Configuración y resolución de problemas de alta disponibilidad ZBFW

Contenido

Introducción

Esta guía proporciona la configuración básica para Zone Firewall High Availability (HA) para una configuración activa/en espera, así como comandos de resolución de problemas y problemas comunes observados con la función.

Cisco IOS® Zone-Based Firewall (ZBFW) es compatible con HA para que dos routers Cisco IOS puedan configurarse en una configuración activa/en espera o activa/activa. Esto permite la redundancia para evitar un único punto de falla.

Prerequisites

Requirements

Debe tener una versión posterior a Cisco IOS Software Release15.2(3)T.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

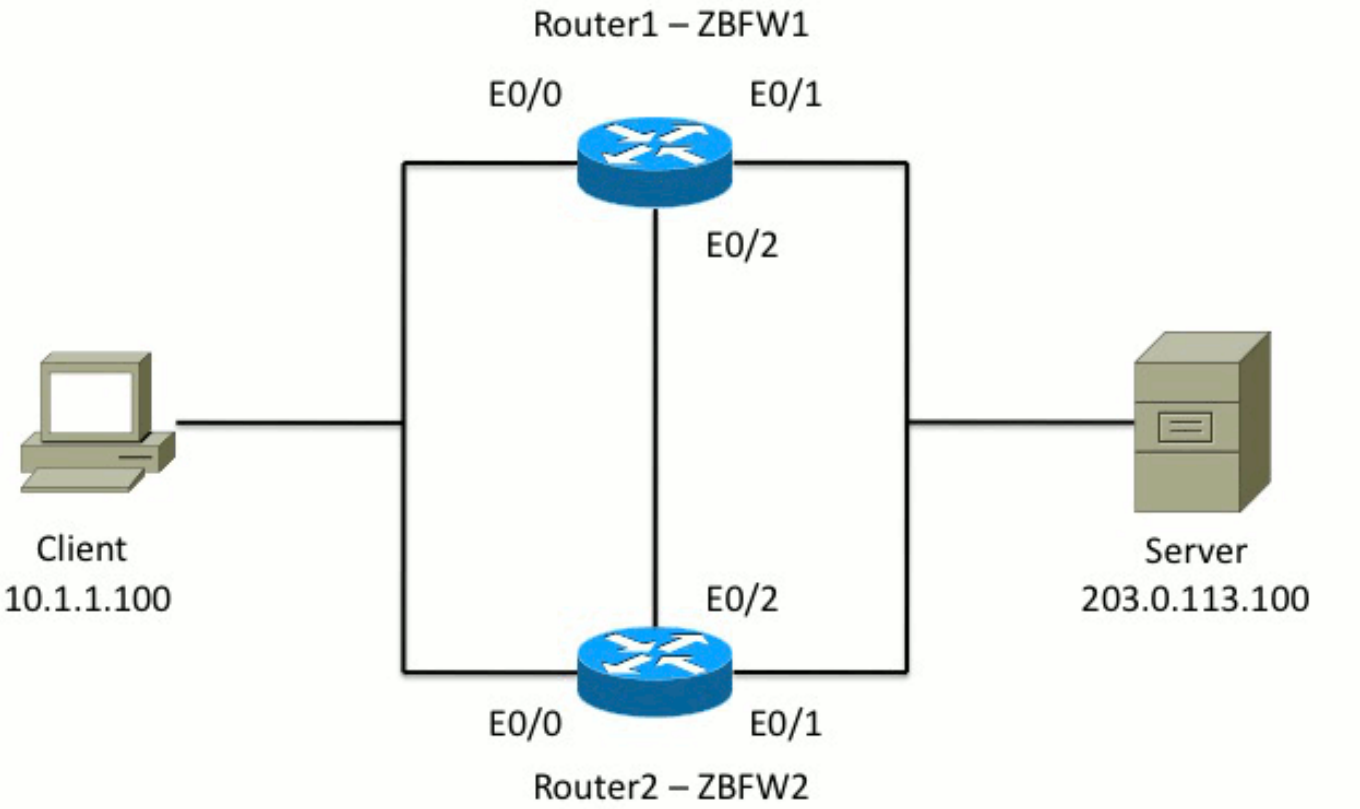
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configurar

Este diagrama muestra la topología utilizada en los ejemplos de configuración.



En la configuración que se muestra en el ejemplo 1, ZBFW se configura para inspeccionar el tráfico TCP, UDP y el protocolo de mensajes de control de Internet (ICMP) desde el interior al exterior. La configuración mostrada en negrita configura la función HA. En los routers Cisco IOS, HA se configura a través del comando **redundancy** subconfig. Para configurar la redundancia, el primer paso es habilitar la redundancia en el mapa de parámetros de inspección global.

Después de habilitar la redundancia, ingrese la subconfiguración de **redundancia de la aplicación** y seleccione las interfaces que se utilizan para **control** y **datos**. La interfaz de control se utiliza para intercambiar información sobre el estado de cada router. La interfaz de datos se utiliza para intercambiar información sobre las conexiones que se deben replicar.

En el Ejemplo 2, el comando **priority** también se establece para hacer del Router 1 la unidad activa en el par si tanto el Router 1 como el Router 2 están operativos. El comando **preempt** (que también se analiza más a fondo en este documento) se utiliza para garantizar que se produce un error una vez que cambia la prioridad.

El paso final es asignar el **Identificador de interfaz redundante (RII)** y el **Grupo de redundancia (RG)** a cada interfaz. El número de grupo **RII** debe ser único para cada interfaz, pero debe coincidir entre los dispositivos para las interfaces en la misma subred. El RII sólo se utiliza para el proceso de sincronización masiva cuando los dos routers sincronizan la configuración. Así es como los dos routers sincronizan las interfaces redundantes. El **RG** se utiliza para indicar que las conexiones a través de esa interfaz se replican en la tabla de conexión HA.

En el Ejemplo 2, se utiliza el comando **redundancy group 1** para crear una dirección IP virtual (VIP) en la interfaz interna. Esto asegura la HA, porque todos los usuarios internos sólo se comunican con el VIP, para el cual se procesa la unidad activa.

La interfaz externa no tiene ninguna configuración RG porque ésta es la interfaz WAN. La interfaz externa del router 1 y del router 2 no pertenece al mismo proveedor de servicios de Internet (ISP). En la interfaz exterior, se requiere un protocolo de ruteo dinámico para asegurar que el tráfico

pase al dispositivo correcto.

Ejemplo 1: Fragmento de configuración del router 1 (nombre 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
```

Ejemplo 2: Fragmento de configuración del router 2 (nombre 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

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Confirme que los dispositivos pueden comunicarse entre sí

Para confirmar que los dispositivos pueden verse entre sí, debe verificar que el estado operativo del grupo de aplicaciones de redundancia esté activo. A continuación, asegúrese de que cada dispositivo ha asumido la función correcta y puede ver a su par en sus funciones correctas. En el ejemplo 3, ZBFW1 está activo y detecta su peer como standby. Esto se invierte en ZBFW2.

Cuando ambos dispositivos también muestran que el estado operativo está activo y se detecta su presencia de peer, los dos routers pueden comunicarse con éxito a través del link de control.

Ejemplo 3: Detección de presencia de pares

```
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
```

El resultado del Ejemplo 4 muestra un resultado más granular sobre la interfaz de control de los dos routers. El resultado confirma la interfaz física utilizada para controlar el tráfico y también confirma la dirección IP del par.

Ejemplo 4: Salida 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
```

Cuando se establece la comunicación, el comando del ejemplo 5 le ayuda a entender por qué cada dispositivo está en su función particular. ZBFW1 está activo porque tiene una prioridad más alta que su peer. ZBFW1 tiene una prioridad de **200**, mientras que ZBFW2 tiene una prioridad de **150**. Este resultado se resalta en negrita.

Ejemplo 5: Estado y prioridad de la función

```
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 última confirmación es para asegurarse de que el ID de grupo RII esté asignado a cada interfaz. Si ingresa este comando en ambos routers, ellos verifican dos veces para asegurarse de que los pares de interfaz en la misma subred entre los dispositivos tengan asignado el mismo ID de RII. Si no se configuran con el mismo ID de RII único, las conexiones no se replican entre los dos dispositivos. Consulte el ejemplo 6.

Ejemplo 6: Confirmar ID de grupo de RII asignado

```
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 las Conexiones se Repliquen al Router de Peer

En el ejemplo 7, ZBFW1 pasa activamente el tráfico para una conexión. La conexión se replica correctamente en el dispositivo en espera ZBFW2. Para ver las conexiones procesadas por el firewall de zona, utilice el comando **show policy-firewall session**.

Ejemplo 7: Conexiones procesadas

```
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 la conexión se replica, pero los bytes transferidos no se actualizan. El estado de conexión (información de TCP) se actualiza regularmente a través de la interfaz de datos para asegurarse de que el tráfico no se vea afectado si se produce un evento de conmutación por fallo.

Para obtener una salida más granular, ingrese el comando **show policy-firewall session zone-pair *<ZP>* ha**. Proporciona un resultado similar al del ejemplo 7, pero permite al usuario restringir el resultado sólo al par de zonas especificado.

Recopilar resultados de depuración

Esta sección muestra los comandos debug que producen resultados relevantes para resolver este problema.

La habilitación de depuraciones puede ser muy intensa en un router ocupado. Por lo tanto, debe comprender el impacto antes de habilitarlo.

- **debug redundancy application group rii event**

  Este comando se utiliza para asegurarse de que las conexiones coincidan con el grupo RII correcto que se replicará correctamente. Cuando el tráfico llega al ZBFW, las interfaces de origen y de destino se comprueban en busca de un ID de grupo RII. Esta información se comunica luego a través del link de datos al par. Cuando el grupo RII del peer en espera se alinea con las unidades activas, se genera el syslog en el Ejemplo 8 y confirma los ID de grupo RII que se utilizan para replicar la conexión:

  Ejemplo 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**

  Este comando se utiliza para confirmar que los dos pares pueden verse entre sí. La dirección IP de peer se confirma en las depuraciones. Como se ve en el Ejemplo 9, ZBFW1 ve a su

peer en el estado de espera con la dirección IP **10.60.1.2**. Lo contrario es cierto para ZBFW2.

Ejemplo 9: Confirmar IP de Peer en 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
```

Problemas comunes

Esta sección detalla algunos problemas comunes que se han encontrado.

Selección de interfaz de datos y control

Estos son algunos consejos para las VLAN de datos y control:

- No incluya las interfaces de datos y control en la configuración de ZBFW. Sólo se utilizan para comunicarse entre sí; por lo tanto, no hay necesidad de asegurar estas interfaces.
- Las interfaces de control y datos pueden estar en la misma interfaz o VLAN. Esto preserva los puertos en el router.

Grupo RII ausente

El grupo RII debe aplicarse tanto en las interfaces LAN como WAN. Las interfaces LAN deben estar en la misma subred, pero las interfaces WAN pueden estar en subredes separadas. Si hay un grupo RII ausente en una interfaz, este syslog ocurre en la salida del **evento rii del grupo de aplicaciones de redundancia de debug** y **error rii del grupo de aplicaciones de redundancia de debug**:

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

Conmutación por error automática

Para configurar la conmutación por fallas automática, se debe configurar el HA de ZBFW para realizar un seguimiento de un objeto de acuerdo de nivel de servicio (SLA) y reducir dinámicamente la prioridad en función de este evento SLA. En el Ejemplo 10, ZBFW HA realiza un seguimiento del estado del link de la interfaz **GigabitEthernet0**. Si esta interfaz se desactiva, la prioridad se reduce para que el dispositivo de peer sea más favorecido.

Ejemplo 10: Configuración automática de conmutación por fallas de 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
```

A veces, el ZBFW HA no conmuta por error automáticamente aunque haya un evento de prioridad reducida. Esto se debe a que la palabra clave **preempt** no está configurada en ambos dispositivos. La palabra clave **preempt** tiene una funcionalidad diferente a la de conmutación por fallo de Hot Standby Router Protocol (HSRP) o Adaptive Security Appliance (ASA). En ZBFW HA, la palabra clave **preempt** permite que ocurra un evento de failover si cambia la prioridad del dispositivo. Esto se documenta en la Guía de Configuración de Seguridad: Firewall de Políticas Basado en Zona, Cisco IOS Release 15.2M&T. A continuación se muestra un extracto del capítulo de alta disponibilidad del firewall de políticas basado en zonas:

"Un switchover al dispositivo en espera puede ocurrir en otras circunstancias. Otro factor que puede provocar un switchover es una configuración de prioridad que se puede configurar en cada dispositivo. El dispositivo con el valor de prioridad más alto es el dispositivo activo. Si se produce una falla en el dispositivo activo o en espera, la prioridad del dispositivo disminuye en una cantidad configurable, conocida como peso. Si la prioridad del dispositivo activo cae por debajo de la prioridad del dispositivo en espera, se produce un switchover y el dispositivo en espera se convierte en el dispositivo activo. Este comportamiento predeterminado se puede invalidar desactivando el atributo de prioridad para el grupo de redundancia. También puede configurar cada interfaz para disminuir la prioridad cuando el estado de la Capa 1 de la interfaz se desactiva. La prioridad configurada invalida la prioridad predeterminada de un grupo de redundancia".

Estos resultados indican el estado adecuado:

```
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
```

Estos registros se generan en el ZBFW sin ninguna depuración habilitada. Este registro muestra cuando el dispositivo se activa:

```
*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 muestra cuando el dispositivo se encuentra en 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
```

Ruteo Asimétrico

El soporte de ruteo asimétrico se describe en la guía Soporte de Ruteo Asimétrico.

Para configurar el ruteo asimétrico, agregue las funciones tanto a la configuración global del grupo de aplicaciones de redundancia como a la subconfiguración de la interfaz. Es importante tener en cuenta que el ruteo asimétrico y un RG no se pueden habilitar en la misma interfaz, porque no se soportan. Esto se debe a cómo funciona el ruteo asimétrico. Cuando una interfaz se designa para el ruteo asimétrico, no puede ser parte de la replicación de conexión HA en ese punto, porque el ruteo es inconsistente. La configuración de un RG confunde al router, porque un RG especifica que una interfaz es parte de la replicación de la conexión HA.

Ejemplo 11: Configuración de Ruteo Asimétrico

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

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

Esta configuración se debe aplicar en ambos routers en el par HA.

La interfaz **Ethernet0/3** mencionada anteriormente es un nuevo link dedicado entre los dos routers. Este link se utiliza exclusivamente para pasar tráfico ruteado asimétricamente entre los dos routers. Esta es la razón por la que debería ser un link dedicado equivalente a la interfaz orientada externamente.

Información Relacionada

- Guía de configuración de seguridad: Firewall de políticas basado en zonas, Cisco IOS Release 15.2M&T
- Guía de configuración de seguridad de alta disponibilidad de firewall de políticas basadas en zonas
- Cisco IOS 15.2M&T
- Cisco IOS Firewall
- Avisos de campo de productos de seguridad
- Soporte Técnico y Documentación - Cisco Systems