

vShield Endpoint (vCNS) から NSX for vShield Endpoint へのアップグレード手順

2016年12月02日
VMware株式会社

vmware®

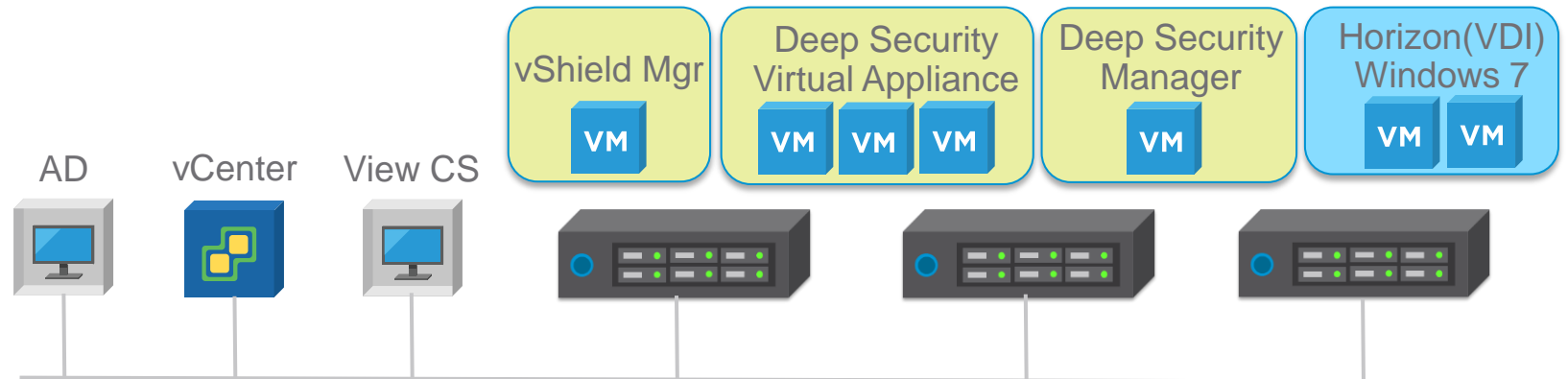
© 2016 VMware Inc. All rights reserved.

本検証の背景

- vCNS (vCloud Networking and Security) の販売終了に伴い、vCNS のジェネラルサポートは 2016年9月 をもって終了、テクニカルガイダンスも 2017年3月 をもって終了致します。
- 詳細につきましては、以下KBをご覧ください。
 - 英語版 : <https://kb.vmware.com/kb/2110078>
 - 日本語版 : <https://kb.vmware.com/kb/2146576>
- vCNS の後継として、NSX for vShield Endpoint が提供されています。
- 本資料ですが、Deep Security と連携して使われている既存の vCNS を NSX for vShield Endpoint にアップグレードする手順についてご案内を致します。

検証構成

- vCenter Server 6.0 Update2
- ESXi 6.0 Update 2 (VSSを使用)
- Horizon View 7.0.2
- ***vShield Manager 5.5.4.3 -> NSX for vShield Endpoint 6.2.4***
- Deep Security Manager 9.6 SP1



主な手順

1. DSVA(Dep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Dep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Dep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

主な手順

1. DSVA(Dep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Dep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Dep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

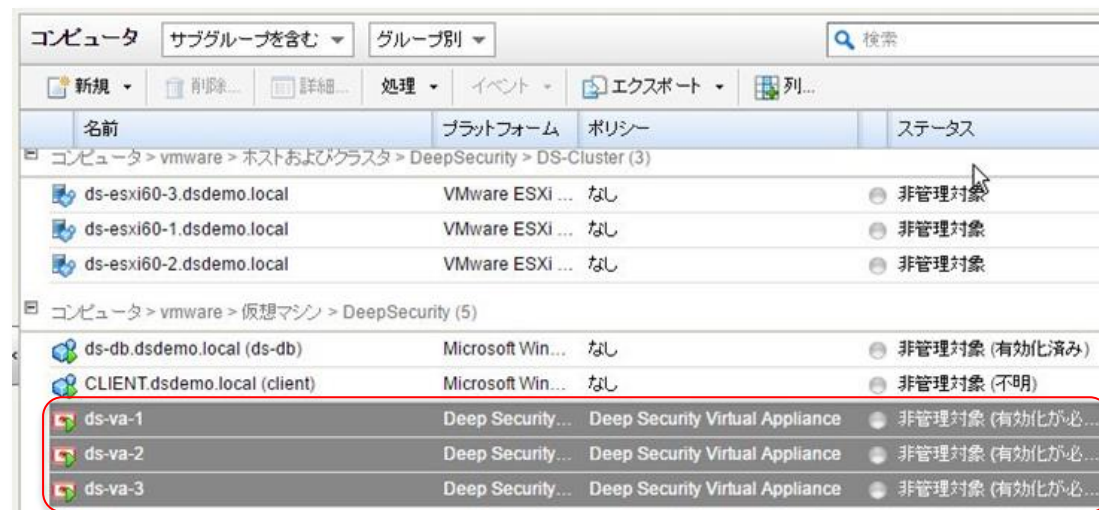
DSVA(Dep Security Virtual Appliance)の無効化(1)

- Deep Security Managerにログイン
- 全てのDSVAを選択し 処理 - Applianceの無効化を選択する



DSVA(Deep Security Virtual Appliance)の無効化(2)

- 確認画面が表示されるので、OKを押下
- 全てのDSVAが**非管理対象（有効化が必要）**というステータスになったことを確認



主な手順

1. DSVA(Deep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Deep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Deep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

vShield Manager の停止

- Web ClientからvShield Managerを選択しシャットダウン

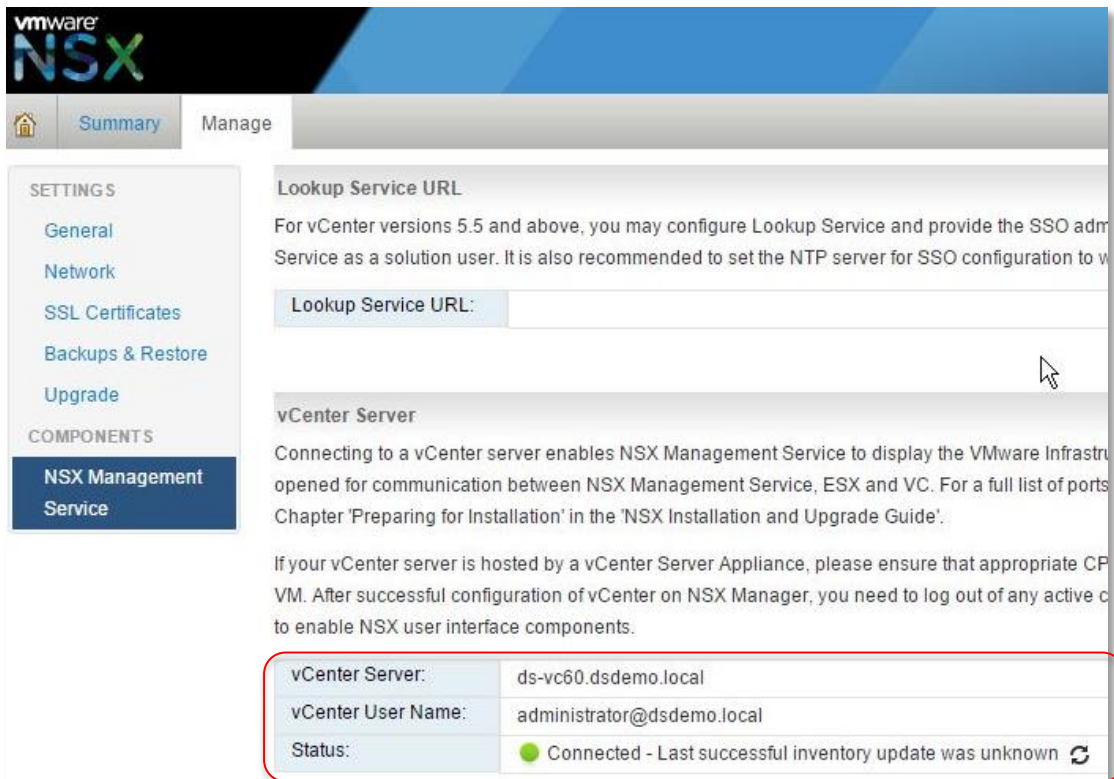


主な手順

1. DSVA(Deep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Deep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Deep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

NSX Manager のデプロイ

- NSX Managerをデプロイし、vCenterとの接続設定を実施
- デプロイ手順詳細については割愛



主な手順

1. DSVA(Deep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Deep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Deep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

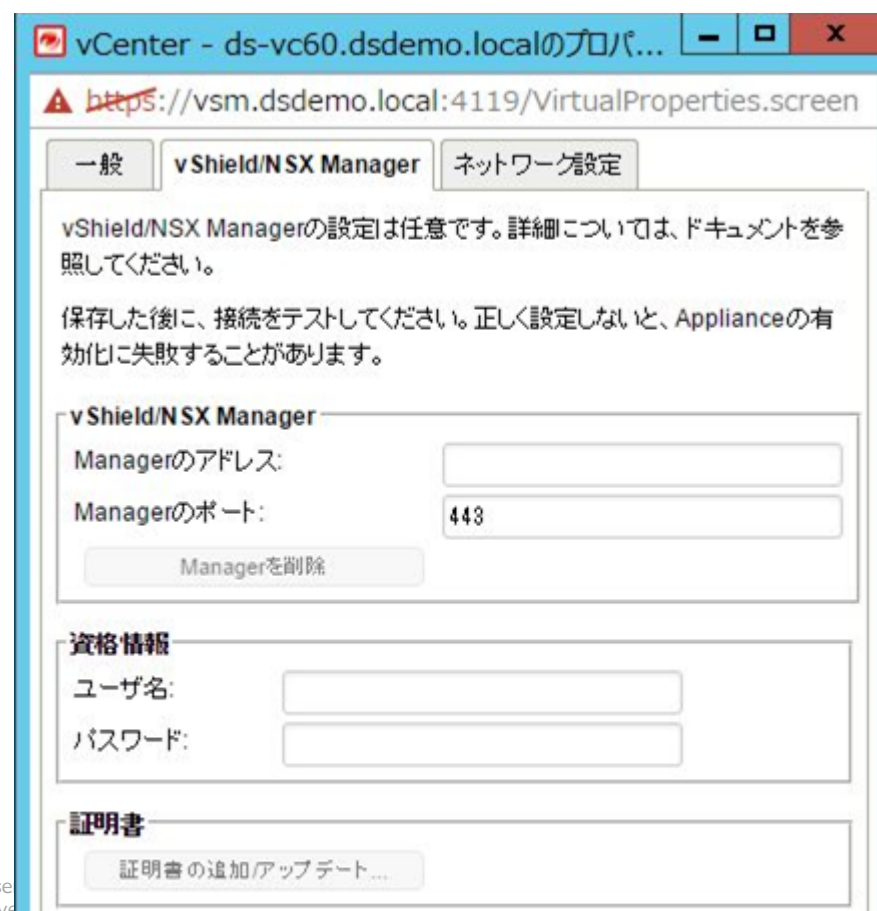
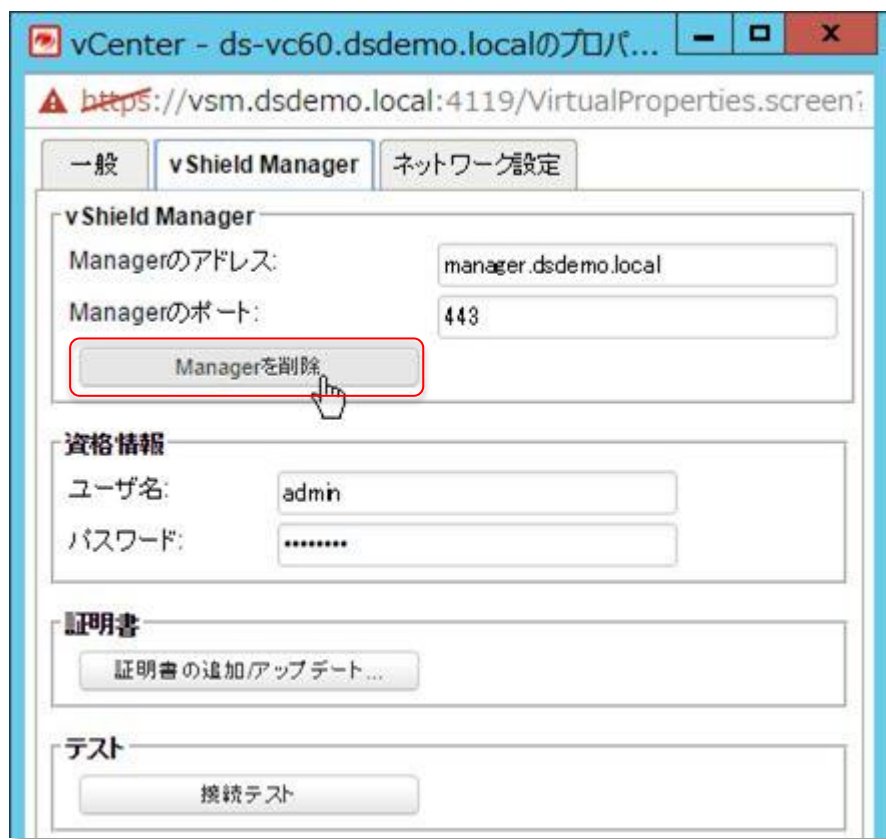
Deep Security Manager と vShield Manager の連携解除(1)

- Deep Security Managerにログイン
- コンピュータタブから、左ウインドウのvCenterを右クリックしてプロパティを選択



Deep Security Manager と vShield Manager の連携解除(2)

- vShield Manager タブから、Managerを削除を押下
- 下図のように、vShield Managerとの連携が解除されたことを確認



主な手順

1. DSVA(Deep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Deep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Deep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

DSVA(Deep Security Virtual Appliance)の停止

- Web Clientから、ESXiホストの数だけ存在するDSVAをシャットダウン
- 以下は、3 台のESXiで構成された例
- 3 台のDSVAがシャットダウンされたことを確認



主な手順

1. DSVA(Dep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Dep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Dep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

Deep Security Manager と NSX の連携設定(1)

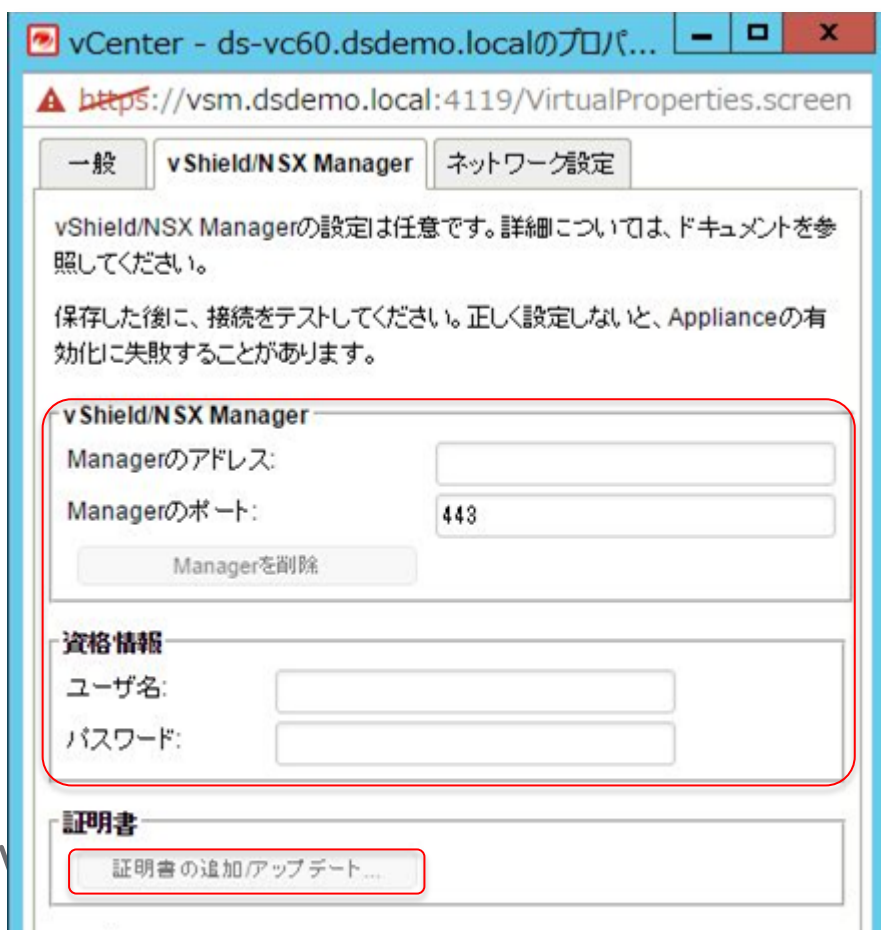
- Deep Security Managerにログイン
- コンピュータタブから、左ウインドウのvCenterを右クリックしてプロパティを選択



Deep Security Manager と NSX の連携設定(2)

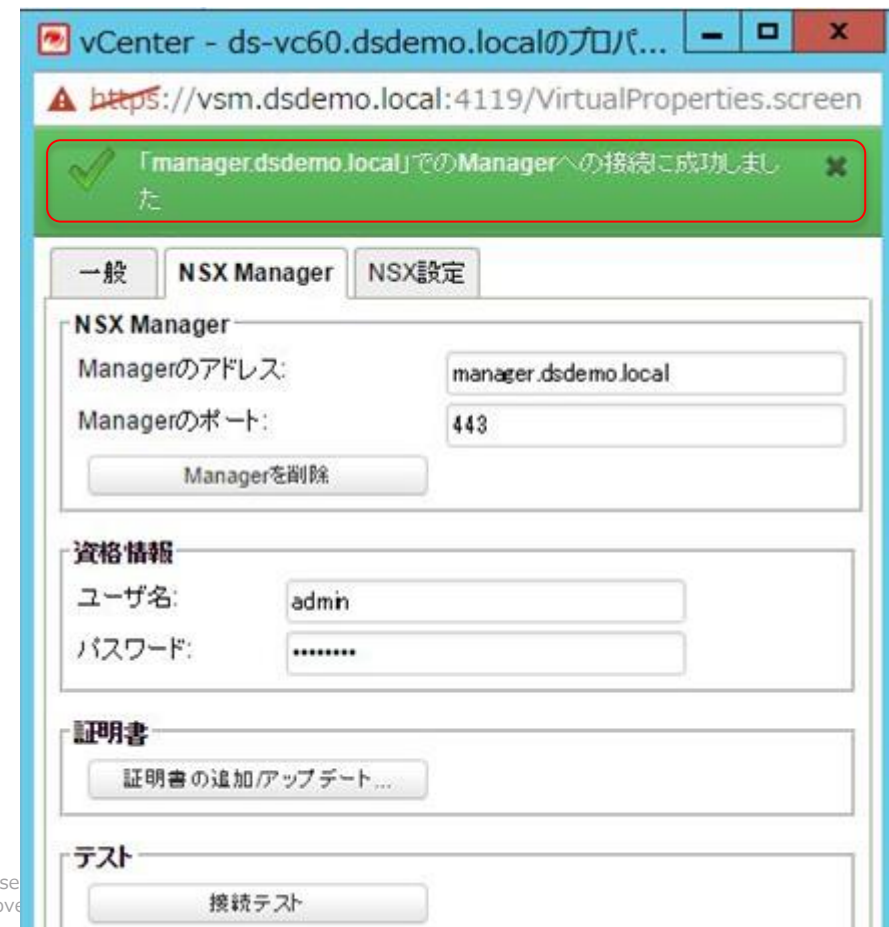
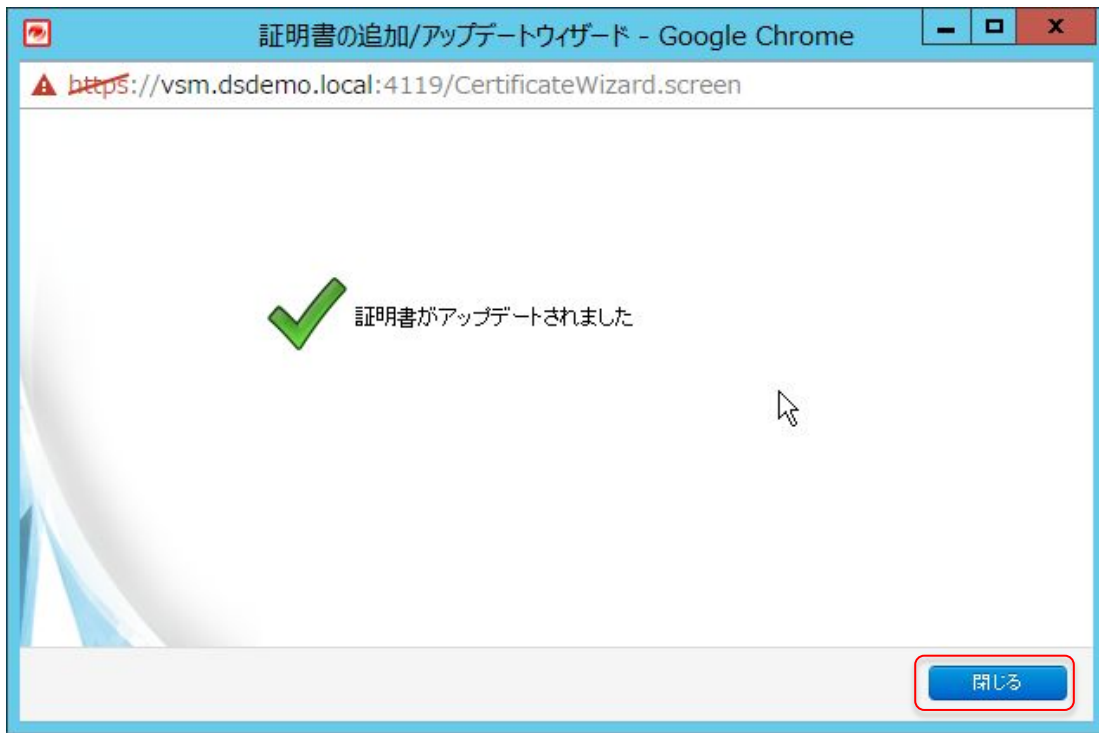
- vShield/NSX Manager タブから、NSX Managerのアドレス、ポート、ユーザ名、パスワードを入力し、証明書の追加/アップデートを押下

- 受け入れるを押下



Deep Security Manager と NSX の連携設定(3)

- 証明書がアップデートされたことを確認し、閉じるを押下
- NSX Managerへの接続が成功したことを確認

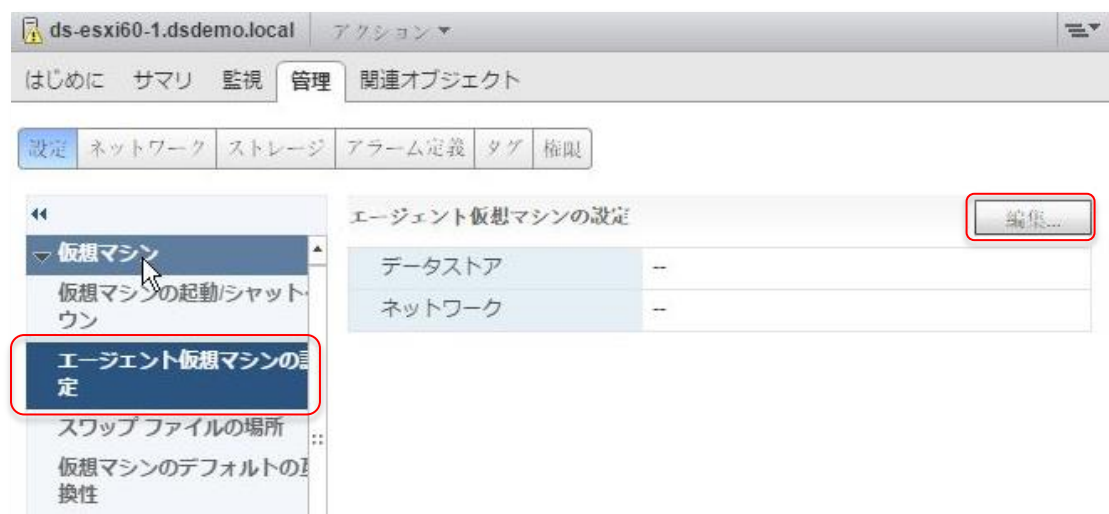


主な手順

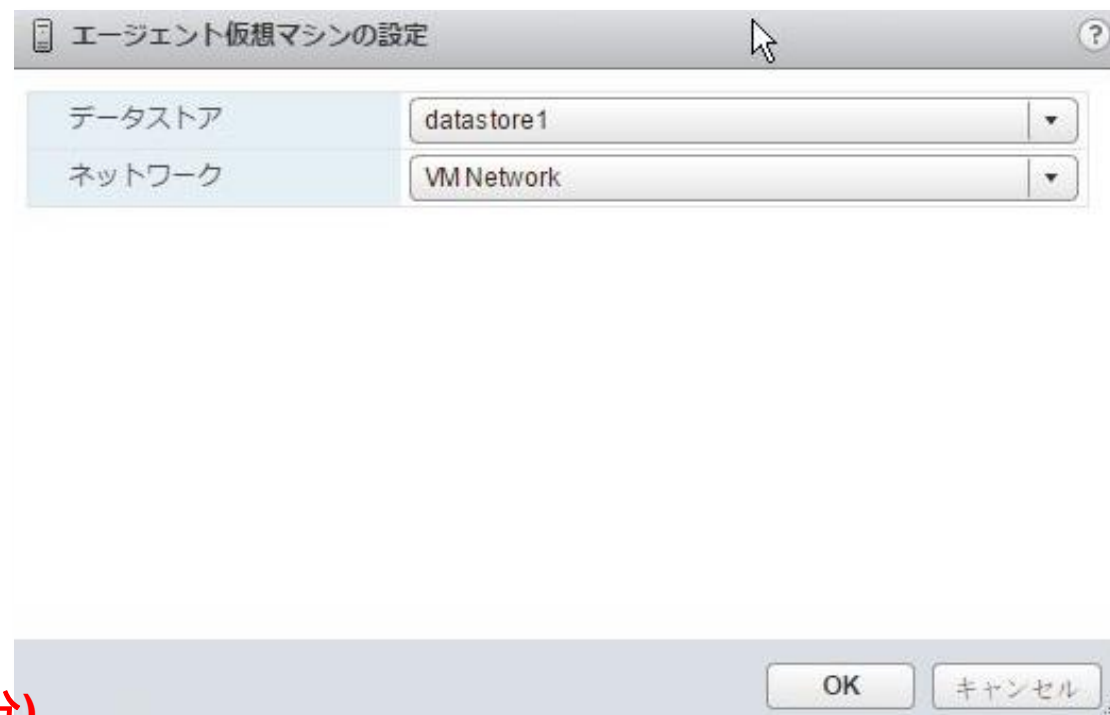
1. DSVA(Deep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Deep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Deep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

Guest Introspection のデプロイ(1)

- Web Clientから**各ESXiを選択**し、「**管理**」
- 「**設定**」から**エージェント仮想マシンの設定**を選択して**編集**を押下



- Guest Introspection VMが展開されるデータストア、接続されるネットワークを選択(注1)
- Guest Introspection VMがvMotion又はストレージvMotionされないように、データストアは、ESXiのローカルディスクを選択(注2)



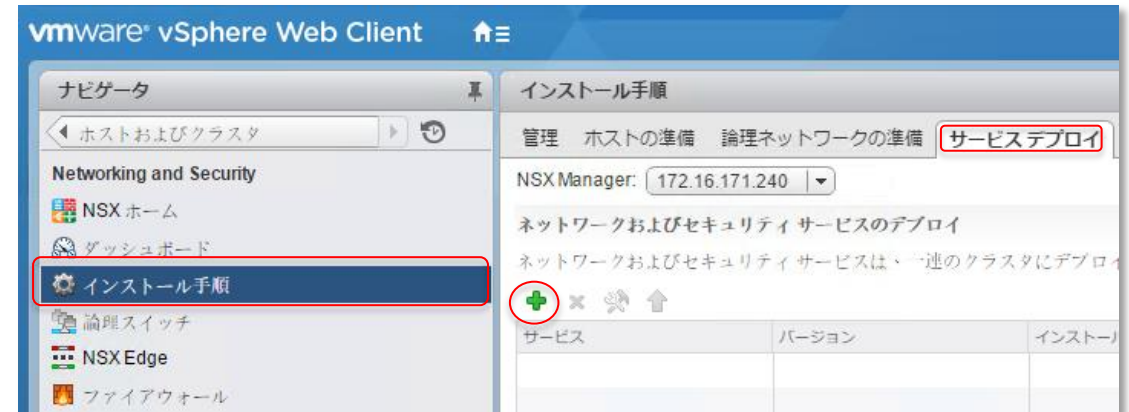
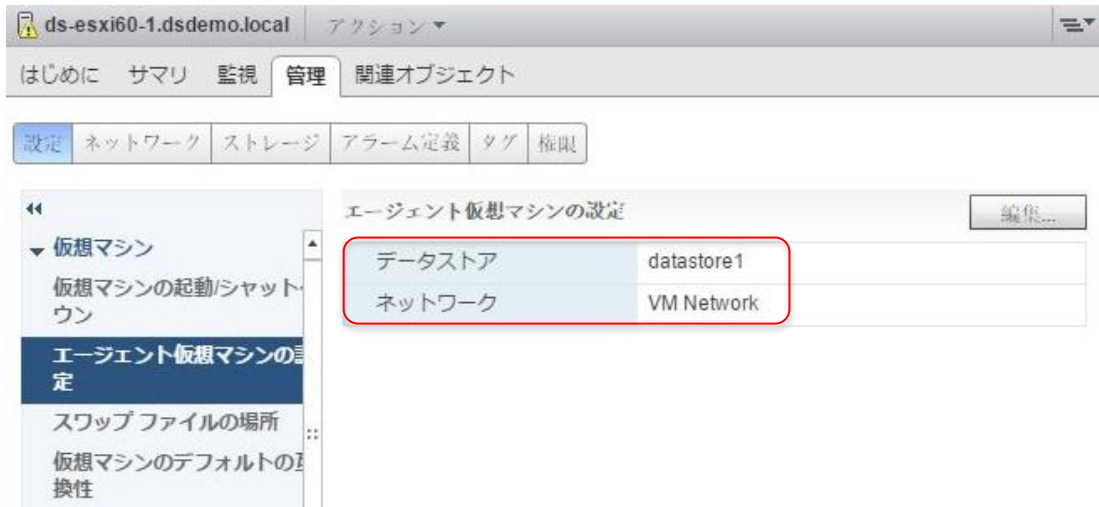
(注1) VSS使用時はこの設定が必須(ネットワーク部分)

(注2) Trendmicro社のKBを参照: <http://esupport.trendmicro.com/solution/ja-JP/1115886.aspx>

-> Guest Introspection VM が vMotion 又は Storage vMotion されないために必要な設定

Guest Introspection のデプロイ(2)

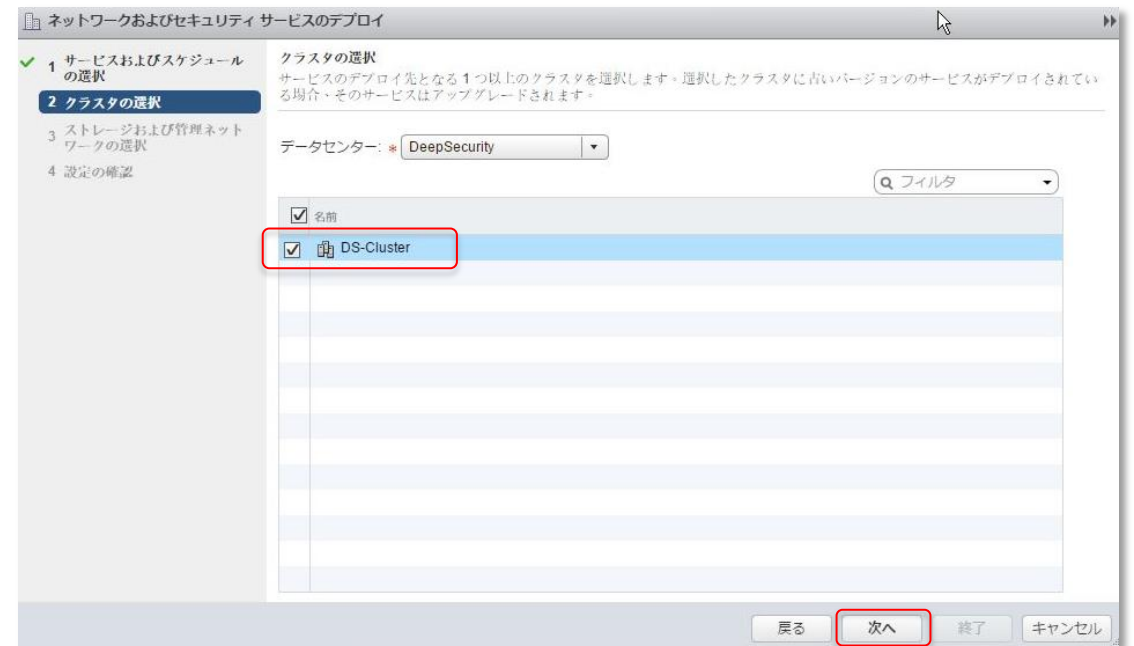
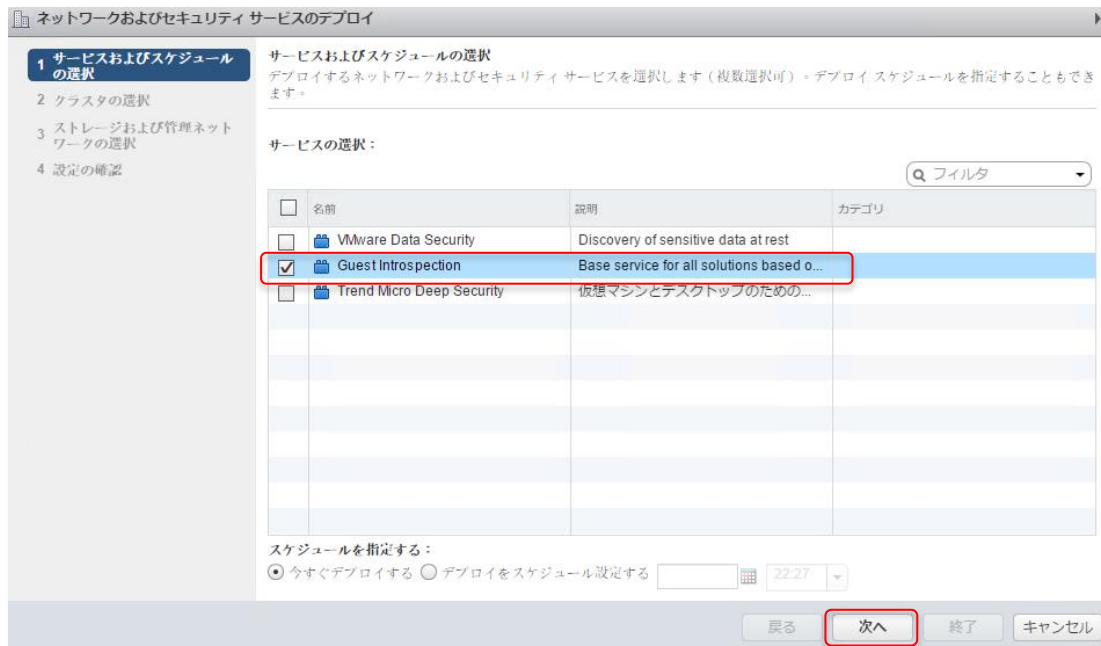
- 設定が反映されたことを確認
- NSX管理画面からインストール手順を選択
- サービスデプロイタブから+を押下



Guest Introspection のデプロイ(3)

- Guest Introspectionを選択し、次へを押下

- Guest Introspection VMを展開するクラス
タを選択し、次へを押下



Guest Introspection のデプロイ(4)

- データストア、ネットワーク共に、**ホスト上**が指定済みを選択されていることを確認し、**次へ**を押下

ネットワークおよびセキュリティ サービスのデプロイ

✓ 1 サービスおよびスケジュールの選択
✓ 2 クラスタの選択
3 **ストレージおよび管理ネットワークの選択**
4 設定の確認

ストレージおよび管理ネットワークの選択
使用するサービスごとにネットワークおよび IP アドレス範囲を割り当てます。

サービス	クラスタ	データストア	ネットワーク	IP 割り当て
Guest Introspection	DS-Cluster	ホスト上が...	ホスト上が指定...	DHCP 変更

戻る 次へ 終了 キャンセル

- 全ての設定が正しく選択されていることを確認し、**終了**を押下
- Guest Introspection VMのデプロイ開始

ネットワークおよびセキュリティ サービスのデプロイ

✓ 1 サービスおよびスケジュールの選択
✓ 2 クラスタの選択
✓ 3 ストレージおよび管理ネットワークの選択
4 **設定の確認**

設定の確認
ウィザードを終了する前に設定を確認してください。

スケジュール時刻: 現在

サービス	クラスタ	データストア	ネットワーク	IP 割り当て
Guest Introspection	DS-Cluster	ホスト上が指定済み	ホスト上が指定済み	DHCP

戻る 次へ 終了 キャンセル

Guest Introspection のデプロイ(5)

- 必要に応じて、Web Clientの**タスク**から Guest Introspection VMのデプロイが行われていることを確認
- サービスデプロイ**タブから、インストールが成功し、サービスステータスが**接続中**であることを確認

タスク コンソール

タスク名	ターゲット	ステータス
OVF テンプレートのデプロイ	Guest Introspection...	87 %
フォルダの作成	DeepSecurity	✓ 完了
リソース プールの作成	DS-Cluster	✓ 完了
インストール	ds-esxi60-2.dsdem...	✓ 完了
インストール	ds-esxi60-3.dsdem...	✓ 完了
インストール	ds-esxi60-1.dsdem...	✓ 完了
スキャン	ds-esxi60-3.dsdem...	✓ 完了
スキャン	ds-esxi60-2.dsdem...	✓ 完了
スキャン	ds-esxi60-1.dsdem...	✓ 完了
エージェントの有効化	ds-esxi60-2.dsdem...	20 %
エージェントの有効化	ds-esxi60-1.dsdem...	20 %
エージェントの有効化	ds-esxi60-3.dsdem...	20 %

ナビゲータ

インストール手順

管理 ホストの準備 論理ネットワークの準備 **サービスデプロイ**

NSX Manager: 172.16.171.240

ネットワークおよびセキュリティ サービスのデプロイ

ネットワークおよびセキュリティ サービスは、一連のクラスタにデプロイされています。新しいサービスを追加したり、既存のサービスを削除したりして、ここでサービスのデプロイを管理します。

サービス	バージョン	インストールの	サービスステ	クラスタ	データストア	ポートグループ	IP アドレス範囲
Guest Intr...	6.2.3	✓ 成功し...	✓ 接続中	DS-Cl...	ホス...	ホス...	DHCP

- クラスタを構成する各ESXi上でGuest Introspection VMの稼働を確認

ESX Agents

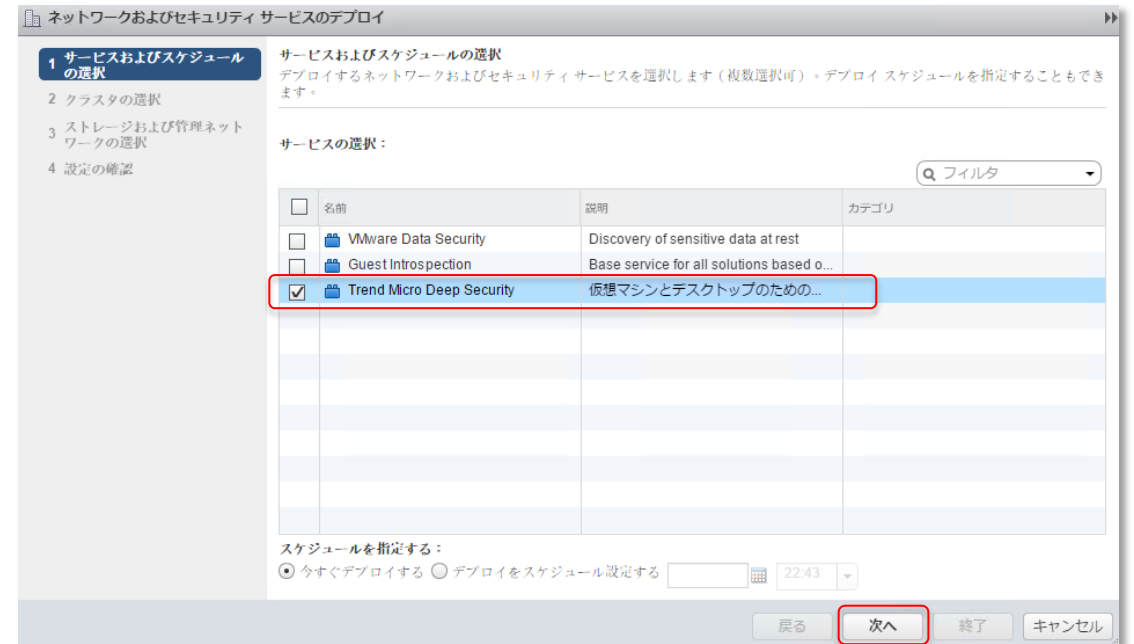
- Guest Introspection (1)
- Guest Introspection (2)
- Guest Introspection (3)

主な手順

1. DSVA(Deep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Deep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Deep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

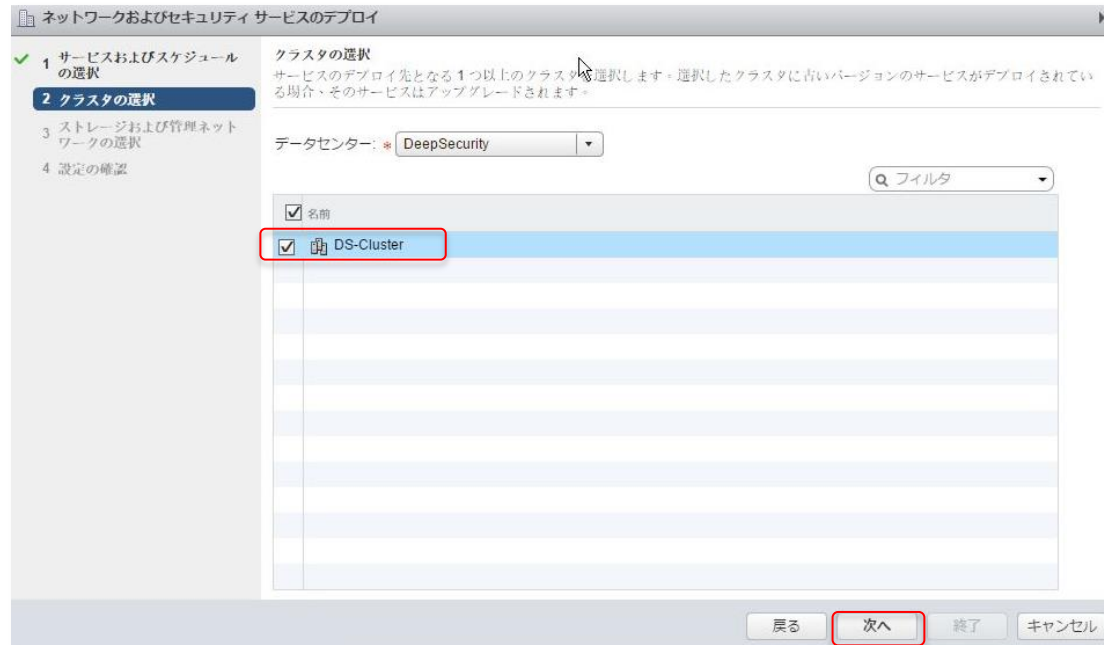
DSVA(Deep Security Virtual Appliance)のデプロイ(1)

- NSX管理画面からインストール手順を選択
- サービスデプロイタブから+を押下
- Trend Micro Deep Security を選択し、次へを押下

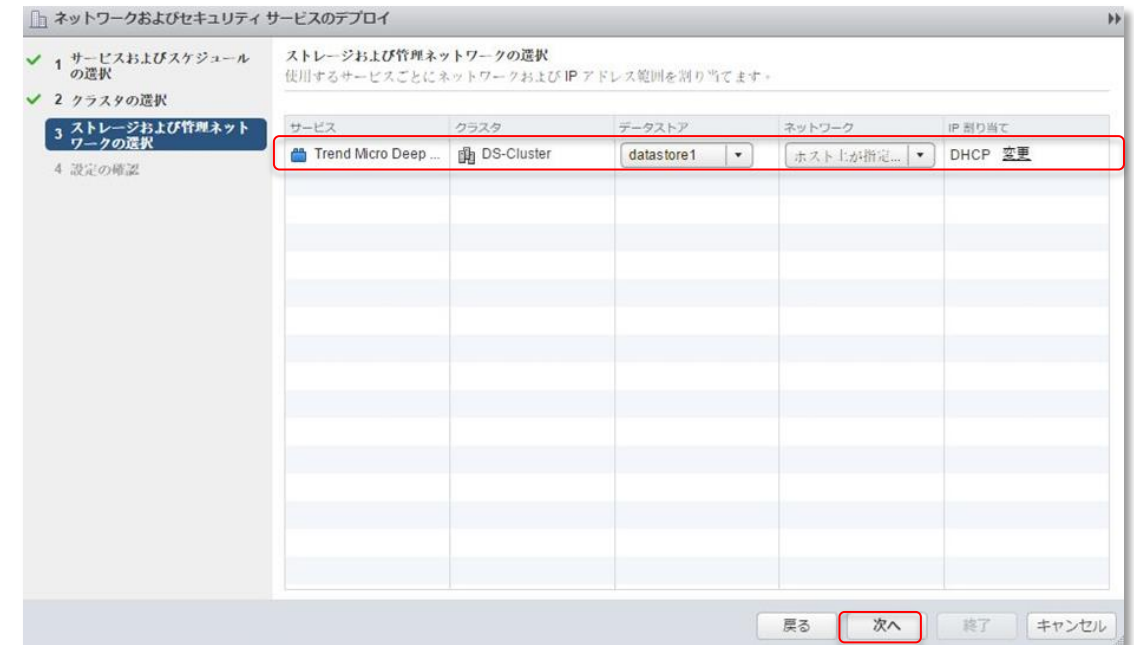


DSVA(Deep Security Virtual Appliance)のデプロイ(2)

- DSVA を展開するクラスタを選択し、次へを押下

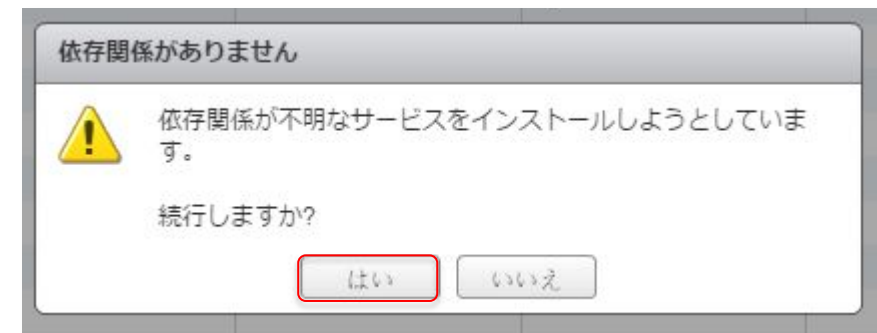
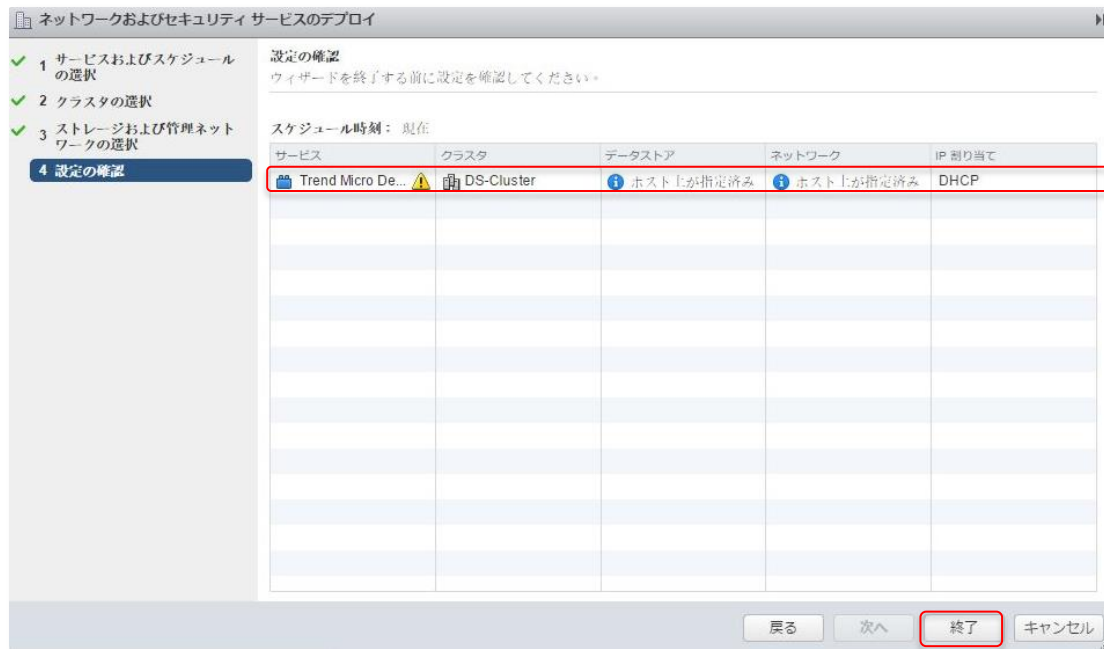


- データストア、ネットワーク共に、ホスト上が指定済みを選択されていることを確認し、次へを押下



DSVA(Deep Security Virtual Appliance)のデプロイ(3)

- 全ての設定が正しく選択されていることを確認し、**終了**を押下
- 以下確認画面が表示されるので、**はい**を押下



DSVA(Deep Security Virtual Appliance)のデプロイ(4)

- インストールの状態が失敗として表示されるが、**既知の表示の問題（注）**のため無視
- 必要に応じて、Web ClientのタスクからDSVA のデプロイが行われていることを確認

インストール手順

管理 ホストの準備 論理ネットワークの準備 **サービスデプロイ**

NSX Manager: 172.16.171.240

ネットワークおよびセキュリティ サービスのデプロイ

ネットワークおよびセキュリティ サービスは、一連のクラスタにデプロイされています。新しいサービスを追加したり、既存のサービスを削除したりして、ここでサービスのデプロイを管理します。

+ × 🔄 ⬆

フィルタ

サービス	バージョン	インストールの	サービス ステータス	クラスタ	データストア	ポートグループ	IP アドレス範囲
Guest ...	6.2.3	✓ 成功し...	✓ 接続中	DS-Cl...	ホスト...	ホスト...	DHCP
Trend ...	9.6	❗ 失敗	不明	DS-Cl...	ホスト...	ホスト...	DHCP

サービス Trend Micro Deep Security が機能するためには、以下のサービスが正しくインストールされている必要があります: VMware Network Fabric

タスク コンソール

フィルタ

タスク名	ターゲット	ステータス	開始者
OVF テンプレートのデプロイ	Trend Micro Deep ...	26 %	com.vmw...
エージェントの有効化	ds-esxi60-2.dsdem...	0 %	com.vmw...
エージェントの有効化	ds-esxi60-1.dsdem...	0 %	com.vmw...
エージェントの有効化	ds-esxi60-3.dsdem...	0 %	com.vmw...
オプション値の更新	ds-esxi60-2.dsdem...	✓ 完了	DSDEMO
オプション値の更新	ds-esxi60-1.dsdem...	✓ 完了	DSDEMO
オプション値の更新	ds-esxi60-3.dsdem...	✓ 完了	DSDEMO
オプション値の更新	ds-esxi60-3.dsdem...	✓ 完了	DSDEMO
オプション値の更新	ds-esxi60-2.dsdem...	✓ 完了	DSDEMO

104 項目 ◀ 前へ 次へ ▶

(注) <失敗(VMware Network Fabric)>が出るのは、既知の問題。詳細については下記KBを参照。

<http://esupport.trendmicro.com/solution/ja-JP/1115601.aspx>

DSVA(Deep Security Virtual Appliance)のデプロイ(5)

- サービスステータスが接続中になったことを確認
- クラスタを構成する各ESXi上でDVSA (Trend Micro Deep Security) の稼働を確認

インストール手順

管理 ホストの準備 論理ネットワークの準備 **サービスデプロイ**

NSX Manager: 172.16.171.240

ネットワークおよびセキュリティ サービスのデプロイ

ネットワークおよびセキュリティ サービスは、一連のクラスタにデプロイされています

サービス	バージョン	インストールの状態	サービス ステータス
Trend Micro Deep Security	9.6	❗ 失敗	✅ 接続中
Guest Introspection	6.2.3	✅ 成功しました	✅ 接続中

ESX Agents

- Guest Introspection (1)
- Guest Introspection (2)
- Guest Introspection (3)
- Trend Micro Deep Security (1)
- Trend Micro Deep Security (2)
- Trend Micro Deep Security (3)

DSVA(Dep Security Virtual Appliance)のデプロイ(6)

- Deep Security Managerにログイン
- コンピュータタブから、DSVAが管理対象(オンライン)になっていることを確認

セッションがタイムアウトしました。ログオン直してください。

ログオン

ユーザ名: masteradmin

パスワード:

☐ 多要素認証を使用する

ログオン

TREND MICRO Deep Security

ダッシュボード 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

vCenter - ds-vc60.dsdemo.local サブグループを含む グループ別

新規 削除... 詳細... 処理 イベント エクスポート 列...

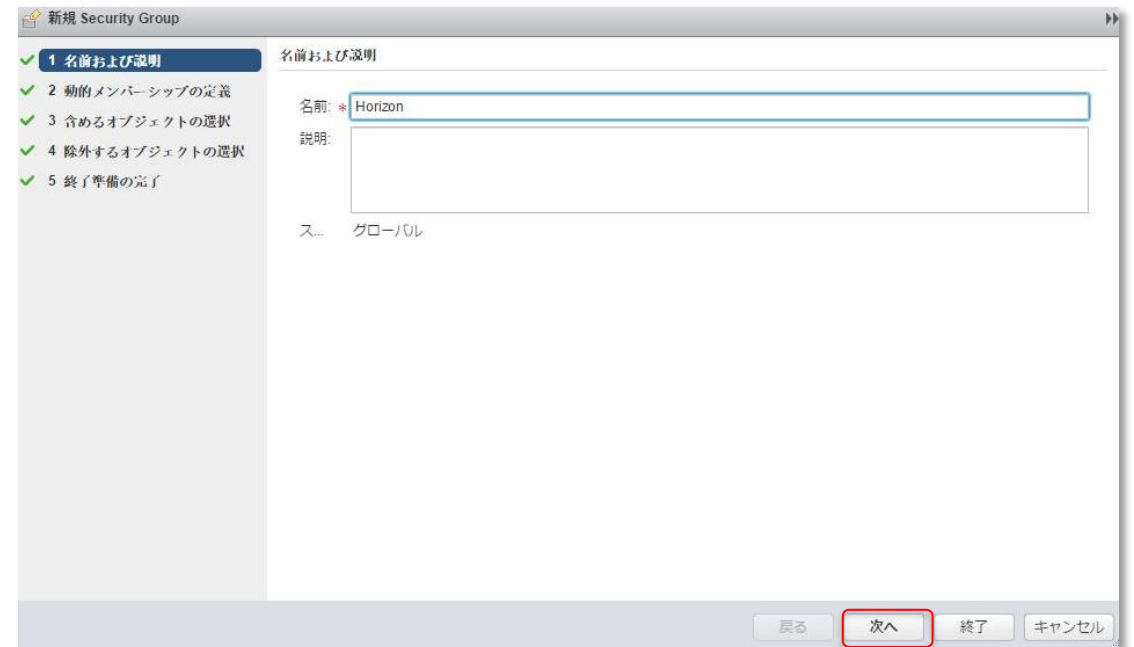
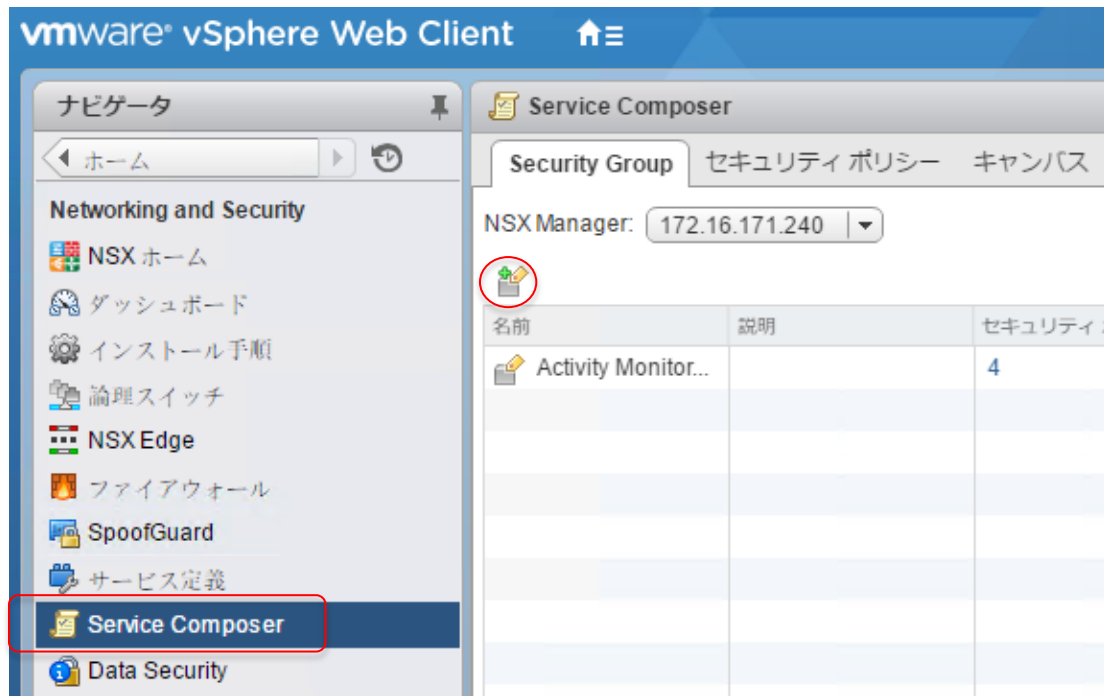
名前	ポリシー	プラットフォーム	ステータス
ds-esxi60-2.dsdemo.local	なし	VMware ESXi ...	● 非管理対象
ds-esxi60-1.dsdemo.local	なし	VMware ESXi ...	● 非管理対象
コンピュータ > vCenter - ds-vc60.dsdemo.local > 仮想マシン > DeepSecurity (5)			
win7-template.dsdemo.loc...	Windows Anti-Malware Prote...	Microsoft Win...	● 非管理対象 (不明)
vsm.dsdemo.local (vsm)	なし	Microsoft Win...	● 非管理対象 (有効化済み)
ds-va-3	Deep Security Virtual Appla...	Deep Security...	● 非管理対象 (VM停止)
ds-va-2	Deep Security Virtual Appla...	Deep Security...	● 非管理対象 (VM停止)
ds-va-1	Deep Security Virtual Appla...	Deep Security...	● 非管理対象 (VM停止)
コンピュータ > vCenter - ds-vc60.dsdemo.local > 仮想マシン > DeepSecurity > Discovered virtual machine (2)			
manager (NSX Manager)	なし	Other Linux (6...	● 非管理対象 (不明)
(vShield Manager)	なし	Other Linux (6...	● 非管理対象 (VM停止)
コンピュータ > vCenter - ds-vc60.dsdemo.local > 仮想マシン > DeepSecurity > Discovered virtual machine > test (2)			
TEST2.dsdemo.local (test2)	Windows Anti-Malware Prote...	Microsoft Win...	● 非管理対象 (Agentなし)
TEST1.dsdemo.local (test1)	Windows Anti-Malware Prot...	Microsoft Win...	● 非管理対象 (Agentなし)
コンピュータ > vCenter - ds-vc60.dsdemo.local > 仮想マシン > DeepSecurity > ESX Agents (6)			
localhost.localdom (Trend ...	Deep Security Virtual Appla...	Deep Security...	● 管理対象 (オンライン)
localhost.localdom (Trend ...	Deep Security Virtual Appla...	Deep Security...	● 管理対象 (オンライン)
localhost.localdom (Trend ...	Deep Security Virtual Appla...	Deep Security...	● 管理対象 (オンライン)
localhost.localdom (Guest...	Windows Anti-Malware Prote...	SUSE Linux E...	● 管理対象 (オンライン)
localhost.localdom (Guest...	Windows Anti-Malware Prote...	SUSE Linux E...	● 管理対象 (オンライン)
localhost.localdom (Guest...	Windows Anti-Malware Prote...	SUSE Linux E...	● 管理対象 (オンライン)

主な手順

1. DSVA(Dep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Dep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Dep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

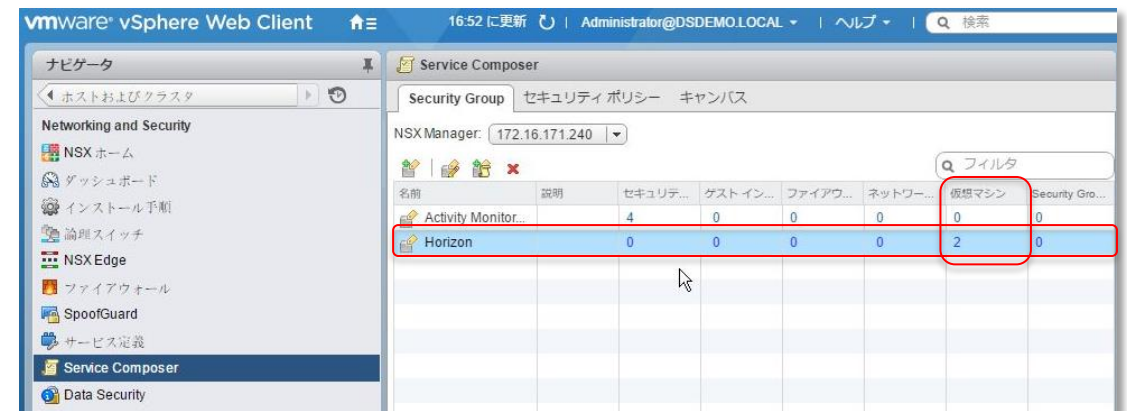
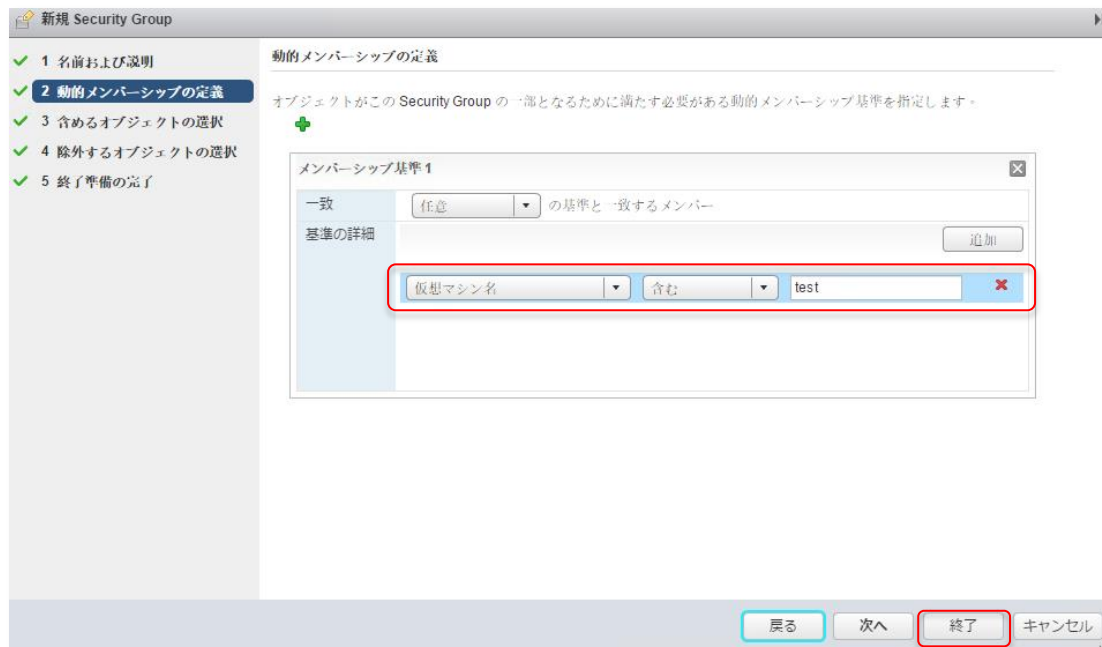
Security Policy、Security Groupの作成等(1)

- Service ComposerのSecurity Groupタブから、新規セキュリティグループを作成
- 新規セキュリティグループの名前を入力し、次へを押下



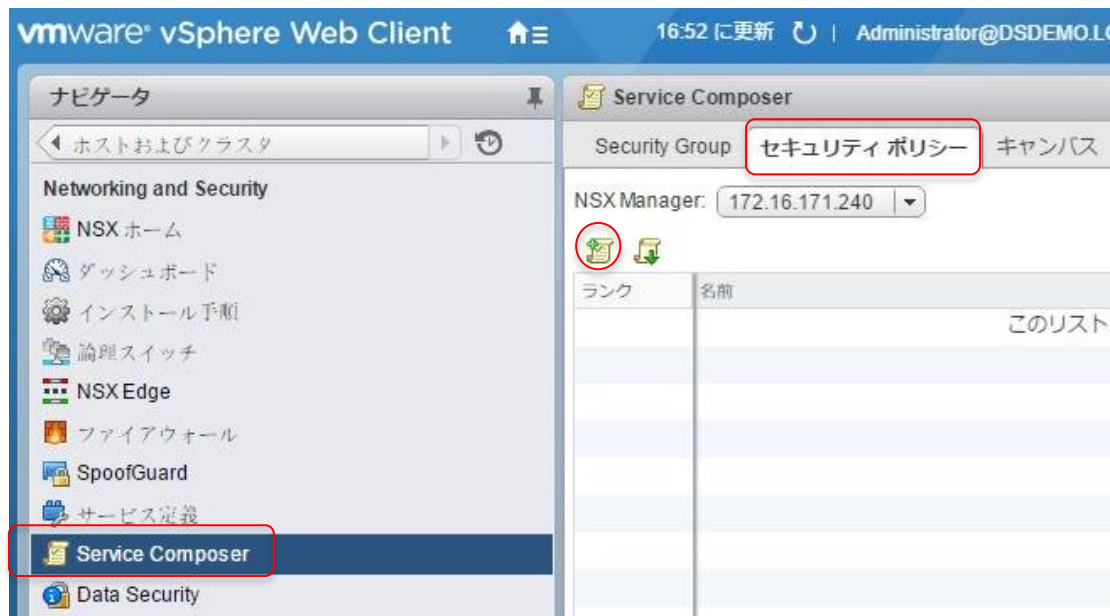
Security Policy、Security Groupの作成等(2)

- 作成したセキュリティグループのネーミングルール（文字列：testを含む仮想マシン名）を動的メンバーシップの定義として設定し、**終了**を押下
- 作成したセキュリティグループに Test01/Test02 の2 台の仮想マシンが含まれていることを確認

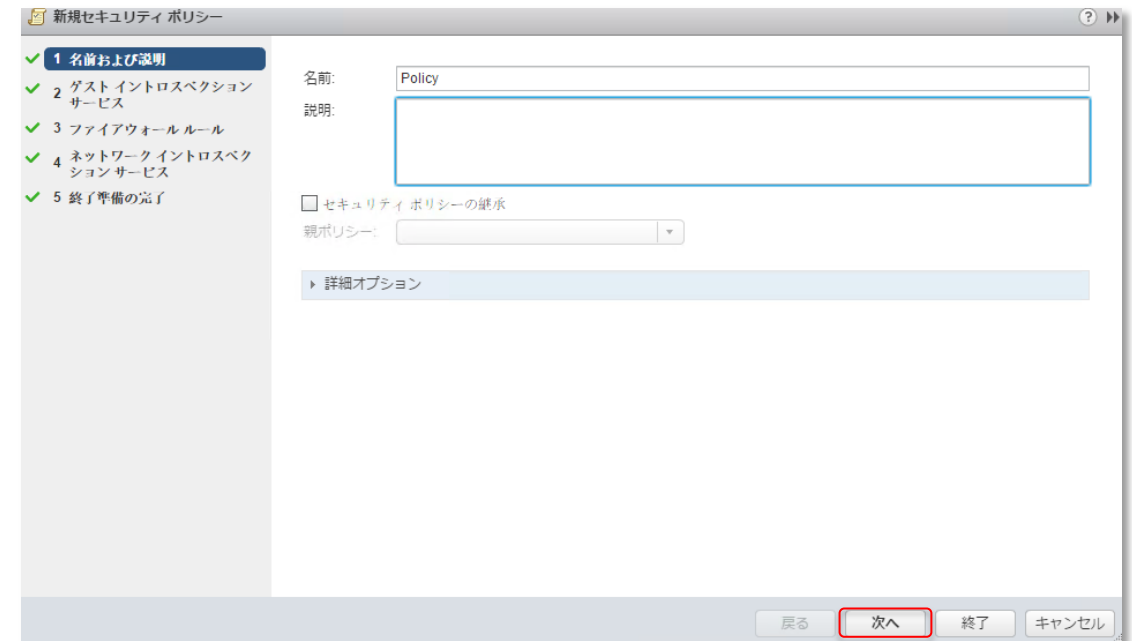


Security Policy、Security Groupの作成等(3)

- Service Composerのセキュリティポリシータブから、新規セキュリティポリシーを作成

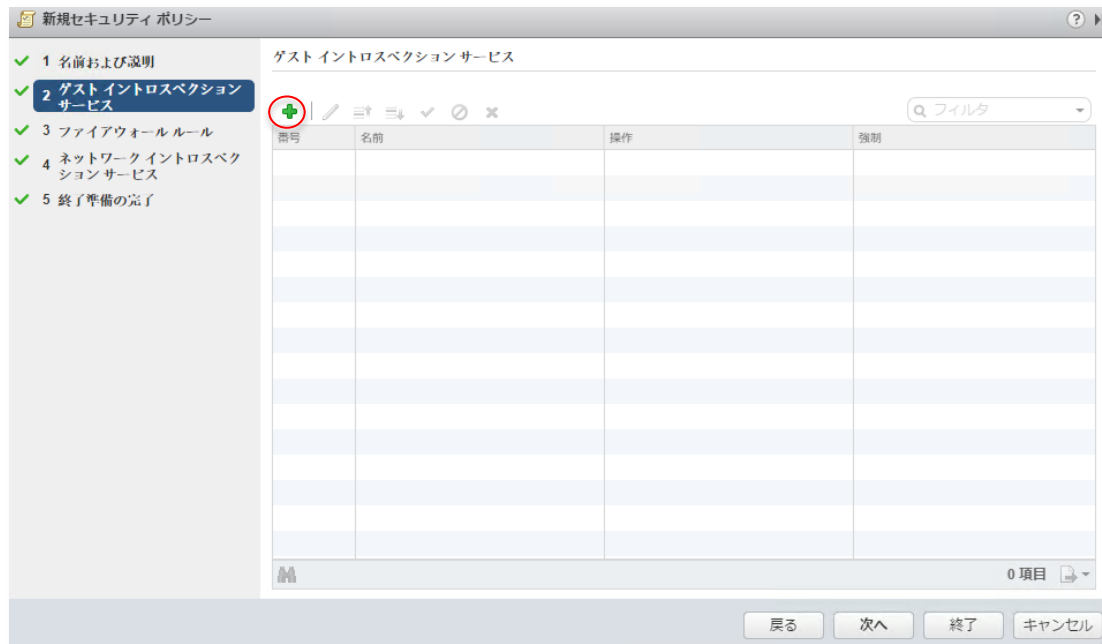


- 新規セキュリティポリシーの名前を入力し、次へを押下



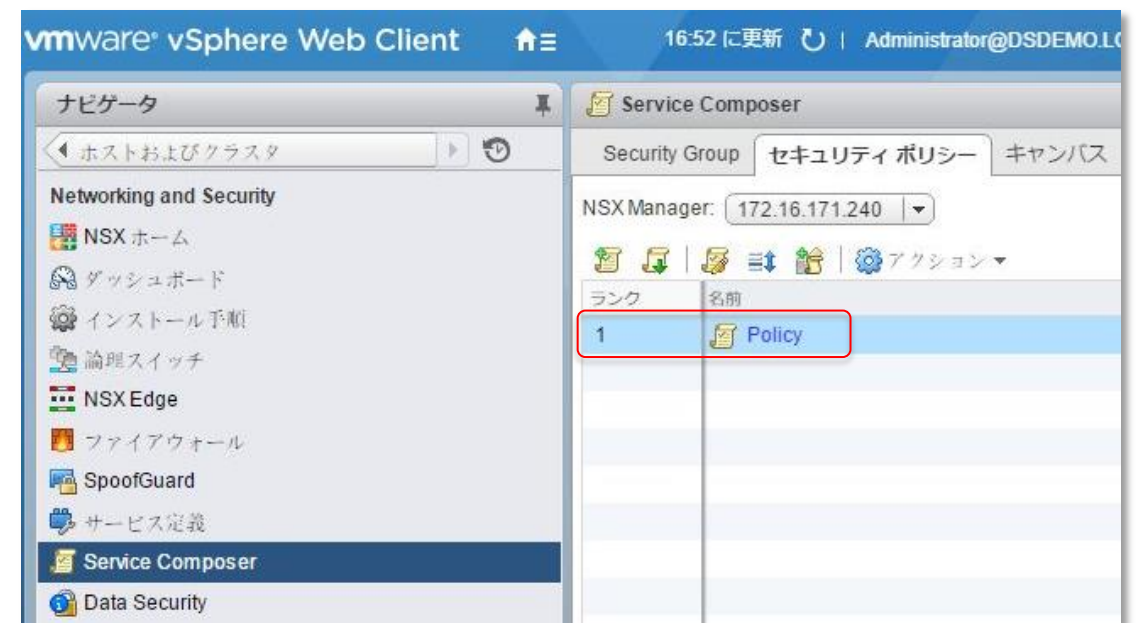
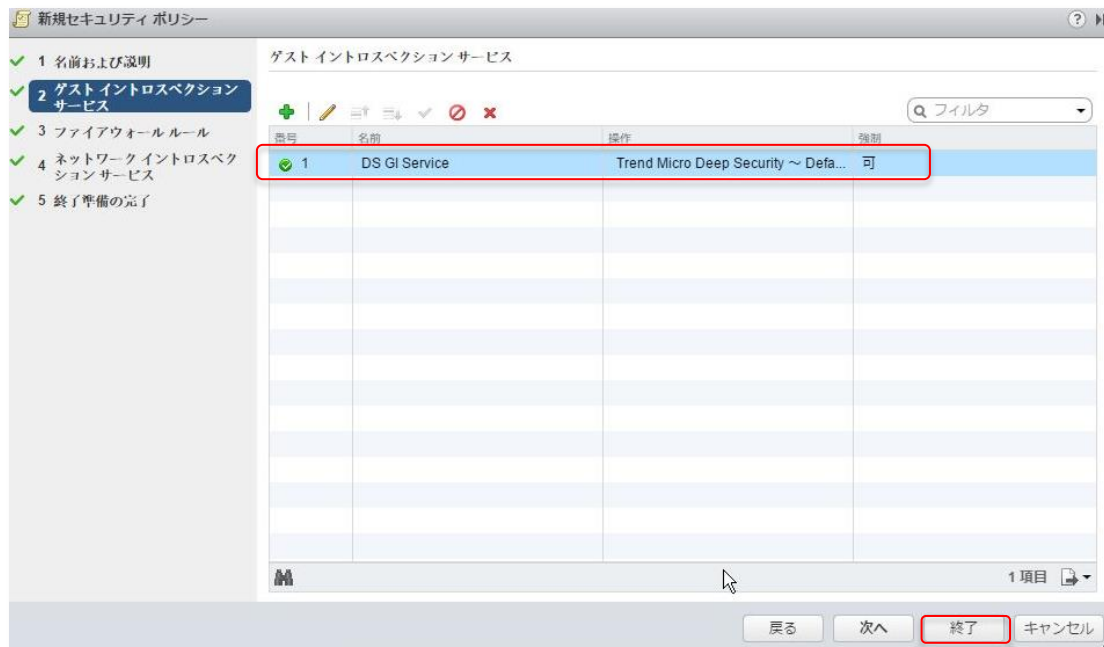
Security Policy、Security Groupの作成等(4)

- ゲストイントロスペクションサービスを追加
- 名前をDS GI Service、サービス名としてTrend Micro Deep Security、を選択して下記の画面のように設定し、OKを押下



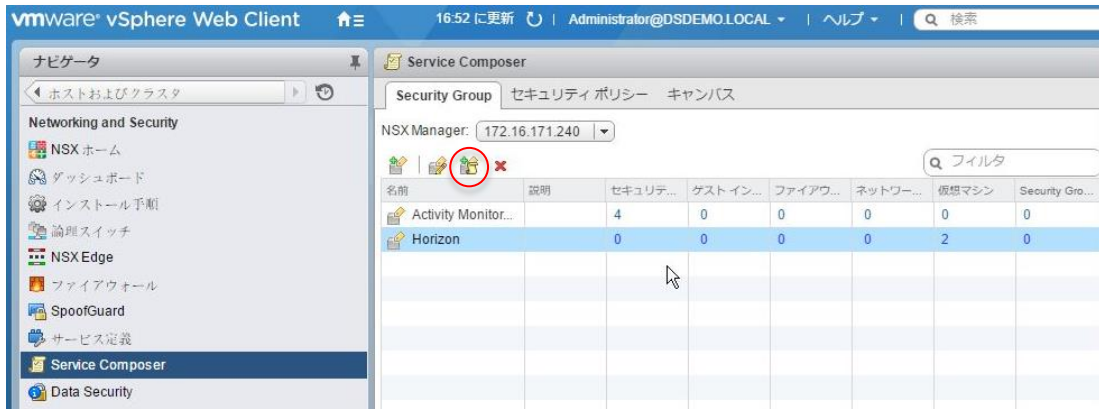
Security Policy、Security Groupの作成等(5)

- ゲストイントロスペクションサービスとして、**DS GI Service**が追加されたことを確認し**終了**を押下
- 新規セキュリティポリシーが作成されたことを確認

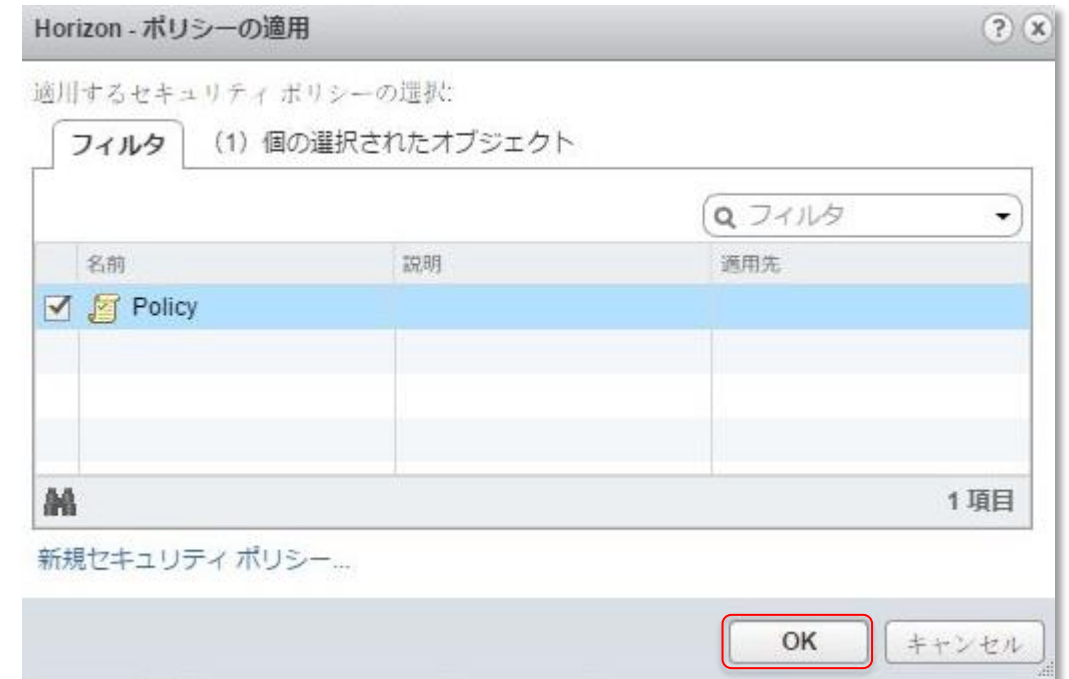


Security Policy、Security Groupの作成等(6)

- セキュリティグループに対して、セキュリティポリシーを割り当て



- 作成したセキュリティポリシーを選択して **OK**を押下
- セキュリティグループとセキュリティポリシーの紐づけが完了



主な手順

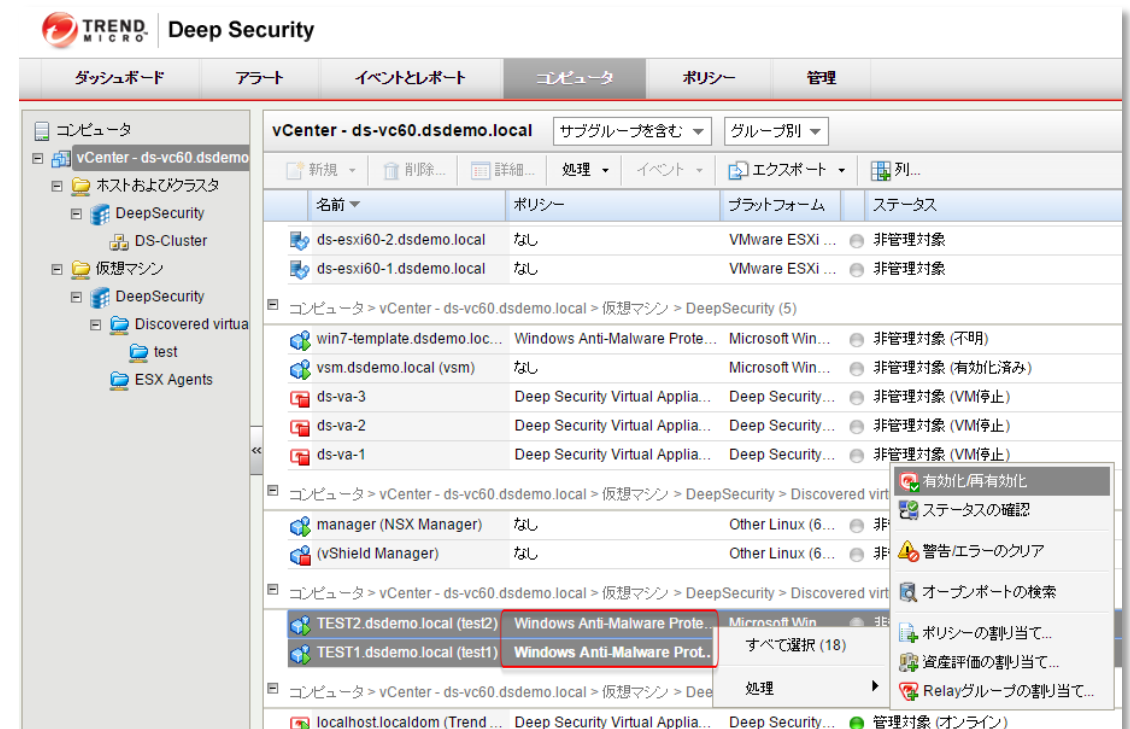
1. DSVA(Dep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Dep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Dep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

対象VMを順次有効化(1)

- Deep Security Managerにログイン



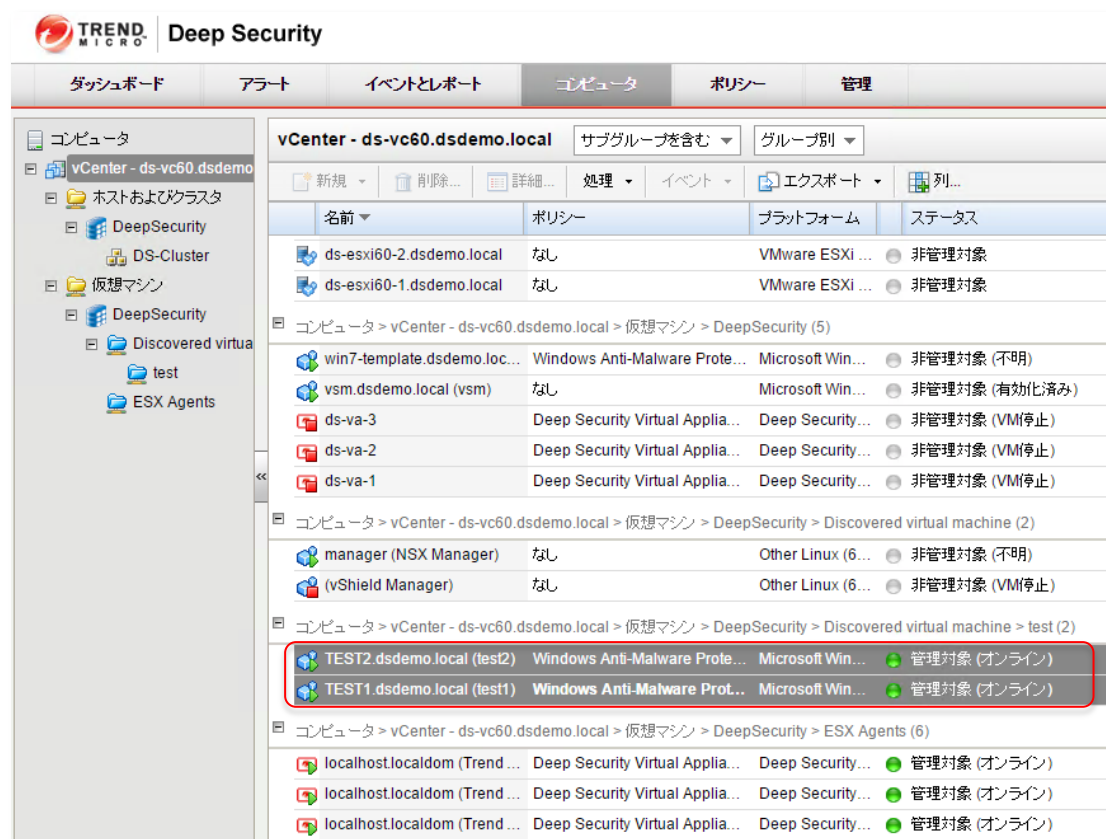
- 任意の**ポリシー(赤枠)**が選択されている事を確認
- コンピュータ**タブから対象VM (VDI) を選択し、順次**有効化/再有効化 (注)**を実施



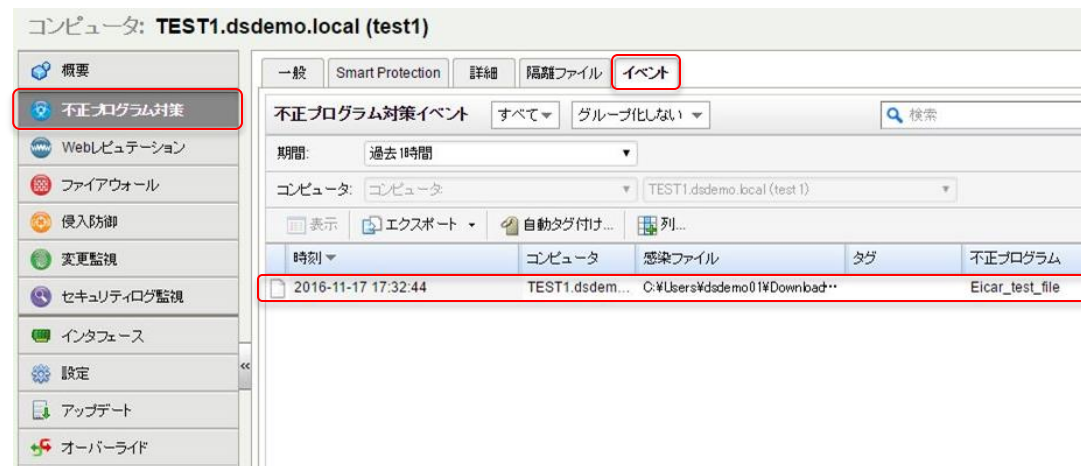
(注) 有効化に時間がかかる、又は失敗する場合は、同時に有効化するVM数を減らして実行してください

対象VMを順次有効化(2)

- 対象VM (VDI) のステータスが、管理対象 (オンライン) になったことを確認



- 管理対象VMをウイルスに感染 (Eicar ファイルをデスクトップにコピー) させることで、セキュリティイベントが検出されることを確認
- Deep Security Managerから、該当VMをダブルクリックし、不正プログラム対策-イベントタブから感染ファイルを確認



主な手順

1. DSVA(Dep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Dep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Dep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

新規VMの自動有効化設定(1)

- Deep Security Managerにログイン

セッションがタイムアウトしました。ログオン直してください。

ログオン

ユーザ名: masteradmin

パスワード:

☐ 多要素認証を使用する

ログオン

- 管理タブ-イベントベースタスクから、新規を押下

TREND MICRO Deep Security

ダッシュボード アラート イベントとレポート コピュータ ポリシー **管理**

システム設定
予約タスク
イベントベースタスク
Managerノード
ライセンス
ユーザ管理
システム情報
アップデート
セキュリティ
ソフトウェア
Relayグループ

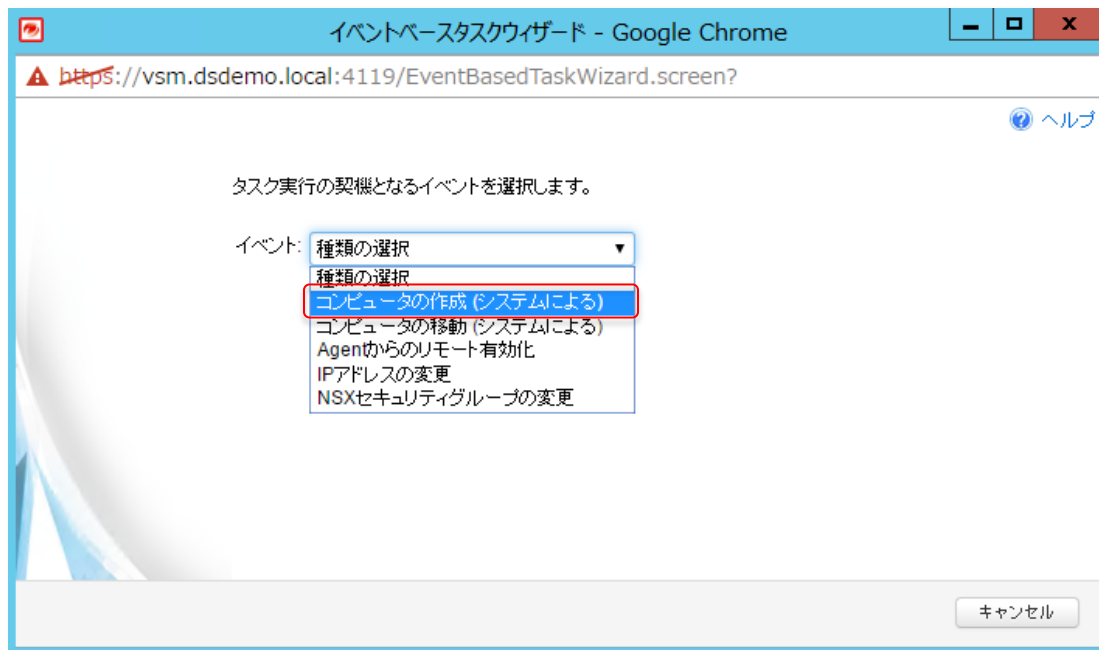
イベントベースタスク

新規... 削除... プロパティ... 複製

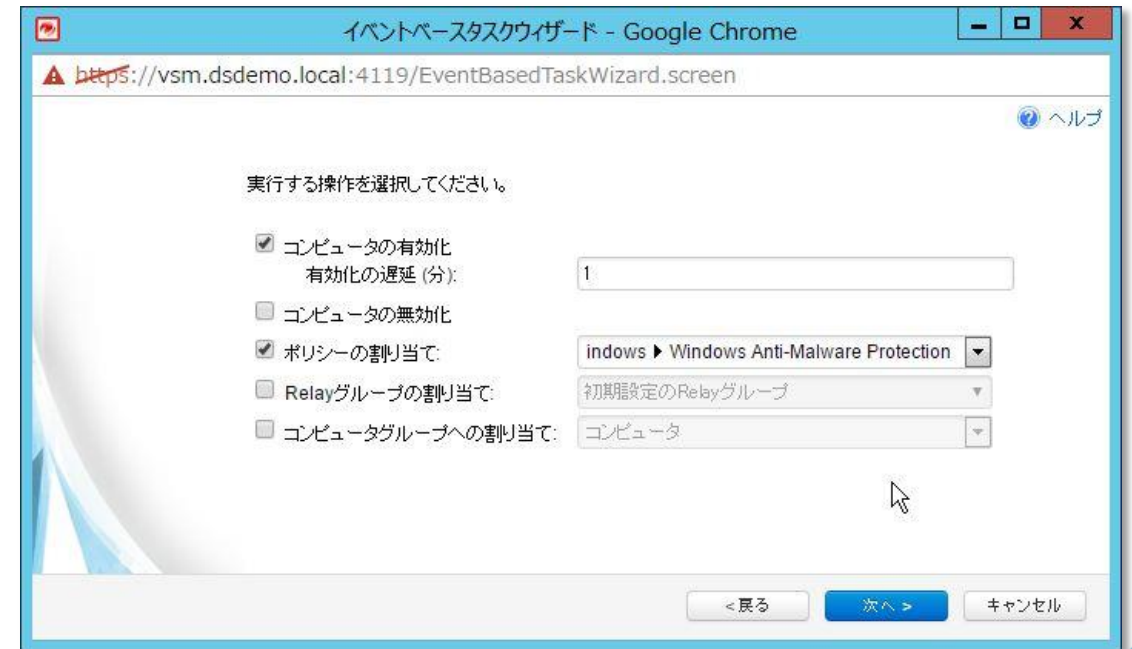
名前	種類	前回の実行日時
リストにアイテムがありません		

新規VMの自動有効化設定(2)

- イベントから、コンピュータの作成（システムによる）を選択



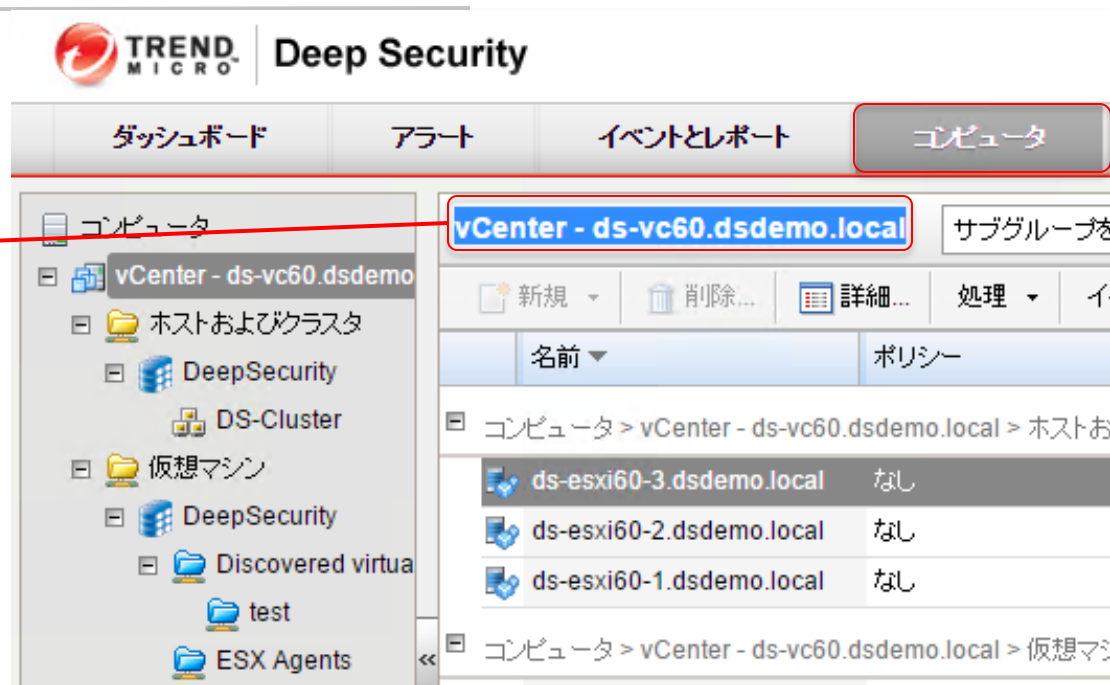
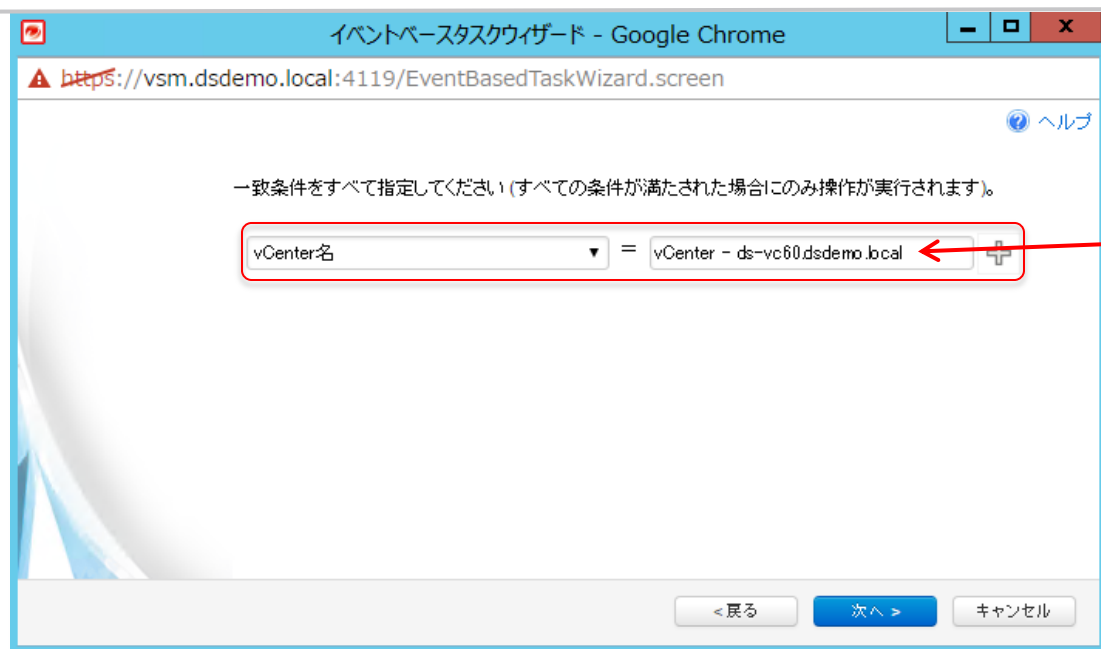
- コンピュータの有効化をチェックし、有効化の遅延として1（分）（注）と入力
- ポリシー割り当てをチェックし、Windows Anti-Malware Protectionを選択



（注）VDIのOSが起動完了後、DSから有効化する必要があります。
環境により有効化遅延時間の調整をお願い致します。

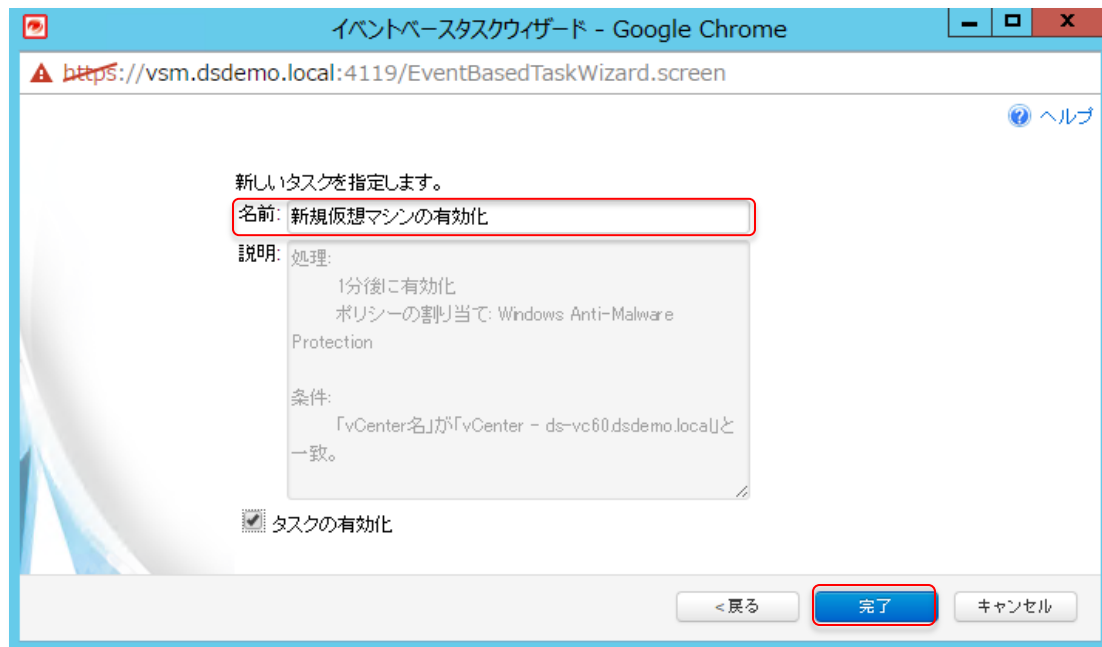
新規VMの自動有効化設定(3)

- 一致条件としてvCenter名を選択
- vCenter名は、コンピュータタブの以下文字列を選択

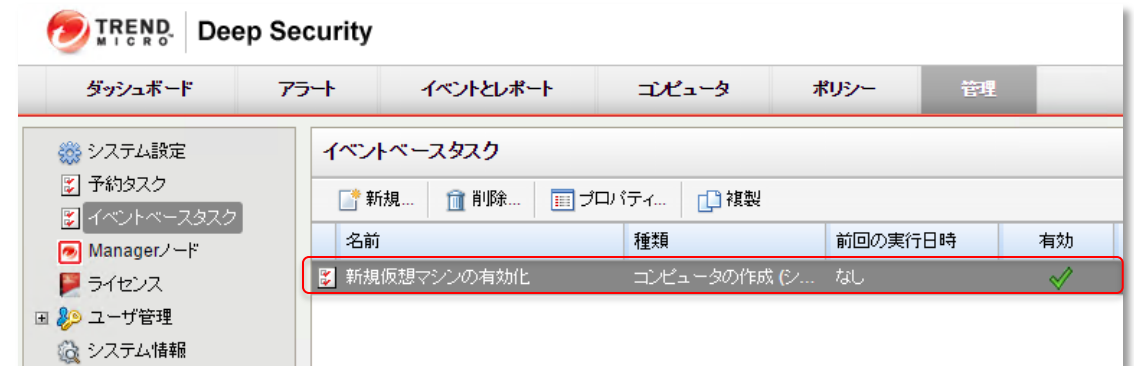


新規VMの自動有効化設定(4)

- 名前として、“新規仮想マシンの有効化”と入力し、**完了**を押下



- イベントベースタスクが追加され、ステータスが有効になっていることを確認



主な手順

1. DSVA(Deep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Deep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Deep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

旧環境のDSVA、およびvShield Managerを削除

- 手順2、手順5でそれぞれ停止したVMは不要なのでWeb Client から削除

主な手順

1. DSVA(Deep Security Virtual Appliance)の無効化
2. vShield Manager の停止
3. NSX Manager のデプロイ
4. Deep Security Manager と vShield Manager の連携解除
5. DSVA(Deep Security Virtual Appliance)の停止
6. Deep Security Manager と NSX の連携設定
7. Guest Introspection のデプロイ
8. DSVA(Deep Security Virtual Appliance)のデプロイ
9. Security Policy、Security Groupの作成等
10. 対象VMを順次有効化
11. 新規VMの自動有効化設定
12. 旧環境のDSVA、およびvShield Managerを削除
13. 注意点

注意点

- 手順8でデプロイするDSVA(Deep Security Virtual Appliance)は、DHCPもしくはIP Poolを事前に設定しておくことで、IPの割り当てを実施する。
- DSVAは各ESXi毎にデプロイされるので、ESXiの台数分のIPアドレスを確保している必要がある。
- ただし、**DHCP使用時**は設定したスコープ内で一時的に「DSVA台数×2」(今回だと6つのIPアドレス)が確保されている必要がある。

DSVAの展開が完了次第、不要なIPアドレスはリリースされます(今回だと3つのIPアドレス)

- **IP Pool使用時は、「DSVA台数分」(今回だと3つのIPアドレス)を確保**しておけば、3台のDSVAの展開を行うことが可能。

