Déploiement de FireSIGHT Management Center sur VMware ESXi

Contenu

Introduction Conditions préalables Components Used Configuration Déployer un modèle OVF Mise sous tension et initialisation complète Configuration des paramètres réseau Effectuer la configuration initiale Informations connexes

Introduction

Ce document décrit la configuration initiale d'un FireSIGHT Management Center (également appelé Defense Center) qui s'exécute sur VMware ESXi. Un FireSIGHT Management Center vous permet de gérer un ou plusieurs appliances FirePOWER, des appliances virtuels NGIPS (Next Generation Intrusion Prevention System) et des appliances de sécurité adaptatives (ASA) avec les fonctionnalités FirePOWER.

Note: Ce document est un supplément du Guide d'installation et du Guide de l'utilisateur de FireSIGHT System. Pour obtenir des informations spécifiques sur la configuration et le dépannage d'ESXi, reportez-vous à la base de connaissances et à la documentation VMware.

Conditions préalables

Components Used

Les informations de ce document sont basées sur ces plates-formes :

- Cisco FireSIGHT Management Center
- Appliance virtuelle Cisco FireSIGHT Management Center
- VMware ESXI 5.0

Dans ce document, un « périphérique » fait référence à ces plates-formes :

- Appareils Sourcefire FirePOWER 7000 et appareils 8000
- Appareils virtuels Sourcefire NGIPS pour VMware ESXi
- Gamme Cisco ASA 5500-X avec service FirePOWER

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Configuration

Déployer un modèle OVF

- 1. Téléchargez l'**appareil virtuel Cisco FireSIGHT Management Center** à partir du site <u>d'assistance et de téléchargements Cisco</u>.
- 2. Extrayez le contenu du fichier tar.gz vers un répertoire local.
- 3. Connectez-vous à votre serveur ESXi avec un client VMware

ć	VMware vSphere Client
	vmware [*] VMware vSphere ^{**} Client
	To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server. IP address / Name:
	Password:
	Use Windows session credentials
e	Login Close Help

vSphere.

4. Une fois connecté au client vSphere, sélectionnez Fichier > Déployer le modèle

Ċ	2						
	File	Edit View Inventory	Administ	tration	Plug	-ins Hel	I
		New	•	ntory	Þ 🗊	Inventor	1
		Deploy OVF Template					
Export			•				
		Report	•	localh	ost. Vŀ	1ware ES	
Browse VA Marketplace			Gettir	ng Start	ed Sum		
	Print Maps		►				
OVF.		Exit					

5. Cliquez sur **Parcourir** et localisez les fichiers que vous avez extraits à l'étape 2. Choisissez le fichier OVF Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf et cliquez sur **Suivant.**

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. Dans l'écran **Détails du modèle OVF**, cliquez sur **Suivant** afin d'accepter les paramètres par défaut.

Ø	Deploy OVF Template			
OVF Template Details Verify OVF template details				
Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	Product: Version: Vendor: Publisher: Download size: Size on disk: Description:	VirtualDC64 No certificate present 523.4 MB 1.4 GB (thin provisioned) 250.0 GB (thick provisioned) Sourcefire Defense Center Virtual64 Sourcefire Inc. 9770 Patuxent Woods Drive Columbia, MD 21046		
Help			< Back Next >	Cancel

7. Indiquez un nom pour le Centre de gestion et cliquez sur

Suivant.

Ø	Deploy OVF Template	×

Name and Location

Specify a name and location for the deployed template

Name and Location	
Datastore Disk Format Network Mapping Ready to Complete	

8. Choisissez un **data store** sur lequel vous voulez créer l'ordinateur virtuel et cliquez sur **Suivant**.

	Deple	oy OVF Templ	ate				
Where do you want to	o store the virtual machine	files?					
Source	Select a datastore in	which to store the	VM files:				
OVF Template Details	Name	Capacity	Provisioned	Free	Туре	Thin Provisioning	Acces
Datastore	[datastore2]	1.29 TB	866.14 GB	469.36 GB	VMFS	Supported	Singl
Disk Format Network Mapping Ready to Complete	[Gatastore1]	459.75 GB	563.UU MB	459.20 GB	VMFS	Supporteo	Singi
Help	<			< B.	ack I	Next > C	ancel

9. Cliquez sur la case d'option Épaisseur du format provisionné pour le format de disque et cliquez sur Suivant. Le format d'approvisionnement épais alloue l'espace disque nécessaire au moment de la création d'un disque virtuel, tandis que le format d'approvisionnement léger utilise l'espace à la demande.

a	
Disk Format In which format do you	I want to store the virtual disks?
Source OVF 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 virtual disks: C Thin provisioned format The storage is allocated on demand as data is written to the virtual disks. This is supported only on VMFS3 and newer datastores. Other types of datastores might create thick disks. Estimated disk usage: 1.4 GB C Thick provisioned format All storage is allocated immediately. Estimated disk usage: 250.0 GB
Help	< Back Next > Cancel

10. Dans la section **Mappage réseau**, associez l'interface de gestion de FireSIGHT Management Center à un réseau VMware et cliquez sur **Suivant**.

9	Deploy OVF Temp	
Network Mapping What networks should	the deployed template use?	
Source OVF Template Details	Map the networks used in this OVF	template to networks in your inventory
Datastore	Source Networks	Destination Networks
Disk Format	Management	VM Network
Network Mapping		VM Network
Ready to complete		VM Network 2
	Description:	
	The Management network	^
		~
Help		< Back Next > Cancel

11. Cliquez sur **Terminer** afin de terminer le déploiement du modèle OVF.



Mise sous tension et initialisation complète

 Accédez à la machine virtuelle nouvellement créée. Cliquez avec le bouton droit sur le nom du serveur et choisissez Power > Power On afin de démarrer le serveur pour la première fois.



2. Accédez à l'onglet **Console** afin de surveiller la console du serveur. Le menu de démarrage LILO

s'affiche.	
VirtualDC64	
Getting Started Summary Re	source Allocation Performance Events Console Permissions
	LILO 22.8 Boot Menu
	3D-5.3.0
	Hit any key to cancel timeout $00:00$ Use $\uparrow\uparrow\downarrow\Rightarrow$ arrow keys to make selection Enter choice & options, hit CR to boot
boot: Loading 3D-5.3.0	

Une fois la vérification des données du BIOS terminée, le processus d'initialisation démarre. Le premier démarrage peut prendre plus de temps lorsque la base de données de configuration est initialisée pour la première fois.

```
Firstboot detected, executing scripts
Executing S03install-math-pari.sh
                                                                       E
                                                                          OK
                                                                               ]
                                                                               ]
                                                                       E
                                                                          OK
Executing S04async_syslog_dc.sh
                                                                       E
                                                                               ]
Executing S04fix-httpd.sh
                                                                          OK
                                                                       Ľ
                                                                               ]
Executing S05set-MgMnt-port
                                                                          OK
                                                                               ]
                                                                       E
                                                                          OK
Executing S06addusers
                                                                       E
                                                                          OK
                                                                               ]
Executing S07uuid-init
                                                                       E
                                                                          OK
                                                                               ]
Executing S09configure_mysql
************ Attention ********
   Initializing the configuration database.
                                              Depending on available
   system resources (CPU, memory, and disk), this may take 30 minutes
   or more to complete.
************ Attention ********
Executing S10database
```

Une fois terminé, un message peut s'afficher pour Aucun périphérique de ce

type.

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

3. Appuyez sur Entrée pour obtenir une invite de

connexion.

```
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: _
```

Note: Un message "WRITE SAME a échoué. Mise à zéro manuelle." peut s'afficher après le premier démarrage du système. Cela n'indique pas de défaut, cela indique correctement que le pilote de stockage VMware ne prend pas en charge la commande WRITE SAME. Le système affiche ce message et exécute une commande de secours pour effectuer la même opération.

Configuration des paramètres réseau

- Àl'invite de connexion Sourcefire3D, utilisez ces informations d'identification pour vous connecter : Pour la version 5.xusername (nom d'utilisateur) : adminMot de passe : SourcefirePour les versions 6.x et ultérieuresusername (nom d'utilisateur) : adminMot de passe : Admin123Astuce : Vous pouvez modifier le mot de passe par défaut lors du processus de configuration initiale dans l'interface utilisateur graphique.
- 2. La configuration initiale du réseau s'effectue à l'aide d'un script. Vous devez exécuter le script en tant qu'utilisateur racine. Afin de passer à l'utilisateur racine, entrez la commande sudo su avec le mot de passe Sourcefire ou Admin123 (pour 6.x). Soyez prudent lorsque vous êtes connecté à la ligne de commande Management Center en tant qu'utilisateur racine.

```
admin@Sourcefire3D:~$ sudo su -
Password:
```

3. Afin de commencer la configuration du réseau, entrez le script **configure-network** en tant que racine.

```
root@Sourcefire3D:~# configure-network
Do you wish to configure IPv4? (y or n) y
```

Vous serez invité à fournir une adresse IP de gestion, un masque de réseau et une passerelle par défaut. Une fois les paramètres confirmés, le service réseau redémarre. Par conséquent, l'interface de gestion tombe en panne, puis

revient. 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? 192.0.2.1 192.0.2.2 Management IP address? Management netmask? 255.255.255.0 Management default gateway? 192.0.2.1 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:~#

Effectuer la configuration initiale

- Une fois les paramètres réseau configurés, ouvrez un navigateur Web et accédez à l'adresse IP configurée via HTTPS (<u>https://192.0.2.2</u> dans cet exemple). Si vous y êtes invité, authentifiez le certificat SSL par défaut. Utilisez ces informations d'identification afin de vous connecter :Pour la version 5.x username (nom d'utilisateur) : adminMot de passe : SourcefirePour les versions 6.x et ultérieuresusername (nom d'utilisateur) : adminMot de passe : Admin123
- 2. Dans l'écran qui suit, toutes les sections de configuration de l'interface utilisateur graphique sont facultatives, à l'exception du changement de mot de passe et de l'acceptation des conditions d'utilisation. Si ces informations sont connues, il est recommandé d'utiliser l'assistant de configuration afin de simplifier la configuration initiale de Management Center. Une fois configuré, cliquez sur **Apply** afin d'appliquer la configuration au Management Center et aux périphériques enregistrés. Voici un bref aperçu des options de configuration : Modifier le mot de passe : Permet de modifier le mot de passe du compte d'administrateur par défaut. Il est nécessaire de modifier le mot de passe. Paramètres réseau : Permet de modifier les paramètres réseau IPv4 et IPv6 précédemment configurés pour l'interface de gestion de l'appliance ou de la machine virtuelle. Paramètres de temps : il est recommandé de synchroniser le Management Center avec une source NTP fiable. Les capteurs IPS peuvent être configurés via la stratégie système pour synchroniser leur temps avec le Management Center. Vous pouvez également définir manuellement l'heure et le fuseau horaire d'affichage. Imports de mise à jour de règle récurrente : activez les mises à jour de règle Snort récurrentes et, éventuellement, installez maintenant lors de la configuration initiale. Mises à jour de géolocalisation récurrentes : activez les mises à jour de règles de

géolocalisation récurrentes et installez-les maintenant lors de la configuration initiale.**Sauvegardes automatiques :** Planification des sauvegardes automatiques de configuration.**Paramètres de licence :** ajoutez la licence de fonction.**Enregistrement de périphérique :** vous permet d'ajouter, de mettre en licence et d'appliquer des stratégies de contrôle d'accès initiales aux périphériques préenregistrés. Le nom d'hôte/adresse IP et la clé d'enregistrement doivent correspondre à l'adresse IP et à la clé d'enregistrement configurées sur le module IPS FirePOWER.**Contrat de licence de l'utilisateur final :** acceptation du CLUF

•	
Change Password	
Use these fields to change the password for the adm characters of mixed case and includes at least one r	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 Management IP Netmask IPv4 Default Network Gateway	IPv4 O IPv6 O Both
Hostname	
Domain	
Primary DNS Server	
Secondary DNS Server	
Tertiary DNS Server	

Informations connexes

requise.

- <u>Guide de démarrage rapide virtuel de Firepower Management Center pour VMware, version</u>
 <u>6.0</u>
- Support et documentation techniques Cisco Systems