تكوين التوفر العالي لـ ZBFW واستكشاف أخطائه وإصلاحها

المحتويات

المقدمة

يوفر هذا الدليل التكوين الأساسي لجدار حماية المنطقة عالي التوفر (HA) للإعداد النشط/الاحتياطي، بالإضافة إلى أوامر أستكشاف الأخطاء وإصلاحها والمشاكل الشائعة التي يتم رؤيتها مع الميزة.

يدعم جدار الحماية القائم على المنطقة (ZBFW)® من Cisco IOS حتى يمكن تكوين موجهات Cisco IOS في إعداد نشط/إحتياطي أو نشط/نشط. وهذا يسمح بالتكرار لمنع نقطة واحدة من الفشل.

المتطلبات الأساسية

المتطلبات

يجب أن يكون لديك إصدار أحدث من برنامج Cisco IOS Software، الإصدار 15.2(3)T.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

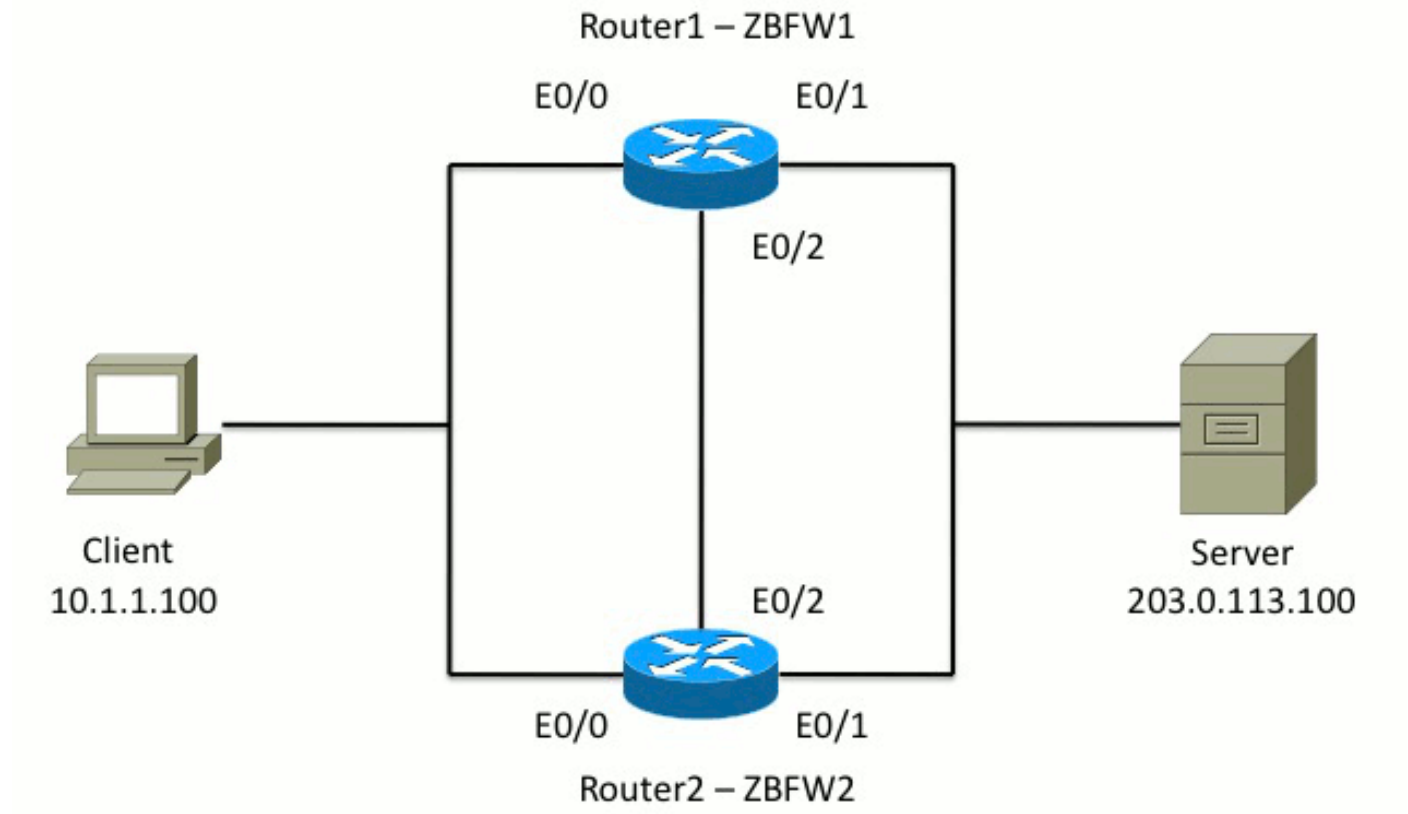
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

التكوين

يوضح هذا المخطط المخطط المخطط المستخدم في أمثلة التكوين.



في التكوين الموضح في المثال 1، يتم تكوين ZBFW من أجل فحص حركة مرور بروتوكول TCP و UDP و Internet Control Message Protocol (ICMP) من الداخل إلى الخارج. يقوم التكوين الموضح بالأسود بإعداد ميزة HA. في موجهات Cisco IOS، يتم تكوين HA عبر أمر **التكرار** subconfig. لتكوين التكرار، تتمثل الخطوة الأولى في

تمكين التكرار في خريطة معلمات الفحص العام.

بعد تمكين التكرار، أدخل التكوين الفرعي **تكرار التطبيق**، وحدد الواجهات التي يتم إستخدامها **للتحكم والبيانات**. يتم إستخدام واجهة التحكم لتبادل المعلومات حول حالة كل موجه. يتم إستخدام واجهة البيانات لتبادل المعلومات حول الاتصالات التي يجب نسخها نسخا متماثلا.

في المثال 2، يتم تعيين الأمر **priority** أيضا لجعل الموجه 1 الوحدة النشطة في الزوج إذا كان كل من الموجه 1 والموجه 2 قيد التشغيل. يتم إستخدام الأمر **pre** (الذي تمت مناقشته أيضا أكثر في هذا المستند) لضمان حدوث الفشل بمجرد تغيير الأولوية.

تتمثل الخطوة الأخيرة في تخصيص **معرف الواجهة المتكرر (RII)** و**مجموعة التكرار (RG)** لكل واجهة. يجب أن يكون رقم مجموعة **RII** فريدا لكل واجهة، ولكن يجب أن تتطابق عبر الأجهزة للواجهات في الشبكة الفرعية نفسها. لا يتم إستخدام RII إلا لعملية المزامنة المجمعة عندما يقوم كلا الموجهين بمزامنة التكوين. هذه هي الطريقة التي يقوم بها الموجهان بمزامنة الواجهات المتكررة. يتم إستخدام **RG** للإشارة إلى نسخ الاتصالات من خلال تلك الواجهة في جدول اتصال HA.

في المثال 2، يتم إستخدام الأمر **تكرار مجموعة 1** لإنشاء عنوان IP ظاهري (VIP) على الواجهة الداخلية. وهذا يضمن التوفر الفائق للطاقة (HA)، نظرا لأن جميع المستخدمين الداخليين يتواصلون فقط مع الشخصية المهمة، والتي تقوم الوحدة النشطة بمعالجتها.

لا تحتوي الواجهة الخارجية على أي تكوين RG لأن هذه هي واجهة WAN. لا تنتمي الواجهة الخارجية لكل من الموجه 1 والموجه 2 إلى موفر خدمة الإنترنت (ISP) نفسه. على الواجهة الخارجية، يلزم بروتوكول توجيه ديناميكي لضمان مرور البيانات إلى الجهاز الصحيح.

مثال 1: قصاصة تكوين الموجه 1 (hostname zbfw1)

```
parameter-map type inspect global
redundancy
log dropped-packets enable
!
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 200
control Ethernet0/2 protocol 1
data Ethernet0/2
!
class-map type inspect match-any PROTOCOLS
match protocol tcp
match protocol udp
match protocol icmp
class-map type inspect match-all INSIDE_TO_OUTSIDE_CMAP
match class-map PROTOCOLS
match access-group name INSIDE_TO_OUTSIDE_ACL
!
policy-map type inspect INSIDE_TO_OUTSIDE_PMAP
class type inspect INSIDE_TO_OUTSIDE_CMAP
inspect
class class-default
drop
!
ip access-list extended INSIDE_TO_OUTSIDE_ACL
permit ip any any
!
```

```
 zone security INSIDE
 zone security OUTSIDE
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE_TO_OUTSIDE_PMAP
 !
 interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 zone-member security INSIDE
 redundancy rii 100
 redundancy group 1 ip 10.1.1.3 exclusive
 !
 interface Ethernet0/1
 ip address 203.0.113.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 zone-member security OUTSIDE
 redundancy rii 200
```

مثال 2: قصاصة تكوين الموجه 2 (hostname zbfw2)

```
 parameter-map type inspect global
 redundancy
 log dropped-packets enable
 !
 redundancy
 application redundancy
 group 1
 name ZBFW_HA
 preempt
 priority 200
 control Ethernet0/2 protocol 1
 data Ethernet0/2
 !
 class-map type inspect match-any PROTOCOLS
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all INSIDE_TO_OUTSIDE_CMAP
 match class-map PROTOCOLS
 match access-group name INSIDE_TO_OUTSIDE_ACL
 !
 policy-map type inspect INSIDE_TO_OUTSIDE_PMAP
 class type inspect INSIDE_TO_OUTSIDE_CMAP
 inspect
 class class-default
 drop
 !
 ip access-list extended INSIDE_TO_OUTSIDE_ACL
 permit ip any any
 !
 zone security INSIDE
 zone security OUTSIDE
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE_TO_OUTSIDE_PMAP
 !
 interface Ethernet0/0
 ip address 10.1.1.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
```

```
 zone-member security INSIDE
 redundancy rii 100
 redundancy group 1 ip 10.1.1.3 exclusive
 !
 interface Ethernet0/1
 ip address 203.0.113.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 zone-member security OUTSIDE
 redundancy rii 200
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تأكيد أن الأجهزة يمكنها الاتصال ببعضها البعض

للتأكد من أن الأجهزة يمكن أن ترى بعضها البعض، يجب التحقق من أن الحالة التشغيلية لمجموعة تطبيقات التكرار قيد التشغيل. بعد ذلك، تأكد من أن كل جهاز قد أخذ الدور الصحيح، ومن أنه يمكنه رؤية النظير الخاص به في الأدوار الصحيحة الخاصة به. في المثال 3، يكون ZBFW1 نشطا ويكشف عن النظير الخاص به على أنه في وضع الاستعداد. وهذا معكوس على ZBFW2. عندما يظهر كلا الجهازين أيضا أن حالة التشغيل قيد التشغيل، ويتم اكتشاف وجود النظير الخاص بهما، يمكن أن يتصل الموجهان بنجاح عبر إرتباط التحكم.

المثال 3: اكتشاف وجود النظير

```
ZBFW1# show redundancy application group 1
 Group ID:1
 Group Name:ZBFW_HA

 Administrative State: No Shutdown
 Aggregate operational state : Up
 My Role: ACTIVE
 Peer Role: STANDBY
 Peer Presence: Yes
 Peer Comm: Yes
 Peer Progression Started: Yes

 RF Domain: btob-one
 RF state: ACTIVE
 Peer RF state: STANDBY COLD-BULK
 !
ZBFW2# show redundancy application group 1
 Group ID:1
 Group Name:ZBFW_HA

 Administrative State: No Shutdown
 Aggregate operational state : Up
 My Role: STANDBY
 Peer Role: ACTIVE
 Peer Presence: Yes
 Peer Comm: Yes
 Peer Progression Started: Yes

 RF Domain: btob-one
 RF state: STANDBY COLD-BULK
```

```
Peer RF state: ACTIVE
```

يوضح الإخراج في المثال 4 المزيد من الإخراج متعدد المستويات حول واجهة التحكم في الموجهين. يؤكد الإخراج الواجهة المادية المستخدمة لحركة مرور التحكم، كما يؤكد عنوان IP الخاص بالنظير.

المثال 4: النواتج المحببة

```
ZBFW1#  show redundancy application control-interface group 1
The control interface for rg[1] is Ethernet0/2
Interface is Control interface associated with the following protocols: 1
BFD Enabled
:Interface Neighbors
Peer: 10.60.1.2 Standby RGs: 1 BFD handle: 0

ZBFW1# show redundancy application data-interface group 1
The data interface for rg[1] is Ethernet0/2
!
ZBFW2# show redundancy application control-interface group 1
The control interface for rg[1] is Ethernet0/2
Interface is Control interface associated with the following protocols: 1
BFD Enabled
:Interface Neighbors
Peer: 10.60.1.1 Active RGs: 1 BFD handle: 0

ZBFW2# show redundancy application data-interface group 1
The data interface for rg[1] is Ethernet0/2
```

عندما يتم تأسيس الاتصال، يساعدك الأمر في المثال 5 على فهم سبب وجود كل جهاز في دوره الخاص. ZBFW1 نشط لأن له أولوية أعلى من نظيره. ويتكون ZBFW1 من أولوية 200، في حين أن ZBFW2 له أولوية مقدارها 150. يتم إبراز هذا الإخراج باللون الغامق.

المثال 5: حالة الدور والأولوية

```
ZBFW1#  show redundancy application protocol group 1

RG Protocol RG 1
Role: Active
Negotiation: Enabled
Priority: 200
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 10.60.1.2, priority 150, intf Et0/2
:Log counters
role change to active: 1
role change to standby: 0
disable events: rg down state 0, rg shut 0
ctrl intf events: up 1, down 0, admin_down 0
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Active
Protocol ID: 1
Media type: Default
Control Interface: Ethernet0/2
Current Hello timer: 3000
```

```
                Configured Hello timer: 3000, Hold timer: 10000
                 Peer Hello timer: 3000, Peer Hold timer: 10000
                                                        :Stats
Pkts 249, Bytes 15438, HA Seq 0, Seq Number 249, Pkt Loss 0
                                    Authentication not configured
                                        Authentication Failure: 0
                                          Reload Peer: TX 0, RX 0
                                               Resign: TX 0, RX 0
                                 Standby Peer: Present. Hold Timer: 10000
 Pkts 237, Bytes 8058, HA Seq 0, Seq Number 252, Pkt Loss 0

                                                                !
ZBFW2# show redundancy application protocol group 1

                                                  RG Protocol RG 1
                                                 ------------------
                                                      Role: Standby
                                                Negotiation: Enabled
                                                      Priority: 150
                                             Protocol state: Standby-cold
                                                   Ctrl Intf(s) state: Up
   Active Peer: address 10.60.1.1, priority 200, intf Et0/2
                                                  Standby Peer: Local
                                                          :Log counters
                                               role change to active: 0
                                              role change to standby: 1
                                  disable events: rg down state 0, rg shut 0
                                ctrl intf events: up 1, down 0, admin_down 0
                               reload events: local request 0, peer request 0

                                                  RG Media Context for RG 1
                                                 --------------------------
                                                          Ctx State: Standby
                                                              Protocol ID: 1
                                                     Media type: Default
                                           Control Interface: Ethernet0/2
                                                Current Hello timer: 3000
                Configured Hello timer: 3000, Hold timer: 10000
                 Peer Hello timer: 3000, Peer Hold timer: 10000
                                                        :Stats
Pkts 232, Bytes 14384, HA Seq 0, Seq Number 232, Pkt Loss 0
                                    Authentication not configured
                                        Authentication Failure: 0
                                          Reload Peer: TX 0, RX 0
                                               Resign: TX 0, RX 0
                                  Active Peer: Present. Hold Timer: 10000
 Pkts 220, Bytes 7480, HA Seq 0, Seq Number 229, Pkt Loss 0
```

التأكيد الأخير هو التأكد من تعيين معرف مجموعة RII لكل واجهة. إذا قمت بإدخال هذا الأمر على كلا الموجهين، فيمكنك التحقق مرتين للتأكد من أن أزواج الواجهة على الشبكة الفرعية نفسها بين الأجهزة يتم تخصيصها لنفس معرف RII. إن لا يشكل هم يكون مع ال نفسه فريد RII id، توصيل لا يكرر بين الإثنان أداة. راجع المثال 6.

المثال 6: تأكيد تعيين معرف مجموعة RII

```
                                                ZBFW1# show redundancy rii
                                                No. of RIIs in database: 2
                                                Interface RII Id decrement
                                              Ethernet0/1 : 200           0
                                              Ethernet0/0 : 100           0
                                                                          !
```

```
ZBFW2# show redundancy rii
No. of RIIs in database: 2
Interface RII Id decrement
Ethernet0/1 : 200           0
Ethernet0/0 : 100           0
```

التحقق من تكرار الاتصالات بالموجه النظير

في المثال 7، يقوم ZBFW1 بتمرير حركة مرور البيانات لاتصال. تم نسخ الاتصال نسخا متماثلا بنجاح إلى ZBFW2 للجهاز الاحتياطي. لعرض الاتصالات التي تمت معالجتها بواسطة جدار حماية المنطقة، أستخدم الأمر **show policy-firewall session**.

المثال 7: الاتصالات التي تمت معالجتها

```
ZBFW1#show policy-firewall session
Session B2704178 (10.1.1.100:52980)=>(203.0.113.100:23) tcp
                                                SIS_OPEN/TCP_ESTAB
                                    Created 00:00:31, Last heard 00:00:30
                                [Bytes sent (initiator:responder) [37:79
                                    HA State: ACTIVE, RG ID: 1
                                      Established Sessions = 1

ZBFW2#show policy-firewall session
Session B2601288 (10.1.1.100:52980)=>(203.0.113.100:23) tcp
                                                SIS_OPEN/TCP_ESTAB
                                    Created 00:00:51, Last heard never
                                [Bytes sent (initiator:responder) [0:0
                                    HA State: STANDBY, RG ID: 1
                                      Established Sessions = 1
```

الإعلام بنسخ الاتصال المتماثل، لكن لم يتم تحديث وحدات البايت التي تم نقلها. يتم تحديث حالة الاتصال (معلومات TCP) بشكل منتظم من خلال واجهة البيانات لضمان عدم تأثر حركة المرور إذا حدث تجاوز الفشل.

للحصول على مخرجات أكثر دقة، أدخل الأمر **show policy-firewall session-pair <*ZP*>ha**. يوفر مخرجات مماثلة على سبيل المثال 7، ولكنه يسمح للمستخدم بتقييد المخرجات على زوج المناطق المحدد فقط.

تجميع إخراج تصحيح الأخطاء

يبدي هذا قسم ال debug أمر أن ينتج إنتاج ذو صلة إنتاج in order to تحريت هذا سمة.

يمكن أن يكون تمكين تصحيح الأخطاء صعبا جدا على موجه مشغول. لذلك، يجب أن تفهم التأثير قبل تمكينها.

- **حدث RII لمجموعة تطبيقات تصحيح الأخطاء المتكررة**

يتم إستخدام هذا الأمر للتأكد من تطابق الاتصالات مع مجموعة RII الصحيحة ليتم نسخها بشكل صحيح. عندما تصل حركة المرور على ZBFW، يتم التحقق من واجهات المصدر والوجهة لمعرف مجموعة RII. ثم يتم توصيل هذه المعلومات عبر إرتباط البيانات بالنظير. عندما تتم محاذاة مجموعة RII الخاصة بالنظير الاحتياطي مع الوحدات النشطة، يتم إنشاء syslog في المثال 8، ويؤكد معرفات مجموعة RII التي يتم إستخدامها لنسخ الاتصال:

المثال 8: Syslog

```
debug redundancy application group rii event
debug redundancy application group rii error
!
Feb 1 21:13:01.378: [RG-RII-EVENT]: get idb: rii:100*
Feb 1 21:13:01.378: [RG-RII-EVENT]: get idb: rii:200*
```

- **بروتوكول مجموعة تطبيقات تكرار التصحيح الكل**

يتم إستخدام هذا الأمر لتأكيد إمكانية رؤية النظامين لبعضهما البعض. يتم تأكيد عنوان IP النظير في عمليات تصحيح الأخطاء. كما هو موضح في المثال 9، يرى ZBFW1 نظيره في حالة الاستعداد مع عنوان IP **10.60.1.2**. وبصدق العكس على ZBFW2.

المثال 9: تأكيد عناوين IP النظيرة في تصحيح الأخطاء

```
debug redundancy application group protocol all
!
ZBFW1#
,Feb 1 21:35:58.213: RG-PRTCL-MEDIA: RG Media event, rg_id=1, role=Standby*
.addr=10.60.1.2, present=exist, reload=0, intf=Et0/2, priority=150
.Feb 1 21:35:58.213: RG-PRTCL-MEDIA: [RG 1] [Active/Active] set peer_status 0*
Feb 1 21:35:58.213: RG-PRTCL-MEDIA: [RG 1] [Active/Active] priority_event*
.'media: low priority from standby', role_event 'no event'
,Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] select fsm event*
.priority_event=media: low priority from standby, role_event=no event
Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] process FSM event*
.'media: low priority from standby'
Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] no FSM transition*

ZBFW2#
,Feb 1 21:36:02.283: RG-PRTCL-MEDIA: RG Media event, rg_id=1, role=Active*
.addr=10.60.1.1, present=exist, reload=0, intf=Et0/2, priority=200
[Feb 1 21:36:02.283: RG-PRTCL-MEDIA: [RG 1] [Standby/Standby-hot*
.set peer_status 0
Feb 1 21:36:02.283: RG-PRTCL-MEDIA: [RG 1] [Standby/Standby-hot] priority_event*
.'media: high priority from active', role_event 'no event'
Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] select*
.fsm event, priority_event=media: high priority from active, role_event=no event
Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] process*
.'FSM event 'media: high priority from active
Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] no FSM*
transition
```

المشكلات الشائعة

يوضح هذا القسم تفاصيل بعض المشكلات الشائعة التي تمت مواجهتها.

التحكم وتحديد واجهة البيانات

فيما يلي بعض التلميحات لشبكات VLAN الخاصة بالتحكم والبيانات:

- لا تقم بتضمين واجهات التحكم والبيانات في تكوين ZBFW. يتم إستخدامها فقط للتواصل مع بعضها البعض، وبالتالي، لا توجد حاجة لتأمين هذه الواجهات.
- يمكن أن تكون واجهات التحكم والبيانات على نفس الواجهة أو شبكة VLAN. يحافظ هذا على المنافذ على الموجه.

مجموعة أبناء العراق الغائبين

يجب تطبيق مجموعة RII على كل من واجهات LAN و WAN. يجب أن تكون واجهات شبكة LAN على الشبكة الفرعية نفسها، ولكن يمكن أن تكون واجهات WAN على شبكات فرعية منفصلة. إذا كانت هناك مجموعة RII غائبة على واجهة، فإن هذا syslog يحدث في إخراج **حدث RII لمجموعة تطبيقات تصحيح الأخطاء** و**خطأ RII لمجموعة تطبيقات تصحيح الأخطاء المتكررة**:

```
Dec 20 14:35:07.753 EST: FIREWALL*: RG not found for ID 0 :000515
```

تجاوز الفشل التلقائي

من أجل تكوين تجاوز الفشل التلقائي، يجب تكوين ZBFW HA لتعقب كائن إتفاقية مستوى الخدمة (SLA)، وتقليل الأولوية بشكل ديناميكي استنادا إلى حدث SLA هذا. في المثال 10، يتتبع ZBFW HA حالة الارتباط لواجهة **GigabitEthernet0**. إذا انخفضت هذه الواجهة، يتم تقليل الأولوية بحيث يكون جهاز النظير أكثر تفضيلا.

مثال 10: تهيئة تلقائية لتجاوز الأعطال وفقا لمعيار ZBFW HA

```
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 230
control Vlan801 protocol 1
data Vlan801
track 1 decrement 200
!
track 1 interface GigabitEthernet0 line-protocol

redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 180
control Vlan801 protocol 1
data Vlan801
```

وفي بعض الأحيان، لا يقوم ZBFW HA تلقائيا بتجاوز الفشل على الرغم من انخفاض عدد الأحداث ذات الأولوية. وذلك نظرا لعدم تكوين الكلمة الأساسية **preest** ضمن كلا الجهازين. تحتوي الكلمة الأساسية **الحظر** على وظائف مختلفة عن الوظائف المتوفرة في بروتوكول موجه الاستعداد السريع (HSRP) أو ميزة التغلب على أعطال أجهزة الأمان المعدلة (ASA). في ZBFW HA، تسمح الكلمة الأساسية **preest** بحدث تجاوز الفشل إذا تغيرت أولوية الجهاز. وهذا موثق في دليل تكوين الأمان: جدار حماية السياسات المستند إلى المناطق، الإصدار 15.2M&T من Cisco IOS. فيما يلي مقتطف من فصل التوفر العالي لجدار الحماية القائم على المناطق:

"يمكن أن يحدث التحويل إلى الجهاز الاحتياطي في ظل ظروف أخرى. هناك عامل آخر يمكن أن يتسبب في التبديل وهو إعداد الأولوية الذي يمكن تكوينه على كل جهاز. الجهاز صاحب أعلى قيمة أولوية هو الجهاز النشط. إذا حدث خطأ في الجهاز النشط أو في الجهاز الاحتياطي، يتم تقليل أولوية الجهاز بمقدار قابل للتكوين، يعرف باسم الوزن. إذا انخفضت أولوية الجهاز النشط إلى أقل من أولوية الجهاز الاحتياطي، يحدث تبديل ويصبح الجهاز الاحتياطي هو الجهاز

النشط. يمكن تجاوز هذا السلوك الافتراضي عن طريق تعطيل سمة الاستباق لمجموعة التكرار. أنت يستطيع أيضا شكلت كل قارن أن يقلل الأولوية عندما الطبقة 1 دولة من القارن سقطت. تتجاوز الأولوية التي تم تكوينها الأولوية الافتراضية لمجموعة تكرار.

وتشير هذه المخرجات إلى الحالة الصحيحة:

```
ZBFW01#show redundancy application group 1
                                Group ID:1
                            Group Name:ZBFW_HA

                 Administrative State: No Shutdown
                  Aggregate operational state : Up
                               My Role: ACTIVE
                             Peer Role: STANDBY
                          Peer Presence: Yes
                              Peer Comm: Yes
                  Peer Progression Started: Yes

                              RF Domain: btob-one
                                RF state: ACTIVE
                          Peer RF state: STANDBY HOT

ZBFW01#show redundancy application faults group 1
                        :Faults states Group 1 info
                            [Runtime priority: [230
                        .RG Faults RG State: Up
                  Total # of switchovers due to faults: 0
              Total # of down/up state changes due to faults: 0
```

يتم إنشاء هذه السجلات على ZBFW بدون تمكين أي تصحيح أخطاء. يظهر هذا السجل عندما يصبح الجهاز نشطا:

```
Feb  1 21:47:00.579: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from*
                                                              Init to Standby
Feb 1 21:47:09.309: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from Standby*
                                                                 to Active
Feb 1 21:47:19.451: %RG_VP-6-BULK_SYNC_DONE: RG group 1 BULK SYNC to standby*
                                                                 .complete
Feb 1 21:47:19.456: %RG_VP-6-STANDBY_READY: RG group 1 Standby router is in*
                                                              SSO state
```

يظهر هذا السجل عندما يكون الجهاز في وضع الاستعداد:

```
Feb  1 21:47:07.696: %RG_VP-6-BULK_SYNC_DONE: RG group 1 BULK SYNC to standby*
                                                                 .complete
Feb 1 21:47:07.701: %RG_VP-6-STANDBY_READY: RG group 1 Standby router is in*
                                                              SSO state
Feb 1 21:47:09.310: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from Active*
                                                                 to Init
Feb 1 21:47:19.313: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from*
                                                              Init to Standby
```

توجيه لاتناظري

دعم التوجيه غير المتماثل خارجي في دليل دعم التوجيه غير المتماثل.

لتكوين التوجيه غير المتماثل، قم بإضافة الميزات إلى كل من التكوين العام لمجموعة تطبيقات التكرار والتكوين الفرعي للواجهة. من المهم ملاحظة أنه لا يمكن تمكين التوجيه غير المتماثل و RG على نفس الواجهة، لأنه غير مدعوم. وهذا يرجع إلى كيفية عمل التوجيه غير المتماثل. عندما يتم تعيين واجهة للتوجيه غير المتماثل، فلا يمكن أن

تكون جزءا من النسخ المتماثل لاتصال HA في تلك النقطة، لأن التوجيه غير متسق. يشكل RG المسحاج تخديد، لأن RG يعين أن قارن يكون جزء من HA توصيل جواب.

مثال 11: تشكيل التوجيه غير المتماثل

```
redundancy
application redundancy
group 1
asymmetric-routing interface Ethernet0/3

interface Ethernet0/1
redundancy asymmetric-routing enable
```

يجب تطبيق هذا التكوين على كلا الموجهين في زوج HA.

تعد واجهة Ethernet0/3 المدرجة سابقا إرتباطا مخصصا جديدا بين الموجهين. يتم إستخدام هذا الارتباط بشكل حصري لاجتياز حركة مرور موجهة بشكل غير متناسق بين الموجهين. ولهذا السبب ينبغي أن يكون صلة مخصصة مكافئة للواجهة الخارجية.

معلومات ذات صلة

- دليل تكوين الأمان: جدار حماية السياسات القائم على المناطق، الإصدار 15.2M&T من Cisco IOS
- دليل تكوين الأمان عالي التوافر لجدار الحماية المستند إلى المناطق
- Cisco IOS 15.2M&T
- جدار حماية Cisco IOS
- إعلامات حقل منتج الأمان
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).