Configurar e solucionar problemas de alta disponibilidade do ZBFW

Contents

Introduction

Este guia fornece a configuração básica de alta disponibilidade (HA) do Zone Firewall para uma configuração ativa/em standby, bem como comandos de solução de problemas e problemas comuns observados com o recurso.

O Cisco IOS® Zone-Based Firewall (ZBFW) suporta HA para que dois roteadores Cisco IOS possam ser configurados em uma configuração ativa/standby ou ativa/ativa. Isso permite redundância para evitar um único ponto de falha.

Prerequisites

Requirements

Você deve ter uma versão posterior ao Cisco IOS Software Release 15.2(3)T.

Componentes Utilizados

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

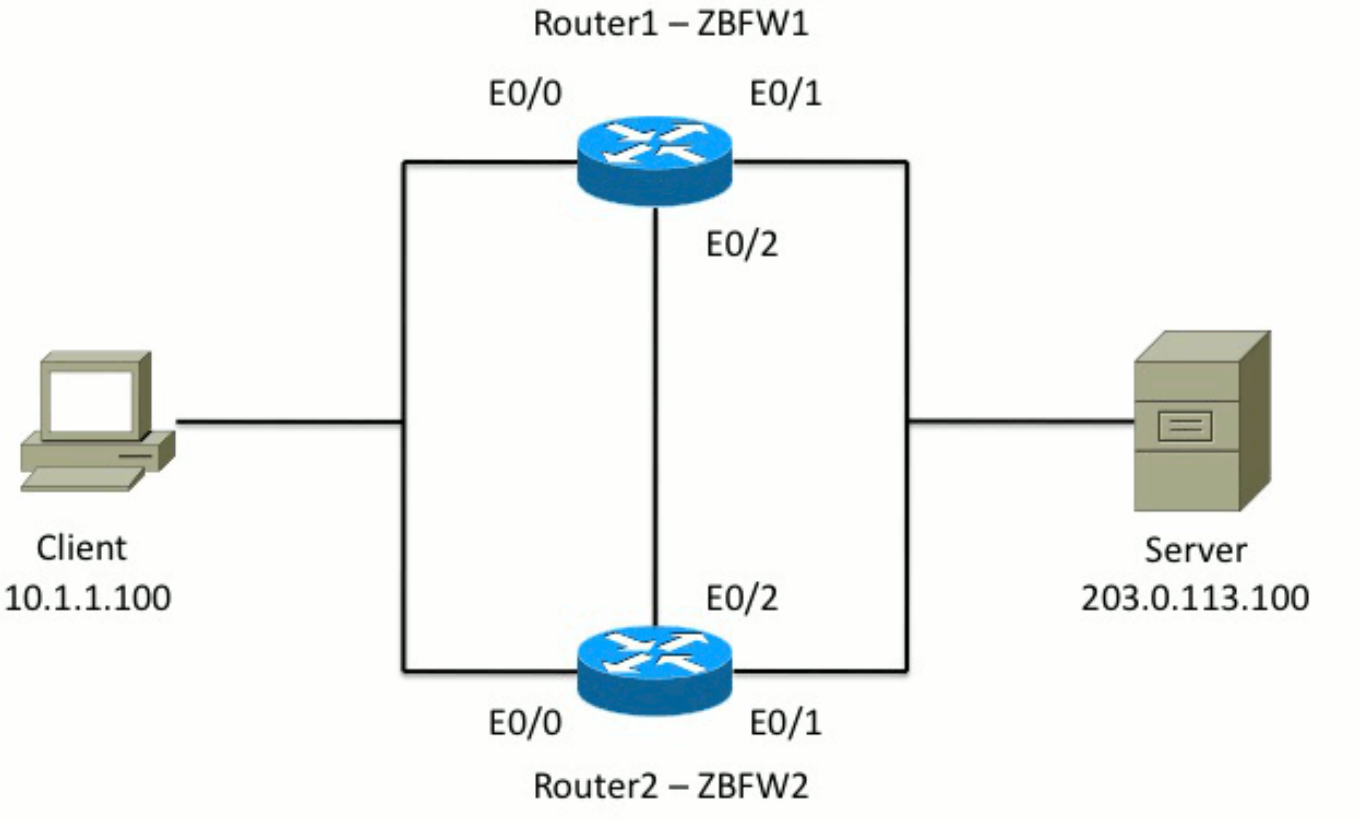
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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, o ZBFW é configurado para inspecionar o tráfego TCP, UDP e ICMP (Internet Control Message Protocol) de dentro para fora. A configuração mostrada em negrito configura o recurso HA. Nos roteadores Cisco IOS, o HA é configurado através do comando **redundancy** subconfig. Para configurar a redundância, a primeira etapa é ativar a redundância no mapa de parâmetros de inspeção global.

Depois de habilitar a redundância, insira a subconfiguração **de redundância de aplicativo** e selecione as interfaces usadas para **controle** e **dados**. A interface de controle é usada para trocar informações sobre o estado de cada roteador. A interface de dados é usada para trocar informações sobre as conexões que devem ser replicadas.

No Exemplo 2, o comando **priority** também é definido para tornar o Roteador 1 a unidade ativa no par se o Roteador 1 e o Roteador 2 estiverem operacionais. O comando **preempt** (também discutido neste documento) é usado para garantir que a falha ocorra quando a prioridade for alterada.

A etapa final é atribuir o **Redundant Interface Identifier (RII)** e o **Redundancy Group (RG)** a cada interface. O número do grupo **RII** deve ser exclusivo para cada interface, mas deve corresponder entre dispositivos para interfaces na mesma sub-rede. O RII é usado somente para o processo de sincronização em massa quando os dois roteadores sincronizam a configuração. É assim que os dois roteadores sincronizam interfaces redundantes. O **RG** é usado para indicar que as conexões por meio dessa interface são replicadas na tabela de conexão HA.

No Exemplo 2, o comando **redundancy group 1** é usado para criar um endereço IP virtual (VIP) na interface interna. Isso garante o HA, pois todos os usuários internos se comunicam somente com o VIP, para o qual a unidade ativa processa.

A interface externa não tem nenhuma configuração de RG porque esta é a interface de WAN. A interface externa do Roteador 1 e do Roteador 2 não pertence ao mesmo Provedor de Internet (ISP). Na interface externa, um protocolo de roteamento dinâmico é necessário para garantir que o tráfego passe para o dispositivo correto.

Exemplo 1: Trecho de configuração do roteador 1 (nome de host 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: Trecho de configuração do roteador 2 (nome de host 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
```

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Confirme se os dispositivos podem se comunicar entre si

Para confirmar se os dispositivos podem se ver, você deve verificar se o estado operacional do grupo de aplicativos de redundância está ativo. Em seguida, certifique-se de que cada dispositivo tenha assumido a função correta e possa ver seu peer em suas funções corretas. No Exemplo 3, o ZBFW1 está ativo e detecta seu peer como standby. Isso é invertido em ZBFW2. Quando ambos os dispositivos também mostram que o estado operacional está ativo e sua presença de peer é detectada, os dois roteadores podem se comunicar com êxito através do link de controle.

Exemplo 3: Detecção de presença de mesmo nível

```
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 no Exemplo 4 mostra uma saída mais granular sobre a interface de controle dos dois roteadores. A saída confirma a interface física usada para controlar o tráfego e também confirma o endereço IP do peer.

Exemplo 4: Saída Granular

```
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 você a entender por que cada dispositivo tem sua função específica. O ZBFW1 está ativo porque tem uma prioridade mais alta que seu peer. O ZBFW1 tem uma prioridade de 200, enquanto o ZBFW2 tem uma prioridade de 150. Esta saída está realçada em negrito.

Exemplo 5: Status e prioridade da função

```
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 garantir que a ID do grupo RII seja atribuída a cada interface. Se você inserir esse comando em ambos os roteadores, eles verificarão duas vezes para garantir que os pares de interface na mesma sub-rede entre os dispositivos recebam a mesma ID de RII. Se não

estiverem configuradas com a mesma ID RII exclusiva, as conexões não serão replicadas entre os dois dispositivos. Veja o exemplo 6.

Exemplo 6: Confirmar se a ID do grupo RII está atribuída

```
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 se as conexões se replicam para o roteador peer

No exemplo 7, o ZBFW1 passa ativamente o tráfego para uma conexão. A conexão foi replicada com êxito para o dispositivo de espera ZBFW2. Para visualizar as conexões processadas pelo firewall de zona, use o comando **show policy-firewall session**.

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 a conexão é replicada, mas os bytes transferidos não são atualizados. O estado da conexão (informações TCP) é atualizado regularmente através da interface de dados para garantir que o tráfego não seja afetado se ocorrer um evento de failover.

Para uma saída mais granular, insira o comando **show policy-firewall session zone-pair *<ZP>* ha**. Ele fornece saída semelhante à do Exemplo 7, mas permite que o usuário restrinja a saída somente ao par de zonas especificado.

Obter saída de depuração

Esta seção mostra os comandos debug que produzem saída relevante para solucionar problemas deste recurso.

A ativação de depurações pode ser muito intensa em um roteador ocupado. Portanto, você deve entender o impacto antes de ativá-los.

- **debug redundancy application group rii event**

  Esse comando é usado para garantir que as conexões correspondam ao grupo RII correto a ser replicado corretamente. Quando o tráfego chega no ZBFW, as interfaces origem e destino são verificadas quanto a uma ID de grupo RII. Essas informações são então comunicadas através do enlace de dados ao peer. Quando o grupo RII do peer de standby se alinha com as unidades ativas, o syslog no Exemplo 8 é gerado e confirma as IDs de grupo RII que são usadas para replicar 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
```

- **debug redundancy application group protocol all**

  Esse comando é usado para confirmar se os dois pares podem se ver. O endereço IP do peer é confirmado nas depurações. Como visto no Exemplo 9, o ZBFW1 vê seu peer no estado de standby com o endereço IP **10.60.1.2**. O inverso é verdadeiro para ZBFW2.

  Exemplo 9: Confirmar IPs pares em depurações

```
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 encontrados.

Controle e seleção de interface de dados

Aqui estão algumas dicas para VLANs de controle e dados:

- Não inclua as interfaces de controle e de dados na configuração do ZBFW. Apenas são utilizados para comunicar entre si; portanto, não há necessidade de proteger essas interfaces.
- As interfaces de controle e de dados podem estar na mesma interface ou VLAN. Isso preserva as portas no roteador.

Grupo de RII ausente

O grupo RII deve ser aplicado nas interfaces LAN e WAN. As interfaces LAN devem estar na mesma sub-rede, mas as interfaces WAN podem estar em sub-redes separadas. Se houver um grupo RII ausente em uma interface, esse syslog ocorrerá na saída do **comando debug redundancy application group rii event** e **debug redundancy application group rii error**:

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

Failover automático

Para configurar o failover automático, o HA do ZBFW deve ser configurado para rastrear um objeto SLA (Service Level Agreement, contrato de nível de serviço) e diminuir dinamicamente a prioridade com base nesse evento SLA. No Exemplo 10, o ZBFW HA rastreia o status do link da interface **GigabitEthernet0**. Se essa interface ficar inativa, a prioridade será reduzida para que o dispositivo peer seja mais favorecido.

Exemplo 10: Configuração de failover automático do 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 HA do ZBFW não faz failover automaticamente, mesmo que haja um evento de prioridade menor. Isso ocorre porque a palavra-chave **preempt** não está configurada em ambos os dispositivos. A palavra-chave **preempt** tem funcionalidade diferente da do failover do Hot Standby Router Protocol (HSRP) ou do Adaptive Security Appliance (ASA). No ZBFW HA, a palavra-chave **preempt** permite que um evento de failover ocorra se a prioridade do dispositivo for alterada. Isso está documentado no Guia de Configuração de Segurança: Zone-Based Policy Firewall, Cisco IOS versão 15.2M&T. Aqui está um extrato do capítulo de alta disponibilidade do firewall de política baseado em zona:

"Uma comutação para o dispositivo de espera pode ocorrer em outras circunstâncias. Outro fator que pode causar um switchover é uma configuração de prioridade que pode ser configurada em cada dispositivo. O dispositivo com o maior valor de prioridade é o dispositivo ativo. Se ocorrer uma falha no dispositivo ativo ou em standby, a prioridade do dispositivo será reduzida por uma quantidade configurável, conhecida como peso. Se a prioridade do dispositivo ativo cair abaixo da prioridade do dispositivo em standby, um switchover ocorrerá e o dispositivo em standby se tornará o dispositivo ativo. Esse comportamento padrão pode ser substituído desabilitando o atributo de preferência para o grupo de redundância. Você também pode configurar cada interface para diminuir a prioridade quando o estado da Camada 1 da interface for desativado. A prioridade configurada substitui a prioridade padrão de um grupo de redundância."

Essas saídas indicam o estado correto:

```
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
```

Esses registros são gerados no ZBFW sem nenhuma depuração ativada. Este registro 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 registro mostra quando o dispositivo fica em espera:

```
*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 suporte ao roteamento assimétrico está descrito no guia Asymmetric Routing Support.

Para configurar o roteamento assimétrico, adicione os recursos à configuração global do grupo de aplicativos de redundância e à subconfiguração da interface. É importante observar que o roteamento assimétrico e um RG não podem ser habilitados na mesma interface, porque não são suportados. Isso se deve ao modo como o roteamento assimétrico funciona. Quando uma interface é designada para roteamento assimétrico, ela não pode fazer parte da replicação da conexão HA nesse ponto, porque o roteamento é inconsistente. Configurar um RG confunde o roteador, porque um RG especifica que uma interface faz parte da replicação da conexão HA.

Exemplo 11: Configuração de roteamento assimétrico

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

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

Essa configuração deve ser aplicada em ambos os roteadores no par HA.

A interface **Ethernet0/3** listada anteriormente é um novo link dedicado entre os dois roteadores. Esse link é usado exclusivamente para transmitir tráfego roteado assimetricamente entre os dois roteadores. É por isso que ele deve ser um link dedicado equivalente à interface externa.

Informações Relacionadas

- Guia de configuração de segurança: Firewall de política baseado em zona, Cisco IOS versão 15.2M&T
- Guia de configuração de segurança de alta disponibilidade do firewall de política baseado em zona
- Cisco IOS 15.2M&T
- Cisco IOS Firewall
- Avisos de campo do produto de segurança
- Suporte Técnico e Documentação - Cisco Systems