Garantizar la funcionalidad adecuada del grupo WSA HA virtual en un entorno VMware

Contenido

Introducción

Este documento describe el proceso que se debe completar para que la función de alta disponibilidad (HA) de Cisco Web Security Appliance (WSA) funcione correctamente en un WSA virtual que se ejecuta en un entorno VMware.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco WSA
- HTTP
- Tráfico Multicast
- Protocolo común de resolución de direcciones (CARP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- AsyncOS para la versión 8.5 o posterior de Web

- VMware ESXi versión 4.0 o posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problema

Un WSA virtual que se configura con uno o más grupos HA siempre tiene el HA en el estado *de respaldo*, incluso cuando la prioridad es la más alta.

Los registros del sistema muestran constantes inestables, como se muestra en este fragmento de registro:

```
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)
```

Si toma una captura de paquetes (para la dirección IP de multidifusión 224.0.0.18 en este ejemplo), puede observar un resultado similar a este:

```
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
```

Análisis de problemas

Los registros del sistema WSA que se proporcionan en la sección anterior indican que cuando el grupo HA se convierte en maestro en la negociación CARP, hay un anuncio que se recibe con una mejor prioridad.

También puede verificar esto desde la captura de paquetes. Este es el paquete que se envía desde el WSA virtual:

```
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
```

En un intervalo de tiempo de milisegundos, puede ver otro conjunto de paquetes de la misma dirección IP de origen (el mismo dispositivo WSA virtual):

```
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
```

En este ejemplo, la dirección IP de origen de 192.168.0.131 es la dirección IP del WSA virtual problemático. Parece que los paquetes multicast se vuelven a enviar en loop al WSA virtual.

Este problema ocurre debido a un defecto en el lado de VMware, y la siguiente sección explica los pasos que debe completar para resolver el problema.

Solución

Complete estos pasos para resolver este problema y detener el loop de paquetes multicast que se envían en el entorno VMware:

1. Habilite el modo **promiscuo** en el switch virtual (vSwitch).

2. Habilite **los cambios de dirección MAC**.

3. Habilitar **transmisiones falsificadas**.

4. Si existen varios puertos físicos en el mismo vSwitch, la opción **Net.ReversePathFwdCheckPromisc** se debe habilitar para solucionar un error de vSwitch donde el tráfico multicast vuelve a bucles al host, lo que hace que CARP no funcione con los *estados de link* mensajes combinados. (Consulte la sección siguiente para obtener más información).

Modificar la opción *Net.ReversePathFwdCheckPromisc*

Complete estos pasos para modificar la opción *Net.ReversePathFwdCheckPromisc*:

1. Inicie sesión en el cliente VMware vSphere.

2. Complete estos pasos para cada host VMware:

   Haga clic en **host** y navegue a la *ficha Configuration*.

   Haga clic en **Software Advanced Settings** en el panel izquierdo.

   Haga clic en **Net** y desplácese hacia abajo hasta la **opción Net.ReversePathFwdCheckPromisc**.

   Establezca la opción *Net.ReversePathFwdCheckPromisc* en **1**.

   Click OK.

Las interfaces que están en modo *Promiscuous* deben configurarse o apagarse y luego volver a encenderse. Esto se completa por host.

Complete estos pasos para configurar las interfaces:

1. Vaya a la sección *Hardware* y haga clic en **Networking**.

2. Complete estos pasos para cada vSwitch o grupo de puertos de máquina virtual (VM):

   Haga clic en **Propiedades** desde el vSwitch.

   De forma predeterminada, el modo Promiscuous se establece en *Rechazar*. Para cambiar esta configuración, haga clic en **editar** y navegue a la *ficha* Seguridad.

   Seleccione **Aceptar** en el menú desplegable.

Click OK.

Nota: Esta configuración se suele aplicar por grupo de puertos VM (que es más segura), donde el vSwitch se deja en el valor predeterminado (Rechazar).

Complete estos pasos para inhabilitar y luego volver a habilitar el modo Promiscuous:

1. Vaya a **Editar > Seguridad > Excepciones de política**.
2. Desmarque la casilla de verificación **Modo promiscuo**.
3. Click OK.
4. Vaya a **Editar > Seguridad > Excepciones de política**.
5. Marque la casilla de verificación **Modo promiscuo**.
6. Seleccione **Aceptar** en el menú desplegable.

Información Relacionada

- Resolución de problemas de configuración CARP
- Soporte Técnico y Documentación - Cisco Systems