Configurazione di RADKit per la risoluzione remota dei problemi su HyperFlex

Sommario

Introduzione

Questo documento descrive come iniziare e preparare un ambiente RADKit per la risoluzione dei problemi remota di un ambiente Cisco HyperFlex.

Premesse

Lo scopo principale di questo documento è spiegare come preparare l'ambiente per l'utilizzo da parte di TAC per utilizzare RADKit per la risoluzione dei problemi.

Cos'è RADKit?

RADKit è un orchestrator a livello di rete. Trasforma in modo radicale il modo con cui indirizzare le apparecchiature, potenzia i servizi Cisco ed espande la capacità.

Ulteriori informazioni su RADKit sono disponibili all'indirizzo: https://radkit.cisco.com/

Perché scegliere RADKit per HX?

Cisco HyperFlex è costituito da diversi componenti: interconnessioni fabric, server UCS, ESXi, vCenter e SCVM. In molti casi, le informazioni provenienti da dispositivi diversi devono essere raccolte e correlate. Anche se la risoluzione dei problemi può richiedere nuove informazioni nel tempo e questa operazione in una (lunga) sessione WebEx o recuperando (grandi) pacchetti di supporto tramite Intersight non è sempre il modo più efficace. Utilizzando RADKit, un tecnico TAC può richiedere le informazioni richieste durante il processo di risoluzione dei problemi, dai vari dispositivi e servizi, in modo sicuro e controllato.

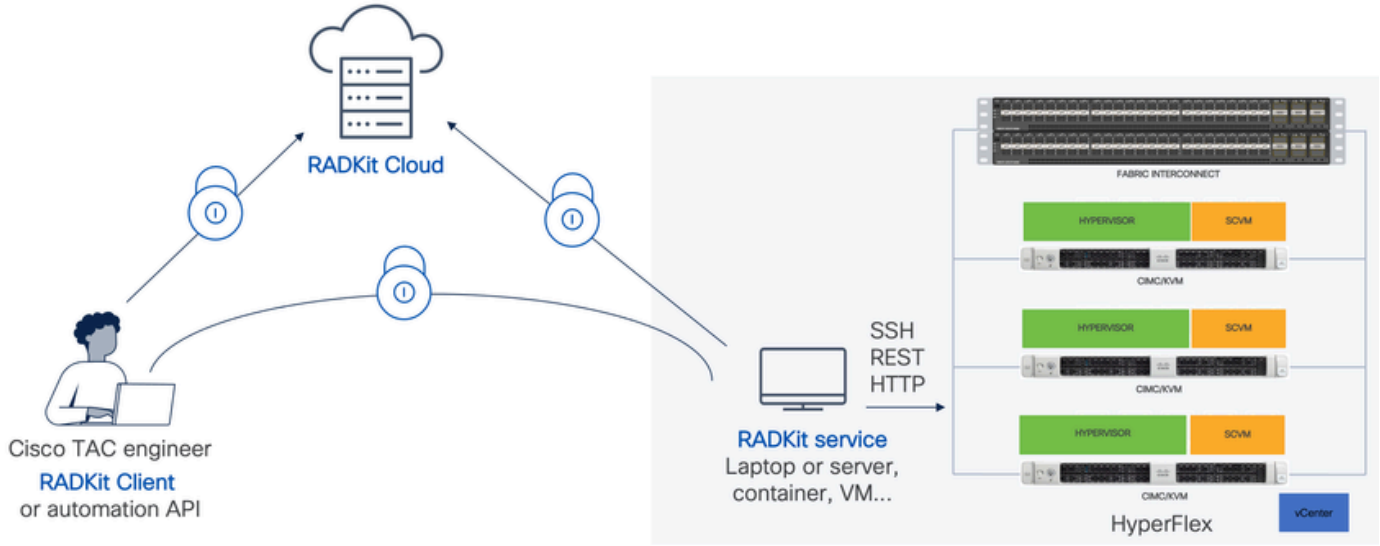
RADKit vs. Intersight

Intersight rimane il metodo di connettività principale per i cluster HyperFlex, fornendo numerosi vantaggi, quali la raccolta automatica dei registri, la telemetria e il monitoraggio proattivo dell'ambiente per l'hardware e altri avvisi noti.

Sebbene molti cluster HX siano connessi a Intersight, Intersight è attualmente destinato principalmente all'installazione, alla manutenzione e al monitoraggio dei cluster HyperFlex. Intersight consente di raccogliere pacchetti di supporto e informazioni di telemetria, che in genere rappresentano un buon punto di partenza per la risoluzione dei problemi. Per la risoluzione dei problemi in tempo reale, in uno scenario classico in cui un tecnico TAC utilizza una sessione WebEx, viene implementato RADKit. Non sostituisce Intersight, ma aggiunge un approccio diverso alla risoluzione dei problemi, utilizzando una sessione interattiva o utilizzando sequenze di richiesta-risposta programmatiche.

Panoramica di alto livello

Diagramma connettività



Componenti

- Servizio RADKit: componente del servizio RADkit in sede, utilizzato come gateway sicuro per l'ambiente HX. In qualità di cliente, l'utente mantiene il controllo completo su quali dispositivi sono accessibili e chi può accedervi in quale momento. Questo servizio può essere ospitato su qualsiasi computer Linux, MacOS o Windows.
- Client RADKit: front-end utilizzato dal tecnico TAC per accedere all'ambiente, tramite la risoluzione dei problemi e il monitoraggio a livello di programmazione, il recupero automatico e l'analisi degli output dei dispositivi tramite strumenti interni Cisco o l'interazione diretta con i dispositivi tramite CLI.
- RADKit Cloud: fornisce un trasporto sicuro tra il client e il servizio.

Preparazione

Panoramica delle operazioni da eseguire

Questi passaggi sono necessari prima che un tecnico TAC possa utilizzare RADKit per connettere e risolvere i problemi dell'ambiente HX:

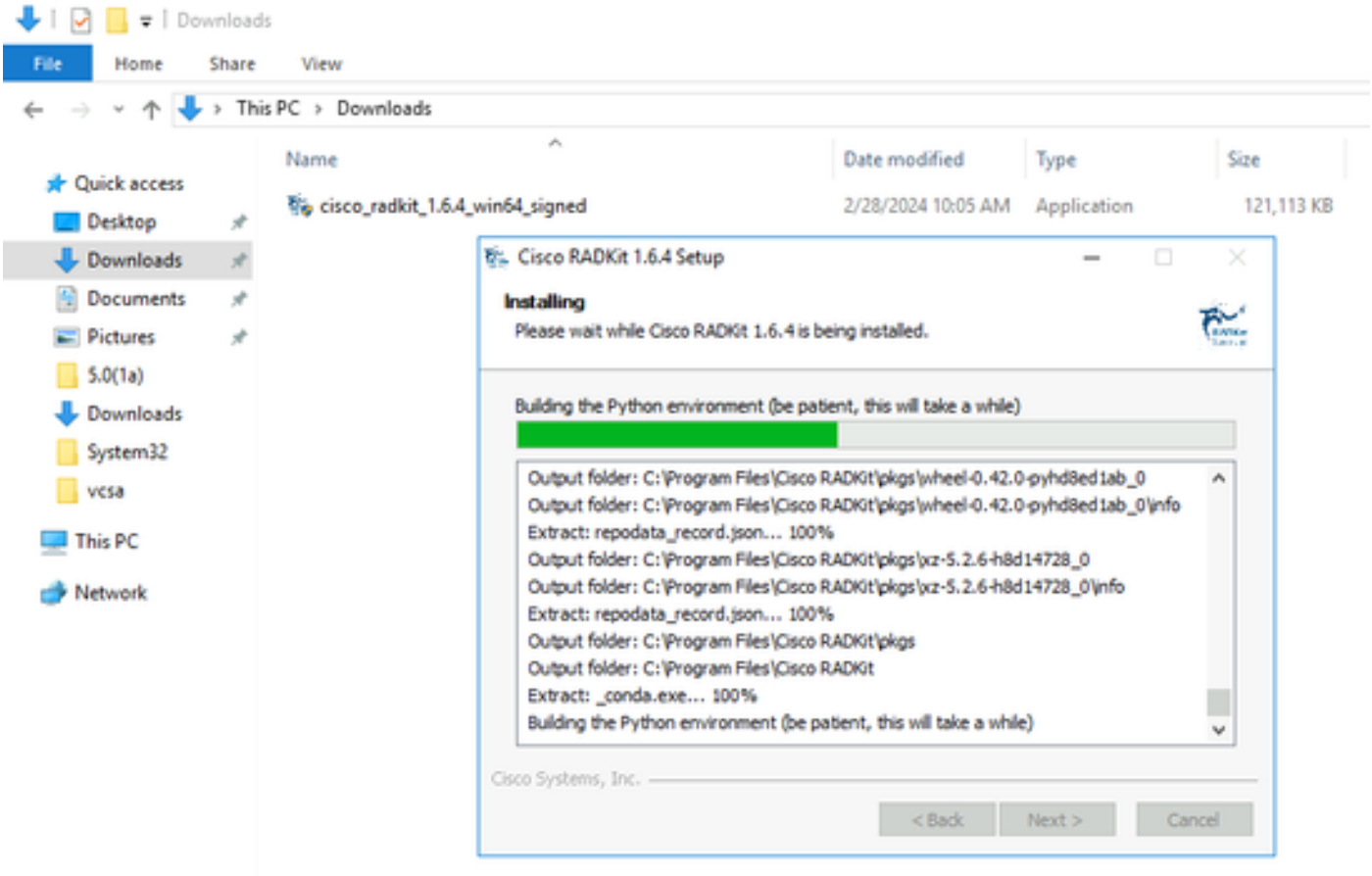
1. Scaricare e installare il servizio RADkit. Può essere installato su qualsiasi computer Linux, MacOS o Windows.
2. Avviare il servizio RADKit ed eseguire la configurazione iniziale (bootstrap). Creare un account di amministratore privilegiato per gestire ulteriormente il servizio RADKit tramite un'interfaccia Web.
3. Registra il servizio RADKit con il cloud RADKit. Registrare il servizio RADKit con il cloud RADKit e generare un ID servizio per identificare l'ambiente.
4. Aggiungere dispositivi ed endpoint. Fornire un elenco di dispositivi e archiviare le credenziali per i dispositivi a cui potrebbe essere necessario accedere.

Una spiegazione più dettagliata/generica di questi passaggi è disponibile qui: https://radkit.cisco.com/docs/pages/one_page_setup.html

Passaggio 1. Scarica e installa il servizio RADKit

I dettagli in questo passaggio possono essere leggermente diversi, a seconda del sistema operativo utilizzato per installare il servizio RADKit, ma in generale, il processo è molto simile. Scaricare l'ultima release del sistema operativo da qui: https://radkit.cisco.com/downloads/release/.

Eseguire il programma di installazione del sistema e seguire le istruzioni fino al completamento dell'installazione:



Una volta installati tutti i componenti RADKit, è possibile passare alla fase successiva in cui si esegue la configurazione iniziale.

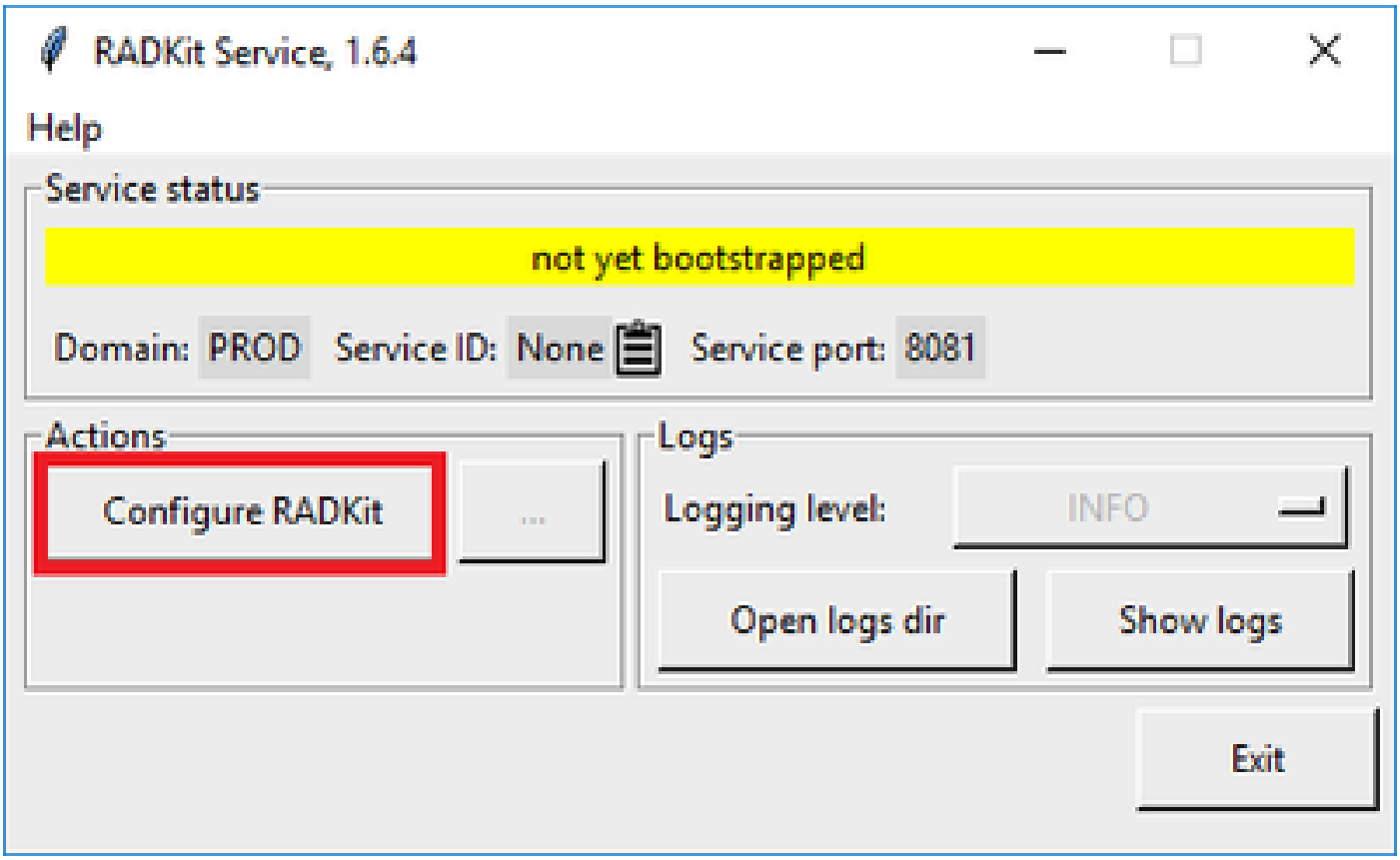
Passaggio 2. Avviare il servizio RADKit ed eseguire la configurazione iniziale (bootstrap)

In questo passaggio, creare un account superadmin per gestire ulteriormente il servizio RADKit tramite un'interfaccia Web.

Individuare e avviare il menu Start (in Windows) o la cartella Applicazioni (in macOS)RADKit Service:

La prima volta che viene avviato, l'avvio del servizio RADKit può richiedere qualche istante (da 10 a 30 secondi a seconda della velocità del sistema). Le esecuzioni successive saranno molto più veloci.

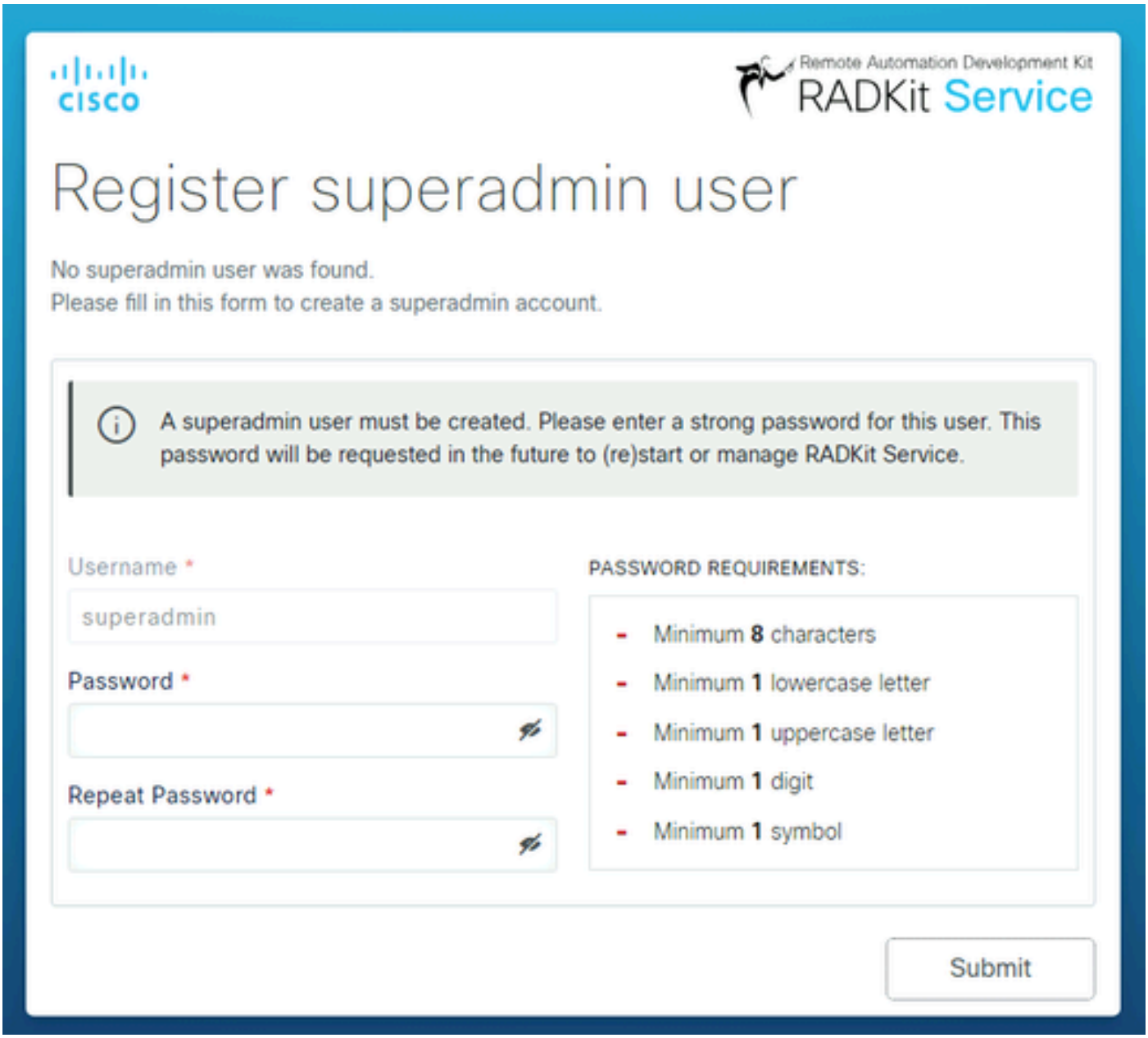
Al termine dell'avvio, nella finestra di dialogo del servizio RADKit, quando lo stato cambia in not yet bootstrapped premereConfigure RADKit:



In questo modo si apre il browser Web e si accede al servizio RADKit WebUI, un'interfaccia di gestione basata sul Web che consente di gestire il servizio RADKit.

Quando ci si connette a questo URL con un certificato autofirmato, è previsto un avviso di certificato che è possibile ignorare.

Poiché non esiste ancora un utente superadmin, WebUI richiederà di creare una password per questo utente:



Selezionare una password conforme ai requisiti di complessità della password visualizzati a destra.

La password di questo account verrà utilizzata per proteggere segreti come le chiavi private e le credenziali del dispositivo. Se la si perde, tutti i segreti andranno persi e il servizio RADKit dovrà essere reinizializzato, quindi sceglierla con attenzione e annotarla in un percorso sicuro. Può essere modificato in un secondo momento, se necessario.

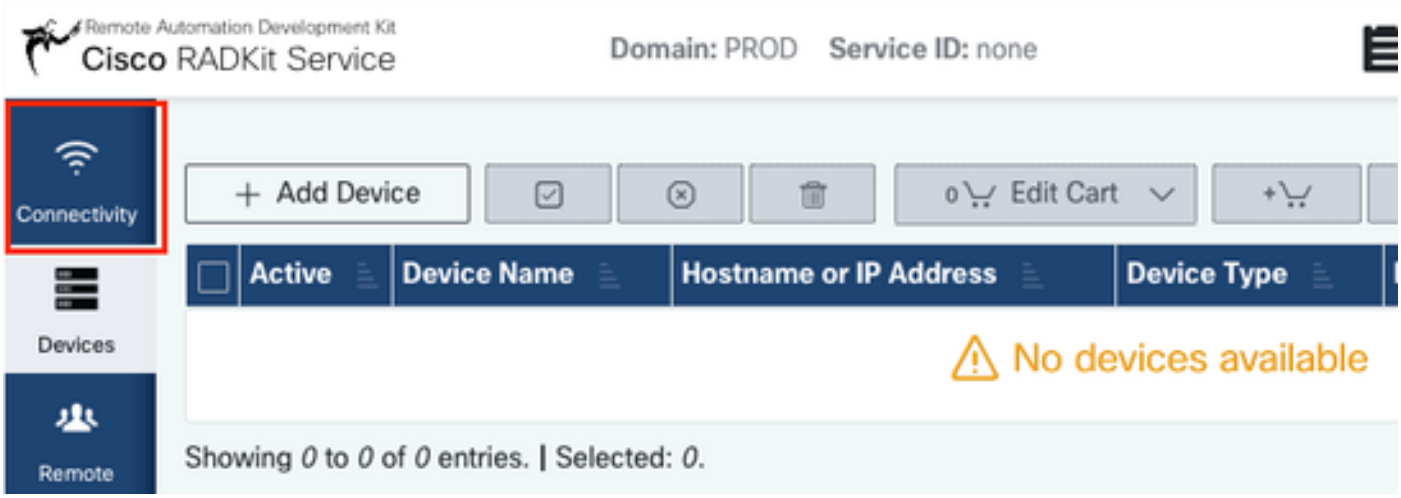
Dopo aver creato l'account superadmin, utilizzarlo per accedere a WebUI:

Dopo aver creato l'account superadmin e aver eseguito correttamente l'accesso a WebUI, è possibile continuare con il passaggio successivo in cui il servizio RADKit è registrato con il componente cloud RADKit.

Passaggio 3. Registra il servizio RADKit con RADKit Cloud

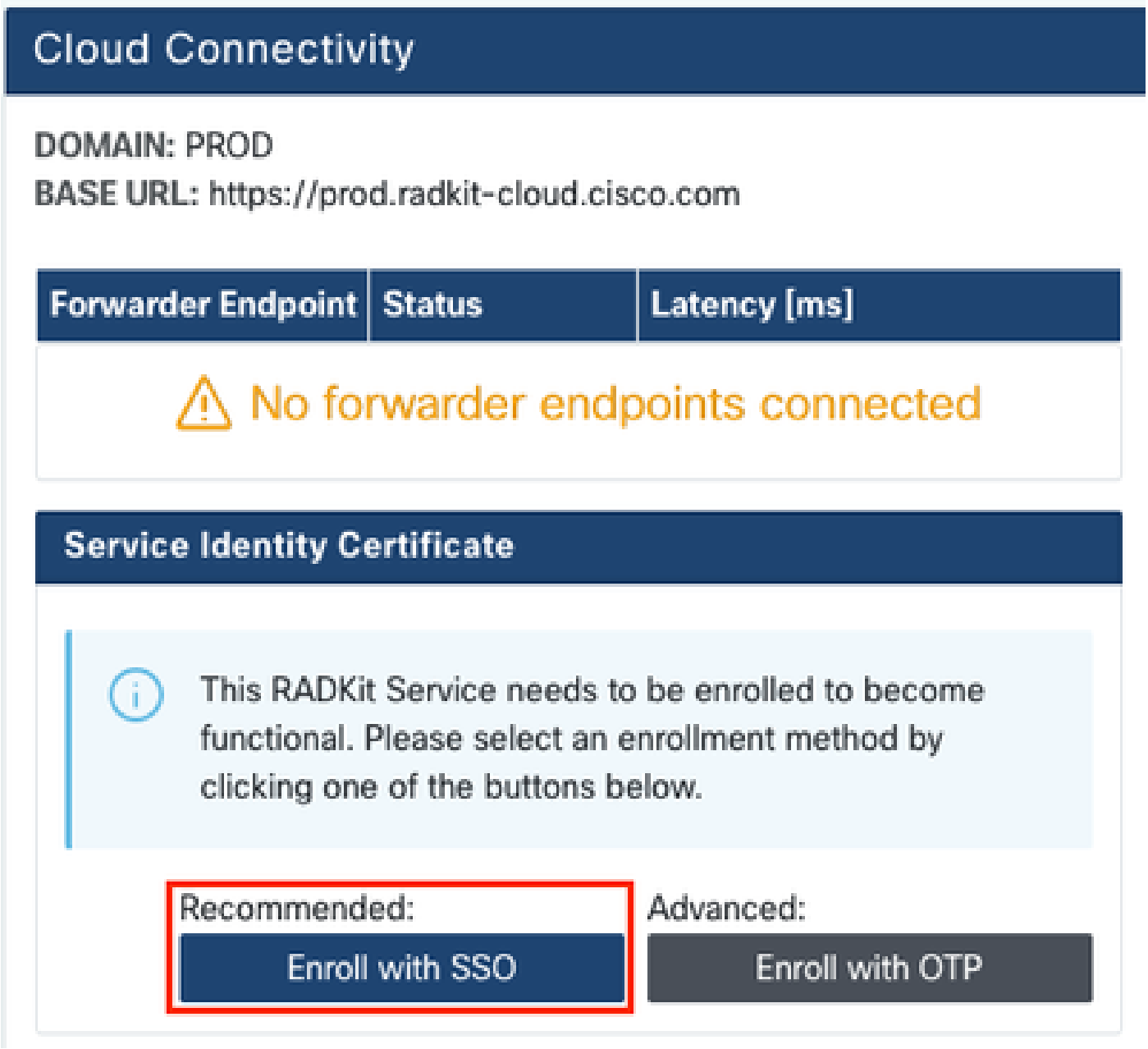
In questo passaggio, registrare il servizio RADKit con il cloud RADKit e generare un ID servizio per identificare l'ambiente.

Dopo aver effettuato l'accesso a WebUI con l'utente superadmin (vedere il passaggio 2), passare alla schermata di connettività:

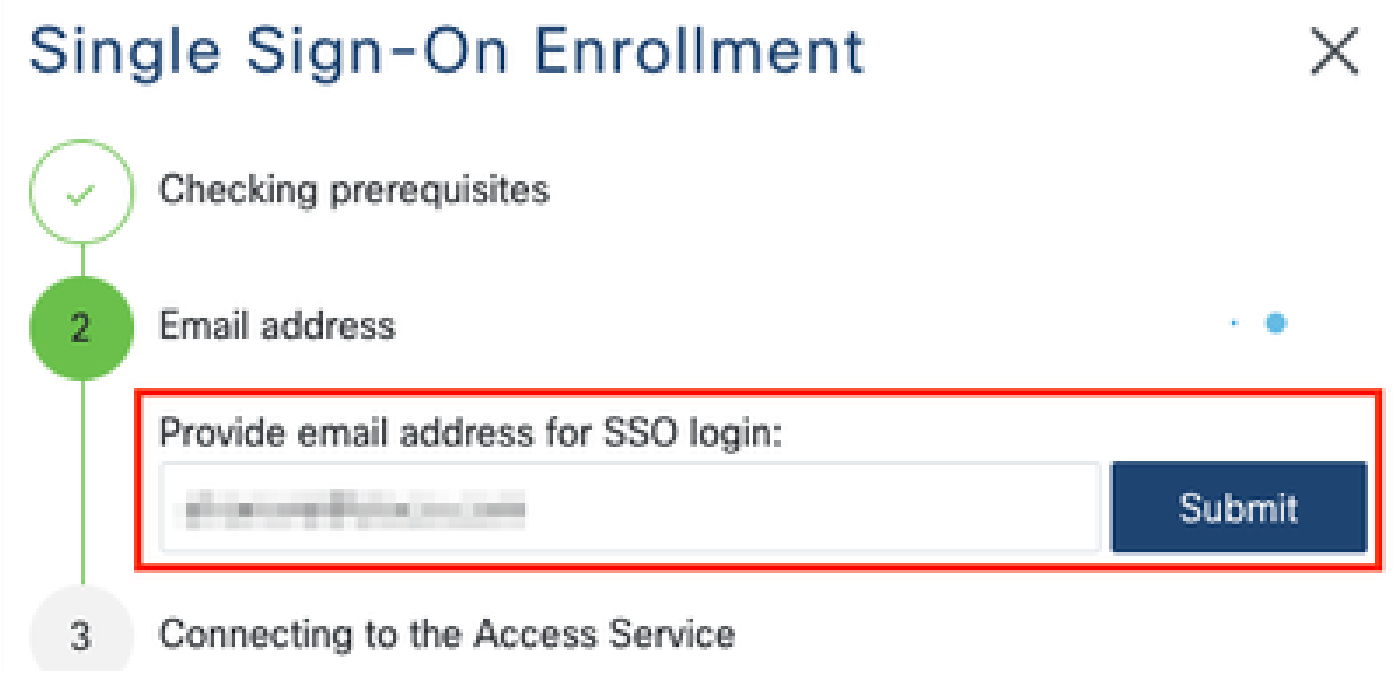


Se è necessario un proxy per la connessione a Internet, fare riferimento alle istruzioni di configurazione dettagliate disponibili qui: https://radkit.cisco.com/docs/pages/one_page_setup.html

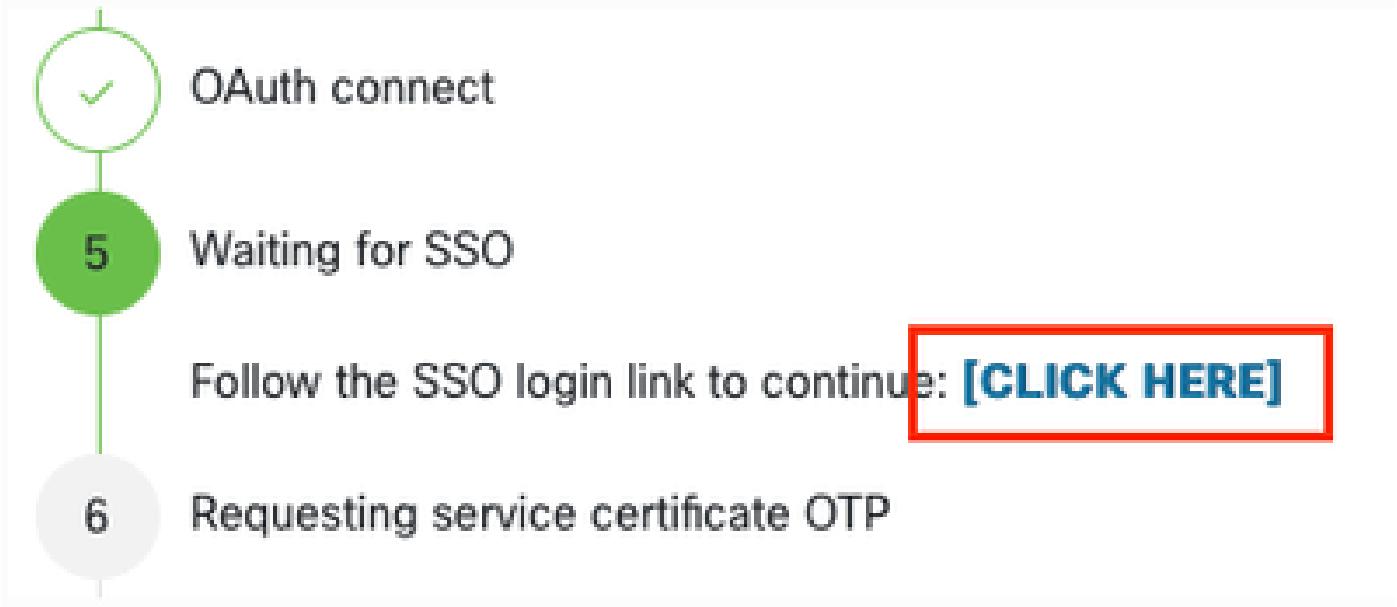
Ora è necessario registrare il Servizio per consentirne la connessione al cloud RADKit. Per eseguire questa operazione, accedere tramite Service WebUI utilizzando l'account Cisco.com (CCO). Fare clic perEnroll with SSO continuare:



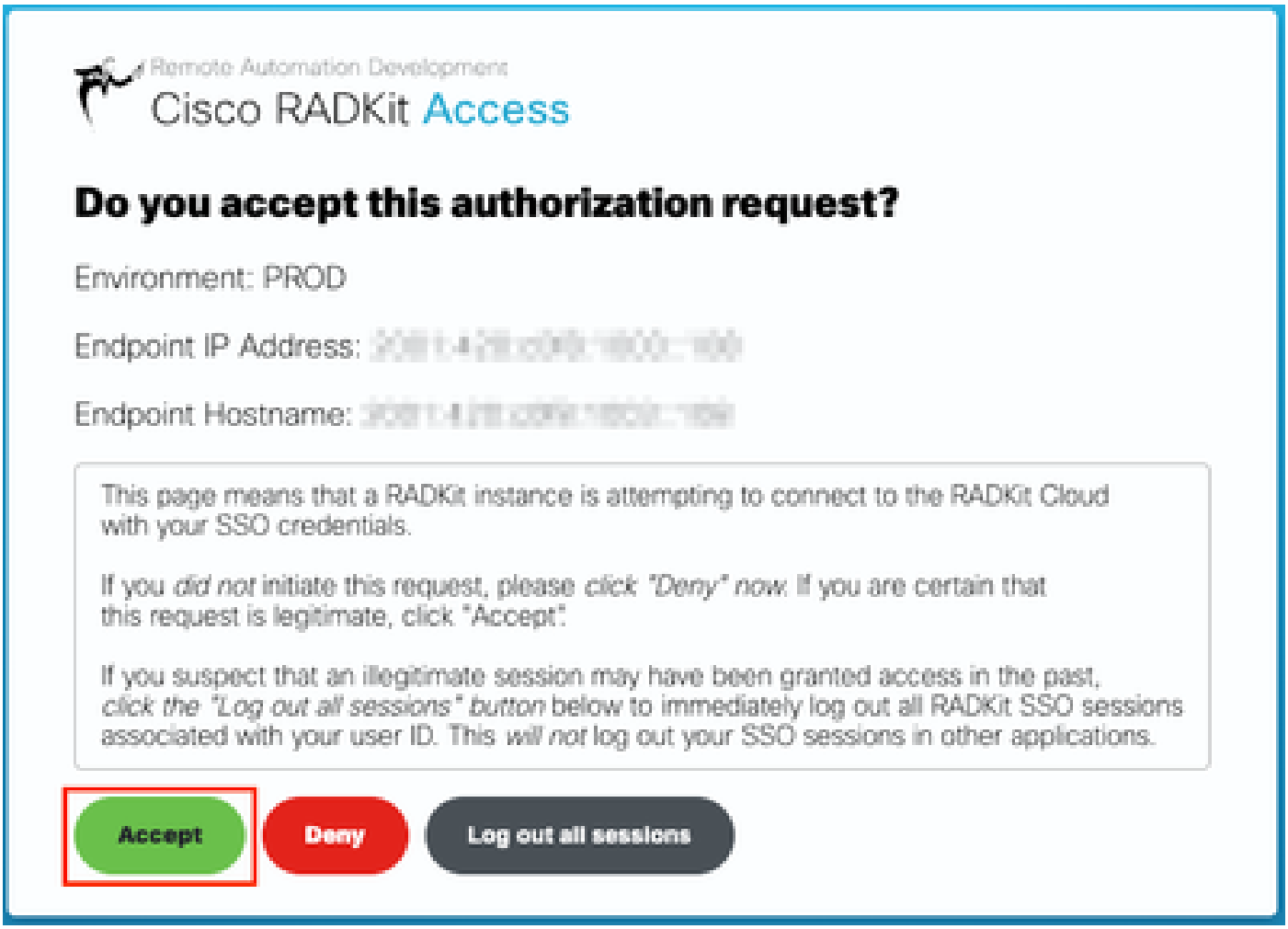
Immettere l'indirizzo di posta elettronica corrispondente al proprio account Cisco.com (CCO) nel campo dell'indirizzo di posta elettronica nel passaggio 2. e fare clic su Submit as shown in the image:



Dopo la connessione del servizio RADKit al cloud RADKit per l'autorizzazione, viene visualizzato un [CLICK HERE] collegamento che consente di connettersi al server Cisco SSO per l'autenticazione. Fare clic sul collegamento per continuare. Verrà aperto in una nuova scheda/finestra del browser. Assicurarsi di utilizzare lo stesso indirizzo e-mail per accedere a SSO, come quello immesso nel passaggio indicato in precedenza:



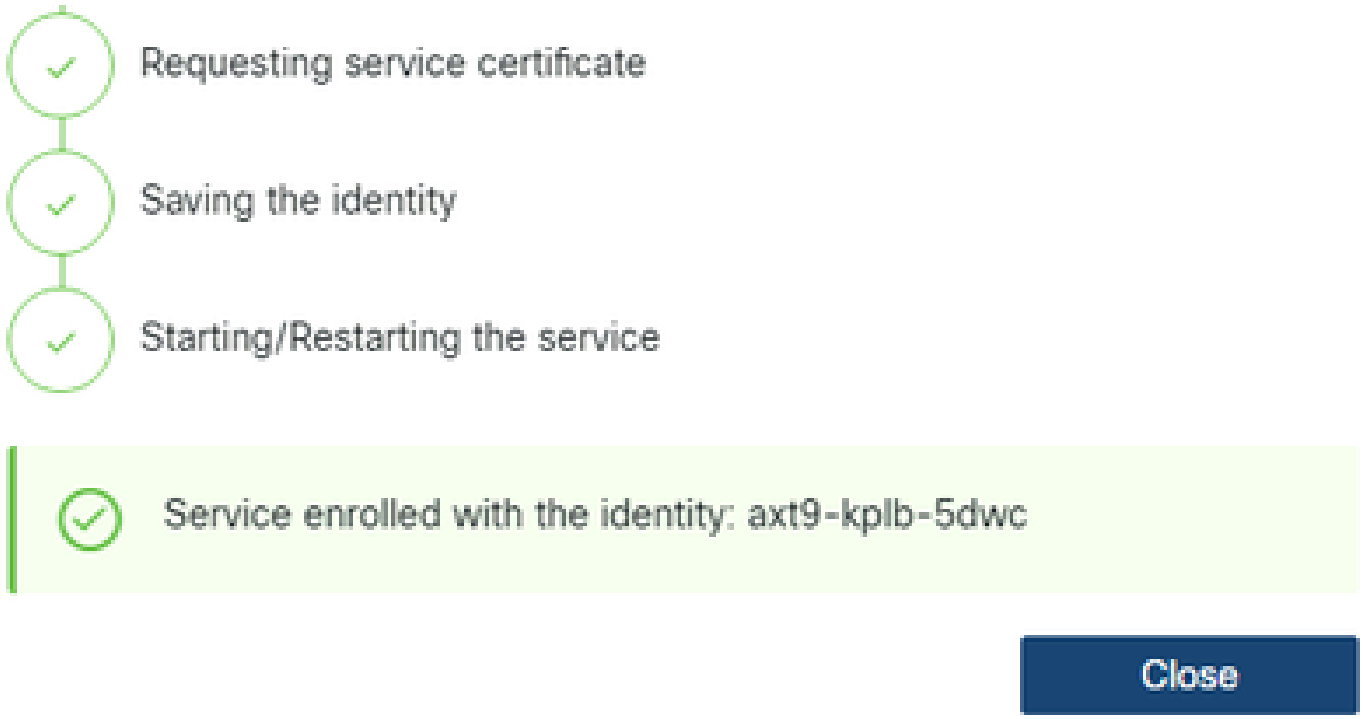
Al termine dell'autenticazione SSO (o immediatamente, se l'utente è già stato autenticato) viene visualizzata una pagina di conferma di accesso RADKit. Leggere le informazioni contenute nella pagina e fare clic su Accept per autorizzare il servizio RADKit a registrarsi con l'account CCO come proprietario.



Poi si arriva a uno schermo che dice Authentication result: Success .

Non fare clic sul Log out all sessions pulsante, ma chiudere semplicemente la scheda/finestra SSO e tornare alla WebUI del servizio RADKit.

Questo mostra Service enrolled with the identity: … . L'identificatore univoco che segue è l'ID servizio RADKit, noto anche come numero di serie del servizio. Nella schermata di esempio, l'ID del servizio è il tuoaxt9-kplb-5dwc sarà diverso.



Fare clic su Close per chiudere la finestra di dialogo e tornare alla Connectivity schermata.

Dopo l'aggiornamento di WebUI, l'ID servizio viene visualizzato nella parte superiore dell'interfaccia grafica di RADKit, insieme allo stato della connettività, come mostrato di seguito:

Ogni volta che un tecnico TAC deve accedere a uno dei dispositivi dell'ambiente, richiede questo ID servizio per identificare il servizio RADKit.

Ora che è stata stabilita una connettività con il componente cloud RADKit e generato un ID di servizio durante l'operazione, nel passaggio successivo aggiungere i dispositivi che possono essere raggiunti tramite RADKit.

Passaggio 4. Aggiungi dispositivi ed endpoint

In questo passaggio, aggiungere i dispositivi e le relative credenziali per i dispositivi a cui è possibile accedere tramite RADKit. Per HyperFlex, questo significa che idealmente, questi dispositivi e le loro credenziali devono essere aggiunti:

Sul dispositivo bootflash o slot0:	Tipo di dispositivo	Protocolli di gestione	Credenziali	Porte TCP inoltrate	Osservazioni
Hypervisor	Linux	Terminale	radice		

(host ESXi)		(SSH)			
Controller di archiviazione (SCVM)	HyperFlex	Swagger Terminal (SSH)	admin radice (attiva)	443	Immettere la password di root nel campo enable password. Verrà utilizzato quando è necessario un token di consenso. Per Swagger: deselezionare Verifica certificato TLS e lasciare vuoto il campo URL di base
vCenter	Linux	Terminale (SSH)	radice		
UCSM	Generico	Terminale (SSH)	admin		
Programma di installazione (facoltativo)	Linux	Terminale (SSH)	radice	443	
CIMC (solo per i cluster edge)	Generico	Terminale (SSH)	admin		
Controllo (solo per cluster estesi)	Linux	Terminale (SSH)	radice		
Intersight CVA/PCA (opzionale)	Linux	Terminale (SSH)	admin	443	

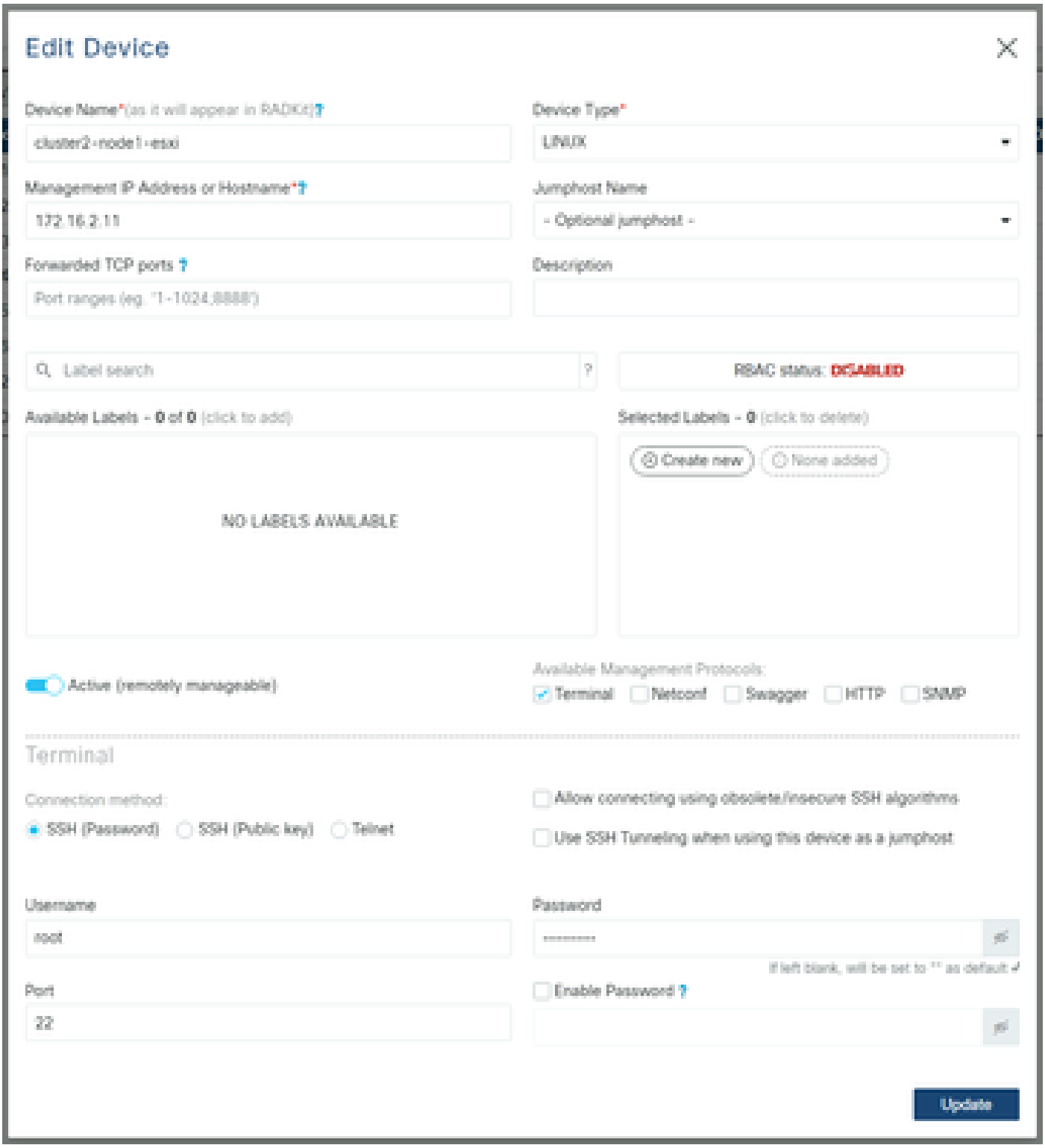
È importante aggiungere i dispositivi solo utilizzando il relativo indirizzo IP e non il nome host, in quanto questo è necessario per correlare i dispositivi che appartengono allo stesso cluster.

Per aggiungere questi dispositivi, in RADKit WebUI, passare alla schermata Dispositivi:

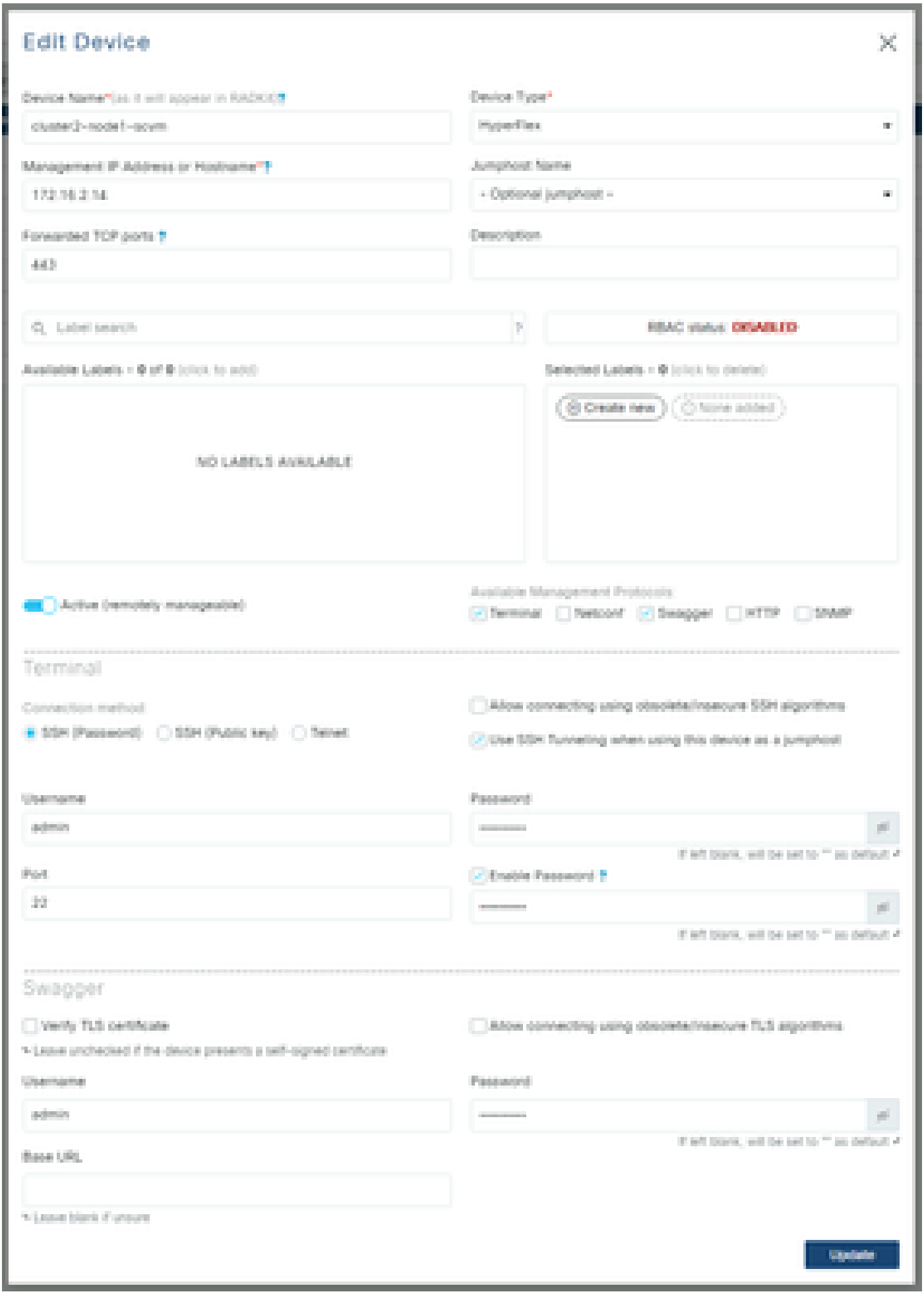
Per ognuna delle periferiche elencate sopra, creare una nuova voce facendo clic su Add Device . Immettere l'indirizzo IP, selezionare il tipo di dispositivo e fornire i dettagli per tutti i nodi del cluster in base a ciascun tipo di dispositivo. Al termine, fare clic su Add & closeper tornare alla schermata Dispositivi o Add & continue per aggiungere un altro dispositivo.

Qui è possibile trovare voci di esempio e la loro configurazione per ciascun tipo di dispositivo:

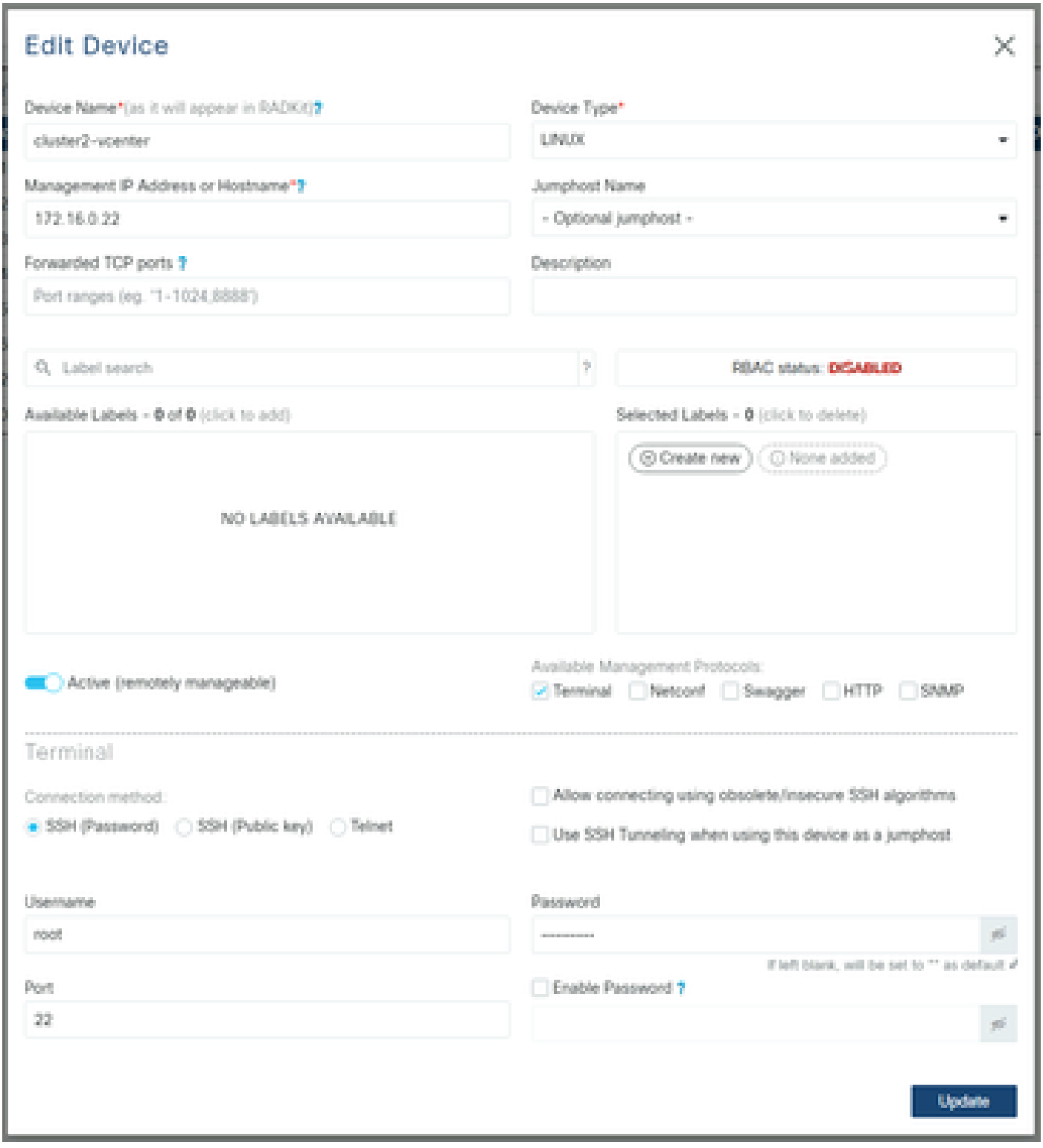
Esempio di host ESXi:



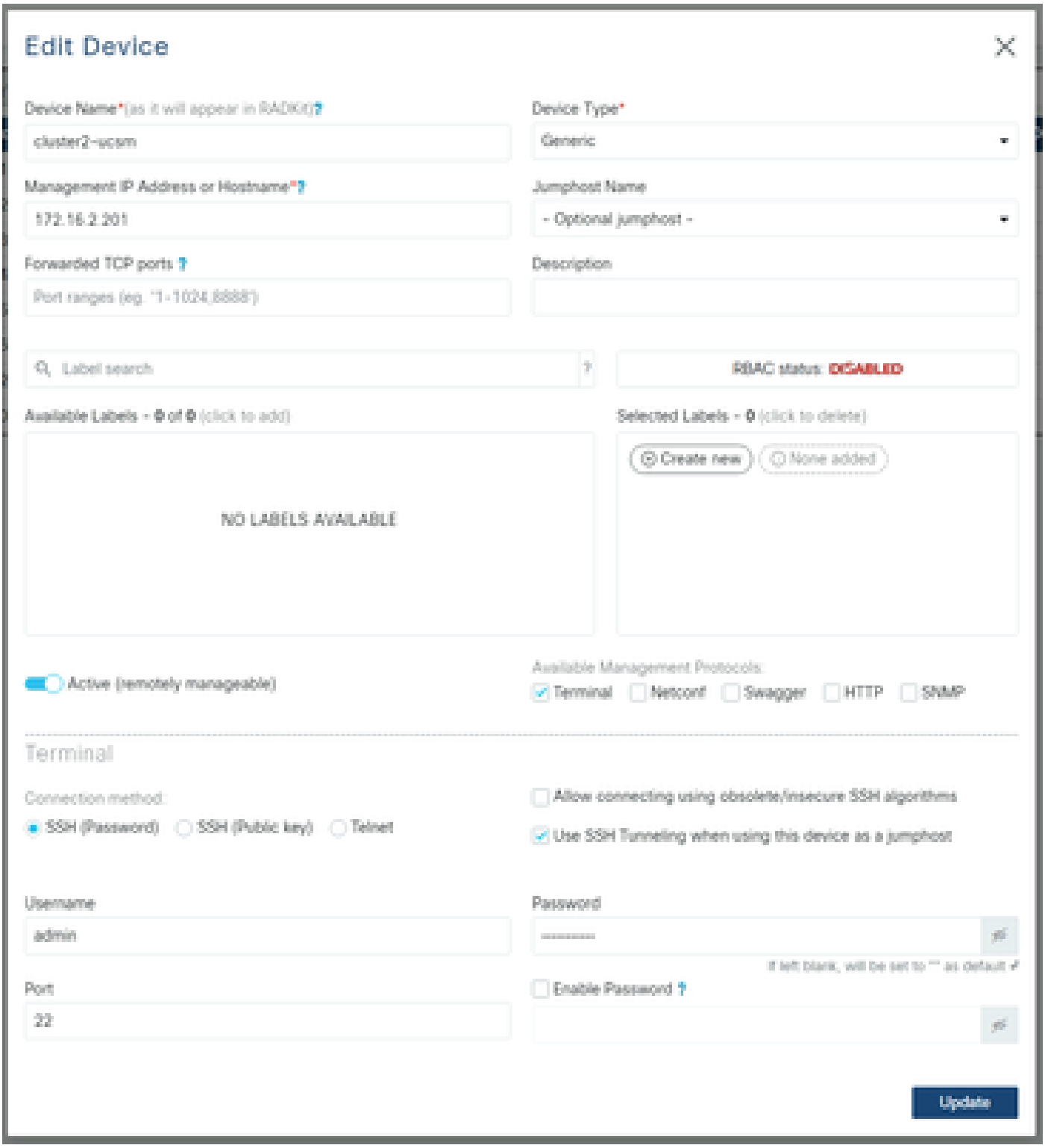
Esempio di controller di storage:


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

Esempio per vCenter:



Esempio di UCSM:



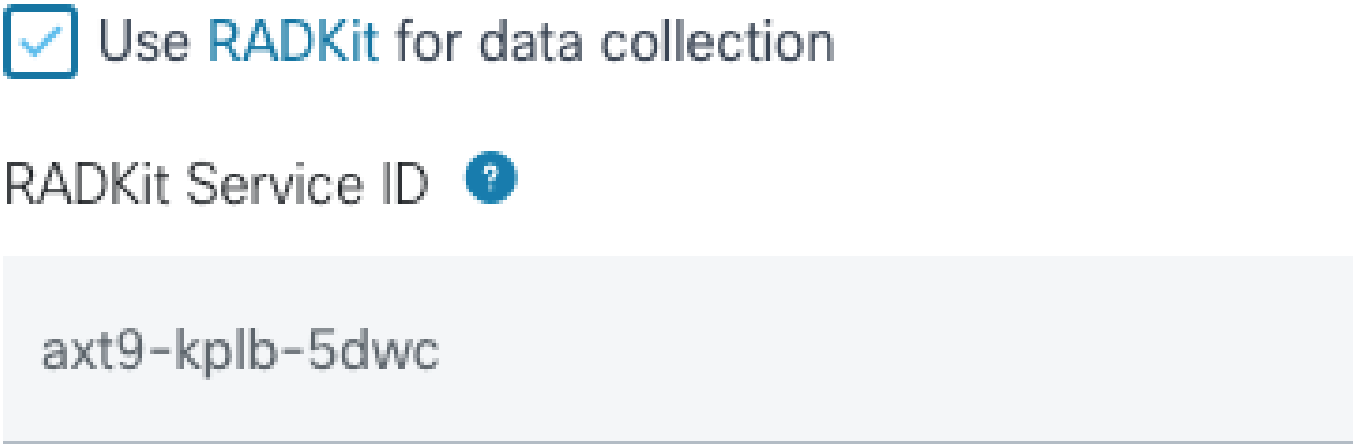
Utilizzo di RADKit su TAC SR

Al termine dei preparativi, se si desidera fornire l'accesso ai propri dispositivi a un tecnico TAC, procedere come segue.

Un tecnico necessita dell'ID del servizio RADKit e dell'accesso all'ambiente o ai dispositivi selezionati (quando si utilizza RBAC) per il tempo necessario.

1. Fornire ID servizio RADKit

Se non è stata ancora aperta una richiesta TAC, è possibile farne riferimentoUse RADKit for data collection in Support Case Manager all'indirizzo Cisco.com:

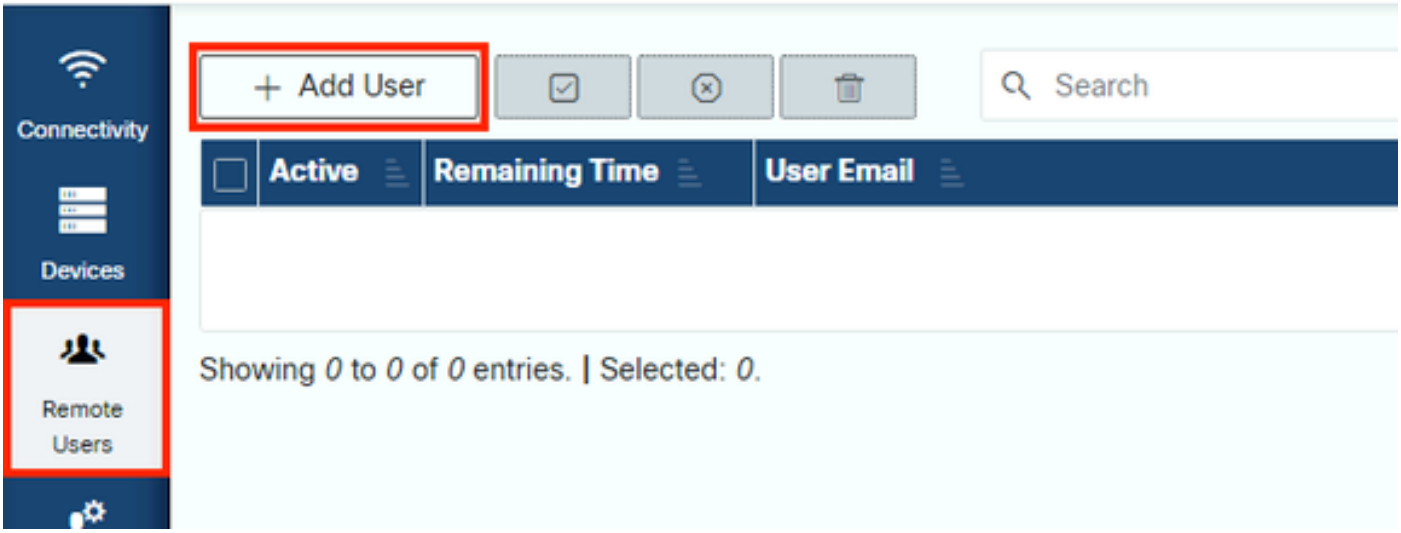


Se è già presente una richiesta di assistenza aperta, è possibile aggiungere l'ID servizio RADKit in Support Case Manager con la sezione Informazioni di contatto del cliente:

In alternativa, è possibile comunicare il proprio ID al tecnico TAC che sta lavorando al proprio caso.

2. Aggiungi utente remoto

Prima che qualsiasi utente possa utilizzare i dispositivi, è necessario fornire l'accesso esplicito e configurare un intervallo di tempo per il quale tale accesso rimane valido. A tale scopo, in RADKit WebUI, passare alla Remote Users schermata e creare un nuovo utente remoto facendo clic su Add User.



Immettere l'indirizzo e-mail @cisco.com del tecnico TAC (prestare attenzione agli errori di battitura). Assicurarsi di prestare attenzione alla casella di spunta e alleActivate this user Time slice Manual impostazioni o.

Quando l'utente è attivo, può accedere ai dispositivi configurati tramite il servizio RADKit, a condizione che tali dispositivi siano abilitati e che il criterio RBAC lo consenta.

La sezione temporale rappresenta il periodo di tempo trascorso il quale l'utente viene disattivato automaticamente; in altre parole, una sezione temporale rappresenta una sessione di risoluzione dei problemi con limiti di tempo. La sessione dell'utente può essere estesa fino alla durata della porzione di tempo per l'utente. Se si preferisce attivare/disattivare manualmente gli utenti, selezionare Manual.

Gli utenti possono sempre essere attivati/disattivati manualmente, indipendentemente dalla configurazione o meno di una fascia oraria. Quando un utente viene disattivato, tutte le sue sessioni tramite il servizio RADKit vengono immediatamente disconnesse.

Al termine, fare clic su Add & close per tornare alla schermata Utenti remoti.

Informazioni correlate

- Ulteriori informazioni e risposte alle domande più frequenti sono disponibili sul sito web di RADKit: https://radkit.cisco.com/
- **Supporto tecnico Cisco e download**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).