

WSA ةومجمل ةبسانم فئاظورفوت نم دكأت VMware ةئي ب ي ف HA

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[المشكلة](#)

[تحليل المشاكل](#)

[الحل](#)

[تعديل خيار `Net.ReversePathFwdCheckPromisc`](#)

[معلومات ذات صلة](#)

المقدمة

يصف هذا المستند العملية التي يجب إكمالها حتى تعمل ميزة التوفر العالي (WSA) لأجهزة أمان الويب (WSA) من Cisco بشكل صحيح على شبكة WSA افتراضية تعمل في بيئة VMware.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco WSA
- HTTP
- حركة مرور البث المتعدد
- بروتوكول تحليل العنوان الشائع (CARP)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Web J AsyncOS الإصدار 8.5 أو الأحدث

• برنامج VMware ESXi الإصدار 4.0 أو إصدار أحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المشكلة

دائما ما تتضمن WSA الظاهرية التي تم تكوينها باستخدام مجموعة HA واحدة أو أكثر HA حالة النسخ الاحتياطي، حتى عندما تكون الأولوية هي الأعلى.

تظهر سجلات النظام التدفق المستمر، كما هو موضح في قصاصة السجل هذه:

```
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)
```

إذا أخذت التقاط حزمة (لعنوان IP للث المتعدد 224.0.0.18 في هذا المثال)، فقد تلاحظ مخرجات مماثلة:

```
,[IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF 13:49:04.601713
(proto VRRP (112), length 56
:carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36 :224.0.0.18 < 192.168.0.131
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
,[IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF 13:49:04.601931
(proto VRRP (112), length 56
:carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36 :224.0.0.18 < 192.168.0.131
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
,[IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF 13:49:04.602798
(proto VRRP (112), length 56
:carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36 :224.0.0.18 < 192.168.0.131
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
,[IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF 13:49:04.602809
(proto VRRP (112), length 56
:carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36 :224.0.0.18 < 192.168.0.131
vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
,[IP (tos 0x10, ttl 255, id 24801, offset 0, flags [DF 13:49:13.621706
(proto VRRP (112), length 56
```

```

:carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36 :224.0.0.18 < 192.168.0.131
      vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178284
      ,[IP (tos 0x10, ttl 255, id 24801, offset 0, flags [DF 13:49:13.622007
      (proto VRRP (112), length 56
:carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36 :224.0.0.18 < 192.168.0.131
      vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178284
      ,[IP (tos 0x10, ttl 255, id 24801, offset 0, flags [DF 13:49:13.622763
      (proto VRRP (112), length 56
:carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36 :224.0.0.18 < 192.168.0.131
      vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178284
      ,[IP (tos 0x10, ttl 255, id 24801, offset 0, flags [DF 13:49:13.622770
      (proto VRRP (112), length 56
:carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36 :224.0.0.18 < 192.168.0.131
      vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178284
      ,[IP (tos 0x10, ttl 255, id 44741, offset 0, flags [DF 13:49:22.651653
      (proto VRRP (112), length 56
:carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36 :224.0.0.18 < 192.168.0.131
      vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178285

```

تحليل المشاكل

تشير سجلات نظام WSA المقدمة في القسم السابق إلى أنه عندما تصبح مجموعة HA رئيسيا في تفاوض CARP، هناك إعلان يتم إستقباله بأولوية أفضل.

أنت تستطيع دقت هذا أيضا من الربط التقاط. هذا الربط أن يكون أرسلت من ال WSA ظاهري:

```

      ,[IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF 13:49:04.601713
      (proto VRRP (112), length 56
:carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36 :224.0.0.18 < 192.168.0.131
      vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283

```

في الإطار الزمني بالمللي ثانية، يمكنك رؤية مجموعة أخرى من الحزم من نفس عنوان IP المصدر (نفس جهاز WSA الظاهري):

```

      ,[IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF 13:49:04.602798
      (proto VRRP (112), length 56
:carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36 :224.0.0.18 < 192.168.0.131
      vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283
      ,[IP (tos 0x10, ttl 255, id 4785, offset 0, flags [DF 13:49:04.602809
      (proto VRRP (112), length 56
:carp 192.168.0.131 > 224.0.0.18: CARPv2-advertise 36 :224.0.0.18 < 192.168.0.131
      vhid=94 advbase=3 advskew=1 authlen=7 counter=15790098039517178283

```

في هذا المثال، عنوان IP المصدر 192.168.0.131 هو عنوان IP الخاص ب WSA الظاهري الإشكالي. يبدو أن الربط multicast أنشطت - خلفي إلى ال WSA ظاهري.

يقع هذا إصدار واجب إلى خلل على ال VMware جانب، وبشرح القسم تالي الخطوات أن أنت ينبغي أتمت in order to حللت الإصدار.

الحل

أتمت هذا steps in order to حللت هذا إصدار وإيقاف أنشوطه من multicast ربط أن يكون أرسلت في ال VMware بيئة:

1. قم بتمكين الوضع المختلطة على المحول الظاهري (vSwitch).

تمكين تغييرات عنوان MAC.

.2

تمكين رسائل الإرسال المزورة.

.3

4. إذا كانت هناك منافذ مادية متعددة على المحول vSwitch نفسه، فيجب تمكين خيار `Net.ReversePathFwdCheckPromisc` للعمل حول خطأ vSwitch حيث تكرارات حركة مرور البث المتعدد مرة أخرى إلى المضيف، مما يتسبب في عدم عمل بروتوكول CARP مع رسائل حالات الارتباط التي تم دمجها. (راجع القسم التالي للحصول على معلومات إضافية).

تعديل خيار `Net.ReversePathFwdCheckPromisc`

أكمل الخطوات التالية لتعديل خيار `Net.ReversePathFwdCheckPromisc`:

.1

قم بتسجيل الدخول إلى عميل vSphere من VMware.

2. أكمل الخطوات التالية لكل مضيف VMware:

انقر فوق المضيف، وانتقل إلى علامة التبويب التكوين.

انقر على إعدادات متقدمة للبرامج من اللوحة اليسرى.

انقر فوق Net وانتقل لأسفل إلى خيار `Net.ReversePathFwdCheckPromisc`.

قم بتعيين خيار `Net.ReversePathFwdCheckPromisc` على 1.

وانقر فوق OK.

يجب الآن تعيين الواجهات الموجودة في وضع *المختلطة* أو إيقاف تشغيلها ثم إعادة تشغيلها. ويتم إكمال ذلك على أساس كل مضيف.

أتمت هذا steps in order to ثبتت القارن:

.1

انتقل إلى قسم الأجهزة وانقر فوق الشبكة.

2. أكمل الخطوات التالية لكل محول vSwitch و/أو مجموعة منافذ الأجهزة الظاهرية (VM):

انقر فوق خصائص من vSwitch.

بشكل افتراضي، يتم تعيين الوضع المختلط على الرفض. لتغيير هذا الإعداد، انقر فوق تحرير وانتقل إلى علامة التبويب أمان.

حدد قبول من القائمة المنسدلة.

وانقر فوق OK.

ملاحظة: يطبق هذا الإعداد عادة على أساس كل مجموعة منافذ VM (وهو أكثر أماناً)، حيث يتم ترك vSwitch في الإعداد الافتراضي (رفض).

أكمل الخطوات التالية لتعطيل الوضع المختلط ثم إعادة تمكينه:

- .1 انتقل إلى تحرير < التأمين > إستثناءات السياسة.
- .2 قم بإلغاء تحديد خانة الاختيار الوضع المختلط.
- .3 وانقر فوق OK.
- .4 انتقل إلى تحرير < التأمين > إستثناءات السياسة.
- .5 حدد خانة الاختيار الوضع المختلط.
- .6 حدد قبول من القائمة المنسدلة.

معلومات ذات صلة

- [أستكشاف أخطاء تكوين CARP وإصلاحها](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل