設定FTD HA的虛擬MAC位址

目錄

簡介

本檔案介紹如何在防火牆威脅防禦(FTD)高可用性(HA)配對上設定虛擬MAC位址。

必要條件

需求

思科建議您瞭解以下主題:

- 安全防火牆威脅防禦(FTD)
- 安全防火牆管理中心(FMC)

採用元件

- FMC虛擬版本7.2.8
- FTD虛擬版本7.2.7

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

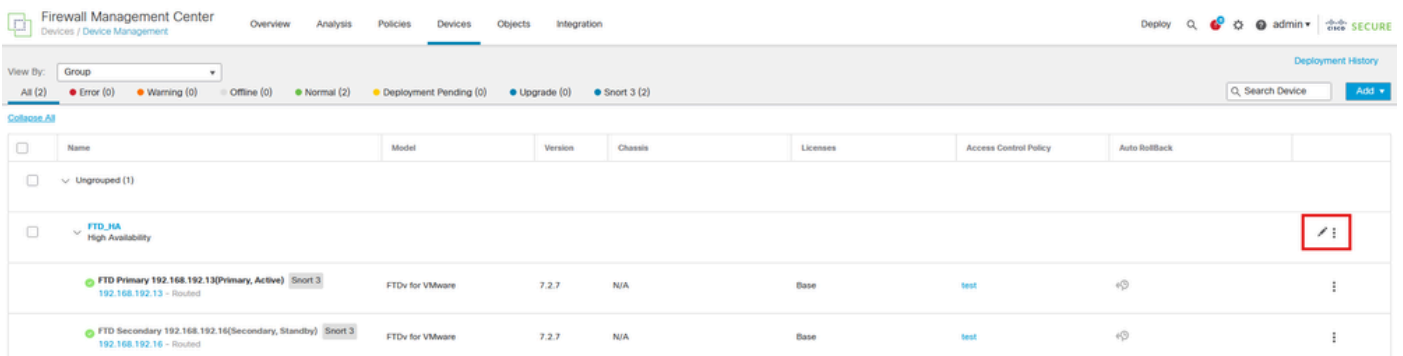在FTD HA配對上設定虛擬MAC位址有利於網路的可用性。虛擬MAC位址允許主要和輔助FTD維持一致的MAC位址,以避免特定流量中斷。

如果未配置虛擬MAC地址,則HA對的每個單元都會使用其固化的MAC地址啟動。如果輔助裝置在啟動時未檢測到主裝置,它將成為活動裝置並使用其固化的MAC地址。當主裝置最終上線時,輔助裝置會獲取主裝置的MAC地址,從而導致網路中斷。如果用新硬體替換主裝置,也會使用新的MAC地址。在裝置上配置虛擬MAC地址可防止這種中斷。這是因為輔助裝置始終知道主裝置的MAC地址,並且當它是活動裝置時,即使它比主裝置先聯機,也會繼續使用正確的MAC地址。

注意：術語「虛擬MAC地址」和「介面Mac地址」可以互換使用。

有關此配置的優點的其他資訊，請參閱此[指南](#)。

組態

1. 在FMC GUI中，導航至裝置頁面，並透過點選最右側鉛筆圖示編輯HA對。

2. 在高可用性頁籤下，找到標籤為介面MAC地址的框。按一下+圖示以訪問編輯器。

Interface MAC Addresses框

3. 從編輯器選擇物理介面並配置主用/備用介面Mac地址。完成後按一下OK。

Add Interface Mac Address   ?

Physical Interface:*

GigabitEthernet0/1 ▼

Active Interface Mac Address:*

dead.beef.0001

Standby Interface Mac Address:*

dead.beef.0002

ⓘ Enter the Mac addresses in hexadecimal
format such as 0123.4567.89ab

Cancel   OK

介面Mac地址建立

注意：在配置虛擬MAC地址時，遵守標準約定會很有幫助。介面內的地址必須是有效的MAC地址，但可以是任意地址。使用標準約定可以在檢查上游或下游MAC地址表時簡化管理。MAC位址格式化需要12個十六進位數字，每個四位數字組之間用句號分隔。

4. 對需要虛擬Mac地址配置的任何其餘介面重複此過程。

5. 確認組態是否正確。

Interface MAC Addresses			+
Physical Interface	Active Mac Address	Standby Mac Address	
GigabitEthernet0/1	dead.beef.0001	dead.beef.0002	✏🗑
GigabitEthernet0/2	dead.beef.0003	dead.beef.0004	✏🗑

介面Mac地址配置

6. 儲存並部署組態至FTD HA配對。

驗證

從運行配置的每台裝置中，虛擬Mac地址現在會出現。

主要（有效）FTD：

```
firepower# show run | grep failover
failover
failover lan unit primary
failover lan interface fover_link GigabitEthernet0/0
failover replication http
failover mac address GigabitEthernet0/1 dead.beef.0001 dead.beef.0002
failover mac address GigabitEthernet0/2 dead.beef.0003 dead.beef.0004
failover link fover_link GigabitEthernet0/0
failover interface ip fover_link 1.1.1.1 255.255.255.0 standby 1.1.1.2
```

顯示執行容錯移轉結果

```
> show interface "Inside"
Interface GigabitEthernet0/1 "Inside", is up, line protocol is up
  Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address dead.beef.0001, MTU 1500
        IP address 10.10.75.254, subnet mask 255.255.255.0
        1639 packets input, 108958 bytes, 0 no buffer
```

Show Interface Inside結果

```
> show interface "Outside"
Interface GigabitEthernet0/2 "Outside", is up, line protocol is up
  Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address dead.beef.0003, MTU 1500
        IP address 10.10.10.231, subnet mask 255.255.255.0
```

顯示介面外部結果

次要（待命）FTD：

```
. end
firepower# show run | grep failover
failover
failover lan unit secondary
failover lan interface fover_link GigabitEthernet0/0
failover replication http
failover mac address GigabitEthernet0/1 dead.beef.0001 dead.beef.0002
failover mac address GigabitEthernet0/2 dead.beef.0003 dead.beef.0004
failover link fover_link GigabitEthernet0/0
failover interface ip fover_link 1.1.1.1 255.255.255.0 standby 1.1.1.2
```

顯示執行容錯移轉結果

```
> show interface "Inside"
Interface GigabitEthernet0/1 "Inside", is up, line protocol is up
  Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address dead.beef.0002, MTU 1500
```

Show Interface Inside結果

```
> show interface "Outside"
Interface GigabitEthernet0/2 "Outside", is up, line protocol is up
  Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address dead.beef.0004, MTU 1500
```

顯示介面外部結果

這確認配置成功。

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）。