に使用されます。詳細については、"ユーザ向けのAPIキーの作成" on page 1559を参照してください。
4. AWS Control Towerのマスターアカウントにログインします。CloudFormation Serviceに移動し、AWS Control Towerが配信された地域を選択してライフサイクルテンプレートを起動します。
5. ライフサイクルテンプレートで、手順3で生成したAPIキーを入力します。次に、コンソールのFQDNを入力します(https://) が指定されていない場合は、手順2で記録されたDeepSecurityConsole値として表示されます) 。
6. AWS CloudFormationでIAMリソースを作成する可能性があることを示すボックスを選択します。スタックの作成を選択すると、AWSアカウントがDeep Securityに追加されます。
7. すべてのアカウントをインポートしたら、"エージェントをインストールする" on page 536して保護を有効にしてください。

AWS Control Towerの統合をアップグレードする

新しい機能がDeep Securityに追加されると、アプリケーションのクロスアカウントロールの権限をアップデートする必要が生じることがあります。ライフサイクルフックによって配信された役割をアップデートするには、Deep Securityスタックを元のURLで最新のテンプレートにアップデートします。パラメータ値は、トレンドマイクロのサポート担当者が指示しない限り、元の値から変更しないでください。
CloudFormationスタックをアップデートすると、既存のすべてのアカウントで使用される役割と、今後の登録で作成される役割が更新されます。

AWS Control Tower統合の削除

ライフサイクルフックを削除するには、CloudFormationスタックを特定して削除します。既に追加されている管理下のアカウントの保護はそのまま維持されます。Deep SecurityからAWSアカウントを削除する方法の詳細については、"AWSアカウントを削除する" on page 679するを参照してください。

AWS Systems Manager Distributorとの統合

AWS Systems Manager Distributor は、AWS Systems Managerと統合された機能で、アカウントにソフトウェアパッケージを安全に保存および配布するために使用できます。AWS Systems Manager

Distributorと統合することで、Deep Security Agentを複数のプラットフォームに分散し、管理対象インスタンスへのアクセスを制御し、配置を自動化できます。

IAMポリシーを作成する

[既存の管理下のポリシーをインポートする]の手順に従います。

[管理対象ポリシーのインポート] [ ]画面で、「AmazonSSMManagedInstanceCore」ポリシーを追加します。

役割を作成し、ポリシーを割り当てます。

「AWSサービスの役割の作成」の手順に従ってください。

[添付パーミッションポリシー]画面で、「AmazonSSMManagedInstanceCore」権限を追加します。

パラメータの作成

1. AWSコンソールで、AWS Systems Manager>アプリケーション管理>パラメータストアに移動します。
2. 4つのパラメータを作成する必要があります。パラメータの作成をクリックし、表に記載されているように名前と値を入力します。以下のとおりです。その他のフィールドは初期設定値のままにできます。

Name	値
dsActivationUrl	dsm://dsm.company.com:4120/
dsManagerUrl	https://dsm.company.com:443
dsTenantId	シングルテナント環境の場合、このパラメータは不要です。マルチテナントの場合は、Deep Security Managerで>配信スクリプトをサポートに移動します。スクロールして生成されたスクリプトの一番下まで移動し、*tenantID*をコピーします。
dsToken	シングルテナント環境の場合、このパラメータは不要です。マルチテナントの場合は、Deep Security Managerで>配信スクリプトをサポートに移動します。生成されたスクリプトの一番下までスクロールし、*トークン*をコピーします。

注意: dsActivationUrlとdsManagerUrlの値が表示されているとおりに入力されていることを確認してください。適用できる場合は末尾にスラッシュを挿入してください。

AWS Systems Manager Distributorとの統合

1. AWSコンソールで、[AWS Systems Manager]→[ノード管理]→[Distributor]の順に選択します。
2. TrendMicro-CloudOne-WorkloadSecurityパッケージを選択し、スケジュールに基づいてインストールします。
3. 関連付けの作成ページが開きます。必要なフィールドに入力します。インストールの種類の場合は、*インプレースアップデートオプション*を使用することをお勧めします。
4. スケジュールを作成します。予約されたState Manager Associationを活用することで、エージェントが常に最新で最新にインストールされます。

コンピュータを保護する

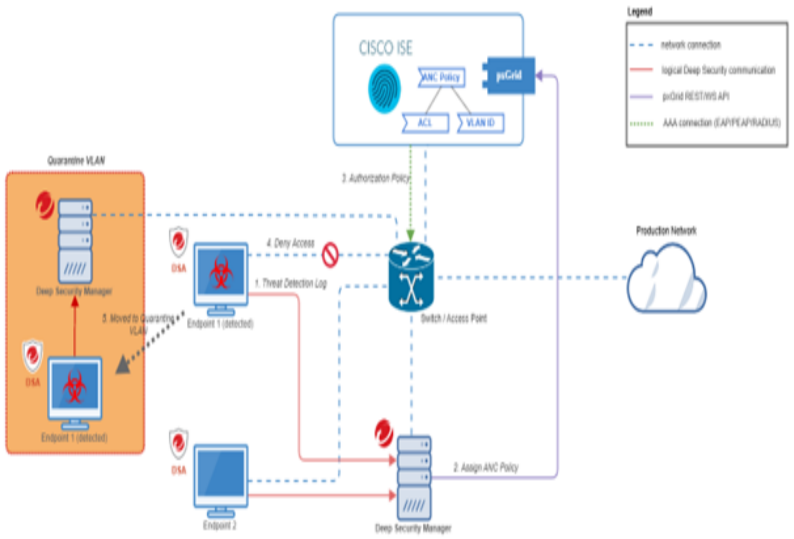
管理対象クライアントが含まれるAWSアカウントごとにクラウドコネクタを設定することをお勧めします。また、Distributorによって管理されるシステムに固有のポリシーを作成することが必要な場合もあります。

Cisco Identity Services Engine (ISE) と統合する

Deep SecurityのCisco Identity Services Engine (ISE) は、特定のホストで脅威が検出されるとすぐに、ターゲットMACアドレスに適応型ネットワーク制御 (ANC) ポリシーを割り当てることでネットワーク封じ込めを実行します。

この機能により、Deep Security Managerは不正プログラム対策や侵入防御システムの保護モジュールからのものなど、脅威の検出イベントを継続的にモニタできます。検出イベントが特定の設定可能な基準を満たすと、マネージャはCisco ISEに対し、検出イベントが発生したホストに関連付けられたすべてのMACアドレスにANCポリシーを迅速に適用するよう指示します。ANCポリシーにより、Cisco ISEは、対象のMACアドレスを隔離VLANに移動したり、MACが接続されているネットワークデバイスポートをシャットダウンしたりするなどのセキュリティ対策を実施できます。

統合フローは以下の図に示されています。



統合フローは次のように機能します。

1. Deep Security Agentは検出ログをDeep Security Managerに送信します。
2. 検出ログがCVSSスコアやランサムウェア不正プログラムの種類などの設定された基準を満たす場合、マネージャは影響を受けたエンドポイントに関連付けられたすべてのMACアドレスに対して、Cisco ISEにAdaptive Network Control (ANC) ポリシーを適用するよう指示します。
3. Cisco ISEは、認証サーバとしてCisco ISEを使用するように設定されたネットワークスイッチに対して、ANCポリシーに関連付けられたネットワークアクセス制御リスト(ACL) を適用します。
4. エンドポイントのネットワークセッションがネットワークスイッチによって再認証され、アクセスが拒否されました。
5. エンドポイントは隔離VLANに移動される可能性があり、脅威の診断と修復はそのVLAN内にあるマネージャノードによって管理されます。

注意: この記事では、Cisco Identity Services Engine (ISE) 接続の設定と、Deep Securityとの統合の利用に関するガイドラインを提供します。Cisco ISE、Adaptive Network Control (ANC) ポリシー、およびアクセス制御リスト(ACL) の詳細については、公式のCisco ISE ドキュメントを参照してください。

前提条件Cisco ISE接続設定

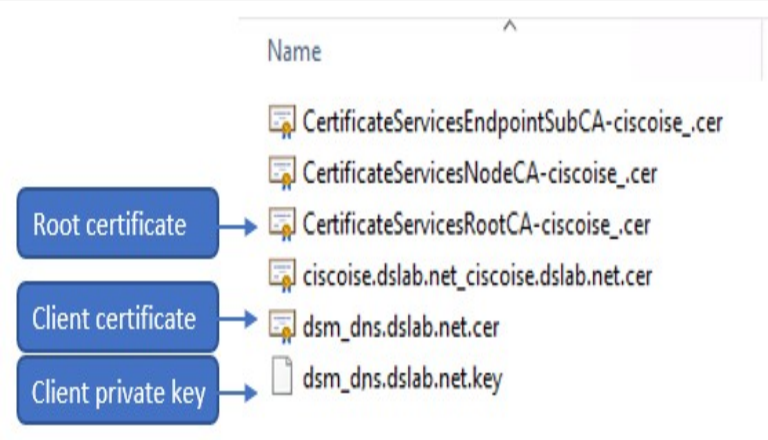
Deep Security ManagerはCisco Platform Exchange Grid (pxGrid) を通じてCisco ISEに接続します。pxGridはクライアントが情報を交換し、REST APIとWebsocketを介して通信することを可能にします。pxGridは安全な通信を保証し、信頼されたクライアントのみが制御されたpxGrid接続を通じて共有データにアクセスできます。

Deep Security Managerに接続する前に、Cisco ISE Webコンソールで次の設定を行う必要があります。

1. 管理 > pxGridサービス > クライアント管理 > 証明書に移動し、作成をクリックして、pxGridクライアント証明書、秘密鍵、およびルート証明書をPEM形式で生成します。
   ブラウザは、ルート証明書 (名前にRootCAが含まれるファイル)、クライアント証明書 (pxGridクライアント証明書作成時に指定されたコモンネームを含むファイル)、および秘密鍵を含むZIPバンドルをダウンロードします。

   注意: ZIPファイルには複数の証明書が含まれており、以下の命名規則が使用されています。
   - RootCAを名前に含むファイルは通常、自己署名証明書用のCisco ISEルート証明書を表します。
   - pxGridクライアント証明書の作成時に指定されたCommon Nameを含むファイルは、一般的にクライアント証明書と関連するクライアント秘密鍵に対応しています。

   以下の画像は、ZIPバンドル内に含まれるファイルの例を示しています。



   ヒント: Cisco ISEが公開認証局によって署名された証明書を使用して展開された場合、ZIPバンドルからルート証明書を抽出し、"Deep Security ManagerでCisco ISE接続を構成する" on the next page際に提出する必要があります。

2. Operations > Adaptive Network Control > ポリシーリストに移動し、Deep Security Managerで使用するためのAdaptive Network Control (ANC) ポリシーを作成または提供してください。
   Deep Security ManagerのpxGrid接続を構成するためにANCポリシー名が必要になるので、メモしておいてください。
3. すべてのDeep Security Managerノードをシャットダウンして、マネージャノード間でキャッシュデータが残るのを防ぎます。

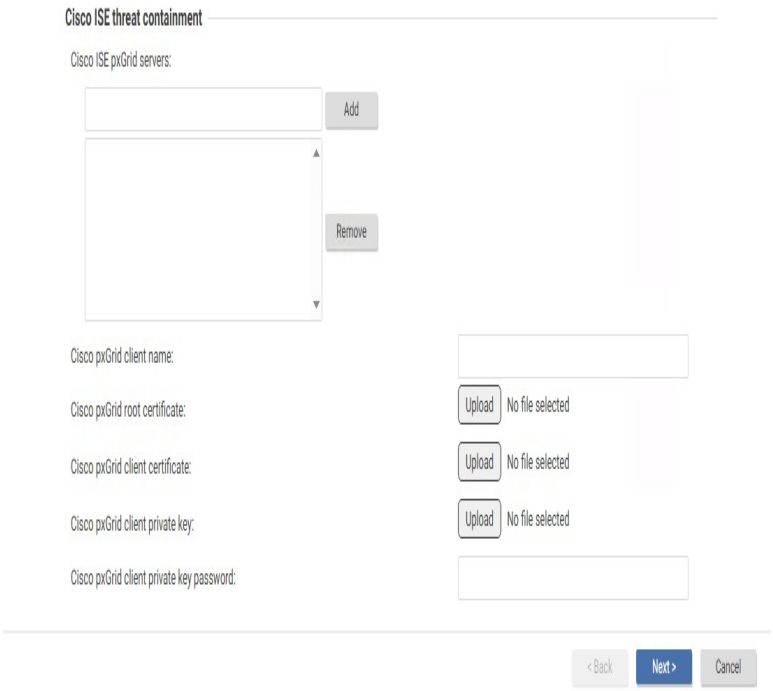
4. IoT/MQTTを介して高速パスイベント取得を有効にし、次のコマンドを使用してイベント取得をほぼリアルタイムに高速化します。
   `dsm_c -action iotevent -configuration enable -ciscortc`

   注意: 1つのマネージャに対してこのコマンドを実行すると、すべてのマネージャノードに変更が適用されます。これは、Cisco ISEをDeep Security Managerと統合するために必要なほぼリアルタイムのイベント送信を提供するために必要です。
5. すべてのマネージャノードを手動で開始します。

Deep Security ManagerでCisco ISE接続を構成する

Cisco ISEをDeep Security Managerに接続するには:

1. 管理 > システム設定 > Cisco脅威封じ込めに移動します。
2. Cisco脅威封じ込めを有効にするを選択し、pxGrid接続を構成するをクリックします。
   Cisco ISE脅威封じ込めウィンドウが表示されます。



3. Cisco pxGridクライアントに必要な情報を追加し、ファイルをアップロードしてください。詳細は以下の表を参照してください。

フィールド名	説明
Cisco ISE pxGridサーバ	pxGridサーバアドレスをhttps://<fqdn>:<port>形式で入力してください。例えば、URL内に複数のサーバアドレスを入力することができます。API呼び出しはラウンドロビン方式でこれらのアドレスを巡回します。
Cisco pxGridクライアント名	これはpxGridクライアントを登録するために使用される名前です。クライアント登録リクエストが送信されると、この名前は組織ISE内のpxGridクライアントリストに表示されます。
Cisco pxGridルート証明書	これは、pxGridサーバ証明書の公開鍵基盤 (PKI) 署名パスのルート証明書です。このファイルの取得方法については、上記の"前提条件Cisco ISE接続設定" on page 1909を参照してください。
Cisco pxGridクライアント証明書	pxGridクライアント証明書。このファイルの取得方法については、上記の"前提条件Cisco ISE接続設定" on page 1909を参照してください。
Cisco pxGridクライアント秘密鍵	pxGridクライアント証明書の秘密鍵。ファイルの取得方法については、上記の"前提条件Cisco ISE接続設定" on page 1909を参照してください。
Cisco pxGridクライアントプライベートキーパスワード	これはpxGridクライアント証明書の生成時に使用されるパスフレーズです。

4. すべてのフィールドが完了したら、次へをクリックします。Deep Security Managerは、提供された情報を使用してpxGridへの接続を試みます。
   - 接続が成功すると、マネージャはクライアント登録要求をpxGridサーバに送信し、Cisco ISE管理者の承認が必要になります。
   - 接続に失敗した場合、情報入力ページにリダイレクトされます。上記の手順3に戻り、入力した情報とアップロードしたファイルが正確で完全であることを確認してください。
5. クライアント登録要求を承認するには、Cisco ISE管理者はCisco ISEの管理 > pxGridサービス > クライアント管理 > クライアント> pxGridクライアントに移動します。そこから、適切な名前を選択し、承認をクリックします。
6. 管理者が登録リクエストを承認したら、Deep Security ManagerのCisco Threat Containmentタブに戻り、接続ステータスを更新をクリックしてください。接続ステータスラベルが有効に変わり、ANCポリシー名とネットワーク封じ込め基準のフィールドが有効になります。
7. ANCポリシー名を選択し、適切なアラート基準のチェックボックスを選択してから、保存をクリックします。これで構成が完了し、Deep Security Managerは指定されたアラート基準に一致するセキュリティイベントを積極的に監視し、イベントに関与する元のホストのMACアドレスにANCポリシーを適用します。

Cisco ISE接続ステータスリスト

ステータス	説明
Cisco pxGrid接続情報が設定されていません。	DSMにCisco pxGrid接続情報が設定されていません。
Cisco pxGridクライア	Cisco pxGrid接続情報が構成され、DSMはすでにクライアントアカウント登録

ステータス	説明
ント登録が送信されました。	要求を送信しました。DSMはISE管理者がクライアント要求を承認するのを待っています。
Cisco pxGridが接続され、クライアントステータスが有効です。	Cisco pxGrid接続情報が構成され、クライアントアカウントが承認 (有効化) されました。DSMのpxGridへの接続は正常に動作しています。ただし、ユーザはANCポリシー名を提供する必要があります。
Cisco pxGridが接続され、ANCポリシーが設定されました。	DSMはpxGridへの接続が正常に動作しており、ANCポリシー名がDSMに設定されています。さらに、DSMはANCポリシーがCisco ISEに存在することをすでに検証しています。注: これは完全に機能している接続状態です。
Cisco pxGridクライアントのステータスは無効です。	Cisco ISEでpxGridクライアントアカウントが無効になっています。ISE管理者はpxGridクライアントアカウントを有効にする必要があります。
Cisco ISE pxGridサーバに接続できません。	DSMがCisco pxGridサーバに接続できません。エラーの詳細についてはDSMログを参照してください。考えられる原因: • ファイアウォールによってCisco pxGridへのネットワーク接続がブロックされているか、アクセスできません。 • Root/クライアント証明書の有効期限が切れているか、Cisco ISE管理者によってクライアント資格情報が取り消された/削除されました。

モニタとトラブルシューティング

コンピュータまたはホストにANCポリシーが割り当てられた場合、または割り当てに失敗した場合、さらにCisco pxGrid接続が失敗した場合やCisco pxGridクライアント証明書が期限切れになった場合に、システムイベントが生成されます。

- イベントID: 9210
- イベント名: Cisco ANCポリシーが割り当てられました
- イベントID: 9211
- イベント名: Cisco ANCポリシー割り当て失敗
- イベントID: 9212
- イベント名: Cisco pxGrid接続失敗
- イベントID: 9213
- イベント名: Cisco pxGridクライアント証明書の有効期限が切れました

システムイベントの説明には、ANCポリシーの名前と、正常に割り当てられたMACアドレスが含まれます。

詳細については、システムイベントを参照してください。

MACアドレスがANC割り当てリストに存在するかどうかは、Cisco ISE Operations > Adaptive Network Control > Endpoint Assignmentに移動して確認できます。

注意: Deep Security Managerは、使用されているMACアドレスがCisco ISEで既に割り当てられている場合、ANCポリシーを再割り当てしません。ホストによって不正プログラムやランサムウェアイベントが生成されるが、MACアドレスにANCポリシーが割り当てられていない場合、イベントを生成する代わりに、マネージャは次のメッセージをログに記録します。

```
Jun 04, 2025 2:29:42.268000000 PM [+0800]
com.trendmicro.manager.core.cisco.RapidThreatContainmentHandler assignAncPolicy INFO:
ThID:258|TID:0|TNAME:Primary|UID:-1|UNAME:|Skipping assign ANC policy ANC_QUARANTINE to
MAC 00:50:56:75:**:** as it has been already assigned in Cisco ISE. Jun 04, 2025 2:29:42.271000000
PM [+0800] com.trendmicro.manager.core.cisco.RapidThreatContainmentHandler assignAncPolicy
INFO: ThID:258|TID:0|TNAME:Primary|UID:-1|UNAME:|Skipping assign ANC policy ANC_
QUARANTINE to HostID 1 as all MACs already assigned in Cisco ISE
```

SAP NetWeaverとの統合

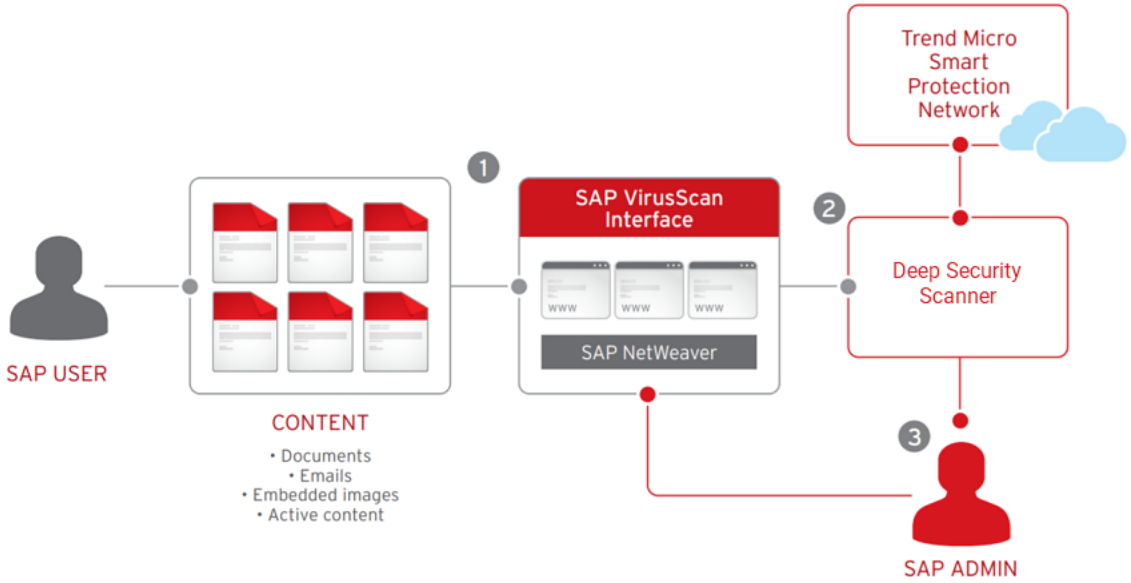
Deep Security Scanner により、Workload Security を使用して SAP デプロイメントを保護し、マルウェア、クロスサイトスクリプティング、SQL インジェクションなどの脅威から重要な情報を保護することができます。Workload Security は、SAP NetWeaver テクノロジープラットフォームにアップロードされたコンテンツをスキャンし、その真のタイプを判断し、NetWeaver-VSI インターフェイスを介して SAP システムに報告します。コンテンツスキャンにより、文書内に埋め込まれたまたは偽装された悪意のあるスクリプトコンテンツに対して保護が行われます。その後、SAP 管理者は、許可されるドキュメントタイプに応じてポリシーを設定できます。

Deep Security Scannerは、リレーが有効になっているエージェントを搭載したコンピュータではサポートされません。

注意: FIPSモードが有効な場合、Deep Security Scannerはサポートされません。"FIPS 140のサポート" on page 1870を参照してください。

Deep Security スキャナーは以下のように機能します:

1. SAPの顧客環境は、SAP NetWeaverプラットフォームのセキュリティコンポーネントであるSAP Virus Scan Interface(VSI) によって保護されています。VSIは、ドキュメント、埋め込み画像、JavaScriptおよびPDFおよびMicrosoft Officeドキュメントのスクリプトを含むアクティブコンテンツを含むすべての顧客コンテンツを保護するために使用されます。Deep Security Scannerは、SAP NetWeaverテクノロジーとSAP HANAプラットフォームとシームレスに連携します。
2. Deep Security Scanner は、SAP NetWeaver テクノロジープラットフォームにアップロードされたコンテンツのスキャンを実行し、その真のタイプを判断し、NetWeaver VSI インターフェースを介して SAP システムに報告します。コンテンツスキャンにより、文書内に埋め込まれたまたは偽装された悪意のあるスクリプトコンテンツに対して保護されます。
3. SAP管理者は、許可する実際のドキュメントの種類に応じてポリシーを設定できます。



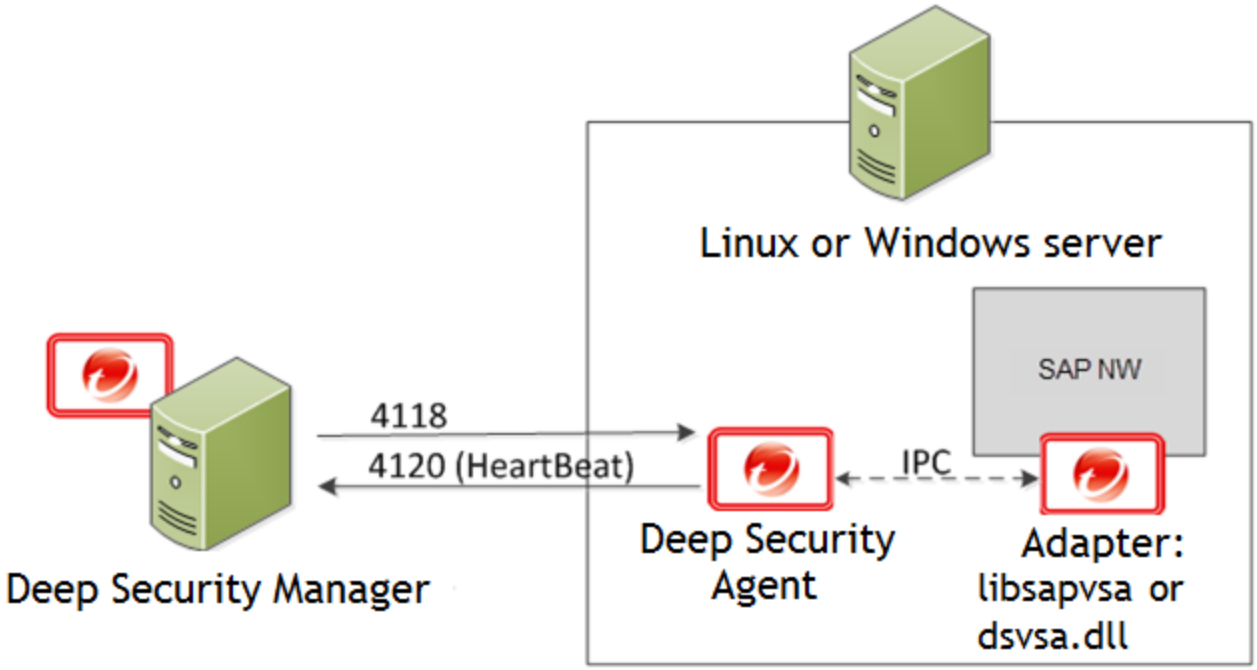
Deep SecurityおよびSAPコンポーネント

Deep Security Manager は SAP NetWeaver サーバー上にある Deep Security Agent に接続します。エージェントは、スキャン目的のためにトレンドマイクロが提供するウイルスアダプタである libsapvsa または dsvsa.dll に接続します。

Deep Security Scanner には、以下のコンポーネントが含まれています:

- Deep Security Manager:管理者がセキュリティポリシーを設定してDeep Security Agentの保護を実施するのに使用する、Webベースの管理コンソール。
- Deep Security Agent:コンピューターに直接展開されるセキュリティエージェントです。保護の内容は、各Deep Security AgentがDeep Security Managerから受け取るルールとセキュリティ設定によって異なります。

- SAP NetWeaver:SAPに統合された技術コンピューティングプラットフォーム。SAP NetWeaverウイルススキャンインターフェース(NW-VSI) は、実際のスキャンを実行するサードパーティ製品のウイルススキャン機能を提供します。NW-VSIインターフェースをアクティブ化する必要があります。
- SAP NetWeaver ABAP WinGUI: SAP NetWeaverに使用されるWindows管理コンソール。このドキュメントでは、Deep Security AgentおよびSAP NetWeaver Virus Scan Interfaceの設定に使用されます。



Deep Security ScannerとSAP NetWeaverの統合を有効にする

1. "Deep Security Scannerをアクティブ化" below.
2. Deep Security Scannerをサポートしているosについては、"各プラットフォームでサポートされている機能" on page 417を参照してください。
3. サポートされているオペレーティングシステムの1つを実行しているSAPアプリケーションサーバーにDeep Security Agentをインストールしてください。"Agentをインストールする" on the next pageを参照してください。
4. Deep SecurityにSAPサーバを追加し、SAPサーバでエージェントを有効化します。「 "Deep Security ManagerにSAPサーバを追加してエージェントを有効化する" on page 1920」を参照してください。
5. コンピュータまたはポリシーでSAP統合を有効にします。"セキュリティプロファイルを割り当てる" on page 1923を参照してください。
6. 次のトランザクションを呼び出して、SAPウイルススキャンインターフェース(VSI) を構成します("Agentを使用するようにSAPを設定する" on page 1926を使用するように構成する)
   - VSCANGROUP
   - VSCAN
   - VSCANPROFILE
   - VSCANTEST

使用するosや環境によっては、見る出力が若干異なる場合があります。

Deep Security Scannerをアクティブ化

1. Deep Security Managerで、[管理]→[ライセンス] に進みます。
2. [新しいアクティベーションコードの入力]を選択します。
3. [Deep Security Scanner] エリア ([追加機能] の下) で、Deep Security Scannerアクティベーションコードを入力し、[次へ] を選択して、画面の指示に従います。

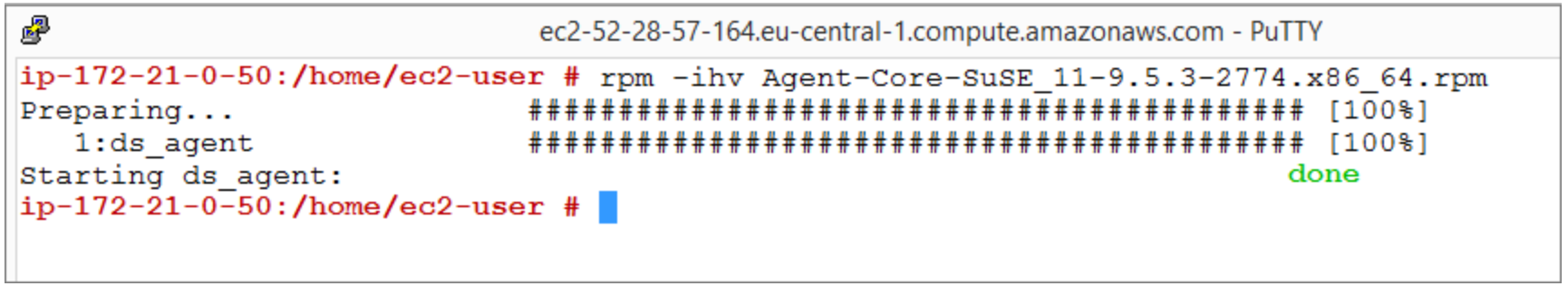
コンピュータエディタまたはポリシーエディタ[1]で設定 > Scannerタブに進み、個々のポリシーやコンピュータに対してSAPを有効にできます。

Deep Security検索ツールを使用するには、不正プログラム対策モジュールも有効にする必要があります。

Agentをインストールする

Deep Security Agentは、コアのエージェント機能のみでインストールされます。SUSE Linux Enterprise ServerまたはRed Hat Enterprise Linuxにエージェントがインストールされた後、エージェントで保護モジュールを有効にできます。その時点で、保護モジュールに必要なプラグインがダウンロードされ、インストールされます。

1. トレンドマイクロのダウンロードセンター(http://downloadcenter.trendmicro.com) にアクセスし、お使いのOSに対応するDeep Security Agentパッケージをダウンロードしてください。
2. Agentをターゲットシステムにインストールします。OSに応じて、rpmまたはzypperを使用できます。この例ではrpmを使用し、次のように入力します。
   `rpm -ihv Agent-Core-SuSE_<version>.x86_64.rpm`
3. この例で示されているような、Agentのインストールが完了したことを示す出力が表示されるはずです



Deep Security Managerで生成されたデプロイメントスクリプトを使用してエージェントをデプロイすることもできます。

[1] これらの設定は、ポリシーまたは特定のコンピュータについて変更できます。ポリシーの設定を変更するには、[ポリシー] 画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して [詳細] をクリック) します。コンピュータの設定を変更するには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して [詳細] をクリック) します。

Deep Security ManagerにSAPサーバを追加してエージェントを有効化する

1. SAPサーバーを追加するには、Deep Security Managerコンソールを開き、コンピュータータブでNewをクリックします。Microsoft Active Directory、VMware vCenter、Amazon Web Services、またはMicrosoft Azureと同期するなど、サーバーを追加する方法はいくつかあります。また、FQDNまたはIPアドレスを使用してコンピューターを追加することもできます。詳しい手順については、"コンピュータの追加について" on page 655を参照してください。
2. インスタンスのステータスは、Unmanaged (Activation Required) または Unmanged (Unknown) のいずれかです。次に、マネージャーがコンピューターを保護するためのルールとポリシーを割り当てる前に、エージェントをアクティブ化する必要があります。アクティベーションプロセスには、エージェントとマネージャー間でユニークな指紋の交換が含まれます。これにより、Deep Security Manager がエージェントと通信できるのは1つだけであることが保証されます。エージェントをアクティブ化する方法は2つあります。エージェント起動またはマネージャー起動です。
   - マネージャーによるアクティベーション:この方法では、Deep Security Managerがエージェントのハートビートのリッスンポート番号を介してFQDNまたはIPに接続できる必要があります。これは、NATポートフォワーディング、ファイアウォール、またはAWSセキュリティグループのために、時に困難になることがあります。マネージャーによるアクティベーションを実行するには、Deep Security Managerコンソールのコンピュータータブに移動し、エージェントがインストールされているインスタンスを右クリックし、アクション>アクティベートを選択します。マネージャーによるアクティベーションを使用する場合、不正なDeep Securityマネージャーからも"Deep Security Agentの保護" on page 1618。
   - Agentからリモートで有効化する方法:この方法では、設定されているDeep Security Managerのアドレスに、Deep Security AgentがManagerのハートビート用待機ポート番号経由で接続できることが必要です。

     Deep Security Managerのアドレス(FQDNまたはIP) は、Deep Security Managerコンソールの の[管理]→[Managerノード]で確認できます。

     また、Deep Security Managerコンソールで[管理] > [システム設定] > [Agents]を選択し、次に[Agentからのリモート有効化を許可]を選択して、Agentからのリモート有効化を有効にする必要があります。

     次に、Deep Security Agent 上でローカルに実行されるコマンドラインツールを使用して、アクティベーションプロセスを開始します。最小限のアクティベーション手順には、アクティベーションコマンドとマネージャーの URL(ポート番号を含む) が含まれています

```
dsa_control -a dsm://[managerurl]:[port]/
```

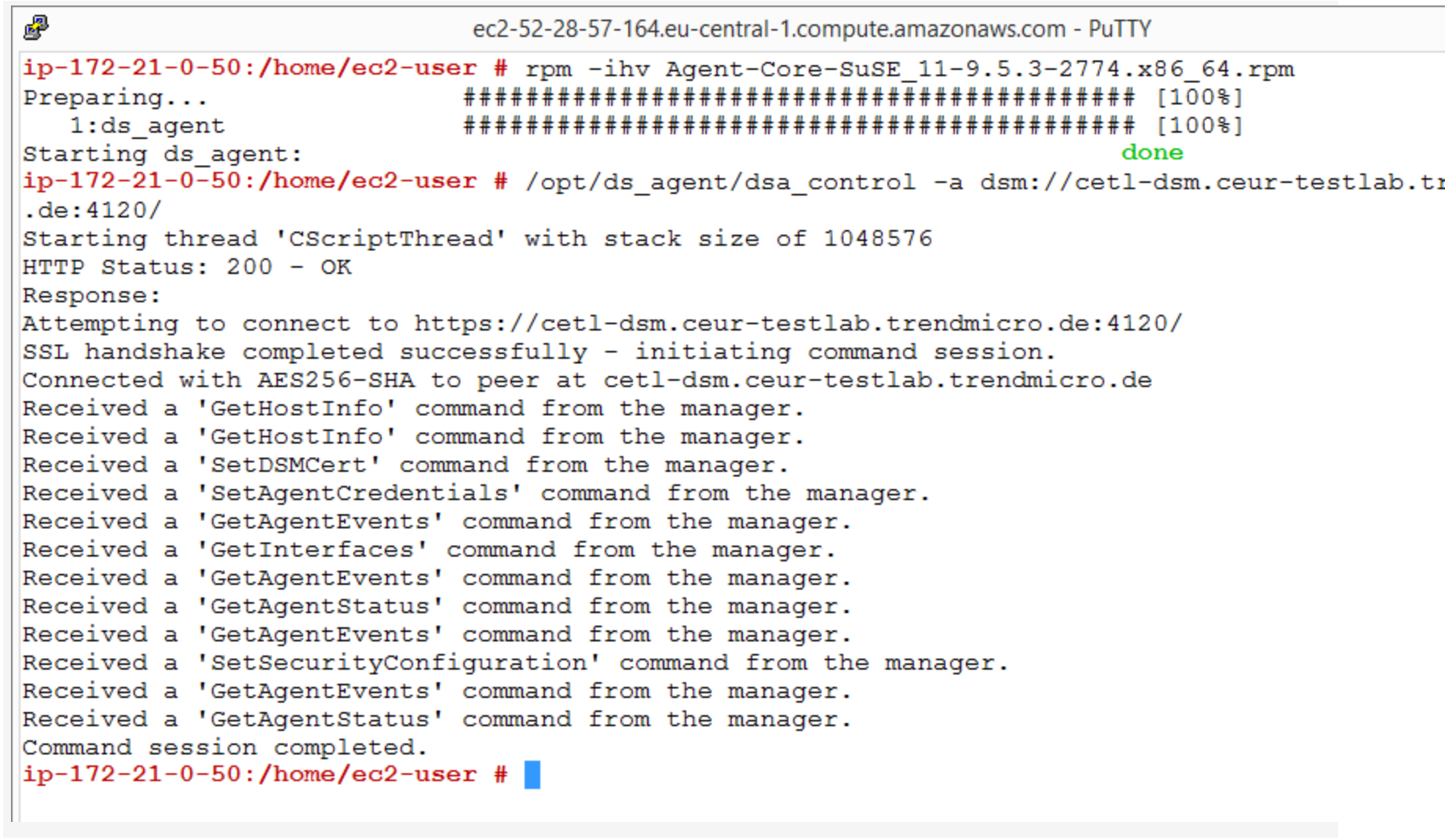
指定する項目は次のとおりです。

- -aはAgentを有効化するコマンドです
- dsm://managerurl:4120/は、Agentに接続先のDeep Security Managerを指示するパラメータです。managerurl Deep Security ManagerのURLであり、4120は、デフォルトのエージェントからマネージャーへの通信ポートです。

マネージャーURLは、アクティベーションコマンドの唯一必須パラメーターです。追加のパラメーターも利用可能です("コマンドラインの基本" on page 1793を参照)

以下の例では、タイピングによるAgentからのリモート有効化が使用されます

```
/opt/ds_agent/dsa_control -a dsm://cetl-dsm.ceur-testlab.trendmicro.de:4120/
```



上記の出力は、Agentの有効化が完了したことを示しています。

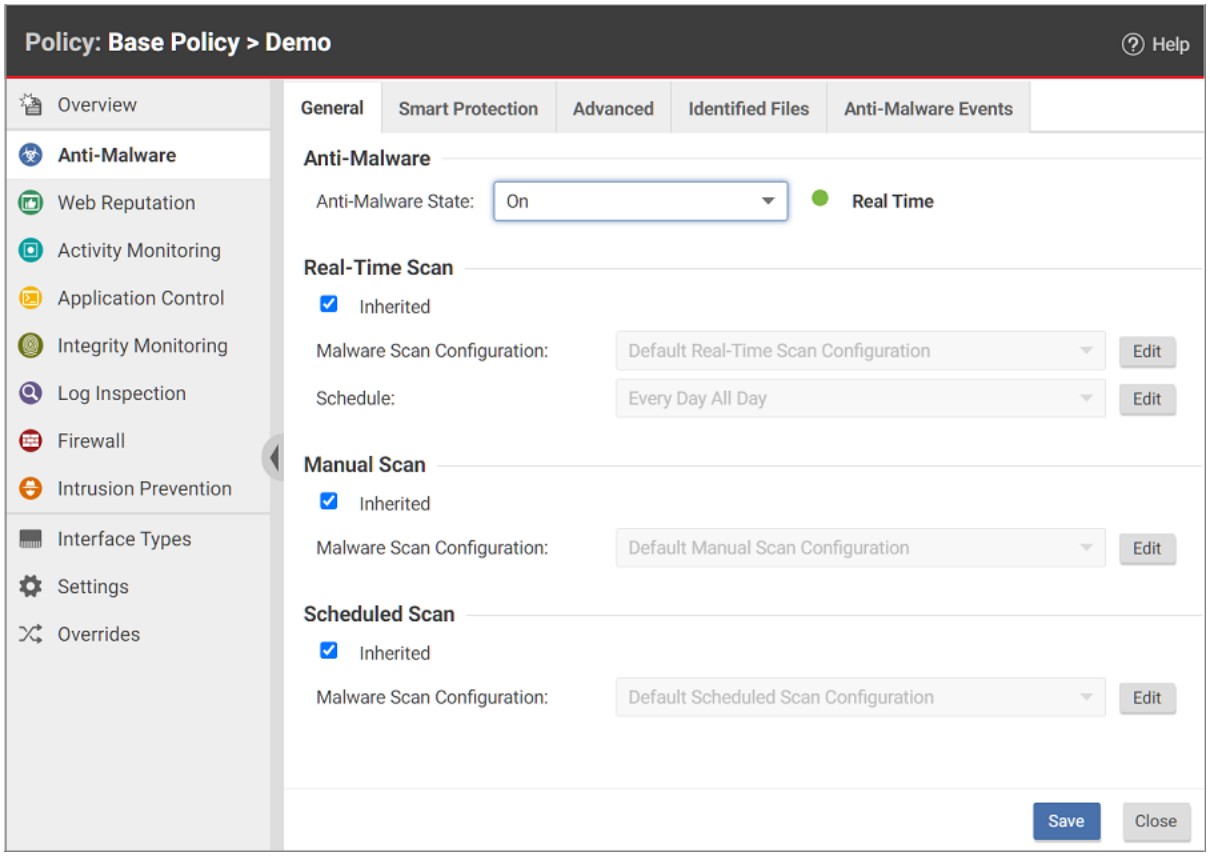
3. アクティベーションを確認するには、Deep Security Managerコンソールでコンピュータータブに移動し、コンピューター名を選択してから詳細を選択して、コンピューターのステータスが管理されていることを確認してください。

セキュリティプロファイルを割り当てる

この時点で、エージェントのステータスは管理されています(オンライン) が、保護モジュールがインストールされていません。これは、エージェントとマネージャーが通信していることを意味しますが、エージェントはどの構成も使用していません。

保護を適用するには、いくつかの方法があります。この例では、SAPインスタンスで直接設定を行います。これには、SAPを有効化し、不正プログラム対策 を有効化してエージェントに最新のパターンファイルと検索エンジンを提供し、初期設定の検索設定を割り当てます。

1. コンピュータエディタ[1]で、[不正プログラム対策]→[一般]の順に選択します。
2. 不正プログラム対策 セクションで、[設定]を[オン](または [継承 (オン)]) に設定し、[保存]をクリックします。



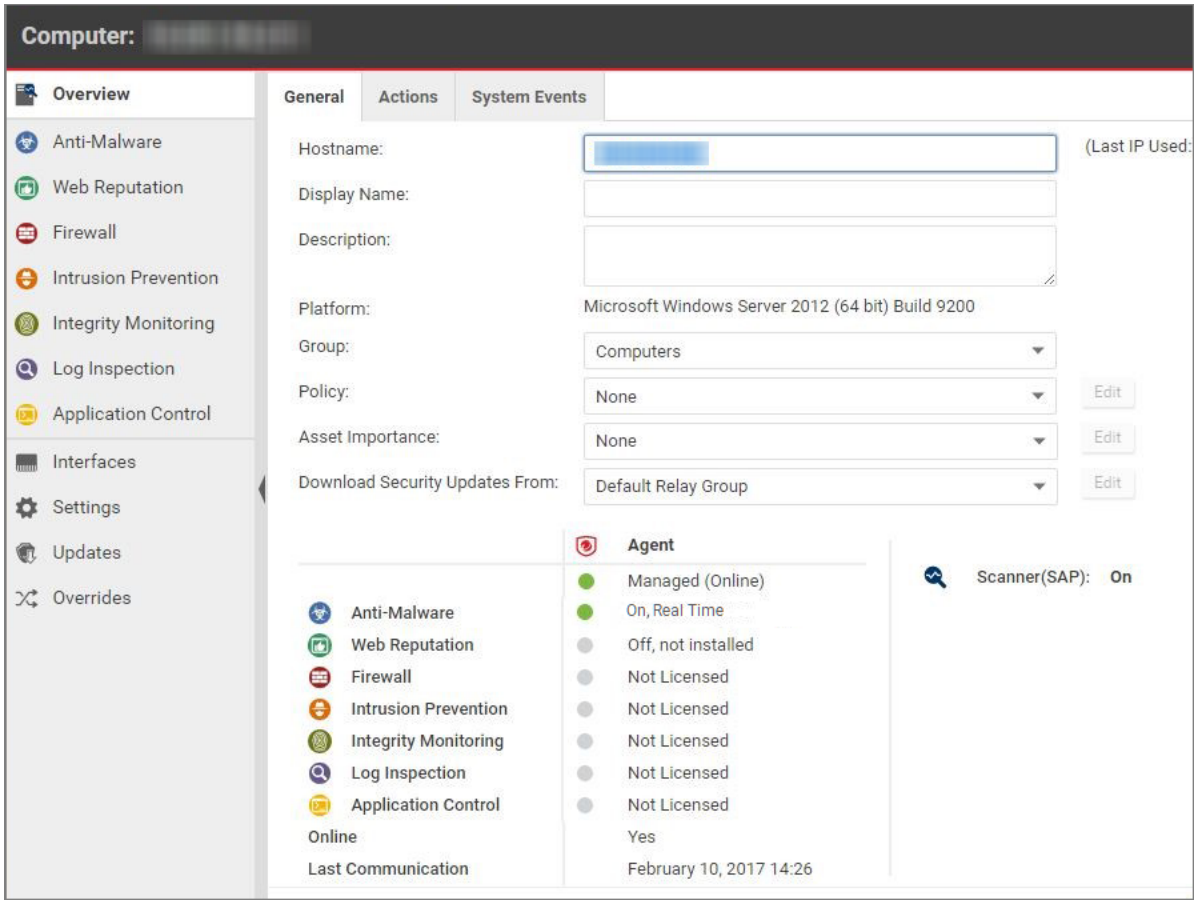
3. [リアルタイム検索]、[手動検索]、または [予約検索] のセクションで、[不正プログラム検索設定] および [スケジュール] を設定するか、それらの設定を親ポリシーから継承するように設定します。
4. 保存をクリックします。不正プログラム対策モジュールのステータスがオフ、インストール待ちに変わります。これは、エージェントがDeep Security Managerから必要なモジュールを取得していることを意味します。これを実現するには、クライアントがリレーのリスニングポー

[1] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック(またはコンピュータを選択して[詳細]をクリック)します。

ト番号でDeep Security Relayにアクセスする必要があります。数秒後、エージェントは不正プログラム対策パターンやスキャンエンジンなどのセキュリティ更新プログラムのダウンロードを開始するはずです。

5. コンピュータエディタで、[設定] > [Scanner] に進みます。
6. [SAP] セクションで、[設定] を [オン] (または [継承 (オン)]) に設定し、保存 をクリックします。

Agentのステータスが再び [管理対象 (オンライン)] に変わり、不正プログラム対策モジュールとScanner (SAP) モジュールのステータスが [オン] に変わったら、SAPの設定に進むことができます。



Agentを使用するようにSAPを設定する

Deep Security Agent が実行され、オペレーティングシステムのファイルシステムをスキャンできるようになりました。次に、SAPアプリケーションサーバーでエージェントを認識できるようにします。これを使用するには、アプリケーションサーバー内にウイルススキャンアダプタを作成します。ウイルススキャンアダプタはグループの一部である必要があります。ウイルススキャンアダプタとウイルススキャングループが作成されたら、ウイルススキャンプロファイルを使用して、スキャンする内容と動作方法を構成します。

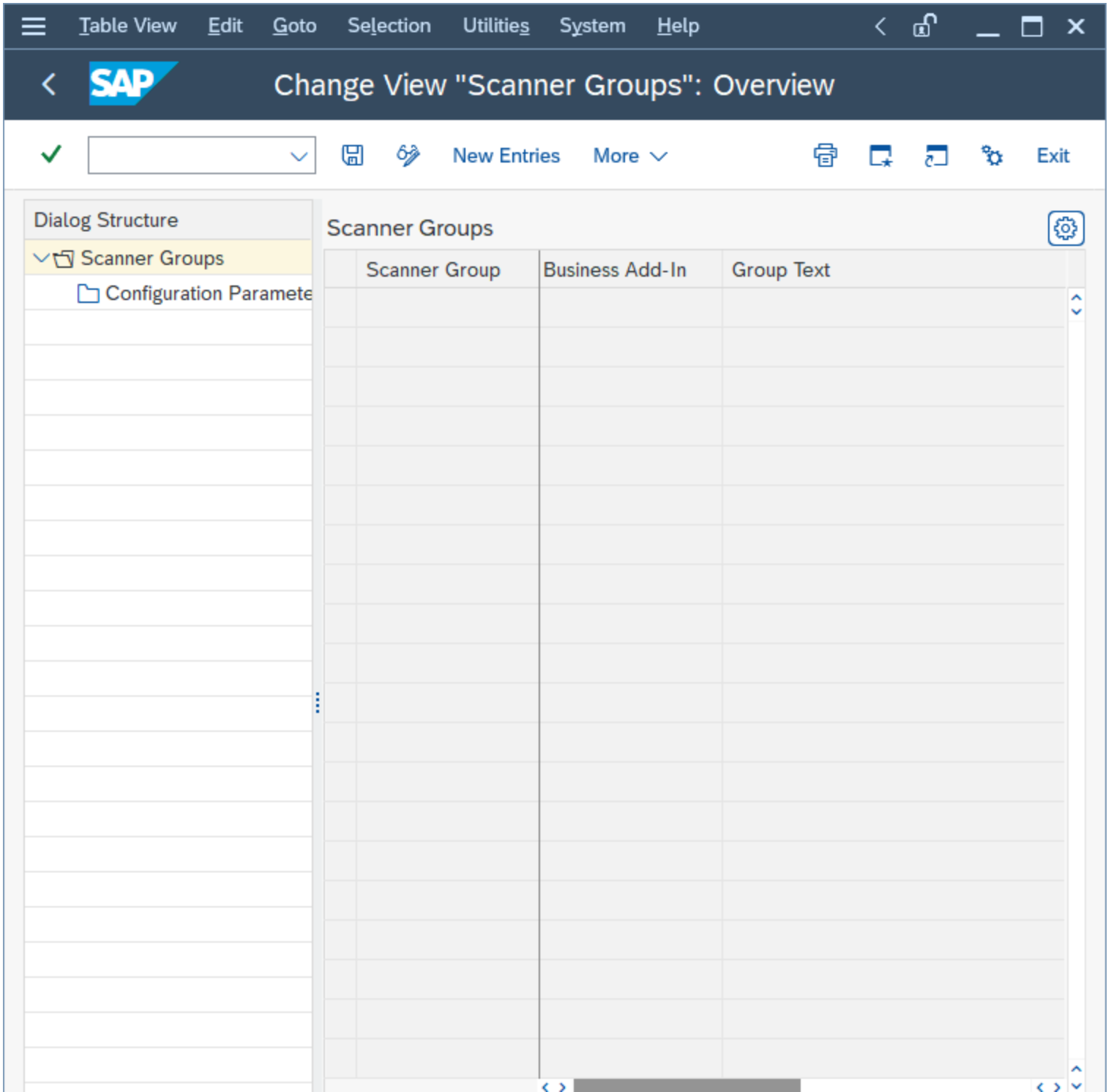
環境によって、以下の手順が必要です

1. "トレンドマイクロのスキャナグループを設定する" on the next page または"Java 環境でトレンドマイクロ スキャナー グループを構成する" on page 1954
2. "トレンドマイクロのウイルススキャンプロバイダを設定する" on page 1933 または"Java環境でトレンドマイクロウイルススキャンプロバイダを設定する" on page 1956
3. "トレンドマイクロのウイルススキャンプロファイルを設定する" on page 1939 または"Java環境でトレンドマイクロウイルススキャンプロファイルを設定する" on page 1958
4. "ウイルススキャンインタフェースをテストする" on page 1948 または"Java環境でウイルススキャンインターフェースをテストする" on page 1963

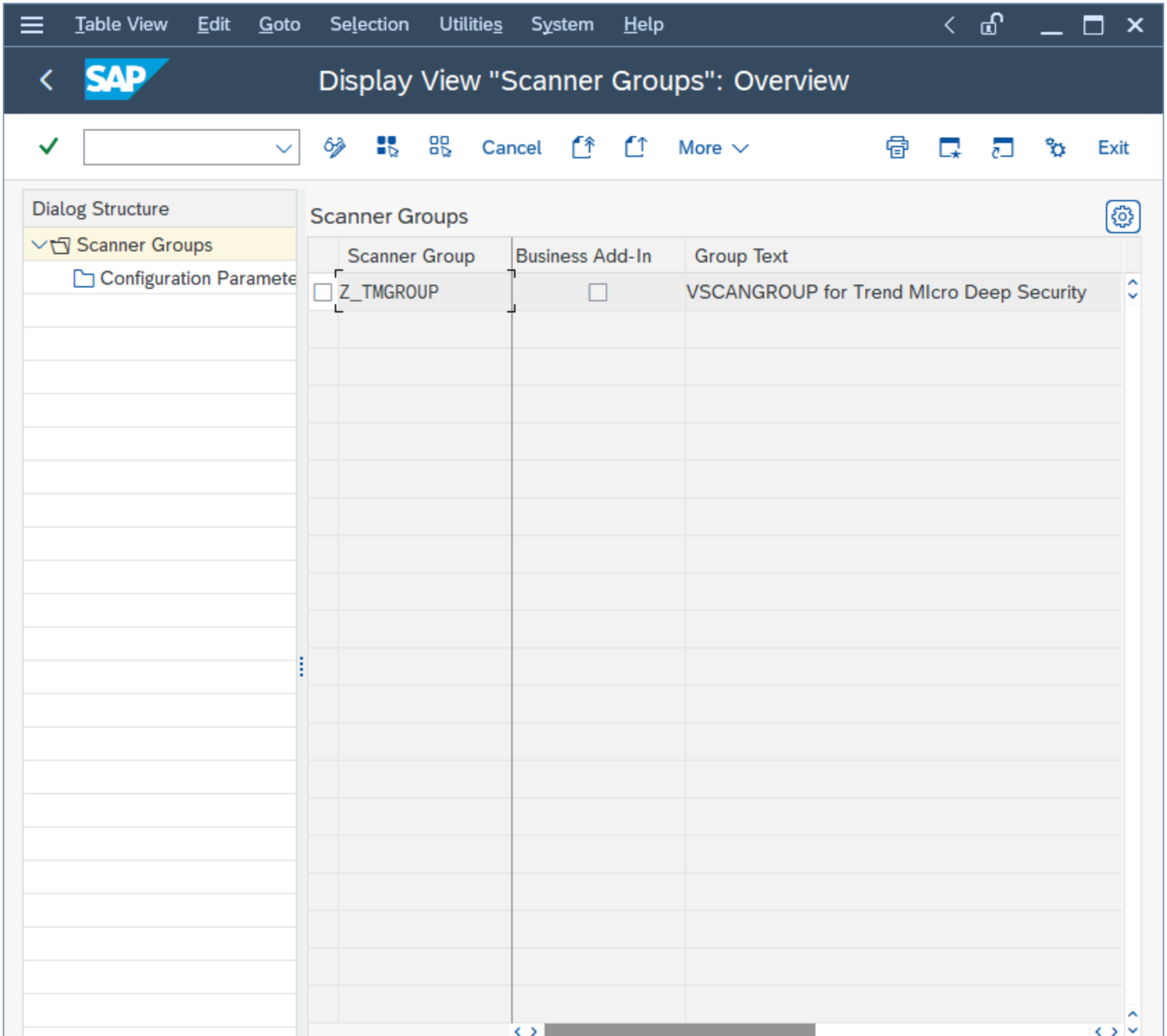
ウイルススキャングループとウイルススキャンアダプターは両方ともグローバル設定(クライアント00) です。ウイルススキャンプロファイルは、各テナント(クライアント01、02など) で設定する必要があります。

トレンドマイクロのスキャナグループを設定する

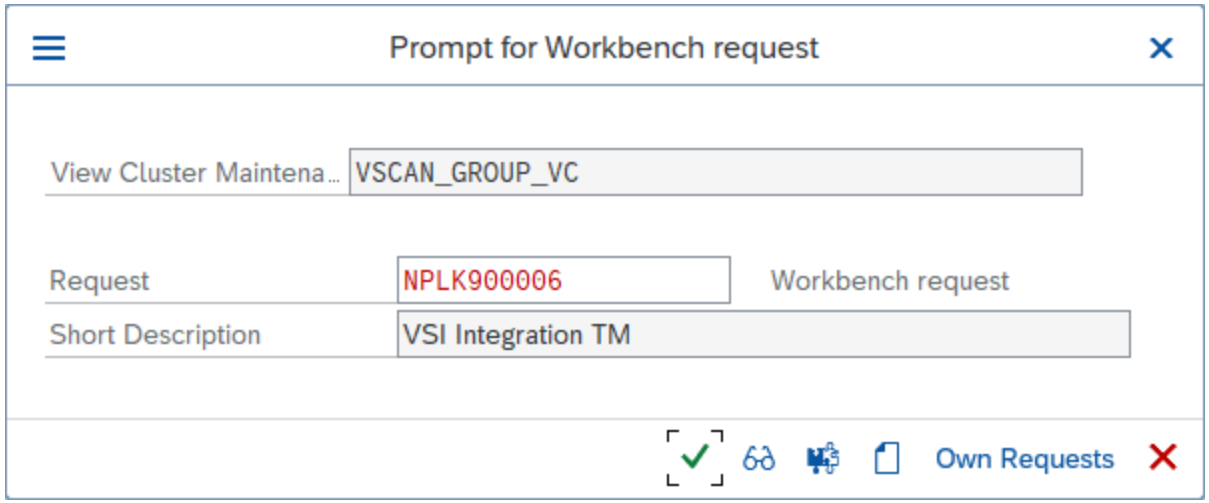
1. SAP WinGUI で、VSCANGROUP トランザクションを実行します。編集モードで、New Entries をクリックします。


Table View
Edit
Goto
Selection
Utilities
System
Help
SAP
Change View "Scanner Groups": Overview
New Entries
More
Exit
Dialog Structure
Scanner Groups
Configuration Paramete
Scanner Groups
Scanner Group
Business Add-In
Group Text

2. 新しいスキャナグループを作成して、[Scanner Group] 領域でグループ名を指定し、[Group Text] 領域でスキャナグループの説明を指定します。


Table View
Edit
Goto
Selection
Utilities
System
Help
SAP
Display View "Scanner Groups": Overview
Cancel
More
Exit
Dialog Structure
Scanner Groups
Configuration Paramete
Scanner Groups
Scanner Group
Business Add-In
Group Text
Z_TMGROUP
VSCANGROUP for Trend MIcro Deep Security

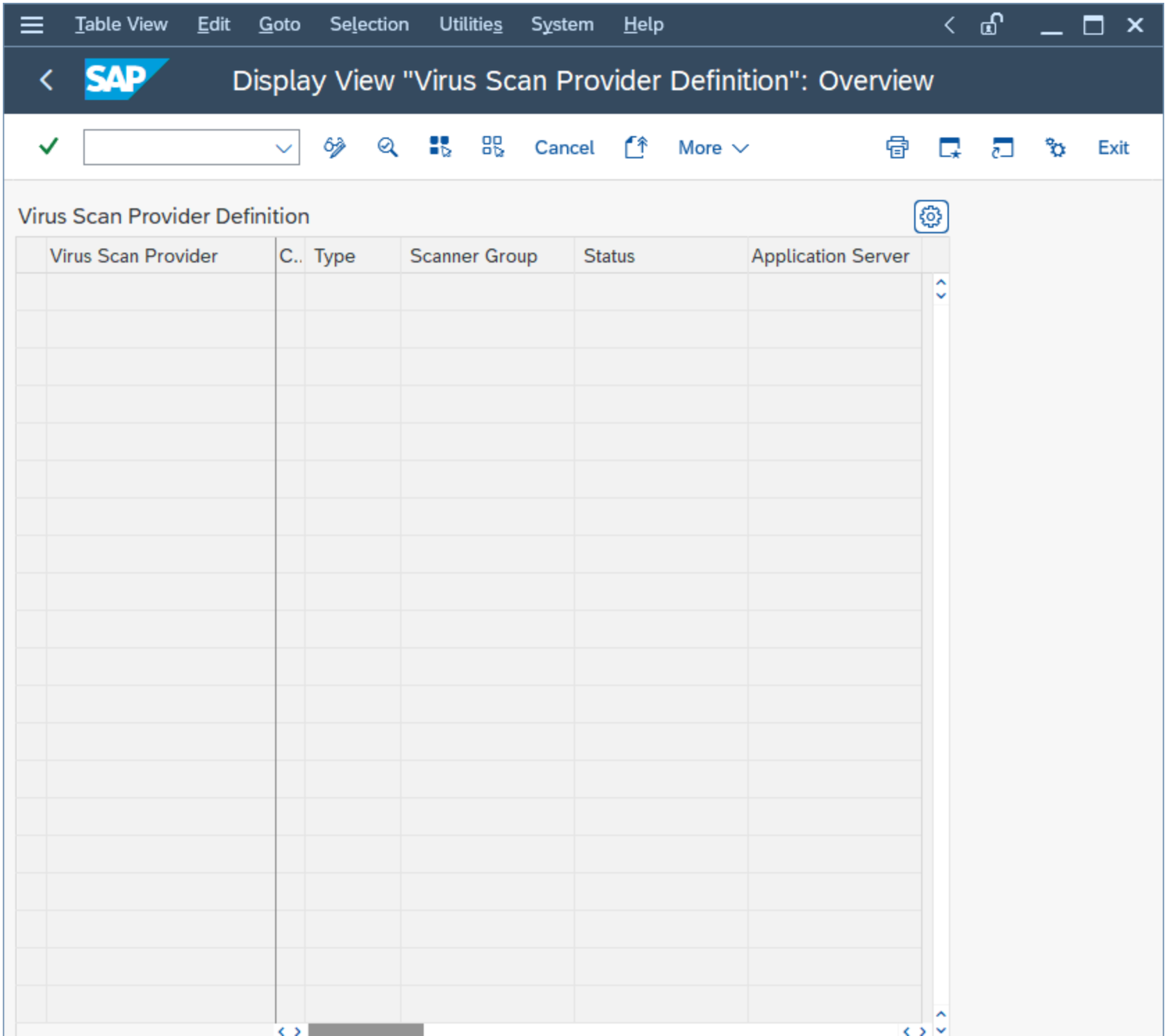
3. 編集モードを終了するには保存アイコンをクリックしてください。
   ワークベンチ要求のプロンプトダイアログが表示されます。以下の例では、すべてのVSI関連の変更を追跡するために新しいワークベンチ要求が作成されます。



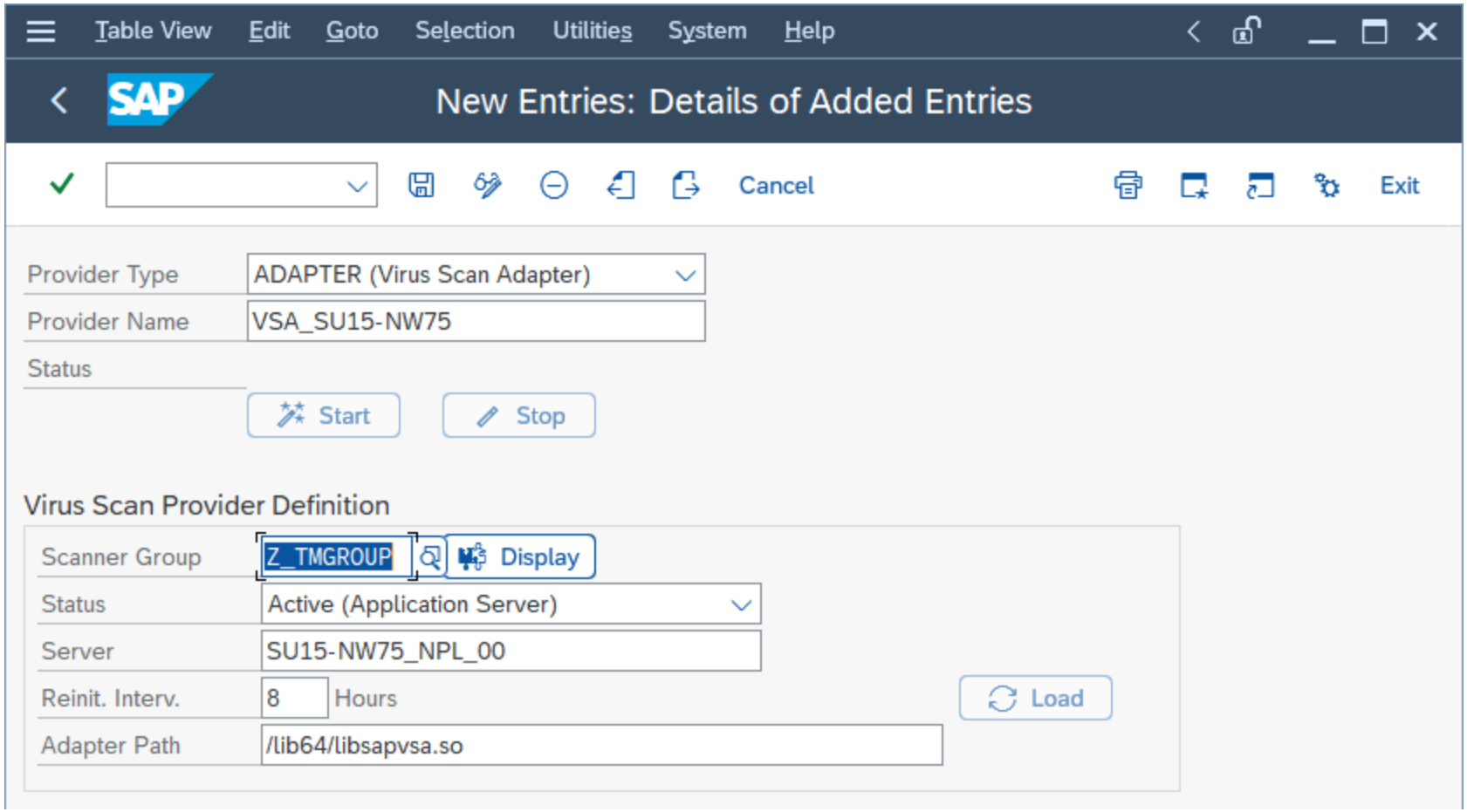
次の手順で、VSI統合を実際に設定します。これはウイルススキャンアダプタと呼ばれます。

トレンドマイクロのウイルススキャンプロバイダを設定する

1. SAP WinGUIで、VSCANトランザクションを実行します。編集モードで、新規エントリをクリックします。

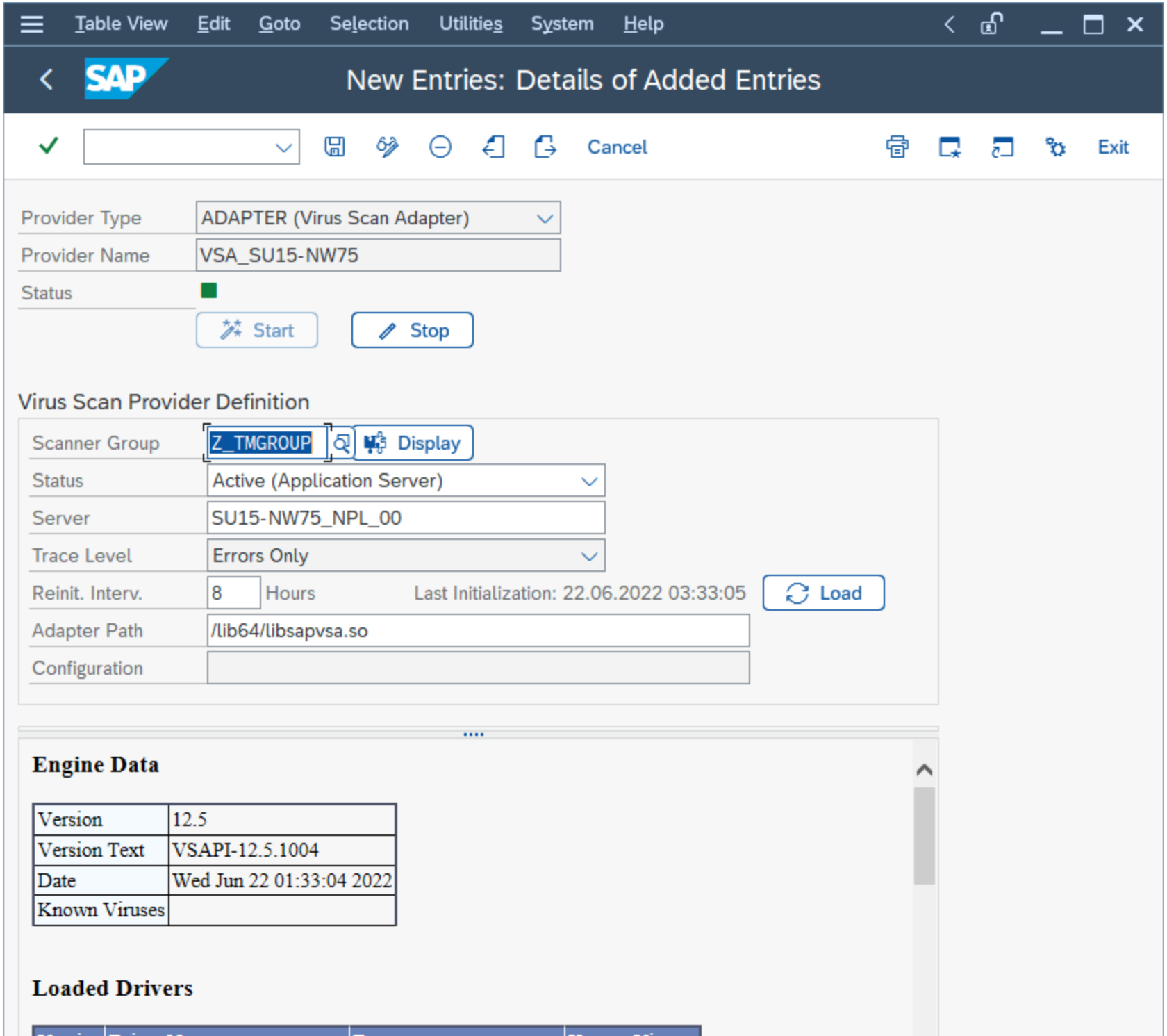

Table View
Edit
Goto
Selection
Utilities
System
Help
SAP
Display View "Virus Scan Provider Definition": Overview
Cancel
More
Exit
Virus Scan Provider Definition
Virus Scan Provider
C..
Type
Scanner Group
Status
Application Server

2. VSI認定ソリューションの新しい設定を入力します。
   以下の例では、次の構成パラメータが設定されています。



設定	値	説明
Provider Type	ADAPTER (Virus Scan Adapter)	自動的に設定されます(初期設定)。
Provider Name	VSA_<ホスト名>	自動的に設定され、エイリアスとして機能します。
Scanner Group	前の手順で設定したグループを選択します。	入力ヘルプを使用して、以前に作成されたすべてのスキャナグループを表示できます。
Status	Active (Application Server)	自動的に設定されます(初期設定)。
Server	nplhost_NPL_42	自動的に設定されるホスト名です。
Reinit.Interv.	8 Hours	ウイルススキャンアダプタが再初期化されて新しいウイルス定義がロードされるまでの時間を指定します。
Adapter Path (Linux)	/lib64/libsapvsa.so	初期設定のパスです。
Adapter Path (Windows)	C:\Program Files\Trend Micro\Deep Security Agent\lib\dsvsa.dll	初期設定のパスです。

3. 編集モードを終了するには、[保存] アイコンをクリックしてください。
   この設定をワークベンチリクエストにまとめるように求めるプロンプトが表示されます。
4. リクエストを確認し、開始をクリックしてください。
   ステータスライトが緑になり、アダプタがロードされ、アクティブになります:


Table View
Edit
Goto
Selection
Utilities
System
Help
SAP
New Entries: Details of Added Entries
Cancel
Exit
Provider Type
ADAPTER (Virus Scan Adapter)
Provider Name
VSA_SU15-NW75
Status
Start
Stop
Virus Scan Provider Definition
Scanner Group
Z_TMGROUP
Display
Status
Active (Application Server)
Server
SU15-NW75_NPL_00
Trace Level
Errors Only
Reinit. Interv.
8
Hours
Last Initialization: 22.06.2022 03:33:05
Load
Adapter Path
/lib64/libsapvsa.so
Configuration
Engine Data
Version
12.5
Version Text
VSAPI-12.5.1004
Date
Wed Jun 22 01:33:04 2022
Known Viruses
Loaded Drivers

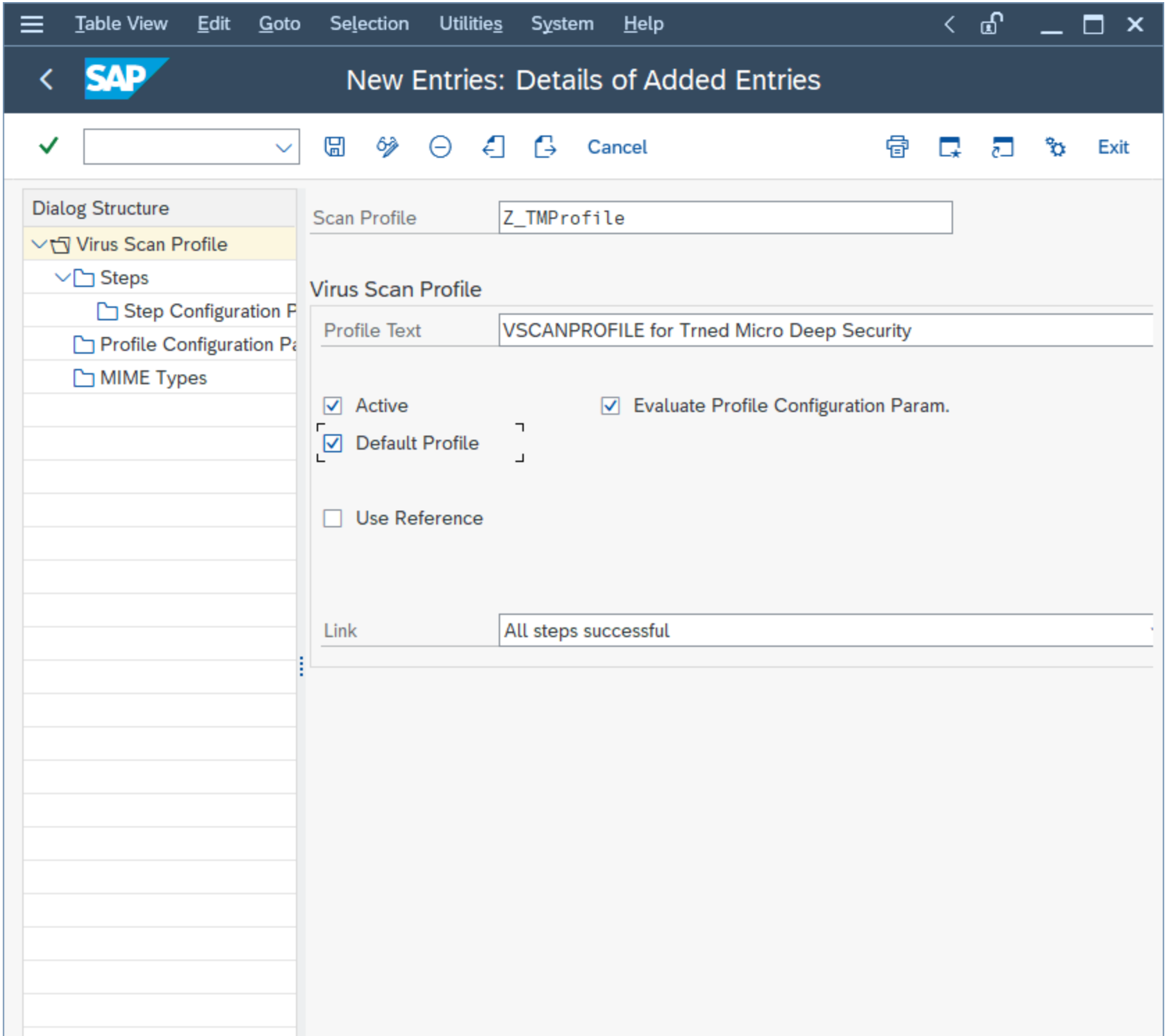
ここまでで、VSIの設定はほぼ完了です。これで、アプリケーションサーバは、Trend Micro Deep Securityが提供するウイルス検索を使用してファイルトランザクションを処理できるようになります。

トレンドマイクロのウイルススキャンプロファイルを設定する

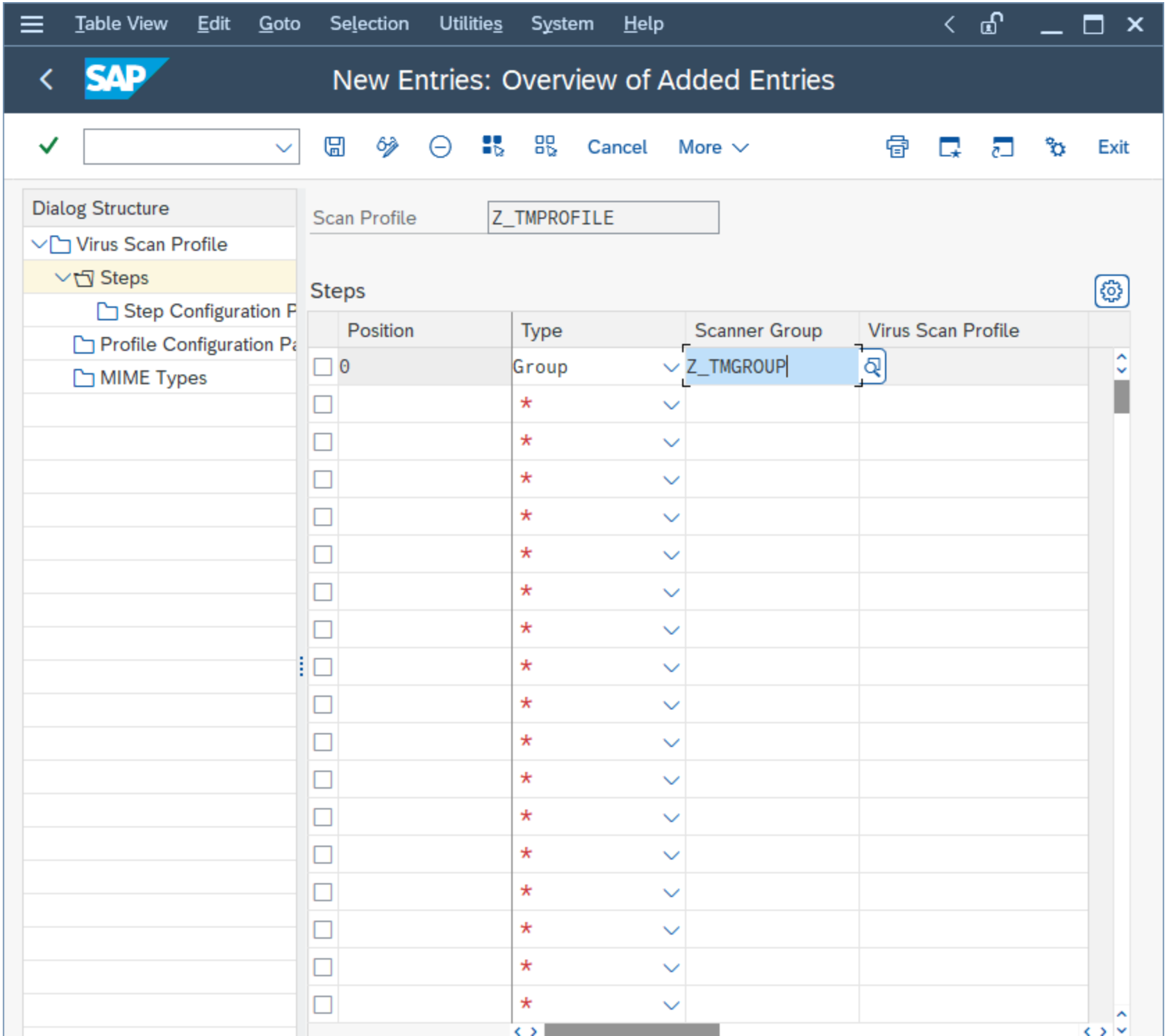
1. SAP WinGUI で、VSCANPROFILE トランザクションを実行し、ウイルススキャンが必要な SAP 操作を選択します。
   例えば、/SCET/GUI_UPLOAD または /SCET/GUI_DOWNLOAD の「アクティブ」チェックボックスを確認し、保存 アイコンをクリックし

ます。

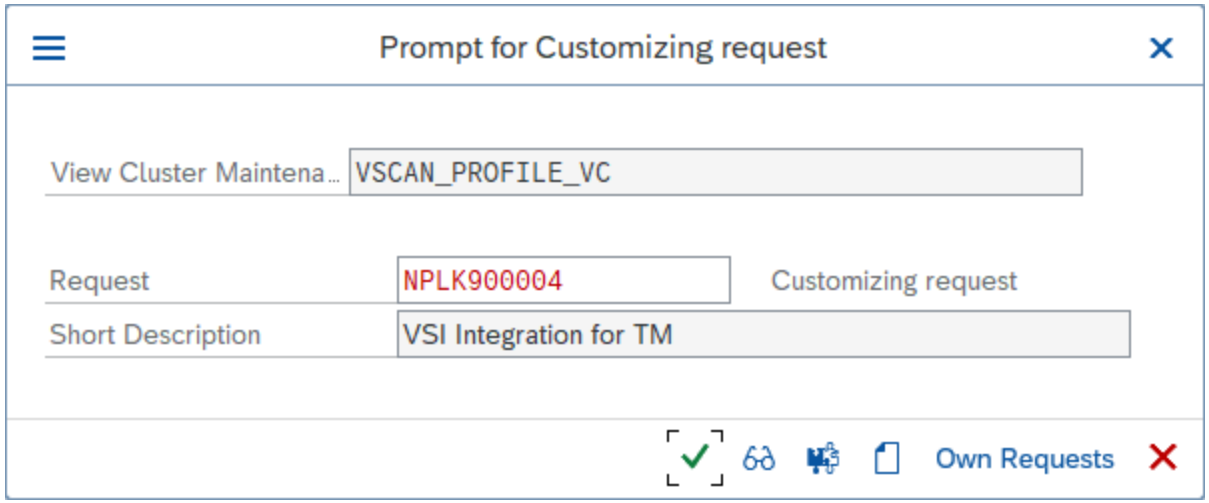
2. 編集モードで、新しいエントリをクリックします。
   ウイルススキャンプロファイルは、ウイルススキャンインターフェースに対応して、特定のトランザクション(ファイルのアップロード、ダウンロードなど) がどのように処理されるかを定義します。アプリケーションサーバーで以前に構成されたウイルススキャンアダプタを使用するには、新しいウイルススキャンプロファイルを作成する必要があります
3. [Scan Profile] フィールドにZ_TMProfileを入力し、[Active]、[Default Profile]、[Evaluate Profile Configuration Param]を選択してください。


Table View
Edit
Goto
Selection
Utilities
System
Help
SAP
New Entries: Details of Added Entries
Cancel
Exit
Dialog Structure
Virus Scan Profile
Steps
Step Configuration P
Profile Configuration Pa
MIME Types
Scan Profile
Z_TMProfile
Virus Scan Profile
Profile Text
VSCANPROFILE for Trned Micro Deep Security
Active
Evaluate Profile Configuration Param.
Default Profile
Use Reference
Link
All steps successful

4. 編集モードのまま、左側のステップをダブルクリックして、ステップを構成します:


Table View
Edit
Goto
Selection
Utilities
System
Help
New Entries: Overview of Added Entries
Cancel
More
Exit
Dialog Structure
Virus Scan Profile
Steps
Step Configuration P
Profile Configuration Pa
MIME Types
Scan Profile
Z_TMPROFILE
Steps
Position
Type
Scanner Group
Virus Scan Profile
0
Group
Z_TMGROUP

5. [New Entries] をクリックします。
   ステップは、プロファイルがトランザクションから呼び出されたときの動作を定義します。
6. [Position] を「0」に、[Type] を「Group」に、[Scanner Group] を前の手順で設定したグループの名前に、それぞれ設定します。
7. 編集モードを終了するには保存アイコンをクリックしてください。
   既存のウイルススキャンプロファイル、/SCET/DP_VS_ENABLEDに関する通知が表示されます。
8. プロファイルがアクティブでなく使用されていないため、既存のプロファイルに関する通知を無視してください。
   この通知を確認した後、この構成をカスタマイズリクエストにパックするように求められます。新しいリクエストを作成することで、行われた変更を追跡するのに役立ちます:



9. ステップの構成パラメータを作成するには、左側のプロファイル構成パラメータをダブルクリックし、新しいエントリをクリックしてパラメータを設定してください

パラメータ	種類	説明
CUST_ACTIVE_CONTENT	BOOL	ファイルにスクリプト(JavaScript、PHP、またはASPスクリプト) が含まれているかどうかを確認し、ブロックします。

パラメータ	種類	説明
CUST_ CHECK_ MIME_TYPE	BOOL	ファイル拡張子名がMIMEタイプと一致しているかどうかを確認します。一致しない場合、ファイルはブロックされます。すべてのMIMEタイプと拡張子名を完全に一致させることができます。例: • Microsoft Word ファイルは必須です .doc または .dot • JPEGファイルは .jpg • テキストファイルとバイナリファイルには、他の既知のファイルの拡張子でない限り、任意の拡張子を使用できます。つまり、txt または .bin, ただし .doc または .jpg 「サポートされているMIMEタイプ」を参照してください。

10. 左側のステップ構成パラメータをダブルクリックし、新規エントリを選択してパラメータを設定してください

パラメータ	種類	説明	初期設定(Linux)	初期設定 (Windows)
SCANBESTEFFORT	BOOL	検索はベストエフォートで実行する必要があります。つまり、SCANALLFILESやSCANEXTRACTなど、VSAによるオブジェクトの検索を許可するすべてのセキュリティクリティカルフラグを有効にする必要があります。また、内部フラグも有効にする必要があります。これらのフラグの詳細は、証明書に保存できます。	(未設定)	(未設定)
SCANALLFILES	BOOL	ファイル拡張子に関係なくすべてのファイルをスキャンします。	disabled	disabled
SCANEXTENSIONS	CHAR	VSAが検索するファイル拡張子のリスト。設定された拡張子のみがチェックされます。他の拡張子はブロックされます。パターンを検索す	null	「」

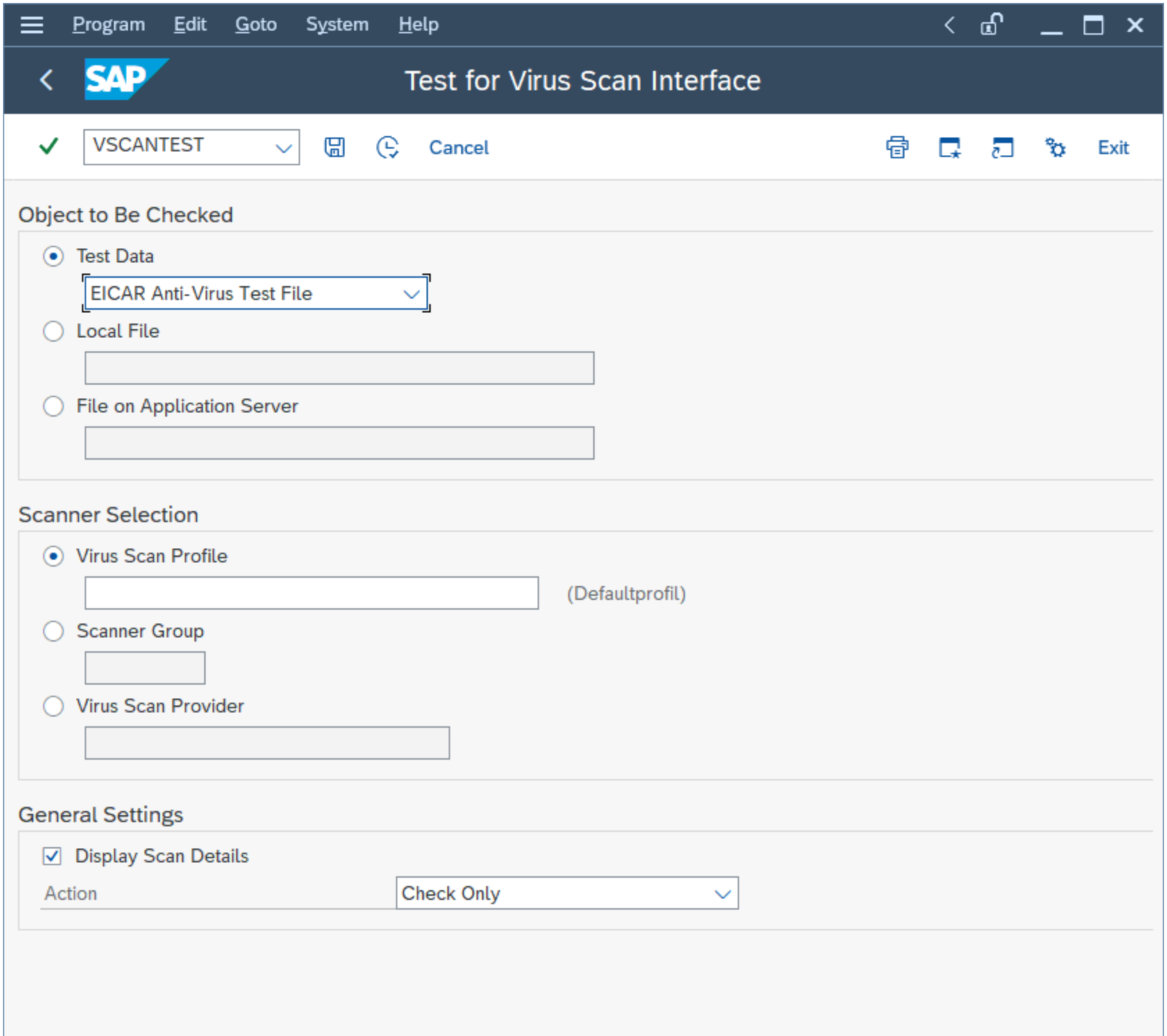
パラメータ	種類	説明	初期設定(Linux)	初期設定(Windows)
		るためにワイルドカードも使用できます。* この場所とその後を表します ? はこの文字のみを表します。例えば、exe;com;do?;ht* => \`*\ すべてのファイルをスキャンすることを意味します。		
SCANLIMIT	INT	この設定は、圧縮ファイルに適用されます。解凍して検索するファイルの最大数を指定します。	INT_MAX	65535
SCANEXTRACT	BOOL	アーカイブまたは圧縮オブジェクトを解凍します。	有効	有効
SCANEXTRACT_SIZE	SIZE_T	最大解凍サイズです。	0x7FFFFFFF	62914560 (60 MB)
SCANEXTRACT_DEPTH	INT	オブジェクトが解凍される最大の深さ(階層)です。	20	20
SCANLOGPATH	CHAR	VSAのカスタムログパス。	(未設定)	(未設定)
SCANMIMETYPES	CHAR	検索対象のMIMEタイプのリスト。MIMEタイプが設定されているファイルのみがチェックされます。他のMIMEタイプはブロックされます。このパラメータは、CUST_CHECK_MIME_TYPEが有効な場合にのみ機能します。	(未設定)	(未設定)

パラメータ	種類	説明	初期設定(Linux)	初期設定(Windows)
BLOCKMIMETYPES	CHAR	ブロックするMIMEタイプのリスト。このパラメータは、CUST_CHECK_MIME_TYPEが有効な場合にのみ機能します。	(未設定)	(未設定)
BLOCKEXTENSIONS	CHAR	ブロックするファイル拡張子のリスト。	(未設定)	(未設定)

この設定はクライアント単位であり、SAPアプリケーションサーバの各テナントで設定する必要があります。

ウイルススキャンインタフェースをテストする

1. SAP WinGUIで、VSCANTESTトランザクションを実行します。


Program
Edit
Goto
System
Help
SAP
Test for Virus Scan Interface
VSCANTEST
Cancel
Exit
Object to Be Checked
Test Data
EICAR Anti-Virus Test File
Local File
File on Application Server
Scanner Selection
Virus Scan Profile
(Defaultprofil)
Scanner Group
Virus Scan Provider
General Settings
Display Scan Details
Action
Check Only

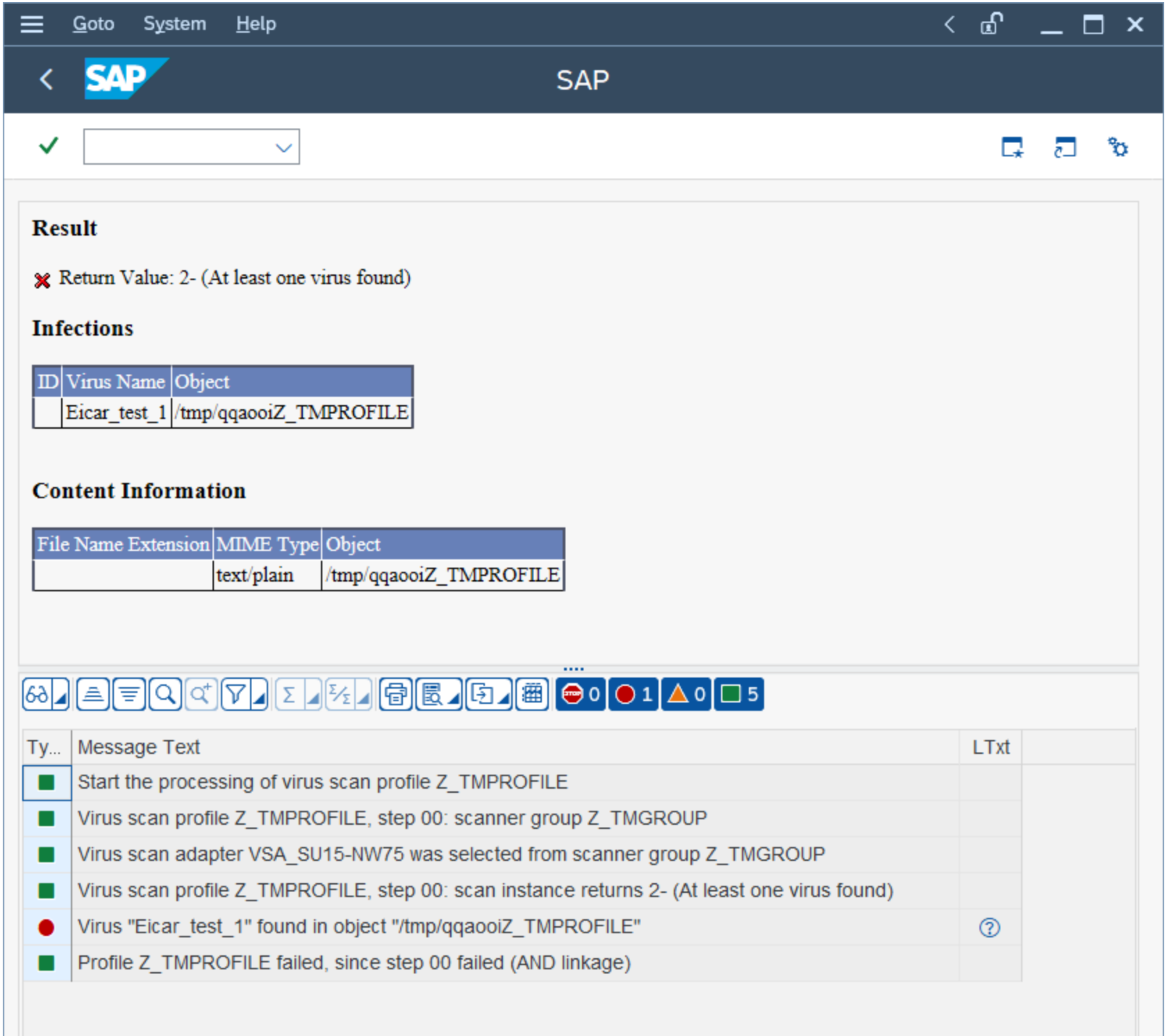
VSI対応の各SAPアプリケーションサーバには、設定ステップが正しく実行されたかどうかをチェックするテストも組み込まれています。そのため、特定のスキャンツールを呼び出すことのできるトランザクションにEICARテストウイルス(www.eicar.org) が追加されます。

2. 値を指定しない場合、前のステップで設定されたデフォルトプロファイルが呼び出されるため、何も設定しないでください。
3. 実行をクリックします。

   EICARテストウイルスについて説明する通知が表示されます。

4. 通知を確認します。

   トランザクションがインターセプトされました:


Goto System Help
SAP
SAP
Result
Return Value: 2- (At least one virus found)
Infections
ID Virus Name Object
Eicar_test_1 /tmp/qqaooiZ_TMPROFILE
Content Information
File Name Extension MIME Type Object
text/plain /tmp/qqaooiZ_TMPROFILE
0 1 0 5
Ty... Message Text LTxt
Start the processing of virus scan profile Z_TMPROFILE
Virus scan profile Z_TMPROFILE, step 00: scanner group Z_TMGROUP
Virus scan adapter VSA_SU15-NW75 was selected from scanner group Z_TMGROUP
Virus scan profile Z_TMPROFILE, step 00: scan instance returns 2- (At least one virus found)
Virus "Eicar_test_1" found in object "/tmp/qqaooiZ_TMPROFILE"
Profile Z_TMPROFILE failed, since step 00 failed (AND linkage)

[感染] には、検出された不正プログラムに関する情報が表示されます。

[Content Information] には、ファイルの正しいMIMEタイプが表示されます。

ファイルには、ランダムに生成された7文字のアルファベットにウイルススキャンプロファイル名を付加した名前が付けられます。

この後に、トランザクションの各ステップに関する出力が表示されます。

1. トランザクションが初期設定のウイルススキャンプロファイル (Z_TMPROFILE) を呼び出します。
2. ウイルススキャンプロファイルZ_TMPROFILEは、ウイルススキャングループZ_TMGROUPからアダプタを呼び出すように設定されています。
3. ウイルススキャングループZ_TMGROUPには複数のアダプタが設定されており、そのうちの1つが呼び出されます (この例ではVSA_NPLHOST)。
4. ウイルススキャンアダプタから、ウイルスが見つかったことを示す値「2-」が返されます。
5. 検出された不正プログラムに関する情報として、Eicar_test_1およびファイルオブジェクト/tmp/ zUeEbZZ_TMPROFILEが表示されます。
6. ステップ00 (ウイルススキャングループ) が失敗してファイルトランザクションの処理が停止されたため、呼び出された初期設定のウイルススキャンプロファイルZ_TMPROFILEが失敗します。

クロスチェックには、Deep Security Managerコンソールのこの「不正プログラム」イベントに関する情報もあります。このイベントを表示するには、**コンピュータエディタ**[1] を開き、[不正プログラム対策]→[イベント] を選択します。

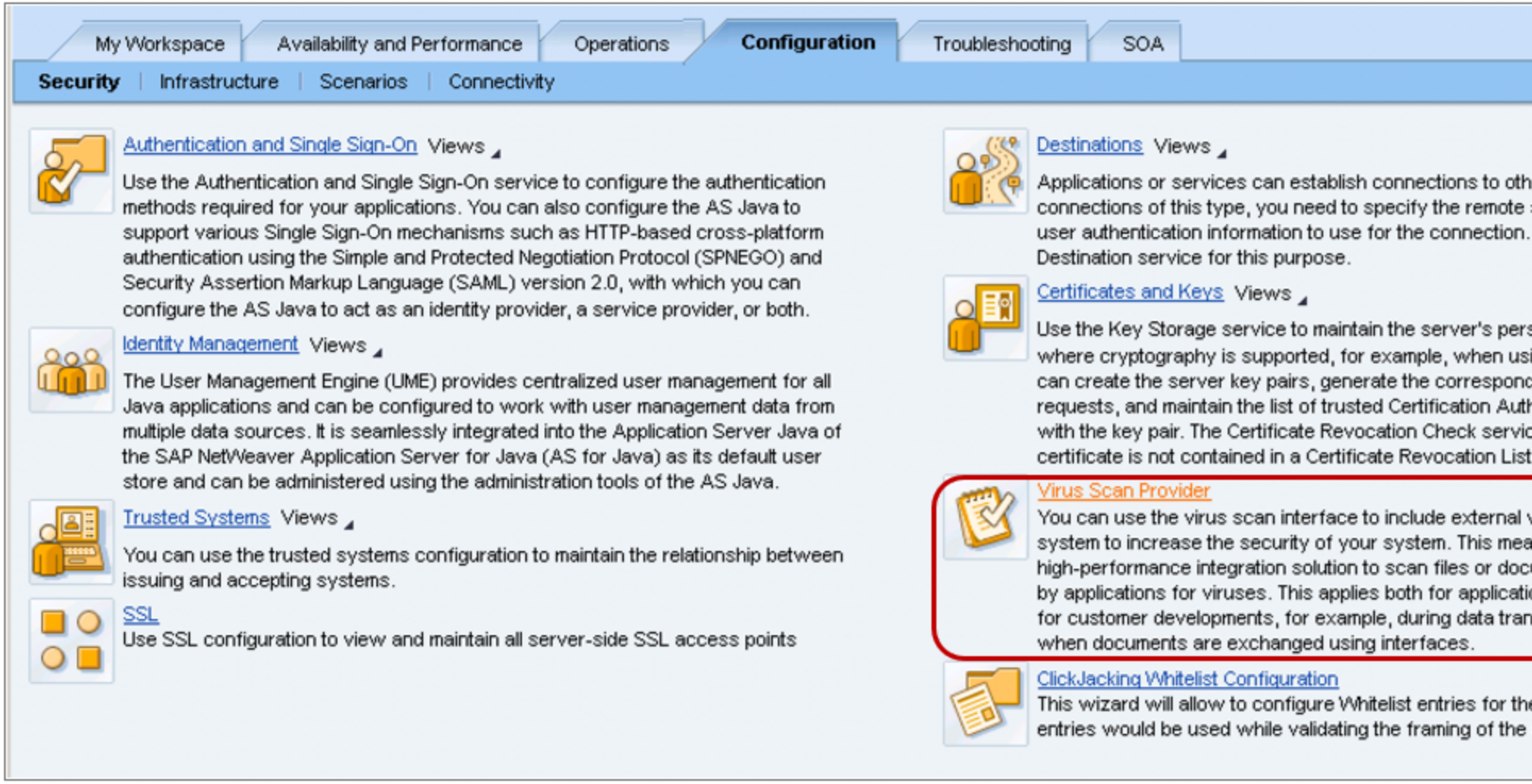
Java環境でトレンドマイクロスキャナーグループを構成する

スキャナーグループは、同じタイプの複数のウイルススキャナーを組み合わせます。後でウイルススキャンプロファイルを指定するために、グループが必要です。

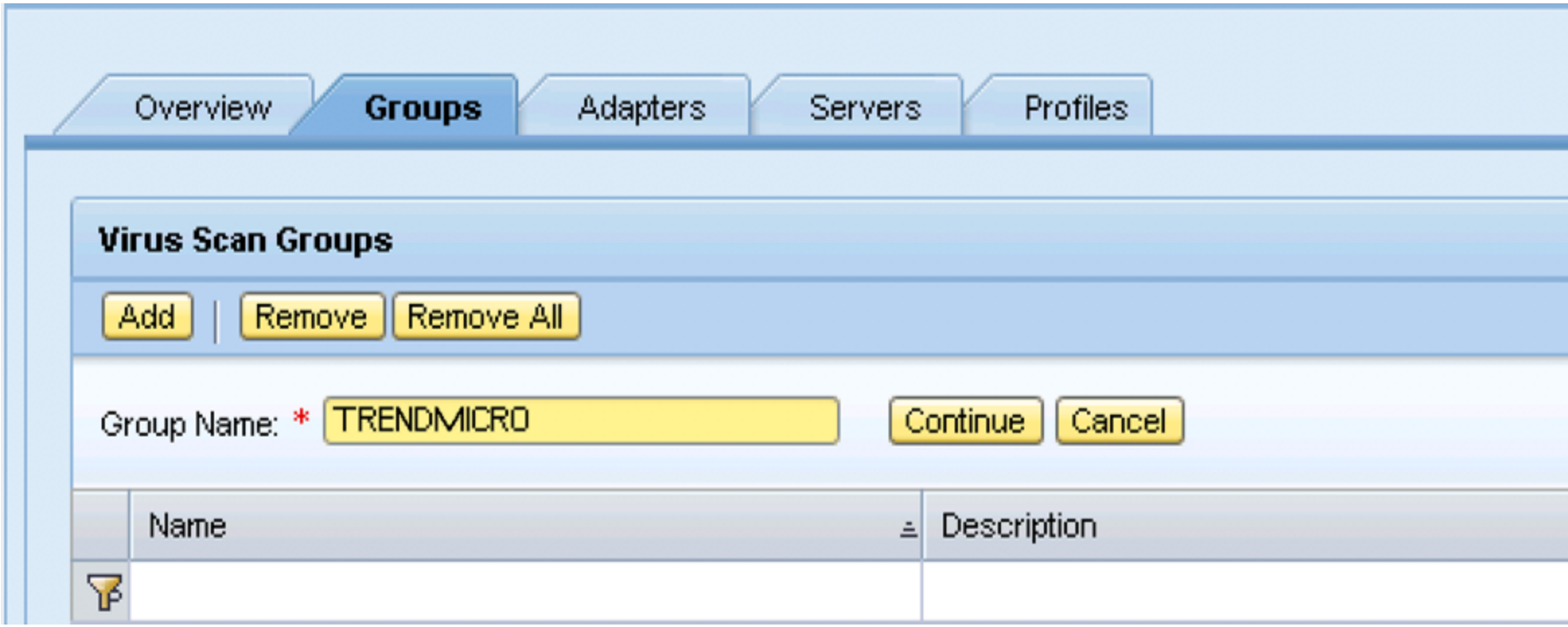
以下のようにして、Scannerグループを作成できます

[1] コンピュータエディタを開くには、[コンピュータ] 画面に移動し、編集するコンピュータをダブルクリック (または コンピュータを選択して [詳細] をクリック) します。

1. SAP NetWeaver管理者にログインしてください。
2. 構成タブを選択し、ウイルススキャンプロバイダーを選択します。



3. 変更モードで、グループタブで追加をクリックしてください。



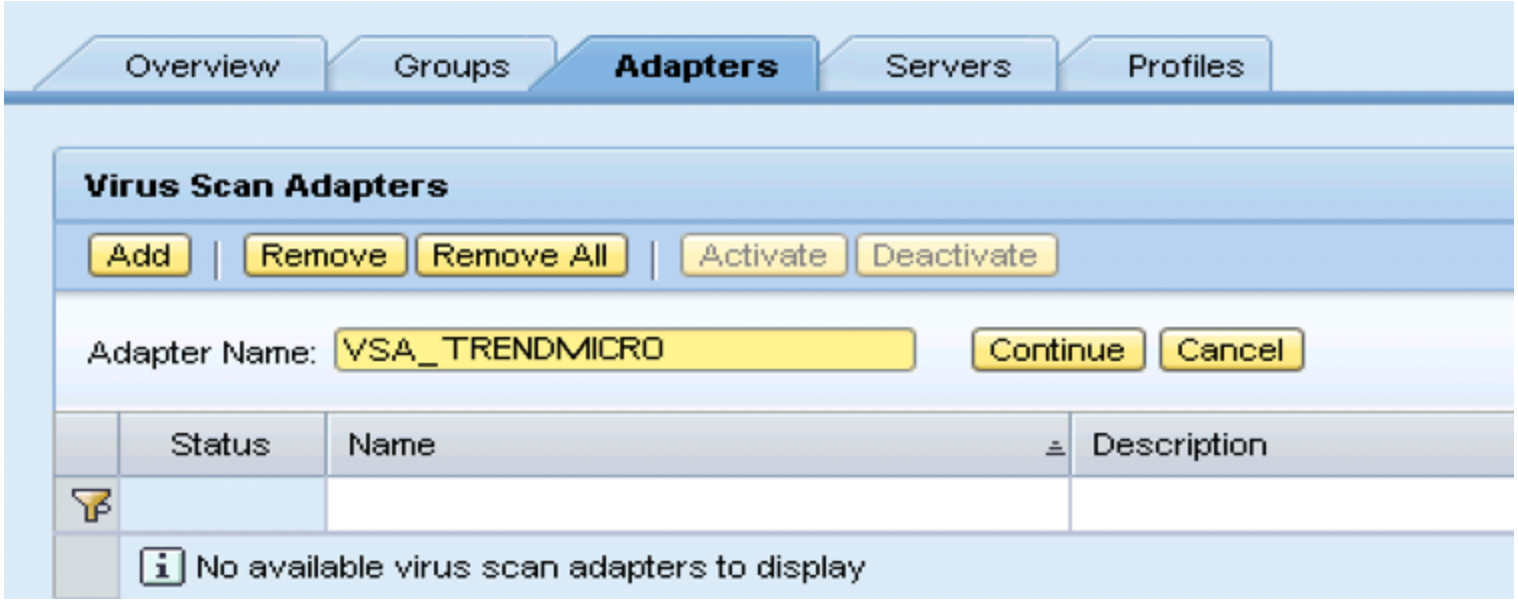
4. 設定タブで、Virus Scan Group Detailsの一部であるグループの説明フィールドにグループの説明を入力してください。
5. デフォルトスキャングループを選択して、このグループをデフォルトグループとして使用します。

Java環境でトレンドマイクロウイルススキャンプロバイダを設定する

次のようにウイルススキャンプロバイダを設定できます:

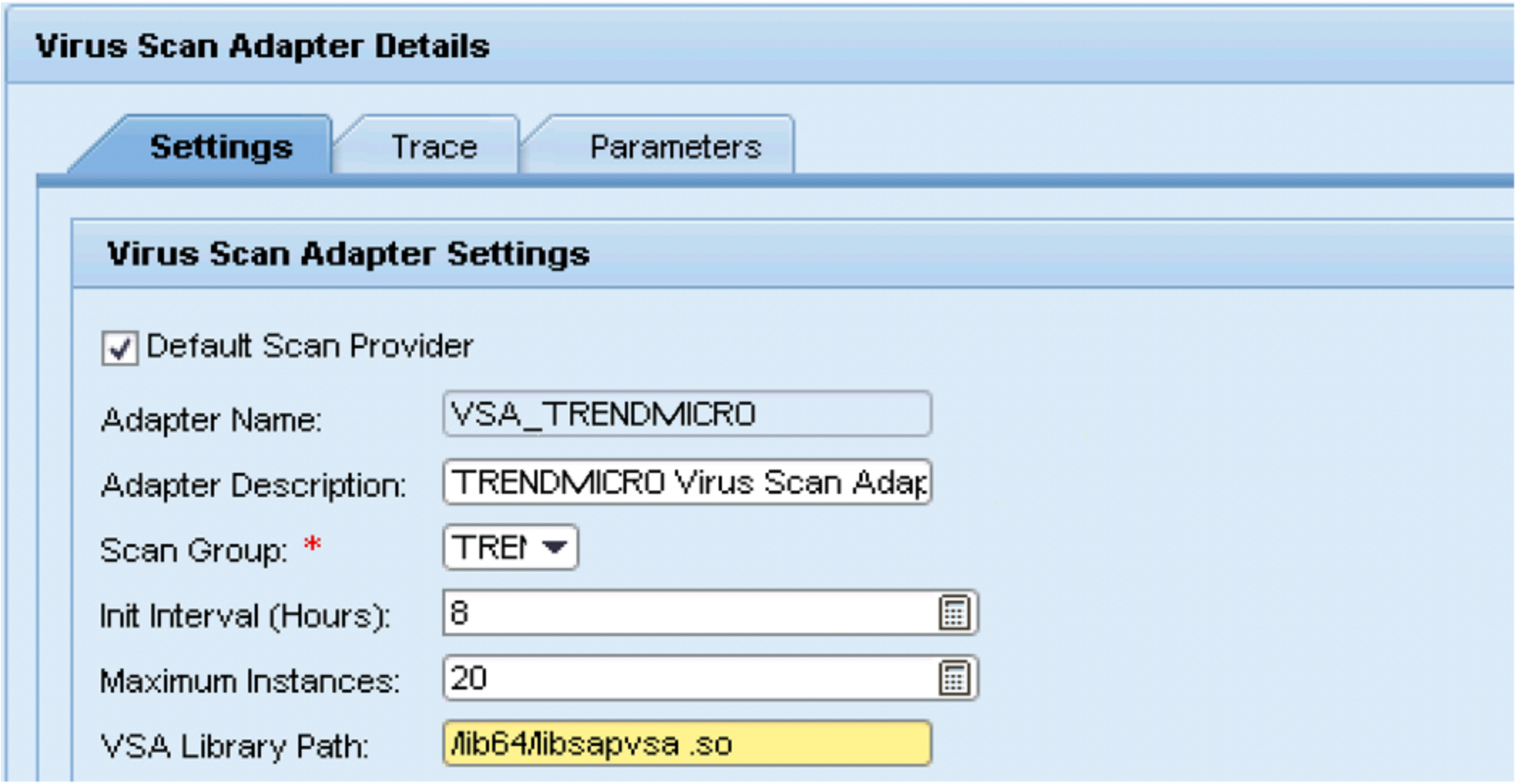
1. 変更モードで、アダプタータブで、追加をクリックして、ウイルススキャンプロバイダをウイルススキャンアダプタとして作成します。

2. アダプター名フィールドを使用して、事前定義された接頭辞の後に名前の残りを追加し、続行をクリックします。名前はVSA_で始まる必要があります。これにより、ウイルススキャンアダプターグループに新しい行が追加されます。



3. VSA共有ライブラリへのパスを指定してください /lib64/libsapvsa.so Linux systems C:\Program Files\Trend Micro\Deep Security Agent\lib\dsvsa.dll Windowsの場合。
4. スキャングループリストから選択してください。
5. Default Scan Providerを選択してください。

6. 設定を保存し、ウイルススキャンプロバイダーを有効にしてください。



Java環境でトレンドマイクロウイルススキャンプロファイルを設定する

アプリケーションは、データをウイルススキャンするためにウイルススキャンプロファイルを使用します。ウイルススキャンプロファイルには、ドキュメントをチェックするスキャナグループのリストが含まれています。また、ウイルススキャナの構成パラメータを割り当てるためにも、ウイルススキャ

ンプロファイルを使用できます。このウイルススキャンプロファイルでウイルスをスキャンする場合、ウイルススキャナはパラメータを受け取ります。

ウイルススキャンプロファイルは、スキャン中に処理される手順を指定します。ステップは、通常はScannerグループを使用して見つかるウイルススキャナーであるか、ウイルススキャンプロファイルを指定するステップである場合があります。このステップは、囲むウイルススキャンプロファイルの一部として実行されます。

ウイルススキャンはウイルススキャンプロファイルの名前で実行されます。システム管理者は、各コンポーネントのウイルススキャンを有効化または無効化するためにプロファイルを使用できます。

デフォルトでは、ウイルススキャンが統合された各SAPアプリケーションに対して、ウイルススキャンプロファイルが提供されます。

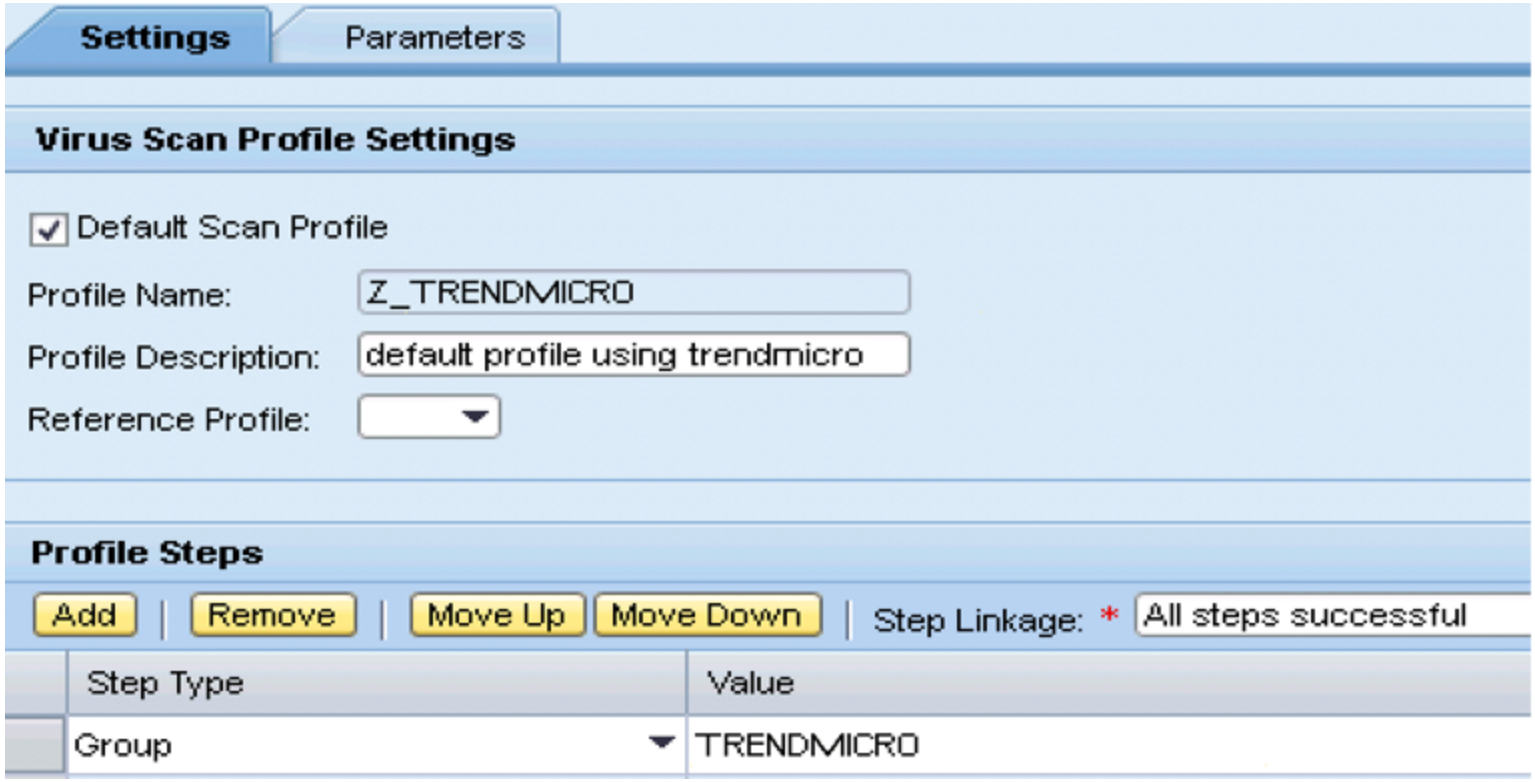
次のようにウイルススキャンプロファイルを構成できます:

1. プロファイルタブで、変更モードでウイルススキャンプロファイルを作成するには、追加をクリックしてください。
2. プロファイル名フィールドに、定義済みの接頭辞の後に名前の残りを入力し、続行をクリックします。これにより、ウイルススキャンプロファイルグループに新しい行が追加されます。
3. ウイルススキャンプロファイルの詳細で、設定タブを選択し、デフォルトスキャンプロファイルインジケータを設定して、編集するプロファイルを参照プロファイルとして選択します
   - デフォルトプロファイルを使用するには、参照プロファイルリストからデフォルトプロファイルを選択してください。
   - 参照プロファイルを使用するには、参照プロファイルリストから、新しいプロファイルにリンクする既存の参照プロファイルを選択します。ウイルススキャンプロファイルは他のウイルススキャンプロファイルを参照プロファイルとして使用できるため、同じウイルススキャンプロファイルを介して複数のアプリケーションを操作することができます。
4. 新しいプロファイルを定義するには、追加をクリックし、以下のフィールドを入力してください:

フィールド	説明
プロファイル名	新しいプロファイルの名前。
プロフィールの説明	新しいプロファイルの説明。

フィールド	説明
参照プロファイル	選択された場合、他のフィールドは非表示になります。
ステップ連動	このプロファイルの手順の連携: • すべてのステップが成功しました:ANDリンケージ。全体的な結果が成功するには、すべてのステップが成功する必要があります。 • 少なくとも1つのステップが成功:ORリンケージ。全体的な結果が成功するには、1つのステップだけが成功すればよい。
プロフィールの手順	このプロファイルの手順。

5. 次のように、プロファイル ステップ グループ内のプロファイル ステップを指定します
   - [追加] をクリックします。
   - グループまたは別のプロファイルとして使用するために、tep Typeリストから選択してください。
   - グループまたはプロファイルの値を指定してください。
   - [上へ移動]、[下へ移動]、および [削除] を使用して、[プロファイルステップ] リストを設定します。



6. プロファイルを有効にするには、エントリーを保存してから、ウイルススキャンプロファイルグループでプロファイルを選択し、有効化をクリックしてください。

以下のようにプロファイルパラメータを設定してください

1. 編集モードで、関連するプロファイルのパラメータタブを選択してください。
2. 追加をクリックして新しいエントリーを作成してください。
3. エントリを保存します。

以下の表はプロファイル構成パラメータを一覧表示します

パラメータ	種類	説明
CUST_ACTIVE_CONTENT	BOOL	ファイルにJavaScript、PHP、またはASPスクリプトなどのスクリプトが含まれているかどうかをチェックし、それをブロックします。
CUST_CHECK_MIME_TYPE	BOOL	ファイル拡張子名がそのMIMEタイプと一致するかどうかを確認します。一致しない場合、ファイルはブロックされます。 すべてのMIMEタイプと拡張子名は正確に一致させることができます。例えば: • Microsoft Wordファイルは .doc または .dot • JPEGファイルは .jpg • テキストファイルおよびバイナリファイルは、他の既知のファイルの拡張子でない限り、任意の拡張子を持つことができます。つまり、.txt または .bin, ただし .doc または .jpg 「サポートされているMIMEタイプ」を参照してください。

次の表は、ステップ構成パラメータを一覧表示しています

パラメータ	種類	説明	Linux のデフォルト	Windows のデフォルト
SCANBESTEFFORT	BOOL	スキャンをベストエフォートベースで実行します。つまり、VSAにオブジェクトの検索を許可するセキュリティ上重要なフラグ(SCANALLFILESやSCANEXTRACTなど) をすべて有効化するだけでなく、内部フラグも有効にします。可能なフラグに関する詳細は認証情報に保存されています。	1	1
SCANALLFILES	BOOL	ファイル拡張子に関係なくすべてのファイルをスキャンします。	1	1
SCANLIMIT	INT	解凍されてスキャンされるファイルの最大数を指定し	INT_MAX	65535

パラメータ	種類	説明	Linux のデフォルト	Windows のデフォルト
		ます。圧縮ファイルのみに適用されます。		
SCANEXTRACT	BOOL	アーカイブまたは圧縮オブジェクトを解凍します。	有効	有効
SCANEXTRACT_SIZE	SIZE_T	最大解凍サイズです。	0x7FFFFFFF	62914560 (60 MB)
SCANEXTRACT_ DEPTH	INT	オブジェクトが解凍される最大の深さ(階層) です。	20	20
SCANLOGPATH	CHAR	VSAのカスタムログパス。	(未設定)	(未設定)

Java環境でウイルススキャンインターフェースをテストする

1. テストアプリケーションを起動してください /vscantest パス。
2. 提供されたテストデータまたはあなた自身のローカルファイルを使用して、チェックするオブジェクトを指定してください。
3. ウイルススキャンプロファイル、スキャナーグループ、またはウイルススキャンプロバイダーを選択してテストしてください。
4. 次のオプションのいずれかを選択します。
   - チェックのみ - 指定されたウイルス対策製品がデータをスキャンし、結果を表示します。
   - チェックしてクリーンアップ - スキャンして結果を表示するだけでなく、指定されたアンチウイルス製品は、ウイルス感染が診断された場合にデータをクリーンアップしようとします。
5. テストを開始するにはアクションを実行をクリックしてください。

サポートされているMIMEタイプ

Deep Security Scannerでサポートされ るMIMEタイプは、使用しているDeep Security Agentのバージョンによって異なります:

- Deep Security Agent 9.6ではVSAPI 9.85を使用
- Deep Security Agent 10.0ではATSE 9.861を使用
- Deep Security Agent 10.1ではATSE 9.862を使用
- Deep Security Agent 10.2、10.3、11.0、11.1、および11.2ではATSE 10.000を使用
- Deep Security Agent 11.3以降ではATSE 11.0.000を使用

MIMEタイプ	説明	拡張子	agent 9.6でサポート	agent 10.0でサポート	agent 10.1以降でサポート
application/octet-stream		*	○	○	○
application/com	COMファイル	com	○	○	○
application/ecmascript	EMCScriptファイル	es	○	○	○
application/hta	HTAファイル	hta	○	○	○
application/java-archive	Java Archive (JAR) ファイル	ear, jar, rar, sar, war, zip	○	○	○
application/javascript	JavaScriptファイル	js、jsxinc、jsx、ztl	○	○	○
application/msword	Word for Windows	doc、dot	○	○	○
application/vnd.ms-access	MS Access	mdb	×	×	×
application/vnd.ms-project	MS Project	mpp	×	×	×
application/octet-stream	COMファイル	com	○	○	○
application/octet-stream	EXEファイル	exe	○	○	○
application/pdf	Adobe Portable Document Formatファイル	pdf	○	○	○
application/postscript	Postscript	ai, ps	○	○	○
application/rar	RARファイル	rar	○	○	○
application/rtf	Microsoft RTF	rtf	○	○	○
application/sar	Sarファイル	sar	○	○	○
application/vnd.ms-excel	Excel for Windows	xls、xlt、xla	○	○	○
application/vnd.ms-outlook	Outlook for Windows	msg	×	○	○
application/vnd.ms-powerpoint	Windows PowerPoint	ppt、pot、pps、ppa	○	○	○
application/vnd.ms-publisher	MS Publisher	pub	×	×	○
application/vnd.oasis.opendocument	Open Document	odf	○	○	○

MIMEタイプ	説明	拡張子	agent 9.6でサポート	agent 10.0でサポート	agent 10.1以降でサポート
application/vnd.openxmlformats-officedocument.presentationml.presentation	MS Officeファイル	pptx、potx、ppsx、ppam、pptm、potm、ppsm	○	○	○
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	MS Officeファイル	xlsx、xltx、xlsm、xltm、xlam、xlsb	○	○	○
application/vnd.openxmlformats-officedocument.wordprocessingml.document	MS Officeファイル	docx、dotx、docm、dotm	○	○	○
application/vnd.rn-realmedia	Real Media	rm	○	○	○
application/wordperfect	WOrdPerfect	wp、wp5、wp6、wpd、w60、w61	○	○	○
application/x-alf		alf	○	○	○
application/x-arc-compressed	ARCファイル	arc	○	○	○
application/x-bzip2	bZIPファイル	*	○	○	○
application/x-cpio	CPIOファイル	*	○	○	○
application/x-director	Macromedia Director Shockwave Movie	dcr	○	○	○
application/x-gzip	Gzip	*	○	○	○
application/xhtml+xml	XHTML	dhtm、dhtml、htm、html、htx、sht、shtm、shtml、stml、xht、xhtm、xhtml、xml、txt	○	○	○
application/x-java-class	JAVAアプレット	class	○	○	○
application/x-kep		kep	○	○	○
application/x-otf		otf	○	○	○
application/x-sapshortcut		sap、sapc	○	○	○
application/x-shockwave-flash	Macromedia Flash	swf	○	○	○
application/x-silverlight-app	PKZIP	xap	○	○	○
application/x-sim		sim	○	○	○
application/x-tar	TARファイル	tar	○	○	○
application/x-vbs		*	○	○	○
application/zip	ZIPファイル	zip、zipx	○	○	○
audio/basic	Audio	snd、au	○	○	○
audio/midi	MIDI	mid、midi、rmi、mdi、kar	○	○	○
audio/x-aiff	Apple/SGIのAudio InterChangeファイル形式	aiff、aif、aifc	○	○	○

MIMEタイプ	説明	拡張子	agent 9.6でサポート	agent 10.0でサポート	agent 10.1以降でサポート
audio/x-mpeg-3	MP3	mp3	○	○	○
audio/x-realaudio	Real Audio	ra	○	○	○
audio/x-voc	Creative Voice Format(VOC)	voc	○	○	○
image/bmp	Windows BMP	bmp	○	○	○
image/gif	GIF	gif	○	○	○
image/ico	Windowsアイコン	ico	○	○	○
image/jpeg	JPEG	jpg、jpeg、jpe、jif、jfif、jfi	○	○	○
image/msp	Microsoft Paint	msp	○	○	○
image/png	Portable Network Graphics	png	○	○	○
image/ppm	PPM画像	ppm	○	○	○
image/svg+xml		svg	○	○	○
image/tiff	TIFF	tif、tiff	○	○	○
image/vnd.ms-modi	Microsoft Document Imaging	mdi	○	○	○
image/x-cpt	Corel PhotoPaint	cpt	○	○	○
image/x-pcx	PCX	pcx	○	○	○
image/x-pict	Macintosh Bitmap	pct	○	○	○
image/x-ras	Sun Raster(RAS)	ras	○	○	○
image/x-wmf	Windowsメタファイル	wmf	○	○	○
image/vnd.dwg	DWGファイル	dwg	いいえ	いいえ	○
text/csv	CSV	csv、txt	○	○	○
text/html	HTML	dhtm、dhtml、htm、html、htx、sht、shtm、shtml、stml、xht、xhtm、xhtml、xml、txt	○	○	○
text/plain		*	○	○	○
text/plain	テキストファイル	msg、txt	○	○	○
text/xml	XML	dhtm、dhtml、htm、html、htx、sht、shtm、shtml、stml、xht、xhtm、xhtml、xml、txt	○	○	○
text/xsl	XSL	xsl	○	○	○
unknown/unknown		*	○	○	○
video/mpeg		*	○	○	○
video/quicktime	Quick Time Media	m4a, m4b, m4p, m4r, m4v, mov, movie,	○	○	○

MIMEタイプ	説明	拡張子	agent 9.6でサポート	agent 10.0でサポート	agent 10.1以降でサポート
		mp4, heic, heics, heif, heifs, qt			
video/x-fli	AutoDesk Animator	fli	○	○	○
video/x-flv	Macromedia Flash FLV Video	flv	○	○	○
video/x-ms-asf	Advanced Streaming Format	asf, wma, wmv	○	○	○
video/x-scm	Lotus ScreenCam Movie	scm	○	○	○
font/ttf	TrueType フォント	dfont, otc, otf, ttc, tte, ttf	いいえ	いいえ	○
text/x-msdos-batch	バッチファイルは、DOS、OS/2、Microsoft Windowsで使用されるスクリプトファイルです	bat, cmd, btm, txt	いいえ	いいえ	いいえ

Trend Vision Oneと統合する

Trend Vision One (XDR) と統合する

XDR in Trend Vision One は、複数のベクター(メール、エンドポイント、サーバー、クラウドワークロード、ネットワーク) から収集されたデータを使用して、専門的な分析とグローバルな脅威インテリジェンスを適用します。

注意: 個人を特定できる情報はTrend Vision Oneによって収集されます。詳細については、Trend Micro XDRデータ収集通知をご覧ください。

Trend Vision One を Deep Security と統合するには、ライセンスを購入する必要があります。詳細については、"Trend Vision One (XDR) に登録" on the next page を参照してください。

Trend Vision One (XDR) に登録すると、保護モジュールのセキュリティイベントがデフォルトで Trend Vision One に転送されます。アクティビティデータを Trend Vision One に転送するには、関連するデプロイスクリプトまたはTrend Vision One コンソールからダウンロードしたインストーラーを使用して Trend Micro Endpoint Basecamp をインストールする必要があります。

Trend Vision One (XDR) に登録

1. 組織の管理者からTrend Vision One登録トークンを取得してください。管理者はDeep Security Softwareの設定に記載されている指示に従ってトークンを取得する必要があります。

   注意: トークンは生成後24時間のみ有効です。期限が切れた場合は、同じ手順で新しいトークンを生成してください。

2. Deep Security Managerで、[管理]→[システム設定]→[Trend Vision One] に進みます。
3. [登録トークンを登録]をクリックします。
4. 組織の管理者から受け取った登録トークンを貼り付けるために開くダイアログを使用し、次に 登録 をクリックします。

登録が完了すると、Deep Securityはデータを分析のために自動的にTrend Vision Oneプラットフォームに転送します。

プロキシサーバを介してTrend Vision One (XDR) に登録するには、管理 > システム設定 > プロキシ > プロキシサーバの使用 > Deep Security Manager (トレンドマイクロサービスへの接続)に移動し、正しいプロキシ設定を選択してください。

セキュリティイベントをTrend Vision One (XDR)に転送

Trend Vision One (XDR) に正常に登録すると、セキュリティイベントをTrend Vision One に転送する設定がデフォルトで有効になります。この設定が有効になると、以下の保護モジュールからのイベントがTrend Vision One に転送されます:

- 不正プログラム対策
- Webレピュテーション
- デバイスコントロール
- 変更監視とアプリケーションコントロール
- セキュリティログ監視
- 侵入防御

セキュリティイベントの転送をTrend Vision Oneに停止するには、管理 > システム設定 > Trend Vision Oneに移動し、セキュリティイベントをTrend Vision Oneに転送オプションの選択を解除します。

エージェントとリレーをプロキシ経由でプライマリセキュリティ更新ソースに接続している場合、同じプロキシ設定が自動的に使用されます。

アクティビティデータをTrend Vision One (XDR)に転送

アクティビティデータをTrend Vision Oneに転送するには、関連するデプロイスクリプトまたはTrend Vision Oneコンソールからダウンロードしたインストーラーを使用してTrend Micro Endpoint Basecampをインストールします。

デプロイメントスクリプトは、RightScale、Chef、Puppet、またはSSHなどのツールを使用して管理者としてデプロイできます。デプロイメントスクリプトを生成する前に、XDRセンサーシステム要件でシステム要件とサポートされているオペレーティングシステムを確認し、スクリプトで実行される前提条件の確認に注意してください。

インストールスクリプトを生成する

1. 開始する前に、Deep Security Managerが Trend Vision One に接続されていることを確認してください。
2. [管理]→[システム設定]→[Trend Vision One] に進みます。
3. アクティビティデータ転送で、プラットフォームを選択します。展開スクリプトジェネレータには、関連するスクリプトが表示されます。
4. [クリップボードにコピー] をクリックして、使用する配信ツールにインストールスクリプトを貼り付けるか、[ファイルに保存] をクリックします。

   Deep Security Manager for Windowsによって生成された配信スクリプトには、Windows PowerShell 4.0以上が必要です。PowerShellを管理者として実行する必要があります。スクリプトが実行されていない場合は、次のコマンドを入力します。
   `Set-ExecutionPolicy RemoteSigned`
   PowerShell 4.0またはcurl 7.34.0を含まないWindowsまたはLinuxにエージェントを配信する必要がある場合は、次の手順を実行します。
   - Linux: `--tls1.2` タグを削除します。
   - Windows: `[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;` 行を削除します。

   上記の行を削除すると、以前のバージョンのTLS(バージョン1.0) がマネージャと通信できるようになります。以前のTLSもマネージャと

リレーでも許可されていることを確認してください。詳細については、"TLS 1.2が強制されているかどうかを確認する" on page 1895および"初期のTLS (1.0) を有効にする" on page 1893を参照してください。

5. プロキシが必要な場合は、スクリプトを変更してプロキシサーバアドレスを追加します。

Trend Micro Endpoint Basecamp をインストールしたら、Trend Vision One Endpoint Inventory でセンサーを有効にします。

注意: Endpoint Basecamp ではプロキシアカウント情報がサポートされていません。

エージェントインストーラーをダウンロードする

エージェントインストーラーをダウンロードするには、Trend Vision One > エンドポイントインベントリに移動し、エージェントの前提条件の確認手順に従ってください。

Trend Vision One Service Gatewayとの統合

サポートされているService Gatewayのバージョン

Deep SecurityはService Gatewayバージョン1.0、2.0、および3.0をサポートしています

システム要件

Service Gatewayのシステム要件については、Service Gatewayアプライアンスのシステム要件を参照してください。

Service Gatewayを使用するWindowsおよびLinuxでは、Deep Security Agentバージョン20.0.1-690以降を使用することをお勧めします。

Service Gatewayの配信

ネットワークにService Gatewayを展開する方法については、Service Gatewayの展開とファイアウォール例外の設定を参照してください。

Service Gatewayフォワードプロキシを統合する

Service Gatewayでフォワードプロキシを有効にし、Deep Securityに適用できます。その後、Deep Securityはフォワードプロキシの設定をDeep Security Agentに展開します。

エージェントが設定を受信すると、フォワードプロキシを介して各サービスサーバ(例えば、Smart Protection Service)に接続します。サーバに接続できない場合、エージェントはエージェントのポリシーで設定された代替プロキシを試みます。

フォワードプロキシはTrend Vision Oneから有効にする必要があります。手順については、Service Gatewayでのサービスの管理を参照してください。

Deep SecurityがTrend Vision Oneと統合されると、フォワードプロキシ情報はDeep Securityコンソールの管理 > システム設定 > プロキシ > プロキシサーバーに表示されます。

プロキシの設定がDeep Securityに同期された後、エージェントは次回のポリシーチェック時に設定を受け取ります。

Service Gateway ActiveUpdate Serviceを統合する

Service GatewayでActiveUpdateを有効にして、Deep Securityの更新ソースとして機能させることができます。

ActiveUpdateサービスを有効にする

ActiveUpdate ServiceはDeep Securityと統合する前にTrend Vision Oneで有効にする必要があります。詳細については、Service Gatewayでのサービス管理を参照してください。

Deep Security ActiveUpdateソースURLを取得

ActiveUpdateのソースURLは、Deep Securityコンソールの管理 > システム設定 > 更新 > セキュリティ更新 > プライマリセキュリティ更新ソース > トレンドマイクロ更新サーバから取得します。

ActiveUpdate Serviceを構成する

Trend Vision OneでActiveUpdate Serviceを設定する方法については、ActiveUpdateの設定を参照してください。

ActiveUpdate Serviceを構成する

Deep Securityの更新ソース設定を構成するには、エージェント設定を適用し、このTrend Vision Oneから新しいActiveUpdateコンポーネントを取得します。

1. Deep Securityコンソールで、管理 > システム設定 > アップデートに移動します。
2. 他の更新ソースを選択し、ActiveUpdate Serviceを設定する際に生成してコピーしたActiveUpdate URLを貼り付けてください。
3. 保存をクリックしてください。

Service Gateway Smart Protectionサービスを統合する

Service GatewayでSmart Protection Servicesを有効にして、Deep Securityのローカルsmart Protection Serverにすることができます。

Smart Protectionサービスを有効にする

Smart Protectionサービスは Trend Vision Oneから有効にする必要があります。手順については、Service Gatewayでのサービス管理を参照してください。

Deep Securityポリシーでローカルファイルレピュテーションサービスを構成する

1. Deep Securityコンソールで、ポリシー > 詳細 > 不正プログラム対策 > 一般タブに移動し、不正プログラム対策の状態がオンに設定されていることを確認してください。
2. Smart Protectionタブで、スマートスキャンがオンに設定されていることを確認してください。
3. Smart Protect server to File Reputation Serviceで、ローカルにインストールされたSmart Protection Serverを使用を選択します。
4. ファイルレピュテーションサーバURLの値を入力し、Service Gatewayページからコピーして、追加をクリックしてください。
5. 保存をクリックしてください。

Deep SecurityポリシーでローカルWebレピュテーションサービスを構成する

1. Deep Securityコンソールで、ポリシー > 詳細 > Webレピュテーション > 一般タブに移動し、Webレピュテーション状態がオンに設定されていることを確認してください。
2. Smart ProtectサーバからWebレピュテーションサービスで、ローカルにインストールされたSmart Protection Serverを使用を選択します。
3. Webレピュテーションサーバ URLの値を入力してください。この値はService Gatewayページからコピーできます。その後、追加をクリックしてください。
4. 保存をクリックしてください。

よくある質問

保護をオンにするとWindowsマシンのネットワーク接続が失われる理由

Deep Security Agentがネットワークドライバをインストールしてトラフィックを調査している間は、ネットワークドライバのインストール中にWindowsコンピュータの接続が短時間停止することがあります。この状況は、次のいずれかを含むポリシーを初めて適用する場合にのみ発生します。

- Webレピュテーション
- ファイアウォール
- 侵入防御

Windowsマシンでは、上記3つの保護モジュールすべてに同じドライバを使用します。Webレピュテーション、ファイアウォールまたは侵入防御のいずれかがすでにオンの状態であれば、これらの機能の1つをオンにしても、ネットワークの切断は発生しません。Agentのアップグレード時にも、同様にネットワーク接続が一時的に途切れることがあります(ドライバもアップグレードする必要があるため)。

Deep Securityに関するニュースの取得方法

Deep Securityのニュースフィードは廃止されました。代わりに、"新機能" on page 134 の記事。

トレンドマイクロでは、毎週火曜日に新しいルールのアップデートをリリースし、新しい脅威が検出された場合には更なるアップデートを行います。各ルールのアップデートに関する詳細は、トレンドマイクロのThreat Encyclopediaに記載されています。

Solarisゾーンでのエージェント保護はどのように機能しますか?

Deep Security Agentは、Solarisグローバルゾーンにのみインストールできます。お使いのSolaris環境で非グローバルゾーンを使用している場合、グローバルゾーンと非グローバルゾーンに対してAgentが提供可能な保護は、各保護モジュールによって異なります。

- 侵入防御
- ファイアウォール
- Webレピュテーション
- 不正プログラム対策
- 変更監視
- セキュリティログ監視

Deep Security AgentのSolarisへのインストールについては、"エージェントを手動でインストールする" on page 537)を参照してください。

侵入防御 (IPS)、ファイアウォール、およびWebレピュテーション

お使いのSolaris環境で非グローバルゾーンを使用している場合、侵入防御、ファイアウォール、およびWebレピュテーションのモジュールによって保護できるのは、グローバルゾーン、非グローバルゾーン、および外部IPアドレスの間でやり取りされる特定のトラフィックフローのみです。Agentが保護できるトラフィックフローは、非グローバルゾーンで共有IPネットワークインタフェースと専用IPネットワークインタフェースのどちらを使用しているかで決まります。

カーネルゾーンでは専用IPネットワークインタフェースが使用され、トラフィックフローに対するAgentの保護はそのネットワーク設定に制限されます。

共有IPネットワークインタフェースを使用する非グローバルゾーン

共有IPの設定でAgentの保護対象となるトラフィックフローは次のとおりです。

トラフィックフロー	Agentによる保護
外部アドレス <-> 非グローバルゾーン	○
外部アドレス <-> グローバルゾーン	○
グローバルゾーン <-> 非グローバルゾーン	×
非グローバルゾーン <-> 非グローバルゾーン	×

専用IPネットワークインタフェースを使用する非グローバルゾーン

専用IPの設定でAgentの保護対象となるトラフィックフローは次のとおりです。

トラフィックフロー	Agentによる保護
外部アドレス <-> 非グローバルゾーン	×
外部アドレス <-> グローバルゾーン	○
グローバルゾーン <-> 非グローバルゾーン	○
非グローバルゾーン <-> 非グローバルゾーン	×

不正プログラム対策、変更監視、およびセキュリティログ監視

不正プログラム対策、変更監視、およびセキュリティログ監視モジュールは、グローバルゾーンを保護します。非グローバルゾーンについては、グローバルゾーンでも参照可能なファイルまたはディレクトリは保護されます。非グローバルゾーン固有のファイルは保護されません。

AWS GovCloud(US) インスタンスを保護するにはどうすればよいですか?

Deep SecurityがAWS GovCloud(US) のサポートを提供するには、次の2つの方法があります。

- AWS GovCloud(US) のAWS Marketplaceから入手できるTrend Micro Deep Security AMI(Per Protected Instance HourまたはBYOLライセンスの種類) を使用できます。AWS GovCloud (米国) リージョンのインストール手順は、その他のリージョンと同じです。「Deep Security AMI from AWS Marketplaceの使用開始」を参照してください。
- Deep Securityソフトウェアのエンタープライズ版は、AWS GovCloud(US) 地域で実行されているAWSインスタンスにインストールできます。

AWS GovCloud(US) のAWSインスタンスの管理者によるインスタンスの保護

警告: Deep Security ManagerがAWS GovCloudの外部にある場合、Deep Security Managerを使用してAWS GovCloudのコンピュータを管理すると、ITARのコンプライアンスが損なわれる可能性があることに注意してください。

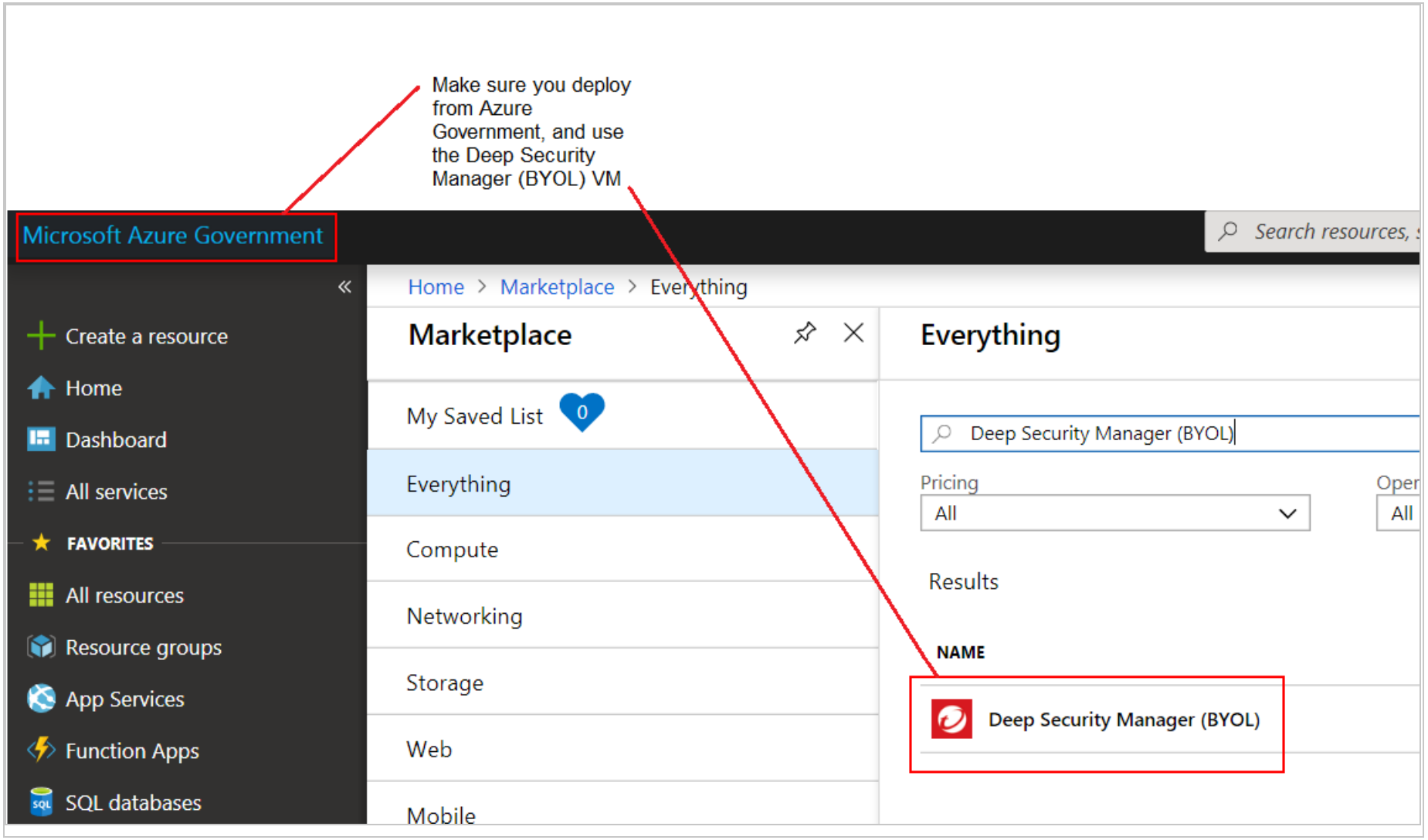
Deep Security Managerが商用AWSインスタンスにあり、このインスタンスを使用してAWS GovCloudインスタンスを保護する場合は、Deep Security Managerコンソールにあるクラウドコネクタを使用してインスタンスを追加することはできません。Deep Security Managerが(AWS GovCloud), などの) 特定の地域で実行されている場合、その地域に接続したり、商用AWS地域のインスタンスに接続したりできます。ただし、Deep Security Managerが商業地域にある場合、AWS GovCloudなどの特別な地域ではなく、すべての商用AWS地域に接続できます。

あなたは、商業AWSで実行されているのDeep Security Managerに(AWS GovCloudのような) 特殊な領域コネクタを追加したい場合は、そうしていることのDeep Security Managerを伝えるためにseedRegion引数を供給するためのDeep Securityレガシー—REST APIを使用する必要があります商用AWSの外部に接続しています。APIの詳細については、"Deep Security APIを使用したタスクの自動化" on page 1824を参照してください。

Azure Governmentのインスタンスを保護するにはどうすればいいですか?

Azure Governmentのインスタンスを保護するには、次のオプションがあります。

- Deep Security Managerは、Azure Governmentのマーケットプレイスにリストされているの Deep Security Manager(BYOL) VMを使用して配信できます(下の画像を参照) 。Azure Governmentの配置手順は他の地域と同じです。
- Deep Security Managerのオンプレミスソフトウェアは、Azure Government内で実行されるAzure VMにインストールできます。


Make sure you deploy from Azure Government, and use the Deep Security Manager (BYOL) VM
Microsoft Azure Government
Search resources,
Home > Marketplace > Everything
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function Apps
SQL databases
Marketplace
My Saved List
0
Everything
Compute
Networking
Storage
Web
Mobile
Everything
Deep Security Manager (BYOL)
Pricing
All
Oper
All
Results
NAME
Deep Security Manager (BYOL)

グローバルAzureのマネージャを使用してAzure Governmentのインスタンスを保護する

警告: Deep Security ManagerがAzure Governmentの外部にある場合、ManagerでAzure Government内のコンピュータを管理すると、ITARコンプライアンスに違反することになるので注意してください。

Deep Security ManagerコンソールでComputers>Add>Add Accountオプションを使用してAzure Governmentのインスタンスをグローバル Azureのマネージャに追加することはできません。また、その逆もできません。これは、管理者が独自のクラウド内のAzureインスタンスとのみ通信できるためです。

Deep Security ManagerがAzure Governmentクラウドの外部にあり、Azure Governmentクラウド内のインスタンスを保護するためにDeep Security Managerを使用する場合は、Deep SecurityレガシREST APIを使用して `azureADLoginEndPoint` および `azureEntryPoint` 引数を指定する必要があります。APIの使用の詳細については、クラウドアカウントの作成を参照してください。

Deep Security AgentはAmazonインスタンスメタデータサービスをどのように使用しますか

AWSのEC2インスタンスで実行している場合、Deep Security AgentはAmazonインスタンスメタデータサービス(IMDS) を使用してEC2インスタンスに関する情報をクエリします。

注意: IMDS v2のDeep Securityのサポートは、Deep Security Manager FR 2020-04-29およびDeep Security Agent FR 2020-05-19で追加されました。以前のバージョンのDeep Securityを使用している場合は、IMDS v1のみがサポートされているため、IMDS v1を使用してDeep Security Agentがメタデータをホストするためのの設定を行う必要があります。

Deep Security Agentによって取得された情報は、適切なAWSの下でエージェントが作動をDeep Securityのために使用されていることを確認する必要があります。

Deep Security Agentがメタデータサービスバージョン1(IMDSv1) または2(IMDSv2),) を使用してインスタンスからデータを正常に取得できない場合は、次の問題が発生することがあります。

問題	根本原因	解決方法	その他の注意事項
重複したコンピュータが表示されます.1つはAWSアカウントの下、もう1つはAWSアカウントの外部に表示されます。	Deep Security AgentがInstance Metadata Service Version 1(IMDSv1) または2(IMDSv2), Deep Securityは、このアクティベーションを目的のクラウドアカウントに適切に関連付けることができません。	Deep SecurityがIMDS v1またはIMDS v2にアクセスできることを確認してください。	あなたが重複したコンピュータの作成が発生したと判断した場合は、自動的にこれらのコンピュータを削除するには非アクティブなエージェントのクリーンアップを使用することができます。
スマートフォルダまたはAWSメタデータに基づくイベントベースのタスクが失敗します。	Deep Security Agentがインスタンスメタデータサービスバージョン1(IMDSv1) または2 (IMDSv2), Deep Securityはこれらの操作に必要なAWSメタデータにアクセスできません) へのアクセス権を持っていない場合。	詳細については、インスタンスメタデータサービスの設定を参照してください。	N/A

AWS Elastic Beanstalk環境でオフライン環境に対するハートビートアラートを最小限に抑える方法

AWS Elastic Beanstalkを使用すると、複数の環境を作成して異なるバージョンのアプリケーションを同時に実行することができます。複数の環境には一般に実稼働環境と開発環境が含まれ、多くの場合、夜間は開発環境の電源が停止されます。翌日になって開発環境をオンラインに戻すと、オフラインだった時間帯について、Deep Securityから通信の問題に関するアラートが生成されます。これらのアラートは実際には不要なものですが、Deep Securityでは指定の数のハートビートが失われると常にアラートを生成するため誤検出というわけではありません。

これらのハートビート関連のアラートを最小限に抑え、毎日同じ時間帯にオフラインになることがわかっている環境についてアラートが生成されないようにするには、ハートビート設定を含むポリシーを作成し、そのポリシーを時間帯によってオフラインになる環境のサーバに適用します。

1. Deep Security Managerのメイン画面の[ポリシー]タブに移動します。
2. 新しいポリシーを作成するか、既存のポリシーを編集します。
3. **ポリシーエディタ**[1]で[設定]タブをクリックし、[コンピュータ]タブに移動します。
4. Elastic Beanstalk環境がオフラインになる時間を考慮して、[ハートビート間隔]設定または[次の数を超えるハートビートが失われた場合にアラートを発令]設定、あるいはその両方を変更します。
   たとえば、サーバが1日のうち12時間はオフラインになることがわかっていて、[ハートビート間隔]が10分に設定されている場合は、[次の数を超えるハートビートが失われた場合にアラートを発令]設定を「無制限」に設定してアラートが発令されないようにしたり、[ハートビート間隔]を10分よりも長くしてアラートの数を抑えたりできます。
5. [保存]をクリックし、関連するすべてのサーバにポリシーを適用します。

AWS Elastic Beanstalk環境でのDeep Securityの使用の詳細については、トレンドマイクロのウェビナー「Deploying Scalable and Secure Web Apps with AWS Elastic Beanstalk and Deep Security」をご覧ください。

Azureクラウドコネクタを使用してAzureサーバを追加できない

Azureサーバが Azure メタデータサービスへの接続を失うと、Deep Security ManagerはAzureサーバとして識別できなくなり、Azureクラウドコネクタを使用して追加できなくなります。

この状況は、Azureコンソールの外部でサーバのパブリックIPアドレスまたはプライベートIPアドレスが変更された場合に発生することがあります。AzureサーバはDHCPを使用してメタデータサービスと通信しますが、コンソールの外部でIPを変更するとDHCPが無効になります。

Microsoftでは、Windows仮想マシンに複数のIPアドレスを割り当てるなどの必要がない限り、Azure仮想マシンのオペレーティングシステム内からIPアドレスを変更しないことを推奨しています。詳細については、こちらのAzureの記事を参照してください。

---

[1] ポリシーエディタを開くには、[ポリシー]画面に移動し、編集するポリシーをダブルクリック(またはポリシーを選択して[詳細]をクリック)します。

AzureサーバがAzureメタデータサービスに接続できるかどうかを確認するには、Windows Azure仮想マシンを検出するためのPowerShellスクリプトをMicrosoftスクリプトセンターからダウンロードして実行します。

Deep SecurityでAzureサブスクリプションの一部の仮想マシンが表示されない

Azureサブスクリプション内のすべての仮想マシンリソースがDeep Security Managerの[コンピュータ]ページに表示されていない場合、Azure配信モデルのResource Managerを使用して配信された可能性があります。[Select a deployment model]リストから[Classic]を選択しないかぎり、このモデルを使用してすべてのリソースがデプロイされます。

以前のバージョンのDeep Security Managerでは、従来のAzure配信モデル(サービス管理モデル)が提供するサービス管理APIを使用してAzure仮想マシンに接続するため、Classicモデルで配信されたVMのみを列挙できるため、すべてのVMが表示されるわけではありません。。

クラシック仮想マシンとResource Manager仮想マシンの両方を表示するには、クラウドコネクタをアップグレードします。詳細については、"新しいAzure Resource Manager接続機能へのアップグレードについて" on page 691を参照してください。

注意: 上記のトピックのようにResource Managerサーバをアップグレードできない場合でも、仮想マシン上でインストールスクリプトを使用して、有効化によりコネクタ外に新しいコンピュータオブジェクトが作成されるようにすることで、保護できます。

Log4jの脆弱性に対するDeep Securityの対応範囲

2021年12月9日、人気のApache Log4j 2ログライブラリの複数のバージョンに影響する重大なゼロデイ脆弱性が公開されました。この脆弱性が悪用されると、影響を受けるインストールで特定の文字列がログに記録され、リモートでコードが実行される可能性があります。この脆弱性はCVE-2021-44228に割り当てられており、さまざまなブログやレポートで「Log4Shell」と呼ばれています。

Deep Securityには、侵入防御 モジュール(IPS)が含まれており、ゼロデイ脆弱性やその他の攻撃からコンピュータを保護します。侵入防御 ルールは、脆弱性を悪用しようとするトラフィックをインターセプトすることで「仮想パッチ」を提供し、脆弱性を修正するベンダのパッチがリリース、テスト、および配信されるまでコンピュータを保護します。

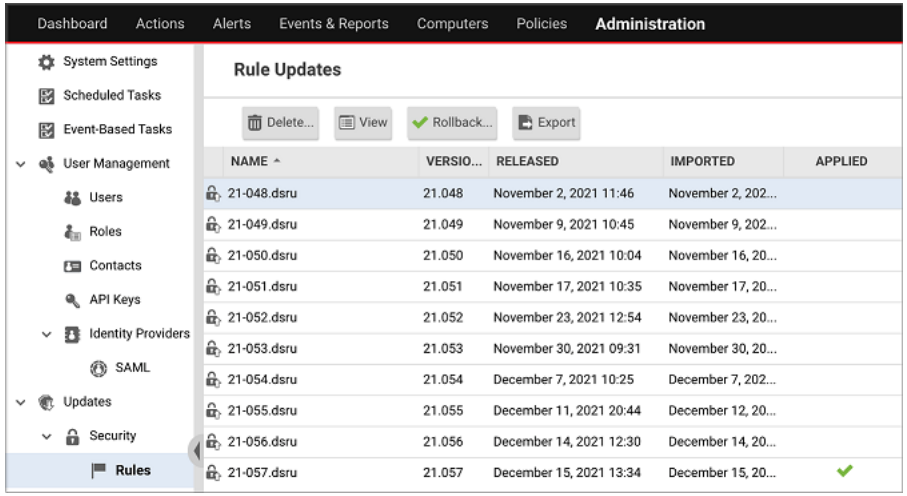
Trend Micro Labsチームは、この脆弱性に対処する新しいIPSルールを提供しました。

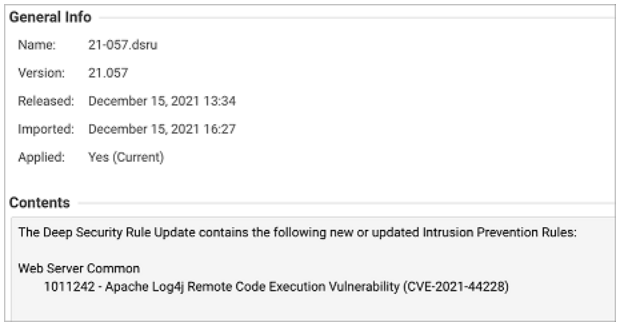
1011242-Apache Log4jにおけるリモートコード実行の脆弱性(CVE-2021-44228)

Log4jの脆弱性に対する仮想パッチの適用

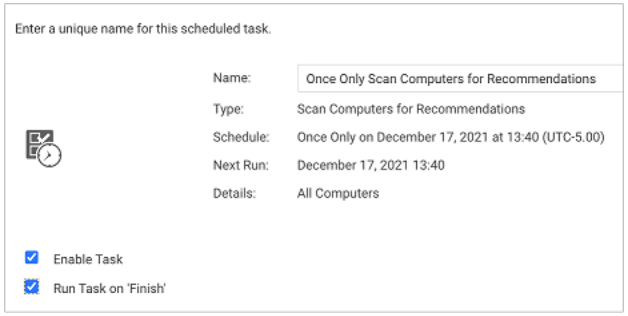
次の手順に従って、新しいルールがコンピュータを保護しているかどうかを確認します。

1. Deep Security Managerで、[管理]→[アップデート]→[セキュリティ]→[ルール] に移動します。
2. 新しいルールは、21-057.dsruに含まれています。ルールのアップデートが「Applied」と表示されていることを確認します。





3. ルールが適用されていない場合、推奨設定の検索を実行します。「1回実行」のスケジュールされたタスクを作成し、[完了]でタスクを実行オプションを選択することをお勧めします。



4. 推奨される場所にルールが適用されるようにするには、検索したコンピュータに割り当てられているポリシーを開き、[侵入防御]→[一般]の順に選択し、ルール「1011242」を検索します。ポリシーに割り当てるルール名の横にあるチェックボックスをオンにします。このポリシーで保護されているすべてのコンピュータにルールが適用されます。
5. 侵入防御は、検出モードと防御モードのいずれかで動作します。検出モードでは、ルール違反に関するイベントが生成されますが、トラフィックはブロックされません。防御モードでは、イベントを生成し、ルールに一致するトラフィックをブロックして攻撃を防ぎます。防御モードを設定するには、コンピュータまたはポリシーエディタを開き、侵入防御 > 一般 に移動し、侵入防御の動作 を防御に設定します。[保存] をクリックします。

影響を受ける可能性のあるホストの特定

Trend Micro Vision Oneも使用している場合は、次のクエリを使用して、この脆弱性の影響を受ける可能性のあるホストを特定できます。

```
eventName:DEEP_PACKET_INSPECTION_EVENT AND (ruleId:1008610 OR ruleId:1011242 OR ruleId:1005177) AND ("${" AND ("lower:" OR "upper:" OR "sys:" OR "env:" OR "java:" OR "jndi:"))
```

セキュリティログ監視 ルールを使用してアクティビティを調査する

トレンドマイクロでは、この脆弱性に関連するアクティビティの特定に役立つ セキュリティログ監視 ルールを提供しています。

1011241-Apache Log4jにおけるリモートコード実行の脆弱性(CVE-2021-44228)

将来発見されるパターンを検出するために、カスタムセキュリティログ監視ルールを作成することもできます。詳細については、Trend Cloud One - Endpoint & Workload Security および Deep Security における Log4Shell 脆弱性のためのカスタムセキュリティログ監視ルール を参照してください。

この脆弱性に関するトレンドマイクロのその他のリソース

- 最新の情報については、Apache Log4j (Log4Shell) 脆弱性 をご覧ください。トレンドマイクロがどのように支援できるかをご確認いただけます。
- この脆弱性に関する情報を含むビデオをご覧ください。
- この脆弱性の詳細と、トレンドマイクロがどのようにして攻撃から環境を保護するのかについては、セキュリティアラート: Apache Log4j "Log4Shell" リモートコード実行 0-Day 脆弱性 (CVE-2021-44228)をご覧ください。

トラブルシューティング

オフラインエージェント

コンピュータステータスがオフラインまたは管理 (オフライン) の場合、Deep Security ManagerがDeep Security Agentのインスタンスとしばらく通信しておらず、ハートビートのしきい値を超えたことを意味します ("ハートビートを設定する" on page 1499を参照)。このステータスの変更は、アラートやイベントにも表示されることがあります。

原因

ハートビート接続が失敗する理由は次のとおりです:

- エージェントは、シャットダウンされたワークステーションまたは他のコンピュータにインストールされています。Deep Securityを使用して、時々シャットダウンされるコンピュータを保護する場合、それらのコンピュータに割り当てられたポリシーがハートビートの欠落時にアラートを発生させないようにしてください。ポリシーエディタで、設定 > 一般 > アラートが発生する前に欠落できるハートビートの数 に移動し、設定を無制限に変更します。
- ファイアウォール、IPSルール、またはセキュリティグループが、ハートビートポート番号をブロックしている。
- 送信 (エフェメラル) ポートが誤ってブロックされた。トラブルシューティングのヒントについては、"ブロックされたポート" on page 1427を参照してください。
- 双方向通信が有効になっているが、許可されている、または安定しているのが一方向のみである("通信方向を設定する" on page 1500を参照)。
- コンピュータの電源がオフになった。
- コンピュータがプライベートネットワークのコンテキスト外に移動した。
  この状況は、ローミングを使用しているエンドポイント(ノートパソコンなど) が現在の場所でManagerに接続できない場合に発生します。たとえば、ゲストWi-Fiではオープンポートを制限することが多く、トラフィックがインターネットを通過するときにNATを使用します。

- Amazon WorkSpaceコンピュータがシャットダウンされており、ハートビート間隔が速くなっています(例えば、1分)。この場合、WorkSpaceが完全にシャットダウンされるまで待機し、その時点でステータスがオフラインからVM停止に変更されるはずです。
- DNSが停止したか、Managerのホスト名を解決できなかった。
- Manager、Agent、またはその両方で、システムリソースの負荷が非常に高い。
- Agentプロセスが稼働していない可能性がある。
- SSLまたはTLS接続の相互認証用証明書が無効になったか失効した("Deep Security ManagerのTLS証明書を変更します。" on page 1622を参照)。
- エージェントまたはマネージャのシステム時間が正しくありません(SSL/TLS接続で必要です)。
- Deep Securityルールアップデートはまだ完了しておらず、一時的に接続が中断されています。
- AWS EC2で、ICMPトラフィックが必要だが、ブロックされている。
- エージェントバージョン20.0.0.6313以降にアップグレードした後も、エージェントがSHA-1アルゴリズムを使用している場合、エージェントはマネージャとの通信に対して新しく、より安全な暗号アルゴリズムのみを許可します。

ヒント: マネージャ開始または双方向通信を使用していて通信の問題が発生している場合は、エージェント開始のアクティベーションに変更する必要があります("Agentからのリモート有効化およびAgentからの通信を使用してAgentを有効化して保護する" on page 1511を参照)。

エラーをトラブルシューティングするには、エージェントが実行中であり、マネージャと通信できることを確認してください。

Agentが実行されていることを確認する

エージェントがインストールされているコンピュータで、Trend Micro Deep Securityエージェントサービスが実行中であることを確認します。方法はOSによって異なります。

- Windowsの場合は、Microsoft Windowsサービスコンソール(services.msc)またはタスクマネージャーを開きます。ds_agentという名前のサービスを探します。

- Linuxの場合は、ターミナルを開き、プロセスをリストするコマンドを入力します。次のコマンドを実行して、ds_agentまたはds-agentという名前のサービスを検索します。

```
sudo ps -aux | grep ds_agent
```

```
sudo service ds_agent status
```

- Solarisの場合は、ターミナルを開き、プロセスをリストするコマンドを入力します。次のコマンドを実行して、ds_agentという名前のサービスを検索します。

```
sudo ps -ef | grep ds_agent
```

```
sudo svcs -l svc:/application/ds_agent:default
```

DNSを検証する

AgentがIPアドレスではなくドメイン名またはホスト名でManagerに接続する場合は、DNS解決をテストします。

```
nslookup [manager domain name]
```

DNSサービスは信頼できる必要があります。

テストが失敗した場合、エージェントが正しいDNSプロキシまたはサーバを使用していることを確認してください(内部ドメイン名はGoogleやISPなどの公共DNSサーバでは解決できません)。dsm.example.comのような名前がIPアドレスに解決できない場合、IPアドレスに対する正しいルートとFirewall Policiesが存在していても、通信は失敗します。

コンピュータがDHCPを使用している場合、コンピュータまたはポリシー設定の高度なネットワークエンジンエリアでDHCP DNSの強制許可を有効にする必要があるかもしれません("ネットワークエンジン設定" on page 747を参照)。

送信ポートを許可する(Agentからのハートビート)

Managerの必要なポート番号にtelnetで接続して、ルートが存在し、ポートが開いていることを確認します。

```
telnet [manager IP]:4120
```

Telnetの成功は、ルートと正しいファイアウォールポリシーが存在し、イーサネットフレームサイズが正しいことを示す点で、ほとんどpingと同じことを証明します。マネージャのデフォルトのセキュリティポリシーを使用しているコンピュータでは、pingが無効になっています。ネットワークは、攻撃者の攻撃の予兆スキャンをブロックするために、ICMP pingとtracerouteをブロックすることがあります。そのため、通常はマネージャにpingを送信してテストすることはできません。

telnetが失敗した場合、ネットワーク上のどの地点で接続が中断されているかを特定するためにルートをトレースしてください。

- Linuxで、次のコマンドを入力してください。

  ```
  traceroute [agent IP]
  ```

- Windowsで次のコマンドを入力してください。

  ```
  tracert [agent IP]
  ```

ファイアウォールポリシー、ルート、NATポートフォワーディング、またはそのすべてを調整して問題を修正してください。Windowsファイアウォールや Linuxのiptablesなど、ネットワークおよびホストベースのファイアウォールの両方を確認してください。AWS EC2インスタンスの場合は、Amazonのドキュメント Amazon EC2 Security Groups for Linux Instances または Amazon EC2 Security Groups for Windows Instances を参照してください。Azure VMインスタンスの場合は、Microsoft Azureのドキュメント Modifying a Network Security Group を参照してください。

エージェントからマネージャへの接続テストが成功した場合、次に逆方向の接続テストを行う必要があります (ファイアウォールやルーターは、接続を許可するためにポリシールートのペアを必要とすることがよくあります。必要な2つのポリシーまたはルートのうち1つしか存在しない場合、パケットは一方向には許可されますが、もう一方向には許可されません)。

受信ポートを許可する (Managerからのハートビート)

ManagerからAgentにpingを実行し、ハートビートポート番号にtelnetで接続して、ハートビートと設定のトラフィックがAgentに到達できることを確認します。

```
ping [agent IP]
```

```
telnet [agent IP]:4118
```

pingとtelnetが失敗した場合は、次のコマンドを実行します。

```
traceroute [agent IP]
```

これによって、ネットワークのどのポイントで接続が中断されているかを検出します。ファイアウォールポリシー、ルート、NATポート転送、またはこれら3つすべてを調整して、問題を解決します。

IPSルールまたはファイアウォールルールがAgentとManagerの間の接続をブロックしている場合は、Managerが接続して問題の原因であるポリシーを割り当て解除することができません。解決するには、コンピュータで次のコマンドを実行してAgentのポリシーをリセットします。

```
dsa_control -r
```

このコマンドを実行した後、エージェントを再アクティブ化する必要があります。

Amazon AWS EC2インスタンスでICMPを許可する

AWSクラウドでは、ルータにICMP type3 code4が必要です。このトラフィックがブロックされていると、AgentとManager間の接続が中断される場合があります。

Deep Securityで強制的にこのトラフィックを許可できます。強制的に許可するファイアウォールポリシーを作成するか、コンピュータまたはポリシーの[ネットワークエンジンの詳細オプション]で、[ICMP type3 code4を強制的に許可]を有効にします ("ネットワークエンジン設定" on page 747を参照)。

Solaris 11でのアップグレードの問題を解決する

以前にSolaris 11にDeep Security Agent 9.0をインストールし、その後9.0.0-5616またはそれ以降の9.0エージェントをインストールせずにエージェントソフトウェアを11.0に直接アップグレードした場合、問題が発生する可能性があります。このシナリオでは、アップグレード後に

エージェントが起動に失敗し、Deep Security Managerでオフラインとして表示されることがあります。この問題を解決するには:

1. サーバからAgentをアンインストールします。"Deep Security Agentをアンインストールする" on page 1728を参照してください。
2. Deep Security Agent 11.0をインストールします。"エージェントを手動でインストールする" on page 537。
3. マネージャでエージェントを再アクティブ化します。"Agentの有効化" on page 559を参照してください。

CPU使用率が高い

Deep Security Agentで保護されているコンピュータでは、次の手順を実行することで、CPU使用率が高い原因を特定して問題を解決することができます。

1. Trend Micro Deep Security Agentのプロセス(Windowsではds_agent.exe)のCPU使用率が異常に高いことを確認します。方法はOSによって異なります。

   Windows: タスクマネージャー

   Linux:`top`

   Solaris: `prstat`

   AIX:`topas`

2. Agentが最新バージョンにアップデートされていることを確認します。
3. "不正プログラム対策のパフォーマンスを向上させる" on page 850および"侵入防御のパフォーマンスに関するヒント" on page 951の推奨設定を適用します。
4. アプリケーションコントロールを有効にしたばかりの場合は、初期ベースラインルールセットの作成が完了するまで待機します。必要な時間は、ファイルシステム上のファイル数によって異なります。CPU使用率が低下するはずです。
5. 推奨設定の検索を実行している場合は、コンピュータの負荷が低いときに検索を実行するようにします。仮想マシンの場合は、vCPUをさらに割り当てます。
6. 一時的に不正プログラム対策などの各保護機能を1つずつ無効にします。無効にするたびにCPU使用率を確認し、特定のモジュールが原因かどうかを確認します。

7. CPU使用率が依然として高い場合は、Agentを一時的に停止します。Agentが停止されているときに問題が解決するかどうかを確認します。問題が解決した場合、診断情報を収集し、サポート担当者に提出してください。

Agent配信での問題の診断 (Windows)

WindowsでDeep Security Agentのインストールまたは有効化に失敗した場合、配信ログを確認し原因を検索して、トラブルシューティングします。

1. Agentのインストールを試行したコンピュータにログインします。
2. %appdata%\Trend Micro\Deep Security Agent\installerに移動します。
3. 下記のファイルを確認します。
   - dsa_deploy.txt - PowerShellスクリプトのログ。Agentの有効化の問題についての記録が含まれています。
   - dsa_install.txt - MSIインストーラのログ。Agentのインストールの問題についての記録が含まれています。

VMwareの「不正プログラム対策ドライバがオフライン」ステータス

不正プログラム対策ドライバーのオフラインステータスは、vShieldマネージャーを使用してDeep Security Manager (DSM)コンソールにログオンすると表示されます。

Windowsプラットフォーム用不正プログラム対策のアップデート失敗

935 ソフトウェアアップデート: Windowsプラットフォーム用不正プログラム対策のアップデート失敗 エラーが発生した場合は、エラーメッセージをダブルクリックして詳細情報を表示します。エラーイベントの「メッセージ」には、次のような内容が含まれます。

- "互換性のない他のトレンドマイクロ製品の不正プログラム対策コンポーネント" below
- "互換性のないサードパーティ製品の不正プログラム対策コンポーネント" below
- "証明書がトレンドマイクロによって署名されていない場合" belowによって署名されていない場合
- "署名された証明書が信頼されていない場合" on the next pageいない場合
- "署名された証明書が適切な目的で認証されていない場合" on the next page
- "その他/不明なエラー" on the next page

互換性のない他のトレンドマイクロ製品の不正プログラム対策コンポーネント

このエラーを解決する方法を以下に示します。

1. 互換性のないトレンドマイクロ製品 (ウイルスバスター コーポレートエディション、Endpoint Sensorなど) をアンインストールします。
2. Deep Security Agentを再インストールします。

互換性のないサードパーティ製品の不正プログラム対策コンポーネント

このエラーを解決する方法を以下に示します。

1. サードパーティ製品をアンインストールします。
2. Deep Security Agentを再インストールします。
3. サードパーティソフトウェアの例外リストにDeep Securityを追加します。不明点がある場合は、トレンドマイクロのサポートにお問い合わせください。

証明書がトレンドマイクロによって署名されていない場合

このエラーを解決する方法を以下に示します。

1. Windowsコンピュータを更新してSHA-2コード署名をサポートしてください。詳細については、Windows用の新しいバージョンのTrend Micro Deep SecurityエージェントはSHA-2でのみ署名されますをご覧ください。
2. Deep Security Agentを再起動します。
3. エラーが解決しない場合は、エージェント診断パッケージを収集して、トレンドマイクロのサポートに問い合わせてください。

署名された証明書が信頼されていない場合

このエラーを解決する方法を以下に示します。

1. Deep SecurityでのVeriSign、DigiCert、USERTrust RSA証明書の更新の指示に従って、必要な証明書をインポートしてください。
2. Deep Security Agentを再起動します。
3. エラーが解決しない場合は、エージェント診断パッケージを収集して、トレンドマイクロのサポートに問い合わせてください。

署名された証明書が適切な目的で認証されていない場合

このエラーを解決する方法を以下に示します。

1. Deep Security での証明書の目的を調べるの指示に従って、証明書の目的を有効にしてください。
2. Deep Security Agentを再起動します。
3. エラーが解決しない場合は、エージェント診断パッケージを収集して、トレンドマイクロのサポートに問い合わせてください。

その他/不明なエラー

このエラーを解決する方法を以下に示します。

1. Deep Security Agentを一度アンインストールして再インストールします。
2. エラーが解決しない場合は、エージェント診断パッケージを収集して、トレンドマイクロのサポートに問い合わせてください。

注意: 次の3つの条件はこのカテゴリに属します。

- デジタル署名が見つかりません。
- 証明書を確認できませんでした。
- 証明書の確認中に予期しないエラーが発生しました。

Agentレスによる仮想マシンのパフォーマンスの問題

原因: 限られたリソース

1. Deep Security Virtual Agentのリソースが設定から予約されていることを確認してください。
2. インストール手順に指定されている要件を環境が満たしていることを確認します。

原因: 不正プログラム対策

1. Deep Security Managerで、[コンピュータ] に進みます。
2. 保護されているコンピュータをダブルクリックします。
3. [不正プログラム対策] で [オフ] を選択します。

原因: ネットワークトラフィック

- パフォーマンスを低下させるがセキュリティを向上させない場所に対して検索除外を追加します。詳細については、トレンドマイクロ Endpoint 製品の推奨検索除外リストを参照してください。

注意: ドライバレベルの検索除外では大文字と小文字が区別されます。

原因: ポリシー

- 仮想マシンのポリシー設定を[なし] に変更します。

原因: CPU使用率が高い

1. Deep Security Virtual AgentのCPU使用率が高いことを確認します。
   - vCenterコンソールに移動して、各Deep Security Virtual Agentをクリックし、[製品パフォーマンス]を選択してCPU使用率の高いコンピュータを特定します。
2. topコマンドを実行して、最もCPUを消費しているプロセスを確認します。
3. CPU使用率が高いプロセスのメモリ消費量を特定します。
   a. 次のコマンドを実行して、プロセスメモリのステータスを確認します。`#cat /proc/$PID/status` (`$PID`は実際のPIDに置き換えます。)
   b. 仮想マシンのサイズが妥当であることを確認します。
   c. 次のコマンドを使用して、コンテンツをログファイルにエクスポートします。

      ```
      #cat /proc/$PID/status > /tmp/HighCPUProcessMemory.txt
      ```

      ```
      #sudo lsof -p $PID > /tmp/HighCPUProcessOpenedFile.t
      ```
4. Deep Security Virtual Agentに十分な空きメモリがあるかどうかを確認します。
   a. `cat /proc/meminfo` コマンドを実行して、Deep Security Virtual Agentのシステムの空きメモリを特定します。
   b. `cat /proc/meminfo > /tmp/DSVAMemory.txt`コマンドを実行して、コンテンツをログファイルにエクスポートします。

原因: セキュリティアップデート

1. Relayとそのアップデート元またはプロキシサーバ間の接続を確認します。
   a. プロキシサーバを使用する必要があるかどうかを確認します。
   b. Deep Securityにログインし、[管理]→[システム設定]→[Proxy]の順に選択して、設定が正しいことを確認します。
2. AgentとRelay有効化済みAgent間のpingテストを実行します。
3. `telnet [relay IP] [port number]` を実行して、Relayのポート番号が開いていることを確認します。

4. DNSをテストして、Relayのホスト名を解決できるかどうかを確認します。
5. 通信がファイアウォールによってブロックされているかどうかを確認し、ブロックされている場合はファイアウォールを無効にします。
6. 現在のポリシーの割り当てを解除して、問題が解決されたかどうかを確認します。

セキュリティアップデートの接続

Relayサーバとそのアップデート元またはプロキシサーバとの間の接続を確認します。

1. ルートが存在すること、およびRelayのポート番号が開いていることを確認するために、次のコマンドを入力します。

   ```
   telnet [relay IP] [port number]
   ```

   telnetが失敗した場合は、pingまたはtracerouteを実行して、ルートが存在すること、およびファイアウォールポリシー(存在する場合)がトラフィックを許可していることを確認します。また、ポート番号が開いていて、ポートの競合が発生していないことも確認します。

2. DNSサーバがRelayのドメイン名を解決できることを確認するために、次のコマンドを入力します。

   ```
   nslookup [relay domain name]
   ```

   テストが失敗した場合は、Agentが正しいDNSプロキシまたはDNSサーバを使用していることを確認します (GoogleやISPなどのパブリックDNSサーバでは内部ドメイン名を解決できません)。

3. プロキシサーバを使用する場合は、Deep Securityで、プロキシ設定が正しいことを確認してください。
4. Deep Securityの設定で接続がブロックされているかどうかを確認するには、現在のポリシーの割り当てを解除します。

SQL Serverドメイン認証の問題

Deep Security Managerのインストール時にMicrosoft SQL Serverデータベースに接続できない場合は、次の手順に従って問題のトラブルシューティングを実行してください。

注意: このトピックで扱う範囲は、Windowsドメイン認証の問題に限定されています。SQL Server認証を代わりに使用している場合は、"データベースの設定" on page 455 を設定し、そのトピックに記載されている設定手順を確認して問題をトラブルシューティングしてください。

ヒント: 「Windowsドメイン認証」は、さまざまな名前で呼ばれます。Kerberos認証、ドメイン認証、Windows認証、統合認証などです。このトピックでは、「Kerberos」および「Windowsドメイン認証」という用語を使用しています。

"手順1: ホスト名とドメインを確認する" below

"手順2: servicePrincipalName (SPN) を確認する" on the next page

"手順3: krb5.confファイルを確認する (Linuxのみ)" on page 2013

"手順4: システム時計を確認する" on page 2015

"手順5: ファイアウォールを確認する" on page 2015

"手順6: dsm.propertiesファイルを確認します" on page 2016を確認します

手順1: ホスト名とドメインを確認する

[ホスト名] フィールドがFQDN形式であり、DNSサーバによって解決可能であることを確認する必要があります。

1. Deep Security Managerのインストーラを実行して、データベースの手順まで来たら、必ずSQLサーバのFQDNを指定してください。IPアドレスやNetBIOSホスト名を入力しないでください。

   有効なホスト名の例: `sqlserver.example.com`

2. FQDNが登録されていて、DNSサーバによって解決可能であることを確認してください。DNSエントリに正しいホスト名が設定されているかどうかを確認するには、`nslookup`コマンドラインユーティリティを使用します。このユーティリティは、ドメイン上の任意のコンピュータから呼び出すことができます。次のコマンドを入力します。

`nslookup <SQL Server FQDN>`

ここで、`<SQL_Server_FQDN>` は、SQLサーバのFQDNに置き換えます。指定したFQDNをユーティリティが正常に解決できる場合、DNSエントリは正しく設定されています。FQDNを解決できない場合は、DNS Aレコードと、FQDNを含むリバースレコードを設定します。

3. さらに、インストーラのデータベースページで [詳細] をクリックし、[ドメイン] フィールドにSQLサーバの完全ドメイン名を指定します。ドメインには1つ以上のドット(「.」) を含める必要があります。短縮ドメイン名やNetBIOS名を入力しないでください。

   有効なドメイン名の例: `example.com`

4. `nslookup` コマンドラインユーティリティを使用して、ドメイン名がFQDN形式であることを確認します。次のコマンドを入力します。

   `nslookup <Domain_Name>`

   ここで、`<Domain_Name>` は、SQLサーバの完全ドメイン名に置き換えます。指定したドメイン名をユーティリティが解決できる場合、それは完全なドメイン名です。

   注意: Microsoftワークグループを使用したデータベース認証は、Deep Security Manager 10.2以降ではサポートされていません。Windowsドメイン認証の場合は、Active Directoryドメインコントローラをインストールし、ドメインを設定して、このドメインにSQLサーバを追加する必要があります。環境にActive Directoryドメインインフラストラクチャがない場合は、代わりにSQL Server認証を使用する必要があります。Windowsドメイン認証の代わりにSQL Server認証を使用するには、Managerのインストーラの [データベース] ページにある [ユーザ名] フィールドと [パスワード] フィールドに、Deep Security Managerデータベースの所有者のユーザ名とパスワードを入力します。ドメインを入力しないでください。ドメイン名を省略すると、SQL Server認証が使用されます。詳細については、"Managerをインストールする" on page 460を実行します。)

手順2: servicePrincipalName (SPN) を確認する

servicePrincipalName (SPN) がActive Directoryで正しく構成されていることを確認する必要があります。

Microsoft SQL Serverの場合、SPNは次の形式です。

```
MSSQLSvc/<SQL_Server_Endpoint_FQDN>
```

```
MSSQLSvc/<SQL_Server_Endpoint_FQDN>:<PORT>
```

SPNが正しいことを確認するには、以下のタスクを実行します。最後に、特定の使用例での詳細な手順、他のドキュメントへの参照、およびデバッグのヒントがあります。

"手順2a: SQL Serverサービスを実行しているアカウント(SID) を特定する" below

"手順2b: Active Directoryでアカウントを確認する" on page 2002

"手順2c: SPNで使用するFQDNを特定する" on page 2003

"手順2d: 初期設定のインスタンスを使用しているのか、名前付きインスタンスを使用しているのかを特定する" on page 2003

"ケース1: ローカル仮想アカウントでSPNを設定する" on page 2004

"ケース2: ドメインアカウントでSPNを設定する" on page 2006

"ケース3:管理されたサービスアカウントでSPNを設定する" on page 2008

"ケース4: フェールオーバークラスタのSPNを設定する" on page 2010

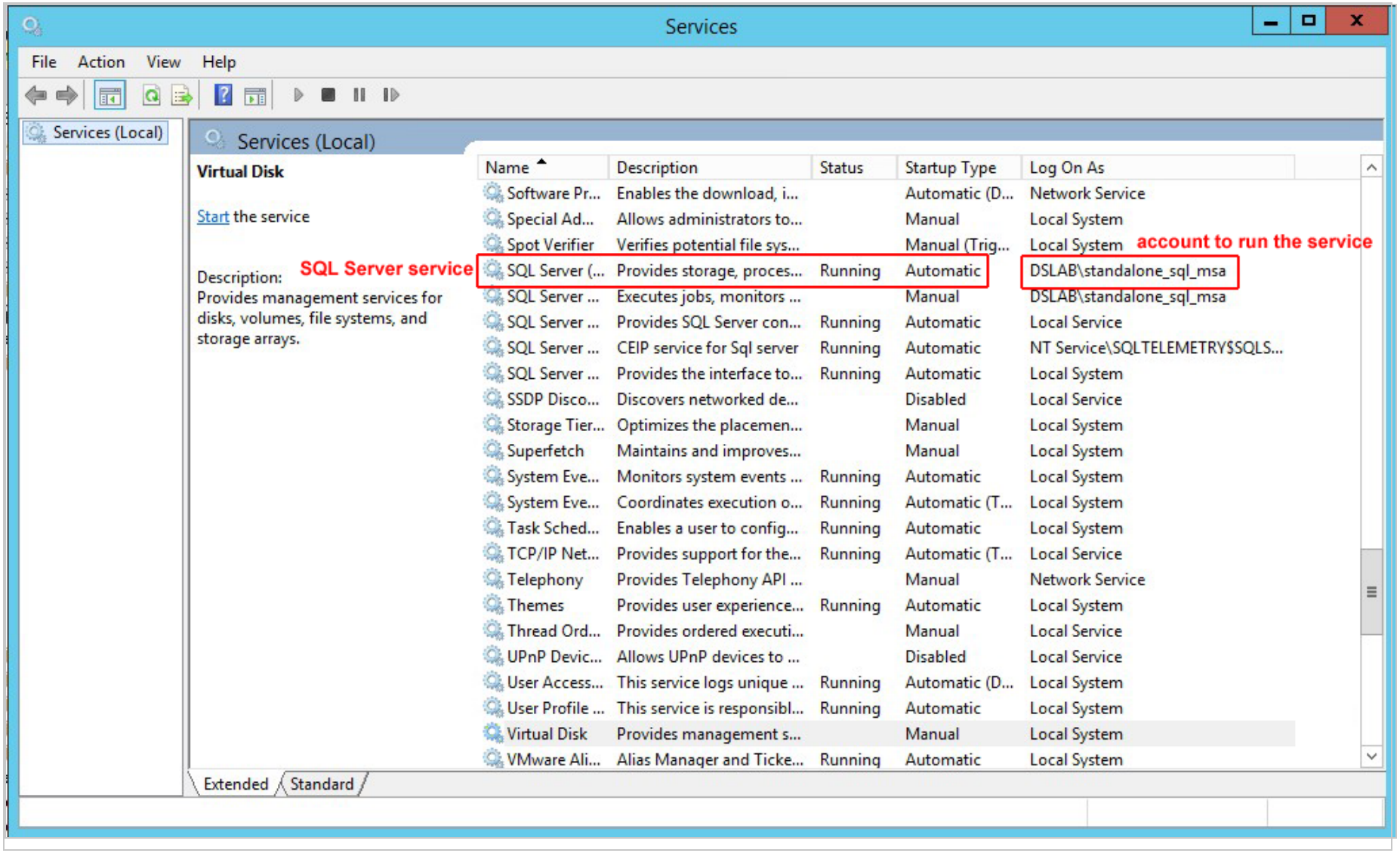
"SPNリファレンス" on page 2012

"SPNのデバッグのヒント" on page 2012

手順2a: SQL Serverサービスを実行しているアカウント(SID) を特定する

SPNは、SQL Serverサービスを実行しているアカウント内で設定されます。

どのアカウントがSQL Serverサービスを実行しているかを特定するには、services.mscユーティリティを使用します。SQL Serverサービスが、関連付けられているアカウントと共に表示されます。


Services
File Action View Help
Services (Local)
Services (Local)
Virtual Disk
Start the service
Description:
Provides management services for disks, volumes, file systems, and storage arrays.
SQL Server service
account to run the service
Name | Description | Status | Startup Type | Log On As
Software Pr... | Enables the download, i... | | Automatic (D... | Network Service
Special Ad... | Allows administrators to... | | Manual | Local System
Spot Verifier | Verifies potential file sys... | | Manual (Trig... | Local System
SQL Server (... | Provides storage, proces... | Running | Automatic | DSLAB\standalone_sql_msa
SQL Server ... | Executes jobs, monitors ... | | Manual | DSLAB\standalone_sql_msa
SQL Server ... | Provides SQL Server con... | Running | Automatic | Local Service
SQL Server ... | CEIP service for Sql server | Running | Automatic | NT Service\SQLTELEMETRY$SQLS...
SQL Server ... | Provides the interface to... | Running | Automatic | Local System
SSDP Disco... | Discovers networked de... | | Disabled | Local Service
Storage Tier... | Optimizes the placemen... | | Manual | Local System
Superfetch | Maintains and improves... | | Manual | Local System
System Eve... | Monitors system events ... | Running | Automatic | Local System
System Eve... | Coordinates execution o... | Running | Automatic (T... | Local System
Task Sched... | Enables a user to config... | Running | Automatic | Local System
TCP/IP Net... | Provides support for the... | Running | Automatic (T... | Local Service
Telephony | Provides Telephony API ... | | Manual | Network Service
Themes | Provides user experience... | Running | Automatic | Local System
Thread Ord... | Provides ordered executi... | | Manual | Local Service
UPnP Devic... | Allows UPnP devices to ... | | Disabled | Local Service
User Access... | This service logs unique ... | Running | Automatic (D... | Local System
User Profile ... | This service is responsibl... | Running | Automatic | Local System
Virtual Disk | Provides management s... | | Manual | Local System
VMware Ali... | Alias Manager and Ticke... | Running | Automatic | Local System
Extended Standard

手順2b: Active Directoryでアカウントを確認する

SQL Serverサービスを実行しているアカウントの名前がわかったら、それをActive Directory内で見つける必要があります。アカウントが存在する可能性のある場所は、ローカル仮想アカウントであるか、ドメインアカウントであるか、管理されたサービスアカウントであるかに応じて決まります。以下の表は、それらの可能性のある場所をまとめたものです。Active DirectoryコンピュータでADSIエディター (adsiedit.msc) を使用して、Active Directory内のさまざまなフォルダを探し、アカウントを見つけることができます。

アカウントの種類	アカウントの名前	Active Directory内のアカウントの場所	説明
ローカル仮想アカウント	NT SERVICE\MSSQLSERVER (初期設定のインスタンス) NT SERVICE\MSSQL$InstanceName (名前付きインスタンス)	CN=Computer CN=<コンピュータ名>	仮想アカウントで実行されるサービスは、コンピュータアカウントの資格情報を使用してネットワークリソースにアクセスします。初期設定のスタンドアロンSQL Serverサービスは、このアカウントを使用して起動されます。
ドメインアカウント	ドメインユーザ名 (例 : SQLServerServiceUser)	CN=Users CN=<ユーザ名>	このアカウントを使用して開始されたサービスは、ドメインユーザの資格情報を使用してネットワークリソースにアクセスします。SQL Serverフェールオーバークラスタでは、サービスを実行するためにドメインアカウントが必要です。スタンドアロンSQL Serverサービスは、起動にドメインアカウントを使用するように設定することもできます。
管理されたサービスアカウント	管理されたサービスアカウント(MSA)名 (例 : SQLServerMSA)	CN=Managed Service Account CN=<アカウント名>	Windows Server 2008 R2で導入された、管理されたサービスアカウントは、ドメインアカウントに似ていますが、対話形式のログオンを実行するために使用できます。スタンドアロンのSQL Serverサービスと SQL Serverクラスタサービスの両方を、管理されたサービスアカウントを使用して起動するように設定できます。

手順2c: SPNで使用するFQDNを特定する

命名の一貫性を保つために、SPNをエンドポイントのFQDNに設定することをお勧めします。エンドポイントは、SQL Serverクライアント(Deep Security Manager)の接続先であり、個々のSQL Serverまたはクラスタである場合があります。使用するFQDNの詳細については、以下の表を参照してください。

SQL Serverのインストールの種類	SPNの設定
スタンドアロンSQL Server	SQL Serverがインストールされているホストの FQDN
フェールオーバーSQL Serverクラスタ	SQL Serverクラスタの FQDN (個々のSQL Serverノードはエンドポイントではないため、FQDNで使用しないでください)

手順2d: 初期設定のインスタンスを使用しているのか、名前付きインスタンスを使用しているのかを特定する

ポート番号とインスタンス名 (指定した場合) をSPNに含める必要があるため、SQL Serverが初期設定のインスタンスと名前付きインスタンスのどちらとしてインストールされたかを知っておく必要があります。

- 初期設定のインスタンスは、通常、ポート1433を使用します。
- 名前付きインスタンスは、別のポートを使用します。このポートを判断するには、このWebページを参照してください。

例: SQL ServerサービスのFQDNエンドポイントが`sqlserver.example.com`であり、それが初期設定のインスタンスである場合、SPNは次の形式になります。

```
MSSQLSvc/sqlserver.example.com
```

```
MSSQLSvc/sqlserver.example.com:1433
```

例2: SQL ServerサービスのFQDNエンドポイントがsqlserver.example.comであり、それがポート51635を使用するDEEPSECURITYというインスタンス名の名前付きインスタンスである場合、SPNは次の形式になります。

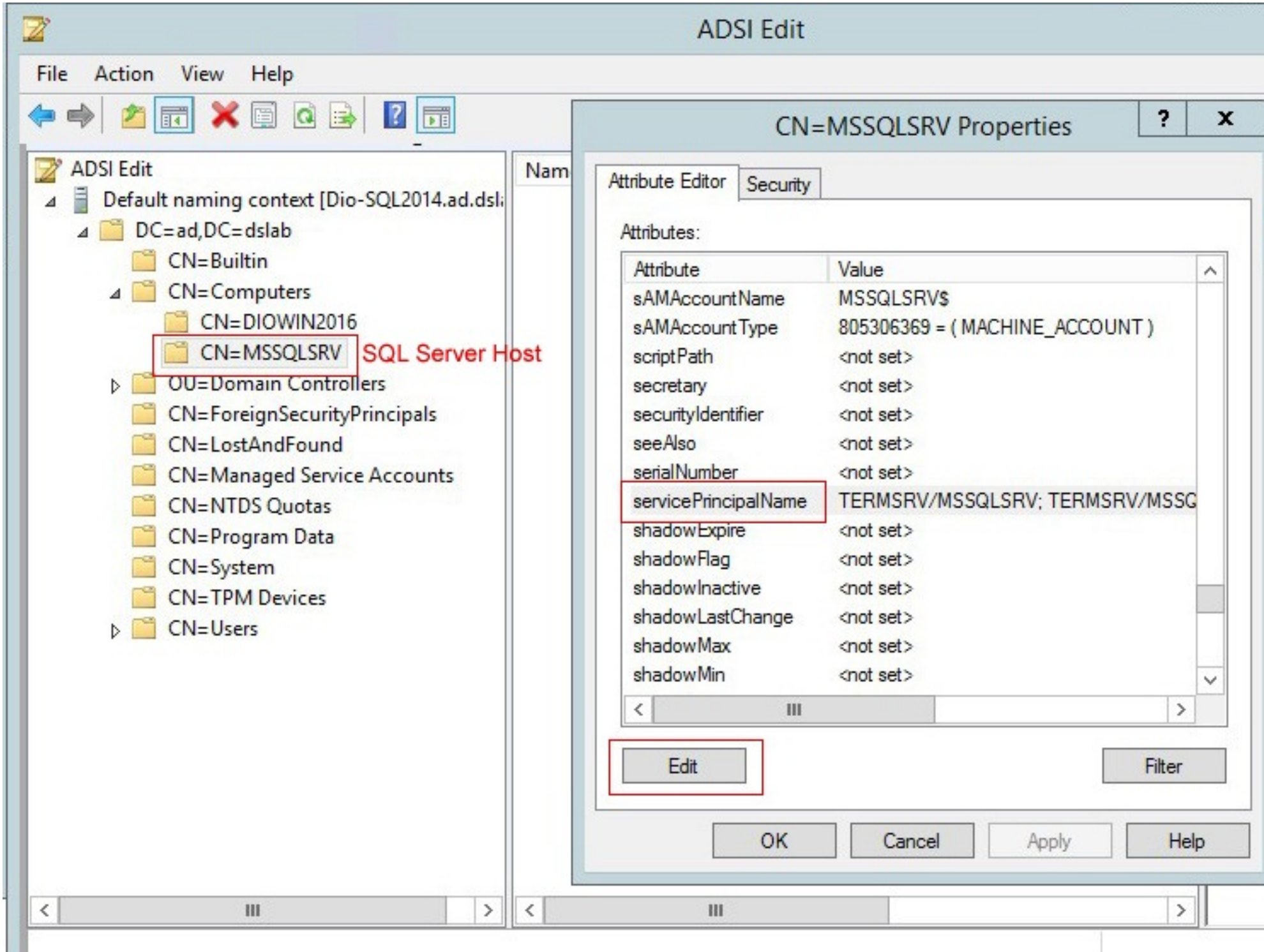
```
MSSQLSvc/sqlserver.example.com:DEEPSECURITY
```

```
MSSQLSvc/sqlserver.example.com:51635
```

ケース1:ローカル仮想アカウントでSPNを設定する

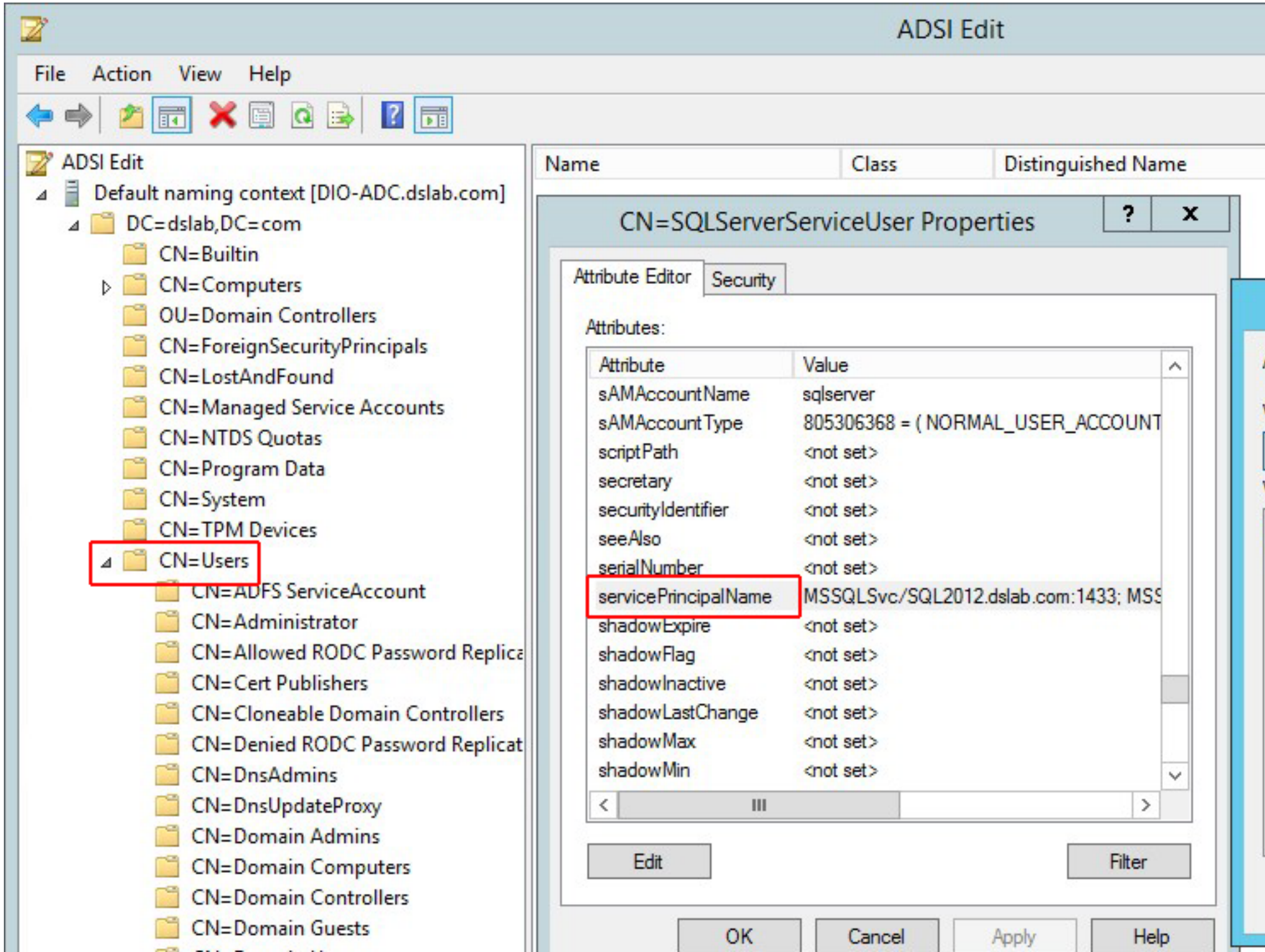
ローカル仮想アカウントで実行されるスタンドアロンSQL ServerのSPNを設定するには:

1. Active DirectoryコンピュータでADSIEdit.mscを開きます。ADSI エディターが開きます。
2. [CN=Computers] でSQL Serverホストを見つけます。
3. SQL Serverホストを右クリックし、[プロパティ] を選択します。
4. [属性エディター] タブで、[servicePrincipalNames] までスクロールし、[編集] ボタンをクリックします。
5. 属性値が存在しない場合は、[追加] ボタンを使用して個別に追加します。[OK] をクリックします。


ADSI Edit
File Action View Help
ADSI Edit
Default naming context [Dio-SQL2014.ad.dsl
DC=ad,DC=dslab
CN=Builtin
CN=Computers
CN=DIOWIN2016
CN=MSSQLSRV
SQL Server Host
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=LostAndFound
CN=Managed Service Accounts
CN=NTDS Quotas
CN=Program Data
CN=System
CN=TPM Devices
CN=Users
CN=MSSQLSRV Properties
Attribute Editor
Security
Attributes:
Attribute
Value
sAMAccountName
MSSQLSRV$
sAMAccountType
805306369 = (MACHINE_ACCOUNT)
scriptPath
<not set>
secretary
<not set>
securityIdentifier
<not set>
seeAlso
<not set>
serialNumber
<not set>
servicePrincipalName
TERMSRV/MSSQLSRV; TERMSRV/MSSG
shadowExpire
<not set>
shadowFlag
<not set>
shadowInactive
<not set>
shadowLastChange
<not set>
shadowMax
<not set>
shadowMin
<not set>
Edit
Filter
OK
Cancel
Apply
Help

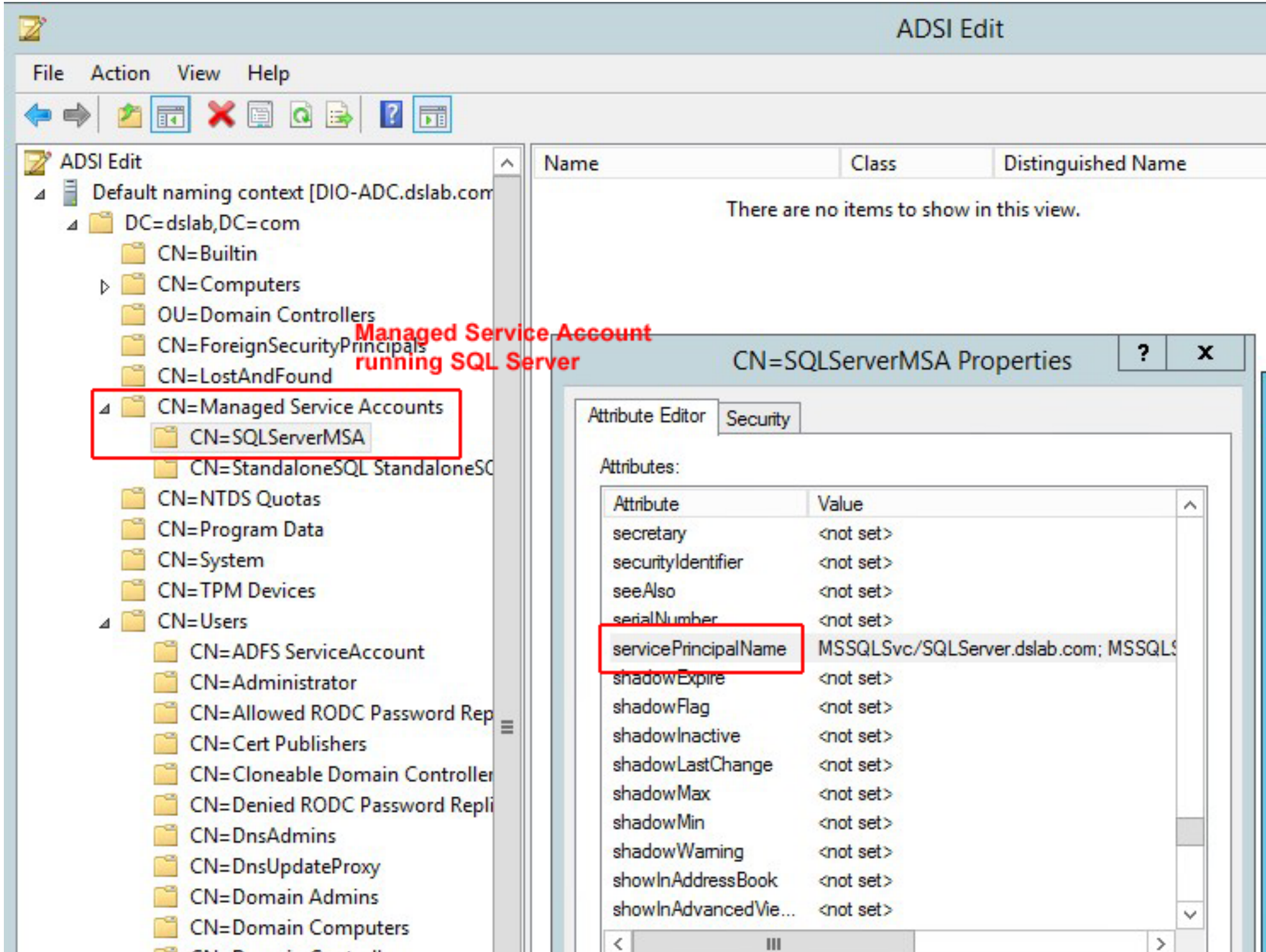
ケース2: ドメインアカウントでSPNを設定する

SQL Serverサービスを実行しているドメインアカウント(CN=Users) でSPNが設定されることを除き、SPN設定はローカル仮想アカウント設定と似ています。


ADSI Edit
File Action View Help
ADSI Edit
Default naming context [DIO-ADC.dslab.com]
DC=dslab,DC=com
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=LostAndFound
CN=Managed Service Accounts
CN=NTDS Quotas
CN=Program Data
CN=System
CN=TPM Devices
CN=Users
CN=ADFS ServiceAccount
CN=Administrator
CN=Allowed RODC Password Replica
CN=Cert Publishers
CN=Cloneable Domain Controllers
CN=Denied RODC Password Replicat
CN=DnsAdmins
CN=DnsUpdateProxy
CN=Domain Admins
CN=Domain Computers
CN=Domain Controllers
CN=Domain Guests
Name
Class
Distinguished Name
CN=SQLServerServiceUser Properties
Attribute Editor
Security
Attributes:
Attribute
Value
sAMAccountName
sqlserver
sAMAccountType
805306368 = (NORMAL_USER_ACCOUNT
scriptPath
<not set>
secretary
<not set>
securityIdentifier
<not set>
seeAlso
<not set>
serialNumber
<not set>
servicePrincipalName
MSSQLSvc/SQL2012.dslab.com:1433; MSS
shadowExpire
<not set>
shadowFlag
<not set>
shadowInactive
<not set>
shadowLastChange
<not set>
shadowMax
<not set>
shadowMin
<not set>
Edit
Filter
OK
Cancel
Apply
Help

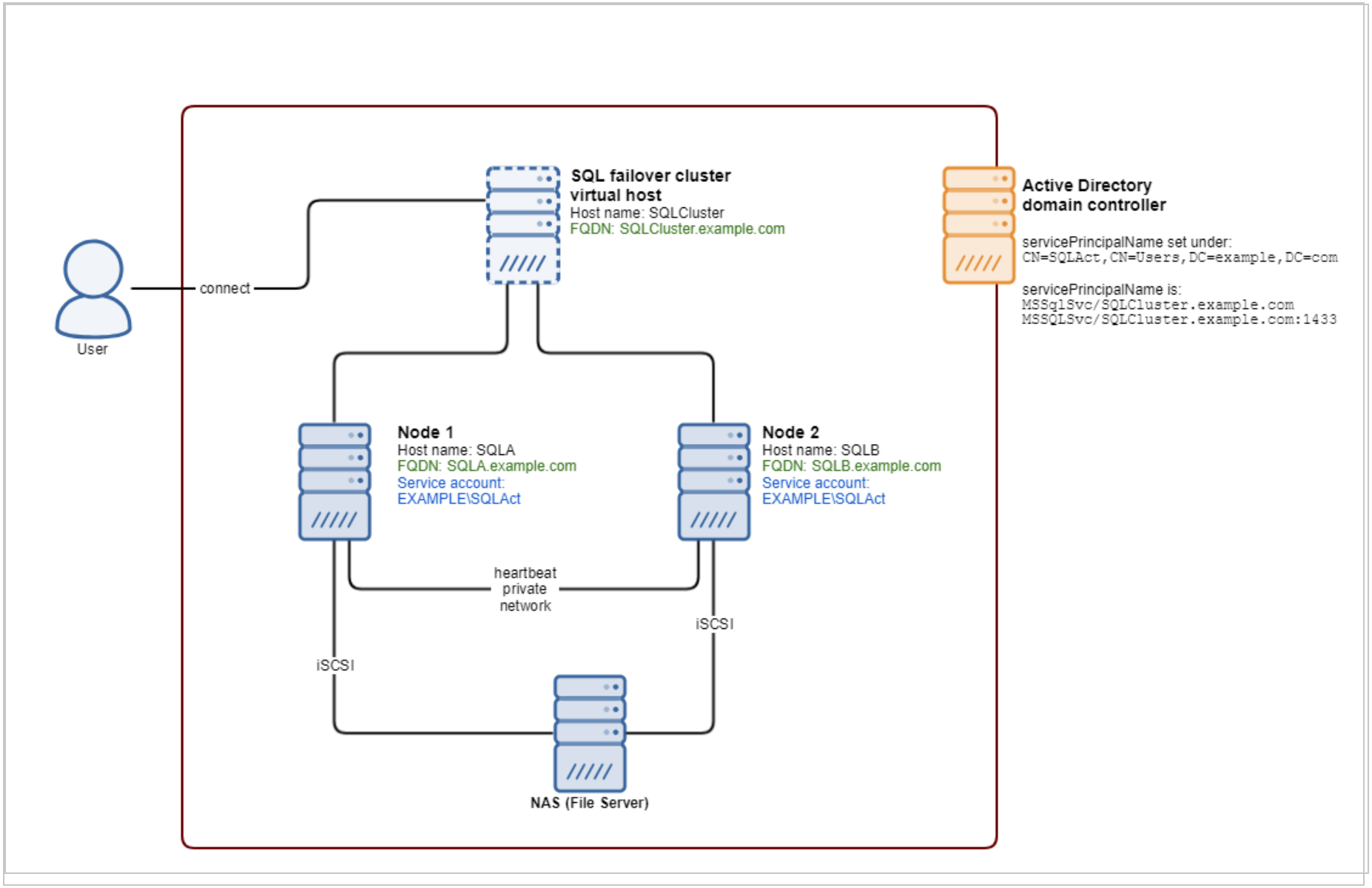
ケース3:管理されたサービスアカウントでSPNを設定する

SPNは、SQL Serverサービスを実行している管理されたサービスアカウント(CN=Managed Service Account) で設定されます。


ADSI Edit
File Action View Help
ADSI Edit
Default naming context [DIO-ADC.dslab.com
DC=dslab,DC=com
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=LostAndFound
CN=Managed Service Accounts
CN=SQLServerMSA
CN=StandaloneSQL StandaloneSC
CN=NTDS Quotas
CN=Program Data
CN=System
CN=TPM Devices
CN=Users
CN=ADFS ServiceAccount
CN=Administrator
CN=Allowed RODC Password Rep
CN=Cert Publishers
CN=Cloneable Domain Controller
CN=Denied RODC Password Repli
CN=DnsAdmins
CN=DnsUpdateProxy
CN=Domain Admins
CN=Domain Computers
Managed Service Account
running SQL Server
Name
Class
Distinguished Name
There are no items to show in this view.
CN=SQLServerMSA Properties
Attribute Editor
Security
Attributes:
Attribute
Value
secretary
securityIdentifier
seeAlso
serialNumber
servicePrincipalName
MSSQLSvc/SQLServer.dslab.com; MSSQLS
shadowExpire
shadowFlag
shadowInactive
shadowLastChange
shadowMax
shadowMin
shadowWarning
showInAddressBook
showInAdvancedVie...
<not set>

ケース4:フェールオーバークラスタのSPNを設定する

SQL Serverフェールオーバークラスタは、ドメインアカウントまたは管理されたサービスアカウントで実行できます。手順については、"ケース2:ドメインアカウントでSPNを設定する" on page 2006または"ケース3:管理されたサービスアカウントでSPNを設定する" on page 2008を参照してください。SPNは、個々のSQLノードではなく、必ずSQL「クラスタ」エンドポイントのFQDNに設定してください。


SQL failover cluster
virtual host
Host name: SQLCluster
FQDN: SQLCluster.example.com
Active Directory
domain controller
servicePrincipalName set under:
CN=SQLAct,CN=Users,DC=example,DC=com
servicePrincipalName is:
MSSqlSvc/SQLCluster.example.com
MSSQLSvc/SQLCluster.example.com:1433
connect
User
Node 1
Host name: SQLA
FQDN: SQLA.example.com
Service account:
EXAMPLE\SQLAct
Node 2
Host name: SQLB
FQDN: SQLB.example.com
Service account:
EXAMPLE\SQLAct
heartbeat
private
network
iSCSI
iSCSI
NAS (File Server)

SPNリファレンス

以下は、SPN設定に関するMicrosoftの公式文書へのリンクです。

Kerberos接続用のサービスプリンシパル名の登録

SQL ServerフェールオーバークラスタでKerberos認証を有効にする方法

SPNのデバッグのヒント

SPNが正しく設定されていることを確認するには、コマンドラインツールsetspnを使用して、登録済みのSPNエントリを検索します。コマンド構文は次のとおりです。

```
setspn -T <Full_Domain_Name> -F -Q MSSQLSvc/<SQL_Server_Endpoint_FQDN>*
```

指定する項目は次のとおりです。

- <Full_Domain_Name>は、お使いの環境のドメイン名に置き換えます。
- <SQL_Server_Endpoint_FQDN>は、SQL ServerのFQDNに置き換えます。

たとえば、スタンドアロンのSQL ServerがSQL2012.dslab.comにあり、ドメインdslab.comのローカル仮想アカウントで実行されているとします。次のコマンドを使用して、MSSQLSvc/SQL2012.dslab.comというプレフィックスを持つすべての登録済みSPNを検索し、それが正しく設定されているかどうかを確認できます。



コマンドの結果から、SPNが、正しいLDAPパスおよびSQL Serverサービスを実行しているアカウントに、設定および登録されていることを確認できます。

手順3: krb5.confファイルを確認する(Linuxのみ)

LinuxにManagerをインストールする場合は、/etc/krb5.confが存在していることと、それに正しいドメインとレルムの情報が含まれていることを確認する必要があります。

1. Kerberosを設定するには、テキストエディタで/etc/krb5.confファイルを開くか作成します。
2. 以下の情報を指定します。

```
[libdefaults]
  ...
  default_realm = <DOMAIN>
  ...
[realms]
  <DOMAIN> = {
    kdc = <ACTIVE_DIRECTORY_CONTROLLER_FQDN>
```

```
    admin_server = <ACTIVE_DIRECTORY_CONTROLLER_FQDN>
  }
[domain_realm]
  .<DOMAIN FQDN> = <DOMAIN>
  <DOMAIN FQDN> = <DOMAIN>
```

ここで、<DOMAIN>、<ACTIVE_DIRECTORY_CONTROLLER_FQDN>、および<DOMAIN_FQDN>は、独自の値に置き換えます。

サンプルファイル:

```
[libdefaults]
  default_realm = EXAMPLE.COM
  default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
  default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc
  dns_lookup_kdc = true
  dns_lookup_realm = false

[realms]
  EXAMPLE.COM = {
    kdc = kerberos.example.com
    kdc = kerberos-1.example.com
    admin_server = kerberos.example.com
```

```
    }

[domain_realm]
    .example.com = EXAMPLE.COM
    example.com = EXAMPLE.COM

[logging]
    kdc = SYSLOG:INFO
    admin_server = FILE=/var/kadm5.log
```

3. ファイルを保存して、閉じます。

手順4: システム時計を確認する

ドメインコントローラ、SQL Server、およびDeep Security Managerコンピュータのシステム時計が同期していることを確認する必要があります。Kerberosでは、最大許容クロックスキューは、初期設定で5分です。

手順5: ファイアウォールを確認する

ファイアウォールがSQL接続をブロックしていないことを確認する必要があります。初期設定のSQL Serverインスタンスでは、ポート1433を介した接続が許可されますが、名前付きSQL Serverインスタンスでは、ランダムに選択されたポートが使用されます。接続先のポートを見つけるために、SQLクライアント(この場合はDeep Security Manager)は利用可能な名前付きインスタンスを検索し、SQL Serverブラウザサービスにルックアップ要求を発行して、マッピングポートを見つけます。SQL Serverブラウザサービスは、ポート1434 (UDP) で実行されます。ファイアウォール設定で、ポート1433 (初期設定インスタンスを使用している場合)、または1434 (名前付きインスタンスを使用している場合) が許可されていることを確認してください。

手順6：dsm.propertiesファイルを確認します

dsm.properties ファイルが正しく構成されていることを確認してください。

1. dsm.properties ファイルをテキストエディタで開きます。Windowsでは、ファイルは通常 C:\Program Files\Trend Micro\Deep Security Manager\webclient\webapps\ROOT\WEB-INFにあります。
2. ファイルに次の行が含まれていることを確認してください。

   database.SqlServer.server=YOUR-SERVER.EXAMPLE.COM //ドメイン名を含めます。ドメイン名には大文字を使用する必要があります。

   database.SqlServer.trustServerCertificate=true //この行は、SQLサーバーが強制暗号化を有効にする場合に必要です。

   database.SqlServer.domain=EXAMPLE.COM //ドメイン名は大文字を使用する必要があります。

   database.SqlServer.user=sqlUser@EXAMPLE.COM //ユーザー名にはドメイン名を含める必要があり、ドメイン名には大文字を使用する必要があります。

   database.SqlServer.integratedSecurity=true

   database.SqlServer.authenticationScheme=JavaKerberos

   database.directory=null

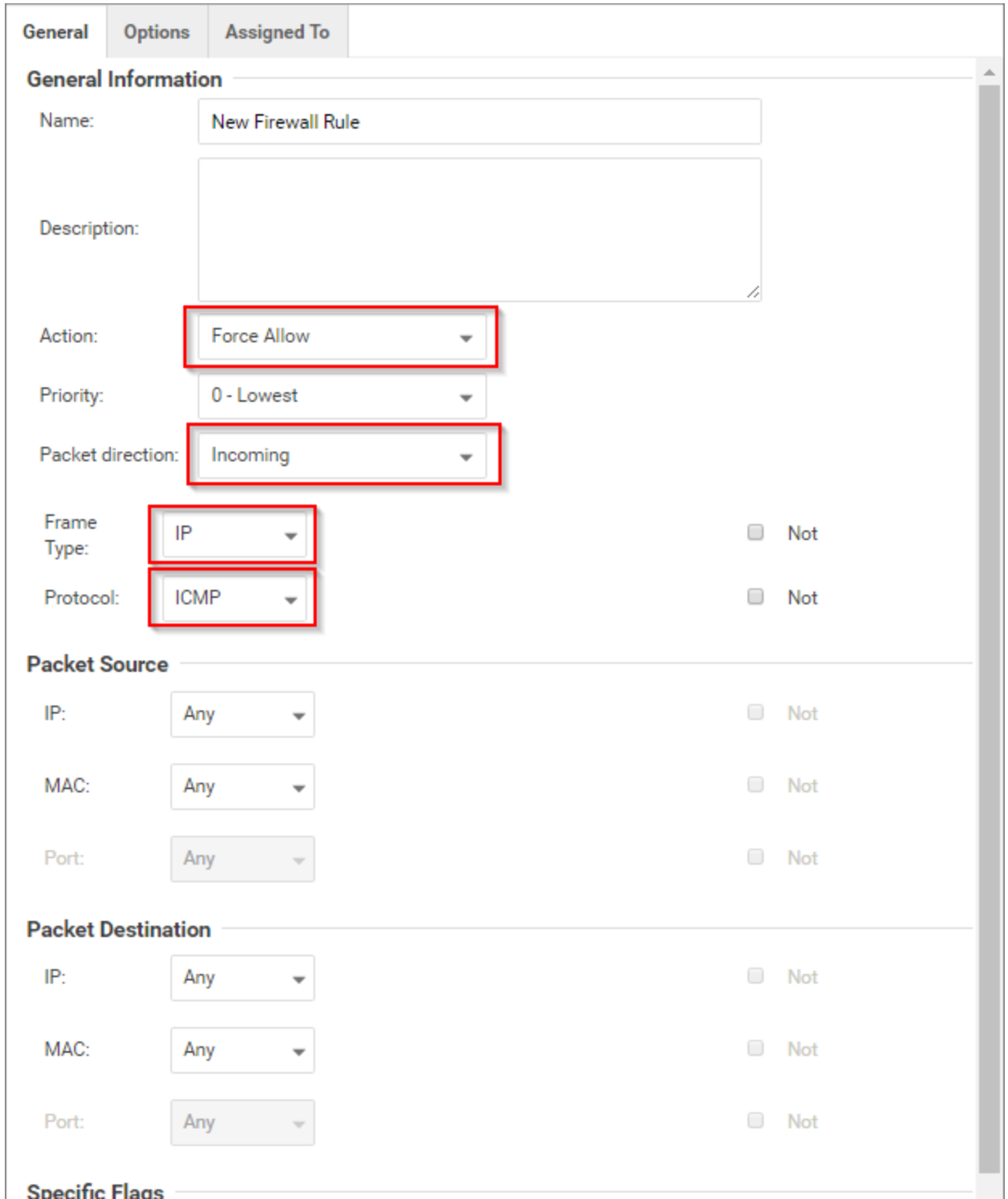
   database.SqlServer.namedPipe=false

3. 必要な変更を加えてファイルを保存します。

複数のAmazon Virtual Private Cloud (VPC) からのAgent通信でMTUが原因で発生する問題の回避

Deep Security Managerと通信しようとすると、さまざまなVPC内のクライアントで問題が発生することがあります。これは、Amazon Web Servicesでサポートされるネットワーク MTU(Maximum Transmission Unit) が1500になり、Deep Security Agentの通信トラフィックがこれを超える可能性があり、パケットが断片化して破棄される可能性があるためです。

このようなMTUに起因する通信の問題が発生しないようにするには、すべてのファイアウォールポリシーに新しいファイアウォールルールを追加します。この新しいファイアウォールルールの重要な設定を次の図に示します。


General
Options
Assigned To
General Information
Name:
New Firewall Rule
Description:
Action:
Force Allow
Priority:
0 - Lowest
Packet direction:
Incoming
Frame Type:
IP
Not
Protocol:
ICMP
Not
Packet Source
IP:
Any
Not
MAC:
Any
Not
Port:
Any
Not
Packet Destination
IP:
Any
Not
MAC:
Any
Not
Port:
Any
Not
Specific Flags

診断パッケージの作成

問題を診断するために、サポートプロバイダがDeep Security Manager、Deep Security Agent、またはその両方のデバッグ情報を含む診断パッケージを送信するよう依頼する場合があります。

Deep Security Managerの診断

Deep Security Manager (DSM) の診断は、ログ、システム情報、および Java Flight Recorder (JFR) の記録を含む診断パッケージを通じて提供されます。

Deep Security Managerのデバッグログを有効にする

診断パッケージに加えて、サポート担当者から診断ログを有効にするように求められることがあります。

1. [管理]→[システム情報] の順に選択します。
2. [診断ログ] をクリックします。
3. 表示されるダイアログで、サポート担当者から求められたオプションを選択します。

   マルチテナントのDeep Security Managerを使用していて、診断したい問題が特定のテナントでのみ発生する場合は、表示されるオプションでそのテナントの名前を選択してください。これにより、デバッグログが集中し、デバッグログが有効になっている間のパフォーマンスへの影響が最小限に抑えられます。

   一部の機能領域では、十分なデバッグログを収集するために、より多くの時間とディスクスペースが必要です。たとえば、[データベース関連の問題] や [クラウドアカウント同期 - AWS] については、[ログファイルの最大サイズ] を25MBに増やし、期間を24時間に延長することが必要になる場合があります。

   [ログファイルの最大数] を減らした場合、既存のログファイルの数が指定した値を超えていても、Deep Security Managerによって既存のログが自動的に削除されることはありません。たとえば、ログファイルの最大数を10から5に変更しても、server5.logから

server9.logまでのログファイルを含め、すべてのログファイルがそのまま維持されます。ディスク容量を解放するには、それらのファイルをファイルシステムから手動で削除します。

診断ログが実行中の場合、Deep Security Managerはステータスバーに診断ログが有効というメッセージを表示します。デフォルトのオプションを変更した場合、診断ログの完了時にステータスバーにデフォルト以外のログが有効というメッセージが表示されます。

4. 診断ログファイルを見つけるには、Deep Security Managerのルートディレクトリに移動し、server#.logというパターンのファイル名(server0.logなど)を探します。

警告: サポートプロバイダからの推奨がない限り、診断ログを有効にしないでください。診断ログは大量のディスクスペースを消費し、CPU使用率を増加させる可能性があります。

Deep Security Manager の Java Flight Recorder を有効にする

Java Flight Recorder (JFR) は、Java Virtual Machine (JVM) の内部イベントに関連する情報を収集します。JFR は DSM の問題を監視およびトラブルシューティングするために使用できます。サポートプロバイダから要求された場合にのみ JFR を有効にする必要があります。

1. [管理]→[システム情報] の順に選択します。
2. 診断ログをクリックします。
3. 表示されるダイアログで、Java Flight Recorder を有効にするを選択し、記録が終了するまでの時間を選択します。
4. 必要に応じて、最大記録ファイルサイズを使用して記録ファイルの上限 (メガバイト単位) を選択します。記録データが許可されたサイズを超えると、JFRは古いデータを破棄します。
5. [保存] をクリックして録音を開始します。

記録データはDSMインストールディレクトリにあるdsm.jfrというファイルに保存されます。記録が進行中の場合、dsm.jfrファイルのサイズは0 MBです。データは記録が終了した後にのみファイルに追加されます。デフォルトでは、dsm.jfrファイルはDSM診断パッケージに含まれ、7日間保持されます。その後、ファイルは削除されます。

Deep Security Managerの診断パッケージを作成する

1. [管理]→[システム情報] の順に選択します。
2. [診断パッケージの作成] をクリックします。

   パッケージの作成には数分かかります。パッケージが生成されると、概要が表示され、診断情報を含むzipファイルがブラウザにダウンロードされます。

Deep Security Agentの診断

エージェントの場合、次のいずれかの方法で診断パッケージを作成できます:

- Deep Security Manager経由
- 保護されているコンピュータでCLIを使用 (Deep Security Managerがリモートからアクセスできない場合)

診断パッケージに使用する不正プログラム対策のデバッグログレベルの調整に関するLinux固有の情報については、"保護対象のLinuxインスタンスにおける不正プログラム対策のデバッグログレベルの引き上げ" on page 897を参照してください。

サポートプロバイダから、次の情報の収集を依頼される場合があります。

- タスクマネージャーのスクリーンショット (Windows) か、`top` (Linux)、`prstat` (Solaris)、または`topas` (AIX) からの出力
- デバッグログ
- Perfmonログ (Windows) または Syslog
- メモリダンプ (Windows) または コアダンプ (Linux、Solaris、AIX)

Deep Security Managerを使用してAgentの診断パッケージを作成する

Deep Security Managerは、Agentの診断パッケージを作成するためにリモートでAgentに接続できる必要があります。Deep Security ManagerがリモートからAgentにアクセスできない場合や、AgentがAgentからのリモート有効化を使用している場合は、Agentから直接診断パッケージを作成する必要があります。

Deep Security Manager を使用して診断パッケージを作成するには、次の手順に従います

1. [コンピュータ] に移動します。
2. 診断パッケージを生成するコンピュータの名前をダブルクリックします。
3. [処理] タブを選択します。
4. [サポート情報] の [診断パッケージの作成] をクリックします。
5. [次へ] をクリックします。

   パッケージの作成には数分かかります。完了すると、概要が表示され、ブラウザが診断情報を含むZIPファイルをダウンロードします。

システム情報が有効になっている場合、非常に大きな診断パッケージが作成され、パフォーマンスに悪影響を与える可能性があることに注意してください。システム情報オプションは、プライマリテナントでない場合や必要な権限がない場合はグレー表示されます。

保護されているコンピュータでCLIを使用してAgentの診断パッケージを作成する

Linux、AIX、またはSolarisの場合:

1. 診断パッケージを生成するサーバに接続します。
2. 次のコマンドを入力します。

   ```
   sudo /opt/ds_agent/dsa_control -d
   ```

   診断パッケージのファイル名と場所が出力されます。`/var/opt/ds_agent/diag`

Windowsの場合:

1. 診断パッケージを生成するコンピュータに接続します。
2. コマンドプロンプトを管理者として開き、コマンドを入力します。

   PowerShellの場合:

   ```
   & "\Program Files\Trend Micro\Deep Security Agent\dsa_control" -d
   ```

   Cmd.exeの場合:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Agent
   ```

   ```
   dsa_control.cmd -d
   ```

   診断パッケージのファイル名と場所が出力されます。`C:\ProgramData\Trend Micro\Deep Security Agent\diag`

DebugViewを使用してデバッグログを収集する

Windowsコンピュータでは、DebugViewソフトウェアを使用してデバッグログを収集できます。

警告: サポートプロバイダから要求された場合にのみ、デバッグログを収集してください。デバッグログの収集中はCPU使用率が増加し、高いCPU使用率の問題が悪化します。

1. DebugViewユーティリティをダウンロードします。
2. セルフプロテクションが有効になっている場合は、無効にします。
3. Trend Micro Deep Security Agentサービスを停止します。
4. C:\WindowsディレクトリにDS_agent.iniという名前のプレーンテキストファイルを作成します。
5. DS_agent.iniファイルに次の行を追加します

   ```
   trace=*
   ```

6. DebugView.exeを起動します。

7. メニューの [Capture] を選択します。
8. 次の設定を有効にします。
    - Capture Win32
    - Capture Kernel
    - Capture Events
9. Trend Micro Deep Security Agentサービスを開始します。
10. DebugViewの情報をCSVファイルにエクスポートします。
11. この手順の最初にセルフプロテクションを無効にした場合は再び有効にします。

詳細な診断パッケージのプロセスメモリを増やす

多数のホスト(たとえば10,000以上)が存在する環境では、診断パッケージの作成中に、詳細な診断パッケージのプロセス(dsm_c.exe)でメモリが不足する場合があります。これを回避するために、詳細な診断パッケージのJVMプロセスに割り当てられたメモリを2GBまで増やすことができます。

1. Deep Security Managerのインストールディレクトリに移動します。
2. 「dsm_c.vmoptions」という名前の新しいファイルを作成します。
3. 作成したファイルを開き、-Xmx2gという行を追加します。

    注意: メモリが2GBでも足りない場合は、上記の行の値を変更して、割り当てられているメモリをさらに増やすこともできます。たとえば、4GBに増やす場合は-Xmx4g、6GBの場合は-Xmx6gとします。

4. ファイルを保存し、dsm_c.exeを実行します。

旧バージョンのソフトウェアの削除

特定の状況において、以前にリリースされたバージョンのソフトウェアへのアクセスを削除することがお客様の最善の利益になると判断する場合があります。私たちは、そのリリースで既知の既知の問題がある場合にのみソフトウェアを削除します。これは、顧客の既知の問題への露出を制限するために行われます。

古いソフトウェアバージョンへのアクセスが削除されると、ダウンロードリンクは、ソフトウェアの削除を引き起こした問題の詳細を記載した「サポート技術情報」(Knowledge Base) の記事へのリンクに置き換えられます。

削除された古いバージョンへのアクセスが必要な場合は、ソフトウェアバージョンと製品Q&Aにサポート担当者にお問い合わせください。

Azure コード署名のトラブルシューティング

Microsoft Windows Agentコンポーネントが[Azureコード署名 (ACS)]で署名されるようになったため、以前のバージョンのWindowsを実行しているコンピュータを[Microsoft KB5022661]パッチでアップデートして、Azureコード署名証明書を識別できるようにする必要があります。このパッチが適用されていない場合、Deep Security Agentのインストールまたはアップグレードが失敗し、Deep Security Managerにその旨の警告が表示されます。

アップグレードに失敗したときに生成されるDeep Security Agentのログの一部を次に示します。

```
MSI (s) (E8:24) [01:16:53:747]: Executing op: ActionStart(Name=_ACSVerification,,)
MSI (s) (E8:24) [01:16:53:747]: Executing op:
CustomActionSchedule(Action=_ACSVerification,ActionType=1025,Source=BinaryData,Target=ACS
Verification,CustomActionData=C:\Program Files\Trend Micro\Deep Security Agent\)
MSI (s) (E8:B0) [01:16:53:747]: Invoking remote custom action. DLL: C:\Windows\Installer
\MSIFC3A.tmp, Entrypoint: ACSVerification
ds_agent [01:16:53:763]: Azure Code Sign Verification Begin ...
ds_agent [01:16:53:763]: Installation property TARGETDIR is C:\Program Files\Trend
Micro\Deep Security Agent\
ds_agent [01:17:05:616]: Azure Code Sign (ACS) Verification Failed (error: 0x577). The KB
for ACS is probably required.
CustomAction _ACSVerification returned actual error code 1603 (note this may not be 100%
accurate if translation happened inside sandbox)
Action ended 1:17:05: InstallFinalize. Return value 3.
```

アップグレードの失敗時に生成されるDeep Security Managerのシステムイベントログの一部を次に示します。

```
After 2023/2/18, agent components on Windows will use Azure Code Signing. If you use an
older Windows version, then you must apply the patch in Microsoft KB5022661 so that
Windows can validate the certificate. Agent installations and upgrades will fail if you
do not apply the update. Consult the install log for the running process:
```

詳細については、トレンドマイクロ Server and Endpoint Protection Agent の 2023年2月以降の更新バイナリに対する最小 Windows バージョン要件をご覧ください。

IoTイベント過負荷アラートのトラブルシューティング

IoTイベントFully overloaded alert (Error: Activation Failed) は、Deep Security Managerが通常よりも長い時間をかけてIoTイベントを処理しているときにDeep Securityに表示されます。

この問題を解決するには、Deep Security Agentが予期せず大量のセキュリティイベントを生成していないか確認してください。

- イベントとレポートでセキュリティイベントを確認し、どのコンピュータが多くのイベントを生成しているかを確認してください。
- それらのコンピュータの設定ミスのあるルールを確認してください。

問題が解決しない場合は、サポートに連絡してください。

SELinuxアラートのトラブルシューティング

SELinuxが有効になっているかどうかを確認するには、`sestatus`コマンドを使用します。

SELinuxがDeep Security Agentサービスをブロックする

SELinuxポリシーが有効に設定されていて、Deep Security Agentサービスがブロックされている場合、次のアラートサンプルがシステム監査ログ `/var/log/audit/audit.log` またはSELinuxログ `/var/log/audit/audit.log` に表示されることがあります。

```
[TIMESTAMP] [HOSTNAME] python: SELinux is preventing [/PATH/BINARY] from 'read, write' accesses on the file /var/opt/ds_agent/dsa_core/ds_agent.db-shm.

***** Plugin leaks (86.2 confidence) suggests ****************************

If you want to ignore [BINARY] trying to read write access the ds_agent.db-shm file, because you believe it should not need this access. Then you should report this as a bug.
```

```
You can generate a local policy module to dontaudit this access.

Do

ausearch -x [/PATH/BINARY] --raw | audit2allow -D -M [POLICYNAME]

semodule -i POLICYNAME.pp
```

この問題を解決するには、以下のようにAudit2allowを使用してカスタムSELinuxポリシーを作成します。

1. rootユーザとしてDeep Security Agentシステムに接続します。
2. 次のコマンドを実行して、Deep Security Agentファイルへのアクセスを許可するカスタムポリシーを作成します。

   ```
   cd /tmp

   grep ds_agent /var/log/audit/audit* | audit2allow -M ds_agent

   semodule -i ds_agent.pp
   ```

3. ds_agentを再起動します。
4. 次のコマンドを実行して、システムメッセージを確認し、ds_agentに関連するアラートがないことを確認してください。

   ```
   cat /var/log/messages | grep ds_agent
   ```

5. アラートが引き続き発生する場合は、手順2からコマンドを再実行して、既存のポリシーをアップデートし、再適用します。

SELinuxポリシーを削除するには、次のコマンドを使用します。

`semodule -r ds_agent`.

Berkeley Packet Filter (BPF) 操作がブロックされる

この問題は、次の状況で発生する可能性があります。

Trend Micro Deep Security(オンプレミス) 20

- AgentのOSがRed Hat Enterprise Linux 7 (64ビット)
- SELinuxが強制モードで有効になっている
- Agentで高度なTLSトラフィック監視機能が有効になっている

以下のようなアラートがシステム監査ログ `/var/log/audit/audit.log` またはSELinuxログ `/var/log/audit/audit.log` に表示されることがあります。

```
type=AVC msg=audit(1682773485.952:1080): avc: denied { map_create } for pid=12807 comm="ds_nuagent" scontext=system_u:system_r:unconfined_service_t:s0 tcontext=system_u:system_r:unconfined_service_t:s0 tclass=bpf permissive=0

type=SYSCALL msg=audit(1682773485.952:1080): arch=c000003e syscall=321 success=no exit=-13 a0=0 a1=c000a25800 a2=2c a3=0 items=0 ppid=12802 pid=12807 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="ds_nuagent" exe="/opt/ds_agent/nuagent/ds_nuagent" subj=system_u:system_r:unconfined_service_t:s0 key=(null)
```

この問題を解決するには、次の手順に従ってカスタムSELinuxポリシーを作成します。

1. rootユーザとしてDeep Security Agentシステムに接続します。
2. `nuagent.te` という名前のType Enforcementファイルを作成します。

   ```
   module nuagent 1.0;

   require {

   type unconfined_service_t;

   class bpf { map_create map_read map_write prog_load prog_run };

   }

   #============= unconfined_service_t ==============

   allow unconfined_service_t self:bpf { map_create map_read map_write prog_load prog_run };
   ```

3. 次のコマンドを実行して、`ds_nuagent` に対するbpfアクセスを許可するカスタムポリシーを作成します。

```
checkmodule -M -m -o nuagent.mod nuagent.te

semodule_package -o nuagent.pp -m nuagent.mod

semodule -i nuagent.pp
```

4. ds_agentサービスを再起動します。

Deep Security Agentバージョン20.0.0-8137以降では、tm_netagentという新しいプロセスのサポートが追加されました。ds_nuagentプロセスは引き続きサポートされており、プロセス名は同じように使用できます。

ネットワークエンジンのステータス (Windows OS)

ネットワークエンジンステータスの警告

ネットワークエンジンステータスの警告は、トレンドマイクロLightWeight Filter Driverに関するイベントをエージェントが生成し、ネットワークエンジンのステータスチェックが有効になっている場合に、コンピュータの [ステータス] 領域に表示される可能性のある警告とエラーの集合です。

次のいずれかの警告が表示された場合は、エージェントのネットワーク機能が無効になっているか、正常に機能していない可能性があります。

- Webレピュテーションエンジンが無効
- ファイアウォールエンジンが無効
- 侵入防御エンジンが無効
- 機能が制限された状態でWebレピュテーションエンジンが動作
- 機能が制限された状態でファイアウォールエンジンが動作
- 機能が制限された状態で侵入防御エンジンが動作

Agentは、影響を受けるネットワークインタフェースごとに、より多くのセキュリティイベントを表示します。詳細については、「ドライバ関連イベント」を参照してください。

ドライバのステータスの確認

ドライバのステータスは、次の方法で確認できます。

1. [コントロールパネル]→[ネットワークとインターネット]→[ネットワークと共有センター] の順に開きます。
2. 左側の[アダプタ設定の変更]を選択して、[ネットワーク接続]を開きます。
3. アクティブな各ネットワークアダプタを右クリックし、[プロパティ] を選択します。
4. [トレンドマイクロ LightWeight Filter Driver]が選択されていることを確認します。

ネットワークエンジンステータスの警告を無効にする

次のようにして、ネットワークエンジンステータスの警告を無効にできます。

1. Deep Security Managerで、[コンピュータ]に移動します。
2. 警告を無効にするコンピュータを選択し、[詳細] をクリックします。
3. コンピュータの詳細画面で、[設定] → [詳細] → [ネットワークエンジンの設定]の順に選択します。
4. [ネットワークエンジンステータスチェック]で、[無効]を選択します。

PDF

Deep Security管理ガイド

このDeep Security管理ガイドは、Deep SecurityヘルプセンターのPDFバージョンです。フォントや表示形式に乱れが発生している場合があります。

Deep Security 20管理ガイドを開く

Deep Securityのベストプラクティスガイド

Deep Security Best Practice Guideは、製品の生産性を最大限に引き出すのに役立つ情報を提供します。エンタープライズ規模の導入事例、ラボでの検証、現場で得られた教訓など、これまでに培われた知識に基づくベストプラクティスを紹介しています。事例や注意事項はあくまでも指針であり、厳格な設計要件ではありません。これらのガイドラインはすべての環境に適用されるわけではありませんが、Deep Securityを最適なパフォーマンスで設定するために必要な決定の手引きに役立ちます。

Deep Security 20のベストプラクティスガイドは現在 でPDF形式の で利用でき、次の内容が含まれています。

- 導入に際しての注意事項と推奨事項
- アップグレードのガイドラインとシナリオ
- サイジングの注意事項と推奨事項
- システムのパフォーマンスを最大化し、管理の手間を削減するための推奨設定
- VDI、プライベート、およびパブリッククラウド環境でのベストプラクティスのヒント