確保VMware環境中適當的虛擬WSA HA組功能

目錄

簡介

本檔案介紹必須完成的程式，才能使思科網路安全裝置(WSA)高可用性(HA)功能在在VMware環境中執行的虛擬WSA上正常工作。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco WSA
- HTTP
- 多點傳送流量
- 通用位址解析通訊協定(CARP)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- AsyncOS for Web 8.5或更高版本
- VMware ESXi版本4.0或更高版本

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。

問題

配置了一個或多個HA組的虛擬WSA一律會將HA置於*backup*狀態，即使優先順序最高也是如此。

系統日誌顯示持續的抖動，如以下日誌片段所示：

```
Tue May 19 08:05:52 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:05:52 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:01 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:01 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:06:01 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:10 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:10 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:06:10 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:19 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:19 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:06:19 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:28 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:28 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
Tue May 19 08:06:28 2015 Info: Interface Failover Group 94 is down
Tue May 19 08:06:37 2015 Info: Interface Failover Group 94 is up
Tue May 19 08:06:37 2015 Info: Interface Failover Group 94 has changed
role from Master to Backup (more frequent advertisement received)
```

如果您採用封包擷取（在本範例中為多點傳送IP位址224.0.0.18），可能會看到類似以下的輸出：

```
13:49:04.601713 IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
13:49:04.601931 IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
13:49:04.602798 IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
13:49:04.602809 IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
13:49:13.621706 IP (tos 0x10, ttl 255, id 24801, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178284
13:49:13.622007 IP (tos 0x10, ttl 255, id 24801, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178284
```

```
13:49:13.622763 IP (tos 0x10, ttl 255, id 24801, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178284
13:49:13.622770 IP (tos 0x10, ttl 255, id 24801, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178284
13:49:22.651653 IP (tos 0x10, ttl 255, id 44741, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178285
```

問題分析

前面部分中提供的WSA系統日誌表明，當HA組成為CARP協商中的主節點時，會收到一個具有更好優先順序的通告。

您也可以在封包擷取中驗證這點。這是從虛擬WSA傳送的資料包：

```
13:49:04.601713 IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
```

在毫秒的時間範圍內，您可以看到來自同一源IP地址（同一虛擬WSA裝置）的另一組資料包：

```
13:49:04.602798 IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
13:49:04.602809 IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF],
proto VRRP (112), length 56)
  192.168.0.131 > 224.0.0.18: carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36:
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
```

在本示例中，源IP地址192.168.0.131是有問題的虛擬WSA的IP地址。組播資料包似乎回送至虛擬WSA。

此問題是由於VMware端的一個缺陷導致的，下一部分介紹了解決該問題必須完成的步驟。

解決方案

完成以下步驟即可解決此問題，並停止在VMware環境中傳送的組播資料包的環路：

1. 在虛擬交換機(vSwitch)上啟用**混雜模式**。
2. 啟用**MAC地址更改**。
3. 啟用**偽造傳輸**。
4. 如果同一vSwitch上存在多個物理埠，則必須啟用**Net.ReversePathFwdCheckPromisc**選項，才能解決vSwitch錯誤(在該錯誤中，組播流量回送至主機，導致CARP在鏈路狀態合併消息

*下不起作*用)。（請參見下一節以獲取更多資訊）。

修改*Net.ReversePathFwdCheckPromisc*選項

完成以下步驟即可修改*Net.ReversePathFwdCheckPromisc*選項：

1. 登入到VMware vSphere客戶端。
2. 為每個VMware主機完成以下步驟：

   按一下**host**，然後導航到*Configuration*頁籤。

   從左窗格中按一下「**Software Advanced Settings**」。

   按一下**Net**，向下滾動到**Net.ReversePathFwdCheckPromisc**選項。

   將*Net.ReversePathFwdCheckPromisc*選項設定為**1**。

   按一下「**OK**」（確定）。

處於*Promiscuous*模式的介面現在必須設定或關閉，然後重新開啟。此操作按主機完成。

完成以下步驟以設定介面：

1. 導覽至*Hardware*區段，然後按一下**Networking**。
2. 為每個vSwitch和/或虛擬機器(VM)埠組完成以下步驟：

   在vSwitch上按一下**Properties**。

   預設情況下，「混雜」模式設定為*拒絕*。要更改此設定，請按一下**編輯**並導航到*Security*頁籤。

   從下拉選單中選擇**Accept**。

   按一下「**OK**」（確定）。

   附註：此設定通常基於每個VM埠組應用（更安全），其中vSwitch保留預設設定（拒絕）。

完成以下步驟即可停用然後重新啟用混雜模式：

1. 導航到**編輯>安全>策略例外**。
2. 取消選中**混雜模式**覈取方塊。
3. 按一下「**OK**」（確定）。
4. 導航到**編輯>安全>策略例外**。

5. 選中**Promiscuous Mode**覈取方塊。

6. 從下拉選單中選擇**Accept**。

相關資訊

- CARP配置故障排除
- 技術支援與文件 - Cisco Systems