

اهال صإو FWSM ءاطخأ فاشككسأ

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [معلومات أساسية](#)
- [قائمة التحقق من تجاوز الفشل](#)
- [التحقق من الواجهات](#)
- [التراخيص](#)
- [وضع السياق](#)
- [متطلبات البرامج](#)
- [أدنى تكوين FWSM لتخطي الفشل ذو الحالة](#)
- [الحد الأدنى لتكوين المحول](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [عدم تطابق الإصدار](#)
- [التراخيص غير المتوافقة](#)
- [صيغ مختلفة \(سياق واحد مقابل سياق متعدد\)](#)
- [FWSMs يصبح نشط](#)
- [VLAN حالة عدم توافق](#)
- [تم تعطيل تجاوز الفشل](#)
- [معلومات ذات صلة](#)

المقدمة

يشرح هذا المستند الإجراءات التي يمكنك استخدامها لحل المشاكل المتعلقة بتكوين تجاوز الفشل للوحدة النمطية لخدمة جدار الحماية (FWSM).

كما يوفر هذا المستند قائمة تحقق من الإجراءات الشائعة لمحاولة استكشاف أخطاء اتصال تجاوز الفشل وإصلاحها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى FWSM 2.3 والإصدارات الأحدث.

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.

الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

معلومات أساسية

تتيح ميزة تجاوز الفشل ل FWSM الاستعداد إمكانية تولى وظائف فشل FWSM. يجب أن يكون لكل من FWSMs المعنية نفس إصدار البرنامج الرئيسي (الرقم الأول) والإصدار الثانوي (الرقم الثاني) والترخيص وأوضاع التشغيل (موجه أو شفاف وسياق فردي أو متعدد). وعندما يفشل الوحدة النشطة، تتغير الحالة إلى وضع الاستعداد، بينما تنتقل الوحدة الاحتياطية إلى الحالة النشطة. بعد حدوث تجاوز الفشل، تتوفر نفس معلومات الاتصال في الوحدة النشطة الجديدة.

لمزيد من المعلومات، ارجع إلى قسم [تكوين تجاوز الفشل](#) في استخدام تجاوز الفشل.

قائمة التحقق من تجاوز الفشل

تساعدك قائمة التحقق هذه على تكوين تجاوز الفشل في FWSM بنجاح:

- [التحقق من الواجهات](#)
- [التراخيص](#)
- [وضع السياق](#)
- [متطلبات البرامج](#)
- [أدنى تكوين FWSM لتخطي الفشل ذو الحالة](#)
- [الحد الأدنى لتكوين المحول](#)

التحقق من الواجهات

دققت أن يتلقى كل قارن على ال FWSM عنوان يشكل إستعداد. إذا لم تكن قد قمت بذلك بالفعل، فقم بتكوين عناوين IP النشطة والاحتياطية لكل واجهة (الوضع الموجه)، أو لعنوان الإدارة (الوضع الشفاف). يتم استخدام عنوان IP الاحتياطي على FWSM الذي يمثل حالياً الوحدة الاحتياطية. يجب أن يكون في الشبكة الفرعية نفسها الخاصة بعنوان IP النشط.

هذا مثال على التكوين:

```
<ip address <active-ip> <netmask> standby <standby-ip>
```

ملاحظة: لا تقم بتكوين عنوان IP لارتباط تجاوز الفشل أو ارتباط الحالة (إذا كنت تريد استخدام تجاوز الفشل ذو الحالة).

ملاحظة: لا تحتاج إلى تحديد قناع الشبكة الفرعية للعنوان الاحتياطي. لا يتغير عنوان IP لارتباط تجاوز الفشل وعنوان MAC عند تجاوز الفشل. يظل عنوان IP النشط لارتباط تجاوز الفشل دائماً مع الوحدة الأساسية، بينما يظل عنوان IP الاحتياطي مع الوحدة الثانوية.

التراخيص

يجب أن يكون لكل من الوحدات النشطة والاحتياطية نفس الترخيص.

وضع السياق

إذا كانت الوحدة الأساسية في وضع سياق واحد، يجب أن تكون الوحدة الثانوية أيضا في وضع سياق واحد وفي نفس وضع جدار الحماية كوحدة أساسية.

إذا كانت الوحدة الأساسية في وضع سياق متعدد، يجب أن تكون الوحدة الثانوية أيضا في وضع سياق متعدد. لا تحتاج إلى تكوين وضع جدار الحماية لسياقات الأمان على الوحدة الثانوية لأن إرتباطات الحالة وتجاوز الفشل موجودة في سياق النظام. تحصل الوحدة الثانوية على تكوين سياق الأمان من الوحدة الأساسية.

ملاحظة: لا يتم نسخ الأمر mode نسخا متماثلا إلى الوحدة الثانوية.

ملاحظة: لا يتم دعم البث المتعدد في وضع السياق المتعدد الخاص بجهاز الأمان. راجع قسم [الميزات غير المدعومة](#) للحصول على مزيد من المعلومات.

متطلبات البرامج

يجب أن تحتوي الوحدات في تكوين تجاوز الفشل على نفس إصدار البرنامج الرئيسي (الرقم الأول) والصغير (الرقم الثاني). ومع ذلك، يمكنك استخدام إصدارات مختلفة من البرنامج أثناء عملية ترقية. على سبيل المثال، يمكنك ترقية وحدة واحدة من الإصدار 3.1(1) إلى الإصدار 3.1(2) وتبقى عملية تجاوز الفشل نشطة. توصي Cisco بترقية كلتا الوحدتين إلى نفس الإصدار لضمان التوافق طويل الأجل.

أدنى تكوين FWSM لتخطي الفشل ذو الحالة

FWSM أساسي

```
failover lan unit primary
failover lan interface if_name vlan vlan failover interface ip if_name ip_addr mask standby
ip_addr failover link if_name vlan vlan failover interface ip if_name ip_addr mask standby
ip_addr
```

FWSM الثانوي

```
failover lan unit secondary
failover lan interface if_name vlan vlan failover interface ip if_name ip_addr mask standby
ip_addr failover link if_name vlan vlan failover interface ip if_name ip_addr mask standby
ip_addr
```

لمزيد من المعلومات حول كيفية تكوين تجاوز الفشل في وضع الاستعداد والنشاط، ارجع إلى [تكوين تجاوز الفشل في وضع الاستعداد/النشط](#).

الحد الأدنى لتكوين المحول

• ال VLANs يرسل إلى الأساسي FWSM ب المادة حفازة أن يحتوي الأساسي ينبغي طبقت VLANs يرسل إلى الثانوي FWSM بالمادة حفازة أن يحتوي على الثانوي. (إخراج تشغيل العرض | يجب أن يكون الأمر ifirewall

مطابقا.) الهيكل الأساسي

```
cat6k-7(config)#do sh run | i fire
firewall multiple-vlan-interfaces
firewall module 9 vlan-group 1
firewall vlan-group 1 3,4,100-106
```

الهيكل الثانوي

```
cat6k-7(config)#do sh run | i fire
firewall multiple-vlan-interfaces
firewall module 9 vlan-group 1
firewall vlan-group 1 3,4,100-106
```

• all the VLANs أن يكون أرسلت ينبغي كنت حاضر في ال VLAN قاعدة معطيات وكنت نشط. أصدرت in order to أنجزت هذا، هذا أمر على المفتاح في تشكيل أسلوب:

```
vlan 10
no shut
```

in order to دقت إن يكون VLANs في القاعدة معطيات ونشيط، الإنتاج من العرض vlan أمر على كلا هيكل ينبغي احتويت VLANs يرسل إلى ال FWSM ويدي بما أن نشط. هذا نموذج للمخرجات: الهيكل الأساسي

```
cat6k-7(config)#do sh vlan
```

VLAN Name	Status	Ports
default	active	1
VLAN0003	active	Fa4/47 3
VLAN0004	active	Fa4/48 4

الهيكل الثانوي

```
cat6k-7(config)#do sh vlan
```

VLAN Name	Status	Ports
default	active	1
VLAN0003	active	Fa4/47 3
VLAN0004	active	Fa4/48 4

• تأكدت أن الإثان FWSMs يتلقى طبقة 2 موصولية في كل VLAN (هم ينبغي كنت في ال نفسه subnet). متطلبات جدار الحماية الشفافة: لتجنب حلقات التكرار عند استخدام تجاوز الفشل في الوضع الشفاف، يجب أن تستخدم برنامج المحول الذي يدعم إعادة توجيه وحدة بيانات بروتوكول الجسر (BPDU). أيضا، أنت ينبغي شكلت ال FWSM أن يسمح in order to سمحت BPDUs من خلال ال FWSM، شكلت EtherType ACL وتطبيقها على كلا الواجهات. ملاحظة: بخلاف النظام الأساسي لكل من PIX و ASA، فإن الأجهزة الخاصة بمقامين نصليين FWSM هي نفسها دائما، وليس هناك طرز أو تكوينات مختلفة للذاكرة.

استكشاف الأخطاء وإصلاحها

عند إعادة تحميل FWSM، ستسبب السيناريوهات الموضحة في هذا القسم في تعطيل تجاوز الفشل.

يمكن إعادة تحميل FWSM لأسباب مثل عطل، أو إعادة ضبط من الهيكل، أو إعادة تحميل تم إصدارها من واجهة سطر الأوامر (CLI) ل FWSM، أو يمكن أن تكون مجرد وحدة نمطية جديدة يتم إدراجها أو إعادة تعيينها في فتحة مختلفة أو تتم إعادة تشغيلها من الهيكل.

عدم تطابق الإصدار

يجب أن تحتوي الوحدات في تكوين تجاوز الفشل على نفس إصدار البرنامج الرئيسي (الرقم الأول) والصغير (الرقم الثاني).

رسالة syslog ذات الصلة: [105040](#)

التراخيص غير المتوافقة

قد تتلقى هذا syslog بسبب ترخيص غير متوافق:

```
FWSM-1-105045: (Primary) Mate license (number contexts) is not compatible
.(with my license (number contexts
.FWSM-1-105001: (Primary) Disabling failover
رسائل syslog ذات الصلة: 105045 و 105001
```

صنع مختلفة (سياق واحد مقابل سياق متعدد)

يجب أن يكون كل من FWSM الأساسي والثانوي في الوضع نفسه (أحادي أو متعدد). على سبيل المثال، إذا تم تكوين الأساسي كوضع واحد والثانوي كوضع متعدد والثانوي كما تم إعادة تحميل الثانوي، فستقوم كلتا الوحدتين بإيقاف تشغيل تجاوز الفشل.

أساسي في الوضع المفرد:

```
.(FWSM-1-103001: (Primary) No response from other firewall (reason code = 1%
FWSM-1-105044: (Primary) Mate operational mode (Multi) is not compatible%
.(with my mode (Single
.FWSM-1-105001: (Primary) Disabling failover%
ثانوي في وضع متعدد (يتم إعادة تحميل هذا الخادم النصلي):
```

```
.FWSM-5-111008: User 'Config' executed the 'no snmp-server location' command%
.FWSM-5-111008: User 'Config' executed the 'inspect tftp' command%
'FWSM-5-111008: User 'Config' executed the 'service-policy global_policy global%
.command
.FWSM-5-111008: User 'Config' executed the 'config-url disk:/admin.cfg' command%
.FWSM-5-111008: User 'Config' executed the 'prompt hostname context' command%
FWSM-4-411001: Line protocol on Interface LAN, changed state to up%
FWSM-4-411001: Line protocol on Interface LAN, changed state to up%
FWSM-1-105044: (Secondary) Mate operational mode (Single) is not compatible%
.(with my mode (Multi
.FWSM-1-105001: (Secondary) Disabling failover%
.FWSM-6-199002: Startup completed. Beginning operation%
FWSM-6-605005: Login permitted from 127.0.0.51/15518 to eobc:127.0.0.91/telnet%
" " for user
FWSM-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15%
.FWSM-5-111008: User 'enable_15' executed the 'changeto context admin' command%
أساسي في الوضع المتعدد:
```

```
FWSM-1-105044: (Primary) Mate operational mode (Single) is not compatible%
.(with my mode (Multi
.FWSM-1-105001: (Primary) Disabling failover%
رسائل syslog ذات الصلة: 105044، 103001، 105001
```

FWSMs يصبح نشط

عندما ترى رسالة الخطأ هذه في السجل:

```
fw_create_pc_sw: fw_create_portchannel failed
السبب ل هذا خطأ لأن الرقم الموصى به من قناة أيسر في المفتاح تجاوز الحد الأقصى (128 هو الحد الأقصى في
cisco ios برمجية إطلاق 12.2(33)sxh4 على Cat6000/6500). لذلك، يتم الآن استنفاد حد كتلة واصف الواجهة
.(IDB)
```

بسبب هذا، قد ينتهي بك الأمر مع هاتين المسألتين:

- عندما يكون لديك محولان بوحدات FWSM النمطية للعمل كنشطة واحتياطية، تصبح وحدات FWSM نشطة في نفس الوقت.
 - لا يمكنك إنشاء قناة منفذ إضافية.
- احذف قنوات المنفذ غير الضرورية وأعد تحميل FWSMs، كجزء من حل المشكلة.

VLAN حالة عدم توافق

المشكلة

يستلم FWSM هذا خطأ رسالة: 'تم الكشف عن شريك نشيط' 'عدم تطابق تكوين شبكة VLAN' 'سيتم تعطيل تجاوز الفشل!'

أو

يبدو أن تكوين الوحدات النمطية لخدمة جدار الحماية وتكوين المحول المقابل قد اكتمل. ومع ذلك، يتعذر على FWSMs مزامنة بعضها البعض. يتم تلقي هذه الرسالة على المضيف الثانوي:

```
State check detected an Active mate
```

```
.Unable to verify vlan configuration with mate  
Check that mate's failover is enabled
```

```
No Response from Mate
```

أو

تظهر مخرجات الأمر **show failover** حالة تجاوز الفشل على الوحدة الثانوية وحالة تجاوز الفشل لـ FWSM في () .

```
FWSM-secondary(config)#show failover  
(Failover Off (pseudo-Standby
```

الحل

قد تكون المشكلة عدم توافق VLAN تنازل عبر جدار الحماية (FWSMs والمشرفين). على سبيل المثال، في بيان المجموعة 1 لجدار الحماية vlan، يمكن أن يختلف نفس عدد شبكات VLAN التي تم تعيينها على كل محول إلى جدار الحماية. قد يتسبب ذلك في حدوث المشكلة. إن يعين أنت ال نفسه رقم VLANs في جدار الحماية، بعد ذلك الفشل يعمل.

in order to تفاديت يحصل VLAN تشكيل حالة عدم توافق خطأ، العرض vlan أمر إنتاج ينبغي كنت متماثل على كلا FWSMs. تحدث رسالة الخطأ هذه فقط عندما تقوم بتعديل تكوين تجاوز الفشل أو تحميله على FWSM. على سبيل المثال، عند تمهيد FWSM، فإنه يقوم بتحميل startup-config من الذاكرة المؤقتة ويحاول تهينة تجاوز الفشل. في هذا الوقت، هو يتحقق أن كلا وحدة نمطية يستلم ال VLANs صحيح. إذا لم تتطابق شبكات VLAN، يتم عرض رسالة الخطأ ويبقى تجاوز الفشل معطلا.

ملاحظة: يتطلب بروتوكول FWSM، من أجل العمل على تجاوز الأعطال، تكوينات ومهام منافذ متطابقة. من الممكن تجاوز الفشل بين الهياكل، ولكن يجب أن تكون كل شبكة VLAN معينة إلى جدار الحماية في خط الاتصال بين الهيكلين.

لا يتضمن FWSM أي واجهات مادية خارجية. وبدلاً من ذلك، يستخدم واجهات شبكات VLAN. يعين VLANs إلى ال FWSM مماثل إلى يعين VLAN إلى مفتاح ميناء. يتضمن ال FWSM قارن داخلي إلى المفتاح بناء وحدة نمطية (إن يتواجد) أو ال يشارك حافلة. لمزيد من المعلومات، ارجع إلى [تعيين شبكات VLAN إلى الوحدة النمطية لخدمات جدار الحماية](#).

مدرك أن ال VLAN يخطط يستطيع كنت عدلت أثناء عمل FWSM setup وسوف يفشل أثناء جزمة تالي.

[تم تعطيل تجاوز الفشل](#)

عندما تقوم بتعطيل تجاوز الفشل باستخدام الأمر [no failover](#)، يتم الحفاظ على الحالة الحالية للوحدة (سواء كانت نشطة أو في وضع الاستعداد) حتى يتم إعادة تحميل الوحدة. لا يستخدم هذا إلا لتعطيل تجاوز الفشل. لتغيير حالة الوحدة من الوضع النشط إلى وضع الاستعداد أو العكس، يلزمك استخدام الأمر [\[no\] failover active](#).

[معلومات ذات صلة](#)

- [FWSM: تهينة تجاوز الفشل](#)
- [FWSM: رسائل سجل النظام](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا