Asegure las funciones virtuales apropiadas del grupo WSA HA en un entorno de VMware

Contenido

Introducción

Este documento describe el proceso que debe ser completado de modo que la característica de gran disponibilidad del dispositivo de seguridad de la red de Cisco (WSA) (HA) trabaje correctamente en un WSA virtual que se ejecute en un entorno de VMware.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco WSA
- HTTP
- Tráfico Multicast
- Protocolo Protocolo de resolución de la dirección (ARP) común (CARPA)

Componentes Utilizados

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

- AsyncOS para Web versión 8.5 o más adelante

- Versión 4.0 o posterior de VMware ESXi

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Problema

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

Los registros del sistema muestran el cambio constante, tal y como se muestra en de este snippet del 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 usted toma a una captura de paquetes (para el Multicast IP Address 224.0.0.18 en este ejemplo), usted puede ser que observe una salida similar a esto:

```
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 problema

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

Usted puede verificar esto también de la captura de paquetes. Éste es el paquete que se envía del 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 calendario de los milisegundos, usted puede ver otro conjunto de los paquetes de la misma dirección IP de origen (el mismo dispositivo virtual WSA):

```
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. Aparece que los paquetes de multidifusión son circuito hecho atrás al WSA virtual.

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

Solución

Complete estos pasos para resolver este problema y parar el loop de los paquetes de multidifusión que se envían en el entorno de VMware:

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

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

3. El permiso **forjado transmite**.

4. Si los puertos del múltiple físico existen en el mismo vSwitch, después la opción **Net.ReversePathFwdCheckPromisc** se debe habilitar para trabajar alrededor de un bug del vSwitch donde el tráfico Multicast coloca - detrás al host, que causa la CARPA a no funcionar con los *estados del link se unió los* mensajes. (Refiera a la siguiente sección para la información adicional).

Modifique la opción *Net.ReversePathFwdCheckPromisc*

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

1. Registre en el cliente del vSphere de VMware.

2. Complete estos pasos para cada host de VMware:

   Haga clic el **host**, y navegue a la *ficha de configuración*.

   Haga clic las **configuraciones avanzadas software del** panel izquierdo.

   Haga clic la **red** y navegue hacia abajo a la opción **Net.ReversePathFwdCheckPromisc**.

   Fije la opción *Net.ReversePathFwdCheckPromisc a* **1.**

   Haga clic en OK.

Las interfaces que están en el *modo promiscuo* se deben ahora fijar, o apagado y después dar vuelta detrás encendido. Esto se completa sobre una base del por-host.

Complete estos pasos para fijar las interfaces:

1. Navegue a la sección del *hardware* y haga clic el **establecimiento de una red**.

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

   Haga clic las **propiedades del** vSwitch.

   Por abandono, fijan al modo promiscuo *para rechazar*. Para cambiar esta configuración, el tecleo **edita** y navega a la *ficha de seguridad*.

   Selecto **valide del** menú desplegable.

   Haga clic en OK.

   Nota: Esta configuración se aplica generalmente sobre una base del grupo de puertos por-VM (que sea más segura), donde el vSwitch se deja en la configuración predeterminada

(rechazo).

Complete estos pasos para inhabilitar y después volver a permitir al modo promiscuo:

1. Navegue **para editar el > Security (Seguridad) > las excepciones de la directiva**.
2. Desmarque el checkbox del **modo promiscuo**.
3. Haga clic en OK.
4. Navegue **para editar el > Security (Seguridad) > las excepciones de la directiva**.
5. Marque el checkbox del **modo promiscuo**.
6. Selecto **valide del** menú desplegable.

Información Relacionada

- Troubleshooting de la configuración de la CARPA
- Soporte Técnico y Documentación - Cisco Systems