Функциональность Ensure Proper Virtual WSA HA Group в среде VMware

Содержание

Введение

Этот документ описывает процесс, который должен быть завершен так, чтобы Cisco Web Security Appliance (WSA), функция Высокой доступности (HA) работает должным образом на Действительный WSA, который выполняется в среде VMware.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco WSA
- HTTP
- Многоадресный трафик
- Общий протокол разрешения адресов (CARP)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- AsyncOS для Версии веб - приложения 8.5 или позже

- VMware Версия 4.0 ESXi или позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Проблема

Действительный WSA, который настроен с одной или более группами HA всегда, имеет HA в *состоянии резервирования*, даже когда приоритет является самым высоким.

Системные журналы показывают постоянную переброску, как показано в этом регистрационном фрагменте:

```
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)
```

При взятии захвата пакета (для IP-адреса групповой адресации 224.0.0.18 в данном примере), вы могли бы наблюдать выходные данные, подобные этому:

```
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
```

Анализ задач

Системные журналы WSA, которые предоставлены в предыдущем разделе, указывают, что, когда группа HA становится Ведущим устройством на согласовании CARP, существует реклама, которая получена с лучшим приоритетом.

Можно проверить это также от захвата пакета. Это - пакет, который передан от действительного WSA:

```
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
```

Во временной рамке миллисекунд вы видите другой набор пакетов от того же IP - адреса источника (то же действительное устройство 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
```

В данном примере IP - адресом источника 192.168.0.131 является IP-адрес проблематичного действительного WSA. Кажется, что пакеты групповой адресации циклично выполнены назад к действительному WSA.

Эта проблема происходит из-за дефекта на стороне VMware, и следующий раздел объясняет шаги, которые необходимо выполнить для решения вопроса.

Решение

Выполните эти шаги, чтобы решить этот вопрос и остановить петлю пакетов групповой адресации, которые передаются в среде VMware:

1. Включите **случайный режим** на Виртуальном коммутаторе (vSwitch).

2. Включите **изменения MAC-адреса**.

3. Включите **Подделанные передачи**.

4. Если порты несколька физических каналов существуют на том же vSwitch, то **Сеть.** Опция **ReversePathFwdCheckPromisc** должна быть включена для обхождения vSwitch дефекта, где петли многоадресного трафика назад к хосту, который заставляет CARP не функционировать с *состояниями канала, объединили* сообщения. (См. следующий раздел для дополнительных сведений).

Модифицируйте *сеть.* Опция *ReversePathFwdCheckPromisc*

Выполните эти шаги для изменения *Сети.* Опция *ReversePathFwdCheckPromisc*:

1. Войдите в клиента VMware vSphere.

2. Выполните эти шаги для каждого хоста VMware:

   Нажмите **хост** и перейдите к *Вкладке конфигурация*.

   Нажмите **Software Advanced Settings** от левой панели.

   Нажмите **Net** и прокрутите вниз к **Сети.** Опция **ReversePathFwdCheckPromisc**.

   Поставьте *Сеть.* Опция *ReversePathFwdCheckPromisc* к **1**.

   Нажмите кнопку ОК.

Интерфейсы, которые находятся в *Случайном режиме*, должны теперь быть установлены или выключены и затем назад на. Это завершено на основе на хост.

Выполните эти шаги для установки интерфейсов:

1. Перейдите к *Разделу оборудования* и нажмите **Networking**.

2. Выполните эти шаги для каждого vSwitch и/или группы портов Виртуальной машины (VM):

   Нажмите **Properties** от vSwitch.

   По умолчанию Случайный режим собирается *Отклонить*. Для изменения этих настроек, щелчок **редактируют** и перешли к *Вкладке Безопасность*.

   Выберите **Accept** от раскрывающегося меню.

   Нажмите кнопку ОК.

Примечание: Эта установка обычно применяется на основе группы портов на VM (который более безопасен), где vSwitch оставляют при настройке по умолчанию (Отклонение).

Выполните эти шаги, чтобы отключить и затем реактивировать Случайный режим:

1. Перейдите для **Редактирования> Security> Исключения Политики**.
2. Анчек флажок **Promiscuous Mode**.
3. **Нажмите кнопку ОК.**
4. Перейдите для **Редактирования> Security> Исключения Политики**.
5. Проверьте флажок **Promiscuous Mode**.
6. Выберите **Accept** от раскрывающегося меню.

Дополнительные сведения

- Устранение проблем конфигурации CARP
- Cisco Systems – техническая поддержка и документация