

# 為思科路由器上的IKEv2路由隧道配置HSRP的IPsec冗餘

## 目錄

---

### [簡介](#)

### [必要條件](#)

[需求](#)

[採用元件](#)

### [設定](#)

[網路圖表](#)

[主要/次要路由器配置](#)

[使用HSRP配置物理介面](#)

[配置IKEv2提議和策略](#)

[配置金鑰環](#)

[配置IKEv2配置檔案](#)

[配置IPsec轉換集](#)

[配置IPSec配置檔案](#)

[配置虛擬隧道介面](#)

[配置動態和/或靜態路由](#)

[對等路由器配置](#)

[配置IKEv2提議和策略](#)

[配置金鑰環](#)

[配置IKEv2配置檔案](#)

[配置IPsec轉換集](#)

[配置IPSec配置檔案](#)

[配置虛擬隧道介面](#)

[配置動態和/或靜態路由](#)

### [驗證](#)

[案例 1.主路由器和輔助路由器都處於活動狀態](#)

[案例 2.主路由器處於非活動狀態，輔助路由器處於活動狀態](#)

[案例 3.主路由器恢復運行，輔助路由器進入待機狀態](#)

### [疑難排解](#)

---

## 簡介

本文檔介紹如何使用HSRP為思科路由器上的IKEv2基於路由的隧道配置IPsec冗餘。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 站點到站點VPN
- 熱待命路由器通訊協定[HSRP]
- IPsec和IKEv2的基礎知識

## 採用元件

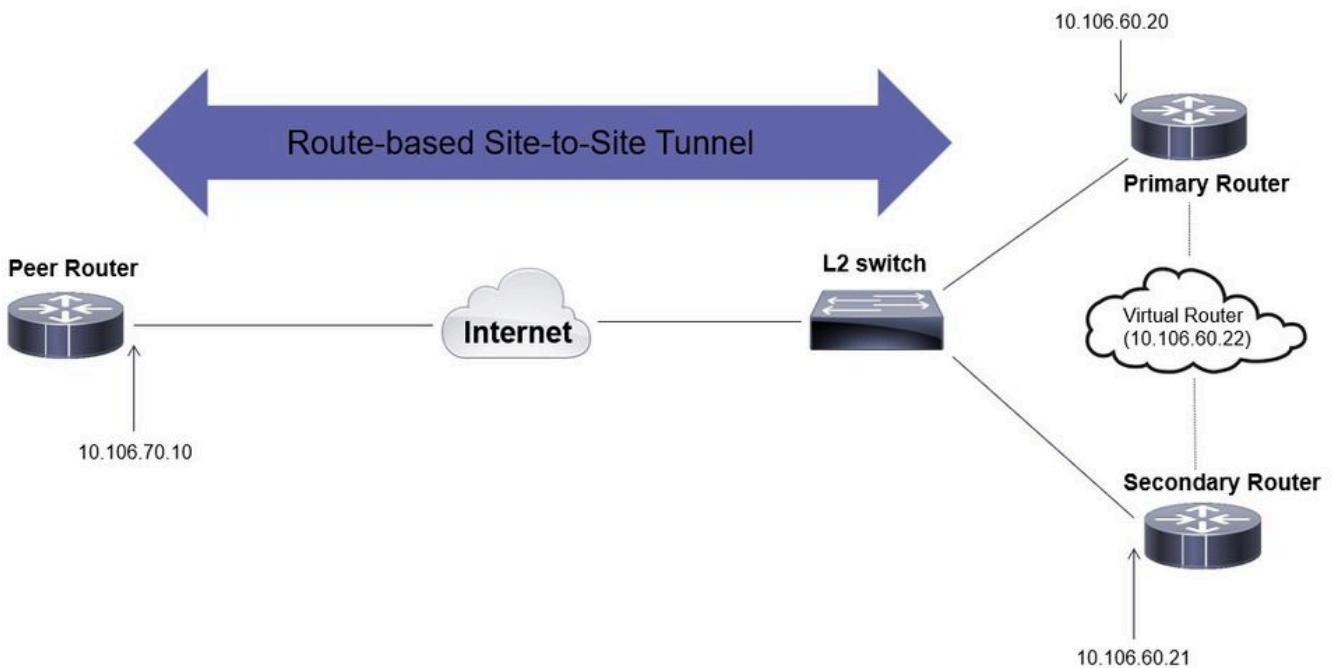
本文中的資訊係根據以下軟體和硬體版本：

- 運行IOS XE軟體 ( 版本17.03.08a ) 的思科CSR1000v路由器
- 運行Cisco IOS軟體 ( 版本15.2 ) 的第2層交換機

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 設定

### 網路圖表



### 主要/次要路由器配置

#### 使用HSRP配置物理介面

配置主要路由器 ( 優先順序較高 ) 和輔助路由器 ( 預設優先順序為100 ) 的物理介面：

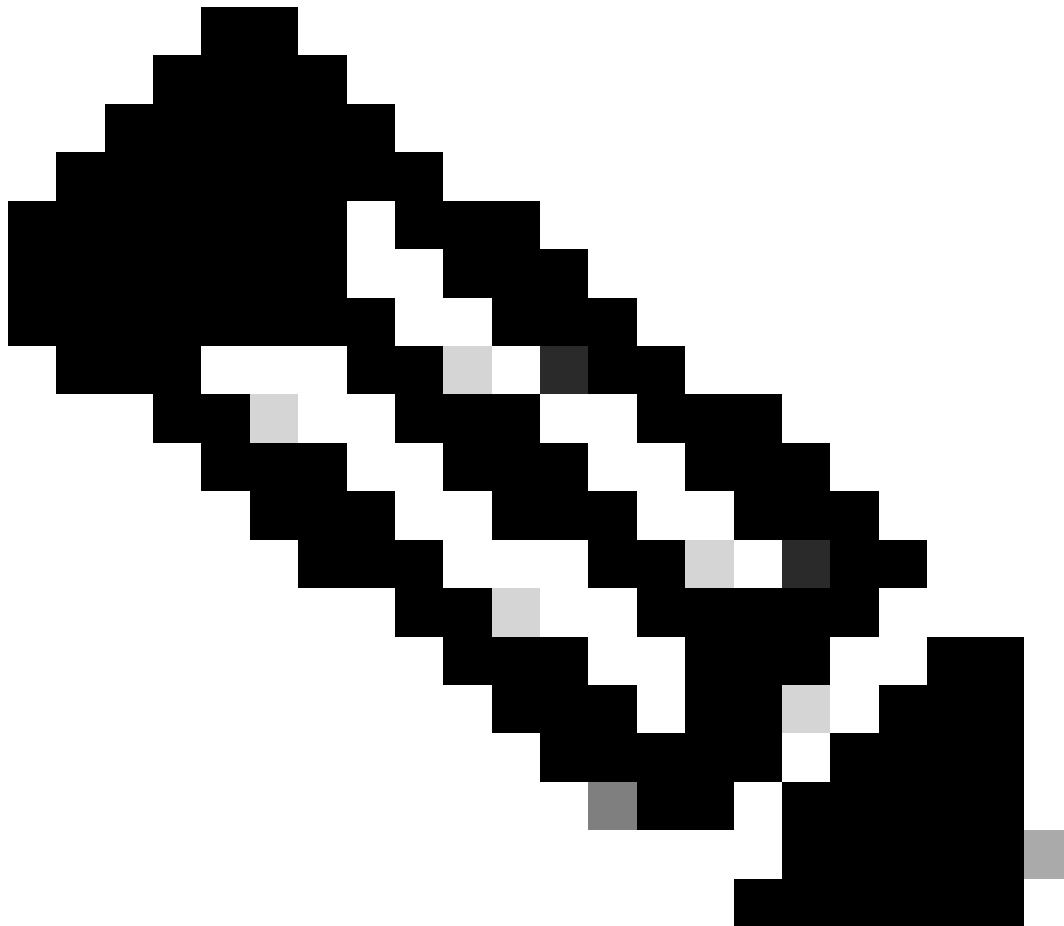
主要路由器：

```
interface GigabitEthernet1 ip address 10.106.60.20 255.255.255.0 standby 1 ip 10.106.60.22 standby 1 priority 105 standby 1 preempt standby 1 name VPN
```

輔助路由器：

```
interface GigabitEthernet1 ip address 10.106.60.21 255.255.255.0 standby 1 ip 10.106.60.22 standby 1 preempt standby 1 name VPN-HSRP
```

---



註：確保為預設主路由器配置了更高的優先順序，以使該路由器成為活動對等體，即使兩個路由器都已啟動並正常運行，且沒有任何問題。在本示例中，主路由器的優先順序配置為105，而輔助路由器的優先順序配置為100（這是HSRP的預設設定）。

---

## 配置IKEv2提議和策略

使用您選擇的加密、雜湊和DH組配置IKEv2提議，並將其對映到IKEv2策略。

```
crypto ikev2 proposal prop-1
  encryption aes-cbc-256
  integrity sha256
  group 14

crypto ikev2 policy IKEv2_POL
  proposal prop-1
```

## 配置金鑰環

配置金鑰環以儲存用於驗證對等體的預共用金鑰。

```
crypto ikev2 keyring keys
  peer 10.106.70.10
  address 10.106.70.10
  pre-shared-key local C!sco123
  pre-shared-key remote C!sco123
```

## 配置IKEv2配置檔案

配置IKEv2配置檔案並將金鑰環附加到該配置檔案。將本地地址設定為用於HSRP的虛擬IP地址，並將遠端地址設定為路由器面向Internet介面的IP。

```
crypto ikev2 profile IKEv2_PROF
  match identity remote address 10.106.70.10 255.255.255.255
  identity local address 10.106.60.22
  authentication remote pre-share
  authentication local pre-share
  keyring local keys
```

## 配置IPsec轉換集

使用IPSec轉換集配置加密和雜湊的第2階段引數。

```
crypto ipsec transform-set ipsec-prop esp-aes 256 esp-sha256-hmac
```

## 配置IPSec配置檔案

配置IPSec配置檔案以對映IKEv2配置檔案和IPSec轉換集。IPSec配置檔案將應用到隧道介面。

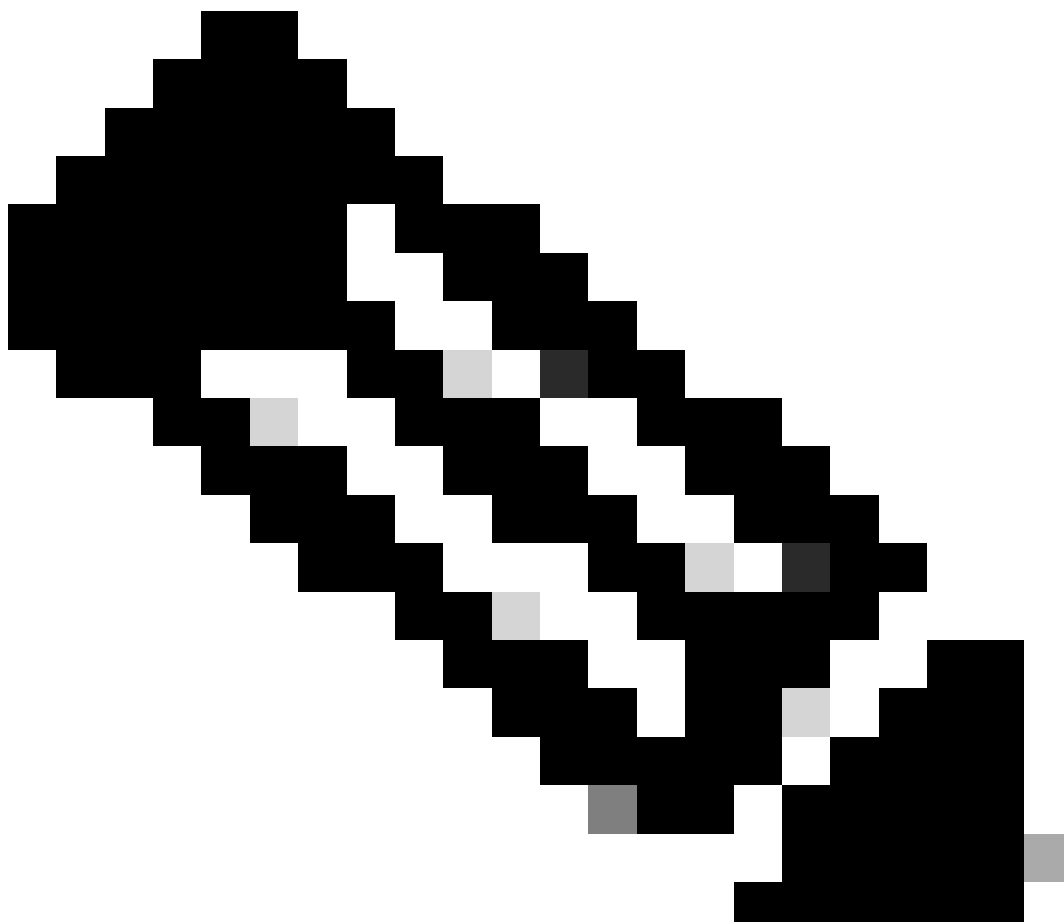
```
crypto ipsec profile IPsec_PROF
  set transform-set ipsec-prop
  set ikev2-profile IKEv2_PROF
```

## 配置虛擬隧道介面

配置虛擬隧道介面以指定隧道源和目標。這些IP將用於加密隧道上的流量。確保IPSec配置檔案也應用於此介面，如下所示。

```
interface Tunnel0
  ip address 10.10.10.10 255.255.255.0
  tunnel source 10.106.60.22
  tunnel mode ipsec ipv4
  tunnel destination 10.106.70.10
  tunnel protection ipsec profile IPsec_PROF
```

---



注意：您需要指定用於HSRP的虛擬IP作為隧道源。使用物理介面（在本場景中為GigabitEthernet1）將導致隧道協商失敗。

---

## 配置動態和/或靜態路由

根據要求和網路設計，您必須使用動態路由協定和/或靜態路由配置路由。在本示例中，結合使用EIGRP和靜態路由，透過站點到站點隧道建立底層通訊和重疊資料流量流。

```
router eigrp 10
 network 10.10.10.0 0.0.0.255
 network 10.106.60.0 0.0.0.255

ip route 192.168.30.0 255.255.255.0 Tunne10
```

---

注意：請確保通告隧道介面子網(在本場景中為10.10.10.0/24)。

---

## 對等路由器配置

### 配置IKEv2提議和策略

使用您選擇的加密、雜湊和DH組配置IKEv2提議，並將其對映到IKEv2策略。

```
crypto ikev2 proposal prop-1
  encryption aes-cbc-256
  integrity sha256
  group 14
```

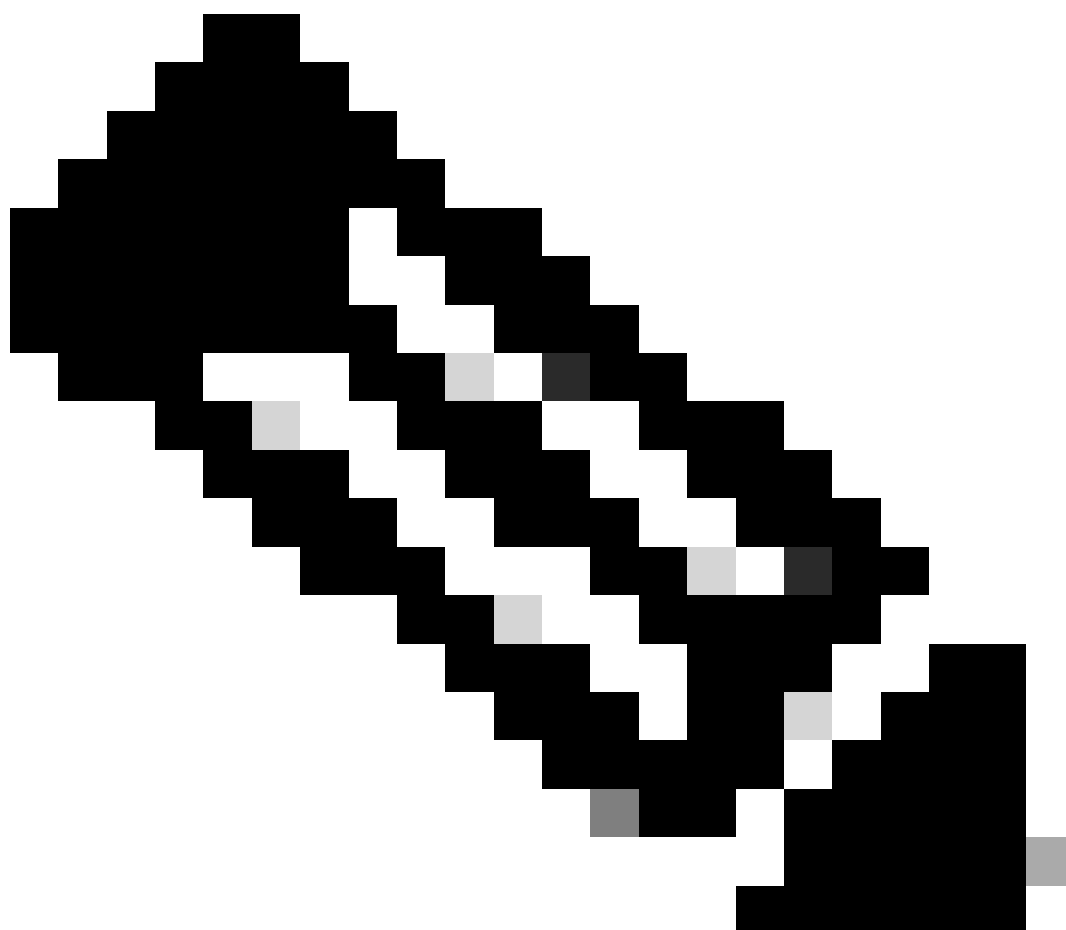
```
crypto ikev2 policy IKEv2_POL
  proposal prop-1
```

## 配置金鑰環

配置金鑰環以儲存用於驗證對等體的預共用金鑰。

```
crypto ikev2 keyring keys
peer 10.106.60.22
address 10.106.60.22
pre-shared-key local C!sco123
pre-shared-key remote C!sco123
```

---



注意：此處使用的對等體IP地址將是在對等體的HSRP配置中配置的虛擬IP地址。確保您未為主要/輔助對等體的物理介面IP配置金鑰環。

---



## 配置IKEv2配置檔案

配置IKEv2配置檔案並將金鑰環附加到該配置檔案。將本地地址設定為路由器面向網際網路介面的IP，將遠端地址設定為主/輔助對等體上用於HSRP的虛擬IP地址。

```
crypto ikev2 profile IKEv2_PROF
 match identity remote address 10.106.60.22 255.255.255.255
 identity local address 10.106.70.10
 authentication remote pre-share
 authentication local pre-share
 keyring local keys
```

## 配置IPsec轉換集

使用IPsec轉換集配置加密和雜湊的第2階段引數。

```
crypto ipsec transform-set ipsec-prop esp-aes 256 esp-sha256-hmac
```

## 配置IPsec配置檔案

配置IPsec配置檔案以對映IKEv2配置檔案和IPsec轉換集。IPsec配置檔案將應用到隧道介面。

```
crypto ipsec profile IPsec_PROF
 set transform-set ipsec-prop
 set ikev2-profile IKEv2_PROF
```

## 配置虛擬隧道介面

配置虛擬隧道介面以指定隧道源和目標。必須將隧道目標設定為主/輔助對等體上用於HSRP的虛擬IP。確保IPsec配置檔案也已應用於此介面，如下所示。

```
interface Tunnel0
 ip address 10.10.10.11 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 10.106.60.22
 tunnel protection ipsec profile IPsec_PROF
```

## 配置動態和/或靜態路由

使用動態路由協定或靜態路由配置所需的路由，就像您為其他終端配置路由一樣。

```
router eigrp 10
network 10.10.10.0 0.0.0.255
network 10.106.70.0 0.0.0.255

ip route 192.168.10.0 255.255.255.0 Tunnel0
```

## 驗證

為了瞭解預期行為，以下三種情況會出現。

### 案例 1.主路由器和輔助路由器都處於活動狀態

由於主路由器配置了更高的優先順序，因此會在此路由器上協商並建立IPSec隧道。要檢驗兩台路由器的狀態，您可以使用show standby命令。

```
<#root>
```

```
pri-router#show standby
GigabitEthernet1 - Group 1
```

```
State is Active
```

```
7 state changes, last state change 00:00:21
Virtual IP address is 10.106.60.22
Active virtual MAC address is 0000.0c07.ac01 (MAC In Use)
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.864 secs
Preemption enabled
```

```
Active router is local
```

```
standby router is 10.106.60.21, priority 100 (expires in 9.872 sec)
```

```
Priority 105 (configured 105)
Group name is "VPN-HSRP" (cfgd)
FLAGS: 1/1
```

```
sec-router#show standby
GigabitEthernet1 - Group 1
```

```
State is Standby
```

```
11 state changes, last state change 00:00:49
Virtual IP address is 10.106.60.22
Active virtual MAC address is 0000.0c07.ac01 (MAC Not In Use)
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.888 secs
Preemption enabled

Active router is 10.106.60.20, priority 105 (expires in 8.768 sec)
```

```
Standby router is local
```

```
Priority 100 (default 100)
Group name is "VPN-HSRP" (cfgd)
FLAGS: 0/1
```

要驗證隧道的第1階段(IKEv2)和第2階段(IPsec)安全關聯，您可以使用show crypto ikev2 sa和show crypto ipsec sa命令。

```
pri-router#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA
```

```
Tunnel-id          Local          Remote          fvrf/ivrf      Status
1                  10.106.60.22/500 10.106.70.10/500 none/none      READY
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify:
Life/Active Time: 86400/444 sec
```

```
IPv6 Crypto IKEv2 SA
```

```
pri-router#show crypto ipsec sa
```

```
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.106.60.22

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 10.106.70.10 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 36357, #pkts encrypt: 36357, #pkts digest: 36357
#pkts decaps: 36354, #pkts decrypt: 36354, #pkts verify: 36354
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.106.60.22, remote crypto endpt.: 10.106.70.10
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0x4967630D(1231512333)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xBA711B5E(3127974750)
transform: esp-256-aes esp-sha256-hmac ,
in use settings = {Tunnel, }
```

```
conn id: 2216, flow_id: CSR:216, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4607986/3022)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

inbound ah sas:

inbound pcp sas:

```
outbound esp sas:
spi: 0x4967630D(1231512333)
transform: esp-256-aes esp-sha256-hmac ,
in use settings ={Tunnel, }
conn id: 2215, flow_id: CSR:215, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4607992/3022)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

outbound ah sas:

outbound pcp sas:

## 案例 2.主路由器處於非活動狀態，輔助路由器處於活動狀態

在主要路由器發生故障或關閉的情況下，次要路由器會成為使用中路由器，且會與此路由器交涉站台對站台通道。

可以使用show standby 命令再次驗證輔助路由器的HSRP狀態。

```
<#root>
```

```
sec-router#show standby
GigabitEthernet1 - Group 1
```

**State is Active**

```
12 state changes, last state change 00:00:37
Virtual IP address is 10.106.60.22
Active virtual MAC address is 0000.0c07.ac01 (MAC In Use)
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.208 secs
Preemption enabled
```

```
Active router is local
```

```
Standby router is unknown  
Priority 100 (default 100)  
Group name is "VPN-HSRP" (cfgd)  
FLAGS: 1/1
```

此外，當此中斷發生時，您還將觀察以下日誌。這些日誌還顯示輔助路由器現在處於活動狀態，並且已建立隧道。

```
*Jul 18 10:28:21.881: %HSRP-5-STATECHANGE: GigabitEthernet1 Grp 1 state Standby -> Active  
*Jul 18 10:28:44.647: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
```

若要檢查階段1和階段2的安全關聯，您可以再次使用show crypto ikev2 sa和show crypto ipsec sa，如下所示。

```
sec-router#show crypto ikev2 sa  
IPv4 Crypto IKEv2 SA
```

```
Tunnel-id Local Remote fvrf/ivrf Status  
1 10.106.60.22/500 10.106.70.10/500 none/none READY  
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK  
Life/Active Time: 86400/480 sec
```

```
IPv6 Crypto IKEv2 SA
```

```
sec-router# show crypto ipsec sa
```

```
interface: Tunnel0  
Crypto map tag: Tunnel0-head-0, local addr 10.106.60.22
```

```
protected vrf: (none)  
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
current_peer 10.106.70.10 port 500  
PERMIT, flags={origin_is_acl,}  
#pkts encaps: 112, #pkts encrypt: 112, #pkts digest: 112  
#pkts decaps: 112, #pkts decrypt: 112, #pkts verify: 112  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 0, #pkts compr. failed: 0  
#pkts not decompressed: 0, #pkts decompress failed: 0  
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 10.106.60.22, remote crypto endpt.: 10.106.70.10  
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1  
current outbound spi: 0xFC4207BF(4232185791)  
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
```

spi: 0x5F6EE796(1601103766)  
transform: esp-256-aes esp-sha256-hmac ,  
in use settings ={Tunnel, }  
conn id: 2170, flow\_id: CSR:170, sibling\_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0  
sa timing: remaining key lifetime (k/sec): (4607988/3107)  
IV size: 16 bytes  
replay detection support: Y  
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:  
spi: 0xFC4207BF(4232185791)  
transform: esp-256-aes esp-sha256-hmac ,  
in use settings ={Tunnel, }  
conn id: 2169, flow\_id: CSR:169, sibling\_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0  
sa timing: remaining key lifetime (k/sec): (4607993/3107)  
IV size: 16 bytes  
replay detection support: Y  
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

### 案例 3.主路由器恢復運行，輔助路由器進入待機狀態

一旦主路由器恢復且不再關閉，它將再次成為活動路由器，因為它配置了更高的優先順序，並且輔助路由器進入備用模式。

在此場景中，當發生此轉換時，您會在主要和輔助路由器上看到這些日誌。

在主要路由器上，將顯示以下日誌：

```
*Jul 18 11:47:46.590: %HSRP-5-STATECHANGE: GigabitEthernet1 Grp 1 state Listen -> Active  
*Jul 18 11:48:07.945: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
```

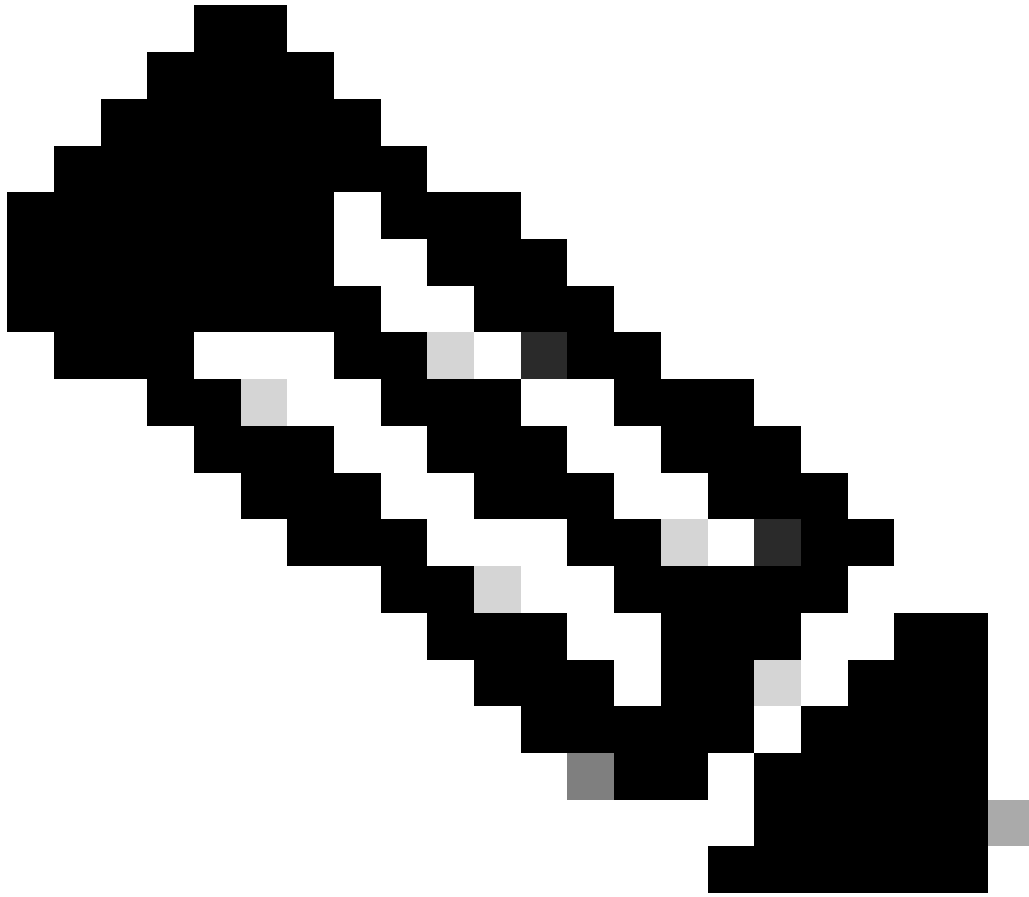
在輔助路由器上，您會看到這些日誌，它們顯示輔助路由器已再次成為備用路由器：

```
*Jul 18 11:47:46.370: %HSRP-5-STATECHANGE: GigabitEthernet1 Grp 1 state Active -> Speak  
*Jul 18 11:47:52.219: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down  
*Jul 18 11:47:57.806: %HSRP-5-STATECHANGE: GigabitEthernet1 Grp 1 state Speak -> Standby
```

要檢查階段1和階段2的安全關聯的狀態，可以使用show crypto ikev2 sa和show crypto ipsec sa來驗證。

---

---



**注意：**如果在啟動並運行的路由器上配置了多個隧道，可以使用`show crypto session remote X.X.X.X`和`show crypto ipsec sa peer X.X.X.X`命令檢查隧道的第1階段和第2階段狀態。

---

## 疑難排解

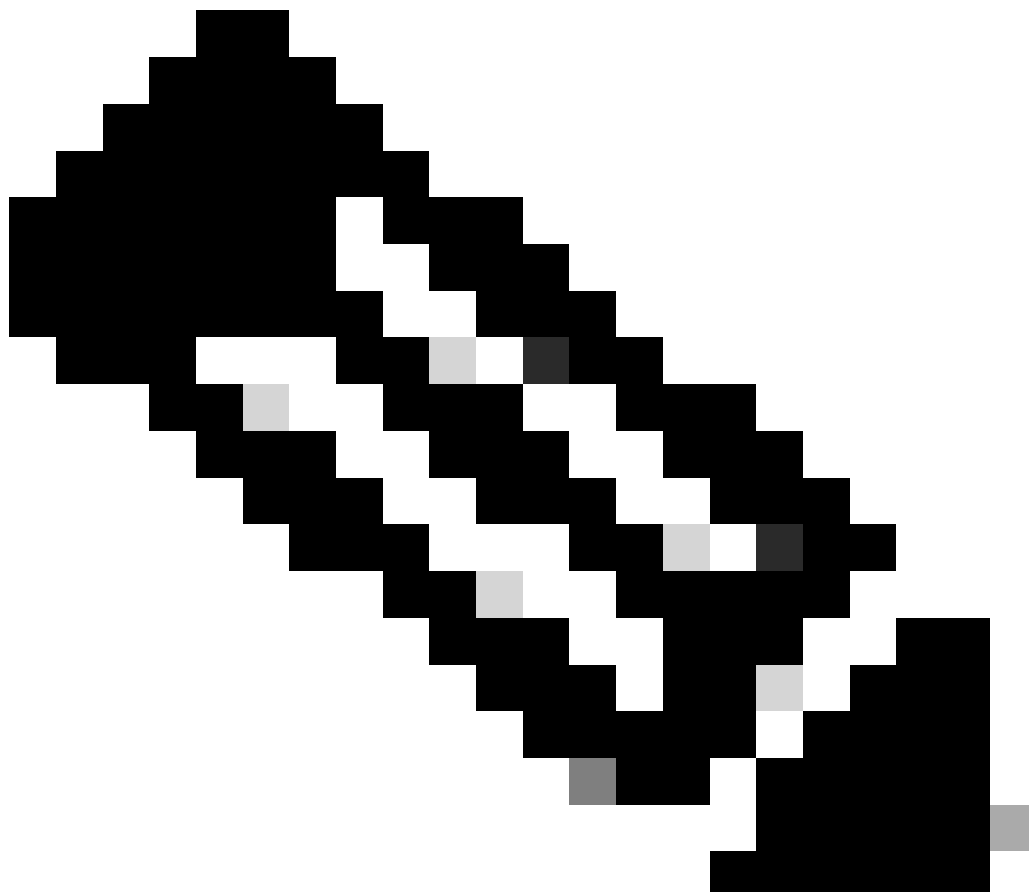
本節提供的資訊可用於對組態進行疑難排解。

可以啟用這些調試來排除IKEv2隧道的故障。

```
debug crypto ikev2
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
```

debug crypto ipsec message

---



注意：如果您希望僅排除一個隧道的故障（如果裝置處於生產狀態，則必須進行此情況），則必須使用命令 `debug crypto condition peer ipv4 X.X.X.X`.

---



## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。