Configuración de RADKit para resolución de problemas remota en HyperFlex

Contenido

Introducción

Este documento describe cómo comenzar y preparar un entorno RADKit para la resolución remota de problemas de un entorno Cisco HyperFlex.

Antecedentes

El objetivo principal de este documento es explicar cómo preparar su entorno para el uso del TAC para aprovechar RADKit para la resolución de problemas.

¿Qué es RADKit?

RADKit es un orquestador de toda la red. Experimente una manera radicalmente nueva de abordar los equipos, mejorar los servicios de Cisco y ampliar las capacidades.

Puede encontrar más información sobre RADKit aquí: https://radkit.cisco.com/

¿Por qué RADKit para HX?

Cisco HyperFlex consta de varios componentes: Fabric Interconnects, servidores UCS, ESXi, vCenter y SCVM. En muchos casos, es necesario recopilar y correlacionar la información de diferentes dispositivos. Mientras se solucionan los problemas, puede que se necesite nueva información con el tiempo y hacerlo durante una (larga) sesión de WebEx o buscando paquetes de asistencia (grandes) a través de Intersight no siempre es la forma más eficaz. Con RADKit, un ingeniero del TAC puede solicitar la información necesaria durante el proceso de resolución de problemas, desde los diversos dispositivos y servicios, de una manera segura y controlada.

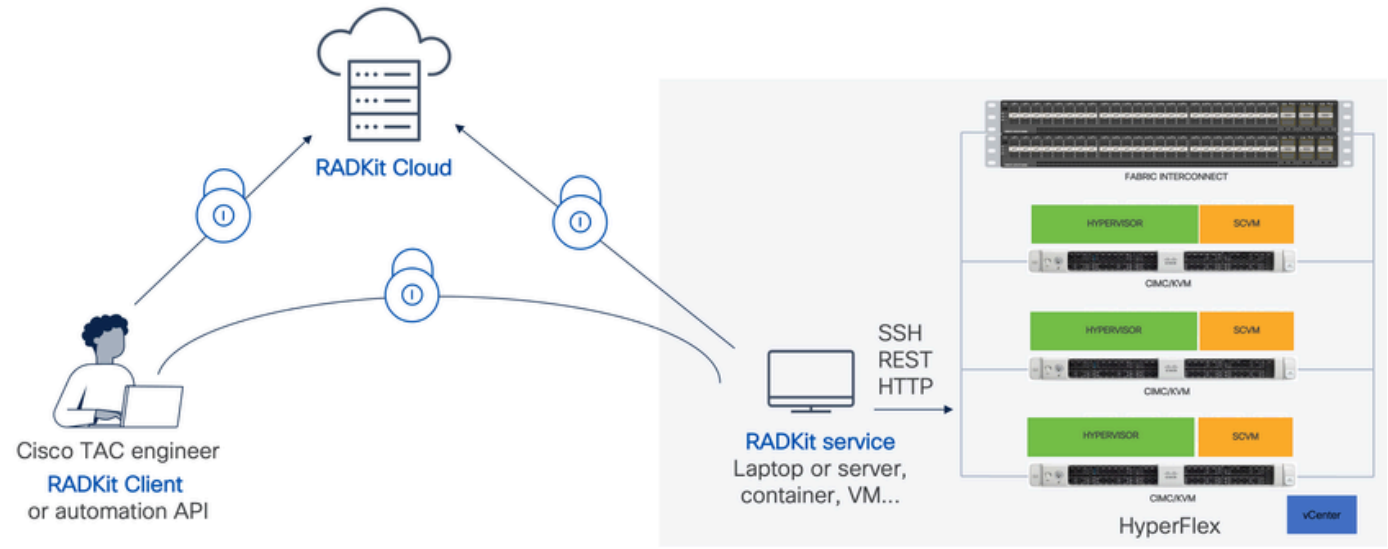
RADKit vs. Intersight

La intersección sigue siendo el método de conectividad principal para los clústeres de HyperFlex, lo que proporciona numerosas ventajas, como la recopilación automática de registros, la telemetría y la supervisión proactiva de su entorno en busca de hardware y otras alertas conocidas.

Aunque muchos clústeres HX están conectados a Intersight, Intersight está pensado principalmente para la implementación, el mantenimiento y la supervisión de los clústeres HyperFlex. Intersight permite recopilar paquetes de asistencia e información de telemetría, lo que suele ser un buen punto de partida para la resolución de problemas. Para la resolución de problemas en tiempo real, cuando en un escenario clásico, un ingeniero del TAC utilizaría una sesión de WebEx, RADKit viene en su lugar. No sustituye a Intersight, sino que añade un enfoque diferente a la resolución de problemas, ya sea mediante una sesión interactiva o aprovechando secuencias de solicitud-respuesta programáticas.

Descripción general de alto nivel

Diagrama de conectividad



Componentes

- Servicio RADKit: componente de servicio RADkit en las instalaciones, que se utiliza como un gateway seguro a su entorno HX. Como cliente, puede mantener un control total sobre qué dispositivos son accesibles y quién puede acceder a ellos en qué momento. Este servicio se puede alojar en cualquier máquina Linux, MacOS o Windows.
- Cliente RADKit: interfaz utilizada por el ingeniero del TAC para obtener acceso a su entorno, mediante la resolución de problemas y la supervisión programáticas, la recuperación automatizada y el análisis de las salidas de los dispositivos mediante herramientas internas de Cisco o la interacción directa con los dispositivos a través de CLI.
- RADKit Cloud: proporciona transporte seguro entre el cliente y el servicio.

Preparación

Descripción general de los pasos a seguir

Estos pasos son necesarios antes de que un ingeniero del TAC pueda aprovechar RADKit para conectar y solucionar problemas en su entorno HX:

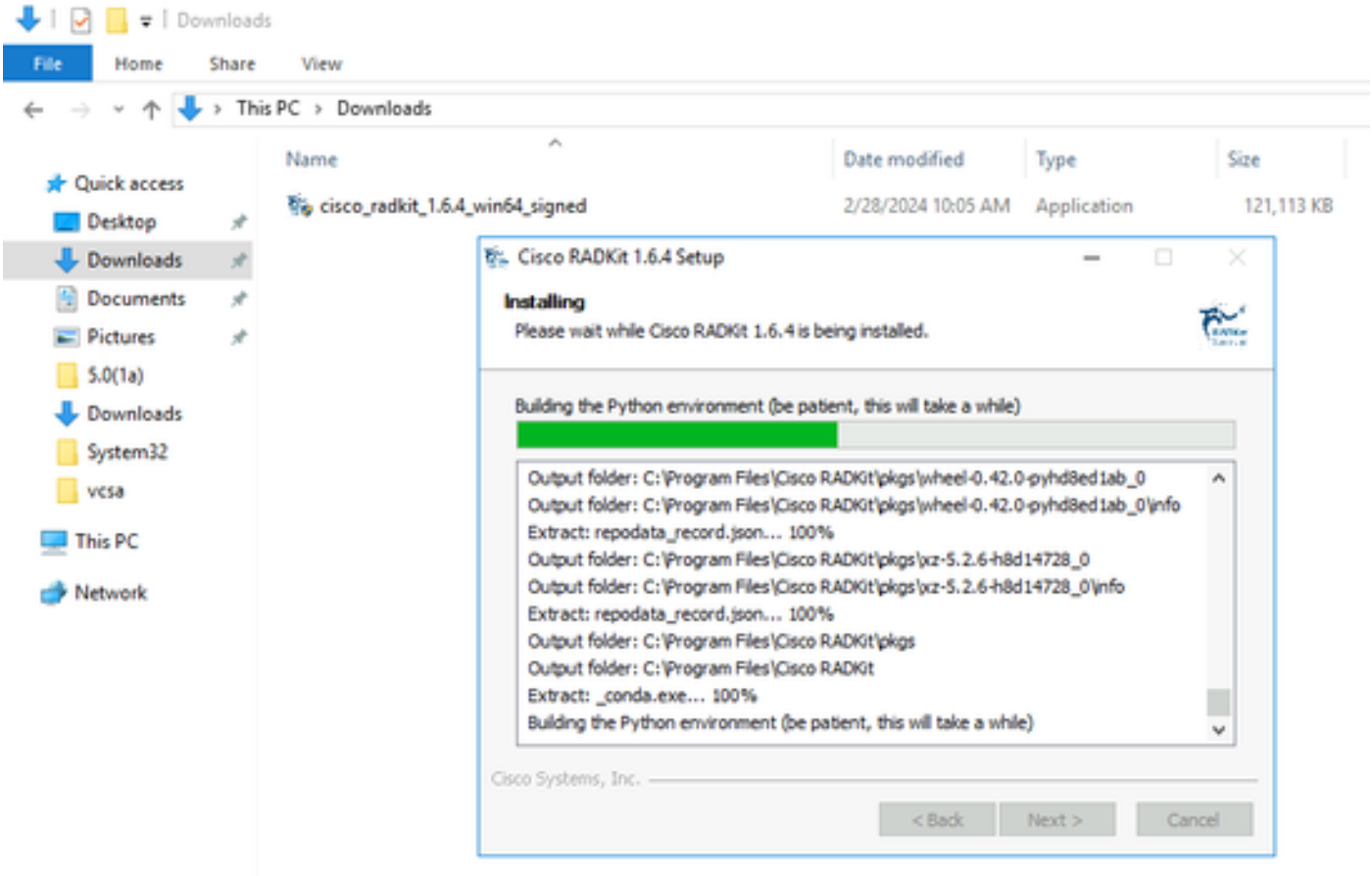
1. Descargue e instale el servicio RADkit. Se puede instalar en cualquier máquina Linux, MacOS o Windows.
2. Inicie el servicio RADKit y realice la configuración inicial (bootstrap). Cree una cuenta de superadministrador para gestionar el servicio RADKit a través de una interfaz web.
3. Inscriba su servicio RADKit con la nube RADKit. Registre su servicio RADKit con la nube RADKit y genere una ID de servicio para identificar su entorno.
4. Agregue dispositivos y terminales. Proporcione una lista de dispositivos y almacene las credenciales de los dispositivos a los que es posible que deba accederse.

Puede encontrar una explicación más detallada/genérica de estos pasos aquí: https://radkit.cisco.com/docs/pages/one_page_setup.html

Paso 1. Descargar e instalar el servicio RADKit

Los detalles de este paso pueden ser un poco diferentes, dependiendo del sistema operativo que esté utilizando para instalar el servicio RADKit, pero en general, el proceso es muy similar. Descargue la última versión para su sistema operativo desde aquí: https://radkit.cisco.com/downloads/release/.

Ejecute el instalador del sistema y siga las indicaciones hasta que se complete la instalación:



Una vez que todos los componentes RADKit están instalados, puede continuar con el siguiente paso donde se realiza la configuración inicial.

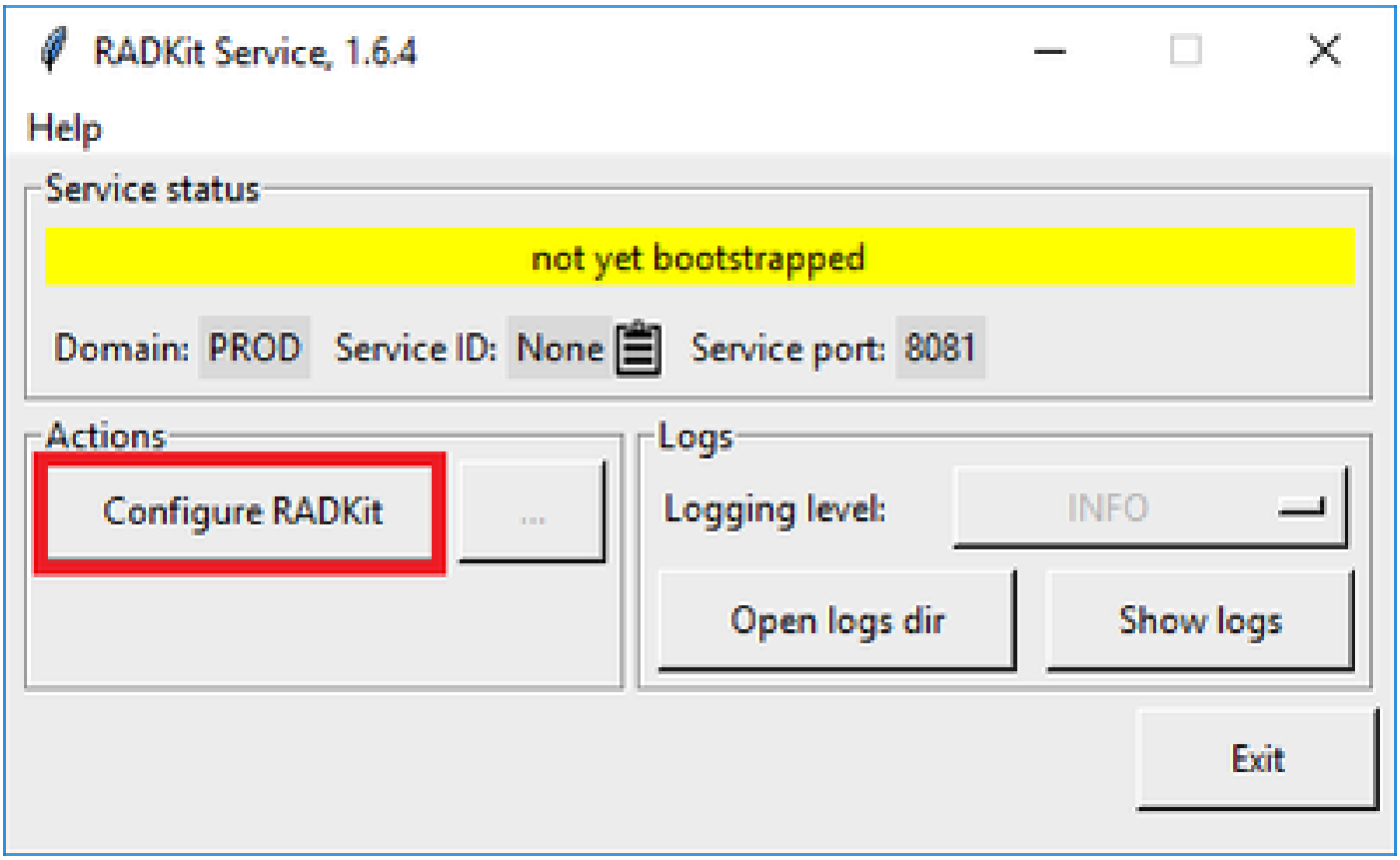
Paso 2. Inicie el servicio RADKit y realice la configuración inicial (Bootstrap)

En este paso, cree una cuenta superadmin para administrar aún más el servicio RADKit a través de una interfaz web.

Localice RADKit Service en el menú Inicio (en Windows) o en la carpeta Aplicaciones (en macOS) e inícielo:

La primera vez que lo inicie, puede tomar un poco de tiempo para que el servicio RADKit se inicie (aproximadamente 10 a 30 segundos dependiendo de la velocidad de su sistema). Las ejecuciones posteriores serán mucho más rápidas.

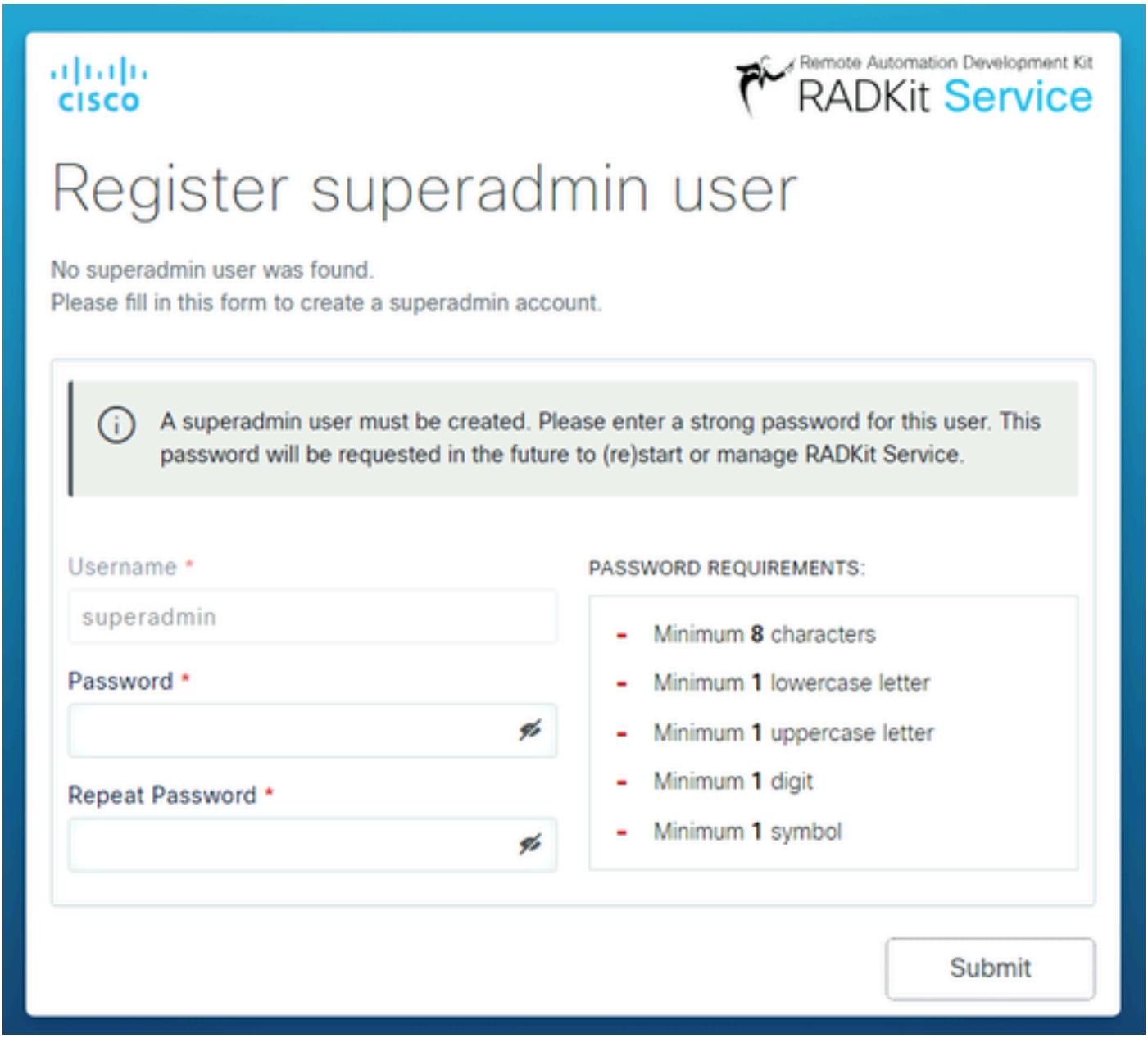
Una vez finalizado el inicio, en el cuadro de diálogo Servicio RADKit, una vez que el estado cambie a not yet bootstrapped presione Configure RADKit :



Esto abre su navegador web y lo lleva a la WebUI del servicio RADKit, una interfaz de administración basada en la web que le permite administrar el servicio RADKit.

Se espera que obtenga una advertencia de certificado, que puede omitir, cuando se conecte a esta URL ya que está utilizando un certificado autofirmado.

Dado que todavía no existe un usuario superadmin, la interfaz de usuario Web le solicitará que cree una contraseña para este usuario:



Seleccione una contraseña que cumpla los requisitos de seguridad de contraseña que se muestran a la derecha.

La contraseña de esta cuenta se utilizará para proteger secretos como claves privadas y credenciales de dispositivo; si la pierde, se perderán todos los secretos y el servicio RADKit tendrá que reinicializarse, así que selecciónela con cuidado y anótela en una ubicación segura. Se puede cambiar más adelante según sea necesario.

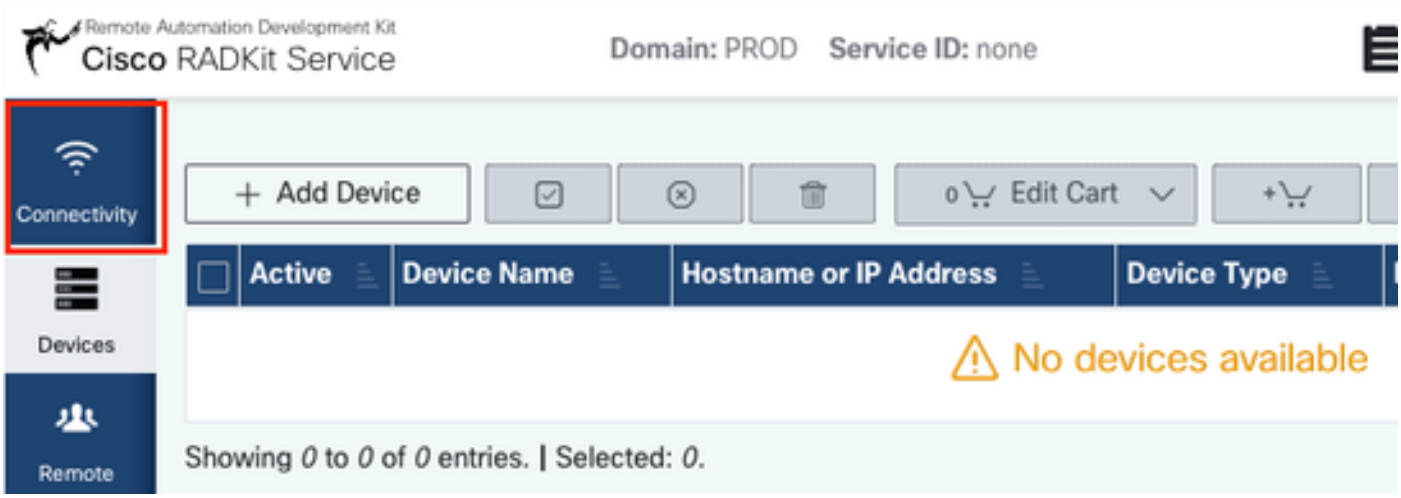
Después de crear la cuenta superadmin, utilícela para iniciar sesión en la interfaz de usuario web:

Una vez que se haya creado la cuenta superadmin y haya iniciado sesión correctamente en la interfaz de usuario de Web, puede continuar con el siguiente paso en el que su servicio RADKit está registrado con el componente de nube RADKit.

Paso 3. Inscriba su servicio RADKit con RADKit Cloud

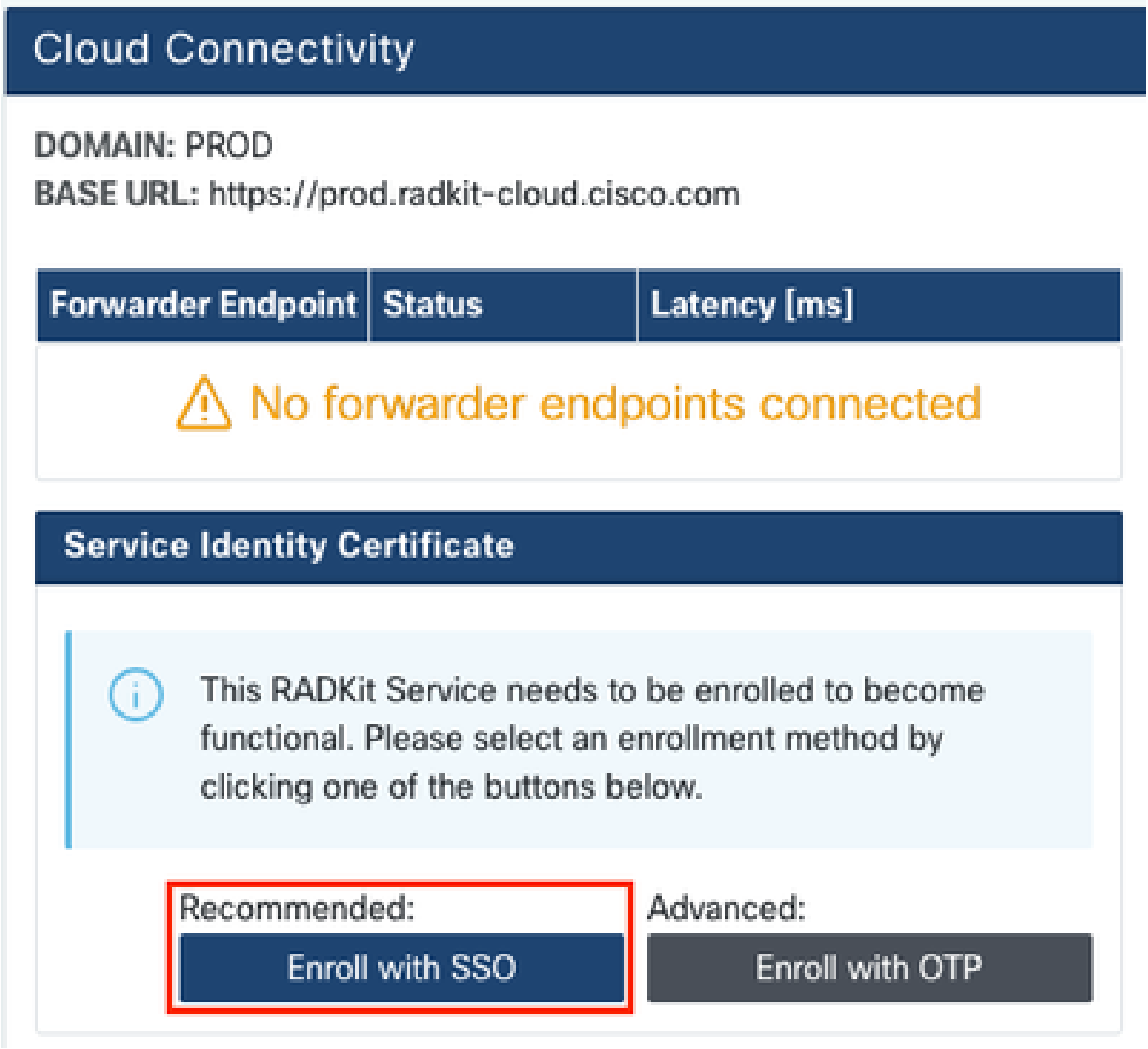
En este paso, registre su servicio RADKit con la nube RADKit y genere un ID de servicio para identificar su entorno.

Después de iniciar sesión en la interfaz de usuario Web con el usuario superadmin (consulte el paso 2), vaya a la pantalla de conectividad:

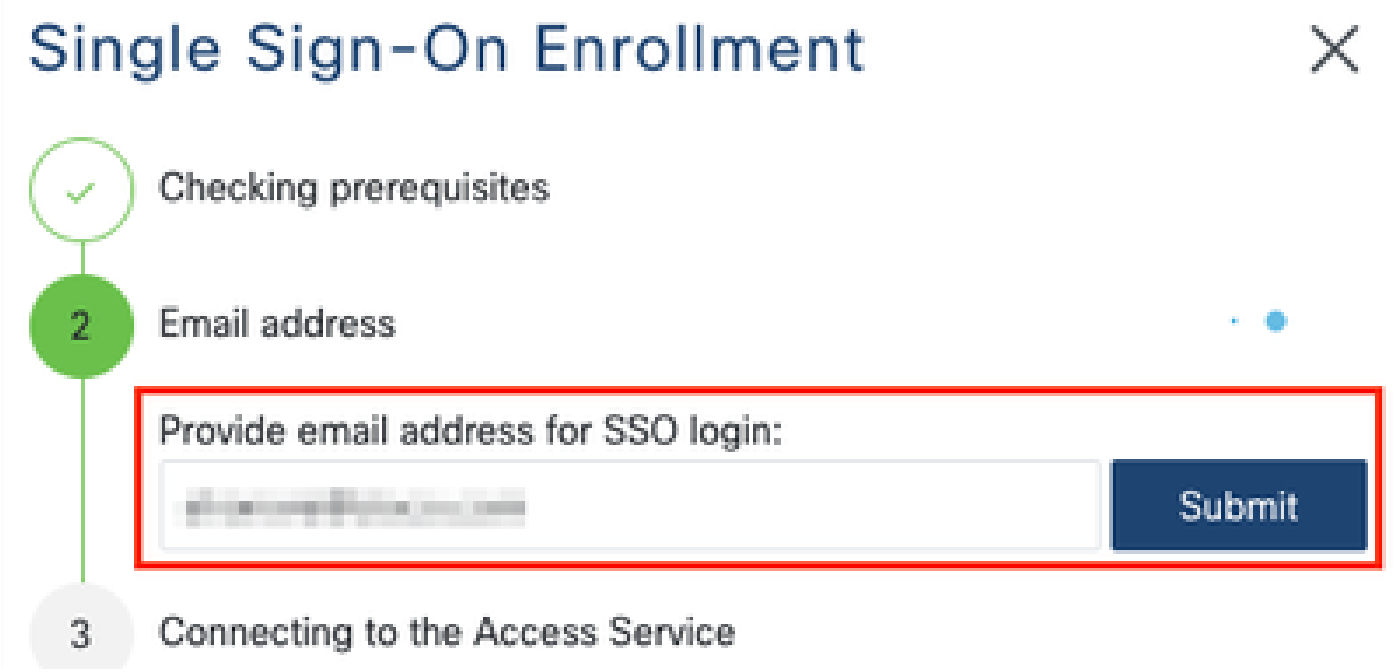


En caso de que necesite un proxy para conectarse a Internet, consulte las instrucciones de configuración detalladas disponibles aquí: https://radkit.cisco.com/docs/pages/one_page_setup.html

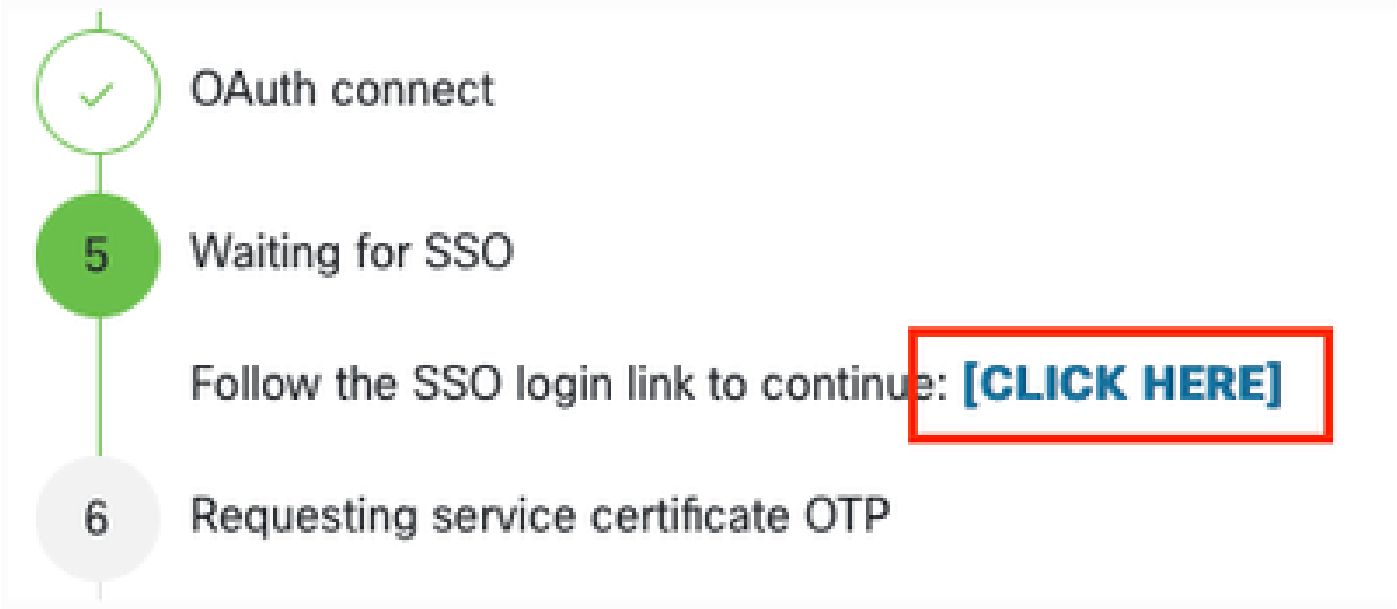
Ahora debe inscribir el servicio para que se conecte a la nube de RADKit. Para ello, inicie sesión mediante la interfaz de usuario web del servicio con la cuenta Cisco.com (CCO). Haga clic Enroll with SSO para continuar:



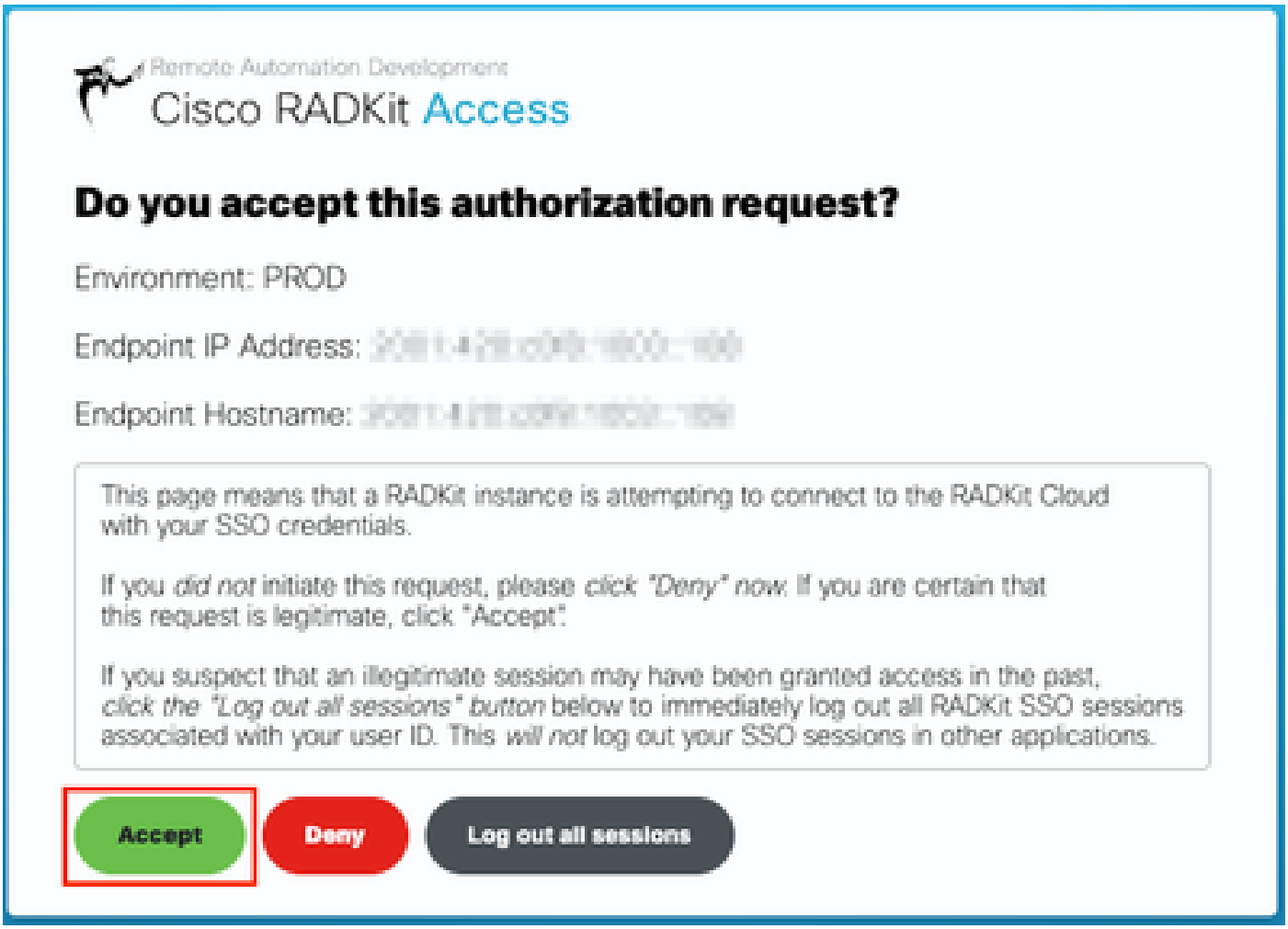
Introduzca la dirección de correo electrónico correspondiente a su cuenta Cisco.com (CCO) en el campo de dirección de correo electrónico del paso 2 y haga clic en Submit as shown in the image:



Después de que el servicio RADKit se conecte a RADKit Cloud para la autorización, le muestra un [CLICK HERE] enlace que le lleva al servidor SSO de Cisco para la autenticación. Haga clic en el enlace para continuar; se abrirá en una nueva pestaña o ventana del navegador. Asegúrese de utilizar la misma dirección de correo electrónico para iniciar sesión en SSO, como la que introdujo en el paso mencionado anteriormente:



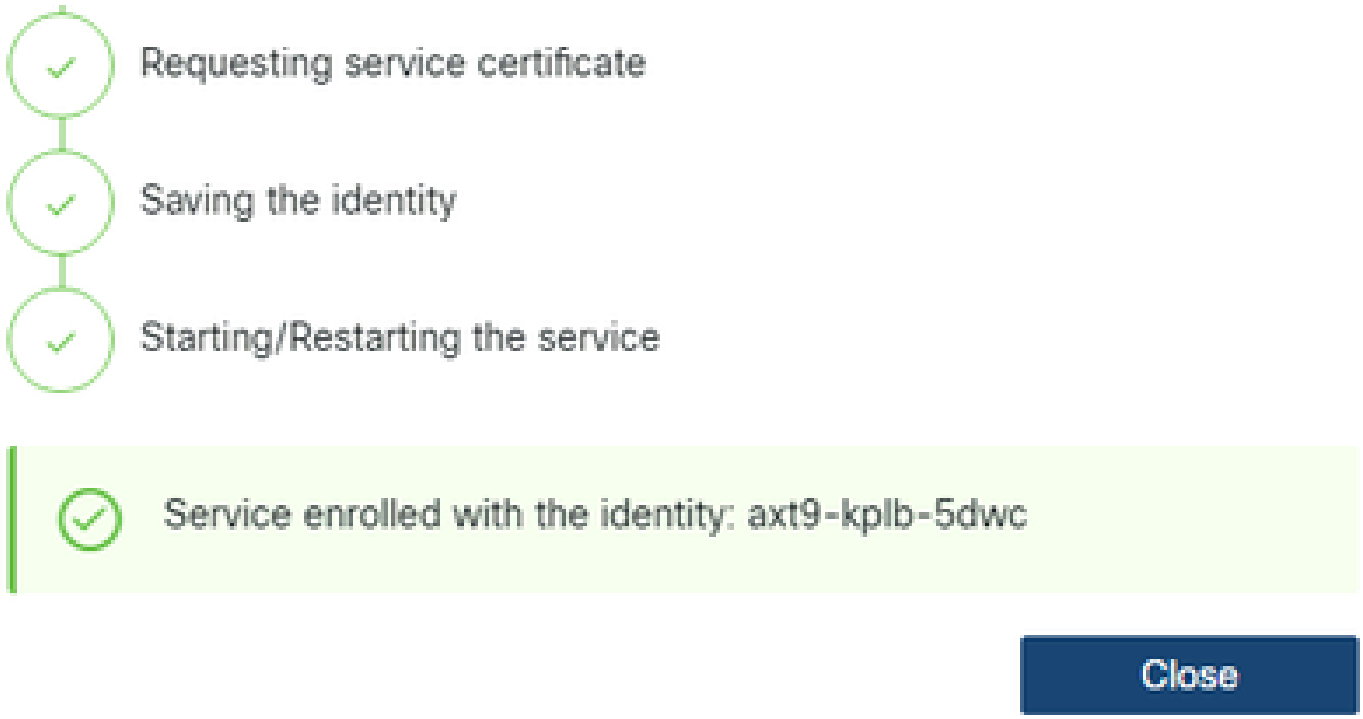
Una vez completada la autenticación de SSO (o inmediatamente, si ya estaba autenticado), se le dirigirá a una página de confirmación de Acceso a RADKit. Lea la información que aparece en la página y haga clic en Accept para autorizar al servicio RADKit a inscribirse con su cuenta CCO como propietario.



A continuación, aparece una pantalla con el texto Authentication result: Success .

No haga clic en el Log out all sessions botón; en su lugar, simplemente cierre la ficha/ventana SSO y vuelva a la WebUI del servicio RADKit.

Esto muestra Service enrolled with the identity: … . El identificador único que aparece a continuación es su ID de servicio de RADKit, también conocido como número de serie de servicio. En la captura de pantalla de ejemplo, el ID de servicio es axt9-kplb-5dwc suyo y será diferente.



Haga clic Close para cerrar el cuadro de diálogo y volver a la Connectivity pantalla.

Después de actualizar la interfaz de usuario web, la ID de servicio se muestra sobre la interfaz gráfica de usuario de RADKit, junto con el estado de la conectividad, como se muestra a continuación:

Siempre que un ingeniero del TAC necesite acceder a cualquiera de los dispositivos de su entorno, necesitará esta ID de servicio para identificar su servicio RADKit.

Ahora que se ha establecido una conectividad con el componente RADKit Cloud y se ha generado una ID de servicio, en el siguiente paso, agregue los dispositivos a los que se puede acceder a través de RADKit.

Paso 4. Agregar dispositivos y terminales

En este paso, agregue los dispositivos y sus credenciales para los dispositivos a los que se puede acceder a través de RADKit. Para HyperFlex, esto significa que, idealmente, se deben agregar estos dispositivos y sus credenciales:

Dispositivo	tipo de dispositivo	Protocolos de gestión	Credenciales	Puertos TCP reenviados	Comentarios
Hipervisor (hosts ESXi)	Linux	Terminal (SSH)	raíz		

Controlador de almacenamiento (SCVM)	HyperFlex	Interruptor de terminal (SSH)	admin root (enable)	443	Introduzca la contraseña raíz en el campo enable password (activar contraseña). Esto se utilizará cuando se requiera un token de consentimiento. Para Swagger: desmarque "Verificar certificado TLS" y deje vacío el campo URL base
vCenter	Linux	Terminal (SSH)	raíz		
UCSM	GENÉRICO	Terminal (SSH)	admin		
Instalador (opcional)	Linux	Terminal (SSH)	raíz	443	
CIMC (solo para clústeres perimetrales)	GENÉRICO	Terminal (SSH)	admin		
Testigo (solo para grupos extendidos)	Linux	Terminal (SSH)	raíz		
Intersight CVA/PCA (opcional)	Linux	Terminal (SSH)	admin	443	

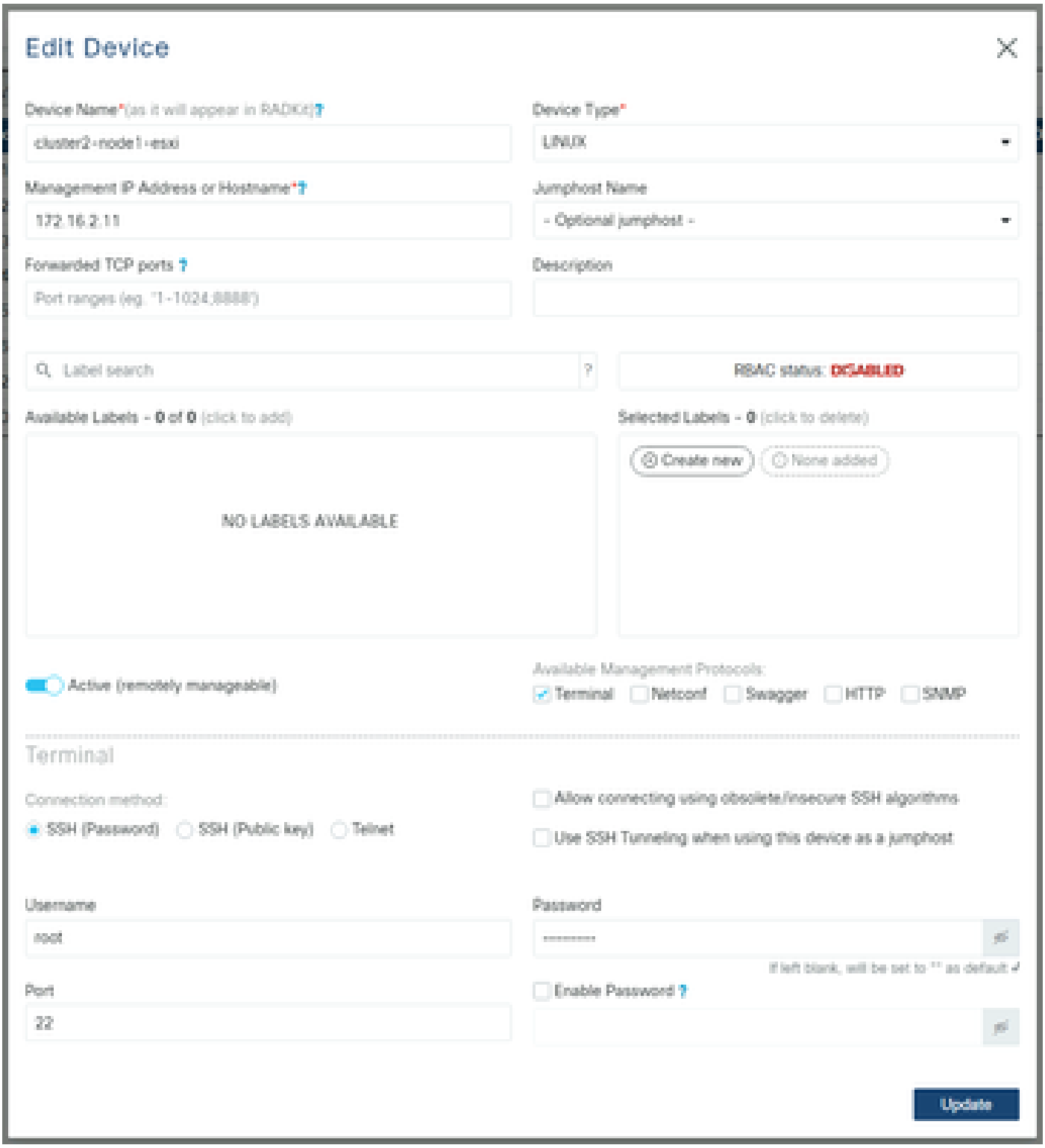
Es importante agregar los dispositivos solamente usando su dirección IP y no su nombre de host, ya que esto es necesario para correlacionar los dispositivos que pertenecen al mismo clúster.

Para agregar estos dispositivos, en la interfaz de usuario web de RADKit, vaya a la pantalla Devices (Dispositivos):

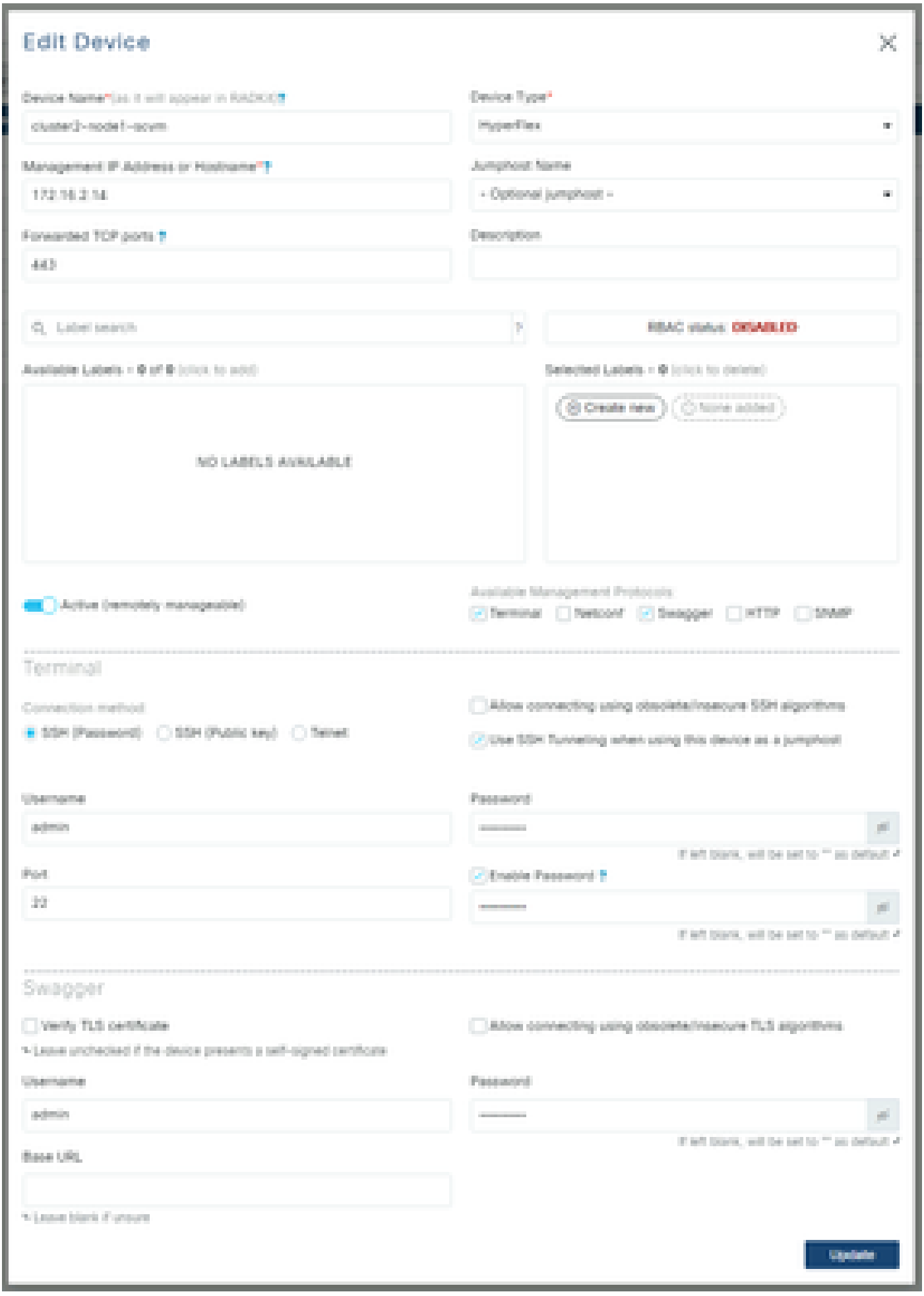
Para cada uno de los dispositivos enumerados anteriormente, cree una nueva entrada haciendo clic en Add Device . Introduzca la dirección IP, seleccione el tipo de dispositivo y proporcione detalles en función de cada tipo de dispositivo para todos los nodos del clúster. Cuando haya terminado, haga clic Add & closepara volver a la pantalla Devices (Dispositivos) o Add & continue para agregar otro dispositivo.

Aquí puede encontrar ejemplos de entradas y su configuración para cada tipo de dispositivo:

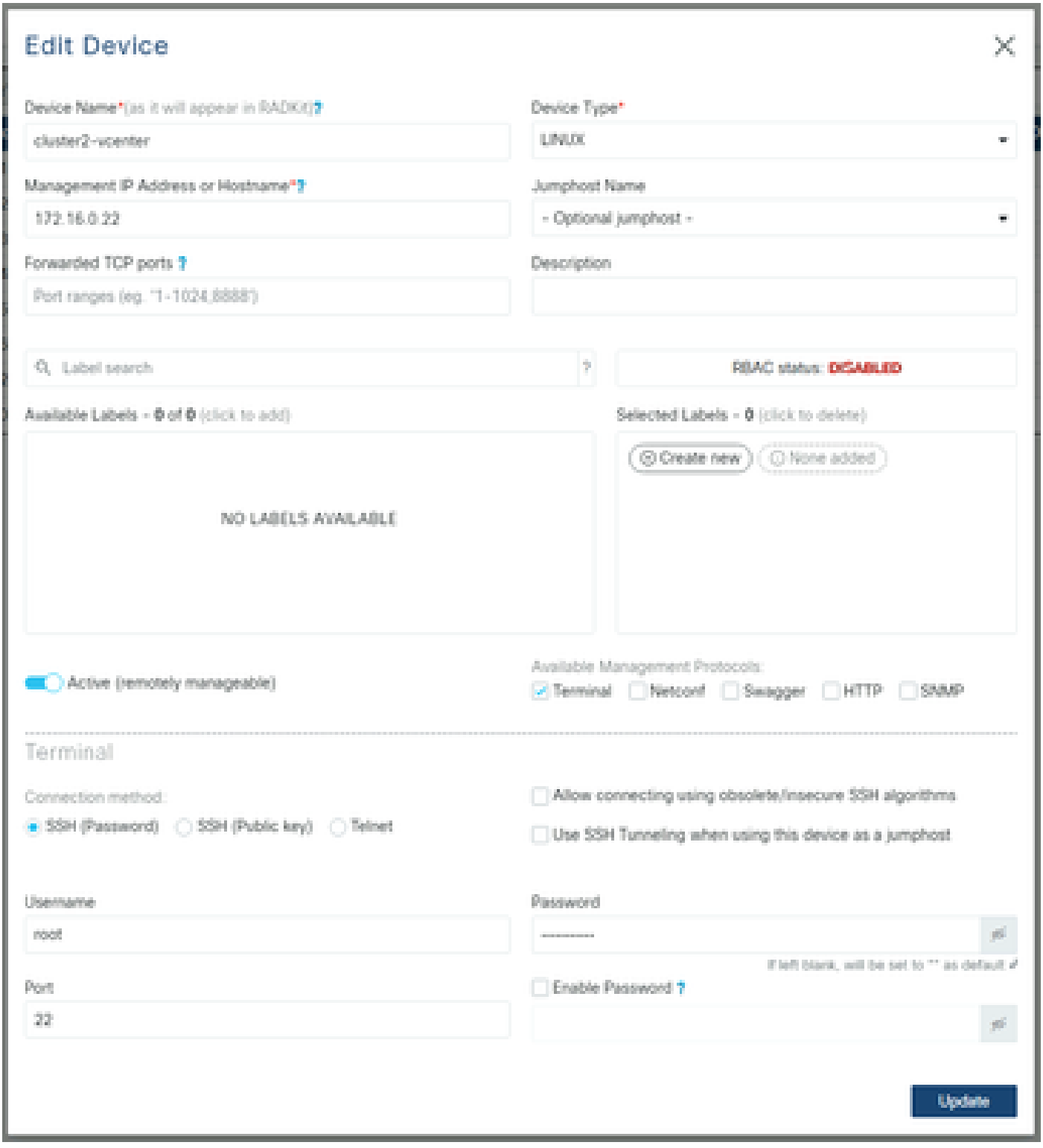
Ejemplo para hosts ESXi:



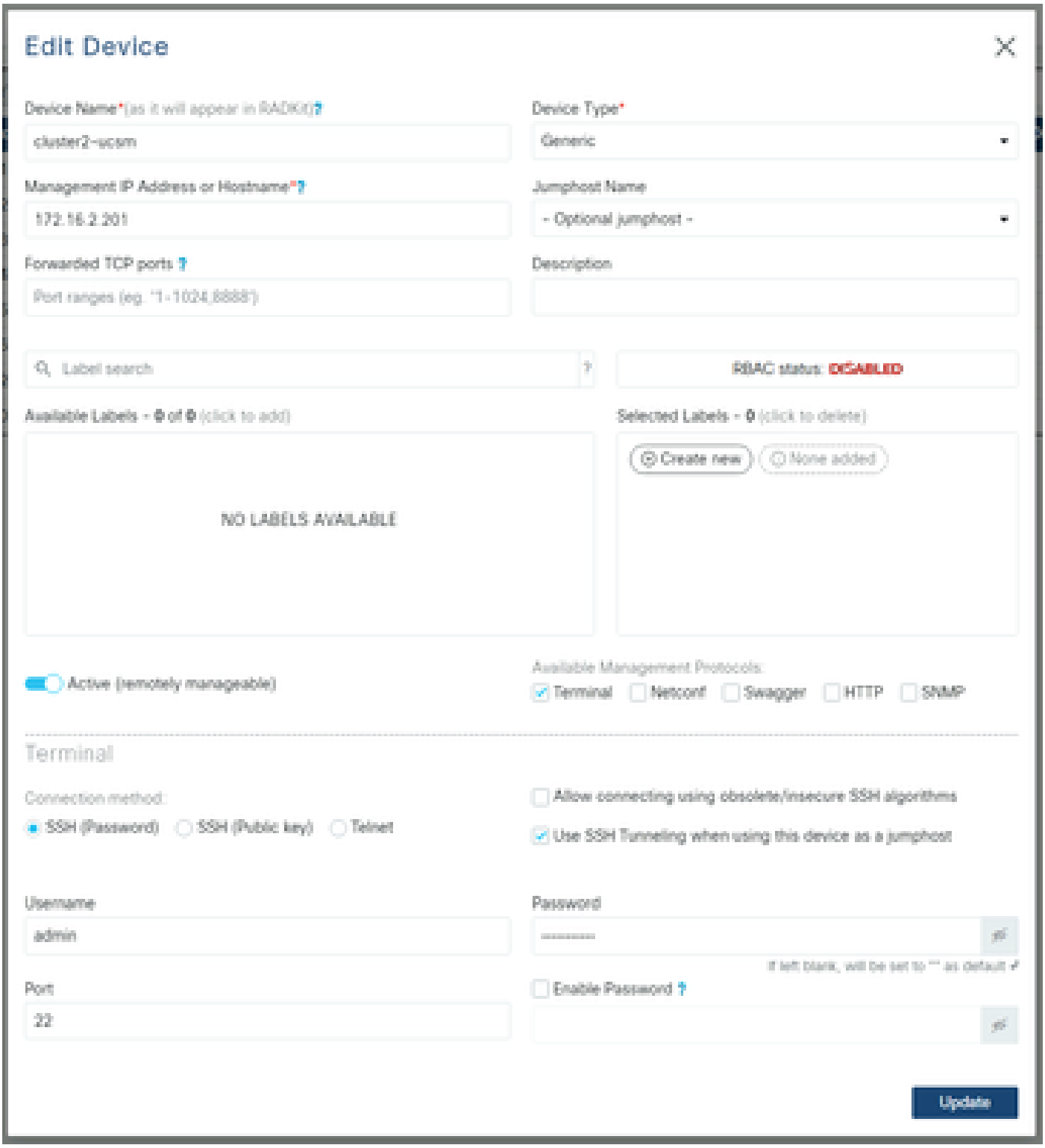
Ejemplo de controladores de almacenamiento:


Edit Device
Device Name*(as it will appear in RADKit)
cluster3-node1-acvm
Device Type*
HyperFlex
Management IP Address or Hostname*
172.16.2.14
Jumphost Name
- Optional jumphost -
Forwarded TCP ports
443
Description
Label search
RBAC status: DISABLED
Available Labels - 0 of 0 (click to add)
NO LABELS AVAILABLE
Selected Labels - 0 (click to delete)
Create new
None added
Active (remotely manageable)
Available Management Protocols
Terminal
Netconf
Swagger
HTTP
SNMP
Terminal
Connection method
SSH (Password)
SSH (Public key)
Telnet
Allow connecting using obsolete/insecure SSH algorithms
Use SSH Tunneling when using this device as a jumphost
Username
admin
Password
If left blank, will be set to "" as default
Port
22
Enable Password
If left blank, will be set to "" as default
Swagger
Verify TLS certificate
Allow connecting using obsolete/insecure TLS algorithms
* Leave unchecked if the device presents a self-signed certificate
Username
admin
Password
If left blank, will be set to "" as default
Base URL
* Leave blank if unsure
Update

Ejemplo de vCenter:



Ejemplo de UCSM:



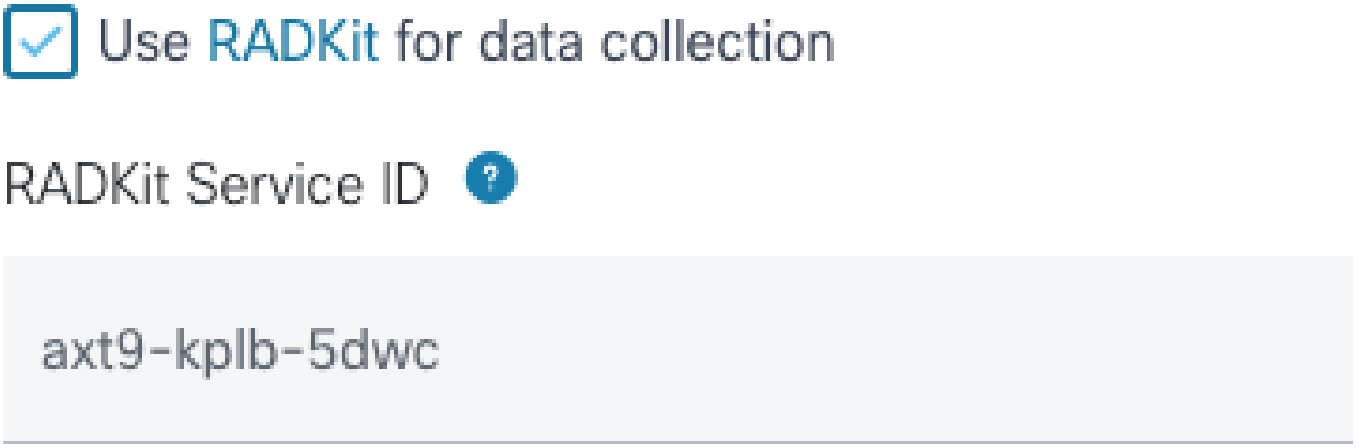
Uso de RADKit en un TAC SR

Si se ha realizado toda la preparación y desea proporcionar acceso a sus dispositivos a un ingeniero del TAC, puede seguir estos pasos.

Un ingeniero necesita su ID de servicio de RADKit y acceso a su entorno o a los dispositivos seleccionados (cuando se utiliza RBAC) durante el tiempo que sea necesario.

1. Proporcione la ID del servicio RADKit

Si aún no ha abierto un caso de TAC, tiene la oportunidad de mencionarlo Use RADKit for data collection en el Support Case Manager en Cisco.com:

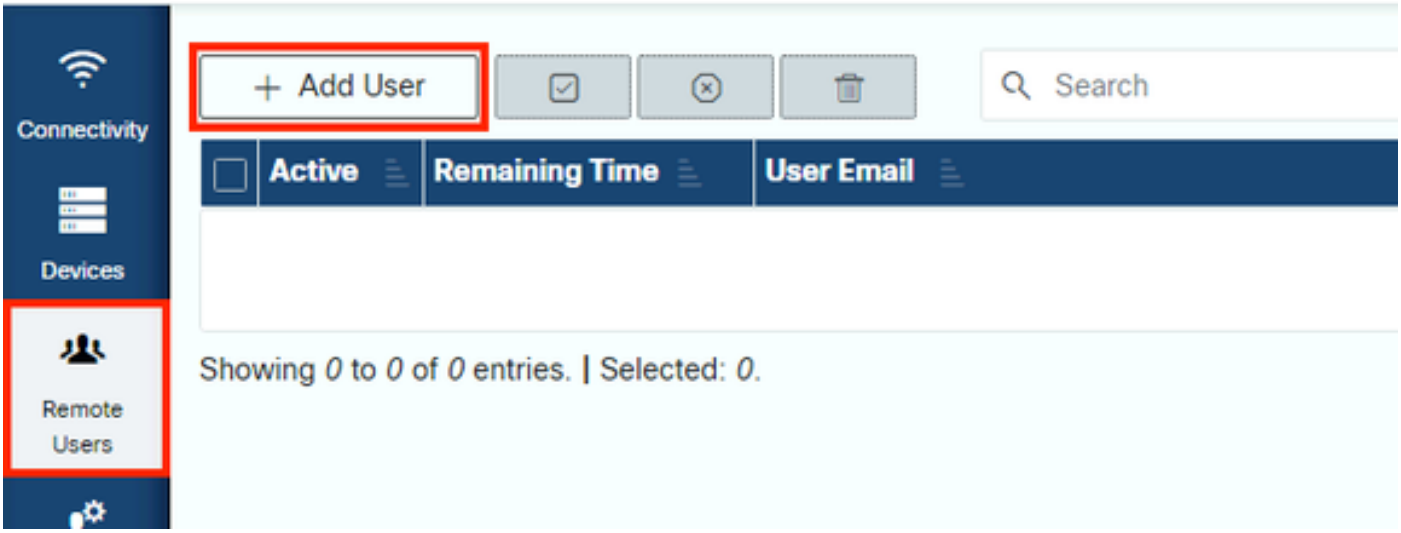


En caso de que ya tenga una solicitud de servicio abierta, puede agregar la ID de servicio de RADKit en Support Case Manager con la sección Información de contacto del cliente:

O simplemente mencione su ID al ingeniero del TAC que está trabajando en su caso.

2. Agregar usuario remoto

Antes de que cualquier usuario pueda trabajar con sus dispositivos, debe proporcionar un acceso explícito y configurar un período de tiempo durante el cual este acceso siga siendo válido. Para ello, en la interfaz de usuario web de RADKit, desplácese a la Remote Users pantalla y cree un nuevo usuario remoto haciendo clic en Add User.



Introduzca la dirección de correo electrónico @cisco.com del ingeniero del TAC (tenga cuidado con los errores tipográficos). Asegúrese de prestar atención a la Activate this user casilla de verificación y a los parámetros Time slice o Manual e.

Mientras el usuario está activo, tiene acceso a los dispositivos configurados a través del servicio RADKit, siempre que dichos dispositivos estén habilitados y que la política RBAC lo permita.

El intervalo de tiempo representa la cantidad de tiempo tras el cual el usuario se desactivará automáticamente; en otras palabras, un intervalo de tiempo representa una sesión de solución de problemas con límite de tiempo. La sesión del usuario se puede ampliar hasta la duración del período de tiempo de dicho usuario. Si prefiere activar/desactivar usuarios manualmente, selecciónelos Manual.

Los usuarios siempre se pueden activar/desactivar manualmente, independientemente de si tienen un intervalo de tiempo configurado o no. Cuando un usuario se desactiva, todas sus sesiones a través del servicio RADKit se desconectan instantáneamente.

Cuando haya terminado, haga clic en Add & close para volver a la pantalla Remote Users (Usuarios remotos).

Información Relacionada

- Puede encontrar más información y respuestas a preguntas comunes en el sitio web de RADKit: https://radkit.cisco.com/
- **Soporte técnico y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).