

Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド 2019 年 12 月 27 日 第 1.0 版

> トレンドマイクロ株式会社 セールスエンジニアリング部

VMware NSX-T Data Center & Trend Micro Deep Security インテグレーションガイド

~エージェントレスセキュリティとマイクロセグメンテーション~

[VMware NSX-T Data Center 2.4/2.5.0 + Deep Security Virtual Appliance 12.0 対応]



VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

Public

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

TRENDMICRO、ウイルスバスター、ウイルスバスター On-Line-Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL, ISVW, InterScanWebManager, ISWM, InterScan Message Security Suite, InterScan Web Security Suite, IWSS, TRENDMICRO SERVERPROTECT, PortalProtect, Trend Micro Control Manager, Trend Micro MobileSecurity、VSAPI、トレンドマイクロ・プレミアム・サポート・プログラム、License for Enterprise Information Security, LEISec, Trend Park, Trend Labs, InterScan Gateway Security Appliance, Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、LEAKPROOF、Trend プロテクト、Expert on Guard、 InterScan Messaging Security Appliance, InterScan Web Security Appliance, InterScan Messaging Hosted Security, DataDNA, Trend Micro Threat Management Solution, Trend Micro Threat Management Services, Trend Micro Threat Management Agent, Trend Micro Threat Mitigator, Trend Micro Threat Discovery Appliance, Trend Micro USB Security, InterScan Web Security Virtual Appliance, InterScan Messaging Security Virtual Appliance, Trend Micro Reliable Security License, TRSL, Trend Micro Smart Protection Network, Smart Protection Network, SPN, SMARTSCAN, Trend Micro Kids Safety, Trend Micro Web Security, Trend Micro IM Security, Trend Micro Email Encryption, Trend Micro Email Encryption Client, Trend Micro Email Encryption Gateway, Trend Micro Collaboration Security, Trend Micro Portable Security, Portable Security, Trend Micro Standard Web Security、トレンドマイクロ アグレッシブスキャナー、Trend Micro Hosted Email Security、Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、ウイルスバスターCLOUD、Smart Surfing、 スマートスキャン、Trend Micro Instant Security、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways, Trend Micro Email Security Platform, Trend Smart Protection, Vulnerability Management Services, Trend Micro Vulnerability Management Services, Trend Micro PCI Scanning Service, Trend Micro Titanium, Trend Micro Titanium AntiVirus Plus, Smart Protection Server, Deep Security, Worry Free Remote Manager、ウイルスバスター ビジネスセキュリティサービス、HOUSECALL、SafeSync、トレンドマイ クロ オンラインストレージ SafeSync、Trend Micro InterScan WebManager SCC、Trend Micro NAS Security、 Trend Micro Data Loss Prevention, TREND MICRO ENDPOINT ENCRYPTION, Securing Your Journey to the Cloud、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security PCI DSS, Trend Micro Deep Security Virtual Patch, Trend Micro Threat Discovery Software Appliance, SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Trend Micro Deep Security あんしんパック、こども一ど、Deep Discovery、および TCSE は、トレンドマイクロ株式会社の登録商標 です。

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



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

改定履歴

| Revision | No. | Date | Change | Author |
|----------|-----|------------|--------|-------------|
| 1.0 | | 2019/12/27 | 初版作成 | Trend Micro |
| | | | | |
| | | | | |
| | | | | |
| | | | | |



| 目次 | |
|--------------------------------------------------------------|-----|
| はじめに | 6 |
| 本ガイドについて | 6 |
| 用語について | 6 |
| 本ガイドの作成時の検証バージョン | 6 |
| 1. Deep SecurityとVMware NSX について | 7 |
| 1.1. Deep SecurityとVMware NSX 連携ソリューション | 7 |
| 1-1-1. Deep SecurityとVMware NSX の連携メリット | 7 |
| 1−1−2. DSVA による仮想マシン要塞化とNSX セキュリティタグを利用した分散ファイアウォールによ | る自動 |
| 隔離 | 8 |
| 1−2. システム要件および互換性の確認 | 8 |
| 1-3. コンポーネントの概要 | 9 |
| 1−3−1. 各コンポーネントの役割 | 9 |
| 1−3−2. コンポーネント間の関係性 | 12 |
| 1−3−3. Deep Security 管理コンポーネントの構成と配置 | 13 |
| 1-4. 構築時にチェックするべき点 | 16 |
| 1-4-1. 通信要件と時刻同期 | 16 |
| 1−4−3. NSX ライセンスと Deep Security のセキュリティ機能 | 18 |
| 1-4-4. NSX-T 環境における DSVA 展開の前提条件と把握しておくべき事項 | 18 |
| 1-4-5. NSX Data Center for vSphereとNSX-T Data Centerの相違点 | 19 |
| 1-4-6. NSX-T 2.5.0 以降のセキュリティ VM 配信時の仕様変更に伴う DSVA ソフトウェアパッケージ | の変更 |
| | 19 |
| 2. VMware NSX 環境における DSVA エージェントレスセキュリティ保護環境の構築手順 | 22 |
| 2−1. 本構築ガイドにおける事前準備しておくべき環境と想定環境 | 22 |
| 2−2. 本ガイドで想定する環境 | 23 |
| 2−3. エージェントレスによる仮想マシン保護 構築手順 | 24 |
| 2−3−1. DSM 用 SQL サーバ構築 | 25 |
| 2–3–2. Deep Security Manager(DSM) インストール | 35 |
| 2−3−3. NSX ファブリック設定 – NSX Manager への vCenter Server の登録 | 45 |
| 2−3−4. NSX ファブリック設定 – トランスポートゾーンの設定 | 47 |
| 2−3−5. NSX ファブリック設定 – トランスポートノードプロファイルの設定 | 49 |
| 2−3−6. NSX ファブリック設定 – トランスポートノードプロファイルの vSphere クラスタへの適用 | 51 |
| 2−3−7. DSM&vCenter Server▪NSX Manager 連携設定 | 54 |
| 2–3–8. DSVA デプロイ | 58 |
| 2−3−9. Deep Security 基本設定とセキュリティポリシーの策定 | 65 |
| 2-3-10. 保護対象仮想マシンへの VMware Tools 及び Notifier のインストール | 70 |
| 2−3−11. エンドポイントの保護を設定 NSX セキュリティポリシー・セキュリティグループ作成 | 73 |
| 2-3-12. 仮想マシン展開時の有効化の確認とセキュリティ機能の検証 | 83 |



| 2-4. セキュリティタグを利用した自動隔離の考え方と設定手順85 |
|---------------------------------------------------|
| 2-4-1. セキュリティタグと分散ファイアウォールを利用した自動隔離の仕組み85 |
| 2-4-2. Deep Security NSX セキュリティタグ追加設定 86 |
| 2-4-3. 不正プログラム対策イベント 即時通知の設定 88 |
| 2-4-4. 分散ファイアウォールと連携した自動隔離設定 89 |
| 3. 設計・導入時に留意するべきポイント |
| 3-1. 設計上留意しておくべきポイント 97 |
| 3-1-1.システム全般 |
| 3-1-2. セキュリティ VM の特性 |
| 3-1-3. Deep Security が付与する NSX セキュリティタグの特性 |
| 3-2. 導入時に留意しておくべきポイント |
| 3-2-1. DSVA リソースチューニング後の OVF ファイルの更新 |
| 3-2-2. マルチノード DSM の導入手順 100 |
| 3-3. 管理サーバ群を DSVA で保護する場合の考慮事項 106 |
| 3-4. 仮想デスクトップ環境における NSX、DSVA のサイジング 107 |
| 3-4-1. DSM サーバのサイジング指標 107 |
| 3-4-2. DSM 用 SQL サーバのサイジング指標 109 |
| 3-4-3. DSVA のサイジング指標 |
| 3-4-4. DSR のサイジング指標 |
| 4. 参考資料 |



はじめに

本ガイドについて

本ガイドは、VMware NSX-T Data Center 環境にて、エージェントレスによるセキュリティ保護を目的として Trend Micro Deep Security 12.0 を導入する際のトレンドマイクロが推奨する構成、設定手順および関連情報を取りまと めたものです。

また、特に関連性の深い VMware NSX Manager、Guest Introspection Service、分散ファイアウォールについての仕組み、構築にあたって知っておくほうがよいと思われる事項についても記載しています。

(VMware NSX-T Data Center を前提として記載をしており、VMware NSX for vSphere については本ガイドでは 触れておりません。)

なお、本ガイドに記載されている内容については、あくまで弊社での実績を元に指標となる内容をまとめて記載 をしています。実環境における性能、動作を必ずしも保証するものではありません。また、お客様環境、要件によ っては弊社エンジニアおよびサポート担当より異なる設定、推奨内容の提案、提示がされる場合があります。

用語について

本ガイドでは、特別に必要な場合を除いて、下記の略称を使用します。 「Trend Micro Deep Security」→「DS」 「Deep Security Manager」→「DSM」 「Deep Security Agent」→「DSA」 「Deep Security Relay」→「DSR」 「Deep Security Virtual Appliance」→「DSVA」 「VMware vSphere」→「vSphere」 「VMware vCenter Server」→「vCenter Server」 「VMware ESXi」→「ESXi」 「VMware NSX-T Data Center」→NSX-T

本ガイドの作成時の検証バージョン

VMware vSphere 6.7.0 VMware NSX-T Data Center 2.4.2 (一部 2.5 に添った記載を追記) Deep Security 12.0



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

1. Deep Security と VMware NSX について

1.1. Deep Security と VMware NSX 連携ソリューション

1-1-1. Deep SecurityとVMware NSX の連携メリット

Deep SecurityとVMware NSX を組み合わせて導入することにより、サーバ・ネットワークの仮想化により効率化 されたプラットフォーム環境に対して、運用性を担保しながら必要なセキュリティを柔軟に提供することが可能と なります。

特に VMware Horizon などで仮想マシンが展開される仮想デスクトップ環境では、エージェントレスでのセキュリ ティ実装と多くの仮想マシンに対する均一なセキュリティサービスを提供できます。

Deep Security と VMware NSX の連携によるメリットは以下のとおりです。

- > VMware NSX の分散ファイアウォールによる仮想マシン毎にきめ細やかなアクセス制御の実現
- Deep Security による仮想マシンの要塞化の実現



仮想マシンにエージェントを導入しないエージェントレス型の採用によるセキュリティレベルの統一 とユーザにとってストレスフリーな利便性の両立

vCenter Server と Deep Security Manager のインベントリ情報の同期によって、仮想環境のリソース変化による仮想マシンのホスト間移動へのシームレスなセキュリティ適用の継続とセキュリティ機能の実装状況の可視化

- Deep Security のセキュリティイベント検出時に NSX セキュリティタグを付与することで、仮想マシンに適用される分散ファイアウォールの付け替えによる自動隔離を実現するとともに、一次対処の迅速化と運用負荷の軽減が可能 (物理環境において、ウイルス検出をした際に LAN ケーブルを抜線する運用を自動化するイメージ)
- 2019 年 12 月時点では、VMware NSX-TとDeep Security のポリシー連携が不可のため、仮想マシン生成時に適切なセキュリティポリシーを自動適用する場合には、DSM でイベントベースタスクを別途設定する必要があります。



VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

Public

1-1-2. DSVA による仮想マシン要塞化とNSX セキュリティタグを利用した分散ファイアウォールによる自動隔離 DSM にてある仮想マシンでセキュリティイベントが検出された際に NSX セキュリティタグを付与するオプションを 設定しておくことにより、Deep Security のイベントをトリガーとして該当する仮想マシンの属性(所属するセキュリ ティグループ)をセキュリティタグによって変更することによって、適用されるファイアウォールポリシーを変更する ことが可能となります。



実装方法については、以下のセクションを参照してください。

2-4. セキュリティタグを利用した自動隔離の考え方と設定手順

1-2. システム要件および互換性の確認

設計及び導入を行う前にお使いの環境が DS12.0 のシステム要件、および VMware 関連ソリューションとの互換 性を満たしているか確認する必要があります。

以下にソリューション間の互換性の関係性を記載します。





詳細の互換性情報については以下のページをご確認ください。

■ DS12.0のシステム要件

<u>http://www.trendmicro.co.jp/jp/business/products/tmds/index.html?cm_sp=GNav-_-Business-_-tmds#requirement</u> ※システム要件を満たしていないコンピュータでの動作検証は行っていない為、サポート対象外となります。

■ Deep Security Virtual Appliance と VMware 製品の互換性対応表

http://esupport.trendmicro.com/solution/ja-jp/1314170.aspx

■ Deep Security and VMware compatibility matrix(VMware各コンポーネントの対応互換表)

http://www.vmware.com/resources/compatibility/sim/interop_matrix.php

■ VMware Compatibility Guide (VMware ESXiに対するDSVAを含む3rd Party製品の互換対応表)

1-3. コンポーネントの概要

1-3-1. 各コンポーネントの役割



<NSX 環境における Deep Security Virtual Appliance 基本構成>

Copyright (c) 2019 Trend Micro Incorporated. All rights reserved.



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

Trend Micro Deep Security

Deep Security Manager (DSM)

Deep Security Manager (DSM)は、Web ベースの強力な中央管理システムです。DSM は、データベースを使用しており、セキュリティ管理者が実行する包括的なセキュリティポリシーの作成や管理、記録(ログ)を集中的に管理します。また、状況を把握するためのダッシュボードやレポートの作成、サーバに対するタスクを 作成するなど、Deep Security におけるすべての管理処理を実行します。なお、データベースについては構成によって、DSM と同じ OS 上に構築する場合と、DSM 用のデータベースを別 OS 上で構築する場合があ ります。

Deep Security Agent (DSA)

Deep Security Agent (DSA)は、最小限のリソースで最大限のセキュリティ保護を提供するソフトウェアで、 仮想マシンの OS 上に直接インストールされ動作することで、Deep Security で提供されるほぼすべてのセ キュリティ保護機能を一括で提供できます。また、DSA をリレー化することによって DSR として機能させるこ とも可能です。

> Deep Security Virtual Appliance (DSVA)

Deep Security Virtual Appliance(DSVA)は、仮想化環境で実行されるセキュリティコンポーネントです。 Agent が直接仮想マシンの OS 上にインストールされるのに対して、DSVA は VMware NSX と連携し、 VMware ESXi 上で実行される仮想アプライアンスとして動作し、ESXi ホスト上の他の仮想マシンの OS 上に セキュリティソフトウェアをインストールすること無く、エージェントレスによる Deep Security のセキュリティ機 能を提供することができます。

Deep Security Relay(DSR)

Deep Security は新たな脅威に対応するため、Deep Security ソフトウェアやウイルスパターンファイル、侵入防御シグネチャなどを日々アップデートする必要があります。Deep Security システムにおいて、コンポーネントのアップデートを実行するのが Deep Security Relay(DSR)です。DSR はインターネット上から最新コンポーネントをダウンロードし、DSA および DSVA に配信します。そのため、DSR はシステム全体で最低 1 台は必要となります。

DSR は DSA の一機能として該当の DSA をインストールされたコンピュータを Relay Group に所属させるこ とにより Relay 機能を有効化します。通常は DSM と DSR を同居させてください。また、DSVA 環境では仮想 マシンに対する一部の設定情報を DSR 同士でやりとりする場合があります。複数の Relay Group を作成す る場合には、DSVA の配信するホストの範囲と DSR の Relay Group が合致するように設定するようにしてく ださい。

> Notifier

DSVA で保護されている仮想マシン(Windows)内で動作します。Notifier をインストールしていると不正プロ グラムをブロックしたとき、または不正な Web ページにアクセスしたときなどに、ユーザにポップアップ通知 が表示されます。Notifier がクライアントマシン上で占有するスペースは小さく、必要なディスク容量は 1MB 未満、メモリサイズは 1MB 未満です。

Smart Protection Server(SPS:オプション)

Smart Protection Server(SPS)は、Web レピュテーションおよびファイルレピュテーションのデータベースを ローカルに保持するための仮想アプライアンスです。SPS は社内ネットワークに構築され、トレンドマイクロ



がクラウド提供している Smart Protection Network(SPN)と連携します。DSA や DSVA は SPS を参照して Web レピュテーションおよびファイルレピュテーションの機能を提供します。

■ VMware

➢ ESXi(ハイパーバイザ)

ESXi は ハイパーバイザ型仮想化ソフトウェアのことであり、ホスト OS の代わりにハードウェア上で直接 動作し、ESXi 上でゲスト OS を複数台動作させることが可能です。NSX-T 環境では ESXi ホストは Transport Node の1つとして管理されます。

vCenter Server

vSphere 環境において、各 ESXi ホスト、仮想マシンの管理、機能の有効化・リソース監視などの統合管理 を実現します。管理者は vCenter から、ESXi や仮想マシンの状態をリアルタイムに確認し、仮想マシンの デプロイやスマップショットの取得、バックアップ等も実行することができます。NSX-T 環境で Deep Security を展開する場合には、予め NSX Manager から vCenter Server をコンピュートマネージャとして登録しておく 必要があります。

NSX Manager

NSX Manager はすべての NSX コンポーネントの管理を実施する管理サーバとして動作します。DSVA の 展開に必要となる Transport Node Profile (N-VDS)の ESXi への展開、セキュリティポリシーの作成、DSVA の展開を NSX Manager から行います。また、NSX Manager は本番環境では 3 台をクラスタとして展開する ことが必要となります。

Guest Introspection Service

Deep Security などサードパーティ連携機能を使用する場合に各 ESXi ホストに配信される分散型のサービ スモジュールです。エージェントレスにて主に不正プログラム対策などを行う際に各仮想 OS から DSVA へ 検索対象などの情報をオフロードする際にハイパーバイザ間のやりとりを許可するためのコネクション管理 機能を担います。

> VMware Tools VMCIドライバ - NSX ファイル自己検証ドライバ

エージェントレスで仮想マシンの不正プログラム対策などを行う際に保護対象の仮想マシンにこのドライバ をインストールすることで、仮想マシンで検出されるファイルへのアクセス情報を ESXi 経由で DSVA へ連携 します。(VMware Tools の VMCI ドライバとして統合されています。)

ファイアウォール、侵入防御、Webレピュテーション機能を利用する場合には直接このコンポーネントは利用 されません。

VMware Tools についても vSphere/NSX とのバージョン依存があるため、互換性の確認を必ず行う必要があります。

NSX 分散スイッチ(N-VDS)

複数の ESXi ホストをまたがって構成する NSX 仮想スイッチで、Transport Node でスイッチング機能を実行 する NSX ソフトウェアコンポーネントです。

N-VDS は vCenter Server 上で仮想スイッチとして生成されますが、vSphere 環境で生成される標準仮想ス イッチ(vSS)、分散仮想スイッチ(vDS)とは異なる属性を持ち、vCenter Server からは設定変更などを行うこ とができません。また、vSS または vDS から N-VDS へ移行することはできず、独立管理されています。



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

DSVA を配信は必ず N-VDS が展開された Transport Node に対して行う必要があります。

1-3-2. コンポーネント間の関係性

- ・ vCenter ServerとNSX Manager は 1:1 で対応させる必要があります。
- DSM(データベースインスタンス単位)は、該当クラスタの ESXiホストと仮想マシンのインベントリ情報やセッション情報を管理するために vCenter Server、NSX Manager が 1:1 で同期する必要があります。
- 保護対象の仮想マシンが配置される各 ESXi ホストに対して、Guest Introspection、DSVA をそれぞれ配信する必要があります。



<NSX · Deep Security コンポーネントの関係性>

コンポーネント間の関係性からも分かるとおり、DSVA を利用したエージェントレス型セキュリティ対策は NSX と の連携がキーとなっており、仮想デスクトップの展開方式には依存していません。 Horizon によるフルクローン、リンククローン、インスタントクローンに関わらず適用することが可能です。 (展開方式によって仮想マシンの展開スピードが異なるため、サイジング、チューニングが必要になります。)



1-3-3. Deep Security 管理コンポーネントの構成と配置

Deep Security を機能させるためには、必ず DSM、DSR を配置する必要があります。NSX 環境において DSVA を展開する際の標準的な構成と配置について以下に解説します。

Deep Security Manager (DSM)

DSM が管理するセキュリティポリシー、インベントリ情報、イベント情報などすべての情報はデータベースに格納 されます。DSM ソフトウェアパッケージにはデータベースは含まれておらず、事前に Microsoft SQL、Oracle また は PostgreSQL のデータベースを準備しておく必要があります。データベースは DSM をインストールするサーバ に同居させることも可能ですが、VDI 環境など一定規模以上での展開を行う場合、DSM を 2 台構成以上で接続 する場合には、データベースは別サーバで構築することを推奨します。

NSX 環境において、DSM を複数ノードで構成する場合、以下の点を留意して設計してください。

DSMを2台以上で構成する場合には、各DSMからデータベースサーバに対して同ーインスタンスへ接続させる ことで同一の情報を参照することで、DSMの負荷分散、冗長性の担保がされます(データベースの冗長化は別 途検討する必要があります)。

複数 DSM ノードと vCenter Server の同期

最後にデータベース接続された DSM が vCenter Server との同期処理を実行します(設定による変更は不可)。



<複数 DSM ノード構成時の vCenter Server とのコネクション>

Copyright (c) 2019 Trend Micro Incorporated. All rights reserved.

Securing Your Journey to the Cloud

を 複数 DSM ノードと NSX Manager の同期

デフォルトでは最初にデータベース接続された DSM は、NSX Manager とのコネクション処理を行うとともに、 NSX Manager 経由で vCenter Server から DSVA を配信する際に DSVA の ovf ファイルの格納先としても指 定されます。NSX Manager との同期する DSM は、以下の設定で変更可能です。

| [管理]>[システム設定]> | ▶[詳細]>[NSX 通信の Managerノ | 'ード] |
|----------------|-------------------------|------|
|----------------|-------------------------|------|

| 🕖 IREND Deep Securit | Y MasterAdmin - ⑦ ヘルブ ⑦ サポート情報 ■ - Q ヘルブセンターの検索 | |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|----|
| ダッシュボード 処理 アラート | イベントとレポート コンピュータ ポリシー 管理 | |
| 🏟 システム設定 | システム設定 | |
| 📓 予約タスク | | |
| 📓 イベントベースタスク | アッフテート スマートフィートハック Connected Threat Defense SMTP ストレージ フロキシ 計組 使業キャッシュ設定の表示 | • |
| 🕖 Managerノート" | | |
| 57EVZ | TE 実践定め 快来 FOO FOR M-F CPU使用率レベルを下げると、ファイル検索間の待機時間が長くなり、CPUリソースの消費を抑えることができます。 | |
| ~ 📢 ユーザ管理 | CPU使用率L ベル: 高 🔹 | |
| 🏭 ユーザ | (通考) この設定は、Deep Security Managerの推奨設定の検索プロセスで使用されるCPUリンースにのみ影響します。Dee Security Managerで案行されているその他のプロセスは、引き続きCPUの会計負荷に影響します。 | *p |
| ▲ 役割 | | |
| ■ 連絡先 | NSX | |
| ② システム情報 | NSX0#1EU/Manager2~F: dsm01.trendnsx.local dsm01.trendnsx.local | |
| ∨ 🌒 アップデート | 미그 dsm02.trendnsx.local DSM03.trendnsx.local | |
| > 🔒 セキュリティ | ロゴのインボート ロゴのワセット | |

<複数 DSM ノード構成時の NSX Manager と同期する DSM の設定>

Deep Security Relay (DSR)

DSR については、通常 DSM と同一サーバに同居するケースが一般的です。構成にあたっては以下の点に留意 して設計してください。

- > インターネットへの接続性の確保
 →SPN からのパターンファイル、ルール(DSRU)のダウンロード
- 通常のパターンやコンポーネントのダウンロード機能に加え、vMotion/DRS 実行時に移動する仮想マシンのポリシーを DSVA 間で移行する際にも利用されます。そのため、VDI 環境などで仮想マシンの移動が多く見込まれる環境では最低でも DSM ノード数と同数(DSM ノードと同居を推奨)、またはそれ以上の DSR を配置してください。
- DSR は必ず Relay グループに所属する必要があります。Relay グループに DSR を所属させることにより、 サービスを提供する DSVA(及び DSA)を規定します。通常は DSM をインストール時に生成される「初期設 定の Relay グループ」を利用することで問題ありません。大規模環境な VDI 環境において VDI グループ単 位で分割したい場合や DSM に同居した DSR が直接インターネットへ接続できず、SPN からのダウンロード 専用に DSR を別セグメントに配置したい場合(DSR の多段構成)などに複数の Relay グループを作成する ことも可能です。



<複数 DSM ノード構成と Relay グループ>

> DSM/vCenter Server/NSX Manager 管理マネージャ群の基本構成

NSX 環境で DSVA を展開する上では、DSM が vCenter Server と NSX Manager が常にリアルタイムかつ安定的にコネクションをされている必要があります。それにより、仮想マシンの生成、移行(vMotion 及び DRS など)、仮想マシン単位(NSX ではセキュリティグループ単位)でのポリシーの管理を行うことが可能となります。



<管理マネージャ群の基本構成>

また、上記管理マネージャ群の基本構成を踏まえて、DSVA を配信するプロダクションのクラスタ(または NSX-T における Transport Zone)を設計してください。仮想デスクトップ環境のようにフローティング方式で仮想マシンが



展開・削除が繰り返される環境の場合、または、仮想マシンの集約率が高い環境では、複数の vCenter Block を 1 セットの DSM セットで管理することは、パフォーマンス面から推奨していません。



※NSX-T 環境では、NSX Manager が複数の vCenter Server と連携(コンピュートマネージャとして登録)する ことで

1:N での構成を組むことが可能となりました。ただし、Deep Security 12.0 では、NSX Manager と vCenter Server が 1:N で構成された環境で DS を構成することはできません。(12.5:Feature Release で(FR)対応 していますが、サポート期間が通常のメジャーリリース(Long Term Support)に比べると短くなっていますの で、ご注意ください。NSX Manager と vCenter Server が 1:N で構成された環境への対応は次期メジャーリ リースを予定しています。)

1-4. 構築時にチェックするべき点

1-4-1. 通信要件と時刻同期

Deep Securityを導入する際には、各コンポーネント間で指定の通信が許可されている必要があります。

> Trend Micro Deep Security コンポーネント間の通信ポート

以下の FAQ をご参照ください。

Trend Micro Deep Security の使用通信ポート

http://esupport.trendmicro.com/solution/ja-jp/1313476.aspx

Deep Security ヘルプセンター

https://help.deepsecurity.trendmicro.com/ja-jp/Manage-Components/ports.html



Frend Micro Deep Security とVMware コンポーネント間の使用通信ポート

DSM から vCenter Server、NSX Manager に対しては TCP443 でアクセスできることが必要となります。また、 NSX 環境では、各 ESXi ホストへの Guest Introspection Service コネクションをハンドルする Multiplxer に 紐づく Kernel Module と DSVA のコネクションは ESXi ホスト上に内部コネクション用の仮想スイッチ (vmservice-vswitch)を通して行われます。vmservice-vswitch は自動的に生成されます。この仮想スイッチ のポートグループ、IP アドレス、ポート番号は手動で変更する必要はありません。

| o esx-sv01.trendnsx.local アクション マ | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| サマリ 監視 設定 権限 仮想マシン データストア ネットワーク アップデート | |
| ストレージアダプタ ストレージアダプタ ストレージデバイス ホストキャジュの オストキャジュの オストキャジュの オストキャンシュの 信準スイッチ: vSwitch1 | ネットワークの追加 更新 ▲ |
| ノロトコルエントホ //のフィルタ ✓ 標準スイッチ: vmservice-vswitch ネットワークの追加 編集 物理アダ ・ ネットワーク ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ | プタの管理 … |
| VMkernel アダプタ 物理アダプタ TCP/IP設定 シレAN ID: マレMkernel ポート(1) | 物理 <i>アダプタ</i> 物理ネットワーク アダプタはありません |
| ✓ 仮想マシン 仮想マシンの起動/シ | |
| エージェント仮想マ ♀ vmservice-vshield-pg •••• 仮想マシンのデフォ VLAN ID: スワップ ファイルの ∨ 仮想マシン (1) | |
| ◆ ジステム オイセンス ホマトプロファイリ、 | |

<vmwervice-vswitch イメージ図>

▶ 名前解決

Deep Security を利用する環境においては、コンポーネント間の通信において名前解決が可能な設計を行う 必要があります。また、ローカル環境での名前解決をスムーズに行えるようにするため、DNS サフィックスに ローカルドメインを規定しておくことを推奨します。

> ハートビート

DSMとDSVA/DSAの間ではステータス管理のため、10分毎(デフォルト:最短1分に変更可能)にハートビート通信を行っています。DSM⇔DSVA間のハートビートは双方向通信(デフォルト)が必須となりますので、 ハートビートの通信方向の変更を行わないようにしてください。

▶ 時刻同期

Deep Security の環境構築においては、システム間の連携が重要となること、イベントログの正確な取得の ためにシステム全体を NTP による時刻同期を計ることが重要です。また、Deep Security Manager の OS の システム時間は、データベースコンピュータの時間と同期している必要があります。コンピュータの時間がデ ータベースの時間と 30 秒以上前後すると、Manager 管理コンソールの [アラートステータス] ウィジェットに このアラートが表示されます。NTP の設定においては、タイムゾーンが一致するように同一の NTP ソースを 指定するようにしてください。



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

1-4-2. DSM を vCenter Server/NSX Manager と同期する際に必要な権限

DSM を vCenter Server と同期する際にユーザが必要とする権限 以下の FAQ をご参照ください。 vCenter Server との同期に使用するユーザに必要な権限 <u>http://esupport.trendmicro.com/solution/ja-JP/1313306.aspx?print=true</u>

> DSM を NSX Manager と同期する際にユーザが必要とする権限

Enterprise Administrator ロールの割り当てが必要です。(NSX Administrator ロール以下の権限では同期 はできません。)

1-4-3. NSX ライセンスと Deep Security のセキュリティ機能

DSVA によるエージェントレスでのセキュリティ機能の提供を行う場合には、VMware NSX のコンポーネントと連携をする必要があります。NSX のライセンスによって DSVA で提供することができるセキュリティ機能が異なりますので、留意が必要です。

| NSXライセンス | 不正プログラム 対策 | 変更監視 | DSポリシー 連携 | セキュリティタグ NSXと連携した 自動隔離機能 | 侵入防御 ファイアウォール | Web レピュテーション | セキュリティ ログ監視 | アプリケーション コントロール |
|-----------------------------|---------------|---------------|---------------|--------------------------------|------------------|-----------------|----------------|--------------------|
| Standard Professional | × | %1 | ※2 | × | %1 | %1 | ※1 | %1 |
| Advanced Enterprise plus | 0 | ※1 | ※2 | 0 | ※1 | ※1 | ※1 | ※1 |

| 記号 | 対応状況 |
|-----|--------------------------------------------------------------------------------------------------------------------------------|
| 0 | 対応可能。 |
| 0 | Windows OS に対して、Deep Security Virtual Appliance (=DSVA) と Deep Security Agent (=DSA) 双方で利用可能。 Linux OS に対しては、DSA のみ対応可能。 |
| 1 | DSAで利用可能。 |
| ∆%2 | イベントベースタスクで仮想マシン生成時の有効化、 ポリシー適用を代替可能。 |
| × | 対応不可。 |

NSX-T 2.4 及び 2.5.0 と Deep Secuiry 12.0 において実現できるエージェントセキュリティ機能は以下の通りです。

- NSX-T Manager & vCenter Server 連携による仮想マシン情報の取得
- VMware ESXi に対して NSX-T を展開することで DSVA によるエージェントレス型不正プログラム対策を 提供 ※Windows OS のみ
- 不正プログラム対策イベント検出時の NSX-T Manager への NSX セキュリティタグの付与

1-4-4. NSX-T 環境における DSVA 展開の前提条件と把握しておくべき事項

NSX-T を展開した ESXi に対して DSVA によるエージェントレス型セキュリティ保護を提供するためには事前に NSX Transport Node Profile を適用しておく必要があります。

- DSVA が展開できる NSX-T 環境は、VMware ESXi のみ(KVM は現時点では対応不可)
- DSVA によるエージェントレスセキュリティを展開するためには、保護対象仮想マシンをNSX-T で指定する Transport Zone で指定された Overlay または VLAN ネットワークに配置



 ESXi ホストでは Transport Node Profile をベースにホスト上へ N-VDS(NSX 仮想スイッチ)を生成、 Transport Zone の物理アップリンクポートを指定



1-4-5. NSX Data Center for vSphere とNSX-T Data Center の相違点

DSVA の展開にあたり、NSX-T 環境では NSX Data Center for vSphere とは仕様面で違いがあります。相違点を理解した上で設計を行う必要があります。

- セキュリティ仮想アプライアンス(SVM)としての Guest Introspection 廃止
 - NSX-T Manager から各 ESXi ホストに展開される Guest Introspection Service によってエージェントレス型ウイルス対策(エンドポイントセキュリティ)を提供
- NSX-T サービスは NSX-T Manager から直接管理を行うため、vCenter Server を中心とした管理体系から NSX-T Manager GUI による管理へ変更
 - ▶ NSX-T Manager から vCenter Server をノード登録
 - ➢ 各仮想マシンの NSX サービスステータスは NSX-T Manager で管理
- vCenter Server では仮想マシンの NSX セキュリティグループやセキュリティタグは表示できない
- NSX-T セキュリティプロファイル(ポリシー)に対する Deep Security ポリシーの連携は未対応
- NSX-T2.4 より NSX-T Manager に Controller が内蔵されたことにより、商用利用では NSX-T Manager を 3 セット構築することが必要
 - ▶ DSM からの登録は NSX-T Manager Cluster VIP を設定することを推奨
- NSX for vShield Endpoint 相当のライセンスなしでの DSVA 展開は不可

1-4-6. NSX-T 2.5.0 以降のセキュリティ VM 配信時の仕様変更に伴う DSVA ソフトウェアパッケージの変更

VMware NSX-T Data Center(以下 NSX-T)2.5 から Trend Micro Deep Security Virtual Appliance(以下 DSVA) を含めた VMware NSX Guest Introspection を利用する 3rd Party Security VM をデプロイする際の仕様に変更 がありました。この NSX-T 2.5 における Guest Introspection 関連の仕様変更により DSVA パッケージの仕様変 更、DSVA デプロイ手順についても変更があります。



■NSX-T 2.5 Guest Introspection の仕様変更の概要

NSX-T 2.5 における Guest Introspection の仕様の変更により、DSVA など 3rd Party Security VM を各ホストへ デプロイする際に NSX Manager がソフトウェアパッケージに対するデジタル署名のチェックを実行するプロセス が追加されています(ソフトウェアパッケージに含まれる.ovf 及び.vmdk ファイルに VMware 社によるデジタル署 名が付与されます)。この仕様変更に伴い、DSVA を NSX-T 環境でデプロイする際に以下の影響が発生しま す。

- ・ VMware 社によってデジタル署名がされたソフトウェアパッケージのみが NSX-T 環境にデプロイできる
- Deep Security Manager(以下 DSM)DSM へ DSVA ソフトウェアパッケージをアップロード後、DSM 上で 事前に DSVA に割り当てる vCPU 及びメモリの指定を実施することができない

■NSX-T2.5 以降の DSVA の展開方法について

NSX-T2.5 以降では VMware 社によりデジタル署名された DSVA ソフトウェアパッケージを利用してデプロイをす る必要があります。

ー方で従来 DSVA のソフトウェアパッケージ内の OVF ファイルはメジャーリリース毎に 1 つずつ提供されていま したが、今回の NSX-T Guest Introspection に関する仕様変更に伴い、デプロイ前に DSVA OVF ファイルの割 り当て vCPU 及びメモリを指定することができなくなりました。

上記の観点から、トレンドマイクロでは今後リリースする DSVA のソフトウェアパッケージでは以下の4種類の OVF が提供される方針に変更されます。

| OVF Files | vCPU | Memory |
|-----------------|------|---------|
| dsva.ovf | 2 | 4096MB |
| dsva-small.ovf | 2 | 8192MB |
| dsva-medium.ovf | 4 | 16384MB |
| dsva-large.ovf | 6 | 24576MB |

VMware NSX for vSphere(以下 NSX-V)及び NSX-T 2.4 までの環境では、DSVA を各ホストヘデプロイする際 には、DSVA ソフトウェアパッケージを DSM にアップロード後、OVF ファイル内の vCPU 及びメモリの値を変更す ることにより、DSVA の展開リソースを事前に指定した上で NSX Manager から DSVA を展開することが可能で す。

Deep Security 12.0 では、DSVA 12.0 Update 3(Deep Security Appliance 12.0.0-682 for ESX-x86_64:2019 年 12 月 5 日リリース)から上記 4 つのタイプのソフトウェアパッケージに対して VMware 社のデジタル署名がされ た形で提供されます。

(初期リリースの DSVA12.0.0-364 は NSX-V または NSX-T2.4 環境でのみ利用できます。)

上記の対応により、NSX Manager において DSVA をデプロイする際には、デプロイするソフトウェアパッケージを 指定することが可能となります。なお、2019 年 12 月末時点での最新ビルドである Deep Security 12.0 Update 4 では NSX Manager から DSVA をデプロイする際の"展開の仕様"は"Deep Security-Medium"以外の選択がで きません。

また、NSX-T2.5.0 以降の既知の不具合により、ワークアラウンドとして DSVA の展開にあたっては、DSVA のソフトウェアパッケージを DSM サーバ上にアップロードするだけではなく、外部の HTTP サーバ(HTTPS では NG)



にもソフトウェアパッケージをアップロードする必要があります。DSM ではその外部 HTTP サーバを DSVA ソフト ウェアパッケージの格納先として明示的に設定することで DSVA の展開が可能となります。 (この設定をしていない場合には DSVA のデプロイに失敗します。)

[コンピュータ] > [該当 vCenter Server からプロパティ]> [NSX 設定] > [Virtual Appliance OVF の URL:]

| 💋 IREND Deep Security | ダッシュボード 処理 アラート イベントとレポート コンビュ ー |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ✓ ▲ スマートフォルダ ▲ TEST | vCenter - vc01.trendnsx.local サブグループを含まない ▼ © vCenter - vc01.trendnsx.localのプロパティ - Google Chro □ × |
| ✓ ■ ⊐𝟸= ¬𝔅 ✓ ⑦ vCenter - vc01.trendnsx.local | ▲ 保護されていない通信 4119/VirtualProperties.scree 一般 NSX Manager NSX設定 |
| ・ 本ストおよびクラスタ ・ 「● NSX ・ 「● NSX-T ・ ・ ・ | 一般 Deep Security Managerデータベースではなく、ローカルWebサーバ上 ICDeep Security Virtual Applianceアブライアンスパッケージをホストする Virtual Appliance OVFのURL: |
| > 🞒 NSX ✓ 🞒 NSX-T | |

設定する URL は以下の形式で記載してください。

https://[DSM_ Hostname or IP]:4119/appliance/NSX/dsva.ovf(or dsva-small/medium/large.ovf) ※今後の Deep Security Manager の仕様の拡張に伴い指定方法が変わる可能性があります。

指定できる URL パスは 1 つのみのため、複数のソフトウェアパッケージを環境に応じて使い分ける場合には、 デプロイごとに本設定の URL の書き換えを行う必要があります。 設定方法の詳細についてはヘルプセンターの内容も参考にしてください。

NSX-T2.5.0 の仕様変更及び制約事項に伴う Deep Security への影響に関する情報の詳細については以下のサイトを参照してください。

VMware NSX-T Data Center 2.5 環境における Trend Micro Deep Security Virtual Appliance (DSVA) デプロイに関する留意事項

https://www.trendmicro.com/ja_jp/business/campaigns/vmware/resources/nsx-t25-and-DSVA_kb.html

また、NSX-T2.5.0の仕様変更、制約事項の内容の詳細は VMware 社に問合わせしてください。



2. VMware NSX 環境における DSVA エージェントレスセキュリティ保護環境の構築手順

2-1. 本構築ガイドにおける事前準備しておくべき環境と想定環境

本ガイドに従って作業する際に、事前に以下の環境が準備されていることを確認してください。

- 管理サーバクラスタ、保護対象クラスタのESXiホスト
- vCenter Server
- NSX Manager
- VMware Horizon 7 環境
 (仮想デスクトップ環境利用の場合:WindowsクライアントOSによるリンククローン展開環境を想定)
- 仮想デスクトップ用マスターイメージ(WindowsクライアントOS)
- DSM用Microsoft SQLサーバ インストール環境(WindowsサーバOS)
- VMware NSX コンポーネント myVMwareからダウンロードしてください(myVMwareアカウントが必要となります。) <u>https://my.vmware.com/ja/group/vmware/downloads</u>
- Deep Security コンポーネント
 トレンドマイクロダウンロードセンターからダウンロードしてください。
 http://downloadcenter.trendmicro.com/index.php?regs=jp

また、DSVAの展開にあたっては予めNSX-Tを展開するESXiホストに対してTransport Node Profileの展開及び Deep Securityの不正プログラム対策イベントの検出をトリガーに仮想マシンを隔離したい場合には、分散ファイ アウォールの有効化をする必要があります。



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

2-2. 本ガイドで想定する環境

- ▶ Horizon にて仮想マシン(VDI用 Windows クライアント)が展開される
- 仮想マシンに対して、Deep Securityの不正プログラム対策を有効化
 適用する Deep Securityのポリシーは、トレンドマイクロが提供するデフォルトのポリシーである
 "Windows 10 Desktop"を継承してカスタマイズした"VDI_Windows Desktop_Demo01 "を設定
- オプションとして、Deep Security で不正プログラム対策イベントを検出した際に分散ファイアウォールと 連携した自動隔離ができるように隔離用セキュリティグループも設定





Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

2-3. エージェントレスによる仮想マシン保護 構築手順

構築の全体の流れは以下となります。





Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

2-3-1. DSM 用 SQL サーバ構築

Deep Security の設定、イベントを格納するためのデータベースを構築します。

DSM 用 SQL サーバを構築する前に、SQL インストール時に必要となる.NET Framework3.5 を事前インストール しておく必要があります。



1) DSM 用 SQL サーバ上でインストーラを実行し、インストールを開始する

| 🖬 I ⊋ 🔢 🖛 I | アプリケーション ツール 🛛 | VD ドライブ (E:) SQL20 | 14_x64_JPN | . 🗆 X |
|--------------------|-------------------------------|--------------------|-------------------|--------------|
| ファイル ホーム 共有 | 表示管理 | | | ~ () |
| 🐑 💿 👻 🕇 🖾 🕨 PC | ▶ DVD ドライブ (E:) SQL2014_x64_3 | N × C | DVD ドライブ (E:) SQL | 2014 P |
| 🚖 お気に入り | 名前 | 更新日時 | 種類 | サイズ |
| 🍺 ダウンロード | 1041_JPN_LP | 2016/06/19 18:0 | 16 ファイル フォルダー | |
| ■ デスクトップ | PCUSOURCE | 2016/06/19 18:0 | 17 ファイル フォルダー | |
| 💹 最近表示した場所 | 퉬 redist | 2016/06/19 18:0 | 17 ファイル フォルダー | |
| | 퉬 resources | 2016/06/19 18:0 |)7 ファイル フォルダー | |
| 👰 PC | 퉬 StreamInsight | 2016/06/19 18:0 |)7 ファイル フォルダー | |
| 🚺 ダウンロード | 🎳 Tools | 2016/06/19 18:0 |)7 ファイル フォルダー | |
| 隆 デスクトップ | 퉬 x64 | 2016/06/19 18:0 |)7 ファイル フォルダー | |
| F#1 | autorun 😥 | 2014/02/07 5:56 | 5 セットアップ情報 | 1 KB |
| 🎉 ピクチャ | 🕋 MediaInfo | 2016/06/19 1:05 | 5 XML ドキュメント | 1 KB |
| 🍺 ビデオ | 🔛 setup | 2016/06/18 17:4 | 14 アプリケーション | 70 KB |
| 🜗 ミュージック | setup.exe.config | 2014/01/17 18:2 | 27 CONFIG ファイル | 1 KB |
| 📥 ローカル ディスク (C:) | SqlSetupBootstrapper.dll | 2016/06/18 17:4 | 15 アプリケーション拡張 | 193 KB |
| 🔽 DVD ドライブ (E:) S(| 🔊 sqmapi.dll | 2014/02/21 22:2 | 20 アプリケーション拡張 | 147 KB |
| | | | | |
| 📬 ネットワーク | | | | |

| | | SQL Server インストール センター | ۲ |
|---------------------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| インストール | 9 | <u>ハードウェアとソフトウェアの要件</u> ハードウェアとソフトウェアの要件を表示します。 | ^ |
| メンテナンス ツール | 9 | セキュリティに関するドキュメント セキュリティに関するドキュメントを表示します。 | |
| リソース 詳細設定 | 9 | リリース ノート リリースの最新情報を表示します。 | = |
| オプション | ľ | SQL Server Data Tools の取得方法 SQL Server Data Tools は、データベース開発者が任意の SQL Server プラットフォームで データベースのあらゆるデザイン作業を実行するための統合環境を提供します。 | |
| | 9 | システム構成チェッカー SQL Server が正常にインストールできなくなるような条件があるかどうかを確認するツールを起動 します。 | |
| | ľ | アップガレードアドバイザーのインストール アップガレードアドバイザーを使用することで、インストール済みの任意の SQL Server 2012 コン ポーネント、SQL Server 2008 R2 コンポーネント、SQL Server 2008 コンポーネント、または SQL Server 2005 コンポーネンを加加し、SQL Server 2014 にアップグレードする商または 後に修正が必要な問題を特定します。 | |
| | 9 | インストールのヘルプ インストールに関するドキュメントを開きます。 | |
| | 9 | SQL Server 2014 フェールオーバー クラスタリングの開始方法 SQL Server 2014 フェールオーバー クラスタリングの構成方法に関する説明を参照してください。 | |
| Microsoft SQL Server 2014 | • | PowerPivot for SharePoint Standalone Server インストールの開始方法 新しい SharePoint 2010 サーバーに最小限の手順で PowerPivot for SharePoint をイン | ~ |



2) **[SQL Server の新規スタンドアロンインストールを実行するか、既存のインストールに機能を追加します**を 選択し、スタンドアロンインストールを実行する



3) プロダクトキーを入力する

| 1 | SQL Server 2014 セットアップ |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ★ プロダクト キー インストールする SQL Server : プロタクト キー ライセンス条項 グローバル ルール Microsoft Update 製品の更新プログラム セットアップ フーバルのインストール インストール ルール セットアップ ロール 機能の選択 機能にール 機能の選択 機能の、ルール インストールの進信状況 完了 | SQL Server 2014 セットアップ _ □ × 2014 のエディションを指定します。 _ □ × Microsoft 証明書または製品パッケーシに記載されている 25 文字のキーを入力して、SQL Server 2014 のごのイ ンスタンスを検証してください。または、SQL Server の無償のエディション (Evaluation Express など)を指定するこ とちできず、SQL Server オンライン フックに記載されているように、Evaluation には SQL Server の機能が最大 間に含まれてもり、180 日間の有効期限付きアクティブにはます。あエディションから別のエディションにアップガレー ドするには、エディション アップガレード ウィザードを実行してください。 ○ 無償のエディションを指定する(5): Evaluation ● プロダクト キーを入力する(E): |
| | < 戻る(B) 次へ(N) > キャンセル |



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

4) ライセンス条項に同意する



5) Microsoft Update の更新プログラムの確認をするようにチェックする

| 1 | SQL Server 2014 セットアップ |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft Update Microsoft Update を使用して重 プロダクトキー | 重要な更新プログラムを確認する |
| ライセンス条項 グローバルルール Microsoft Update 製品の更新プログラム セットアップ ファイルのインストール インストールルール セットアップ ロール 機能の選択 機能ルール 機能構成ルール 検能構成ルール インストールの準備完了 インストールの進行状況 完了 | Microsoft Update is、Microsoft ンJP11P (SQL Selver 2014 i3C) のビキゴウオ 美術プ ログラムや他の重要な要素が TDグラムを提供します。更新 TDグラムは、自動更新 を使用するか、Microsoft Update Web サイトにアクセスして取得することができます。 「Microsoft Update を使用して更新プログラムを確認する (推奨)(M) <u>Microsoft Update のプライパシー に関する声明</u> |
| | < 戻る(B) 次へ(N) > キャンセル |



6) インストール要件のチェックを実行し、問題がないことを確認して[次へ]

| 1 | SQL Server 2014 セットアップ | _ 🗆 X |
|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| インストール ルール セットアップのルールでは、セットアッ おく必要があります。 | プの実行中に発生する可能性がある問題を特定します。セットアップを続行する前に、エラーを修正して | |
| プロダクトキー ライセンス条項 グローバル ルール Microsoft Update セットアップ ファイルのインストール インストール ルール | 操作が完了しました。成功 7、失敗 0、警告 0、スキップ 0。 詳細の非表示(S) << 詳細 <u>しポートの表示(V)</u> | 再実行(R) |
| セットアップ ロール 機能の選択 機能ルール 機能構成ルール インストールの準備完了 インストールの進行状況 完了 | ルール 状態 マユージョン アウティブ テンプレート ライブラリ (ATL) 合格 SQL Server 2008 より前のリリーズの Business Intelligence De 合格 SQL Server レジストリ キーの整合性の検証 合格 コンピューター ドメイン コントローラー 合格 Microsoft .NET アプリケーション セキュリティ 合格 Windows ファイアウォール 合格 Microsoft SQL Server 2014 CTP1 が存在する場合にインストー 合格 | |
| | < 戻る(B) 次へ(N) > キャンセル | へルプ |

7) [SQL Server 機能のインストール]を選択する

| 1 | SQL Server 2014 セットアップ |
|------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| セットアップ ロール [SQL Server 機能のインストー. て特定の構成をインストールします | ル] オプションをグリックしてインストールする機能コンポーネントを個別に選択するか、機能ロールをクリックし 「= |
| プロダクト キー ライセンス条項 グローバル ルール | SQL Server 機能のインストール(S) SQL Server デーダベース エンジン サービス, Analysis Services, Reporting Services, Integration Services, およびその他の機能をインストールします。 |
| Microsoft Update セットアップファイルのインストール インストール ルール セットアップロール 機能の選択 機能ルール 機能構成ルール インストールの準備完了 インストールの進行状況 完了 | ○ SQL Server PowerPivot for SharePoint(P) ファームでの PowerPivot データ アクセスをサポートするために、PowerPivot for SharePoint を新規または既存 の SharePoint サーバーにインストールします。必要に応じて、新しいファームのデータベース、サーバーとして使用する SQL Server リレーショナル データベース リレーショナル エンジン サービスを追加する。(R) ③ さのインストールに SQL Server データベース リレーショナル エンジン サービスを追加する。(R) ③ すへての機能に既定値を使用(D) サービス アカウントに既定値を使用してすべての機能をインストールします。 |
| | < 戻る(B) 次へ(N) > キャンセル ヘルプ |



8) [機能選択]にて、[データベースエンジンサービス][管理ツール・基本]を選択する

| 1 | SQL Server 2014 セットアップ | _ _ X |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 機能の選択 インストールする Evaluation 機 | 能を選択します。 | |
| プロダクトキー ライセンス条項 グローバル ルール Microsoft Update セットアップ ファイルのインストール インストール ルール セットアップ ロール 機能の選択 機能リール インスタンスの構成 サーバーの構成 データベース エンジンの構成 株能構成ルール インストールの準備完了 インストールの進行状況 完了 | 機能(E): インスタンス機能 ダ テータペース エンジン サービス □ SQL Server レブリケーション □ 体表のためのフルテキスト抽出とセマンティック抽出 □ Data Quality Services □ Analysis Services - ネイティブ 共有機能 □ Reporting Services - ネイティブ 共有機能 □ Integration Services □ Jota Quality Client ダ プライアント ツール以長: □ Integration Services □ クライアント ツール以長: □ イモュンメ1 コンパ キント ○ ジェッル - 完全 □ 分数両キニントローラー □ 分数両キントローラー □ 分数両キニントローラー □ 分数両キニントローラー □ 分数両キニントローラー □ 分数両キニントローラー □ 分数両キントローラー □ 分数両キニントローラー □ 分数両キントローラー □ 分数両キニントローラー □ 分数両キニントローラー □ 分数両キニントローラー □ 分数両キニントローラー □ 分数両キニントローラー □ 分数両キントローラー □ 分数両キニントローラー □ 分数両キニント □ クラー □ 分数 □ クラー □ 分数 □ クラー □ 分数 □ クラー □ 分数 □ クラー □ 分数 □ 分 □ 分数 □ 分数 □ 分数 □ 分数 □ 分 □ 分数 □ 分数 □ 分数 □ 分数 □ 分 □ 分数 □ 分数 □ 分 □ 分数 □ 分 □ 分 □ 分 □ 分 □ | 機能の説明: クライアントとサーバー間の通信用のコンボーネン ^ トを含みます。 避沢した機能に必要なコンボーネント(P): インストール済み: インストール済み: 小(crosoft NET Framework 4.0 メディアからインストール: 小(crosoft NET Framework 4.0 メディアからインストール: 小(crosoft NET Framework 4.0) メディアからインストール: 小(crosoft NET Framework 4.0) メディアからインストール: ・ Microsoft Visual Studio 2010 再頒布戸 < |
| | < 戻る(B) | 次へ(N) > キャンセル ヘルプ |

9) [インスタンスの構成]を確認して[次へ]

| 1 | SQL Server 2014 セットアップ – 🗖 🗙 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| インスタンスの構成 SQL Server インスタンスの名言 プロダクト キー ライセンス条項 グローバル ルール | 前およびインスタンス ID を指定します。インスタンス ID は、インストール パスの一部になります。 |
| Microsoft Update セットアップ ファイルのインストール インストール ルール セットアップ ロール 機能の選択 機能リール インスタンスの構成 サーバーの構成 データベース エンジンの構成 機能構成ルール インストールの準備完了 インストールの進行状況 完了 | インズタンズ ID(I): MSSQLSERVER SQL Server ディレクトリ: C:¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER インストール溶みのインスタンズ(L): |
| | インスタンス名 インスタンス ID 機能 エディション |
| | - < 戻る(B) 次へ(N) > キャンセル ヘルプ |



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

10) [サーバ構成を確認して[次へ]

| 1 | SQL Server 20: | 14 セットアップ | | _ | D X |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|-----------------|-----------------------------------------|--------------------|
| サーバーの構成 サービス アカウントと照合順序の構 プロダクト キー | 成を指定します。 | | | | |
| ライセンス条項 グローバル・ルール Microsoft Update セットアップ ファイルのインストール インストール・ルール セットアップ ロール 機能の選択 機能ルール インスタンスの構成 サーバーの構成 サーバーの構成 サーバーの構成 ファータベースエンジンの構成 機能構成ルール インストールの準備完了 インストールの進行状況 完了 | 各 SQL Server サービスに別々のアナ サービス SQL Server エージェント SQL Server データベース エンジン SQL Server Browser | hウントを使用することをお勧めし アカウント名 NT Service¥SQLSER NT AUTHORITY¥LOC | ょます(M) パスワード | スタートアップ(手動) 手動) 無助) | D種類 > > > |
| | | < 戻る(B) 次へ(1 | V) > ‡t | r>teil / | ∖ ルプ |

11) [データベース エンジンの構成を設定する

- ・ [認証モード]
- ・[パスワードの入力] : sa アカウントのパスワードを設定

: [混合モード]を選択

- [パスワード確認入力] : sa アカウントのパスワードを設定
- [SQL Server 管理者の指定] : [現在のユーザの追加] でユーザ追加

| 1 | SQL Server 2014 セットアップ | | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|--|--|--|
| データベース エンジンの構 | 成 | | | |
| データベース エンジンの認証セキュリ | ティモード、管理者、およびテータ ティレクトリを指定します。 | | | |
| プロダクト キー ライヤンス条項 | サーバーの構成 データディレクトリ FILESTREAM | | | |
| グローバル ルール Microsoft Undate | データベース エンジンの認証モードおよび管理者を指定します。 | | | |
| Twhere are a series of the se | 窓祉モート ○ Windows 認証モード(W) | | | |
| インストール ルール セットアップ ロール | ● 混合モード(M) (SQL Server 認証と Windows 認証) | | | |
| 機能の選択 機能ルール | SQL Server のシステム管理者 (sa) アカウントのパスワードを指定します。 パスワードの入力(E): | | | |
| インスタンスの構成 | パスワードの確認入力(<u>Q</u>): | | | |
| データベースエンジンの構成 | SQL Server 管理者の指定 | | | |
| 機能構成ルール インストールの準備完了 | WIN-53RD24EIP59¥Administrator (Administrator) SQL Server の管理 者には、データベースエ となって対する無知道の | | | |
| インストールの進行状況 完了 | アクセス権があります。 | | | |
| | | | | |
| | 現在のユーザーの追加(<u>C</u>) 追加(<u>A</u>) 削除(<u>R</u>) | | | |
| | < 戻る(<u>B</u>) 次へ(<u>N</u>) > キャンセル ヘルブ | | | |
| | | | | |



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

12) [インストール]をクリックする

| 1 | SQL Server 2014 セットアップ | _ 🗆 X |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| インストールの準備完了 インストールする SQL Server 20 プロダウトキー - ベロコタマ | 14の機能を確認します。 SQL Server 2014 インストールの準備完了: | |
| ライセンス条項 ゲローバル ルール Microsoft Update セットアップ ファイルのインストール インストール ルール セットアップ ロール 機能の選択 機能ルール インスタンスの構成 サーバーの構成 サーバーの構成 サーバーの構成 大クトールの準備完了 インストールの進行状況 完了 | ● 敬要 「エディション: Evaluation - アウション: Install ● 必要なコンポーネント ● Windows PowerShell 2.0 - Microsoft .NET Framework 3.5 - Microsoft .NET Framework 4.0 B - メディアからインストール: - Microsoft Visual Studio 2010 再頒布可能ファイル - Microsoft Visual Studio 2010 Shell B - 全般構成 ● 常理>ール - 基本 - 管理>ール - 基本 - 管理>ール - デニタ B - インスやンスの構成 マンオシスの構成 ▲ (1) ▲ (1)<!--</td--><td>× 12_162518¥Configurati</td> | × 12_162518¥Configurati |
| | < 戻る(B) 【ノンストール(I)】 キャン | セル ヘルプ |

13) インストールが正常に完了したことを確認する

| 1 | SQL Server 2014 | 4 セットアップ | x |
|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| 完了 SQL Server 2014 のインストー | ルが正常に完了しました: 。 | | |
| プロダクトキー ライセンス条項 グローバル・ルール Microsoft Update セットアップ ファイルのインストール インストール ルール セットアップ ロール | セットアップ操作または実行可能な次の手順 機能 ② 管理ソール - 完全 ③ 管理ソール - 基本 ③ データベース エンジン サービス ③ SQL ラパクー ④ SQL ライアント提編 | iに関する情報(I): | × III |
| 機能の選択 機能ルール インスタンスの構成 サーバーの構成 データベースエンジンの構成 機能構成ルール インストールの準備完了 インストールの進行状況 完了 | 詳細(D): SQL Server の製品ドキュメントの表: SQL Server に関するドキュメントを表示 います。既定で、ハルラゼニーアーコンポ ストールドム、ハルラグブラリマネージャー ダウンロードできます。詳細については、「S (chttp://go.microsoft.com/fwink/?Lim | 示 あよび管理するのに使用するコンボーネントのみがインストールされて ーネントではオンライン ライブラリが使用されます。SQL Server のイン - コンボーネントを使用すると、ローカル コングニッケーにドキュメントを SQL Server 2014 のオンライン ブック」を参照してください kkD=2995782-)。 | < III > |
| | 概要ログ ファイルの保存先: C:¥Program Files¥Microsoft SOL S: ¥Summary WIN-5JRD24EIP59 201 | erver¥120¥Setup_Bootstrap¥Log¥20171212_162518 171212_162518.txt 聞じる ヘルプ | |



14) SQL Server 構成マネージャにログインし、[MSSQLSERVER のプロトコル]から[TCP/IP]を選択する

| Sql Server Configuration Manager | | | | _ D X |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|----------|--|--------------|
| ファイル(F) 操作(A) 表示(V) ヘルプ(H) | | | | |
| 🗢 🔿 🙍 🗟 | | | | |
| 🕵 SQL Server 構成マネージャー (ローカル) | プロトコル名 | 状態 | | |
| 目 SQL Server のサービス <u>↓</u> SQL Server ネットワーク構成 (32 ビット) | ☞ 共有メモリ ☞ 名前付きパイプ | 有効 無効 | | |
| ● . SQL Native Client 11.0 の構成 (32 ビッ) ▲ . SQL Server ネットワークの構成 □ . MSSQLSERVER のプロトコル ▶ . SQL Native Client 11.0 の構成 | ≩ <mark>⊤</mark> CP/IP | 有効 | | |
| | | | | |
| | | | | |

15) [TCP/IP のプロパティ]で、[IPALL]のポート番号(1433)を指定し、[適用]する

| | TCP/IPのプロパティ ? | x |
|---------------------------|--------------------------------|---|
| דראם TD אובאם לעבא | 2 | |
| 有効 | いいえ | ^ |
| IP5 | | |
| IP アドレス | 127.0.0.1 | |
| TCP ポート | 1433 | |
| TCP 動的ポート | | |
| アクティブ | はい | |
| 有効 | いいえ | |
| □ IP6 | | |
| IP アドレス | fe80::5efe:10.3.225.186%13 | |
| TCP ポート | 1433 | |
| TCP 動的ポート | | |
| アクティブ | はい | |
| 有効 | 2002 | ≡ |
| | | |
| TCP ポート | 1433 | |
| TCP 動的ポート | | |
| TCP ポート TCP ポート | | × |
| ОК | キャンセル 適用(<u>A</u>) へル | Ĵ |



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

16) SQL Management Studio にログインし、[オブジェクト エクスプローラ] > [データベース]を右クリックして、[新 しいデータベース]を選択する

ファイル(F) 編集(E) 表示(V) デバッグ(D) ツール(T) ウィンドウ(W) ヘルプ(H) : 🛅 • 回 • 💕 🚚 🥥 🏥 新しいカエリ(N) 🕞 🔧 🐴 🏠 🐇 🕾 🕒 • ભ • 💷 • 🖳 🖓 **▼**₽× オブジェクト エクスプローラ・ 接続 📲 🛃 💷 🍸 🛃 📓 ■ び WIN-53RD24EIP59 (SQL Server 12.) ■ で 新しいデータベース(N)... ■ サ・ アタッチ(A)... アタッチ(A)... ■ □ レ ■ □ レ ■ □ Alv ■ □ 管 データベースの復元(R)... ファイルおよびファイル グループの復元(E)... ■ 🚞 統 🏦 SC データ層アプリケーションの配置(L).. データ層アプリケーションのインポート(I).. PowerShell の起動(H) レポート(P) 最新の情報に更新(F)

17) [データベース名]にデータベース名(dsm)を入力する

| 8 | 新しいデータベース | | | | |
|--------------------------|-------------|------------|-----------|------------|-------------|
| ページの選択 | 🔄 スクリプト 👻 | [ヘルプ | | | |
| ゴ ± 82 ゴ オブション | 18友 | | | | |
| 🖙 ファイル グループ | データベース名(N): | | dsm | | |
| | 所有者(0): | | 〈既定〉 | | |
| | 🔽 フルテキスト・ | インデックスを使用す | tā(U) | | |
| | データベース ファ | イル(F): | | | |
| | 論理名 | ファイルの種類 | ファイル グループ | 初期サイズ (MB) | 自動拡張/最大サイズ |
| | dsm | 行データ | PRIMARY | 5 | 1 MB 単位で無制限 |
| | dsm_log | ログ | 適用なし | 1 | 10 % 単位で無制限 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| 接続 | | | | | |
| サーバー: WIN-5JRD24EIP59 | | | | | |
| 接続: sa | | | | | |
| 野 接続のプロパティの表示 | | | | | |
| 進行状況 | | | | | |
| 準備完了 | < | Ш | | | > |
| New Y | | | | 追加(A) |)除(R) |
| | | | | | OK キャンセル |
| | | | | | h. |



18) [オプション]で復旧モデルから[単純を選択して、[OK]を選択する

[TIPS]

復旧モデルは、「完全」や「一括ログ」を選択することも可能ですが、データベースの肥大防止やメンテナン ス負荷軽減の観点から、復旧モデルを[単純]にすることを推奨しています。

関連 FAQ: SQL Server の復旧モデルについて

http://esupport.trendmicro.com/solution/ja-JP/1112366.aspx

| 8 | 新しいデータベース | _ D X | | | |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|--|--|--|
| ページの選択 | 【 2カリプト ★ 【 人 ルプ | | | | |
| | | | | | |
| ☆ オプション ☆ ファイル グループ | 照合順序(C): | ~ | | | |
| | 復旧モデル(M): 単純 | | | | |
| | | → | | | |
| | 互換性レベル(L): SQL Server 2014 (120) | SQL Server 2014 (120) | | | |
| | コンテインメントの種類(T): なし | ~ | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | ⊿ FILESTREAM | ^ | | | |
| | FILESTREAM ディレクトリ名 | | | | |
| | FILESTREAM 非トランザクション アクセス Off | | | | |
| | ⊿ Service Broker | = | | | |
| | Broker が有効 False | False | | | |
| | Broker の優先度の許可 False False | | | | |
| | Service Broker 識別子 00000000-0000- | /0000-0000-00000000000 | | | |
| | | | | | |
| | コミットでカーソルを閉じる False | | | | |
| 接続 | 以定のカーソル GLOBAL | | | | |
| 11 | | | | | |
| | 2 117次記の年の基準になる年 2049 | 2049 | | | |
| WINT BOILD24EIN 83 | アイス ソニア変換 Faise Frage Frage | False | | | |
| 接続: | | | | | |
| sa | | | | | |
| ■9 接続のプロパティの表示 | 4 7mh | | | | |
| | ANSI NIILL 联定值 False | | | | |
| | ANSI NULL 有効 False | | | | |
| 進行状況 | 9 桁手戸の午の其進にわる午 | | | | |
| 準備完了 | ઽ ៕ ૩ ૹਛ©ᡩ₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩ | | | | |
| | | | | | |
| | | OK キャンセル | | | |
| | | | | | |

19) 新しいデータベースインスタンスができていることを確認する





2-3-2. Deep Security Manager(DSM) インストール

DSM を Windows サーバにインストールし、DSM 用に設定した SQL サーバに接続します。



1) DSM 用サーバ上で Deep Security Manager のインストーラを実行する

| 🏨 l ⊋ 🚯 = 1 | インストーラ | | _ | D X |
|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|------------------|---------------|------------|
| ファイル ホーム 共有 | 表示 | | | ~ ? |
| (e) (e) < ↑ (f) (e) (e) (e) | ンストーラ 🕨 | ✓ C 12 | ストーラの検索 | Q |
| ☆ お気に入り | 名前 | 更新日時 | 種類 | サイズ |
| 🧯 ダウンロード | DeepSecurityInstallerReport.csv | 2019/07/11 13:45 | CSV ファイル | 2 |
| ■ デスクトップ | 🖟 Notifier-Windows-10.0.0-2094.i386.msi | 2017/03/09 11:50 | Windows インスト | 6,580 |
| 3 最近表示した場所 | Manager-Windows-10.0.3259.x64.exe | 2017/03/09 13:06 | アプリケーション | 294,702 |
| | Manager-Windows-11.0.349.x64.exe | 2019/07/08 16:29 | アプリケーション | 343,243 |
| PC 💀 | Manager-Windows-12.0.296.x64.exe | 2019/07/08 16:37 | アプリケーション | 402,839 |
| 📕 ダウンロード | memo.txt | 2019/07/11 14:19 | テキスト ドキュメント | 1 |
| 📔 デスクトップ | Agent-RedHat_EL6-10.0.0-2094.x86_64.zip | 2017/03/09 13:44 | 圧縮 (zip 形式) フ | 46,736 |
| 1 </th <th>Agent-RedHat_EL7-10.0.0-2094.x86_64.zip</th> <th>2017/03/09 12:02</th> <th>圧縮 (zip 形式) フ</th> <th>24,309</th> | Agent-RedHat_EL7-10.0.0-2094.x86_64.zip | 2017/03/09 12:02 | 圧縮 (zip 形式) フ | 24,309 |
| 📔 ピクチャ | Agent-Windows-10.0.0-2094.i386.zip | 2017/03/09 12:18 | 圧縮 (zip 形式) フ | 60,639 |
| 📴 ビデオ | Agent-Windows-10.0.0-2094.x86_64.zip | 2017/03/09 12:20 | 圧縮 (zip 形式) フ | 72,346 |
| 📗 ミュージック | Agent-Windows-11.0.0-796.x86_64.zip | 2019/07/08 16:30 | 圧縮 (zip 形式) フ | 87,829 |
| 🚢 ローカル ディスク (C:) | Agent-Windows-12.0.0-360.x86_64.zip | 2019/07/08 16:31 | 圧縮 (zip 形式) フ | 93,922 |
| | Appliance-ESX-10.0.0-2888.x86_64.zip | 2019/07/16 10:56 | 圧縮 (zip 形式) フ | 524,033 |
| 📬 ネットワーク | Appliance-ESX-11.0.0-211.x86_64.zip | 2019/07/16 11:13 | 圧縮 (zip 形式) フ | 498,058 |
| 🖳 tsclient | Appliance-ESX-12.0.0-364.x86_64.zip | 2019/07/11 13:29 | 圧縮 (zip 形式) フ | 525,599 |
| | 🛃 Notifier-Windows-12.0.0-360.i386.msi | 2019/07/16 11:48 | Windows インスト | 14,756 |
| | | | | |
| 16 佃の頂日 | < 111 | | | |
| 101回の現日 | | | | |
| | | | | |
| 0 | セットアップウィザード 🗕 🗆 🗙 | | | |
| | ····································· | | | |
| Deep Si ています | ecurity Manager(ルビット/ツノリイザ ートを準1/届し | | | |
| | キャンセル | | | |



[TIPS]

DSM をインストールする際に、インストーラと同一ディレクトリに DSA や DSVA などのインストールコンポー ネントを配置しておくと、インストール時にコンポーネントを自動的に DSM にアップロードされます。

Deep Security では、管理対象となる防御用プログラム(DSA/DSVA)を DSM にインポートしておく必要があります。以下のコンポーネントをインストール時に準備しておくようにしてください。

- DSMのOSにあわせたDSA(DSRとして利用するため)
- DSVA のソフトウェアパッケージについてはヘルプセンターに展開されている最新のビルドを利用してく ださい。
- RHEL 7 (x64) 用 Deep Security Agent (DSVA Build 単位でのバージョンアップ用)
 - DSVA のソフトウェアパッケージは、メジャーリリース毎及び大幅なエンハンスメントが発生した場合にリリースされます。
 - 適宜リリースされる Update については、Redhat(64bit)版 DSA を利用してアップデートしたい Appliance バージョンのアップデートを行います。 (実際は、DSVA OVF と該当の DSA を DSM ローカルにダウンロードしておくことで、NSX からの "デプロイ"時に自動的に指定された Build で展開されます。)
 - RHEL 7 (x64) 用 Deep Security Agent (DSVA Build 単位でのバージョンアップ用)
 - ▶ ソフトウェアパッケージの例

Appliance-ESX-12.x.x-xxxx.x86-64.zip Agent-RedHat-EL7-<version>-<build>.x86-64.zip Agent-Windows-<version>-<build>.x86_64.zip :DSVA パッケージ本体(DS12.0 以降)

:DSVAを最新版で配置するための DSA

:DSR 用 DSA(導入が Linux 版の場合は Linux 版 DSA)

 DSVA 展開ビルドの指定方法(デフォルトでは DSM ローカルにアップロードされている DSVA と RHEL 7 (x64) 用 DSA の中で最新のビルドが選択)

[管理]>[システム設定]>[アップデート]>[Virtual Appliance の配置]

| Virtual Applianceの 配置 | |
|--------------------------------------------------------|--------------------|
| 配置と同時にDeep Security Virtual Applianceを次のバージョンにアップグレード: | 利用可能な最新バージョン(推奨) 💌 |
| | 利用可能な最新バージョン(推奨) |
| | 12.0.0.767 |
| | 12.0.0.725 |
| | 12.0.0.682 |

また、ソフトウェアバージョンについては、VMware 各ソリューションとの互換性を確認の上、その中で最新のビルドを利用することを推奨します。

2) 言語選択を行う

| 0 | | 言語の選択 | - 🗆 X |
|---|--------|-------|-------|
| | 言語を選択: | | |
| | 日本語 | | ¥ |
| | | ОК | キャンセル |


Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

3) セットアップウィザードで[次へを選択する

| | Trend Micro Deep Security Manager 12.0.296のセットアップウィザード | | x |
|---------------------|-------------------------------------------------------------------------------------------------|-------|---|
| Trend Micro | Trend Micro Deep Security Managerのセットアップウィザードへようこそ | | |
| DEEP SECURITY 12 | このウィザードの指示に従って、Deep Security Manager 12.0.286をセットアップします。 (本リリースの <mark>新聞住た</mark> 参照してください) | | |
| | インストールを続行する場合は【次へ】をグリックしてください。 | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| 9 | | | |
| | | | |
| | | | _ |
| | ×^* | キャンセノ | L |

4) 使用許諾契約に同意する

| 0 | Trend Micro Deep Security Manager 12.0.296のセットアップウィザード – 🗖 🗴 |
|-------------------|--------------------------------------------------------------------------------|
| 使用許諾契 | #* 🥏 |
| 次の使用許 | 諸契約書をよくお読みください。 |
| 使用許諾 | 契約書について |
| 本製品の使 | 使用許諾契約の内容につきましては、製品インストールメディア内に格納されている使用許諾契約書をご確認とださい。 |
| 格納されて 先されます。 | いる使用許諾契約書と当社Webサイドに掲載している使用許諾契約書に異なる定約があった場合には、当社Webサイドに掲載されている使用許諾契約書が優。 。 |
| また、CD-F | ROMなどのインストールメディアのない製品やサービスにつきましては、当社Webサイドに掲載している契約書をご確認なださいますようお願いいたします。 |
| https://ww | ww.trendmicro.com/ja.jp/about/legal/eula.html |
| トレンドマイ 2017年9月 | 夕0時55余社 9 |
| • FIZE | マイクロの使用料装装約の空楽項に回覧(支) - (|
| 0 FU2F | マイクロの1世用計論発行の発現に可感しません |
| | (戻る)「次へ>」「キャンセル」 |

5) インストールパスを指定する

| • | Trend Micro Deep Security Manager 12.0.296のセットアップウィザード | _ 🗆 X |
|----------------------------------|--------------------------------------------------------|------------|
| インストールパス | | Ð |
| Deep Security Manager(| Dインストールパスを指定し、〔太へ〕をクリックしてください。 | |
| インストールパス C.¥Program Files¥Tre | nd Micro¥Deep Security Manager | 参照 |
| ディスク所要量: 555 M ディスク空き容量: 29 G | 8 | |
| | | 次<>> キャンセル |



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

6) データベースの接続設定を行う

- [オプション]: データベース種類を選択 .

[接続設定]: DSM 用 SQL の[ホスト名][データベース名)を指定 トランスポートを*[TCP]*で設定

データベースインスタンスに対する[ユーザ名(sa)][パスワード]を指定

| 0 | Trend Micro Deep Security Man | ager 12.0.296のセットアップウィザード | × |
|----------------------------------|-------------------------------------------------------------|---------------------------|-------------|
| データベース | | | Ø |
| データベースおよび 種類 ・ Microsoft : | 接続設定を指定してください。 SQL Server ○ Oracle Database ○ PostgreSQL | | |
| 接続設定 | | | |
| ホスト名: | jpsv01 | | |
| データベース名: | dsm | | |
| ユーザ名: | sa | | |
| パスワード: | •••••• | | |
| | | | 言羊糸田 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | A > = ====: |
| | | 〈戻る 次 | |

7) [システムチェックを開始]をクリックして、インストールチェックを行う

| 0 | Trend Mic | ro Deep Security Ma | anager 12.0.296のセットアッ | プウィザード | _ 🗆 X | | | |
|-----------------------------|-----------------------------------------------------------------|-------------------------------------|------------------------------------------------|------------|-------|--|--|--|
| Trend Micro D | Trend Micro Deep Security Manager 12.0システムチェック | | | | | | | |
| 既存のコンポー 了 このチェ システムチェ | -ネントがDeep Security Manager 12 :ックを実行してもインストールは開始され :ックを開始 | 0に対応しているかどうかを確認 れません。チェックの完了後に、^ | するには、[システムチェックを開始] をか。 (ンストールするかどうかを選択できます。 | Jックしてください。 | | | | |
| 結果 | コンボーネント | 理由 | | 書羊糸田 | | | | |
| | Deep Security Managerのホストの Deep Security Managerホストの: | JS メモリ | | | | | | |
| 0 | Deep Security Managerホストの 空母 | ディスク | | | | | | |
| 0 | データベース | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | キャンセル | | | |



8) システムチェックの結果がすべてグリーンステータスとなることを確認して、

[Deep Security Manager をインストールをクリックする

|) | Trend Micro D | eep Security Manager 12.0.296のセ | ットアップウィザード | _ 🗆 🗙 | | |
|-----------------------------------------------|-------------------------------------|----------------------------------------------|------------|---------------|--|--|
| rend Micro Deep Security Manager 12.0システムチェック | | | | | | |
| | | | | > | | |
| インストールのシ | ステムチェックが完了しました。 | | 結果の概要を表示 | インストール手順を表示 | | |
| 結果 | コンポーネント | 理由 | | 目羊糸田 | | |
| O | Deep Security ManagerのホストOS | Windows Server 2012 R2はサポートされます。 | | なし | | |
| O | Deep Security Managerホストのメモリ | 8 GB RAM | | なし | | |
| 0 | Deep Security Managerホストのディスク 容量 | 29.4 GBの空き | | なし | | |
| 0 | データベース | jpsv01: Microsoft SQL Server 2012 Standardエデ | イション | なし | | |
| | | | | | | |
| Deep Seci | urity Managerをインストール | チェックを再開 | | | | |
| | | | | الجار لاستغار | | |

9) アクティベーションコードを入力する

| Trend Micro De | ep Security | / Manag | er 12.0.2 | 296のセット | 、アップウィサ | ^r ード | | - 🗆 X |
|------------------------------|-------------|---------|-----------|---------|---------|-----------------|-----|-------|
| 製品のアクティベーション | | | | | | | | Ø |
| アクティベーションコードを入力してください。 | | | | | | | | |
| ● 複数の保護モジュール用の単一アクティベーションコード | | | | | | | | |
| すべての保護モジュール | - | - | - | | | - | | |
| ○ 各保護モジュール用の個別アクティベーションコード | | | | | | | | |
| 不正プログラム対策とWebレビュテーション | - | - | - | - | - | - | | |
| ファイアウォールと侵入防御 | - | - | - | - | - | - | | |
| 変更監視とアプリケーションコントロール | | - | - | - | - | - | | |
| セキュリティログ監視 | _ | - | - | - | - | - | | |
| ○ アクティベーションを実行せずに続け | | | | | | | | |
| | | | | | | | 次へ> | キャンセル |





Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

12) セキュリティアップデートの設定を行う

・ [セキュリティアップデートを定期的に実行する予約タスクを作成する] :

チェックボックスを入力

[トレンドマイクロのアップデートサーバに接続するときにプロキシサーバを使用] :

- プロキシサーバ経由でアクセスする場合にはチェックボックスを入力し、プロキ

シサーバの情報、認証情報(オプション)を入力

- 対応するプロトコルは HTTP、SOCKS4、SOCKS5

| Trend Micro Deep Security Manager 12.0.296のセットアップウィザード | _ 🗆 🗙 |
|--------------------------------------------------------|---------|
| セキュリティアップデートの設定 | 🥏 |
| セキュリティアップデートはお使いのシステムを最新の客蔵から保護します | |
| ✓ セキュリティアップデートを定期的に実行する予約タスクを作成 | |
| □ トレンドマイクロのアップデートサーバに接続するときにプロキシサーバを使用 | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| 〈厧る】 | > キャンセル |

13) ソフトウェアアップデートの設定を行う

・ [ソフトウェアアップデートを定期的に実行する予約タスクを作成する]:

チェックボックスを入力

· [トレンドマイクロのダウンロードセンターに接続するときにプロキシサーバを使用]:

プロキシサーバ経由でアクセスする場合にはチェックボックスを入力し、プロキ

- シサーバの情報、認証情報(オプション)を入力
- 対応するプロトコルは HTTP、SOCKS4、SOCKS5

| • | Trend Micro Deep Security Manager 12.0.2 | 296のセットアップウィザード | _ • × |
|--------------------------------------------------------------|--------------------------------------------------------------------------------|-----------------|-----------|
| ソフトウェアアップデートの | 設定 | | 1 |
| ソフトウェアアップデートは改善され ✓ ソフトウェアアップデートを定期 □ トレンドマイカロのダウンロード・ | にた機能と修正すログラムでお使いのシステムを常に最新の状態に維持し 的に実行する予約タスクを作成 や /5~(抹線をする)をにつたりサーバを使用 | 187 | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | 〈 戻る | 次ヘン キャンセル |



14) マスターキーを生成して暗号化するためのオプションについては[後で設定]を選択する

| Trend Micro Deep Security Manager 12.0.296のセットアップウィザード |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 729-4- |
| マスターキーを生成して暗号化するためのオブションを選択します。 |
| マスターキーを使用して、データベース内の個人データ、設定ファイル内のデータベースとKeystore/スワードを暗号化することができます。ストレージ内の個人データ(個人情報ま たはPIDEも呼ばれます)やハスワードの暗号化により、セキュリティが強化されます。これは、欧州協連合(EU)の一般データ保護規則(GDPR)などの要求事項でもあります。イ ンストール完了では、必要なときにマスターキーを接号して使用するため、Deep Security Managerサーバのすべてのノードから、下記のオブションを選択する際に生成されたファイ ルビッビーロンPTである人の単体があります。 |
| ● 後で設定 <u>詳細を表示。</u> |
| Amazon Web Services (AWS) Key Management Service (KMS) を使用する |
| Amazon Resource Name (ARN): |
| ○ ローカル環境変数(自動作成)を使用する |
| |
| 〈戻る 次へ〉 キャンセル |

15) DSM に Relay サーバ(DSR)を同居させるため、[*Relay 有効化済み Agent をインストール]*にチェックを入 れる

| Trend Mi | ro Deep Security Manag | er 12.0.296のセットアップウィザ | <u>~</u> ۴ | - 🗆 X |
|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|----------------------------------------------------|---------------------------------------|-----------------------|
| Relay 有効化済み Agent | | | | 0 |
| Relay有効化済みのDeep Security AgentをDeep デートおよびソフトウェアアップデートをダウンロードして い場合、後からインストールして設定する必要があり。 「Relay有効化済みAgentをインストール | Security Managerと同じコンピュータにイ 2件するためには、少なくとも1つのRela す。 | ′ンストールするには、このオプションを使用 /有効化/済み Aeentが必要です。Relay4 | します。Deep Securityで 見か比済み Agentをここで | セキュリティアップ インストールしな |
| | | | | |
| | | | 〈戻る 次へ〉 | キャンセル |



16) トレンドマイクロスマートフィードバックを有効にしたまま、業種情報を入力する(任意)

| 0 | Trend Micro Deep Security Manager 12.0.296のセットアップウィザード | - 🗆 X |
|-----------------------------------------------|------------------------------------------------------------------------------------------------|----------|
| Smart Protection Network | с с | 0 |
| TRENO MICRO SMART PROTECTION NETWORK | Trend Micro Smart Protection Networkは、最新の脅威に対してプロアクティブな保護を提供するように設計された、 ド型のコンテンツセキュリティ基盤です。 | 次世代のクラウ |
| | ードハックを有効にする(推奨) | |
| トレンドマイクロスマートフィ コンソールからいつでも無い | ードバックを有効にすると、匿名の脅威情報がSmart Protection Networkに送信され、分析に役立てられます。スマートフィードバ 防にできます。 | (ックは、製品の |
| 業種 (オプション): 指定が | ลเ | * |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | 〈戻る〉 | キャンセル |

17) インストール情報を確認し、【インストール】ボタンをクリックする

インストールの完了まで10分程度かかります。

| インストール情報 Deep Security Managerのインストーノ インストールパス: | ルの横要を確認してください。 | Õ |
|-------------------------------------------------------|---------------------------------------------------|---|
| Deep Security Managerのインストール | ルの概要を確認してください。 | |
| インストールパス: | | |
| | C#Program Files#Trend Micro#Deep Security Manager | ^ |
| インストールモード: | 新規インストール | |
| Managerアドレス: | https://DSM03.trendnsx.local | |
| Manager# | 4119 | |
| //-re-r#-r: | 4120 | = |
| 管理者アカウント: | Master Admin | |
| データベース: | Microsoft SQL Server | |
| データベースのホスト名: | jpsv01 | |
| データベース名: ニータベース名: | dsm | |
| 7-91-21-94: | 80 | |
| マスターキーの設定: | 設定されていません | × |





18) インストール完了を確認する



19) Deep Security Manager にログインできることを確認する

インストール完了画面からログインしない場合には、ブラウザにて以下の URL でアクセスしてトップ画面が表示されることを確認します。

https:// < DSM_Host_Name_or_IP >:4119

| | 💋 IRENS Deep Security MasterAdmin・1 ② ヘルブ ③ サボード捕服 | ・ Q ヘルブセンターの検索 |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| | ダッシュボード アラート イベントとレボート コンピュータ ポリシー 管理 | |
| | Default + | |
| | すべて ▼ 24時間表示 ▼ すべてのコンピュータ ▼ ▶ フィルタの適用 | 🔶 ウィジェットの追加/削除 |
| 🕖 I९६२२ Deep Security ॒ ≎ ७.स.–।/तिस | ▲ アラートステータス × ■ コンピュータのステータス × 🔹 ユーザ情報の概要 | |
| ログオン | ● 重大: 1 ● 警告: 0 2者のアラート: 那日 ● CPUの重大しきい値の超過 0分 ス ● 2日の ● 2日の | 1 |
| 今要共認証を使用する ログオン | | |



20) DSM に必要なパッケージがインポートされていることを確認する [管理]>[ソフトウェア]>[ローカル]

| ~ | 6 | セキュリティ | | | | | |
|---|---|------------|------------------------------------------|-------------------------------|------------|----------|------------------|
| | | | 🖲 Agent-Windows-12.0.0-481.i386.zip | Microsoft Windows (32 bit) | 12.0.0.481 | | 2019-08-10 14:22 |
| | | ▶ ルール | Agent-Windows-12.0.0-481.x86_64.zip | Microsoft Windows (64 bit) | 12.0.0.481 | | 2019-08-10 14:21 |
| | | 🔹 パターンファイノ | Agent-Windows-12.0.0-682.i386.zip | Microsoft Windows (32 bit) | 12.0.0.682 | 0 | 2019-11-06 14:21 |
| ~ | 0 | ソフトウェア | Agent-Windows-12.0.0-682.x86_64.zip | Microsoft Windows (64 bit) | 12.0.0.682 | 0 | 2019-11-06 14:20 |
| | | 🕭 ダウンロードセ | Appliance-ESX-12.0.0-206.x86_64.zip | ESX (64 bit) | 12.0.0.206 | | 2019-05-23 23:11 |
| | | 📄 ローカル | Agent-CloudLinux_7-12.0.0-682.x86_64.zip | CloudLinux 7 (64 bit) | 12.0.0.682 | × | 2019-11-06 14:21 |
| | 1 | Relayの管理 | Agent-RedHat_EL7-12.0.0-682.x86_64.zip | Red Hat Enterprise 7 (64 bit) | 12.0.0.682 | × - | 2019-11-06 14:21 |
| | | | Agent-Windows-12.0.0-563.i386.zip | Microsoft Windows (32 bit) | 12.0.0.563 | * | 2019-09-14 14:20 |
| | | | Agent-Windows-12.0.0-563.x86_64.zip | Microsoft Windows (64 bit) | 12.0.0.563 | * | 2019-09-14 14:20 |
| | | | Appliance-ESX-12.0.0-364.x86_64.zip | ESX (64 bit) | 12.0.0.364 | × | 2019-06-27 17:05 |
| | | | IternelSupport-CloudLinux_7−12.0.0−65… | CloudLinux 7 (64 bit) | 12.0.0.657 | × | 2019-10-18 14:21 |
| | | | KernelSupport-RedHat_EL7-12.0.0-716 | Red Hat Enterprise 7 (64 bit) | 12.0.0.716 | × | 2019-11-15 14:20 |

2-3-3. NSX ファブリック設定 - NSX Manager への vCenter Server の登録

NSX Manager から vCenter Server をコンピュートマネージャとして登録を行います。





1) NSX Manager にアクセスをして

[システム]>[ファブリック]>[コンピュート マネージャを選択して、[追加]を選択する

| vm NSX-T | | |
|------------------------------|-----------------------------------|------------|
| ホーム ネットワーク セキ | ュリティ インベントリ プランとトラブルシュー | -ティング システム |
| ~ | コンビュート マネージャ | |
| ② システム概要 | +追加 ∂ 編集 前削除 @ アクション、 | |
| 設定 ① アプライアンス | コンビュート マネージャの作成 | () × |
| 旦 はじめに | 名前• vc01.trendnsx.local | |
| コアブリック | 説明 | |
| プロファイル | ドメイン名/IP アドレス vc01.trendnsx.local | |
| トランスポート ゾーン コンピュート マネージャ | タイプ・ vCenter Server | ~ |
| - | ユーザー名・ Administrator | |
| | パスワード・ | |
| | SHA-256 サムプリント | |
| | +v | ンセル 追加 |

- 【名前】 : vCenter Server 名を設定
 [ドメイン名/IP アドレス] : vCenter Server のドメイン名または IP アドレスを設定
 [タイプ] : "vCenter Server"を選択
 [ユーザ名] : vCenter Server の管理者権限を持ったユーザ名を設定
 [パスワード] : 管理者権限を持ったユーザの管理者パスワード
- 2) コンピュートマネージャとして vCenter Server が正常に登録されていることを確認する

| ホーム ネットワーク | セキュリティ インベントリ ツール システム ネットワークとセキュリティの詳細段定 | |
|------------------------------------------|---------------------------------------------------------------------------|-------|
| | ベ コンピュート マネージャ | |
| 2 根要 2 はじゅに | + 遠加 ⊘ 編集 ① 削除 ⑧ アクション マ | Q. 検索 |
| | □ コンピュートマネージャ ↑ ID ドメイン名/IP アドレス タイプ 登録状態 バージョン | 接続状態 |
| D ファブリック | ▼ □ vc01.trendnsx.local 1a56693e vc01.trendnsx.local vCenter ● 登録済み 6.7.0 | ● 稼動中 |
| ノード | | |
| プロファイル | | |
| トランスボート ゾーン | | |
| コンピュート マネージャ | | |
| ・ [登録状態 ・ 「接続状態 | | |



2-3-4. NSX ファブリック設定 - トランスポートゾーンの設定

DSVA で保護を行う仮想マシンが展開される ESXi ホスト及びホスト上のネットワークを指定するための"トランス ポートゾーン"を設定します。(すでに設定されている場合はスキップしてください。)

"トランスポートゾーン"は、vCenter Server 上のクラスタとは別の概念として設定されますが、ESXi ホストに展開 される仮想マシンは vCenter Server で規定されるクラスタ・リソースプールに応じて vMotion/DRS が実行される ことになります。DSVA によるセキュリティを担保するためには vCenter Server で規定されているクラスタに所属 する ESXi ホストの範囲と同一となるように"トランスポートゾーン"を規定することを推奨します。





1) NSX Manager にアクセスをして

[システム]>[ファブリック]>[トランスポート ゾーンを選択して、[追加を選択する

| ホーム ネットワーク | セキュリティ | インベントリ : | プランとトラブルシューティング | システム |
|----------------|-----------------------------------------|------------------------|-------------------------------------------------------------------------|--------------|
| " | トランス | ボート ゾーン | | |
| ② システム概要 | 十追加 | ∽編集 前削除 | ◎ アクション ~ | |
| 設定 | | >スポートゾーン ↑ | ID | トラフィック |
| ☺ アプライアンス | | トランスボー | トゾーンの作成 | () × |
| 旦 はじめに | | 2 #• | Nevt eV TO Tere | |
| Jァブリック マ | | 石削。 | NSX1-SV-TP-Zone | |
| ノード | | 説明 | | |
| プロファイル | | NUDS 7 | | |
| トランスポート ゾーン | | ホストのメンバーシ | | |
| | | - ップ基準 | ・ 標準(すべてのホスト) ・ ・ ・ | の ESXi ホスト用) |
| | | トラフィック タイプ | 0 オーバーレイ | |
| | | | • VLAN | |
| | | アップリンク チーミ ング ポリシータ | | |
| | | 22 M 22 M | | |
| | | | | |
| | | | | キャンセル 追加 |
| | | | | |
| ・ [名前] | : トラ | ランスポートゾーン | レ名を設定 | |
| ・ [接続状態] | : N- | VDS 名を設定 | | |
| · [ホストのメンバーシップ | 基準] :"樗 | [準(すべてのホ) | スト)"または"拡張データパン | ス"を構成に従って選 |
| ・「トラフィックタイプ」 | : "オ | ーバーレイ"また | -は"VLAN"を構成に従って | 巽択 |
| | • | | | |
| | | 言定されているこ | レを確認する | |
| 設定したトランスポート ゾー | - ///////////////////////////////////// | | | |

| ② 概要 | | + 追加 ⊘ 編集 − 前 削除 ◎ アク | 7ション ∽ | | | | |
|-------------|------------------------------------------------|-----------------------|----------|------------|----------------|-------|---------------|
| 旦 はじめに | | □ トランスポート ゾーン ↑ | ID | トラフィック タイプ | N-VDS 名 | 状態 | ホストのメンバーシップ基3 |
| 显 ファブリック | ~ | NSXT-SV-TP-Zone | 6b64274c | VLAN | NSXT-SV-TP-VDS | ● 稼動中 | 標準 |
| ノード | | | | | | | |
| プロファイル | | | | | | | |
| トランスポート ゾーン | | | | | | | |
| · [N-VDS | ・ [N-VDS 名] : 設定した N-VDS 名が指定されていることを確認 | | | | | | |
| ・ [状態] | | :"稼働中"となっていることを確認 | | | | | |



2-3-5. NSX ファブリック設定 - トランスポートノードプロファイルの設定

DSVA で保護を行う仮想マシンが展開される ESXi ホスト上のネットワーク設定するために、トランスポートゾーン プロファイルを設定する必要があります。(すでに設定されている場合はスキップしてください。)



1) NSX Manager にアクセスをして

*[システム]>[ファブリック]>[プロファイル]>[トランスポート ノード プロファイルを*選択して、 *[追加*を選択する

| VM NSX-T | | | | | | | Q | Д | ?~ |
|------------|----|----------------|---------------|------------------|---------------------|--------------|-----|-----|------|
| ホーム ネットワーク | セキ | ュリティ インベントリ プラ | ンとトラブルシューティング | システム ネットワークと | セキュリティの詳細設定 | | | | |
| | ~ | アップリンク ブロファイル | NIOC プロファイル | Edge クラスタ ブロファイル | Edge ブリッジ プロファイル 設定 | ミートランスボート | ノード | ・ブロ | ファイル |
| ② システム概要 | Î | + 追加 ⊘ 繰集 前 削除 | | | | | | | |
| 設定 | | □ 名前 ↑ ID | 説明 | トランスポート ゾーン 適用され | たクラスタ ホスト スイッチのタイ | (フ ホスト スイッチ名 | 物理N | C | IP |
| 🗊 アプライアンス | | | | | | | | | |
| 旦 はじめに | | | | | | | | | |
| ファブリック 、 | / | | | | | | | | |
| ノード | | | | | | | | | |
| プロファイル | | | | | | | | | |

| MICRO [™] <i>「全船</i> 内ブでトランス; | to the Cloud ポートノードの概要設定を行う | インテグレーションガ |
|-------------------------------------------|--------------------------------|---------------|
| トランスボート ノード J | アロファイルの追加 ③ × | |
| 全般 * N-VDS * | | |
| 名前★ TRENDNSX-NSX-T-01_F | Profile | |
| 兑明 | | |
| トランスポート ゾーン | | |
| ☑ 使用可能 (1) | 🗌 選択済み (1) | |
| Q NSXT-SV-TP-Zone (VLAN) | Q | |
| | 0 | |
| | | |
| < 戻る 次へ > レコード:1個中1~1 | 上限: 10 | |
| | | |
| | キャンセル 追加 | |
| ・ [名前] | : プロファイル名を | 指定 |
| ・「トランスポートバ | ーン] 先ほど作成した | -ランスポートゾーンを選択 |

| ·服 • N-VDS • | Î | 関連付けられたトラ ンスポート ゾーン | NSXT-SV-TP-Zone | |
|----------------------------------------|---------------------------------------|--------------------------------------|------------------------------------------|--------------------|
| I-VDS の作成● <mark>+ N-VDS の追加</mark> | ● NSX 作成 ○ 事前設定済み | Network I/O Control (NIOC) プロファイル | nsx-default-nioc-hostswitch-profile | * |
| > ノード スイッチの作 | FIQ | | NIOC | プロファイル の新規作成 |
| N-VDS名• | NSXT-SV-TP-VDS | アップリンク プロフ アイル・ | nsx-default-uplink-hostswitch-profile | ~ |
| 関連付けられたトラ ンスポート ゾーン | NSXT-SV-TP-Zone | LLDP プロファイル・ | アップリング LLDP [Send Packet Disabled] | 7 プロファイルの新規作成 〜 |
| Network I/O Control (NIOC) プロファイル | nsx-default-nioc-hostswitch-profile | IP アドレスの割り当 て・ | | ~ |
| | NIOC プロファイル の新規作成 | 物理 NIC | vmnic1 uplink-1 | ~ |
| アップリンク プロフ ァイル・ | nsx-default-uplink-hostswitch-profile | | | 物理 NIC |
| | アップリンク プロファイルの新規作成 | 物理 NIC のみの移行 | ltv | の追加 |
| LLDP プロファイル・ | LLDP [Send Packet Disabled] | Enable this option if no v | mks exist on PNIC selected for migration | |
| IP アドレスの割り当 て・ | | インストール用のネッグ | トワーク マッピン マッピングの追加 | |
| 物理 NIC | vmnici unlink-1 | アンインストール用の ピング | ネットワーク マッ マッピングの追加 | |



- ・ [物理 NIC]
- : 展開する ESXi ホストの環境に応じてアップリンクポートを指定

※プロファイル情報を含めて構築されている環境に応じて、適切なパラメータを設定してください。

4) トランスポートノードプロファイルが作成されていることを確認する

| ホーム ネットワーク | セキュリティ インベン | トリールシールシー | ステム ネットワー | -クとセキュリティの詳 | 細設定 | | | |
|-------------|-----------------------------------------|-------------|-------------------|-----------------|---------------|--------------|----------------|------------|
| « | ブリンク ブロファイル | Network I/O | Control (NIOC) ブロ | コファイル Edge | クラスタ ブロファイル E | dge ブリッジ ブロコ | ファイル 設定 | トランスボート ノ- |
| ② 概要 | ▲ 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 | 削除 | | | | | | |
| 旦 はじめに | □ 名前 ↑ | ID | 説明 | トランスポート ゾーン | 適用されたクラスタ | ホスト スイッチのタイプ | ホスト スイッチ名 | 物理 NIC |
| コアブリック | TRENDNSX-NSX | f01fe62c | | NSXT-SV-TP-Zone | SV | NSX 作成 | NSXT-SV-TP-VDS | vmnic1 |
| ノード | | | | | | | | |
| プロファイル | | | | | | | | |
| トランスポート ゾーン | | | | | | | | |

2-3-6. NSX ファブリック設定 - トランスポートノードプロファイルの vSphere クラスタへの適用

トランスポートノードプロファイルを DSVA が展開される ESXi ホスト(vCenter Server 上のクラスタ単位で指定)に対して適用します。





1) *[システム]>[ファブリック]>[ノード]>[ホストトランスポートノード]*から*[管理元]*から登録した vCenter Server を選択

NSX を展開するクラスタを選択して[NSX の設定]を選択

| ホーム ネットワーク | セキュリティ インベントリ | プランとトラブルシューティング システム |
|----------------|-----------------------|------------------------------------|
| « | ホスト トランスボート | ノード Edge トランスポート ノード Ed |
| | 管理元 vc01.trendnsx.l | local 🗸 |
| 設定 | 像 NSX の設定 前 NSX の削 | 川除 遼 アクション ~ |
| ☆ アプライアンス | コーノード | ID IP アドレス OS タイプ |
| | □ ▷ VDI-Seg (1) | MoRef ID: |
| 旦 ほしめに | ✓ ▲ SV (3) | MoRef ID: |
| 🗄 ファブリック 🛛 🗸 🗸 | | |
| ノード | esx-sv02.trendns | 56b39f09 10.3.225.147、1 ESXI 6.7.0 |
| プロファイル | esx-sv03.trendns | eafc7be8 10.3.225.148、1 ESXi 6.7.0 |
| ノロノアイル | esx-sv01.trendnsx | 5848543f 10.3.225.146、1 ESXi 6.7.0 |
| トランスポート ゾーン | | |
| コンピュート マネージャ | □ ▷ Manage (3) | MoRef ID: |

2) 先ほど設定したトランスポートノードプロファイルを展開プロファイルとして選択して保存をする



3) 配信先のクラスタに対してトランスポートノードプロファイルが正常に展開されているかを確認する

| vm NSX-T | | | | | | | | | Ql |) () | admin v |
|--------------|--------------------|-----------|-----------------|------------|-----------|-------------|-----------------------------|-----------|-------------|--------------------|---------|
| ホーム ネットワーク せ | 2キュリティ インベントリ | プランとトラス | ブルシューティング | システム | ネットワー | クとセキュリティの詳 | 細設定 | | | | |
| * | ホスト トランスボート | ノード Edg | ge トランスボート | トノード | Edge クラスタ | ・ ESXI ブリッジ | クラスタ | | | | |
| ② システム概要 | 管理元 vc01.trendnsx. | local 🗸 | | | | | | | | | |
| 設定 | 億 NSX の設定 前 NSX の前 | 降 🔞 アクシ | (=>~ | | | | | | 表示 3 | 777 | v |
| の アプライアンス | ローノード | ID | IP アドレス | OS タイプ | NSX證定 | 設定の状態 | ノードの状態 | トンネル | トランスポート | ゾーン NSX パージョン | N-VDS |
| 旦 はじめに | □ ▷ VDI-Seg (1) | MoRef ID: | | | _ | | ●1台のホストが未構 | | | | |
| □ ファブリック v | □ ▲ SV (3) | MoRef ID: | | | Ø TRENDNS | X | ● 3 台の木ストが稼動 | | | | |
| ノード | esx-sv02.trendns | 56b39f09 | 10.3.225.147、 1 | ESXi 6.7.0 | 設定済み | ● 成功 | ● 稼動中 ① | 使用不可 | NSXT-SV-TP- | Zo 2.5.0.0.0.14663 | L 1 |
| プロファイル | esx-sv01.trendnsx | 5848543f | 10.3.225.146. 1 | ESXi 6.7.0 | 設定済み | ● 成功 | ● 稼動中 ② | 使用不可 | NSXT-SV-TP- | Zo 2.5.0.0.0.14663 | L 1 |
| トランスポート ゾーン | esx-sv03.trendns | eafc7be8 | 10.3.225.148、 1 | ESXi 6.7.0 | 設定済み | ● 成功 | ● 線動中 ② | 使用不可 | NSXT-SV-TP- | Zo 2.5.0.0.0.14663 | 1 |
| コンピュート マネージャ | □ ▷ Manage (3) | MoRef ID: | | | | | ◎ 3 台のホストが未構 | | | | |
| | | | | | | | | 表示 | ন কাশব | | ~ |
| | | | | | | | ι, | N-VDS: 6 | sx-sv02.tre | nunsx.local | × |
| | | | | | | | - T | N-VDS 名 | | アップリンクプロフ | アイノ |
| | | | | | | | 7 | NSXT-SV-T | P-VDS | nsx-default-uplink | ¢ |
| | | | | | | | 귀 | | | | 1 |
| | | | | | | | F | | | | 1 |
| | | | | | | | | | | | .:: |

| | Securing Your Journey to the Cloud | Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド |
|------------|---------------------------------------|--------------------------------------------------------------------|
| ・ [NSX 設定] | : クラスタに対して適用 | したトランスポートノードプロファイルが適用されており、 |
| | "x台のホストが稼働中 | "となっていることを確認 |
| | また、各ホストでは"討 | と定済み"となっていることも確認 |
| ・ [設定の状態] | :各ホストの状態が"尿 | え功"となっていることを確認 |
| ・ [ノードの状態] | : 各ホストの状態が"和 | 家働中"となっていることを確認 |
| • [N-VDS] | : トランスポートノード | プロファイルで指定した N−VDS の展開を確認する |

また、vCenter Server 上でも各ホスト上で N-VDS が展開されていることを確認する

| 🐻 esx-sv02.trend | nsx.local アクション ~ |
|--------------------------------------|--------------------------------------------------------------------------------------------|
| サマリ 監視 設定 | 権限 仮想マシン データストア ネットワーク アップデート |
| マストレージ ▲ ストレージアダプタ | 仮想スイッチ [|
| ストレージデバイス | > 標準スイッチ: vSwitch0 |
| プロトコルエンドボー | > 標準スイッチ: vSwitch1 |
| 1/0 フィルタ ▼ ネットワーク | > 標準スイッチ: vmservice-vswitch |
| 仮想スイッチ VMkernel アダプタ | > 標準スイッチ: vSwitch2 |
| 物理アダプタ TCP/IP 設定 | V N-VDS: NSXT-SV-TP-VDS |
| ▼ 仮想マシン | |
| 仮想マシンの起動/シ エージェント仮想マ 仮想マシンのデフォ | ▲ TEST VLAN 10 仮想マシン(0) ● 物理アダプタ ■ vmnic11000 完全 |
| スワップ ファイルの マ システム | WMNetwork_NSX-T 仮想マシン (0) |
| フィセンス ホスト プロファイル | |
| 時間の設定 認証サービス | |



2-3-7. DSM&vCenter Server NSX Manager 連携設定

DSM にてvCenter Server 及び NSX Manager の連携設定を行い、インベントリ情報/セキュリティポリシーの同期、DSVA のデプロイが行えるようにします。



1) [コンピュータ]タブから右側ペインの[コンピュータ]を右クリックして、[VMware vCenter の追加]を選択する

| neep : | Security | MasterAdmin - ⑦ ヘルブ 〇 サボート情報 🕕 - 🔾 |
|----------------------------------------------|----------------------------------------------------------------------------------|----------------------------------------------|
| ダッシュボード 処理 🗄 | דאר איזא איז איז איז איז איז איז איז איז אי | ポリシー 管理 |
| スマートフォルダ | コンピュータ サブグルーブを含む 🔹 | グルーブ別 ▼ |
| ■ コンピュータ ■ コンピュータの追加 | +追加 - 面削除 国詳細 4 | 処理 • 首イベント • 臣 エクスポート • 田 列 |
| 🚦 Active Directoryの追加 🔐 VMware vCenterの追加 | 名前・説明 | ブラットフォー・・ ボリシー ステータス |
| ▲ AWSアカウントの追加 ▲ Azureアカウントの追加 | ✓ JJZューダ(1) [™] DSM03.trendnsx.local | Microsoft Win… Deep Security… 🔵 管理対象 (オンライン) |
| 🙆 vCloudアカウントの追加 | | |
| ▶ グループの作成 | | |
| | | |



2) 接続する vCenter Server の情報を設定する

| • | VMware vCenterの追加ウィザード - Google Chrome | - 🗆 | x |
|------------------------------------|-----------------------------------------|-------|---|
| ▲ 保護されていません │ https :// | 10.3.225.183:4119/VirtualWizard.screen? | | |
| 追加するvCenterの次の | 情報を指定してください。 | | |
| サーバ | | | |
| サーバのアドレス: | vc01.trendnsx.local | | |
| サーバのポート: | 443 | | |
| 名前 | | | |
| 名前: | vCenter - vo01.trendnsx.local | | |
| 説 明: | | | |
| 資格情報 | | | |
| ユーザ名: | administrator@trendnsx.local | | |
| パスワード: | | | |
| | | | |
| | | | |
| | 〈戻る 汝へ〉 | キャンセル | |
| ・「サーバのアドレ | val · vCenter Server サーバ名 | | |

- [**サーバのアドレス**] : .
- ・ **[サーバのポート]** :
- 【ユーザ名】 :
- [パスワード] : .
- 管理者権限を持ったユーザ名
- パスワード

443



3) [次へ]を押して、vCenter Server の接続を確認する

SSL 証明書を受け入れるかどうかの確認があった場合には**[受け入れる]**を選択します。

| 🤣 VMware vCenterの追加ウィザード - Google Chrom | ie 💶 🗆 🗙 |
|--------------------------------------------------------------|----------|
| ▲ 保護されていません https://10.3.225.183:4119/VirtualWizard.screen | |
| VMware vCenterに接続しています。しばらくお待ちください… | |
| | |
| | |
| | |
| | キャンセル |

※vCenter Server へのアクセスができない場合には、以下のようなエラーメッセージが表示されるため、vCenter Server へのアクセス情報を再確認します。

| 🥑 V | Mware vCenterの追加ウィザード - Google Chrome | - 🗆 X |
|---------------------------|---------------------------------------|-------|
| ▲ 保護されていません https://1 | 0.3.225.183:4119/VirtualWizard.screen | |
| vCenterFvc01.trendnsx.loc | 山に接続できません。接続を確認して再度実行してください。 | |
| 追加するvCenterの次の | 青報を指定してください。 | |
| サーバ | | |
| サーバのアドレス: | vc01.trendnsx.local | |
| サーバのボート: | 443 | |
| 名前 | | |
| 名前: | vCenter – vc01.trendnsx.local | |
| i兑8月: | | |
| 資格情報 | | |
| ユーザ名: | administrator@trendnsx.local | |
| パスワード: | | |
| | | |
| | 〈戻る 次へ〉 | キャンセル |



4) 接続する NSX Manager の情報を設定する

本番環境においては、NSX Manager は 3 台構成にすることを構成要件となっています。 vCenter Server から設 定する NSX Manager については NSX Manager で設定している Cluster VIP を必ず指定してください。

| 🧿 VMware vCenterの追加ウイザード - Goog | Jle Chrome | - | | Х |
|---------------------------------|-------------------------------|-----|-------|---|
| ▲ 保護されていない通信 10.3.225 | 183:4119/VirtualWizard.screen | | | |
| NSX Managerの設定は任意 | です。詳細については、ドキュメントを参照してください。 | | | |
| NSX Manager | | | | |
| Managerのアドレス: | 10.3.225.179 | | | |
| Managerのポート: | 443 | | | |
| 資格情報 | | | | |
| ユーザ名: | admin | | | |
| パスワード: | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | 〈戻る | 次へと | キャンセノ | ŀ |
| ・「Manager のアド | いしょう NSX Manager サー | -バ名 | | |

- [Manager のポート] : 443
- ・ [ユーザ名] :

[パスワード] :

NSX Manager 管理者権限を持ったユーザ名 パスワード

5) 【次へを押して、NSX Manager の接続を確認する

SSL 証明書を受け入れるかどうかの確認があった場合には「受け入れる」を選択します。

6) [コンピュータ内ブで右側ペインに vCenter Server のインベントリ情報が連携されていることを確認する





2-3-8. DSVA デプロイ

保護対象クラスタの各 ESXi ホストに対して DSVA を配信します。



NSX 環境においては、DSVA は NSX Manager からデプロイを行います。NSX Manager 経由で DSM または指定 された外部 Web サーバに格納されるソフトウェアパッケージに含まれる OVF ファイルを指定して、各 ESXi ホス トに対するデプロイを行う仕様となっています。

DSM を vCenter Server・NSX Manager と連携することにより、DSM ローカルに配置される DSVA ソフトウェアパ ッケージの URL(デフォルト)または、任意に指定した外部 Web サーバの DSVA ソフトウェアパッケージの URL が NSX Manager にリアルタイムに通知され、DSVA デプロイ時に使用する OVF URL が自動的に指定されま す。

DSVA は NSX に管理されたセキュリティ VM として ESX Agent Manager(EAM)に管理されたセキュリティアプラ イアンスとして扱われます。EAM により管理されたセキュリティ VM は、NSX Manager が vCenter Server 上で配 信対象のクラスタの配下に生成する"ESX Agents"フォルダの配下に配置されます。

> DSVA ソフトウェアパッケージとデプロイに必要なコンポーネント

DSVA のメジャーリリース(Long Term Support)毎に GM(初期リリース)版 OVF がリリースされます。メジャーリ リースで適宜リリースされる Update については、Redhat(64bit)版 DSA を利用してアップデートしたい Appliance バージョンのアップデートを行います。

(実際は、DSVA ソフトウェアパッケージと該当の DSA を DSM ローカルにダウンロードしておくことで、NSX からの"デプロイ"時に自動的に実行されます。)

※仕様変更などにより GM 以外でもメジャーリリース中に DSVA ソフトウェアパッケージがリリースされることがあります。できる限り最新のソフトウェアパッケージを利用することを推奨します。

(以下は 2019 年 12 月末時点の DS12.0 DSVA ソフトウェアパッケージ)



Appliance

| ソフト | ウェア | リリースの種類 | ビルド | リリース詳細 | リリース日 | ダウンロード |
|-----|-------------------------------------------------------------------------|---------|------------|--------|--------------|--------|
| ٠ | Deep Security Appliance 12.0.0-682 for ESX- x86_64 (12 LTS Update 3) | LTS | 12.0.0-682 | LTS | Dec 5, 2019 | Ŧ |
| ٠ | Deep Security Appliance 12.0.0-364 for ESX- x86_64 (12 LTS) | LTS | 12.0.0-364 | GA | Jun 19, 2019 | Ŧ |

DSVA の配信にあたっては、以下のコンポーネントを事前に DSM ヘアップロードされている必要があります。 【DS12.0】

DSM に以下の 2 つのコンポーネントをアップロードして、NSX から配信

- Deep Security Appliance 12.0.0-XXX for ESX-x86_64 (12 LTS Update 3) "Appliance-ESX-12.0.0-XXX.x86_64.zip"(XXX はビルド番号)
- RHEL 7 (x64) 用 Deep Security Agent

実際に配信したい Appliance バージョンについては、以下の設定画面から指定することが可能です。

(プルダウンには、DSM ローカルにアップロードした Appliance OVF と RHEL7 (x64) 用 Deep Security Agent の バージョンにより指定可能な DSVA 配信バージョンが表示されます。

[管理]>[システム設定]>[アップデート]>[Virtual Appliance の配置]

| 💋 TREND Deep S | Security | | | Master/ | Admin → 🃣=ュー | | 🔘 サポート情 | i報 → Q ヘルブセンタ | -の検索 |
|------------------|--------------------|--------------------------------------------|----------------|------------|----------------|------------------------------|---------------------|-----------------|------------------|
| ダッシュボード 処理 ・ | | | | — 管理 | | | | | |
| 🍄 システム設定 | システ | ム設定 | | | | | | | |
| 🔛 予約タスク | Agent 7 | アラート コンテキスト | イベントの転送 | ランク付け | システムイベント | セキュリティ | アップデート | スマートフィードバック | Connected Thr. 4 |
| 🕑 イベントベースタスク | | | | 1700-1 | | | | | |
| 🕖 Managerノード | Deep Secu | inity Relayの代わりとなる: | ノノトリェアアッフテー | ト間C1言サ 〜ハ: | | | | | |
| 5イセンス | | | | | | | 追加 | | |
| ◇ 📢 ユーザ管理 | | | | | | ^ | 削胏 | | |
| 48 ユーザ | 0 | | | | | | | | |
| 礼 役割 | | | | | | - | | | |
| ■ 連絡先 | 彌考 | ソフトウェアアップデートの | 配信サーバの設定方 | 法については、: | オンラインヘルプの「ソフ | ^ハウェアアップデ ー | -トサーバの設定 | 」を参照してください。 | |
| 🔍 API+ | | 「「の副署 | | | | _ | | | |
| > 🖪 アイデンティティン | virtual Ap 配置と同 | ppliance이머니브. 司時ICDeep Security Virtual | Applianceを次のバー | -ジョン/こアップグ | (レード: | | 利用可能な最 | 新バージョン (推奨) | - |
| 砲 システム情報 | | | | | | | 利用可能な最 12.0.0364 | 新バージョン (推奨) | |
| ◇ @ アップデート | | | | | | | | | |

▶ デプロイする DSVA のリソース設定

NSX-T2.4 までは、DSM へ DSVA OVF をアップロード後、DSM インストールフォルダ配下の以下のフォルダに格 納される dsva.ovf ファイルの中の以下のパラメータを修正することで変更が可能です。



<DSM_Install>¥temp¥Appliance-ESX-<appliance_version>



NSX-T2.5 以降の環境では、セクション 1.4.6 で記載の通り、NSX の仕様の変更に伴い、DSVA など 3rd Party Security VM を各ホストヘデプロイする際に NSX Manager がソフトウェアパッケージに対するデジタル署名のチ ェックを実行するプロセスが追加されています(ソフトウェアパッケージに含まれる.ovf 及び.vmdk ファイルに VMware 社によるデジタル署名が付与されます)。

NSX-T2.5 以降では、VMware 社によるデジタル署名が付与されている Deep Security 12.0 Update 3 以降の OVF パッケージを必ず使用する必要があり、DSVA に割り振るリソースに応じて以下の 4 種類の OVF ファイル から選択をする必要があります。

| OVF Files | vCPU | Memory |
|-----------------|------|---------|
| dsva.ovf | 2 | 4096MB |
| dsva-small.ovf | 2 | 8192MB |
| dsva-medium.ovf | 4 | 16384MB |
| dsva-large.ovf | 6 | 24576MB |

NSX-T2.5.0 以降の環境での DSVA ソフトウェアパッケージの扱い、デプロイの方法の詳細はセクション 1.4.6. NSX-T 2.5.0 以降のセキュリティ VM 配信時の仕様変更に伴う DSVA ソフトウェアパッケージの変更 を参照し てください。



展開する DSVA の基本設定(vCenter Server 上の配信先のクラスタ、配信するデータストア、DSVA の管理ポートが所属するネットワーク、配信する DSVA の仕様など)を選択する

: DSVA を配信するクラスタを指定

- ・ [サービス展開名]
- : 任意の名称を設定
- ・ [コンピュート マネージャ] : DSVA を配信するクラスタが所属する vCenter Server を指定
- ・ [クラスタ]
- ・ [データ ストア]
- ・ [ネットワーク]
- : DSVA を配信するデータストアを指定。"ホストで指定済み"または 任意のストレージデータストア
- : "詳細の編集"を選択"IP Pool"(推奨)または"DHCP"を選択

| 4IC 情報 | ネットワーク | ネットワーク タイプ | IP プール | |
|-----------------|------------|-------------|-------------------|---|
| 🖌 ens0 - 管理 NIC | VM Network | ✓ 静的 IP ブール | V NSXT-SVM-Pool01 | / |
| ens1 - 制御 NIC | システム設定 | システム設定 | システム設定 | |
| プールの管理 | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |



 IP プールを利用する場合で IP プールの設定がされていない場合には、"IP プールの管理"を選択して、[ネットワークとセキュリティの詳細設定]>[インベントリ]>[グループ]>[IP プール]へ移動 [追加ボタンを押して、"新しい IP プールの追加"を行う

| vm NSX-T | | | | | | | | |
|--------------------|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|-------------------------------------------------------|-----------------|
| ホーム ネッ | ットワーク | セキュリティ | インベントリ プラ | ランとトラブルシューティ | ング システム | ネットワークとセキュリ | ティの詳細設定 | |
| | « | グループ IP f | セット IP ブール | MACセット | | | | |
| 🛿 ネットワーク | > | 2010 《 45年 | | N | | | | |
| ◯ セキュリティ | > | 」 □ IPプール↑ | | ID | | 93 | ブネット | |
| う パートナー サービ | こス | | | | | | | |
| ら ツール | > | 新しいIPプ | ールの追加 | | | | | 0 |
| る インベントリ | ~ | 名前• | NSXT-SVM-Pool01 | | | | | |
| グループ | | 説明 | | | | | | |
| サービス | | | | | | | | |
| コンテキスト プロ 仮想マミハ | コファ | サブネット | | | | | | |
| 10/23 マンン | | 十追加 前削除 | | | | | | |
| | | | | | | | Date Handler | |
| | | ☑ 印範囲・ ☑ 10.3.225.243 | - 10.3.225.245 | ゲートウェイ 10.3.225.254 | CDR* | DNSサーバ 10.3.224.170 | trandnsx.local | ウス |
| | | ✓ IP範囲・ ✓ 10.3.225.243 | - 10.3.225.245 | ゲートウェイ 10.3.225.254 | 00R* | DNS サ− /(10.3.224.170 | trandnsx.local | <i>7</i> 2 |
| | | ✓ IP範囲・ ✓ 10.3.225.243 | - 10.3.225.245 | ゲートウェイ 10.3.225.254 | CDR * | DNS サ− / (10.3.224.170 | trendnsx.local | <u>うえ</u> 追加 |
| . | [IP 範囲 | ○ IP 範囲・ ○ 10.3.225.243 | · 10.3.225.245 : DSV/ (最低 | ^{ダートウェイ} 10.3.225.254 A (こ設定する管 DSVA を配信す | ^{でDR*} 10.3.225.0/24 [*] 理 IP の範囲 する ESXi ホス | DNS サーバ 10.3.224.170 を指定 ト数を設定) | trandnsx.local | <u>追加</u> |
| • | [IP 範囲 [ゲート [」] | ○ P 範囲・ ○ 10.3.225.243 引 うエイ] | - 10.3.225.245 : DSV/ (最低 : DSV/ | <u>ゲートウェイ</u> 10.3.225.254 A に設定する管 DSVA を配信す A に設定するテ | ^{で取・} 10.3.225.0/24 ^で 理 IP の範囲 する ESXi ホス でフォルトゲート | DNS サーバ 10.3.224.170 を指定 ト数を設定) -ウェイを設定 | レNS サブイター <u>trandnsx.local</u> キャンセル | 追加 |
| · · | [IP 範囲 [ゲート [」] [CIDR] | ○ P 範囲・ ○ 10.3.225.243 日] ウェイ] | - 10.3.225.245 : DSV/ (最低 : DSV/ : DSV/ | ^{タートウェイ} 10.3.225.254 A に設定する管 DSVA を配信で A に設定するテ A の管理 IP が | ^{でDR・} 10.3.225.0/24 ⁵ 理 IP の範囲 する ESXi ホス ⁵ フォルトゲート 所属するサブ | DNS サーバ 10.3.224.170 を指定 ト数を設定) 、ウェイを設定 ネットを CIDR 形 | UNS サブイサ・ <u>trendnsx.local</u> キャンセル | <u>送加</u> |
| · · | [IP 範囲 [ゲート [」] [CIDR] | ○ P範囲・ ○ 10.3.225.243 日 □ □< | - 10.3.225.245 : DSV/ (最低 : DSV/ : DSV/ (個)) | ^{タートウェイ} 10.3.225.254 A に設定する管 DSVA を配信で A に設定するテ A の管理 IP が 10.3.225.0/24 | ^{でDR・} ^{10.3.225.0/24 ⁵理 IP の範囲 する ESXi ホス ⁵フォルトゲート 所属するサブ} | ^{DNS サ−JK} 10.3.224.170 を指定 ト数を設定) >ウェイを設定 ネットを CIDR 形 | UNS 9 J 49 <u>trendnsz.local</u> キャンセル ジ式で設定 | 追加 |
| · · | [IP 範囲 [ゲート [」] [CIDR] | ○ P 範囲・ ○ 10.3.225.243 日] ウェイ] | - 10.3.225.245 : DSV/ (最低 : DSV/ : DSV/ (例) | ^{タートウェイ} 10.3.225.254 A に設定する管 DSVA を配信で A に設定するテ A の管理 IP が 10.3.225.0/24 A が参照するこ | TER 10.3.225.0/24 TER の範囲 する ESXi ホス フォルトゲート 所属するサブ | DNS サーバ 10.3.224.170 を指定 ト数を設定) 、ウェイを設定 ネットを CIDR 形 | UNS 9749- <u>trendnsz.local</u> キャンセル ジ式で設定 | <u>注色かれ</u> |
| · • • | [IP 範囲 [ゲート [,] [CIDR] [DNS サ | □ P範囲・ □ 10.3.225.243 □ 10.3.225.243 □ 10.3.225.243 □ 10.3.225.243 | - 10.3.225.245 : DSV/ (最低 : DSV/ : DSV/ (例) : DSV/ | ^{タートウェイ} 10.3.225.254 A に設定する管 DSVA を配信で A に設定するテ A の管理 IP が 10.3.225.0/24 A が参照するロ | T理 IP の範囲 する ESXi ホス フォルトゲート 所属するサブ | DNS サーバ 10.3.224.170 を指定 ト数を設定) 、ウェイを設定 ネットを CIDR 形 サーバを設定 | Uns 9979- <u>trandnsz.locat</u> キャンセル ジ式で設定 | 道加 |

② IP プールが正しく設定されていることを確認する

| vm NSX-T | | | | | ς φ | admin ~ |
|-----------------|--------------|-----------------------------|--------------------|--------------------|------|---------|
| ホーム ネット | ・ワーク | セキュリティ インベントリ プラ | ンとトラブルシューティング システム | ネットワークとセキュリティの詳細設定 | | |
| | ~ | グループ IP セット IP プール | MAC セット | | | |
| ◎ ネットワーク | > | +追加 2 編集 前剤降 @ アクション | / v | | | |
| ○ セキュリティ | > | □ ₽プール † | ID | サブネット | 割り当て | |
| ◇ バートナー サービス | | NSXT-SVM-Pool01 | 066d1ed4 | | 1 | 3/3 |
| @ ツール | > | SI_Destination_IP_Pool | 7f048047 | | 1 | 0/248 |
| あ インベントリ | ~ | SI_Service_Chain_ID_IP_Pool | 654d1040 | | 1 | 0/1022 |
| グループ | | SI_Source_IP_Pool | 6113f603 | | 1 | 0/248 |
| サービス | | | | | | |
| コンテキスト プロフ | ? <i>?</i> ? | | | | | |
| 仮想マシン | | | | | | |



[TIPS]

DSVA を配信するデータストア、ネットワークがプルダウンから表示されない場合には、vCenter Server にて配 信先のホストの*[設定]>[仮想マシン]>[エージェント仮想マシンの設定]*からデプロイしたいデータストア、ネット ワークを指定する必要があります(このパラメータが NULL/空欄の場合には DSVA のデプロイに失敗します)。

| vm vSphere Client メニュー ∨ Q す | べて <i>の</i> 環境を検索 | |
|----------------------------------|-------------------------------------------|----------------|
| | ■ esx-sv03.trendnsx.local アクション ~ | |
| > 🗍 Manage | ▲ サマリ 監視 設定 権限 仮想マシン データストア ネットワーク アップデート | |
| > 📋 VDI-Seg -> <u>I</u> NSX-T | TCP/IP 設定 ◆ 仮想マシン | |
| ∨ 📋 sv | 仮想マシンの起動/シ データストア | datastore1 (2) |
| 👵 esx-sv01.trendnsx.local | エージェント仮想マ | |
| 🔓 esx-sv02.trendnsx.local | 仮想マシンのデフォ ネットワーク | VM Network |
| le esx-sv03.trendnsx.local | スワップ ファイルの | |

- 2) すべての設定が終わったら[保存]ボタンを選択して、DSVA のデプロイを開始する
 - デプロイの状態が"進行中"になっていることを確認して、デプロイの完了を待つ(数分かかります。適 宜 Web Client GUI のリロードを行って状態を確認してください。)

| | サービス展開名 | コンピュート マネージャ | クラスタ | データストア | ネットワーク | 状態 |
|-------|--------------------------------------|---------------------|--------------------|--------|--------|---------|
| : > 🖓 | 4039a490-2ab8-11ea-9348-09101749499a | vc01.trendnsx.local | SV (domain-c14117) | ホストに指定 | 詳細の表示 | 😑 進行中 🕕 |

- 進行中の状態にならず、配信が失敗する場合には NSX Manager が正しく DSVA のソフトウェアパッケ ージが認識できない、またはデプロイに必要なパラメータに不足または修正が必要な状態であると考 えられるため、エラー状態の確認・修正の上、DSVA を再度デプロイする必要があります。
- 3) DSVA が正常にデプロイされたことを確認する

| vm NSX-T | | | | | | QA | ⊘~ adn | nin 🗸 |
|-------------|-----------------------------------|--------------------------------------|---------------------|--------------------|---------|-------------------------|---------|-------|
| ホーム ネットワーク | セキュリティ インハ | ベントリ プランとトラブルシューティング | システム ネットワークと | セキュリティの詳細設定 | | | | |
| (2) システム概要 | ▲ Ø ² 展開 サ パートナーサービ | ービス インスタンス カタログ | 細衣表示 | | | | | 0 |
| 設定 | | | 44 C 500 | | | | | |
| ☺ アプライアンス | DEPLOY SERVICE | | | | | すべてを非表示 Q | 検索 | |
| 旦 はじめに | | サービス展開名 | コンピュート マネージャ | クラスタ | データストア | ネットワーク | 秋熙 | |
| コアブリック | : ~ 🕫 | 4039a490-2ab8-11ea-9348-09101749499a | vc01.trendnsx.local | SV (domain-c14117) | ホストに指定 | 詳細の表示 | ● 稼動中 ① | |
| ノード | | | | | | | | |
| プロファイル | | 展開の仕様 Deep Security | - Medium () | 展開テンプレート | EPP_Att | tributes_For_OVF_Env_Va | ars | |
| トランスポート ゾーン | | | | | 腐性の表 | দ্য | | |

· [状態] : 稼働中



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

また、該当クラスタ配下の[ESX Agents]に対象となる ESXi ホスト台数分の DSVA が配信されていることを確認 してください。

| vm vSphere Client ×= | Q | | | | |
|-----------------------------------|--------------------------------------------------|----------------------------------|---------------------------------|---------------------------------|------------------------|
| | | | | | |
| vc01.trendnsx.local | | | | | |
| | | | | | |
| > 🗍 Manage | | | | | |
| > 🕅 VDI-Seg | | | | | |
| ✓ In NSX-T | | | | | |
| √ □ sv | | | | | |
| esx-sv01.trendnsx.local | | | | | |
| esx-sv02.trendnsx.local | | | | | |
| esx-sv03.trendnsx.local | | | | | |
| V R ESX Agents | | | | | |
| Trend Micro_Deep Secu | rity (1) | | | | |
| Trend Micro_Deep Secu | rity (2) | | | | |
| Trend Micro_Deep Secu | rity (3) | | | | |
| | | | | | |
| | ュポード 処理 アラート イベン | +とレポート コンピュータ ポリ | シー 管理 | MasterAdmin 👻 🔌====ス | - ⑦ ヘルブ ◎ サポート情報 - |
| ✓ ■ スマートフォルダ | ESX Agents #17/1L=18/ | M: ▼ //L | | | |
| E TEST | | | | | |
| ~ 📓 31H a-9 | -+ illin | ₩ ◆処理 ▼ 首イベント ▼ | ■ エクスポート ・ 田 列… | | |
| ✓ Ø vGenter = vc01.trendnsx.local | 名前 | 設明 | ブラットフォーム | ポリシー | ステータス ・ |
| > 連 ホストあよびクラスタ | コンピュータ> vCenter - vc01.tr | endnsx.local 〉 仮想マシン 〉 NSX-T 〉 E | SX Agents (3) | | |
| 🗸 連 仮想マシン | Iocalhost.localdomain (Trend Mic | ro_Deep Security (3)) | Deep Security Virtual Appliance | Deep Security Virtual Appliance | 管理対象 (オンライン) |
| > 🔗 NSX | Iocalhost localdomain (Trend Mic Trend Mic | pro_Deep Security (2)) | Deep Security Virtual Appliance | Deep Security Virtual Appliance | 管理対象(オンライン) |
| V 🎒 NSX-T | Iocalhost.localdomain (Trend Mic | ro_Deep Security (1)) | Deep Security Virtual Appliance | Deep Security Virtual Appliance | 管理対象(オンライン) |
| CionePrepinternalTemplateFolder | | | | | |
| ClonePrepParentVmFolder | | | | | |
| ClosePrepReplicaVmFolder | | | | | |
| ESX Agents | | | | | |
| - Lunt regimes | | | | | |

合わせて、DSM 上で DSVA の"ステータス"が"管理対象(オンライン)"になっていることを確認する必要があり ます。

また、DSVA の"Virtual Appliance のバージョン"が "DSVA ソフトウェアパッケージとデプロイに必要なコンポー ネント"で前述をした[管理]>[システム設定]>[アップデート]>[Virtual Appliance の配置]で指定したバージョン と同じバージョンとなっていることを確認します。"Appliace(SVM)のバージョン"と同じままの場合などには、 DSVA がセキュリティ VM としては配信されているものの、適切なバージョンにアップデートされていないものと考 えられるため、DSA パッケージが正常にダウンロードできる状態になっているか、DSM と DSVA が適切に通信 できているかどうかを確認する必要があります。





DSVA のステータスが"管理対象(オンライン)"とならず、何らかのエラーが発生している場合には、以下のよう な原因が考えられます(これ以外の原因がある場合も考えられます)。適切なシステム環境となっていることを確 認して、一旦 DSVA のデプロイを解除(削除)を行い、再度デプロイを設定する必要があります。

- ・ DSVA のデプロイに必要な適切なソフトウェアパッケージが DSM または外部 Web サーバにインポ ートされていない
- DSVA の管理 IP が DSM と正常に通信するために必要なネットワークの設定または IP プールまた は DHCP で割り当てたネットワークレンジ、デフォルトゲートウェイ、DNS サーバなどの設定に不備 がある
- ・ DSMとDSVA間で適切なファイアウォールルールの開放または適切な DNS 名前解決ができない
- ・ 上記の要因などにより DSVA が正しく DSM を認識できていない

vCenter Server から DSVA に対して Web コンソールでアクセスした際のトップ画面で下記のように DSM の情報 が常時されず、何も表示されない場合には、DSVA は正しくデプロイされていない状態となります。また、合わせ て割り当てたネットワークレンジから DSVA の管理 IP が割り振られていることも確認してください。

| | Trend Micro(TM) Deep Security Virtual Appliance 12.0.0-767 |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C | Management Address IPv4: (ens160) 10.3.225.243/24 Management Address IPv6: (ens160) 2400:4010:413:224:250:56ff:fe83:9db5/64 Deep Security Manager URL: https://dsm03.trendnsx.local:4120/ .https://DSM03.trendnsx.local:4120/ Mon Dec 30 04:03:18 UTC 2019 |

2-3-9. Deep Security 基本設定とセキュリティポリシーの策定

DSM から Deep Security を運用する上で必要な基本設定およびセキュリティポリシーの策定を行います。

· Relay グループの設定の確認

デフォルトでは DSM は、インストール時に生成される[初期設定の Relay グループ]に所属します。通常は、[初期設定の Relay グループ]を利用することで問題はありません。

| 💋 TREND Deep Secur | ity ダッシュボード 処理 ア | | ビュータ ボリシー 管理 | MasterAdmin 👻 🦺 💷 🗁 | ヽ ▼ ② ヘルブ ③ サポート情報 ▼ Q、ヘルブセンターの検索 |
|-----------------------------------------------|----------------------------|-----------------|--------------|-----------------------|-----------------------------------------------------|
| ✓ 11 アイデンティティブロバ [▲] A SAML | Relayの管理 | | | | i Relayのプロパティ |
| ⑥ システム情報 | 新規Relayグループ Relayグループの話 | 削除 Relayの追加 Rel | ayの削除 | | ホスト名またはIPアドレス: dsm03.trendnsx.local |
| で、アップデート | 名前▼ グル | ループのステータス | | アップデート元 | Delevitin - C |
| ✓ | ✓ 参 初期設定のRelayグループ ● | すべてオンライン | | セキュリティアップデート元 | Naray シルーフ: 初期設定のRelay グループ ・ |
| ☆ バターンファイル | 名前 | AGENTのステータス | バージョン | | ステータス: ● オンライン |
| ▼ ▼ ◎ ソフトウェア ④ ダウンロードセン: ― | 📓 dsm03.trendnsx.local | ● オンライン | 12.0.0.767 | × | ブラットフォーム: Microsoft Windows Server 2012 R2 (64 bit) |
| □ ーカル ● Relayの管理 | | | | | |

[初期設定の Relay グループ]に DSR となるサーバが一台も所属していない状態の場合には、[新規 Relay グループ...]から DSR とする DSA サーバを指定する必要があります。通常は DSM サーバに DSA をインストールして DSR として導入してください。



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

Relay を多段構成で構成したい場合などには Relay グループを追加で設定することが可能です。 詳細は以下のヘルプセンターの情報を参照してください。

<u>https://help.deepsecurity.trendmicro.com/12_0/on-premise/ja-jp/Set-Up-Relays.html?redirected=true&Highlight=Relay</u> また、DSM がインターネットに接続できないオフライン環境でアップデートを行う方法については以下の FAQ を参照して運用方法を検討ください。

https://success.trendmicro.com/jp/solution/1096762

予約タスクの設定

必要に応じて、定期的に実行するタスクを設定することができます。セキュリティの観点から最低限以下の 予約タスクが設定されているかを確認し、設定されていない場合は予約タスクの新規作成を行ってくださ い。また、適宜、タスクの実行間隔、実行するコンピュータの調整をしてください。(以下の2つの予約タスク はインストール時に自動的に設定されています。)

- セキュリティアップデートの確認
- ソフトウェアアップデート確認

また、不正プログラム対策で予約検索を行う場合には、[コンピュータの不正プログラムを検索]も設定する 必要があります。

詳細は以下のヘルプセンターの情報を参照してください。

https://help.deepsecurity.trendmicro.com/12_0/on-premise/ja-jp/scheduled-tasks.html

Deep Security セキュリティポリシーの作成

Deep Security の各機能では詳細な設定が可能です。

それらの設定を、保護対象のコンピュータに個別に設定するのではなく、まずは設定をセットにした「ポリシ ー」を作成し、コンピュータに対してはどのポリシーで保護するのかを選択して適用します。

ポリシー作成は、新規作成することも、既存のポリシーをコピーして部分的に修正することも可能です。また、「継承」オプションを利用することにより親子関係のポリシーを作ることも可能です。親ポリシーを継承した子ポリシーを作成した場合、親ポリシーの変更は子ポリシーにも自動的に反映されます。また、子ポリシーにて個別設定を行った場合には、該当の設定項目だけが変更(継承から除外される)されて、それ以外の設定項目は親ポリシーに準じる、といった柔軟なセキュリティポリシーの適用が可能となります。



▶ 継承に関する詳細は以下のヘプルセンターを参照してください。



https://help.deepsecurity.trendmicro.com/ja_jp/policies_inheritance_overrides.html

Deep Security では、予めいくつかのポリシーがプリセットされています。

ポリシーは新規に1から作成することもできますが、OS 毎にトレンドマイクロが定義したポリシーをベースに個別にカスタマイズをすることも可能です。

| ポリシー | | | | |
|-----------------------------------|--|--|--|--|
| 🏠 新規 👻 🧰 削除 🔳 詳細 🍺 複製 📑 エク | | | | |
| Hase Policy | | | | |
| > 🍓 Deep Security | | | | |
| 🐴 Linux Server | | | | |
| 🍅 Solaris Server | | | | |
| ✓ 🍓 Windows | | | | |
| > 🍓 Windows 10 Desktop | | | | |
| 🚵 Windows 7 Desktop | | | | |
| 曫 Windows 8 Desktop | | | | |
| 曫 Windows Anti-Malware Protection | | | | |
| 曫 Windows Mobile Laptop | | | | |
| 曫 Windows Server 2000 | | | | |
| Windows Server 2003 | | | | |
| Windows Server 2008 | | | | |
| Windows Server 2012 | | | | |
| Windows Server 2016 | | | | |
| 🍅 Windows Vista Desktop | | | | |
| Windows XP Desktop | | | | |

仮想デスクトップとして利用する仮想マシンを保護する場合には、以下の点を参考にポリシー作成をしてみてく ださい。(以下の内容によって必ずしもセキュリティリスクのすべてを回避できるわけではないことを予めご了承く ださい。)

- > 不正プログラム対策を有効にしてください。
- 不正プログラム対策の予約検索については、仮想デスクトップの展開方法、セキュリティポリシーに応じて 実施の必要性の検討、実施間隔の設定を行ってください。
- Web レピュテーション、侵入防御については、NSX-T2.4 及び 2.5 環境において DSVA で提供することはで きません。(2019 年 12 月現在)

サーバ OS を保護する場合には、上記に加えて Web レピュテーション、侵入防御、変更監視、セキュリティログ 監視、アプリケーションコントロールなどの機能を DSA で併用して適用することを検討してください。

- そしていては推奨設定の検索を利用することで効率的なルール運用が可能となります。推奨 設定の検索の詳細については、Deep Security ヘプルセンターを参照してください。
- 変更監視、セキュリティログ監視の利用にあたっては、ルールに対してユーザ、システム固有のパラメータ 設定する必要がある"設定可能ルール"(ルールマークに歯車マークがついているルール)が多く存在しま



す。ルール適用にあたっては、推奨設定の検索の利用とあわせて適用するサーバの情報を確認した上で 行うことを推奨します。

変更監視を有効化する場合には、ベースラインの再構築、予約タスクの実行などの設定をあわせて行って ください。

本セクションでは、以下のシチュエーションを想定した設定を行っていきます。

実際の環境では、利用される環境及びセキュリティポリシーに応じて設定を行ってください。

- ▶ Horizon にて仮想マシン(VDI用 Windows クライアント)が展開される環境
- ▶ 仮想マシンに対して、Deep Security の不正プログラム対策を有効化
- Deep Security で不正プログラム対策イベントを検出した際に分散ファイアウォールと連携した自動隔 離ができるように隔離用セキュリティグループも設定
- > 本セクションでは、ポリシーを以下のとおり指定

Deep Security セキュリティポリシー : VDI_Windows Desktop_Demo01

トレンドマイクロが提供するデフォルトのポリシーである"Windows Desktop"を継承してカスタマイズし、以下の機能を有効化

・ 不正プログラム対策



1) DSM から[ポリシー]>[ポリシー]から定義済のポリシーである[Windows Desktop]を選択して、複製する

| 🕖 IREND Deep Sec | urity ダッシュボード 処理 アラート イベントとレポート コンピュータ ポリシー 管理 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| 為 ポリシー | ポリシー |
| ∨ 🗳 共通オブジェクト | |
| > 🖷 ルール | 🎬 新規 🔹 🧰 削除 🔳 詳細 🏥 複製 📑 エクスポート 🍷 |
| ✓ ■ UZF | 🗸 🚡 Base Policy |
| E PUZH | ✓ ↓ Deep Security |
| MACUZE | ia Deep Security Manager |
| ■ デルクトリリスト | a Deep Security Virtual Appliance |
| ■ ファイルリスト | 🚡 Linux Server |
| 📄 ファイル拡張子リスト | ≧ Solaris Server |
| ■ ボートリスト | ✓ 诌 Windows |
| 🗸 🤹 その他 | > 谙 Windows C ··· |
| New Syslog and Syslog | Windows Se |
| 🍰 コンテキスト | 🦉 複製 |
| 薗 スケジュール | 面 別除 |
| 🎴 95 | ■ 詳細 |
| -0 | |

2) 複製したポリシーをカスタマイズして、保存

| 概要 | 一般 | このボリシーを使用して | いるコンピュータ | イベント | | |
|---------------|-----------------------------------------|----------------|----------------------|-------------------|--------------|-----|
| ▶ 不正プログラム対策 | 名前: | VE | I_Windows Desktop_[| Demo01 | | |
| Webレビュテーション | 說明: | An | example policy for V | Vindows desktops. | | |
|) ファイアウォール | | | | | | |
| 侵入防御 | | | | | | |
| 変更監視 | | | | | | |
| セキュリティログ監視 | 継承一 | | | | | |
| アプリケーションコントロー | 林元ノハリンノ | | '値 なし | | | |
| インタフェースの種類 | | 2 | 👌 🏠 Base Policy | | | |
| 設定 | | | | | | |
| オーバーライド | | | | | | |
| | ±:7 | | | | | |
| | U L L L L L L L L L L L L L L L L L L L | デ Eプログラム対策: | 継承 (オン) | | • リアルタイム | |
| | 👩 We | ыビュテーション: | オフ | | ● オフ | |
| | 😇 7r | ィアウォール: | オフ | • | ● オフ, 11 ルール | |
| | 🔒 侵) | 入防御: | オフ | ~ | ● オフ,ルールなし | |
| | 💿 変更 | 更監視: | オフ | | ● オフ,ルールなし | |
| | Q 24 | キュリティログ監視: | オフ | ~ | ● オフ,ルールなし | |
| | 🗵 75 | ガリケーションコントロール | ,: 継承 (オフ) | ~ | ● オフ | |
| | | | | | | |
| | | | | | 保存 | 閉じる |

- [継承:親ポリシー] : .
- Windows Desktop
- [不正プログラム対策] : .
- 継承(オン)



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

- [Web レピュテーション]: オフ<変更>
 [ファイアウォール]: オフ<変更>
 [侵入防御]: オフ<変更>
 [変更監視]: オフ<変更>
 [セキュリティログ監視]: オフ<変更>
- 「アプリケーションコントロール」 : 継承(オフ)

2-3-10. 保護対象仮想マシンへの VMware Tools 及び Notifier のインストール

エージェントレスによるセキュリティ機能を提供するためには、仮想マシンに VMware Tools を導入することで、 仮想マシンで発生したトランザクションを ESXi ホスト経由で DSVA が受け取れる必要があります。また、エージ ェントが導入されないため、イベントが発生した場合に仮想マシンのユーザがそれに気づくことが困難です。 仮 想デスクトップなどのユーザがログインをして利用する仮想マシンについては、Trend Micro が提供する通知ツ ール Notifier を導入しておくことを推奨しています。

仮想デスクトップ環境においては、マスターイメージに VMware Tools、Notifier をあらかじめインストールしておく ことによりスムーズな展開が可能です。

- > VMware Tools のインストール
- 1) 仮想マシン上で VMware Tools のセットアップファイルを実行し、セットアップウィザードを進める *[セットアップの種類の選択]で[カスタム]*を選択する





2) **[カスタム***セットアップ]***で[VMCIドライバ]**から以下のドライバを[ローカルハードドライブにインストール]を選択 して、インストールを行う



- "NSX ファイル自己検証ドライバ"を選択
 ※NSX ネットワーク自己検証ドライバについては選択しない
- 3) インストールを完了する

| 谩 VMware Tools セットア | ນ ້ 🗆 🖬 💌 |
|-----------------------------|-------------------------------------------|
| | VMware Tools セットアップウィザードが完了し ました |
| | セットアップ ウィザードを終了するには、[完了] ボタンをクリックし ます。 |
| | |
| | |
| vm ware [.] | |
| | <戻る(B) 完了(E) キャンセル |



- Notifier のインストール
- 1) 仮想マシン上で Notifier のセットアップファイルを実行し、セットアップウィザードを進め、使用許諾に同意する



2) インストールを実行する



3) 仮想マシンのデスクトップに Deep Security のアイコンが表示されることを確認する




Notifier では仮想マシンに適用されているセキュリティ機能の概要と検出したイベントが表示されます。 (以下のキャプチャは、DSVA にポリシーが配信された後のステータスを表示したものです。)

| ・ ・ ・ | ◆ 不正プログラム対策 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ● Webレビュテーション 設定なし ファイアウォール 設定なし ● 保入防御 設定なし ● 変更監視 設定なし ● ジェリティログ監視 保護できません ● プリリアーションコントロール 保護できません ● プリリーションコントロール 保護できません ● プリリーションコントロール 保護できません ● プリレーションコントロール 保護できません ● プリレーションコントロール 15.589.00 IntelliTapk% トリュンファイル 1.673.00 IntelliTapk% トリュンファイル 2.245.00 スマートスキャンエージコントリカ ・ファイル 15.587.00 音频済み 振び間 いちーンファイル 1.00007.00 高度な 争感相関いちーンファイル 1.112.00 | Webuピュテーション 設定なし ファイアウォール 設定なし 受ィアクラオール 設定なし 健入防御 設定なし 変支なし セオュリティロク騒視 保護できません アフリケーションファール 保護できません アイルフシュンファール (強度できません) アイルフシュンファール 15,589,00 IntellTrapkがパターンファール 16,73,00 IntellTrapkがパターンファール 0,251,00 スパーケスアを振現や、シファール 2,245,00 スマートスキャンエージェントパや、シファール 15,587,00 信都添み話明書情報パターンファール 1,112,00 |
| ファイアウォール 設定なし (星人防衛) 設定なし 変更整視 設定なし を支配 設定なし (日本)ワイログ監視 保護できません アブリケーションコントロール 保護できません (オーネント (日本)ログラムからの保護 ウイルスパキン・ファイル 15 589.00 IntelliTapk為小はキンファイル 1.573.00 IntelliTapk為ーンファイル 0.251.00 スマートスキャンエーショント/り、シファイル 15 589.7.00 (富焼な 脅威相関い キーンファイル 1.0007.00 高炭な 脅威相関い キーンファイル 1.112.00 | ファイアウォール 設定なし ④人防衛 設定なし ● 変更監視 設定なし ● セキュリティロ?監視 保護できません ● セキュリティロ?監視 保護できません ● アブリケーションコントロール 保護できません ● アブリケーションコントロール 保護できません ● レキュリティン アブリケーションコントロール ● レキュリティンションファイル 15,589,00 IntellTrapk% -ンファイル 1673,00 IntellTrapk% -ンファイル 0,251,00 スマートスキャンニージェントパターンファイル 15,587,00 尾袋方 証明書情報/% ーンファイル 1,00007,00 高炭な 骨感相関ロ % ーンファイル 1,112,00 |
| ● 役入防御 設定なし ● 変更読視 設定なし ● ときュリティログ覧視 保護できません ● アブリウ・ションントロール 保護できません ● アブリウ・ションントロール 保護できません ● オーネント ● ホーネント ● ホーネーネント ● ホーネーネント ● ホーネント ● ホーネント ● ホーネーネント ● ホーネーネーネーネーネーネーネーネーネーネーネーネーネーネーネーネーネーネーネ | ● 役入防御 設定なし ● 変互監視 設定なし ● セキュリティログ監視 保護できません ● アフリケーションコントロール 保護できません > アブリケーションコントロール 保護できません > アブリケーションコントロール 保護できません > マンボーネント ● イルスパなーンファイル 15,589,00 InteliTrapt%カン的マンファイル 16,73,00 InteliTrapt%カンジャンファイル 0,251,00 スパイウェア監視りなーンファイル 0,251,00 スパイウェア監視りなーンファイル 2,245,00 スマートスキッレーシェンテントパターンファイル 1,5587,00 信頓済み証明書情報/1%ローンファイル 1,00007,00 高度な事成相関1%ローンファイル 1,112,00 |
| ● 変更整視 設定なし ● セキュリティログ脳視 保護でをません アプリケーションロ・ロール 保護でをません マアプリケーションロ・ロール 保護でをません マボーネント | ● 変更整視 設定なし ● セネリティログ監視 保護できません アプリケーションコントロール 保護できません ンパーネント |
| ● セキュリティログ監視 保護できません ● アフリケーションコントロール 保護できません マボーネント ・ボーネント ・ ホーネント ・ ホーズン「 15,589,00 InteliTrapk%パリターンファイル 1,673,00 InteliTrapk%パリターンファイル 0,251,00 スパークスア奮現リターンファイル 0,251,00 スパークスア奮現リターンファイル 15,587,00 「商病多ル証明書情報19~ンファイル 1,00007,00 高度な脅感相関いターンファイル 1,112,00 | ● セキリティログ転視 保護できません ● アブリケーションコントロール 保護できません × マガルテンキンコントロール 保護できません × マガルスパなーンファイル 15,589,00 IntelliTrapRを外パなーンファイル 15,589,00 IntelliTrapRを外パなーンファイル 0,251,00 スパトイプェア警視がなーンファイル 2,245,00 スマートスキャンエージェントパなーンファイル 15,587,00 信徳派み 証明書情報がなーンファイル 1,00007,00 高度な 春感相関がなーンファイル 1,112,00 |
| アブリケーションコントロール 保護できません ★ボーネント ★正プログラムからの保護 ケルシスパターンフアイル 15,589,00 IntelliTrapk3かいなーンファイル 1,573,00 IntelliTrapk3かいなーンファイル 0,251,00 スパイシア警告ルやシンファイル 2,245,00 スマートスキャンエーショントパなーンファイル 15,597,00 信病決み正明書店報いやーンファイル 1,00007,00 高度な春感相関いやーンファイル 1,112,00 | ● アプリケーションコントロール 保護できません ◆ アプリケーションコントロール 保護できません ◆ ・ホーネント ・ホーボブログラムからの保護 ・ケルスパキー・ファイル 15589.00 IntellTrapRA/1% >>ファイル 1.673.00 IntellTrapRA/1% >>ファイル 0.251.00 スパイケア電池1% >>ファイル 0.251.00 スマートスキャンエージェントパか >>ファイル 15.587.00 信頼法会証明書情報パタ >>ファイル 1.00007.00 高度な春感相関いや >>ファイル 1.112.00 |
| ンポーキント 不正プログラムからの保護 ウイルスパターンファイル 15,583,00 IntellTrapk&パターンファイル 1,673,00 IntellTrapkのシンファイル 0,251,00 スパイウェア酸温パターンファイル 2,245,00 スマートスキッシェーシュントパターンファイル 1,587,00 信頼済み証明書店格パターンファイル 1,00007,00 高度な事感相関パターンファイル 1,112,00 | ンポーネント 不正プログラムからの保護 ウイルスパな ーンファイル 15.589.00 IntellTrapk% ノンファイル 1.673.00 IntellTrapk% レンファイル 2.245.00 スマートスキッシュージェントパな ーンファイル 15.587.00 信報済み証明書情報パな ーンファイル 1.00007.00 高度な 身感相関パな ーンファイル 割0 |
| 不正プログラムからの保護 ウイルスパなーンファイル 15,589,00 IntelliTapk%トジカーンファイル 1,673,00 IntelliTapk%トジカーンファイル 1,673,00 IntelliTapk%トジカーンファイル 0,251,00 スパイウエア警視パなーンファイル 2,245,00 スマートスキャンエー・ジェントパル・ンファイル 15,587,00 信頼決済と調査情報パターンファイル 1,00007,00 高度な事感相関パターンファイル 1,112,00 | 不正プログラムからの保護 ウイルスパターンファイル 15.589.00 IntellTrapk外パターンファイル 1.673.00 IntellTrapkシーンファイル 0.251.00 スパイウェア監視パターンファイル 2.245.00 スマートスキッシュージェンパターンファイル 15.587.00 信頼済み証明書情報パターンファイル 1.00007.00 高炭な存成相関パターンファイル 1.112.00 |
| ウイルスパターンファイル 15,589,00 Intel/Trapkターンファイル 1,673,00 Intel/Trapkターンファイル 0,251,00 スパインア警視パターンファイル 2,245,00 スマートスキッシェーンジェントパターンファイル 15,587,00 信頼済み近明書情報パターンファイル 1,00007,00 高度な争感相関パターンファイル 1,112,00 | ウイルス1% -ンファイル 15,589,00 IntellTrapt%クリな -ンファイル 1.673,00 IntellTrapt%クリな -ンファイル 0.251,00 スリイウェア監視1% -ンファイル 2.245,00 スマトスキシンエーシェント% >ンファイル 15,587,00 信節(含み証明書情報)% -ンファイル 1.00007,00 高度な 存成相関1% -ンファイル 1.112,00 動 |
| IntelliTrap総外パターンファイル 1.673.00 IntelliTrapパターンファイル 0.251.00 スパインア警視パターンファイル 2.245.00 スマートスキャンエージェントパターンファイル 15.587.00 信頼済み正明書店報いターンファイル 10.0007.00 高度な争感相関パターンファイル 1.112.00 | IntellTrap能分がなーンファイル 1.673.00 IntellTrap能やニンファイル 0.251.00 スパイウェア監視がなーンファイル 2.245.00 スマートスキャンエー・ジェントパなーンファイル 15.587.00 信報読み証明書情報がなーンファイル 1.00007.00 高度な専惑相関がなーンファイル 1.112.00 |
| IntelliTrapt%・ンファイル 0.251.00 スパインア輸出(約・ンファイル 2.245.00 スマートスキャンエージェント/約・ンファイル 15.597.00 信頼済み証明書店報約、シーンファイル 1.00007.00 高度な春感相関いなーンファイル 1.112.00 | IntelliTrapt%>ンファイル 0.251.00 スパイウェア監視パタンファイル 2.245.00 スマートスキャンエージェントパターンファイル 15.587.00 信報済み証明書情報パターンファイル 1.00007.00 高度な春感相関パターンファイル 1.112.00 |
| スパイケエア監視しなーンファイル 2.245.00 スマートスキャンエージェントパなーンファイル 15.587.00 信頼済み証明書情報パなーンファイル 1.00007.00 高度な春感相関いなーンファイル 1.112.00 | スパイウェア監視1次・ンファイル 2.245.00 スマートスキャンエージェント1次・ンファイル 15.587.00 信報済み証明書情報1次・ンファイル 1.00007.00 高度な春感相関1次・ンファイル 1.112.00 |
| スマートスキャンエージェントパターンファイル 15.587.00 信頼済み証明書情報パターンファイル 1.00007.00 高度な事感相関パターンファイル 1.112.00 | スマートスキャンエージェント/はーンファイル 15,587.00 信頼(済み証明書情報)はーンファイル 1.00007.00 高度な存成相関)はーンファイル 1.112.00 動1 |
| 信頼済み証明書存載パなーンファイル 1.00007.00 高度な事感相関パターンファイル 1.112.00 | 信報済み証明書情報パな ーンファイル 1.00007.00 高度な 存成相関パな ーンファイル 1.112.00 動1 |
| 高度な脅感相関いな - ンファイル 1.112.00 | 高度な骨感相関パターンファイル 1.112.00 1.112.00 動D |
| | <u> </u> |
| | ₫¥0 |
| i¥0 | _ |
| | ✓ 不正プログラムの検出時に通知(M) |
| 。]不正プログラムの検出時に通知(M) | a second but has the state of the state of the |
|]不正ナロゲラムの検出時に通知(M)]不正なWebx≪-ぶのナロック時にご通知(W) | ✓1 小正な Webページのチロック時に通知1W1 |
|]不正ナロゲラムの検出時に通知(M)]不正なWebページのナロック時に通知(W) | ✓] 小正な Webページのフロック時に通知(W) |
| 知 | □ 不正プログラムの検出時に通知(M) |
| 」 了不正プログラムの検出時に通知(M) | |
| □ 不正プログラムの検出時に通知(M) | ALL A LEADER ALL AS A TATA REPORT OF A CONTRACT AND A LEADER A |
| 」 「不正プログラムの検出時に通知(M) | The second |
| | □ 不正プログラムの検出時にご通知(M) |
| 知 | |

2-3-11. エンドポイントの保護を設定 NSX セキュリティポリシー・セキュリティグループ作成

ESXi ホスト上に展開される仮想マシンに適用する Deep Security セキュリティポリシーを定義するために、NSX セキュリティグループ、セキュリティポリシーの作成を行います。また、Deep Security で検出したセキュリティイベ ントに応じて仮想マシンを自動隔離する場合には、隔離用のセキュリティグループも作成をしておきます。









この設定を行うことにより、仮想マシンが新たに生成された際に、セキュリティポリシーに従って自動的に Deep Security のセキュリティポリシーが適用され、セキュリティ機能を有効化することができます。

本セクションでは、以下のシチュエーションを想定した設定を行っていきます。

実際の環境では、利用される環境及びセキュリティポリシーに応じて設定を行ってください。

- ➢ Horizon にて仮想マシン(VDI用 Windows クライアント)が展開される環境
- 仮想マシンに対して、Deep Securityの不正プログラム対策、侵入防御、Web レピュテーション機能を 有効化
- Deep Security で不正プログラム対策イベントを検出した際に分散ファイアウォールと連携した自動隔 離ができるように隔離用セキュリティグループも設定
- 不正プログラム対策イベント検出時に付与する NSX セキュリティタグを "ANTI_VIRUS.VirusFound.threat=high"に設定
- ▶ 本セクションでは、各設定の名称を以下のとおり指定

| • | Deep Security セキュリティポリシー | : VDI_Windows Desktop_Demo01 |
|---|--------------------------|----------------------------------------|
| | | (セクション 2-3-7 で作成したセキュリティポリシー) |
| • | NSX セキュリティポリシー | : Win-VDI-Policy |
| • | NSX セキュリティプロファイル | : Win-VDI-Profile |
| • | NSX セキュリティグループ | : TRENDNSX-VDI(VDIドメインセキュリティグループ:正常時) |
| | | TRENDNSX-VDI-Quarantine(隔離用セキュリティグループ) |
| | | |

[1] VDI ドメインセキュリティグループの作成

正常時に仮想マシンが所属するセキュリティグループを作成します。

1) NSX Manager にアクセスし、[インベントリ]>[グループ]を選択し、[グループの追加]をクリックする

| ホーム ネットワーク | セキュリティ イン | ベントリ ツール ミ | システム ネットワークとセ | キュリティの詳細設定 | | | | |
|---------------------------------------------|---------------------------------------|----------------------------|------------------------------|----------------------|----|----------------------------------|--------|------------|
| ~ | □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ | ドキュメント | | | | | | |
| 設定の概要 10.10.10 | グループ の追加 | | | | | | すべてを表示 | 0 検索 |
| ふ トメイン 〇 サービス | | 名前 | ドメイン | | | コンピュート メンバー | 使用場所 | 状態 |
| 田 グループ 団 仮想マシン | ÷ | TRENDNSX-VDI | * default 選択しない場合は、デフォルトで | (default」ドメインに設定されます | | メンバーの設定 | | |
| 🔓 コンテキスト プロファイル | | 說明 | 說明 | | タグ | Tag (Required) Maximum 30 tac | Scope | (Optional) |
| | | 保存 キャンセ | IL | | | | | |
| | | 18 4 | | | | | 、 | |

• 名前

: VDIドメインセキュリティグループ名を設定("TRENDNSX-VDI")



2) "コンピュートメンバー"で"メンバーの設定"をクリックして、"基準の追加"を選択する



3) **"仮想マシン名"の"コンピュータ名"**が**"次を含む"="AM-Win10"**だった場合に TRENDNSX-VDI グループ

に所属するためのメンバーシップ基準を設定して適用する

| パーシップ基準 (1) メンバー (0) IP/MAC アドレス (0) Active Directory グループ (0) | |
|-----------------------------------------------------------------------|-------|
| 劇中を追加 | 上限:5つ |
| 基準1 | |
| 想マシン - コンピュータ名 - 次を含む - AM- <u>Winto</u> | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

4) [グループの追加]で"保存"する

[2] 隔離セキュリティグループの作成

Deep Security で不正プログラム対策イベントを検出した際に仮想マシンが隔離されるセキュリティグループを 作成します。

※自動隔離を行わない場合、設定は不要です。

1) VDIドメインセキュリティグループ同様に、[インベントリ]>[グループ]を選択し、[グループの追加]をクリッ クする



2) セキュリティグループの名前"TRENDNSX-VDI-Quarantine"を設定する

| : | TRENDNSX-VDI – Quar * | default 選択しない場合は、デフォルトで「default」ドメイン | ⊗ × * 設定されます | メンバーの設定 | |
|---|-----------------------|-----------------------------------------|-----------------|--------------------------------------------|--------------------|
| | 説明 | 說明 | タヴ | Tag (Required) Maximum 30 tags are allo | Scope (Optional) 🔗 |
| | 保存 キャンセル | | | | |

・ 名前

: 隔離用セキュリティグループ名を設定("TRENDNSX-VDI-Quarantine")

3) "コンピュートメンバー"で"メンバーの設定"をクリックして、"基準の追加"を選択する

| メンバーの選択 コンピュート メンバーを作 せでグループ内の有効なメ | TRENDNS 成して追加するか ンバーシップを定 | X-VDI 、または直接追加します。ID メン/ 義します。 | 「一を個別に追加することもできます。ID メンバーは、コンピュート メンバーとの組a | X み合わ |
|--------------------------------------------|---------------------------------|--------------------------------------|--------------------------------------------|----------|
| メンバーシップ基準 (0) | メンバー (0) | IP アドレス/MAC アドレス (0) | Active Directory グループ (0) | |
| +基準を追加 | | | 上限: 5 1 | つの基準 |
| | | | | |

4) "仮想マシン名"に付与される"タグ"として"次を含む"="ANTI_VIRUS.VirusFound.threat"だった場合に

TRENDNSX-VDI-Quarantine グループに所属するためのメンバーシップ基準を設定して適用する

| | | IP アトレス/MAC アトレ | イス (0) Act | ive Directory グルーフ | プ (0) | | |
|-------|------|-----------------|------------|--------------------|---------|-------|---------|
| 基準を追加 | | | | | | | 上限: 5 つ |
| 基準 1 | | | | | | | |
| 想マシン | ✓ タグ | > 次を含む | ~ A | NTI_VIRUS.VirusFot | Scope ④ | Scope | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

5) [グループの追加]で"保存"する



6) セキュリティグループが2つ作成されていることを確認する

| ホーム ネットワーク せ | 2キュリティ イン | ベントリ ツール システ | ム ネットワークとセキュリティの詳細設定 | | | |
|-----------------------------------|-----------|----------------------------|----------------------|----|-------------|---------|
| « | ⊞ グループ | ドキュメント | | | | |
| 設定の概要 | | | | | | |
| 品 ドメイン | グループ の追加 | | | | | すべてを非表示 |
| ○ サービス | | 名前 | ドメイン | | コンピュート メンバー | 使用場所 |
| 田 グループ | : 🗸 🖽 | TRENDNSX-VDI | default | | メンバーの表示 | 使用場所 |
| 🗗 仮想マシン | | 5H 00 | | | | |
| 🔓 コンテキスト プロファイル | | 19CPH | 木設定 | 30 | 0 | |
| | : 🗸 🖽 | TRENDNSX-VDI-Quarantine | default | | メンバーの表示 | 使用場所 |
| | | 説明 | 未設定 | タグ | 0 | |

[3] サービスプロファイルの作成

NSX 環境において Deep Security によりエージェントレス型セキュリティを実現するための定義をプロファイル として設定します。

1) NSX Manager にアクセスし、[セキュリティ]>[エンドポイントの保護]>[サービスプロファイル]へ移動し、 [パートナーサービス]で "Trend Micro Deep Security"を選択した上で、""サービスプロファイルの追加"をクリッ クする

| | « | | |
|-------------------------------------|---|-------------------------------------------|---------------------------------------------------------------|
| ② 設定の概要 ≒ East-West のセキュリテ | > | 「「」ルール サービスプロフォ パートナーサービス* Trend Micro | アキュメント Deep Securit 〜 サービスの詳細を表示 |
| ♪ North-South のセキュリ 1 エンドポイントの保護 | > | サービス プロファイルの追加 | サードスプロファイルの認知 |

2) サービスプロファイル名を指定し、ベンダープレートを選択して"保存す"る

| ホーム ネットワーク | セキュリティ | インベントリ ツール シスラ | テム ネットワークとセキュリティの詳細設成 | Ê | | | |
|---------------------------------------------------------|----------|---------------------------------------------|-----------------------|---------------------|-----------------|--|--|
| ② 設定の概要 ☆ East-West のセキュリテ | (1) パートナ | ール サービスプロファイル ーサービス* Trend Micro Deep Se | • ドキュメント | | | | |
| ♪ North-South のセキュリ | > サービス | サービス プロファイルの追加 | | | | | |
| 聞 エンドポイントの保護 | | サービスプロファイル名 | サービス プロファイルの説明 | ベンダーテンプレート | タヴ | | |
| | : | WIN-VDI-Profile * | サービス プロファイルの説明 | Default (EBT) 🛞 🗸 * | Tag (Ri Scope 🧭 | | |

- サービスプロファイル名
- ・ ベンダーテンプレート
- : サービスプロファイル名を設定("Win-VDI-Profile")
- : "Default(EBT)"を選択する

→ Deep Security のイベントンベースタスク(EBT)により仮想マシン 生成時を vCenter Server から通知された際にその仮想マシンに対して Deep Security のポリシーを自動的に適用させることを宣言



3) サービスプロファイルが設定されていることを確認する

| ホーム ネットワーク | セキュリティ | インベントリ ツール システム | ネットワークとセキュリティの詳細設定 | | |
|--------------------------------------------------------------|------------|---------------------------------|--------------------|---------------|----|
| « | < 【聞 ルー | ル サービス プロファイル | • ř=1x>> | | |
| ② 設定の概要 S East-West のセキュリテ > | パートナー | - サービス * Trend Micro Deep Secur | it > サービスの詳細を表示 | | |
| ↓↑ North-South のセキュリ… > | サービス: | プロファイルの追加 | | | |
| 1日 エンドポイントの保護 | | サービスプロファイル名 | サービス プロファイルの説明 | ベンダーテンプレート | タグ |
| | : | WIN-VDI-Profile | | Default (EBT) | 0 |
| | | | | | |

[4] エンドポイントの保護のためのルールの作成

[4-1]エンドポイントの保護のための VDI ドメイン用ルールを作成する

VDIドメイン用セキュリティグループとサービスプロファイルを紐づけるためにルールを作成します。

1) NSX Manager にアクセスし、[セキュリティ]>[エンドポイントの保護]>[ルール]へ移動して[ポリシーの追 加をクリックし、[名前] 列で、"New Policy" をクリックして名前を変更する("*Win-VDI-Policy"*)

| ホーム ネットワーク | セ | キュリティ インベントリ ツール システム ネットワークとセキュリティの詳細設定 |
|---------------------------|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | « | |
| 設定の概要 | | $\square \frac{\mu - \mu}{\mu} \qquad \forall - \forall z \ z \$ |
| ≒ East-West のセキュリテ | > | |
| ♪ North-South のセキュリ | > | + ポリシーの追加 + ルールを追加 🔲 クローン作成 🕤 取り消す 🗓 削除 🚥 |
| 聞 エンドポイントの保護 | | 合前 グループ |
| | | : > WIN-VDI-Policy O) ドメイン: default |

2) 作成したポリシーの横にあるチェックボックスをオンにし、[ルールを追加]をクリックする

作成したポリシーの下に表示されたルールの[名前] 列で、"New Rule"をクリックして名前を変更する("Win-VDI-Rule")

| ガール サービスプロファイル ・ ドキュメント | | | | | | | | | |
|-----------------------------------------------------------------------|---------------|-------------|--|--|--|--|--|--|--|
| 未発行の変更の合計:2件 元に戻す 十 ポリシーの追加 + ルールを追加 ① クローン作成 う 取り消す ① 削除 ・・・ | | | | | | | | | |
| ✓ 名前 | グループ | サービス プロファイル | | | | | | | |
| : V VIN-VDI-Policy (0) | ドメイン: default | | | | | | | | |
| : ① WIN-VDI-Rule | グループの選択 | サービス プロファ | | | | | | | |



3) [グループ列]で[グループの選択を選択し、VDIドメインセキュリティグループを("TRENDNSX-VDI")選択して[適用]する。

| TRE | NDNS> | -VDI > | \bigcirc | | | | |
|-----|-------|--------|------------|-------------------------|---------|-------------|---------|
| ブルー | ープのi | 8,70 | | | | | すべてを表示 |
| | | | | 名前 | ドメイン | コンビュート メンバー | 状態 |
| ~ | : | > | | TRENDNSX-VDI | default | メンバーの表示 | ● 稼動中 ℃ |
| | | > | ⊞ | TRENDNSX-VDI-Quarantine | default | メンバーの表示 | ● 稼動中 C |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

4) [サービスプロファイル]列で[サービスプロファイルの選択を選択し、サービスプロファイル("Win-VDI-Profile")を選択して[保存]する。

| サービス | ブロファイルの設定 | | | | | > | | | | |
|----------|-----------------------------------------------------------------------|----|------------------------|------|-----|----------------|--|--|--|--|
| パートナー サー | 〔ートナー サービス [▲] <u>Trend Micro Deep Security 〜</u> サービスの詳細を表示 | | | | | | | | | |
| サービス プロフ | サービスプロファイルの逸加 | | | | | | | | | |
| | サービス プロファイル名 | タヴ | 状態 | | | | | | | |
| • : | Win-VDI-Profile | | Default (EBT) 属性の表示 | Gold | 0 | ● 稼動中 C | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| € 更新 | | | | | サービ | スプロファイル:1個中1~1 | | | | |
| | | | | | [| キャンセル 保存 | | | | |

[4-2] エンドポイントの保護のための隔離用ルールを作成する

隔離用セキュリティグループとサービスプロファイルを紐づけるためにルールを作成します。 ※自動隔離を実施しない場合は作成する必要はありません。

1) [4-1]の手順と同様に*[セキュリティ]>[エンドポイントの保護]>[ルール]*へ移動し、*[ポリシーの追加]*をク リックして、[名前] 列で、"New Policy" をクリックして名前を変更する(*"Quarantine-Policy"*)



- 2) 作成したポリシーの横にあるチェックボックスをオンにし、[ルールを追加]をクリックする
 - 作成したポリシーの下に表示されたルールの[名前] 列で、"New Rule"をクリックして名前を変更する
 - ("Quarantine-Rule")

| (🛱 ม | 間 <u>ルール</u> サービス プロファイル - ドキュメント | | | | | | | | | | |
|---------------------------------------------|-----------------------------------|---------------|-----------------|--|--|--|--|--|--|--|--|
| + ポリシーの違加 + ルールを追加 □ クローン作成 う 取り消す □ 剤除 ・・・ | | | | | | | | | | | |
| | □ 名前 | グループ | サービス プロファイル | | | | | | | | |
| : ~ | Quarantine-Policy (0) | ドメイン: default | | | | | | | | | |
| : 🕕 | New Rule | グループの違択 | サービス プロファ | | | | | | | | |
| ÷ ~ | WIN-VDI-Policy (0) | ドメイン: default | | | | | | | | | |
| : | WIN-VDI-Rule | TRENDNSX-VDI | WIN-VDI-Profile | | | | | | | | |

3) [グループ列]で[グループの選択を選択し、隔離用セキュリティグループを("TRENDNSX-VDI")選択して[適用]する。

| REN | IDNS) | -VDI- | э Х | | | | |
|-----|-------|-------|-----|-------------------------|-----------|-------------|-------------------------|
| ı | プの | 自加 | | | | | すべてを表示 |
| | | | | 名前 | ראל> | コンピュート メンバー | 状態 |
|) | : | > | ⊞ | TRENDNSX-VDI | default > | インバーの表示 | ● 稼動中 ℃ |
| 1 | : | > | ⊞ | TRENDNSX-VDI-Quarantine | default | インバーの表示 | ● 稼動中 C |
| | | | | | | | |
| | | | | | | | 1 0 10 M ² 1 |

4) [4-1]と同様、**[サービスプロファイル]列**で**[サービスプロファイルの選択**を選択し、サービスプロファイル (*"Win-VDI-Profile"*)を選択して*[保存]*する。



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

[4-3] エンドポイントの保護のためのルールの発行

設定したルールを各 ESXi ホストに適用するために発行を行います。

1) 作成した VDI ドメイン用ルールと隔離用ルールの順番の設定

後段で設定する分散ファイアウォールと連携して自動隔離を行う場合、通常運用時には仮想デスクトップは VDI ドメイン用ルールに所属します。この状態で Deep Security にて不正プログラム対策イベントを検出すると DSM は NSX Manager に対してセキュリティタグ情報を連携します。これにより該当仮想デスクトップを隔離用セキュリ ティグループへ所属させるための NSX セキュリティタグが付与されますが、VDI ドメイン用セキュリティグループ と隔離用セキュリティグループの両方に所属することになります。

エンドポイントの保護におけるポリシー、ルールについては、上位に配置されているものが優先して適用されま す。ある仮想マシンが、複数のセキュリティグループに所属している状態になった場合には、上位に配置されて いるルールが優先して適用されます。

自動隔離を行う場合には、必ず隔離用セキュリティグループが適用されているポリシー、ルールが上位になるように設定してください。

ポリシーの順番を変える場合には、該当のポリシーをマウスで選択して移動したい位置へ移動します。

2) ルールの ESXi ホストへの配信の実行

作成したポリシー、ルールを各 ESXi ホストへ適用するためにルールー覧の右上にある[発行]ボタンを押す ("未発行の変更の合計"が作成したポリシーとルールの総計になることを予め確認する)

| ホーム ネットワーク セ | 2キュリティ | インベントリ ツール | システム ネットワーク | クとセキュリティの詳細設定 | | | | |
|----------------------------------------------------------------------------|--------------|-------------------|-------------------|-------------------------|------------------------|--|--|--|
| « | -rtĐ | | | | | | | |
| 設定の概要 | <u>(1) –</u> | サービスプロファー | イル・トキュメント | | | | | |
| ≒ East-West のセキュリテ… > | | | | | (来発行の変更の合計:4件) 元に戻す 発行 | | | |
| は* North-South のセキュリ > + ポリシーの違加 + ルールを追加 [] クローン作成 う 取り消す <u>前</u> 削除 ・・・ | | | | | | | | |
| 🕼 エンドポイントの保護 | 1 エンドポイントの保護 | | | グループ | サービス プロファイル | | | |
| | ÷ ~ | Quarantine-Policy | (0) ドメイン: default | | | | | |
| | : | Quarantine-Rule | | TRENDNSX-VDI-Quarantine | Quarantine-Profile | | | |
| | : ~ | WIN-VDI-Policy | (0) ドメイン: default | | | | | |
| | : | WIN-VDI-Rule | | TRENDNSX-VDI | WIN-VDI-Profile | | | |

3) ルールの確認

| ホーム ネットワーク セ | ホーム ネットワーク セキュリティ インベントリ ツール システム ネットワークとセキュリティの詳細設定 | | | | | | | | | | |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------|-------------------|-----|---------------|-------------------------|--------------------|--|--|--|--|--|
| * | | | | | | | | | | | |
| □ 設定の概要 | | | | | | | | | | | |
| ≒ East-West のセキュリテ > | 年 East-West のセキュリテ ・ 、 、 、 、 たに戻す 、 発行 | | | | | | | | | | |
| if North-South のセキュリ > + ポリシーの違い + ルールを違加 □ クローン作成 分散り消す □ 朝降 ・・・ | | | | | | | | | | | |
| 1 エンドポイントの保護 | | 白荷 | | | グループ | サービス プロファイル | | | | | |
| | : ~ | Quarantine-Policy | (1) | ドメイン: default | | | | | | | |
| | : | Quarantine-Rule | | | TRENDNSX-VDI-Quarantine | Quarantine-Profile | | | | | |
| | : ~ | WIN-VDI-Policy | (1) | ドメイン: default | | | | | | | |
| | : | WIN-VDI-Rule | | | TRENDNSX-VDI | WIN-VDI-Profile | | | | | |
| | | | | | | | | | | | |



2-3-12. 仮想マシン展開時の有効化の確認とセキュリティ機能の検証

▶ Deep Security 有効化ステータスの確認

Deep Security の仮想マシン保護においては、保護対象となる仮想マシンが、DSM の管理対象下にある必要があります。仮想マシンが管理対象下に入ると、引き続き DSVA による保護が行われている ESXi ホスト上で仮想 マシン毎に NSX セキュリティグループに紐付くセキュリティポリシーが自動的に配信、適用されます。

セキュリティポリシーの配信が完了して、正常にセキュリティ機能が提供されている状態となると、各仮想マシンのステータスは[管理対象(オンライン)]という状態となります。

[管理対象(オンライン)]の状態に移行する一連の処理を Deep Security では"有効化"と呼びます。

| | ty ಶ್ರುಲ್ತಸರ್- 処1 | 理 アラート イベントとレポート コンビュータ ポリ | シー 管理 | | | | | |
|-----------------------------------|---------------------------------------------------|-------------------------------------------------------|-------------------------------------|--|--|--|--|--|
| ▲ スマートフォルダ CloneVM | コンピュータ サラグルーラを含む * ESXi別 * | | | | | | | |
| | +追加 - 前除… 国 | 詳細 🔸 処理 🔹 📋 イベント 🔹 📑 エクスポート 🔹 | 眼, 列 | | | | | |
| DSVA | 名前 🔺 | ステータス NSXセキュリティグループ | ポリシー | | | | | |
| 📄 コンピュータ | > esx-mgm01.trendnsx.local (4) | | | | | | | |
| ✓ ₽ vCenter - vc01.trendnsx.local | > esx-mgm02.trendnsx.local (1) | | | | | | | |
| 🗸 朣 ホストおよびクラスタ | > esx-mgm03.trendnsx.local (7) | | | | | | | |
| ∽ 🎒 NSX | esx-vdi01.trendnsx.local (29) | r esx−vdi01.trendnsx.local (29) | | | | | | |
| 🧱 Manage | (AM-Win7x64) | ● 疊 非管理対象 (VM停止) | なし | | | | | |
| 🗾 VDI | (DS-Win7_32bt_master) | ● 💁 非管理対象(VM停止) DS-Full Group | Windows XP Desktop | | | | | |
| 🗸 🍉 仮想マシン | (LinkCloneWindows-1) | ● 凾 管理対象 (オンライン) TRENDNSX-VDI | Windows VDI Anti-Malware Protection | | | | | |
| ✓ 🮒 NSX | (LinkCloneWindows-2) | ● 凾 管理対象(オンライン) TRENDNSX-VDI | Windows VDI Anti-Malware Protection | | | | | |
| Hawinan に トロクロマシン | .水```````````````````````````````````` | ● 凾 管理対象(オンライン) TRENDNSX-VDI | Windows VDI Anti-Malware Protection | | | | | |
| norizonにより収息マンノ | が通 <u>し</u> 生 _{ows=4)} | ● 凾 管理対象(オンライン) TRENDNSX-VDI | Windows VDI Anti-Malware Protection | | | | | |
| 成される場合でも自動的 | に有効化 ows-5) | ● 函 管理対象 (オンライン) TRENDNSX-VDI | Windows VDI Anti-Malware Protection | | | | | |
| 処理を行い 順次セキュ! | リティポリ | ● 函 管理対象 (オンライン) TRENDNSX-VDI | Windows VDI Anti-Malware Protection | | | | | |
| | | ● 函 有効化済み TRENDNSX-VDI | Windows VDI Anti-Malware Protection | | | | | |
| シーを適用していきます。 | ows-8) | 小 非管理対象(不明) TRENDNSX-VDI | Windows VDI Anti-Malware Protection | | | | | |
| | (LinkCloneWindows-9) | 💿 📲 非管理対象 (VM停止) | なし | | | | | |

ステータスが[管理対象(オンライン)]であれば、各仮想マシンのセキュリティ機能も有効に機能していることを示しています。

| | ンピュータ: winxp (Li | nkClone | eWindow | /s−1) | | | | | | | | @ ~1 |
|----|------------------|---------|--------------|----------|-------|-------------------------------|-----------|---------|----------|----------|--------------------------|-------------------|
| ₽ | 概要 | 一般 | 処理 | システムイベント | | | | | | | | |
| 0 | 不正プログラム対策 | ホスト宅 | 4: | | winx | p | | | | | | |
| ٢ | Webレビュテーション | 表示名 | | | Link | CloneWindows-1 | | | | | | |
| ۲ | ファイアウォール | 說明: | | | | | | | | ī. | | |
| θ | 侵入防御 | | | | | | | | | | | |
| 0 | 変更監視 | ブラット | フォーム: | | Micro | soft Windows | | | | <u> </u> | | |
| 0 | セキュリティログ監視 | グルーフ | ブ: | | | vCenter - vc01.trendnsx.local | ▶ 仮想マ | 2921 | NSX - | | | |
| 0 | アブリケーションコントロー | ポリシー | -; | | WS | 10 Desktop 🕨 Windows VDI Ant | i-Malware | e Prote | ection 👻 | | 編集 | |
| | インタフェース | | | | 備考 | 】 Deep Securityポリシーが₩ | /ware NS: | xからi | 選択されて | います | ŧ | |
| \$ | 設定 | 資産の | 重要度 | | なし | , | | | | ·] | 編集 | |
| • | アップデート | セキュリ | ノティアップラ - | ドートのダウン | 初期 | fl設定のRelayグループ | | | | • | 編集 | |
| х; | オーバーライド | ロードカ | 5 | | | | | | | | | |
| | | | | | 8 | Appliance | _ | | | | | |
| | | | | | ٠ | 管理対象(オンライン) | ÷. | ES> | (i e | sx-vdi | i01.trendnsx.local | |
| | | 8 | 不正プログラ | ラム対策 | • | オン,リアルタイム | 9 | App | liance l | ocalho | st.localdom (Trend Micro | Deep Security (1) |
| | | | Webレビュテ | モション | • | オン | | | | | | |
| | | • | ファイアウォ | ール | | オフ, 11 ルール | | | | | | |
| | | θ | 侵入防御 | | • | オン, 防御, 391 ルール | | | | | | |
| | | ۲ | 変更監視 | | | オフ, 27 ルール | | | | | | |



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

有効化により何かしらのエラーが発生している場合には、意図したセキュリティ機能が提供できていない可能性 がありますので、エラー原因を特定して対処する必要があります。

※自動的に有効化を行わない場合には、DSM 上から個別に仮想マシンの有効化を行う、または、イベントベー スタスク(EBT)を設定する必要があります。イベントベースタスクを設定する場合には、NSX セキュリティポリシ 一のセキュリティプロファイルを[Default(EBT)]に設定しておく必要があります。

(NSX for vShield Endpoint、NSX for vSphere Standard を利用している場合にもサービスプロファイルを [Default(EBT)]に指定する必要があります。)

| vm vSphere Cli | | 7ション サービスの編集 | | × | .ocal ~ 🛛 🤤 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|-------------------------------|-------------------|----------|-------------|
| ネットワークとセキュリ | 名前 * | TRENDNSX-VDI-AM | | | |
| Øッシュボード | 14 70 | | | | |
| 愛 インストールとアップ たき 2000 たまで たまで まで までので までので までので までので までので までので までので まで | 武明 | | | | |
| 20 諸柱入イッナ 同 NSX Edge | | | | | 同規 |
| セキュリティ | アクション | | | | |
| 🧧 Service Composer | | | | | |
| ファイアウォール | ▲ 適田 | | | | |
| | 1100011 | | 0,10,10 | | |
| SpoofGuard | サービフタ Trend Micro | Deep Security 👻 | | | |
| D グループとタグ | サービス プロファイル | | サービス タイプ | | |
| - ツール | | | | | |
| 図 フロー モニタリング | Default (EBT) | * | | | |
| 電 トレースフロー | | | | | |
| サポートノンドル | 状態 | 有効 🌑 | | | |
| IPFIX | 強制 | はい 🌑 | | | |
| - システム | 選択したサービス プロファ | (」」」 (」」は 複数のサービス カテゴロをサポー | トレアおり 強制的に適用されます。 | | |
| ユーザーとドメイン | C ALICOLU CAUCON | | | | |
| | | | | | |
| | | | | | |
| | | | | キャンセル OK | 四中1・3 のアイテム |
| | | | | | ` |
| 最近のタスク アラ | 24 | | | | |

▶ Deep Security 有効化ステータスの確認

各セキュリティ機能における実際の動作確認については、以下の方法で実施することが可能です。実際には環境に応じて必要な検証を実施してください。不正プログラム対策については、DSVAのファイル検出機能(Guest Introspection に依存)が正常に動作をしているか、Web レピュテーションについては、ネットワーク検出機能(Network Introspection に依存)が正常に動作しているかを確認することができます。

不正プログラム対策
 保護対象仮想マシンからテスト用ウイルスファイル(EICAR)をダウンロードして不正プログラム対策イベントが発報するかを確認する。
 詳細及びテスト用ウイルスファイルの取得については、以下の FAQ を参照してください。
 http://esupport.trendmicro.com/solution/ja-JP/1114066.aspx
 Web レピュテーション

(保護対象仮想マシンからトレンドマイクロが用意するテスト用サイトへアクセスを行い、Web レピュテーションイベントが発報するかを確認する。 詳細及びテストサイトの情報は、以下の FAQ を参照してください。 http://esupport.trendmicro.com/solution/ja-JP/1114067.aspx



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

2-4. セキュリティタグを利用した自動隔離の考え方と設定手順

セクション 2-3 のエージェントレスによる仮想マシン保護を行うことでセキュリティレベルを一定レベルに維持する ことが可能となりました。このセクションでは、分散ファイアウォールを利用して DSVA で保護されている仮想マシ ンで検出されたセキュリティイベントをトリガーに該当の仮想マシンを他のネットワークと通信できないように自動 隔離する設定を行います。

2-4-1. セキュリティタグと分散ファイアウォールを利用した自動隔離の仕組み

分散ファイアウォールによるアクセス制御を行うためには、仮想マシンを NSX セキュリティグループに紐付け、それをオブジェクトとしてファイアウォールルールの設定を行います。

セキュリティグループの設定を行う際に、グループのメンバーシップに所属させる基準として、コンピュータ名や オブジェクトタイプ(クラスタなど)とあわせてセキュリティタグを利用することによって、Deep Security のセキュリ ティイベントをトリガーとして該当の仮想マシンの所属するセキュリティグループを動的に変更することが可能と なります。その結果として、適用される分散ファイアウォールルールを変更されることとなります。

セキュリティタグが付与された仮想マシンが所属するセキュリティグループに対して他のネットワークと通信不能 なファイアウォールルールを適用することによって、仮想マシンがあたかもネットワーク設定が変更されて隔離ネ ットワークに移行したような効果を適用することができます(実際は仮想マシンのネットワーク設定は変更されま せん。)



※上記のルールの記載は本ガイドのサンプルの設定内容とは合致していません。



本セッションでは、セクション 2-3-11 で設定したサービスプロファイル及びセキュリティグループを利用して、分散 ファイアウォールによる自動隔離の設定を行います。

分散ファイアウォールのポリシーは以下のルールを設定しています。

(実際のルール設定を行う場合には、適用する環境のセキュリティポリシーにしたがってルール設計を行ってくだ さい。)

| ポリシー/ルール名 | 送信元 | 送信先 | サービス | アクション |
|----------------------------------|-------------------------|-------------------------|------|--------|
| Quarantine | | | | |
| TRENDNSX-VDI-Quarantine-outbound | TRENDNSX-VDI-Quarantine | Any | Any | Block |
| TRENDNSX-VDI-Quarantine-Inbound | Any | TRENDNSX-VDI-Quarantine | Any | Block |
| TRENDNSX-VDItoVDI | | | | |
| VDItoVDI | TRENDNSX-VDI | TRENDNSX-VDI | Any | Block |
| All Permit-Rule | | | | |
| All Permit-Rule | Any | Any | Any | Permit |

NSX セキュリティタグと分散ファイアウォールを利用した自動隔離の設定は以下の流れで行います。



2-4-2. Deep Security NSX セキュリティタグ追加設定

不正プログラム対策イベントを検出した際に NSX セキュリティタグを付与する設定を行います。

DSM から[ポリシー]>[ポリシー]から [VDI_Windows Desktop_Demo01]を選択し、[不正プログラム対策]の
 [詳細]タブを選択する

[NSX セキュリティのタグ付け]で以下の設定を行う



・ [NSX セキュリティのタグ付け] 💠

オン("継承"のチェックボックスを外す)

・ [NSX セキュリティタグ] :

ANTI_VIRUS.VirusFound.threat=high

・ [修復処理に失敗した場合にのみ、NSX セキュリティタグを適用します。]:

チェックボックスを外す

・ [この後の不正プログラム検索が不正プログラム検出イベントが生成されずに完了した場合、以前に適用された NSX セキュリティタグは削除されます。] :

チェックボックスを入れる

※[修復処理に失敗した場合にのみ、NSX セキュリティタグを適用します。]のチェックボックスを入れた場合、 不正プログラムを検出した際に修復処理が成功した場合には、NSX セキュリティタグは付与されず、自動隔離は 行われません。

修復処理の詳細については、以下のヘルプセンターを参照してください。

<u>https://help.deepsecurity.trendmicro.com/12_0/on-premise/ja-jp/Protection-Modules/Intrusion-</u> Prevention/nsx-security-tags.html#Configur

※[この後の不正プログラム検索が不正プログラム検出イベントが生成されずに完了した場合、以前に適用され たNSX セキュリティタグは削除されます。] のチェックボックスを外した場合、自動隔離後に不正プログラム検索 を手動で実施した際に不正プログラム対策イベントが検出されない場合でも NSX セキュリティタグは外れること はなく、NSX Manager 上で直接セキュリティタグを外す必要があります。



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

2-4-3. 不正プログラム対策イベント 即時通知の設定

自動隔離が実行される流れは、以下のとおりです。

DSVA にて不正プログラムを検出 ↓

DSM⇔DSVA のハートビート間隔で DSM ヘイベントを通知

Ţ

DSM から vCenter Server へ該当仮想マシンに対するセキュリティタグ付与を実行

Ţ

仮想マシンを自動隔離

デフォルトの設定では、DSVA⇔DSM のハートビート間隔が 10 分(最短 1 分に設定可能)のため、DSVA で不正 プログラムイベントが検出されてから、DSM に通知=NSX セキュリティタグの付与まで最大 10 分を要する可能 性があります。ハートビートを待たずに、DSVA が不正プログラム対策を検知した時点で即時イベントを DSM で 検知できるように設定を行います。

1) DSM サーバにアクセスして、Windows コマンドプロンプトを立ち上げ、Deep Security Manager のインストール ディレクトリから以下のコマンドを実行

C:¥Program Files¥Trend Micro¥Deep Security Manager>dsm_c.exe -action changesetting -name com.trendmicro.ds.antimalware:settings.operational.AMNotifyEventImmediate -value true

Stopping Trend Micro Deep Security Manager... System Setting: com.trendmicro.ds.antimalware:settings.operational.AMNotifyEvent Immediate Value: true saved Complete

Starting Trend Micro Deep Security Manager...

C:¥Program Files¥Trend Micro¥Deep Security Manager>

※コマンドを実行すると、DSM プロセスの再起動が発生します。 ※DSM サーバが複数ノードある場合でも1台の DSM サーバで実行すれば変更は反映されます。



2) 設定を各 DSVA に反映させるため、DSVA に対するポリシーの配信を行う

| | SX Agents サブグループを含む 👻 グループ別 👻 |] | | | | | | |
|---|---------------------------------------------------------|---------------|----------|-------|---------------------|---------------|---------------------------------|------|
| | ▶ 追加 → 面削除 回詳細 → 処理 → 自 | | エクス | ボート 👻 | 毘.列 | | | |
| | 名前 🔺 | 説明 | | | ブラットフォーム | ポリシー | | ス |
| ~ | コンピュータ > vCenter - vc01.trendnsx.local > 仮想マシン | > NSX-T > ESX | Agents | (3) | | | | |
| | 🗣 localhost.localdomain (Trend Micro_Deep Security (1)) | | | [| Deep Security Virt… | Deep Security | Virtual Appliance | ● 管理 |
| | 🗣 localhost.localdomain (Trend Micro_Deep Security (2)) | すべて遅れ (3 | 1) | [| Deep Security Virt… | Deep Security | Virtual Appliance | ● 管理 |
| | 획 localhost.localdomain (Trend Micro_Deep Security (3)) | 9. (0.81/(0 | <i>"</i> | | Deep Security Virt… | Deep Security | Deep Security Virtual Appliance | 管理 |
| | | ◆ 処理 | • | 昭 ステ | ータスの確認 | | | |
| | | - | | 🕵 有効 | 帅化/再有効化 | | | |
| | | | | 🐴 Арр | lianceの無効化 | | | |
| | | | | 良が | シーの送信 | | | |

2-4-4. 分散ファイアウォールと連携した自動隔離設定

TRENDNSX-VDI グループに所属する仮想マシン、NSX セキュリティタグが付与され自動隔離された仮想マシン に適用するファイアウォールポリシーを作成します。

1) NSX Manager にアクセスし、[セキュリティ]>[East-West のセキュリティ]>[分散ファイアウォール]を選択し、[カテゴリ固有のルールを選択し、[ポリシーの追加]を行う



2) 隔離用ポリシーを作成する

2-1) [名前]列の"New Policy"をクリックして名前を変更 "Quarantine"して、さらに[ルールの追加を行う

| + ポリシー | -の追加 | 十 ルールを追加 | □ クローン作成 | 5 取り消す 📋 削除 | 未発行の変更:1件 | |
|--------|------|------------|----------|---------------|---------------|--|
| | | 名前 | 送信元 | 宛先 | サービス | |
| : > | | Quarantine | (0) | ドメイン: default | | |



2-2)隔離用ルールを作成する

作成したポリシーの横にあるチェックボックスをオンにして[ルールを追加] する

ポリシーの下に新規に追加されたルールを以下の通り設定してアウトバウンドのブロックルールを作成する



同様にインバウンドのブロックルールを作成し、2つの隔離用ルールが作成できていることを確認する

| + ポリ: | シーの追加 | コーキールを追加 □ クローン作成 ← |)取り消す 🛄 削除 \cdots | 未発行の変更:3件 | | | | |
|-------|-------|----------------------------------|-------------------------|-------------------------|------|--------|---------------------|----------|
| | | 名前 | 送信元 | 宛先 | サービス | プロファイル | 適用先 アクション | |
| ÷ ~ | | Quarantine (0) ドメイ | >: default | | | | | |
| ÷ | ~ | TRENDNSX-VDI-Quarantine-Outbound | TRENDNSX-VDI-Quarantine | 任意 | 任意 | 任意 | 分散ファイアウォ●_ ドロップ ~ | () () |
| : | ~ | TRENDNSX-VDI-Quarantine-Inbound | 任意 | TRENDNSX-VDI-Quarantine | 任意 | 任意 | 分散ファイアウォ●_ ドロップ ~ 💽 | @ E |



3) VDI ドメイン用ポリシーを作成する

3-1) 1)と同様に新規ポリシーを作成し、[名前]列の"New Policy"をクリックして名前を変更"TRENDNSX-VDItoVDI"して、さらに[ルールの追加)を行う

| + ポリシ- | -の追加 | 十 ルールを追加 | □ クローン作成 | ∽ 取り消す | 前 削除 ••• | 未発行の変更:1件 |
|--------|------|-------------------|----------|---------------|----------|-----------|
| | | 名前 | 送信元 | 宛先 | | サービス |
| : > | | TRENDNSX-VDItoVDI | (0) | ドメイン: default | | |

3-2) VDI 仮想マシン間のアクセスをドロップするルールを作成する

作成したポリシーの横にあるチェックボックスをオンにして[ルールを追加] する

ポリシーの下に新規に追加されたルールを以下の通り設定して VDI 仮想マシン間のブロックルールを作成 する

| | | 各前 | 送信元 | 宛先 | サービス | プロファイル | 邊用先 | アクシ | | | | |
|-----|----------------------------------|-----------------------|---------------------------------------------------------|--------------------------------------------------------------|------------------------------------------|----------------------------|--------------------|-----|--|--|--|--|
| ÷ ~ | | TRENDNSX-VDItoVDI (0) | ドメイン: def | | | | | | | | | |
| : | | VDItoVDI | 任意 🧪 | 任意 | 任意 | 任意 | 分散ファイアウォ | • # | | | | |
| | | 名前 送信元 宛先 | : ルール名を : 宛先カラム "TRENDNSX : 宛先カラム "TRENDNSX | 任意に設定"VC をダブルクリック C-VDI"を選択す をダブルクリック C-VDI"を選択す | DitoVDI" して"宛先の設 る して"宛先の設 る | 定"から VDI ドメ 定"から VDI ドメ | イン用グループ イン用グループ | | | | | |
| | • | サービス | : 任意(デフォ | トルト) | | | | | | | | |
| | • | プロファイル | : 任意(デフォ | トルト) | | | | | | | | |
| | ・ 適用例 : 分散ファイアウォール(デフォルト) | | | | | | | | | | | |
| | アクション : ドロップ | | | | | | | | | | | |

ルールが作成できていることを確認する

| | | | 名前 | 送信元 | 宛先 | サービス | プロファイル | 遼用先 | アクション |
|---|---|---|-----------------------|--------------|--------------|------|--------|----------|--------|
| : | ~ | | TRENDNSX-VDItoVDI (0) | ドメイン: def | fault | | | | |
| : | | ~ | VDItoVDI | TRENDNSX-VDI | TRENDNSX-VDI | 任意 | 任意 | 分散ファイアウォ | ドロップ ~ |

4) VDI ドメインからその他のネットワークに対する通信をすべて許可するルールを同様に作成する

| : ~ | | All Permit-Rule | 0) | 適用先 分散ファイアウォ | | | | | 初期化さ | れていません 🖱 🕕 🎯 |
|-----|------------------|-----------------|-------------------------------|--------------|---------------|---------|----|----------|--------------------------|--------------|
| : | | All Permit-Rule | 1 | 任意 | 任意 | 任意 | なし | 分散ファイアウォ | ●許可 ∨ | • • |
| | \triangleright | ポリシー | | | | | | | | |
| | | • 名前 | :ポリシー名を任意に設定"All Permit-Rule" | | | | | | | |
| | ۶ | ルール | | | | | | | | |
| | | · 名前 | : | ルール名を任意に | こ設定"All Permi | t-Rule" | | | | |
| | | | | | | | | | | |



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

- 送信元 : 任意(デフォルト)
- 宛先
 : 任意(デフォルト)
- ・ **サービス** : 任意(デフォルト)
- プロファイル : 任意(デフォルト)
- **適用例** : 分散ファイアウォール(デフォルト)
- アクション : 許可

5) ルールの各 ESXi ホストへの配信

5-1) ルールの設定が完了したら各 ESXi ホスト上の分散ファイアウォールモジュールにルールを反映させるため、[**発行**を選択する

※ポリシーを発行する前に必ず隔離用ポリシーが VDI ドメイン用ポリシーの上位に配置されるかを確認してく ださい。セキュリティグループの特性上、1 つのオブジェクトが複数のグループに所属している場合、分散ファイ アウォールでは、上位にあるグループのポリシーが適用されます。隔離用ポリシーが下位にある場合には自動 隔離がされなくなるため注意してください。(NSX for vSphere ではセキュリティグループの設定に除外項目があ りましたが、NSX-T ではありません。)

| 木- | -A 7 | ドットワ | ーク セキュリティ インベントリ | ブ | ランとトラブルシューティング システ | ム ネットワークとセキュリ | ティの詳細設定 | | | | |
|-----|----------|------------|----------------------------------|-----------|----------------------------|-------------------------|---------|--------|------------|-----------------------------|------------|
| » | 日 分散: | ファイア | マウォール ⑦ ブラックリスト | | | | | | 末発行の変更の合計: | 2件 アクション 7 | に戻す 発行 |
| ø | すべての | ルール | カテゴリ固有のルール | | | | | | | | |
| | A Identi | ty Firewal | II が無効です。ID エンティティを持つグループ (例: Ac | tive Dire | ctory グループ を含むルールは適用されません。 | | | | | | 有効化 |
| E | | | | | | | | | | | |
| Q. | E | THERNET | T (0) EMERGENCY (0) | | INFRASTRUCTURE (0) ENVIRON | MENT (0) • APPLICATION | 1 (4) | | | | |
| | | | | | | | | | | | |
| | + ポリミ | シーの追加 | 🔹 十 ルールを追加 🔲 クローン作成 | う取! |)消す 🛄 削除 •••• 未発行の変更: | 2 (4 | | | | | Τ |
| 88 | | | 名前 | | 送信元 | 宛先 | サービス | プロファイル | 遍用先 | アクション | |
| Ð | : ~ | | Quarantine | (2) | 適用先 分散ファイアウォー | | | | | ● 初期化されてい | いません 🖱 🕕 🐵 |
| | : | | TRENDNSX-VDI-Quarantine-outbound | 1 | 28 TRENDNSX-VDI-Quarantine | 任意 | 任意 | なし | 分散ファイアウォー | ● ドロップ 〜 | () |
| œ\$ | : | | TRENDNSX-VDI-Quarantine-Inbound | (1) | 任意 | TRENDNSX-VDI-Quarantine | 任意 | なし | 分散ファイアウォ | ドロップ ~ | () |
| | : ~ | | TRENDNSX-VDItoVDI | (1) | 適用先 分散ファイアウォー | | | | | 初期化されてい | いません 🖱 🕦 🛞 |
| 88 | : | | VDitoVDI | 1 | 28 TRENDNSX-VDI | 22 TRENDNSX-VDI | 任意 | なし | 分散ファイアウォー | ● ドロップ 〜 | () |
| | : ~ | | All Permit-Rule | (1) | 適用先 分散ファイアウォ | | | | | ● 初期化されてい | いません 😋 🕕 🔘 |
| | : | | All Permit-Rule | (1) | 任意 | 任意 | 任意 | なし | 分散ファイアウォー | ●許可 ∨ | () |
| | | | | | | | | | | | |

5-2) 各ポリシーが"稼働中"となっていることを確認する

| ホー | A 2 | ネットワーク | セキュリティ インベントリ | プ | ランとトラブルシューティング シス | テム ネットワークとセキュ | リティの詳細設定 | | | | |
|----------|---------|------------------|--------------------------------|----------|----------------------------|----------------------------|----------|--------|-----------|----------|---------------------------------------|
| » | 🔜 分散 | タファイアウォ | tール ⑦ -ロ- ブラックリスト | | | | | | | アクション | 一元に戻す 発行 |
| Ø | すべての | 011-11 <u>1</u> | カテゴリ固有のルール | | | | | | | | |
| E | 🛆 Ident | tity Firewall が無 | 物です。ID エンティティを持つグループ (例: Act | ive Dire | ctory グループ)を含むルールは適用されません。 | | | | | | 有効化 |
| ц. | | ETHERNET (0) | EMERGENCY (D) | | INFRASTRUCTURE (0) ENVIRO | NMENT (0) APPLICATIO | DN (4) | | | | |
| | + #9 | シーの追加 | 十 ルールを追加 🔲 クローン作成 ' | う取り |)消す 前 削除 ・・・ | | | | | | т |
| 88 | | 2 | ň | | 送信元 | 宛先 | サービス | プロファイル | 邊用先 | アクション | |
| Ð | : ~ | Qu | iarantine | (2) | 適用先 分散ファイアウォー | | | | | | ● 稼動中 C ④ |
| | : | □ TR | ENDNSX-VDI-Quarantine-outbound | (1) | 28 TRENDNSX-VDI-Quarantine | 任意 | 任意 | なし | 分散ファイアウォー | ● ドロップ ~ | () 🖗 🖂 |
| CB | : | □ TR | ENDNSX-VDI-Quarantine-Inbound | 1 | 任意 | 28 TRENDNSX-VDI-Quarantine | 任意 | なし | 分散ファイアウォ | ● ドロップ ~ | |
| | : ~ | TR | ENDNSX-VDItoVDI | (1) | 適用先 分散ファイアウォー | | | | | | ● 稼動中 C ④ ◎ |
| 88 | : | | DitoVDI | 1 | 28 TRENDNSX-VDI | TRENDNSX-VDI | 任意 | なし | 分散ファイアウォ | ● ドロップ 〜 | |
| | : ~ | | Permit-Rule | (1) | 適用先 分散ファイアウォー | | | | | | ● 稼動中 ご ① 🐵 |
| | : | | Permit-Rule | (1) | 任意 | 任意 | 任意 | なし | 分散ファイアウォー | •許可 ~ | () 🖗 🖂 |



2-4-5. 分散ファイアウォールによる自動隔離のテスト

仮想マシンで不正プログラム対策イベントを検出した際に、セキュリティタグが付与されて該当端末の通信ができなくなることを確認します。

1) NSX Manager にアクセスし、[インベントリ]>[グループ]を開く

"TRENDNSX-VDI"グループに仮想マシンが所属していることを確認する

| マニックス コンション フランビッフルシューティック システム F ネタドウニックとビオユウティの外部の定 | |
|-------------------------------------------------------|------------------|
| メンバーの表示 TRENDNSX-VDI | |
| 有効なメンバー グループ定義 | |
| 仮想 マシン IP アドレス | |
| | |
| 名崩 | |
| AM-Winto-001 | |
| AM-Win10-002 | |
| AM-Win10-003 | |
| AM-Wint0-004 | |
| AM-Win10-005 | |
| AM-Win10-006 | |
| AM-Win10-007 | |
| AM-Win10-008 | |
| AM-Win10-009 | |
| AM-Win10-010 | |
| | |
| C @w | 仮想マシン: 10 個中 1 ~ |
| | |
| | NO LA |

2) 隔離を実施する仮想マシンから外部ネットワークに対してコマンドプロンプトにて Ping を実行する

| 📾 C:¥WINDOWS¥system32¥cmd.exe | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| C:¥Documents and Settings¥admin>ping 10.3.224.254 -t | |
| Pinging 10.3.224.254 with 32 bytes of data: | |
| Reply from 10.3.224.254: bytes=32 time<1ms TTL=63 Reply from 10.3.224.254: bytes=32 time<1ms TTL=63 Reply from 10.3.224.254: bytes=32 time<1ms TTL=63 | |



 仮想マシンからテスト用ウイルスファイル(EICAR)をダウンロードする (リモートデスクトップでアクセスしている場合にはアクセスが切断されます) 詳細及びテスト用ウイルスファイルの取得については、以下の FAQ を参照してください。 <u>http://esupport.trendmicro.com/solution/ja-JP/1114066.aspx</u>

| 🕗 TREND Deep Security | O AM-Win7-001.trendnsx.local (/ | (/ LL/ LLL []) - Google Chrome — 🗆 🗙 |
|-------------------------------|---------------------------------|-----------------------------------------------------------------------------------------------|
| ダッシュボード 処理 アラート イベントとレポー | ▲ 保護されていない通信 10 | 0.0.000.100.4119/ComputerEditor.screen?hostID=1288#com.trendmicro.ds.antimalwareAntiMalwareMa |
| ✓ N スマートフォルダ ▲ ICO01 ##550 | コンピュータ: | ⑦ ヘルゴ |
| ▶ TEST | ● 概要 | ection Connected Threat Defense 詳細 検出ファイル 不正プログラム対策イベント 📢 🕨 |
| > 目コンビュータ 一部間 | 💿 不正プログラム対策 | |
| ✓ 🔐 vCenter - vc01 名前 | 👩 Webレビュテーション | 1上フロクラム対東1ペント すべて ▼ クループ化しない ▼ Q このページを検索 |
| ✓ → ホストおよて ✓ コンピュータ> vGente | 😑 ファイアウォール | 期間: 過去1時間 |
| > 🗿 NSX 🖓 4 | ● 侵入防御 | コンピュータ: コンピュータ: × AM-Win7-001.trendnsx.local (AM-Win7-0 × |
| > 🎒 NSX-1 🖓 4 | 🔘 変更監視 | |
| ・ | セキュリティログ監視 セキュリティログ監視 | ■表示 🎦 エクスポート 🔹 自動タグ付け 田 列 |
| > 🗿 NSX 👘 4 | 🥺 アブリケーションコントロー | _ 時刻 ▼ コンピュータ 感染ファイル タグ ^ |
| ✓ | 🔳 インタフェース | ■ 2019-12-03 11:44:16 C#Users¥administrator¥Desktop¥新しいテキ… |
| ▶ 0 | | 2019-12-03 11:44:13 C#Users¥administrator¥Desktop¥新しいテキ… C#Users¥administrator¥Desktop¥新しいテキ… |
| È C | 😨 アップデート | 2019-12-03 1143.44 A Character CHUSers+administrator+AppData+Local+Micr*** C |
| ► C | ン、オーバーライド | イベントの取得 |
| 📄 o 🔐 🖓 🚛 😳 111.trend | | (22) 問:"ろ |
| 🔛 Et | < → | |

4) EICAR を検出した仮想マシンが"TRENDNSX-VDI-Quarantine"に移動していることを確認する

| ホーム ネットワーク | セキュ | リティーイン | ベントリ | ツール | システム | ネットワークとセキュ | リティの詳細設定 |
|-----------------|------------|---------|------|-----|------|------------|----------|
| « | < <u>6</u> | の 仮想マシン | / | | | | |
| ② 設定の概要 | | | | | | | |
| ふ ドメイン | | | | | | | |
| ⇔ サービス | | | 名前 | | | | タグ |
| 田 グループ | | : 👦 | AM | 001 | | | 1 |
| 🔂 仮想マシン | - | : @ | AM | 002 | | | 0 |
| 🔓 コンテキスト プロファイル | _ | | | | | | |
| - | | : 🗗 | AM | 003 | | | 0 |

また、2)で実行していた Ping が、仮想マシンが分散ファイアウォールにより隔離されたことにより、疎通 NG となっていることを確認してください。(Web コンソールなどで確認ができる場合)

| 🔤 C:¥WINDOWS¥system32¥cmd.exe | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| C:¥Documents and Settings¥admin>ping 10.3.224.254 -t | ^ |
| | |
| Pinging IU.3.224.254 with 32 bytes of data: | |
| Reply from 10.3.224.254: bytes=32 time<1ms TTL=63 Reply from 10.3.224.254: bytes=32 time<1ms TTL=63 | |
| Request timed out. | |
| Request timed out. Request timed out | |
| Request timed out. | |
| Kequest timed out. | |



5) NSX Manager から該当仮想マシンのセキュリティタグを手動で削除することによって、隔離の解除

(**"TRENDNSX-VDI"**への復帰)を行う

(セキュリティタグの横についている[×]マークで削除)

| ホーム ネットワーク t « | セキュリティ インベントリ ツール システム | ネットワークとセキュリティの詳細設定 | |
|-----------------------------|------------------------|--------------------|---------------------|
| ② 設定の概要 | | | |
| 品 ドメイン | | | <u>इ</u> / |
| ◎ サービス | 名前 | タヴ | |
| 田 グループ | : 編集 (M001 | 1 | |
| 🔂 仮想マシン | | | |
| 🔓 コンテキスト プロファイル | 名前 | タヴ | |
| | AM001 | Tag (Requ 🕻 |) Scope (Op 🕢 高度な設定 |
| | | Maximum 25 ta | as are allowed. |
| | | Total: 1 ① | VirusFoun Secur X |
| | | | |
| | 保存 キャンセル | | |
| | | | |
| | 名前 | タグ | |
| | : AM7-001 | Tag (Requ |) Scope (Op 🕢 高度な設定 |
| | | Maximum 25 ta | ags are allowed. |
| ホーム ネットワーク | セキュリテ 保存 キャンセル | | |
| « | | | |
| | | | |
| | | | すべてを表示 |
| | | | |
| ♀ サービス | 名 册 | 90 | |
| 田 クループ | E AM 001 | 0 | 高度な設定 |
| 📅 仮想マシン | : AM002 | 0 | 官僚补验党 |

または、DSM から該当仮想マシンに対して不正プログラムのフル検索を行い、完了後に隔離が解除されること

を確認する

([この後の不正プログラム検索が不正プログラム検出イベントが生成されずに完了した場合、以前に適用さ れた NSX セキュリティタグは削除されます。]のチェックボックスをオンにしていた場合のみ)

| コンピュータ: AM-Win | 10-001.trendnsx.local (AM- | -Win10-001) | | | | ⑦ へルブ |
|--------------------------------|--------------------------------------|-----------------------------|-----------|--------|---------------|-------|
| ● 概要 | 一般 Smart Protection (| Connected Threat Defense | 詳細 | 検出ファイル | 不正プログラム対策イベント | |
| 😵 不正プログラム対策 | 設定: 維承 (オン) | • | | | | * |
| 🕐 Webレビュテーション | ステータス: 🌒 オン,リアルタイム | 4 | | | | |
| 😳 ファイアウォール | リアルタイム論索 | | | | | |
| ⊖ 侵入防御 | ☑ 継承 | | | | | |
| ◎ 変更監視 | 不正プログラム検索設定: | Default Real-Time Scan Con | iguration | | ~ 編集 | |
| セキュリティログ監視 | スケジュール: | Every Day All Day | | | ~ 編集 | |
| 🧔 アブリケーションコントロー | 7245 | | | | | |
| ■ インタフェース | 于朝使来 | | | | | |
| 🖨 設定 | 不正プログラム検索設定 | Default Manual Scan Configu | ation | | ~ 編集 | |
| ⑦ アップデート | | | | | | |
| ン\$ オーバーライド | 予約検索 | | | | | |
| | ◎ 超示 不正プログラム検索設定: | Default Scheduled Scan Cont | inuration | | ~ 續生 | |
| | Tables Services | | | | 1mort | |
| | 不正プログラム検索 | | | | | _ |
| | 不正プログラムの前回の手動検索: 不正プログラムの前回の予約検索: | 72U | | | | |
| | 不正プログラムのクイック検索 | 不正プログラムのフル | 食索 | 不正プログ | ラム検索のキャンセル | |
| | | | | - | | ¥ |
| () | | | | | 保存 | 閉じる |



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

6) セキュリティタグが外れたことを確認し、実行していた Ping 疎通が復旧していることを確認する

| 📾 C:¥WINDOWS¥system32¥cmd.exe | _ 🗆 🗡 |
|---------------------------------------------------|-------|
| Request timed out. | - |
| Request timed out. | |
| Reply from 10.3.224.254: bytes=32 time=1ms TTL=63 | |
| Reply from 10.3.224.254: bytes=32 time=1ms TTL=63 | |
| Reply from 10.3.224.254: bytes=32 time<1ms TTL=63 | |
| Reply from 10.3.224.254: bytes=32 time<1ms TTL=63 | |
| Reply from 10.3.224.254: bytes=32 time<1ms TTL=63 | |
| Reply from 10.3.224.254: bytes=32 time<1ms TTL=63 | |
| Reply from 10.3.224.254: bytes=32 time<1ms TTL=63 | |
| Reply from 10.3.224.254: bytes=32 time<1ms TTL=63 | |



3. 設計・導入時に留意するべきポイント

3-1. 設計上留意しておくべきポイント

3-1-1. システム全般

- DSM を稼動させるノードは DSR 以外のアプリケーションを同居させないでください。
 (小規模環境において、DSM 用 SQL サーバが同居することは可能)
- ▶ DSM 用 SQL サーバには、スケーラビリティの観点から Express 版の利用は避けるようにしてください。
- DSM 用 SQL サーバと DSM ノードは同一サイトに設置してください。DSM 用 SQL サーバと DSM サーバ間の通信遅延が大きい場合、DSM が正常に動作しない可能性があります。

DSVA は各 ESXi ホストに 1 台ずつ配置される必要があります。特に共有ディスク上に配置しなくてはならない場合には、DRS/vMotion、Storage vMotion が発生しないように設計をしてください。 また、他の保護対象マシンとのリソースを共有しないようにしてください。オーバーコミット状態の場合、正常に動作しない場合があります。 詳細は以下の FAQ も参照してください。

http://esupport.trendmicro.com/solution/ja-jp/1115886.aspx

仮想デスクトップ環境においては、仮想マシンが常に生成される状態が継続することから、クラスタ上で DRS を有効にしている環境では、仮想マシンの ESXi ホスト間の移動が発生しやすくなります。可能な限り、 DRS の移行のしきい値を優先順位2または優先順位3(デフォルト)に設定してください。

3-1-2. セキュリティ VM の特性

NSX Manager と連携をして vCenter Server から ESXi ホストへ配信される Guest Introspection、DSVA は、セキ ュリティ VM として ESX Agent Manager(EAM)によって管理されています。



DSM は vCenter Server と同期をすることにより、ESXi ホスト、仮想マシンのインベントリ情報を取得しています。 また、NSX Manager は ESXi ホスト上の Guest Introspection Service のステータスを監視するとともに、Guest Introspection サービスを提供する仮想マシン毎に 3rd Party 連携を提供するためのサービスプロファイルを



Context Multiplexer へ提供します。そして、Context Multiplexer は仮想マシン毎に TCP コネクションを DSVA に 張ることにより保護対象仮想マシンの情報を提供します。

一方 Deep Security では、NSX セキュリティポリシー連携またはイベントベースタスク(EBT)により仮想マシンに 対して有効化、セキュリティポリシーの配信が行われ、Deep Security のポリシーが適用されます。このタイミング で Context Multiplexer からの TCP コネクションが何らかの理由で張られていない場合、正常にセキュリティ機能 を提供することができません。

また、DRS/vMotion により仮想マシンが他の ESXi ホストに移動した場合でも DSM は vCenter Server とリアルタ イムに同期しているため、新たな ESXi ホスト上で有効化、セキュリティポリシーの配信を自動的に行うことができ ます。

上記仕様から、NSX Manager、DSVA は常に稼働している必要があります。

そして DSVA は EAM により以下のような制御もされています。

- ・ ホスト起動時の起動順序
- vMotion/DRS による仮想マシン移動の制限
- ・ ステータスチェックと異常検出時の再配信などの解決策の提供

3-1-3. Deep Security が付与する NSX セキュリティタグの特性

Deep Security は、不正プログラム対策イベントが発生した場合に NSX セキュリティタグを付与することができま す。(その他のイベントをトリガーにしてセキュリティタグを付与することはできません。) それぞれのセキュリティタグには異なる属性がありますので、実装時には留意をして設計を行ってください。

> 不正プログラム対策 セキュリティタグ

3 つのタグには差異はなく、仮想マシングループ毎にセキュリティタグが付与された際に適用される分散ファイア ウォールルール(所属するセキュリティグループ)を変えたい場合に利用します。

| AV セキュリティタグ | NSX セキュリティタグ | セキュリティタグ 付与条件 |
|-------------------------------------|-------------------------------------|---------------------------------|
| ANTI_VIRUS.VirusFound.threat=high | ANTI_VIRUS.VirusFound.threat=high | |
| ANTI_VIRUS.VirusFound.threat=medium | ANTI_VIRUS.VirusFound.threat=medium | Deep Security ポリシーにて任 意に設定可能 |
| ANTI_VIRUS.VirusFound.threat=low | ANTI_VIRUS.VirusFound.threat=low | |



3-2. 導入時に留意しておくべきポイント

3-2-1. DSVA リソースチューニング後の OVF ファイルの更新

仮想マシンの集約率が高い環境や DSVA の機能を複数利用する場合、DSVA のリソースがデフォルト値以上に 必要になることがあります。その場合には DSVA の OVF ファイル内の下記のパラメータを DSVA のデプロイ前 に変更しておく必要があります。

NSX-T2.4 までは、DSM へ DSVA OVF をアップロード後、DSM インストールフォルダ配下の以下のフォルダに格 納される dsva.ovf ファイルの中の以下のパラメータを修正することで変更が可能です。

<DSM_Install>¥temp¥Appliance-ESX-<appliance_version>

| ·· - 7 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <item></item> |
| <pre><rasd:allocationunits>hertz * 10^6</rasd:allocationunits></pre> |
| <ragd:description>Number of virtual CPUs</ragd:description> |
| <pre><rasd:elementname xmlng:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_ResourceAllocationSettingData">4 virtual CPU</rasd:elementname></pre> |
| <pre><rasd:instanceid xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_ResourceAllocationSettingData">>1</rasd:instanceid></pre> |
| < <u>rasd</u> :ResourceType>3 |
| < <u>rasd</u> :VirtualQuanti <mark>y</mark> >4 <mark sasd:VirtualQuantity> |
| |
| <item></item> |
| <pre><rasd:allocationunits>byte * 2^20</rasd:allocationunits></pre> |
| < <u>rasd</u> :Description>Memory Size <u rasd:Description> |
| <rest: star<="" start="" td=""></rest:> |
| <pre><ragd:instanceid_xmlna:ragd="http: 1="" 2="" cim-schema="" cim_resourceallocationsettingdata"="" schemas.dmtf.org="" wbem="" wscim="">2</ragd:instanceid_xmlna:ragd="http:></pre> |
| < <u>razd</u> :Reservation>6144 <mark .agd:Reservation> |
| < <u>ragd</u> :ResourceType>i |
| <rest:virtualquantity>6144</rest:virtualquantity> |
| |

NSX-T2.5 以降の環境では、セクション 1.4.6 で記載の通り、NSX の仕様の変更に伴い、DSVA など 3rd Party Security VM を各ホストヘデプロイする際に NSX Manager がソフトウェアパッケージに対するデジタル署名のチ ェックを実行するプロセスが追加されています(ソフトウェアパッケージに含まれる.ovf 及び.vmdk ファイルに VMware 社によるデジタル署名が付与されます)。

※Deep Security11.0/NSX-T2.4 までのバージョンで可能であった上記方法(DSVA Zip アップロード後に DSM イ ンストールフォルダの OVF ファイルの変更する方法)を NSX-T2.5 以降の環境行う場合、DSVA デプロイ時に NSX Manager によるデジタル証明書のチェックが行われるためデプロイに失敗します。

NSX-T2.5 以降では、VMware 社によるデジタル署名が付与されている Deep Security 12.0 Update 3 以降の OVF パッケージを必ず使用する必要があり、DSVA に割り振るリソースに応じて以下の 4 種類の OVF ファイル から選択をする必要があります。

| OVF Files | vCPU | Memory |
|-----------------|------|---------|
| dsva.ovf | 2 | 4096MB |
| dsva-small.ovf | 2 | 8192MB |
| dsva-medium.ovf | 4 | 16384MB |
| dsva-large.ovf | 6 | 24576MB |

デプロイの方法を含めて詳細、セクション 1.4.6. NSX-T 2.5.0 以降のセキュリティ VM 配信時の仕様変更に伴う DSVA ソフトウェアパッケージの変更 を参照してください。

※ DSVA デプロイ後に vCenter Server から DSVA に対するリソースを変更することも可能ですが、DSVA の再



配信が発生した場合、パラメータ変更前の状態で再配信されてしまいますので留意が必要です。 本番環境では OVF ファイルの変更を行って運用することを推奨しています。

3-2-2. マルチノード DSM の導入手順

仮想デスクトップ(VDI)環境などにおいて、1000 台の仮想マシンを越える環境で運用する場合、2 台以上の DSM を配置することを推奨しています。DSM を増設することにより各仮想マシンに対する有効化処理や管理な どの負荷分散を図ることが可能です。(複数のセキュリティ機能を利用する場合や有効化処理、ポリシー再配信 などが頻繁に発生することでジョブの処理が多い場合には、1000 台以下であっても DSM の増設が必要な場合 があります。)

▶ 1 台の DSM 用 SQL サーバに接続する DSM は最大 2 台までとすることを推奨しています。

➢ 各 DSM サーバのビルドは統一してください。





以下に DSM を増設するための手順を記載します。

1) 新規に追加する DSM サーバ上で DSM インストーラを実行し、セットアップウィザードにてデータベースの接続 設定まで進み、現在動作している SQL インスタンスを指定する(それまでの手順はセクション 2-3-2 を参照)

| | Trend Micro Deep Security Manag | er 12.0.296のセットアップウィザード | _ 🗆 X |
|------------------------|-------------------------------------------|-------------------------|----------|
| データベース | | | |
| データベースおよび | び接続設定を指定してください。 | | |
| ┌種類──── ● Microsoft | SQL Server 🔿 Oracle Database 🔿 PostgreSQL | | |
| 接続設定 | | | |
| ホスト名: | jpsv01 | | |
| データベース名: | dsm | | |
| ユーザ名: | sa | | |
| パスワード | ••••• | | |
| | | | 言羊糸田 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | く戻る)次 | ヘン キャンセル |

2) データベースオプションで[Manager ノードを新規追加]をクリックし、追加する DSM サーバの情報を設定する (Manager ポート、ハートビートポートは 1 台目の DSM と同様にする)

| Trend Micro Deep Security Mana | ager 12.0.296のセットアップウィザード | _ _ X |
|--------------------------------------------|---------------------------|--------------|
| ータベースオプション | | Ð |
| 選択したデータベースにはすでにデータが含まれています。以下のいずれかのアップグレード | *オブションを選択してください: | |
| ● Managerノードを新規追加 | | |
| Managerアドレス: | jpsv01 | |
| Managerボート | 4119 | |
| | 4120 | |
| ○ 既存のデータベースを上書きする | | |
| ○ 修復として続行 | | |
| | | |
| | | |
| | | |
| | | |
| 備考 | | |
| データベースを上書きすると、既存のデータがすべて削除されます。 | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | < 戻る | 次へ > キャンセル |
| | | |



3) インストールチェックを行う

| 0 | Trend Micro E | Deep Security Manager 12.0.296の† | セットアップウィザード - ロ × | | | |
|----------|------------------------------------------------|----------------------------------|----------------------|--|--|--|
| Trend Mi | Frend Micro Deep Security Manager 12.0システムチェック | | | | | |
| | | | | | | |
| インスト・ | ールのシステムチェックが完了しました。 | | 結果の概要を表示 インストール手順を表示 | | | |
| | | 1 | | | | |
| 結果 | コンポーネント | 理由 | 言羊糸田 | | | |
| | Deep Security ManagerのホストのS | Windows Server 2012 R2はサポートされます。 | なし | | | |
| | Deep Security Managerホストのメモリ | 8 GB RAM | | | | |
| (| Deep Security Managerホストのティスタ 容量 | 24.8 GB(0空き | なし なし | | | |
| | · · · · | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Dee | p Security Managerをインストール システム | チェックを再開 | | | | |
| | | | | | | |
| | | | キャンセル | | | |

4) インストール情報を確認し、[インストール]ボタンをクリックする

| 0 | Trend Micro Deep Security Manager 12.0.296のセットアップウィザード | _ 🗆 X |
|-------------------------------------------------|--------------------------------------------------------|-------|
| インストール情報 | | Ð |
| Deep Security Manage | rrのインストールの概要を確認してください。 | |
| インストールパス: | C#Program Files#Trend Micro#Deep Security Manager | |
| インストールモード: | Managerノードを新規追加 | |
| Managerアドレス: Managerボート: ハートピートボート: | https://jpsv01 4119 4120 | |
| データベース: データベースのホスト データベース名: データベースユーザ名 | Microsoft SQL Server 42:jpsv01 dsm i: sa | |
| | | |
| | | |
| | | |
| | 1221-11 | キャンセル |



5) インストール完了を確認する

| | Trend Micro Deep Security Manager 12.0.296のセットアップウィザード | × |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Trend Micro | インストールが完了しました | |
| DEEP SECURITY | ー Deep Security Managerがインストールされました。Deep Security Managerのコンソールを起動するには、Windowsの [スタート] メニューから てのプログラム]→[Trend Micro]→[Deep Security Manager] の順に選択します。 | [すべ |
| 12 | 「終了」をクリックすると、セットアップウィザードが終了します。 | |
| | ✔ Deep Security Managerコンソールを起動する | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| \overline{O} | | |
| | | |
| | | |
| | | |
| | | 7 |

DSM ヘアクセスし、DSM が複数ノード SQL サーバに接続していることを確認することができます。 [**管理]>[システム情報]>[システムノアクティビティ]>[アクティビティグラフ付きネットワークマップ]**



DSM が複数ノードで構成されると有効化処理やイベントの取得などは DSM 間で負荷分散することが可能となります。



▶ vCenter Server との同期処理については、最後に SQL サーバに接続された DSM サーバが行います。

[管理]>[システム情報]>[システムノアクティビティ]>[ノードおよび種類別ジョブの総数]

青い"その他"の部分の処理の中に vCenter との同期処理などが含まれています。



NSX Manager とのコミュニケーションについては、デフォルトでは最初に SQL サーバに接続された DSM が行います。また、NSX Manager はその DSM サーバの URL 情報を保持し、ステータスを監視しています。

NSX Manager と通信をする DSM サーバは以下の設定により変更が可能です。

[管理]>[システム設定]>[詳細]>[NSX 通信の Manager ノード]

| | ∕ュボード | 処理 | アラート | イベントと | ビレボート | コンビュータ | ポリシー 管 | 理 | | | | | |
|----------------------------------------|----------------------|-------------------------|------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------|---------|--------|------------------------|--------|----------------------|-------------|---------|
| 🍄 システム設定 | | | シス | システム設定 | | | | | | | | | |
| | 予約タスク | 7 | | Agent | アラート | コンテキスト | イベントの転送 | ランク付け | システムイベント | セキュリティ | アップデート | スマートフィードバック | Connt 🔍 |
| E | イベントベー: Managerノー | スタスク ド | : | 推奨設 | 推奨設定の検索中のCPU使用率 | | | | | | | | |
| 6 | ライセンス | | | CPU使用 | CPU使用率レベルを下げると、ファイル検索間の待機時間が長くなり、CPUリソースの消費を抑えることができます。 | | | | | | | | |
| ~ 🥠 | ユーザ管理 | | | - (備考 | OF VIZ 加辛レン ソル・ 同 「 「 「 の 」 の の に 、 Deep Security Managerの 推奨設定の 検索プロセスで 使用される CPU/ソースにの み影響します。 Deep Security Managerで 実行されている その他の プ | | | | | | | | |
| | 装 ユーザ | | | ロセスは、引き続きCPUの合計負荷に影響します。 | | | | | | | | | |
| | 指 役割 | | | NSX | | | | | | | | | |
| | 🔚 連絡先 | ■ 連絡先 NSX通信のManagerノード: | | | | | | dsm0* | dsm01.trendnsx.local 🔹 | | | | |
| ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ | システム情報 | R | | П <u>і</u> – | ПЭ ———————————————————————————————————— | | | | | | dsm01.trendnsx.local | | |
| ~ C | アップデート | | | | ロゴのイン | ポート | | iのリセット | | DSM03 | trendnsx.local. | | |

ここで指定された DSM サーバは DSVA を配信する際に NSX Manager が OVF ファイルをダウンロードする ノードでもあります。

マルチノード DSM 環境では、コミュニケーションしている DSM サーバがメンテナンスなどでシャットダウンした場合、他の通信可能な DSM サーバの情報が NSX Manager 側に自動的に通知されます。 NSX Manager は DSVA の OVF ファイルのダウンロード先 DSM サーバの URL が更新されると、DSVA の再 デプロイが必要と判断する仕様となっており、意図せず DSVA の再配信が発生します。



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

上記のような意図しない再配信を回避するためには、DSM にて DSVA OVF ファイルのダウンロード先 URL を明示的に設定してください。(一意の DSM サーバの DSVA パッケージアップロード URL または外部 Web サーバに格納したソフトウェアパッケージの URL を指定)

DSM の[コンピュータ]画面から連携している vCenter Server の[プロパティ]を選択して、[NSX Manager]で以下の設定を実施

 [Deep Security Manager データベースではなく、ローカル Web サーバ上に Deep Security Virtual Appliance アプライアンスパッケージをホストする] :

チェックボックスを入れる

・ [Virtual Appliance OVF の URL] :

特定の DSM サーバまたは OVF ファイルを 格納した外部 Web サーバ

| 一般 | NSX Manager | NSX設定 | | | | | | | | | |
|----|--------------------------------------------------------------------------------------------------|-------|----|-------|----|--|--|--|--|--|--|
| 一般 | | | | | | | | | | | |
| | Deep Security Managerデータベースではなく、ローカルWebサーバ上にDeep Security Virtual Applianceアブライアンスパッケージをホストする | | | | | | | | | | |
| | Virtual Appliance OVFのURL: | | | | | | | | | | |
| | http://10.3.225.186/DSVA12.0u3/dsva-medium.ovf | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | ОК | キャンセル | 適用 | | | | | | |

指定した NSX Manager からも以下の画面で OVF ファイルの URL が確認できます。

[ネットワークとセキュリティの詳細設定]>[パートナーサービス]>[カタログ]>[登録されたサービス]





Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

3-3. 管理サーバ群を DSVA で保護する場合の考慮事項

vCenter Server や DSM サーバを配置する ESXi ホストを DSVA で保護することも可能です。ただし、管理サーバ である DSM を管理される DSVA で保護する場合、障害発生時の切り分けに時間を要することが懸念されます。 そのような環境に DSM を配置する場合には、DSM と同居している DSR(リレー化した DSA)にてセキュリティ保 護を行うことを推奨しています。

Deep Security では DSA と DSVA を同時に稼動させるコンバインモードの実装が可能です。 コンバインモードの特徴は以下のとおりです。

- DSVA が動作する ESXi ホスト上に DSA がインストールされた仮想マシンが配置されると自動的にコン バインモードとして動作します。
- ・ コンバインモードでは機能ごとに DSA または DSVA を使い分けることができます。

| ステータス | | |
|-------------|------------------|------------------------------|
| | Appliance | 阃 Agent |
| ステータス: | 🌖 管理対象 (オンライン) | 😝 管理対象 (オンライン) |
| 不正プログラム対策: | 🎧 オン, リアルタイム | 💿 無効 |
| Webレビュテーション | < 🌚 サポートされていませ/ | し 😱 オン |
| ファイアウォール: | 💮 サポートされていません | ん 🌚 オフ, インストールされていません, ルールなし |
| 侵入防御: | 🛞 サポートされていませ/ | ん 🍈 オフ, インストールされていません, ルールなし |
| 変更監視: | 🍈 オフ, ルールなし | () 無効 |
| セキュリティログ監視 | 🗄 💽 サポートされていません | ん 🍥 オフ, インストールされていません, ルールなし |
| オンライン: | はい | はい |
| 前回の通信: | 2015-10-07 20:18 | 2015-10-07 20:19 |

・ コンバインモードの動作仕様は以下の4つから選択可能です(DS9.6 ではデフォルトから変更不可)

Appliance 優先 : Appliance 障害時に Agent にてセキュリティ機能継続

- Agent 優先 : Agent 障害時に Appliance にてセキュリティ機能継続
- Appliance のみ : Appliance 障害時に Agent へのセキュリティ保護移行を行わない
- Agent のみ: Agent 障害時に Appliance へのセキュリティ保護移行を行わない
- デフォルトでは以下のように動作します。
 - 不正プログラム対策 : Appliance 優先
 Web レピュテーション/ファイアウォール/侵入防御 : Agent 優先
 - 変更監視 :

コンバインモードとなっている DSM サーバは、すべての機能を"Agent のみ"にて設定することをご検討ください。(Deep Security では DSM と同居する DSA のライセンスはかかりません)

| コンピュータ: dsm01.trendnsx.local | | | | | | | | | |
|------------------------------|--------------|----------------------------------------------------|--------|---------|-------------|---|-------------|---|--|
| 📓 概要 | - | 一般 | 詳細 | Scanner | イベントの転送 | | | | |
| 💿 不正ブ | ログラム対策 | | | | | | •••••• | | |
| 👩 Webl/t | ニュテーション | パスワードの確認入力: | | | | | | | |
| 😳 ファイフ | "ウォール コ | コンパインモードの場合の保護ソース | | | | | | | |
| 🖯 侵入防 | 御 | AgentとApplianceの両方が存在する場合に保護対象供するコンボーネントを選択してください。 | | | | | | | |
| 🔘 変更監 | 視 | ব | 下正プログラ | ラム対策: | | | Agentのみ | - | |
| t+1 | リティログ監視 | Webレビュテーション / ファイアウォール / 侵入防御: | | 防御: | Agent()) 24 | - | | | |
| 😕 アプリク | 「ーションコントロー | Ŧ | 変更監視: | | | | Agent()) 73 | - | |
| 🔳 インタン | ² | 「 「「「「「「「「「「「」」」」」」「「「」」」」」」」」「「「」」」」」」」 | | | | | | | |
| 西 設定 | | | | | | | | | |

Copyright (c) 2019 Trend Micro Incorporated. All rights reserved.

Appliance 優先



Public VMware NSX-T & Trend Micro Deep Security インテグレーションガイド

3-4. 仮想デスクトップ環境における NSX、DSVA のサイジング

NSX 環境において、DSVA を利用したエージェントレスによる仮想デスクトップの保護を行う場合のサイジング、 導入時に必要となるチューニングについて記載します。

サイジングについては、運用開始後のチューニング、ノード追加はシステム影響、作業工数に影響がありますの で、できる限り余裕をもった設計を行うことを推奨します。

Deep Security に関する各種パフォーマンス情報は、DSM 上から確認することができます。

[管理]>[システム情報]>[システムの詳細]>[Manager ノード]

3-4-1. DSM サーバのサイジング指標

▶ リソースの割り当て

- 不正プログラム対策を利用して 500~1000 台程度の仮想デスクトップを保護する場合には、DSM アプリケーション用として以下のリソースを割り当てることを推奨します。(DSM 用 SQL データベースを別サーバに構築することを前提)
 - 4vCPU
 - メモリ 8GB(サーバに対しては OS のオーバヘッドを考慮して 12GB 程度)
 - ディスク 10GB 以上
 すべての構成・イベント情報をデータベースに保存するため、プログラム自体のディスク容量としては 5GB 程度確保いただければ問題ありませんが、障害発生時など、デバッグレベルのログを
 生成する場合は一時的に大量のログを保存する場合があるため
- ・ IOPS については OS およびデータベースの使用を満たしていれば問題ありません。
- 1000 台を超える仮想デスクトップ環境を保護する場合、または DSM の冗長化が必要な場合には、
 DSM の増設(同一データベースインスタンスへの接続)を推奨します。
- ・ 仮想デスクトップ環境において、DSVA による不正プログラム対策のみを利用する場合、VDI1000 台か ら 1200 台毎に DSM を増設することを推奨します。
 - 「不正プログラム対策エンジンがオフライン」エラーの発生がないこと、Deep Security システム全体として稼働に問題がないと判断される場合には、リソース使用状況に応じてそれ以上の台数を収容しても問題ありませんが、導入初期段階から本指標以上を前提とした構成は推奨しておりません。)
 - フルクローンの固定割り当て型の場合には、DSM での仮想マシンへの有効化処理などのジョブ が多くなく、比較的多くの仮想デスクトップ端末を DSM で管理することができる傾向にあります。
 ー方リンククローンやインスタントクローンなどフローティング割り当てが採用されている場合には、 常に仮想デスクトップ端末の有効化処理やポリシー配信などのジョブ処理が DSM 上で行われる ことになるため、DSM での管理台数をベースとして上記指標をベースに構成いただくことを推奨し ています。
- 同一データベースインスタンスに対する DSM の接続は 2 台までとして DSM セットを構成することを推 奨しています。
- ・ 仮想デスクトップ環境の場合、vCenter 1Block あたりに1DSM セットで構成してください。
- ・ DS が利用するコンポーネント間の通信に関しては最低 1Gbps の帯域を推奨しています。



▶ 【TIPS】DSM アプリケーションに対するメモリ割り当て

DSM は標準インストール状態では OS に割り振っているメモリ容量に関わらず、4GB までしかメモリを使用 しないように制御されています。物理リソースの割り当て以外に必ず以下の手順に添って、DSM アプリケー ションの最大メモリ使用量の変更を行ってください。

- Deep Security Manager のインストールディレクトリに移動する (Deep Security Manager の実行 可能ファイルと同じディレクトリ)
- 2)新しいファイルを作成し、プラットフォームに応じて、次のようにファイル名を設定する。
 - Windows : Deep Security Manager.vmoptions
 - Linux : dsm_s.vmoptions
- 3) ファイルに「-Xmx10g 」という行を追加する

(この例では「10g」を指定することにより、Deep Security Manager で 10GB のメモリを使用可能となる)

4) ファイルを保存し、Deep Security Manager を再起動します。

- 5) [管理]>[システム情報] に進み、[システムの詳細]>[Manager ノード]>[メモリ] を展開して、 [最大メモリ] に新しいパラメータが反映されていることを確認する
- 仮想デスクトップ環境におけるパフォーマンスプロファイルの変更による DSM のジョブ処理能力の向上 DSM の各種処理はすべてジョブとして管理されており、ジョブの同時処理能力は CPU に依存しています。 そのため、DSM における有効化処理、ポリシー配信が遅いなどの事象が発生する場合には、
 - DSM に対する vCPU の追加割り当て
 - DSM の増設

を検討する必要があります。

また、1000 台を超える仮想マシンの保護を行う場合、短期間にジョブ処理が集中することにより処理遅延、 有効化の失敗などが発生する場合があります。その場合には、パフォーマンスプロファイルの変更を行うこ とで処理効率を向上することが可能となります。

必要に応じて、以下の FAQ よりパフォーマンスプロファイルをダウンロードして適用してください。

http://esupport.trendmicro.com/solution/ja-JP/1119051.aspx

※DSM サーバが複数ノード存在する場合には全ノードで適用してください。

※パフォーマンスプロファイルは、DSM アプリケーションが正常に動作できるように考慮したチューニング がされていますので、お客様独自でカスタマイズすることは避けてください。必要な場合には弊社までご 相談ください。


Securing Your Journey to the Cloud

3-4-2. DSM 用 SQL サーバのサイジング指標

DSM アプリケーションとの同居について

DSM と SQL データベースを同一サーバで稼動することは可能ですが、仮想デスクトップ環境を保護する場合、または一定以上の規模で展開する場合には、DSM サーバと DSM 用 SQL サーバを別仮想マシンとして 構築してください。

SQL サーバについては必ずしも DSM サーバ専用に用意する必要はありません。

ただし、vCenter Block が複数ある場合に、同一 SQL サーバにインスタンスを複数作成して、2 つ以上の DSM セットを接続することはパフォーマンス面から推奨していません。

▶ リソースの割り当て

データベースのシステム要件に従い、サイジングを行っていただくことが前提となりますが、DSM からのデ ータベースアクセスのボトルネックにならないように設定することが重要です。

- 4~8vCPU
- メモリ 8~16GB
- ディスクについては、イベント発生量やイベント保持期間設定により、必要なディスク容量は大きく
 異なります

以下の FAQ を参考にデータベース容量のサイジングを行ってください。

http://esupport.trendmicro.com/solution/ja-JP/1310096.aspx

※Microsoft SQL を想定

また、DSM のパフォーマンスに問題がないにもかかわらず、多くのジョブが滞留するような場合には、SQL サーバ側で「max worker threads」などの値をチューニングすることで改善できる場合があります。

3-4-3. DSVA のサイジング指標

DSVA に割り振るリソースについては、Deep Security で利用する機能により判断をする必要があります。

- 不正プログラム対策のみ使用する場合のリソースの割り当て
 - ・ 仮想デスクトップ環境ではホストあたりの仮想デスクトップ集約率は 100~120 台程度を推奨します。
 - ・ 不正プログラム対策のフルスキャンを行う場合は、DSVA のリソース、対象ストレージに IOPS、同時実 行数に考慮が必要です。
 - ・ VMware NSX では Guest Introspection Service を展開している場合のホストの最大集約率が定義されています。NSX-T 環境では 250 台が ESXi ホストあたりの最大仮想デスクトップとして定義されていますが、この値は仮想デスクトップの保護完了が即時に行われることを保証する値ではありません。水準の集約率で DSVA の保護を利用した場合、ユーザが仮想デスクトップのログインを完了するまでにセキュリティ保護が完了しない事象が発生する可能性が高まります。NSX の要件も含めて 100-120 台の集約率に抑えて設計することを強く推奨します。

上記情報は VMware Configure Maximum で確認可能です。

https://configmax.vmware.com/

Deep Security において最大要件は明示していませんが、Deep Security のセキュリティ機能を安定して適応するために集約率は 100-120 台/1ESXi に収めるようにしてください。



Public

- ・ 集約率が高くない場合には、2vCPU/4-10GBメモリ)で対応可能なケースが多いと想定されます。環境 に応じてサイジングを決定してください(なるべく 8-10GB の割り振りができることが理想です。)
- ESXi ホストあたりの仮想マシンの集約率が 100 台を超える場合、4vCPU/10~12GB メモリを割り当てることを推奨します。
- 集約率が150台近くなる場合には、上記に加えてさらに2vCPU/4GBメモリの追加を検討してください。
 (あくまで弊社で確認をした実績ベースであり、指標として検討してください。環境によってそれ以上の リソースが必要になる場合があり、NSX 側のパフォーマンスとの兼ね合いも出てくるため、できる限り 集約率はそれよりも余裕がある設計にすることを強く推奨します。)
- 予約検索を実行するは環境によって検索に要する時間が異なります。お客様環境に応じて同時検索 台数を5台以上に設定する場合には、適宜CPU、メモリの割り当てを増やすことが必要になる場合が あります。(不正プログラム対策のフルスキャンを行う場合は、DSVAのリソース、対象ストレージに IOPS、同時実行数に考慮が必要となるため)

3-4-4. DSR のサイジング指標

DSR は通常 DSM と同居してインストールされます。DSVA によるエージェントレス型セキュリティを利用する場合、 DSR はパターンファイルやコンポーネントのダウンロード機能に加えて、DRS/vMotion 時の DSVA 巻の設定以 降に利用されるため、DSM ノードと同居させることで、同数以上の DSR を配置することを推奨します。

- ▶ リソースの割り当て
 - DSMとDSRが同居している場合には、DSR用にCPU/メモリを追加する必要はありません。DSMサーバが直接インターネットに接続できない場合など、DSRを単体で配置する場合、DSAのシステム要件に従ってサイジングを行ってください。
 - DSR はエンジン、ルール、パターンファイルなどのコンポーネントに加え、DSA などのアップグレード用 プログラムを配信するためにローカルディスクを使用します。配信用データを格納するために 10GB 程 度のディスク容量を確保してください。



4. 参考資料

本ガイドのほかに、必要に応じて以下の情報を参照してください。

- > 全般情報
 - Trend Micro Deep Security サポートウェブ
 <u>http://esupport.trendmicro.com/ja-jp/enterprise/ds/top.aspx</u>
 - NSX と Trend Micro Deep Security DSVA 9.5/9.6/10.0 トラブルシューティングガイド <u>https://campaign.vmware.com/imgs/apac/jp_dwn/PDF/techresources/DSVA_9.5-</u> <u>10TroubleshootingTips_NSX_r2.1.pdf</u>
 - Deep Security+VMware NSX 関連情報(ブログ、アーキテクチャなど)
 <u>https://www.trendmicro.com/ja_jp/business/campaigns/vmware.html</u>
- > バージョンアップ
 - Deep Security12.0 アップグレードガイドブック(DSVA 編)
 <u>http://files.trendmicro.com/jp/ucmodule/tmds/doc/ds12_upgradeguide_dsa.pdf</u>