Configuração de alta disponibilidade e pesquisa de defeitos ZBFW de TechNote

Índice

Introdução

Este guia fornece a configuração básica para a Alta disponibilidade do Firewall da zona (HA) para instalação ativa/à espera, assim como comandos de Troubleshooting, e problemas comuns considerados a característica.

O ® do Cisco IOS Zona-baseou os apoios HA do Firewall (ZBFW) de modo que dois Roteadores do Cisco IOS pudessem ser configurados instalação ativa/à espera ou ativa/ativa. Isto permite que a Redundância a fim impedir um ponto de falha único.

Pré-requisitos

Requisitos

Você deve ter uma liberação mais tarde do que o Cisco IOS Software Release15.2(3)T.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

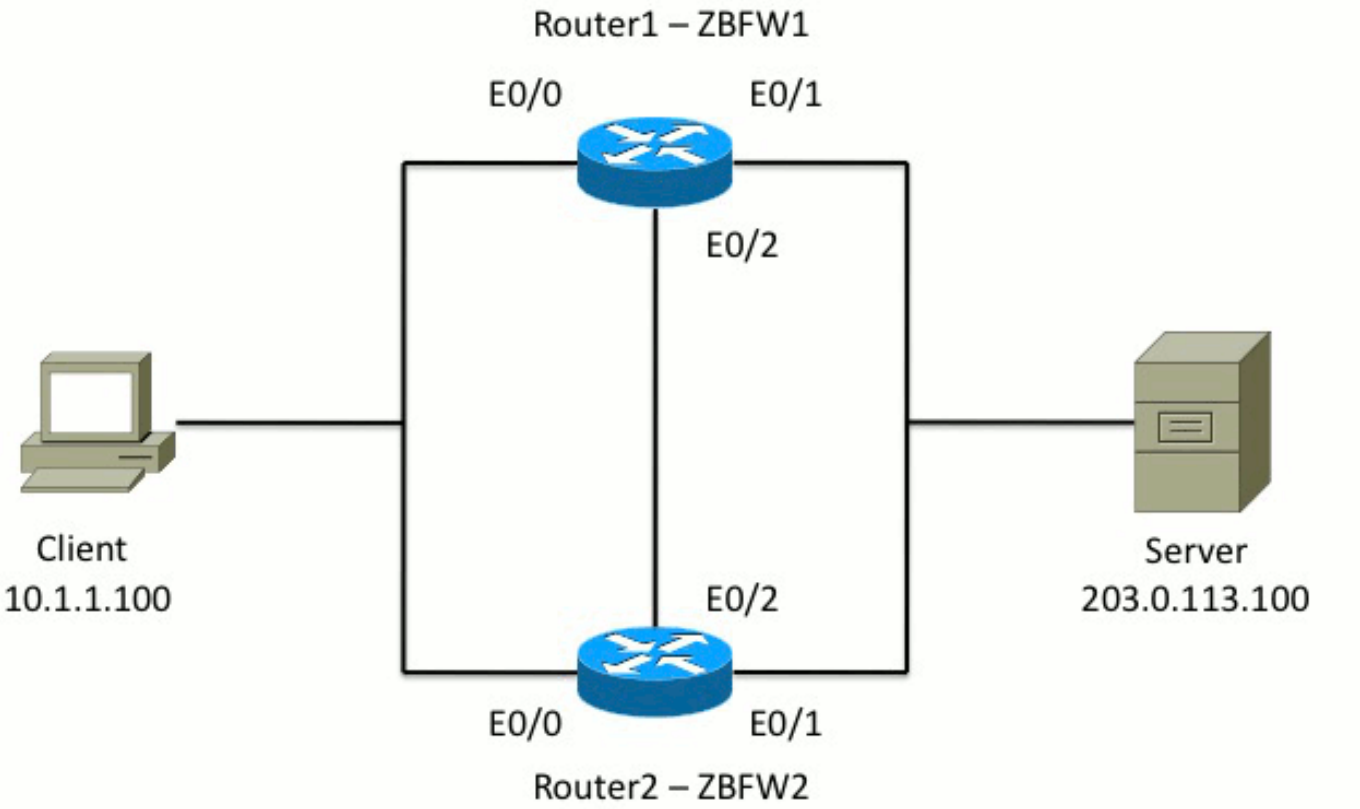
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Este diagrama mostra a topologia usada nos exemplos de configuração.



Na configuração mostrada no exemplo 1, ZBFW é configurado a fim inspecionar do interior o TCP, o UDP, e o tráfego do Internet Control Message Protocol (ICMP) à parte externa. A configuração mostrada em grupos corajosos - acima da característica HA. No Roteadores do Cisco IOS, o HA é configurado através do comando do subconfig da **Redundância**. A fim configurar a Redundância, a primeira etapa é permitir a Redundância no mapa global do parâmetro de inspeção.

Depois que você permite a Redundância, incorpore o subconfig da **Redundância do aplicativo**, e selecione as relações que são usadas para o **controle** e os **dados**. A interface de controle é usada a fim trocar a informação sobre o estado de cada roteador. A interface de dados é usada a fim trocar a informação sobre as conexões que devem ser replicated.

No exemplo 2, o **comando priority** está igualmente feito a roteador1 a unidade ativa nos pares se o roteador1 e o roteador2 são operacionais. O comando **cancelar** (igualmente discutido mais neste documento) é usado a fim assegurar-se de que a falha ocorra uma vez as mudanças da prioridade.

A etapa final é atribuir o **identificador da interface redundante (RII)** e o **grupo de redundância (RG) a** cada relação. O número do grupo **RII** tem que ser original para cada relação, mas deve combinar através dos dispositivos para relações na mesma sub-rede. O RII está usado somente para o processo maioria da sincronização quando os dois Roteadores sincronizam a configuração. Isto é como os dois Roteadores sincronizam interfaces redundantes. **O RG** é usado a fim indicar que as conexões através dessa relação replicated na tabela de conexão HA.

No exemplo 2, o **comando 1 do grupo de redundância** é usado a fim criar um endereço do IP virtual (VIP) na interface interna. Isto assegura o HA, porque todos os usuários internos se comunicam somente com o VIP, para que os processos de unidade ativa.

A interface externa não tem nenhuma configuração RG porque esta é a interface WAN. A interface externa de ambo o roteador1 e o roteador2 não pertencem ao mesmo provedor de

serviço do Internet (ISP). Na interface externa, um protocolo de roteamento dinâmico é exigido a fim assegurar-se de que o tráfego passe ao dispositivo correto.

Exemplo 1: Snippet de configuração do roteador1 (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
```

Exemplo 2: Snippet de configuração do roteador2 (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
```

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Confirme que os dispositivos podem se comunicar um com o otro

A fim confirmar que os dispositivos podem se ver, você deve verificar que o estado operacional do grupo de aplicativo da Redundância está acima. Então, assegure-se de que cada dispositivo tome o papel correto, e possa-se ver seu par em seus papéis corretos. No exemplo 3, ZBFW1 é ativo e detecta seu par como o apoio. Isto é invertido em ZBFW2. Quando ambos os dispositivos

igualmente mostram que o estado operacional está acima, e sua presença do par está detectada, os dois Roteadores podem com sucesso comunicar-se através do link de controle.

Exemplo 3: Detecção da presença do par

```
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
```

A saída na saída mais granulada das mostras do exemplo 4 sobre a interface de controle dos dois Roteadores. A saída confirma a interface física usada para o tráfego de controle, e igualmente confirma o endereço IP de Um ou Mais Servidores Cisco ICM NT do par.

Exemplo 4: Saída granulada

```
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
```

Quando a comunicação é estabelecida, o comando no exemplo 5 ajuda-o a compreender porque cada dispositivo está em seu papel particular. ZBFW1 é ativo porque tem uma prioridade mais alta do que seu par. ZBFW1 tem uma prioridade de **200**, quando ZBFW2 tiver uma prioridade de **150**. Esta saída é destacada em corajoso.

Exemplo 5: Estado e prioridade do papel

```
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
```

A última confirmação é assegurar-se de que o ID de grupo RII esteja atribuído a cada relação. Se você incorpora este comando em ambo o Roteadores, verificam novamente a fim assegurar-se de que os pares da relação na mesma sub-rede entre dispositivos estejam atribuídos o mesmo RII ID. Se não são configurados com o mesmo RII original ID, as conexões não replicate entre os dois dispositivos. Veja o exemplo 6.

Exemplo 6: Confirme o ID de grupo RII é atribuído

```
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
```

Verifique que Replicate das conexões ao roteador de peer

No exemplo 7, ZBFW1 passa ativamente o tráfego para uma conexão. A conexão replicated com sucesso ao dispositivo à espera ZBFW2. A fim ver as conexões processadas pelo Firewall da zona, use o **comando session do política-Firewall da mostra**.

Exemplo 7: Conexões processadas

```
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
```

Observe que os replicates da conexão, mas os bytes transferidos não estão atualizados. O estado de conexão (informação TCP) é atualizado regularmente através da interface de dados a fim assegurar-se de que o tráfego não seja afetado se um evento do Failover ocorre.

Para uma saída mais granulada, incorpore o comando dos zona-**pares *<ZP>* ha da sessão do política-Firewall da mostra**. Fornece a saída similar como o exemplo 7, mas permite que o usuário restrinja a saída somente aos zona-pares especificados.

Resultado do debug do recolhimento

Esta seção mostra os comandos debug que produzem a saída relevante a fim pesquisar defeitos esta característica.

A habilitação de debuga pode ser muito árdua em um roteador ocupado. Consequentemente, você deve compreender o impacto antes que você os permita.

- **debugar o evento do rii do grupo de aplicativo da Redundância**

  Este comando é usado a fim certificar-se do fósforo das conexões o grupo correto RII a ser replicated corretamente. Quando o tráfego chega no ZBFW, a fonte e as interfaces de destino estão verificadas para ver se há um ID de grupo RII. Esta informação é comunicada então através do link de dados ao par. Quando o grupo RII do par à espera alinha com as unidades ativa, a seguir o Syslog no exemplo 8 está gerado, e confirma os ID de grupo RII que são usados a fim replicate a conexão:

  Exemplo 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
  ```

- **debugar o protocolo todo do grupo de aplicativo da Redundância**

  Este comando é usado a fim confirmar que os dois pares podem se ver. O endereço IP do peer é confirmado no debuga. Como visto no exemplo 9, ZBFW1 vê seu par no estado à espera com endereço IP 10.60.1.2. O reverso é verdadeiro para ZBFW2.

  Exemplo 9: Confirme o par que o IPs debuga dentro

  ```
  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
```

Problemas comuns

Esta seção detalha alguns problemas comuns que são encontrados.

Controle e seleção da interface de dados

Estão aqui algumas pontas para o controle e os VLAN de dados:

- Não inclua o controle e as interfaces de dados na configuração ZBFW. São usados somente a fim comunicar-se um com o otro; consequentemente, não há nenhuma necessidade de fixar estas relações.
- O controle e as interfaces de dados podem estar na mesmo relação ou VLAN. Isto preserva portas no roteador.

Grupo ausente RII

O grupo RII deve ser aplicado no LAN e em interfaces WAN. As interfaces de LAN devem estar na mesma sub-rede, mas as interfaces WAN podem estar em sub-redes separadas. Se há um grupo RII ausente em uma relação, este Syslog ocorre na saída de **debuga o evento do rii do grupo de aplicativo da Redundância** e **debuga o erro do rii do grupo de aplicativo da Redundância**:

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

Failover automático

A fim configurar o failover automático, o ZBFW HA deve ser configurado a fim seguir um objeto do contrato de nível de serviço (SLA), e diminui dinamicamente a prioridade baseada neste evento SLA. No exemplo 10, ZBFW HA segue o estado do link da relação **GigabitEthernet0**. Se esta

relação vai para baixo, a prioridade está reduzida de modo que o dispositivo de peer seja mais favorecido.

Exemplo 10: Configuração do failover automático 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
```

Às vezes o ZBFW HA não faz automaticamente Failover mesmo que haja um evento diminuído da prioridade. Isto é porque a palavra-chave **cancelar** não é configurada sob ambos os dispositivos. A palavra-chave **cancelar** tem a funcionalidade diferente do que no Hot Standby Router Protocol (HSRP) ou no Failover adaptável da ferramenta de segurança (ASA). Em ZBFW HA, a palavra-chave **cancelar** permite que um evento do Failover ocorra se a prioridade do dispositivo muda. Isto é documentado no guia de configuração de segurança: Firewall Zona-baseado da política, Cisco IOS Release 15.2M&T. Está aqui um extrato da Alta disponibilidade Zona-baseada do capítulo do Firewall da política:

“Um switchover ao dispositivo à espera pode ocorrer sob outras circunstâncias. Um outro fator que possa causar um switchover é uma configuração de prioridade que possa ser configurada em cada dispositivo. O dispositivo com o valor o mais prioritário seja o dispositivo ativo. Se uma falha ocorre no dispositivo ativo ou à espera, a prioridade do dispositivo está decrescida por uma quantidade configurável, conhecida como o peso. Se a prioridade do dispositivo ativo cai abaixo da prioridade do dispositivo à espera, um switchover ocorre e o dispositivo à espera transforma-se o dispositivo ativo. Este comportamento padrão pode ser cancelado desabilitando o atributo da preempção para o grupo de redundância. Você pode igualmente configurar cada relação para diminuir a prioridade quando o estado do Layer 1 da relação vai para baixo. A prioridade que é configurada cancela a prioridade padrão de um grupo de redundância.”

Estas saídas indicam o estado apropriado:

```
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
```

Estes logs são gerados no ZBFW sem alguns debugam permitido. Este log mostra quando o dispositivo se torna ativo:

```
*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
```

Este log mostra quando o dispositivo vai no apoio:

```
*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
```

Roteamento assimétrico

O apoio do roteamento assimétrico outined no guia do apoio do roteamento assimétrico.

A fim configurar o roteamento assimétrico, adicionar as características à configuração global do grupo de aplicativo da Redundância e à secundário-configuração da relação. É importante notar esse roteamento assimétrico e um RG não pode ser permitido na mesma relação, porque não é apoiado. Isto é devido a como o roteamento assimétrico trabalha. Quando uma relação é designada para o roteamento assimétrico, não pode ser parte de replicação da conexão HA nesse ponto, porque o roteamento é incompatível. Configurar um RG confunde o roteador, porque um RG especifica que uma relação é parte de replicação da conexão HA.

Exemplo 11: Configuração do roteamento assimétrico

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

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

Esta configuração deve ser aplicada em ambo o Roteadores nos pares HA.

A relação **Ethernet0/3** alistada previamente é um link dedicado novo entre os dois Roteadores. Este link é usado exclusivamente a fim passar o tráfego assimetricamente-roteado entre os dois

Roteadores. Eis porque deve ser um link dedicado equivalente à relação do externo-revestimento.

Informações Relacionadas

- Guia de configuração de segurança: Firewall Zona-baseado da política, Cisco IOS Release 15.2M&T
- Alta disponibilidade Zona-baseada do guia de configuração de segurança do Firewall da política
- Cisco IOS 15.2M&T
- Cisco IOS Firewall
- Field Notice de produto de segurança
- Suporte Técnico e Documentação - Cisco Systems