# Configuration facilement disponible et dépannage ZBFW de TechNote

## Contenu



## Introduction

Ce guide fournit à la configuration de base pour la Haute disponibilité de Pare-feu de zone (ha) pour installation active/de réserve, aussi bien que des commandes de dépannage, et des problèmes courants vus la configuration.

Le Pare-feu basé sur zone de Cisco IOS® (ZBFW) prend en charge l'ha de sorte que deux routeurs Cisco IOS puissent être configurés dans un actif/standby ou installation active/active. Ceci permet à la Redondance afin d'empêcher un point de défaillance unique.

# Conditions préalables

## Conditions requises

Vous devez avoir une release plus tard que le logiciel Release15.2(3)T de Cisco IOS.

## Composants utilisés

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

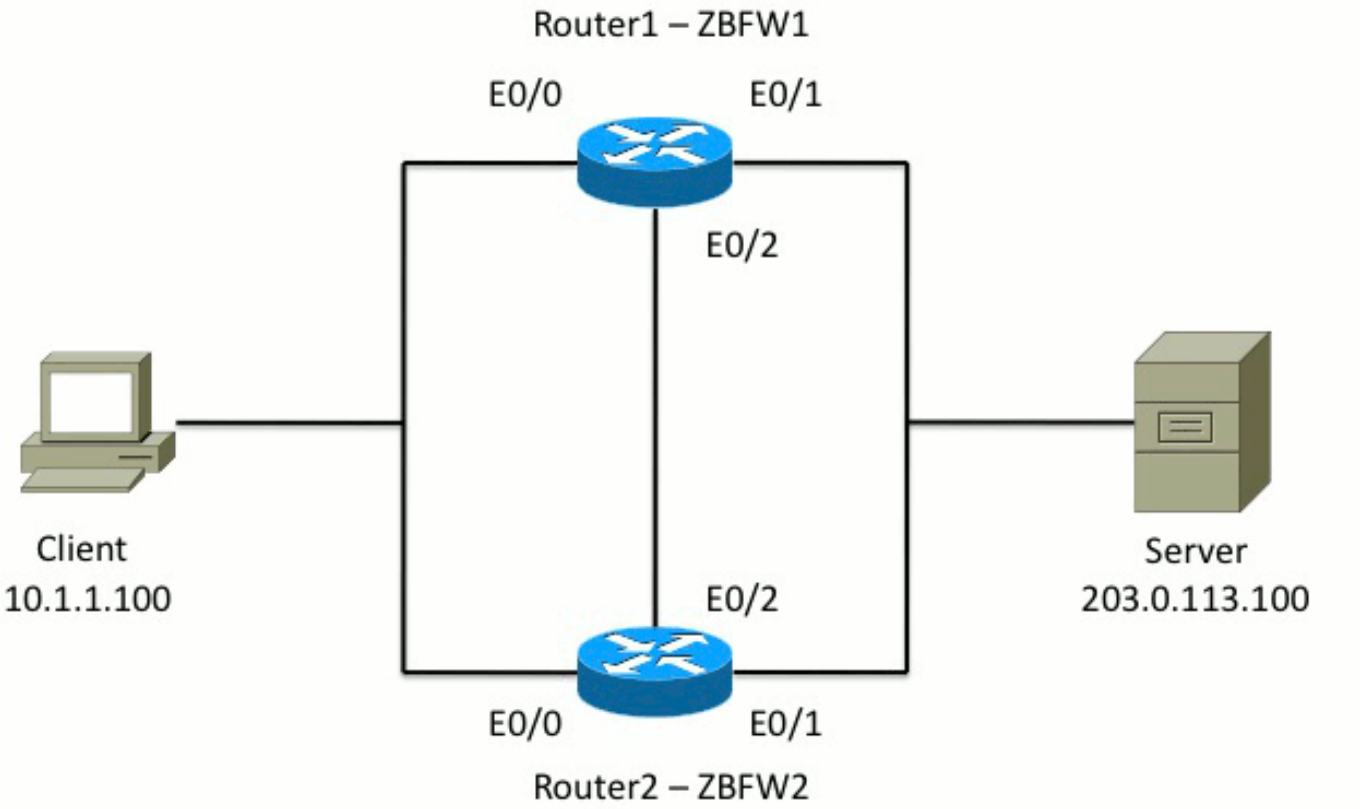
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

# Conventions

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

# Configurez

Ce diagramme affiche la topologie utilisée dans les exemples de configuration.




En configuration illustrée dans l'exemple 1, ZBFW est configuré afin d'examiner le TCP, l'UDP, et le trafic de Protocole ICMP (Internet Control Message Protocol) de l'intérieur à l'extérieur. La configuration illustrée en gras a installé la caractéristique ha. Dans des routeurs Cisco IOS, l'ha est configuré par l'intermédiaire de la commande de subconfig de **Redondance**. Afin de configurer la Redondance, la première étape est d'activer la Redondance dans la carte globale de paramètre d'inspection.

Après que vous activiez la Redondance, écrivez le subconfig de **Redondance d'application**, et sélectionnez les interfaces qui sont utilisées pour le **contrôle** et les **données**. L'interface de contrôle est utilisée afin de permuter des informations sur l'état de chaque routeur. L'interface de données est utilisée afin de permuter des informations sur les connexions qui devraient être répliquées.

Dans l'exemple 2, la commande **prioritaire** est également placée de faire à routeur 1 l'unité d'active dans les paires si le routeur 1 et le Router2 sont opérationnels. La commande d'**acquisition** (également discutée plus loin dans ce document) est utilisée afin de s'assurer que la panne se produit une fois les modifications prioritaires.

La dernière étape est d'assigner l'**identifiant d'interface redondant (RII)** et le **redundancy group (RG) à** chaque interface. Le nombre de groupe **RII** doit être seul pour chaque interface, mais il doit s'assortir à travers des périphériques pour des interfaces dans le même sous-réseau. Le RII est seulement utilisé pour le processus en vrac de sync quand les deux Routeurs synchronisent la configuration. C'est comment les deux Routeurs synchronisent les interfaces redondantes. **Le RG** est utilisé afin d'indiquer que des connexions par cette interface sont répliquées dans la table de connexion ha.

Dans l'exemple 2, la commande du **redundancy group 1** est utilisée afin de créer une adresse virtuelle IP (VIP) sur l'interface interne. Ceci assure l'ha, parce que tous les utilisateurs internes communiquent seulement avec le VIP, pour lequel l'unité d'active traite.

L'interface extérieure n'a aucune configuration RG parce que c'est l'interface WAN. L'interface extérieure du routeur 1 et du Router2 n'appartiennent pas au même fournisseur de services Internet (ISP). Sur l'interface extérieure, un protocole de routage dynamique est exigé afin de s'assurer que le trafic passe au périphérique correct.

## Exemple 1 : Extrait de configuration du routeur 1 (adresse Internet 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 de Router2 (adresse Internet 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
```

# Dépannez

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

## Confirmez que les périphériques peuvent communiquer les uns avec les autres

Afin de confirmer que les périphériques peuvent se voir, vous devez vérifier que l'état opérationnel du groupe d'applications de Redondance est en hausse. Puis, assurez-vous que chaque périphérique a joué le rôle correct, et pouvez voir son pair dans ses rôles corrects. Dans l'exemple 3, ZBFW1 est en activité et détecte son pair comme standby. Ceci est renversé sur ZBFW2.

Quand les deux périphériques prouvent également que l'état opérationnel est en hausse, et leur présence de pair est détectée, les deux Routeurs peuvent avec succès communiquer à travers le lien de contrôle.

### Exemple 3 : Détection de présence de pair

```
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
```

La sortie dans l'exemple 4 affiche une sortie plus granulaire au sujet de l'interface de contrôle des deux Routeurs. La sortie confirme l'interface physique utilisée pour le trafic de contrôle, et elle confirme également l'adresse IP du pair.

### 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
```

Quand la transmission est établie, la commande dans l'exemple 5 vous aide à comprendre pourquoi chaque périphérique est dans son rôle particulier. ZBFW1 est en activité parce qu'il a une haute priorité que son pair. ZBFW1 a une priorité de 200, alors que ZBFW2 a une priorité de 150. Cette sortie est mise en valeur en gras.

## Exemple 5 : État et priorité de 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'identification groupe RII est assignée à chaque interface. Si vous sélectionnez cette commande sur les deux Routeurs, ils revérifient afin de s'assurer que les paires d'interface sur le même sous-réseau entre les périphériques sont assignées le même ID RII. S'ils ne sont pas configurés avec le même seul ID RII, les connexions ne répliquent pas entre les deux périphériques. Voir l'exemple 6.

### Exemple 6 : Confirmez l'identification groupe RII est assigné

```
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
```

## Vérifiez que réplique de connexions au routeur de pair

Dans l'exemple 7, activement les passages ZBFW1 trafiquent pour une connexion. La connexion est avec succès répliquée vers le périphérique de réserve ZBFW2. Afin de visualiser les connexions traitées par le Pare-feu de zone, utilisez la commande de **session de stratégie-Pare-feu d'exposition**.

### 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 les répliques de connexion, mais les octets transférés ne sont pas mis à jour. L'état de connexion (les informations de TCP) est mis à jour régulièrement par l'interface de données afin de s'assurer que le trafic n'est pas affecté si un événement de Basculement se produit.

Pour une sortie plus granulaire, sélectionnez la commande du **zone-paire *<ZP>* ha de session de stratégie-Pare-feu d'exposition**. Il fournit la sortie semblable comme exemple 7, mais il permet à l'utilisateur de limiter la sortie seulement au zone-paire spécifié.

## Sortie de débogage de rassemblement

Cette section affiche les commandes de débogage qui produisent la sortie appropriée afin de dépanner cette caractéristique.

L'activation de met au point peut être très laborieuse sur un routeur saturé. Par conséquent, vous devriez comprendre l'incidence avant que vous les activiez.

- **événement de rii de groupe d'applications de debug redundancy**

  Cette commande est utilisée afin de s'assurer la correspondance de connexions le groupe correct RII à répliquer correctement. Quand le trafic arrive sur le ZBFW, la source et les interfaces de destination sont vérifiées une identification groupe RII. Ces informations sont alors communiquées à travers la liaison de données au pair. Quand le groupe RII du pair de réserve aligne avec les unités d'active, alors le Syslog dans l'exemple 8 est généré, et confirme les identifications groupe RII qui sont utilisées 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
  ```

- **protocole tout de groupe d'applications de debug redundancy**

  Cette commande est utilisée afin de confirmer que les deux pairs peuvent se voir. Le pair que l'adresse IP est confirmée dans met au point. Comme vu dans l'exemple 9, ZBFW1 voit son pair dans l'état de réserve avec l'adresse IP **10.60.1.2**. L'inverse est vrai pour ZBFW2.

  **Exemple 9 : Confirmez le pair IPS dans les debugs**

  ```
  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 détaille quelques problèmes courants qui sont produits.

## Contrôle et sélection d'interface de données

Voici quelques conseils pour le contrôle et les données VLAN :

- N'incluez pas les interfaces de contrôle et de données dans la configuration ZBFW. Ils sont seulement utilisés afin de communiquer les uns avec les autres ; donc, il n'y a aucun besoin de sécuriser ces interfaces.
- Les interfaces de contrôle et de données peuvent être sur la même interface ou VLAN. Ceci préserve des ports sur le routeur.

## Groupe absent RII

Le groupe RII doit être appliqué sur les les deux les interfaces de LAN et WAN. Les interfaces de RÉSEAU LOCAL doivent être sur le même sous-réseau, mais les interfaces WAN peuvent être sur des sous-réseaux distincts. S'il y a un groupe RII absent sur une interface, ce Syslog se produit dans la sortie de l'**erreur de rii d'événement de rii de groupe d'applications de debug redundancy** et de **groupe d'applications de debug redundancy** :

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

## Basculement automatique

Afin de configurer le Basculement automatique, le ZBFW ha doit être configuré afin de dépister un objet d'accord de niveau de service (SLA), et diminue dynamiquement la priorité basée sur cet

événement de SLA. Dans l'exemple 10, ZBFW ha dépiste le statut de lien de l'interface **GigabitEthernet0**. Si cette interface descend, la priorité est réduite de sorte que le périphérique de pair soit plus favorisé.

### Exemple 10 : Configuration automatique de 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 le ZBFW ha ne fait pas automatiquement Basculement quoiqu'il y ait un événement diminué prioritaire. C'est parce que le mot clé d'**acquisition** n'est pas configuré sous les deux périphériques. Le mot clé d'**acquisition** a la fonctionnalité différente que dans le Basculement de Protocole HSRP (Hot Standby Router Protocol) ou d'appliance de sécurité adaptable (ASA). Dans ZBFW ha, le mot clé d'**acquisition** permet à un événement de Basculement pour se produire si la priorité du périphérique change. Ceci est documenté du guide de configuration de sécurité : Pare-feu basé sur zone de stratégie, version de Cisco IOS 15.2M&T. Voici un extrait du chapitre facilement disponible de Pare-feu basé sur zone de stratégie :

« Un basculement au périphérique de réserve peut se produire sous d'autres circonstances. Un autre facteur qui peut entraîner un basculement est une configuration de la priorité qui peut être configurée sur chaque périphérique. Le périphérique avec la valeur la plus prioritaire soit le périphérique actif. Si un défaut se produit sur le périphérique actif ou de réserve, la priorité du périphérique est décrémentée par une quantité configurable, connue sous le nom de poids. Si la priorité du périphérique actif tombe au-dessous de la priorité du périphérique de réserve, un basculement se produit et le périphérique de réserve devient le périphérique actif. Ce comportement par défaut peut être ignoré en désactivant l'attribut de préemption pour le redundancy group. Vous pouvez également configurer chaque interface pour diminuer la priorité quand l'état de la couche 1 de l'interface descend. La priorité qui est configurée ignore la priorité par défaut d'un redundancy group. »

Ces sorties 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 logs sont générés sur le ZBFW sans rien met au point activé. Ce log affiche 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 log affiche quand le périphérique va en état d'alerte :

```
*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

Le support asymétrique de routage outined du guide asymétrique de support de routage.

Afin de configurer le routage asymétrique, ajoutez les caractéristiques à la configuration globale de groupe d'applications de Redondance et à la sous-titre-configuration d'interface. Il est important de noter ce routage asymétrique et un RG ne peut pas être activé sur la même interface, parce qu'il n'est pas pris en charge. C'est dû à la façon dont le routage asymétrique fonctionne. Quand une interface est indiquée pour le routage asymétrique, ce ne peut pas faire partie de réplication de connexion ha à ce moment là, parce que le routage est contradictoire. Configurer un RG confond le routeur, parce qu'un RG spécifie qu'une interface fait partie de réplication de connexion ha.

### Exemple 11 : Configuration asymétrique de routage

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

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

Cette configuration doit être appliquée sur les deux Routeurs dans les paires ha.

L'interface **Ethernet0/3** répertoriée précédemment est une nouvelle liaison dédiée entre les deux Routeurs. Ce lien est utilisé exclusivement afin de passer le trafic asymétrique-conduit entre les deux Routeurs. C'est pourquoi ce devrait être une liaison dédiée équivalente à l'interface d'externe-revêtement.

## Informations connexes

- Guide de configuration de sécurité : Pare-feu basé sur zone de stratégie, version de Cisco IOS 15.2M&T
- Guide de configuration de sécurité facilement disponible de Pare-feu basé sur zone de stratégie
- Cisco IOS 15.2M&T
- Cisco IOS Firewall
- Notes de terrain relatives aux produits de sécurité
- Support et documentation techniques - Cisco Systems