# PIX/ASA Esempio di configurazione del failover attivo/attivo

## Sommario

# Introduzione

La configurazione di failover richiede due appliance di sicurezza identiche collegate tra loro tramite un collegamento di failover dedicato e, facoltativamente, un collegamento di failover con stato. Lo stato delle interfacce e delle unità attive viene monitorato per determinare se sono soddisfatte condizioni di failover specifiche. Se tali condizioni sono soddisfatte, si verifica il failover.

L'appliance di sicurezza supporta due configurazioni di failover, **Active/Active Failover** e **Active/Standby Failover**. Ogni configurazione di failover dispone di un metodo specifico per determinare ed eseguire il failover. Con il failover attivo/attivo, entrambe le unità possono superare il traffico di rete. In questo modo è possibile configurare il bilanciamento del carico sulla rete. Il failover attivo/attivo è disponibile solo sulle unità eseguite in modalità contesto multiplo. Con il failover attivo/standby, solo una unità passa il traffico mentre l'altra è in stato di standby. Il failover attivo/standby è disponibile sulle unità che vengono eseguite in modalità contesto singolo o multiplo. Entrambe le configurazioni di failover supportano il failover con o senza stato (regolare).

In questo documento viene illustrato come configurare il failover attivo/attivo in Cisco PIX/ASA Security Appliance.

Per ulteriori informazioni sulle configurazioni di failover attivo/standby, consultare l'esempio di configurazione del failover attivo/standby di PIX/ASA 7.x.

**Nota:** il failover della VPN non è supportato sulle unità eseguite in modalità contesto multiplo, poiché la VPN non è supportata in più contesti. Il failover VPN è disponibile solo per le configurazioni di **failover attivo/standby** in un singolo contesto.

Questa guida alla configurazione fornisce un esempio di configurazione per includere una breve introduzione alla tecnologia Active/Active di PIX/ASA 7.x. Per una descrizione più dettagliata della teoria alla base di questa tecnologia, consultare la guida di riferimento dei comandi di Cisco Security Appliance, versione 7.2.

# Prerequisiti

## Requisiti

### Requisiti hardware

Le due unità in una configurazione di failover devono avere la stessa configurazione hardware. Devono avere lo stesso modello, lo stesso numero e lo stesso tipo di interfacce e la stessa quantità di RAM.

**Nota:** le due unità non devono avere la stessa dimensione di memoria flash. Se nella configurazione di failover vengono utilizzate unità con memoria flash di dimensioni diverse, verificare che l'unità con la memoria flash più piccola disponga di spazio sufficiente per contenere i file di immagine software e i file di configurazione. In caso contrario, la sincronizzazione della configurazione dall'unità con la memoria flash più grande all'unità con la memoria flash più piccola non riesce.

### Requisiti software

Le due unità in una configurazione di failover devono essere in modalità operativa (instradate o trasparenti, contesto singolo o multiplo). Devono avere la stessa versione del software principale (primo numero) e secondaria (secondo numero), ma è possibile utilizzare versioni diverse del software in un processo di aggiornamento; ad esempio, è possibile aggiornare un'unità dalla versione 7.0(1) alla versione 7.0(2) e mantenere attivo il failover. Cisco consiglia di aggiornare entrambe le unità alla stessa versione per garantire la compatibilità a lungo termine.

Per ulteriori informazioni sull'aggiornamento del software su una coppia di failover, fare riferimento a Esecuzione di aggiornamenti senza downtime per le coppie di failover.

### Requisiti di licenza

Sulla piattaforma dell'appliance di sicurezza PIX/ASA, almeno una delle unità deve avere una **licenza senza restrizioni (UR)**. L'altra unità può avere una licenza di failover attivo-attivo (FO_AA) o un'altra licenza URL. Le unità con una licenza Restricted non possono essere utilizzate per il failover e due unità con licenze FO_AA non possono essere utilizzate insieme come coppia di failover.

**Nota:** per ottenere funzionalità e vantaggi aggiuntivi, potrebbe essere necessario aggiornare le licenze su una coppia di failover. Per ulteriori informazioni sull'aggiornamento, vedere Aggiornamento della chiave di licenza su una coppia di failover

**Nota:** le funzionalità concesse in licenza, ad esempio peer VPN SSL o contesti di sicurezza, su entrambi gli accessori di sicurezza che partecipano al failover devono essere identici.

**Nota:** la licenza FO non supporta il failover attivo/attivo.

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- PIX Security Appliance con versione 7.x e successive

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.

## Prodotti correlati

Questa configurazione può essere utilizzata anche con le seguenti versioni hardware e software:

- ASA con versione 7.x e successive

**Nota:** il failover attivo/attivo non è disponibile sull'appliance ASA serie 5505 adaptive security.

### Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

## Failover attivo/attivo

Questa sezione descrive il failover attivo/standby e include gli argomenti riportati di seguito.



### Panoramica del failover attivo/attivo

Il failover attivo/attivo è disponibile solo per le appliance di sicurezza in modalità contesto multiplo. In una configurazione di failover attivo/attivo, entrambi i dispositivi di sicurezza possono passare il traffico di rete.

In Failover attivo/attivo, i contesti di protezione dell'accessorio di protezione vengono suddivisi in gruppi di failover. Un gruppo di failover è semplicemente un gruppo logico di uno o più contesti di sicurezza. È possibile creare un massimo di due gruppi di failover sull'appliance di sicurezza. Il contesto admin è sempre un membro del gruppo di failover 1. Per impostazione predefinita, tutti i contesti di sicurezza non assegnati sono anche membri del gruppo di failover 1.

Il gruppo di failover costituisce l'unità di base per il failover attivo/attivo. Monitoraggio degli errori dell'interfaccia, failover e stato attivo/standby sono tutti attributi di un gruppo di failover anziché dell'unità. Quando un gruppo di failover attivo ha esito negativo, passa allo stato di standby mentre il gruppo di failover in standby diventa attivo. Le interfacce nel gruppo di failover che diventano attive presuppongono gli indirizzi MAC e IP delle interfacce nel gruppo di failover non riuscite. Le interfacce nel gruppo di failover che ora si trova nello stato di standby assumono gli indirizzi MAC e IP in standby.

**Nota:** un errore di un gruppo di failover su un'unità non significa che si sia verificato un errore nell'unità. È possibile che l'unità disponga di un altro gruppo di failover che trasmette il traffico su di essa.

### Stato principale/secondario e Stato attivo/standby

Come nel caso del failover attivo/standby, un'unità in una coppia di failover attivo/attivo è designata come unità principale, mentre l'altra unità è l'unità secondaria. A differenza del failover attivo/standby, questa designazione non indica quale unità diventa attiva quando entrambe le unità iniziano contemporaneamente. Al contrario, la designazione primaria/secondaria esegue due

operazioni:

- Determina quale unità fornisce la configurazione in esecuzione alla coppia all'avvio simultaneo.
- Determina su quale unità ogni gruppo di failover viene visualizzato nello stato attivo quando le unità vengono avviate contemporaneamente. Ogni gruppo di failover nella configurazione è configurato con una preferenza di unità primaria o secondaria. È possibile configurare entrambi i gruppi di failover in stato attivo su una singola unità della coppia, mentre l'altra unità contenente i gruppi di failover è in stato di standby. Tuttavia, una configurazione più tipica consiste nell'assegnare a ciascun gruppo di failover una preferenza di ruolo diversa, in modo da rendere ciascuno attivo su un'unità diversa, distribuendo il traffico tra i dispositivi.**Nota:** l'appliance di sicurezza **non** fornisce servizi di bilanciamento del carico. Il bilanciamento del carico deve essere gestito da un router che trasmette il traffico all'appliance di sicurezza.

L'unità su cui ciascun gruppo di failover diventa attivo viene determinata come illustrato

- Quando un'unità viene avviata mentre l'unità peer non è disponibile, entrambi i gruppi di failover diventano attivi sull'unità.
- Quando un'unità viene avviata mentre l'unità peer è attiva (con entrambi i gruppi di failover nello stato attivo), i gruppi di failover rimangono nello stato attivo sull'unità attiva indipendentemente dalla preferenza primaria o secondaria del gruppo di failover fino a quando non si verifica una delle condizioni seguenti:Si verifica un failover.Il gruppo di failover viene forzato manualmente sull'altra unità con il comando **no failover active**Il gruppo di failover è stato configurato con il comando **preempt**, in modo che diventi automaticamente attivo sull'unità preferita quando l'unità diventa disponibile.
- Quando entrambe le unità vengono avviate contemporaneamente, ciascun gruppo di failover diventa attivo sull'unità preferita dopo la sincronizzazione delle configurazioni.

## Inizializzazione e sincronizzazione della configurazione del dispositivo

La sincronizzazione della configurazione viene eseguita quando una o entrambe le unità in una coppia di avvio di failover. Le configurazioni vengono sincronizzate come illustrato di seguito:

- Quando un'unità viene avviata mentre l'unità peer è attiva (con entrambi i gruppi di failover attivi), l'unità di avvio contatta l'unità attiva per ottenere la configurazione in esecuzione indipendentemente dalla designazione primaria o secondaria dell'unità di avvio.
- Quando entrambe le unità vengono avviate contemporaneamente, l'unità secondaria ottiene la configurazione in esecuzione dall'unità primaria.

All'avvio della replica, sulla console dell'appliance di sicurezza dell'unità che invia la configurazione viene visualizzato il messaggio **"Beginning configuration replication: Invio in corso"** e al termine dell'operazione il dispositivo di sicurezza visualizza il messaggio **"End Configuration Replication to mate".** Durante la replica, i comandi immessi sull'unità che invia la configurazione potrebbero non essere replicati correttamente sull'unità peer e i comandi immessi sull'unità che riceve la configurazione potrebbero essere sovrascritti dalla configurazione che si riceve. Evitare di immettere comandi su entrambe le unità nella coppia di failover durante il processo di replica della configurazione. A seconda delle dimensioni della configurazione, la replica può richiedere da alcuni secondi a diversi minuti.

Sull'unità che riceve la configurazione, la configurazione esiste solo nella memoria in esecuzione. Per salvare la configurazione nella memoria flash dopo la sincronizzazione, immettere il comando

**write memory all** nello spazio di esecuzione del sistema sull'unità con il gruppo di failover 1 nello stato attivo. Il comando viene replicato sull'unità peer, che procede a scrivere la configurazione nella memoria flash. Se si utilizza la parola chiave **all** con questo comando, il sistema e tutte le configurazioni di contesto verranno salvati.

**Nota:** le configurazioni di avvio salvate su server esterni sono accessibili da entrambe le unità attraverso la rete e non devono essere salvate separatamente per ciascuna unità. In alternativa, è possibile copiare i file di configurazione dei contesti dal disco dell'unità principale a un server esterno e quindi copiarli sul disco dell'unità secondaria, dove diventano disponibili al riavvio dell'unità.

## Replica dei comandi

Dopo l'esecuzione di entrambe le unità, i comandi vengono replicati da un'unità all'altra come illustrato di seguito:

- I comandi immessi in un contesto di protezione vengono replicati dall'unità in cui il contesto di protezione è presente nello stato attivo all'unità peer.**Nota:** Il contesto viene considerato nello stato attivo su un'unità se il gruppo di failover a cui appartiene è nello stato attivo su tale unità.
- I comandi immessi nello spazio di esecuzione del sistema vengono replicati dall'unità in cui il gruppo di failover 1 è in stato attivo all'unità in cui il gruppo di failover 1 è in stato di standby.
- I comandi immessi nel contesto admin vengono replicati dall'unità in cui il gruppo di failover 1 si trova nello stato attivo all'unità in cui il gruppo di failover 1 si trova nello stato standby.

Tutti i comandi di configurazione e file (**copy, rename, delete, mkdir, rmdir** e così via) vengono replicati, con le eccezioni seguenti. I comandi **show, debug, mode, firewall e failover dell'unità lan** non sono replicati.

Se non si immettono i comandi sull'unità appropriata per la replica dei comandi, le configurazioni non saranno sincronizzate. Le modifiche potrebbero andare perse alla successiva sincronizzazione della configurazione iniziale.

Èpossibile utilizzare il comando **write standby** per risincronizzare le configurazioni non più sincronizzate. Per il failover attivo/attivo, il comando **write standby** ha il seguente comportamento:

- Se si immette il comando **write standby** nello spazio di esecuzione del sistema, la configurazione del sistema e le configurazioni di tutti i contesti di sicurezza dell'accessorio di sicurezza vengono scritte nell'unità peer. Sono incluse le informazioni di configurazione per i contesti di sicurezza in stato standby. È necessario immettere il comando nello spazio di esecuzione del sistema sull'unità con il gruppo di failover 1 nello stato attivo.**Nota:** se nell'unità peer sono presenti contesti di sicurezza nello stato attivo, il comando **write standby** determina l'interruzione delle connessioni attive attraverso tali contesti. Utilizzare il comando **failover active** sull'unità che fornisce la configurazione per assicurarsi che tutti i contesti siano attivi sull'unità prima di immettere il comando **write standby**.
- Se si immette il comando **write standby** in un contesto di sicurezza, solo la configurazione del contesto di sicurezza viene scritta sull'unità peer. È necessario immettere il comando nel contesto di protezione dell'unità in cui il contesto di protezione è attivo.

I comandi replicati non vengono salvati nella memoria flash quando vengono replicati nell'unità peer. Vengono aggiunti alla configurazione corrente. Per salvare i comandi replicati nella memoria flash di entrambe le unità, usare il comando **write memory** o **copy running-config startup-config** sull'unità su cui sono state apportate le modifiche. Il comando viene replicato sull'unità peer e la

configurazione viene salvata nella memoria flash sull'unità peer.

## Trigger di failover

Nel failover attivo/attivo, il failover può essere attivato a livello di unità se si verifica uno dei seguenti eventi:

- L'unità presenta un guasto hardware.
- L'unità ha un'interruzione di corrente.
- L'unità presenta un errore software.
- Il comando **no failover active** o **failover active** viene immesso nello spazio di esecuzione del sistema.

Il failover viene attivato a livello di gruppo di failover quando si verifica uno dei seguenti eventi:

- Troppe interfacce monitorate nel gruppo non riuscite.
- Il comando **no failover active group_id** o **failover active group_id** viene immesso.

## Azioni di failover

In una configurazione di failover attivo/attivo, il failover viene eseguito in base al gruppo di failover e non in base al sistema. Ad esempio, se entrambi i gruppi di failover vengono designati come attivi sull'unità primaria e il gruppo di failover 1 ha esito negativo, il gruppo di failover 2 rimane attivo sull'unità primaria mentre il gruppo di failover 1 diventa attivo sull'unità secondaria.

**Nota:** quando si configura il failover attivo/attivo, verificare che il traffico combinato di entrambe le unità rientri nella capacità di ciascuna unità.

In questa tabella viene illustrata l'azione di failover per ogni evento di errore. Per ogni evento di errore vengono specificati il criterio (indipendentemente dal fatto che si verifichi o meno il failover), le azioni per il gruppo di failover attivo e le azioni per il gruppo di failover in standby.

| Evento di errore | Policy | Azione gruppo attivo | Azione gruppo di standby | Note |
|---|---|---|---|---|
| Un'unità presenta un guasto di alimentazione o software | Failover | Diventa standby Contrassegna come non riuscito | Passate alla modalità standby. Contrassegna attivo come non riuscito | Quando un'unità in una coppia di failover si guasta, qualsiasi gruppo di failover attivo su tale unità viene contrassegnato come guasto e diventa attivo sull'unità peer. |
| Errore di interfaccia sul gruppo | Failover | Contrassegna gruppo | Diventa attivo | Nessuna |

| | | | | |
|---|---|---|---|---|
| di failover attivo oltre la soglia | | attivo come non riuscito | | |
| Errore di interfaccia sul gruppo di failover in standby superiore alla soglia | Nessun failover | Nessuna azione | Contrassegna il gruppo in standby come non riuscito | Quando il gruppo di failover in standby è contrassegnato come non riuscito, il gruppo di failover attivo non tenta di eseguire il failover, anche se viene superata la soglia di errore dell'interfaccia. |
| Ripristino del gruppo di failover precedentemente attivo | Nessun failover | Nessuna azione | Nessuna azione | A meno che non sia configurato con il comando **preempt**, i gruppi di failover rimangono attivi sull'unità corrente. |
| Collegamento di failover non riuscito all'avvio | Nessun failover | Diventa attivo | Diventa attivo | Se il collegamento di failover non è attivo all'avvio, entrambi i gruppi di failover su entrambe le unità diventano attivi. |
| Collegamento di failover stateful non riuscito | Nessun failover | Nessuna azione | Nessuna azione | Le informazioni sullo stato diventano obsolete e le sessioni vengono terminate in caso di failover. |
| Collegamento di failover non | Nessun failover | n/d | n/d | Ogni unità contrassegna l'interfaccia di failover come |

| | | | | |
|---|---|---|---|---|
| riuscito durante l'operazione | | | | guasta. È necessario ripristinare il collegamento di failover il prima possibile perché l'unità non può eseguire il failover sull'unità in standby mentre il collegamento di failover è inattivo. |

# Failover regolare e stateful

L'appliance di sicurezza supporta due tipi di failover, normale e con conservazione dello stato. In questa sezione sono inclusi gli argomenti seguenti:

- Failover regolare
- Failover stateful

## Failover regolare

Quando si verifica un failover, tutte le connessioni attive vengono eliminate. I client devono ristabilire le connessioni quando la nuova unità attiva subentra.

## Failover stateful

Quando il failover con conservazione dello stato è abilitato, l'unità attiva passa continuamente all'unità di standby le informazioni sullo stato per connessione. Dopo un failover, le stesse informazioni di connessione sono disponibili nella nuova unità attiva. Le applicazioni utente finali supportate non devono riconnettersi per mantenere la stessa sessione di comunicazione.

Le informazioni sullo stato passate all'unità di standby includono:

- Tabella di conversione NAT
- Gli stati della connessione TCP
- Stati di connessione UDP
- Tabella ARP
- Tabella bridge di layer 2 (quando viene eseguito in modalità firewall trasparente)
- Stati della connessione HTTP (se la replica HTTP è abilitata)
- Tabella delle associazioni di protezione ISAKMP e IPSec
- Il database delle connessioni PDP GTP

Le informazioni che non vengono passate all'unità di standby quando il failover con stato è abilitato includono:

- Tabella delle connessioni HTTP (a meno che non sia abilitata la replica HTTP)

- Tabella di autenticazione utente (uauth)
- Tabelle di routing
- Informazioni sullo stato dei moduli del servizio di sicurezza

**Nota:** Se il failover si verifica all'interno di una sessione Cisco IP SoftPhone attiva, la chiamata rimane attiva perché le informazioni sullo stato della sessione di chiamata vengono replicate sull'unità in standby. Quando la chiamata viene terminata, il client IP SoftPhone perde la connessione con Gestione chiamate. Questo si verifica perché non vi sono informazioni sulla sessione per il messaggio di interruzione CTIQBE sull'unità di standby. Quando il client IP SoftPhone non riceve una risposta dal gestore delle chiamate entro un determinato periodo di tempo, considera il gestore delle chiamate non raggiungibile e annulla la registrazione.

## Limitazioni della configurazione di failover

Non è possibile configurare il failover con questi tipi di indirizzi IP:

- Indirizzi IP ottenuti tramite DHCP
- Indirizzi IP ottenuti tramite PPPoE
- Indirizzi IPv6

Inoltre, si applicano le seguenti restrizioni:

- Il failover stateful non è supportato sull'appliance ASA 5505 adaptive security.
- Il failover attivo/attivo non è supportato sull'appliance ASA 5505 adaptive security.
- Non è possibile configurare il failover quando Easy VPN Remote è abilitato sull'appliance ASA 5505 adaptive security.
- Il failover VPN non è supportato in modalità contesto multiplo.

### Funzionalità non supportate

La modalità a contesto multiplo non supporta le funzionalità seguenti:

- Protocolli di routing dinamicoI contesti di protezione supportano solo route statiche. Non è possibile abilitare OSPF o RIP in modalità contesto multiplo.
- VPN
- Multicast

## Configurazione del failover attivo/attivo basato su cavo

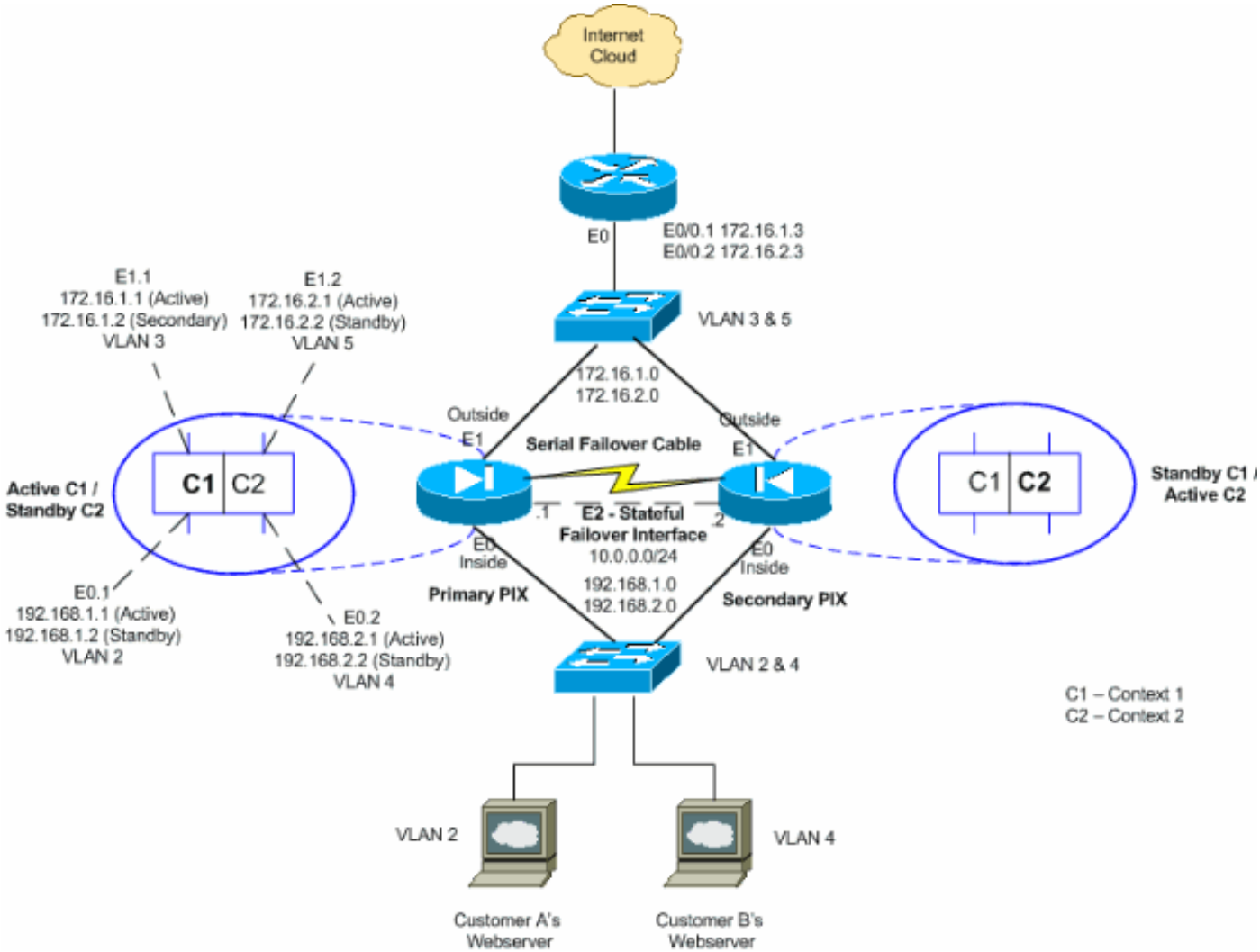
### Prerequisiti

Prima di iniziare, verificare quanto segue:

- Entrambe le unità dispongono dello stesso hardware, della stessa configurazione software e della stessa licenza.
- Entrambe le unità si trovano nella stessa modalità (singola o multipla, trasparente o stesa).

### Esempio di rete

Nel documento viene usata questa impostazione di rete:




Per configurare il failover attivo/attivo utilizzando un cavo seriale come collegamento di failover, attenersi alla seguente procedura. I comandi di questa attività vengono immessi nell'unità primaria della coppia di failover. L'unità primaria è quella a cui è collegata l'estremità del cavo "principale". Per i dispositivi in modalità contesto multiplo, i comandi vengono immessi nello spazio di esecuzione del sistema, a meno che non sia diversamente indicato.

non è necessario avviare l'unità secondaria nella coppia di failover quando si utilizza il failover basato su cavi. Lasciare spenta l'unità secondaria finché non viene richiesto di accenderla.

**Nota: il** failover basato su cavi è disponibile solo sull'appliance di sicurezza PIX serie 500.

Completare questa procedura per configurare il failover attivo/attivo basato su cavi:

1. Collegare il cavo di failover ai dispositivi di sicurezza PIX serie 500. Assicurarsi di collegare l'estremità del cavo contrassegnato come "Principale" all'unità utilizzata come unità principale e di collegare l'estremità del cavo contrassegnata come "Secondaria" all'unità utilizzata come unità secondaria.
2. Accendere l'unità principale.
3. Se non è già stato fatto, configurare gli indirizzi IP attivo e in standby per ciascuna interfaccia dati (modalità instradata), per l'indirizzo IP di gestione (modalità trasparente) o per l'interfaccia di sola gestione. L'indirizzo IP di standby viene utilizzato sull'appliance di sicurezza che attualmente è l'unità di standby. Deve trovarsi nella stessa subnet dell'indirizzo

IP attivo.Ènecessario configurare gli indirizzi di interfaccia dall'interno di ogni contesto. Per passare da un contesto all'altro, utilizzare il comando **cambia in contesto**. Il prompt dei comandi viene modificato in `nomehost/contesto(config-if)#`, dove contesto è il nome del contesto corrente. Immettere un indirizzo IP di gestione per ogni contesto in modalità di contesto multiplo del firewall trasparente.**Nota:** non configurare un indirizzo IP per il collegamento di failover stateful se si intende utilizzare un'interfaccia di failover stateful dedicata. Il comando **failover interface ip** viene utilizzato per configurare un'interfaccia di failover stateful dedicata in un passaggio successivo.

```
hostname/context(config-if)#ip address active_addr netmask standby standby_addr
```

Nell'esempio, l'interfaccia esterna per context1 del PIX primario è configurata nel modo seguente:

```
PIX1/context1(config)#ip address 172.16.1.1 255.255.255.0
                                    standby 172.16.1.2
```

Per Context2:

```
PIX1/context2(config)#ip address 192.168.2.1 255.255.255.0
                                      standby 192.168.2.2
```

In modalità firewall indirizzato e per l'interfaccia di sola gestione, questo comando viene immesso in modalità di configurazione interfaccia per ciascuna interfaccia. In modalità firewall trasparente, il comando viene immesso in modalità di configurazione globale.

4. Per abilitare il failover stateful, configurare il collegamento Failover stateful.Specificare l'interfaccia da utilizzare come collegamento di failover stateful:

   ```
   hostname(config)#failover link if_name phy_if
   ```

   In questo esempio, l'interfaccia Ethernet2 viene utilizzata per scambiare le informazioni sullo stato del collegamento di failover con stato.

   ```
   failover link stateful Ethernet2
   ```

   L'argomento if_name assegna un nome logico all'interfaccia specificata dall'argomento phy_if. L'argomento phy_if può essere il nome della porta fisica, ad esempio Ethernet1, o una sottointerfaccia creata in precedenza, ad esempio Ethernet0/2.3. Questa interfaccia non deve essere utilizzata per altri scopi, ad eccezione facoltativamente del collegamento di failover.Assegnare un indirizzo IP attivo e in standby al collegamento Failover stateful:

   ```
   hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
   ```

   Nell'esempio, la versione 10.0.0.1 viene usata come attiva e la versione 10.0.0.2 come indirizzo IP di standby per il collegamento di failover con stato.

   ```
   PIX1(config)#failover interface ip stateful 10.0.0.1
                       255.255.255.0 standby 10.0.0.2
   ```

   L'indirizzo IP di standby deve trovarsi nella stessa subnet dell'indirizzo IP attivo. Non è necessario identificare la subnet mask dell'indirizzo IP di standby.L'indirizzo IP e l'indirizzo MAC del collegamento di failover stateful non cambiano durante il failover, ad eccezione dei casi in cui il failover stateful utilizza una normale interfaccia dati. L'indirizzo IP attivo rimane sempre associato all'unità primaria, mentre l'indirizzo IP in standby rimane associato all'unità secondaria.Abilitare l'interfaccia:

   ```
   hostname(config)#interface phy_if
   hostname(config-if)#no shutdown
   ```

5. Configurare i gruppi di failover. È possibile avere al massimo due gruppi di failover. Il

comando **failover group** crea il gruppo di failover specificato se non esiste ed entra in modalità di configurazione del gruppo di failover.Per ogni gruppo di failover è necessario specificare se il gruppo di failover ha la preferenza primaria o secondaria utilizzando il comando **primaria** o **secondaria**. È possibile assegnare la stessa preferenza a entrambi i gruppi di failover. Per le configurazioni di bilanciamento del carico, è necessario assegnare a ogni gruppo di failover una preferenza di unità diversa.L'esempio seguente assegna al gruppo di failover 1 una preferenza primaria e al gruppo di failover 2 una preferenza secondaria:

```
hostname(config)#failover group 1
hostname(config-fover-group)#primary
hostname(config-fover-group)#exit
hostname(config)#failover group 2
hostname(config-fover-group)#secondary
hostname(config-fover-group)#exit
```

6. Assegnare ogni contesto utente a un gruppo di failover utilizzando il comando **join-failover-group** in modalità di configurazione contesto.Qualsiasi contesto non assegnato viene assegnato automaticamente al gruppo di failover 1. Il contesto admin è sempre membro del gruppo di failover 1.Immettere i comandi seguenti per assegnare ogni contesto a un gruppo di failover:

   ```
   hostname(config)#context context_name
   hostname(config-context)#join-failover-group {1 | 2}
   hostname(config-context)#exit
   ```

7. Abilita failover:

   ```
   hostname(config)#failover
   ```

8. Accendere l'unità secondaria e abilitare il failover se non è già abilitata:

   ```
   hostname(config)#failover
   ```

   L'unità attiva invia la configurazione nella memoria in esecuzione all'unità di standby. Durante la sincronizzazione della configurazione, viene visualizzato il messaggio "Beginning configuration replication: "Invio in corso" e "Fine replica configurazione da associare" vengono visualizzati sulla console primaria.**Nota:** eseguire prima il comando **failover** sul dispositivo primario, quindi sul dispositivo secondario. Dopo aver eseguito il comando **failover** sul dispositivo secondario, quest'ultimo estrae immediatamente la configurazione dal dispositivo primario e si imposta come dispositivo in *standby*. L'ASA primaria rimane accesa e trasmette il traffico normalmente e si contrassegna come dispositivo *attivo*. Da quel momento in poi, ogni volta che si verifica un guasto sul dispositivo attivo, il dispositivo di standby diventa attivo.
9. Salvare la configurazione nella memoria flash dell'unità principale. Poiché i comandi immessi sull'unità primaria vengono replicati sull'unità secondaria, quest'ultima salva anche la configurazione nella memoria flash.

   ```
   hostname(config)#copy running-config startup-config
   ```

10. Se necessario, impostare qualsiasi gruppo di failover attivo sul server primario sullo stato attivo sul server secondario. Per forzare un gruppo di failover a diventare attivo sull'unità secondaria, eseguire questo comando nello spazio di esecuzione del sistema sull'unità primaria:

    ```
    hostname#no failover active group group_id
    ```

L'argomento group_id specifica il gruppo che si desidera rendere attivo sull'unità secondaria.

## Configurazioni

Nel documento vengono usate queste configurazioni:

- PIX1 - Configurazione del sistema
- PIX1 - Configurazione Context1
- PIX1 - Configurazione Context2

**PIX1 - Configurazione del sistema**

```
PIX1#show running-config
: Saved
PIX Version 7.2(2)




!
hostname PIX1
enable password 8Ry2YjIyt7RRXU24 encrypted
no mac-address auto

!--- Enable the physical and logical interfaces in the
system execution !--- space by giving "no shutdown"
before configuring the same in the contexts ! interface
Ethernet0 ! interface Ethernet0.1
 vlan 2
!
interface Ethernet0.2
 vlan 4
!
interface Ethernet1
!
interface Ethernet1.1
 vlan 3
!
interface Ethernet1.2
 vlan 5
!
!--- Configure "no shutdown" in the stateful failover
interface !--- of both Primary and secondary PIX.
interface Ethernet2
 description STATE Failover Interface
!
interface Ethernet3
 shutdown
!
interface Ethernet4
 shutdown
!
interface Ethernet5
 shutdown
!
class default
  limit-resource All 0
```

```
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
!

ftp mode passive
pager lines 24
!--- Command to enable the failover feature failover
!--- Command to assign the interface for stateful
failover failover link stateful Ethernet2
!--- Command to configure the active and standby IP's
for the !--- stateful failover failover interface ip
stateful 10.0.0.1 255.255.255.0 standby 10.0.0.2
!--- Configure the group 1 as primary failover group 1
!--- Configure the group 1 as secondary failover group 2
  secondary
no asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
  config-url flash:/admin.cfg
!
!--- Command to create a context called "context1"
context context1
!--- Command to allocate the logical interfaces to the
contexts allocate-interface Ethernet0.1 inside_context1
  allocate-interface Ethernet1.1 outside_context1
  config-url flash:/context1.cfg
!--- Assign this context to the failover group 1 join-
failover-group 1
!

context context2
  allocate-interface Ethernet0.2 inside_context2
  allocate-interface Ethernet1.2 outside_context2
  config-url flash:/context2.cfg
  join-failover-group 2
!

prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

## PIX1 - Configurazione Context1

```
PIX1/context1(config)#show running-config
: Saved
:
PIX Version 7.2(2)




!
hostname context1
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface inside_context1
 nameif inside
```

```
 security-level 100
!--- Configure the active and standby IP's for the
logical inside !--- interface of the context1. ip
address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
interface outside_context1
 nameif outside
 security-level 0
!--- Configure the active and standby IP's for the
logical outside !--- interface of the context1. ip
address 172.16.1.1 255.255.255.0 standby 172.16.1.2
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list 100 extended permit tcp any host 172.16.1.1
eq www
pager lines 24
mtu inside 1500
mtu outside 1500
monitor-interface inside
monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
static (inside,outside) 172.16.1.1 192.168.1.5 netmask
255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
telnet timeout 5
ssh timeout 5
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
```

```
service-policy global_policy global
Cryptochecksum:00000000000000000000000000000000
: end
```

## PIX1 - Configurazione Context2

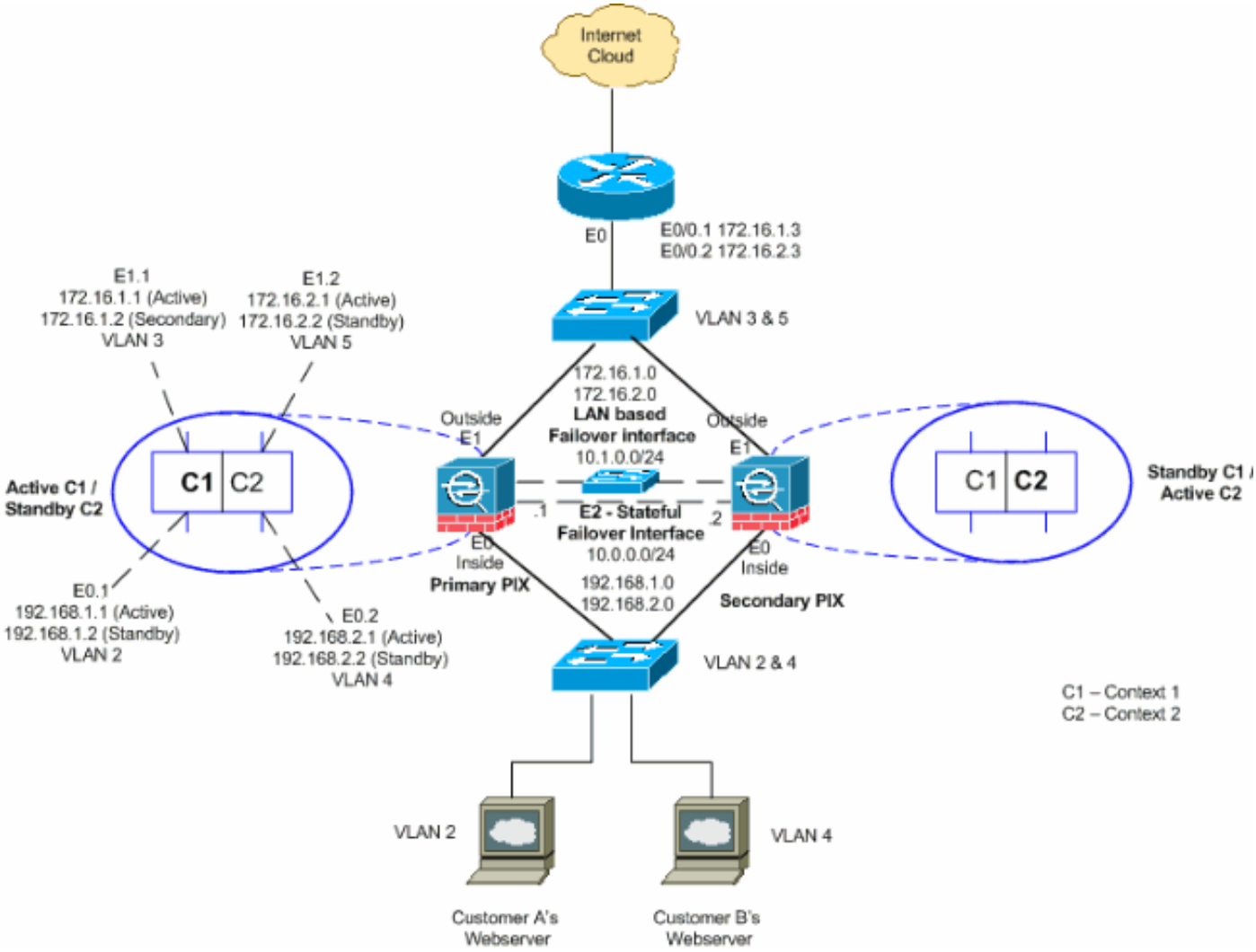
```
PIX1/context2(config)#show running-config
: Saved
:
PIX Version 7.2(2)




!
hostname context2
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface inside_context2
 nameif inside
 security-level 100
!--- Configure the active and standby IP's for the
logical inside !--- interface of the context2. ip
address 192.168.2.1 255.255.255.0 standby 192.168.2.2
!
interface outside_context2
 nameif outside
 security-level 0
!--- Configure the active and standby IP's for the
logical outside !--- interface of the context2. ip
address 172.16.2.1 255.255.255.0 standby 172.16.2.2
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list 100 extended permit tcp any host 172.16.2.1
eq www
pager lines 24
mtu inside 1500
mtu outside 1500
monitor-interface inside
monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
static (inside,outside) 172.16.2.1 192.168.2.5 netmask
255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.2.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
telnet timeout 5
ssh timeout 5
!
class-map inspection_default
```

```
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:00000000000000000000000000000000
: end
```

# Configurazione del failover attivo/attivo basato su LAN

## Esempio di rete

Nel documento viene usata questa impostazione di rete:




In questa sezione viene descritto come configurare il failover attivo/attivo utilizzando un collegamento di failover Ethernet. Quando si configura il failover basato su LAN, è necessario avviare il dispositivo secondario per riconoscere il collegamento di failover prima che il dispositivo secondario possa ottenere la configurazione in esecuzione dal dispositivo primario.

**Nota:** anziché utilizzare un cavo Ethernet crossover per collegare direttamente le unità, Cisco consiglia di utilizzare uno switch dedicato tra le unità primarie e secondarie.

Questa sezione include gli argomenti riportati di seguito.

- Configurazione unità primaria
- Configurazione unità secondaria

## Configurazione unità primaria

Completare questi passaggi per configurare l'unità primaria in una configurazione di failover attivo/attivo:

1. Se non è già stato fatto, configurare gli indirizzi IP attivo e in standby per ciascuna interfaccia dati (modalità instradata), per l'indirizzo IP di gestione (modalità trasparente) o per l'interfaccia di sola gestione. L'indirizzo IP di standby viene utilizzato sull'appliance di sicurezza che attualmente è l'unità di standby. Deve trovarsi nella stessa subnet dell'indirizzo IP attivo.Ènecessario configurare gli indirizzi di interfaccia dall'interno di ogni contesto. Per

passare da un contesto all'altro, utilizzare il comando **cambia in contesto**. Il prompt dei comandi viene modificato in nomehost/contesto(config-if)#, dove contesto è il nome del contesto corrente. In modalità firewall trasparente è necessario immettere un indirizzo IP di gestione per ogni contesto.**Nota:** non configurare un indirizzo IP per il collegamento di failover stateful se si intende utilizzare un'interfaccia di failover stateful dedicata. Il comando **failover interface ip** viene utilizzato per configurare un'interfaccia di failover stateful dedicata in un passaggio successivo.

```
hostname/context(config-if)#ip address active_addr netmask standby standby_addr
```

Nell'esempio, l'interfaccia esterna per context1 del PIX primario è configurata nel modo seguente:

```
PIX1/context1(config)#ip address 172.16.1.1 255.255.255.0
                                  standby 172.16.1.2
```

Per Context2:

```
PIX1/context2(config)#ip address 192.168.2.1 255.255.255.0
                                  standby 192.168.2.2
```

In modalità firewall indirizzato e per l'interfaccia di sola gestione, questo comando viene immesso in modalità di configurazione interfaccia per ciascuna interfaccia. In modalità firewall trasparente, il comando viene immesso in modalità di configurazione globale.

2. Configurare i parametri di failover di base nello spazio di esecuzione del sistema.(solo per appliance di sicurezza PIX) Abilitazione del failover basato su LAN:

```
hostname(config)#failover lan enable
```

Designare l'unità come unità principale:

```
hostname(config)#failover lan unit primary
```

Specificare il collegamento di failover:

```
hostname(config)#failover lan interface if_name phy_if
```

Nell'esempio, viene utilizzata l'interfaccia ethernet 3 come interfaccia di failover basata su LAN.

```
PIX1(config)#failover lan interface LANFailover ethernet3
```

L'argomento if_name assegna un nome logico all'interfaccia specificata dall'argomento phy_if. L'argomento phy_if può essere il nome della porta fisica, ad esempio Ethernet1, o una sottointerfaccia creata in precedenza, ad esempio Ethernet0/2.3. Sull'appliance ASA 5505 Adaptive Security, phy_if specifica una VLAN. Questa interfaccia non deve essere utilizzata per altri scopi (ad eccezione, facoltativamente, del collegamento Failover stateful).Specificare gli indirizzi IP attivi e in standby del collegamento di failover:

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

Nell'esempio, viene usato 10.1.0.1 come indirizzo attivo e 10.1.0.2 come indirizzo IP di standby per l'interfaccia di failover.

```
PIX1(config)#failover interface ip LANFailover
      10.1.0.1 255.255.255.0 standby 10.1.0.2
```

L'indirizzo IP di standby deve trovarsi nella stessa subnet dell'indirizzo IP attivo. Non è necessario identificare la subnet mask dell'indirizzo IP di standby. L'indirizzo IP e l'indirizzo MAC del collegamento di failover non cambiano al momento del failover. L'indirizzo IP attivo

rimane sempre associato all'unità primaria, mentre l'indirizzo IP in standby rimane associato all'unità secondaria.

3. Per abilitare il failover stateful, configurare il collegamento Failover stateful:Specificare l'interfaccia da utilizzare come collegamento di failover stateful:
```
hostname(config)#failover link if_name phy_if
```

```
PIX1(config)#failover link stateful ethernet2
```

L'argomento if_name assegna un nome logico all'interfaccia specificata dall'argomento phy_if. L'argomento phy_if può essere il nome della porta fisica, ad esempio Ethernet1, o una sottointerfaccia creata in precedenza, ad esempio Ethernet0/2.3. Questa interfaccia non deve essere utilizzata per altri scopi, ad eccezione facoltativamente del collegamento di failover.**Nota:** se il collegamento Failover stateful utilizza il collegamento di failover o un'interfaccia dati regolare, è sufficiente specificare l'argomento if_name.Assegnare un indirizzo IP attivo e in standby al collegamento Failover stateful.**Nota:** se il collegamento Failover stateful utilizza il collegamento di failover o un'interfaccia dati regolare, ignorare questo passaggio. Gli indirizzi IP attivo e in standby per l'interfaccia sono già stati definiti.
```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

```
PIX1(config)#failover interface ip stateful 10.0.0.1
                    255.255.255.0 standby 10.0.0.2
```

L'indirizzo IP di standby deve trovarsi nella stessa subnet dell'indirizzo IP attivo. Non è necessario identificare la subnet mask dell'indirizzo di standby. L'indirizzo IP e l'indirizzo MAC del collegamento di stato non cambiano al failover. L'indirizzo IP attivo rimane sempre associato all'unità primaria, mentre l'indirizzo IP in standby rimane associato all'unità secondaria.Abilitare l'interfaccia.**Nota:** se il collegamento Failover stateful utilizza il collegamento di failover o l'interfaccia dati regolare, ignorare questo passaggio. L'interfaccia è già stata abilitata.
```
hostname(config)#interface phy_if
hostname(config-if)#no shutdown
```

4. Configurare i gruppi di failover. È possibile avere al massimo due gruppi di failover. Il comando **failover group** crea il gruppo di failover specificato se non esiste ed entra in modalità di configurazione del gruppo di failover.Per ogni gruppo di failover, specificare se il gruppo di failover ha la preferenza **primaria** o **secondaria** utilizzando il comando primario o secondario. È possibile assegnare la stessa preferenza a entrambi i gruppi di failover. Per le configurazioni di bilanciamento del carico, è necessario assegnare a ogni gruppo di failover una preferenza di unità diversa.L'esempio seguente assegna al gruppo di failover 1 una preferenza primaria e al gruppo di failover 2 una preferenza secondaria:
```
hostname(config)#failover group 1
hostname(config-fover-group)#primary
hostname(config-fover-group)#exit
hostname(config)#failover group 2
hostname(config-fover-group)#secondary
hostname(config-fover-group)#exit
```

5. Assegnare ogni contesto utente a un gruppo di failover utilizzando il comando **join-failover-group** in modalità di configurazione contesto.Qualsiasi contesto non assegnato viene

assegnato automaticamente al gruppo di failover 1. Il contesto admin è sempre membro del gruppo di failover 1.Immettere i comandi seguenti per assegnare ogni contesto a un gruppo di failover:

```
hostname(config)#context context_name
hostname(config-context)#join-failover-group {1 | 2}
hostname(config-context)#exit
```

6. Abilitare il failover.

```
hostname(config)#failover
```

## Configurazione unità secondaria

Quando si configura il failover attivo/attivo basato su LAN, è necessario avviare l'unità secondaria per riconoscere il collegamento di failover. In questo modo, l'unità secondaria può comunicare con l'unità primaria e ricevere la configurazione corrente.

Completare questi passaggi per avviare l'unità secondaria in una configurazione di failover attivo/attivo:

1. (solo per appliance di sicurezza PIX) Abilitazione del failover basato su LAN.

```
hostname(config)#failover lan enable
```

2. Definire l'interfaccia di failover. Utilizzare le stesse impostazioni utilizzate per l'unità principale:Specificare l'interfaccia da utilizzare come interfaccia di failover.

```
hostname(config)#failover lan interface if_name phy_if
```

```
PIX1(config)#failover lan interface LANFailover ethernet3
```

L'argomento if_name assegna un nome logico all'interfaccia specificata dall'argomento phy_if. L'argomento phy_if può essere il nome della porta fisica, ad esempio Ethernet1, o una sottointerfaccia creata in precedenza, ad esempio Ethernet0/2.3. Sull'appliance ASA 5505 Adaptive Security, phy_if specifica una VLAN.Assegnare l'indirizzo IP attivo e in standby al collegamento di failover:

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

```
PIX1(config)#failover interface ip LANFailover 10.1.0.1
                      255.255.255.0 standby 10.1.0.2
```

**Nota:** immettere questo comando esattamente come è stato immesso nell'unità principale quando è stata configurata l'interfaccia di failover.L'indirizzo IP di standby deve trovarsi nella stessa subnet dell'indirizzo IP attivo. Non è necessario identificare la subnet mask dell'indirizzo di standby.Abilitare l'interfaccia.

```
hostname(config)#interfacephy_if
hostname(config-if)#no shutdown
```

3. Designare questa unità come unità secondaria:

```
hostname(config)#failover lan unit secondary
```

**Nota:** questo passo è facoltativo in quanto, per default, le unità vengono designate come

secondarie se non diversamente configurato in precedenza.

4. Abilitare il failover.
   ```
   hostname(config)#failover
   ```

   Dopo aver attivato il failover, l'unità attiva invia la configurazione nella memoria in esecuzione all'unità di standby. Durante la sincronizzazione della configurazione, vengono visualizzati i messaggi **Avvio replica configurazione: L'invio per l'accoppiamento e la fine della replica di configurazione per l'accoppiamento** vengono visualizzati sulla console dell'unità attiva.**Nota:** eseguire prima il comando **failover** sul dispositivo primario, quindi sul dispositivo secondario. Dopo aver eseguito il comando **failover** sul dispositivo secondario, quest'ultimo estrae immediatamente la configurazione dal dispositivo primario e si imposta come dispositivo in *standby*. L'ASA primaria rimane accesa e trasmette il traffico normalmente e si contrassegna come dispositivo *attivo*. Da quel momento in poi, ogni volta che si verifica un guasto sul dispositivo attivo, il dispositivo di standby diventa attivo.
5. Al termine della replica della configurazione in esecuzione, immettere questo comando per salvare la configurazione nella memoria flash:
   ```
   hostname(config)#copy running-config startup-config
   ```

6. Se necessario, forzare qualsiasi gruppo di failover attivo sul server primario allo stato attivo sull'unità secondaria. Per forzare un gruppo di failover a diventare attivo sull'unità secondaria, immettere questo comando nello spazio di esecuzione del sistema sull'unità primaria:
   ```
   hostname#no failover active group group_id
   ```

   L'argomento group_id specifica il gruppo che si desidera rendere attivo sull'unità secondaria.

## Configurazioni

Nel documento vengono usate queste configurazioni:

**PIX primario**

```
PIX1(config)#show running-config
: Saved
:
PIX Version 7.2(2) <system>
!
hostname PIX1
enable password 8Ry2YjIyt7RRXU24 encrypted
no mac-address auto
!
interface Ethernet0
!
interface Ethernet0.1
 vlan 2
!
interface Ethernet0.2
 vlan 4
!
interface Ethernet1
!
interface Ethernet1.1
 vlan 3
!
```

```
interface Ethernet1.2
 vlan 5
!
 !--- Configure "no shutdown" in the stateful failover
interface as well as !--- LAN Failover interface of both
Primary and secondary PIX/ASA. interface Ethernet2
description STATE Failover Interface
!
interface Ethernet3
 description LAN Failover Interface
!
interface Ethernet4
 shutdown
!
interface Ethernet5
 shutdown
!
class default
  limit-resource All 0
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
!

ftp mode passive
pager lines 24
failover
failover lan unit primary
!--- Command to assign the interface for LAN based
failover failover lan interface LANFailover Ethernet3
!--- Command to enable the LAN based failover failover
lan enable
!--- Configure the Authentication/Encryption key
failover key *****
failover link stateful Ethernet2
!--- Configure the active and standby IP's for the LAN
based failover failover interface ip LANFailover
10.1.0.1 255.255.255.0 standby 10.1.0.2
failover interface ip stateful 10.0.0.1 255.255.255.0
standby 10.0.0.2
failover group 1
failover group 2
  secondary
no asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
  config-url flash:/admin.cfg
!

context context1
  allocate-interface Ethernet0.1 inside_context1
  allocate-interface Ethernet1.1 outside_context1
  config-url flash:/context1.cfg
  join-failover-group 1
!

context context2
  allocate-interface Ethernet0.2 inside_context2
  allocate-interface Ethernet1.2 outside_context2
  config-url flash:/context2.cfg
  join-failover-group 2
```

```
!

prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

**Nota:** per la configurazione del contesto nello scenario di failover basato su LAN, fare riferimento alla sezione Configurazione di failover basata su cavo PIX1 - Configurazione contesto1 e PIX1 - Configurazione contesto2.

**PIX secondario**

```
PIX2#show running-config

failover
failover lan unit secondary
failover lan interface LANFailover Ethernet3
failover lan enable
failover key *****
failover interface ip LANFailover 10.1.0.1 255.255.255.0
standby 10.1.0.2
```

# Verifica

## Uso del comando show failover

In questa sezione viene descritto l'output del comando **show failover**. Su ciascuna unità, è possibile verificare lo stato del failover con il comando **show failover**.

### PIX primario

```
PIX1(config-subif)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: LANFailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(2), Mate 7.2(2)
Group 1 last failover at: 06:12:45 UTC Apr 16 2007
Group 2 last failover at: 06:12:43 UTC Apr 16 2007

  This host:    Primary
  Group 1       State:          Active
                Active time:    359610 (sec)
  Group 2       State:          Standby Ready
                Active time:    3165 (sec)

                  context1 Interface inside (192.168.1.1): Normal
                  context1 Interface outside (172.16.1.1): Normal
                  context2 Interface inside (192.168.2.2): Normal
                  context2 Interface outside (172.16.2.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
```

```
               Active time:    0 (sec)
  Group 2      State:          Active
               Active time:    3900 (sec)

                 context1 Interface inside (192.168.1.2): Normal
                 context1 Interface outside (172.16.1.2): Normal
                 context2 Interface inside (192.168.2.1): Normal
                 context2 Interface outside (172.16.2.1): Normal

Stateful Failover Logical Update Statistics
        Link : stateful Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         48044      0          48040      1
        sys cmd         48042      0          48040      1
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         2          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       72081
        Xmit Q:         0       1       48044
```

## PIX secondario

```
PIX1(config)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: LANFailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(2), Mate 7.2(2)
Group 1 last failover at: 06:12:46 UTC Apr 16 2007
Group 2 last failover at: 06:12:41 UTC Apr 16 2007

  This host:    Secondary
  Group 1       State:          Standby Ready
                Active time:    0 (sec)
  Group 2       State:          Active
                Active time:    3975 (sec)

                  context1 Interface inside (192.168.1.2): Normal
                  context1 Interface outside (172.16.1.2): Normal
                  context2 Interface inside (192.168.2.1): Normal
                  context2 Interface outside (172.16.2.1): Normal

  Other host:   Primary
  Group 1       State:          Active
                Active time:    359685 (sec)
  Group 2       State:          Standby Ready
                Active time:    3165 (sec)

                  context1 Interface inside (192.168.1.1): Normal
                  context1 Interface outside (172.16.1.1): Normal
                  context2 Interface inside (192.168.2.2): Normal
                  context2 Interface outside (172.16.2.2): Normal
```

```
Stateful Failover Logical Update Statistics
        Link : stateful Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         940        0          942        2
        sys cmd         940        0          940        2
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          2          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1419
        Xmit Q:         0       1       940
```

Utilizzare il comando **show failover state** per verificare lo stato.

### PIX primario

```
PIX1(config)#show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
    Group 1    Active         None
    Group 2    Standby Ready  None
Other host -   Secondary
    Group 1    Standby Ready  None
    Group 2    Active         None

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

### Unità Secondaria

```
PIX1(config)#show failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Standby Ready  None
    Group 2    Active         None
Other host -   Primary
    Group 1    Active         None
    Group 2    Standby Ready  None

====Configuration State===
        Sync Done - STANDBY
====Communication State===
        Mac set
```

Per verificare gli indirizzi IP dell'unità di failover, utilizzare il comando **show failover** interface.

### Unità Principale

```
PIX1(config)#show failover interface
        interface stateful Ethernet2
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.1
```

```
                Other IP Address : 10.0.0.2
        interface LANFailover Ethernet3
                System IP Address: 10.1.0.1 255.255.255.0
                My IP Address    : 10.1.0.1
                Other IP Address : 10.1.0.2
```

### Unità Secondaria

```
PIX1(config)#show failover interface
        interface LANFailover Ethernet3
                System IP Address: 10.1.0.1 255.255.255.0
                My IP Address    : 10.1.0.2
                Other IP Address : 10.1.0.1
        interface stateful Ethernet2
                System IP Address: 10.0.0.1 255.255.255.0
                My IP Address    : 10.0.0.2
                Other IP Address : 10.0.0.1
```

## Visualizzazione interfacce monitorate

Per visualizzare lo stato delle interfacce monitorate: In modalità contesto singolo, immettere il comando `show monitor-interface` in modalità di configurazione globale. In modalità contesto multiplo, immettere il comando `show monitor-interface` in un contesto.

**Nota:** per abilitare il monitoraggio dello stato su un'interfaccia specifica, usare il comando monitor-interface in modalità di configurazione globale:

```
monitor-interface <if_name>
```

### PIX primario

```
PIX1/context1(config)#show monitor-interface
        This host: Secondary - Active
                Interface inside (192.168.1.1): Normal
                Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Interface inside (192.168.1.2): Normal
                Interface outside (172.16.1.2): Normal
```

### PIX secondario

```
PIX1/context1(config)#show monitor-interface
        This host: Secondary - Standby Ready
                Interface inside (192.168.1.2): Normal
                Interface outside (172.16.1.2): Normal
        Other host: Secondary - Active
                Interface inside (192.168.1.1): Normal
                Interface outside (172.16.1.1): Normal
```

**Nota:** se non si immette un indirizzo IP di failover, il comando **show failover** visualizza 0.0.0.0 per l'indirizzo IP e il monitoraggio delle interfacce rimane in stato di attesa. Per il corretto funzionamento del failover, è necessario impostare un indirizzo IP di failover. Per ulteriori informazioni sui diversi stati del failover, vedere show failover.

Per impostazione predefinita, il monitoraggio delle interfacce fisiche è abilitato e il monitoraggio delle sottointerfacce è disabilitato.

## Visualizzazione dei comandi di failover nella configurazione in esecuzione

Per visualizzare i comandi di failover nella configurazione in esecuzione, immettere questo comando:

```
hostname(config)#show running-config failover
```

Vengono visualizzati tutti i comandi **di failover**. Nelle unità in esecuzione in modalità a più contesti, immettere il comando `show running-config failover` nello spazio di esecuzione del sistema. Immettere il comando **show running-config all failover** per visualizzare i comandi di failover nella configurazione in esecuzione e includere i comandi per i quali non è stato modificato il valore predefinito.

## Test della funzionalità di failover

Per testare la funzionalità di failover, effettuare le seguenti operazioni:

1. Verificare che l'unità attiva o il gruppo di failover passi il traffico come previsto con FTP (ad esempio) per inviare un file tra host su interfacce diverse.
2. Forzare un failover sull'unità in standby con questo comando:Per il failover attivo/attivo, immettere il seguente comando sull'unità in cui è attivo il gruppo di failover contenente l'interfaccia che collega gli host:
   ```
   hostname(config)#no failover active group group_id
   ```
3. Utilizzare FTP per inviare un altro file tra gli stessi due host.
4. Se il test non è riuscito, immettere il **comando show failover** per controllare lo stato del failover.
5. Al termine, è possibile ripristinare lo stato attivo dell'unità o del gruppo di failover con questo comando:Per il failover attivo/attivo, immettere il seguente comando sull'unità in cui è attivo il gruppo di failover contenente l'interfaccia che collega gli host:
   ```
   hostname(config)#failover active group group_id
   ```

## Failover forzato

Per forzare l'unità di standby a diventare attiva, immettere uno dei seguenti comandi:

Immettere questo comando nello spazio di esecuzione del sistema dell'unità in cui il gruppo di failover si trova nello stato di standby:

```
hostname#failover active group group_id
```

In alternativa, immettere questo comando nello spazio di esecuzione del sistema dell'unità in cui il gruppo di failover è nello stato attivo:

```
hostname#no failover active group group_id
```

Se si immette questo comando nello spazio di esecuzione del sistema, tutti i gruppi di failover diventano attivi:

```
hostname#failover active
```

## Failover disabilitato

Per disabilitare il failover, immettere questo comando:

```
hostname(config)#no failover
```

Se si disabilita il failover su una coppia di dispositivi attivo/standby, lo stato attivo e di standby di ciascuna unità viene mantenuto fino al riavvio. Ad esempio, l'unità di standby rimane in modalità standby in modo che entrambe le unità non inizino a trasmettere il traffico. Per rendere attiva l'unità in standby (anche con il failover disabilitato), vedere la sezione Failover forzato.

Se si disabilita il failover su una coppia Attivo/Attivo, i gruppi di failover rimarranno nello stato Attivo su qualsiasi unità su cui sono attualmente attivi, indipendentemente dall'unità che preferiscono. È possibile immettere il comando **no failover** nello spazio di esecuzione del sistema.

## Ripristino di un'unità guasta

Per ripristinare un gruppo di failover attivo/attivo non riuscito a uno stato non riuscito, immettere questo comando:

```
hostname(config)#failover reset group group_id
```

Se si ripristina un'unità guasta in uno stato che non presenta alcun problema, l'unità non viene automaticamente attivata; le unità o i gruppi ripristinati rimangono nello stato di standby fino a quando non vengono resi attivi per failover (forzati o naturali). Un'eccezione è un gruppo di failover configurato con il comando **preempt**. Se precedentemente attivo, un gruppo di failover diventa attivo se è configurato con il comando **priority** e se l'unità su cui si è verificato l'errore è l'unità preferita.

## Sostituire l'unità guasta con una nuova unità

Per sostituire un'unità guasta con una nuova, completare i seguenti passaggi:

1. Eseguire il comando **no failover** sull'unità primaria.Lo stato dell'unità secondaria indica che l'**unità di standby non è stata rilevata**.
2. Scollegare l'unità principale e collegarla.
3. Verificare che l'unità sostitutiva esegua lo stesso software e la stessa versione ASDM dell'unità secondaria.
4. Eseguire i seguenti comandi sull'unità sostitutiva:

```
ASA(config)#failover lan unit primary
ASA(config)#failover lan interface failover Ethernet3
ASA(config)#failover interface ip failover 10.1.0.1 255.255.255.0 standby 10.1.0.2
ASA(config)#interface Ethernet3
```

```
ASA(config-if)#no shut
ASA(config-if)#exit
```

5. Collegare l'unità principale sostitutiva alla rete ed eseguire questo comando:
   ```
   ASA(config)#failover
   ```

# Risoluzione dei problemi

Quando si verifica un failover, entrambi gli accessori di sicurezza inviano messaggi di sistema. In questa sezione sono inclusi gli argomenti seguenti:

1. Messaggi di sistema di failover
2. Messaggi di debug
3. SNMP

## Messaggi di sistema di failover

L'appliance di sicurezza invia una serie di messaggi di sistema relativi al failover al livello di priorità 2, che indica una condizione critica. Per visualizzare questi messaggi, consultare i messaggi Cisco Security Appliance Logging Configuration e System Log per abilitare la registrazione e vedere le descrizioni dei messaggi di sistema.

**Nota:** nello switchover, il failover viene arrestato logicamente e quindi richiama le interfacce, generando messaggi syslog **411001** e **411002**. Si tratta di un'attività normale.

## Comunicazioni principali di failover perso con mate sull'interfaccia nome_interfaccia

Questo messaggio di failover viene visualizzato se un'unità della coppia di failover non è più in grado di comunicare con l'altra unità della coppia. Il database primario può anche essere elencato come secondario per l'unità secondaria.

*(Principale) Comunicazioni di failover perse con mate sull'interfaccia nome_interfaccia*

Verificare che la rete connessa all'interfaccia specificata funzioni correttamente.

## Messaggi di debug

Per visualizzare i messaggi di debug, immettere il comando **debug failover**. per ulteriori informazioni, consultare la guida di riferimento dei comandi di Cisco Security Appliance, versione 7.2.

**Nota:** poiché all'output di debug viene assegnata una priorità alta nel processo CPU, può influire in modo significativo sulle prestazioni del sistema. Per questo motivo, usare i comandi **debug fover** solo per risolvere problemi specifici o nelle sessioni di risoluzione dei problemi con il personale del supporto tecnico Cisco.

## SNMP

Per ricevere le trap syslog SNMP per il failover, configurare l'agente SNMP in modo che invii le

trap SNMP alle stazioni di gestione SNMP, definire un host syslog e compilare il MIB syslog Cisco nella stazione di gestione SNMP. Per ulteriori informazioni, consultare i comandi **snmp-server** e **logging** nella guida di riferimento dei comandi di Cisco Security Appliance, versione 7.2.

### Polltime di failover

Per specificare i tempi di polling e attesa dell'unità di failover, eseguire il comando **failover polltime** in modalità di configurazione globale.

L'`unità polltime di failover msec [time]` rappresenta l'intervallo di tempo per verificare l'esistenza dell'unità in standby mediante il polling dei messaggi di benvenuto.

Analogamente, l'`unità di tempo di attesa del failover msec [time]` rappresenta il periodo di tempo durante il quale un'unità deve ricevere un messaggio di saluto sul collegamento del failover, dopo il quale viene dichiarato che l'unità peer ha avuto esito negativo.

Per ulteriori informazioni, fare riferimento a polltime di failover.

### AVVISO: Errore di decrittografia del messaggio di failover.

Messaggio di errore:

```
Failover message decryption failure. Please make sure both units have the
same failover shared key and crypto license or system is not out of memory
```

Il problema si verifica a causa della configurazione della chiave di failover. Per risolvere il problema, rimuovere la chiave di failover e configurare la nuova chiave condivisa.

## Informazioni correlate

- Cisco serie 500 PIX Support Page
- Configurazione di failover del modulo Servizi firewall (FWSM)
- Risoluzione dei problemi di failover FWSM
- Funzionamento del failover sul firewall Cisco Secure PIX
- Cisco serie 5500 Adaptive Security Appliance - Pagina di supporto
- Documentazione e supporto tecnico – Cisco Systems