Garanta a funcionalidade adequada do grupo HA do WSA virtual em um ambiente VMware

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Problema](#)
[Análise de problemas](#)
[Solução](#)
[Modifique a opção *Net.ReversePathFwdCheckPromisc*](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve o processo que deve ser concluído para que o recurso de alta disponibilidade (HA) do Cisco Web Security Appliance (WSA) funcione corretamente em um WSA virtual executado em um ambiente VMware.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco WSA
- HTTP
- Tráfego multicast
- Common Address Resolution Protocol (CARP)

Componentes Utilizados

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

- AsyncOS para Web versão 8.5 ou posterior

- VMware ESXi versão 4.0 ou 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

Um WSA virtual configurado com um ou mais grupos HA sempre tem o HA no estado *de backup*, mesmo quando a prioridade é a mais alta.

Os registros do sistema mostram oscilação constante, como mostrado neste trecho de 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 capturar um pacote (para o endereço IP multicast 224.0.0.18 neste exemplo), poderá observar uma saída semelhante 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 problemas

Os registros do sistema WSA fornecidos na seção anterior indicam que quando o grupo HA se torna um Mestre na negociação CARP, há um anúncio recebido com uma prioridade melhor.

Você também pode verificar isso a partir da captura de pacotes. Este é o pacote 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 um período de tempo de milissegundos, você pode ver outro conjunto de pacotes do mesmo endereço IP de origem (o mesmo 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
```

Neste exemplo, o endereço IP origem de 192.168.0.131 é o endereço IP do WSA virtual problemático. Parece que os pacotes multicast são retornados ao WSA virtual.

Esse problema ocorre devido a um defeito no lado do VMware, e a próxima seção explica as etapas que você deve concluir para resolver o problema.

Solução

Conclua estes passos para resolver esse problema e parar o loop de pacotes multicast enviados no ambiente VMware:

1. Ative o modo **promíscuo** no Virtual Switch (vSwitch).

2. Habilitar **alterações de endereço MAC**.

3. Habilitar **transmissões forjadas**.

4. Se existirem várias portas físicas no mesmo vSwitch, a opção **Net.ReversePathFwdCheckPromisc** deve ser ativada para funcionar em torno de um bug do vSwitch no qual o tráfego multicast faz loops de volta para o host, o que faz com que o CARP não funcione com mensagens *agrupadas de estados de link*. (Consulte a próxima seção para obter informações adicionais).

Modifique a opção *Net.ReversePathFwdCheckPromisc*

Conclua estes passos para modificar a opção *Net.ReversePathFwdCheckPromisc*:

1. Faça login no cliente VMware vSphere.

2. Conclua estes passos para cada host VMware:

   Clique em **host** e navegue até a guia *Configuração*.

   Clique em **Configurações avançadas de software** no painel esquerdo.

   Clique em **Net** e role para baixo até a opção **Net.ReversePathFwdCheckPromisc**.

   Defina a opção *Net.ReversePathFwdCheckPromisc como* **1**.

   Click **OK**.

As interfaces que estão no modo *promíscuo* devem agora ser definidas ou desligadas e depois ligadas novamente. Isso é concluído por host.

Conclua estes passos para definir as interfaces:

1. Navegue até a seção *Hardware* e clique em **Rede**.

2. Conclua estes passos para cada grupo de portas do vSwitch e/ou da Máquina Virtual (VM):

   Clique em **Propriedades** no vSwitch.

   Por padrão, o modo promíscuo é definido como *Rejeitar*. Para alterar essa configuração, clique em **editar** e navegue até a guia *Segurança*.

   Selecione **Aceitar** no menu suspenso.

   Click **OK**.

   Note: Essa configuração é geralmente aplicada em um grupo de portas por VM (que é mais seguro), onde o vSwitch é deixado na configuração padrão (Rejeitar).

Conclua estes passos para desabilitar e reabilitar o modo promíscuo:

1. Navegue até **Edit > Security > Policy Exceptions**.
2. Desmarque a caixa de seleção **Modo promíscuo**.
3. Click **OK**.
4. Navegue até **Edit > Security > Policy Exceptions**.
5. Marque a caixa de seleção **Modo promíscuo**.
6. Selecione **Aceitar** no menu suspenso.

Informações Relacionadas

- Solução de problemas de configuração de CARP
- Suporte Técnico e Documentação - Cisco Systems