Sicherstellen der ordnungsgemäßen Funktion der virtuellen WSA HA-Gruppe in einer VMware-Umgebung

Inhalt

Einführung

In diesem Dokument wird der Prozess beschrieben, der abgeschlossen werden muss, damit die Hochverfügbarkeitsfunktion der Cisco Web Security Appliance (WSA) auf einer virtuellen WSA, die in einer VMware-Umgebung ausgeführt wird, ordnungsgemäß funktioniert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco WSA
- HTTP
- Multicast-Datenverkehr
- Common Address Resolution Protocol (CARP)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- AsyncOS für Web Version 8.5 oder höher
- VMware ESXi ab Version 4.0

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Eine virtuelle WSA, die mit einer oder mehreren HA-Gruppen konfiguriert ist, verfügt immer über die HA im *Backup*-Zustand, selbst wenn die Priorität die höchste ist.

Die Systemprotokolle zeigen wie in diesem Protokollausschnitt gezeigt eine konstante Flapping:

```
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)
```

Wenn Sie eine Paketerfassung vornehmen (in diesem Beispiel für die Multicast-IP-Adresse 224.0.0.18), können Sie eine Ausgabe beobachten, die der folgenden ähnelt:

```
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
```

Problemanalyse

Die im vorherigen Abschnitt bereitgestellten WSA-Systemprotokolle zeigen an, dass eine mit einer besseren Priorität empfangene Meldung vorhanden ist, wenn die HA-Gruppe in der CARP-Aushandlung Master wird.

Sie können dies auch über die Paketerfassung überprüfen. Dies ist das Paket, das von der virtuellen WSA gesendet wird:

```
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
```

Innerhalb eines Millisekunden-Zeitrahmens sehen Sie eine weitere Gruppe von Paketen von derselben Quell-IP-Adresse (dieselbe virtuelle WSA-Appliance):

```
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 diesem Beispiel ist die Quell-IP-Adresse 192.168.0.131 die IP-Adresse der problematischen virtuellen WSA. Es scheint, dass die Multicast-Pakete an die virtuelle WSA zurückgeleitet werden.

Dieses Problem tritt aufgrund eines Fehlers auf der VMware-Seite auf. Im nächsten Abschnitt werden die Schritte erläutert, die Sie zum Beheben des Problems ausführen müssen.

Lösung

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben und die Schleife von Multicast-Paketen zu stoppen, die in der VMware-Umgebung gesendet werden:

1. Aktivieren Sie den **Promiscuous**-Modus auf dem Virtual Switch (vSwitch).

2. Aktivieren Sie **MAC-Adressänderungen**.

3. Aktivieren **gefälschter Übertragungen**.

4. Wenn mehrere physische Ports auf demselben vSwitch vorhanden sind, muss die Option **Net.ReversePathFwdCheckPromisc** aktiviert werden, um einen vSwitch-Fehler zu umgehen, bei dem der Multicast-Datenverkehr zurück zum Host schleift, wodurch die CARP nicht mit *Verbindungszuständen synchronisierten* Nachrichten funktioniert. (Weitere Informationen finden Sie im nächsten Abschnitt.)

Ändern Sie die *Net.ReversePathFwdCheckPromisc*-Option.

Gehen Sie wie folgt vor, um die Option *Net.ReversePathFwdCheckPromisc* zu ändern:

1. Melden Sie sich beim VMware vSphere-Client an.

2. Führen Sie die folgenden Schritte für jeden VMware-Host aus:

   Klicken Sie auf **Host**, und navigieren Sie zur Registerkarte *Konfiguration*.

   Klicken Sie im linken Fensterbereich auf **Software Advanced Settings** (Erweiterte **Softwareeinstellungen**).

   Klicken Sie auf **Net**, und scrollen Sie nach unten zur Option **Net.ReversePathFwdCheckPromisc**.

   Legen Sie die Option *Net.ReversePathFwdCheckPromisc* auf **1 fest**.

   Klicken Sie auf **OK**.

Die Schnittstellen, die sich im *Promiscuous*-Modus befinden, müssen nun eingestellt oder deaktiviert und dann wieder aktiviert werden. Dies wird für jeden Host abgeschlossen.

Gehen Sie wie folgt vor, um die Schnittstellen festzulegen:

1. Navigieren Sie zum Abschnitt *Hardware*, und klicken Sie auf **Networking**.

2. Führen Sie die folgenden Schritte für jede vSwitch- und/oder VM-Portgruppe aus:

   Klicken Sie auf **Eigenschaften** des vSwitch.

   Der Promiscuous-Modus ist standardmäßig auf *Ablehnen* eingestellt. Um diese Einstellung

zu ändern, klicken Sie auf **Bearbeiten** und navigieren Sie zur Registerkarte *Sicherheit*.

Wählen Sie **im** Dropdown-Menü die Option **Akzeptieren** aus.

Klicken Sie auf **OK**.

Hinweis: Diese Einstellung wird in der Regel pro VM-Portgruppe angewendet (was sicherer ist), wobei der vSwitch bei der Standardeinstellung belassen wird (Ablehnen).

Gehen Sie wie folgt vor, um den Promiscuous-Modus zu deaktivieren und wieder zu aktivieren:

1. Navigieren Sie zu **Bearbeiten > Sicherheit > Richtlinienausnahmen**.
2. Deaktivieren Sie das Kontrollkästchen **Promiscuous Mode**.
3. Klicken Sie auf **OK**.
4. Navigieren Sie zu **Bearbeiten > Sicherheit > Richtlinienausnahmen**.
5. Aktivieren Sie das Kontrollkästchen **Promiscuous Mode**.
6. Wählen Sie im Dropdown-Menü **Accept (Akzeptieren)** aus.

Zugehörige Informationen

- Fehlerbehebung bei CARP-Konfiguration
- Technischer Support und Dokumentation - Cisco Systems