ASA/PIX: Configura failover attivo/standby in modalità trasparente

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:

- Failover attivo/attivo
- Failover attivo/standby

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).

Un firewall trasparente è un firewall di layer 2 che funziona come un *bump in the wire*, o un *firewall stealth*, e non viene visto come un router hop per i dispositivi connessi. L'accessorio di protezione connette la stessa rete alle porte interne ed esterne. Poiché il firewall non è un hop indirizzato, è possibile introdurre facilmente un firewall trasparente in una rete esistente; non è necessario ridefinire l'indirizzo IP. È possibile impostare l'accessorio Adaptive Security in modo che venga eseguito in modalità firewall con routing predefinito o in modalità firewall trasparente. Quando si modificano le modalità, l'accessorio Adaptive Security cancella la configurazione perché molti comandi non sono supportati in entrambe le modalità. Se si dispone già di una configurazione compilata, eseguire un backup di questa configurazione prima di modificare la modalità; è possibile utilizzare questa configurazione di backup come riferimento quando si crea una nuova configurazione. Per ulteriori informazioni sulla configurazione dell'accessorio firewall in modalità trasparente, fare riferimento a Esempio di configurazione di un firewall trasparente.

In questo documento viene spiegato come configurare il failover attivo/standby in modalità trasparente sull'appliance di sicurezza ASA.

Nota: il failover VPN non è supportato sulle unità eseguite in modalità a più contesti. Il failover VPN è disponibile solo per le configurazioni di **failover attivo/standby**.

Cisco consiglia di non utilizzare l'interfaccia di gestione per il failover, in particolare per il failover

stateful in cui l'appliance di sicurezza invia costantemente le informazioni di connessione da un appliance di sicurezza all'altro. L'interfaccia per il failover deve avere almeno la stessa capacità delle interfacce che passano il traffico regolare e, mentre le interfacce sull'appliance ASA 5540 sono Gigabit, l'interfaccia di gestione è solo Fast Ethernet. L'interfaccia di gestione è progettata esclusivamente per il traffico di gestione e viene specificata come management0/0. Tuttavia, è possibile utilizzare il comando **management-only** per configurare qualsiasi interfaccia in modo che sia di sola gestione. Inoltre, per Management 0/0, è possibile disabilitare la modalità di sola gestione in modo che l'interfaccia possa passare attraverso il traffico come qualsiasi altra interfaccia. Per ulteriori informazioni sul comando **management-only**, consultare la guida di riferimento dei comandi di Cisco Security Appliance, versione 8.0.

Questa guida alla configurazione fornisce un esempio di configurazione per includere una breve introduzione alla tecnologia Active/Standby di PIX/ASA 7.x. Per un'analisi più dettagliata della teoria alla base di questa tecnologia, consultare la guida di riferimento ai comandi ASA/PIX.

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 su come aggiornare il software su una coppia di failover, consultare la sezione Performing Zero Downtime Upgrades for Failover Pairs della *guida alla configurazione della riga di comando di Cisco Security Appliance, versione 8.0*.

Requisiti di licenza

Sulla piattaforma dell'appliance di sicurezza ASA, almeno una delle unità deve avere una **licenza senza restrizioni (UR)**.

Nota: potrebbe essere necessario aggiornare le licenze su una coppia di failover per ottenere funzionalità e vantaggi aggiuntivi. per ulteriori informazioni, fare riferimento a 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, in entrambi gli accessori di sicurezza che partecipano al failover devono essere identiche.

Componenti usati

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

- ASA 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:

- PIX Security Appliance con versione 7.x e successive

Convenzioni

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

Failover attivo/standby

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

Panoramica del failover attivo/standby

Il failover attivo/standby consente di utilizzare un'appliance di sicurezza di standby per gestire le funzionalità di un'unità guasta. Quando l'unità attiva non funziona, passa allo stato di standby mentre l'unità di standby passa allo stato attivo. L'unità che diventa attiva presuppone gli indirizzi IP o, per un firewall trasparente, l'indirizzo IP di gestione e gli indirizzi MAC dell'unità guasta e inizia a trasmettere il traffico. L'unità in stato di standby assume gli indirizzi IP e MAC in standby. Poiché i dispositivi di rete non vedono alcuna modifica nell'accoppiamento da MAC a indirizzo IP, nessuna voce ARP cambia o timeout in qualsiasi punto della rete.

Nota: in modalità contesto multiplo, l'appliance di sicurezza può eseguire il failover dell'intera

unità, che include tutti i contesti, ma non dei singoli contesti separatamente.

Stato principale/secondario e Stato attivo/standby

Le principali differenze tra le due unità in una coppia di failover sono correlate a quale unità è attiva e a quale unità è in standby, in particolare a quali indirizzi IP utilizzare e quale unità è primaria e passa attivamente il traffico.

Esistono alcune differenze tra le unità in base a quale unità è principale, come specificato nella configurazione, e quale unità è secondaria:

- L'unità primaria diventa sempre l'unità attiva se entrambe le unità vengono avviate contemporaneamente (e hanno lo stesso stato operativo).
- L'indirizzo MAC dell'unità primaria è sempre abbinato agli indirizzi IP attivi. L'eccezione a questa regola si verifica quando l'unità secondaria è attiva e non è in grado di ottenere l'indirizzo MAC primario sul collegamento di failover. In questo caso, viene utilizzato l'indirizzo MAC secondario.

Inizializzazione e sincronizzazione della configurazione del dispositivo

La sincronizzazione della configurazione viene eseguita quando uno o entrambi i dispositivi nella coppia di failover vengono avviati. Le configurazioni vengono sempre sincronizzate dall'unità attiva all'unità di standby. Quando l'unità in standby completa l'avvio iniziale, cancella la configurazione in esecuzione, ad eccezione dei comandi di failover necessari per comunicare con l'unità attiva, che a sua volta invia l'intera configurazione all'unità in standby.

L'unità attiva è determinata dai seguenti fattori:

- Se un'unità si avvia e rileva un dispositivo peer già operativo come attivo, diventa l'unità di standby.
- Se un'unità si avvia e non rileva un peer, diventa l'unità attiva.
- Se entrambe le unità si avviano contemporaneamente, l'unità principale diventa l'unità attiva e l'unità secondaria diventa l'unità di standby.

Nota: se l'unità secondaria si avvia e non rileva l'unità principale, diventa l'unità attiva. Utilizza i propri indirizzi MAC per gli indirizzi IP attivi. Quando l'unità primaria diventa disponibile, l'unità secondaria cambia gli indirizzi MAC in quelli dell'unità primaria, causando un'interruzione nel traffico di rete. Per evitare questo problema, configurare la coppia di failover con indirizzi MAC virtuali. Per ulteriori informazioni, vedere la sezione Configurazione del failover attivo/standby di questo documento.

All'avvio della replica, sulla console dell'appliance di sicurezza dell'unità attiva viene visualizzato il messaggio `Beginning configuration replication: Invio in corso` e, al termine dell'operazione, l'appliance di sicurezza visualizza il messaggio `End Configuration Replication to mate.` Durante la replica, i comandi immessi nell'unità attiva non possono essere replicati correttamente nell'unità in standby e i comandi immessi nell'unità in standby possono essere sovrascritti dalla configurazione replicata dall'unità attiva. Non immettere comandi su nessuna delle due unità nella coppia di failover all'interno del processo di replica della configurazione. A seconda delle dimensioni della configurazione, la replica può richiedere da alcuni secondi a diversi minuti.

Dall'unità secondaria è possibile osservare il messaggio di replica durante la sincronizzazione dall'unità principale:

```
ASA> .

        Detected an Active mate
Beginning configuration replication from mate.
End configuration replication from mate.

ASA>
```

Sull'unità di standby, la configurazione è presente solo nella memoria in esecuzione. Per salvare la configurazione nella memoria flash dopo la sincronizzazione, immettere questi comandi:

- Per la modalità a contesto singolo, immettere il comando **copy running-config startup-config** sull'unità attiva. Il comando viene replicato sull'unità di standby, che procede alla scrittura della configurazione sulla memoria flash.
- Per la modalità a contesto multiplo, immettere il comando **copy running-config startup-config** sull'unità attiva dallo spazio di esecuzione del sistema e da ciascun contesto sul disco. Il comando viene replicato sull'unità di standby, che procede alla scrittura della configurazione sulla memoria flash. I contesti con configurazioni di avvio su server esterni sono accessibili da entrambe le unità attraverso la rete e non devono essere salvati separatamente per ciascuna unità. In alternativa, è possibile copiare i contesti su disco dall'unità attiva a un server esterno e quindi copiarli su disco nell'unità di standby, dove diventano disponibili quando l'unità viene ricaricata.

Replica dei comandi

La replica dei comandi viene sempre eseguita dall'unità attiva all'unità in standby. I comandi immessi sull'unità attiva vengono inviati tramite il collegamento di failover all'unità in standby. non è necessario salvare la configurazione attiva nella memoria flash per replicare i comandi.

Nota: le modifiche apportate all'unità in standby non vengono replicate nell'unità attiva. Se si immette un comando sull'unità di standby, l'accessorio di sicurezza visualizza il messaggio `**** AVVISO **** NON viene eseguita la replica della configurazione dall'unità di standby all'unità attiva.` Le configurazioni non sono più sincronizzate. Questo messaggio viene visualizzato anche se si immettono comandi che non influiscono sulla configurazione.

Se si immette il comando **write standby** sull'unità attiva, l'unità in standby cancella la configurazione in esecuzione, ad eccezione dei comandi di failover utilizzati per comunicare con l'unità attiva, che a sua volta invia l'intera configurazione all'unità in standby.

In modalità contesto multiplo, quando si immette il comando **write standby** nello spazio di esecuzione del sistema, vengono replicati tutti i contesti. Se si immette il comando write standby in un contesto, il comando replica solo la configurazione del contesto.

I comandi replicati vengono archiviati nella configurazione in esecuzione. Per salvare i comandi replicati nella memoria flash dell'unità in standby, immettere i seguenti comandi:

- Per la modalità a contesto singolo, immettere il comando **copy running-config startup-config** sull'unità attiva. Il comando viene replicato sull'unità di standby, che procede alla scrittura della configurazione sulla memoria flash.
- Per la modalità a contesto multiplo, immettere il comando **copy running-config startup-config** sull'unità attiva dallo spazio di esecuzione del sistema e in ciascun contesto su disco. Il comando viene replicato sull'unità di standby, che procede alla scrittura della configurazione

sulla memoria flash. I contesti con configurazioni di avvio su server esterni sono accessibili da entrambe le unità attraverso la rete e non devono essere salvati separatamente per ciascuna unità. In alternativa, è possibile copiare i contesti su disco dall'unità attiva a un server esterno e quindi copiarli su disco nell'unità di standby.

Trigger di failover

L'unità può avere esito negativo se si verifica uno dei seguenti eventi:

- L'unità presenta un guasto hardware o un'interruzione dell'alimentazione.
- L'unità presenta un errore software.
- Troppe interfacce monitorate non riuscite.
- Il comando **no failover active** viene immesso sull'unità attiva oppure il comando **failover active** viene immesso sull'unità di standby.

Azioni di failover

Nel failover attivo/standby, il failover viene eseguito su base unitaria. Anche nei sistemi eseguiti in modalità a più contesti non è possibile eseguire il failover di singoli contesti o di gruppi di contesti.

In questa tabella viene illustrata l'azione di failover per ogni evento di errore. Per ogni evento di errore, la tabella mostra i criteri di failover (failover o nessun failover), l'azione eseguita dall'unità attiva, l'azione eseguita dall'unità in standby e qualsiasi nota speciale relativa alla condizione e alle azioni di failover. Nella tabella viene illustrato il comportamento del failover.

Evento di errore	Policy	Azione attiva	Azione standby	Note
Errore dell'unità attiva (alimentazione o hardware)	Failover	n/d	Diventare attivi; contrassegna attivo come non riuscito	Non vengono ricevuti messaggi di benvenuto su alcuna interfaccia monitorata o sul collegamento di failover.
Ripristino dell'unità precedentemente attiva	Nessun failover	Diventa standby	Nessuna azione	Nessuna
Errore dell'unità di standby (alimentazione o hardware)	Nessun failover	Contrassegna standby come non riuscito	n/d	Quando l'unità di standby è contrassegnata come guasta, l'unità attiva non tenta di eseguire il failover, anche se viene superata la soglia di errore dell'interfaccia.

Collegamento di failover non riuscito nell'operazione	Nessun failover	Contrassegna l'interfaccia di failover come non riuscita	Contrassegna l'interfaccia di failover come non riuscita	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.
Collegamento di failover non riuscito all'avvio	Nessun failover	Contrassegna l'interfaccia di failover come non riuscita	Diventa attivo	Se il collegamento di failover non è attivo all'avvio, entrambe le unità diventano attive.
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.
Errore di interfaccia sull'unità attiva oltre la soglia	Failover	Contrassegna attivo come non riuscito	Diventa attivo	Nessuna
Errore di interfaccia sull'unità di standby oltre la soglia	Nessun failover	Nessuna azione	Contrassegna standby come non riuscito	Quando l'unità di standby è contrassegnata come guasta, l'unità attiva non tenta di eseguire il failover anche se viene superata la soglia di errore dell'interfaccia.

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 (solo quando il firewall è in esecuzione 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:

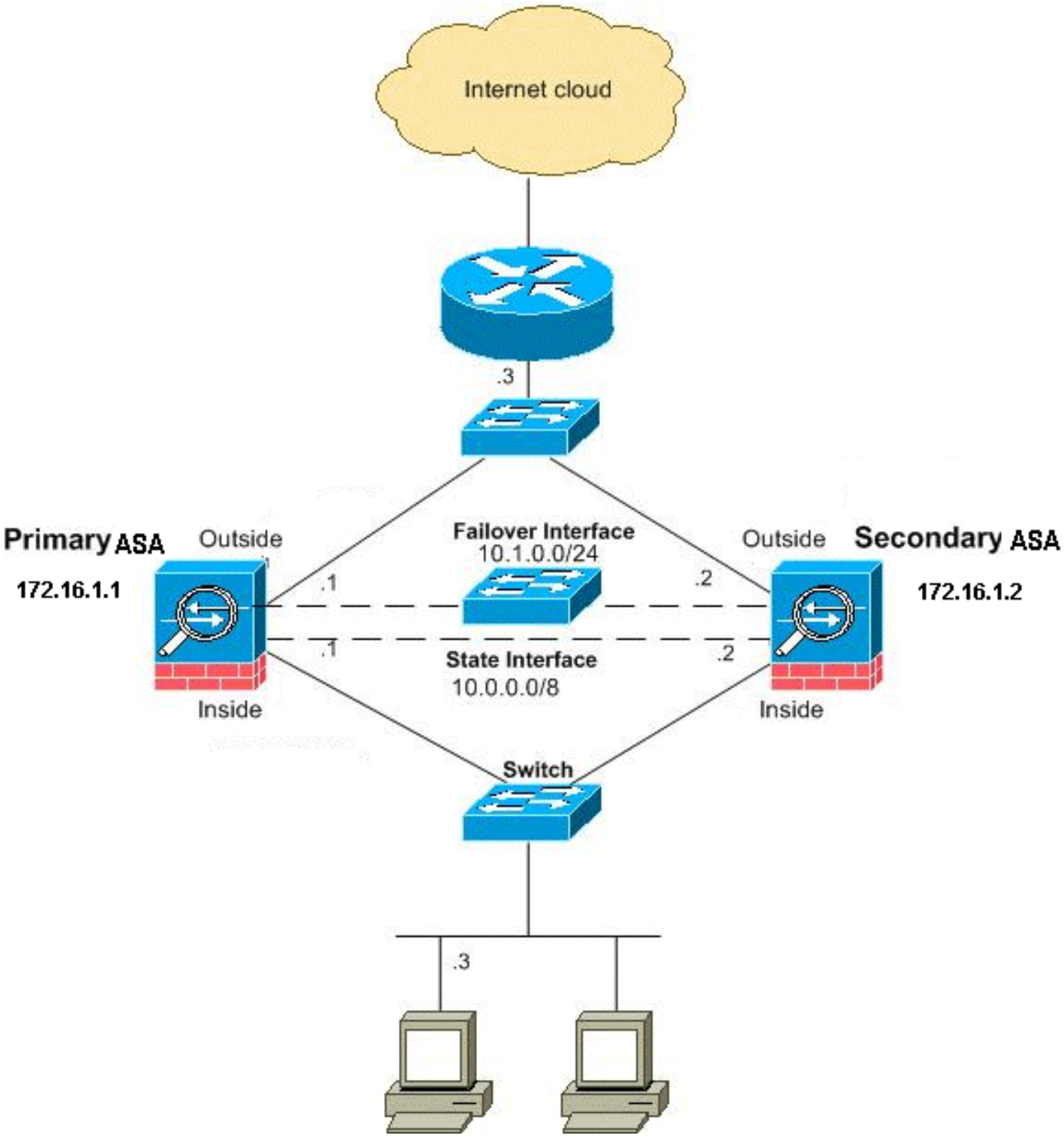
- Tabella delle connessioni HTTP (a meno che non sia abilitata la replica HTTP)
- Tabella di autenticazione utente (uauth)
- Tabelle di routing
- Informazioni sullo stato dei moduli del servizio di sicurezza

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 Cisco CallManager. Questo si verifica perché non vi sono informazioni sulla sessione per il messaggio di interruzione CTIQBE sull'unità di standby. Quando il client SoftPhone IP non riceve una risposta da Cisco CallManager entro un determinato periodo di tempo, considera Cisco CallManager non raggiungibile e annulla la registrazione.

Configurazione del failover attivo/standby basata su LAN

Esempio di rete

Nel documento viene usata questa impostazione di rete:



In questa sezione viene descritto come configurare il failover attivo/standby in modalità trasparente con 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: se si passa dal failover basato su cavo al failover basato su LAN, è possibile saltare molti passaggi, ad esempio l'assegnazione degli indirizzi IP attivo e in standby per ogni interfaccia, completati per la configurazione del failover basato su cavo.

Configurazione unità primaria

Completare questa procedura per configurare l'unità primaria in una configurazione di failover

attivo/standby basata su LAN. Questi passaggi forniscono la configurazione minima necessaria per abilitare il failover sull'unità primaria. In modalità contesto multiplo, tutti i passi vengono eseguiti nello spazio di esecuzione del sistema, se non diversamente indicato.

Per configurare l'unità primaria in una coppia di failover attivo/standby, attenersi alla seguente procedura:

1. Se non è già stato fatto, configurare gli indirizzi IP attivo e in standby per l'interfaccia di gestione (modalità trasparente). 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.**Nota:** non configurare un indirizzo IP per il collegamento di failover con stato se si utilizza un'interfaccia di failover con stato dedicata. Il comando **failover interface ip** viene utilizzato per configurare un'interfaccia di failover con stato dedicato in un passaggio successivo.
   ```
   hostname(config-if)#ip address active_addr netmask
                           standby standby_addr
   ```

   A differenza della modalità routing, che richiede un indirizzo IP per ciascuna interfaccia, un firewall trasparente ha un indirizzo IP assegnato all'intero dispositivo. L'accessorio di sicurezza utilizza questo indirizzo IP come indirizzo di origine dei pacchetti provenienti dall'accessorio di sicurezza, ad esempio messaggi di sistema o comunicazioni AAA. Nell'esempio, l'indirizzo IP dell'appliance ASA primaria è configurato come mostrato di seguito:
   ```
   hostname(config)#ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2
   ```

   In questo caso, 172.16.1.1 viene utilizzato per l'unità primaria e 172.16.1.2 viene assegnato all'unità secondaria (standby).**Nota:** in modalità contesto multiplo, è necessario configurare gli indirizzi di interfaccia da ogni contesto. Per passare da un contesto all'altro, utilizzare il comando **change to context**. Il prompt dei comandi viene modificato in `nomehost/contesto(config-if)#`, dove contesto è il nome del contesto corrente.
2. (solo piattaforma per appliance di sicurezza PIX) Abilitare il failover basato su LAN.
   ```
   hostname(config)#failover lan enable
   ```

3. Designare l'unità come unità primaria.
   ```
   hostname(config)#failover lan unit primary
   ```

4. Definire l'interfaccia di failover.Specificare l'interfaccia da utilizzare come interfaccia di failover.
   ```
   hostname(config)#failover lan interface if_name phy_if
   ```

   In questa documentazione, il "failover" (nome interfaccia per Ethernet0) viene utilizzato per un'interfaccia di failover.
   ```
   hostname(config)#failover lan interface failover Ethernet3
   ```

   L'argomento *if_name* assegna un nome 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.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
   ```

In questa documentazione, per configurare il collegamento di failover, viene utilizzato 10.1.0.1 per il collegamento attivo, 10.1.0.2 per l'unità di standby e "failover" è il nome di interfaccia Ethernet0.

```
hostname(config)#failover interface ip failover 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 di standby.L'indirizzo IP e l'indirizzo MAC del collegamento di failover non cambiano al momento del failover. L'indirizzo IP attivo per il collegamento di failover rimane sempre associato all'unità principale, mentre l'indirizzo IP di standby rimane associato all'unità secondaria.Abilitare l'interfaccia

```
hostname(config)#interface phy_if

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

Nell'esempio, Ethernet3 viene utilizzato per il failover:

```
hostname(config)#interface ethernet3

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

5. (Facoltativo) Per abilitare il failover con stato, configurare il collegamento al failover con stato.Specificare l'interfaccia da utilizzare come collegamento di failover con stato.

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

In questo esempio viene utilizzato "state" come nome di interfaccia per Ethernet2 per scambiare le informazioni sullo stato del collegamento di failover:

```
hostname(config)#failover link state Ethernet2
```

Nota: se il collegamento di failover con stato utilizza il collegamento di failover o un'interfaccia dati, è sufficiente specificare l'argomento *if_name*.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 di failover con stato.**Nota:** se il collegamento di failover con stato utilizza il collegamento di failover o l'interfaccia dati, 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
```

In questo esempio, 10.0.0.1 viene utilizzato come indirizzo IP attivo e 10.0.0.2 come indirizzo IP di standby per il collegamento di failover con stato.

```
hostname(config)#failover interface ip state 10.0.0.1 255.0.0.0
                      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 failover con stato non cambiano al failover a meno che non utilizzino un'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.**Nota:** se il collegamento di failover con stato utilizza il collegamento di failover o l'interfaccia dati, ignorare questo passaggio. L'interfaccia è già stata abilitata.

```
hostname(config)#interface phy_if

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

Nota: ad esempio, in questo scenario, Ethernet2 viene utilizzato per il collegamento di failover con stato:

```
hostname(config)#interface ethernet2

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

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

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.

7. Salvare la configurazione del sistema nella memoria flash.
```
hostname(config)#copy running-config startup-config
```

Configurazione unità secondaria

L'unica configurazione richiesta sull'unità secondaria è per l'interfaccia di failover. L'unità secondaria richiede che questi comandi comunichino inizialmente con l'unità primaria. Dopo che l'unità primaria invia la configurazione all'unità secondaria, l'unica differenza permanente tra le due configurazioni è il comando **failover lan unit**, che identifica ciascuna unità come primaria o secondaria.

In modalità contesto multiplo, tutti i passi vengono eseguiti nello spazio di esecuzione del sistema, se non diversamente specificato.

Per configurare l'unità secondaria, attenersi alla seguente procedura:

1. (solo piattaforma 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
```

   Nella presente documentazione, Ethernet0 viene utilizzato per un'interfaccia di failover LAN.
```
hostname(config)#failover lan interface failover Ethernet3
```

   L'argomento *if_name* assegna un nome all'interfaccia specificata dall'argomento *phy_if.*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
```

   In questa documentazione, per configurare il collegamento di failover, viene utilizzato 10.1.0.1 per il collegamento attivo, 10.1.0.2 per l'unità di standby e "failover" è il nome di

interfaccia Ethernet0.

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

Nota: immettere questo comando esattamente come è stato immesso sull'unità principale quando è stata configurata l'interfaccia di failover sull'unità principale.Abilitare l'interfaccia.

```
hostname(config)#interface phy_if

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

Ad esempio, in questo scenario per il failover viene utilizzato Ethernet0.

```
hostname(config)#interface ethernet3

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

3. (Facoltativo) 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 sono state precedentemente configurate.

4. Abilitare il failover.

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

Nota: dopo aver abilitato il failover, l'unità attiva invia la configurazione nella memoria in esecuzione all'unità in 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.

5. Al termine della replica della configurazione in esecuzione, salvare la configurazione nella memoria flash.

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

Configurazioni

Nel documento vengono usate queste configurazioni:

ASA principale

```
ASA#show running-config
 ASA Version 7.2(3)
!
!--- To set the firewall mode to transparent mode, !---
use the firewall transparent command !--- in global
configuration mode.

firewall transparent
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
```

```
 nameif failover

  description LAN Failover Interface
!
interface Ethernet1
 nameif inside
 security-level 100
!
interface Ethernet2
 nameif outside
 security-level 0

!--- Configure no shutdown in the stateful failover
interface !--- of both Primary and secondary ASA.

interface Ethernet3
 nameif state
 description STATE Failover Interface
!
interface Ethernet4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
access-list 100 extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500

!--- Assign the IP address to the Primary and !---
Seconday ASA Security Appliance. ip address 172.16.1.1
255.255.255.0 standby 172.16.1.2

failover
failover lan unit primary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover link state Ethernet3
failover interface ip failover 10.1.0.1 255.255.255.0
standby 10.1.0.2
failover interface ip state 10.0.0.1 255.0.0.0 standby
10.0.0.2

asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
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
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
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
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

ASA secondaria

```
ASA#show running-config
ASA Version 7.2(3)
!
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
failover
failover lan unit secondary
failover lan interface failover Ethernet0
failover lan enable
failover key ******
failover interface ip failover 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**.

ASA principale

```
ASA#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 00:08:03 UTC Jan 1 1993
        This host: Primary - Active
                Active time: 1820 (sec)
                  Interface inside (172.16.1.1): Normal
                  Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface inside (172.16.1.2): Normal
                  Interface outside (172.16.1.2): Normal

Stateful Failover Logical Update Statistics
        Link : state Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         185        0          183        0
        sys cmd         183        0          183        0
        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          0          0
        L2BRIDGE Tbl    2          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7012
        Xmit Q:         0       1       185
```

ASA secondaria

```
ASA(config)#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Secondary
Failover LAN Interface: failover Ethernet0 (up)
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(3), Mate 7.2(3)
Last Failover at: 16:39:12 UTC Aug 9 2009
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
```

```
                Interface inside (172.16.1.2): Normal
                Interface outside (172.16.1.2): Normal
        Other host: Primary - Active
                Active time: 1871 (sec)
                Interface inside (172.16.1.1): Normal
                Interface outside (172.16.1.1): Normal

Stateful Failover Logical Update Statistics
        Link : state Ethernet3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         183        0          183        0
        sys cmd         183        0          183        0
        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          0          0
        L2BRIDGE Tbl    0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       7043
        Xmit Q:         0       1       183
```

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

ASA principale

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             00:02:36 UTC Jan 1 1993

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

Unità Secondaria

```
ASA#show failover state
               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Standby Ready  None
Other host -   Primary
               Active         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

```
ASA#show failover interface
        interface failover Ethernet0
```

```
                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
        interface state Ethernet3
                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
```

Unità Secondaria

```
ASA#show failover interface
        interface failover Ethernet0
                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 state Ethernet3
                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.

ASA principale

```
ASA(config)#show monitor-interface
        This host: Primary - Active
                Interface inside (172.16.1.1): Normal
                Interface outside (172.16.1.1): Normal
        Other host: Secondary - Standby Ready
                Interface inside (172.16.1.2): Normal
                Interface outside (172.16.1.2): Normal
```

ASA secondaria

```
ASA(config)#show monitor-interface
        This host: Secondary - Standby Ready
                Interface inside (172.16.1.2): Normal
                Interface outside (172.16.1.2): Normal
        Other host: Primary - Active
                Interface inside (172.16.1.1): 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 per l'indirizzo IP e il monitoraggio dell'interfaccia rimane in stato di *attesa*. Per ulteriori informazioni sui diversi stati del failover, consultare la sezione show failover della *guida di riferimento dei comandi di Cisco Security Appliance, versione 7.2*.

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, completare i seguenti passaggi:

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/standby, immettere questo comando sull'unità attiva:
   ```
   hostname(config)#no failover active
   ```
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/standby, immettere questo comando sull'unità attiva:
   ```
   hostname(config)#failover active
   ```

Failover forzato

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

Immettere questo comando sull'unità di standby:

```
hostname#failover active
```

Immettere questo comando sull'unità attiva:

```
hostname#no 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 Imposizione del failover.

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'unità guasta a uno stato non guasto, immettere questo comando:

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

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 di interruzione per diritti di priorità e se l'unità su cui si è verificato l'errore è l'unità preferita.

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

- Monitoraggio failover
- Errore dell'unità
- %ASA-3-210005: Connessione di allocazione LU non riuscita
- Messaggi di sistema di failover
- Messaggi di debug
- SNMP
- Problemi noti

Monitoraggio failover

In questo esempio viene illustrato ciò che accade quando il failover non ha avviato il monitoraggio delle interfacce di rete. Il failover non inizia a monitorare le interfacce di rete fino a quando non riceve il secondo pacchetto `hello` dall'altra unità su quell'interfaccia. Questa operazione richiede circa 30 secondi. Se l'unità è collegata a uno switch di rete con Spanning Tree Protocol (STP), il tempo di `ritardo` in `avanti` configurato nello switch, in genere configurato come 15 secondi, più questo ritardo di 30 secondi. Infatti, all'avvio dell'ASA e subito dopo un evento di failover, lo switch di rete rileva un loop di bridge temporaneo. Dopo aver rilevato il loop, si ferma per inoltrare i pacchetti su queste interfacce per il tempo di `ritardo in avanti`. Entra quindi in modalità di `ascolto` per un ulteriore tempo di `ritardo`, entro il quale lo switch rimane in ascolto di loop del bridge ma non inoltra il traffico o i pacchetti `hello di` failover in avanti. Dopo il doppio del tempo di ritardo in avanti (30 secondi), il flusso del traffico riprende. Ciascuna appliance ASA rimane in modalità `di attesa` finché non riceve pacchetti di `benvenuto` dell'altra unità per 30 secondi. Nel periodo di tempo in cui l'ASA supera il traffico, non guasta l'altra unità a causa del mancato ascolto dei pacchetti `hello`. Il monitoraggio di tutti gli altri tipi di failover viene ancora eseguito, ovvero alimentazione, perdita del collegamento all'interfaccia e cavo di failover `pronto`.

Per il failover, Cisco consiglia di abilitare portfast su tutte le porte degli switch che si connettono a

interfacce ASA. Inoltre, su queste porte, il channeling e il trunking devono essere disabilitati. Se l'interfaccia dell'ASA si interrompe durante il failover, lo switch non deve attendere 30 secondi mentre la porta passa da uno stato di ascolto a uno stato di inoltro.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Active
Active time: 6930 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
Other host: Secondary - Standby
Active time: 15 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Normal (Waiting)
```

In sintesi, controllare questi passaggi per ridurre i problemi di failover:

- Controllare i cavi di rete collegati all'interfaccia in stato di attesa/guasto e, se possibile, sostituirli.
- Se tra le due unità è collegato uno switch, verificare che le reti collegate all'interfaccia in stato di attesa/errore funzionino correttamente.
- Verificare la porta dello switch connessa all'interfaccia in stato di attesa/errore e, se possibile, utilizzare l'altra porta FE sullo switch.
- Verificare di aver abilitato la porta fast e aver disabilitato sia il trunking che il channeling sulle porte dello switch connesse all'interfaccia.

Errore dell'unità

In questo esempio il failover ha rilevato un errore. Notare che l'origine dell'errore è l'interfaccia 1 sull'unità principale. Le unità sono di nuovo in modalità `attesa` a causa del guasto. L'unità guasta si è rimossa dalla rete (le interfacce sono inattive) e non invia più pacchetti `hello` sulla rete. L'unità attiva rimane in stato di `attesa` finché l'unità guasta non viene sostituita e le comunicazioni di failover vengono riavviate.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Standby (Failed)
Active time: 7140 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Failed (Waiting)
Other host: Secondary - Active
Active time: 30 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
```

Connessione di allocazione LU non riuscita

Se viene visualizzato questo messaggio di errore, è possibile che si sia verificato un problema di memoria:

```
Connessione di allocazione LU non riuscita
```

Questo problema è documentato nell'ID bug Cisco CSCte80027 (solo utenti registrati). Per risolvere il problema, aggiornare il firewall a una versione software in cui il bug è stato risolto. Alcune delle versioni software ASA in cui è stato risolto il bug sono la 8.2(4), la 8.3(2) e la 8.4(2).

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.

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.

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.

Polltime di failover

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

L'`unità polltime di failover msec [time]` esegue il polling dei messaggi di saluto per rappresentare l'intervallo di tempo in modo da verificare l'esistenza dell'unità di standby.

Analogamente, l'`unità di tempo di attesa del failover msec [time]` rappresenta l'impostazione di un periodo di tempo durante il quale un'unità deve ricevere un messaggio di benvenuto sul collegamento del failover, dopo il quale l'unità peer viene dichiarata non riuscita.

Per specificare i tempi di polling e di attesa dell'interfaccia dati in una configurazione di failover attivo/standby, utilizzare il comando **failover_time interface** in modalità di configurazione globale. Per ripristinare i tempi di polling e di attesa predefiniti, utilizzare la forma **no** di questo comando.

failover polltime interface [msec] *time* **[holdtime** *time***]**

Per modificare la frequenza di invio dei pacchetti hello sulle interfacce dati, usare il comando **failover polltime interface**. Questo comando è disponibile solo per il failover attivo/standby. Per il failover attivo/attivo, utilizzare il comando **polltime interface** in modalità di configurazione del gruppo di failover anziché il comando **failover polltime interface**.

Non è possibile immettere un valore di *tempo di attesa* inferiore a 5 volte il tempo di polling dell'interfaccia. Con tempi di polling più rapidi, l'appliance di sicurezza è in grado di rilevare i guasti e attivare il failover più rapidamente. Tuttavia, una rilevazione più rapida può causare switchover non necessari quando la rete è temporaneamente congestionata. Il test dell'interfaccia inizia quando un pacchetto hello non viene udito sull'interfaccia per oltre la metà del tempo di attesa.

Nella configurazione è possibile includere sia l'unità polltime di failover che i comandi dell'interfaccia polltime di failover.

Questo esempio imposta la frequenza del tempo di polling dell'interfaccia su 500 millisecondi e il tempo di attesa su 5 secondi:

```
hostname(config)#failover polltime interface msec 500 holdtime 5
```

Per ulteriori informazioni, consultare la sezione failover polltime della *guida di riferimento dei comandi di Cisco Security Appliance, versione 7.2*.

Esporta certificato/chiave privata nella configurazione di failover

Il dispositivo primario replica automaticamente la chiave privata o il certificato nell'unità secondaria. Usare il comando **write memory** nell'unità attiva per replicare la configurazione, compresa la chiave privata o del certificato, sull'unità in standby. Tutte le chiavi/i certificati sull'unità di standby vengono cancellati e ripopolati dalla configurazione dell'unità attiva.

Nota: non è necessario importare manualmente i certificati, le chiavi e i trust point dal dispositivo attivo ed esportarli nel dispositivo in standby.

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.

Problema: Il failover viene sempre eseguito dopo la configurazione del failover trasparente in modalità attiva/standby a più modalità

Il failover viene eseguito in modo stabile quando le interfacce interne di entrambe le appliance ASA sono connesse direttamente e le interfacce esterne di entrambe le appliance sono connesse direttamente. Tuttavia, il failover lampeggia quando si utilizza uno switch nel mezzo.

Soluzione: Per risolvere il problema, disabilitare la BPDU sulle interfacce ASA.

Failover dei moduli ASA

Se si utilizzano i moduli AIP-SSM (Advanced Inspection and Prevention Security Services Module) o CSC-SSM (Content Security and Control Security Services Module) in unità attive e in standby, il modulo funziona indipendentemente dall'ASA in termini di failover. **I moduli devono essere configurati manualmente nelle unità attive e in standby. Il failover non replica la configurazione del modulo.**

In termini di failover, le unità ASA che dispongono di moduli AIP-SSM o CSC-SSM devono essere dello stesso tipo di hardware. Ad esempio, se l'unità principale ha il modulo ASA-SSM-10, l'unità secondaria deve avere il modulo ASA-SSM-10.

Allocazione blocco messaggi di failover non riuscita

Messaggio di errore `%PIX|ASA-3-105010: Allocazione blocco messaggi di failover (primario) non riuscita`

Spiegazione: Memoria del blocco esaurita. Si tratta di un messaggio temporaneo che deve essere ripristinato dall'appliance di sicurezza. È inoltre possibile elencare *Primario* come *Secondario* per l'unità secondaria.

Azione consigliata: Usare il comando **show block** per monitorare la memoria del blocco corrente.

Problema di failover del modulo AIP

Se si hanno due appliance ASA in una configurazione di failover e ognuna ha un modulo AIP-SSM, è necessario replicare manualmente la configurazione degli accessori AIP-SSM. Solo la configurazione dell'ASA viene replicata dal meccanismo di failover. AIP-SSM non è incluso nel failover.

In primo luogo, l'AIP-SSM funziona indipendentemente dall'ASA in termini di failover. Per il failover, dal punto di vista dell'ASA è sufficiente che i moduli AIP siano dello stesso tipo di hardware. Inoltre, come per qualsiasi altra parte del failover, la configurazione dell'ASA tra lo stato attivo e quello in standby deve essere sincronizzata.

Per quanto riguarda la configurazione delle AIP, esse sono effettivamente sensori indipendenti. Non c'è failover tra i due, e non hanno alcuna consapevolezza l'uno dell'altro. Possono eseguire versioni indipendenti del codice. In altre parole, non devono corrispondere e l'ASA non è interessata alla versione del codice sull'AIP per quanto riguarda il failover.

ASDM avvia una connessione all'AIP tramite l'IP dell'interfaccia di gestione configurato sull'AIP. In altre parole, si connette al sensore in genere tramite HTTPS, che dipende da come è stato configurato il sensore.

Èpossibile avere un failover dell'ASA indipendente dai moduli IPS (AIP). Si è ancora connessi alla stessa rete perché si è connessi all'IP di gestione. Per connettersi all'altro provider di servizi Internet, è necessario riconnettersi al relativo indirizzo IP di gestione per configurarlo e accedervi.

Per ulteriori informazioni, fare riferimento al documento ASA: Inviare il traffico di rete dall'ASA all'esempio di configurazione SSM dell'AIP per ulteriori informazioni e configurazioni di esempio su come inviare il traffico di rete che attraversa l'appliance ASA 5500 Adaptive Security (ASA) al modulo AIP-SSM (Advanced Inspection and Prevention Security Services Module)

Problemi noti

Quando si tenta di accedere ad ASDM sull'appliance ASA secondaria con software versione 8.x e ASDM versione 6.x per la configurazione del failover, viene visualizzato questo errore:

```
Errore: Il nome nel certificato di protezione non è valido o non corrisponde al nome del sito
```

Nel certificato, l'autorità emittente e il nome del soggetto corrispondono all'indirizzo IP dell'unità *attiva* e non all'indirizzo IP dell'unità *di standby*.

In ASA versione 8.x, il certificato interno (ASDM) viene replicato dall'unità attiva all'unità di standby, generando un messaggio di errore. Tuttavia, se lo stesso firewall viene eseguito sul codice versione 7.x con ASDM 5.x e si tenta di accedere ad ASDM, viene visualizzato questo normale avviso di protezione:

```
Il nome del certificato di protezione è valido e corrisponde al nome della pagina che si sta
tentando di visualizzare
```

Quando si controlla il certificato, l'autorità emittente e il nome del soggetto corrispondono all'indirizzo IP dell'unità di standby.

Informazioni correlate

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