ZBFW の高可用性設定およびトラブルシューティング テクニカルノート

目次

概要

このガイドはアクティブ/スタンバイ な セットアップ用のゾーン ファイアウォール 高可用性（HA）に基本設定に、また機能を見られるトラブルシューティング コマンドおよびよくある 問題与えます。

2 つの Cisco IOS ルータがアクティブ/スタンバイかアクティブで/アクティブなセットアップで設定することができるように Cisco IOS® ゾーン ベースのファイアウォール（ZBFW）は HA をサポートします。 これはシングル ポイント障害を防ぐことを冗長性が可能にします。

前提条件

要件

Cisco IOSソフトウェア Release15.2(3)T よりリリース 以降がなければなりません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

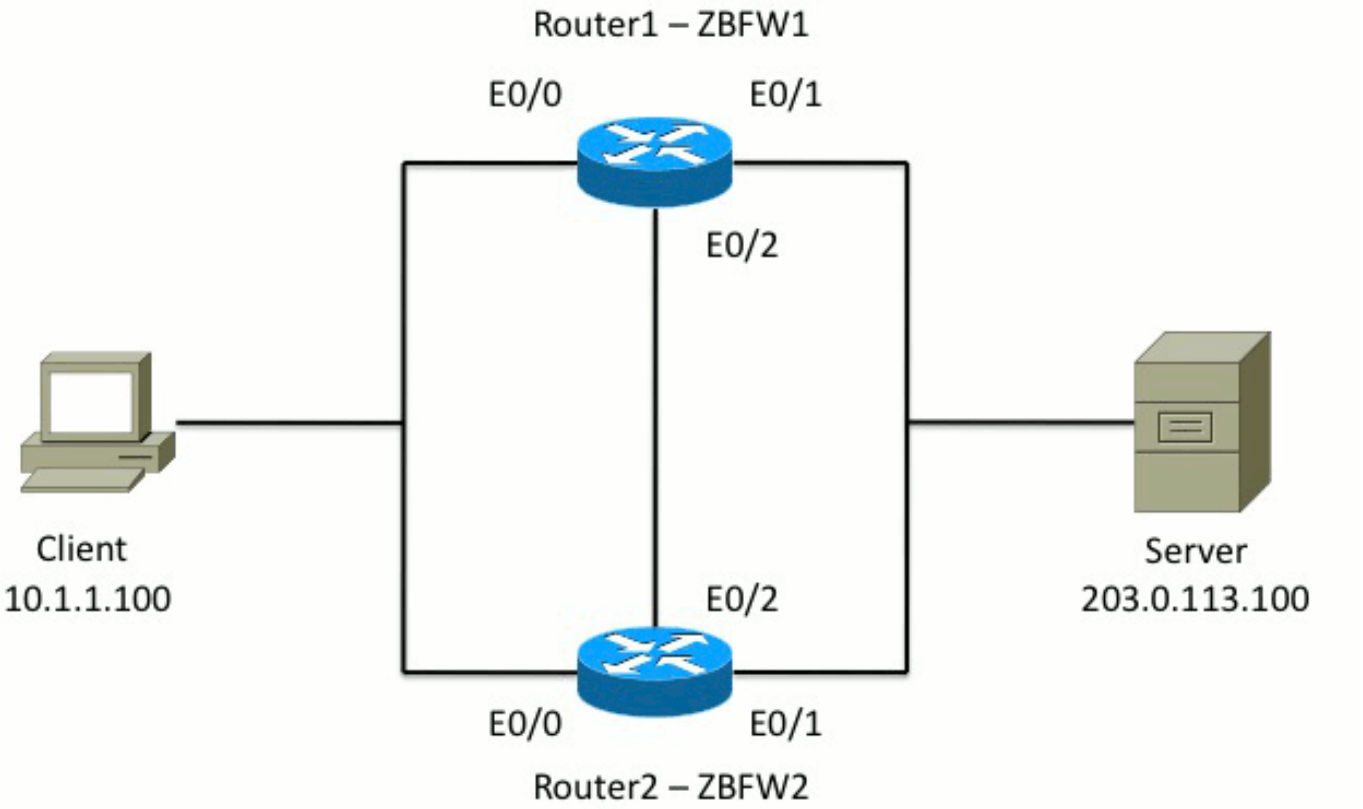
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

このダイアグラムは設定例で使用されるトポロジーを示します。



Example 1:示されている TCP、UDP およびインターネット制御メッセージ プロトコル（ICMP）トラフィックを内部から外部へ検査するために設定では ZBFW は設定されます。 太字で示されている設定は HA 機能を設定しました。 Cisco IOS ルータでは、HA は**冗長性** subconfig コマンドによって設定されます。 冗長性を設定するために、第一歩はグローバル な インスペクション パラメータ マップの冗長性を有効に することです。

冗長性を有効に した後、**アプリケーション 冗長性** subconfig を入力し、**制御**および**データ**のために使用するインターフェイスを選択して下さい。 制御 インタフェースは各ルータの状態についての情報を交換するために使用されます。 データインターフェイスは複製する必要がある接続についての情報を交換するために使用されます。

Example 2:ではルータ 1 にルータ 1 およびルータ両方 2 が正常に動作している場合ペアのアクティブユニットをする、**priority コマンドは**また設定 されます。 **preempt** コマンドは（またこの資料で更に説明されている）失敗が優先順位変更一度発生するようにするために使用されます。

最後の段階は各インターフェイスに**冗長なインターフェイス 識別子（RII）**および**冗長性グループ（RG）を**割り当てることです。 **RII** グループ番号は各インターフェイスのためにユニークでなければなりません同じ サブネットのインターフェイスのためのデバイスを渡って一致する必要があります。 RII はバルク同期化プロセスのために 2 人のルータが設定を同期するときだけ使用されます。 これは 2 人のルータが冗長なインターフェイスをどのように同期するかです。 **RG は**そのインターフェイスを通した接続が HA 接続テーブルに複製されることを示すために使用されます。

Example 2:では内部インターフェイスの Virtual IP（VIP）アドレスを作成するために、**冗長性グループ 1** コマンドは使用されます。 これはすべての内部ユーザがアクティブユニット プロセス VIP とだけ通信するので、HA を確認します。

これが WANインターフェイスであるので outside インターフェイスに RG 設定がありません。 ルータ 1 およびルータ両方 2 の outside インターフェイスは同じインターネットサービスプロバイダー（ISP）に属しません。 outside インターフェイスでトラフィックが正しいデバイスに通

じるようにするために、ダイナミック ルーティング プロトコルが必要となります。

例 1： ルータ 1 コンフィギュレーション の 断片（ホスト名 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
```

例 2： ルータ 2 コンフィギュレーション の 断片（ホスト名 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
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

デバイスが互いに交信を行うことができることを確認して下さい

デバイスが互いに会う場合があることを確認するために冗長性 アプリケ– ショングループのオペレーショナル ステートが稼働していることを確認して下さい。 それから各デバイスが正しいロールを果たしたし、正しいロールのピアを見る場合がありますように。 Example 3:では、ZBFW1 はアクティブで、スタンバイとしてピアを検出する。 これは ZBFW2 で反転します。 オペレーショナル ステートは稼働していることをデバイスが両方ともまた示し、ピア存在が検出するとき、2 人のルータは制御リンクを渡ってうまく交信できます。

例 3： ピア存在検出

```
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
```

出力は Example 4: 2 人のルータの制御 インタフェースについての粒状出力を示したものです。出力はコントロール トラフィックに使用する物理インターフェイスを確認しまたピアの IP アドレスを確認します。

例 4： 粒状出力

```
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
```

通信が確立されるとき、コマンドはの Example 5:各デバイスが特定の口ールになぜあるか理解するのを助けます。 ZBFW1 はピアより高優先順位があるのでアクティブです。 ZBFW2 に 150 の優先順位があるが、ZBFW1 に 200 の優先順位があります。 この出力は太字で強調表示されています。

例 5： ステータス ロールのおよび優先順位

```
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
```

最後の確認は RII グループ ID が各インターフェイスに割り当てられるようにすることです。 両方のルータのこのコマンドを入力する場合デバイス間の同じ サブネットのインターフェイス ペア同じ RII ID が割り当てられるようにするために、それらはダブルチェックします。 それらが同じユニークな RII ID で設定されない場合、接続は 2 つのデバイスの間で複製しません。 例 6」を参照してください。

例 6： RII グループ ID を割り当てられます確認して下さい

```
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
```

ピアルータにことを接続レプリケート確認して下さい

Example 7:では、ZBFW1 はアクティブに接続のためのトラフィックを通過させます。 スタンバイ デバイス ZBFW2 への接続は正常に複製されます。 ゾーン ファイアウォールによって処理された接続を表示するために**提示ポリシー ファイアウォール session コマンドを**使用します。

例 7： 処理される接続

```
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
```
接続レプリケート、転送されるバイトが更新済ではないがことに注意して下さい。 接続状態（TCP 情報）はデータインターフェイスを通してフェールオーバー イベントが発生する場合トラフィックが影響を受けていないことを確認するために定期的にアップデートされます。

粒状出力に関しては、**提示ポリシー ファイアウォール セッション ゾーン ペア *<ZP>* ha** コマンドを入力して下さい。 それは Example 7:として同じような出力を提供しますが、ユーザが規定 されるゾーン ペアだけに出力を制限することを可能にします。

収集する デバッグ 出力

このセクションはこの機能を解決するために関連した出力を生成 する debug コマンドを示します。

デバッグの enablement はビジー状態のルータで非常に精力的である場合もあります。 従ってそれらを有効に する前に、影響を理解するはずです。

- **デバッグ冗長性 アプリケーションググループ rii イベント**

  このコマンドは接続が正しい RII グループをきちんと複製されるべき一致することを確かめるために使用されます。 トラフィックが ZBFW に到着するとき、送信元および宛先 インターフェイスは RII グループ ID があるように確認されます。 この情報はピアへのデータリンクを渡ってそれから伝えられます。 スタンバイ ピアの RII グループがアクティブユニットと一直線に並ぶとき、syslog は Example 8:生成され、接続を複製するために使用する RII グループ ID を確認します:

  例 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
```

- **デバッグ冗長性 アプリケーションググループ プロトコルすべて**

  このコマンドは 2 同位が互いに会う場合があることを確認するために使用されます。 ピアIP アドレスはデバッグで確認されます。 Example 9:に見られるように、ZBFW1 は IP アドレス 10.60.1.2 との STANDBY 状態のピアを見ます。 反転は ZBFW2 にあてはまます。

  例 9： デバッグのピア IP を確認して下さい

```
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
```

一般的な問題

このセクションは見つけられるいくつかのよくある 問題を詳述します。

コントロールおよびデータインターフェイス選択

制御およびデータVLAN のためのいくつかの助言はここにあります:

- ZBFW 設定に制御およびデータインターフェイスを含めないで下さい。 彼らは互いに通信するためにただ使用されます; 従って、これらのインターフェイスを保護する必要がありません。
- 制御およびデータインターフェイスは同じインターフェイスか VLAN である場合もあります。 これはルータのポートを維持します。

不在 RII グループ

RII グループは LAN および WANインターフェイス両方で適用する必要があります。 LAN インターフェイスは同じ サブネットである必要があります WANインターフェイスは別個のサブネットである場合もあります。 インターフェイスで不在 RII グループがある場合この syslog は**デバッグ冗長性 アプリケ– ショングループ rii イベント**および**デバッグ冗長性 アプリケ– ショングループ rii エラー**の出力に発生します:

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

自動フェールオーバー

自動フェールオーバーを設定するために、ZBFW HA は Service Level Agreement (SLA; サービス レベル契約) オブジェクトをトラッキングするために設定する必要があり動的にこの SLA イベントに基づいて優先順位を減少させます。 Example 10:では、ZBFW HA は **GigabitEthernet0** インターフェイスのリンクステータスをトラッキングします。 このインターフェイスがダウン状態になる場合、優先順位はピアデバイスがより支持されてように減ります。

例 10： ZBFW HA 自動フェールオーバー設定

```
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
```

時々減少させた優先順位 イベントがあるのに ZBFW HA はフェールオーバー自動的に。 これは **preempt** キーワードが両方のデバイスの下で設定されないという理由によります。 **preempt** キーワードに Hot Standby Router Protocol （HSRP）でより別の機能性がまたは適応型セキュリティ アプライアンス（ASA）ソフトウェア（ASA）フェールオーバーあります。 ZBFW HA では、 **preempt** キーワードはデバイスの優先順位が変更する場合フェールオーバー イベントが発生するようにします。 これはセキュリティ構成ガイドで文書化されています: ゾーン ベースのポリシー ファイアウォール、Cisco IOS リリース 15.2M&T。 ゾーン ベースのポリシー ファイアウォール高可用性の章からの抽出はここにあります:

「スタンバイ デバイスへのスイッチオーバは他の状況のもとで行われる場合があります。 スイッチオーバを引き起こす場合があるもう一つのファクタは各デバイスで行うことができるプライオリティ設定です。 高優先順位値のデバイスはアクティブデバイスです。 エラーがアクティブなかスタンバイ デバイスに発生する場合、デバイスの優先順位は重量として知られている設定可能な量減少されます。 アクティブデバイスの優先順位がスタンバイ デバイスの優先順位の下で下る場合、スイッチオーバは行われ、スタンバイ デバイスはアクティブデバイスになります。 このデフォルトの動作は冗長性グループのためのプリエンプション アトリビュートをディセーブルにすることによって無効にすることができます。 インターフェイスのレイヤ1 状態がダウン状態になるときまた優先順位を減少させるために各インターフェイスを設定できます。 設定される優先順位は無効にします冗長性グループのデフォルトプライオリティを」。

これらの出力は適切な状態を示します:

```
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
```
これらの口グは有効に なるデバッグなしで ZBFW で生成されます。 この口グはデバイスがアクティブになると示します:

```
*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
```
この口グはデバイスがスタンバイで行くと示します:

```
*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
```

非対称ルーティング

非対称 ルーティング サポートは非対称 ルーティング サポート ガイドで outined。

非対称 ルーティングを設定するために、冗長性 アプリケ– ショングループ グローバルコンフィギュレーションおよびインターフェイス副設定両方に機能を追加して下さい。 その非対称 ルーティングに注意することは重要であり、RG は同じインターフェイスでサポートされないので有効に することができません。 これは非対称 ルーティングがどのようにがはたらくか原因です。 インターフェイスは非対称 ルーティングのために指定されるとき、ルーティングが矛盾しているので HA 接続複製のその時一部である場合もありません。 RG を設定することはインターフェイスは HA 接続複製の一部であること RG が規定 するので、ルータを混同します。

例 11： 非対称 ルーティング 設定

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

interface Ethernet0/1
redundancy asymmetric-routing enable
```
この設定は HA ペアの両方のルータで適用する必要があります。

以前にリストされている Ethernet0/3 インターフェイスは 2 人のルータ間の新しい専用 リンクです。 このリンクは 2 人のルータの間で非対称的経路選択済み トラフィックを通過させるために特に使用されます。 こういうわけでそれは外部に直面インターフェイスと同等の専用 リンクであるはずです。

関連情報

- セキュリティの設定ガイド： ゾーン ベースのポリシー ファイアウォール、Cisco IOS リリース 15.2M&T
- セキュリティ構成ガイド ゾーン ベースのポリシー ファイアウォール 高可用性の
- Cisco IOS 15.2M&T
- Cisco IOS ファイアウォール
- セキュリティ製品フィールド通知
- テクニカルサポートとドキュメント - Cisco Systems