瞭解使用HSRP路由器的透明模式上的ASA高可用性MAC表同步

目錄

簡介

本文檔介紹連線到使用HSRP的路由器集群的一對ASA的行為。

必要條件

- 調適型安全裝置(ASA)
- ASA高可用性(HA)。
- 熱待命路由器通訊協定(HSRP)。
- 透明模式下的防火牆。

採用元件

- 2台具有HSRP的CSR路由器。
- 2在HA中配置的ASA，指向HSRP對。

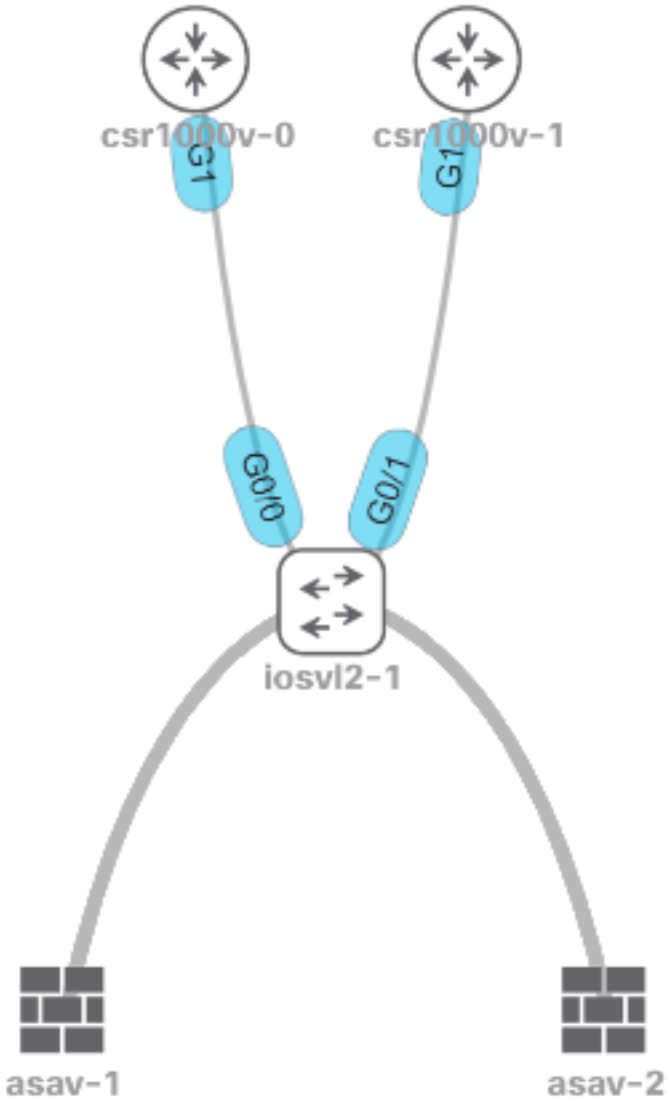
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

對於在高可用性透明模式下配置的一對ASA，如果一對防火牆上游連線到路由器集群，並且這些相鄰路由器使用HSRP，則來自防火牆的流量將定向到路由器IP地址，該地址也指向特定路由器的MAC地址。但是，如果返回流量源自HSRP對中的另一個路由器介面的MAC地址，則可能導致網路中斷。

問題在於mac-address-table age timeout為5分鐘（300秒），而地址解析協定(ARP)超時預設情況下為14400秒。由於下一跳路由器使用HSRP，因此從沒有源自HSRP MAC地址的任何流量。如果發生這種情況，則ASA上的mac-address-table條目會過期且流量會失敗。

網路圖表



疑難排解

瞭解使用HSRP在透明模式下的ASA HA的MAC表同步

這些輸出顯示了活動裝置獲取新條目並刪除舊條目時ASA裝置如何同步其MAC表。

主用裝置**asav-1**從其中一個HSRP路由器(本例中為**csr1000v-0**)丟失**5254.0017.8a8c** MAC地址。

```
ASAv-primary# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
inside 5254.001f.dfa8 dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

您可以看到5254.0017.8a8c在5分鐘後如何消失。

```
ASAv-primary# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

備用裝置不會丟失5254.0017.8a8c MAC條目。這種行為可能造成混淆，但這是完全預料到的。

備用裝置不會更新MAC地址表，除非它成為新的主用裝置。

備用裝置在數小時後保持5254.0017.8a8c，並且始終保持一(1)分鐘的老化時間。

```
ASAv-secondary(config)# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

您可以等待數小時/數天，然後運行相同的命令並檢視相同的結果。

```
ASAv-secondary(config)# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

此外，如果您發出 **show failover** 指令，當作用中單元遺失HSRP專案時，L2BRIDGE Tbl計數器上沒有變化。

```
Stateful Failover Logical Update Statistics
Link : failoverlink GigabitEthernet0/3 (up)
Stateful Obj xmit xerr rcv rerr
General 86751 0 77968 8
sys cmd 77854 0 77853 0
up time 0 0 0 0
RPC services 0 0 0 0
<--- More --->

TCP conn 0 0 0 0
UDP conn 8882 0 90 0
ARP tbl 4 0 1 0
L2BRIDGE Tbl 3 0 22 0
Xlate_Timeout 0 0 0 0
IPv6 ND tbl 0 0 0 0
SIP Session 0 0 0 0
SIP Tx 0 0 0 0
SIP Pinhole 0 0 0 0
Route Session 8 0 0 8
```

由於非對稱路由，MAC地址表條目過期

當流量直接在兩個MAC地址之間通過透明防火牆傳輸時，由於ASA接收來自傳送流量的兩個MAC地址的幀，因此這些地址不會在流量傳輸時過期。

當流量不對稱時，如果ASA沒有收到來自該特定MAC地址的響應，則條目超時。

> **附註**：非對稱路由意味著ASA會看到發往特定MAC地址的流量，但不會看到源自同一MAC地址的流量

此問題的症狀是，在ASA使MAC地址條目變舊後（在5分鐘後沒有源自該MAC地址的流量），目的地為該MAC地址的流量將被丟棄，直到再次填充MAC條目。

通常，如果表明在一兩次嘗試後重新建立與伺服器的連線，問題就會出現，這是因為第一個資料包被丟棄，因此ASA可以完成步驟來瞭解MAC地址的位置。

建議的解決方案

為了解決此問題，請在防火牆上為HSRP IP新增靜態MAC地址條目表，或將老化時間增加為某個值，以便在條目超時之前ARP應答來自相應的HSRP路由器。

更好的解決方案是新增靜態MAC條目，因為它不能確定ASA是否收到來自HSRP活動路由器的ARP應答。

相關資訊

- 技術支援與文件 - Cisco Systems

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）。