在VMware ESXi上部署FireSIGHT管理中心

目錄

<u>簡介</u> <u>必要條件</u> <u>採用元件</u> <u>組態</u> <u>部署OVF模板</u> <u>開啟電源並完成初始化</u> <u>配置網路設定</u> <u>執行初始設定</u> 相關資訊

簡介

本文檔介紹在VMware ESXi上運行的FireSIGHT管理中心(也稱為防禦中心)的初始設定。 FireSIGHT管理中心允許您管理一個或多個FirePOWER裝置、下一代入侵防禦系統(Next Generation Intrusion Prevention System, NGIPS)虛擬裝置以及具備FirePOWER服務的自適應安全 裝置(ASA)。

附註:本文檔是《FireSIGHT系統安裝指南》和《使用手冊》的補充。有關ESXi特定的配置和 故障排除問題,請參閱VMware知識庫和文檔。

必要條件

採用元件

本檔案中的資訊是根據以下平台:

- Cisco FireSIGHT管理中心
- Cisco FireSIGHT管理中心虛擬裝置
- VMware ESXI 5.0

在本檔案中,「裝置」是指以下平台:

- Sourcefire FirePOWER 7000系列裝置和8000系列裝置
- 適用於VMware ESXi的Sourcefire NGIPS虛擬裝置
- 具備FirePOWER服務的Cisco ASA 5500-X系列

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

組態

部署OVF模板

- 1. 從思科支援和下載站點下載Cisco FireSIGHT管理中心虛擬裝置。
- 2. 將tar.gz檔案的內容解壓到本地目錄。
- 3. 使用VMware vSphere Client連線到ESXi伺服器。

2 VN	/ware vSphere Client	—
vmware [•] VMware vSphere ^{••} Client		
To directly manage a sir To manage multiple host vCenter Server. IP address / Name: User name: Password:	ngle host, enter the IP address or host na ts, enter the IP address or name of a	ame. s Help

4. 登入到vSphere客戶端後,選擇**File > Deploy OVF Template**。

ł	<i></i>						
	File	Edit View Inventory	Adminis	tration	Plug	-ins	Helj
		New	•	ntory	Þ 🗊	Inve	entory
		Deploy OVF Template					
		Export	•				
		Report	•	localh	ost. VI	1war	e ES
		Browse VA Marketplace		Gettir	ng Start	ed	Sum
		Print Maps	Þ				
		Exit					

5. 按一下**瀏覽**並找到在步驟2中解壓的檔案。選擇OVF檔案 Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf,然後按一下**下一步。**

	Deploy	y OVF Template		[-	
Source Select the source location.						
Source OVF Template Details Name and Location Datastore Disk Format Ready to Complete	Deploy from C:\Temp\Sc Enter a URL specify a loc network sha	a file or URL purcefire_Defense_Center_Virtual64_Vi to download and install the OVF packa ation accessible from your computer, s are, or a CD/DVD drive.	Mware-5.3 ▼ ge from the Inte such as a local ha	Browse rnet, or ard drive, a		
Help		[< Back	Next >		Canc
OVF Template Deta	ils螢幕上,按−	- 下 Next 以接受預設設定。	•			
OVF Template Deta OVF Template Details Verify OVF template details	ils螢幕上,按一 Deploj s.	-下 Next 以接受預設設定。 y OVF Template				
OVF Template Details OVF Template Details Verify OVF template details Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	ils螢幕上,按一 Deploy s. Product: Version: Vendor:	- 下 Next 以接受預設設定。 y OVF Template VirtualDC64	5			
OVF Template Details OVF Template Details Verify OVF template details Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	ils螢幕上,按一 Deploy s. Product: Version: Vendor: Publisher: Download size: Size on disk:	- 下Next以接受預設設定。 y OVF Template VirtualDC64 No certificate present 523.4 MB 1.4 GB (thin provisioned)	5			
OVF Template Details OVF Template Details Verify OVF template details Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	ils螢幕上,按一 Deploy s. Product: Version: Vendor: Publisher: Download size: Size on disk: Description:	- 下Next以接受預設設定。 y OVF Template VirtualDC64 No certificate present 523.4 MB 1.4 GB (thin provisioned) 250.0 GB (thick provisioned) 250.0 GB (thick provisioned) Sourcefire Defense Center Virtual64 Sourcefire Inc. 9770 Patuxent Woods Drive Columbia, MD 21046	5			
OVF Template Details Verify OVF template details Verify OVF template details Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	ils螢幕上,按一 Deploy s. Product: Version: Vendor: Publisher: Download size: Size on disk: Description:	- 下Next以接受預設設定。 y OVF Template VirtualDC64 No certificate present 523.4 MB 1.4 GB (thin provisioned) 250.0 GB (thick provisioned) 250.0 GB (thick provisioned) Sourcefire Defense Center Virtual64 Sourcefire Inc. 9770 Patuxent Woods Drive Columbia, MD 21046	•			

7.	提供管理中心的名稱,	然後按一下 下一步 。			
	Ø	Deploy OVF Template			×
	Name and Location Specify a name and locatio	n for the deployed template			
	Source	Name:			
	OVF Template Details	VirtualDC64			_
	Datastore Disk Format Network Mapping Ready to Complete	The name can contain up to 80 characters and it must be unique within the inventory fold	ler.		
	Help	< Back Next >		Cance	<u> </u>

8. 選擇要在其上建立虛擬機器的**資料儲存區**,然後按一下**下一步**。

2	Depl	oy OVF Temp	olate				•
Datastore Where do you want to st	tore the virtual machine	files?					
Source	Select a datastore in	which to store th	e VM files:				
OVF Template Details	Name	Capacity	Provisioned	Free	Туре	Thin Provisionin	a Acce
Name and Location	[datastore2]	1.29 TB	866.14 GB	469.36 GB	VMFS	Supported	Sing
Disk Format Network Mapping Ready to Complete	[datastore1]	459.75 GB	563.00 MB	459.20 GB	VMFS	Supported	Sing
ttele	<						
нер				< B	ack	Next >	Cancel
 ġ一下Disk Format的 韋立虛擬磁碟時分配≠ ⋧	I Thick provisio r 必要的磁碟空間 Depl	ned format [⊑] Ⅰ,而精簡酝 oy OVF Temp	單選按鈕, 已置格式則 blate	8 然後按一 按需使用	∝k [·下Nex 空間。	Next> ct。密集配置	Cancel 格式在
y y y y y w w w bisk Format In which format do you w	「 Thick provisio r 必要的磁碟空間 Depl want to store the virtual	ned format [⊑]],而精簡酝 oy OVF Temp Idisks?	單選按鈕, 2置格式則 blate	<в 然後按一 按需使用	≪ ┃[·下Ne≫ 空間。	Next> ct。密集配置	Cancel 格式在
pep 安一下Disk Format的 建立虛擬磁碟時分配∉ pisk Format In which format do you v	「Thick provision 必要的磁碟空間 Depl want to store the virtual	ned format ^国 ,而精簡面 oy OVF Temp I disks? the selected data	^程 選按鈕, 2置格式則 blate store:	 然後按一 按需使用	∝k [下Nex 空間。	Next> ct。密集配置	Cancel 格式在
中国 安一下Disk Format的 建立虛擬磁碟時分配。 Disk Format In which format do you v Source OVF Template Details Name and Location Datastore	「Thick provision 必要的磁碟空間 Depl want to store the virtual Information about Name: Capacity: Free space:	ned format ^国 ,而精簡面 oy OVF Temp disks? the selected data datastore2 1.3 TB 469.4 GB	單選按鈕, 2置格式則 blate store:	<₿ 然後按一 按需使用	∝ [下Nex 空間。	Next>	Cancel 格式在
中国 安一下Disk Format的 建立虛擬磁碟時分配少 Disk Format In which format do you v Source OVF Template Details Name and Location Datastore Disk Format	VThick provision 必要的磁碟空間 Depl want to store the virtual Information about Name: Capacity: Free space: Select a formation	ned format ^国 , 而精簡面 oy OVF Temp disks? the selected data datastore2 1.3 TB 469.4 GB	^程 選按鈕, 2置格式則 blate store:	_ <b 然後按一 按需使用</b 	∝ [·下Ne> 空間。	Next >	Cancel 格式在
中国 安一下Disk Format的 建立虛擬磁碟時分配。 Disk Format In which format do you w Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	「Thick provision 必要的磁碟空間 Depl want to store the virtual Information about Name: Capacity: Free space: Select a format in v	ned format ^国 , 而精簡面 oy OVF Temp disks? the selected data datastore2 1.3 TB 469.4 GB which to store the	單選按鈕, 2置格式則 blate store:	<ba 然後按一 按需使用</ba 	∝ [下Nex 空間。	Next>	Cancel 格式在
pep 安一下Disk Format的 建立虛擬磁碟時分配/ P Disk Format In which format do you w Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	VThick provision 必要的磁碟空間 Depl want to store the virtual Information about Name: Capacity: Free space: Select a format in v C Thin provis The stora supported create thi	ned format ,而精簡面 oy OVF Temp disks? the selected data datastore2 1.3 TB 469.4 GB which to store the ioned format ge is allocated on if only on VMFS3 ar dx disks.	單選按鈕, 2置格式則 blate store: virtual machine demand as data nd newer datas	<bi 然後按一 按需使用 es virtual disks: a is written to t tores. Other t</bi 	ack [一下 Ne 空間。	Next > kt。密集配置	Cancel 格式在
中国 安一下Disk Format的 建立虚擬磁碟時分配。 Disk Format In which format do you v Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	の で が 要的磁碟空間 の し epl want to store the virtual Information about Name: Capacity: Free space: Select a format in viso て Thin provis The stora supported create thi Estimated	ned format , 而精簡西 oy OVF Temp disks? the selected data datastore2 1.3 TB 469.4 GB which to store the ioned format ge is allocated on fonly on VMFS3 aid ck disks. disk usage: 1.4 G	單選按鈕, 2置格式則 blate store: virtual machine demand as data nd newer datas B	<ba 然後按一 按需使用 es virtual disks: a is written to t itores. Other t</ba 	ack [下 Ne) 空間。	Next > ct。密集配置	Cancel 格式在
中国 安一下Disk Format的 建立虛擬磁碟時分配。 Disk Format In which format do you w Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	シ要的磁碟空間 必要的磁碟空間 Depl want to store the virtual Information about Name: Capacity: Free space: Select a format in v C Thin provis The stora supported create thi Estimated C Thick provi	ned format , 而精簡面 oy OVF Temp disks? the selected data datastore2 1.3 TB 469.4 GB which to store the ioned format ge is allocated on a only on VMFS3 ar ck disks. disk usage: 1.4 G sioned format	單選按鈕, 2置格式則 olate store: virtual machine demand as data nd newer datas	<bi 然後按一 按需使用 es virtual disks: a is written to t tores. Other t</bi 	ack [下 Ne 空間。	Next > kt。密集配置	Cancel 格式在
中国 安一下Disk Format的 建立虛擬磁碟時分配。 Disk Format In which format do you v Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	の の で の で の の の の の の の の の の の の の	ned format , 而精簡西 oy OVF Temp disks? the selected data datastore2 1.3 TB 469.4 GB which to store the ioned format ge is allocated on if only on VMFS3 ar ck disks. disk usage: 1.4 G sioned format te is allocated imme	單選按鈕, 2置格式則 olate store: virtual machine demand as data nd newer datas B ediately.	<bi 然後按一 按需使用 es virtual disks: a is written to t itores. Other t</bi 	ack [下 Ne) 空間。	Next > ct。密集配置 	Cancel 格式在
中国 安一下Disk Format的 建立虛擬磁碟時分配。 Disk Format In which format do you v Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	シ要的磁碟空間 必要的磁碟空間 Depl want to store the virtual Information about Name: Capacity: Free space: Select a format in v C Thin provis The stora supported create thi Estimated	ned format , 而精簡面 oy OVF Temp disks? the selected data datastore2 1.3 TB 469.4 GB which to store the ioned format ge is allocated on a only on VMFS3 ai ck disks. disk usage: 1.4 G sioned format e is allocated imme disk usage: 250.0	遅選按鈕, 2置格式則 olate store: virtual machine demand as data nd newer datass B ediately. o GB	<bi 然後按一 按需使用 es virtual disks: a is written to t tores. Other t</bi 	ack [一下 Ne 空間。	Next > kt。密集配置	Cancel 格式在
中中 安一下Disk Format的 建立虛擬磁碟時分配。 Disk Format In which format do you v Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	Thick provision 必要的磁碟空間 Depl want to store the virtual Information about Name: Capacity: Free space: Select a format in v C Thin provis The stora supported create thi Estimated C Thick provi All storage Estimated	ned format , 而精簡西 oy OVF Temp disks? the selected data datastore2 1.3 TB 469.4 GB which to store the ioned format ge is allocated on 1 only on VMFS3 ar ck disks. disk usage: 1.4 G sioned format e is allocated imme disk usage: 250.0	單選按鈕, 2置格式則 olate store: virtual machine demand as data nd newer datas B ediately. 0 GB	<ba 然後按一 按需使用 es virtual disks: a is written to t itores. Other t</ba 	ack [- 下 Ne) 空間。	Next >	Cancel 格式?

1

< Back

1

Next >

Cancel

1

Help

10. 在**Network Mapping**部分中,將FireSIGHT管理中心的管理介面與VMware網路相關聯,然後 按一下**Next**。

J~~		
2	Deploy OVF Template	- • ×
	Network Mapping What networks should the deployed template use?	

	Source Networks	Destination Networks	
<u>sk Format</u>	Management	VM Network	
eady to Complete		VM Network VM Network 2	
	Description: The Management network		

11. 按一下**完成**以完成OVF模板部署。



開啟電源並完成初始化

 導航到新建立的虛擬機器。按一下右鍵伺服器名稱,然後選擇Power > Power On以首次啟動 伺服器。

-	Infrastruc	ture		VirtualDO	64				
((Linux			Getting S	Started Sum	mary	Resou	rce Allocation P	erformance E
	🖬 Virtua	IDCC4							
			Power			•	P	ower On	Ctrl+B
			Guest			•	P	ower Off	Ctrl+E
			Snapshot			•	S	uspend	Ctrl+Z
		9	Open Console	2			R	eset	Ctrl+T
		₿	Edit Settings				S	hut Down Guest	Ctrl+D
			Add Permissio	on	Ctrl+P		R	estart Guest	Ctrl+R
			Report Perform	mance					
			Rename						
			Open in New	Window	Ctrl+Alt+N				
			Remove from	Inventory					
			Delete from D	isk					

2. 導航到**Console**頁籤以監視伺服器控制檯。出現「LILO Boot Menu(LILO引導選單)」。 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資料檢查成功後,初始化過程開始。首次啟動可能需要額外的時間才能完成,因為配置 資料庫是首次初始化的。

Firstboot detected, executing scripts			
Executing S03install-math-pari.sh	I	OK]
Executing S04async_syslog_dc.sh	I	OK	1
Executing S04fix-httpd.sh	Γ	OK	1
Executing S05set-mgmnt-port	I	OK]
Executing S06addusers	Ι	OK]
Executing S07uuid-init	Ι	OK	1
Executing S09configure_mysql	I	OK]
********** 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			
-			
完成後,您可能會看到No these device的消息。			
Copyright (c) 1999-2010 Intel Corporation.			
Silicom Bypass-SD Control driver v5.0.39.5			
No ouch doution			

3. 按Enter鍵以取得登入提示。

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: _

附註:消息「WRITE SAME failed.手動清零。」 首次引導系統後可能會出現。這並非表示存 在缺陷,而是正確地表明VMware儲存驅動程式不支援WRITE SAME命令。 系統會顯示此消 息,並繼續執行回退命令以執行相同操作。

配置網路設定

1. 在Sourcefire3D登入提示中,使用以下憑證登入: 5.x版使用者名稱:admin密碼

:**Sourcefire**6.x及更新版本使用者名稱:admin密碼:Admin123提示:您可以在GUI中更改初始 設定過程中的預設密碼。

2. 網路的初始配置使用指令碼完成。您需要以root使用者身份運行指令碼。若要切換到root使用者,請輸入sudo su -命令以及密碼Sourcefire或Admin123(6.x版)。以root使用者身份登入管理中心命令列時要小心。 admin@Sourcefire3D:~\$ sudo su -

Password:

3. 若要開始網路配置,請輸入**configure-network**指令碼作為root。

root@Sourcefire3D:~# configure-network

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

系統將要求您提供管理IP地址、網路掩碼和預設網關。確認設定後,網路服務將重新啟動。因此,管理介面關閉並返回。

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? Management netmask? 192.0.2.2 255.255.255.0 Management default gateway? 192.0.2.1 Are these settings correct? (y or m) 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:"# _

執行初始設定

- 設定網路設定後,開啟Web瀏覽器並透過HTTPS(在本範例中為<u>https://192.0.2.2</u>)瀏覽至設定的 IP。 出現提示時,驗證預設SSL證書。使用以下憑據登入:5.x版 使用者名稱:admin密碼 :Sourcefire6.x及更新版本使用者名稱:admin密碼:Admin123
- 2. 在接下來的螢幕中,除了密碼更改和服務條款接受外,所有GUI配置部分都是可選的。如果已知資訊,建議使用設定嚮導來簡化管理中心的初始配置。配置後,按一下Apply將配置應用到管理中心和註冊裝置。配置選項的簡要概述如下:更改密碼:允許您更改預設管理員帳戶的密碼。需要更改密碼。網路設定:允許您為裝置或虛擬機器的管理介面修改先前配置的IPv4和IPv6網路設定。時間設定:建議您使用可靠的NTP源同步管理中心。可以通過系統策略配置IPS感測器,使其時間與管理中心同步。可以選擇手動設定時間和顯示時區。定期規則更新匯入: 在初始設定期間啟用定期的Snort規則更新,也可以立即安裝。定期地理位置更新:在初始設定期間啟用定期地理定位規則更新,也可以立即安裝。自動備份:計畫自動配置備份。許可證設定:新增功能許可證。裝置註冊: 允許您新增、許可初始訪問控制策略並將其應用於預註冊裝置。 主機名/IP地址和註冊金鑰應與FirePOWER IPS模組上配置的IP地址和註冊金鑰匹配。一般使用者授權合約:需要接受EULA。

Change Password	
Use these fields to change the password for the ad characters of mixed case and includes at least one	Imin 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 information	ition 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	

相關資訊

- 適用於VMware的Firepower管理中心虛擬快速入門手冊6.0版
 技術支援與文件 Cisco Systems