保证在VMware环境的适当的虚拟WSA HA组功能

目录

简介

本文描述必须完成的进程，以便思科Web安全工具(WSA)高性能的(HA)功能在VMware环境运行的虚拟WSA适当地运作。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科WSA
- HTTP
- 多播流量
- 地址解析协议共同性(鲤鱼)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Web版本8.5或以上的AsyncOS
- VMware ESXi版本4.0或以上

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

配置与一个或更多HA组的虚拟WSA总是有HA在*备份*状态，既使当优先级最高。

如此日志片断所显示，系统日志显示不变飘荡， ：

```
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)
```

如果采取数据包捕获(在本例中的组播IP地址224.0.0.18)，您也许观察输出类似于此：

```
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

在前面部分提供的WSA系统日志表明，当HA组变为在鲤鱼协商时的万事达，有接收以更加好的优先级的广告。

您能从数据包捕获也验证此。这是从虚拟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
```

在毫秒期限，您能看到另一套从同样源IP地址(同一个虚拟WSA设备)的数据包：

```
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， 192.168.0.131源IP地址是有问题的虚拟WSA的IP地址。看来组播信息包被反向循环对虚拟WSA。

此问题发生由于在VMware侧的一个缺陷，并且下一部分解释您必须完成为了解决问题的步骤。

解决方案

完成这些步骤为了解决此问题和终止在VMware环境被发送组播信息包的环路：

1. 启动在虚拟交换机(vSwitch)的**混杂模式**。
2. 启用**MAC地址更改**。
3. **伪造的**Enable (event)**传送**。
4. 如果多个物理端口在同一vSwitch存在，则必须启用**Net.ReversePathFwdCheckPromisc**选项为了在组播数据流反向循环到主机，造成鲤鱼不作用以*链路状态联合*消息的vSwitch bug附近工作。(参考其他信息的下一部分)。

修改*Net.ReversePathFwdCheckPromisc*选项

完成这些步骤为了修改*Net.ReversePathFwdCheckPromisc*选项：

1. 登录VMware vSphere客户端。
2. 完成每台VMware主机的这些步骤：

   点击**主机**，并且导航对*Configuration选项*。

   点击**软件**从左窗格的**提前的设置**。

   点击**网络**并且移下来对**Net.ReversePathFwdCheckPromisc**选项。

   设置*Net.ReversePathFwdCheckPromisc*选项到**1**。

   单击 **Ok**。

在*混杂模式的*接口必须当前设置或者然后启用上一步。这完成根据一个每主机基本类型。

完成这些步骤为了设置接口：

1. 导航对*硬件*部分并且点击**网络**。
2. 完成每个vSwitch和虚拟机端口组的这些步骤：

   点击从vSwitch的**属性**。

   默认情况下，混杂模式设置*拒绝*。为了更改此设置，请单击**编辑**并且导航对*安全选项卡*。

   选择从下拉菜单**接受**。

   单击 **Ok**。

   注意：此设置通常应用根据是安全的更多)的每VM端口组基本类型(其中vSwitch被留下在默认设置(拒绝)。

完成这些步骤为了禁用然后重新启用混杂模式：

1. 导航**编辑> Security >Policy例外**。
2. 不选定**混杂模式**复选框。
3. 单击 **Ok**。
4. 导航**编辑> Security >Policy例外**。
5. 检查**混杂模式**复选框。
6. 选择从下拉菜单**接受**。

相关信息

- 鲤鱼配置故障排除
- 技术支持和文档 - Cisco Systems