Preguntas frecuentes sobre Cisco FindIT Network Management

Objetivo

Cisco FindIT Network Management es un software que le permite administrar fácilmente toda la red, incluidos los dispositivos de Cisco, a través de su navegador web. Detecta, supervisa y configura automáticamente todos los dispositivos de Cisco admitidos en su red. Este software también le envía notificaciones sobre las actualizaciones de firmware y la información sobre los dispositivos de la red que ya no son compatibles con la garantía.

Cisco FindIT Network Management tiene dos componentes independientes: un único administrador conocido como FindIT Network Manager y una o más sondas conocidas como la sonda de red FindIT.

Este artículo contiene las preguntas frecuentes sobre la configuración, configuración y resolución de problemas de Cisco FindIT Network Management y sus respuestas.

Preguntas Frecuentes

Table Of Contents

Acceso remoto

Actualización de software

General

1. ¿Qué idiomas admite FindIT Network Management?

FindIT Network Management se traduce a los siguientes idiomas:

- Chino
- Inglés
- Francés
- Alemán
- Japonés
- Español

Descubrimiento

2. ¿Qué protocolos utiliza FindIT para administrar mis dispositivos?

FindIT utiliza diversos protocolos para descubrir y gestionar la red. El protocolo exacto que se utiliza para un dispositivo determinado varía en función del tipo de dispositivo. Estos protocolos incluyen:

- Sistema de nombres de dominio multidifusión (mDNS) y Detección de servicios DNS:

este protocolo también se conoce como Bonjour. Localiza dispositivos como impresoras, otros ordenadores y los servicios que ofrecen esos dispositivos en una red local. Para obtener más información sobre mDNS, haga clic aquí. Para obtener más información sobre DNS Service Discovery, haga clic aquí.
- Cisco Discovery Protocol (CDP): protocolo exclusivo de Cisco utilizado para compartir información sobre otros equipos de Cisco conectados directamente, como la versión del sistema operativo y la dirección IP.
- Protocolo de descubrimiento de la capa de enlace (LLDP): protocolo neutral de proveedor utilizado para compartir información sobre otros equipos conectados directamente, como la versión del sistema operativo y la dirección IP.
- Protocolo simple de administración de red (SNMP): protocolo de administración de red utilizado para recopilar información y configurar dispositivos de red como servidores, impresoras, hubs, switches y routers en una red de protocolo de Internet (IP).
- RESTCONF: un borrador del Grupo de Trabajo de Ingeniería de Internet (IETF) que describe cómo asignar una especificación de lenguaje de modelado de datos Otra generación (YANG) a una interfaz RESTful. Para obtener más información, haga clic aquí.

3. ¿Cómo detecta FindIT mi red?

La sonda de red FindIT genera una lista inicial de dispositivos en la red desde la escucha a los anuncios CDP, LLDP y mDNS. A continuación, la sonda se conecta a cada dispositivo mediante un protocolo compatible y recopila información adicional como tablas de adyacencia CDP y LLDP, tablas de direcciones de Control de acceso a medios (MAC) y listas de dispositivos asociadas. Esta información se utiliza para identificar dispositivos adicionales en la red y el proceso se repite hasta que se descubren todos los dispositivos.

4. ¿FindIT realiza análisis de red?

FindIT no analiza activamente los rangos de direcciones de red. Utiliza una combinación de supervisión pasiva de ciertos protocolos de red y consulta activa a los dispositivos de red para obtener información.

Administración de puertos

5. ¿Por qué la Administración de puertos no muestra los puertos de pila?

Las ilustraciones de Administración de puertos se dibujan en función de la lista de puertos que proporciona el dispositivo a través de los protocolos de administración. Cuando se encuentra en modo de apilamiento, los puertos de pila se consideran una conexión interna dentro de la pila, por lo que el dispositivo no incluye estos puertos en las listas proporcionadas a través de los protocolos de administración.

Configuración

6. ¿Qué ocurre cuando se detecta un dispositivo nuevo? ¿Se cambiará su configuración?

Se agregarán nuevos dispositivos al grupo de dispositivos predeterminado. Si los perfiles de configuración se han asignado al grupo de dispositivos predeterminado, esa configuración también se aplicará a los dispositivos recién descubiertos.

7. ¿Qué ocurre cuando muevo un dispositivo de un grupo de dispositivos a otro?

Se quitará cualquier configuración de red de área local virtual (VLAN) o de red de área local inalámbrica (WLAN) asociada a perfiles que actualmente se aplican al grupo de dispositivos original y no se aplican al nuevo grupo de dispositivos, y se agregará al dispositivo la configuración de VLAN o WLAN asociada a perfiles que se aplican al nuevo grupo y que no se aplican al grupo original. Los perfiles aplicados al nuevo grupo sobrescribirán los parámetros de configuración del sistema. Si no se definen perfiles de configuración del sistema para el nuevo grupo, la configuración del sistema para el dispositivo no cambiará.

Consideración de seguridad

8. ¿Qué rangos de puertos y protocolos requiere FindIT Network Manager?

La siguiente tabla contiene los protocolos y puertos que usa FindIT Network Manager:

Puerto	Dirección:	Protocolo	Uso
TCP 22	Entrante	SSH	Acceso de línea de comandos al administrador
TCP 80	Entrante	HTTP	Acceso Web al administrador. Redirige al servidor web seguro (puerto 443)
TCP 443	Entrante	HTTPS	Acceso web seguro al administrador
TCP 1069	Entrante	NETCONF/TLS	Comunicación entre sondeo y administrador
TCP 9443	Entrante	HTTPS	Acceso remoto a la GUI de sondeo
TCP 50000-51000	Entrante	Depende del dispositivo	Acceso remoto a dispositivos
UDP 53	Salientes	DNS	Resolución de nombres de dominio
UDP 123	Salientes	NTP	Sincronización horaria
UDP 5353	Salientes	mDNS	Anuncios de servicio DNS de multidifusión a la red local anunciando al administrador

9. ¿Qué rangos de puertos y protocolos requiere la sonda de red FindIT?

En la tabla siguiente se enumeran los protocolos y puertos utilizados por la sonda de red FindIT:

Puerto	Dirección:	Protocolo	Uso
TCP 22	Entrante	SSH	Acceso de línea de comandos a sondeo
TCP 80	Entrante	HTTP	Acceso Web al administrador. Redirige al servidor web seguro (puerto 443)
TCP 443	Entrante	HTTPS	Acceso web seguro al administrador

UDP 5353	Entrante	mDNS	Anuncios de servicio DNS de multidifusión desde la red local. Se utiliza para la detección de dispositivos.
TCP 10000-10100	Entrante	Depende del dispositivo	Acceso remoto a dispositivos
UDP 53	Salientes	DNS	Resolución de nombres de dominio
UDP 123	Salientes	NTP	Sincronización horaria
TCP 80	Salientes	HTTP	Gestión de dispositivos sin servicios web seguros habilitados
UDP 161	Salientes	SNMP (Protocolo de administración de red simple)	Gestión de dispositivos de red
TCP 443	Salientes	HTTPS	Gestión de dispositivos con servicios web seguros habilitados. Acceda a los servicios web de Cisco para obtener información como actualizaciones de software, soporte, estado y avisos de fin de vida útil
TCP 1069	Salientes	NETCONF/TLS	Comunicación entre sondeo y administrador
UDP 5353	Salientes	mDNS	Anuncios de servicio DNS de multidifusión a la red local anunciando la sonda

10. ¿Qué grado de seguridad ofrece la comunicación entre FindIT Network Manager y FindIT Network Probe?

Toda la comunicación entre el administrador y la sonda se cifra mediante una sesión de seguridad de la capa de transporte (TLS) 1.2 autenticada con certificados de cliente y servidor. La sesión se inicia desde la sonda al administrador. Cuando se establece por primera vez la asociación entre el administrador y la sonda, el usuario debe iniciar sesión en el administrador desde la sonda, momento en el que el administrador y la sonda intercambian certificados para autenticar futuras comunicaciones.

11. ¿FindIT tiene acceso "puerta trasera" a mis dispositivos?

No. Cuando FindIT detecte un dispositivo de Cisco compatible, intentará acceder al dispositivo utilizando las credenciales predeterminadas de fábrica para ese dispositivo con el nombre de usuario y la contraseña predeterminados: cisco o la comunidad SNMP predeterminada: público. Si la configuración del dispositivo se ha cambiado del valor predeterminado, será necesario que el usuario proporcione las credenciales correctas a FindIT.

12. ¿Qué grado de seguridad tienen las credenciales almacenadas en FindIT?

Las credenciales para acceder a FindIT se hash de forma irreversible mediante el algoritmo

SHA512. Las credenciales de los dispositivos y otros servicios, como **Cisco Active Advisor**, se cifran de forma irreversible mediante el algoritmo AES-128.

13. ¿Cómo puedo recuperar una contraseña perdida para la GUI de administración?

Si ha perdido la contraseña de todas las cuentas de administración en la GUI de administración, puede restablecer la contraseña iniciando sesión en la consola de la sonda o el administrador y ejecutando la herramienta **recovery password**. Esta herramienta restablece la contraseña predeterminada de la cuenta de cisco o, si se ha eliminado la cuenta de cisco, volverá a crearla con la contraseña predeterminada. A continuación se muestra un ejemplo de los comandos que se deben proporcionar para restablecer la contraseña usando esta herramienta.

```
cisco@FindITProbe:~# recovery password

¿Está seguro? (s/n) y

Restablecer la cuenta de Cisco a la contraseña predeterminada

cisco@FindITProbe:~#
```

Acceso remoto

14. Cuando me conecto a la GUI de administración de un dispositivo desde FindIT Network Management, ¿la sesión es segura?

FindIT Network Management tuneliza la sesión de acceso remoto entre el dispositivo y el usuario. El protocolo utilizado dependerá de la configuración del dispositivo final, pero FindIT siempre establecerá la sesión utilizando un protocolo seguro si se activa uno (por ejemplo, se preferirá HTTPS a HTTP). Si el usuario se conecta al dispositivo a través del administrador, la sesión pasará a través de un túnel cifrado a medida que pasa entre el administrador y la sonda, independientemente de los protocolos habilitados en el dispositivo.

15. ¿Por qué se desconecta inmediatamente mi sesión de acceso remoto con un dispositivo cuando abro una sesión de acceso remoto a otro dispositivo?

Al acceder a un dispositivo mediante FindIT Network Management, el explorador considera que cada conexión se encuentra con el mismo servidor web (FindIT), por lo que presentará cookies de cada dispositivo a cada otro dispositivo. Si varios dispositivos utilizan el mismo nombre de cookie, existe la posibilidad de que otro dispositivo sobrescriba una cookie de dispositivo. Esto se ve con más frecuencia con las cookies de sesión, y el resultado es que la cookie sólo es válida para el dispositivo más recientemente visitado. Todos los demás dispositivos que utilizan el mismo nombre de cookie verán que la cookie no es válida y finalizarán la sesión.

16. ¿Por qué falla mi sesión de acceso remoto con un error como el siguiente: Error de acceso: Solicitar entidad demasiado grande, el campo de encabezado HTTP supera el tamaño admitido?

Después de realizar muchas sesiones de acceso remoto con diferentes dispositivos, el navegador tendrá un gran número de cookies almacenadas para el dominio de sonda. Para solucionar este problema, utilice los controles del explorador para borrar las cookies del dominio y volver a cargar la página.

Actualización de software

17. ¿Cómo puedo mantener actualizado el sistema operativo del jefe?

El Administrador utiliza la distribución CentOS Linux para un sistema operativo. Los paquetes y el kernel pueden actualizarse usando los procesos estándar de CentOS. Por ejemplo, para realizar una actualización manual, inicie sesión en la consola como el usuario de cisco e ingrese el comando *sudo yum -y* update. El sistema no debe actualizarse a una nueva versión de CentOS y no deben instalarse paquetes adicionales que no sean los incluidos en la imagen de máquina virtual suministrada por Cisco.

18. ¿Cómo se actualiza Java en el jefe?

Las actualizaciones de Java deben descargarse de Oracle e instalarse manualmente mediante los siguientes comandos:

Para descargar un nuevo paquete Java directamente al administrador:

```
curl -L -O -H "Cookie: oraclelicense=accept-securebackup-cookie" -k
http://download.oracle.com/otn-pub/java/jdk/<version>-<build>/jre-<version>-linux-x64.rpm
```

Debajo tiene un ejemplo:

```
curl -L -O -H "Cookie: oraclelicense=accept-securebackup-cookie" -k
"http://download.oracle.com/otn-pub/java/jdk/8u102-b14/jre-8u102-linux-x64.rpm"
```

Para instalar la versión actualizada de Java:

Paso 1. Quite la versión anterior con el comando *sudo yum -y remove jre1.8.0_102*

Paso 2. Instale la nueva versión con el comando *sudo yum -y localinstall jre-<version>-linux-x64.rpm*

19. ¿Cómo puedo mantener actualizado el sistema operativo de sondeo?

La sonda utiliza OpenWRT para un sistema operativo. Los paquetes incluidos pueden actualizarse utilizando la herramienta **opkg**. Por ejemplo, para actualizar todos los paquetes del sistema, inicie sesión en la consola como el usuario de cisco e introduzca el comando update-packets. Cuando sea necesario, Cisco proporcionará actualizaciones del núcleo como parte de una nueva versión de la sonda. No se deben instalar paquetes adicionales más allá de los incluidos en la imagen de máquina virtual proporcionada por Cisco.

20. ¿Qué es el complemento Cisco FindIT Kaseya?

El complemento Cisco FindIT Kaseya se ha diseñado para aumentar la eficacia operativa mediante la estrecha integración de Cisco FindIT Network Manager con el administrador del sistema virtual Kaseya (VSA). El complemento Cisco FindIT Kaseya ofrece potentes funciones, como administración de acciones, paneles, detección de dispositivos, topología de red, gestión de dispositivos remotos, alertas procesables e historial de eventos.

El plug-in está diseñado para ser extremadamente fácil de instalar y requiere sólo unos cuantos clics. Cumple con todos los requisitos de integración de terceros para las versiones 9.3 y 9.4 de VSA in situ de Kaseya. Para obtener más información, haga clic aquí.