ASA/PIX: Verwendung der CLI zum Aktualisieren des Software-Images auf einem Failover-Paar

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie das Software-Image mithilfe der CLI auf einem Failover-Paar der Cisco Adaptive Security Appliances der Serie ASA 5500 aktualisieren.

Hinweis: Der Adaptive Security Device Manager (ASDM) funktioniert nicht, wenn Sie die Security Appliance-Software direkt von 7.0 auf 7.2 aktualisieren (oder herabstufen) oder die ASDM-Software direkt von 5.0 auf 5.2 aktualisieren (oder herabstufen). Sie müssen ein Upgrade (oder Downgrade) in inkrementeller Reihenfolge durchführen.

Weitere Informationen zum Upgrade von ASDM und Software-Image auf ASA finden Sie unter PIX/ASA: Aktualisieren eines Software-Image mithilfe eines ASDM- oder CLI-Konfigurationsbeispiels

Hinweis: Im Multi-Context-Modus können Sie den Befehl **copy tftp flash** nicht verwenden, um das PIX/ASA-Image in allen Kontexten zu aktualisieren oder herabzusetzen. wird nur im System Exec-Modus unterstützt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance (ASA) ab Version 7.0
- Cisco ASDM Version 5.0 oder höher

Hinweis: Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco Security Appliance Software Version 7.0 und höher der Serie PIX 500 verwendet werden.

Konventionen

Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Konfiguration

Durchführung von Upgrades ohne Ausfallzeiten für Failover-Paare

Die beiden Einheiten in einer Failover-Konfiguration sollten die gleiche Version der Haupt- (First Number) und Nebensoftware (Second Number) aufweisen. Sie müssen jedoch während des Aktualisierungsvorgangs keine Versionsparität auf den Einheiten beibehalten. Sie können auf jeder Einheit verschiedene Softwareversionen ausführen und weiterhin Failover-Unterstützung erhalten. Um langfristige Kompatibilität und Stabilität zu gewährleisten, empfiehlt Cisco, dass Sie beide Geräte so bald wie möglich auf die gleiche Version aktualisieren.

Es stehen drei Arten von Upgrades zur Verfügung. Sie sind wie folgt:

1. **Maintenance Release** - Sie können von jeder Maintenance-Version auf jede andere Maintenance-Version in einer Nebenversion aktualisieren. Beispielsweise können Sie ein Upgrade von 7.0(1) auf 7.0(4) durchführen, ohne zuvor die Wartungsversionen dazwischen zu installieren.
2. **Nebenversion** - Sie können von einer Nebenversion auf die nächste Nebenversion aktualisieren. Eine Nebenversion kann nicht übersprungen werden. Beispielsweise können Sie ein Upgrade von 7.0 auf 7.1 durchführen. Upgrades von 7.0 direkt auf 7.2 werden bei Upgrades ohne Ausfallzeiten nicht unterstützt. Sie müssen zuerst ein Upgrade auf 7.1 durchführen
3. **Hauptversion** - Sie können von der letzten Nebenversion der vorherigen Version auf die

nächste Hauptversion aktualisieren. Beispielsweise können Sie ein Upgrade von 7.9 auf 8.0 durchführen, vorausgesetzt, dass 7.9 die letzte Nebenversion in der Version 7.x ist.

Aktualisieren einer Active/Standby-Failover-Konfiguration

Gehen Sie wie folgt vor, um zwei Einheiten in einer *Aktiv/Standby-Failover*-Konfiguration zu aktualisieren:

1. Laden Sie die neue Software auf beide Einheiten herunter, und geben Sie das neue Image an, das mit dem Boot-System-Befehl geladen werden soll.Weitere Informationen finden Sie unter Aktualisieren eines Software-Images und eines ASDM-Images mithilfe der CLI.
2. Laden Sie die Standby-Einheit neu, um das neue Image zu starten, indem Sie den **Befehl Failover reload-standby auf der aktiven Einheit wie folgt** eingeben:
   ```
   active#failover reload-standby
   ```
3. Wenn die Standby-Einheit das Neuladen abgeschlossen hat und sich im Standby-Bereitschaftszustand befindet, erzwingen Sie den Failover-Aktiv-Vorgang zum Standby-Gerät, indem Sie den **Befehl no failover active auf der aktiven Einheit** eingeben.
   ```
   active#no failover active
   ```

   Hinweis: Verwenden Sie den **Befehl show failover**, um zu überprüfen, ob sich die Standby-Einheit im Standby-Bereitschaftszustand befindet.
4. Laden Sie die frühere aktive Einheit (jetzt die neue Standby-Einheit) neu, indem Sie den **Befehl reload (Neuladen) eingeben**:
   ```
   newstandby#reload
   ```
5. Wenn die neue Standby-Einheit das Neuladen beendet hat und sich im Standby-Bereitschaftszustand befindet, setzen Sie die ursprüngliche aktive Einheit wieder in den aktiven Status zurück, indem Sie den **Befehl failover active eingeben**:
   ```
   newstandby#failover active
   ```

Damit ist das Upgrade eines Active/Standby-Failover-Paars abgeschlossen.

Upgrade einer Active/Active Failover-Konfiguration

Gehen Sie wie folgt vor, um zwei Einheiten in einer *Aktiv/Aktiv-Failover*-Konfiguration zu aktualisieren:

1. Laden Sie die neue Software auf beide Einheiten herunter, und geben Sie das neue Image an, das mit dem Boot-System-Befehl geladen werden soll.Weitere Informationen finden Sie unter Aktualisieren eines Software-Images und eines ASDM-Images mithilfe der CLI.
2. Aktivieren Sie beide Failover-Gruppen auf der Primäreinheit, indem Sie den **Befehl failover active im Systemausführungsbereich der Primäreinheit** eingeben:
   ```
   primary#failover active
   ```
3. Laden Sie die Sekundäreinheit neu, um das neue Image zu starten, indem Sie den **Befehl Failover reload-standby in den Systemausführungsbereich der Primäreinheit** eingeben:
   ```
   primary#failover reload-standby
   ```

4. Wenn die zweite Einheit das Neuladen abgeschlossen hat und sich beide Failover-Gruppen auf dieser Einheit im Standby-Bereitschaftszustand befinden, aktivieren Sie beide Failover-Gruppen auf der zweiten Einheit mithilfe des **Befehls** no failover active **im Systemausführungsbereich der primären Einheit:**
```
primary#no failover active
```

   Hinweis: Verwenden Sie den **Befehl** show failover, um zu überprüfen, ob sich beide Failover-Gruppen auf der Sekundäreinheit im Standby-Bereitschaftszustand befinden.
5. Stellen Sie sicher, dass sich beide Failover-Gruppen auf der primären Einheit im Standby-Bereitschaftszustand befinden, und laden Sie die primäre Einheit dann mithilfe des **Befehls** reload (Neuladen) neu:
```
primary#reload
```

6. Wenn die Failover-Gruppen mit dem **Befehl** preempt konfiguriert sind**,** werden sie nach Ablauf der Freischaltungsverzögerung automatisch auf ihrer festgelegten Einheit aktiv. Wenn die Failover-Gruppen nicht mit dem **Befehl** preempt konfiguriert sind, können Sie sie mithilfe des **Befehls Failover active group** in den aktiven Status der angegebenen Einheiten zurücksetzen.

Fehlerbehebung

%ASA-5-72012: (VPN-Sekundär) Aktualisierung der IPSec-Failover-Laufzeitdaten auf der Standby-Einheit (oder) %ASA-6-720012: (VPN-Einheit) IPsec-Failover-Laufzeitdaten auf der Standby-Einheit konnten nicht aktualisiert werden

Problem

Eine der folgenden Fehlermeldungen wird angezeigt, wenn Sie versuchen, ein Upgrade der Cisco Adaptive Security Appliance (ASA) durchzuführen:

```
%ASA-5-72012: (VPN-Sekundär) IPSec-Failover-Laufzeitdaten konnten auf der Standby-Einheit nicht
aktualisiert werden.
```

```
%ASA-6-72012: (VPN-Einheit) IPsec-Failover-Laufzeitdaten konnten auf der Standby-Einheit nicht
aktualisiert werden.
```

Lösung

Diese Fehlermeldungen sind informative Fehler. Die Nachrichten wirken sich nicht auf die Funktionen der ASA oder des VPN aus.

Diese Meldungen werden angezeigt, wenn das VPN-Failover-Subsystem IPsec-bezogene Laufzeitdaten nicht aktualisieren kann, da der entsprechende IPsec-Tunnel auf der Standby-Einheit gelöscht wurde. Um diese Probleme zu beheben, führen Sie den Befehl **wr standby** auf der aktiven Einheit aus.

Zwei Fehler wurden zur Behebung dieses Verhaltens eingereicht. Sie können auf eine Softwareversion der ASA aktualisieren, in der diese Fehler behoben sind. Weitere Informationen finden Sie unter Cisco Bug IDs CSCtj58420 (nur registrierte Kunden) und CSCtn56517 (nur registrierte Kunden).

Zugehörige Informationen

- Cisco Adaptive Security Appliances der Serie ASA 5500
- Cisco Adaptive Security Device Manager
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems