REVIEW DRAFT - CISCO CONFIDENTIAL

Guía de inicio rápido de Cisco Business Dashboard y Probe

Primera publicación: 2020-11-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883


El logotipo de Java es una marca comercial o una marca comercial registrada de Sun Microsystems, Inc. en Estados Unidos u otros países.

CONTENIDO

CAPÍTULO 1

Descripción general de Cisco Business Dashboard

Este capítulo contiene las siguientes secciones:

Acerca de Cisco Business Dashboard

Cisco Business Dashboard proporciona herramientas que le ayudan a supervisar y administrar su red de las series de Cisco Business. Cisco Business Dashboard detecta automáticamente la red y permite configurar y controlar todos los dispositivos compatibles de Cisco Business, como, por ejemplo, puntos de acceso inalámbricos, routers y conmutadores. También notifica sobre la disponibilidad de las actualizaciones del firmware e informa sobre dispositivos que ya no están en garantía o bajo un contrato de soporte.

Cisco Business Dashboard es una aplicación distribuida que se compone de dos componenetes o aplicaciones independientes: la aplicación principal Cisco Business Dashboard, también conocida como *Dashboard* y una o más instancias de Cisco Business Dashboard Probe, también conocido como *Probe*.

Se instala una única instancia de Cisco Business Dashboard en una ubicación adecuada de la red. Desde la interfaz de usuario de Dashboard, puede obtener una vista de alto nivel del estado de todos los sitios de la red o centrarse en un solo sitio o dispositivo para ver información específica al respecto.

Una instancia de Cisco Business Dashboard Probe se instala en cada sitio de la red y se asocia con Dashboard. La sonda realiza exploraciones de la red y se comunica directamente con cada dispositivo administrado en nombre de Dashboard.

Ciertos dispositivos de red admiten que se asocien directamente con Dashboard y que se manejen sin la presencia de una sonda. Cuando los dispositivos de red se administran directamente de esta manera, todas las funciones de administración están disponibles para el dispositivo, pero puede que el proceso de descubrimiento de la red no sea tan exhaustivo que cuando hay una sonda presente.

REVIEW DRAFT - CISCO CONFIDENTIAL

Público

Esta guía está destinada principalmente a administradores de red responsables de la administración e instalación del software Cisco Business Dashboard.

Documentos Relacionados

La documentación de Cisco Business Dashboard se compone de varias guías independientes. Estos son algunos de ellos:

- **Guía de inicio rápido (este documento)**: esta guía facilita detalles sobre cómo realizar la configuración inicial de Cisco Business Dashboard mediante las opciones más usadas.
- **Guías de instalación**

  En la siguiente tabla, se muestran todas las guías de instalación del software Dashboard, que puede implementarse en diferentes plataformas. Consulte la ruta facilitada en la columna de ubicación para obtener más detalles:

Plataformas admitidas	Ubicación
Amazon Web Services	Guía de instalación de Cisco Business Dashboard para Amazon Web Services
Oracle VirtualBox	Guía de instalación de Cisco Business Dashboard para Oracle VirtualBox
Microsoft Hyper-V	Guía de instalación de Cisco Business Dashboard para Microsoft Hyper-V
VMware vSphere, Workstation y Fusion	Guía de instalación de Cisco Business Dashboard para VMWare
Ubuntu Linux (Dashboardy Probe) y Raspbian Linux (solo Probe)	Guía de instalación de Cisco Business Dashboard para Linux

- **Guía de administración**: esta guía de referencia proporciona información sobre todas las funciones y opciones del software, así como la forma de configurarlas y utilizarlas. Consulte la guía de administración de Cisco Business Dashboard.
- **Lista de compatibilidad de dispositivos**: esta lista proporciona información de los dispositivos admitidos porCisco Business Dashboard y las funciones disponibles para cada tipo de dispositivo. Para obtener una lista de todos los dispositivos que Cisco Business Dashboard admite, consulte Cisco Business Dashboard: lista de dispositivos admitidos.

Terminología

Plazo	Descripción
Hyper-V	Plataforma de virtualización proporcionada por Microsoft Corporation.
Archivo OVF (Open Virtualization Format)	Archivo TAR que contiene una o varias máquinas virtuales en formato OVF. Es un método independiente de la plataforma que permite empaquetar y distribuir máquinas virtuales (VM).
Archivo OVA (Open Virtual Appliance or Application)	Paquete que contiene los siguientes archivos usados para describir una máquina virtual. Se guarda como un único archivo con empaquetado .TAR: • Archivo descriptor (.OVF) • Archivos opcionales de certificado y de manifiesto (.MF).
Raspberry Pi	Un ordenador de placa única y muy bajo coste desarrollado por la Raspberry Pi Foundation. Para obtener más información, consulte *https://www.raspberrypi.org/*.
Raspbian	Una distribución de Linux basada en Debian y optimizada para Raspberry Pi. Para obtener más información, consulte *https://www.raspbian.org/*.
VirtualBox	Plataforma de virtualización proporcionada por Oracle Corporation.
Disco duro virtual (VHD)	Un disco duro virtual es un formato de archivo de imagen de disco donde se puede almacenar todo el contenido de un disco duro.
Máquina virtual (VM)	Entorno informático virtual en el que se puede ejecutar un sistema operativo invitado y el software de las aplicaciones asociadas Se pueden operar varias máquinas virtuales en el mismo sistema host de forma simultánea.
• VMware ESXi • VMware Fusion • vSphere Server • VMware Workstation	Plataforma de virtualización proporcionada por VMware Inc.
vSphere Client	Interfaz de usuario que permite a los usuarios conectarse de forma remota a vCenter Server o ESXi desde cualquier PC Windows. La interfaz principal de vSphere Client se puede usar para crear, administrar y supervisar las máquinas virtuales, sus recursos y los hosts. También proporciona acceso de consola a las máquinas virtuales.

CAPÍTULO 2

Realización de la configuración inicial de Dashboard

Este capítulo contiene las siguientes secciones:

Realización de la configuración inicial de Dashboard

Hay algunas tareas de configuración que se deben llevar a cabo para asegurarse de que Dashboard se ajuste a sus requisitos.

Configuración básica del sistema en la imagen de máquina virtual o la instancia de AWS

Para definir la configuración básica del sistema (por ejemplo, la dirección IP y la hora) en Dashboard, haga lo siguiente:

1. Conéctese a la consola de Dashboard utilizando las herramientas adecuadas para su hipervisor si utiliza una máquina virtual o si se conecta a su instancia de AWS mediante SSH.
2. Si utiliza una máquina virtual, inicie sesión con la contraseña y el nombre de usuario predeterminados con el valor: `cisco`. Para una instancia de AWS, utilice el par de claves que especificó cuando se creó la instancia y el nombre de usuario: `cisco`.

   Se le pedirá que cambie la contraseña de la cuenta cisco justo después de iniciar sesión. La nueva contraseña debe ser una palabra compleja que no aparezca en el diccionario y que esté compuesta por diversos tipos de caracteres.
3. Especifique el comando `sudo config_vm` para llevar a cabo la configuración inicial. Cuando se le solicite, especifique la contraseña de la cuenta de Cisco. La utilidad `config_vm` mostrará una serie de pasos para cambiar la configuración de la plataforma.
4. En primer lugar, se le pedirá que cambie el nombre de host de Dashboard. El nombre de host se utiliza para identificar Dashboard en la red. Aquí puede elegir un nombre significativo u omitir este paso si desea conservar el nombre de host predeterminado.

Nota Este paso no está disponible con Cisco Business Dashboard para el AWS.

Realización de la configuración inicial de Dashboard

5. A continuación, se le solicitará que cambie los puertos del servidor web. Si se cambian los valores predeterminados de estos puertos, es posible que también deba cambiarse la configuración del firewall en su red o la configuración del grupo de seguridad en AWS.
6. A continuación, se le pedirá que configure la interfaz de red. Las opciones aquí son Estático y DHCP (valor predeterminado). Si elige Estático, se le solicitará información sobre la dirección IP, la gateway predeterminada y el servidor DNS. La interfaz de red se restablecerá si hace cambios aquí.

Nota Este paso no está disponible con Cisco Business Dashboard para el AWS. Para modificar la configuración de red, utilice la consola EC2 en AWS.

7. Después se le pedirá que defina la configuración de hora para Dashboard. Puede optar por configurar uno o varios servidores NTP para la sincronización de la hora (recomendado). Se le pedirá que elija una zona horaria.

Nota Si el hipervisor en uso es VirtualBox y las Guest Additions de VirtualBox están instaladas en la máquina virtual, el servicio NTP (timesyncd) no funcionará.

8. Por último, se le preguntará si desea cambiar la contraseña del cargador de arranque. El nombre de usuario y la contraseña del cargador de arranque se pueden utilizar en la consola al iniciar el sistema para cambiar el proceso de arranque del sistema o recuperar las contraseñas perdidas del sistema operativo. Las credenciales predeterminadas del cargador de arranque son nombre de usuario: **root** y contraseña: **cisco**.

Podrá cambiar esta configuración cuando lo desee. Para ello, vuelva a ejecutar el script o acceda mediante la interfaz web a **Administración** > **Configuración de plataforma**.

Inicio de la interfaz de usuario de Dashboard

1. Abra un navegador web, por ejemplo **Google Chrome** o **Microsoft Edge**.
2. En el campo **Dirección**, escriba la dirección IP o el nombre de host de Dashboard y pulse **Intro**.
3. Introduzca el nombre de usuario predeterminado: `cisco`; y la contraseña: `cisco`. Si está utilizando Cisco Business Dashboard para AWS, la contraseña predeterminada es la ID de instancia. Puede ver la ID de instancia en la consola EC2 de AWS.
4. Haga clic en **Inicio de sesión**. Se le pedirá que cambie la contraseña de la cuenta de Cisco. La nueva contraseña debe tener como mínimo 8 caracteres y debe incluir, al menos, 3 tipos de caracteres diferentes.
5. Haga clic en **Next (Siguiente)**. Se le presentará información sobre cómo Cisco Business Dashboard usa sus datos y qué información se comparte con Cisco. Realice los cambios necesarios y haga clic en **Finalizar**.

Aparecerá la interfaz de usuario de Cisco Business Dashboard.

Crear organizaciones (opcional)

En Cisco Business Dashboard, las organizaciones se emplean para dividir redes, usuarios y dispositivos en grupos que normalmente se administran por separado. Cada red o dispositivo pertenece a una organización y cada usuario puede administrar una o más organizaciones. Una organización puede representar a un cliente o un departamento o una región, pero el uso de las organizaciones posibilita un control más granular sobre

Realización de la configuración inicial de Dashboard

quién puede administrar las distintas partes de la red. Cuando se instala Dashboard, se crea una sola organización de forma predeterminada.

Para crear una nueva organización, siga estos pasos:

1. Acceda a **Administración** > **Organizaciones**.
2. Haga clic en el icono ✚ (más) situado en la parte superior de la tabla.
3. Especifique un nombre para la organización e introduzca los detalles necesarios.
4. Escriba un nombre para un nuevo grupo de dispositivos que deberá convertirse en el predeterminado para los dispositivos recién detectados. El nuevo grupo de dispositivos se creará junto con la organización.
5. Haga clic en **Save** (Guardar)
6. Repita los pasos del 1 al 5 para cada organización que desee crear.

Creación de usuarios y cambio de contraseñas

Dashboard está configurado inicialmente con un valor único predeterminado para la contraseña y el nombre de usuario.

Para agregar usuarios nuevos, haga lo siguiente:

1. Acceda a **Administración** > **Usuarios**.
2. Haga clic en el icono ✚ (más) situado en la parte superior de la tabla **Usuarios**.
3. En la ventana **Agregar usuario** que aparece, introduzca los detalles del usuario que va a crear. Especifique si este usuario es administrador, administrador de organización o de solo lectura. A continuación, se indican los privilegios proporcionados según el tipo de usuario.
   - Los administradores tienen acceso a todas las funcionalidades, incluida la administración del sistema.
   - Los administradores de la organización tienen acceso a todas las funcionalidades en una o más organizaciones, pero no tienen acceso a los menús del sistema.
   - Los operadores tienen acceso a todas las funciones dentro de las organizaciones asignadas, pero no tienen la capacidad de administrar a los usuarios. No tienen acceso a los menús del sistema.
   - Los usuarios de solo lectura no pueden realizar modificaciones en la configuración, solo tienen acceso limitado a los menús de administración y no tienen acceso a los menús del sistema.
4. Haga clic en **Guardar** para crear el nuevo usuario.

También puede configurar las restricciones de complejidad de la contraseña en la página **Usuarios** seleccionando la pestaña **Configuración de usuarios**. Las nuevas contraseñas deberán ajustarse a estas restricciones.

Para cambiar la contraseña, haga lo siguiente:

1. En la parte superior derecha de la interfaz de usuario, haga clic en su nombre de usuario para mostrar el menú desplegable y seleccionar **Mi perfil**. Se muestra una página.
2. Haga clic en el enlace para restablecer la contraseña.
3. En los recuadros proporcionados, especifique la contraseña actual y la nueva.
4. Haga clic en **Guardar**.

Realización de la configuración inicial de Dashboard

Configuración de licencias

Nota Esto no se aplica a la versión Metered de Cisco Business Dashboard para AWS.

Cisco Business Dashboard tiene licencia para usar Cisco Smart Licensing. Cuando se instala por primera vez, Dashboard se establece en el modo de evaluación. El modo de evaluación permite gestionar hasta diez dispositivos de red sin restricción y da un plazo de 90 días para obtener licencias si se van a gestionar más de diez dispositivos. Para aplicar las licencias adquiridas al sistema, debe asociar Dashboard con una Cisco Smart Account que contenga suficientes licencias de dispositivos para su red.

Para asociar Dashboard a su Smart Account, lleve a cabo estos pasos:

1. Inicie sesión en su Smart Account en *https://software.cisco.com*. Seleccione el enlace **Licencias de software Smart** situado en la sección **License** (licencia).
2. Seleccione la página **Inventario** y, si es necesario, cambie la cuenta virtual seleccionada de la predeterminada. Después, haga clic en la pestaña **General**.
3. Cree un nuevo token de registro de la instancia del producto haciendo clic en **Nuevo token…**. Opcionalmente, añada una descripción y cambie el tiempo de **Expirar tras**. Haga clic en **Crear token**.
4. Copie el token que acaba de crear al portapapeles seleccionando **Copiar** del menú desplegable **Acciones** situado a la derecha del token.
5. Acceda a la interfaz de usuario de Cisco Business Dashboard y seleccione **Administración** > **Licencia**.
6. Haga clic en **Registrar** y pegue el token en el campo provisto. Haga clic en **Aceptar**.

Dashboard se registrará en Cisco Smart Licensing y solicitará suficientes licencias para la cantidad de dispositivos de red que se estén gestionando. Si no hay suficientes licencias disponibles, se mostrará un mensaje en la interfaz de usuario y dispondrá de 90 días para obtenerlas antes de que se limiten las funciones del sistema. Para obtener más detalles sobre el proceso de concesión de licencias, consulte la sección *Administración de licencias* en la Guía de administración de Cisco Business Dashboard.

Deshabilitación de Probe integrado en la imagen de máquina virtual

Nota Esto no se aplica a Cisco Business Dashboard para AWS.

La imagen de máquina virtual de Dashboard incluye el software Probe para gestionar dispositivos en la red local de Dashboard. Si no desea gestionar la red local, puede deshabilitar el Probe integrado llevando a cabo estos pasos:

1. Acceda a **Sistema** > **Probe local**.
2. Haga clic en el botón conmutador para deshabilitar el Probe integrado.
3. Haga clic en **Guardar**.

Realización de la configuración inicial de Dashboard

Crear redes (opcional)

Puede definir previamente los registros de red en Dashboard para Probe que asociará más adelante. Por lo general, cada red representa un sitio independiente, pero puede tener varias redes en la misma ubicación. Para crear una nueva red, siga estos pasos:

1. Vaya a **Red**.
2. Haga clic en **Añadir red** en **Vista de mapa** o en el icono + (más) de **Vista de lista**.
3. Especifique un nombre, una organización y un grupo de dispositivos predeterminado para la red.
4. Indique la dirección de la red en los campos correspondientes. Si escribe una dirección parcial, se mostrará una lista con posibles coincidencias en la que podrá seleccionar la ubicación que desee. Si lo desea, también puede hacer clic en la ubicación en el mapa.
5. Haga clic en **Guardar**.
6. Repita los pasos del 1 al 5 para cada red que desee crear.

Realización de la configuración inicial de Dashboard

CAPÍTULO 3

Realización de la configuración inicial de Probe

Este capítulo contiene las siguientes secciones:

Realización de la configuración inicial de Probe

Hay algunas tareas de configuración que se deben llevar a cabo para asegurarse de que la sonda (Probe) se ajuste a sus requisitos.

Localización de la dirección IP de Probe

Para encontrar la dirección IP que la sonda está usando, use uno de los siguientes métodos:

1. La configuración de la dirección IP predeterminada para Probe se realiza mediante DHCP. Asegúrese de que el servidor DHCP esté funcionando y sea accesible. Si no hay ningún servidor DHCP disponible, la dirección IP se establecerá de forma predeterminada en 192.168.1.10.
2. Con la herramienta **Cisco FindIT Network Discovery Utility** se puede detectar una instancia de Probe y acceder a ella. De este modo, puede detectar automáticamente todos los dispositivos Cisco compatibles que se encuentren en el mismo segmento de red local que su equipo. Puede disponer de una vista instantánea de cada dispositivo o abrir la utilidad de configuración del producto para ver y configurar los ajustes. Para obtener más información, consulte http://www.cisco.com/go/findit.
3. Probe se puede utilizar con Bonjour y se anuncia automáticamente a través del protocolo Bonjour. En caso de que tenga un explorador habilitado para Bonjour podrá encontrar Probe en su red local aunque no conozca la dirección IP.
4. Si está utilizando la imagen de máquina virtual, puede recuperar la dirección IP de Probe desde la consola de la máquina virtual. Use las herramientas de administración del hipervisor para conectarse a la consola de la máquina virtual e inicie sesión con el nombre de usuario predeterminado: `cisco`; y la contraseña: `cisco`. Se le pedirá que cambie la contraseña justo después de iniciar sesión. La nueva contraseña debe ser una palabra compleja que no aparezca en el diccionario y que esté compuesta por diversos tipos de caracteres. Aparecerá un banner con la dirección IP actual.

   Si ha instalado Probe en su propia instalación de Ubuntu o Raspbian Linux, puede usar las herramientas del sistema operativo para detectar la dirección IP. Por ejemplo, puede introducir el comando `ifconfig` en una ventana de shell y ver una lista de interfaces y sus direcciones.

5. Para localizar la dirección IP asignada por el servidor DHCP, acceda al router o al servidor DHCP. Consulte las instrucciones del servidor DHCP para obtener más información.

Configuración de Probe de software

Probe de software es una sonda que se ejecuta en una máquina virtual o en un host de Linux cuando Dashboard no se está ejecutándo en la misma máquina virtual o host.

Para configurar Probe de software, haga lo siguiente:

1. Abra un navegador web, por ejemplo **Google Chrome** o **Microsoft Edge**.
2. En el campo **Dirección**, escriba la dirección IP asignada de DHCP y haga clic en **Intro**.
3. Introduzca el nombre de usuario predeterminado: `cisco`; y la contraseña: `cisco`. Haga clic en **Inicio de sesión**.
4. Se le pedirá que cambie la contraseña de la cuenta de Cisco. La nueva contraseña debe tener como mínimo 8 caracteres y debe estar formada por 3 tipos de caracteres diferentes. Haga clic en **Guardar**.
5. Especifique la dirección o el nombre de host de Dashboard al que desea conectarse y haga clic en **Siguiente**.
6. El navegador se redirigirá a la pantalla de inicio de sesión de Dashboard. Inicie sesión usando las credenciales de administrador en Dashboard. A continuación, el navegador se redirigirá de nuevo a Probe.
7. Elija crear una nueva red o seleccionar una red existente de la lista desplegable proporcionada. Si elige crear una red nueva, especifique un nombre y una ubicación para la red en los cuadros proporcionados.

   Puede especificar la dirección de la red en los campos correspondientes. Si escribe una dirección parcial, se mostrará una lista con posibles coincidencias en la que podrá seleccionar la ubicación que desee. Si lo desea, también puede hacer clic en la ubicación en el mapa.
8. Haga clic en **Finalizar**.

Configuración de Probe integrado en un producto de las series 100 a 500 de Cisco

El proceso de asociar una sonda integrada con el panel requiere una configuración explícita en Dashboard y Probe antes de la conexión. Este proceso permite que el dispositivo que alberga la sonda incorporada se preconfigure antes de su instalación, o que se configure automáticamente mediante un mecanismo de implementación sin intervención del usuario como el Network Plug and Play.

Para configurar una sonda integrada, haga lo siguiente:

1. Cree un nuevo registro de red para la sonda integrada siguiendo los pasos descritos en Realización de la configuración inicial de Dashboard, en la página 5. Tome nota del nombre de la organización y del nombre de la red.
2. En la IU de Dashboard, vaya a la página **Mi perfil** haciendo clic en su nombre de usuario en la parte inferior del panel de navegación. Utilice esta página para crear una nueva **Clave de acceso** pulsando el botón **Generar clave de acceso**. Si lo prefiere, también puede utilizar una clave de acceso existente.

Realización de la configuración inicial de Probe

Nota La clave de acceso utilizada para asociar una sonda integrada con el panel no necesita ser una clave de larga duración. Esta clave solo debe ser válida en el momento en que tenga lugar la asociación inicial. Una vez que la sonda y el panel están asociados, la conexión se autentica mediante acceso limitado, credenciales de corta duración que son únicas para la red y se regeneran periódicamente.

3. Con la interfaz de usuario del dispositivo, vaya a la página de configuración de Probe y rellene los campos proporcionados. Como mínimo, deberá proporcionar la configuración de la dirección y el puerto del panel, el nombre de la organización, el nombre de la red y el ID y secreto de la clave de acceso. También puede ser necesario configurar el certificado del panel. Consulte más abajo para obtener más información. Si lo desea, puede realizar otros cambios.
4. Envíe los cambios. La sonda se conectará al panel y se asociará a la red creada en el paso 1.

Verificación de la identidad de Dashboard

Al establecer una conexión con el panel, la sonda comprueba si el certificado presentado por el panel es válido y se puede confiar en él. Para que el certificado sea aceptable y la conexión pueda realizarse, el certificado debe cumplir las siguientes condiciones:

- El certificado debe estar firmado por una entidad de certificación (CA) de confianza, o bien el certificado se debe añadir a la configuración del dispositivo como un certificado de confianza. Consulte la guía de administración del dispositivo para obtener más información sobre cómo agregar un certificado de confianza.
- Si el panel está configurado como una dirección IP, el campo Common Name o el campo Subject-Alt-Name del certificado deben contener esa dirección IP
- Si el panel está configurado como un nombre de host, el campo Common Name o el campo Subject-Alt-Name del certificado deben contener ese nombre de host

Configuración básica del sistema en la imagen de la máquina virtual mediante la interfaz de usuario web (opcional)

Para definir la configuración básica del sistema (por ejemplo, la dirección IP y la hora) en Probe mediante la interfaz de usuario web, siga estos pasos:

1. Acceda a **Administración** > **Configuración de plataforma**.
2. Especifique un nombre de host para Probe. El nombre de host se utiliza para identificar Probe en la red.
3. Si lo desea, puede especificar parámetros de IP estática en los campos proporcionados. De forma predeterminada, Probe determinará automáticamente la configuración de IP usando DHCP.
4. Alternativamente, puede configurar Probe para que use el reloj interno para mantener la hora. También puede especificar los servidores NTP que prefiera. De forma predeterminada, Probe sincronizará su reloj con los servidores NTP públicos.

Nota Si el hipervisor en uso es VirtualBox y las Guest Additions de VirtualBox están instaladas en la máquina virtual, el servicio NTP (timesyncd) no funcionará.

Realización de la configuración inicial de Probe

Configuración básica del sistema en la imagen de máquina virtual mediante la línea de comandos (opcional)

Como alternativa a la definición de la configuración básica del sistema mediante la interfaz web, puede definirla usando la línea de comandos de la siguiente forma:

1. Conéctese a la consola de la máquina virtual.
2. Inicie sesión con la contraseña y el nombre de usuario predeterminados con el valor: `cisco`. Se le pedirá que cambie la contraseña justo después de iniciar sesión. La nueva contraseña debe ser una palabra compleja que no aparezca en el diccionario y que esté compuesta por diversos tipos de caracteres.
3. Especifique el comando `sudo config_vm` para llevar a cabo la configuración inicial. La utilidad `config_vm` mostrará una serie de pasos para cambiar la configuración de la plataforma.
4. En primer lugar, se le pedirá que cambie el nombre de host de Probe. El nombre de host se utiliza para identificar Probe en la red. Aquí puede elegir un nombre significativo u omitir este paso si desea conservar el nombre de host predeterminado.
5. A continuación, se le solicitará que cambie los puertos del servidor web. Si se cambian los valores predeterminados de estos puertos, es posible que también deba cambiarse la configuración del firewall en su red.
6. A continuación, se le pedirá que configure la interfaz de red. Las opciones aquí son Estático y DHCP (valor predeterminado). Si elige Estático, se le solicitará información sobre la dirección IP, la gateway predeterminada y el servidor DNS. La interfaz de red se restablecerá si hace cambios aquí.
7. Después se le pedirá que defina la configuración de hora para Probe. Puede optar por configurar uno o varios servidores NTP para la sincronización de la hora (recomendado). Se le pedirá que elija una zona horaria.

Nota Si el hipervisor en uso es VirtualBox y las Guest Additions de VirtualBox están instaladas en la máquina virtual, el servicio NTP (timesyncd) no funcionará.

8. Por último, se le preguntará si desea cambiar la contraseña del cargador de arranque. El nombre de usuario y la contraseña del cargador de arranque se pueden utilizar en la consola al iniciar el sistema para cambiar el proceso de arranque del sistema o recuperar las contraseñas perdidas del sistema operativo. Las credenciales predeterminadas del cargador de arranque son nombre de usuario: **root** y contraseña: **cisco**.

Configuración básica del sistema cuando Probe está integrado en un producto de la serie Cisco Business

Si está utilizando Probe incorporado en un producto de la serie Cisco Business, entonces se accede a la interfaz de usuario de Probe a través de la interfaz de administración de dispositivos. Consulte la guía de administración de dispositivos para obtener más información sobre cómo asociar Dashboard con Manager y realizar cambios en la configuración del sistema.

Configuración básica del sistema cuando Probe se aloja conjuntamente con Cisco Business Dashboard

Cuando Probe se aloja conjuntamente con Cisco Business Dashboard, no tiene ninguna interfaz de usuario. Probe se administra por completo a través de la interfaz de usuario de Dashboard.

CAPÍTULO 4

Realización de la configuración inicial de los dispositivos administrados directos

Este capítulo contiene las siguientes secciones:

Realización de la configuración inicial de los dispositivos administrados directos

Los dispositivos administrados directos son dispositivos de red que pueden asociarse directamente con Dashboard y administrarse sin que una sonda esté presente en la red. Solo determinados dispositivos son compatibles con la gestión directa. Consulte Cisco Business Dashboard: lista de dispositivos admitidos para obtener una lista de versiones de software y dispositivos que admiten la administración directa. Los dispositivos administrados directos detectarán otros dispositivos en la red más amplia y los agregarán al inventario de Dashboard. Sin embargo, este proceso de detección no es tan completo como el realizado por una sonda y, como resultado, la topología de red resultante puede ser menos precisa.

El proceso de asociar un dispositivo administrado directo con el panel requiere una configuración explícita en Dashboard y el dispositivo antes de la conexión. Este proceso permite que el dispositivo se configure previamente antes de su instalación, o que se configure automáticamente mediante un mecanismo de implementación sin intervención del usuario como el Network Plug and Play.

Para configurar un dispositivo administrado directo, haga lo siguiente:

1. Cree un nuevo registro de red para la red en la que se va a instalar el dispositivo siguiendo los pasos descritos en Realización de la configuración inicial de Dashboard, en la página 5. Tome nota del nombre de la organización y del nombre de la red.
2. En la IU de **Dashboard**, vaya a la página **Mi perfil** haciendo clic en su nombre de usuario en la parte inferior del panel de navegación. Utilice esta página para crear una nueva **Clave de acceso** pulsando el botón **Generar clave de acceso**. Si lo prefiere, también puede utilizar una clave de acceso existente.

Realización de la configuración inicial de los dispositivos administrados directos

Nota La clave de acceso utilizada para asociar un dispositivo administrado directo con el panel no necesita ser una clave de larga duración. Esta clave solo debe ser válida en el momento en que tenga lugar la asociación inicial. Una vez que el dispositivo y el panel están asociados, la conexión se autentica mediante acceso limitado, credenciales de corta duración que son únicas para el dispositivo y se regeneran periódicamente.

3. Con la interfaz de usuario del dispositivo, vaya a la página de configuración de Cisco Business Dashboard y rellene los campos proporcionados. Como mínimo, deberá proporcionar la configuración de la dirección y el puerto del panel, el nombre de la organización, el nombre de la red y el ID y secreto de la clave de acceso. También puede ser necesario configurar el certificado del panel. Consulte más abajo para obtener más información. Consulte la guía de administración del dispositivo en cuestión para obtener más información.
4. Envíe los cambios. El dispositivo se conectará al panel y se asociará a la red creada en el paso 1.

Al establecer una conexión con el panel, el dispositivo comprueba si el certificado presentado por el panel es válido y se puede confiar en él. Para que el certificado sea aceptable y la conexión pueda realizarse, el certificado debe cumplir las siguientes condiciones:

- El certificado debe estar firmado por una entidad de certificación (CA) de confianza, o bien el certificado se debe añadir a la configuración del dispositivo como un certificado de confianza. Consulte la guía de administración del dispositivo para obtener más información sobre cómo agregar un certificado de confianza.
- Si el panel está configurado como una dirección IP, el campo **Common Name** o el campo **Subject-Alt-Name** del certificado deben contener esa dirección IP
- Si el panel está configurado como un nombre de host, el campo **Common Name** o el campo **Subject-Alt-Name** del certificado deben contener ese nombre de host

CAPÍTULO 5

Configuración de la red

Este capítulo contiene las siguientes secciones:

Configuración de la red para Cisco Business Dashboard

Configuración de credenciales de dispositivo

Para que Cisco Business Dashboard pueda administrar los dispositivos de red, debe especificar las credenciales adecuadas que permitan acceder a cada dispositivo.

Cuando Probe detecta un dispositivo, intenta acceder a este inicialmente usando las credenciales predeterminadas con el nombre de usuario: `cisco`; la contraseña: `cisco`; y la comunidad SNMP definida en el valor: `public`. Sin embargo, si el dispositivo no está usando las credenciales predeterminadas, habrá que especificar las credenciales correctas, tal y como se indica en los pasos siguientes:

1. Acceda a **Administración** > **Credenciales del dispositivo**. En la primera tabla de esta página, se enumeran todos los dispositivos que se han detectado y requieren credenciales mientras que, en la segunda tabla, se enumeran todos los dispositivos descubiertos para los que se conocen las credenciales de trabajo.
2. Especifique una combinación de nombre de usuario y contraseña o credenciales de SNMP en los campos correspondientes de la parte superior de la página. Si se requieren más conjuntos de credenciales, haga clic en el icono **+** (más). Esta función permite especificar hasta tres conjuntos más de credenciales de cada tipo.
3. Haga clic en **Apply** (Aplicar). Probe probará cada credencial con cada dispositivo que requiera una credencial. Las credenciales operativas se guardan para cada dispositivo.

   Probe detectará cada red y generará un mapa topológico e inventario para la red después de que se proporcione con las credenciales de trabajo.

Más información sobre su red

ofrece una vista general sobre su red en forma de mapa o de lista de redes. Para ver la vista general de todas las redes, lleve a cabo estos pasos:

1. Asegúrese de haber asociado Probes con las Cisco Business Dashboard que se describen en el capítulo anterior.
2. Haga clic en **Red** en la navegación de Dashboard. Haga clic en el botón para mostrar la **Vista de mapa** o la **Vista de lista**.
3. En la **Vista de mapa**, puede hacer clic en el mapa y arrastrarlo para recolocarlo. Los botones de los signos más y menos sirven para acercar o alejar el zoom. Cada red donde esté instalado Cisco Business Dashboard Probe aparecerá como un icono en el mapa. Cada icono tiene un número que muestra el número de notificaciones pendientes que existen para esa red. El color del icono indica el nivel de gravedad más alto pendiente. Haga clic en un icono para ver más información sobre ese sitio. Si hay varios iconos demasiado cerca para distinguirlos fácilmente, se reemplazarán con un marcador de clúster que muestra el número de iconos de red en dicho clúster. Haga clic en el marcador de clúster para acercar los sitios de ese clúster.

   En la **Vista de lista**, puede hacer clic en el icono de la esquina superior izquierda de la tabla para seleccionar las columnas que desea que se muestren y en los encabezados de la columna para organizar la tabla.
4. Utilice el cuadro de búsqueda para encontrar una red determinada o la red que contiene un dispositivo concreto. Puede introducir el nombre, la dirección o la dirección IP de una red en el cuadro de búsqueda, o el nombre, la dirección IP, la dirección MAC o el número de serie de un dispositivo.
5. Al hacer clic en una red, se muestra el panel **Información básica**, que ofrece más información sobre la red. Esta información incluye la dirección, el nombre de la red y una lista de notificaciones pendientes para la red.
6. Puede hacer clic en **Ver** en el panel **información básica** para ver una información detallada sobre esa red, incluidos el diagrama de topología de la red y los planos de la planta. Al hacer clic en **Más** se abre la vista **Detalle de red**, que le permite modificar la configuración de esta red y ver todos los dispositivos detectados en esta red.

También puede utilizar el **inventario** para ver información detallada sobre todos los dispositivos de la red. La página **Inventario** proporciona una lista de todos los dispositivos detectados en una vista de tabla. Puede filtrar la lista para restringir los dispositivos que se muestran, y hacer clic en dispositivos individuales para ver más información sobre ese dispositivo.

Personalización del mapa Topología (opcional)

Una vez que se proporcionan credenciales de trabajo, **Probe** detectará cada red y generará un mapa de **topología**. El mapa se puede modificar según sea necesario.

1. Vaya a **Red** y seleccione la red de interés. Haga clic en **Vista** para mostrar la topología.
2. Puede arrastrar los iconos de dispositivos individuales para mejorar el diseño. Todos los cambios que realice en el diseño son permanentes. Cisco Business Dashboard no realizará más cambios en la ubicación de los iconos. Si desea volver a habilitar la colocación automática de los iconos, haga clic en **Rediseño topología**.
3. Haga clic en **Superposiciones** para abrir el panel **Superpos. y filtros** y use las casillas para limitar los tipos de dispositivos que se mostrarán en el diagrama de topología.

Carga de planos de planta (opcional)

Puede cargar planos de planta de cada red y situar los dispositivos de red en ellos para documentar la ubicación de los equipos. Los siguientes pasos le guiarán durante este proceso:

1. Al ver el diagrama de topología de una red, haga clic en **Plano de la planta**.
2. Especifique el nombre del edificio y la planta. A continuación, arrastre un archivo de imagen hasta la zona de carga. También puede hacer clic dentro del widget para seleccionar una imagen de su PC. Los formatos de imagen admitidos son `.png, .gif y .jpg`.
3. Haga clic en **Guardar** para guardar los cambios.
4. Para situar un dispositivo en el plano de la planta, haga clic en **Añadir dispositivos** y escriba el nombre del dispositivo o la dirección IP en el cuadro de búsqueda situado en la parte inferior de la pantalla. Se mostrarán los dispositivos que coincidan con el texto introducido. Los dispositivos que ya se hayan colocado en el plano de planta aparecerán atenuados.
5. Haga clic en un dispositivo y arrástrelo para agregarlo al plano de planta en la ubicación correspondiente.

Personalización del panel de supervisión

Puede personalizar el panel supervisión para que se adapte a sus necesidades. Debe seguir estos pasos:

1. Seleccione **Dashboard** en el área de navegación a la izquierda de la pantalla. Aparecerá el panel de control predeterminado.
2. Para reubicar widgets individuales dentro del panel, haga clic en el icono del engranaje ubicado en la parte superior derecha del panel y seleccione la opción **Modo de edición**. Haga clic y mantenga pulsado para arrastrar cada widget a la ubicación deseada. Para cambiar el tamaño de un widget, haga clic y mantenga pulsado el borde o la esquina del widget para cambiarlo de tamaño.
3. Para agregar un nuevo widget al panel, haga clic en el icono del engranaje situado en la parte superior derecha del panel y seleccione la opción para añadir un widget. Seleccione el widget que desee de la lista. Para eliminar un widget del panel, haga clic en el icono ✖ (**Eliminar widget**), situado en la esquina superior derecha del widget en el modo de edición.
4. Una vez que el panel se haya colocado correctamente, haga clic en el icono del engranaje situado en la parte superior derecha del panel y seleccione **Modo de visualización** para bloquear los cambios.
5. Para modificar el comportamiento de un widget, haga clic en el icono **Editar configuración del widget**, situado en la parte superior derecha del widget. Use las listas desplegables para seleccionar la red, la interfaz o el dispositivo que el widget debe supervisar en concreto.

Definición de la configuración del correo electrónico (opcional)

Cisco Business Dashboard puede informarle por correo electrónico cuando se produzcan determinados eventos en la red. Para controlar qué eventos generarán un correo electrónico, consulte Personalización de la pantalla de notificaciones, en la página 20. Para definir la configuración del correo electrónico, haga lo siguiente:

1. Acceda a **Sistema** > **Configuración**.
2. En esta página, puede especificar el puerto y el servidor de correo electrónico que se deben usar para los mensajes salientes, el cifrado y la configuración de autenticación, así como las direcciones de correo electrónico que se deben usar.
3. Una vez que haya finalizado la configuración, haga clic en **Guardar**.
4. Haga clic en **Prueba de conectividad** para probar los cambios que ha realizado.

Personalización de la pantalla de notificaciones

Para personalizar el comportamiento de las notificaciones, siga estos pasos:

1. Acceda a **Administración** > **Organizaciones** y seleccione la organización en la que desea personalizar el comportamiento de las notificaciones.
2. Haga clic en **Notificación**.
3. Desmarque la casilla **Heredar los valores predeterminados de las notificaciones**. Use las casillas para determinar qué notificaciones generarán una alerta emergente en la interfaz de usuario y cuáles generarán una notificación por correo electrónico. Si usa notificaciones por correo electrónico, debe asegurarse de que la configuración del correo electrónico sea correcta. Consulte Definición de la configuración del correo electrónico (opcional), en la página 19 para obtener más información.
4. Haga clic en **Guardar**.

También puede personalizar **Valores predeterminados de notificación** al acceder a **Administración** > **Valores predeterminados de notificación**.

Configuración de Plug and Play de red

Cisco Business Dashboard proporciona un servicio Plug and Play de red de Cisco que permite gestionar de forma centralizada archivos de configuración y firmware para dispositivos Cisco seleccionados. Para obtener más información sobre el servidor Plug and Play de red, consulte la Guía de la solución PnP.

Para configurar Plug and Play de red, lleve a cabo las siguientes tareas:

Actualización de firmware

1. Acceda a **Plug and Play de red** > **Imágenes**.
2. Haga clic en el icono ✚ (más).
3. Seleccione una organización y, a continuación, arrastre un archivo de firmware desde su PC y suéltelo en la zona de destino de la ventana **Cargar archivo**. También puede hacer clic en la zona de destino y seleccionar una imagen de firmware para cargarla.
4. Haga clic en **Cargar**.

Puede designar una imagen como imagen predeterminada para uno o varios tipos de dispositivo. Para designar una imagen como imagen predeterminada, haga lo siguiente:

1. Marque la casilla de la imagen en la tabla **Imágenes** y haga clic en **editar**.
2. Introduzca una lista de ID de producto separados por comas en el campo **Imagen predeterminada para los id. de productos**. Los ID de producto pueden contener caracteres comodín “?”, que representa un único carácter, y “*”, que representa una cadena de caracteres.
3. Haga clic en **guardar**.

Carga de configuraciones (opcional)

1. Acceda a **Plug and Play de red** > **Configuraciones**.

2. Haga clic en el icono ✚ (más).
3. Seleccione una organización y, a continuación, arrastre un archivo de configuración desde su PC y suéltelo en la zona de destino de la ventana **Cargar archivo**. También puede hacer clic en la zona de destino y seleccionar un archivo de configuración para cargarlo.
4. Haga clic en **Cargar**.

En lugar de cargar configuraciones, puede utilizar las plantillas de configuración incluidas que se suministran con la aplicación Dashboard. Si lo desea, puede hacer clic en el nombre de un archivo de configuración para ver el contenido.

Configuración de la detección

Para que los dispositivos de red usen **Plug and Play de red**, primero es necesario que detecten el servidor de **Plug and Play de red**. Existen tres mecanismos que pueden usarse para proporcionar esta información a los dispositivos:

1. **DHCP**: El dispositivo de red puede detectar la dirección del servidor Plug and Play de red usando la opción 43 DHCP. Para obtener más información sobre el formato de las opciones, consulte la sección *Acerca de Plug and Play de red* en la Guía de administración de Cisco Business Dashboard.
2. **DNS**: Si el dispositivo de red no detecta la dirección del servidor mediante DHCP, tratará de buscar un nombre de host conocido, pnpserver, en el dominio local. Por ejemplo: *pnpserver.ejemplo.com*. Puede configurar su infraestructura de DNS para garantizar que este nombre detecte la dirección de Cisco Business Dashboard.
3. **Plug and Play Connect**: Cisco proporciona un servicio de redireccionamiento, **Plug and Play Connect**, que el dispositivo consultará si no es capaz de encontrar la dirección del servidor de ninguna otra forma. Para establecer el servicio de redireccionamiento en su red, consulte Plug and Play Connect.

Registro de dispositivos

Para registrar dispositivos como preparación para la instalación, haga lo siguiente:

1. Acceda a **Plug and Play de red** > **Dispositivos habilitados**.
2. Haga clic en el icono ✚ (más).
3. Introduzca el nombre, la ID de producto (PID) y el número de serie del dispositivo que se registrará y seleccione una organización, una red, un grupo de dispositivos y un tipo de dispositivo de las listas desplegables.
4. Puede seleccionar una imagen de firmware o un archivo de configuración (o ambos) para su uso con este dispositivo. Si elige Imagen predeterminada como imagen, el dispositivo usará la imagen designada como predeterminada para ese tipo de dispositivo cuando este se conecte al servidor.
5. Haga clic en **Guardar**.

Autorreclamación de dispositivos

Un dispositivo que se conecta al servidor y que no está presente en el inventario se considera un dispositivo no reclamado. El servidor puede reclamar y aprovisionar automáticamente los dispositivos no reclamados creando una regla de autorreclamación para ese ID de producto. Para crear una regla de autorreclamación, haga lo siguiente:

1. Acceda a **Plug and Play de red** > **Dispositivos autorreclamados**.
2. Haga clic en el icono ✚ (más).
3. Introduzca la ID de producto (PID) para reclamar y seleccionar automáticamente una organización, una red, un grupo de dispositivos y un tipo de dispositivo de las listas desplegables.
4. Puede seleccionar una imagen de firmware o un archivo de configuración (o ambos) para su uso con este ID de producto. Si elige Imagen predeterminada como imagen, los dispositivos autorreclamados usarán la imagen designada como predeterminada para ese tipo de dispositivo cuando este se conecte al servidor.
5. Haga clic en **Guardar**.

Configuración de la red

Si está instalando una red nueva, puede aprovechar esta oportunidad para llevar a cabo la configuración inicial de la red. Incluso en una red existente, puede realizar cambios de configuración en este momento.

Actualización del firmware de los dispositivos (opcional)

Dashboard le informará cuando haya actualizaciones de firmware disponibles para los dispositivos. Aparecerá un icono **Actualizar firmware** junto al dispositivo en varias áreas de la interfaz de usuario.

Para actualizar el firmware de un único dispositivo, haga lo siguiente:

1. Haga clic en el dispositivo en el **Mapa de topología** para abrir el panel **Información básica**.
2. Abra el panel **Acción** y haga clic en el botón **Actualizar firmware a la última versión**. Dashboard descargará el firmware correspondiente desde Cisco y aplicará la actualización al dispositivo. El dispositivo se reiniciará durante el proceso.

   Otra forma de proceder consiste en actualizar el firmware desde el PC haciendo clic en la opción **Actualizar desde local**, especificando la imagen de firmware que se debe cargar.
3. Para ver el progreso de la actualización, haga clic en el icono **Estado de la tarea** en la parte superior derecha de la interfaz de usuario.

También puede actualizar dispositivos individuales desde la vista **Inventario**. Para obtener información, consulte la sección *Visualización del inventario del dispositivos* en la guía de administración de Cisco Business Dashboard.

Actualización del firmware de una red

Si desea actualizar toda una red al firmware más reciente disponible, haga lo siguiente:

1. Abra el **mapa de topología** para la red que desea actualizar.
2. Haga clic en **Acciones de red**, en la parte superior de la página, y seleccione la opción **Actualizar firmware**. Dashboard descargará los archivos de firmware correspondientes de Cisco para cada dispositivo para el que haya disponible una actualización y los instalará en cada dispositivo de uno en uno. Los dispositivos se reiniciarán durante el proceso.
3. Para ver el progreso de la actualización, haga clic en el icono **Estado de la tarea** en la parte superior derecha de la interfaz de usuario.

Configuración de grupos de dispositivos

Dashboard usa el concepto de "grupos de dispositivos" para aplicar configuraciones a varios dispositivos a la vez y asegurarse de que la configuración sea la misma en toda la red. Para asignar dispositivos a un grupo de dispositivos, haga lo siguiente:

1. Acceda a **Administración** > **Grupos de dispositivos**.
2. Haga clic en el icono ✚ (más) para agregar un grupo nuevo.
3. Especifique una organización, un nombre y una descripción para el grupo de dispositivos. Haga clic en **Guardar**.
4. Para agregar dispositivos al grupo de dispositivos, haga clic en el icono ✚ (más) en la tabla **Dispositivos**. Use el cuadro de búsqueda para encontrar dispositivos que agregar al grupo. Seleccione uno o varios dispositivos para incorporarlos al grupo. Cada dispositivo puede ser miembro de un único grupo. Si un dispositivo seleccionado pertenecía antes a un grupo diferente, se eliminará de dicho grupo. Si desea eliminar un dispositivo del grupo, haga clic en el icono **Cancelar** situado junto al dispositivo. Este pasará a formar parte del grupo de dispositivos **Predeterminado**. Los grupos de dispositivos pueden estar formados por distintos tipos de dispositivos.

Creación de perfiles de configuración

Dashboard permite aplicar fácilmente la configuración común a varios dispositivos de red. Puede usar el **Asistente de configuración de red** para crear perfiles de configuración destinados a cada sección de la configuración. También puede crear los perfiles individualmente. Para usar el **Asistente de configuración de red**, haga lo siguiente:

1. Acceda a **Configuración de red** > **Asistente**.
2. Especifique un nombre de perfil para los perfiles de configuración que se van a crear, elija una organización y seleccione uno o varios grupos de dispositivos para aplicar la configuración.
3. Haga clic en **Siguiente**.
4. Especifique la configuración de la hora para este grupo. Un perfil de **Administración del tiempo** contiene configuraciones para la zona horaria, el horario de verano y el protocolo NTP (protocolo de tiempo de red). Si no desea crear un perfil de **Administración del tiempo** para este grupo, haga clic en **Omitir**. De lo contrario, haga clic en **Siguiente**.
5. Especifique la **Configuración de DNS** para este grupo. Un perfil de **Analizadores de DNS** incluye configuraciones para el nombre de dominio y los servidores DNS que se deben usar. Si no desea crear un perfil de Analizadores de DNS para este grupo, haga clic en **Omitir**. De lo contrario, haga clic en **Siguiente**.
6. Especifique la configuración de autenticación de usuario para este grupo. Un **Perfil de autenticación** contiene configuraciones para la base de datos local de usuarios de los dispositivos. Si no desea crear un **Perfil de autenticación** para este grupo, haga clic en **Omitir**. De lo contrario, haga clic en **Siguiente**.
7. Especifique las LAN virtuales que se crearán para este grupo. Un perfil de VLAN contiene los detalles de una o más VLAN. Si no desea crear un perfil de VLAN, haga clic en **Omitir**. Para agregar varias VLAN, haga clic en **Agregar otra** después de completar cada VLAN. Haga clic en **Siguiente**.
8. Especifique las LAN inalámbricas que se crearán para este grupo. Un perfil de LAN inalámbrica contiene los detalles de uno o más SSID. Si no desea crear un perfil de LAN inalámbrica, haga clic en **Omitir**.

Configuración de la red

Para agregar varios SSID, haga clic en **Agregar otro** después de completar cada SSID. Haga clic en **Siguiente**.

9. Revise la configuración que haya especificado. Si necesita realizar cambios, use el botón **Editar** o **Atrás** para volver a la pantalla especificada. Cuando haya terminado, haga clic en **Finalizar** para crear los perfiles y aplicarlos a los dispositivos en los grupos de dispositivos seleccionados.
10. Para ver el progreso de la configuración, haga clic en el icono **Estado de la tarea** en la parte superior derecha de la interfaz de usuario.

Realizar una copia de seguridad de las configuraciones de los dispositivos

Dashboard permite realizar copias de seguridad de las configuraciones de los dispositivos de red. Para realizar la copia de seguridad de un único dispositivo, haga lo siguiente:

1. Haga clic en el dispositivo en el **Mapa de topología** para abrir el panel **Información básica**.
2. Abra el panel **Acción** y haga clic en el botón **Configuración de copia de seguridad**. Si lo desea, puede agregar una nota para describir la copia de seguridad en la ventana que aparece. **Dashboard** copiará la configuración del dispositivo.
3. Para ver el progreso de la copia de seguridad, haga clic en el icono **Estado de la tarea** en la parte superior derecha de la interfaz de usuario.

También puede realizar copias de seguridad de dispositivos individuales haciendo clic en **Configuración de copia de seguridad** en la vista **Inventario**.

Si desea hacer una copia de seguridad de la configuración de toda la red, haga lo siguiente:

1. Abra el **mapa de topología** para la red de la que desea hacer una copia de seguridad.
2. Haga clic en el botón **Acciones**, en la parte superior de la página, y seleccione la opción **Configuraciones de copia de seguridad**. Si lo desea, agregue una nota para describir la copia de seguridad en la ventana que aparece. Dashboard copiará la configuración de cada dispositivo.
3. Para ver el progreso de la copia de seguridad, haga clic en el icono **Estado de la tarea** en la parte superior derecha de la interfaz de usuario.

CAPÍTULO 6

Preguntas frecuentes

En este capítulo, se responden las preguntas frecuentes sobre las funciones de Cisco Business Dashboard y los problemas que se pueden producir. Los temas se organizan en las siguientes categorías:

Preguntas frecuentes generales

Q. ¿Qué idiomas son compatibles con Cisco Business Dashboard?

A. Cisco Business Dashboard se ha traducido a los siguientes idiomas:

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

Preguntas frecuentes sobre detección

Q. ¿Qué protocolos usa Cisco Business Dashboard para administrar mis dispositivos?

A. Cisco Business Dashboard usa diversos protocolos para detectar y administrar las redes. Los protocolos exactos que se usarán para un dispositivo concreto varían según los tipos de dispositivos.

Entre los protocolos utilizados, podemos destacar los siguientes:

- Detección de servicios DNS y DNS multidifusión (también conocidos como *Bonjour*, consulte los *RFC 6762 y 6763*)

- Protocolo de detección de Cisco (CDP)
- Protocolo de detección de capa de enlace (consulte la *especificación IEEE 802.1AB*)
- Protocolo simple de administración de red (SNMP)
- RESTCONF (consulte *https://datatracker.ietf.org/doc/draft-ietf-netconf-restconf/)*
- API de servicios web propias

Q. ¿Cómo detecta Cisco Business Dashboard las redes?

A. Cisco Business Dashboard Probe elabora una lista inicial de dispositivos de la red a partir de los anuncios de CDP, LLDP y mDNS. A continuación, Probe se conecta a cada dispositivo usando un protocolo compatible y recopila información adicional, como las tablas de adyacencia CDP y LLDP, las tablas de direcciones MAC y las listas de dispositivos asociados. Esta información se usa para identificar dispositivos adicionales de la red. El proceso se repite hasta que se hayan detectado todos los dispositivos.

Q. ¿Realiza Cisco Business Dashboard exploraciones de red?

A. Cisco Business Dashboard no explora activamente la red. Probe usará el protocolo ARP para explorar la subred IP a la que está directamente asociado pero no tratará de explorar otros rangos de direcciones. Probe también probará todo dispositivo detectado en busca de un servidor web y un servidor SNMP en los puertos estándar.

Preguntas frecuentes sobre configuración

Q. ¿Qué sucede cuando se detecta un nuevo dispositivo? ¿Cambiará su configuración?

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

Q. ¿Qué sucede cuando muevo un dispositivo de un grupo de dispositivos a otro?

A. Se eliminará cualquier configuración de VLAN o WLAN asociada con perfiles que se apliquen actualmente al grupo de dispositivos original y que no se apliquen también al nuevo grupo de dispositivos. Por otra parte, se agregarán al dispositivo las configuraciones VLAN o WLAN asociadas con perfiles que se apliquen al nuevo grupo y que no se apliquen al grupo original. Los ajustes de configuración de sistema se sobrescribirán con los perfiles aplicados al nuevo grupo. Si no se han definido perfiles de configuración de sistema para el nuevo grupo, la configuración de sistema del dispositivo no cambiará.

Preguntas frecuentes sobre consideraciones de seguridad

Q. ¿Qué rangos de puertos y protocolos requiere Cisco Business Dashboard?

A. En la siguiente tabla, se muestran los protocolos y los puertos que usa Cisco Business Dashboard:

Tabla 1: Cisco Business Dashboard - Protocolos y puertos

Puerto	Dirección	Protocolo	Uso
TCP 22	Tácticas	SSH	Acceso de línea de comandos a Dashboard. SSH está deshabilitado de forma predeterminada en la imagen de máquina virtual de Cisco.
TCP 80	Tácticas	HTTP	Acceso web a Dashboard. Redirecciona a un servidor web seguro (puerto 443).
TCP 443	Tácticas	HTTPS TCP multiplexado	Acceso web seguro a Dashboard. Comunicación entre Probe y Dashboard.
TCP 50000-51000	Tácticas	HTTPS	Acceso remoto a los dispositivos.
UDP 53	Saliente	DNS	Resolución de nombres de dominio.
UDP 123	Saliente	NTP	Sincronización de tiempo.
TCP 443	Saliente	HTTPS	Acceso a los servicios web de Cisco para obtener información como actualizaciones de software, estado de soporte y avisos de fin de vida útil. Acceso a los servicios de actualización del sistema operativo y de las aplicaciones.
UDP 5353	Saliente	mDNS	Anuncios de servicio DNS multidifusión a la red local donde se anuncia Dashboard.

Q. ¿Qué rangos de puertos y protocolos requiere Cisco Business Dashboard Probe?

A. En la siguiente tabla, se muestran los protocolos y los puertos que usa Cisco Business Dashboard Probe :

Tabla 2: Cisco Business Dashboard - Protocolos y puertos

Puerto	Dirección	Protocolo	Uso
TCP 22	Tácticas	SSH	Acceso de línea de comandos a Probe. SSH está deshabilitado de forma predeterminada en la imagen de máquina virtual de Cisco.
TCP 80	Tácticas	HTTP	Acceso web a Probe. Redirecciona a un servidor web seguro (puerto 443).
TCP 443	Tácticas	HTTPS	Acceso web seguro a Probe.

Puerto	Dirección	Protocolo	Uso
UDP 5353	Tácticas	mDNS	Anuncios de servicio DNS multidifusión desde la red local. Usado para la detección de dispositivos
UDP 53	Saliente	DNS	Resolución de nombres de dominio.
UDP 123	Saliente	NTP	Sincronización de tiempo
TCP 80	Saliente	HTTP	Administración de dispositivos sin la seguridad de servicios web habilitada.
UDP 161	Saliente	SNMP	Administración de dispositivos de red.
TCP 443	Saliente	HTTPS TCP multiplexado	Administración de dispositivos con la seguridad de servicios web habilitada Acceso a los servicios web de Cisco para obtener información como actualizaciones de software, estado de soporte y avisos de fin de vida útil. Acceso a los servicios de actualización del sistema operativo y de las aplicaciones. Comunicación entre Probe y Dashboard.
UDP 5353	Saliente	mDNS	Anuncios de servicio DNS multidifusión a la red local donde se anuncia Probe.

Q. ¿Cuánta seguridad hay en la comunicación entre Cisco Business Dashboard y Probe?

A. Todas las comunicaciones entre Dashboard y Probe se cifran con una sesión TLS 1.2 autenticada con certificados de servidor y cliente. La sesión se inicia desde Probe hasta Dashboard. Cuando se establece por primera vez la asociación entre Dashboard y Probe, el usuario debe iniciar sesión en Dashboard a través de Probe.

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

A. No. Cuando Cisco Business Dashboard detecta un dispositivo compatible, intenta acceder al dispositivo usando las credenciales predeterminadas de fábrica de dicho dispositivo con el nombre de usuario y la

contraseña "cisco" o la comunidad SNMP "public". Si la configuración del dispositivo no es la predeterminada, el usuario deberá especificar las credenciales correctas en Cisco Business Dashboard.

Q. ¿Están seguras las credenciales que se almacenan en Cisco Business Dashboard?

A. Las credenciales para acceder a Cisco Business Dashboard se codifican mediante hash de forma irreversible mediante el algoritmo SHA512. Las credenciales para dispositivos y otros servicios, como **Cisco Active Advisor**, se cifran de forma reversible mediante el algoritmo AES-128.

Q. ¿Cómo recupero una contraseña perdida para la interfaz de usuario web?

A. Si ha perdido la contraseña para todas las cuentas de administración de la interfaz de usuario web, la puede recuperar iniciando sesión en la consola de Probe y ejecutando la herramienta **cbdprobe recoverpassword** o iniciando sesión en la consola de Dashboard y ejecutando la herramienta **cisco-business-dashboard recoverpassword**. Esta herramienta restablece la contraseña de la cuenta de Cisco al valor predeterminado, que es cisco. En caso de que la cuenta de Cisco se haya eliminado, se volverá a crear la cuenta con la contraseña predeterminada. A continuación, puede ver un ejemplo de los comandos que se deben proporcionar con objeto de recuperar la contraseña usando esta herramienta.

```
cisco@cisco-business-dashboard:~$ cisco-business-dashboard recoverpassword ¿Está seguro?
 (s/n) s Se recuperó la cuenta Cisco con la contraseña predeterminada recoverpassword
de Cisco Business Dashboard con éxito cisco@cisco-buisness-dashboard:~$
```

Nota Al emplear Cisco Business Dashboard para AWS, la contraseña se definirá como el ID de instancia de AWS.

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

A. Las credenciales predeterminadas de la máquina virtual son nombre de usuario: **root** y contraseña: **cisco**. Estos se pueden cambiar ejecutando la herramienta config_vm y respondiendo sí cuando se le pregunte si quiere cambiar la contraseña del cargador de arranque.

Preguntas frecuentes sobre el acceso remoto

Q. Si me conecto a la interfaz de administración de un dispositivo desde Cisco Business Dashboard, ¿la sesión es segura?

A. Cisco Business Dashboard tuneliza la sesión de acceso remoto entre el dispositivo y el usuario. El protocolo que se use entre Probe y el dispositivo dependerá de la configuración del dispositivo de extremo; en cualquier caso, Cisco Business Dashboard siempre establecerá la sesión usando un protocolo seguro si hay uno habilitado (por ejemplo, HTTPS tendrá preferencia sobre HTTP). Si el usuario está conectado al dispositivo a través de Dashboard, la sesión pasará por un túnel cifrado en su recorrido entre Dashboard y Probe, con independencia de los protocolos habilitados en el dispositivo. La conexión entre el navegador web del usuario y Dashboard siempre será del tipo HTTPS.

Q. ¿Por qué se cierra inmediatamente mi sesión de acceso remoto en un dispositivo cuando abro una sesión de acceso remoto en otro dispositivo?

A. Cuando se accede a un dispositivo a través de Cisco Business Dashboard, el navegador considera cada conexión como si fuera con el mismo servidor web (Dashboard) y, por lo tanto, presentará las cookies de cada dispositivo a los demás dispositivos. Si varios dispositivos usan el mismo nombre de cookie, es posible que la cookie de un dispositivo se sobrescriba con la de otro. Esto suele pasar con las cookies de sesión y el resultado es que la cookie solo es válida para el dispositivo visitado más recientemente. Los

demás dispositivos que usan el mismo nombre de cookie considerarán que la cookie no es válida y cerrarán la sesión.

Q. ¿Por qué falla la sesión de acceso remoto con un error como el siguiente? **Error de acceso: La entidad solicitada es demasiado grande El campo del encabezado HTTP es superior al tamaño admitido**.

A. Tras efectuar numerosas sesiones de acceso remoto con distintos dispositivos, el navegador tendrá un gran número de cookies almacenadas para el dominio de Dashboard. Para solucionar este problema, use los controles del navegador para borrar las cookies del dominio y, después, vuelva a cargar la página.

Preguntas frecuentes sobre la actualización del software

Q. ¿Cómo mantengo actualizado el sistema operativo de Dashboard?

A. Dashboard usa como sistema operativo la distribución Linux Ubuntu. Los paquetes y el núcleo se pueden actualizar usando los procesos estándares de Ubuntu. Por ejemplo, para realizar una actualización manual, inicie sesión en la consola con el usuario cisco e introduzca los comandos `sudo apt-get update` y `sudo apt-get upgrade`. El sistema no debe actualizarse a una nueva versión de Ubuntu y se recomienda no instalar otros paquetes aparte de los que suministra Cisco en la imagen de la máquina virtual o los instalados como parte de una instalación mínima de Ubuntu.

Q. ¿Cómo actualizo Java en Dashboard?

A. Cisco Business Dashboard utiliza los paquetes OpenJDK de los repositorios de Ubuntu. OpenJDK se actualizará automáticamente como parte de la actualización del sistema operativo central.

Q. ¿Cómo mantengo actualizado el sistema operativo de Probe?

A. Cisco Business Dashboard usa como sistema operativo la distribución Linux Ubuntu. Los paquetes y el núcleo se pueden actualizar usando los procesos estándares de Ubuntu. Por ejemplo, para realizar una actualización manual, inicie sesión en la consola con el usuario cisco e introduzca los comandos `sudo apt-get update` y `sudo apt-get upgrade`. El sistema no debe actualizarse a una nueva versión de Ubuntu y se recomienda no instalar otros paquetes aparte de los que suministra Cisco en la imagen de la máquina virtual o los instalados como parte de una instalación mínima de Ubuntu.

Q. ¿Cómo mantengo actualizado el sistema operativo de Probe al utilizar Raspberry Pi?

A. Los paquetes y kernel de Raspbian pueden actualizarse mediante los procesos estándar utilizados para las distribuciones de Linux basadas en Debian. Por ejemplo, para realizar una actualización manual, inicie sesión en la consola con el usuario cisco e introduzca los comandos `sudo apt-get update` y `sudo apt-get upgrade`. El sistema no debería 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 de Raspbian y los añadidos por el instalador de Probe.