确保在VMware环境中具有适当的虚拟WSA高可用性组功能

目录

简介

本文档介绍在VMware环境中运行的虚拟WSA上，思科网络安全设备(WSA)高可用性(HA)功能正常工作所必须完成的流程。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科WSA
- HTTP
- 多播流量
- 通用地址解析协议(CARP)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- AsyncOS for Web 8.5或更高版本

- VMware ESXi版本4.0或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题

配置了一个或多个HA组的虚拟WSA始终具有处于备份状态的HA，*即*使优先级最高时也是如此。

系统日志显示持续抖动，如以下日志片段所示：

```
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)
```

如果您捕获数据包（本例中为组播IP地址224.0.0.18），您可能会看到类似以下的输出：

```
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
```

问题分析

上一节中提供的WSA系统日志表明，当HA组成为CARP协商中的主设备时，会收到优先级更高的通告。

您也可以从数据包捕获中检验这一点。以下是从虚拟WSA发送的数据包：

```
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
```

在毫秒的时间段内，您可以看到来自同一源IP地址（同一虚拟WSA设备）的另一组数据包：

```
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
```

在本例中，源IP地址192.168.0.131是有问题的虚拟WSA的IP地址。组播数据包似乎已环回到虚拟WSA。

此问题是由于VMware端存在缺陷而发生的，下一节将说明您必须完成的步骤才能解决问题。

解决方案

要解决此问题并停止在VMware环境中发送的组播数据包的环路，请完成以下步骤：

1. 在虚拟交换机(vSwitch)上启用**混杂模式**。
2. 启用**MAC地址更改**。
3. 启用**Ferged传输**。

4. 如果同一vSwitch上存在多个物理端口，则必须启用Net.ReversePathFwdCheckPromisc选项，以解决组播流量回路到主机的vSwitch漏洞，这会导致CARP无法与链路状态消息*合并*。（请参阅下一节了解更多信息）。

修改*Net.ReversePathFwdCheckPromisc*选项

要修改Net.ReversePathFwdCheckPromisc选*项，请完成以下*步骤：

1. 登录VMware vSphere客户端。
2. 为每台VMware主机完成以下步骤：

   单击**host**，然后导航至*Configuration*选项卡。

   从左窗格**中单击"软件**高级设置"。

   单击**Net**并向下滚动到**Net.ReversePathFwdCheckPromisc选项。**

   将Net.*ReversePathFwdCheckPromisc选项*设置为**1**。

   Click **OK**.

现在必须设置处于混合模式的接口，或关闭然后重新打开。这是按主机完成的。

要设置接口，请完成以下步骤：

1. 导航至"硬件*"部*分，然后单**击"网络**"。
2. 为每个vSwitch和/或虚拟机(VM)端口组完成以下步骤：

   从vSwitch单击**Properties**。

   默认情况下，混合模式设置为*拒绝*。要更改此设置，请单击"编辑"**并导**航至"安全"*选项*卡。

   从下拉菜单中选择**Accept**。

   Click **OK**.

   注意：此设置通常应用于每个VM端口组（更安全），其中vSwitch保留为默认设置（拒绝）。

要禁用并重新启用混合模式，请完成以下步骤：

1. 导航至**编辑>安全>策略例外**。
2. 取消选中"混**杂模式"**复选框。
3. Click **OK**.
4. 导航至**编辑>安全>策略例外**。

5. 选中混**杂模式复**选框。

6. 从下拉菜单中选择Accept。

相关信息

- CARP配置故障排除
- 技术支持和文档 - Cisco Systems