



Trend Micro Deep Security™ 9.0SP1 Development Guide with VMware Auto Deploy



◎掲載内容の無断転載を禁じます。

本ドキュメントならびに本ドキュメントに記載されている URL のウェブサイト(以下「本ウェブサイト」と言います) 上に掲載されるテキスト、グラフィックス及びその他の情報 (以下、あわせて「ドキュメント」と言います) に関する著作権、並びに、その他のすべての知的所有権は、トレンドマイクロ株式会社又はトレンドマイクロ株式会社へドキュメントを提供している第三者へ独占的に帰属します。お客様は、トレンドマイクロ株式会社の事前の書面による承諾を得ることなく、ドキュメントをダウンロード、アップロード、複製、改変、翻訳、使用許諾、又は、手段を問わず転送することはできないものとします。

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 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アップサービス、Trend Micro Deep Security あんしんパック、こどもーど、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、トレンドマイクロ バッテリーエイド、Trend Micro Safe Lock、トレンドマイクロ セーフバックアップ、Deep Discovery Advisor、Deep Discovery Inspector、Trend Micro Mobile App Reputation、あんしんブラウザ、および Jewelry Box は、トレンドマイクロ株式会社の登録商標です。

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。

Copyright (c) 2014 Trend Micro Incorporated. All rights reserved.

目次

第 1 章 はじめに	5
1-1. ドキュメント内の略称表記について	5
1-2. 目的	5
1-3. メリット	6
1-4. 対象ユーザ	6
1-5. 必要なスキルセット	6
1-6. 注意事項	7
1-7. 関連資料	7
第 2 章 環境概要	9
2-1. 各コンポーネントについて	9
2-2. 事前準備	11
第 3 章 導入手順	13
3-1. 全体構成図	13
3-2. 全体の流れ	14
3-3. 導入作業	15
第 4 章 Tips 集	40
4-1. システムアップグレード時の Auto Deploy 手順	40
4-2. ヒープメモリサイズの設定変更をデプロイ時に組み込む	50
4-3. 「エンジンがオフライン」が発生する場合	51
4-4. vShield Endpoint が認識されない場合	53

第1章 はじめに

1-1. ドキュメント内の略称表記について

本ドキュメント内では下記の略称を利用します。

用語・略語	説明
ESXi	VMware vSphere Hypervisor
vSM	VMware vShield Manager
vCSA	VMware vCenter Server Appliance
vSE	VMware vShield Endpoint
PowerCLI	VMware vSphere PowerCLI
DSM	Trend Micro Deep Security Manager
DSR	Trend Micro Deep Security Relay
DSVA	Trend Micro Deep Security Virtual Appliance
F.D	Trend Micro Filter Driver
A.V	Anti-Virus
Victim	動作確認用仮想マシン

1-2. 目的

Auto Deploy を利用するような案件導入時にいかに手間をかけずにセキュリティを実装出来るか、また導入後のパッチメンテナンスといった一連の運用作業においても、可能な限り自動化を用いて運用者の負荷を軽減する事を目的に本検証を実施しております。

コストや工数の割には費用対効果が見えづらい、しかし重要なコンポーネントのひとつでもあるセキュリティの実装に関して、自動に展開されるホストにあわせてセキュリティの実装も出来る限り自動化出来ないか、という考えをもとに VMware 社と本共同検証を行っております。

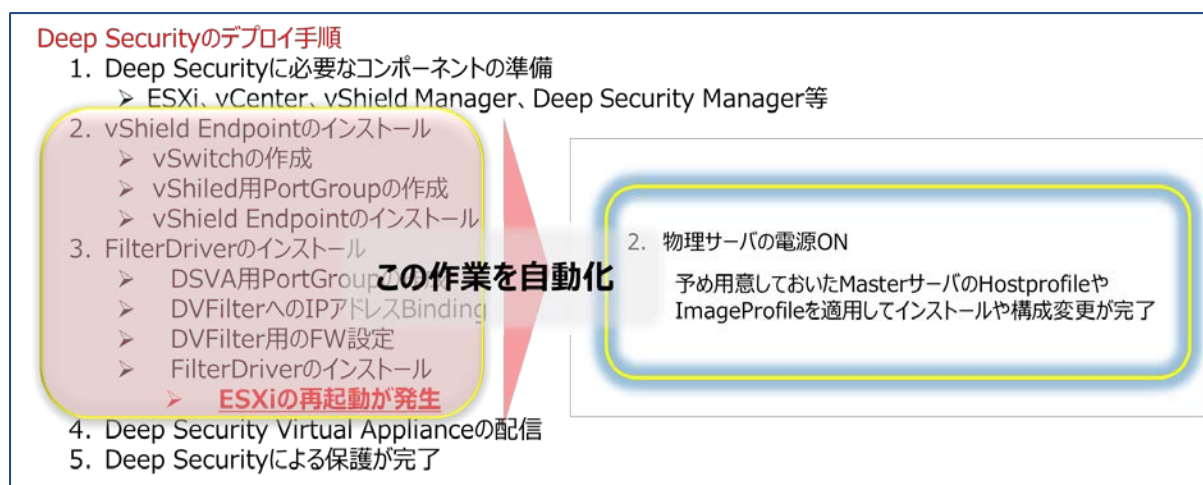
1-3. メリット

1.

VMware 社の Auto Deploy ソリューションと連携する事で Deep Security のデプロイメントにかかる工数を簡略化し、迅速なプロビジョニングを可能と致します。

2.

システム導入後のパッチ適用といった一連の運用作業においても、マスターとなる ESXi イメージを用意するだけで作業の一元化が可能となり、運用工数の削減が可能となります。



1-4. 対象ユーザ

- ・Auto Deploy を使った環境の構築 ・ 運用を現在行っており(又はこれから行う)、今後 Security の実装をご検討をされているユーザ
- ・Deep Security の導入 ・ 運用に対して出来る限り工数をかけずに実装したいユーザ

本ドキュメントは上記ユーザを対象として作成しております。

1-5. 必要なスキルセット

- ・VMware vSphere 環境の構築 及び運用管理について理解している
- ・VMware Auto Deploy の実装方法について理解している
- ・Trend Micro Deep Security (DSVA) 環境の構築 について理解している

1-6. 注意事項

•このドキュメントの使い方

このドキュメントは、VMware vSphere 環境での Auto Deploy を利用した Deep Security 9.0 SP1 の構築支援を目的としております。インストールガイドや管理者ガイドとして使用するものではございません。それらについては他のドキュメントをご参照願います。

•シナリオ実施にあたっての注意事項

本シナリオは弊社の検証環境において動作している事を確認しておりますが、このドキュメントの実行によりお客様の環境での動作を保証するわけではございません。

可能な限り正確を期するように努めておりますが、本資料の情報は、使用者の責任において使用されるべきものであることを、予めご了承下さいますようお願い致します。

vShield Endpoint は 2014 年 7 月現在、Auto Deploy 環境において他社ソリューションとの組み合わせまで動作確認が出来ておらず、正式サポートとなっております。

今回の共同検証で Auto Deploy 環境下においても Deep Security と問題なく連携する事が確認出来ましたので、今後のサポートに向け VMware 社にて検討を進める予定です。

1-7. 関連資料

ドキュメント内で情報が確認できなかった場合には以下の URL にて各種情報をご用意しておりますので合わせてご確認ください。

参考 : VMware Auto Deploy 関連資料

VMware 技術者 虎の穴

vSphere 5.1-Auto Deploy / Host Profiles / Power CLI

<<http://www.vmware.com/jp/partners>>

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

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

参考 : Deep Security Virtual Appliance インストール手順

<<http://esupport.trendmicro.com/solution/ja-JP/1097198.aspx>>

参考 : Trend Micro Filter Driver のヒープメモリサイズ設定資料

Trend Micro Deep Security 9.0 Service Pack1 管理者ガイド

P618 : パフォーマンスの要件 (Filter Driver のヒープメモリサイズ設定)

参考 : Trend Micro Deep Security 導入時、導入後のサポートサイト

Trend Micro Deep Security サポートウェブ

<<http://esupport.trendmicro.com/ja-jp/enterprise/ds/top.aspx>>

参考 : Deep Security Virtual Appliance 9.0 トラブルシューティングガイド

<http://files.trendmicro.com/jp/ucmodule/tmds/90SP1/DSVA_9.0TroubleshootingTips_extermal_r1.pdf>

第2章 環境概要

2-1. 各コンポーネントについて

- 本ドキュメントは下記の環境において動作を確認したものとなります。

メーカー	製品	バージョン	備考
VMware	VMware vSphere Hypervisor	ESXi5.5U1 (1623387)	※Auto Deploy を使用するためには Enterprise Plus が必要
	VMware vShield Manager	5.5.2	
	VMware vShield Endpoint	5.1.0 (01255202)	
	VMware vCenter Server Appliance	5.5.0.b (1476389)	vCSA で vCenter を構築すれば DHCP、FTP サーバが含まれているので個別に用意する必要はない。
	VMware vSphere PowerCLI	5.5	DSM ヘインストール
Trend Micro	Trend Micro Deep Security Manager	9.0SP1Patch3 (9.0.6500)	
	Trend Micro Deep Security Virtual Appliance	9.0SP1Patch3 (9.0.0-3500)	
	Trend Micro Filter Driver	9.0SP1Patch3 (9.0.0-3500)	
Microsoft			
	Microsoft Windows Server	2008 R2	DSM の OS
	Microsoft Windows	7	Victim

- **Auto Deploy で利用するインストールファイルに関する注意事項**

Auto Deploy では、EsxSoftwareDepot に登録されるファイルは Zip 形式となっております。

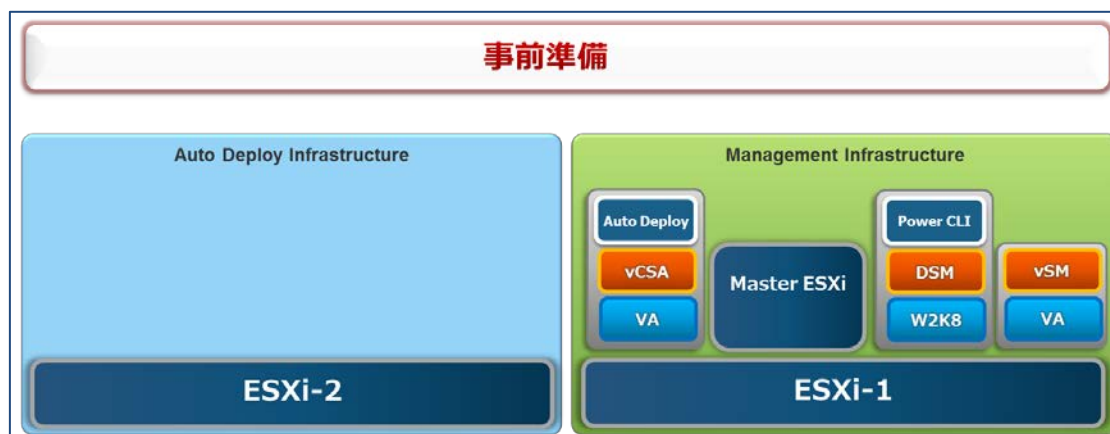
「VMware vSphere Hypervisor」、「VMware vShield Endpoint」、「Trend Micro Filter Driver」に関しては Zip 形式のファイルを EsxSoftwareDepot に登録する必要がありますので、事前に各社のダウン

ロードサイトや vSM から Zip 形式ファイルをダウンロードして頂きたくお願い致します。vSM からのダウンロード方法は「3-3. 導入作業」に記載しております。

2-2. 事前準備

本ドキュメント実施にあたり事前に構成されている環境

下記の環境については本ドキュメントの手順を実施する事前準備として、既に構築が完了されているものとします。本ドキュメントでは下記コンポーネントの作成手順については特に記載はしていません。構築に関する資料が必要な場合は「1-7. 関連資料」をご参照願います。



※VA・・・Virtual Appliance

- Management Infrastructure の構築

※ここでは、vSphere や Deep Security を管理するための基盤を「Management Infrastructure」と記載しております。

- ESXi サーバ(ESXi-1)のセットアップが完了している事。
 - vCenter(vCSA) / Auto Deploy / DSM / vSM の準備が完了している事。
 - ◇ Auto Deploy に必要なサーバ(DHCP、FTP、Auto Deploy サーバ等)は vCSA の機能として提供されております。ゆえに、vCSA で vCenter を構築した場合は、上記サーバを別途用意する必要はございません。
 - ◇ Auto Deploy に関するセットアップが完了している事。
 - ◇ DSM のインストールが完了し、vCenter や vSM との連携設定が完了している事。
- 手順に関しては「1-7.関連資料」の「参考：Deep Security Virtual Appliance インストール手順」を参照下さい。
- ◇ Power CLI のインストールが完了している事。
 - Auto Deploy が稼働している vCSA と通信可能なサーバであれば、DSM 以外のサーバにインストールして頂いても問題ございません。

➤ MasterとなるESXi(ここではNested ESXiを使用)のインストール及び基本設定が完了している事。

◇ Auto Deployで展開されるESXiの構成情報(Host Profile)のベースとなるサーバです。Auto Deployにて展開されたESXiはこのHost Profileを参照し、設定変更が行われます。

Masterサーバに対しては、

1. 「通常のESXiセットアップ」
2. 「Deep Securityに関するコンポーネントのインストールや設定変更を適用」
3. 「Host Profileを作成」

という手順を踏みますので、ESXiに関する通常の設定は、事前に作業の実施をお願い致します。

例：vSwitch、Portgroup、NIC チーミング、Datastore、NTP、管理者パスワード、Syslogサーバ(Syslog.global.logHost)、ネットワークコアダンプ(ESXi Dump Collector)、ステートレスキャッシュ、ステートフル等の設定。詳細は「VMware 技術者 虎の穴」を参照下さい。

◇ 事前準備として用意するMasterサーバの構築に関しては、展開されるホスト同様Auto Deployを使用して起動してください。

本ドキュメントではAuto Deployに関する説明は行いませんが、Auto DeployやPowerCLIの動作を理解した上で実施された方がより効果的に作業を進める事が出来る為、事前の準備としてAuto Deployをご利用頂ければと思います。

◇ 以降では、このMaster ESXiに対して、Deep Securityを実装する上で必要なコンポーネントのインストールや設定変更を実施していきます。

● Auto Deploy Infrastructureの構築

※ここでは、Auto Deployにより展開されるESXiが稼働する基盤を「Auto Deploy Infrastructure」と記載しております。

➤ ESXiサーバ(ESXi-2)のセットアップが完了している事。

第3章 導入手順

3-1. 全体構成図



本ドキュメントを実施後に構築される最終構成図となります。

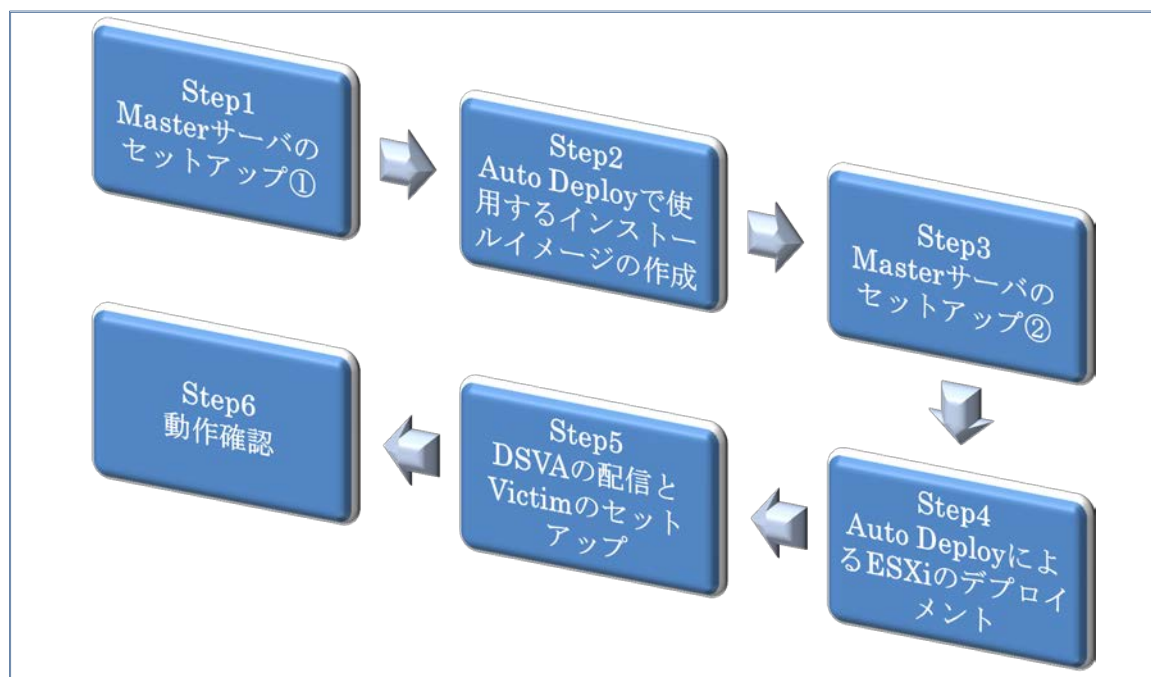
以降の導入手順に従い Auto Deploy を利用した Deep Security の実装を行う事で、DSVA にて保護されたシステムを構成する事が可能となります。

シングルホスト構成及び HA クラスタ構成の 2 パターンで検証を行っておりますが、本ドキュメントは HA クラスタ構成をベースに記載をしております。

シングルホスト構成または HA クラスタ構成であっても導入に関する基本的な考え方は同様となります。

3-2. 全体の流れ

導入手順



導入全体の流れとして以下の様になります。

1. Master サーバのセットアップ①（vSE インストール及び F.D の導入準備）
2. Auto Deploy で使用するインストールイメージの作成
3. Master サーバのセットアップ②（DSVA 有効化によるパラメータ変更）
この時点で参照用となる Host Profile とインストールイメージの準備は完了。
1 回ここまで作成出来れば後は No4、No5、No6 をサーバ台数分実施するのみ。
4. Auto Deploy による ESXi のデプロイメント
5. DSVAs の配信と Victim のセットアップ
6. 動作確認

3-3. 導入作業

1. Master サーバのセットアップ①（vSE インストール及び F.D の導入準備）

※黄色枠線内が変更対象



ここでは既に基本設定が完了している Master サーバに対して、Deep Security の実装に必要な各種コンポーネントのインストールや設定変更を実施し、Master となる Host Profile を作成致します。

1-1 Master サーバに対して、vSE をインストールする。

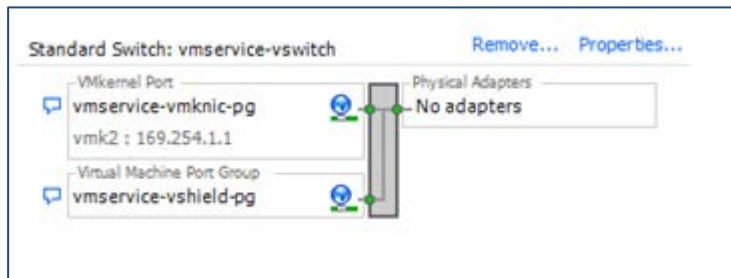
1-1.1 vSM の管理画面より vSE の「install」を実行する。

1-1.2 vSE が正常にインストールされた事を確認する。

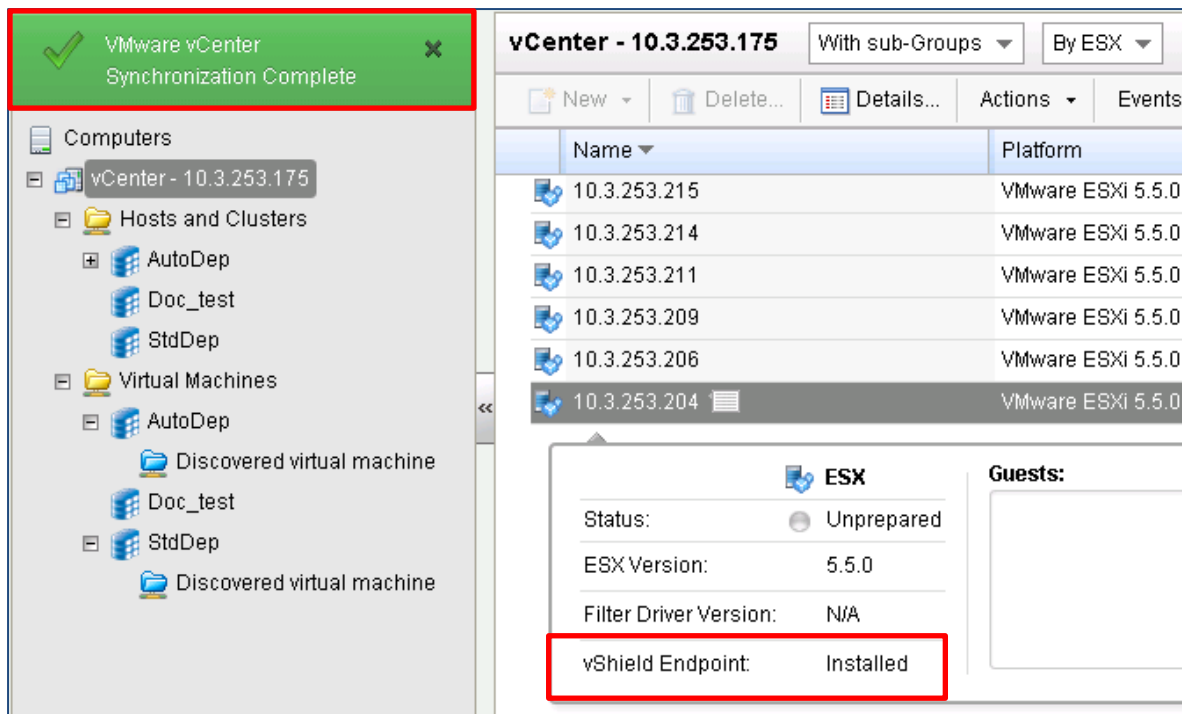
- vSM の管理画面より vSE が正常にインストールされた事を確認する。

General		Endpoint		
vShield Host Preparation Status for 10.3.253.91				
<i>Last updated</i>				
Service	Installed	Available		
vShield App	Not installed	5.5.0-1447281	Not licensed	?
vShield Endpoint	5.1.0-01255202	-	Uninstall	?
vShield Data Security	Not installed	5.1.0.0-833296	Not licensed	?

- vmservice-vswitch が作成され、vmservice-vshield-pg、vmservice-vmknic-pg 及び vmk*:169.254.1.1 が設定されている事を確認する。



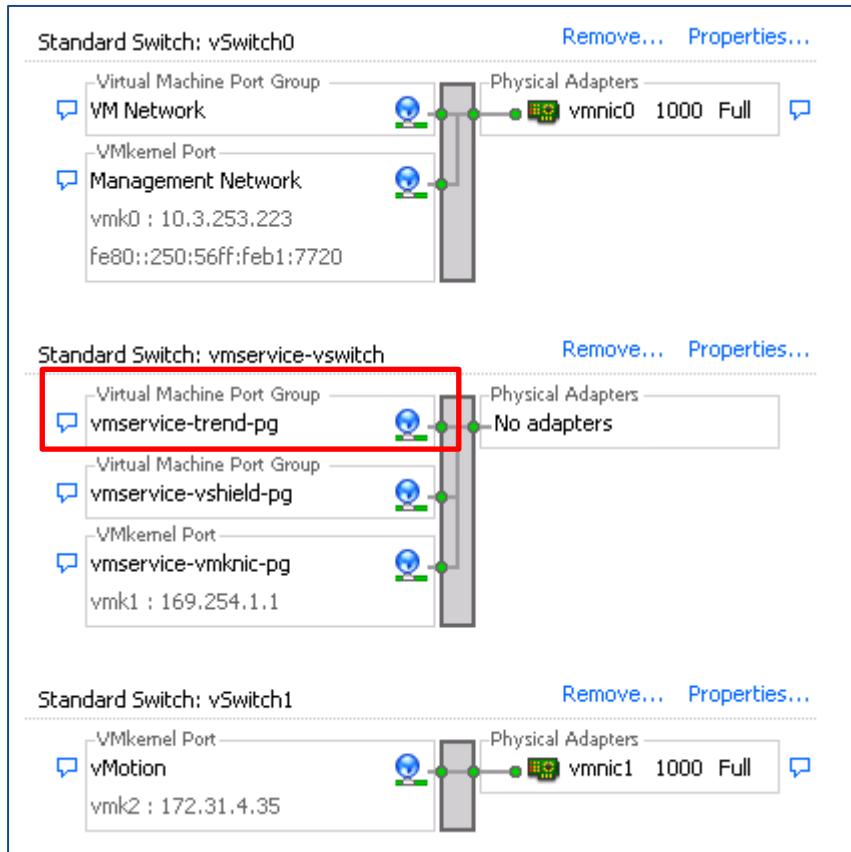
- DSM の管理画面より、vCenter との同期「今すぐ同期」を実行し、vSE が正常にインストールされた事を確認する。



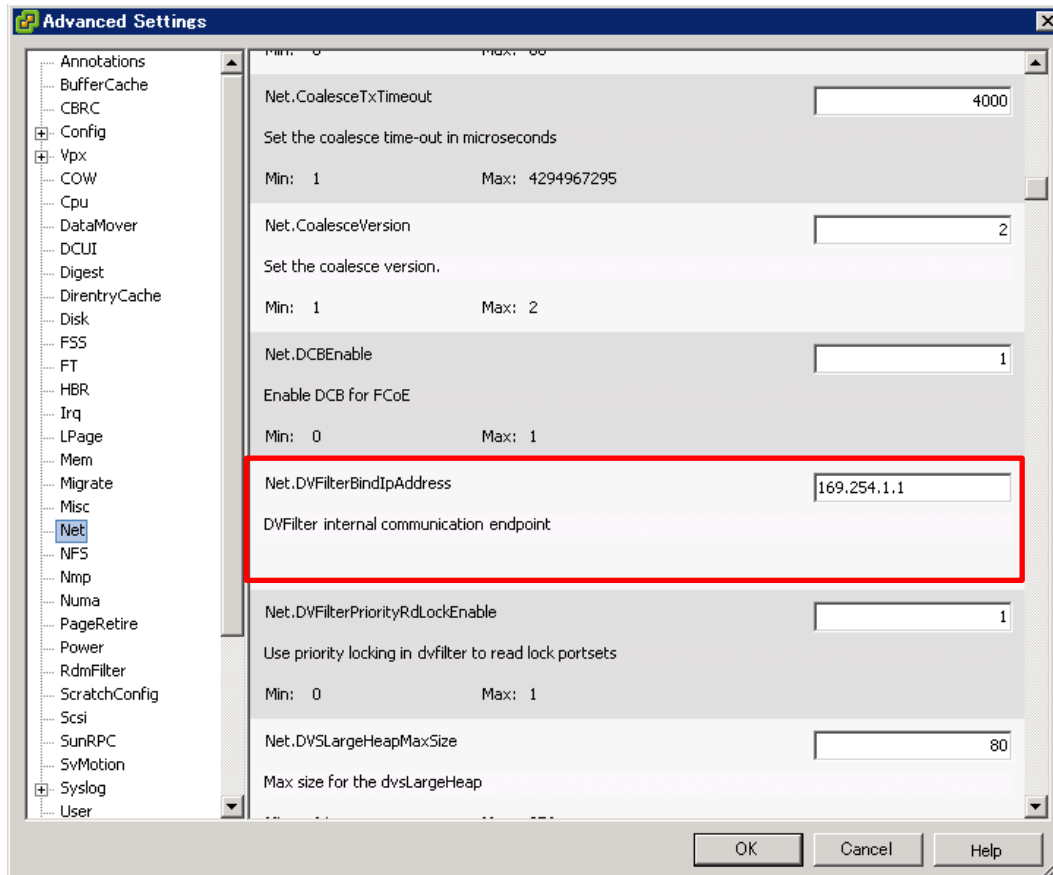
1-2 F.D の導入準備を行う。

1-2.1 vSE のインストールにて作成された vmervice-vswitch に対し、DSVA 用の PortGroup を作成する。

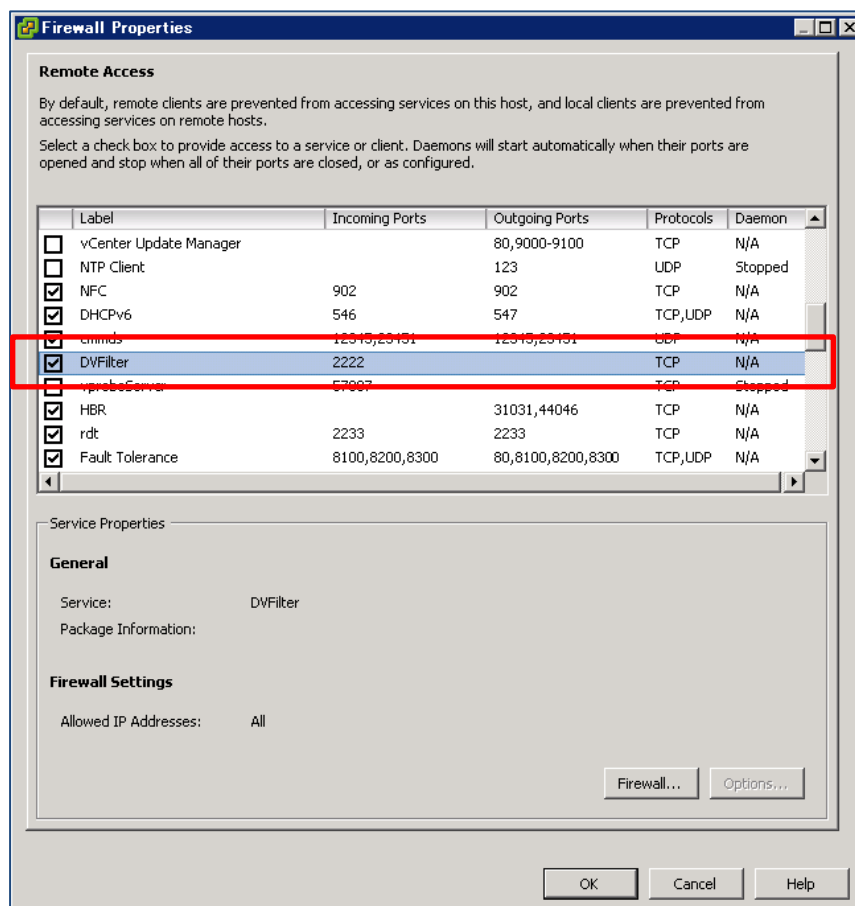
ポートグループ名 : 「vmervice-trend-pg」を作成



1-2.2 ホストの詳細設定にて DVFilter に Bind させる IP Address を設定する。
Net.DVFilterBindIpAddress = 169.254.1.1



1-2.3 ホストのセキュリティプロファイルにて DVFilter が使用するポートを許可する。



1-3 Master となる Host Profile を作成する。

1-3.1 Master サーバの Host Profile を作成し、Host Profile 名を「autoDep01_std_ep_fd」と命名しておく。

※F.D のヒープメモリサイズの調整が必要な場合は「4-2.ヒープメモリサイズの設定変更をデプロイ時に組み込む」を参考にしてください。

1-3.2 Host Profile の編集① - Host Profile の自動適応のため

vSE 構成時に作成される vmkernel の IP は固定(169.254.1.1/24)で設定されます。

このため前項で取得した Master サーバの Host Profile には IPAddress は保存されず、応答ファイル扱いとなります。

このままでは、新規で起動したホストには自動適応されず、メンテナンスモードで起動するため手作業が発生します。

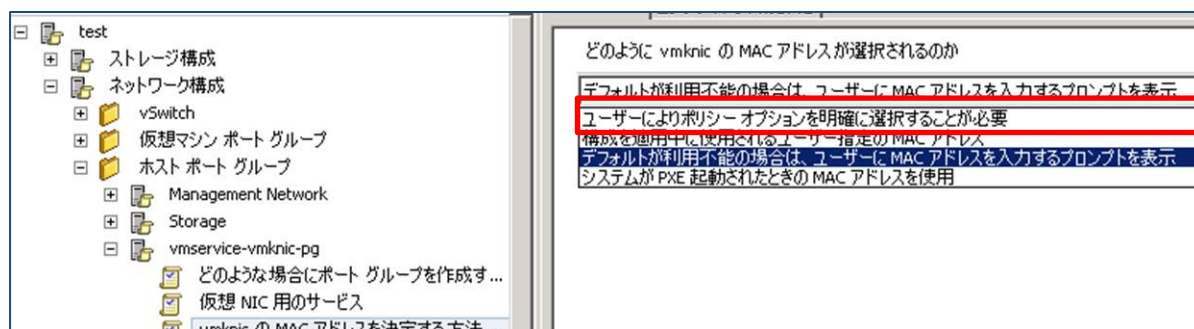
新規ホストの起動時に自動適応させるため、以下の 2 つのパラメータの変更を実施します。

【1 点目】

「ホストプロファイル」→「ネットワーク構成」→「ホストポートグループ」→「vmervice-vmknic-pg」→「vmknic の MAC アドレスを決定する方法」

“デフォルトが利用不可の場合は、ユーザーに MAC アドレスを入力するプロンプトを表示”

⇒“ユーザーによりポリシーオプションを明確に選択することが必要”



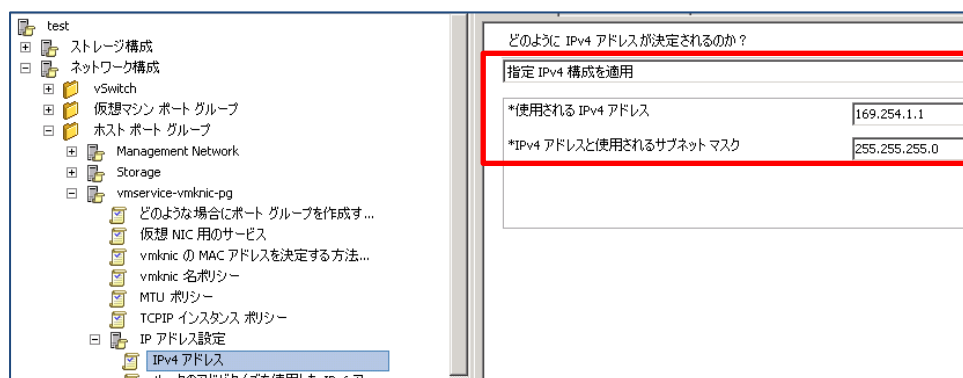
【2 点目】

“デフォルトが利用不可の場合は、ユーザーに IPv4 アドレスを入力するプロンプトを表示”

⇒“指定 IPv4 構成を適応” で以下のパラメータを入力

使用される IPv4 アドレス : **169.254.1.1**

IPv4 アドレスと使用されるサブネットマスク : **255.255.255.0**

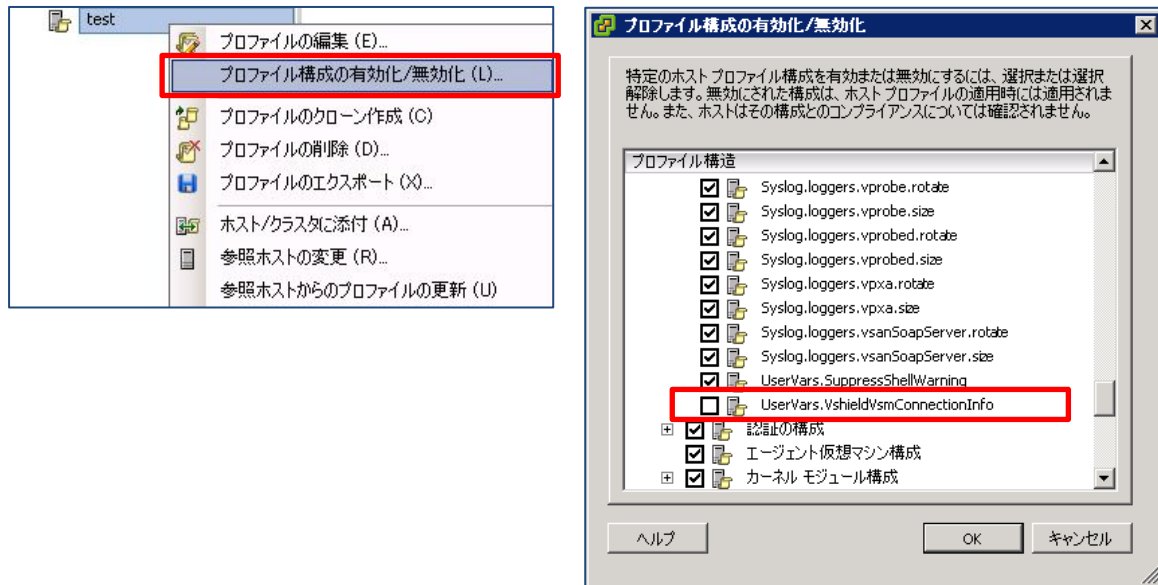


1-3.3 Host Profile の編集② - パラメータの無効化

ESXi ホスト毎に一意の値を持つパラメータが存在するので、Host Profile の適用対象から除外します。

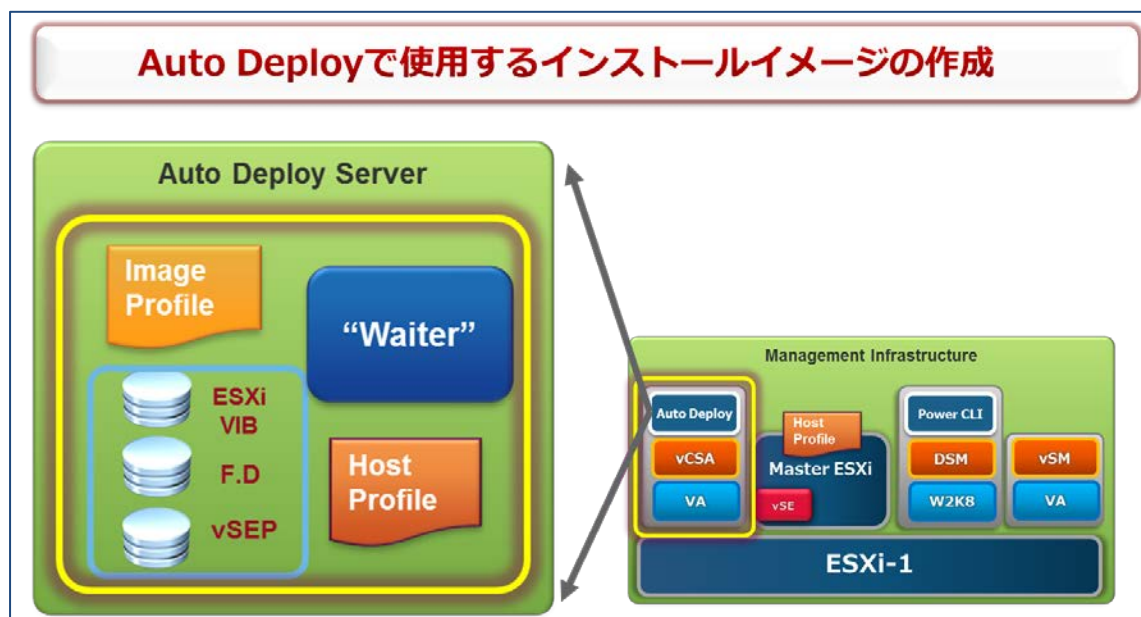
「UserVars.VshieldVsmConnectionInfo」のチェックを外し、OK を押下。

これでパラメータが無効され、Host Profile 適応の対象外となります。



2. Auto Deploy で使用するインストールイメージの作成

※黄色枠線内が変更対象



ここでは PowerCLI を用いて、第 2 章で準備した下記 Zip ファイルを「ESXSoftwareDepo」に登録致します。

- VMware vSphere Hypervisor
- VMware vShield Endpoint
- Trend Micro Filter Driver

その後、「Image Profile」や「DeployRule」といったルールを作成し、Auto Deploy の準備を完了させます。

2-1 DSM にインストールした PowerCLI にてインストールイメージやルールの作成を行う。

※第 2 章で準備頂いた Zip ファイルを DSM の任意ディレクトリに配置しておきます。

2-1.1 vSE は下記より Download して下さい。

<https://vSM IP Address/bin/offline-bundles/vShield-Endpointp-Mux.zip>

ダウンロードしたファイルを解凍すると「esx55」というフォルダがあるので、その中にある「vShield-Endpoint-Mux.zip」を使用します。ここでは分かりやすい様にファイル名を下記に変更しております。

- vShield-Endpoint-Mux.esx55.zip

2-1.2 ESXi の VIB ファイル及び F.D のファイルを各社のページから Download しておく。

- update-from-esxi5.5-5.5_update01.zip
- FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip

2-1.3 PowerCLI を使用して、インストール用イメージやルールの作成を行う。

【EsxSoftwareDepot ハイメージを追加する】

■ インストール用ファイルが配置されているフォルダにて下記コマンドを実行する

```
PowerCLI C:¥ Upgrade_vib> dir
-a---      2014/06/24      5:22   227804      FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip
-a---      2014/03/20      11:12  654389915  update-from-esxi5.5-5.5_update01.zip
-a---      2013/08/01      14:59   125863      vShield-Endpoint-Mux.esx55.zip
```

■ EsxSoftwareDepot にインストール用ファイルを追加していく

```
PowerCLI C:¥ Upgrade_vib> Add-EsxSoftwareDepot .¥vShield-Endpoint-Mux.esx55.zip
Depot Url
-----
zip:C:¥Upgrade_vib¥vShield-Endpoint-Mux.esx55.zip?index.xml
```

```
PowerCLI C:¥Upgrade_vib> Add-EsxSoftwareDepot FilterDriver-ESX_5.0-9.0.0-3500.x86_64.
zip
Depot Url
-----
zip:C:¥Upgrade_vib¥FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip?index.xml
```

■ 正常にファイルが追加されたことを確認する

```
PowerCLI C:¥Upgrade_vib> Get-EsxSoftwareDepot
Depot Url
-----
zip:C:¥Upgrade_vib¥vShield-Endpoint-Mux.esx55.zip?index.xml
zip:C:¥Upgrade_vib¥FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip?index.xml
```

■ Trend Micro 及び VMware 社の VIB ファイルが追加されたことを確認する

- ・Trend Micro : dvfilter-dsa
- ・VMware : epsec-mux

```
PowerCLI C:¥Upgrade_vib> Get-EsxSoftwarePackage
```

Name	Version	Vendor	Creation Date
dvfilter-dsa	9.0.0-3500	Trend	2014/05/12 15...
epsec-mux	5.1.0-01255202	VMware	2013/08/01 21...

■ 最後に ESXi の Update1 ファイルを追加する

```
PowerCLI C:¥ Upgrade_vib> Add-EsxSoftwareDepot update-from-esxi5.5-5.5_update01.zip
```

```
Depot Url
```

```
-----
```

```
zip:C:¥ Upgrade_vib¥update-from-esxi5.5-5.5_update01.zip?index.xml
```

```
PowerCLI C:¥Upgrade_vib> Get-EsxSoftwareDepot
```

```
Depot Url
```

```
-----
```

```
zip:C:¥Upgrade_vib¥vShield-Endpoint-Mux.esx55.zip?index.xml
```

```
zip:C:¥Upgrade_vib¥FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip?index.xml
```

```
zip:C:¥Upgrade_vib¥update-from-esxi5.5-5.5_update01.zip?index.xml
```

【イメージプロファイルの作成を行う】

```
PowerCLI C:¥Upgrade_vib> $ip=Get-EsxImageProfile
```

```
PowerCLI C:¥Upgrade_vib> $ip | select Name
```

```
Name
```

```
----
```

```
ESXi-5.5.0-20140302001-no-tools
```

```
ESXi-5.5.0-20140301001s-no-tools
```

```
ESXi-5.5.0-20140301001s-standard
```

```
ESXi-5.5.0-20140302001-standard
```


- 既存のイメージプロファイルを複製し、今回使用するイメージプロファイルを作成する

```
PowerCLI C:¥ Upgrade_vib> New-ExsImageProfile -CloneProfile $ip[3] -name ESXi5.5.0u1_vSE_FD -vendor VMware
```

Name	Vendor	Last Modified	Acceptance Level
ESXi5.5.0u1_vSE_FD	VMware	2014/02/22 2...	PartnerSupported

- 複製したイメージプロファイルに VMware の vSE と Trend Micro の DriverVIB (Filter Driver) を追加する

```
PowerCLI C:¥Upgrade_vib> Add-ExsSoftwarePackage -ImageProfile ESXi5.5.0u1_vSE_FD -SoftwarePackage epsec-mux, dvfilter-dsa
```

Name	Vendor	Last Modified	Acceptance Level
ESXi5.5.0u1_vSE_FD	VMware	2014/06/24 1...	PartnerSupported

【イメージプロファイルのエクスポートを行う】

- 作成したイメージプロファイルを Depot ファイルとしてエクスポートしておく

(今までの作業は PowerCLI に保存されているわけではないので、エクスポートせずに PowerCLI を終了した場合は再度同作業を実施する必要があるため)

```
PowerCLI C:¥Upgrade_vib> Export-ExsImageProfile -ImageProfile ESXi5.5.0u1_vSE_FD -ExportToBundle -FilePath C:¥Upgrade_vib¥My-ESXi5.5.0u1_vSE_FD.zip
```

```
PowerCLI C:¥Upgrade_vib> dir
```

ディレクトリ: C:¥Upgrade_vib

Mode	LastWriteTime	Length	Name
d----	2014/06/24 14:33		original
-a---	2014/06/24 5:22	227804	FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip
-a---	2014/06/24 15:34	333776738	My-ESXi5.5.0u1_vSE_FD.zip

```
-a---      2014/03/20   11:12  654389915  update-from-esxi5.5-5.5_update01.zip
-a---      2013/08/01   14:59   125863   vShield-Endpoint-Mux.esx55.zip
```

【ルールの作成を行う】

■ vCenter へ接続する

```
PowerCLI C:¥ Upgrade_vib> Connect-VIServer "vCenter IP Address"
```

```
Name          Port  User
----          -
IP Address    443  root
```

```
PowerCLI C:¥Upgrade_vib> $ip=Get-EsxImageProfile
```

```
PowerCLI C:¥Upgrade_vib> $ip | select name
```

```
Name
----
ESXi-5.5.0-20140302001-no-tools
ESXi5.5.0u1_vSE_FD
ESXi-5.5.0-20140301001s-no-tools
ESXi-5.5.0-20140301001s-standard
ESXi-5.5.0-20140302001-standard
```

■ ルール : My-ESXi5.5.0u1_vSE_FD_rule を作成する

補足 : ここでは ESXi が追加されるインベントリをクラスタ配下ではなく、Datacenter 配下にしてあります。DSVA の動作確認時に、DRS により作業対象の ESXi へ仮想マシンが vMotion されるのを防ぐ為となります。

また、オプションに「-allhosts」を指定しておりますが、「-Pattern」にて MAC アドレス指定に変更する事も可能です。こちらに関しては実環境にあわせた設定をお願い致します。

```
PowerCLI C:¥Upgrade_vib> New-DeployRule -name My-ESXi5.5.0u1_vSE_FD_rule -Item $ip
[1], (Get-VMHostProfile autoDep01_std_ep_fd), (Get-Datacenter AutoDep) -allhosts
```

```
Downloading dvfilter-dsa 9.0.0-3500
```

```
Download finished, uploading to AutoDeploy...
```

```
Upload finished.
```

```
Warning: Image Profile ESXi5.5.0u1_vSE_FD contains one or more software packages that are not state
less-ready. You may experience problems when using this profile with Auto Deploy
```

■ 補足

ルール作成時に上記のような Warning が出力されます。

Auto Deploy 環境でホストを再起動した場合のパラメータの再現が出来ない可能性があることを示す物ですが、今回は Host Profile で構成を再現しておりますので上記 Warning は無視して頂いて構いません。

```
Name      : My-ESXi5.5.0u1_vSE_FD_rule
```

```
PatternList :
```

```
ItemList   : {ESXi5.5.0u1_vSE_FD, AutoDep, autoDep01_std_ep_fd}
```

- ルールセットにルールを追加する（作成したルールが 1 番上に登録される事を確認する）

```
PowerCLI C:¥Upgrade_vib> Add-DeployRule -DeployRule My-ESXi5.5.0u1_vSE_FD_rule -at 0
```

```
Name      : My-ESXi5.5.0u1_vSE_FD_rule
```

```
PatternList :
```

```
ItemList   : {ESXi5.5.0u1_vSE_FD, AutoDep, autoDep01_std_ep_fd}
```

- コンプライアンス違反か否かを確認する

```
PowerCLI C:¥Upgrade_vib> $tr=Test-DeployRuleSetCompliance 10.3.253.91
```

```
PowerCLI C:¥Upgrade_vib> $tr.ItemList
```

CurrentItem	ExpectedItem
-----	-----
	ESXi5.5.0u1_vSE_FD

- Auto Deploy サーバ上のルール及びルールセットの更新を行う

```
PowerCLI C:¥Upgrade_vib> Repair-DeployRuleSetCompliance $tr
```

```
Warning: Image Profile esxi5.5.0_endpoint_filterdriver contains one or more software packages that are not stateless-ready. You may experience problems when using this profile with Auto Deploy.
```

```
Warning: Image Profile ESXi5.5.0u1_vSE_FD contains one or more software packages that are not stateless-ready. You may experience problems when using this profile with Auto Deploy
```

- 補足

ルール作成時に上記のような Warning が出力されます。

Auto Deploy 環境でホストを再起動した場合のパラメータの再現が出来ない可能性があることを示すものですが、今回は Host Profile で構成を再現しておりますので上記 Warning は無視して頂いて構いません。

- ルールセットを更新した事でコンプライアンス違反が解消された事を確認する

```
PowerCLI C:¥Upgrade_vib> $tr=Test-DeployRuleSetCompliance 10.3.253.91
```

```
PowerCLI C:¥Upgrade_vib> $tr.ItemList
```

3. Master サーバのセットアップ②（DSVA 有効化によるパラメータ変更）

※黄色枠線内が変更対象





ここでは F.D のインストール及び DSVA 有効化によるパラメータ変更を行います。また、変更されたパラメータを Master サーバの Host Profile に反映させます。

3-1 Master サーバを再起動させ、ホストへの F.D の適応を行う。

DSM 管理画面より、F.D や vSE が正常に認識されている事を確認する。

下記のように表示されない場合は、DSM の管理画面より、vCenter との同期「今すぐ同期」を実行し、ステータスを再度確認してください。

	 ESX	Guests:
Status:	 Prepared	
ESX Version:	5.5.0	
Filter Driver Version:	9.0.0.3500	
vShield Endpoint:	Installed	

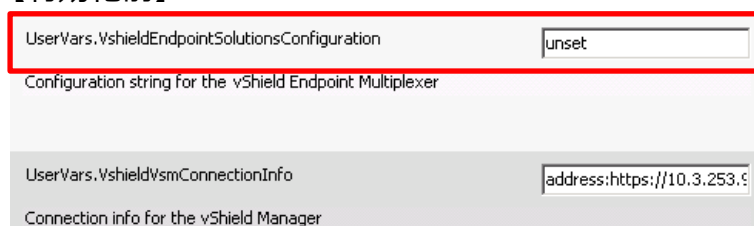
3-2 DSVVA の配信及び有効化を行い、パラメータの変更を行う。

※DSVA の配信及び有効化手順に関しては「1-7.関連資料」の「参考：Deep Security Virtual Appliance インストール手順」を参照下さい。

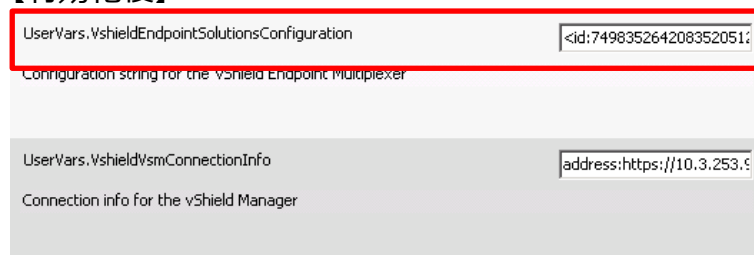
DSVA が有効化された事により ESXi に対して下記パラメータが付与されるので、Master サーバの Host Profile の Update を行う。

- UserVars.VshieldEndpointSolutionsConfiguration

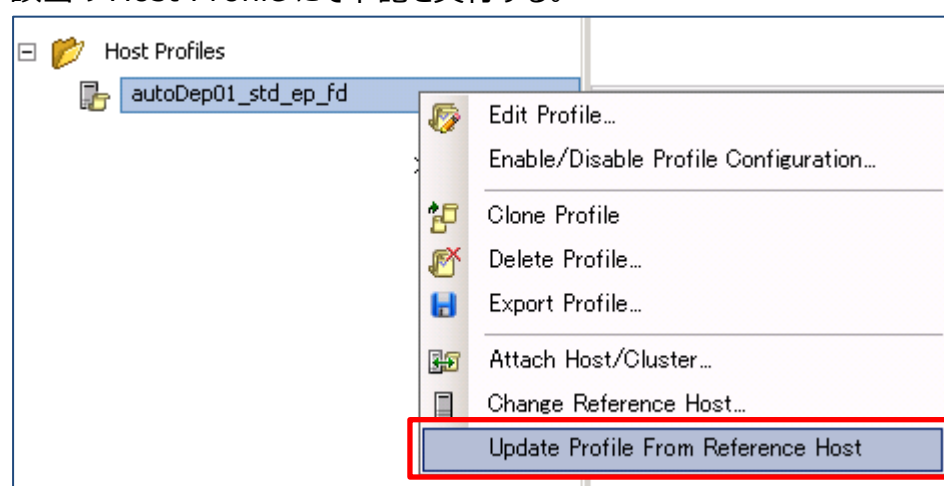
【有効化前】



【有効化後】



該当の Host Profile にて下記を実行する。



■「エンジンがオフライン」が発生する場合



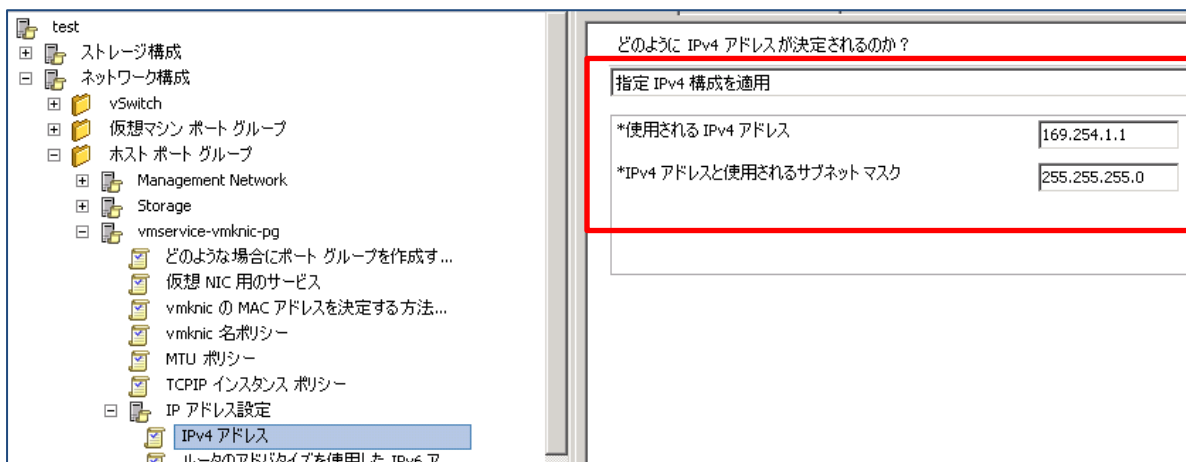
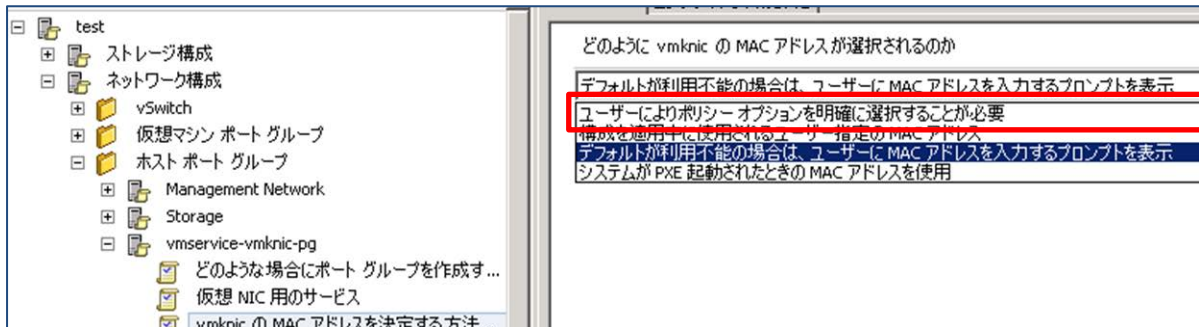
DSVA を有効化した際に保護対象 VM や DSVA の Firewallと IDS/IPSにて「エンジンがオフライン」と表示される場合があります。その場合は「第 4 章 Tips 集」にある下記対処法を実施してください。

【4-3. 「エンジンがオフライン」が発生する場合】

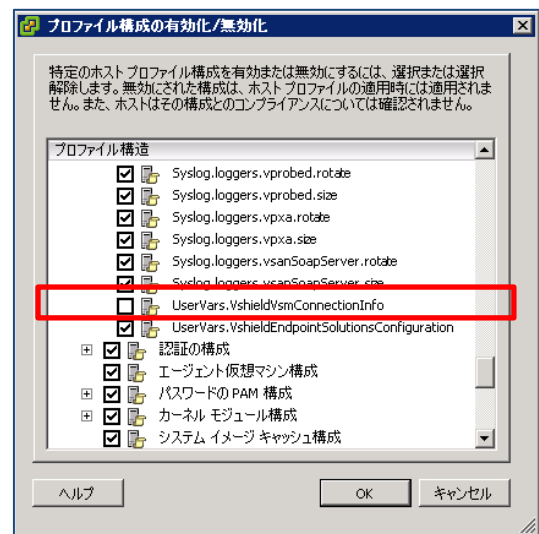
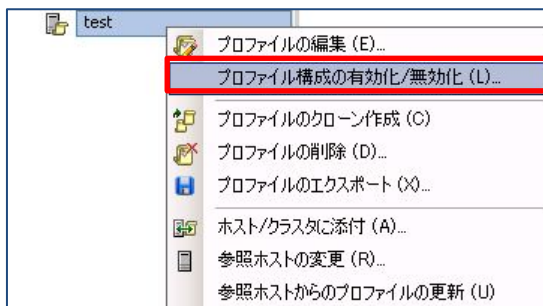
3-3 Host Profile の編集作業を再度行う。

「1-2.2」、「1-2.3」で行った下記設定作業を再度実施する。

● 「1-2.2 Host Profile の編集① - Host Profile の自動適応のため」



● 「1-2.3 Host Profile の編集② - パラメータの無効化」



■ DSVA の動作確認

ここでの動作確認は必須ではありませんが、Auto Deploy 後の問題発生時切り分けの為に実施する事をお勧めいたします。

3-4 Victim の構築を行う。

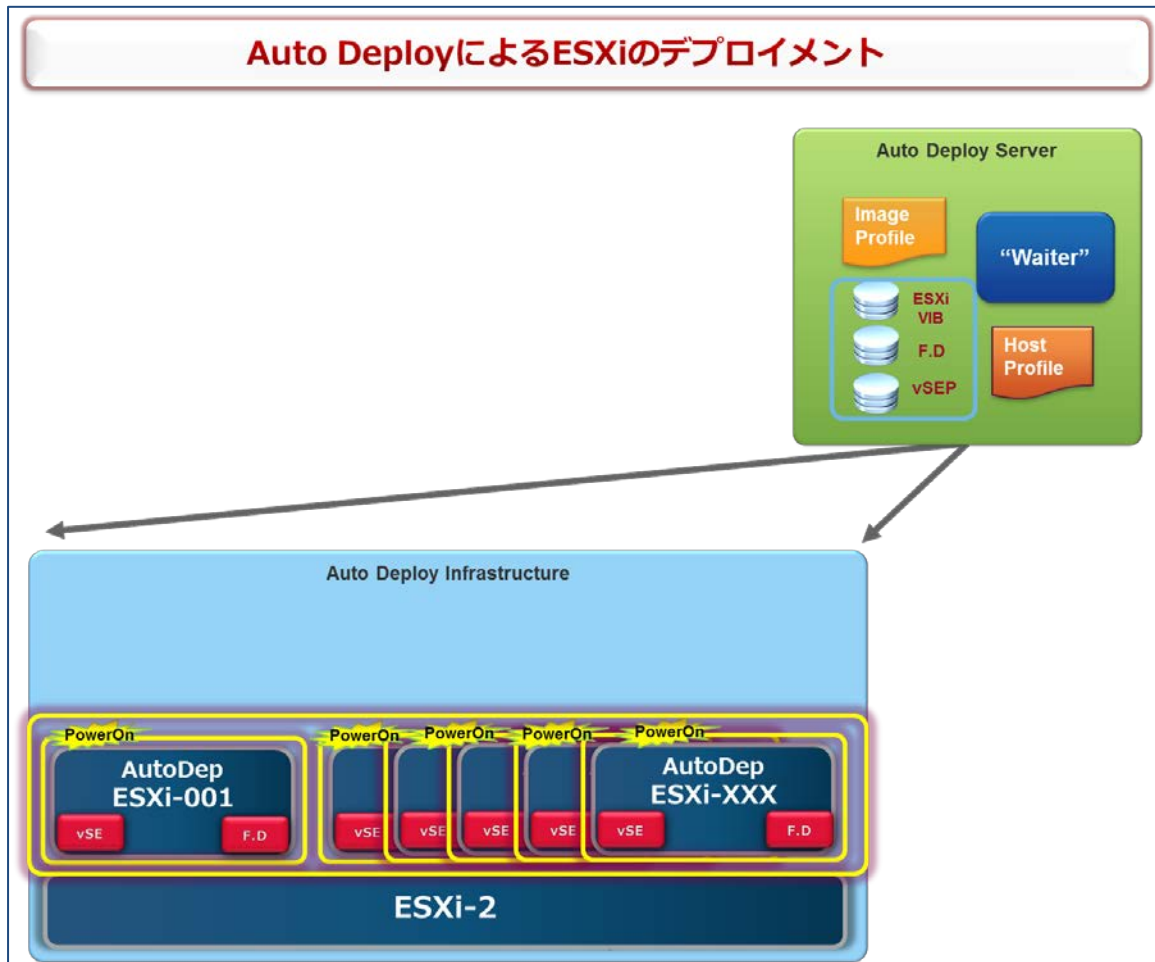
Victim の構築に関しては特別な要件はありませんので、通常通りの OS セットアップを実施してください。

3-5 DSVA の動作確認を行う。

- A.V が正常に機能しているか
 - テスト用ファイル EICAR を使用する
<http://downloadcenter.trendmicro.com/index.php?regs=jp&prodid=1424>
- Firewall が正常に機能しているか
- IDS/IPS が正常に機能しているか
 - 侵入防御の動作確認方法
<http://esupport.trendmicro.com/solution/ja-JP/1097204.aspx>

4. Auto Deploy による ESXi のデプロイメント

※黄色枠線内が変更対象



1 ～ 3 にて Auto Deploy を実行するための Host Profile 及びイメージファイルの準備が完了致しました。

ここからは Auto Deploy を使用して ESXi のデプロイを行っていきます。

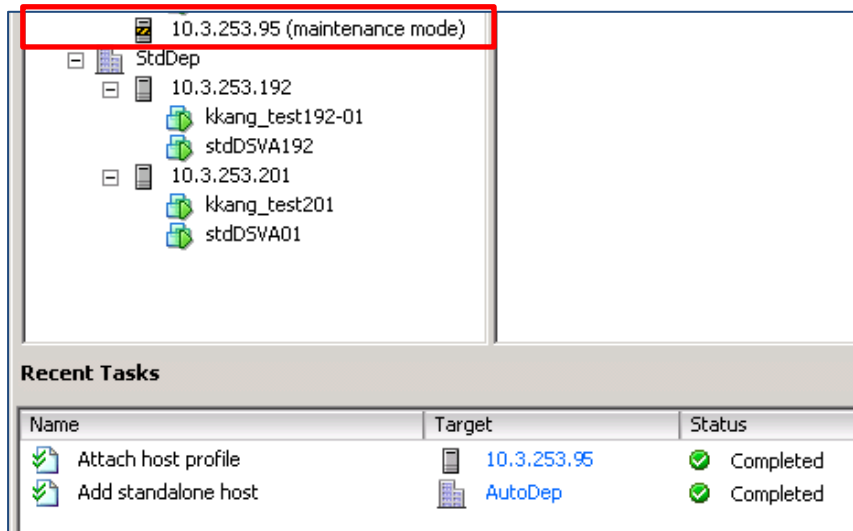
以下の手順では確認事項を記載させていただいてますが、基本的には、Auto Deploy にてホストを起動した後に、DSVA を配信するだけで新規ホストのセットアップは完了です。

4-1 ESXi を PowerON し、ESXi のデプロイを開始する。

4-2 ESXi の設定確認を行う。

もし ESXi がメンテナンスモードで起動している場合は、Host Profile の適用を手動で実施し、メンテナンスモードを解除をする。

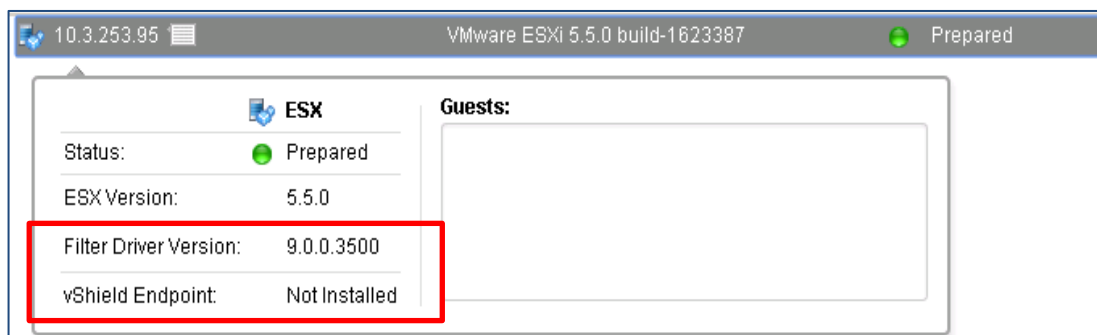
※メンテナンスモードを解除しないと、vSM と ESXi 間で通信が出来ず、vSE の状態が確認出来ないため。



4-3 DSM の管理画面から F.D や vSE が正常にインストールされているかを確認

補足 : DSM の管理画面を見ると、F.D は認識されているが、vSE が DSM から正常に認識されていない(Not Installed)。

これは Auto Deploy した vSE が vSM に登録されるまでに多少の時間を要しているか、または vSE の登録が vSM に対して正常に行えていない可能性があります。

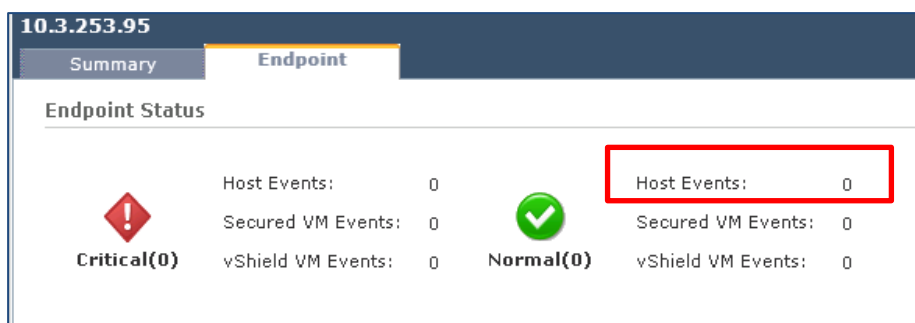


vSM 管理画面の「Summary」タブを見ると表示上は vSE が正常に認識されているように見える。



Service	Installed	Available	
vShield App	Not installed	5.5.0-1620248	Not licensed
vShield Endpoint	5.1.0-01255202	-	Uninstall
vShield Data Security	Not installed	5.1.0.0-833296	Not licensed

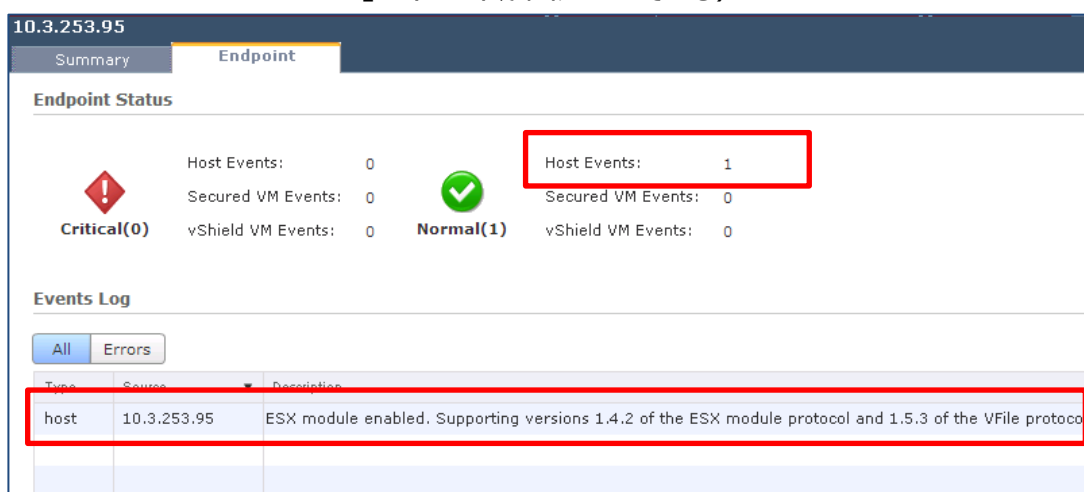
しかし、「Endpoint」タブを見ると vSM から ESXi が正常に認識されていない。Host Events が「0」のまま。



Host Events:	Secured VM Events:	vShield VM Events:
0	0	0

Overall Status: **Critical(0)**

「更新」を何度か実行後、vSM の管理画面を確認すると、ESXi が正常に認識される場合がある。（Host Events が「1」となり、下段 Events Log に「ESX module enabled」のイベントが出力されている）

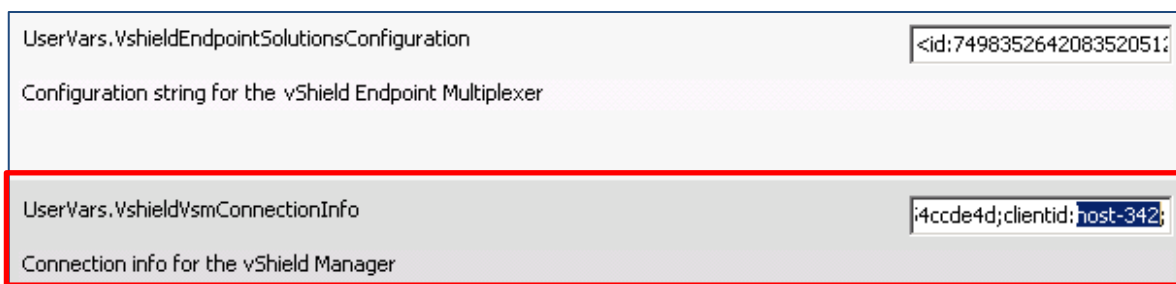


Host Events:	Secured VM Events:	vShield VM Events:
1	0	0

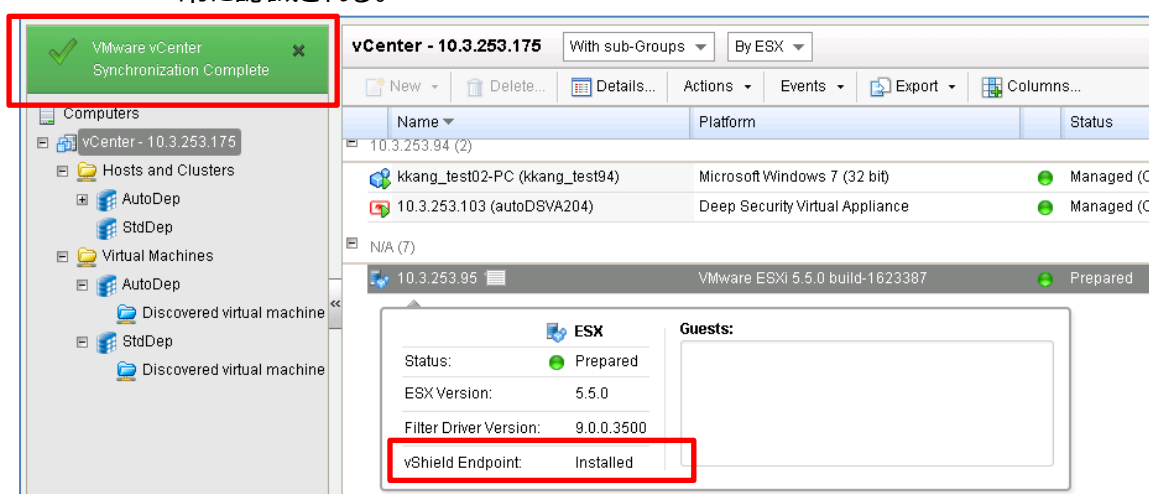
Overall Status: **Normal(1)**

Type	Source	Description
host	10.3.253.95	ESX module enabled. Supporting versions 1.4.2 of the ESX module protocol and 1.5.3 of the VFile protocol.

ESXiの詳細設定値も Host Profile の値ではなく、ホスト固有の値が設定されている。



その後、DSMの管理画面から「今すぐ同期」を実行すると DSM から vSE が正常に認識される。



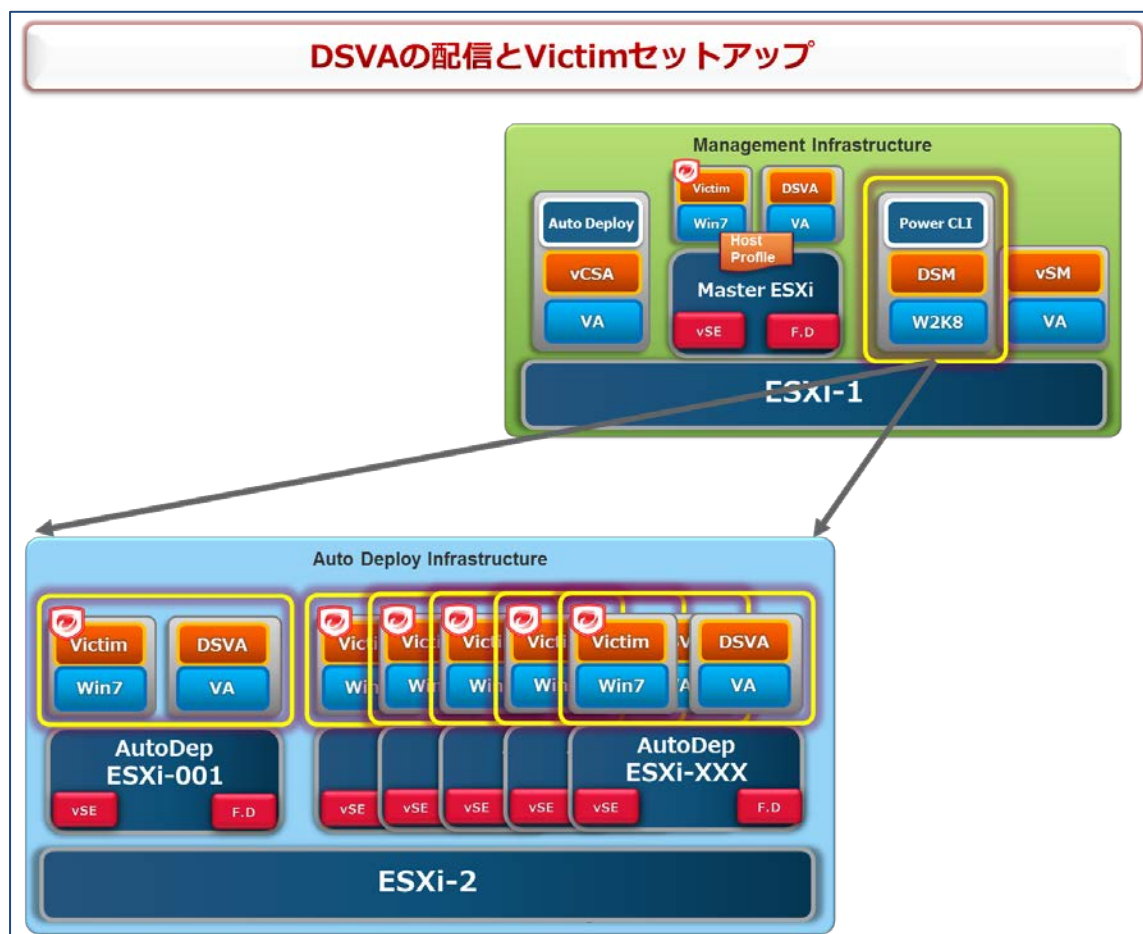
■ 上記を実施しても vSE が認識されない場合

上記を行っても vSE が認識されない場合は、「第 4 章 Tips 集」にある下記対処法を実施してください。

【4-4. vShield Endpoint が認識されない場合】

5. DSVA の配信と Victim のセットアップ

※黄色枠線内が変更対象



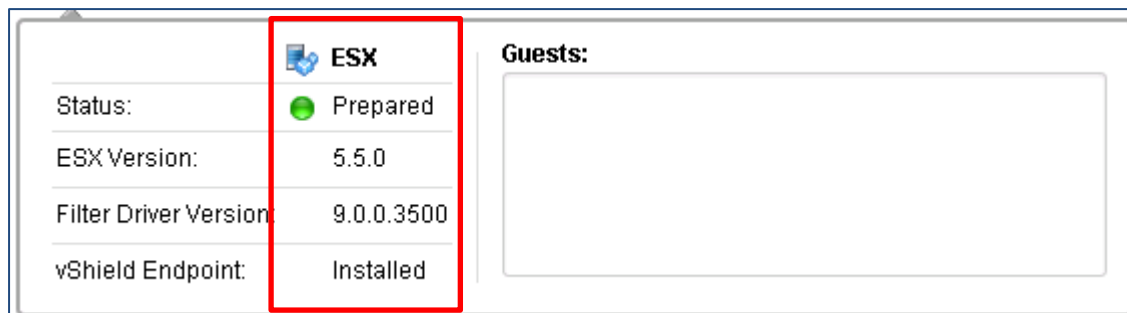
ここでは DSM から各 ESXi に対して DSVA の配信及びセットアップを行う。また動作確認として使用する Victim のセットアップもあわせて実施する。

※DSVA の配信手順に関しては「1-7.関連資料」の「参考：Deep Security Virtual Appliance インストール手順」を参照下さい。

Victim の構築に関しては特別な要件はありませんので、通常通りの OS セットアップを実施してください。

セットアップ完了後、DSM 管理画面より、F.D や vSE が正常に認識されている事を確認する。

下記のように表示されない場合は、DSM の管理画面より、vCenter との同期「今すぐ同期」を実行し、ステータスを再度確認してください。



■「エンジンがオフライン」が発生する場合



DSVA を有効化した際に保護対象 VM や DSVA の Firewallと IDS/IPSにてや「エンジンがオフライン」と表示される場合があります。

その場合は「第 4 章 Tips 集」にある下記対処法を実施してください。

【4-3. 「エンジンがオフライン」が発生する場合】

6. 動作確認



ここでは Deep Security の動作確認を行います。

6-1 下記機能についての動作確認を行う。

- A.V が正常に機能しているか
 - テスト用ファイル EICAR を使用する
<http://downloadcenter.trendmicro.com/index.php?regs=jp&prodid=1424>
- Firewall が正常に機能しているか
- IDS/IPS が正常に機能しているか
 - 侵入防御の動作確認方法
<http://esupport.trendmicro.com/solution/ja-JP/1097204.aspx>

第4章 Tips 集

4-1. システムアップグレード時の Auto Deploy 手順

ESXi5.5U1 をサポートするにあたり、トレンドマイクロの各コンポーネントには DS9.0 SP1 **Patch3**を適用する必要があります。

本セクションでは、ESXi5.5、DSM9.0SP1Patch2 の環境から ESXi5.5**U1**及び DSM9.0SP1**Patch3**へ各コンポーネントをアップグレードする際の注意事項や作業手順を記載しております。

各コンポーネントのバージョンに関しては下記表を参照ください。また、システム構成に関しては、第3章の「最終構成」からの作業を想定しております。

※以降の作業手順に関しては必要事項のみを記載しておりますので、詳細は各種ベンダー資料をご参照下さい。

Upgrade Order	Product	Before	After	Memo
1	DSM	9.0SP1Patch2 (9.0.6019)	9.0SP1Patch3 (9.0.6500)	
2	DSVA	9.0SP1Patch2 (9.0.0-3044)	9.0SP1Patch3 (9.0.0-3500)	
3	vSM	5.5.0a (1473628)	5.5.2	
4	ESXi	5.5.0 (1331820)	5.5.0U1 (1623387)	Auto Deploy にてアップグレード
	vSE	5.1.0 (01255202)	変更なし (vSM に含まれている vSE の Version に変更が 無いため)	Auto Deploy にてアップグレード
	F.D	9.0SP1Patch2 (9.0.0-2636)	9.0SP1Patch3 (9.0.0-3500)	Auto Deploy にてアップグレード

1. DSM のアップグレードを行う

DSM アップグレード後に、DSM 管理画面の ESXi にて Upgrade を推奨する記載が表示されますが ESXi のアップグレード後に表示は消えますので特に問題ございません。

【アップグレード前】



【アップグレード後】



2. DSVA のアップグレードを行う

※DSVA の再起動が発生致します。

- I. DSVA 以外の仮想マシンを作業対象外の ESXi へ退避させる。
DSVA のアップグレード中は仮想マシンに対する保護が継続されませんので、作業対象 ESXi には仮想マシンが vMotion されないようにして下さい。
- II. DSM からアップグレード用の DSVA イメージを配信し、DSVA がアップグレードされている事を確認する。

3. vSM のアップグレードを行う

※vSM の再起動が発生致します。

vShield Manager を一時的に停止する必要がある場合、設定変更や有効化 (再有効化)、vMotion 等で仮想マシンを他の ESX ホストに移動するような操作を行わない時間帯での実施を検討してください。

■ vShield Manager の必要性(停止/稼働)について

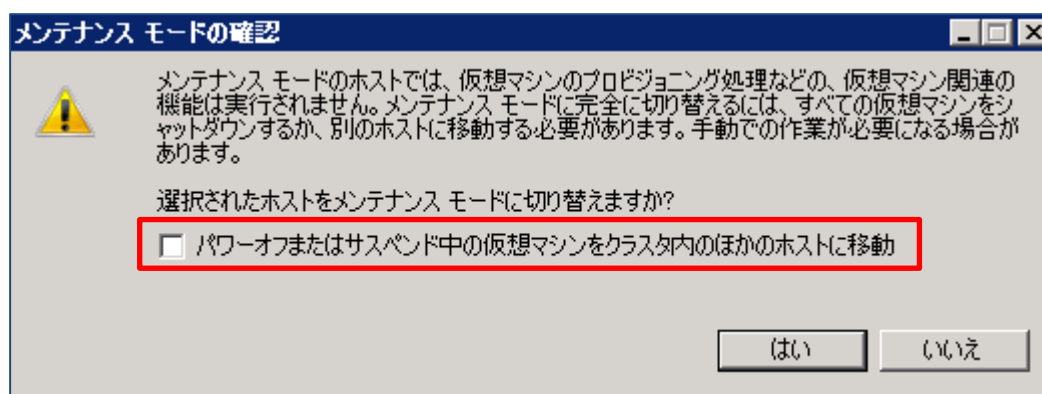
<http://esupport.trendmicro.com/solution/ja-JP/1097016.aspx>

4. ESXi のアップグレードを行う

※Master 用 Host Profile (autoDep01_std_ep_fd) は前項作業で作成したものを使用します。

I. ESXi をメンテナンスモードにする (メンテナンスモードにすると DSVA は自動的に PowerOff されます)

この時、PowerOff された DSVA が他の ESXi へ移動されないように下記チェックボックスを外す。



II. アップグレード用のインストールイメージや Auto Deploy ルールの作成を行う

① vSE は下記より Download しておく。

[https://vSM IP Address/offline-bundles/vShield-Endpoint-Mux.zip](https://vSM_IP_Address/offline-bundles/vShield-Endpoint-Mux.zip)
ダウンロードしたファイルを解凍すると「esx55」というフォルダがあるので、その中にある「vShield-Endpoint-Mux.zip」を使用する。ここではファイル名を下記に変更しております。

- vShield-Endpoint-Mux.esx55.zip

② ESXi の Update1 VIB ファイル及び F.D の Upgrade ファイルを各社のページから Download しておく。

1. update-from-esxi5.5-5.5_update01.zip
2. FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip

③ PowerCLI を使用して、インストール用イメージやルールの作成を行う。

【EsxSoftwareDepot ハイメージを追加する】

- インストール用ファイルが配置されているフォルダにて下記コマンドを実行する

```
PowerCLI C:¥ Upgrade_vib> dir
```

```
-a---      2014/06/24      5:22   227804      FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip
-a---      2014/03/20      11:12  654389915   update-from-esxi5.5-5.5_update01.zip
-a---      2013/08/01      14:59   125863      vShield-Endpoint-Mux.esx55.zip
```

- EsxSoftwareDepot にインストール用ファイルを追加していく

```
PowerCLI C:¥ Upgrade_vib> Add-EsxSoftwareDepot .¥vShield-Endpoint-Mux.esx55.zip
Depot Url
```

```
-----
```

```
zip:C:¥Upgrade_vib¥vShield-Endpoint-Mux.esx55.zip?index.xml
```

```
PowerCLI C:¥Upgrade_vib> Add-EsxSoftwareDepot FilterDriver-ESX_5.0-9.0.0-3500.x86_64.
zip
```

```
Depot Url
```

```
-----
```

```
zip:C:¥Upgrade_vib¥FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip?index.xml
```

- 正常にファイルが追加されたことを確認する

```
PowerCLI C:¥Upgrade_vib> Get-EsxSoftwareDepot
```

```
Depot Url
```

```
-----
```

```
zip:C:¥Upgrade_vib¥vShield-Endpoint-Mux.esx55.zip?index.xml
```

```
zip:C:¥Upgrade_vib¥FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip?index.xml
```

```
PowerCLI C:¥Upgrade_vib> Get-EsxSoftwarePackage
```

Name	Version	Vendor	Creation Date
-----	-----	-----	-----
dvfilter-dsa	9.0.0-3500	Trend	2014/05/12 15...
epsec-mux	5.1.0-01255202	VMware	2013/08/01 21...

■最後に ESXi の Update1 ファイルを追加する

```
PowerCLI C:¥ Upgrade_vib> Add-EsxSoftwareDepot update-from-esxi5.5-5.5_update01.zip
Depot Url
-----
zip:C:¥ Upgrade_vib¥update-from-esxi5.5-5.5_update01.zip?index.xml

PowerCLI C:¥Upgrade_vib> Get-EsxSoftwareDepot
Depot Url
-----
zip:C:¥Upgrade_vib¥vShield-Endpoint-Mux.esx55.zip?index.xml
zip:C:¥Upgrade_vib¥FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip?index.xml
zip:C:¥Upgrade_vib¥update-from-esxi5.5-5.5_update01.zip?index.xml
```

【イメージプロファイルの作成を行う】

```
PowerCLI C:¥Upgrade_vib> $ip=Get-EsxImageProfile
PowerCLI C:¥Upgrade_vib> $ip | select Name
```

```
Name
----
ESXi-5.5.0-20140302001-no-tools
ESXi-5.5.0-20140301001s-no-tools
ESXi-5.5.0-20140301001s-standard
ESXi-5.5.0-20140302001-standard
```

■既存のイメージプロファイルを複製し、今回使用するイメージプロファイルを作成する

```
PowerCLI C:¥ Upgrade_vib> New-EsxImageProfile -CloneProfile $ip[3] -name ESXi5.5.0u1_v
SE_FD
```

コマンド パイプライン位置 1 のコマンドレット New-EsxImageProfile

次のパラメーターに値を指定してください:

(ヘルプを表示するには、「!?」と入力してください。)

Vendor: VMware

Name	Vendor	Last Modified	Acceptance Level
ESXi5.5.0u1_vSE_FD	VMware	2014/02/22 2...	PartnerSupported

- 複製したイメージプロファイルに VMware の vSE と Trend Micro の DriverVIB (Filter Driver) を追加する

```
PowerCLI C:¥Upgrade_vib> Add-EsxSoftwarePackage -ImageProfile ESXi5.5.0u1_vSE_FD -SoftwarePackage epsec-mux, dvfilter-dsa
```

Name	Vendor	Last Modified	Acceptance Level
ESXi5.5.0u1_vSE_FD	VMware	2014/06/24 1...	PartnerSupported

【イメージプロファイルのエクスポートを行う】

- 作成したイメージプロファイルを Depot ファイルとしてエクスポートしておく

(今までの作業は PowerCLI に保存されているわけではないので、エクスポートせずに PowerCLI を終了した場合は再度同作業を実施する必要があるため)

```
PowerCLI C:¥Upgrade_vib> Export-EsxImageProfile -ImageProfile ESXi5.5.0u1_vSE_FD -ExportToBundle -FilePath C:¥Upgrade_vib¥My-ESXi5.5.0u1_vSE_FD.zip
```

```
PowerCLI C:¥Upgrade_vib> dir
```

ディレクトリ: C:¥Upgrade_vib

Mode	LastWriteTime	Length	Name
d----	2014/06/24 14:33		original
-a---	2014/06/24 5:22	227804	FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip
-a---	2014/06/24 15:34	333776738	My-ESXi5.5.0u1_vSE_FD.zip
-a---	2014/03/20 11:12	654389915	update-from-esxi5.5-5.5_update01.zip
-a---	2013/08/01 14:59	125863	vShield-Endpoint-Mux.esx55.zip

【ルールの作成を行う】

■ vCenter へ接続する

```
PowerCLI C:¥Upgrade_vib> Connect-VIServer "vCenter IP Address"
```

```
Name          Port  User
----          -
IP Address    443  root
```

```
PowerCLI C:¥Upgrade_vib> $ip=Get-EsxImageProfile
```

```
PowerCLI C:¥Upgrade_vib> $ip | select name
```

```
Name
----
ESXi-5.5.0-20140302001-no-tools
ESXi5.5.0u1_vSE_FD
ESXi-5.5.0-20140301001s-no-tools
ESXi-5.5.0-20140301001s-standard
ESXi-5.5.0-20140302001-standard
```

■ ルール : My-ESXi5.5.0u1_vSE_FD_rule を作成する

補足 : ここでは ESXi が追加されるインベントリをクラスタ配下ではなく、Datacenter 配下にしてあります。DSVA の動作確認時に、DRS により作業対象の ESXi へ仮想マシンが vMotion されるのを防ぐ為となります。

また、オプションに「-allhosts」を指定しておりますが、「-Pattern」にて MAC アドレス指定に変更する事も可能です。

こちらに関しては実環境にあわせた設定をお願い致します。

```
PowerCLI C:¥Upgrade_vib> New-DeployRule -name My-ESXi5.5.0u1_vSE_FD_rule -Item $ip
[1], (Get-VMHostProfile autoDep01_std_ep_fd), (Get-Datacenter AutoDep) -allhosts
```

```
Downloading dvfilter-dsa 9.0.0-3500
```

```
Download finished, uploading to AutoDeploy...
```

```
Upload finished.
```

```
Warning: Image Profile ESXi5.5.0u1_vSE_FD contains one or more software packages that are not state
less-ready. You may experience problems when using this profile with Auto Deploy
```

```
Name      : My-ESXi5.5.0u1_vSE_FD_rule
```

```
PatternList :
```

```
ItemList  : {ESXi5.5.0u1_vSE_FD, AutoDep, autoDep01_std_ep_fd}
```

■ ルールセットにルールを追加する（作成したルールが 1 番上に登録される事を確認）

```
PowerCLI C:¥Upgrade_vib> Add-DeployRule -DeployRule My-ESXi5.5.0u1_vSE_FD_rule -at 0
```

```
Name      : My-ESXi5.5.0u1_vSE_FD_rule
```

```
PatternList :
```

```
ItemList   : {ESXi5.5.0u1_vSE_FD, AutoDep, autoDep01_std_ep_fd}
```

```
Name      : 5.5u1_std_ep_fd
```

```
PatternList : {mac=00:50:56:b1:2f:7c}
```

```
ItemList   : {5.5u1_ep_fd, AutoDep, autoDep01_std_ep_fd}
```

```
Name      : std_ep_fd
```

```
PatternList : {mac=00:50:56:b1:2f:6e, mac=00:50:56:b1:2f:72, mac=00:50:56:b1:2f:7c, mac=00:50:56:b1:44:5f}
```

```
ItemList   : {esxi5.5.0_endpoint_filterdriver, AutoDep, autoDep01_std_ep_fd}
```

■ コンプライアンス違反か否かを確認する

```
PowerCLI C:¥Upgrade_vib> $tr=Test-DeployRuleSetCompliance 10.3.253.91
```

```
PowerCLI C:¥Upgrade_vib> $tr.ItemList
```

CurrentItem	ExpectedItem
-----	-----
esxi5.5.0_endpoint_filterdriver	ESXi5.5.0u1_vSE_FD

■ Auto Deploy サーバ上のルール及びルールセットの更新を行う

```
PowerCLI C:¥Upgrade_vib> Repair-DeployRuleSetCompliance $tr
```

```
Warning: Image Profile esxi5.5.0_endpoint_filterdriver contains one or more software packages that are not stateless-ready. You may experience problems when using this profile with Auto Deploy.
```

```
Warning: Image Profile ESXi5.5.0u1_vSE_FD contains one or more software packages that are not stateless-ready. You may experience problems when using this profile with Auto Deploy
```

■ ルールセットを更新した事でコンプライアンス違反が解消された事を確認する

```
PowerCLI C:¥Upgrade_vib> $tr=Test-DeployRuleSetCompliance 10.3.253.91
```

```
PowerCLI C:¥Upgrade_vib> $tr.ItemList
```

- I. 対象サーバを再起動し、インストールが正常に完了した事を確認する。また Update1 にアップグレードされている事を確認する。

※応答ファイルが用意されている場合、ESXi 再起動後はメンテナンスモードが自動で解除され、HA により DSVa も自動で PowerON されます。

- II. vSM にて vSE や DSVa が正常に登録されているか確認を行う。

vSM にて「更新」を実行しても DSVa が正常に表示されない場合があります。下記のように「Summary」タブでは DSVa が表示されていても「Endpoint」タブでは DSVa が表示されていない場合があります。

その場合は、10～20 分経過すると vSM に DSVa の表示が現れますので、先に下記手順を進めて下さい。

10.3.253.91 You are logged in as a System Administrator Logged

Summary Endpoint

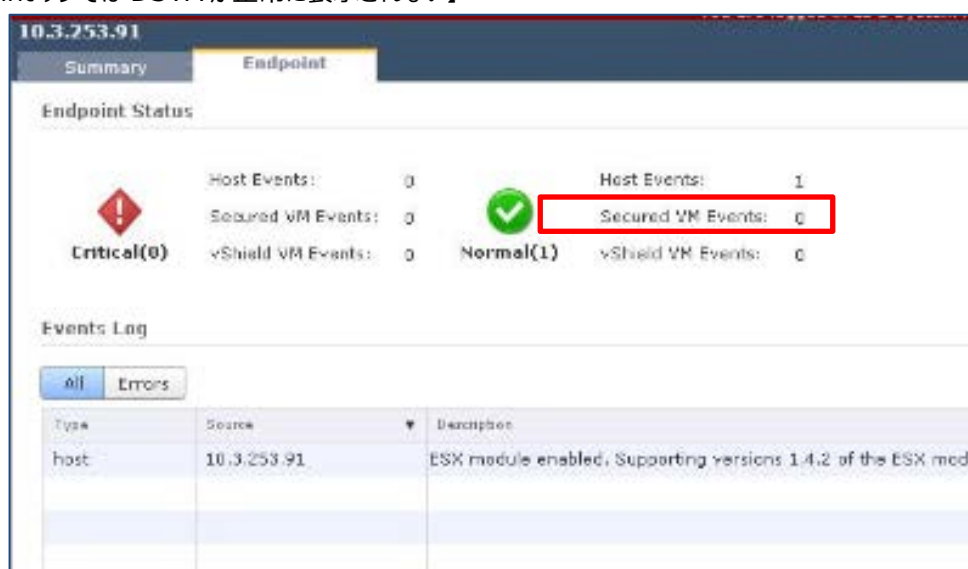
vShield Host Preparation Status for 10.3.253.91

Service	Installed	Available	
vShield App	Not installed	5.5.0-1620248	Not licensed ⓘ
vShield Endpoint	5.1.0-01255202	-	Uninstall ⓘ
vShield Data Security	Not installed	5.1.0.0-833296	Not licensed ⓘ

Service Virtual Machines

Name	Type
autoDSVA01	vShield Endpoint Active SVM

【Endpoint タブでは DSVA が正常に表示されない】



■ 上記を実施しても vSE が認識されない場合

上記を行っても vSE が認識されない場合は、「第 4 章 Tips 集」にある下記対処法を実施してください。

【4-4. vShield Endpoint が認識されない場合】

III. DSM の管理画面から F.D がアップグレードされている事を確認する。

5. 動作確認を行う

Victim を ESXi 上に vMotion させ、A.V、Firewall、IDS/IPS が正常に機能しているか確認する。

- A.V が正常に機能しているか
 - テスト用ファイル EICAR を使用する
<http://downloadcenter.trendmicro.com/index.php?regs=jp&prodid=1424>
- Firewall が正常に機能しているか
- IDS/IPS が正常に機能しているか
 - 侵入防御の動作確認方法
<http://esupport.trendmicro.com/solution/ja-JP/1097204.aspx>

6. ESXi を HA クラスタへ戻し、サービスの提供を行う。

4-2. ヒープメモリサイズの設定変更をデプロイ時に組み込む

DSVA を運用していくうえで考慮すべきパラメータ項目の一つとして、F.D のヒープメモリサイズがあります。

通常、この設定値を変更する場合 ESXi に SSH でログインし、複数のコマンドを実行後に ESXi の再起動を行う必要がございます。

Auto Deploy を利用した場合、Master となる Host Profile の項目に設定値を記載する事で、ESXi のデプロイ後には既に設定値が反映された状態で ESXi が起動します。

故に、設定値を有効化するための再起動運用が不要となります。

尚、ヒープメモリサイズの算出方法に関しては関連資料の「Trend Micro Filter Driver のヒープメモリサイズ設定資料」を参照下さい。

■ Host Profile 内のヒープメモリサイズ設定箇所

「Advanced configuration option」

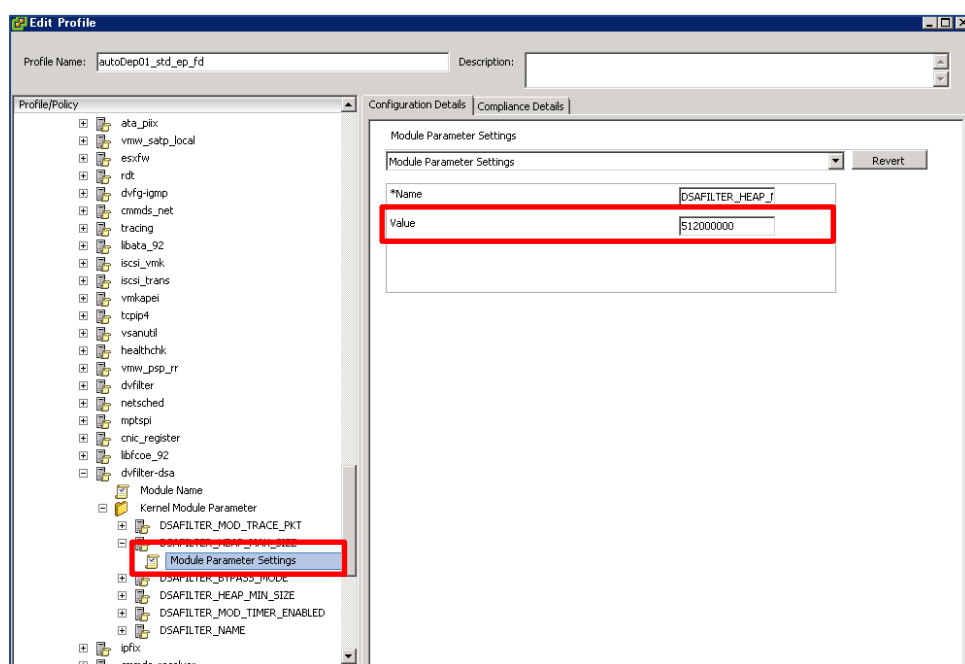
⇒ 「Kernel Module Configuration」

⇒ 「Kernel Module」⇒「dfilter-dsa」

⇒ 「Kernel Module Parameter」

⇒ 「DSAFILTER_HEAP_MAX_SIZE」

⇒ 「Module Parameter Settings」



4-3. 「エンジンがオフライン」が発生する場合

DVFilter が使用するポート「2222」が Listen 出来ていない場合、上記エラーが発生する事があります。

DVFilter に設定した IP Address の再設定を行い、ポートが Listen 出来ているか確認をします。

1. 対象の ESXi に対して PowerCLI を使用して設定変更を行います。

```

■ DVFilter が使用するポートが Listen していない事を確認する
# esxcli network ip connection list | grep 2222

■ DVFilter の IP Address をリセットする
# esxcfg-advcfg -d /Net/DVFilterBindIpAddress
DVFilterBindIpAddress reset to default

# esxcfg-advcfg -g /Net/DVfilterBindIpAddress
Value of DVFilterBindIpAddress is

■ DVFilter に Bind させる IP (169.254.1.1) を設定する
# esxcfg-advcfg -s 169.254.1.1 /Net/DVfilterBindIpAddress
Value of DVFilterBindIpAddress is 169.254.1.1

■ 正常に IP Address が Bind された事を確認する
# esxcfg-advcfg -g /Net/DVfilterBindIpAddress
Value of DVFilterBindIpAddress is 169.254.1.1

■ DVFilter が使用するポートも Listen した事を確認する
# esxcli network ip connection list | grep 2222
tcp      0      0 0.0.0.0:2222      0.0.0.0:0      LISTEN   33173 newreno

```

2. DSVA と VM のステータスを確認

Appliance	
Status:	Managed (Online)
Online:	Yes
Last Communication:	July 6, 2014 08:44
Appliance Version:	9.0.0.3500
vShield Endpoint:	Registered

Protected Guests On: 10.3.253.225

kkangtest93-01 (kkang_test93-01)

Check Status Clear Warnings/Errors

DSVA と VM のステータスを実行し、エラーが解消されている事を確認する。
上記で解消されない場合は、DAVA の再起動を実施し再度ステータス確認をする。

4-4. vShield Endpoint が認識されない場合

vSE が正常に認識されない場合は、vSE の Uninstall & Install を実施してください。

vSM の管理画面から vSE の「Uninstall」⇒「Install」を実行後、DSM の管理画面から「今すぐ同期」を実行すると、vSE が正常に認識されます。



10.3.253.91 You are logged in as a System Administrator Logged

Summary Endpoint

vShield Host Preparation Status for 10.3.253.91

Service	Installed	Available	
vShield App	Not installed	5.5.0-1620248	Not licensed
vShield Endpoint	5.1.0-01255202	-	Uninstall
vShield Data Security	Not installed	5.1.0.0-833296	Not licensed