

Garantir la fonctionnalité de groupe WSA HA virtuel appropriée dans un environnement VMware

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Problème](#)

[Analyse des problèmes](#)

[Solution](#)

[Modifier l'option *Net.ReversePathFwdCheckPromisc*](#)

[Informations connexes](#)

Introduction

Ce document décrit le processus qui doit être terminé pour que la fonction haute disponibilité de Cisco Web Security Appliance (WSA) fonctionne correctement sur un WSA virtuel qui s'exécute dans un environnement VMware.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- WSA Cisco
- HTTP
- trafic multidiffusion
- Protocole CARP (Common Address Resolution Protocol)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- AsyncOS pour Web version 8.5 ou ultérieure
- VMware ESXi version 4.0 ou ultérieure

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.

Problème

Un WSA virtuel configuré avec un ou plusieurs groupes HA a toujours la HA dans l'état de *sauvegarde*, même lorsque la priorité est la plus élevée.

Les journaux système affichent un battement constant, comme illustré dans cet extrait de journal :

```
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 vous prenez une capture de paquets (pour l'adresse IP de multidiffusion 224.0.0.18 dans cet exemple), vous pouvez observer une sortie similaire à ceci :

```
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
```

Analyse des problèmes

Les journaux système WSA fournis dans la section précédente indiquent que lorsque le groupe HA devient maître dans la négociation CARP, une annonce est reçue avec une meilleure priorité.

Vous pouvez également le vérifier à partir de la capture de paquets. Il s'agit du paquet envoyé à partir de l'appareil de sécurité Web virtuel :

```
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 quelques millisecondes, vous pouvez voir un autre ensemble de paquets provenant de la même adresse IP source (la même appliance WSA virtuelle) :

```
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
```

Dans cet exemple, l'adresse IP source 192.168.0.131 est l'adresse IP du WSA virtuel problématique. Il semble que les paquets de multidiffusion soient renvoyés en boucle vers le WSA virtuel.

Ce problème se produit en raison d'un défaut du côté de VMware, et la section suivante explique les étapes à suivre pour résoudre le problème.

Solution

Complétez ces étapes afin de résoudre ce problème et d'arrêter la boucle des paquets de multidiffusion envoyés dans l'environnement VMware :

1. Activez le mode **promiscuité** sur le commutateur virtuel (vSwitch).
2. Activer les **modifications d'adresse MAC**.
3. Activer les **transmissions falsifiées**.
4. Si plusieurs ports physiques existent sur le même vSwitch, l'option **Net.ReversePathFwdCheckPromisc** doit être activée afin de contourner un bogue vSwitch où le trafic de multidiffusion retourne en boucle vers l'hôte, ce qui fait que CARP ne fonctionne pas avec des messages *d'état de liaison* fusionnés. (Reportez-vous à la section suivante pour plus d'informations).

Modifier l'option *Net.ReversePathFwdCheckPromisc*

Complétez ces étapes afin de modifier l'option *Net.ReversePathFwdCheckPromisc* :

1. Connectez-vous au client VMware vSphere.
2. Effectuez les étapes suivantes pour chaque hôte VMware :

Cliquez sur **host**, puis accédez à l'onglet *Configuration*.

Cliquez sur **Paramètres avancés du logiciel** dans le volet gauche.

Cliquez sur **Net** et faites défiler la liste jusqu'à l'option **Net.ReversePathFwdCheckPromisc**.

Définissez l'option *Net.ReversePathFwdCheckPromisc* sur **1**.

Click OK.

Les interfaces en mode *Promiscuité* doivent maintenant être définies, ou désactivées, puis réactivées. Cette opération est effectuée par hôte.

Complétez ces étapes afin de définir les interfaces :

1. Accédez à la section *Matériel* et cliquez sur **Mise en réseau**.
2. Effectuez ces étapes pour chaque groupe de ports vSwitch et/ou VM :

Cliquez sur **Propriétés** dans le vSwitch.

Par défaut, le mode Promiscuité est défini sur *Rejeter*. Pour modifier ce paramètre, cliquez sur **modifier** et accédez à l'onglet *Sécurité*.

Sélectionnez **Accepter** dans le menu déroulant.

Click OK.

Note: Ce paramètre est généralement appliqué par groupe de ports de VM (qui est plus sécurisé), où le vSwitch reste au paramètre par défaut (Rejeter).

Complétez ces étapes afin de désactiver puis réactiver le mode Promiscuité :

1. Accédez à **Edition > Sécurité > Exceptions de stratégie**.
2. Décochez la case **Mode Promiscuité**.
3. Click OK.
4. Accédez à **Edition > Sécurité > Exceptions de stratégie**.
5. Cochez la case **Mode Promiscuité**.
6. Sélectionnez **Accepter** dans le menu déroulant.

Informations connexes

- [Dépannage de la configuration CARP](#)
- [Support et documentation techniques - Cisco Systems](#)