# VMware ESXi への FireSIGHT Management Center の導入

### 内容

<u>概要</u>

<u>前提条件</u> 使用するコンポーネント コンフィギュレーション OVF テンプレートの展開 電源投入と初期設定の実行 ネットワークの設定 初期設定の実行 関連情報

### 概要

このドキュメントでは、VMware ESXi で稼働する FireSIGHT Management Center (Defense Center とも呼ばれる)の初期設定について説明します。FireSIGHT Management Center により、1 つ以上の FirePOWER アプライアンス、次世代侵入防御システム(NGIPS)仮想アプライアンス、および FirePOWER サービスを備えた適応型セキュリティ アプライアンス(ASA)の管理が可能になります。

**注**:このドキュメントは、FireSIGHT システムのインストール ガイドおよびユーザ ガイド の補足です。ESXi 特有の設定およびトラブルシューティングの問題については、VMware のナレッジ ベースとドキュメントを参照してください。

### 前提条件

#### 使用するコンポーネント

このドキュメントの情報は、次のプラットフォームに基づいています。

- Cisco FireSIGHT Management Center
- Cisco FireSIGHT Management Center 仮想アプライアンス
- VMware ESXI 5.0
- このドキュメントでは、「デバイス」は次のプラットフォームを指しています。
  - Sourcefire FirePOWER 7000 シリーズ アプライアンス、および 8000 シリーズ アプライアン ス
  - VMware ESXi 用の Sourcefire NGIPS 仮想アプライアンス
  - Cisco ASA 5500-X シリーズおよび FirePOWER サービス

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

## コンフィギュレーション

#### OVF テンプレートの展開

- 1. <u>Cisco Support & Downloads サイトから</u> Cisco FireSIGHT Management Center 仮想アプライ アンスをダウンロードします。
- 2. ローカル ディレクトリに、tar.gz ファイルの内容を解凍します。
- 3. <u>VMware vSphere クライアントで、ESXi サーバに接続します。</u>

<b>a</b>	VMware vSphere Client	< )
vmware VMware vSphere Client	e"	
To directly manage a To manage multiple b vCenter Server.	a single host, enter the IP address or host name. hosts, enter the IP address or name of a	
IP address / Na	me:	
User name:		
Password:		
	Use Windows session credentials	

4. vSphere クライアントにログインしたら、[File] > [Deploy OVF Template] を選択します。

Ć	7						
	File	Edit View Inventory	Adminis	tration	Plug	-ins	Helj
		New	•	ntory	Þ 🗊	Inver	ntory
		Deploy OVF Template					
		Export	•				
		Report	•	localh	ost. Vŀ	Iware	: ES
		Browse VA Marketplace		Gettir	ng Start	ed	Sum
		Print Maps	Þ				
		Exit					

5. [Browse] をクリックして、ステップ 2 で取得したファイルを検索します。OVF ファイル Sourcefire\_Defense\_Center\_Virtual64\_VMware-ESXi-X.X.X-xxx.ovf を選択して、[Next] をク リックします。

0	Deploy OVF Template
Source Select the source location.	
Source OVF Template Details Name and Location Datastore Disk Format Ready to Complete	Deploy from a file or URL          C:\Temp\Sourcefire_Defense_Center_Virtual64_VMware-5.3       Browse         Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
Help	< Back Next > Cancel

6. [OVF Template Details] 画面で [Next] をクリックして、デフォルトの設定を受け入れます。

	Deplo	y OVF Template		
OVF Template Details Verify OVF template details.				
Source				
OVF Template Details Name and Location	Product:	VirtualDC64		
Datastore	Version:			
Network Mapping	Vendor:			
Ready to Complete	Publisher:	No certificate present		
	Download size:	523.4 MB		
	Size on disk:	1.4 GB (thin provisioned) 250.0 GB (thick provisioned)		
	Description:	Sourcefire Defense Center Virtualé	i4	
		Sourcefire Inc. 9770 Patuxent Woods Drive Columbia, MD 21046		
1				
Help			( Death ) News	
Help			< Back Next	canc
Help Inagement Center の	名前を入力し	て [Next] をクリックし:	< Back Next ます。	canc
нер nagement Center の	名前を入力し Deploy	て [Next] をクリックしま y OVF Template	<back next<br="">ます。</back>	Canc
Help Inagement Center ທ Name and Location	名前を入力し Deploy	て [Next] をクリックし y OVF Template	<back next<br="">ます。</back>	Canc
Help Inagement Center の Name and Location Specify a name and location	名前を入力し Deploy for the deployed temp	て [Next] をクリックしま y OVF Template <sub>Mate</sub>	<back next<="" th=""><th>Canc</th></back>	Canc
Help Inagement Center の Name and Location Specify a name and location	名前を入力し Deploy for the deployed temp	て [Next] をクリックしま y OVF Template <sub>vlate</sub>	_ < Back Next	Canc
Help Inagement Center O Name and Location Specify a name and location	名前を入力し Deploy for the deployed temp Name:	て [Next] をクリックしま y OVF Template	<back next<="" td=""><td>Canc</td></back>	Canc
Help Inagement Center O Name and Location Specify a name and location	名前を入力し Deploy for the deployed temp Name: VirtualDC64	て [Next] をクリックしま y OVF Template	<back next<="" td=""><td>Canc</td></back>	Canc
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template <sup>alate</sup>	<back next<="" td=""><td>y folder.</td></back>	y folder.
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template nate	<back next<="" td=""><td>y folder.</td></back>	y folder.
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template date	<back next<="" td=""><td>y folder.</td></back>	y folder.
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template Nate	<back next<="" td=""><td>y folder.</td></back>	y folder.
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template alate	<back next<="" td=""><td>y folder.</td></back>	y folder.
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name:  VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template Nate	<back next<="" td=""><td>cancelocity of the second s</td></back>	cancelocity of the second s
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template Nate	<back next<="" td=""><td>y folder.</td></back>	y folder.
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template alate	<back next<="" td=""><td>y folder.</td></back>	y folder.
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template Nate	<back next<="" td=""><td>cancella to the second seco</td></back>	cancella to the second seco
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template Nate	<back next<="" td=""><td>y folder.</td></back>	y folder.
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template alate	<back next<="" td=""><td>y folder.</td></back>	y folder.
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template alate	<back next<="" td=""><td>cancella to the second seco</td></back>	cancella to the second seco
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template Nate	<back next<="" td=""><td>y folder.</td></back>	y folder.
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template alate	<back next<="" td=""><td>y folder.</td></back>	y folder.
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template alate	<back next<="" td=""><td>cancelocation of the second second</td></back>	cancelocation of the second
Help Inagement Center O Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template Nate	<back next<="" td=""><td>y folder.</td></back>	y folder.
Help Inagement Center Ø Name and Location Specify a name and location Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template Nate	<back next<="" td=""><td>y folder.</td></back>	y folder.
Help nagement Center Ø Name and Location Specify a name and location Source DVF Template Details Name and Location Datastore Disk Format Vetwork Mapping Ready to Complete	名前を入力し Deploy for the deployed temp Name: VirtualDC64 The name can contain	て [Next] をクリックしま y OVF Template Nate	<back next<="" td=""><td><pre>cance concentration conce</pre></td></back>	<pre>cance concentration conce</pre>

8. 仮想マシンを作成する [Datastore] を選択し、[Next] をクリックします。

þ	Deplo	by OVF Temp	late				×
Datastore Where do you want to	o store the virtual machine f	files?					
Source	Select a datastore in	which to store th	e VM files:				
OVF Template Details	Name	Capacity	Provisioned	Free	Туре	Thin Provisioning	Access
Datastore	[datastore2]	1.29 TB	866.14 GB	469.36 GB	VMFS	Supported	Single
Disk Format Network Mapping Ready to Complete	[datastore1]	459.75 GB	563.00 MB	459.20 GB	VMFS	Supported	Single
	<						>
Help				< B	ack	Next > Ca	ancel

9. [Disk Format] に対して [Thick provisioned format] のオプション ボタンをクリックして、 [Next] をクリックします。シックプロビジョニング形式では、仮想ディスクの作成時に必要 なディスク領域が割り当てられます。シンプロビジョニング形式では、必要に応じて領域が 使用されます。

6		Deploy OVF Template	
0	Disk Format In which format do you wan	t to store the virtual disks?	
	Cource DVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	Information about the selected datastore: Name: datastore2 Capacity: 1.3 TB Free space: 469.4 GB Select a format in which to store the virtual machines v C Thin provisioned format The storage is allocated on demand as data is supported only on VMFS3 and newer datastor create thick disks. Estimated disk usage: 1.4 GB C Thick provisioned format All storage is allocated immediately. Estimated disk usage: 250.0 GB	irtual disks: written to the virtual disks. This is es. Other types of datastores might
	Help		< Back Next > Cancel
). [N ス 00	etwork Mapping] セ を VMware ネット	クションで、FireSIGHT Manageme フークに関連付けて [Next] をクリッ Deploy OVF Template	ent Center の管理インターフェイ クします。
	Network Mapping What networks should the	deployed template use?	
	Source OVF Template Details Name and Location	Map the networks used in this OVF template to netw	orks in your inventory
	Datastore	Source Networks	Destination Networks
	Dick Format		

Source OVF Template Details Name and Location	Map the networks used in this OVF to	emplate to networks in your inventory
Datastore	Source Networks	Destination Networks
Disk Format	Management	VM Network 👻
Network Mapping Ready to Complete		VM Network VM Network 2
	Description: The Management network	
Help		< Back Next > Cancel





- 0 X

#### Ready to Complete

Ø

Are these the options you want to use?

Source OVF Template Details Name and Location	When you click Finish, the deployment task will be started. Deployment settings:			
Datastore Disk Format Network Mapping Ready to Complete	OVF file: Download size: Size on disk: Name: Host/Cluster: Datastore: Disk Format: Network Mapping:	C:\Temp\Sourcefire_Defense_Center_Virtual64_VMware 523.4 MB 1.4 GB VirtualDC64 localhost. datastore2 Thick Provisioning "Management" to "VM Network"		
Help		< Back Finish Cancel		

#### 電源投入と初期設定の実行

1. 新しく作成された仮想マシンにアクセスします。 サーバ名を右クリックし、[Power] > [Power On] を選択して、サーバの最初の起動を実行します。



2. [Console] タブを選択し、サーバのコンソールを監視します。[LILO Boot] メニューが表示されます。

VirtualDC64			
Getting Started Summary Resource Allocation Performance Events Console Permissions			
LILO 22.8 Boot Menu			
3D-5.3.0			
Hit any key to cancel timeout 00:00 Use ←↑↓→ arrow keys to make selection Enter choice & options, hit CR to boot			
boot: Loading 3D-5.3.0			

BIOS のデータのチェックが正常に終了すると、初期設定プロセスが開始されます。最初の 起動には少し時間がかかることがありますが、これは最初に設定データベースを初期設定す るためです。

Firstboot detected, executing scripts			
Executing S03install-math-pari.sh	E	OK	]
Executing S04async_syslog_dc.sh	Ε	OK	]
Executing S04fix-httpd.sh	Ε	OK	]
Executing S05set-MgMnt-port	Ε	OK	1
Executing S06addusers	Ε	OK	]
Executing S07uuid-init	Ε	OK	]
Executing S09configure_mysgl	E	OK	]
********* Attention ******** Initializing the configuration database. Depending on available system resources (CPU, memory, and disk), this may take 30 minute or more to complete.	s		
Executing S10database —			

初期設定プロセスが完了すると、「No such device」というメッセージが表示されることが あります。

```
Copyright (c) 1999-2010 Intel Corporation.
Silicom Bypass-SD Control driver v5.0.39.5
No such device
```

3. [Enter] キーを押すとログイン プロンプトが表示されます。

Copyright (c) 1999-2010 Intel Corporation. Silicom Bypass-SD Control driver v5.0.39.5 No such device Sourcefire Virtual Defense Center 64bit v5.3.0 (build 571) Sourcefire3D login: \_

注:メッセージ「WRITE SAME failed.手動でゼロにする」 システムを初めて起動した後に 表示される場合があります。これは不具合を示すものではなく、VMwareストレージドライ バがWRITE SAMEコマンドをサポートしていないことを正しく示します。 システムはこの メッセージを表示し、フォールバックコマンドを実行して同じ操作を実行します。

#### ネットワークの設定

- Sourcefire3D のログイン プロンプトで、ログインするには次のクレデンシャルを使用します。 バージョン 5.x の場合ユーザ名:adminパスワード: Sourcefireバージョン 6.x 以降の場合ユーザ名:adminパスワード: Admin123ヒント: GUI の初期設定のプロセスにおいて、デフォルトのパスワードを変更することができます。
- 2. ネットワークの初期設定は、スクリプトで行います。スクリプトは root ユーザとして実行 する必要があります。rootユーザーに切り替えるには、sudo su – コマンドとパスワード SourcefireまたはAdmin123 (6.x用)を入力します。 root ユーザとして Management Center のコマンド ラインにログインした場合は注意してください。 admin@Sourcefire3D:~\$ sudo su -Password:
- 3. ネットワークの設定を開始するには、root として、configure-network スクリプトを入力しま す。

root@Sourcefire3D:~# configure-network

Do you wish to configure IPv4? (y or n) y

管理 IP アドレス、ネットマスク、およびデフォルト ゲートウェイを指定するよう要求され

ます。設定を確定すると、ネットワーク サービスが再起動されます。結果として、管理イ ンターフェイスが停止して、その後、元に戻ります。

Do you wish to configure IPv4? (y or n) y Management IP address? [192.168.45.45] 192.0.2.2 Management netmask? [255.255.255.0] Management default gateway? 192.0.2.1 Management IP address? 192.0.2.2 Management netmask? 255.255.25 Management default gateway? 192.0.2.1 255.255.255.0 Are these settings correct? (y or n) y Do you wish to configure IPv6? (y or n) n e1000: eth0: e1000\_watchdog\_task: NIC Link is Up 1000 Mbps Full Duplex, Flow Con trol: None ADDRCONF(NETDEV\_UP): eth0: link is not ready. ADDRCONF(NETDEV\_CHANGE): eth0: link becomes ready Updated network configuration. Updated comms. channel configuration. Please go to https://192.0.2.2/ or https://[]/ to finish installation. root@Sourcefire3D:~# \_

#### 初期設定の実行

- 1. ネットワーク設定が完了したら、Web ブラウザを開いて、設定した IP を HTTPS (この例 では <u>https://192.0.2.2)を通じて検索します。</u>要求された場合は、デフォルトの SSL 証明 書を認証します。ログインには次のクレデンシャルを使用します。バージョン 5.x の場合 ユーザ名:adminパスワード: Sourcefireバージョン 6.x 以降の場合ユーザ名:adminパスワー ド: Admin123
- 2. 次の画面では、パスワードの変更およびサービス利用規約の承認を除いて、GUI のすべての 設定セクションはオプションです。 情報がわかっている場合は、Management Center の初 期設定を簡単に行うために、セットアップ ウィザードを使用することをお勧めします。設 定が完了したら [Apply] をクリックして、Management Center および登録したデバイスに対 して設定を適用します。 設定オプションの概要は次のとおりです。Change Password: デ フォルトの admin アカウントのパスワードを変更することができます。 パスワードを変更 する必要があります。 Network Settings: アプライアンスまたは仮想マシンの管理インタ ーフェイスに対して事前設定されている IPv4 およびIPv6 ネットワークの設定を変更するこ とができます。Time Settings: Management Center を信頼できる NTP ソースと同期させ ることを推奨します。IPS センサーは、システム ポリシーを通じて Management Center の 時刻と同期するように設定することができます。 オプションで、時刻、および表示のタイ ム ゾーンを手動で設定することができます。Recurring Rule Update Imports: Snort ルー ルの定期更新を有効にして、オプションで初期設定中にインストールできます。Recurring Geolocation Updates: 地理情報ルールの定期更新を有効にして、オプションで初期設定中 にインストールできます。Automatic Backups: 設定の自動的なバックアップをスケジュー ルします。License Settings: 機能ライセンスを追加します。Device Registration: ライセ ンスを追加し、最初のアクセス制御ポリシーを、あらかじめ登録されているデバイスに適用 することができます。 ホスト名/IP アドレスと登録キーは、FirePOWER IPS モジュールで 設定した IP アドレスと登録キーと一致しなければなりません。End User License Agreement: EULA の承認は必須です。

Change Password	
Use these fields to change the password for the adm characters of mixed case and includes at least one n	nin account. Sourcefire recommends that you use a password that has at least eight alphanumeric numeric character. Avoid using words that appear in a dictionary.
New Password Confirm	
Network Settings	
Use these fields to specify network-related informat	ion for the management interface on the appliance.
Protocol	● IPv4 ○ IPv6 ○ Both
IPv4 Management IP	
Netmask	
IPv4 Default Network Gateway	
Hostname	
Domain	
Primary DNS Server	
Secondary DNS Server	
Tertiary DNS Server	

## 関連情報

- <u>VMware 向け FirePOWER Management Center 仮想クイック スタート ガイド バージョン</u> <u>6.0</u>
- ・<u>テクニカル サポートとドキュメント Cisco Systems</u>