Assegure a funcionalidade virtual apropriada do grupo WSA HA em um ambiente de VMware

Índice

Introdução

Este documento descreve o processo que deve ser terminado de modo que a Alta disponibilidade da característica da ferramenta de segurança da Web de Cisco (WSA) (HA) trabalhe corretamente em um WSA virtual que seja executado em um ambiente de VMware.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco WSA
- HTTP
- Tráfego multicast
- Protocolo Protocolo de resolución de la dirección (ARP) comum (CARPA)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- AsyncOS para versão da web 8.5 ou mais atrasado

- Versão 4.0 ou mais recente de VMware ESXi

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Problema

Um WSA virtual que seja configurado com uns ou vários grupos HA tem sempre o HA no estado *alternativo*, mesmo quando a prioridade é a mais alta.

Os log de sistema mostram o flapping constante, segundo as indicações deste snippet do log:

```
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)
```

Se você toma uma captura de pacote de informação (para o endereço IP multicast 224.0.0.18 neste exemplo), você pôde observar uma saída similar a esta:

```
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
```

Análise de problema

Os log de sistema WSA que são fornecidos na seção anterior indicam que quando o grupo HA se transforma um mestre na negociação da CARPA, há uma propaganda que esteja recebida com uma prioridade melhor.

Você pode verificar este igualmente da captura de pacote de informação. Este é o pacote que é enviado do 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
```

Em uns milissegundos tempo de frame, você pode ver um outro grupo de pacotes do mesmo endereço IP de origem (o mesmo 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
```

Neste exemplo, o endereço IP de origem de 192.168.0.131 é o endereço IP de Um ou Mais Servidores Cisco ICM NT do WSA virtual problemático. Parece que os pacotes de transmissão múltipla são loop ao WSA virtual.

Esta edição ocorre devido a um defeito no lado de VMware, e a próxima seção explica as etapas que você deve terminar a fim resolver a edição.

Solução

Termine estas etapas a fim resolver esta edição e parar o laço dos pacotes de transmissão múltipla que são enviados no ambiente de VMware:

1. Permita o **modo misturado no** virtual switch (vSwitch).

2. Permita **mudanças do MAC address**.

3. Permita **forjado transmite**.

4. Se as portas do físico múltiplo existem no mesmo vSwitch, a seguir a opção **Net.ReversePathFwdCheckPromisc** deve ser permitida a fim trabalhar em torno de um erro do vSwitch onde o tráfego multicast dê laços - para trás ao host, que causa a CARPA a não funcionar com *estados do link coalesceu* mensagens. (Refira a próxima seção para a informação adicional).

Altere a opção *Net.ReversePathFwdCheckPromisc*

Termine estas etapas a fim alterar a opção *Net.ReversePathFwdCheckPromisc*:

1. Registre no cliente do vSphere de VMware.

2. Termine estas etapas para cada host de VMware:

   Clique o **host**, e navegue ao *guia de configuração*.

   Clique **ajustes avançados software do** painel esquerdo.

   Clique a **rede** e enrole-a para baixo a opção **Net.ReversePathFwdCheckPromisc**.

   Ajuste a opção *Net.ReversePathFwdCheckPromisc a* **1.**

   Clique em **OK**.

As relações que reagem do *modo misturado* devem agora ser ajustadas, ou desligado e então para trás sobre. Isto é terminado em uma base do por-host.

Termine estas etapas a fim ajustar as relações:

1. Navegue à seção do *hardware* e clique **trabalhos em rede**.

2. Termine estas etapas para cada vSwitch e/ou grupo de porta da máquina virtual (VM):

   Clique **propriedades do** vSwitch.

   Àrevelia, o modo misturado é ajustado *para rejeitar*. A fim mudar este ajuste, o clique **edita** e navega à *ABA de segurança*.

   Seleto **aceite do** menu suspenso.

   Clique em **OK**.

   Nota: Este ajuste é aplicado geralmente em uma base do grupo de porta por-VM (que é mais segura), onde o vSwitch é deixado na configuração padrão (rejeição).

Termine estas etapas a fim desabilitar e re-permitir então o modo misturado:

1. Navegue **para editar o > segurança > as exceções da política**.
2. Desmarcar a caixa de seleção do **modo misturado**.
3. Clique em **OK**.
4. Navegue **para editar o > segurança > as exceções da política**.
5. Verifique a caixa de seleção do **modo misturado**.
6. Seleto **aceite do** menu suspenso.

Informações Relacionadas

- Troubleshooting da configuração da CARPA
- Suporte Técnico e Documentação - Cisco Systems