Contenido

Introducción

Este documento describe la configuración de High Availability(HA) para la defensa Centers(DC) de la serie 3.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Tecnología de la potencia de fuego
- Conceptos de gran disponibilidad básicos

Componentes Utilizados

La información en este documento se basa en la versión de software que se ejecuta 5.3 de los dispositivos de la serie 3 del centro de la defensa de la potencia de fuego (DC1500,DC2000,DC3500,DC4000) a la versión de software 5.4.1.6

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.

Antecedentes

Para asegurar la continuidad de las operaciones, la característica de gran disponibilidad permite

que usted señale los centros redundantes de la defensa para manejar los dispositivos. El centro de la defensa mantiene las secuencias de los datos de evento de los dispositivos administrados y de ciertos elementos de configuración de estos dispositivos. Si una defensa de centro falla, usted puede monitorear su red sin la interrupción a través del otro centro de la defensa.

Características de gran disponibilidad

- La sincronización HA es bidireccional que significa aunque hay un primario y un dispositivo secundario señalados, los cambios agregados en de los dispositivos se replica al otro.
- El HA no requiere los dispositivos ser conectado directamente. La conexión HA se puede hacer sobre un Switch pero esta conexión necesita estar en el mismo dominio de broadcast.
- Los dispositivos HA comunican sobre su IP de administración en el puerto 8305.
- El tiempo de sincronización HA para un dispositivo es cinco minutos, así que significa que después de que cada cinco anote las tentativas de un dispositivo de sincronizar su configuración con su par. Desde el tiempo requerido para la sincronización es específico a los dispositivos, acumulativo, el tiempo de sincronización se puede maximizar a diez minutos.
- Si una nueva imagen se requiere para un par específico HA se recomienda para romper el HA y entonces la nueva imagen.
- Si usted planea actualizar el cluster HA no es necesario romper el HA. Cuando usted actualiza de la versión 5.3.0 a 5.4.0, actualice los dispositivos uno por uno y una vez que se actualizan realice una tarea de la sincronización en el centro de la forma de defensa principal.
- La presencia de una política de acceso con el mismo nombre en ambos DCS crea dos directivas del control de acceso del mismo nombre. Una directiva se configura localmente y la otra se sincroniza del par DC.

  Nota: Usted no puede agregar una blanco o aplicar esta directiva porque lanza para arriba un error, que estado que hay ya una directiva con el mismo nombre.
- Las licencias no se sincronizan entre los pares de DC, por lo tanto, se requieren ser agregadas por separado a DCS.
- Todos los dispositivos administrados se agregan solamente a un DC. La configuración se sincroniza entre el par DCS.
- Los dispositivos administrados envían los registros a ambos DCS.
- DCS sincroniza las últimas acciones. Por ejemplo, si usted borra a un usuario de DC-1, el otro par DC-2 no sincroniza la configuración de usuario a DC-1. Sincroniza la **acción de la cancelación** y pierden al usuario de DC-1 y de DC-2.

Configuración compartida bidireccional entre los pares

El HA DCS sincroniza las directivas bidireccional. Estas configuraciones se sincronizan

bidireccional entre los pares. Usted puede también ver la mayor parte de estas configuraciones con la trayectoria definidas a la derecha al lado de ella:

Identidades y autenticación

- La configuración externa LDAP navega al **sistema > al Local > User Management (Administración de usuario) > autenticación externa**
- Usuarios (interno y externo) - Navegue el toSystem **> a los usuarios de Management> del usuario de Local>**
- Los papeles de usuario de encargo navegan el toSystem **> el Local > User Management (Administración de usuario) > los rol del usuario**

Informes

- Las plantillas del informe navegan a la **descripción > a la información > a las plantillas de informes**

Directivas configurables (bajo sección de las directivas)

- Directivas del control de acceso, directivas de la intrusión, directivas del archivo, directivas SSL, directivas de acceso a la red, directivas y reglas de la correlación, lista blanca de la conformidad y perfiles del tráfico.
- Las reglas de la intrusión (Local y SRU) - navegue los toPolicies **> el editor de la regla de Intrusion> > las reglas locales.**
- Detección de red, atributos del host, comentarios del usuario de la detección de red, incluyendo las notas y la criticalidad del host, la cancelacíon de los host, las aplicaciones, y las redes de la correlación de la red y la desactivación o la modificación de las vulnerabilidades.
- Detectores de encargo de la aplicación
- Las conexiones LDAP en las directivas del usuario navegan los toPolicies **> Users**
- Las alarmas navegan a las **acciones > a las alertas de Policies>** (bajo respuestas)

Información del dispositivo

- Las reglas NAT navegan los toDevices **> el NAT**
- Las reglas VPN navegan los toDevices **> el VPN**
- Toda la información del dispositivo incluyendo el nombre y su grupo se sincroniza bidireccional. La ubicación para el almacenamiento del registro para cada dispositivo también se sincroniza entre los pares **> la Administración de dispositivos**
- Clasificaciones de encargo de la regla de la intrusión
- Huellas dactilares de encargo activadas
- Política del sistema y política sanitaria
- Paneles de encargo, flujos de trabajo de encargo y tablas de encargo
- Cambie la reconciliación, las fotos y las configuraciones del informe
- Base de datos de las actualizaciones (SRU), de Geolocation de la regla de Sourcefire (GeoDB), y actualizaciones de la base de datos de la vulnerabilidad (VDB)

La configuración no sincronizó entre DCS

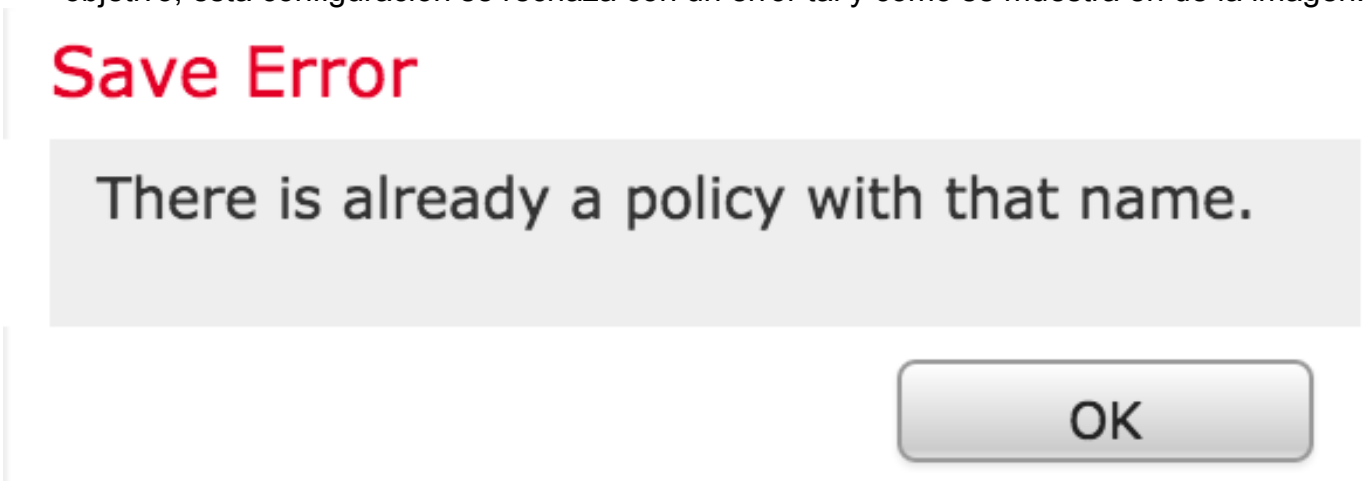
- Información del agente de usuario en política de usuario
- Exploraciones NMAP

- Grupos de la respuesta
- Módulos de la corrección
- Casos de la corrección
- Estreamer y cliente de la entrada del host
- Perfiles de reserva
- Horario
- Licencias
- Actualizaciones
- Alertas de la salud

Configurar

Requisitos previos para configurar la Alta disponibilidad

- Los dispositivos deben estar de la misma versión de software y hardware.
- Los dispositivos deben tener el mismo VDB instalado.
- Los dispositivos deben tener el mismo SRU.
- Asegúrese que ambos centros de la defensa tengan una cuenta de usuario nombrada admin con los privilegios de administrador. Estas cuentas deben utilizar la misma contraseña.
- Asegúrese de que con excepción de la cuenta de administración, los dos centros de la defensa no tengan cuentas de usuario con los nombres de usuario idénticos. Quite o retitule uno de la cuenta de usuarios duplicado antes de que usted establezca la Alta disponibilidad.
- Asegúrese que ambos los dispositivos no tengan ninguna directivas del control de acceso con el mismo nombre. Si hay dos directivas del control de acceso con el mismo nombre ellos ambos coexisten en DCS. Sin embargo, no pueden conseguir asociados con ningún dispositivo. Una vez que usted salva esta directiva después de agregar un dispositivo objetivo, esta configuración se rechaza con un error tal y como se muestra en de la imagen:



- Ambos los centros de la defensa deben tener acceso a Internet.

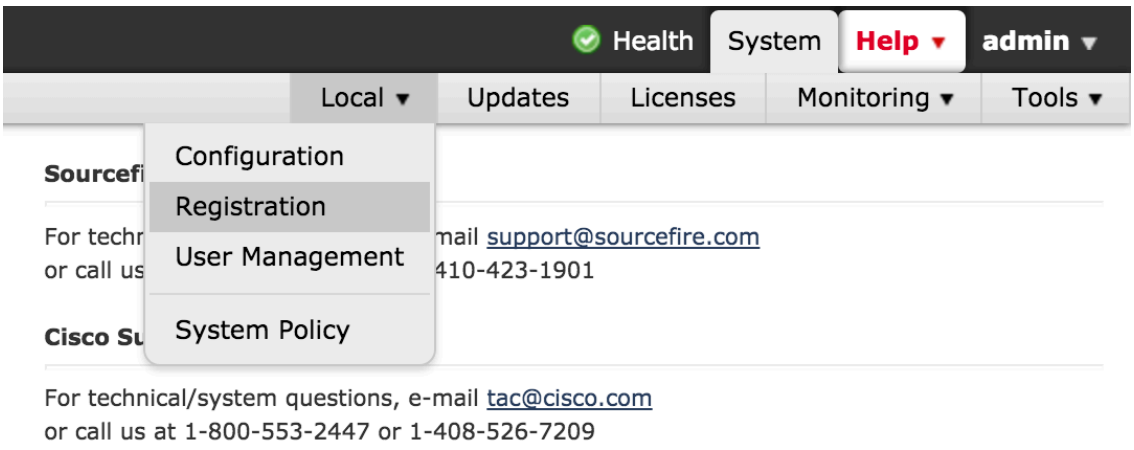
Alta disponibilidad de la configuración

Éstos son los 8 pasos para configurar la Alta disponibilidad.

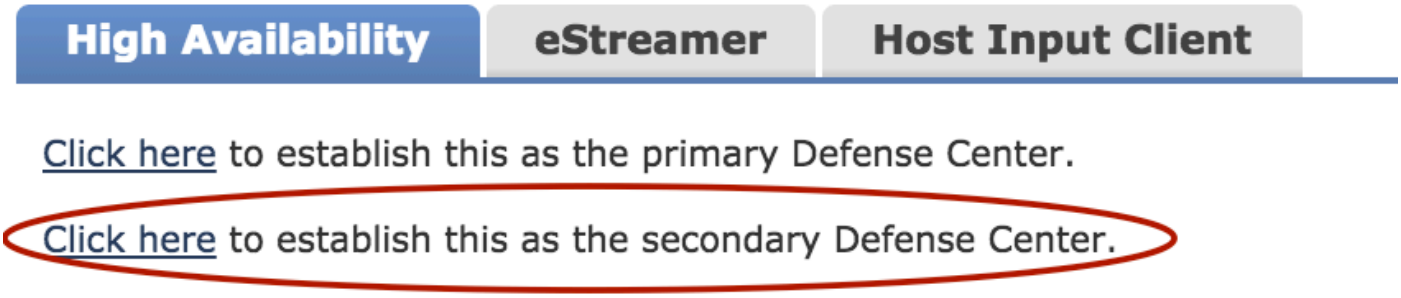
Paso 1. Confirme que la versión de software y hardware junto con la versión VDB y la versión de la actualización de la regla son lo mismo.

Model	Defense Center 1500
Serial Number	BZDW14300158
Software Version	5.4.1.2 (build 38)
OS	Sourcefire Linux OS 5.4.0 (build126)
Snort Version	2.9.7 GRE (Build 262)
Rule Update Version	2015-11-16-001-vrt
Rulepack Version	1606
Module Pack Version	1837
Geolocation Update Version	None
VDB Version	build 258 (2015-11-10 22:58:57)

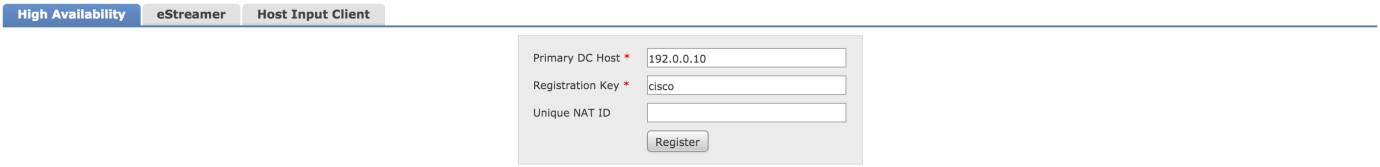
Paso 2. Para hacer su dispositivo secundario, navegue al **sistema > al Local > al registro**, tal y como se muestra en de la imagen. Asegúrese de que usted no tenga ninguna configuración en este DC.



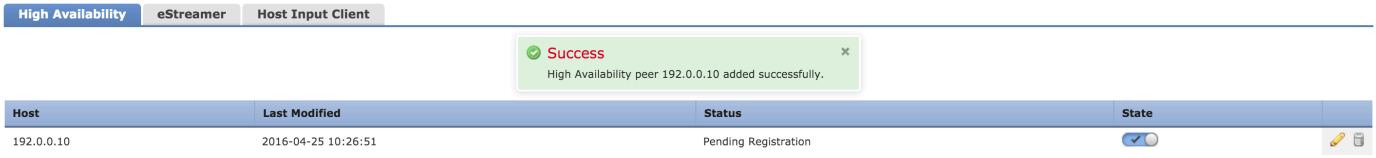
Paso 3. Bajo lengueta **de gran disponibilidad** haga clic en **hacen clic aquí para establecer esto como centro secundario de la defensa**, tal y como se muestra en de la imagen:



Paso 4. Pues usted completa el paso 3, una página se visualiza tal y como se muestra en de la imagen. Agregue el IP de DC primario y de la clave del paso. Asegúrese de que usted agregue una IDENTIFICACIÓN NAT única para los dispositivos, que están detrás de una traducción de dirección de red.



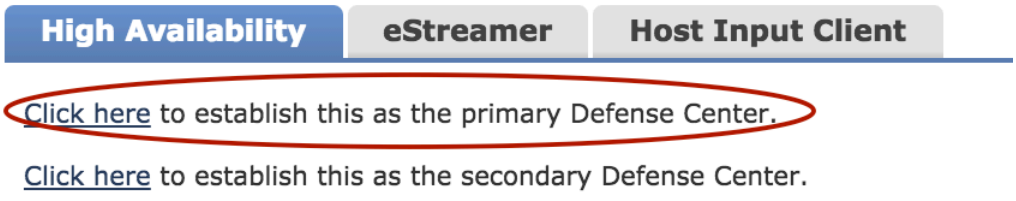
Paso 5. Después de que se verifique el IP Address, si está correcto haga clic en el **registro**. Usted ve una página tal y como se muestra en de la imagen:



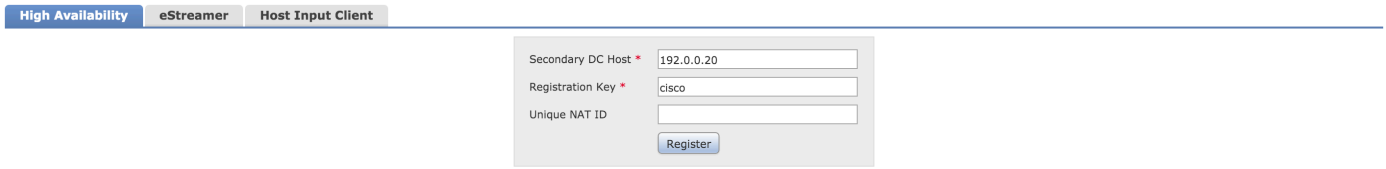
Esto significa que el HA está configurado en DC secundario y usted necesita configurarlo en DC primario.

Paso 6. Login al dispositivo que usted desea configurar como DC primario. Navegue al **sistema > al Local > al registro.**

Bajo lengueta **de gran disponibilidad** haga clic en **hacen clic aquí para agregar como el centro de la forma de defensa principal**, tal y como se muestra en de la imagen:

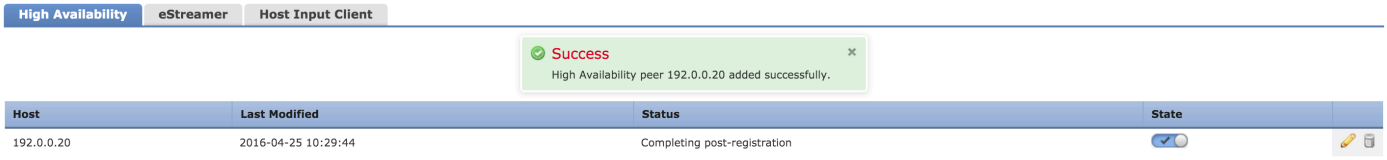


Paso 7. Después de que usted complete el paso 6, una página se visualiza tal y como se muestra en de la imagen:



Agregue el IP secundario de DC. Proporcione la misma clave y identificación NAT del registro que fue proporcionada mientras que usted configuró DC secundario.

Paso 8. Después de los detalles del IP se verifican hacen clic en el **registro.** Una vez que el registro es completo, la página del éxito se considera tal y como se muestra en de la imagen:



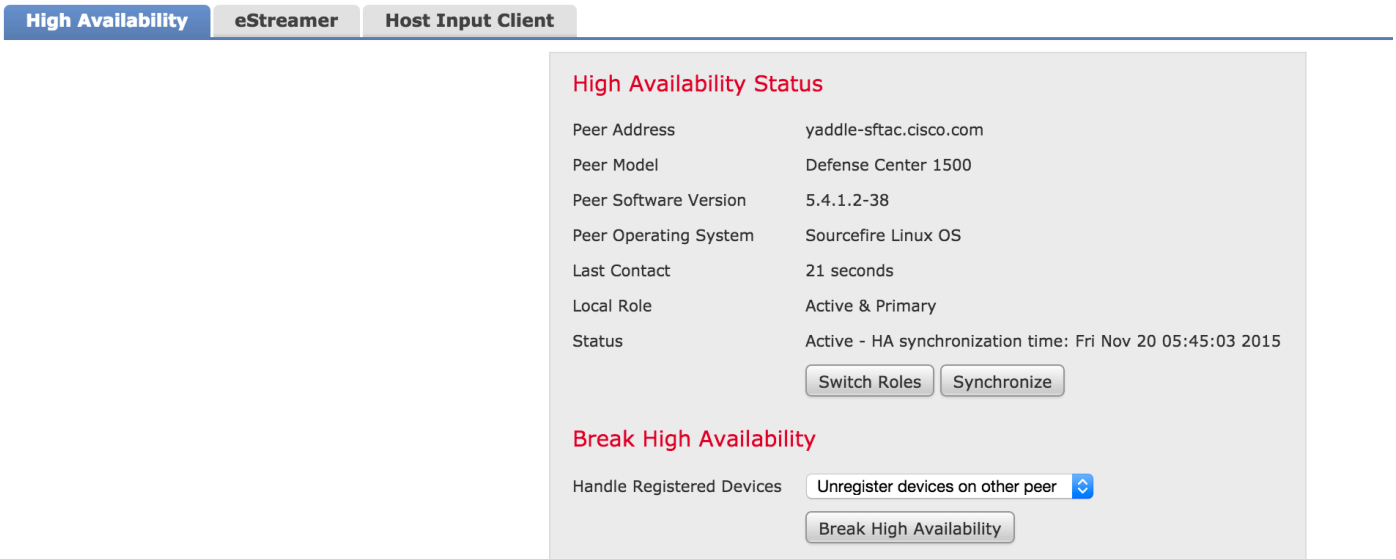
Después 5-10 de los minutos HA se completan la configuración y la sincronización.

Tarda casi 5-10 minutos para completar la configuración y la sincronización HA

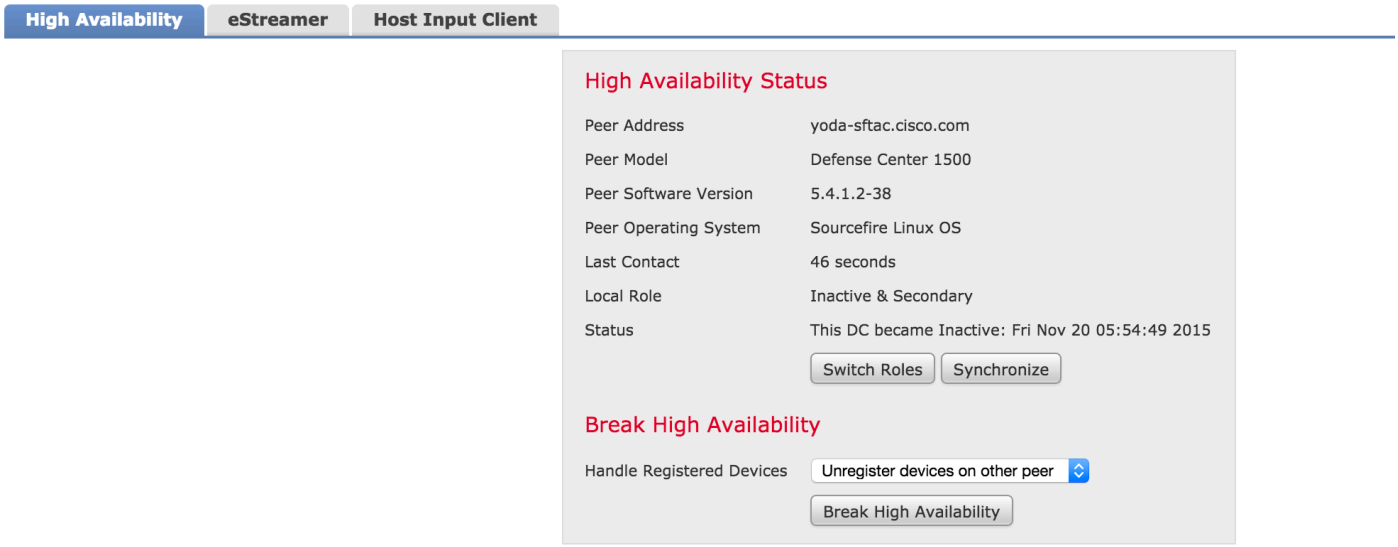
Verificación

Configuración gradual a verificar que su DC esté configurado correctamente para la Alta disponibilidad.

Paso 1. Navegue al **>Registration >Local del sistema** en el Dispositivo principal tal y como se muestra en de la imagen:



Paso 2. **>Registration >Local del sistema** en el dispositivo secundario tal y como se muestra en de la imagen:



Troubleshooting

Esta sección proporciona los pasos básicos para Troubleshooting para la Alta disponibilidad.

- Asegúrese que ambos DC esté escuchando en el puerto TCP 8305, puesto que el HA utiliza este puerto para sincronizar la información y los latidos del corazón.
- Asegúrese que el puerto TCP 8305 no sea bloqueado en la red o por ninguna dispositivos intermedios.
- La creación HA falla si hay una entrada añeja de un dispositivo de peer anterior se quite o se substituya que. La tabla de EM_Peers proporciona más información sobre tales dispositivos de peer.

Información Relacionada

- Configuración del stack en los dispositivos de las 8000 Series de la potencia de fuego de Cisco
- Guía de usuario del sistema de Firesight 5.4.1
- Soporte Técnico y Documentación - Cisco Systems