Technische Anmerkung: Konfiguration der ZBFW-Hochverfügbarkeit und Fehlerbehebung

Inhalt

Einleitung

Dieses Handbuch enthält die grundlegende Konfiguration für die Hochverfügbarkeit der Zone-Firewall (HA) für eine Aktiv/Standby-Konfiguration, Befehle zur Fehlerbehebung sowie häufige Probleme, die mit dieser Funktion auftreten.

Cisco IOS® ZBFW (Zone-Based Firewall) unterstützt HA, sodass zwei Cisco IOS-Router in einer Aktiv/Standby- oder Aktiv/Aktiv-Konfiguration konfiguriert werden können. Dies ermöglicht Redundanz, um einen Single-Point-of-Failure zu verhindern.

Voraussetzungen

Anforderungen

Sie benötigen eine Version, die später als die Cisco IOS Software Release 15.2(3)T ist.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

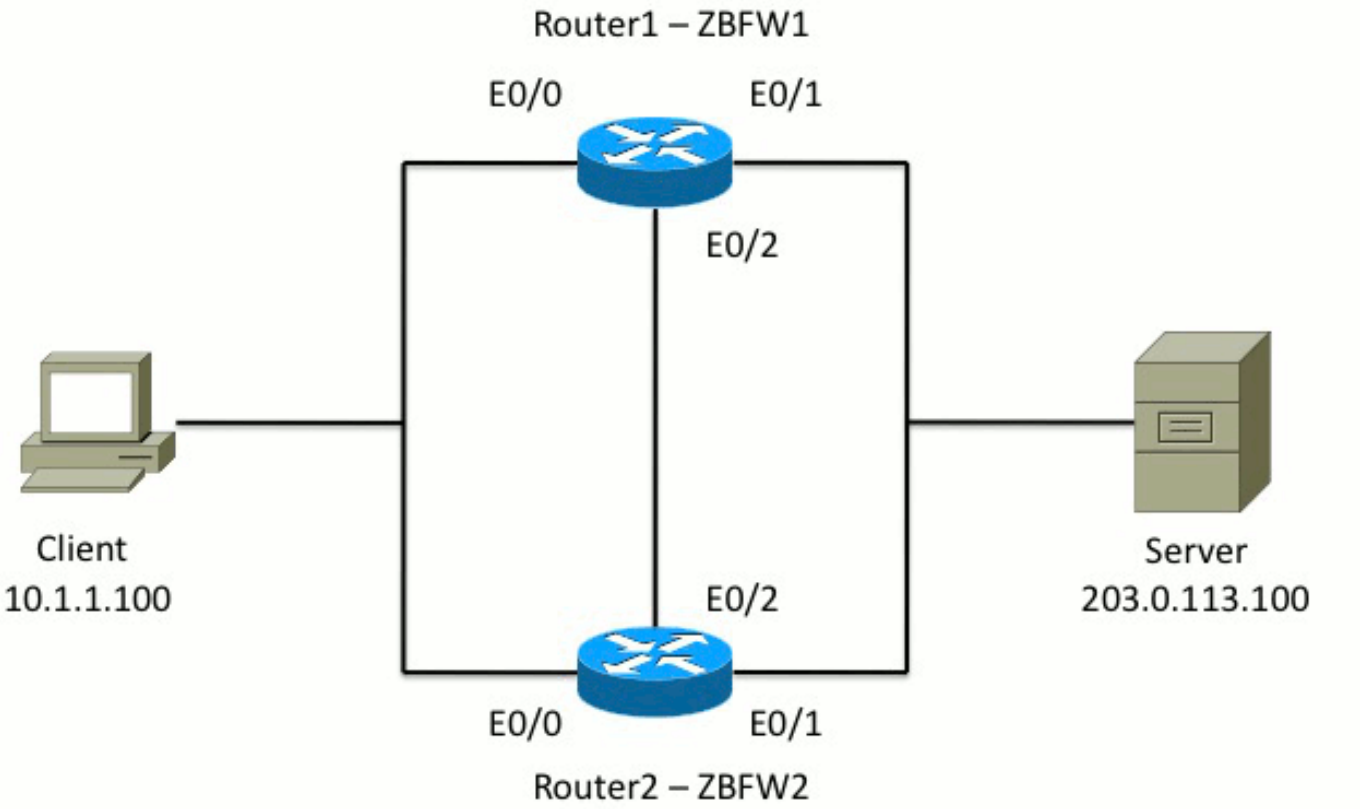
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Konfigurieren

Dieses Diagramm zeigt die in den Konfigurationsbeispielen verwendete Topologie.



In der in Beispiel 1 gezeigten Konfiguration wird ZBFW so konfiguriert, dass der TCP-, UDP- und ICMP-Datenverkehr (Internet Control Message Protocol) von innen nach außen geprüft wird. Die fett dargestellte Konfiguration richtet die HA-Funktion ein. In Cisco IOS-Routern wird die HA-Funktion über den Befehl **redundancy** subconfig konfiguriert. Um Redundanz zu konfigurieren, ist der erste Schritt die Aktivierung der Redundanz in der globalen Prüfparameter-Map.

Wenn Sie die Redundanz aktiviert haben, geben Sie die Subkonfiguration für die **Anwendungsredundanz ein**, und wählen Sie die Schnittstellen aus, die für die **Steuerung** und die **Daten** verwendet werden. Die Steuerungsschnittstelle wird verwendet, um Informationen über den Status der einzelnen Router auszutauschen. Die Datenschnittstelle wird verwendet, um Informationen über die Verbindungen auszutauschen, die repliziert werden sollen.

In Beispiel 2 ist der Befehl **priority** ebenfalls so festgelegt, dass Router 1 die aktive Einheit im Paar bildet, wenn Router 1 und Router 2 betriebsbereit sind. Der **Befehl** preempt (der in diesem Dokument weiter erläutert wird) wird verwendet, um sicherzustellen, dass der Fehler auftritt, wenn sich die Priorität ändert.

Im letzten Schritt werden jeder Schnittstelle der **Redundant Interface Identifier (RII)** und die **Redundancy Group (RG)** zugewiesen. Die **RII-**Gruppennummer muss für jede Schnittstelle eindeutig sein, für Schnittstellen im gleichen Subnetz muss sie jedoch auf allen Geräten übereinstimmen. Der RII wird nur für den Synchronisierungsprozess für Massen verwendet, wenn die Konfiguration von beiden Routern synchronisiert wird. So synchronisieren die beiden Router redundante Schnittstellen. Der **RG** wird verwendet, um anzugeben, dass Verbindungen über diese Schnittstelle in die HA-Verbindungstabelle repliziert werden.

In Beispiel 2 wird der Befehl **Redundanzgruppe 1** verwendet, um eine virtuelle IP (VIP)-Adresse auf der internen Schnittstelle zu erstellen. Dies stellt die hohe Verfügbarkeit sicher, da alle internen Benutzer nur mit dem VIP kommunizieren, für das die aktive Einheit Prozesse durchführt.

Die externe Schnittstelle verfügt über keine RG-Konfiguration, da es sich um die WAN-

Schnittstelle handelt. Die externe Schnittstelle von Router 1 und Router 2 gehört nicht zum gleichen Internet Service Provider (ISP). Auf der externen Schnittstelle ist ein dynamisches Routing-Protokoll erforderlich, um sicherzustellen, dass der Datenverkehr an das richtige Gerät weitergeleitet wird.

Beispiel 1: Konfigurationsausschnitt Router 1 (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
```

Beispiel 2: Router 2-Konfigurationsausschnitt (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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Bestätigen Sie, dass Geräte miteinander kommunizieren können.

Um sicherzustellen, dass sich die Geräte gegenseitig sehen können, müssen Sie überprüfen, ob

der Betriebsstatus der Redundanzanwendungsgruppe aktiv ist. Stellen Sie dann sicher, dass jedes Gerät die richtige Rolle übernommen hat und seine Peer-Rolle in der richtigen Rolle sehen kann. In Beispiel 3 ist ZBFW1 aktiv und erkennt den Peer als Standby. Dies wird auf ZBFW2 umgekehrt. Wenn beide Geräte auch anzeigen, dass der Betriebsstatus aktiv ist und ihre Peer-Präsenz erkannt wird, können die beiden Router erfolgreich über die Steuerungsverbindung kommunizieren.

Beispiel 3: Erkennung von Peer-Presence

```
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
```

Die Ausgabe in Beispiel 4 zeigt eine genauere Ausgabe über die Steuerungsschnittstelle der beiden Router. Die Ausgabe bestätigt die für die Steuerung des Datenverkehrs verwendete physische Schnittstelle und bestätigt auch die IP-Adresse des Peers.

Beispiel 4: Präzise Ausgabe

```
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
```

Wenn die Kommunikation hergestellt ist, hilft Ihnen der Befehl in Beispiel 5 zu verstehen, warum jedes Gerät in seiner jeweiligen Rolle spielt. ZBFW1 ist aktiv, da es eine höhere Priorität als sein Peer hat. Die ZBFW1 hat eine Priorität von **200**, während die ZBFW2 eine Priorität von **150** hat. Diese Ausgabe ist fett markiert.

Beispiel 5: Rollenstatus und Priorität

```
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
```

Die letzte Bestätigung besteht darin, sicherzustellen, dass die RII-Gruppen-ID jeder Schnittstelle zugewiesen wird. Wenn Sie diesen Befehl auf beiden Routern eingeben, überprüfen sie, ob die Schnittstellenpaare im gleichen Subnetz zwischen den Geräten dieselbe RII-ID erhalten. Wenn sie nicht mit derselben eindeutigen RII-ID konfiguriert sind, replizieren Verbindungen zwischen den beiden Geräten nicht. Siehe Beispiel 6.

Beispiel 6: Bestätigung der Zuweisung der RII-Gruppen-ID

```
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
```

Überprüfen der Replizierung von Verbindungen mit dem Peer-Router

In Beispiel 7 leitet ZBFW1 den Datenverkehr für eine Verbindung aktiv weiter. Die Verbindung wird erfolgreich auf das Standby-Gerät ZBFW2 repliziert. Um die von der Zonenfirewall verarbeiteten Verbindungen anzuzeigen, verwenden Sie den Befehl **show policy-firewall session**.

Beispiel 7: Verarbeitete Verbindungen

```
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
```

Beachten Sie, dass die Verbindung repliziert, die übertragenen Bytes jedoch nicht aktualisiert werden. Der Verbindungsstatus (TCP-Informationen) wird regelmäßig über die Datenschnittstelle aktualisiert, um sicherzustellen, dass der Datenverkehr bei einem Failover-Ereignis nicht beeinträchtigt wird.

Geben Sie für eine genauere Ausgabe den Befehl **show policy-firewall session session zone-pair *<ZP>* ha ein**. Sie stellt eine ähnliche Ausgabe wie Beispiel 7 bereit, ermöglicht es dem Benutzer jedoch, die Ausgabe auf das angegebene Zonenpaar zu beschränken.

Erfassen der Debug-Ausgabe

In diesem Abschnitt werden die Debugbefehle veranschaulicht, die relevante Ausgaben zur Fehlerbehebung für dieses Feature liefern.

Die Aktivierung von Debuggen kann auf einem ausgelasteten Router sehr anstrengend sein. Daher sollten Sie die Auswirkungen verstehen, bevor Sie sie aktivieren.

- **debugredundante Application Group Ri-Ereignis**

  Dieser Befehl wird verwendet, um sicherzustellen, dass die Verbindungen der richtigen RII-Gruppe entsprechen, die repliziert werden soll. Wenn der Datenverkehr auf der ZBFW eingeht, werden die Quell- und Zielschnittstellen auf eine RII-Gruppen-ID überprüft. Diese Informationen werden dann über die Datenverbindung an den Peer weitergeleitet. Wenn die RII-Gruppe des Standby-Peers mit den aktiven Einheiten übereinstimmt, wird das Syslog in Beispiel 8 generiert und bestätigt die RII-Gruppen-IDs, die zur Replikation der Verbindung verwendet werden:

  Beispiel 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
  ```

- **Anwendungsgruppenprotokoll für Debug-Redundanz**

  Dieser Befehl wird verwendet, um zu bestätigen, dass die beiden Peers einander sehen können. Die Peer-IP-Adresse wird im Debuggen bestätigt. Wie in Beispiel 9 gezeigt, erkennt ZBFW1 seinen Peer im Standby-Zustand mit der IP-Adresse **10.60.1.2**. Umgekehrt gilt dies für ZBFW2.

Beispiel 9: Bestätigen von Peer-IPs in 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
```

Häufige Probleme

In diesem Abschnitt werden einige häufig auftretende Probleme beschrieben.

Auswahl von Steuerungs- und Datenschnittstellen

Hier einige Tipps für die Steuerungs- und Daten-VLANs:

- Schließen Sie die Steuerungs- und Datenschnittstellen nicht in die ZBFW-Konfiguration ein. Sie werden nur zur Kommunikation untereinander verwendet. Daher müssen diese Schnittstellen nicht gesichert werden.
- Die Steuerungs- und Datenschnittstellen können sich auf derselben Schnittstelle oder im VLAN befinden. Dadurch bleiben die Ports am Router erhalten.

Abwesende RII-Gruppe

Die RII-Gruppe muss sowohl an den LAN- als auch an den WAN-Schnittstellen angewendet werden. Die LAN-Schnittstellen müssen sich im gleichen Subnetz befinden, die WAN-Schnittstellen können sich jedoch in separaten Subnetzen befinden. Wenn eine RII-Gruppe auf einer Schnittstelle nicht vorhanden ist, tritt dieses Syslog in der Ausgabe des **Debug Redundancy Application Group rii-Ereignisses** und des **Debugging Redundancy Application Group RII-Fehlers auf**:

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

Automatischer Failover

Um ein automatisches Failover zu konfigurieren, muss die hohe Verfügbarkeit der ZBFW konfiguriert werden, um ein SLA-Objekt (Service Level Agreement) nachzuverfolgen und die Priorität basierend auf diesem SLA-Ereignis dynamisch zu verringern. In Beispiel 10 verfolgt ZBFW HA den Verbindungsstatus der **GigabitEthernet0-**Schnittstelle. Wenn diese Schnittstelle ausfällt, wird die Priorität so reduziert, dass das Peer-Gerät bevorzugt wird.

Beispiel 10: Automatische Failover-Konfiguration für 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
```

Manchmal führt die ZBFW-HA-Funktion kein automatisches Failover durch, auch wenn ein Ereignis mit reduzierter Priorität auftritt. Dies liegt daran, dass das **preempt-**Schlüsselwort nicht auf beiden Geräten konfiguriert ist. Das **Preempt**-Schlüsselwort hat andere Funktionen als das Hot Standby Router Protocol (HSRP)- oder Adaptive Security Appliance (ASA)-Failover. In ZBFW HA ermöglicht das **Preempt-**Schlüsselwort das Auftreten eines Failover-Ereignisses, wenn sich die Priorität des Geräts ändert. Dies ist im Sicherheitskonfigurationsleitfaden dokumentiert: Zonenbasierte Firewall, Cisco IOS-Version 15.2M&T. Hier ein Auszug aus dem Kapitel "Zonenbasierte Firewall - Hohe Verfügbarkeit":

"Unter anderen Umständen kann ein Switchover zum Standby-Gerät erfolgen. Ein weiterer Faktor, der zu einem Switchover führen kann, ist eine Prioritätseinstellung, die auf jedem Gerät konfiguriert werden kann. Das Gerät mit der höchsten Priorität ist das aktive Gerät. Tritt ein Fehler

auf dem aktiven Gerät oder dem Standby-Gerät auf, wird die Priorität des Geräts um einen konfigurierbaren Betrag, das Gewicht, reduziert. Wenn die Priorität des aktiven Geräts unter die Priorität des Standby-Geräts fällt, erfolgt ein Switchover, und das Standby-Gerät wird zum aktiven Gerät. Dieses Standardverhalten kann überschrieben werden, indem das Preemption-Attribut für die Redundanzgruppe deaktiviert wird. Sie können auch jede Schnittstelle so konfigurieren, dass die Priorität verringert wird, wenn der Layer-1-Status der Schnittstelle ausfällt. Die konfigurierte Priorität überschreibt die Standardpriorität einer Redundanzgruppe."

Diese Ausgaben weisen auf den richtigen Zustand hin:

```
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
```

Diese Protokolle werden auf der ZBFW generiert, ohne dass Debug aktiviert ist. Dieses Protokoll zeigt, wenn das Gerät aktiv wird:

```
*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
```

Dieses Protokoll zeigt, wenn das Gerät im Standby-Modus betrieben wird:

```
*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
```

Asymmetrisches Routing

Die Unterstützung für asymmetrisches Routing ist im Leitfaden zur Unterstützung von asymmetrischem Routing beschrieben.

Um asymmetrisches Routing zu konfigurieren, fügen Sie die Funktionen sowohl zur globalen Konfiguration der Redundanzanwendungsgruppe als auch zur Subkonfiguration der Schnittstelle hinzu. Es ist zu beachten, dass asymmetrisches Routing und ein RG nicht auf derselben Schnittstelle aktiviert werden können, da es nicht unterstützt wird. Dies liegt daran, wie asymmetrisches Routing funktioniert. Wenn eine Schnittstelle für asymmetrisches Routing bestimmt ist, kann sie zu diesem Zeitpunkt nicht Teil der HA-Verbindungsreplikation sein, da das Routing inkonsistent ist. Durch die Konfiguration eines RG wird der Router verwirrt, da ein RG angibt, dass eine Schnittstelle Teil der HA-Verbindungsreplikation ist.

Beispiel 11: Asymmetrische Routing-Konfiguration

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

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

Diese Konfiguration muss auf beide Router im HA-Paar angewendet werden.

Die zuvor aufgeführte **Ethernet0/3-**Schnittstelle ist eine neue dedizierte Verbindung zwischen den beiden Routern. Diese Verbindung wird ausschließlich verwendet, um asymmetrisch gerouteten Datenverkehr zwischen den beiden Routern zu übertragen. Daher sollte es sich um eine dedizierte Verbindung handeln, die der nach außen gerichteten Schnittstelle entspricht.

Zugehörige Informationen

- Leitfaden zur Sicherheitskonfiguration: Zonenbasierte Firewall, Cisco IOS Version 15.2M&T
- Konfigurationsleitfaden für Firewall mit hoher Verfügbarkeit für zonenbasierte Sicherheit
- Cisco IOS 15.2M&T
- Cisco IOS Firewall
- Problemhinweise zu Sicherheitsprodukten
- Technischer Support und Dokumentation für Cisco Systeme