Garantire la corretta funzionalità del gruppo WSA HA virtuale in un ambiente VMware

Sommario

Introduzione

In questo documento viene descritto il processo da completare per garantire il corretto funzionamento della funzionalità ad alta disponibilità (HA, High Availability) di Cisco Web Security Appliance (WSA) su un'appliance WSA virtuale in esecuzione in un ambiente VMware.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- AsyncOS per Web versione 8.5 o successive

- VMware ESXi versione 4.0 o successiva

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

Una WSA virtuale configurata con uno o più gruppi HA presenta sempre HA nello stato di *backup*, anche quando la priorità è la più alta.

I log di sistema mostrano il flapping costante, come mostrato in questo frammento di 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 si acquisisce un pacchetto (per l'indirizzo IP multicast 24.0.0.18 nell'esempio), si potrebbe osservare un output simile al seguente:

```
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
```

Analisi dei problemi

I registri di sistema WSA forniti nella sezione precedente indicano che quando il gruppo HA diventa un master nella negoziazione CARP, viene visualizzato un annuncio pubblicitario con una priorità migliore.

Èpossibile verificare questa condizione anche dall'acquisizione dei pacchetti. Questo è il pacchetto inviato dal server WSA virtuale:

```
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 un intervallo di tempo di millisecondi è possibile visualizzare un altro gruppo di pacchetti provenienti dallo stesso indirizzo IP di origine (lo stesso dispositivo WSA virtuale):

```
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
```

Nell'esempio, l'indirizzo IP di origine 192.168.0.131 è l'indirizzo IP del WSA virtuale che ha causato il problema. I pacchetti multicast vengono quindi rimandati indietro al WSA virtuale.

Questo problema si verifica a causa di un difetto sul lato VMware e nella sezione successiva vengono illustrati i passaggi da completare per risolvere il problema.

Soluzione

Completare questi passaggi per risolvere il problema e interrompere il loop di pacchetti multicast inviati nell'ambiente VMware:

1. Abilitare la modalità **promiscua** sullo switch virtuale (vSwitch).

2. Abilita **modifiche all'indirizzo MAC**.

3. Abilita **trasmissioni forgiate**.

4. Se sullo stesso vSwitch sono presenti più porte fisiche, è necessario abilitare l'opzione **Net.ReversePathFwdCheckPromisc** per risolvere un bug di vSwitch in cui il traffico multicast torna all'host e quindi il CARP non funziona con messaggi *uniti di stati del collegamento*. Per ulteriori informazioni, consultare la sezione successiva.

Modificare l'opzione *Net.ReversePathFwdCheckPromisc*

Completare questa procedura per modificare l'opzione *Net.ReversePathFwdCheckPromisc*:

1. Accedere al client VMware vSphere.

2. Completare questi passaggi per ciascun host VMware:

   Fare clic su **host** e passare alla scheda *Configurazione*.

   Fare clic su **Impostazioni avanzate software** nel riquadro di sinistra.

   Fare clic su **Net** e scorrere verso il basso fino all'opzione **Net.ReversePathFwdCheckPromisc**.

   Impostare l'opzione *Net.ReversePathFwdCheckPromisc* su **1**.

   Fare clic su **OK**.

Le interfacce in modalità *promiscua* devono essere impostate, disattivate e riattivate. Questa operazione viene eseguita per host.

Per impostare le interfacce, completare i seguenti passaggi:

1. Passare alla sezione *Hardware* e fare clic su **Reti**.

2. Completare questi passaggi per ogni gruppo di porte vSwitch e/o Virtual Machine (VM):

   Fare clic su **Proprietà** in vSwitch.

   Per impostazione predefinita, la modalità promiscua è impostata su *Rifiuta*. Per modificare questa impostazione, fare clic su **Modifica** e passare alla scheda *Protezione*.

   Selezionare **Accetta** dal menu a discesa.

Fare clic su **OK**.

Nota: Questa impostazione viene in genere applicata in base al gruppo di porte per VM (che è più sicuro), lasciando vSwitch all'impostazione predefinita (Rifiuta).

Completare questa procedura per disabilitare e quindi riabilitare la modalità promiscua:

1. Passare a **Modifica > Sicurezza > Eccezioni criteri**.
2. Deselezionare la casella di controllo **Modalità promiscua**.
3. Fare clic su **OK**.
4. Passare a **Modifica > Sicurezza > Eccezioni criteri**.
5. Selezionare la casella di controllo **Modalità promiscua**.
6. Selezionare **Accetta** dal menu a discesa.

Informazioni correlate

- Risoluzione dei problemi di configurazione CARP
- Documentazione e supporto tecnico – Cisco Systems