RADKit für Remote-Fehlerbehebung auf HyperFlex einrichten

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine RADKit-Umgebung für die Remote-Fehlerbehebung in einer Cisco HyperFlex-Umgebung vorbereiten.

Hintergrundinformationen

In diesem Dokument wird in erster Linie erläutert, wie Sie Ihre Umgebung für den Einsatz durch das TAC vorbereiten, damit das RADKit zur Fehlerbehebung eingesetzt werden kann.

Was ist RADKit?

RADKit ist ein Orchestrierungssystem für das gesamte Netzwerk. Erleben Sie eine völlig neue Art der Adressierung Ihrer Geräte, verbessern Sie Ihre Cisco Services und erweitern Sie Ihre Funktionen.

Weitere Informationen zu RADKit finden Sie hier: https://radkit.cisco.com/

Warum RADKit für HX?

Cisco HyperFlex besteht aus mehreren Komponenten: Fabric Interconnects, UCS-Server, ESXi, vCenter und SCVMs. In vielen Fällen müssen Informationen von verschiedenen Geräten gesammelt und korreliert werden. Während der Fehlerbehebung können im Laufe der Zeit neue Informationen benötigt werden. Dies kann über eine (lange) WebEx Sitzung oder durch das Abrufen von (großen) Supportpaketen über Intersight erfolgen. Dies ist jedoch nicht immer der effektivste Weg. Mithilfe von RADKit kann ein TAC-Techniker die erforderlichen Informationen während des Fehlerbehebungsprozesses sicher und kontrolliert von den verschiedenen Geräten und Services anfordern.

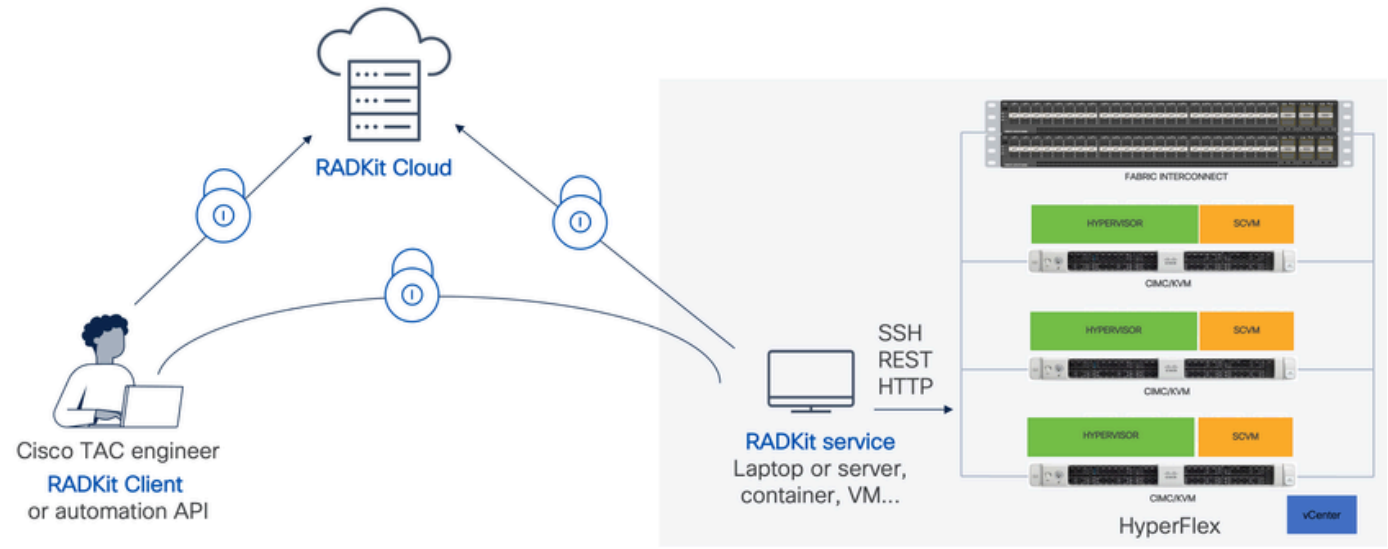
RADKit vs. Intersight

Intersight bleibt die primäre Verbindungsmethode für HyperFlex-Cluster und bietet zahlreiche Vorteile wie automatische Protokollerfassung, Telemetrie und proaktive Überwachung Ihrer Umgebung auf Hardware und andere bekannte Warnmeldungen.

Obwohl viele HX-Cluster mit Intersight verbunden sind, ist Intersight derzeit hauptsächlich für die Bereitstellung, Wartung und Überwachung Ihrer HyperFlex-Cluster vorgesehen. Intersight ermöglicht die Erfassung von Support-Paketen und Telemetrieinformationen, was in der Regel ein guter Ausgangspunkt für die Fehlerbehebung ist. Für die Live-Fehlerbehebung, bei der in einem klassischen Szenario ein TAC-Techniker eine WebEx Sitzung nutzt, wird RADKit eingerichtet. Intersight ersetzt das Programm nicht, sondern bietet einen neuen Ansatz für die Fehlerbehebung, entweder durch eine interaktive Sitzung oder durch die Nutzung programmgesteuerter Anfrageantwortsequenzen.

Allgemeiner Überblick

Verbindungsdiagramm



Komponenten

- RADKit Service: Vor-Ort-RADkit-Servicekomponente, die als sicheres Gateway zu Ihrer HX-Umgebung dient. Als Kunde behalten Sie die volle Kontrolle darüber, welche Geräte zu welchem Zeitpunkt erreichbar sind und wer darauf zugreifen kann. Dieser Dienst kann auf jedem beliebigen Linux-, MacOS- oder Windows-Rechner gehostet werden.
- RADKit-Client: Front-End, das vom TAC-Techniker für den Zugriff auf Ihre Umgebung verwendet wird, mit programmgesteuerter Fehlerbehebung und Überwachung, automatischem Abruf und Analyse von Geräteausgaben mithilfe von Cisco-internen Tools oder direkter Interaktion mit den Geräten über die CLI.
- RADKit Cloud: Bietet sicheren Transport zwischen Client und Service.

Vorbereitung

Überblick über die zu befolgenden Schritte

Diese Schritte sind erforderlich, bevor ein TAC-Techniker RADKit für die Verbindung und Fehlerbehebung in Ihrer HX-Umgebung nutzen kann:

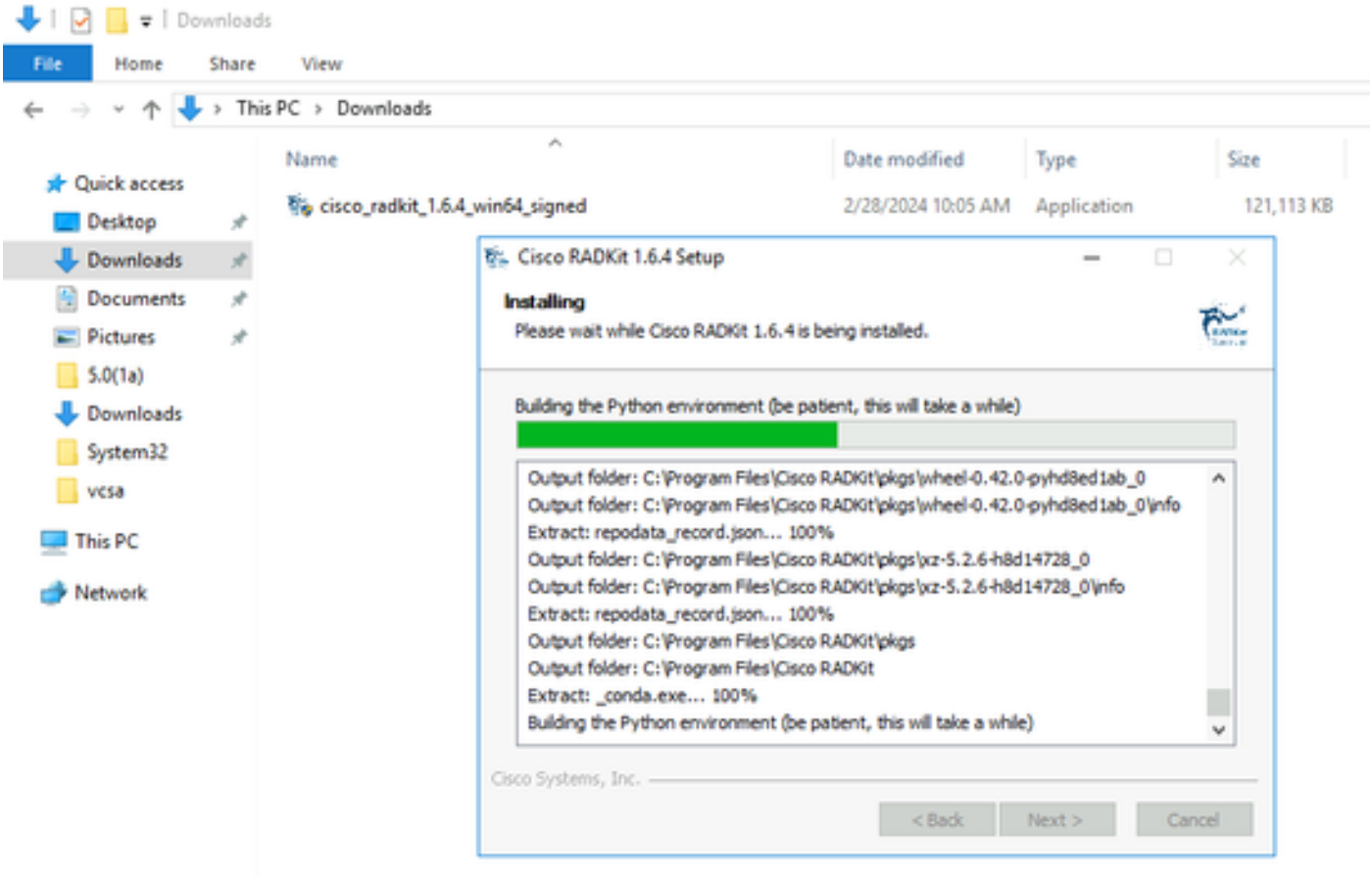
1. Laden Sie den RADkit-Service herunter, und installieren Sie ihn. Es kann auf jedem beliebigen Linux-, MacOS- oder Windows-Rechner installiert werden.
2. Starten Sie den RADKit-Dienst und führen Sie die Ersteinrichtung (Bootstrap) durch. Erstellen Sie ein Administratorkonto, um den RADKit-Dienst über eine Webschnittstelle weiter zu verwalten.
3. Registrieren Sie Ihren RADKit Service mit der RADKit Cloud. Registrieren Sie Ihren RADKit-Service bei der RADKit-Cloud, und generieren Sie eine Service-ID, um Ihre Umgebung zu identifizieren.
4. Hinzufügen von Geräten und Endgeräten Stellen Sie eine Liste der Geräte bereit, und speichern Sie Anmeldeinformationen für Geräte, auf die möglicherweise zugegriffen werden muss.

Eine ausführlichere/allgemeine Erläuterung dieser Schritte finden Sie hier: https://radkit.cisco.com/docs/pages/one_page_setup.html

Schritt 1: RADKit-Dienst herunterladen und installieren

Die Details in diesem Schritt können etwas anders aussehen, je nachdem, welches Betriebssystem Sie zur Installation des RADKit-Dienstes verwenden, aber im Allgemeinen ist der Prozess sehr ähnlich. Laden Sie die neueste Version für Ihr Betriebssystem hier herunter: https://radkit.cisco.com/downloads/release/.

Führen Sie das Installationsprogramm für Ihr System aus, und befolgen Sie die Anweisungen, bis die Installation abgeschlossen ist:



Sobald alle RADKit-Komponenten installiert sind, können Sie mit dem nächsten Schritt fortfahren und die Ersteinrichtung durchführen.

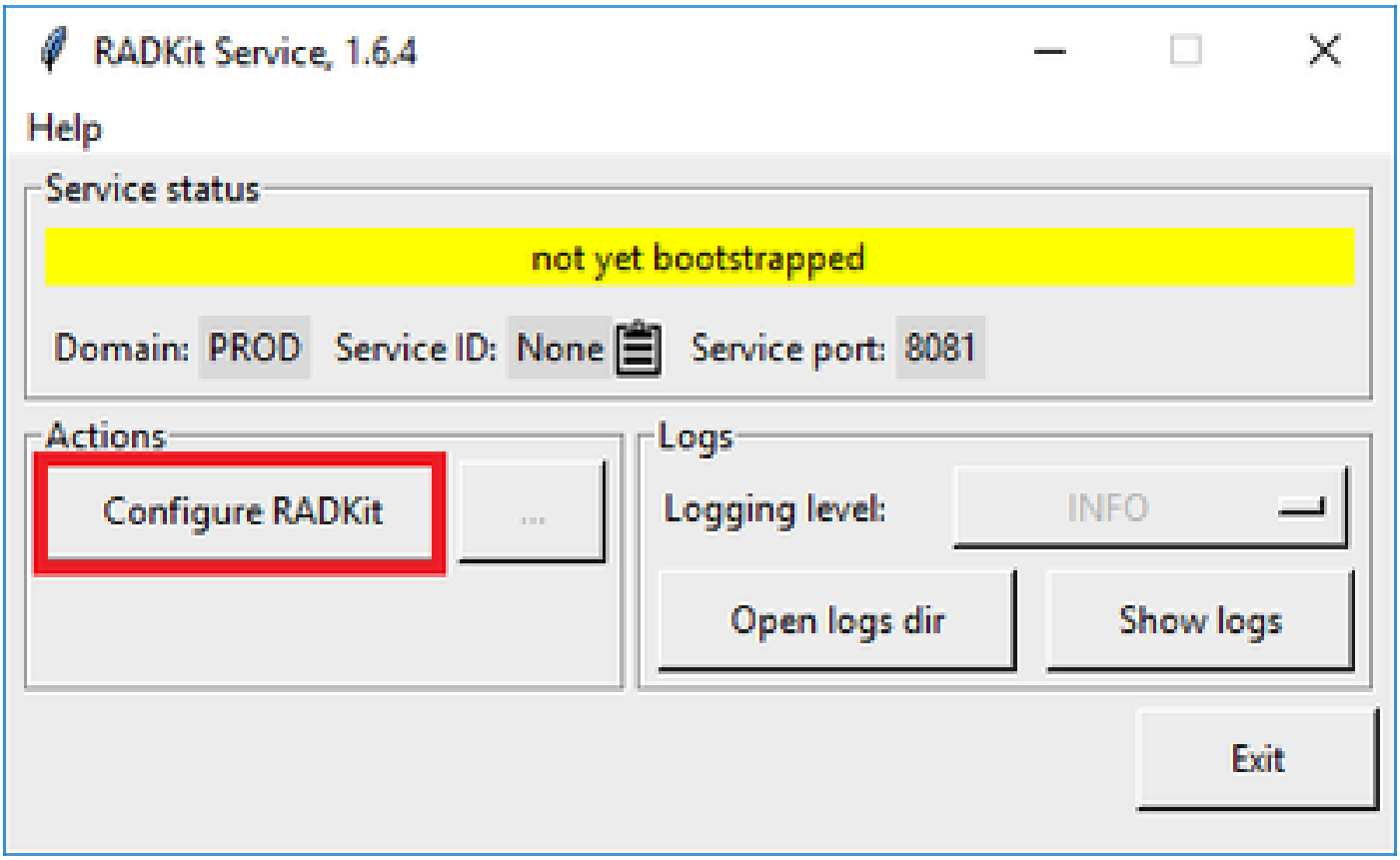
Schritt 2: Starten Sie den RADKit Service und führen Sie die Ersteinrichtung (Bootstrap) durch

In diesem Schritt erstellen Sie ein Superadmin-Konto, um den RADKit-Dienst über eine Webschnittstelle weiter zu verwalten.

Suchen Sie RADKit Service im Startmenü (unter Windows) oder im Ordner Anwendungen (unter MacOS), und starten Sie es:

Beim ersten Start kann es eine Weile dauern, bis der RADKit-Dienst gestartet wird (etwa 10 bis 30 Sekunden, je nach Geschwindigkeit des Systems). Nachfolgende Läufe werden viel schneller sein.

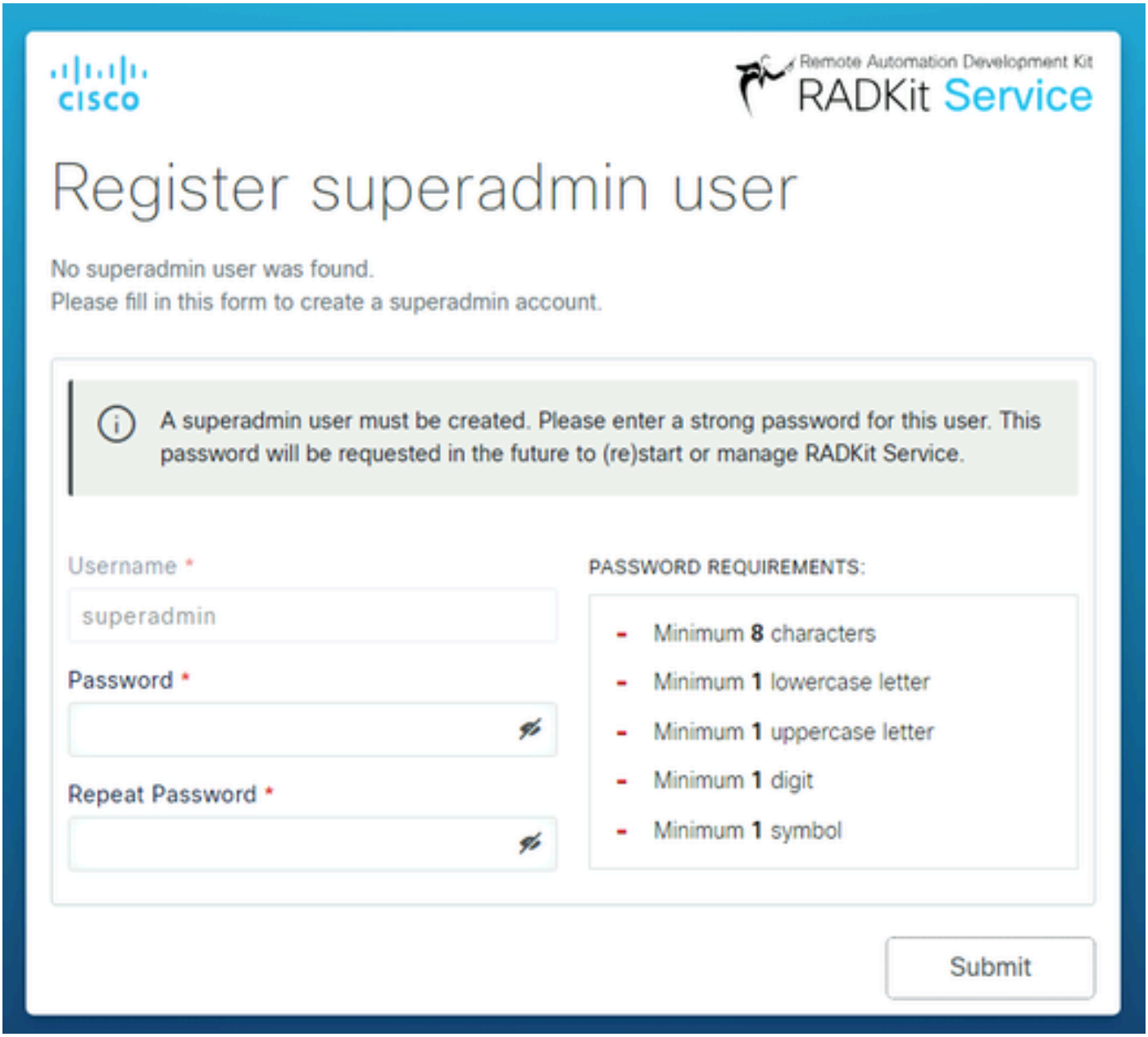
Wenn der Start abgeschlossen ist, drücken Sie im RADKit Service Dialog den Status auf not yet bootstrapped Configure RADKit :



Dadurch wird Ihr Webbrowser geöffnet und Sie gelangen zur RADKit Service WebUI, einer webbasierten Verwaltungsoberfläche, die Ihnen die Verwaltung von RADKit Service ermöglicht.

Es wird eine Zertifikatwarnung erwartet, die Sie überspringen können, wenn Sie eine Verbindung mit dieser URL herstellen, da diese ein selbstsigniertes Zertifikat verwendet.

Da ein Superadmin-Benutzer noch nicht vorhanden ist, fordert die WebUI Sie auf, ein Kennwort für diesen Benutzer zu erstellen:



Wählen Sie ein Kennwort aus, das den rechts angezeigten Anforderungen an die Kennwortsicherheit entspricht.

Das Kennwort für dieses Konto wird verwendet, um geheime Schlüssel wie private Schlüssel und Geräteanmeldeinformationen zu schützen. Wenn Sie es verlieren, gehen alle geheimen Schlüssel verloren, und der RADKit-Dienst muss neu initialisiert werden. Wählen Sie es daher sorgfältig aus, und schreiben Sie es an einem sicheren Ort auf. Sie kann bei Bedarf später geändert werden.

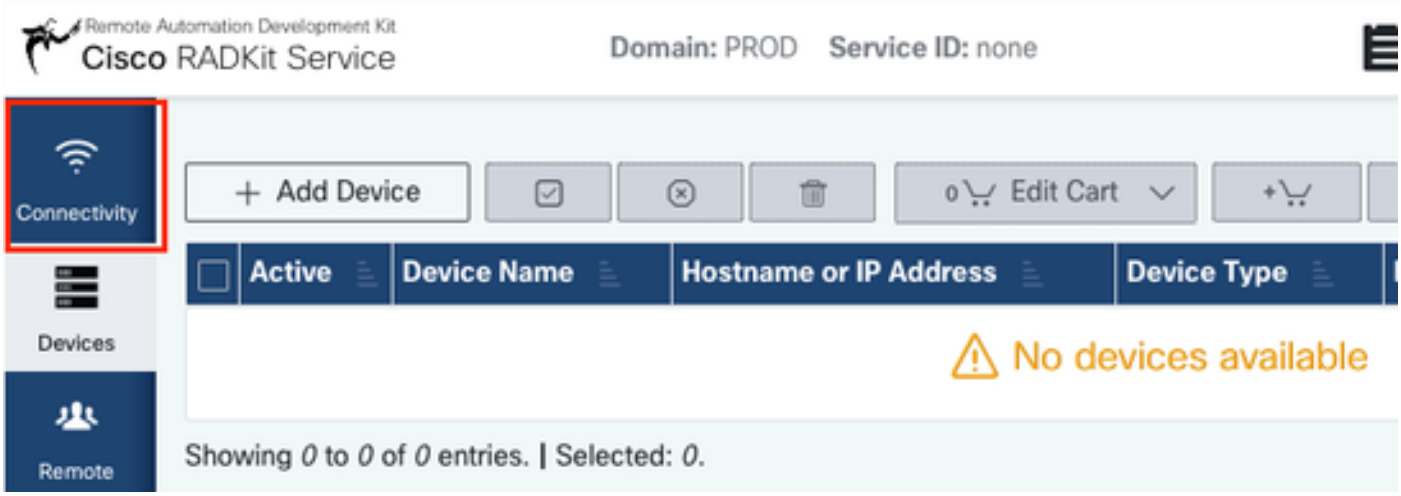
Nachdem Sie das Superadmin-Konto erstellt haben, können Sie sich mit diesem bei der WebUI anmelden:

Sobald das Superadmin-Konto erstellt wurde und Sie sich erfolgreich bei der WebUI angemeldet haben, können Sie mit dem nächsten Schritt fortfahren, in dem Ihr RADKit-Dienst bei der RADKit-Cloud-Komponente registriert ist.

Schritt 3: Registrieren Sie Ihren RADKit Service mit RADKit Cloud

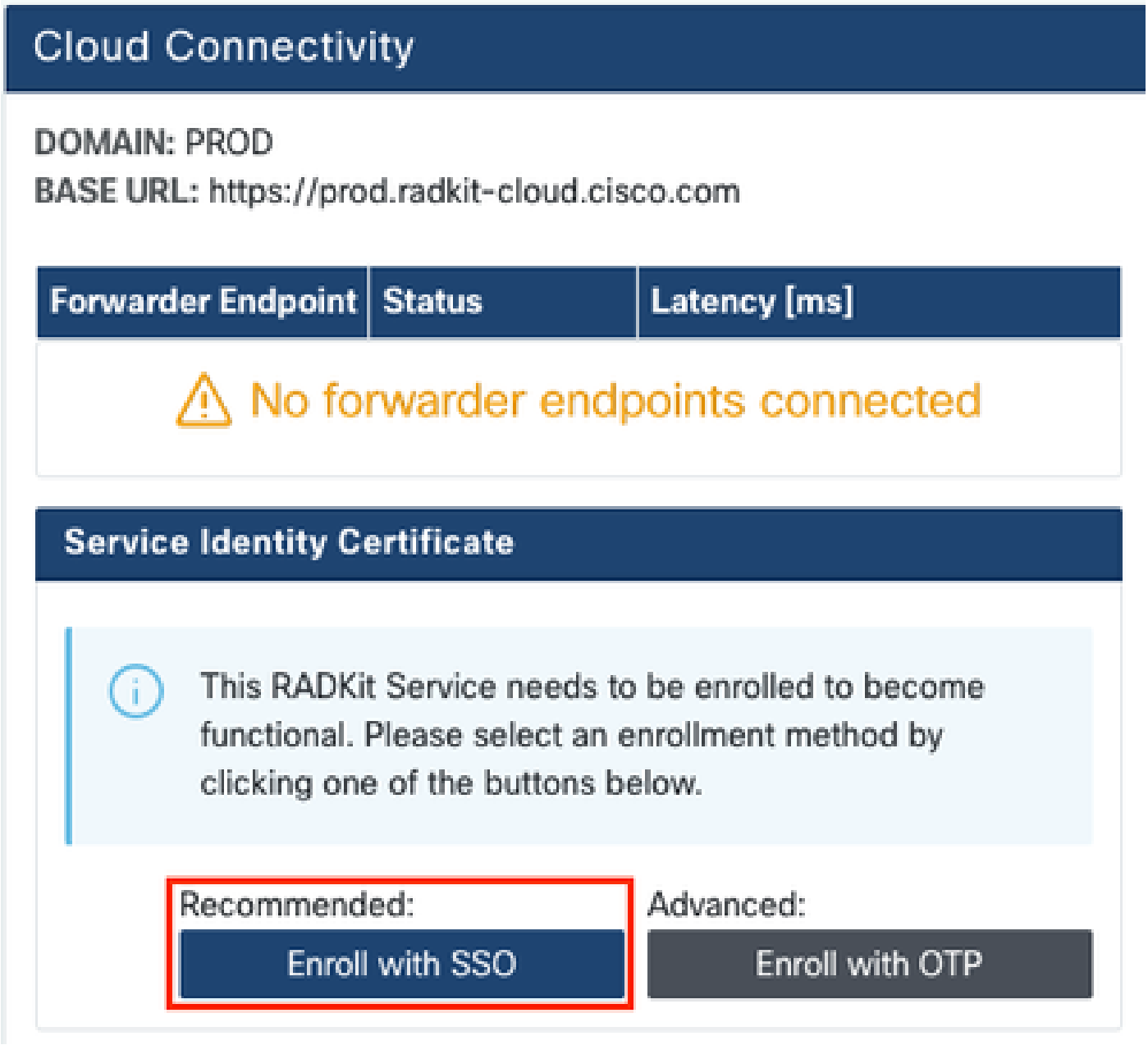
In diesem Schritt registrieren Sie Ihren RADKit-Service bei der RADKit-Cloud und generieren eine Service-ID, um Ihre Umgebung zu identifizieren.

Navigieren Sie nach der Anmeldung bei der WebUI mit dem Benutzer superadmin (siehe Schritt 2) zum Verbindungsbildschirm:

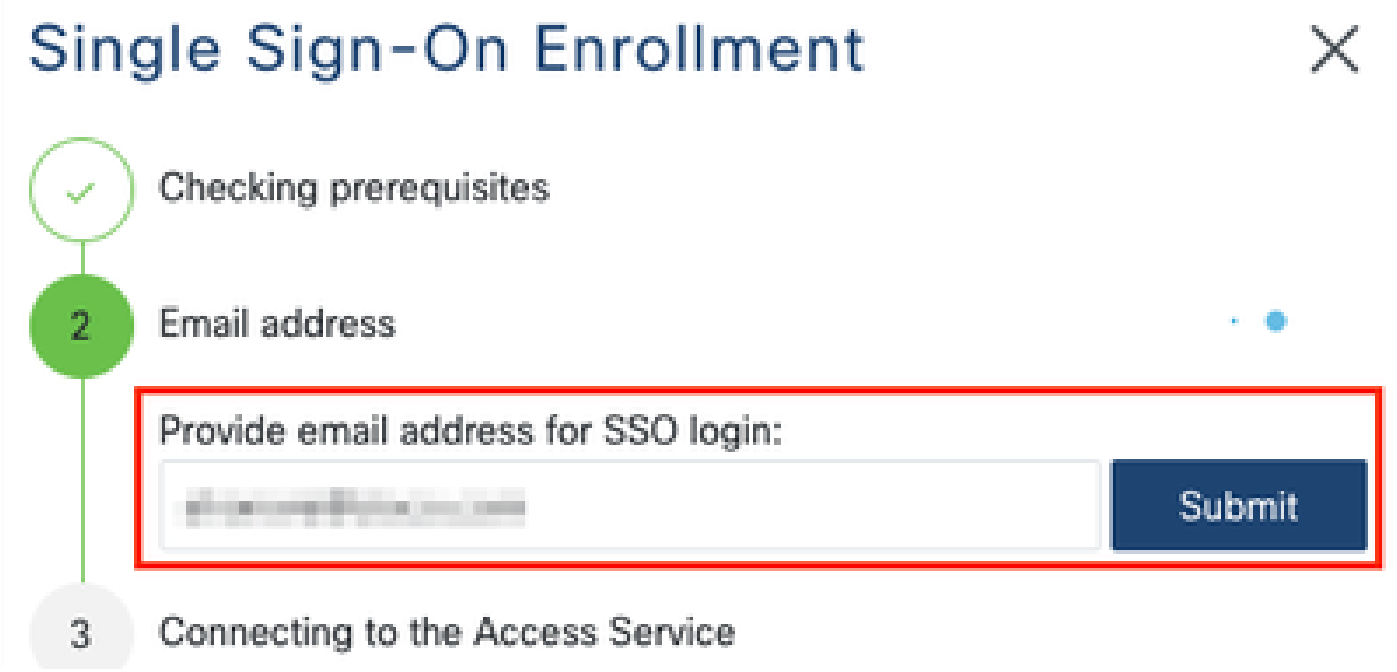


Falls Sie einen Proxy benötigen, um eine Verbindung zum Internet herzustellen, lesen Sie die detaillierte Setup-Anleitung hier: https://radkit.cisco.com/docs/pages/one_page_setup.html

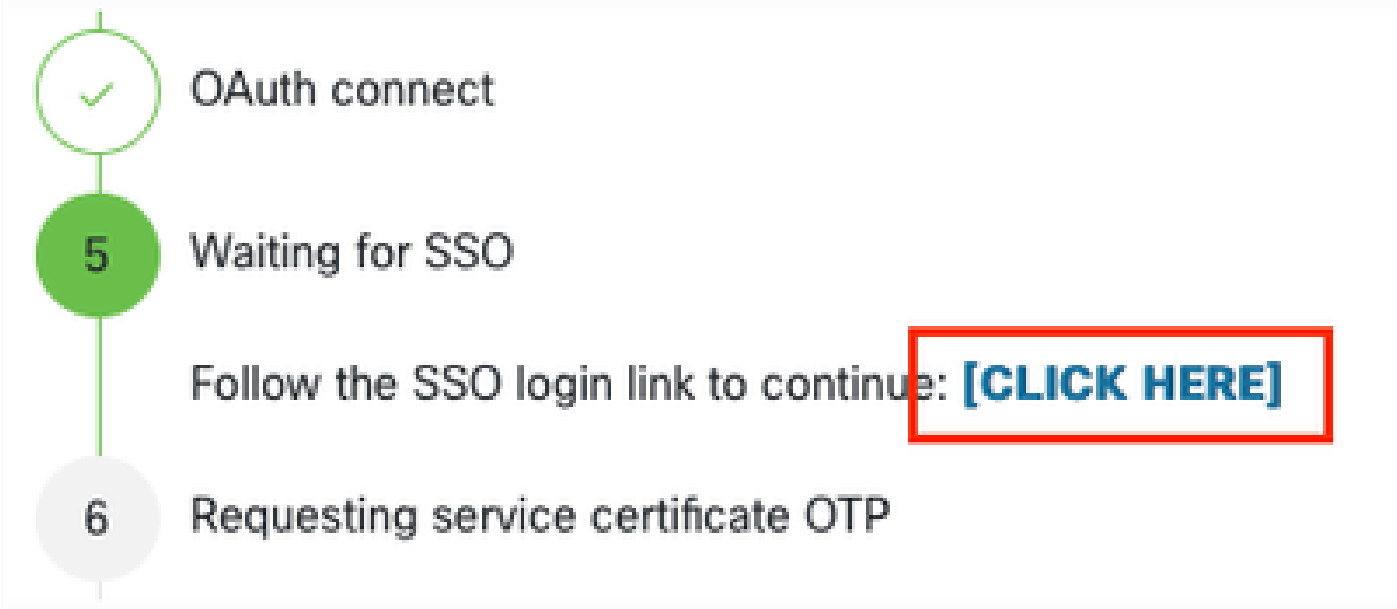
Jetzt müssen Sie den Service registrieren, damit er mit RADKit Cloud verbunden werden kann. Dazu melden Sie sich über die Service-WebUI mit Ihrem Cisco.com (CCO)-Konto an. Klicken Sie Enroll with SSO hier, um fortzufahren:



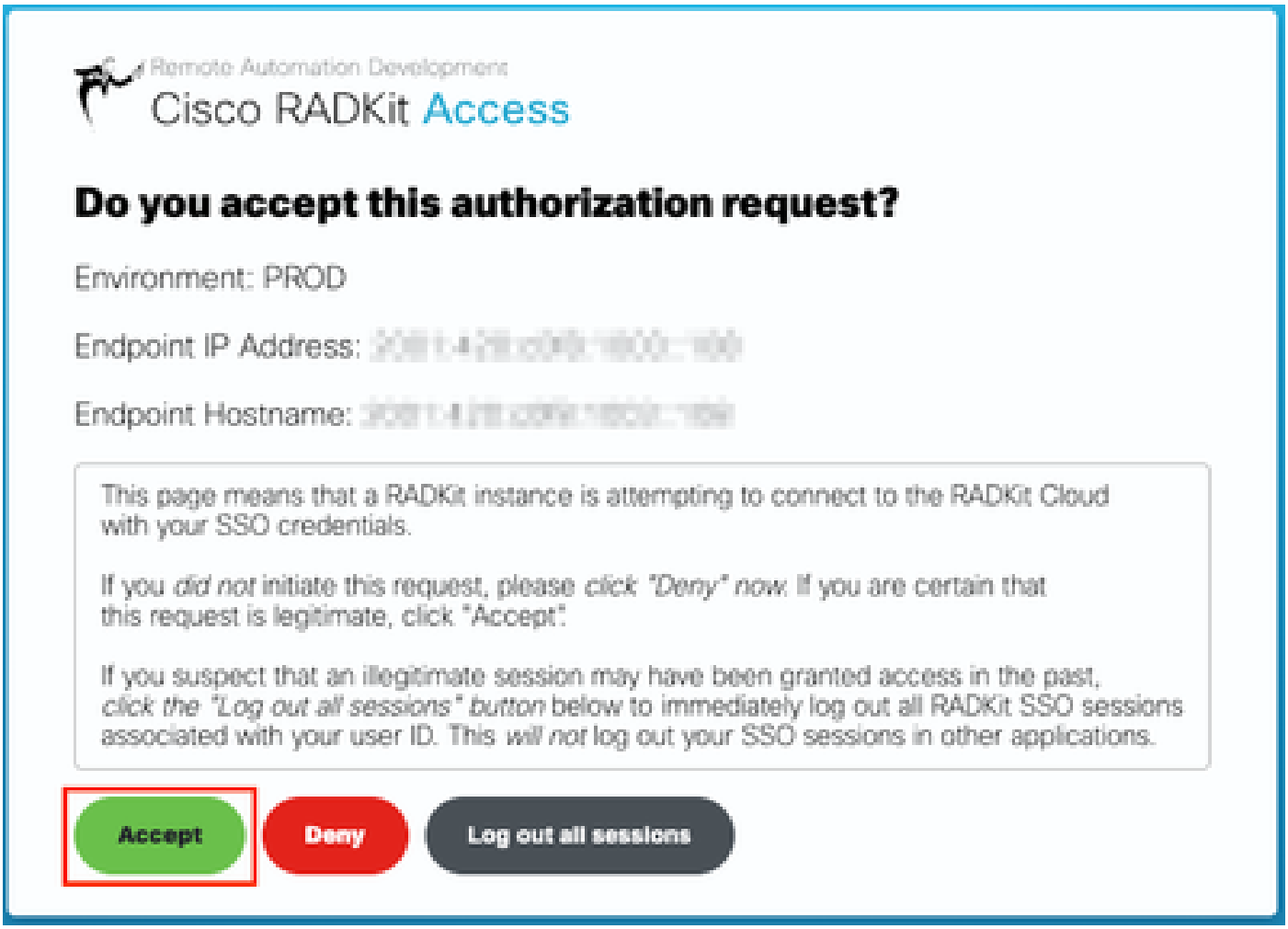
Geben Sie die E-Mail-Adresse für Ihr Cisco.com (CCO)-Konto in das E-Mail-Adressfeld in Schritt 2 ein, und klicken Sie auf Submit as shown in the image:



Nachdem der RADKit-Service zur Autorisierung eine Verbindung mit der RADKit-Cloud hergestellt hat, wird ein Link angezeigt, der Sie zur Authentifizierung zum Cisco SSO-Server führt[CLICK HERE]. Klicken Sie auf den Link, um fortzufahren. Er wird in einem neuen Browserfenster geöffnet. Stellen Sie sicher, dass Sie für die Anmeldung bei SSO dieselbe E-Mail-Adresse verwenden, die Sie bereits in dem oben genannten Schritt eingegeben haben:



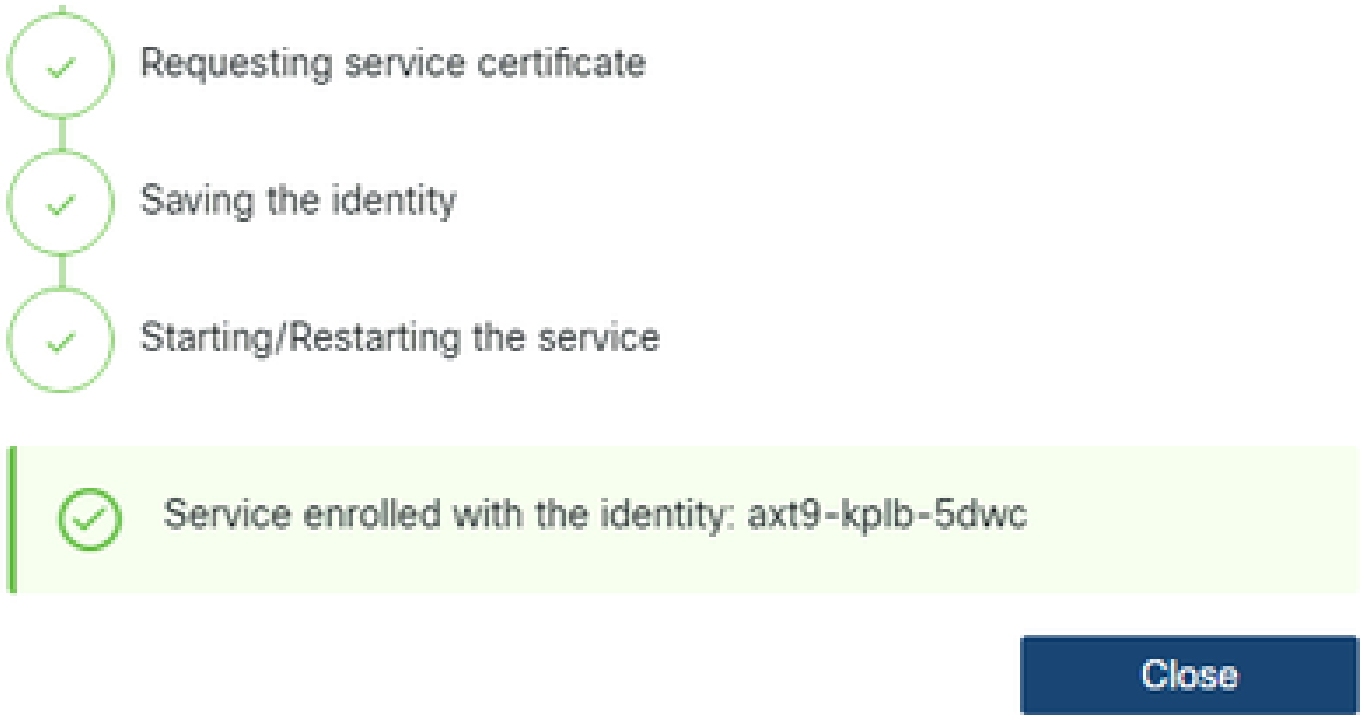
Nach Abschluss der SSO-Authentifizierung (oder sofort, falls Sie bereits authentifiziert waren) gelangen Sie auf eine RADKit-Zugangsbestätigungsseite. Lesen Sie die Informationen auf der Seite, und klicken Sie auf, Accept um den RADKit Service zu autorisieren, sich bei Ihrem CCO-Konto als Eigentümer anzumelden.



Sie gelangen dann zu einem Bildschirm, auf dem steht Authentication result: Success .

Klicken Sie nicht auf die Log out all sessions Schaltfläche, sondern schließen Sie einfach die Registerkarte/das Fenster SSO und kehren Sie zur RADKit Service WebUI zurück.

Dies zeigt Service enrolled with the identity: … . Die nachfolgende eindeutige Kennung ist Ihre RADKit-Service-ID, auch als Service-Seriennummer bezeichnet. Im Beispiel-Screenshot unterscheidet sich die Service-IDaxt9-kplb-5dwc von Ihrer.



Klicken Sie Close hier, um das Dialogfeld zu schließen und zum Bildschirm zurückzukehrenConnectivity.

Nach der Aktualisierung der WebUI wird Ihre Dienst-ID zusammen mit dem Verbindungsstatus wie hier dargestellt über der RADKit-GUI angezeigt:

Immer wenn ein TAC-Techniker auf eines der Geräte in Ihrer Umgebung zugreifen muss, benötigt er diese Service-ID, um Ihren RADKit-Service zu identifizieren.

Nachdem nun eine Verbindung mit der RADKit Cloud-Komponente hergestellt und dabei eine Service-ID generiert wurde, fügen Sie im nächsten Schritt die Geräte hinzu, die über RADKit erreicht werden können.

Schritt 4: Hinzufügen von Geräten und Endgeräten

In diesem Schritt fügen Sie die Geräte und ihre Anmeldeinformationen für die Geräte hinzu, auf die über RADKit zugegriffen werden kann. Für HyperFlex bedeutet dies, dass idealerweise diese Geräte und ihre Anmeldedaten hinzugefügt werden müssen:

"Slot0:"	Gerätetyp	Management-Protokolle	Anmeldeinformationen	Weitergeleitete TCP-Ports	Anmerkungen
Hypervisor (ESXi-Hosts)	Linux	Terminal (SSH)	Wurzel		

Storage-Controller (SCVM)	HyperFlex	Terminal (SSH)Swagger	Administrator root (enable)	443	Geben Sie das Root-Kennwort in das Feld enable password ein. Die wird verwendet, wenn ein Zustimmungstoke erforderlich ist. Fü Swagger: Deaktivieren Sie "TLS-Zertifikat überprüfen", und lassen Sie das Feld "Basis-URL" leer.
vCenter	Linux	Terminal (SSH)	Wurzel		
UCSM	Allgemein	Terminal (SSH)	Administrator		
Installationsprogramm (optional)	Linux	Terminal (SSH)	Wurzel	443	
CIMC (nur für Edge-Cluster)	Allgemein	Terminal (SSH)	Administrator		
Zeuge (nur für ausgedehnte Cluster)	Linux	Terminal (SSH)	Wurzel		
Intersight-CVA/PCA (optional)	Linux	Terminal (SSH)	Administrator	443	

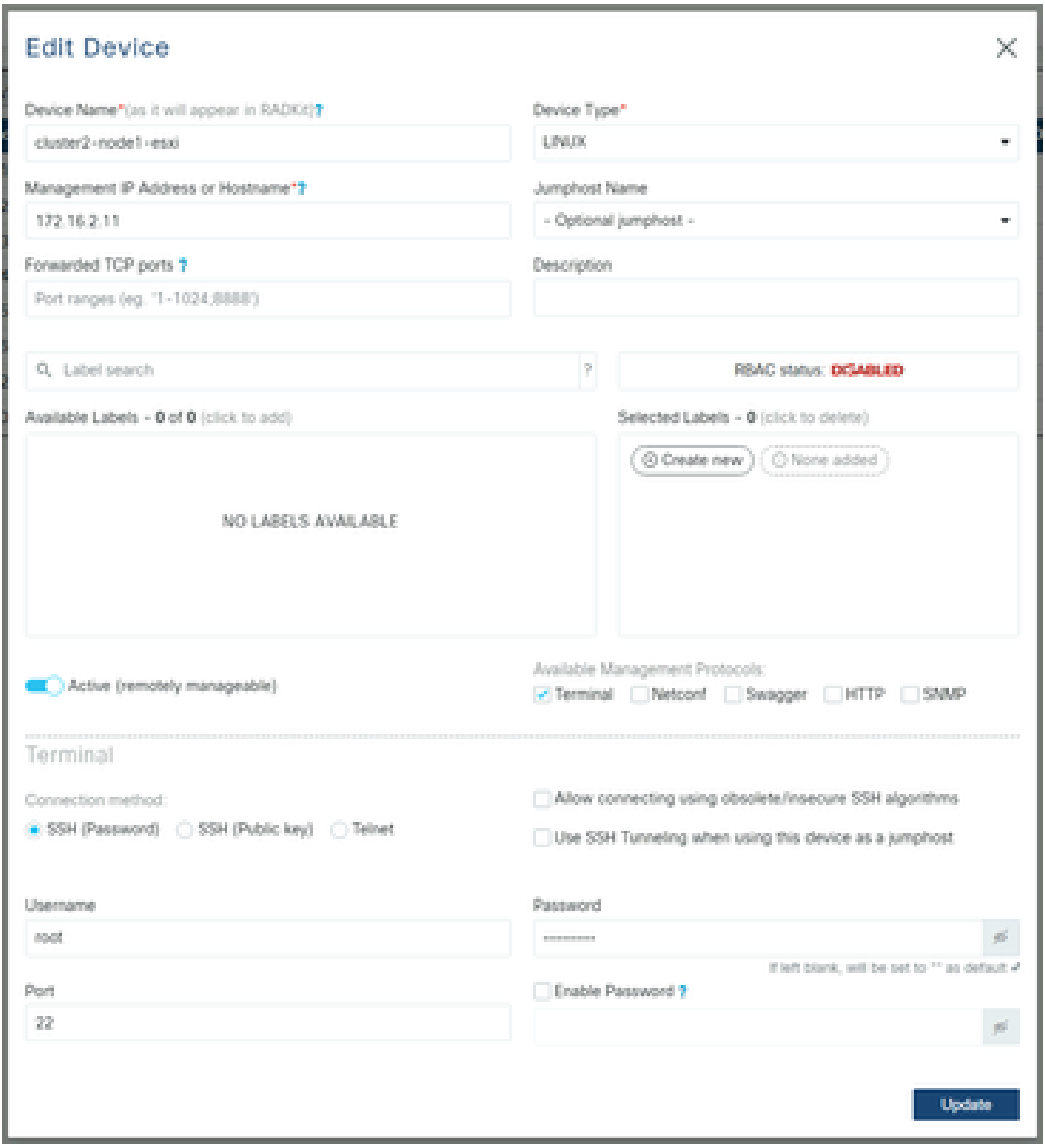
Es ist wichtig, die Geräte nur mit ihrer IP-Adresse und nicht mit ihrem Hostnamen hinzuzufügen, da dies erforderlich ist, um die Geräte zu verknüpfen, die zum gleichen Cluster gehören.

Um diese Geräte hinzuzufügen, navigieren Sie in der RADKit WebUI zum Bildschirm "Devices" (Geräte):

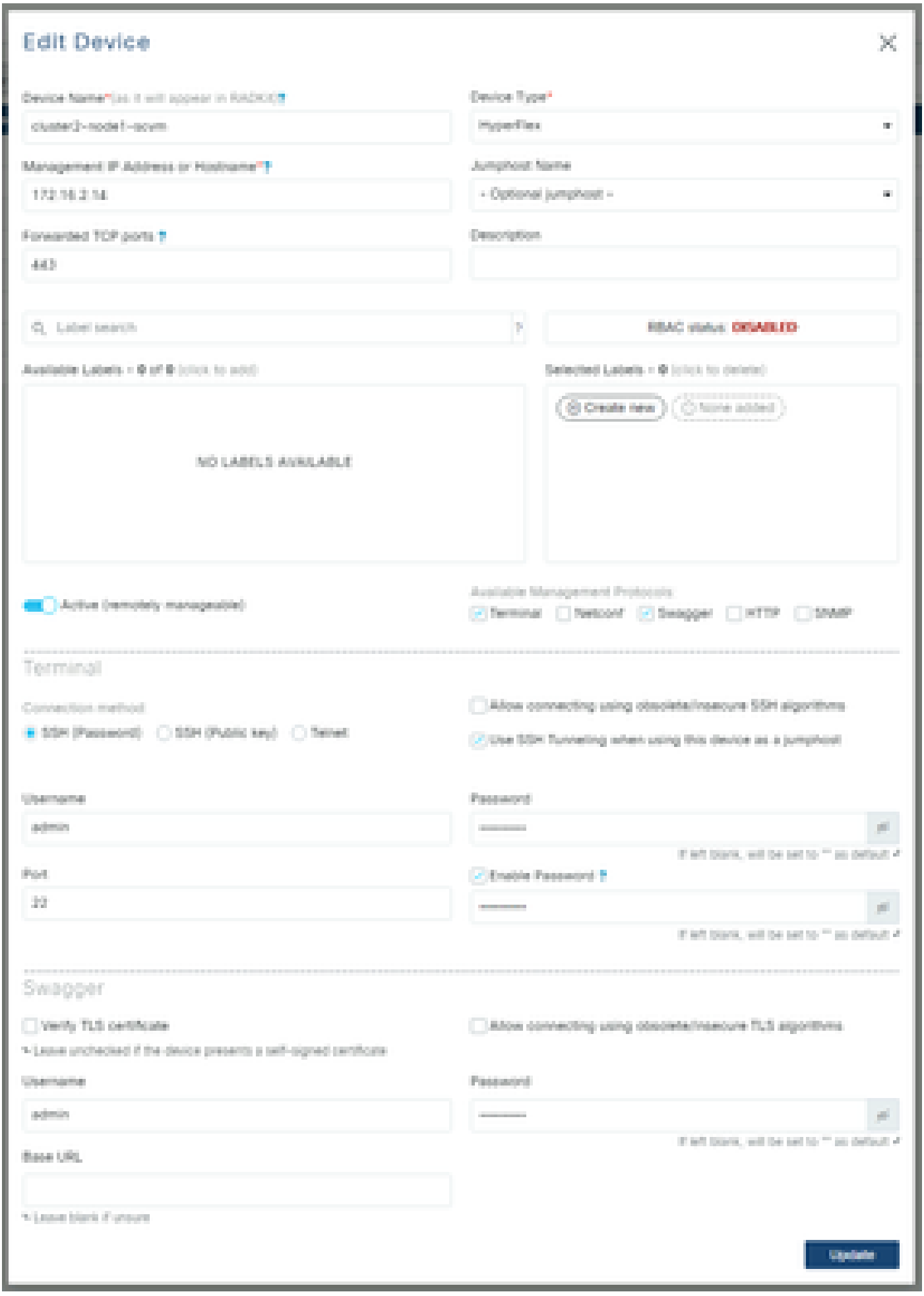
Erstellen Sie für jedes der oben aufgeführten Geräte einen neuen Eintrag, indem Sie auf klickenAdd Device. Geben Sie die IP-Adresse ein, wählen Sie den Gerätetyp aus, und geben Sie Details für alle Knoten in Ihrem Cluster an, je nach Gerätetyp. Wenn Sie fertig sind, klicken Sie auf, Add & closeum zum Bildschirm "Geräte" zurückzukehren oder Add & continue um ein weiteres Gerät hinzuzufügen.

Hier finden Sie Beispieleinträge und ihre Konfiguration für jeden Gerätetyp:

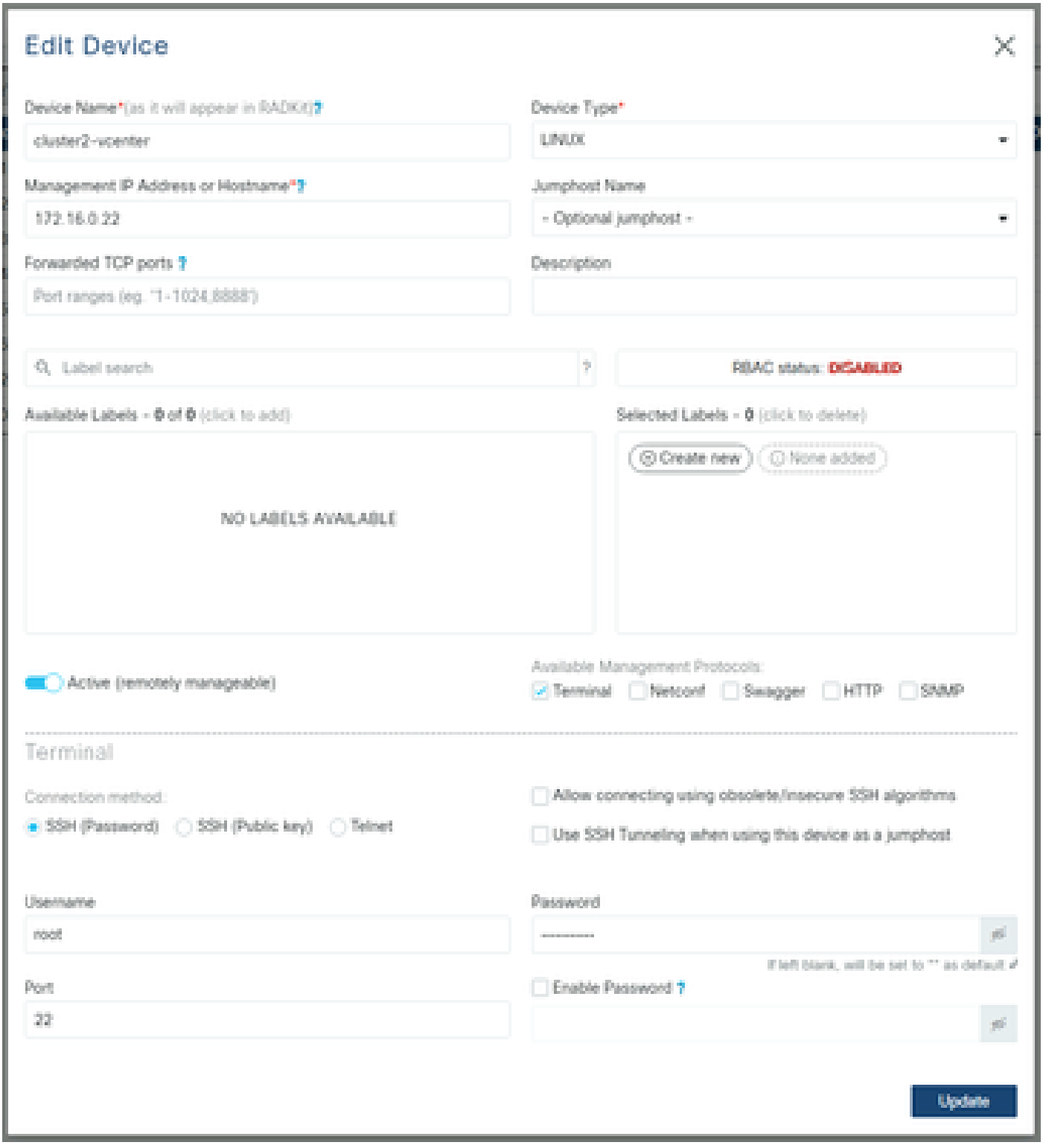
Beispiel für ESXi-Hosts:



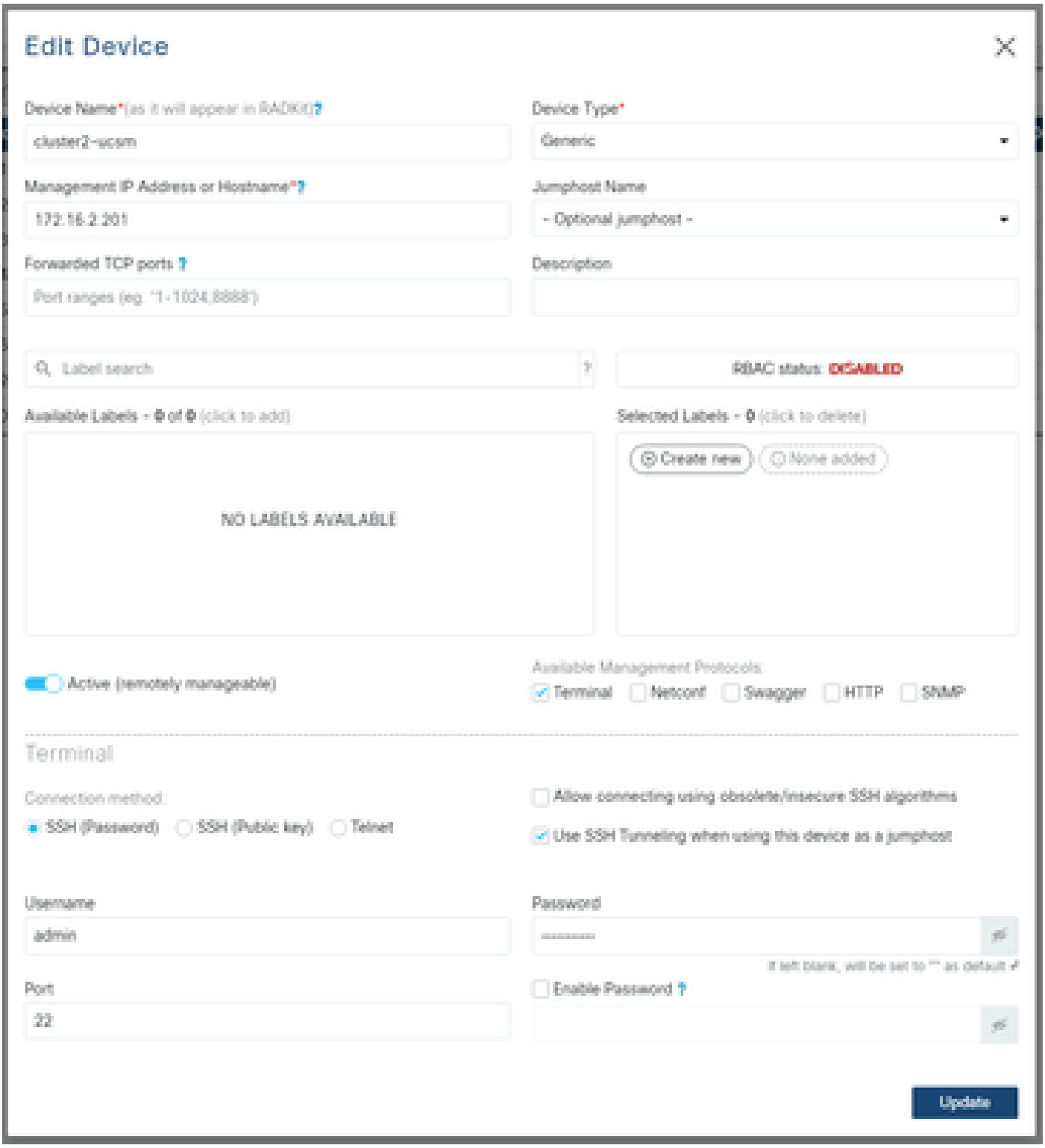
Beispiel für Speichercontroller:


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

Beispiel für vCenter:



Beispiel für UCSM:



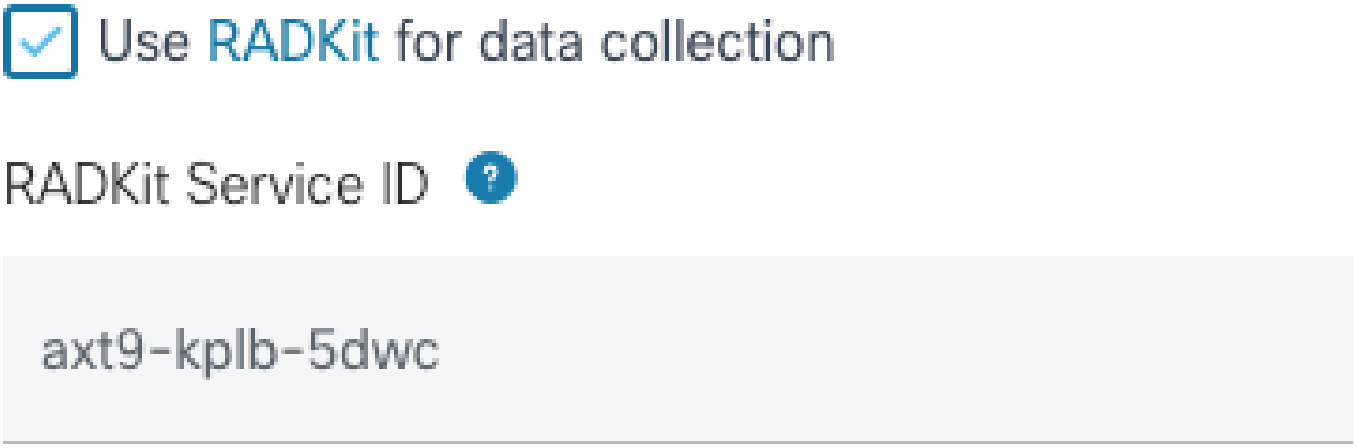
Verwenden von RADKit auf einem TAC-Serviceticket

Wenn die Vorbereitung abgeschlossen ist und Sie einem TAC-Techniker Zugriff auf Ihre Geräte gewähren möchten, können Sie diese Schritte durchführen.

Ein Techniker benötigt Ihre RADKit-Service-ID und Zugriff auf Ihre Umgebung oder ausgewählte Geräte (bei Verwendung von RBAC) für die erforderliche Zeit.

1. RADKit-Dienst-ID bereitstellen

Wenn Sie noch kein TAC-Ticket erstellt haben, können Sie dies im Support Case Manager unter Cisco.com erwähnenUse RADKit for data collection:

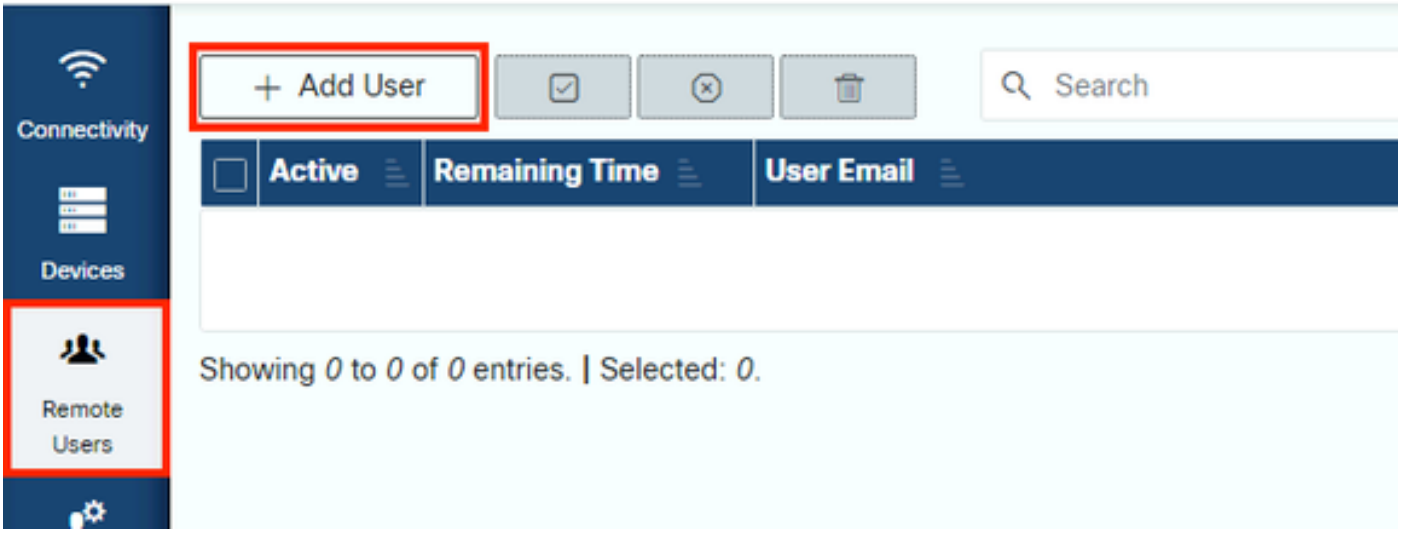


Falls Sie bereits eine offene Serviceanfrage haben, können Sie die RADKit-Service-ID im Support Case Manager im Abschnitt mit den Kundenkontaktdaten hinzufügen:

Oder geben Sie einfach Ihre ID an den TAC-Techniker weiter, der an Ihrem Fall arbeitet.

2. Remote-Benutzer hinzufügen

Bevor ein Benutzer mit Ihren Geräten arbeiten kann, müssen Sie expliziten Zugriff bereitstellen und einen Zeitrahmen konfigurieren, für den dieser Zugriff gültig bleibt. Navigieren Sie dazu in der RADKit-Webbenutzeroberfläche zum Bildschirm, und erstellen Sie einen neuen Remote-Benutzer, indem Sie auf denRemote Users Link klicken. Add User.



Geben Sie die E-Mail-Adresse des TAC-Technikers (@cisco.com) ein (gehen Sie vorsichtig vor Tippfehler vor). Achten Sie auf das Activate this user Kontrollkästchen und die Time sliceoder Manual Einstellungen.

Während der Benutzer aktiv ist, hat er über den RADKit-Service Zugriff auf die konfigurierten Geräte, sofern diese Geräte aktiviert sind und die RBAC-Richtlinie dies zulässt.

Der Zeitabschnitt stellt den Zeitraum dar, nach dem der Benutzer automatisch deaktiviert wird, d. h. ein Zeitabschnitt stellt eine zeitgebundene Fehlerbehebungssitzung dar. Die Sitzung des Benutzers kann bis zur Dauer des Zeitabschnitts für diesen Benutzer verlängert werden. Wenn Sie Benutzer lieber manuell aktivieren/deaktivieren möchten, wählen Sie stattdessen die OptionManual.

Benutzer können immer manuell aktiviert/deaktiviert werden, unabhängig davon, ob sie einen Zeitabschnitt konfiguriert haben oder nicht. Wenn ein Benutzer deaktiviert wird, werden alle Sitzungen über den RADKit-Dienst sofort getrennt.

Wenn Sie fertig sind, klicken Sie auf Add & close, um zum Bildschirm "Remote Users" zurückzukehren.

Zugehörige Informationen

- Weitere Informationen und Antworten auf häufige Fragen finden Sie auf der Website von RADKit: https://radkit.cisco.com/
- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.