Assurez la fonctionnalité virtuelle appropriée de groupe WSA ha dans un environnement de VMware

Contenu

Introduction

Ce document décrit le processus qui doit être terminé de sorte que la caractéristique facilement disponible des appareils de sécurité Web de Cisco (WSA) (ha) fonctionne correctement sur un WSA virtuel qui fonctionne dans un environnement de VMware.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco WSA
- HTTP
- Trafic multidiffusion
- Address Resolution Protocol commun (CARPE)

Composants utilisés

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

- AsyncOS pour la version 8.5 ou ultérieures de Web

- Version 4.0 ou ultérieures de VMware ESXi

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème

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

Les logs système affichent le lien instable constant, suivant les indications de cet extrait 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)
```

Si vous prenez une capture de paquet (pour adresse IP 224.0.0.18 de Multidiffusion dans cet exemple), vous pourriez observer un résultat semblable à ceci :

```
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)
```

Analyse de problème

Les logs système WSA qui sont fournis dans la section précédente indiquent que quand le groupe ha devient un maître dans la négociation de CARPE, il y a une publicité qui est reçue avec une meilleure priorité.

Vous pouvez vérifier ceci également de la capture de paquet. C'est le paquet qui est envoyé du WSA 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
```

Dans un calendrier de millisecondes, vous pouvez voir un autre ensemble de paquets de la même adresse IP source (la même appliance virtuelle 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
```

Dans cet exemple, l'adresse IP source de 192.168.0.131 est l'adresse IP du WSA virtuel problématique. Il s'avère que les paquets de multidiffusion sont faits une boucle - de retour pour le WSA virtuel.

Cette question se produit en raison d'un défaut du côté de VMware, et la section suivante explique les étapes que vous devez se terminer afin de résoudre le problème.

Solution

Terminez-vous ces étapes afin de résoudre ce problème et arrêter la boucle des paquets de multidiffusion qui sont introduits l'environnement de VMware :

1. Activez le mode **promiscueux** sur le commutateur virtuel (vSwitch).
2. **Modifications d'adresse MAC d'**enable.
3. L'enable **modifié transmet**.
4. Si les plusieurs ports physiques existent sur le même vSwitch, alors l'option

Net.ReversePathFwdCheckPromisc doit être activée afin de fonctionner autour d'une bogue de vSwitch où le trafic de multidiffusion fait une boucle - de retour à l'hôte, qui entraîne la CARPE à ne pas fonctionner avec des *états de lien a fusionné des* messages. (Référez-vous à la section suivante pour information les informations complémentaires).

Modifiez l'option *Net.ReversePathFwdCheckPromisc*

Terminez-vous ces étapes afin de modifier l'option *Net.ReversePathFwdCheckPromisc* :

1. Connectez-vous dans le client de vSphere de VMware.

2. Terminez-vous ces étapes pour chaque hôte de VMware :

   Cliquez sur l'**hôte**, et naviguez vers l'onglet de *configuration*.

   Paramètres avancés de logiciel de clic du volet gauche.

   Cliquez sur le **net** et le faites descendre l'écran à l'option **Net.ReversePathFwdCheckPromisc**.

   Placez l'option *Net.ReversePathFwdCheckPromisc à* **1.**

   Cliquez sur **OK**.

Les interfaces qui sont en mode *promiscueux* doivent maintenant être placées, ou arrêtées et puis de retour en fonction. Ceci est terminé sur une base de par-hôte.

Terminez-vous ces étapes afin de placer les interfaces :

1. Naviguez vers la section de *matériel* et cliquez sur le **réseau**.

2. Terminez-vous ces étapes pour chaque groupe de vSwitch et/ou de port du virtual machine (VM) :

   Clic **Properties du** vSwitch.

   Par défaut, le mode promiscueux est placé *pour rejeter*. Afin de changer cette configuration, le clic **éditent** et naviguent vers l'*onglet Sécurité*.

   Choisi **recevez du** menu déroulant.

   Cliquez sur **OK**.

   Remarque: Cette configuration est habituellement appliquée sur une base de groupe du port par-VM (qui est plus sécurisé), où le vSwitch est laissé à la valeur par défaut (anomalie).

Terminez-vous ces étapes afin de désactiver et puis réactiver le mode promiscueux :

1. Naviguez **pour éditer > des exceptions de Sécurité > de stratégie**.

2. Décochez la case à cocher **promiscueuse de mode**.

3. Cliquez sur **OK**.

4. Naviguez **pour éditer > des exceptions de Sécurité > de stratégie**.

5. Vérifiez la case à cocher **promiscueuse de mode**.

6. Choisi **recevez du** menu déroulant.

Informations connexes

- Dépannage de configuration de CARPE
- Support et documentation techniques - Cisco Systems