Zorg ervoor dat de juiste virtuele WSA HA-groepsfuncties in een VMware-omgeving worden gegarandeerd

Inhoud

Inleiding

Dit document beschrijft het proces dat moet worden voltooid zodat de functie Hoge beschikbaarheid (HA) van Cisco Web Security Appliance (WSA) correct werkt op een Virtual WSA dat in een VMware-omgeving draait.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco WSA
- HTTP
- Multicastverkeer
- Gemeenschappelijk Protocol voor adresoplossing (CARP)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- AsyncOS voor webversie 8.5 of hoger
- VMware ESXi versie 4.0 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Probleem

Een virtuele WSA die met één of meer HA-groepen is ingesteld heeft altijd de HA in de *reservestatus*, zelfs wanneer de prioriteit het hoogste is.

De systeemlogs tonen een constante flapper, zoals in dit logfragment wordt getoond:

```
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)
```

Als u een pakketvastlegging (voor multicast IP-adres 224.0.18 in dit voorbeeld) inneemt, kunt u een op dit voorbeeld lijkende uitvoer observeren:

```
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
```

Probleemanalyse

De WSA-systeemlogboeken die in de vorige paragraaf worden verstrekt, geven aan dat wanneer de HA-groep een Master in de CARP-onderhandeling wordt, er een advertentie is die met een betere prioriteit wordt ontvangen.

U kunt dit ook verifiëren bij de pakketvastlegging. Dit is het pakket dat vanuit het virtuele WSA wordt verzonden:

```
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
```

In een tijdframe van een milliseconde kunt u een andere set pakketten zien van hetzelfde bron-IP-adres (hetzelfde virtuele WSA-apparaat):

```
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
```

In dit voorbeeld is het IP-adres van de bron van 192.168.0.131 het IP-adres van de problematische virtuele WSA. Het lijkt erop dat de multicast-pakketten worden teruggekoppeld naar het virtuele WSA-netwerk.

Dit probleem is het gevolg van een defect aan de kant van VMware en in het volgende gedeelte wordt uitgelegd welke stappen u moet uitvoeren om het probleem op te lossen.

Oplossing

Voltooi deze stappen om dit probleem op te lossen en stop de herhaling van multicast-pakketten die in de VMware-omgeving worden verzonden:

1. Schakel de **promiscuous** Mode in op de Virtual Switch (vSwitch).

2. Schakel **MAC-adreswijzigingen in**.

3. Inschakelen **op geforceerde overdrachtspunten**.

4. Als er meerdere fysieke poorten op dezelfde vSwitch zijn, dan moet **de** optie **Net.ReversePathFWdControleer** Promisc ingeschakeld zijn om rond een vSwitch-bug te werken waar het multicast verkeer terugkeert naar de host, waardoor de CARP niet werkt met gecodeerde berichten van *verbindingsstaten*. (Raadpleeg het volgende gedeelte voor aanvullende informatie).

De optie *Net.ReversePathFWDCheckPromisc* wijzigen

Voltooi deze stappen om de optie *Net.ReversePath* FWDControleerPromisc aan te passen:

1. Meld u aan bij de VMware vSphere-client.

2. Voltooi deze stappen voor elke VMware-host:

   Klik op **host** en navigeer naar het tabblad *Configuration*.

   Klik op **Software voor geavanceerde instellingen** in het linker deelvenster.

   Klik op **Net** en rol terug naar de optie **Net.ReversePathFWDControleerPromisc**.

   Stel de optie *Net.ReversePathFWDCheckPromisc* in op **1**.

   Klik op **OK**.

De interfaces die in *Promiscuous* zijn moeten nu worden ingesteld, of uit en dan weer aan. Dit wordt per host ingevuld.

Voltooi deze stappen om de interfaces in te stellen:

1. Navigeer naar het gedeelte *Hardware* en klik op **Netwerk**.

2. Voltooi deze stappen voor elke poortgroep van vSwitch en/of Virtual Machine (VM):

   Klik op **Eigenschappen** in de vSwitch.

   Standaard wordt de modus Promiscuous ingesteld op *Afwijzen*. Als u deze instelling wilt wijzigen, klikt u op **Bewerken** en vervolgens navigeert u naar het tabblad *Beveiliging*.

Selecteer **Aanvaarden** in het vervolgkeuzemenu.

Klik op **OK**.

Opmerking: Deze instelling wordt gewoonlijk toegepast op basis van een poortgroep per VM (wat veiliger is), waarbij de vSwitch bij de standaardinstelling blijft staan (Afwijzen).

Voltooi deze stappen om Promiscuous Mode uit te schakelen en dan opnieuw in te schakelen:

1. Navigeer om **> Security > Policy Exceptions** te **bewerken**.
2. Schakel het vakje **Promiscuous Mode** uit.
3. Klik op **OK**.
4. Navigeer om **> Security > Policy Exceptions** te **bewerken**.
5. Controleer het selectieteken voor **de modus Promiscuous**.
6. Selecteer **Accept** in het vervolgkeuzemenu.

Gerelateerde informatie

- Problemen oplossen bij CARP-configuratie
- Technische ondersteuning en documentatie – Cisco Systems