

## Trend Micro Deep Security<sup>™</sup> 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, h 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 リーンナップサービス、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.

## 改訂履歴

<b>Revision No</b>	Date	Change	Author
1.0	2014/07/08	初版	姜(かん)
1.1	2014/07/29	文言及びリンクの修正	姜
1.2	2014/09/09	vShieldEndpointのDLリンク修正	姜

## 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1	1
第3章	導入手順1	3
3-1.	全体構成図1	3
3-2.	全体の流れ1	4
3-3.	導入作業1	5
第4章	Tips 集4	0
4-1.	システムアップグレード時の Auto Deploy 手順4	0
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5	0
4-3.	「エンジンがオフライン」が発生する場合5	1
4-4.	vShield Endpoint が認識されない場合5	3

# 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 Security9.0SP1 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は動作確認が出来ておらず、正式サポートとなっておりません。

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

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 <<u>http://esupport.trendmicro.com/solution/ja-JP/1097198.aspx</u>> 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 <<u>http://esupport.trendmicro.com/ja-jp/enterprise/ds/top.aspx</u>>

参考: Deep Security Virtual Appliance 9.0 トラブルシューティングガイド <<u>http://files.trendmicro.com/jp/ucmodule/tmds/90SP1/DSVA\_9.0TroubleshootingTips\_exte</u> <u>rnal\_r1.pdf</u>>

# 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	製品	バージョン	備考
VMware			
	VMware vSphere Hypervisor	ESXi5.5U1	※Auto Deploy を使用
		(1623387)	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	5.5.0.b	vCSA で vCenter を構
	Appliance	(1476389)	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	9.0SP1Patch3	
	Manager	(9.0.6500)	
	Trend Micro Deep Security	9.0SP1Patch3	
	Virtual Appliance	(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おりません。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
- 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. DSVA 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 となる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。

G	eneral Endpoint					
	vShield Host Preparatio	on Status for 10.3.	253.91			
					Last upda	tec
	Service	Installed	Available			
	vShield App	Not installed	5.5.0-1447281	Not licensed	2	
	vShield Endpoint	5.1.0-01255202	-	Uninstall	2	
	vShield Data Security	Not installed	5.1.0.0-833296	Not licensed	2	
Γ						

 vmservice-vswitch が作成され、vmservice-vshield-pg、vmservicevmknic-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 vmservice-vswitch に対し、DSVA 用の PortGroup を作成する。

ポートグループ名:「vmservice-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

Idvanced Settings		
Annotations	Piint. 0 Piidx. 00	
BufferCache CBRC	Net.CoalesceTxTimeout	4000
Config	Set the coalesce time-out in microseconds	
vpx COW	Min: 1 Max: 4294967295	
Cpu DataMover	Net.CoalesceVersion	
DCUI Digest	Set the coalesce version.	
DirentryCache	Min: 1 Max: 2	
FSS	Net.DCBEnable	
HBR	Enable DCB for FCoE	
Irq LPage	Min: 0 Max: 1	
Mem Migrate	Net.DVFilterBindIoAddress	169 254 1 1
Misc Net	DVFilter internal communication endpoint	10,23,111
NFS Nmp		
Numa PageRetire	Net.DVFilterPriorityRdLockEnable	1
Power DdmEiltor	Use priority locking in dvfilter to read lock portsets	,
ScratchConfig	Min: 0 Max: 1	
Scsi SunRPC	Net.DVSLargeHeapMaxSize	80
SvMotion Svslog	Max size for the dvsLargeHeap	,

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。

F IFE	ewall Properties					
ken	note Access					
By de	efault, remote clients are	prevented fro	om accessing services of	n this host, and local clients	are prevente	d from
acce	ssing services on remote	hosts.				
5eleo oner	ct a check box to provide bed and stop when all of I	: access to a si their norts are	ervice or client. Daemon . closed, or as configure:	is will start automatically wh d	en their ports	are
opoi			closed, or as configuro.			
	Label		Incoming Ports	Outgoing Ports	Protocols	Daemon 🔺
п	VCenter Lindate Manac	ier	1	80.9000-9100	TCP	N/A
H	NTP Client			123	UDP	Stopped
ቫ	NFC		902	902	TCP	N/A
	DHCPv6		546	547	TCP, UDP	N/A
븕	crimas		12045,20451	12040,20401	UDP	N/A
	DVFilter		2222	-	TCP	N/A
ā			57007		TCP	Chopped
	HBR			31031,44046	TCP	N/A
	rdt		2233	2233	TCP	N/A
	Fault Tolerance		8100,8200,8300	80,8100,8200,8300	TCP,UDP	N/A 🚽
<b>T</b>						
-Ser	rvice Properties					
<b>-</b>						
ье	neral					
s	ervice:	DVFilter				
Р	ackage Information:					
	actago in ormadorn					
rir	ewaii Settings					
A	llowed IP Addresses:	All				
						1
				Fire	ewall	Options

- 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 「<u>autoDep01\_std\_ep\_fd</u>」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」→「vmservice-vmknicpg」→「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

🔓 test	どのように 19v4 アドレス が決定されるのか?
田 🌇 ストレージ構成	COBOLC # (1) T P/(NPC/EC10B/ON) (
🖂 🔓 ネットワーク構成	指定 IPv4 構成を適用
🗄 📁 vSwitch	
🗉 📁 仮想マシン ポート グループ	*使用される IPv4 アドレス 169.254.1.1
□	
🛨 📴 Management Network	*IPv4 アドレスと使用されるサブネットマスク 255.255.255.0
표 📴 Storage	
Image: Second	
🧧 どのような場合にポート グループを作成す	
🧧 仮想 NIC 用のサービス	
🤦 vmknic の MAC アドレスを決定する方法…	
🤦 vmknic 名ポリシー	
🤦 MTU ポリシー	
🤦 TCPIP インスタンス ポリシー	
🖂 📴 IP アドレス設定	
IPv4 アドレス	
□ 1Lーねのアドバねイプを使用した IPv6 ア	

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。



ヘルプ

OK

キャンセル

## 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 ヘ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-EsxSoftwarePackageNameVersionVendorCreation Date-----------------dvfilter-dsa9.0.0-3500Trend2014/05/12 15...epsec-mux5.1.0-01255202VMware2013/08/01 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な	を複製し、今回修	吏用するイメージプロファ	イルを作成する	
PowerCLI C:¥ Upgrade_ SE_FD -vendor VMwar	_vib> New-Es e	sxImageProfile -Cl	oneProfile \$ip[3]	-name ESXi5.5.0u1_v
Name	Vendor	Last Modified	Acceptance Leve	21
ESXi5.5.0u1_vSE_FD	VMware	2014/02/22 2	PartnerSupporte	ed
■複製したイメージプロファイノ	ໄເວັ VMware Ø	vSEとTrend Micro	ののDriverVIB(F	ilter Driver)を追加する
PowerCLI C:¥Upgrade_	vib> Add-Es	SoftwarePackage	-ImageProfile ES	Xi5.5.0u1_vSE_FD -So
ftwarePackage epsec-m	ux, dvfilter-c	lsa		
Name	Vendor	Last Modified	Acceptance Level	
ESXi5.5.0u1_vSE_FD	VMwa	re 2014/06/	24 1 PartnerSu	ipported

#### 【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 -Exp ortToBundle -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	5 update-from-esxi5.5-5.5_update01.zip
-a	2013/08/01	14:59	125863	vShield-Endpoint-Mux.esx55.zip
【ルールの	D作成を行う】			
■vCente	er へ接続する			
PowerCL	I C:¥ Upgrade	_vib> Cor	nnect-VISer	ver "vCenter IP Address"
Name		Port Us	er	
IP Addre	ess	443 roo	Dt	
PowerCl	I C:¥l Ingrado	vih> ¢in-	-Cot-EsvIm	ageProfile
PowerCl	I C:¥Upgrade_	vih> \$ip-	l select nam	
Name				
ESXi-5.5	5.0-201403020	01-no-too	ols	
ESXi5.5.	0u1_vSE_FD			
ESXi-5.5	5.0-201403010	01s-no-to	ols	
ESXi-5.5	5.0-201403010	01s-stanc	lard	
ESXi-5.5	5.0-201403020	01-standa	ard	
■ルール:	My-ESXi5.5.0	u1_vSE_F	D_rule を作り	成する しんしん しんしん しんしん しんしん しんしん
補足:こ	こでは ESXi が追加	はれるインヘ	ベントリをクラスタ	7配下ではなく、Datacenter 配下にしております。DSVA の動
作確認時	に、DRS により作詞	業対象の ES	5Xi へ仮想マシ	ノンが vMotion されるのを防ぐ為となります。
また、オブシ	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。 +
こちりに関	ししは美塚現にめる	りせに設定を	「お願い致しま	9 •
PowerCl	I C:¥l Ingrado	vib> Nev	v-DeployPul	e -name My-ESYIS 5 Au1 VSE ED rule -Item tin
	t-VMHostProfile		01 std en	fd) (Get-Datacenter AutoDen) -allhosts
[1], (00			or_sta_cp_	
Download	ding dvfilter-dsa	9.0.0-350	0	
Download	d finished, uploa	ding to Aut	oDeploy	
Upload fi	nished.			
Warning:	Image Profile E	5Xi5.5.0u1	_vSE_FD cor	ntains one or more software packages that are not state
less-read	y. You may exp	erience pro	bolems when	using this profile with Auto Deploy
	じ時にト記のようか	Warning	が出力さわます	<del>.</del>
Auto De	nlov 環境でホスト	を再記動し	た場合のパラッ	ン。 ミ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 Hos <u>t F</u>	Profile で構成を再	現しておりま	ますので上記 V	Varning は無視して頂いて構いません。

26

Trend Micro Deep Security 9.0<sup>™</sup>SP1 Development Guide with VMware Auto Deploy Solution

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 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か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。

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

3-2 DSVA 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】

UserVars.VshieldEndpointSolutionsConfiguration	unset
Configuration string for the vShield Endpoint Multiplexer	
UserVars.VshieldVsmConnectionInfo	address:https://10.3.253.9
Connection info for the vShield Manager	
【有効化後】	
UserVars.VshieldEndpointSolutionsConfiguration	<id:749835264208352051;< td=""></id:749835264208352051;<>
Configuration string for the Vohield Endpoint Multiplexer	,
UserVars.VshieldVsmConnectionInfo	address:https://10.3.253.9
Connection info for the vShield Manager	

#### 該当の Host Profile にて下記を実行する。

🗆 📂 Host Profiles	
autoDep01_std_ep_fd	<ul> <li>Edit Profile</li> <li>Enable/Disable Profile Configuration</li> <li>Clone Profile</li> <li>Delete Profile</li> <li>Export Profile</li> </ul>
	Attach Host/Cluster Change Reference Host Update Profile From Reference Host

■「エンジンがオフライン」が発生する場合

dcang_test01-01 🔟		Microsoft Windows 7 (32)	Windows 7 D	
	<ul> <li>Appliance</li> </ul>			
ステータス:	● 雑数のエラー	ESX:	1	10.3,253.91
不正プログラム対策:	() リアルタイム	Appliance	. 3	10.3.253.101 (autoDSVA01
Webレビュテーション	a #2			
ファイアウォール:	🕞 ファイアウォールルー	ルエンジンがオフライン		
侵入55御:	😘 使入防御ルールエン:	アンがオフライン		
変更監視:	🝘 オン, 27 ルール			
セキュリティログ監視	(の) 保護できません			

DSVAを有効化した際に保護対象 VM や DSVAの <u>Firewall</u>と <u>IDS/IPS</u>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」

🦻 プロファイルの編集 (E)…
プロファイル構成の有効化/無効化(L)
7 プロファイルのクローン作成 (C)
ティー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
参照ホストの変更 (R)…
- 参照ホストからのプロファイルの更新(U)



#### ■DSVA の動作確認

# ここでの動作確認は必須ではないですが、Auto Deploy 後の問題発生時切り分けの為にも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。

🗧 10.3.253.95 (maintenance m	ode)	
<ul> <li>☐ StdDep</li> <li>☐ 10.3.253.192</li> <li>☆ kkang_test192-01</li> <li>☆ stdDSVA192</li> <li>☐ 10.3.253.201</li> <li>☆ kkang_test201</li> <li>☆ stdDSVA01</li> </ul>		
Recent Tasks		
Name	Target	Status
🌮 Attach host profile	10.3.253.95	📀 Completed
Add standalone host	AutoDep	🥝 Completed

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。

5	10.3.253.95 📜		VMware ESXi 5.5.0 build-1623387	θ	Prepared
ſ		) ESX	Guests:		
	Status: 🧧	Prepared			
	ESX Version:	5.5.0			
	Filter Driver Version:	9.0.0.3500			
	vShield Endpoint:	Not Installed			

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。

5.255.55				
Summary	Endpoint			
Shield Host Preparat	ion Status for 10.3.	253.95		
Service	Installed	Available		_
Service vShield App	Installed Not installed	Available 5.5.0-1620248	Not licensed	
Service vShield App vShield Endpoint	Installed Not installed 5.1.0-01255202	Available 5.5.0-1620248 -	Not licensed Uninstall	

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。

10.3.253.95						
Summary	Endpoint					
Endpoint Status						
•	Host Events:	0		Host Events:	0	
	Secured VM Events:	0		Secured VM Events:	0	
Critical(0)	vShield VM Events:	0	Normal(0)	vShield VM Events:	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)

10.3.253.95									
Summary	Endpoint								
Endpoint Stat	us								
	Host Events:	0		Host Events:	1	1			
•	Secured VM Events:	0		Secured VM Events:	0	-			
Critical(0)	vShield VM Events:	0	Normal(1)	vShield VM Events:	0				
Events Log									
All Errors									
Type Sou	no 💌 Deceription	_							_
host 10.3	3.253.95 ESX modul	ie enal	bled. Supporting	versions 1.4.2 of the ES	X module p	protocol an	d 1.5.3 of	the VFile pro	toco.

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。

VMware vCenter 🗙	v	Center - 10.3.253.175	With sub-Grou	ps ¬	▼ By ESX ▼		
Synchronization Complete		📑 New 👻 💼 Delete	🧰 Details	Ac	tions - Events - 🔂 Export -	强 Column	s
Computers		Name 🔻			Platform		Status
E 🗃 vCenter - 10.3.253.175		10.3.253.94 (2)					
E 🚞 Hosts and Clusters		않 kkang_test02-PC (kkang	1_test94)		Microsoft Windows 7 (32 bit)	0	Managed (O
🖽 📻 AutoDep		🛐 10.3.253.103 (autoDSV/	(204)		Deep Security Virtual Appliance		Managed (O
f StdDep		N/A (7)					
🖻 👮 Virtual Machines	F	N/A (7)					
🗉 💕 AutoDep		<b>10.3.253.95</b>			VMware ESXI 5.5.0 build-1623387	•	Prepared
🚞 Discovered virtual machine			- FEV	Gu	acte.		ר
🖻 🌠 StdDep			y ESA		5010.		
🚞 Discovered virtual machine		Status:	Prepared				
		ESX Version:	5.5.0				
		Filter Driver Version:	9.0.0.3500				
		vShield Endpoint:	Installed	L			

#### ■ 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。

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

#### ■「エンジンがオフライン」が発生する場合

kkang_test01-01 🔳	l Microsoft Wi	Microsoft Windows 7 (32 bib				
	<ul> <li>Appliance</li> </ul>					
ステータス:	😑 雑数のエラー	ESX: 🔣	10.3,253.91			
不正プログラム対策:	(g) UTNA14	Appliance: 🛐	10.3.253.101 (autoDSVA01			
Webレビュテーション	: <b>●</b> わ					
ファイアウォール	🕞 ファイアウォールルールエンジンがオフライン					
侵入5为御:	😘 使入防御ルールエンジンがオフライン					
安更監視:	() オン、27 ルール	•				
セキュリティログ監視	: 💮 保護できません					

DSVA を有効化した際に保護対象 VM や DSVA の <u>Firewall</u>と <u>IDS/IPS</u>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

	最終構成		
Auto Deploy Infrastruct Victim DSVA Win7 VA AutoDep ESXi-001 vse vse vse ESXi-2	ture	Management In Auto Deploy VCSA VA VA Kaster ESXi VA F.D ESXi	frastructure Power CLI DSM VSM W2K8 VA

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

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

# 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ESXi5.5U1及び

DSM9.0SP1Patch3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
		9.0SP1Patch2	9.0SP1Patch3	
1	DSM	(9.0.6019)	(9.0.6500)	
2		9.0SP1Patch2	9.0SP1Patch3	
Z	DSVA	(9.0.0-3044)	(9.0.0-3500)	
2 64		5.5.0a	E E O	
3 VSM	V2I™I	(1473628)	5.5.2	
	ECVi	5.5.0	5.5.0U1	Auto Doploy (TTTWT/)
	ESAI	(1331820)	(1623387)	Auto Deploy is Cyggod - R
			変更なし	
4	vSE	5.1.0	(vSM に含まれている	Auto Doploy (TTTWT/)
4		(01255202)	vSE の Version に変更が	
			無いため)	
	ED	9.0SP1Patch2	9.0SP1Patch3	
	г.∪	(9.0.0-2636)	(9.0.0-3500)	

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。

A		
	SX ESX	Guests:
Status: 🤇 🤇	Upgrade Recommended	10.3.253.101
ESX Version:	5.5.0	Kkang_lestu
Filter Driver Version:	9.0.0.2636	
vShield Endpoint:	Installed	

#### 【アップグレード後】

A		
	> ESX	Guests:
Status: 🤇	Prepared	(kkang_test01)
ESX Version:	5.5.0	10.3.253.101 (autoDSVA01
Filter Driver Version:	9.0.0.3500	
vShield Endpoint:	Installed	

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 ホストに移動するとような操作を行わ 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

※<u>Master 用 Host Profile(autoDep01\_std\_ep\_fd)は前項作業で作成したものを使用し</u> 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。

メンテナンス	モードの確認
<u> </u>	メンテナンス モードのホストでは、仮想マシンのプロビジョニング処理などの、仮想マシン関連の 機能は実行されません。メンテナンス モードに完全に切り替えるには、すべての仮想マシンをシ ャットダウンするか、別のホストに移動する必要があります。手動での作業が必要になる場合が あります。
	選択されたホストをメンテナンス モードに切り替えますか?
	□ パワーオフまたはサスペンド中の仮想マシンをクラスタ内のほかのホストに移動
	(はい いいえ

- 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。

<u>https://vSM</u> 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
- 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 ヘ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
       2014/03/20 11:12 654389915 update-from-esxi5.5-5.5_update01.zip
-a---
       2013/08/01
-a---
                    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...
             5.1.0-01255202 VMware 2013/08/01 21...
epsec-mux
```

43

Trend Micro Deep Security 9.0<sup>™</sup>SP1 Development Guide with VMware Auto Deploy Solution

■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

NameVendorLast ModifiedAcceptance Level--------------------ESXi5.5.0u1\_vSE\_FDVMware2014/02/22 2...PartnerSupported

#### Trend Micro Deep Security 9.0<sup>™</sup>SP1 Development Guide with VMware Auto Deploy Solution

■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 -So ftwarePackage epsec-mux, dvfilter-dsa

Name	Vendor	Last Modified	Acceptance Level
ESXi5.5.0u1_vSE_FD	VMware	2014/0	6/24 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 -Exp ortToBundle -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 配下にしております。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} : std\_ep\_fd Name 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 \_\_\_\_\_ ESXi5.5.0u1 vSE FD esxi5.5.0\_endpoint\_filterdriver ■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 state less-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か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

47

- 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。

.3.253.91	You are l	ogged in as a System	Administrator	Log
Summary	Endpoint			
/Shield Host Prepa	ration Status for 10.3.	253.91		
Service	Installed	Available		
vShield App	Not installed	5.5.0-1620248	Not licensed	0
vShield Endpoint	5.1.0-01255202		Uninstall	C
vShield Data Securi	ty Not installed	5.1.0.0-833296	Not licensed	C
Service Virtual Mac	hines			
Name T	уре			
autoDCV/A01	Shield Endpoint Active S	VM		

【Endpoint タブでは DSVA が正常に表示されない】

10.3.253.91	13			SALESSA	all second second second
Summary	Endpoint				
Endpoint Statu					
	Host Events:	0		Host Events:	1
•	Secured VM Events:	0	$\sim$	Secured VM Events:	c
Critical(8)	vShield VM Events:	0	Normal(1)	vShield VM Events:	c
Events Log					
TV3+	Source	•	Description		
host	10.3.253.91		ESX module enab	led, Supporting version	s 1.4.2 of the ESX modu

#### ■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]
- $\Rightarrow$  [Kernel Module] $\Rightarrow$ [dvfilter-dsa]
- ⇒ [Kernel Module Parameter]
- $\Rightarrow$  [DSAFILTER\_HEAP\_MAX\_SIZE]
- $\Rightarrow$  [Module Parameter Settings]

🛃 Edit Profile	
Brofile Names autoDep01 std ap fd	Description
Profile Name.  autobepox_sta_ep_ra	
Profile/Policy	Configuration Details Compliance Details
🗉 📴 ata_piix	Module Parameter Settings
	module Parameter Settings
🗉 🚡 dvfg-igmp	*Name DSAFILTER HEAP (
🗉 🛃 cmmds_net	
🕀 🕞 tracing	Value 512000000
🗉 📴 libata_92	
Iscs_viik      Iscs_trans	
🗉 🚰 tcpip4	
🗉 🔂 vsanutil	
🗉 📴 healthchk	
T B motspi	
E 📑 cnic_register	
🖃 🚡 dvfilter-dsa	
Module Name	
Module Parameter Settings	
USAFILIER_BIPASS_MODE	
E B DSAFILTER_HEAP_MIN_SIZE	
DSAFILTER_MOD_TIMER_ENABLED	

## 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	3	
# 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/DVfilterBindIp	oaddress	
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

C	Appliance	Protected Guests On: 🌆 10.3.253.225
Status:	) Managed (Online)	Kkangtest93-01 (kkang_test93-01)
Online:	Yes	
Last Communication:	July 6, 2014 08:44	
Appliance Version:	9.0.0.3500	
vShield Endpoint:	Registered	

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。

	You are lo	ogged in as a System	Administrator	Logge
3.253.91 Summary	Endpoint			
Shield Host Preparat	ion Status for 10.3.	253.91		
Service	Installed	Available		
Service vShield App	Installed Not installed	Available 5.5.0-1620248	Not licensed	۲
Service vShield App vShield Endpoint	Installed Not installed 5.1.0-01255202	Available 5.5.0-1620248 -	Not licensed Uninstall	0