Configurazione e risoluzione dei problemi di elevata disponibilità ZBFW

Sommario

Introduzione

Questa guida fornisce la configurazione di base per Zone Firewall High Availability (HA) per un'installazione attiva/standby, nonché i comandi per la risoluzione dei problemi e i problemi comuni rilevati con la funzione.

Cisco IOS® Zone-Based Firewall (ZBFW) supporta HA in modo che due router Cisco IOS possano essere configurati in modalità attivo/standby o attivo/attivo. Ciò consente la ridondanza per evitare un singolo punto di errore.

Prerequisiti

Requisiti

Ènecessario disporre di una versione successiva al software Cisco IOS versione 15.2(3)T.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

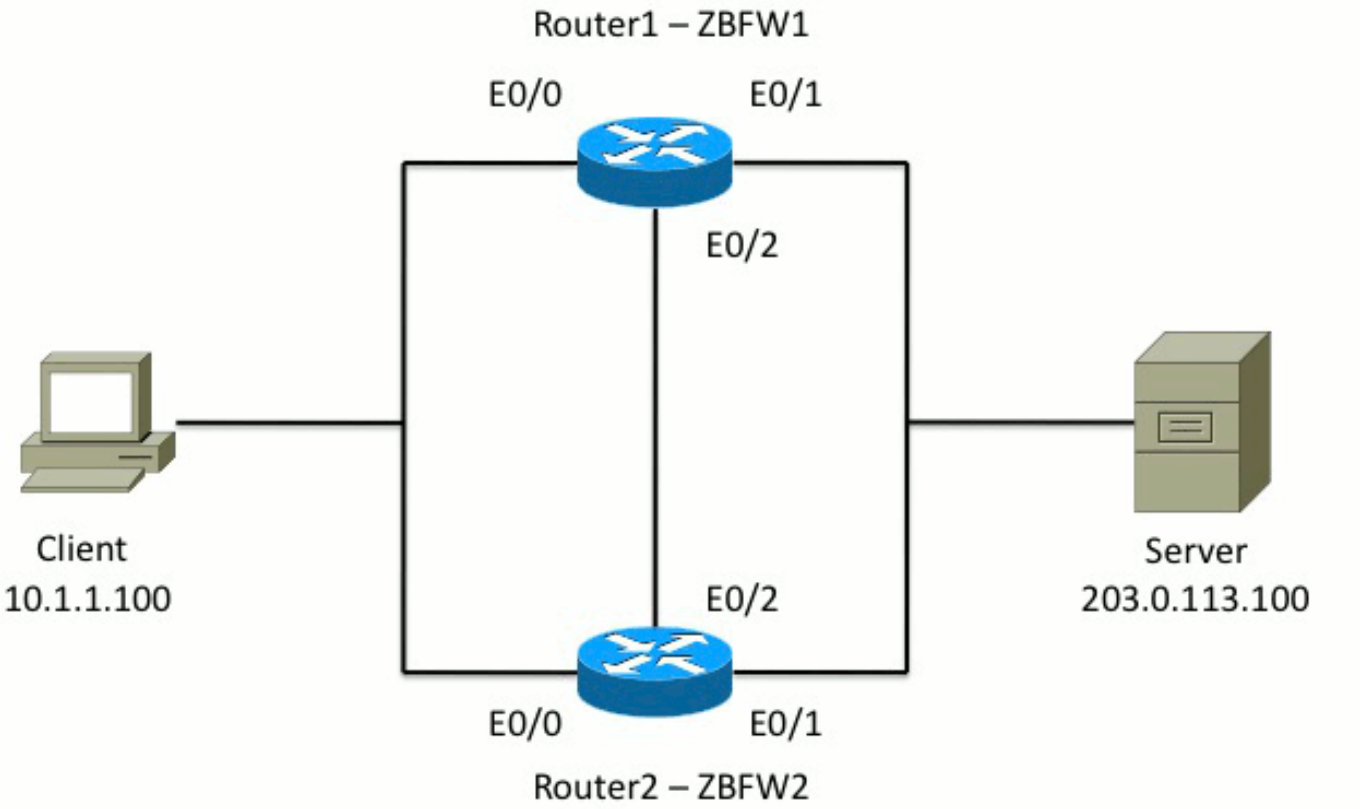
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione

Il diagramma mostra la topologia utilizzata negli esempi di configurazione.



Nella configurazione mostrata nell'Esempio 1, lo ZBFW è configurato per ispezionare il traffico TCP, UDP e ICMP (Internet Control Message Protocol) dall'interno all'esterno. La configurazione mostrata in grassetto imposta la funzione HA. Nei router Cisco IOS, il protocollo HA è configurato tramite il comando **redundancy** subconfig. Per configurare la ridondanza, il primo passaggio consiste nell'abilitare la ridondanza nella mappa dei parametri di ispezione globale.

Dopo aver abilitato la ridondanza, immettere la subconfig di **ridondanza applicazione** e selezionare le interfacce utilizzate per il **controllo** e **i dati**. L'interfaccia di controllo viene usata per scambiare informazioni sullo stato di ciascun router. L'interfaccia dati viene utilizzata per scambiare informazioni sulle connessioni da replicare.

Nell'esempio 2, il comando **priority** è impostato anche per rendere il router 1 l'unità attiva nella coppia se sia il router 1 che il router 2 sono operativi. il comando **preempt** (descritto più avanti in questo documento) viene usato per verificare che l'errore si verifichi quando la priorità cambia.

Il passaggio finale consiste nell'assegnare l'**identificatore di interfaccia ridondante (RII)** e il **gruppo di ridondanza (RG)** a ciascuna interfaccia. Il numero di gruppo **RII** deve essere univoco per ciascuna interfaccia, ma deve corrispondere tra i dispositivi per le interfacce nella stessa subnet. L'interfaccia RII viene utilizzata solo per il processo di sincronizzazione globale quando i due router sincronizzano la configurazione. In questo modo i due router sincronizzano le interfacce ridondanti. L'**RG** viene usato per indicare che le connessioni attraverso quell'interfaccia vengono replicate nella tabella delle connessioni HA.

Nell'esempio 2, il comando **redundancy group 1** viene usato per creare un indirizzo IP virtuale (VIP) sull'interfaccia interna. Ciò assicura un'elevata disponibilità in quanto tutti gli utenti interni comunicano solo con l'indirizzo VIP, per il quale l'unità attiva elabora.

L'interfaccia esterna non ha alcuna configurazione RG perché è l'interfaccia WAN. L'interfaccia esterna del router 1 e del router 2 non appartengono allo stesso provider di servizi Internet (ISP). Sull'interfaccia esterna, è necessario un protocollo di routing dinamico per garantire che il traffico

passi al dispositivo corretto.

Esempio 1: Frammento di configurazione router 1 (nome 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
```

Esempio 2: Frammento di configurazione del router 2 (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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Conferma che i dispositivi possono comunicare tra loro

Per verificare che i dispositivi possano vedersi, è necessario verificare che lo stato operativo del gruppo di applicazioni di ridondanza sia attivo. Verificare quindi che ogni dispositivo abbia assunto il ruolo corretto e che possa vedere il relativo peer nei ruoli corretti. Nell'esempio 3, ZBFW1 è attivo e rileva il peer in standby. Questo è invertito su ZBFW2. Quando entrambi i dispositivi

mostrano anche che lo stato operativo è attivo e viene rilevata la loro presenza peer, i due router possono comunicare correttamente attraverso il collegamento di controllo.

Esempio 3: Rilevamento presenza peer

```
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
```

L'output dell'esempio 4 mostra un output più granulare sull'interfaccia di controllo dei due router. L'output conferma l'interfaccia fisica utilizzata per il controllo del traffico e anche l'indirizzo IP del peer.

Esempio 4: Uscita granulare

```
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
```

Una volta stabilita la comunicazione, il comando riportato nell'Esempio 5 consente di comprendere perché ogni dispositivo svolge il proprio ruolo. ZBFW1 è attivo perché ha una priorità più alta rispetto al peer. ZBFW1 ha una priorità di **200**, mentre ZBFW2 ha una priorità di **150**. Questo output è evidenziato in grassetto.

Esempio 5: Stato e priorità del ruolo

```
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
```

L'ultima conferma consiste nell'assegnare l'ID gruppo RII a ciascuna interfaccia. Se si immette questo comando su entrambi i router, i router eseguono un doppio controllo per verificare che alle coppie di interfacce sulla stessa subnet tra i dispositivi venga assegnato lo stesso ID RII. Se non sono configurate con lo stesso ID RII univoco, le connessioni non vengono replicate tra i due dispositivi. Vedere l'Esempio 6.

Esempio 6: Conferma assegnazione ID gruppo 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
```

Verificare che le connessioni vengano replicate sul router peer

Nell'esempio 7, ZBFW1 trasmette attivamente il traffico per una connessione. Replica della connessione nel dispositivo di standby ZBFW2 completata. Per visualizzare le connessioni elaborate dal firewall della zona, usare il comando **show policy-firewall session**.

Esempio 7: Connessioni elaborate

```
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
```

La connessione viene replicata, ma i byte trasferiti non vengono aggiornati. Lo stato della connessione (informazioni TCP) viene aggiornato regolarmente tramite l'interfaccia dati per garantire che il traffico non venga influenzato dal verificarsi di un evento di failover.

Per un output più granulare, immettere il comando **show policy-firewall session zone-pair *<ZP>* ha**. Fornisce un output simile all'esempio 7, ma consente all'utente di limitare l'output solo alla coppia di zone specificata.

Raccogli output di debug

In questa sezione vengono illustrati i comandi di debug che producono l'output rilevante per la risoluzione dei problemi di questa funzione.

L'abilitazione dei debug può essere molto complessa su un router occupato. Pertanto, è necessario comprendere l'impatto prima di abilitarli.

- **debug redundancy application group rii event**

  Questo comando è usato per assicurarsi che le connessioni corrispondano al gruppo RII corretto per essere replicate correttamente. Quando arriva il traffico sulla ZBFW, le interfacce di origine e di destinazione vengono controllate per trovare un ID gruppo RII. Queste informazioni vengono quindi comunicate al peer attraverso il collegamento dati. Quando il gruppo RII del peer in standby si allinea alle unità attive, viene generato il syslog nell'esempio 8 e viene confermata la presenza degli ID del gruppo RII utilizzati per replicare la connessione:

  Esempio 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**

  Questo comando è usato per verificare che i due peer possano vedersi. L'indirizzo IP del peer

viene confermato nei debug. Come mostrato nell'esempio 9, ZBFW1 vede il suo peer nello stato di standby con l'indirizzo IP **10.60.1.2**. Il contrario è vero per ZBFW2.

Esempio 9: Conferma IP peer nei debug

```
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
```

Problemi comuni

In questa sezione vengono descritti in dettaglio alcuni problemi comuni riscontrati.

Selezione interfaccia dati e controllo

Di seguito sono riportati alcuni suggerimenti per le VLAN di controllo e di dati:

- Non includere le interfacce dati e di controllo nella configurazione ZBFW. sono utilizzate solo per comunicare tra loro; non è necessario quindi proteggere queste interfacce.
- Le interfacce di controllo e dati possono trovarsi sulla stessa interfaccia o VLAN. In questo modo, vengono preservate le porte del router.

Gruppo RII assente

Il gruppo RII deve essere applicato su entrambe le interfacce LAN e WAN. Le interfacce LAN devono trovarsi nella stessa subnet, ma le interfacce WAN possono trovarsi su subnet separate. Se un gruppo RII è assente su un'interfaccia, questo syslog si verifica nell'output dell'**evento rii del**

gruppo di applicazioni di ridondanza di debug e dell'**errore rii del gruppo di applicazioni di ridondanza di debug**:

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

Failover automatico

Per configurare il failover automatico, ZBFW HA deve essere configurato in modo da tenere traccia di un oggetto SLA (Service Level Agreement) e ridurre dinamicamente la priorità in base a questo evento SLA. Nell'esempio 10, ZBFW HA tiene traccia dello stato del collegamento dell'interfaccia **Gigabit Ethernet0**. Se l'interfaccia non è disponibile, la priorità viene ridotta in modo da privilegiare il dispositivo peer.

Esempio 10: Configurazione failover automatico 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 volte ZBFW HA non esegue il failover automatico anche se si verifica un evento con priorità ridotta. Infatti, la parola chiave **preempt** non è configurata su entrambi i dispositivi. La parola chiave **preempt** ha funzionalità diverse rispetto al failover HSRP (Hot Standby Router Protocol) o ASA (Adaptive Security Appliance). In ZBFW HA, la parola chiave **preempt** consente il verificarsi di un evento di failover se la priorità del dispositivo cambia. Questa condizione viene documentata nella Guida alla configurazione della sicurezza: Zone-Based Policy Firewall, Cisco IOS release 15.2M&T. Di seguito viene riportato un estratto del capitolo relativo all'alta disponibilità di Policy Firewall basata su zone:

"Il passaggio al dispositivo di standby può avvenire in altre circostanze. Un altro fattore che può causare lo switchover è l'impostazione della priorità che può essere configurata su ciascun dispositivo. Il dispositivo con il livello di priorità più alto deve essere il dispositivo attivo. Se si verifica un errore sul dispositivo attivo o in standby, la priorità del dispositivo viene ridotta di una quantità configurabile, nota come peso. Se la priorità del dispositivo attivo è inferiore a quella del dispositivo di standby, si verifica un passaggio e il dispositivo di standby diventa il dispositivo attivo. È possibile ignorare questo comportamento predefinito disabilitando l'attributo relativo all'interruzione per diritti di priorità per il gruppo di ridondanza. È inoltre possibile configurare ciascuna interfaccia in modo che diminuisca la priorità quando lo stato del layer 1 dell'interfaccia diventa inattivo. La priorità configurata ha la precedenza sulla priorità predefinita di un gruppo di

ridondanza."

Questi output indicano lo stato corretto:

```
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
```

Questi log vengono generati sullo ZBFW senza alcun debug abilitato. In questo registro viene mostrato quando il dispositivo diventa attivo:

```
*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
```

Questo registro mostra quando il dispositivo entra in standby:

```
*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
```

Routing asimmetrico

Il supporto per il routing asimmetrico è descritto nella guida al supporto del routing asimmetrico.

Per configurare il routing asimmetrico, aggiungere le funzionalità alla configurazione globale del gruppo di applicazioni di ridondanza e alla sottoconfigurazione dell'interfaccia. È importante notare che il routing asimmetrico e un RG non possono essere abilitati sulla stessa interfaccia perché non sono supportati. Ciò è dovuto al funzionamento del routing asimmetrico. Quando

un'interfaccia viene designata per il routing asimmetrico, non può far parte della replica della connessione HA in quel punto, perché il routing è incoerente. La configurazione di un RG confonde il router, in quanto un RG specifica che un'interfaccia fa parte della replica della connessione HA.

Esempio 11: Configurazione routing asimmetrico

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

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

Questa configurazione deve essere applicata a entrambi i router della coppia HA.

L'interfaccia **Ethernet0/3** descritta in precedenza è un nuovo collegamento dedicato tra i due router. Questo collegamento viene usato esclusivamente per passare il traffico con routing asimmetrico tra i due router. Ecco perché dovrebbe essere un collegamento dedicato equivalente all'interfaccia rivolta verso l'esterno.

Informazioni correlate

- Guida alla configurazione della protezione: Zone-Based Policy Firewall, Cisco IOS release 15.2M&T
- Guida alla configurazione della protezione ad alta disponibilità del firewall dei criteri basato su zone
- Cisco IOS 15.2 M e T
- Cisco IOS Firewall
- Avvisi sui prodotti per la sicurezza
- Documentazione e supporto tecnico – Cisco Systems