在FP9300(機箱內)上配置FTD集群

目錄

簡介 必要條件 需求 採用元件 背景資訊 設定 網路圖表 任務1.為FTD集群建立必要的介面 任務2.建立FTD集群 任務3.向FMC註冊FTD集群 任務4.在FMC上配置埠通道子介面 任務5.檢驗基本連通性 從機箱管理器UI捕獲群集 任務6.從群集中刪除從屬裝置 驗證 疑難排解 相關資訊

簡介

本文檔介紹如何在FPR9300裝置上配置和驗證集群功能。

注意:本文檔中提供的資訊涵蓋集群的初始安裝/配置。本文檔不適用於部件更換(退貨審批 — RMA)過程

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:

- 執行1.1(4.95)的Cisco Firepower 9300安全裝置
- 執行6.0.1的Firepower威脅防禦(FTD)(內部版本1213)
- 運行6.0.1.1的FireSIGHT管理中心(FMC)(內部版本1023)

實驗完成時間:1小時。

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

- •在搭載FTD裝置的FPR9300上,您可以在所有支援的版本上設定機箱內集群。
- •6.2引入了機箱間集群。
- •埠通道48建立為集群控制鏈路。對於機箱內集群,此連結利用Firepower 9300背板進行集群通訊。
- •除管理介面外,不支援單個資料介面。
- •管理介面分配給集群中的所有裝置。

設定

網路圖表



任務1.為FTD集群建立必要的介面

工作需求:

建立集群、管理介面和埠通道資料介面。

解決方案:

步驟1.建立埠通道資料介面。

要建立新介面,您必須登入到FPR9300 Chassis Manager並導航到Interfaces頁籤。

選擇Add Port Channel,然後使用以下引數建立新的埠通道介面:

| 埠通道ID | 5 |
|-------|--------------------------|
| 類型 | 資料 |
| 啟用 | 是 |
| 成員ID | Ethernet1/3、Ethernet 1/4 |

選擇OK以儲存配置,如下圖所示。

| Add Port Chan | nel | | | | ? X |
|---|---------------|---|--------------|-----|--------|
| Port Channel ID: 5 | 5 | 🗹 Enable | | | |
| Туре: [| Data 💌 | | | | |
| Speed: 1 | 1gbps 🗸 | | | | |
| Interfaces | | _ | | | |
| Availa | ble Interface | | Member ID | | |
| Sec. Sec. Sec. Sec. Sec. Sec. Sec. Sec. | earch | | Ethernet | 1/3 | |
| III Et | thernet1/2 | | III Ethernet | 1/4 | |
| | thernet1/3 | l de la companya de l | | | 1 |
| Et | thernet1/4 | | | | |
| III Et | thernet1/5 | | | | |
| III Et | thernet1/6 | Add Tabadaaa | | | |
| III Et | thernet1/7 | Add Interface | | | |
| | thernet1/8 | | | | |
| III Et | thernet2/1 | | | | |
| III Et | thernet2/2 | | | | |
| III Et | thernet2/3 | | | | |
| Et Et | thernet2/4 | | | | |
| Et Et | thernet3/1 | | | | |
| Et Et | thernet3/2 | | | | |
| | | | | | |
| | | | | | |
| | | | | ОК | Cancel |

步驟2.建立管理介面。

在Interfaces頁籤上,選擇介面,按一下Edit並配置管理型別介面。

按一下「OK」以儲存組態,如下圖所示。

| Edit Inte | erface - Ethernet1 | /1 ?× Enable |
|-----------|--------------------|-----------------|
| Type: | mgmt | * |
| Speed: | 1gbps | * |
| | ок | Cancel |

步驟3.建立集群控制鏈路介面。

按一下「Add Port Channel」按鈕,用這些引數建立一個新的連線埠通道介面,如下圖所示。

| 埠通道ID | 48 |
|-------|----|
| 類型 | 叢集 |
| 啟用 | 是 |
| 成員ID | - |

| Add Port Cha | annel | | | | ?× | | |
|------------------|-------------------|---------------|-----------|----|--------|--|--|
| Port Channel ID: | 48 | C Enable | | | | | |
| Type: | Cluster |] | | | | | |
| Speed: | 1gbps 👻 |] | ÷ | | | | |
| Interfaces | Interfaces | | | | | | |
| Av | ailable Interface | | Member ID | | | | |
| | Search | | | | | | |
| | Ethernet1/2 | | | | | | |
| | Ethernet1/5 | | | | | | |
| | Ethernet1/6 | | | | | | |
| | Ethernet1/7 | | | | | | |
| | Ethernet1/8 | | | | | | |
| | Ethernet2/1 | Add Interface | | | | | |
| | Ethernet2/2 | | | | | | |
| | Ethernet2/3 | | | | | | |
| | Ethernet2/4 | | | | | | |
| | Ethernet3/1 | | | | | | |
| | Ethernet3/2 | | | | | | |
| | Ethernet3/3 | | | | | | |
| | Ethernet3/4 | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | ОК | Cancel | | |

任務2.建立FTD集群

工作需求:

建立FTD集群裝置。

解決方案:

步驟1.導覽至Logical Devices,然後按一下Add Device按鈕。

建立FTD集群,如下所示:

| FTD_cluster |
|---------------------|
| Cisco Firepower威脅防禦 |
| 6.0.1.1213 |
| 叢集 |
| |

若要新增裝置,請按一下OK,如下圖所示。

| Add Device | | | ?× |
|----------------|--------------------------------|---|--------|
| Device Name: | FTD_cluster | | |
| Template: | Cisco Firepower Threat Defense | ~ | |
| Image Version: | 6.0.1.1213 | ~ | |
| Device Mode: | 🔵 Standalone 💿 Cluster | | |
| | | _ | |
| | ОК | | Cancel |

步驟2.配置和部署FTD集群。

建立FTD裝置後,系統會將您重新導向至Provisioning- device_name視窗。

按一下裝置圖示以啟動組態,如下圖所示。

| 0 | verview | Interfaces Log | ical Devices | Security Mo | lules Platform Settings | | | | System | Tools | Help | admin |
|-----|-----------------------|--------------------------------------|----------------|-------------|-------------------------|---------|-----------------|-----------|--------|-------|-------|-------|
| e l | rovisionin ustered | g - FTD_cluster Cisco Firepower 1 | Threat Defense | 6.0.1.1213 | | | | | Sav | _ | Canod | |
| D | ata Ports | - | | | | | | | | | | |
| 1 | Ethernet1/2 | | | | | | | | | | | |
| 10 | Ethernet1/S | | | | | | | | | | | |
| 10 | Ethernet1/6 | | | | | | C | | | | | |
| 0 | Ethernet1/7 | | | | | | | | | | | |
| | Ethernet1/8 | | | | | | | | | | | |
| | Ethernet2/1 | | | | | | | | | | | |
| | Ethernet2/2 | | | | | | FTD - 6.0.1 | 1.1213 | | | | |
| | Ethernet2/3 | | | | | | Security Mode | ile 1,2,3 | | | | |
| | Ethernet2/4 | | | | | | | | | | | |
| | Ethernet3/2 | | | | | | | | | | | |
| | Ethernet3/3 | | | | | | | | | | | |
| | Ethernet3/4 | | | | | | | | | | | |
| | Port-channel! | | | | | | | | | | | |
| | | | | _ | | | | | | | | _ |
| | Security I | todule Applie | ation | Version | Management IP | Gateway | Management Port | Status | | | | |
| 1 | Security M | odule 1 FTD | | 6.0.1.1213 | | | | | | | | |
| u | Security M | odule 2 PTD | | 6.0.1.1213 | | | | | | | | |
| a | Security M | odule 3 PTD | | 6.0.1.1213 | | | | | | | | |

使用以下設定設定FTD Cluster Information索引標籤,如下圖所示。

| 群集金鑰 | 思科 |
|-------|-------------|
| 群集組名稱 | FTD_cluster |
| 管理介面 | Ethernet1/1 |

| Cisco Firepower Thre | eat Defense - Configuration 📧 🗵 |
|------------------------------|-------------------------------------|
| Cluster Information Setti | ngs Interface Information Agreement |
| Security Module(SM) | |
| Security Module-1,Security M | Iodule-2,Security Module-3 |
| Interface Information | |
| Cluster Key: | ••••• |
| Cluster Group Name: | FTD_cluster |
| Management Interface: | Ethernet1/1 |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | OK Cancel |

使用以下設定設定FTD **Settings**索引標籤,如下圖所示。

| 註冊金鑰 | 思科 |
|-----------------|----------------------------|
| 密碼 | Admin123 |
| Firepower管理中心IP | 10.62.148.73 |
| 搜尋域 | cisco.com |
| 防火牆模式 | 循路 |
| DNS伺服器 | 173.38.200.100 |
| 完全限定主機名 | ksec-fpr9k-1-1-3.cisco.com |
| 事件介面 | 無 |
| | |

| Cisco Firepower Three Cluster Information Settings | at Defense - Config Interface Information | uration ?× |
|--|--|------------|
| Registration Key: | | |
| Password: | ••••• | 5 |
| Firepower Management Center IP: | 10.62.148.73 | |
| Search domains: | cisco.com | |
| Firewall Mode: | Routed | • |
| DNS Servers: | 173.38.200.100 | |
| Fully Qualified Hostname: | ksec-fpr9k-1-1-3.cisco.co | m |
| Eventing Interface: | None | ~ |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | OK | Cancel |

使用這些設定設定FTD Interface Information索引標籤,如下圖所示。

| 地址型別 安全描知1 | 僅限IPv4 |
|---------------|-----------------|
| 安王侯和 管理IP | 10.62.148.67 |
| 網路掩碼 | 255.255.255.128 |
| 閘道 | 10.62.148.1 |
| 安全模組2 | |
| 管理IP | 10.62.148.68 |
| 網路掩碼 | 255.255.255.128 |
| 閘道 | 10.62.148.1 |
| 安全模組3 | |
| 管理IP | 10.62.148.69 |
| 網路掩碼 | 255.255.255.128 |
| 閘道 | 10.62.148.1 |

| Cisco Firepower Threat Defense - Configuration | | | | | |
|--|---------------------------------|--|--|--|--|
| Cluster Information Settings | Interface Information Agreement | | | | |
| Address Type: | IPv4 only | | | | |
| Security Module 1 | | | | | |
| Management IP: | 10.62.148.67 | | | | |
| Network Mask: | 255.255.255.128 | | | | |
| Gateway: | 10.62.148.1 | | | | |
| Security Module 2 | | | | | |
| Management IP: | 10.62.148.68 | | | | |
| Network Mask: | 255.255.255.128 | | | | |
| Gateway: | 10.62.148.1 | | | | |
| Security Module 3 | | | | | |
| Management IP: | 10.62.148.69 | | | | |
| Network Mask: | 255.255.255.128 | | | | |
| Gateway: | 10.62.148.1 | | | | |
| | | | | | |
| | | | | | |
| | OK Cancel | | | | |

接受「**Agreement**」頁籤上的「Agreement」,然後按一下**OK**,如下圖所示。

| Cisco Firepower Threat Defense - Configuration |
|---|
| Cluster Information Settings Interface Information |
| |
| |
| End User License Agreement |
| IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT. |
| CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE |
| I understand and accept the agreement |
| |
| OK Cancel |

步驟3.將資料介面分配給FTD。

展開「Data Ports(資料埠)」區域,然後點選要分配給FTD的每個介面。完成後,選擇**Save**以建 立FTD集群,如下圖所示。

| 0 | verview Interface: | Logical Device | Security Modules Pla | atform Settings | | | | System Tools | Help admin |
|----|---|------------------------------|----------------------|-------------------|-------------|-----------------|----------|--------------|------------|
| P | rovisioning - FTD_clu lustered Cisco Firej | uster power Threat Defens | ie 6.0.1.1213 | | | | | Save | Cancel |
| D | ata Ports | | | | | | | | 1 |
| I. | Ethernet1/7 | | | | | | | | |
| IJ | Ethernet1/8 | | | | | | | | |
| IJ | Ethernet2/1 | | | | | | | | |
| ļ | Ethernet2/2 | | | | | | | | |
| U. | Ethernet2/3 | _ | | Port- channel5 | | _ | | | |
| U. | Ethernet2/4 | _1 | | | | | | | |
| Į, | Ethernet3/1 | _1 | | | | FTD - 6.0.1 | .1213 | | |
| I. | Ethernet3/2 | | | But | | Security Mod | /e 1,2,3 | | |
| l, | Ethernet3/3 | -1 | | channel48 | | _ | | | |
| | Ethernet3/4 | | | | | | | | |
| | Port-channel48 | | | | | | | | |
| Ľ | Port-channels | | | | | | | | _ |
| | Security Module | Application | Version | Management IP | Gateway | Management Port | Status | | |
| 9 | Security Module 1 | FTD | 6.0.1.1213 | 10.62.148.67 | 10.62.148.1 | Ethernet1/1 | | | |
| | Cluster Interfaces: | Port-channel48 | | | | | | | |
| 9 | Security Module 2 | FTD | 6.0.1.1213 | 10.62.148.68 | 10.62.148.1 | Ethernet1/1 | | | |
| | Cluster Interfaces: | Port-channel48 | | | | | | | |
| ۲ | Security Module 3 | FTD | 6.0.1.1213 | 10.62.148.69 | 10.62.148.1 | Ethernet1/1 | | | |
| | Cluster Interfaces: | Port-channel48 | | | | | | | |

等待幾分鐘以部署集群,然後進行主裝置選擇。

• ,如下圖所示。

| 0 | erview Interface | s Logical Device | Security Module | s Platform Settings | | | | System Tools Help admin |
|---|---|-------------------------------------|-----------------|--|---|------------------|--------|-------------------------|
| ۲ | FTD_cluster | Clustered | Status: ok | | | | | C Refresh O Add Device |
| | Security Module | Application | Version | Management IP | Gateway | Management Port | Status | |
| | Security Module 1 | FTD | 6.0.1.1213 | 10.62.148.67 | 10.62.148.1 | Ethernet1/1 | online | Endlief 🔵 🏞 |
| | Ports: Data Interfaces: Cluster Interface | Port-channel5 es: Port-channel48 | | Attributes: Cluster Operational St Firepower Management Cluster Role Management URL UUID | tus : in-cluster t IP : 10.62.148.67 : primary : https://10.62.148.73/ : b2a42bba-5da0-11e6-al | 11e-efdb62t3eab1 | | |
| | Security Module 2 | FTD | 6.0.1.1213 | 10.62.148.68 | 10.62.148.1 | Ethernet1/1 | online | Euthel 🕒 A |
| | Ports: Data Interfaces: Cluster Interface | Port-channel5 es: Port-channel48 | | Attributes: Cluster Operational Sta Firepower Management Cluster Role Management URL UUID | ttus : in-cluster : IP : 10.62.148.68 : secondary : https://10.62.148.73/ : b2c13764-5da0-11e6-8; | 795-e46e09566c19 | | |
| | Security Module 3 | FTD | 6.0.1.1213 | 10.62.148.69 | 10.62.148.1 | Ethernet1/1 | online | Enabled 🕒 A |
| | Ports: Data Interfaces: Cluster Interface | Port-channel5 es: Port-channel48 | | Attributes: Cluster Operational 5ti Firepower Rolagement Cluster Role Management URL UUID | tus : In-cluster t IP : 10.62.146.69 : secondary : https://10.62.148.73/ : beb5ca06-5da0-11e6-bi | 848-450516116340 | | |

• 從FPR9300 CLI

| FPR9K-1-A# | | | | | |
|--------------------|--------------|-------------|-------------------|----------------|------------|
| FPR9K-1-A# scope s | sa | | | | |
| FPR9K-1-A /ssa # s | how app-inst | ance | | | |
| Application Name | Slot ID | Admin State | Operational State | Running Versio | n Startup |
| Version Cluster Op | er State | | | | |
| | | | | | |
| ftd | 1 | Enabled | Online | 6.0.1.1213 | 6.0.1.1213 |
| In Cluster | | | | | |
| ftd | 2 | Enabled | Online | 6.0.1.1213 | 6.0.1.1213 |
| In Cluster | | | | | |
| ftd | 3 | Enabled | Online | 6.0.1.1213 | 6.0.1.1213 |
| In Cluster | | | | | |
| ± | | | | | |

• 在LINA(ASA)CLI上

```
firepower# show cluster info
Cluster FTD_cluster: On
   Interface mode: spanned
   This is "unit-1-1" in state MASTER
             : 0
       ID
       Version : 9.6(1)
       Serial No.: FLM19216KK6
       CCL IP : 127.2.1.1
       CCL MAC : 0015.c500.016f
       Last join : 21:51:03 CEST Aug 8 2016
       Last leave: N/A
Other members in the cluster:
   Unit "unit-1-3" in state SLAVE
       ID
             : 1
       Version : 9.6(1)
       Serial No.: FLM19206H7T
       CCL IP : 127.2.1.3
       CCL MAC : 0015.c500.018f
       Last join : 21:51:05 CEST Aug 8 2016
       Last leave: N/A
   Unit "unit-1-2" in state SLAVE
```

: 2 ΤD Version : 9.6(1) Serial No.: FLM19206H71 CCL IP : 127.2.1.2 CCL MAC : 0015.c500.019f Last join : 21:51:30 CEST Aug 8 2016 Last leave: N/A firepower# cluster exec show cluster interface-mode cluster interface-mode spanned cluster interface-mode spanned cluster interface-mode spanned firepower# firepower# cluster exec show cluster history From State To State Reason _____ 21:49:25 CEST Aug 8 2016 DISABLED DISABLED Disabled at startup 21:50:18 CEST Aug 8 2016 Enabled from CLI DISABLED ELECTION 21:51:03 CEST Aug 8 2016 MASTER_POST_CONFIG Enabled from CLI ELECTION 21:51:03 CEST Aug 8 2016 MASTER_POST_CONFIG MASTER Master post config done and waiting for ntfy _____ _____ To State From State Reason _____ 21:49:44 CEST Aug 8 2016 DISABLED DISABLED Disabled at startup 21:50:37 CEST Aug 8 2016 DISABLED ELECTION Enabled from CLI 21:50:37 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:41 CEST Aug 8 2016 ONCALL Received cluster control message ELECTION 21:50:41 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:46 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:46 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message

21:50:51 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:51 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:56 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:56 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:01 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:51:01 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:04 CEST Aug 8 2016 ONCALL SLAVE_COLD Received cluster control message 21:51:04 CEST Aug 8 2016 SLAVE_COLD SLAVE_APP_SYNC Client progression done 21:51:05 CEST Aug 8 2016 SLAVE_APP_SYNC SLAVE_CONFIG Slave application configuration sync done 21:51:17 CEST Aug 8 2016 SLAVE_CONFIG SLAVE_BULK_SYNC Configuration replication finished 21:51:29 CEST Aug 8 2016 SLAVE_BULK_SYNC SLAVE Configuration replication finished _____ _____ To State From State Reason _____ 21:49:24 CEST Aug 8 2016 DISABLED DISABLED Disabled at startup 21:50:16 CEST Aug 8 2016 DISABLED ELECTION Enabled from CLI 21:50:17 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:21 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:21 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:26 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:26 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:31 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message

21:50:31 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:36 CEST Aug 8 2016 ONCALL ELECTION 21:50:36 CEST Aug 8 2016 ELECTION ONCALL 21:50:41 CEST Aug 8 2016 ONCALL ELECTION 21:50:41 CEST Aug 8 2016 ELECTION ONCALL 21:50:46 CEST Aug 8 2016 ONCALL ELECTION 21:50:46 CEST Aug 8 2016 ELECTION ONCALL 21:50:51 CEST Aug 8 2016 ONCALL ELECTION 21:50:51 CEST Aug 8 2016 ELECTION ONCALL 21:50:56 CEST Aug 8 2016 ELECTION ONCALL 21:50:56 CEST Aug 8 2016 ELECTION ONCALL 21:51:01 CEST Aug 8 2016 ONCALL ELECTION 21:51:01 CEST Aug 8 2016 ELECTION ONCALL 21:51:06 CEST Aug 8 2016 ONCALL ELECTION 21:51:06 CEST Aug 8 2016 ELECTION ONCALL 21:51:12 CEST Aug 8 2016 ONCALL ELECTION 21:51:12 CEST Aug 8 2016 ELECTION ONCALL 21:51:17 CEST Aug 8 2016 ONCALL ELECTION 21:51:17 CEST Aug 8 2016 ELECTION ONCALL 21:51:22 CEST Aug 8 2016 ONCALL ELECTION 21:51:22 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message

Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message Received cluster control message

21:51:27 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:51:27 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:30 CEST Aug 8 2016 ONCALL SLAVE_COLD Received cluster control message 21:51:30 CEST Aug 8 2016 SLAVE_COLD SLAVE_APP_SYNC Client progression done 21:51:31 CEST Aug 8 2016 SLAVE_CONFIG Slave application configuration sync done SLAVE_APP_SYNC 21:51:43 CEST Aug 8 2016 SLAVE_CONFIG SLAVE_BULK_SYNC Configuration replication finished 21:51:55 CEST Aug 8 2016 SLAVE_BULK_SYNC SLAVE Configuration replication finished _____

firepower#

任務3.向FMC註冊FTD集群

工作需求:

將邏輯裝置新增到FMC,然後將它們分組到集群中。

解決方案:

步驟1.將邏輯裝置新增到FMC。自FMC版本6.3起,您只能註冊一個FTD裝置(建議作為主裝置)。 其餘FTD由FMC自動發現。

登入FMC並導覽至Devices > Device Management索引標籤,然後按一下Add Device。

使用映像中提到的設定新增第一個邏輯裝置。

按一下Register開始註冊。

| Add Device | | ?) | × | | | |
|---|---------------|-----|---|--|--|--|
| Host: | 10.62.148.67 | | | | | |
| Display Name: | FTD1 | | | | | |
| Registration Key: | cisco | | | | | |
| Group: | None | ~ | | | | |
| Access Control Policy: | FTD9300 | ~ | | | | |
| 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 Cano | :el | | | | |

驗證如下圖所示。

| Cisco Firepower 9000 Series SM-36 Threat Defense Cluster | | | / 0 |
|--|---|---------|-----|
| PTD1(primary) 10.62.148.67 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed | Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering | FTD9300 | |
| PTD2 10.62.148.68 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed | Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering | FTD9300 | 8 |
| FTD3 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed | Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering | FTD9300 | 8 |

任務4.在FMC上配置埠通道子介面

工作需求:

為埠通道資料介面配置子介面。

解決方案:

步驟1.在FMC GUI中選擇FTD_cluster Edit按鈕。

導覽至Interfaces索引標籤,然後按一下Add Interfaces> Sub Interface,如下圖所示。

| Overview Analysis Policies De | vices Objects AMP | | | Deploy 🧕 | System Help 🛪 olga 🛪 |
|---|---------------------------|--------------------|-----------------------------|------------|-----------------------------------|
| Device Management NAT VPN | Platform Settings | | | | |
| FTD_cluster | | | | | Seve Cancel |
| Cisco Firepower 9000 Series SM-36 Threat De | lense | | | | |
| Cluster Devices Routing N | AT Interfaces Inline Sets | DHCP | | | |
| 2 | | | | | Add Interfaces • |
| Interface | Logical Name | Type Security Zone | Mac Address(Active/Standby) | IP Address | Sub Interface |
| 10 Port-channel5 | | EtherChannel | | | 1 |
| Port-channel48 | | EtherChannel | | | |
| Ethernet1/1 | diagnostic | Physical | | | 1 |

使用這些詳細資訊配置第一個子介面。選擇OK以應用更改,如下圖所示。

| 名稱 常規頁籤 | INSIDE |
|-------------------|------------------|
| 介面 | Port-channel5 |
| 子介面ID | 201 |
| VLAN ID | 201 |
| IPv4頁籖 | |
| IP型別 | 使用靜態IP |
| IP 位址 | 192.168.75.10/24 |

| Add Sub Inte | erface | | | | | | ? × |
|------------------|--------|---------------|-----------|------------------|-----|----|--------|
| Name: | Inside | | 🗹 Enabled | 🗌 Management O | nly | | |
| Security Zone: | | * |] | - | | | |
| Description: | | | | | | | |
| General IPv | 4 IPv6 | Advanced | | | | | |
| MTU: | | 1500 | | (64 - 9000) | | | |
| Interface *: | | Port-channel5 | * | Enabled | | | |
| Sub-Interface ID |) *: | 201 | | (1 - 4294967295) | | | |
| VLAN ID: | | 201 | | (1 - 4094) | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | OK | Cancel |

| Add Sub Interface | ? × | 2 |
|-------------------|---|---|
| Name: Inside | C Enabled Management Only | |
| Security Zone: | ~ | |
| Description: | | |
| General IPv4 IPv6 | Advanced | |
| IP Type: | Use Static IP | |
| IP Address: | eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25 | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | OK Cancel | |

使用這些詳細資訊配置第二個子介面。

| OUTSIDE |
|------------------|
| |
| Port-channel5 |
| 210 |
| 210 |
| |
| 使用靜態IP |
| 192.168.76.10/24 |
| |

按一下**OK**建立子介面。按一下「**Save**」,然後「**Deploy**」變更至FTD_cluster,如下圖所示。

驗證:

| Overview Analysis Policies Devices Objects AMP | | Deploy 🍳 System Help 🔹 olga 🔹 | | | | | | | |
|--|--|-------------------------------|--|--|--|--|--|--|--|
| Device Management NAT VPN Platform Settings | | | | | | | | | |
| FTD_cluster | | | | | | | | | |
| Cisco Firepower 9000 Series SM-36 Threat Defense | | | | | | | | | |
| Cluster Devices Routing NAT Interfaces Inline Sets | DHCP | | | | | | | | |
| 2 | | Add Interfaces • | | | | | | | |
| Interface Logical Name | Type Security Zone Mac Address(Active/Standby) | IP Address | | | | | | | |
| Port-channel5 | EtherChannel | 1 | | | | | | | |
| Port-channel48 | EtherChannel | 9 | | | | | | | |
| Ethernet1/1 diagnostic | Physical | 1 | | | | | | | |
| Port-channel5.201 Inside | SubInterface | 192.168.75.10/24(Static) | | | | | | | |
| Port-channel5.210 Outside | SubInterface | 192.168.76.10/24(Static) | | | | | | | |

任務5.檢驗基本連通性

工作需求:

建立捕獲並檢查兩個VM之間的連線。

解決方案:

步驟1.在所有集群裝置上建立捕獲。

導航到主裝置的LINA(ASA)CLI並為內部和外部介面建立捕獲。

firepower# firepower# cluster exec capture capi interface inside match icmp any any firepower# firepower# cluster exec capture capo interface outside match icmp any any firepower# 驗證: firepower# cluster exec show capture capture capi type raw-data interface Inside [Capturing - 0 bytes] match icmp any any capture capo type raw-data interface Outside [Capturing - 0 bytes] match icmp any any capture capi type raw-data interface Inside [Capturing - 0 bytes] match icmp any any

capture capo type raw-data interface Outside [Capturing - 0 bytes]
match icmp any any

步驟2.執行從VM1到VM2的ping測試。

使用4個資料包進行測試。測試後檢查捕獲輸出:

capture capi type raw-data interface Inside [Capturing - 752 bytes]
match icmp any any
capture capo type raw-data interface Outside [Capturing - 752 bytes]
match icmp any any

match icmp any any capture capo type raw-data interface Outside [Capturing - 0 bytes] match icmp any any firepower#

運行命令以檢查特定裝置上的捕獲輸出:

firepower# cluster exec unit unit-1-3 show capture capi

8 packets captured

| 1: | 12:58:36.162253 | 802.1Q | vlan#201 | РO | 192.168.75.100 | > | 192.168.76.100: | icmp: | echo |
|--------|-----------------|--------|----------|----|----------------|---|-----------------|-------|------------|
| reques | st | | | | | | | | |
| 2: | 12:58:36.162955 | 802.1Q | vlan#201 | PO | 192.168.76.100 | > | 192.168.75.100: | icmp: | echo reply |
| 3: | 12:58:37.173834 | 802.1Q | vlan#201 | РO | 192.168.75.100 | > | 192.168.76.100: | icmp: | echo |
| reques | st | | | | | | | | |
| 4: | 12:58:37.174368 | 802.1Q | vlan#201 | РO | 192.168.76.100 | > | 192.168.75.100: | icmp: | echo reply |
| 5: | 12:58:38.187642 | 802.1Q | vlan#201 | PO | 192.168.75.100 | > | 192.168.76.100: | icmp: | echo |
| reques | st | | | | | | | | |
| 6: | 12:58:38.188115 | 802.1Q | vlan#201 | РO | 192.168.76.100 | > | 192.168.75.100: | icmp: | echo reply |
| 7: | 12:58:39.201832 | 802.1Q | vlan#201 | PO | 192.168.75.100 | > | 192.168.76.100: | icmp: | echo |
| reques | st | | | | | | | | |
| 8: | 12:58:39.202321 | 802.1Q | vlan#201 | P0 | 192.168.76.100 | > | 192.168.75.100: | icmp: | echo reply |
| 8 pacl | kets shown | | | | | | | | |

firepower# cluster exec unit unit-1-3 show capture capo

8 packets captured

1: 12:58:36.162543 802.1Q vlan#210 P0 192.168.75.100 > 192.168.76.100: icmp: echo

| reque | st | | | | | | | | | |
|-------|-----------------|--------|----------|----|----------------|---|-----------------|-------|------|-------|
| 2: | 12:58:36.162894 | 802.1Q | vlan#210 | PO | 192.168.76.100 | > | 192.168.75.100: | icmp: | echo | reply |
| 3: | 12:58:37.174002 | 802.1Q | vlan#210 | PO | 192.168.75.100 | > | 192.168.76.100: | icmp: | echo | |
| reque | st | | | | | | | | | |
| 4: | 12:58:37.174307 | 802.1Q | vlan#210 | PO | 192.168.76.100 | > | 192.168.75.100: | icmp: | echo | reply |
| 5: | 12:58:38.187764 | 802.1Q | vlan#210 | PO | 192.168.75.100 | > | 192.168.76.100: | icmp: | echo | |
| reque | st | | | | | | | | | |
| 6: | 12:58:38.188085 | 802.1Q | vlan#210 | PO | 192.168.76.100 | > | 192.168.75.100: | icmp: | echo | reply |
| 7: | 12:58:39.201954 | 802.1Q | vlan#210 | PO | 192.168.75.100 | > | 192.168.76.100: | icmp: | echo | |
| reque | st | | | | | | | | | |
| 8: | 12:58:39.202290 | 802.1Q | vlan#210 | PO | 192.168.76.100 | > | 192.168.75.100: | icmp: | echo | reply |
| 8 pac | kets shown | | | | | | | | | |
| firep | ower# | | | | | | | | | |

完成此任務後,使用下一命令刪除捕獲:

步驟3.將檔案從VM2下載到VM1。

VM1預配置為FTP伺服器,VM2預配置為FTP客戶端。

使用以下內容建立新捕獲:

使用FTP客戶端將檔案從VM2下載到VM1。

檢查show conn輸出:

UIOeN UDP cluster 255.255.255.255:49495 NP Identity Ifc 127.2.1.1:49495, idle 0:00:00, bytes 17858058, flags -TCP cluster 127.2.1.3:10844 NP Identity Ifc 127.2.1.1:38296, idle 0:00:33, bytes 5496, flags UI TCP cluster 127.2.1.3:59588 NP Identity Ifc 127.2.1.1:10850, idle 0:00:33, bytes 132, flags UO

TCP Outside 192.168.76.100:49175 Inside 192.168.75.100:21, idle 0:00:32, bytes 665, flags

TCP Outside 192.168.76.100:49175 Inside 192.168.75.100:21, idle 0:00:34, bytes 0, flags y
TCP cluster 127.2.1.1:10851 NP Identity Ifc 127.2.1.3:48493, idle 0:00:52, bytes 224, flags UI
.......
TCP cluster 127.2.1.1:64070 NP Identity Ifc 127.2.1.3:10847, idle 0:00:11, bytes 806, flags U0

TCP cluster 127.2.1.1:10851 NP Identity Ifc 127.2.1.2:64136, idle 0:00:53, bytes 224, flags UI TCP cluster 127.2.1.1:15859 NP Identity Ifc 127.2.1.2:10847, idle 0:00:11, bytes 807, flags UO Show capture output:

從機箱管理器UI捕獲群集

在下面的影象中,您可以看到具有2個埠通道(8和48)的FPR9300上的3單元群集。 邏輯裝置是 ASA,但在FTD的情況下將採用相同的概念。需要記住的重要一點是,儘管有3個集群單**元,但從捕 獲的角度來**看,只有一個邏輯設**備**:

| Ov | erview | Interfaces | Logical Devices | Security Mo | dules Platform Sett | ings | | Sys | tem Tools Help admin |
|-----|---------------------|---|---------------------------------|-------------|---|--|-----------------|----------|----------------------|
| Log | ical Devi | ce List | | | | | | c | Refresh 3 Add Device |
| | ASA | с | lustered | Status:ok | | | | | (F.) 🥒 E 🔹 |
| | Securit | y Module | Application | Version | Management IP | Gateway | Management Port | Status | |
| - | Security | Module 1 | ASA | 9.6.2.7 | 0.0.0.0 | 0.0.0.0 | Ethernet1/1 | 🕜 online | 🕶 🎉 |
| | Ports Dat Clu | s: ta Interfaces: ster Interfaces: | Port-channel8 Port-channel48 | | Attributes: Cluster Operational Statu Management IP VIRTUAL Cluster Role Management URL Management IP | s: in-cluster : 10.111.8.206 : master : https://10.111.8.206/ : 10.111.8.193 | | | |
| • | Security | Module 2 | ASA | 9.6.2.7 | 0.0.0.0 | 0.0.0.0 | Ethernet1/1 | 🕜 online | 💌 🏂 🏞 |
| | Ports Dat Clu | s: ta Interfaces: ster Interfaces: | Port-channel8 Port-channel48 | | Attributes: Cluster Operational Statu Management IP VIRTUAL Cluster Role Management URL Management IP | s: in-cluster : 10.111.8.206 : slave : https://10.111.8.206/ : 10.111.8.189 | | | |
| • | Security | Module 3 | ASA | 9.6.2.7 | 0.0.0.0 | 0.0.0.0 | Ethernet1/1 | 🕜 online | 🕶 🎉 🥕 |
| | Ports Dat Clu | s: ta Interfaces: ster Interfaces: | Port-channel8 Port-channel48 | | Attributes: Cluster Operational Statu: Management IP VIRTUAL Cluster Role Management URL Management IP | s: in-cluster : 10.111.8.206 : slave : https://10.111.8.206/ : 10.111.8.190 | | | |

| Overview Interfaces | Logical Devices So | ecurity Modules | Platform Settings | | System Tools Help admin Packet Capture |
|---|--------------------|--|---|--|--|
| | | | Save and Run | Save | Cancel |
| ASA Ethernet1/1 Ethernet1/8 (Portchannel48) Ethernet1/7 | | | | Session Name* Selected Interfaces Buffer Size Snap length: Store Packets | ARP Ethernet1/5 256 MB 1518 Overwrite Append |
| Ethernet1/6 (Portchannel48) Ethernet1/5 (Portchannel48) Ethernet1/4 | | Ethernet1/9, Ethe Ethernet1/12, Eth | ASA ernet1/10, Ethernet1/11, hernet1/13, Ethernet1/14 | Capture Filter | Apply Filter Capture All |
| (Portchannel48) | | | | | |
| Ethernet2/2 (Portchannel8) Ethernet2/1 (Portchannel8) | | | | | |

任務6.從群集中刪除從屬裝置

工作需求:

登入到FMC並從群集中刪除從屬裝置。

解決方案:

步驟1.登入FMC並導航至Device > Device Management。

按一下從屬裝置旁邊的垃圾桶圖示,如下圖所示。

| ∠ | | | <i>2</i> 8 |
|--|---|---------|------------|
| FTD1(primary) 10.62.148.67 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed | Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering | FTD9300 | ~ |
| FTD2 10.62.148.68 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed | Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering | FTD9300 | 6 |
| FTD3 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed | Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering | FTD9300 | 6 |

此時將顯示確認視窗。選擇Yes進行確認,如下圖所示。

| Confirm Delete | | | | | | | | |
|-------------------|---|---|--|--|--|--|--|--|
| availat Do you | Device "FTD2" will b Cluster "FTD_cluster Management Center ole in Firepower Secu want to continue? | e deleted from r [*] in Firepower r but will be rity Appliance. | | | | | | |
| | Yes | No | | | | | | |

• , 如下圖所示。



• 在FXOS CLI上。

| FPR9K-1-A# scope ssa FPR9K-1-A /ssa # show app-instance | | | | | | | | | |
|--|--------------------|-------------|-------------------|-----------------|------------|--|--|--|--|
| Application Name Version Cluster Ope | Slot ID r State | Admin State | Operational State | Running Version | Startup | | | | |
| | | | | | | | | | |
| ftd | 1 | Enabled | Online | 6.0.1.1213 | 6.0.1.1213 | | | | |
| In Cluster | | | | | | | | | |
| ftd | 2 | Enabled | Online | 6.0.1.1213 | 6.0.1.1213 | | | | |
| In Cluster | | | | | | | | | |
| ftd | 3 | Enabled | Online | 6.0.1.1213 | 6.0.1.1213 | | | | |
| In Cluster | | | | | | | | | |
| | | | | | | | | | |

•在LINA(ASA)CLI上。

firepower# show cluster info Cluster FTD_cluster: On Interface mode: spanned This is "unit-1-1" in state MASTER ID : 0 Version : 9.6(1)Serial No.: FLM19216KK6 CCL IP : 127.2.1.1 CCL MAC : 0015.c500.016f Last join : 21:51:03 CEST Aug 8 2016 Last leave: N/A Other members in the cluster: Unit "unit-1-3" in state SLAVE ID : 1 Version : 9.6(1)Serial No.: FLM19206H7T CCL IP : 127.2.1.3 CCL MAC : 0015.c500.018f Last join : 21:51:05 CEST Aug 8 2016 Last leave: N/A Unit "unit-1-2" in state SLAVE : 2 ΤD Version : 9.6(1) Serial No.: FLM19206H71 CCL IP : 127.2.1.2 CCL MAC : 0015.c500.019f Last join : 21:51:30 CEST Aug 8 2016 Last leave: N/A firepower#

附註:裝置已從FMC註銷,但它仍是FPR9300上的群整合員。

驗諍

使用本節內容,確認您的組態是否正常運作。

驗證已完成並涵蓋在單個任務中。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

• 所有版本的Cisco Firepower Management Center配置指南都可以在以下位置找到: <u>https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-</u> <u>roadmap.html#id_47280</u>。

• 所有版本的FXOS Chassis Manager和CLI配置指南都可以在以下位置找到: <u>https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html#pgfld-</u> <u>121950</u>。

• 思科全球技術協助中心(TAC)強烈建議使用以下視覺指南,深入瞭解Cisco Firepower下一代安 全技術(包括本文中提到的技術):

http://www.ciscopress.com/title/9781587144806。

有關與Firepower技術相關的所有配置和故障排除技術說明。
 <u>https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html</u>。

• <u>技術支援與文件 - Cisco Systems</u>