

PIX/ASA: Ejemplo activo/activo de la configuración de failover

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Convenciones](#)

[Conmutación por falla activa/activa](#)

[Descripción activa/activa de la Conmutación por falla](#)

[Estado Primario/Secundario y Estado Activo/Standby](#)

[Sincronización de la Configuración e Inicialización del dispositivo](#)

[Réplica de Comandos](#)

[Disparadores del Failover](#)

[Acciones de Failover](#)

[Regular y Stateful Failover](#)

[Regular Failover](#)

[Stateful Failover](#)

[Limitaciones de la configuración de failover](#)

[Características no admitidas](#)

[Configuración de failover activa/activa Cable-basada](#)

[prerrequisitos](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración de failover activa/activa basada en LAN](#)

[Diagrama de la red](#)

[Configuración de la Unidad Primaria](#)

[Configuración de la Unidad Secundaria](#)

[Configuraciones](#)

[Verificación](#)

[Uso del Comando show failover](#)

[Vista de las Interfaces Monitoreadas](#)

[Visualización de los Comandos de Failover en la Configuración en Ejecución](#)

[Pruebas de Funcionalidad de Failover](#)

[Failover Forzado](#)

[Failover Inhabilitado](#)

[Restauración de una Unidad Defectuosa](#)

[Reemplazar la Unidad Defectuosa por una Nueva Unidad](#)

[Troubleshooting](#)

[Mensajes del sistema de fallas](#)

[Comunicaciones de fallas perdidas primarias con el compañero en el interface name de la interfaz](#)

[Mensajes del debug](#)

[SNMP](#)

[Tiempo de sondeo de fallas](#)

[ADVERTENCIA: Incidente del desciframiento del mensaje de falla.](#)

[Información Relacionada](#)

[Introducción](#)

La configuración de failover requiere dos dispositivos de seguridad idénticos conectados el uno al otro a través de un link de failover dedicado y, opcionalmente, de un link de stateful failover. El estado de las unidades y las interfaces activas se monitorea para determinar si se cumplen las condiciones específicas de failover. Si se cumplen esas condiciones, el failover ocurre.

El dispositivo de seguridad soporta dos **Conmutaciones por falla activas/activas de las** configuraciones de failover, y la **Conmutación por falla activa/espera**. Cada configuración de failover tiene su propio método para determinar y para ejecutar el failover. Con Active/Active Failover, ambas unidades pueden pasar el tráfico de red. Esto le permite configurar el balanceo de carga en su red. Active/Active Failover está solamente disponible en las unidades que se ejecutan en el modo multiple context. Con Active/Standby Failover, solamente una unidad pasa el tráfico mientras que la otra unidad espera en estado standby. Active/Standby Failover está disponible en las unidades que se ejecutan en el modo single context o multiple context. Ambas configuraciones de failover soportan el stateful failover o el stateless (regular) failover.

Este documento se centra en cómo configurar una Conmutación por falla activa/activa en el dispositivo de seguridad del PIX/ASA de Cisco.

Refiera al [PIX/ASA ejemplo activo/espera 7.x de la configuración de failover](#) para aprender más información sobre las configuraciones de failover activas/espera.

Nota: Failover VPN no se soporta en las unidades que se ejecutan en el modo multiple context dado que VPN no se soporta en el contexto múltiple. Failover VPN está disponible solamente para las **configuraciones Active/Standby Failover** en las configuraciones de contexto simple.

Esta guía de configuración proporciona una configuración de muestra para incluir una introducción abreviada al PIX/ASA tecnología activa/activa 7.x. Refiera a la [referencia de comandos del dispositivo del Cisco Security, versión 7.2](#) para un sentido más profundizado de la teoría basada detrás de esta tecnología.

[prerrequisitos](#)

[Requisitos](#)

Requisito de Hardware

Las dos unidades en una configuración de failover deben tener la misma configuración de

hardware. Deben tener el mismo modelo, el mismo número y los mismos tipos de interfaces, y la misma cantidad de RAM.

Nota: Las dos unidades no necesitan tener el mismo tamaño de memoria Flash. Si usted utiliza unidades con diversos tamaños de memoria Flash en su configuración de failover, asegúrese de que la unidad con la memoria Flash más pequeña tenga bastante espacio para acomodar los archivos de imagen de software y los archivos de configuración. Si no lo hace, la sincronización de la configuración de la unidad con la memoria Flash más grande a la unidad con la memoria Flash más pequeña falla.

Requisito de Software

Las dos unidades en una configuración de failover deben estar en los modos de funcionamiento (routed o transparent, single o multiple context). Deben tener la misma versión de software principal (primer número) y de menor importancia (segundo número), pero usted puede utilizar diversas versiones del software dentro de un proceso de actualización; por ejemplo, usted puede actualizar una unidad de la Versión 7.0(1) a la Versión 7.0(2) y hacer que el failover siga siendo activo. Cisco recomienda que usted actualiza ambas unidades a la misma versión para asegurar la compatibilidad a largo plazo.

Refiera a [realizar las actualizaciones cero del tiempo muerto para los pares de fallas](#) para más información sobre actualizar el software en un par de fallas.

Requisitos de Licencia

En la plataforma del dispositivo de seguridad del PIX/ASA, por lo menos una de las unidades debe tener una **licencia sin restricción (del UR)**. La otra unidad puede tener una licencia Activo-activa de la Conmutación por falla solamente (FO_AA), u otra licencia del UR. Las unidades con una licencia limitada no se pueden utilizar para la Conmutación por falla, y dos unidades con las licencias FO_AA no se pueden utilizar juntas como par de fallas.

Nota: Usted puede ser que necesite actualizar las licencias en un par de fallas para obtener las características adicionales y las ventajas. Para obtener más información sobre la actualización, consulte la [Actualización de la Clave de Licencia en un Par de Failover](#)

Nota: Las funciones cubiertas por la licencia, tales como SSL VPN miran o los contextos de seguridad, en ambos dispositivos de seguridad que participen en la Conmutación por falla deben ser idénticos.

Nota: La licencia FO no soporta la Conmutación por falla activa/activa.

Componentes Utilizados

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

- Dispositivo de seguridad PIX con la versión 7.x y posterior

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 las siguientes versiones de hardware y software:

- ASA con la versión 7.x y posterior

Nota: La Conmutación por falla activa/activa no está disponible en el dispositivo de seguridad adaptante de las 5505 Series ASA.

[Convenciones](#)

Refiera a los [convenios de los consejos técnicos de Cisco](#) para más convenciones sobre documentos de la información.

[Conmutación por falla activa/activa](#)

Esta sección describe Active/Standby Failover e incluye estos temas:

- [Descripción activa/activa de la Conmutación por falla](#)
- [Estado Primario/Secundario y Estado Activo/Standby](#)
- [Sincronización de la Configuración e Inicialización del dispositivo](#)
- [Réplica de Comandos](#)
- [Disparadores del Failover](#)
- [Acciones de Failover](#)

[Descripción activa/activa de la Conmutación por falla](#)

La Conmutación por falla activa/activa está solamente disponible para los dispositivos de seguridad en el modo de contexto múltiple. En una configuración de failover activa/activa, ambos dispositivos de seguridad pueden pasar el tráfico de la red.

En la Conmutación por falla activa/activa, usted divide los contextos de seguridad en el dispositivo de seguridad en los grupos de la Conmutación por falla. Un grupo de la Conmutación por falla es simplemente un grupo lógico de uno o más contextos de seguridad. Usted puede crear un máximo de dos grupos de la Conmutación por falla en el dispositivo de seguridad. El contexto admin es siempre un miembro del group1 de la Conmutación por falla. Cualquier contextos de seguridad no asignado es también miembros del group1 de la Conmutación por falla por abandono.

El grupo de la Conmutación por falla forma la unidad base para la Conmutación por falla en la Conmutación por falla activa/activa. Interconecte la supervisión del error, Conmutación por falla, y estado activo/en espera sea todos los atributos de un grupo de la Conmutación por falla bastante que la unidad. Cuando un grupo activo de la Conmutación por falla falla, cambia al estado espera mientras que el grupo espera de la Conmutación por falla hace activo. Las interfaces en el grupo de la Conmutación por falla que hace activo asumen el MAC y los IP Addresses de las interfaces en el grupo de la Conmutación por falla que falló. Las interfaces en el grupo de la Conmutación por falla que ahora está en el estado espera asumen el control el MAC espera y los IP Addresses.

Nota: Un grupo de la Conmutación por falla que falla en una unidad no significa que la unidad ha fallado. La unidad puede todavía tener otro grupo de la Conmutación por falla que pasa el tráfico en ella.

Estado Primario/Secundario y Estado Activo/Standby

Como en la Conmutación por falla activa/espera, una unidad en un par de fallas activo/activo se señala la unidad primaria, y la otra unidad la unidad secundaria. A diferencia de la Conmutación por falla activa/espera, esta designación no indica qué unidad llega a ser activa cuando ambas unidades comienzan simultáneamente. En lugar, la designación primaria/secundaria hace dos cosas:

- Determina qué unidad proporciona la configuración corriente a los pares cuando inician simultáneamente.
- Determina en qué unidad aparece cada grupo de la Conmutación por falla en el estado activo cuando las unidades inician simultáneamente. Configuran a cada grupo de la Conmutación por falla en la configuración con una preferencia primaria o de la unidad secundaria. Usted puede configurar a ambos grupos de la Conmutación por falla esté en el estado activo en una sola unidad en los pares, con la otra unidad conteniendo a los grupos de la Conmutación por falla en el estado espera. Sin embargo, una más configuración típica es asignar a cada grupo de la Conmutación por falla una diversa preferencia del papel para hacer cada uno activo en una diversa unidad, distribuyendo el tráfico a través de los dispositivos. **Nota:** El dispositivo de seguridad no proporciona los servicios del Equilibrio de carga. El Equilibrio de carga se debe manejar por un router que pasa el tráfico al dispositivo de seguridad.

Qué unidad cada grupo de la Conmutación por falla hace activo encendido se determina como se muestra

- Cuando una unidad inicia mientras que la unidad del par no está disponible, ambos grupos de la Conmutación por falla hacen activos en la unidad.
- Cuando una unidad inicia mientras que la unidad del par es activa (con ambos grupos de la Conmutación por falla en el estado activo), sigue habiendo los grupos de la Conmutación por falla en el estado activo en la unidad activa sin importar la preferencia primaria o secundaria del grupo de la Conmutación por falla hasta uno del siguiente: Una Conmutación por falla ocurre. Usted fuerza manualmente al grupo de la Conmutación por falla a la otra unidad con el **comando no failover active** Usted configuró al grupo de la Conmutación por falla con el comando de la **apropiación**, que hace al grupo de la Conmutación por falla hacer automáticamente activo en la unidad preferida cuando la unidad está disponible.
- Cuando ambas unidades inician al mismo tiempo, cada grupo de la Conmutación por falla hace activo en su unidad preferida después de que se hayan sincronizado las configuraciones.

Sincronización de la Configuración e Inicialización del dispositivo

La sincronización de la configuración ocurre cuando una o ambas unidades en un par de fallas inician. Las configuraciones se sincronizan como se muestra:

- Cuando una unidad inicia mientras que la unidad del par es activa (con ambos grupos de la Conmutación por falla activos en ella), la unidad del arranque entra en contacto la unidad activa para obtener la configuración corriente sin importar la designación primaria o secundaria de la unidad del arranque.
- Cuando ambas unidades inician simultáneamente, la unidad secundaria obtiene la configuración corriente de la unidad primaria.

Cuando la replicación comienza, la consola del dispositivo de seguridad en la unidad que envía la configuración visualiza **réplica de la configuración del principio del mensaje** “: **Enviando para acoplarse,**” y cuando es completo, el dispositivo de seguridad visualiza el mensaje **“replicación del fin de configuración para acoplarse.”** Durante la replicación, los comandos entered en la unidad que envía la configuración pueden no replegar correctamente a la unidad del par, y los comandos entered en la unidad que recibe la configuración pueden ser sobregabados por la configuración que es recibida. Evite ingresar los comandos en cualquier unidad en el par de fallas durante el proceso de la réplica de la configuración. Dependiendo del tamaño de la configuración, la replicación puede llevar a partir de algunos segundos varios minutos.

En la unidad que recibe la configuración, la configuración existe solamente en la memoria corriente. Para salvar la configuración a memoria flash después de que la sincronización ingrese el **comando all de la memoria de la escritura** en el espacio de la ejecución del sistema en la unidad que tiene group1 de la Conmutación por falla en el estado activo. El comando se replica a la unidad del par, que procede a escribir su configuración a memoria flash. Usando **toda la** palabra clave con este comando causa el sistema y todas las configuraciones del contexto que se guardarán.

Nota: Las configuraciones de inicio guardadas en los servidores externos son accesibles de cualquier unidad sobre la red y no necesitan ser guardadas por separado para cada unidad. Alternativamente, usted puede copiar los archivos de configuración de los contextos del disco en la unidad primaria a un servidor externo, y después los copia al disco en la unidad secundaria, donde están disponibles cuando las recargas de la unidad.

[Réplica de Comandos](#)

Después de que ambas unidades se estén ejecutando, los comandos se replican a partir de una unidad a la otra como se muestra:

- Repliegan a los comandos entered dentro de los contextos de seguridad de la unidad en la cual los contextos de seguridad aparecen en el estado activo a la unidad del par. **Nota:** el contexto se considera en el estado activo en una unidad si el grupo de la Conmutación por falla al cual pertenece está en el estado activo en esa unidad.
- Repliegan a los comandos entered en el espacio de la ejecución del sistema de la unidad en la cual el group1 de la Conmutación por falla está en el estado activo a la unidad en la cual el group1 de la Conmutación por falla está en el estado espera.
- Repliegan a los comandos entered en el contexto admin de la unidad en la cual el group1 de la Conmutación por falla está en el estado activo a la unidad en la cual el group1 de la Conmutación por falla está en el estado espera.

Replican toda la configuración y comandos file (la **copia, retitula, borra, mkdir, rmdir**, y así sucesivamente), con las excepciones siguientes. **La demostración, el debug, el modo, el Firewall, y los comandos de la unidad lan de la Conmutación por falla** no se replican.

El incidente de ingresar los comandos en la unidad apropiada para que la replicación del comando ocurra hace las configuraciones estar fuera de sincronización. Esos cambios pueden ser perdidos la próxima vez que ocurre la sincronización de la configuración inicial.

Usted puede utilizar el **comando write standby** de resincronizar las configuraciones fuera de las cuales se han convertido sincronizan. Para la Conmutación por falla activa/activa, el **comando write standby** se comporta como se muestra:

- Si usted ingresa el **comando write standby** en el espacio de la ejecución del sistema, la configuración del sistema y las configuraciones para todos los contextos de seguridad en el dispositivo de seguridad se escribe a la unidad del par. Esto incluye la información de la configuración para los contextos de seguridad que están en el estado espera. Usted debe ingresar el comando en el espacio de la ejecución del sistema en la unidad que tiene group1 de la Conmutación por falla en el estado activo. **Nota:** Si hay contextos de seguridad en el estado activo en la unidad del par, el **comando write standby** hace las conexiones activas con esos contextos ser terminado. Utilice el **comando failover active** en la unidad que proporciona a la configuración para asegurarse todos los contextos son activo en esa unidad antes de ingresar el **comando write standby**.
- Si usted ingresa el **comando write standby** en los contextos de seguridad, sólo la configuración para los contextos de seguridad se escribe a la unidad del par. Usted debe ingresar el comando en los contextos de seguridad en la unidad en donde los contextos de seguridad aparecen en el estado activo.

No guardan los comandos replicados a memoria flash cuando están replicados a la unidad del par. Los agregan a la configuración corriente. Para salvar los comandos replicados a memoria flash en ambas unidades, utilice el **comando write memory o copy running-config startup-config** en la unidad que usted realizó los cambios encendido. El comando se replica a la unidad del par y hace la configuración ser guardado a memoria flash en la unidad del par.

Disparadores del Failover

En la Conmutación por falla activa/activa, la Conmutación por falla se puede accionar en el nivel de la unidad si ocurre uno de los eventos siguientes:

- La unidad tiene una falla de hardware.
- La unidad tiene un corte del suministro de electricidad.
- La unidad tiene una falla de software.
- No se ingresa la **ninguna Conmutación por falla activa** o al **comando failover active** en el espacio de la ejecución del sistema.

La Conmutación por falla se acciona en el nivel de grupo de la Conmutación por falla cuando ocurre uno de estos eventos:

- Demasiadas interfaces monitoreadas en el fall del grupo.
- No se ingresa el **ningún group_id activo del grupo de la Conmutación por falla** o comando **activo del group_id del grupo de la Conmutación por falla**.

Acciones de Failover

En una configuración de failover activa/activa, la Conmutación por falla ocurre sobre una base del grupo de la Conmutación por falla, no una base del sistema. Por ejemplo, si usted señala a ambos grupos de la Conmutación por falla como active en la unidad primaria, y group1 de la Conmutación por falla falla, después el group2 de la Conmutación por falla sigue siendo activo en la unidad primaria mientras que el group1 de la Conmutación por falla llega a ser activo en la unidad secundaria.

Nota: Cuando la Conmutación por falla activa/activa el configurar, se asegura que el tráfico combinado para ambas unidades está dentro de la capacidad de cada unidad.

Esta tabla muestra la acción de failover para cada evento de failover. Para cada evento de falla, se dan la directiva (independientemente de si ocurre la Conmutación por falla), las acciones para el grupo activo de la Conmutación por falla, y las acciones para el grupo espera de la Conmutación por falla.

Evento de Falla	Política	Acción de grupo activa	Acción de grupo en espera	Notas
Una unidad experimenta un poder o una falla de software	Failover	Se convierte la marca espera según lo fallado	Haga espera. Marcar activo como fallado	Cuando una unidad en un par de fallas falla, marcan como fallado y llega a ser activo a cualquier grupo de la Conmutación por falla del active en esa unidad en la unidad del par.
Interconecte el error en el grupo activo de la Conmutación por falla sobre el umbral	Failover	Marque al grupo activo según lo fallado	Pasar a activo	Ninguno
Interconecte el error en el grupo espera de la Conmutación por falla sobre el umbral	Ningún failover	Ninguna acción	Marque al grupo en espera según lo fallado	Cuando marcan al grupo espera de la Conmutación por falla como fallado, el grupo activo de la Conmutación por falla no intenta fallar encima, incluso si se supera el umbral del error de la interfaz.
El grupo activo de la Conmutación por falla se recupera	Ningún failover	Ninguna acción	Ninguna acción	A menos que estén configurados con el comando de la apropiación , los grupos de la Conmutación por falla sigan siendo activos en su unidad actual.

antes				
Link de failover fallado en el inicio	Ningún failover	Pasa a activo	Pasar a activo	Si el link de fallas está abajo en el lanzamiento, ambos grupos de la Conmutación por falla en ambas unidades hacen activos.
Link de stateful failover fallado	Ningún failover	Ninguna acción	Ninguna acción	La información de estado llega a estar desactualizada, y se terminan las sesiones si ocurre un failover.
Link de fallas fallado durante la operación	Ningún failover	n/a	n/a	Cada unidad marca la interfaz de la Conmutación por falla según lo fallado. Usted debe restablecer el link de fallas cuanto antes porque la unidad no puede fallar encima a la unidad en espera mientras que el link de fallas está abajo.

[Regular y Stateful Failover](#)

El dispositivo de seguridad soporta dos tipos de failover, regular y stateful. Esta sección incluye estos temas:

- [Regular Failover](#)
- [Stateful Failover](#)

[Regular Failover](#)

Cuando ocurre un failover, se interrumpen todas las conexiones activas. Los clientes necesitan restablecer las conexiones cuando la nueva unidad activa asume el control.

[Stateful Failover](#)

Cuando el stateful failover está habilitado, la unidad activa pasa continuamente la información de estado por conexión a la unidad standby. Después de que ocurre un failover, la misma información de conexión está disponible en la nueva unidad activa. Las aplicaciones del usuario final soportadas no se requieren para volver a conectarse a fin de conservar la misma sesión de comunicación.

La información de estado que se pasa a la unidad standby incluye lo siguiente:

- La tabla de traducción NAT
- Los estados de la conexión TCP
- Los estados de la conexión UDP

- La tabla ARP
- El tabla de bridge de Capa 2 (cuando se ejecuta en el modo transparent firewall)
- Los estados de la conexión HTTP (si se habilita la réplica HTTP)
- La tabla de SA ISAKMP e IPsec
- Las bases de datos de conexiones GTP PDP

La información que no se pasa a la unidad standby cuando stateful failover está habilitado incluye lo siguiente:

- La tabla de la conexión HTTP (a menos que se habilite la réplica HTTP)
- La tabla de la autenticación de usuario (uauth)
- Las tablas de ruteo
- Información del estado para los módulos del servicio de seguridad

Nota: Si el failover ocurre dentro de una sesión activa del Cisco IP SoftPhone, la llamada sigue siendo activa porque la información de estado de la sesión de llamada se replica en la unidad standby. Cuando se termina la llamada, el cliente del IP SoftPhone pierde la conexión con el Administrador de Llamadas. Esto ocurre porque no hay información de la sesión para el mensaje para colgar CTIQBE en la unidad standby. Cuando el cliente del IP SoftPhone no recibe una respuesta del Administrador de Llamadas dentro de cierto período, considera al Administrador de Llamadas inalcanzable y cancela su registro.

Limitaciones de la configuración de failover

Usted no puede configurar la Conmutación por falla con estos tipos de IP Addresses:

- IP Addresses obtenidos con el DHCP
- IP Addresses obtenidos con el PPPoE
- Direccionamientos del IPv6

Además, estas restricciones se aplican:

- No soportan a la falla de estado en el dispositivo de seguridad adaptante ASA 5505.
- La Conmutación por falla activa/activa no se soporta en el dispositivo de seguridad adaptante ASA 5505.
- Usted no puede configurar la Conmutación por falla cuando el Easy VPN Remote se habilita en el dispositivo de seguridad adaptante ASA 5505.
- La Conmutación por falla VPN no se soporta en el modo de contexto múltiple.

Características no admitidas

El modo de contexto múltiple no soporta estas características:

- Dynamic Routing Protocol Los contextos de seguridad soportan solamente las Static rutas. Usted no puede habilitar el OSPF o el RIP en el modo de contexto múltiple.
- VPN
- Multicast (multidifusión)

Configuración de failover activa/activa Cable-basada

prerrequisitos

Antes de que usted comience, verifique el siguiente:

- Ambas unidades tienen el mismo hardware, configuración del software, y licencia apropiada.
- Ambas unidades están en el mismo modo (solo o múltiple, transparente o ruteado).

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Siga los siguientes pasos para configurar la Conmutación por falla activa/activa usando un cable serial como el link de fallas. Los comandos en esta tarea se ingresan en la unidad primaria en el par de failover. La unidad primaria es la unidad que tiene el extremo del cable etiquetado "Primary" conectado en ella. Para los dispositivos en el modo multiple context, los comandos se ingresan en el espacio de la ejecución del sistema a menos que se indique lo contrario.

Usted no necesita ejecutar el proceso de arranque de la unidad secundaria en el par de failover cuando utiliza el failover basado en cable. Deje la unidad secundaria apagada hasta que se le indique que debe encenderla.

Nota: la Conmutación por falla Cable-basada está solamente disponible en el dispositivo de seguridad de la serie PIX 500.

Complete estos pasos para configurar Conmutación por falla cable-basada, activa/activa:

1. Conecte el cable con fallas con los dispositivos de seguridad de la serie PIX 500.
Asegurese que usted asocia el final del "primario marcada cable" a la unidad que usted utiliza como la unidad primaria, y que usted asocia el final del "secundario marcada cable" a la unidad usted utiliza como la unidad secundaria.
2. Encienda la unidad primaria.
3. Si usted no ha hecho tan ya, configure el active y los IP Address en Standby para cada Interfaz de datos (modo ruteado), para el IP Address de administración (modo transparente), o para la interfaz de la Administración-solamente. La dirección IP standby se utiliza en el dispositivo de seguridad que es actualmente la unidad standby. Debe estar en la misma subred que la dirección IP activa. Usted debe configurar los direccionamientos de la interfaz dentro de cada contexto. Utilice el **comando changeto context** para conmutar entre los contextos. El comando indica cambios en `hostname/context(config-if)#`, donde context es el nombre del contexto actual. Usted debe ingresar un IP Address de administración para cada contexto en el modo de contexto múltiple transparente del Firewall. **Nota:** No configure una dirección IP para el link de la falla de estado si usted va a utilizar una interfaz dedicada de la falla de estado. Usted utiliza el **comando failover interface ip** para configurar una interfaz dedicada de stateful failover en un paso posterior.
`hostname/context(config-if)#ip address active_addr netmask standby standby_addr`
En el ejemplo, la interfaz exterior para context1 del PIX principal se configura esta manera:
`PIX1/context1(config)#ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2`
Para Context2:
`PIX1/context2(config)#ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2`
En el modo firewall ruteado y para la interfaz de la Administración-solamente, este comando se ingresa en el modo de configuración de la interfaz para cada interfaz. En el modo firewall transparente, el comando se ingresa en el

modo de configuración global.

4. Para habilitar el stateful failover, configure el link de stateful failover. Especifique la interfaz que se utilizará como link de la falla de estado:

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

En este ejemplo, la interfaz Ethernet2 se utiliza para intercambiar la información del estado del link de la falla de estado.

```
failover link stateful Ethernet2
```

El argumento *if_name* asigna un nombre lógico a la interfaz especificada por el argumento *phy_if*. El argumento *phy_if* puede ser el nombre del puerto físico, como Ethernet1, o una subinterfaz previamente creada, como Ethernet0/2.3. Esta interfaz no se debe utilizar para ningún otro propósito (excepto, opcionalmente, el link de fallas). Asigne una dirección IP activa y standby al link de stateful failover:

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

En este ejemplo, 10.0.0.1 se utiliza como activa, y 10.0.0.2 se utiliza como dirección IP standby para el link de stateful failover.

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

La dirección IP standby debe estar en la misma subred que la dirección IP activa. Usted no necesita identificar la máscara de subred de la dirección IP standby. La dirección IP y la dirección MAC del link de la falla de estado no cambian en la Conmutación por falla a excepción de cuando la falla de estado utiliza una interfaz de los datos comunes. La dirección IP activa permanece siempre con la unidad primaria, mientras que la dirección IP standby permanece con la unidad secundaria. Habilite la interfaz:

```
hostname(config)#interface phy_if hostname(config-if)#no shutdown
```
5. Configure a los grupos de la Conmutación por falla. Usted puede tener a lo más dos grupos de la Conmutación por falla. **El comando group de la Conmutación por falla** crea al grupo especificado de la Conmutación por falla si no existe y ingresa el modo de la configuración de grupo de la Conmutación por falla. Para cada grupo de la Conmutación por falla, usted necesita especificar si el grupo de la Conmutación por falla tenga preferencia primaria o secundaria usando el **primario** o el **comando secondary**. Usted puede asignar la misma preferencia a ambos grupos de la Conmutación por falla. Para las configuraciones del Equilibrio de carga, usted debe asignar a cada grupo de la Conmutación por falla una diversa preferencia de la unidad. El siguiente ejemplo asigna a group1 de la Conmutación por falla una preferencia primaria y el group2 de la Conmutación por falla una preferencia secundaria:

```
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. Asigne cada contexto del usuario a un grupo de la Conmutación por falla usando el comando del unir a-Conmutación por falla-grupo en el modo de configuración del contexto. Cualquier contexto no asignado se asigna automáticamente al group1 de la Conmutación por falla. El contexto admin es siempre un miembro del group1 de la Conmutación por falla. Ingrese estos comandos de asignar cada contexto a un grupo de la Conmutación por falla:

```
hostname(config)#context context_name hostname(config-context)#join-failover-group {1 | 2} hostname(config-context)#exit
```
7. Habilite el failover:

```
hostname(config)#failover
```
8. Encienda la unidad secundaria y habilite el failover en la unidad si aún no está habilitado:

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

La unidad activa envía la configuración en la memoria en ejecución a la unidad standby. A medida que la configuración se sincroniza, aparecen los mensajes "Beginning configuration replication: sending to mate" y "End Configuration Replication to mate" en la consola primaria. **Nota:** Ejecute el **comando failover** en el dispositivo primario primero, y en seguida ejecútelo en el dispositivo secundario. Después de que usted ejecute el **comando failover** en el dispositivo secundario, el dispositivo secundario toma inmediatamente la configuración del dispositivo primario y se establece como *standby*.

El ASA primario permanece activo, y pasa el tráfico normalmente y se marca como el *dispositivo activo*. A partir de ese momento, siempre que una falla ocurra en el dispositivo activo, el dispositivo standby emerge como el activo.

9. Guarde la configuración en la memoria Flash en la unidad primaria. Dado que los comandos ingresados en la unidad primaria se replican en la unidad secundaria, la unidad secundaria también guarda su configuración en la memoria Flash.
`hostname(config)#copy running-config startup-config`
10. En caso necesario, fuerce a cualquier grupo de la Conmutación por falla que sea activo en el primario al estado activo en el secundario. Para forzar a un grupo de la Conmutación por falla a llegar a ser activo en la unidad secundaria, publique este comando en el espacio de la ejecución del sistema en la unidad primaria:
`hostname#no failover active group group_id`
El argumento del `group_id` especifica al grupo que usted quiere hacer activo en la unidad secundaria.

Configuraciones

En este documento, se utilizan estas configuraciones:

- [PIX1 - Configuración del sistema](#)
- [PIX1 - Configuración Context1](#)
- [PIX1 - Configuración Context2](#)

PIX1 - Configuración del sistema

```
PIX1#show running-config : Saved PIX Version 7.2(2)
<system> ! 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 - Configuración Context1

```
PIX1/context1(config)#show running-config : Saved : PIX
Version 7.2(2) <context> ! 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 - Configuración Context2

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

[Configuración de failover activa/activa basada en LAN](#)

[Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:

Esta sección describe cómo configurar la Conmutación por falla activa/activa usando un link de fallas de los Ethernetes. Al configurar la Conmutación por falla basada en LAN, usted debe atar el dispositivo secundario con correa para reconocer el link de fallas antes de que el dispositivo secundario pueda obtener la configuración corriente del Dispositivo principal.

Nota: En vez de utilizar un cable Ethernet crossover para conectar directamente las unidades, Cisco le recomienda que utilice un switch dedicado entre las unidades primarias y secundarias.

Esta sección incluye los temas como se muestra:

- [Configuración de la Unidad Primaria](#)
- [Configuración de la Unidad Secundaria](#)

[Configuración de la Unidad Primaria](#)

Complete estos pasos para configurar la unidad primaria en una configuración de failover activa/activa:

1. Si usted no ha hecho tan ya, configure el active y los IP Address en Standby para cada Interfaz de datos (modo ruteado), para el IP Address de administración (modo transparente), o para la interfaz de la Administración-solamente. La dirección IP standby se utiliza en el dispositivo de seguridad que es actualmente la unidad standby. Debe estar en la misma subred que la dirección IP activa. Usted debe configurar los direccionamientos de la interfaz dentro de cada contexto. Utilice el **comando `changeto context`** para conmutar entre los contextos. El comando indica cambios en `hostname/context(config-if)#`, donde context es el nombre del contexto actual. En el modo firewall transparente, usted debe ingresar un IP Address de administración para cada contexto. **Nota:** No configure una dirección IP para el link de la falla de estado si usted va a utilizar una interfaz dedicada de la falla de estado.

Usted utiliza el comando **failover interface ip** para configurar una interfaz dedicada de stateful failover en un paso posterior.`hostname/context(config-if)#ip address active_addr netmask standby standby_addr` En el ejemplo, la interfaz exterior para context1 del PIX principal se configura esta manera:`PIX1/context1(config)#ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2` Para Context2:`PIX1/context2(config)#ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2` En el modo firewall ruteado y para la interfaz de la Administración-solamente, este comando se ingresa en el modo de configuración de la interfaz para cada interfaz. En el modo firewall transparente, el comando se ingresa en el modo de configuración global.

- Configure los parámetros básicos de la Conmutación por falla en el espacio de la ejecución del sistema.(Dispositivo de seguridad PIX solamente) habilite la Conmutación por falla basada en LAN:`hostname(config)#failover lan enable` Señale la unidad como la unidad primaria:`hostname(config)#failover lan unit primary` Especifique el link de fallas:`hostname(config)#failover lan interface if_name phy_if` En este ejemplo, utilizamos las interfaces Ethernet 3 como el LAN basó la interfaz de la Conmutación por falla.`PIX1(config)#failover lan interface LANFailover ethernet3` El argumento **if_name** asigna un nombre lógico a la interfaz especificada por el argumento **phy_if**. El argumento **phy_if** puede ser el nombre del puerto físico, como Ethernet1, o una subinterfaz previamente creada, como Ethernet0/2.3. En el dispositivo de seguridad adaptante ASA 5505, el phy_if especifica un VLA N. Esta interfaz no se debe utilizar para ningún otro propósito (excepto, opcionalmente, el link de la falla de estado).Especifique el active y los IP Address en Standby del link de fallas:`hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr` Por este ejemplo, utilizamos 10.1.0.1 como el active y 10.1.0.2 mientras que los IP Address en Standby para la Conmutación por falla interconectan.`PIX1(config)#failover interface ip LANFailover 10.1.0.1 255.255.255.0 standby 10.1.0.2` La dirección IP standby debe estar en la misma subred que la dirección IP activa. Usted no necesita identificar la máscara de subred de la dirección IP standby. La dirección IP y la dirección MAC del link de failover no cambian en el failover. La dirección IP activa permanece siempre con la unidad primaria, mientras que la dirección IP standby permanece con la unidad secundaria.
- Para habilitar a la falla de estado, configure el link de la falla de estado:Especifique la interfaz que se utilizará como link de la falla de estado:`hostname(config)#failover link if_name phy_if` `PIX1(config)#failover link stateful ethernet2` El argumento **if_name** asigna un nombre lógico a la interfaz especificada por el argumento **phy_if**. El argumento **phy_if** puede ser el nombre del puerto físico, como Ethernet1, o una subinterfaz previamente creada, como Ethernet0/2.3. Esta interfaz no se debe utilizar para ningún otro propósito (excepto, opcionalmente, el link de fallas).**Nota:** Si el link de la falla de estado utiliza el link de fallas o los datos comunes interconectan, después usted necesita solamente suministrar el argumento del if_name.Asigne una dirección IP activa y standby al link de stateful failover.**Nota:** Si el link de la falla de estado utiliza el link de fallas o los datos comunes interconectan, salte este paso. Usted ha definido ya las direcciones IP activas y standby para la interfaz.`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` La dirección IP standby debe estar en la misma subred que la dirección IP activa. Usted no necesita identificar la máscara de subred de la dirección standby. La dirección IP y la dirección MAC del link del estado no cambian en la Conmutación por falla. La dirección IP activa permanece siempre con la unidad primaria, mientras que la dirección IP standby permanece con la unidad secundaria.Habilite la interfaz.**Nota:** Si el link de la falla de estado utiliza el link de fallas o los datos comunes interconectan, salte este paso. Usted ha

habilitado ya la interfaz.`hostname(config)#interface phy_if hostname(config-if)#no shutdown`

- Configure a los grupos de la Conmutación por falla. Usted puede tener a lo más dos grupos de la Conmutación por falla. **El comando group de la Conmutación por falla** crea al grupo especificado de la Conmutación por falla si no existe y ingresa el modo de la configuración de grupo de la Conmutación por falla. Para cada grupo de la Conmutación por falla, especifique si el grupo de la Conmutación por falla tiene preferencia **primaria** o **secundaria** usando el comando `primary` o el comando `secondary`. Usted puede asignar la misma preferencia a ambos grupos de la Conmutación por falla. Para las configuraciones del Equilibrio de carga, usted debe asignar a cada grupo de la Conmutación por falla una diversa preferencia de la unidad. El siguiente ejemplo asigna a `group1` de la Conmutación por falla una preferencia primaria y el `group2` de la Conmutación por falla una preferencia

```
secundaria: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
```

- Asigne cada contexto del usuario a un grupo de la Conmutación por falla usando el comando del unir a-Conmutación por falla-**grupo** en el modo de configuración del contexto. Cualquier contexto no asignado se asigna automáticamente al `group1` de la Conmutación por falla. El contexto `admin` es siempre un miembro del `group1` de la Conmutación por falla. Ingrese estos comandos de asignar cada contexto a un grupo de la Conmutación por falla:`hostname(config)#context context_name hostname(config-context)#join-
failover-group {1 | 2} hostname(config-context)#exit`

- Habilite el failover.`hostname(config)#failover`

Configuración de la Unidad Secundaria

Al configurar la Conmutación por falla activa/activa basada en LAN, usted necesita atar la unidad secundaria con correa para reconocer el link de fallas. Esto permite que la unidad secundaria comunique con y reciba la configuración corriente de la unidad primaria.

Complete estos pasos para atar la unidad secundaria con correa en una configuración de failover activa/activa:

- (Dispositivo de seguridad PIX solamente) habilite la Conmutación por falla basada en LAN.`hostname(config)#failover lan enable`
- Defina la interfaz de failover. Utilice las mismas configuraciones que usted utilizó para la unidad primaria: Especifique la interfaz que se utilizará como la interfaz de failover.`hostname(config)#failover lan interface if_name phy_if PIX1(config)#failover lan interface LANFailover ethernet3` El argumento **if_name** asigna un nombre lógico a la interfaz especificada por el argumento **phy_if**. El argumento **phy_if** puede ser el nombre del puerto físico, como `Ethernet1`, o una subinterfaz previamente creada, como `Ethernet0/2.3`. En el dispositivo de seguridad adaptante ASA 5505, el **phy_if** especifica un VLA N. Asigne el active y el IP Address en Standby al link de fallas:`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:** Ingrese este comando exactamente como usted lo ingresó en la unidad primaria cuando usted configuró la interfaz de la Conmutación por falla. La dirección IP standby debe estar en la misma subred que la dirección IP activa. Usted no necesita identificar la máscara de subred de la dirección standby. Habilite la interfaz.`hostname(config)#interface phy_if hostname(config-if)#no shutdown`
- Señale esta unidad como la unidad secundaria:`hostname(config)#failover lan unit secondary`

Nota: Este paso es opcional porque por abandono las unidades se señalan como secundario a menos que estén configuradas previamente de otra manera.

4. Habilite el failover.`hostname(config)#failover` Después de que usted habilita el failover, la unidad activa envía la configuración en la memoria en ejecución a la unidad standby. A medida que la configuración se sincroniza, aparecen los mensajes *Beginning configuration replication: Sending to mate* y *End Configuration Replication to mate* en la consola de la unidad activa.**Nota:** Ejecute el **comando failover** en el dispositivo primario primero, y en seguida ejecútelo en el dispositivo secundario. Después de que usted ejecute el **comando failover** en el dispositivo secundario, el dispositivo secundario toma inmediatamente la configuración del dispositivo primario y se establece como *standby*. El ASA primario permanece activo, y pasa el tráfico normalmente y se marca como el *dispositivo activo*. A partir de ese momento, siempre que una falla ocurra en el dispositivo activo, el dispositivo standby emerge como el activo.
5. Después de que la configuración corriente haya completado la replicación, ingrese este comando de salvar la configuración a memoria flash:`hostname(config)#copy running-config startup-config`
6. En caso necesario, fuerce a cualquier grupo de la Conmutación por falla que sea activo en el primario al estado activo en la unidad secundaria. Para forzar a un grupo de la Conmutación por falla a llegar a ser activo en la unidad secundaria, ingrese este comando en el espacio de la ejecución del sistema en la unidad primaria:`hostname#no failover active group group_id` El argumento del `group_id` especifica al grupo que usted quiere hacer activo en la unidad secundaria.

Configuraciones

En este documento, se utilizan estas configuraciones:

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: Refiera la sección de configuración de failover basada cable, [PIX1 - la configuración Context1](#) y [PIX1 - la configuración Context2](#) para la configuración del contexto en el escenario de falla basado LAN.

PIX Secundario

```
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
```

Verificación

[Uso del Comando show failover](#)

Esta sección describe el resultado del **comando show failover**. En cada unidad, usted puede verificar el estado de failover con el **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 Secundario

```
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
```

Utilice el comando **show failover state** para verificar el estado.

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
```

Unidad secundaria

```
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
```

Para verificar las direcciones IP de la unidad de failover, utilice **show failover interfacecommand**.

Unidad primaria

```
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
```

Unidad secundaria

```
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
```

Vista de las Interfaces Monitoreadas

Para ver el estado de las interfaces monitoreadas: En el modo single context, ingrese el comando [show monitor-interface](#) en el modo global configuration. En el modo multiple context, ingrese **show monitor-interface** dentro de un contexto.

Nota: Para habilitar el control de estado en una interfaz específica, utilice el comando [monitor-interface](#) en el modo global configuration:

```
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 Secundario

```
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: Si usted no ingresa un IP Address de la Conmutación por falla, el comando **show failover** visualiza 0.0.0.0 para el IP Address, y sigue habiendo la supervisión de las interfaces en un

estado “en espera”. Usted debe fijar una dirección IP de la Conmutación por falla para que la Conmutación por falla trabaje. Para más información sobre diversos estados para la Conmutación por falla, refiera a la [Conmutación por falla de la demostración](#).

De forma predeterminada, se habilita el monitoreo de las interfaces físicas y se inhabilita el monitoreo de las subinterfaces.

[Visualización de los Comandos de Failover en la Configuración en Ejecución](#)

Para ver los comandos de failover en la configuración en ejecución, ingrese este comando:

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

Se visualizan todos los comandos de failover. En las unidades que se ejecutan en el modo multiple context, ingrese el **comando show running-config failover** en el espacio de la ejecución del sistema. Ingrese los ejecutar-config de la demostración todo el comando failover de visualizar los comandos failover en la configuración corriente y los comandos include para quienes usted no ha cambiado el valor predeterminado.

[Pruebas de Funcionalidad de Failover](#)

Para probar la funcionalidad de failover, realice estos pasos:

1. Pruebe que su grupo de failover o unidad activa pase el tráfico como se espera con FTP (por ejemplo) para enviar un archivo entre hosts en diversas interfaces.
2. Fuerce un failover a la unidad standby con este comando:Para la Conmutación por falla activa/activa, ingrese el siguiente comando en la unidad donde está activo el grupo de la Conmutación por falla que contiene la interfaz que conecta sus host:hostname(config)#no failover active group group_id
3. Utilice FTP para enviar otro archivo entre los dos mismos hosts.
4. Si la prueba no fue satisfactoria, ingrese el **comando show failover** de verificar el estado de failover.
5. Cuando finalice, puede restaurar el grupo de failover o la unidad al estado activo con este comando:Para la Conmutación por falla activa/activa, ingrese el siguiente comando en la unidad donde está activo el grupo de la Conmutación por falla que contiene la interfaz que conecta sus host:hostname(config)#failover active group group_id

[Failover Forzado](#)

Para forzar la unidad standby para pasar a ser activa, ingrese uno de estos comandos:

Ingrese este comando en el espacio de la ejecución del sistema de la unidad donde está el grupo de la Conmutación por falla en el estado espera:

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

O, ingrese este comando en el espacio de la ejecución del sistema de la unidad donde está el grupo de la Conmutación por falla en el estado activo:

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

Ingresar este comando en el espacio de la ejecución del sistema hace a todos los grupos de la Conmutación por falla hacer activos:

```
hostname#failover active
```

[Failover Inhabilitado](#)

Para inhabilitar el failover, ingrese este comando:

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

Si usted inhabilita el failover en un par Active/Standby, hace que el estado activo y standby de cada unidad se mantenga hasta que usted reinicie. Por ejemplo, la unidad standby permanece en el modo standby de modo que ambas unidades no comiencen a pasar el tráfico. Para hacer el active de la unidad en espera (incluso con la Conmutación por falla inhabilitada), vea la sección [forzada de la Conmutación por falla](#).

Si usted inhabilita el failover en un par Activo/Activo, hace que los grupos de failover permanezcan en el estado activo en cualquier unidad en la que actualmente están activos, independientemente de la unidad de preferencia configurada. El comando **no failover** puede ser ingresado en el espacio de la ejecución del sistema.

[Restauración de una Unidad Defectuosa](#)

Para restablecer a un grupo activo/activo fallado de la Conmutación por falla a un estado unfailed, ingrese este comando:

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

Si usted restaura una unidad defectuosa a un estado no defectuosa, no cambia automáticamente a activa; las unidades o los grupos restaurados permanecen en el estado standby hasta que pasan a activos mediante el failover (forzado o natural). Una excepción es un grupo de failover configurado con el comando preempt. Si un grupo de failover estaba previamente activo, un grupo de failover cambia a activo si lo configuran con el comando preempt y si la unidad en la que falló es su unidad preferida.

[Reemplazar la Unidad Defectuosa por una Nueva Unidad](#)

Complete estos pasos para reemplazar una unidad defectuosa por una nueva unidad:

1. Ejecute el **comando no failover** en la unidad primaria.El estado de la unidad secundaria muestra **standby unit as not detected**.
2. Desconecte la unidad primaria, y conecte la unidad primaria de reemplazo.
3. Verifique que las unidades de reemplazo funcionen con la misma versión de software y de ASDM que la unidad secundaria.

4. Ejecute estos comandos en las unidades de reemplazo:

```
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. Conecte la unidad primaria de reemplazo a la red, y ejecute este comando:ASA(config)#failover

[Troubleshooting](#)

Cuando ocurre un failover, ambos dispositivos de seguridad envían mensajes del sistema. Esta sección incluye estos temas:

1. [Mensajes del sistema de fallas](#)
2. [Mensajes del debug](#)
3. [SNMP](#)

[Mensajes del sistema de fallas](#)

El dispositivo de seguridad ejecuta varios mensajes del sistema relacionados con el failover en el nivel de prioridad 2, que indica una Condición crítica. Para ver estos mensajes, consulte la [configuración de registro y a los mensajes del registro del sistema de Dispositivos de Seguridad de Cisco](#) para habilitar el registro y para ver las descripciones de los mensajes del sistema.

Nota: Dentro del intercambio, el failover apaga y después trae lógicamente para arriba las interfaces, que genera los mensajes syslog **411001** y **411002**. Esta es actividad normal.

[Comunicaciones de fallas perdidas primarias con el compañero en el interface_name de la interfaz](#)

Se visualiza este mensaje de falla si una unidad del par de fallas puede comunicar no más con la otra unidad de los pares. Primario puede también ser enumerado como secundario para la unidad secundaria.

((Primario) perdió las comunicaciones de failover con el compañero en la interfaz interface_name

Verificar que esté funcionando la red que está conectada con la interfaz especificada correctamente.

[Mensajes del debug](#)

Para ver los mensajes del debug, ingrese el comando del **fover del debug**. Consulte [Referencia de Comandos de Dispositivos de Seguridad de Cisco, versión 7.2](#) para obtener más información.

Nota: Porque asignan la salida de debbuging prioritario en proceso de la CPU, puede afectar drástico al rendimiento del sistema. Por esta razón, utilice los comandos del **fover del debug** de resolver problemas solamente los problemas específicos o dentro de las sesiones de Troubleshooting con el equipo de Soporte Técnico de Cisco.

[SNMP](#)

Para recibir las trampas de Syslog SNMP para el failover, configurar al agente SNMP para enviar el SNMP traps a las estaciones de la administración de SNMP, definir un syslog host, y compilar Cisco syslog MIB en su estación de la administración de SNMP. Refiera al SNMP-**servidor** y a los **comandos logging** en la [referencia de comandos del dispositivo del Cisco Security, versión 7.2](#) para más información.

[Tiempo de sondeo de fallas](#)

Para especificar la encuesta y los tiempos en espera de la unidad de transmisión por falla, publique el comando del **tiempo de sondeo de fallas** en el modo de configuración global.

El [time] milisegundo de la unidad del tiempo de sondeo de fallas representa el intervalo de

tiempo para marcar la existencia de la unidad en espera sondeando los mensajes Hello Messages.

Semejantemente, el [time] milisegundo de la unidad del holdtime de la Conmutación por falla representa el período de tiempo durante el cual una unidad debe recibir un mensaje Hello Messages en el link de fallas, después de lo cual la unidad del par se declara para haber fallado.

Refiera al [tiempo de sondeo de fallas](#) para más información.

[ADVERTENCIA: Incidente del desciframiento del mensaje de falla.](#)

Mensaje de error:

```
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
```

Este problema ocurre debido a la configuración de la clave de failover. Para resolver este problema, quitar el clave de failover, y configurar la nueva clave compartida.

Información Relacionada

- [Página del soporte de PIX de las Cisco 500 Series](#)
- [Configuración de falla del módulo de servicios del firewall \(FWSM\)](#)
- [Troubleshooting del Failover FWSM](#)
- [Cómo el Failover trabaja en el Cisco Secure PIX Firewall](#)
- [Página de Soporte de Cisco 5500 Series Adaptive Security Appliance](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)