在 Firepower 設備上安裝和升級 FTD

目錄
。 <u>簡介</u>
<u>必要條件</u>
採用元件
<u>背景資訊</u>
<u>網路圖表</u>
<u>任務1.FTD軟體下載</u>
<u>任務2.驗證FXOS-FTD相容性</u>
任務3.將FTD映像上傳到Firepower裝置
任務4.設定FTD管理和資料介面
任務5.建立和配置新的邏輯裝置
任務6.將FTD註冊到Firepower管理中心(FMC)
<u>任務7.升級FTD</u>
<u>解決方案</u> ————————————————————————————————————
<u>驗證</u>
Firepower 2100
在FP2100上安裝FTD
FP2100上的FTD升級
<u>疑難排解</u>
相關資訊

簡介

本檔案介紹Firepower裝置上安裝、升級和註冊Firepower威脅防禦(FTD)軟體。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

• Cisco Firepower 4140安全裝置,運行FXOS 2.0(1.37)

• 運行6.1.0.330的Firepower管理中心

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。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

FTD是可在以下平台上安裝的整合軟體映像:

- ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X
- ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X
- Firepower裝置(FPR2100、FPR4100、FPR9300)
- VMWare (ESXi)
- Amazon Web Services (AWS)
- 基於核心的虛擬機器(KVM)
- 整合服務路由器(ISR)模組

設定

網路圖表



任務1.FTD軟體下載

導覽至Next-Generation Firewalls(NGFW)> FirePOWER 4100 Series > FirePOWER 4140 Security Appliance, 然後選擇Firepower威脅防禦軟體,如下圖所示。

Download Software

Download Cart (0 ite

Downloads Home > Products > Security > Firewalls > Next-Generation Firewalls (NGFW) > Firepower 4100 Series > Firepower 4140 Security Appliance

Select a Software Type:

Adaptive Security Appliance (ASA) Device Manager Adaptive Security Appliance (ASA) Software Adaptive Security Appliance REST API Plugin Firepower Extensible Operating System Firepower Threat Defense Software

任務2.驗證FXOS-FTD相容性

任務需求

驗證機箱上運行的FXOS版本與要在安全模組中安裝的FTD版本是否相容。

解決方案

步驟 1.檢查FXOS-FTD相容性。

將FTD映像安裝到模組/刀鋒之前,請確保Firepower機箱執行相容的FXOS軟體。在《FXOS相容性 指南》中,檢查「邏輯裝置相容性」表。運行FTD 6.1.x所需的最低FXOS版本為1.1(4.95),如表 2所示:

Table 2 Logical Device Compatibility

FXOS	ASA OS	Firepower Threat Defense
1.1(1.147)	9.4(1)	not supported
1.1(1.160)	9.4(1)	
1.1(4.95)	9.6(1)	6.0.1.x
	9.6(2)	6.1

如果FXOS映像與目標FTD映像不相容,請先升級FXOS軟體。

驗證FXOS映像

方法1.在「Firepower機箱管理器(FCM)UI概述」頁面中,如下圖所示:



方法2. 導覽至FCM System > Update頁面,如下圖所示:

Overview Interfaces	Logical Devices Security Engine Platform Settings						System	Tools	нөр	admin
					Configuration	Licensing	Updates	User	Manag	ement
Available Updates						C Refresh	Upload Image			×
Image Name		Туре	Version	Status	Bu	ild Date				
fxos-k9.2.0.1.23.SPA		platform-bundle	2.0(1.23)	Not-Installed	05	/18/2016		5	8	
fxos-k9.2.0.1.37.SPA		platform-bundle	2.0(1.37)	Installed	05	/11/2016			8	
fxos-k9.2.0.1.4.SPA		platform-bundle	2.0(1.4)	Not-Installed	04	/06/2016		5	8	

方法3.在FXOS CLI上:

<#root>

FPR4100#

show fabric-interconnect firmware

```
Fabric Interconnect A:
Running-Kern-Vers: 5.0(3)N2(4.01.35)
Running-Sys-Vers: 5.0(3)N2(4.01.35)
```

Package-Vers: 2.0(1.37)

Startup-Kern-Vers: 5.0(3)N2(4.01.35)
Startup-Sys-Vers: 5.0(3)N2(4.01.35)
Act-Kern-Status: Ready
Act-Sys-Status: Ready
Bootloader-Vers:

任務3.將FTD映像上傳到Firepower裝置

任務需求

將FTD映像上傳到FPR4100機箱。

解決方案

方法1—從FCM UI上傳FTD映像。

登入到FPR4100機箱管理器,然後導航到System > Updates頁籤。選擇Upload Image以上傳檔案 ,如下圖所示。

Overview Interfaces	Logical Devices Security Engine Platform Settings						System	Tools	Help	admin
					Configuration	Licensing	Updates	User	r Mana	gement
Available Updates						C Refresh	Upload Image)		×
Image Name		Туре	Version	Status	Bui	ild Date				
fxos-k9.2.0.1.23.SPA		platform-bundle	2.0(1.23)	Not-Installed	05/	/18/2016		5	18	
fxos-k9.2.0.1.37.SPA		platform-bundle	2.0(1.37)	Installed	06/	/11/2016			8	
fxos-k9.2.0.1.4.SPA		platform-bundle	2.0(1.4)	Not-Installed	04,	/06/2016		5	18	

瀏覽以選擇FTD映像檔,然後按一下Upload,如下圖所示:

Upload Image	? ×
Select File : Browse cisco-ftd.6.1.0.330.SPA.csp	
Upload	Cancel

接受終端使用者許可協定(EULA)。

驗證如下圖所示。

Overview	Interfaces	Logical Devices	Security Engine	Platfor	m Settings	;			System	Tools H	lelp	admin
							Configuration	Licensing	Updates	User M	lanag	gement
Available	Updates							C Refresh	Upioad Image	Filter		×
Image Name			Туре		Version	Status		Build Date				
fxos-k9.2.0.1.0	36.SPA		platfor	m-bundle	2.0(1.86)	Installed		10/15/2016			8	
fxos-k9.2.0.1.4	I.SPA		platfor	m-bundle	2.0(1.4)	Not-Installed		04/06/2016		2	10	
cisco-ftd.6.1.0	.330.csp		ftd		6.1.0.330	Not-Installed		08/26/2016			8	

方法2 — 從FXOS CLI上傳FTD映像

您可以從FTP、安全複製(SCP)、安全FTP(SFTP)或TFTP伺服器上傳FTD映像。

開始映像傳輸之前,驗證機箱管理介面和遠端伺服器之間的連線:

<#root>

FPR4100#

connect local-mgmt

FPR4100(local-mgmt)#

ping 10.229.24.22

PING 10.229.24.22 (10.229.24.22) from 10.62.148.88 eth0: 56(84) bytes of data. 64 bytes from 10.229.24.22: icmp_seq=1 ttl=124 time=0.385 ms 64 bytes from 10.229.24.22: icmp_seq=2 ttl=124 time=0.577 ms 64 bytes from 10.229.24.22: icmp_seq=3 ttl=124 time=0.347 ms

若要下載FTD映像,請導覽至此範圍並使用download image指令:

<#root>

FPR4100#

scope ssa

FPR4100 /ssa #

scope app-software

FPR4100 /ssa/app-software #

download image ftp://ftp_username@10.229.24.22/cisco-ftd.6.1.0.330.SPA.csp

Password:

監控映像上傳進度:

<#root>

FPR4100 /ssa/app-software #

show download-task detail

Downloads for Application Software:

File Name: cisco-ftd.6.1.0.330.SPA.csp

Protocol: Ftp Server: 10.229.24.22 Port: 0 Userid: ftp Path: Downloaded Image Size (KB): 95040 Time stamp: 2016-12-11T20:27:47.856

State: Downloading

Transfer Rate (KB/s): 47520.00000

Current Task: downloading image cisco-ftd.6.1.0.330.SPA.csp from 10.229.24.22(FSM-STAGE:sam:dme:App

使用以下命令驗證下載是否成功:

<#root>

FPR4100 /ssa/app-software #

show download-task

Dowr	nloads for	Application Software	:				
	File Name		Protocol	Server	Port	Userid	State
	cisco-ftd.	.6.1.0.330.SPA.csp	 Ftp	10.229.24.22	C	ftp	

Downloaded

有關其他詳細資訊:

<#root>

```
KSEC-FPR4100 /ssa/app-software #
```

```
show download-task fsm status expand
```

```
File Name: cisco-ftd.6.1.0.330.SPA.csp
```

FSM Status:

Affected Object: sys/app-catalogue/dnld-cisco-ftd.6.1.0.330.SPA.csp/fsm

Current FSM: Download

Status: Success

Completion Time: 2016-12-11T20:28:12.889 Progress (%): 100

FSM Stage:

Order	Stage Name	Status	Try
1	DownloadLocal		

Success

1

- 2 DownloadUnpackLocal
- Success

1 File Name: Cisco_FTD_SSP_Upgrade-6.1.0-330.sh

該影象顯示在機箱儲存庫中:

<#root>

KSEC-FPR4100 /ssa/app-software # exit
KSEC-FPR4100 /ssa #

show app

Application: Name Version Description Author Deploy Type CSP Type Is Default App

ftd 6.1.0.330

N/A cisco Native Application No

任務4.設定FTD管理和資料介面

任務需求

在Firepower裝置上為FTD配置並啟用管理和資料介面。

解決方案

要建立新介面,請登入到FCM並導航到Interfaces頁籤。顯示當前介面。若要建立新的連線埠通道介面,請選擇Add Port Channel按鈕,如下圖所示:

Overview I	nterfaces Logical Devices Security Engine Platform Settings	System	Tools	Help	admin
CONSOLE	Network Module 1 Network Module 2 1 3 5 7 MGMT USB 2 4 6 8				
All Interfaces	Hardware Bypass				
			0	Add Port	Channel

步驟 1.建立埠通道資料介面。

建立一個新的連線埠通道介面,如下圖所示:

埠通道ID	10
類型	資料
啟用	是
成員ID	Ethernet1/1、Ethernet 1/2

埠通道ID為1到47之間的值。

Search and Search

Add Port Ch	annel						? ×
Port Channel ID:	10		Enable				
Type:	Data	¥		1			
Admin Speed:	10gbps	v					
Interfaces							
Ava	ailable Interface				Member ID		
	Search	2			Ethernet1/1	6	
	Ethernet1/1				Ethernet1/2	6	
1.00	Ethernet1/2						
	Ethernet1/6		2				
	Ethernet1/7		5				
	Ethernet1/8		Add				
	Ethernet2/1		Interface				
	Ethernet2/2						

驗證如下圖所示。

Overview Interfaces	Logical Device	es Security Engir	ne Platform Settings				
Network Module 1 Network Module 2 I 3 5 7 CONSOLE IIII 3 5 7 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII							
All Interfaces Hardware By	ypass						
Interface	Туре	Admin Speed	Operational Speed	Application	Operation State	Admin State	
М мбмт	Management					Enabled	
Port-channel10	data	10gbps	10gbps		up	Enabled	
Ethernet1/1					up		
Ethernet1/2					up		

步驟 2.建立管理介面。

在Interfaces索引標籤上,選擇介面,選擇Edit,然後設定管理介面,如下圖所示:

Edit Interface - Ethernet1/3								
Name:	Ethernet1/3 Zenable							
Type:	mgmt	~						
Admin Speed:	10gbps							
	OK Cancel							

任務5.建立和配置新的邏輯裝置

任務需求

建立FTD作為獨立邏輯裝置並進行部署。

解決方案

步驟 1.新增邏輯裝置。

導覽至Logical Devices索引標籤,然後選擇Add Device按鈕以建立新的邏輯裝置,如下圖所示:

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings	System	Tools	Help	admin
					C Refre	sh	Add D	evice
No logical devi	ces available. Cl	ick on Add Device to add	a new logical device.					

使用圖中所示的設定設定FTD裝置:

裝置名稱	FTD
模板	Cisco Firepower威脅防禦

映像版本

6.1.0.330

Add Device			?×
Device Name:	FTD		
Template:	Cisco Firepower Threat Defense	~	
Image Version:	6.1.0.330	~	
Device Mode:	Standalone		
	ок)(Cancel

步驟 2.引導邏輯裝置。

建立邏輯裝置後,將顯示Provisioning - device_name視窗。選擇裝置圖示以啟動配置,如下圖所示 。

C	Overview	Interfaces	Logic	al Devices	Security Engine	Platform Setting	s	System	Tools	Help	admin
FS	P <mark>rovisionin</mark> tandalone	<mark>g - FTD</mark> Cisco Firep	ower Tl	nreat Defense	e 6.1.0.330			Sav	/e	Cance	el
C	ata Ports										
	Ethernet1/4										
	Ethernet1/5							Click	her	6	
	Ethernet1/6							CHCK	nei	C	4.1
	Ethernet1/7										
	Ethernet1/8										
	Ethernet2/1										
	Ethernet2/2										
	Ethernet2/3										
	Ethernet2/4					FTD - 6.1.0.3	30				
	Ethernet2/5					Click to configu	re				
	Ethernet2/6										
	Ethernet2/7										
	Ethernet2/8										
	Ethernet3/1										
	Ethernet3/2										
	Ethernet3/3										
	Ethernet3/4										
	Port-channel	10									
	Applicati	on Versi	on I	Management II	P Gateway I	Management Port	Status				
Ξ	FTD	6.1.0.	330								

設定FTD General Information索引標籤,如下圖所示:

管理介面	Ethernet1/3
地址型別	僅限IPv4
管理IP	10.62.148.84
網路遮罩	255.255.255.128
網路閘道	10.62.148.1

Cisco Firepower Threat Defense - Configuration										
General Information Settings Agreement										
Interface Information										
Management Interface:	Ethemet1/3									
Management										
Address Type:	IPv4 only									
IPv4										
Management IP:	10.62.148.84									
Network Mask:	255.255.255.128									
Network Gateway:	10.62.148.1									

設定FTD Settings索引標籤,如下圖所示:

註冊金鑰	思科
密碼	Pa\$\$w0rd
Firepower管理中心IP	10.62.148.50
搜尋域	cisco.com
防火牆模式	循路
DNS伺服器	192.168.0.1
完全限定的主機名	FTD4100.cisco.com
事件介面	-

Cisco Firepower Threat Defense - Configuration General Information Settings Agreement								
Registration Key:	•••••							
Password:	•••••							
Firepower Management Center IP:	10.62.148.50							
Search domains:	cisco.com							
Firewall Mode:	Routed	*						
DNS Servers:	192.168.0.1							
Fully Qualified Hostname:	FTD4100.cisco.com							
Eventing Interface:		~						

確保Agreement被接受,然後選擇OK。

步驟 3.分配資料介面。

展開Data Ports區域,選擇要分配給FTD的每個介面。在此案例中,指派了一個介面(Portchannel10),如下圖所示:

0	verview	Interfaces	Log	ical Device	Security Engine	e Platforr	n Settings		System	Tools	Help	admin
Pi St	r <mark>ovisionin</mark> tandalone	i g - FTD e Cisco Fireț	power	Threat Defei	nse 6.1.0.330				Sav	/e	Cance	el
Da	ata Ports											
E	thernet1/4											
E	thernet1/5											
E	thernet1/6											
E	thernet1/7											
E	thernet1/8											
E	thernet2/1											
E	thernet2/2											
E	thernet2/3											
E	thernet2/4			Port-			FT	D - 6.1.0.33	30			
E	thernet2/5			citamicizo g			c	Ethernet1/3	a			
E	thernet2/6							and to comigar	-			
E	thernet2/7											
E	thernet2/8											
E	thernet3/1											
E	thernet3/2											
E	thernet3/3											
E	thernet3/4											
P	ort-channel	10										
	Applicati	0.0	Vo	rsion	Management IP	Catoway	Managen	ent Port	Statu	c .		
	ETD	U.I.		0.220	10.62.148.94	10 62 148 1	Ethornott	/2	Statu			
-	Dorte		0.1	1.0.330	10.02.140.04	10.02.140.1	chemeti/	3				
	Ports:	Interfaces	Dent	channel 10								
	Data	interfaces:	Port	-channel10								

選擇Save以完成配置。

步驟 4.監控安裝過程。

以下為從FCM UI進行監控時FTD安裝進行的方式,如下圖所示:

0	verview	Interfaces	Logical Devices	Security Eng	ine Platform	Settings			System	Tools	Help	admin
									C Refi	resh	Add	Device
6	FTD		Standalone	Status: ok							P+ 4	/
	Applica	ation	Version	Mai	nagement IP	Gateway	Management Port	Status				
6	FTD		6.1.0.330	10.6	52.148.84	10.62.148.1	Ethernet1/3	🐝 installing	Disable	e) 🖗		
	Port	5:										
	Da	ita Interfaces:	Port-channel10									

Ove	erview Interfaces	Logical Devi	ces Secu	rity Engine P	latform Set	tings		System T	ools Help admin
								C Refresh	Add Device
	FTD	Standalone	Status: ok						۶.
	Application	Version		Management IP	Gateway	Management Port	Status		
•	FTD	6.1.0.330		10.62.148.84	10.62.148.1	Ethernet1/3	🚇 offline	Enabled	
	Ports:								
	Data Interfaces:	Port-channel10)						
Ove	erview Interfaces	Logical Devi	ces Secu	rity Engine P	latform Set	tings		System T	ools Help admin
		-						C Refresh	Add Device
	FTD	Standalone	Status: ok						۶.
	Application	Version		Management IP	Gateway	Management Port	Status		
	FTD	6.1.0.330		10.62.148.84	10.62.148.1	Ethernet1/3	🐝 starting	Enabled 🌒 😤	
	Ports: Data Interfaces:	Port-channel 10)						
			-						
Ove	erview Interfaces	Logical Devi	ces Secu	rity Engine P	latform Set	tings		System T	ools Help admin
								C Refresh	Add Device
	FTD	Standalone	Status: ok					C Refresh	Add Device
	FTD	Standalone Version	Status: ok	Management IP	Gateway	Management Port	Status	C Refresh	Add Device
•	FTD FTD	Standalone Version 6.1.0.330	Status: ok	Management IP 10.62.148.84	Gateway 10.62.148.1	Management Port Ethernet1/3	Status Started	C Refresh	Add Device
•	FTD FTD Ports:	Standalone Version 6.1.0.330	Status: ok	Management IP 10.62.148.84	Gateway 10.62.148.1	Management Port Ethernet1/3	Status Started	C Refresh	Add Device

從Firepower CLI監控安裝過程:

<#root>
FPR4100#
connect module 1 console
Telnet escape character is '~'. Trying 127.5.1.1 Connected to 127.5.1.1. Escape character is '~'.
CISCO Serial Over LAN: Close Network Connection to Exit
Cisco FTD: CMD=-start, CSP-ID=cisco-ftd.6.1.0.330ftd_001_JAD19500F7YHCNL7715, FLAG=''
Cisco FTD starting
Registering to process manager VNICs requested: 9,22 Cisco FTD started successfully. Cisco FTD initializing Firepower-module1>Setting up VNICs

Found Firepower management vnic 18. No Firepower eventing vnic configured. Updating /ngfw/etc/sf/arc.conf ... Deleting previous CGroup Configuration ... Initializing Threat Defense ... [OK] Starting system log daemon... Г ОК 1 Stopping mysql... Dec 12 17:12:17 Firepower-module1 SF-IMS[14629]: [14629] pmtool:pmtool [ERROR] Unable to connect to UNI Starting mysql... Dec 12 17:12:17 Firepower-module1 SF-IMS[14641]: [14641] pmtool:pmtool [ERROR] Unable to connect to UNI Flushing all current IPv4 rules and user defined chains: ...success Clearing all current IPv4 rules and user defined chains: ...success Applying iptables firewall rules: Flushing chain `PREROUTING' Flushing chain `INPUT' Flushing chain `FORWARD' Flushing chain `OUTPUT' Flushing chain `POSTROUTING' Flushing chain `INPUT' Flushing chain `FORWARD' Flushing chain `OUTPUT' Applying rules successed Flushing all current IPv6 rules and user defined chains: ...success Clearing all current IPv6 rules and user defined chains: ...success Applying ip6tables firewall rules: Flushing chain `PREROUTING' Flushing chain `INPUT' Flushing chain `FORWARD' Flushing chain `OUTPUT' Flushing chain `POSTROUTING' Flushing chain `INPUT' Flushing chain `FORWARD' Flushing chain `OUTPUT' Applying rules successed Starting nscd... mkdir: created directory '/var/run/nscd' Г ОК 1 Starting , please wait.....complete. Firstboot detected, executing scripts OK Executing S01virtual-machine-reconfigure Г ٦ ОК Executing S02aws-pull-cfg Ε ٦ Executing S02configure_onbox Ε OK] Executing SO4fix-httpd.sh Ε 0K] Executing SO6addusers Ε ОК ٦ Executing S07uuid-init OK Ε] Executing SO8configure_mysql Ε 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 S09database-init Ε OK] Executing S11database-populate Ε OK ٦ Executing S12install_infodb Г OK ٦ Executing S15set-locale.sh Ε OK ٦ Executing S16update-sensor.pl Ε OK] Executing S19cert-tun-init Ε OK] Executing S20cert-init Г OK 1

Executing S21disable_estreamer	Ε	OK]		
Executing S25create_default_des.pl	Γ	OK]		
Executing S30init_lights_out_mgmt.pl	Γ	OK]		
Executing S40install_default_filters.pl	Ε	ОК]		
Executing S42install_default_dashboards.pl	Ε	ОК]		
Executing S43install_default_report_templates.pl	Ε	ОК]		
Executing S44install_default_app_filters.pl	Ε	OK]		
Executing S45install_default_realms.pl	Ε	ОК]		
Executing S47install_default_sandbox_E0.pl	Ε	ОК]		
Executing S50install-remediation-modules	Ε	ОК]		
Executing S51install_health_policy.pl	Ε	OK]		
Executing S52install_system_policy.pl	Ε	OK]		
Executing S53change_reconciliation_baseline.pl	Ε	OK]		
Executing S70remove_casuser.pl	Ε	OK]		
Executing S70update_sensor_objects.sh	Γ	OK]		
Executing S85patch_history-init	Ε	OK]		
Executing S90banner-init	Γ	OK]		
Executing S96grow_var.sh	Γ	OK]		
Executing S96install_vmware_tools.pl	Γ	OK	נ		
***** Attention ********					
Initializing the system's localization settings. Depending on av	aila	ble			
system resources (CPU, memory, and disk), this may take 10 minute	S	~			
or more to complete.					
********* Attention *********					
Executing S96localize-templates	Ε	OK]		
Executing S96ovf-data.pl	Ε	OK]		
Executing S97compress-client-resources	Ε	OK]		
Executing S97create_platinum_forms.pl	Ε	OK]		
Executing S97install_cas	Ε	OK]		
Executing S97install_cloud_support.pl	Ε	OK]		
Executing S97install_geolocation.pl	Ε	OK]		
Executing S97install_ssl_inspection.pl	Ε	OK]		
Executing S97update_modprobe.pl	Ε	OK]		
Executing S98check-db-integrity.sh	Ε	OK]		
Executing S98htaccess-init	Ε	ОК]		
Executing S98is-sru-finished.sh	Ε	ОК]		
Executing S99correct_ipmi.pl	Ε	ОК]		
Executing S99start-system	Ε	ОК]		
Executing S99z_db_restore	Ε	ОК]		
Executing S99_z_cc-integrity.sh	Ľ	OK]		
Firstboot scripts finished.	_		_		
Configuring NTP]	OK]		
insmod: ERROR: could not insert module /lib/modules/kernel/drivers/u	10/1	gb_u	10.	ko: File exists	
rw console=ttyS0,38400 loglevel=2 auto kstack=128 reboot=force panic	=1 i	de_g	ene	ric.probe_mask=0x1 i	del=
Fru Size : 512 bytes					
Done					
VNIC command successful					
VNIC command successful					
fatattr: FAI_10CIL_GEI_AITRIBUTES: Inappropriate foct for device					
Tatattr: can't open '/mnt/disk0/.private2': No such file or director	У				
<pre>tatattr: can't open /mnt/diskU/.ngtw': No such file or directory</pre>					
Model reconfigure detected, executing scripts					
Pinging mysql					
Found mysql is running	-	011	-		
Executing 45update-sensor.pl	L	UK	Ţ		
Executing Sprecalculate_arc.pl	L	UK	L		
Mon Dec 12 17:16:15 UIC 2016					
Starting MySQL					
ringing mysql					

Pinging mysql, try 1 Found mysql is running Detecting expanded storage... Running initializeObjects... Stopping MySQL... Killing mysqld with pid 32651 Wait for mysqld to exit\c done Mon Dec 12 17:16:21 UTC 2016 Starting sfifd... [OK] Starting Cisco Firepower 4140 Threat Defense, please wait...No PM running! ...started. Cisco FTD initialization finished successfully. ... output omitted ... Reading from flash... Cryptochecksum (changed): blabfa7e 63faee14 affdddb0 9bc9d8cd INFO: Power-On Self-Test in process. INFO: Power-On Self-Test complete. INFO: Starting HW-DRBG health test (DRBG 0)... INFO: HW-DRBG health test (DRBG 0) passed. INFO: Starting HW-DRBG health test (DRBG 1)... INFO: HW-DRBG health test (DRBG 1) passed. INFO: Starting SW-DRBG health test... INFO: SW-DRBG health test passed. Firepower-module1> Firepower-module1> show services status Services currently running: Feature | Instance ID | State | Up Since _____ ftd | 001_JAD19500F7YHCNL7715 | RUNNING | :00:08:07

任務6.將FTD註冊到Firepower管理中心(FMC)

任務需求

在FMC中註冊FTD。

解決方案

步驟 1.驗證FTD和FMC之間的基本連線。

將FTD註冊到FMC之前,請驗證FTD和FMC之間的基本連線:

<#root>

Firepower-module1>

connect ftd

Connecting to ftd console... enter exit to return to bootCLI

>

ping system 10.62.148.50

PING 10.62.148.50 (10.62.148.50) 56(84) bytes of data. 64 bytes from 10.62.148.50: icmp_seq=1 ttl=64 time=0.133 ms 64 bytes from 10.62.148.50: icmp_seq=2 ttl=64 time=0.132 ms 64 bytes from 10.62.148.50: icmp_seq=3 ttl=64 time=0.123 ms

由於啟動程式配置,FTD已配置管理器FMC:

<#root>

>

show managers

Host	: 10.62.148.50
Registration Key	****
Registration	:
pending	
RPC Status	:

步驟 2.將FTD新增到FMC中。

在FMC上,導覽至Devices> Device Management索引標籤,然後導覽至Add... > Add Device,如 下圖所示。

Overview Analysis	Policies	Devices	Object	s AMI	þ	Deploy	ତ Sy	ystem	Help 🔻	admin 🔻
Device Management	NAT	VPN Qo	S Pla	tform Sett	ings					
						By Group		~	(ا	Add
Name			Group	Model	License Type	Access Control Policy		Ad	d Device	
4 🣁 Ungrouped (6)								💿 Ad	d High Av	ailability

設定FTD裝置設定,如下圖所示:

Add Device		?	×							
Host:	10.62.148.84									
Display Name:	FTD4100		ĺ							
Registration Key:	cisco									
Group:	None	~								
Access Control Policy:	FTD4100	~								
Smart Licensing Malware:	•									
Threat:										
URL Filtering:										
 Advanced On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page. 										
	Register Cance	el								

選擇Register按鈕。

在FMC上,檢查Tasks以檢視註冊進度。除註冊外,FMC還:

- 發現FTD裝置(擷取目前的介面組態)。
- 部署初始策略。

成功註冊如下圖所示:

Overview Analysis	Policies	Devic	ces	Objects	AMP				Deploy	🛛 S	System	Help 🔻	admiı	• •
Device Management	NAT	VPN	QoS	Platfor	m Settings									
									By Group		*	٢	Add	•
Name						Group	Model	License Type	Access Con	trol Poli	icy			
 Ungrouped (7) FTD4100 10.62.148.84 - Cisco Firepower 4140 Threat Defense - v6.1.0 - routed 							Cisco Fir	Base, Threat, Ma	FTD4100		b	۶ (

◆註:在6.1版中,引入了Firepower裝置管理器(FDM)以提供機上管理。Firepower裝置上安裝的FTD無法由FDM管理。

任務7.升級FTD

任務需求

將FTD從6.1.0.330升級到6.1.0.1。

解決方案

步驟 1.驗證相容性。

檢查FXOS版本說明,確保目標FTD版本與FXOS軟體相容。如果需要,請首先升級FXOS軟體。

步驟 2.升級FTD。

FTD軟體由FMC管理,而不是FCM。若要升級FTD模組,請連線到FMC,導覽至System > Updatespage,然後選擇Upload Update,如下圖所示。

Overview	Analysis	Policies	Devices	Objects	AMP						Deploy		System
						Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health	v Mo
Product (Updates	Rule Up	dates	Geolocation	Updates								
					Current	y running software	version: 6.	1.0					
			Updat	Updates									
				Upload	software up	dates and patches	here.						
				Packag	e	Choose File Cis Upload Ca	co_FTD_SS	1.0.1-53.sh					

在FTD模組上安裝更新,如下圖所示:

Overview Ar	nalysis P	olicies	Devices	Objects	AMP						Deploy		System
						Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health	r Mo
Product Upd	lates R	Rule Upd	lates	Geolocation	Update	s							
											(🗿 Uploa	d Update
Currently running	Currently running software version: 6.1.0												
Updates													
Туре						Version	Date			Release Not	es <u>Reboot</u>		
Sourcefire Vulnerability And Fingerprint Database Updates						275	Wed	Nov 16 16:50	:43 UTC 2016		No		1
Cisco FTD SSP Patch						6.1.0.1-53	Fri De	ec 2 17:37:52	UTC 2016		Yes		14

或者,您可以啟動準備情況檢查:

Product Upd	ates	Rule Updates	Geolocation Updates		
				Currently running software ve	ersion: 6.1.0
Selected Upd	late				
Type Version Date Release Notes Reboot	Cisco I 6.1.0.1 Fri Dec Yes	FTD SSP Patch I-53 : 2 17:37:52 UTC 2016			By Group V
🗹 🔻 Ungrouped	l (1 tota	al)			
FTD4100 10.62.148.84	- Cisco I	Firepower 4140 Threat [Defense v6.1.0	Health Policy Initial Health Policy 2 12:21:09	016-11-21 🤡 😒
				Launch Readiness Check	Install Cancel

成功的就緒性檢查如下圖所示:

Readiness Check Status
Current Version: 6.1
Update Version: 6.1.0.1-53
Readiness Check Complete
Total 1 devices Selected
FTD4100 10.62.148.84 - Cisco Firepower 4140 Threat Defensev6.1.0
Status Log:Readiness Check To 10.62.148.84 Success

若要開始升級程式,請按一下Install,如下圖所示:

Product Upd	ates Ru	le Updates	Geolocation Updates		
			Currently running s	oftware version: 6.1.0	
Selected Up	date				
Type Version Date Release Notes Reboot	Cisco FTD SS 6.1.0.1-53 Fri Dec 2 17: Yes	5P Patch :37:52 UTC 2016		By Group	▼.
🕑 🔻 Ungroupe	d (1 total)				
✓ FTD4100 10.62.148.84	- Cisco Firepo	wer 4140 Threat D	Defense v6.1.0	Health Policy Initial Health Policy 2016-11-21 © 12:21:09)
				Launch Readiness Check Install Cance	<u>ا</u>

升級需要FTD重新開機,如下圖所示:

10.62.148.50 says:		×
Update installation will reboot the system(s).	Are you sure you w	ant to continue?
	ок	Cancel

與FTD安裝類似,您可以從FMC UI(任務)監控FTD升級程式。升級進度可在FTD CLI(CLISH模式)中追蹤。

升級完成後,將原則部署到FTD,如下圖所示:

				Depk	oy 📀	System	Help 🔻	admi	in v
De	eployments	Health	Tasks					٥	?
2	0+ total)	0 waiting	0 running	0 retrying	20+ su	ccess 0 f	ailures		
~	Remote Instal						12m :	55s X	-
	Apply to 1 Please rea	0.62.148.8 pply polici	4. es to your i	managed de	vices.				

驗證

在FMC UI中,如下圖所示:

Overview Ana	alysis A	Policies	Devi	ces O	bjects	AMP	
Device Manager	ment	NAT	VPN	QoS	Platform	Settings	
Name							Group
 Ungrouped (7) FTD4100 10.62.148.84 - Cisco Firepower 4140 Threat Defense v6.1.0.1 route 							

在FCM UI中,如下圖所示:

Ove	erview	Interfaces	Logical Devices	Security Engine	Platform Settings
_					
FTD Star		Standalone	Status: ok		
	Applica	tion	Version	Ma	magement IP
•	FTD		6.1.0.1.53	10	.62.148.84

在機箱CLI上:

<#root>						
FPR4100#						
scope ssa						
FPR4100 /ssa #						
show app-instance						
Application Name	Slot ID	Admin State	Operational State	Running Version	Startup Version C	:1
ftd	1	Enabled	Online			_
6.1.0.1.53						
6.1.0.330	Not Applicable					

在FTD CLI上:

```
FPR4100#
```

connect module 1 console Telnet escape character is '~'. Trying 127.5.1.1... Connected to 127.5.1.1. Escape character is '~'. CISCO Serial Over LAN: Close Network Connection to Exit > show version -----[FTD4100.cisco.com]------Mode1 : Cisco Firepower 4140 Threat Defense (76) Version 6.1.0.1 (Build 53) UUID : 22c66994-c08e-11e6-a210-931f3c6bbbea Rules update version : 2016-03-28-001-vrt VDB version : 275 _____

>

Firepower 2100

Firepower 2100上的FTD使用包含FXOS和FTD映像的單一套件組合。因此,安裝和升級程式與 FP4100/FP9300不同。

FP2100上的FTD安裝

有4種不同的過程,具體取決於具體情況:

- 案例1:使用相同的FTD映像清除配置並重新啟動系統。
- 案例2:使用新的應用軟體版本重新映像系統。
- 案例3:將系統重新映像為其出廠預設設定。
- 案例4:將系統重新映像為其出廠預設設定(管理員密碼恢復)。

有關每個案例及其過程的詳細資訊,請檢視:

<u>重新映像過程</u>

案例2為大部分FTD安裝案例服務,而案例3(格式化和從ROMMON啟動)可用於特定案例(例如 ,系統不穩定或處於啟動環路等)。

FP2100上的FTD升級

由於沒有單獨的FXOS套件,要升級FP2100上的FTD,請執行以下步驟:

步驟 1.驗證相容性。

如果FTD由FMC(盒外管理)管理,請檢查軟體目標FTD版本說明中的「相容性」部分。

步驟 2.如有需要,首先升級FMC。始終運行等於或高於FTD目標軟體版本的FMC軟體版本。

步驟 3.升級FTD。

使用與FP4100/9300相同的步驟。升級FTD前須閱讀的重要檔案:

• FTD版本說明(例如,如果要升級到6.3.0.2版,請檢視6.3.0.2版說明以驗證升級路徑和所有相 關詳細資訊。)

<u>版本資訊</u>

• FMC升級指南(章節:升級Firepower威脅防禦:其他裝置)

思科Firepower管理中心升級指南6.0-7.0版

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無特定資訊可用於排解此組態的疑難問題。

相關資訊

- FXOS相容性指南
- <u>思科Firepower NGFW文檔</u>
- <u>技術支援與文件 Cisco Systems</u>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。