ASA/PIX: Cómo utilizar el CLI para actualizar la imagen del software en un par de fallas

Contenido

Introducción

Este documento describe cómo utilizar el CLI para actualizar la imagen del software en un par de fallas del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500.

Nota: El Administrador de dispositivos de seguridad adaptante (ASDM) no trabaja si usted actualiza (o downgrade) el software del dispositivo de seguridad a partir del 7.0 a 7.2 directamente o actualiza (o downgrade) el software ASDM a partir del 5.0 a 5.2 directamente. Usted debe actualizar (o downgrade) en la orden ampliada.

Para más información sobre cómo actualizar el ASDM y la imagen del software en el ASA, refiera al PIX/ASA: Actualice una imagen del software usando el ASDM o el ejemplo de la configuración CLI

Nota: En el modo del multicontext, usted no puede utilizar el **comando copy tftp flash** de actualizar o de retroceder la imagen del PIX/ASA en todos los contextos; se soporta solamente en el modo EXEC del sistema.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo de seguridad adaptante de Cisco (ASA) con la versión 7.0 y posterior
- Cisco ASDM versión 5.0 y posterior

Nota: Refiera a permitir el acceso HTTPS para el ASDM para la información sobre cómo permitir que el ASA sea configurado por el ASDM.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración también se puede utilizar con la Cisco PIX 500 Series Security Appliance Software Version 7.0 y posterior.

Convenciones

Refiera a los convenios de los consejos técnicos de Cisco para la información sobre las convenciones sobre documentos.

Configuración

Realice las actualizaciones del Cero-tiempo muerto para los pares de fallas

Las dos unidades en una configuración de failover deben tener la misma versión de software principal (primer número) y de menor importancia (del segundo número). Sin embargo, usted no necesita mantener la paridad de la versión en las unidades durante el proceso de actualización; usted puede tener diversas versiones en el software que se ejecuta en cada unidad y todavía mantener el soporte de la Conmutación por falla. Para asegurar la compatibilidad a largo plazo y la estabilidad, Cisco recomienda que usted actualiza ambas unidades a la misma versión cuanto antes.

Hay 3 tipos de actualizaciones disponibles. Éstas son:

1. **Versión de mantenimiento** — Usted puede actualizar de cualquier versión de mantenimiento a cualquier otra versión de mantenimiento dentro de una versión menor. Por ejemplo, usted puede actualizar a partir la 7.0(1) a 7.0(4) sin primero instalar las versiones de mantenimiento mientras tanto.
2. **Versión menor** — Usted puede actualizar de una versión menor a la versión menor siguiente. Usted no puede saltar una versión menor. Por ejemplo, usted puede actualizar a partir el 7.0 a 7.1. El actualizar a partir del 7.0 directamente a 7.2 no se soporta para las actualizaciones del cero-tiempo muerto; usted debe primero actualizar a 7.1

3. **Versión principal** — Usted puede actualizar de la versión menor más reciente de la versión anterior a la versión principal siguiente. Por ejemplo, usted puede actualizar a partir el 7.9 a 8.0, si se asume que 7.9 es la versión menor más reciente de la versión 7.x.

Actualice una configuración de failover activa/espera

Complete estos pasos para actualizar dos unidades en una *configuración de failover activa/espera*:

1. Descargue el nuevo software a ambas unidades, y especifique la nueva imagen para cargar con el comando boot system.Refiera a la actualización una imagen del software y una Imagen de ASDM usando el CLI para más información.
2. Recargue la unidad en espera para iniciar la nueva imagen ingresando el comando recarga-espera de la Conmutación por falla en la unidad activa como se muestra abajo:`active#failover reload-standby`
3. Cuando la unidad en espera ha acabado recargar y está en el estado Ready (Listo) espera, fuerce la unidad activa para fallar encima a la unidad en espera ingresando el comando no failover active en la unidad activa.`active#no failover active` **Nota:** Utilice el comando show failover para verificar que la unidad en espera está en el estado Ready (Listo) espera.
4. Recargue la unidad activa anterior (ahora la nueva unidad en espera) ingresando el comando reload:`newstandby#reload`
5. Cuando la nueva unidad en espera ha acabado recargar y está en el estado Ready (Listo) espera, vuelva la unidad activa original al estado activo ingresando el comando failover active:`newstandby#failover active`

Esto completa el proceso de actualizar un par de fallas activo/espera.

Actualice una configuración de failover activa/activa

Complete estos pasos para actualizar dos unidades en una *configuración de failover activa/activa*:

1. Descargue el nuevo software a ambas unidades, y especifique la nueva imagen para cargar con el comando boot system.Refiera a la actualización una imagen del software y una Imagen de ASDM usando el CLI para más información.
2. Haga ambos grupos de la Conmutación por falla el active en la unidad primaria ingresando el comando failover active en el espacio de la ejecución del sistema de la unidad primaria:`primary#failover active`
3. Recargue la unidad secundaria para iniciar la nueva imagen ingresando el comando recarga-espera de la Conmutación por falla en el espacio de la ejecución del sistema de la unidad primaria:`primary#failover reload-standby`
4. Cuando la unidad secundaria ha acabado el recargar, y ambos grupos de la Conmutación por falla están en el estado Ready (Listo) espera en esa unidad, hacen ambos grupos de la Conmutación por falla el active en la unidad secundaria usando el comando no failover active en el espacio de la ejecución del sistema de la unidad primaria:`primary#no failover active` **Nota:** Utilice el comando show failover para verificar que ambos grupos de la Conmutación por falla están en el estado Ready (Listo) espera en la unidad secundaria.
5. Aseegurese a ambos grupos de la Conmutación por falla están en el estado Ready (Listo) espera en la unidad primaria, y después recargan la unidad primaria usando el comando reload:`primary#reload`

6. Si configuran a los grupos de la Conmutación por falla con el comando de la apropiación, harán automáticamente activos en su unidad señalada después de que el retardo de la apropiación haya pasado. Si no configuran a los grupos de la Conmutación por falla con el comando de la apropiación, usted puede volverlos al estado activo en sus unidades señaladas usando el comando group del active de la Conmutación por falla.

Troubleshooting

%ASA-5-720012: ((VPN-Secundario) no podido poner al día los datos del tiempo de ejecución de failover del IPSec sobre la unidad standby (o) %ASA-6-720012: ((VPN-unidad) no podido poner al día los datos del tiempo de ejecución de failover del IPSec sobre la unidad standby

Problema

Uno de estos mensajes de error aparece cuando usted intenta actualizar el dispositivo de seguridad adaptante de Cisco (ASA):

```
%ASA-5-720012: (VPN-Secundario) no podido poner al día los datos del tiempo de ejecución de
failover del IPSec sobre la unidad standby.

%ASA-6-720012: (VPN-unidad) no podido poner al día los datos del tiempo de ejecución de failover
del IPSec sobre la unidad standby.
```

Solución

Estos mensajes de error son errores informativos. Los mensajes no afectan las funciones del ASA o del VPN.

Estos mensajes aparecen cuando el subsistema de failover VPN no puede poner al día los datos IPSec-relacionados del tiempo de ejecución porque el túnel IPsec correspondiente se ha borrado en la unidad standby. Para resolver éstos, funcione con el **comando standby del wr** en la unidad activa.

Dos bug se han clasifiado para dirigir este comportamiento; usted puede actualizar a una versión de software del ASA donde se reparan estos bug. Consulte los ID de bug de Cisco CSCtj58420 (clientes registrados solamente) y CSCtn56517 (clientes registrados solamente) para obtener más información.

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Adaptive Security Device Manager
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems