Preguntas frecuentes sobre Cisco Business Dashboard

Objetivo

Cisco Business Dashboard 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 actualizaciones de firmware e información sobre los dispositivos de la red que ya no están admitidos por la garantía.

Este artículo contiene las respuestas a las preguntas más frecuentes al configurar, configurar y solucionar problemas de Cisco Business Dashboard Network Management.

Preguntas Frecuentes

Table Of Contents

Acceso remoto

Actualización de software

General

1. ¿Qué idiomas admite Cisco Business Dashboard Network Management?

Cisco Business Dashboard Network Management se traduce a los siguientes idiomas:

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

Descubrimiento

2. ¿Qué protocolos utiliza Cisco Business Dashboard para administrar mis dispositivos?

Cisco Business Dashboard utiliza una variedad de 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 descubre Cisco Business Dashboard mi red?

La sonda del panel empresarial de Cisco 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. ¿Cisco Business Dashboard realiza análisis de red?

Cisco Business Dashboard no analiza activamente la red más amplia. La sonda utilizará el protocolo ARP para escanear la subred IP a la que está directamente conectada, pero no intentará escanear ningún otro rango de direcciones. La sonda también probará cada dispositivo detectado para detectar la presencia de un servidor web y un servidor SNMP en los puertos estándar.

Configuración

5. ¿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.

6. ¿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

7. ¿Qué rangos de puertos y protocolos requiere Cisco Business Dashboard Network Manager?

La siguiente tabla contiene los protocolos y puertos que utiliza Cisco Business Dashboard:

Puerto	Dirección:	Protocolo	Uso
TCP 22	Entrante	SSH	Acceso de línea de comandos al panel. SSH está desactivado de forma predeterminada en la imagen de la máquina virtual de Cisco.
TCP 80	Entrante	HTTP	Acceso Web al Panel. Redirige al servidor web seguro (puerto 443).
TCP 443	Entrante	TCP multiplexado HTTPS	Acceso web seguro al panel. Comunicación entre sonda y panel.
TCP 50000 - 51000	Entrante	HTTPS	Acceso remoto a dispositivos.
TCP 53	Salientes	DNS	Resolución de nombres de dominio.
UDP 123	Salientes	NTP	Sincronización horaria.
TCP443	Salientes	HTTPS	Acceda a los servicios web de Cisco para obtener información como actualizaciones de software, estado de soporte y avisos de fin de vida útil. Acceda al sistema operativo y a los servicios de actualización de aplicaciones.
UDP 5353	Salientes	mDNS	Anuncios de servicio DNS de multidifusión a la red local anunciando al administrador

8. ¿Qué intervalos de puertos y protocolos requiere la sonda Cisco Business Dashboard?

En la tabla siguiente se enumeran los protocolos y puertos utilizados por la sonda de Cisco Business Dashboard:

Puerto	Dirección:	Protocolo	Uso
TCP 22	Entrante	SSH	Acceso de línea de comandos a sonda. SSH está desactivado de forma predeterminada en la imagen de la máquina virtual de Cisco.
TCP 80	Entrante	HTTP	Acceso web a sondeo. Redirige al servidor web seguro (puerto 443)
TCP 443	Entrante	HTTPS	Acceso web seguro a sondeo.
UDP 5353	Entrante	mDNS	Anuncios de servicio DNS de multidifusión desde la red local. Se utiliza para la detección de 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	TCP multiplexado HTTPS	Gestión de dispositivos con servicios web seguros habilitados. Acceda a los servicios web de Cisco para obtener información como actualizaciones de

			software, estado de soporte y avisos de fin de vida útil. Acceda al sistema operativo y a los servicios de actualización de aplicaciones.
UDP 5353	Salientes	mDNS	Comunicación entre sonda y panel. Anuncios de servicio DNS de multidifusión a la red local anunciando la sonda.

9. ¿Qué grado de seguridad ofrece la comunicación entre Cisco Business Dashboard Network Manager y Cisco Business Dashboard Probe?

Toda la comunicación entre el panel y la sonda se cifra mediante una sesión TLS 1.2 autenticada con certificados de cliente y servidor. La sesión se inicia desde la sonda hasta el panel. Cuando se establece por primera vez la asociación entre el panel y la sonda, el usuario debe iniciar sesión en el panel a través de la sonda.

10. ¿Tiene Cisco Business Dashboard acceso "puerta trasera" a mis dispositivos?

No. Cuando Cisco Business Dashboard detecte un dispositivo 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 Cisco Business Dashboard.

11. ¿Qué grado de seguridad tienen las credenciales almacenadas en Cisco Business Dashboard?

Las credenciales para acceder a Cisco Business Dashboard se filtran 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.

12. ¿Cómo se recupera una contraseña perdida para la interfaz de usuario web (IU)?

Si ha perdido la contraseña para todas las cuentas de administrador en la interfaz de usuario Web, puede restablecer la contraseña iniciando sesión en la consola de la sonda y ejecutando la herramienta **cbdprobe recovery password**, o iniciando sesión en la consola de la sonda y ejecutando la **herramienta cisco-business-Dashboard 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 mediante esta herramienta.

```
cisco@cisco-business-dashboard:~$ recuperación de contraseña de cisco-business-panel ¿Está seguro? (s/n) y Se recuperó la cuenta de cisco con la contraseña predeterminada recuperación de contraseña Cisco Business Dashboard correcta cisco@Cisco Panel empresarialSondeo:~$
```

Al utilizar Cisco Business Dashboard para AWS, la contraseña se establecerá en la ID de instancia de AWS.

13. ¿Cuál es el nombre de usuario y la contraseña predeterminados para el cargador de inicialización de la máquina virtual?

Las credenciales predeterminadas para el cargador de inicialización de la máquina virtual son nombre de usuario: **raíz** y contraseña: **Cisco.** Estos cambios se pueden modificar ejecutando la herramienta config_vm y respondiendo sí cuando se le pregunte si desea cambiar la contraseña del cargador de inicialización.

Acceso remoto

14. Cuando me conecto a la interfaz de usuario web de un dispositivo desde Cisco Business Dashboard Network Management, ¿la sesión es segura?

Cisco Business Dashboard tuneliza la sesión de acceso remoto entre el dispositivo y el usuario. El protocolo utilizado entre la sonda y el dispositivo dependerá de la configuración del dispositivo final, pero Cisco Business Dashboard 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 panel, la sesión pasará a través de un túnel cifrado a medida que pasa entre el panel y la sonda, independientemente de los protocolos habilitados en el dispositivo. La conexión entre el explorador web del usuario y el panel siempre será HTTPS.

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

Cuando accede a un dispositivo a través de Cisco Business Dashboard, el explorador considera que cada conexión se encuentra con el mismo servidor web (el panel), 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 la cookie de un 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. El resto de dispositivos que utilizan el mismo nombre de cookie verán que la cookie no es válida y se cerrará 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 del Panel. 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 Panel?

El Panel utiliza la distribución Ubuntu Linux para un sistema operativo. Los paquetes y el kernel pueden actualizarse usando los procesos Ubuntu estándar. Por ejemplo, para realizar una actualización manual, inicie sesión en la consola como usuario de cisco e ingrese los comandos:

```
actualización de sudo apt-get y actualización de sudo apt-get
```

El sistema no debe actualizarse a una nueva versión de Ubuntu, y se recomienda no instalar paquetes adicionales más allá de los incluidos en la imagen de máquina virtual suministrada por Cisco, o los instalados como parte de una instalación mínima de Ubuntu.

18. ¿Cómo se actualiza Java en el panel?

Cisco Business Dashboard utiliza los paquetes OpenJDK de los repositorios de Ubuntu. OpenJDK

se actualizará automáticamente como parte de la actualización del sistema operativo principal.

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

Cisco Business Dashboard utiliza la distribución Ubuntu Linux para un sistema operativo. Los paquetes y el kernel pueden actualizarse usando los procesos Ubuntu estándar. Por ejemplo, para realizar una actualización manual, inicie sesión en la consola como usuario de cisco e introduzca los comandos:

```
sudo apt-get update
```

y

```
actualización de sudo apt-get
```

El sistema no debe actualizarse a una nueva versión de Ubuntu, y se recomienda no instalar paquetes adicionales más allá de los incluidos en la imagen de máquina virtual suministrada por Cisco, o los instalados como parte de una instalación mínima de Ubuntu.

20. ¿Cómo mantengo actualizado el sistema operativo de sondeo al utilizar un Pi de frambuesa?

Los paquetes Raspbian y el kernel pueden ser actualizados usando los procesos estándar usados para las distribuciones Linux basadas en Debian. Por ejemplo, para realizar una actualización manual, inicie sesión en la consola como usuario de cisco e introduzca los comandos:

```
sudo apt-get update
```

y

```
actualización de sudo apt-get
```

El sistema no debe actualizarse a una nueva versión principal de Raspbian. Se recomienda que no se instalen paquetes adicionales más allá de los instalados como parte de la versión "Lite" de la distribución Raspbian y los que son agregados por el instalador de sonda.