ZBFWハイアベイラビリティの設定とトラブルシューティング

内容

概要

このガイドでは、アクティブ/スタンバイ設定のゾーンファイアウォールのハイアベイラビリティ(HA)の基本設定、およびトラブルシューティングコマンドと、この機能に関する一般的な問題について説明します。

Cisco IOS® ゾーンベースファイアウォール(ZBFW)はHAをサポートしているため、2台のCisco IOSルータをアクティブ/スタンバイまたはアクティブ/アクティブの設定で設定できます。これにより、シングルポイント障害を防ぐために冗長性が確保されます。

前提条件

要件

Cisco IOSソフトウェアリリース15.2(3)Tよりも後のリリースが必要です。

使用するコンポーネント

このドキュメントの内容は、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。

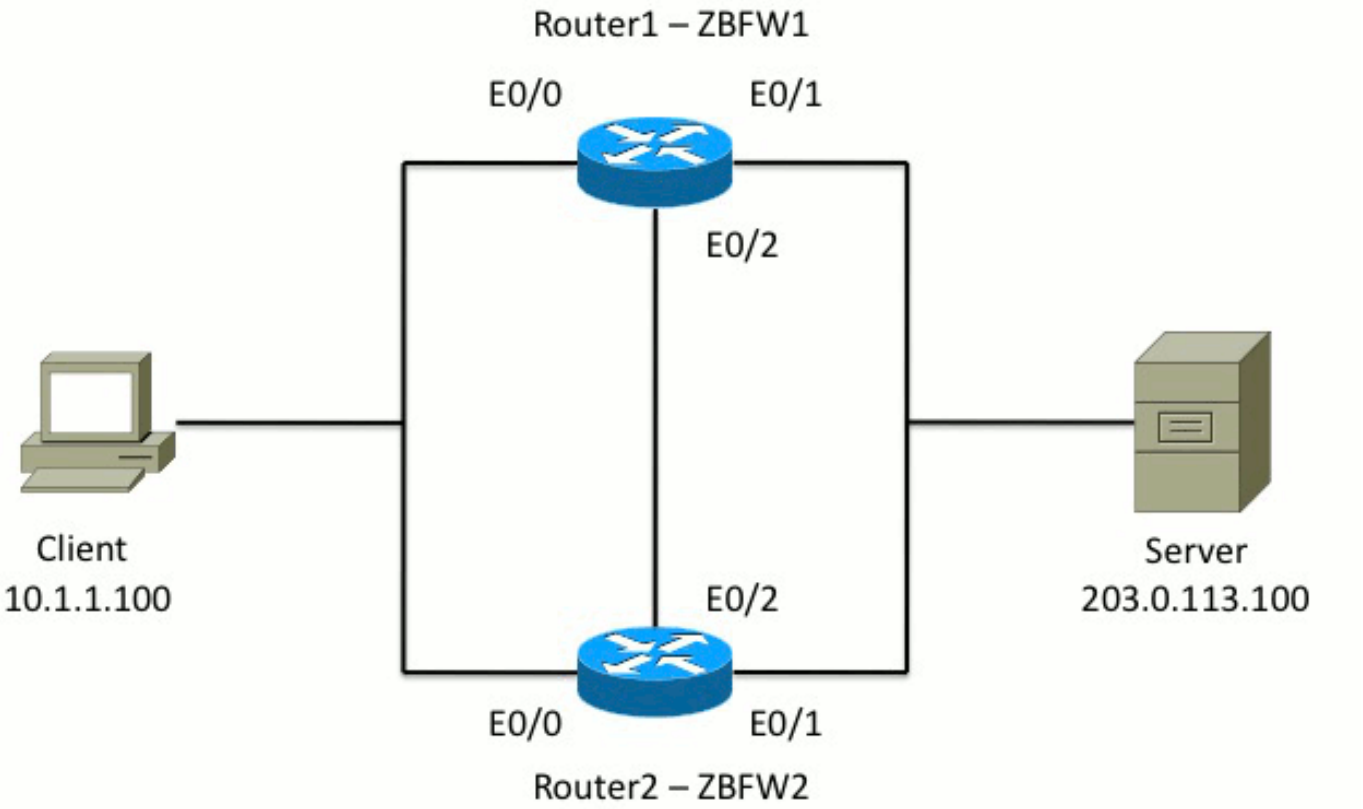
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

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

次の図は、設定例で使用されているトポロジを示しています。



例1に示す設定では、内部から外部への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)トラフィックを検査するために、ZBFWが設定されています。太字で示されている設定は、HA機能を設定します。Cisco IOSルータでは、**redundancy** subconfigコマンドを使用してHAが設定されています。冗長性を設定するための最初のステップは、グローバルインスペクションパラメータマップで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**の冗長性**サブコンフィギュレーションを入力し、制御およびデータに使用されるイ**ンターフ**ェイスを**選択します**。コントロールインターフェイスは、各ルータの状態に関する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関する情報を交換するために使用されます。

例2では、ルータ1とルータ2の両方が動作している場合、ルータ1をペアのアクティブユニットにするために**priority**コマンドも設定されています。**preempt**コマンド（このドキュメントで詳しく説明されています）は、プライオリティが変更された後に障害が発生することを確認するために使用します。

最後のステップは、冗長インターフ**ェイス(RII)と冗長グル**ープ(RG)**を各インターフ**ェイスに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で一意である必要がありますが、同じサブネット内のインターフェイスのデバイス間で一致する必要があります。RIIは、2台のルータが設定を同期する場合にのみ、一括同期プロセスに使用されます。これは、2台のルータが冗長インターフェイスを同期する方法です。**RG**は、そのインターフェイスを介した接続が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。

例2では、**redundancy group 1**コマンドを使用して仮想IP(VIP)アドレスを内部インターフェイスに作成します。これは、すべての内部ユーザがアクティブユニットが処理するVIPとだけ通信するため、HAを保証します。

これはWANインターフェイスであるため、外部インターフェイスにはRG設定がありません。ルータ1とルータ2の外部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)に属していません。 外部インターフェイスでは、トラフィックが正しいデバイスに確実に渡されるよ

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です。

例 1：ルータ1の設定のスニペット（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の設定のスニペット（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
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

デバイスが相互に通信できることを確認する

デバイスが互いを認識できることを確認するには、冗長アプリケーショングループの動作状態がupであることを確認する必要があります。次に、各デバイスが正しい役割を果たし、ピアが正しい役割を果たしていることを確認します。例3では、ZBFW1がアクティブで、そのピアがスタンバイとして検出されます。これはZBFW2では逆になります。両方のデバイスで動作状態がアップ状態で、ピアの存在が検出された場合、2台のルータは制御リンクを介して正常に通信できます。

例 3：ピアプレゼンス検出

```
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
```

例4の出力は、2台のルータの制御インターフェイスに関するより詳細な出力を示しています。出力は、制御トラフィックに使用される物理インターフェイスを確認し、ピアのIPアドレスも確認します。

例 4：きめ細かな出力

```
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、例5のコマンドは、各デバイスが特定の役割を果たす理由を理解するのに役立ちます。ZBFW1は、ピアよりも高いプライオリティを持つため、アクティブです。ZBFW1の優先度は200、ZBFW2の優先度は**150**です。この出力は太字で強調表示**されています**。

例 5：ロールステータスと優先度

```
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
```

最後に、RIIグループIDが各インターフェイスに割り当てられていることを確認します。両方のルータでこのコマンドを入力した場合、デバイス間の同じサブネット上のインターフェイスペアに同じRII IDが割り当てられていることを確認するために、二重チェックが行われます。同じ一意のRII IDで設定されていない場合、2つのデバイス間で接続が複製されません。例 6」を参照してください。

例 6：RIIグループIDが割り当てられていることを確認

```
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
```

ピアルータへの接続が複製されることを確認する

例7では、ZBFW1は接続のトラフィックをアクティブに渡します。接続はスタンバイデバイスZBFW2に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には、show policy-firewall sessionコマンドを使用します。

例 7：処理された接続

```
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
```

接続は複製されますが、転送されたバイトは更新されません。接続状態（TCP情報）は、データインターフェイスを通じて定期的に更新され、フェールオーバーイベントが発生してもトラフィックが影響を受けないようにします。

より詳細な出力を得るには、**show policy-firewall session zone-pair *<ZP>* haコマンドを入力します**。例7と同様の出力を提供しますが、ユーザは指定されたゾーンペアだけに出力を制限できます。

デバッグ出力の収集

このセクションでは、この機能のトラブルシューティングに関連する出力を生成するdebugコマンドを示します。

ビジー状態のルータでデバッグを有効にすることは非常に困難です。したがって、有効にする前に影響を理解しておく必要があります。

- debug redundancy application group rii event

  このコマンドは、接続が正しく複製される正しいRIIグループと一致することを確認するために使用されます。トラフィックがZBFWに到達すると、送信元インターフェイスと宛先インターフェイスでRIIグループIDがチェックされます。この情報は、データリンクを介してピアに伝達されます。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致すると、例8のsyslogが生成され、接続を複製するために使用されるRIIグループIDが確認されます。

  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
  ```

- debug redundancy application group protocol all

  このコマンドは、2つのピアが相互に認識できることを確認するために使用されます。ピアのIPアドレスはデバッグで確認されます。例9に示すように、ZBFW1はIPアドレス**10.60.1.2を持つスタンバイ状態のピアを認識します**。逆はZBFW2に当てはまります。

  例 9：デバッグのピアIPの確認

```
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

このセクションでは、発生する一般的な問題について詳しく説明します。

制御およびデータインターフェイスの選択

コントロールVLANとデータVLANのヒントを次に示します。

- ZBFW設定にコントロールインターフェイスとデータインターフェイスを含めないでください。これらは相互に通信するためにのみ使用されます。したがって、これらのインターフェイスを保護する必要はありません。
- コントロールインターフェイスとデータインターフェイスは、同じインターフェイスまたはVLAN上に配置できます。これにより、ルータのポートが保持されます。

不在RIIグループ

RIIグループは、LANインターフェイスとWANインターフェイスの両方に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上にある必要がありますが、WANインターフェイスは別々のサブネット上に配置できます。インターフェイスにRIIグループがない場合、**debug redundancy application group rii eventおよびdebug redundancy application group rii errorの出力に次のsyslogが表示されます。**

```
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には、サービスレベル契約(SLA)オブジェクトを追跡し、このSLAイベントに基づいて動的に優先順位を下げるようにZBFW HAを設定する必要があります。例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**追跡し**ます。このインターフェイスがダウンすると、プライオリティが下がり、ピアデバイスがより有利になります。

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
```

ZBFW HAは、優先順位が低下したイベントがあっても、自動的にフェールオーバーしないことがあります。これは、**preempt**キーワードが両方のデバイスで設定されていないためです。**preempt**キーワードは、ホットスタンバイルータプロトコル(HSRP)または適応型セキュリティアプライアンス(ASA)のフェールオーバーとは異なる機能を備えています。ZBFW HAでは、**preempt**キーワードを使用すると、デバイスの優先度が変更された場合にフェールオーバーイベントを発生させることができます。この問題については、『Security Configuration Guide:ゾーンベースポリシーファイアウォール、Cisco IOSリリース15.2M&T。「ゾーンベースポリシーファイアウォールのハイアベイラビリティ」の章からの抜粋を次に示します。

「他の状況では、スタンバイデバイスへのスイッチオーバーが発生する可能性があります。スイッチオーバーを引き起こす可能性があるもう1つの要因は、各デバイスで設定可能なプライオリティ設定です。最も高いプライオリティ値を持つデバイスがアクティブデバイスになります。アクティブまたはスタンバイデバイスで障害が発生すると、デバイスの優先順位が設定可能な量（重み）だけ下げられます。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を下回ると、スイッチオーバーが発生し、スタンバイデバイスが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、冗長グループのプリエンプション属性を無効にすることで上書きできます。また、インターフェイスのレイヤ1状態がダウンしたときにプライオリティを下げるように各インターフェイスを設定することもできます。設定されたプライオリティは、冗長グループのデフォルトのプライオリティよりも優先されます。

次の出力は、適切な状態を示しています。

```
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
```

これらのログは、デバッグを有効にせずにZBFWで生成されます。デバイスがアクティブになると、次のログが表示されます。

```
*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
```

次のログは、デバイスがスタンバイ状態になるタイミングを示しています。

```
*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のサポートについては、『非対称ルーティングサポートガイド』を参照してください。

非対称ルーティングを設定するには、冗長アプリケーショングループのグローバル設定とインターフェイスサブ設定の両方に機能を追加します。非対称ルーティングとRGはサポートされていないため、同じインターフェイスでは有効にできないことに注意してください。これは、非対称ルーティングの仕組みによるものです。インターフェイスが非対称ルーティングに指定されている場合、その時点でHA接続レプリケーションの一部になることはできません。これは、ルーティングが一貫性がないためです。RGを設定すると、インターフェイスがHA接続レプリケーションの一部であることがRGによって指定されるため、ルータが混乱します。

例 11：非対称ルーティングの設定

```
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に適用する必要があります。

上記のEthernet0/3インターフェイスは、2台のルータ間の新しい専用リンクです。このリンクは、非対称にルーティングされたトラフィックを2台のルータ間で通過させるために排他的に使用されます。このため、外部インターフェイスと同等の専用リンクを使用する必要があります。

関連情報

- セキュリティの設定ガイド：ゾーンベースポリシーファイアウォール、Cisco IOSリリース15.2M&T
- ゾーンベースポリシーファイアウォールハイアベイラビリティセキュリティ設定ガイド
- Cisco IOS 15.2M&T
- Cisco IOS ファイアウォール
- セキュリティ製品に関するField Notice
- テクニカル サポートとドキュメント – Cisco Systems