ASA/PIX: Come utilizzare la CLI per aggiornare l'immagine software su una coppia di failover

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Prodotti correlati](#)
[Convenzioni](#)
[Configurazione](#)
[Eseguire aggiornamenti senza interruzione delle attività per coppie di failover](#)
[Aggiornare una configurazione di failover attivo/standby](#)
[Aggiornare una configurazione di failover attivo/attivo](#)
[Risoluzione dei problemi](#)
[%ASA-5-72012: (VPN-Secondario) Impossibile aggiornare i dati di runtime del failover IPSec sull'unità di standby o su %ASA-6-720012: (unità VPN) Impossibile aggiornare i dati di runtime di failover di IPSec sull'unità in standby](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive come usare la CLI per aggiornare l'immagine software su una coppia di failover di Cisco ASA serie 5500 Adaptive Security Appliance.

Nota: Adaptive Security Device Manager (ASDM) non funziona se si aggiorna (o si declassa) direttamente il software dell'appliance di sicurezza dalla versione 7.0 alla 7.2 o si aggiorna (o si declassa) direttamente il software ASDM dalla versione 5.0 alla 5.2. È necessario eseguire l'aggiornamento o il downgrade in ordine incrementale.

Per ulteriori informazioni su come aggiornare l'ASDM e l'immagine software sull'appliance ASA, consultare il documento PIX/ASA: esempio di configurazione per aggiornare un'immagine software con ASDM o dalla CLI

Nota: nella modalità multicontext, non è possibile usare il comando **copy tftp flash** per aggiornare o effettuare il downgrade dell'immagine PIX/ASA in tutti i contesti; è supportato solo in modalità di esecuzione del sistema.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Cisco Adaptive Security Appliance (ASA) con versione 7.0 e successive
- Cisco ASDM versione 5.0 e successive

Nota: per informazioni su come consentire all'ASA di essere configurata dall'ASDM, consultare il documento sull'autorizzazione dell'accesso HTTPS per ASDM.

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 il software Cisco PIX serie 500 Security Appliance versione 7.0 e successive.

Convenzioni

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

Configurazione

Eseguire aggiornamenti senza interruzione delle attività per coppie di failover

Le due unità in una configurazione di failover devono avere la stessa versione del software principale (primo numero) e secondaria (secondo numero). Tuttavia, non è necessario mantenere la parità della versione sulle unità durante il processo di upgrade; è possibile avere versioni diverse del software in esecuzione su ciascuna unità e mantenere il supporto del failover. Per garantire compatibilità e stabilità a lungo termine, Cisco consiglia di aggiornare entrambe le unità alla stessa versione il più presto possibile.

Sono disponibili 3 tipi di aggiornamenti. Essi sono i seguenti:

1. **Release di manutenzione**: è possibile eseguire l'aggiornamento da qualsiasi release di manutenzione a qualsiasi altra release di manutenzione all'interno di una release secondaria. Ad esempio, è possibile eseguire l'aggiornamento da 7.0(1) a 7.0(4) senza prima installare le versioni di manutenzione intermedie.
2. **Release secondaria**: è possibile eseguire l'aggiornamento da una release secondaria alla release secondaria successiva. Non è possibile ignorare una versione secondaria. Ad esempio, è possibile eseguire l'aggiornamento da 7.0 a 7.1. L'aggiornamento da 7.0 direttamente a 7.2 non è supportato per gli aggiornamenti senza interruzione delle attività. è necessario eseguire prima l'aggiornamento a 7.1

3. **Release principale** - È possibile eseguire l'aggiornamento dall'ultima release secondaria della versione precedente alla release principale successiva. Ad esempio, è possibile eseguire l'aggiornamento dalla versione 7.9 alla versione 8.0, supponendo che la versione 7.9 sia l'ultima versione secondaria della versione 7.x.

Aggiornare una configurazione di failover attivo/standby

Completare questa procedura per aggiornare due unità in una configurazione di *failover attivo/standby*:

1. Scaricare il nuovo software su entrambe le unità e specificare la nuova immagine da caricare con il comando boot system.per ulteriori informazioni, fare riferimento a Aggiornamento di un'immagine software e di un'immagine ASDM tramite CLI.
2. Ricaricare l'unità in standby per avviare la nuova immagine immettendo il comando **failover reload-standby** sull'unità attiva, come mostrato di seguito:
```
active#failover reload-standby
```

3. Quando l'unità in standby ha terminato il ricaricamento ed è in stato Standby Ready, forzare l'unità attiva a eseguire il failover sull'unità in standby immettendo il comando **no failover active** sull'unità attiva.
```
active#no failover active
```

   Nota: per verificare che l'unità in standby sia in stato pronto, usare il comando **show failover**.
4. Ricaricare la precedente unità attiva (ora la nuova unità in standby) immettendo il comando **reload**:
```
newstandby#reload
```

5. Quando la nuova unità in standby ha terminato il ricaricamento ed è in stato Standby Ready (Pronta per standby), ripristinare lo stato attivo dell'unità attiva originale immettendo il comando **failover active**:
```
newstandby#failover active
```

Il processo di aggiornamento di una coppia di failover attivo/standby è stato completato.

Aggiornare una configurazione di failover attivo/attivo

Completare questa procedura per aggiornare due unità in una configurazione di *failover attivo/attivo*:

1. Scaricare il nuovo software su entrambe le unità e specificare la nuova immagine da caricare con il comando boot system.per ulteriori informazioni, fare riferimento a Aggiornamento di un'immagine software e di un'immagine ASDM tramite CLI.
2. Rendere entrambi i gruppi di failover attivi sull'unità primaria immettendo il comando **failover attivo** nello spazio di esecuzione del sistema dell'unità primaria:
```
primary#failover active
```

3. Ricaricare l'unità secondaria per avviare la nuova immagine immettendo il comando **failover reload-standby** nello spazio di esecuzione del sistema dell'unità primaria:
```
primary#failover reload-standby
```

4. Al termine del ricaricamento dell'unità secondaria ed entrambi i gruppi di failover sono in stato Standby Ready sull'unità, rendere entrambi i gruppi di failover attivi sull'unità secondaria utilizzando il comando no failover active nello spazio di esecuzione del sistema dell'unità primaria:
```
primary#no failover active
```

   Nota: utilizzare il comando show failover per verificare che entrambi i gruppi di failover siano in stato Standby Ready sull'unità secondaria.
5. Verificare che entrambi i gruppi di failover siano in stato Standby Ready sull'unità primaria, quindi ricaricare l'unità primaria utilizzando il comando reload:
```
primary#reload
```

6. Se i gruppi di failover sono configurati con il comando preempt, diventeranno automaticamente attivi sull'unità designata dopo il superamento del ritardo. Se i gruppi di failover non sono configurati con il comando preempt, è possibile ripristinarne lo stato attivo sulle unità designate utilizzando il comando failover active group.

Risoluzione dei problemi

%ASA-5-72012: (VPN-Secondario) Impossibile aggiornare i dati di runtime del failover IPSec sull'unità di standby o su %ASA-6-720012: (unità VPN) Impossibile aggiornare i dati di runtime di failover di IPSec sull'unità in standby

Problema

Quando si cerca di aggiornare Cisco Adaptive Security Appliance (ASA), viene visualizzato uno dei seguenti messaggi di errore:

```
%ASA-5-72012: (VPN-Secondario) Impossibile aggiornare i dati di runtime del failover IPSec
sull'unità in standby.
```

```
%ASA-6-72012: (unità VPN) Impossibile aggiornare i dati di runtime del failover IPsec sull'unità
in standby.
```

Soluzione

Questi messaggi di errore sono errori informativi. I messaggi non influiscono sulla funzionalità dell'ASA o della VPN.

Questi messaggi vengono visualizzati quando il sottosistema di failover VPN non è in grado di aggiornare i dati di runtime relativi a IPsec perché il tunnel IPsec corrispondente è stato eliminato dall'unità in standby. Per risolvere questi problemi, eseguire il comando **wr standby** sull'unità attiva.

Per risolvere questo problema, sono stati archiviati due bug: è possibile aggiornare il software alla versione dell'ASA in cui i bug sono stati risolti. Per ulteriori informazioni, fare riferimento agli ID bug Cisco CSCtj58420 (solo utenti registrati) e CSCtn56517 (solo utenti registrati).

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Cisco Adaptive Security Device Manager
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems