Configuration et dépannage de la haute disponibilité de ZBFW

Contenu

Introduction

Ce guide fournit la configuration de base pour la haute disponibilité du pare-feu de zone (HA) pour une configuration active/de secours, ainsi que des commandes de dépannage et des problèmes courants observés avec la fonctionnalité.

Cisco IOS® Zone-Based Firewall (ZBFW) prend en charge la haute disponibilité afin que deux routeurs Cisco IOS puissent être configurés dans une configuration active/en veille ou active/active. Cela permet la redondance afin d'éviter un point de défaillance unique.

Conditions préalables

Conditions requises

Vous devez disposer d'une version ultérieure à la version 15.2(3)T du logiciel Cisco IOS.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

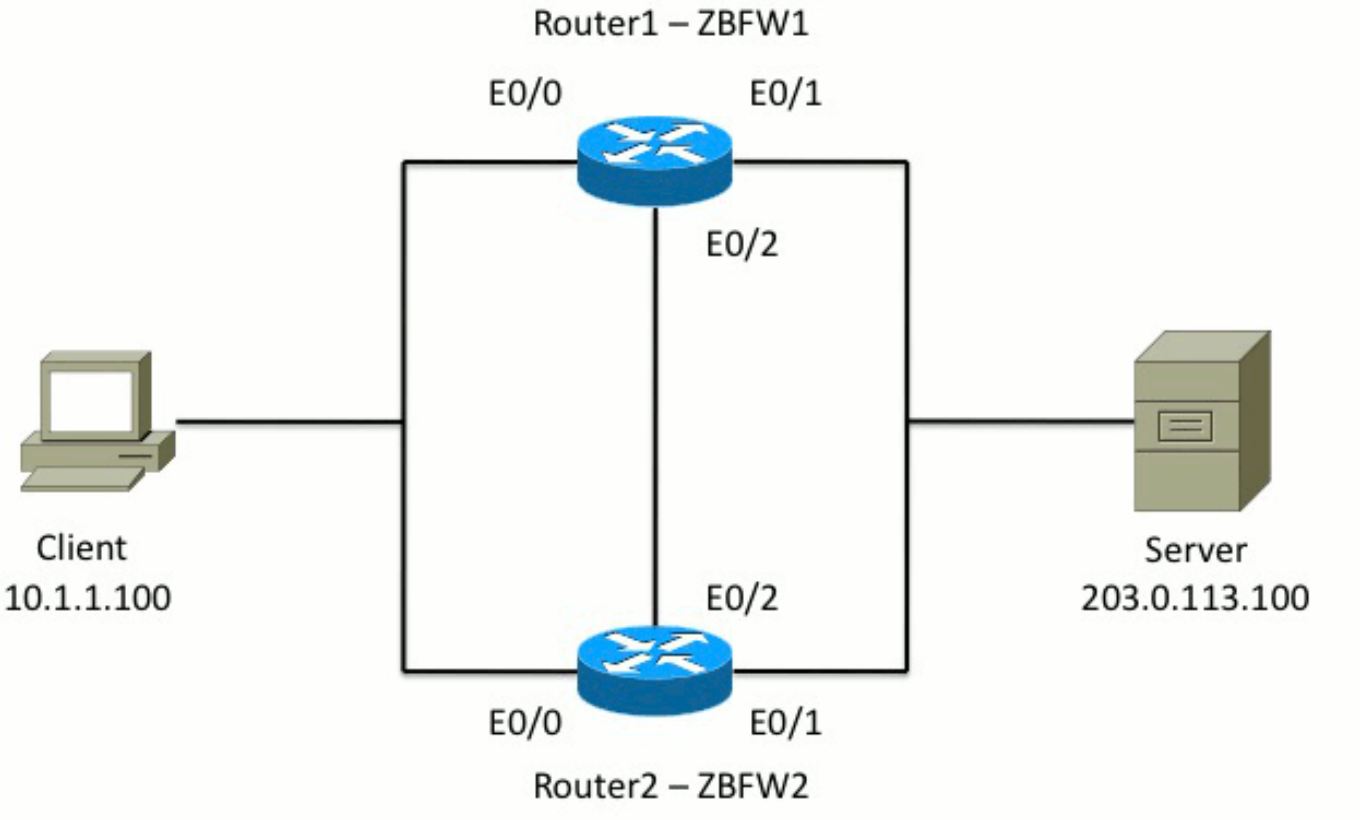
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration

Ce schéma présente la topologie utilisée dans les exemples de configuration.



Dans la configuration illustrée dans l'exemple 1, ZBFW est configuré afin d'inspecter le trafic TCP, UDP et ICMP (Internet Control Message Protocol) de l'intérieur vers l'extérieur. La configuration affichée en gras configure la fonction HA. Dans les routeurs Cisco IOS, la HA est configurée via la commande **redundancy** subconfig. Afin de configurer la redondance, la première étape consiste à activer la redondance dans la carte des paramètres d'inspection globale.

Après avoir activé la redondance, entrez la sous-configuration **de redondance des applications** et sélectionnez les interfaces utilisées pour le **contrôle** et **les données**. L'interface de contrôle est utilisée afin d'échanger des informations sur l'état de chaque routeur. L'interface de données est utilisée afin d'échanger des informations sur les connexions qui doivent être répliquées.

Dans l'exemple 2, la commande **priority** est également définie pour faire du routeur 1 l'unité active de la paire si les routeurs 1 et 2 sont tous deux opérationnels. La commande **preempt** (également abordée dans ce document) est utilisée afin de s'assurer que l'échec se produit une fois la priorité modifiée.

La dernière étape consiste à attribuer l'**identificateur d'interface redondante (RII)** et le **groupe de redondance (RG)** à chaque interface. Le numéro de groupe **RII** doit être unique pour chaque interface, mais il doit correspondre entre les périphériques pour les interfaces du même sous-réseau. Le RII est utilisé uniquement pour le processus de synchronisation en bloc lorsque les deux routeurs synchronisent la configuration. Voici comment les deux routeurs synchronisent les interfaces redondantes. Le **RG** est utilisé afin d'indiquer que les connexions via cette interface sont répliquées dans la table de connexions HA.

Dans l'exemple 2, la commande **redundancy group 1** est utilisée afin de créer une adresse IP virtuelle (VIP) sur l'interface interne. Cela garantit la haute disponibilité, car tous les utilisateurs internes communiquent uniquement avec le VIP, pour lequel l'unité active traite.

L'interface externe n'a pas de configuration RG, car il s'agit de l'interface WAN. L'interface externe des routeurs 1 et 2 n'appartient pas au même fournisseur d'accès à Internet (FAI). Sur l'interface externe, un protocole de routage dynamique est requis pour s'assurer que le trafic passe au périphérique approprié.

Exemple 1 : Extrait de configuration du routeur 1 (nom d'hôte 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
```

Exemple 2 : Extrait de configuration du routeur 2 (nom d'hôte 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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Confirmer que les périphériques peuvent communiquer entre eux

Afin de confirmer que les périphériques peuvent se voir, vous devez vérifier que l'état opérationnel du groupe d'applications de redondance est actif. Ensuite, assurez-vous que chaque périphérique a joué le rôle correct et peut voir son homologue dans ses rôles corrects. Dans l'exemple 3, ZBFW1 est actif et détecte son homologue en veille. Ceci est inversé sur ZBFW2. Lorsque les deux périphériques indiquent également que l'état opérationnel est actif et que leur présence homologue est détectée, les deux routeurs peuvent communiquer correctement via la liaison de contrôle.

Exemple 3 : Détection de présence homologue

```
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
```

Le résultat de l'exemple 4 montre une sortie plus granulaire sur l'interface de contrôle des deux routeurs. Le résultat confirme l'interface physique utilisée pour contrôler le trafic, et il confirme également l'adresse IP de l'homologue.

Exemple 4 : Sortie granulaire

```
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
```

Lorsque la communication est établie, la commande de l'exemple 5 vous aide à comprendre pourquoi chaque périphérique joue un rôle particulier. ZBFW1 est actif car sa priorité est supérieure à celle de son homologue. ZBFW1 a une priorité de **200**, tandis que ZBFW2 a une priorité de **150**. Ce résultat est mis en surbrillance en gras.

Exemple 5 : Statut et priorité du rôle

```
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
```

La dernière confirmation est de s'assurer que l'ID de groupe RII est attribué à chaque interface. Si

vous entrez cette commande sur les deux routeurs, ils effectuent une double vérification afin de s'assurer que les paires d'interface sur le même sous-réseau entre les périphériques se voient attribuer le même ID RII. Si elles ne sont pas configurées avec le même ID RII unique, les connexions ne se répliquent pas entre les deux périphériques. Voir l'exemple 6.

Exemple 6 : Confirmer l'attribution de l'ID de groupe 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
```

Vérifier que les connexions se répliquent sur le routeur homologue

Dans l'exemple 7, ZBFW1 transmet activement le trafic pour une connexion. La connexion est correctement répliquée sur le périphérique de secours ZBFW2. Afin d'afficher les connexions traitées par le pare-feu de zone, utilisez la commande **show policy-firewall session**.

Exemple 7 : Connexions traitées

```
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
```

Notez que la connexion se reproduit, mais que les octets transférés ne sont pas mis à jour. L'état de la connexion (informations TCP) est mis à jour régulièrement via l'interface de données afin de s'assurer que le trafic n'est pas affecté en cas d'événement de basculement.

Pour obtenir des informations plus précises, entrez la commande **show policy-firewall session zone-pair *<ZP>* ha**. Il fournit un résultat similaire à celui de l'exemple 7, mais il permet à l'utilisateur de limiter le résultat à la seule zone-paire spécifiée.

Collecter la sortie de débogage

Cette section présente les commandes de débogage qui produisent les résultats pertinents afin de dépanner cette fonctionnalité.

L'activation des débogages peut être très difficile sur un routeur occupé. Par conséquent, vous devez comprendre l'impact avant de les activer.

- **debug redundancy application group rii event**

  Cette commande est utilisée afin de s'assurer que les connexions correspondent au groupe RII correct à répliquer correctement. Lorsque le trafic arrive sur le ZBFW, les interfaces source et de destination sont vérifiées pour un ID de groupe RII. Ces informations sont ensuite communiquées à l'homologue via la liaison de données. Lorsque le groupe RII de l'homologue de secours s'aligne sur les unités actives, le syslog dans l'exemple 8 est généré et confirme les ID de groupe RII utilisés afin de répliquer la connexion :

  Exemple 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
```

- **debug redundancy application group protocol all**

  Cette commande est utilisée afin de confirmer que les deux homologues peuvent se voir. L'adresse IP de l'homologue est confirmée dans les débogages. Comme le montre l'exemple 9, ZBFW1 voit son homologue en veille avec l'adresse IP **10.60.1.2**. L'inverse est vrai pour ZBFW2.

  Exemple 9 : Confirmer les adresses IP des homologues dans les débogages

```
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
```

Problèmes courants

Cette section décrit certains problèmes courants rencontrés.

Sélection de l'interface de contrôle et de données

Voici quelques conseils pour les VLAN de contrôle et de données :

- N'incluez pas les interfaces de contrôle et de données dans la configuration ZBFW. Ils ne sont utilisés que pour communiquer entre eux ; par conséquent, il n'est pas nécessaire de sécuriser ces interfaces.
- Les interfaces de contrôle et de données peuvent se trouver sur la même interface ou sur le même VLAN. Cela préserve les ports du routeur.

Groupe RII absent

Le groupe RII doit être appliqué aux interfaces LAN et WAN. Les interfaces LAN doivent se trouver sur le même sous-réseau, mais les interfaces WAN peuvent se trouver sur des sous-réseaux distincts. Si un groupe RII est absent sur une interface, ce syslog se produit dans la sortie de l'**événement rii du groupe d'applications de redondance de débogage** et de l'**erreur rii du groupe d'applications de redondance de débogage** :

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

Basculement automatique

Pour configurer le basculement automatique, la HA ZBFW doit être configurée afin de suivre un objet SLA (Service Level Agreement) et de diminuer dynamiquement la priorité en fonction de cet événement SLA. Dans l'exemple 10, ZBFW HA suit l'état de la liaison de l'interface **GigabitEthernet0**. Si cette interface tombe en panne, la priorité est réduite de sorte que le périphérique homologue soit plus favori.

Exemple 10 : Configuration automatique du basculement 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
```

Parfois, la HA ZBFW ne bascule pas automatiquement même s'il y a un événement de priorité réduite. Ceci est dû au fait que le mot clé **preempt** n'est pas configuré sous les deux périphériques. Le mot clé **preempt** a des fonctionnalités différentes de celles du basculement du protocole HSRP (Hot Standby Router Protocol) ou ASA (Adaptive Security Appliance). Dans ZBFW HA, le mot clé **preempt** permet à un événement de basculement de se produire si la priorité du périphérique change. Ceci est documenté dans le Guide de configuration de la sécurité : Pare-feu de stratégie basé sur les zones, Cisco IOS version 15.2M&T. Voici un extrait du chapitre Zone-Based Policy Firewall High Availability :

«Un basculement vers le périphérique de secours peut se produire dans d'autres circonstances. Un autre facteur qui peut provoquer un basculement est un paramètre de priorité qui peut être configuré sur chaque périphérique. Le périphérique dont la priorité est la plus élevée est le périphérique actif. Si une erreur survient sur le périphérique actif ou en veille, la priorité du périphérique est décrémentée par une quantité configurable, appelée poids. Si la priorité du périphérique actif est inférieure à la priorité du périphérique de secours, une commutation se produit et le périphérique de secours devient le périphérique actif. Ce comportement par défaut peut être remplacé en désactivant l'attribut de préemption pour le groupe de redondance. Vous pouvez également configurer chaque interface pour diminuer la priorité lorsque l'état de couche 1 de l'interface tombe en panne. La priorité configurée remplace la priorité par défaut d'un groupe de redondance. »

Ces résultats indiquent l'état approprié :

```
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
```

Ces journaux sont générés sur le ZBFW sans aucun débogage activé. Ce journal indique quand le périphérique devient actif :

```
*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
```

Ce journal indique quand le périphérique est en veille :

```
*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
```

Routage asymétrique

La prise en charge du routage asymétrique est exclue dans le guide Asymmetric Routing Support.

Afin de configurer le routage asymétrique, ajoutez les fonctionnalités à la configuration globale du groupe d'applications de redondance et à la sous-configuration de l'interface. Il est important de noter que le routage asymétrique et un RG ne peuvent pas être activés sur la même interface, car il n'est pas pris en charge. Ceci est dû au fonctionnement du routage asymétrique. Lorsqu'une interface est désignée pour le routage asymétrique, elle ne peut pas faire partie de la réplication de connexion HA à ce stade, car le routage est incohérent. La configuration d'un routeur désigné (RG) confond le routeur, car un routeur désigné (RG) spécifie qu'une interface fait partie de la réplication de connexion haute disponibilité.

Exemple 11 : Configuration du routage asymétrique

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

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

Cette configuration doit être appliquée aux deux routeurs de la paire HA.

L'interface **Ethernet0/3** répertoriée précédemment est une nouvelle liaison dédiée entre les deux routeurs. Cette liaison est utilisée exclusivement afin de transmettre le trafic asymétrique entre les deux routeurs. C'est pourquoi il doit s'agir d'une liaison dédiée équivalente à l'interface externe.

Informations connexes

- Guide de configuration de la sécurité : Pare-feu de stratégie basé sur les zones, Cisco IOS version 15.2M&T
- Guide de configuration de la sécurité haute disponibilité du pare-feu de stratégie basé sur les zones
- Cisco IOS 15.2M&T
- Cisco IOS Firewall
- Avis de champs relatifs aux produits de sécurité
- Support et documentation techniques - Cisco Systems