設定RADKit以便在HyperFlex上進行遠端故障排除

目錄

簡介

本文檔介紹如何開始和準備RADKit環境，以便對Cisco HyperFlex環境進行遠端故障排除。

背景資訊

本文檔的主要目的是說明如何準備您的環境供TAC使用，以利用RADKit進行故障排除。

什麼是RADKit？

RADKit是一個全網協調器。體驗處理設備、提升思科服務成效並擴充功能的嶄新方式。

有關RADKit的詳細資訊，請訪問：https://radkit.cisco.com/

為什麼要使用RADKit來處理HX？

Cisco HyperFlex由多個元件組成：交換矩陣互聯、UCS伺服器、ESXi、vCenter和SCVM。在許多

情況下，需要收集來自不同裝置的資訊，並相互關聯。在排除故障時，可能隨著時間的推移需要新的資訊，透過（長）WebEx會話或透過透過Intersight獲取（大型）支援捆綁包進行故障排除並不總是最有效的方法。使用RADKit，TAC工程師可以在故障排除過程中以安全可控的方式從各種裝置和服務請求所需資訊。

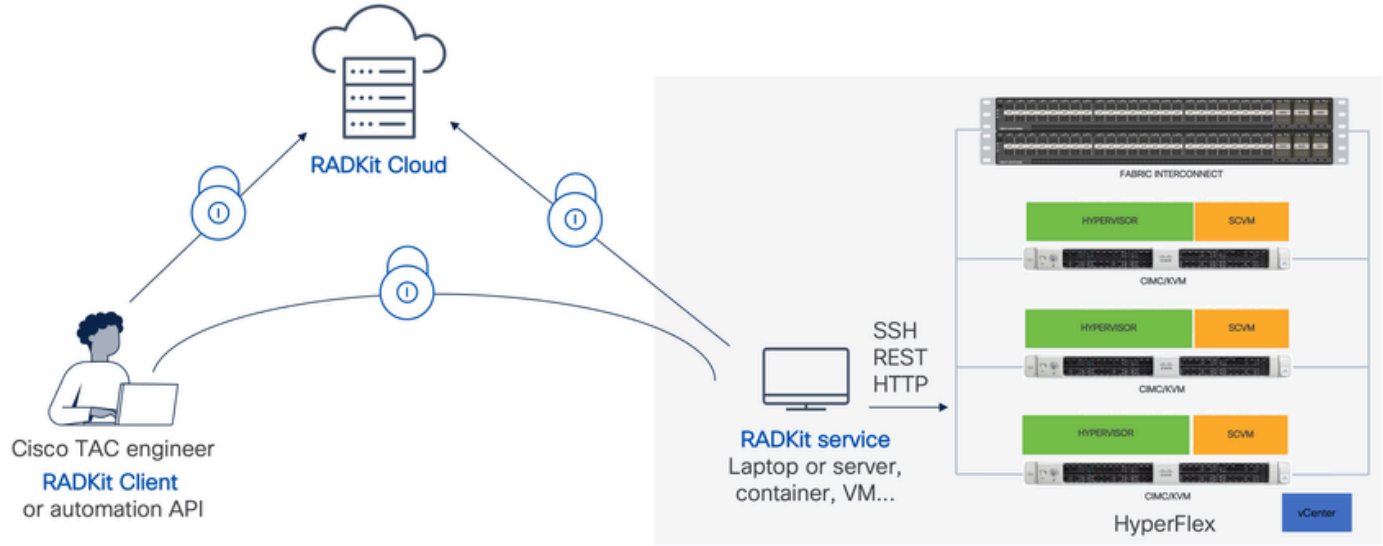
RADKit與Intersight

Intersight仍然是HyperFlex群集的主要連線方法，可提供許多優勢，例如自動日誌收集、遙測以及對您的環境進行主動監控以發現硬體和其他已知警報。

雖然許多HX群集都與Intersight連線，但Intersight當前主要用於部署、維護和監控HyperFlex群集。Intersight允許收集支援捆綁包和遙測資訊，這通常是進行故障排除的良好起點。對於即時故障排除，在典型場景中，TAC工程師會使用WebEx會話，RADKit就位。它不會取代Intersight，但會增加不同的故障排除方法，無論是使用互動式會話還是利用程式設計請求-響應序列。

簡要概述

連線圖表



元件

- RADKit服務：內部部署RADkit服務元件，用作通往HX環境的安全網關。作為客戶，您可以完全控制哪些裝置可以訪問，以及哪些人可以在何時訪問這些裝置。此服務可以託管在任何Linux、MacOS或Windows電腦上。
- RADKit客戶端：TAC工程師使用前端來訪問您的環境，使用程式設計故障排除和監控，使用思科內部工具自動檢索並分析裝置輸出，或透過CLI直接與裝置進行互動。
- RADKit Cloud：提供客戶端和服務之間的安全傳輸。

準備

要遵循的步驟概述

TAC工程師必須完成以下步驟，才能利用RADKit來連線您的HX環境並進行故障排除：

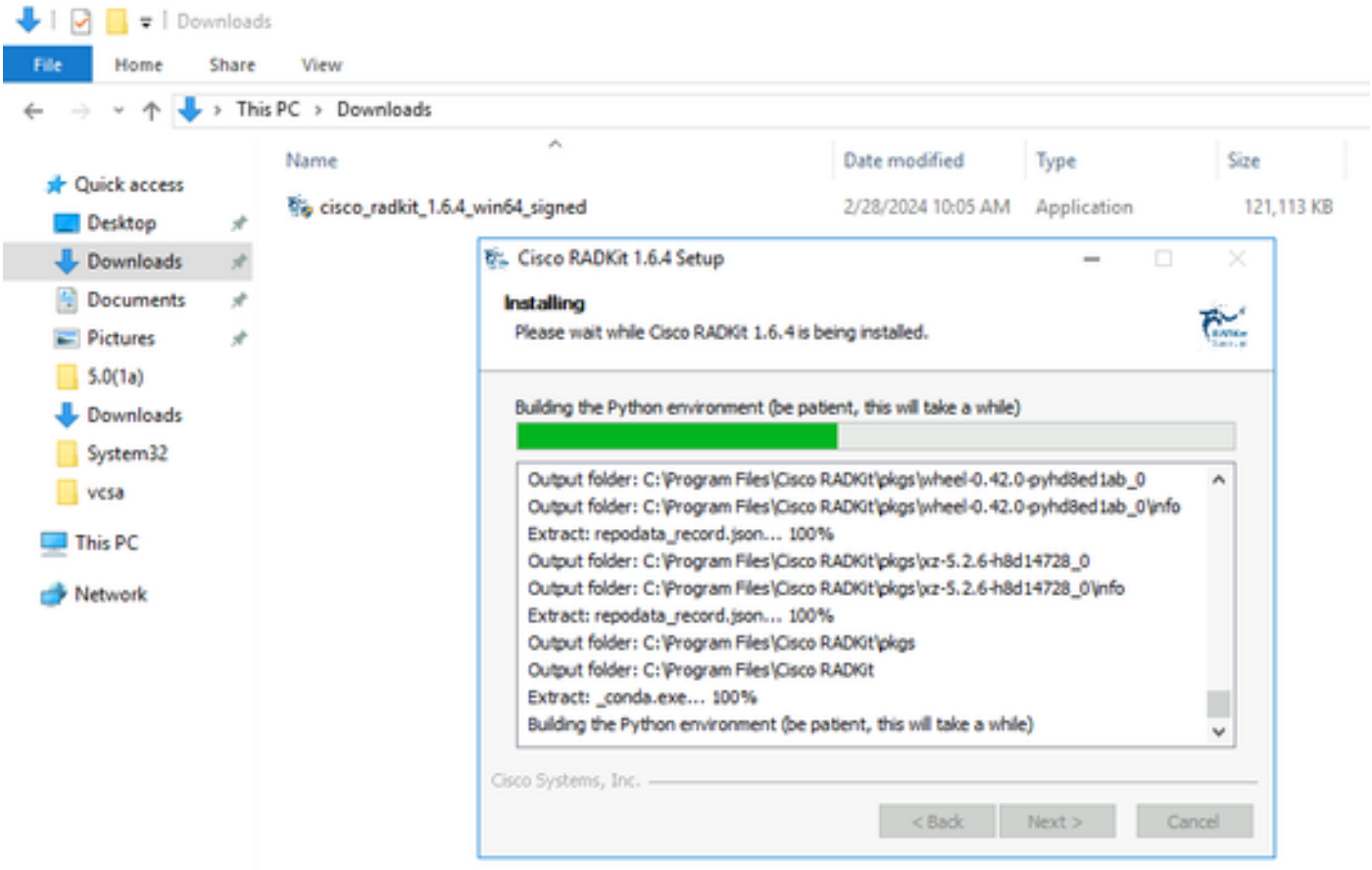
1. 下載並安裝RADkit服務。它可以安裝在任何Linux、MacOS或Windows機器上。
2. 啟動RADKit服務並執行初始設定（載入程式）。建立超級管理員帳戶，以便透過Web介面進一步管理RADKit服務。
3. 向RADKit雲註冊RADKit服務。向RADKit雲註冊RADKit服務並生成服務ID以辨識您的環境。
4. 增加裝置和終端。提供裝置清單，並儲存可能需要存取之裝置的認證。

有關這些步驟的更詳細/一般說明，請參閱
：https://radkit.cisco.com/docs/pages/one_page_setup.html

步驟 1.下載並安裝RADKit服務

此步驟中的詳細資訊可能略有不同，具體取決於用來安裝RADKit服務的作業系統，但一般而言，此過程非常相似。從以下網址下載適用於您作業系統的最新版本
：https://radkit.cisco.com/downloads/release/。

執行系統的安裝程式，並依照提示進行操作，直到安裝完成：



安裝完所有RADKit元件後，您可以繼續執行下一個步驟，完成初始設定。

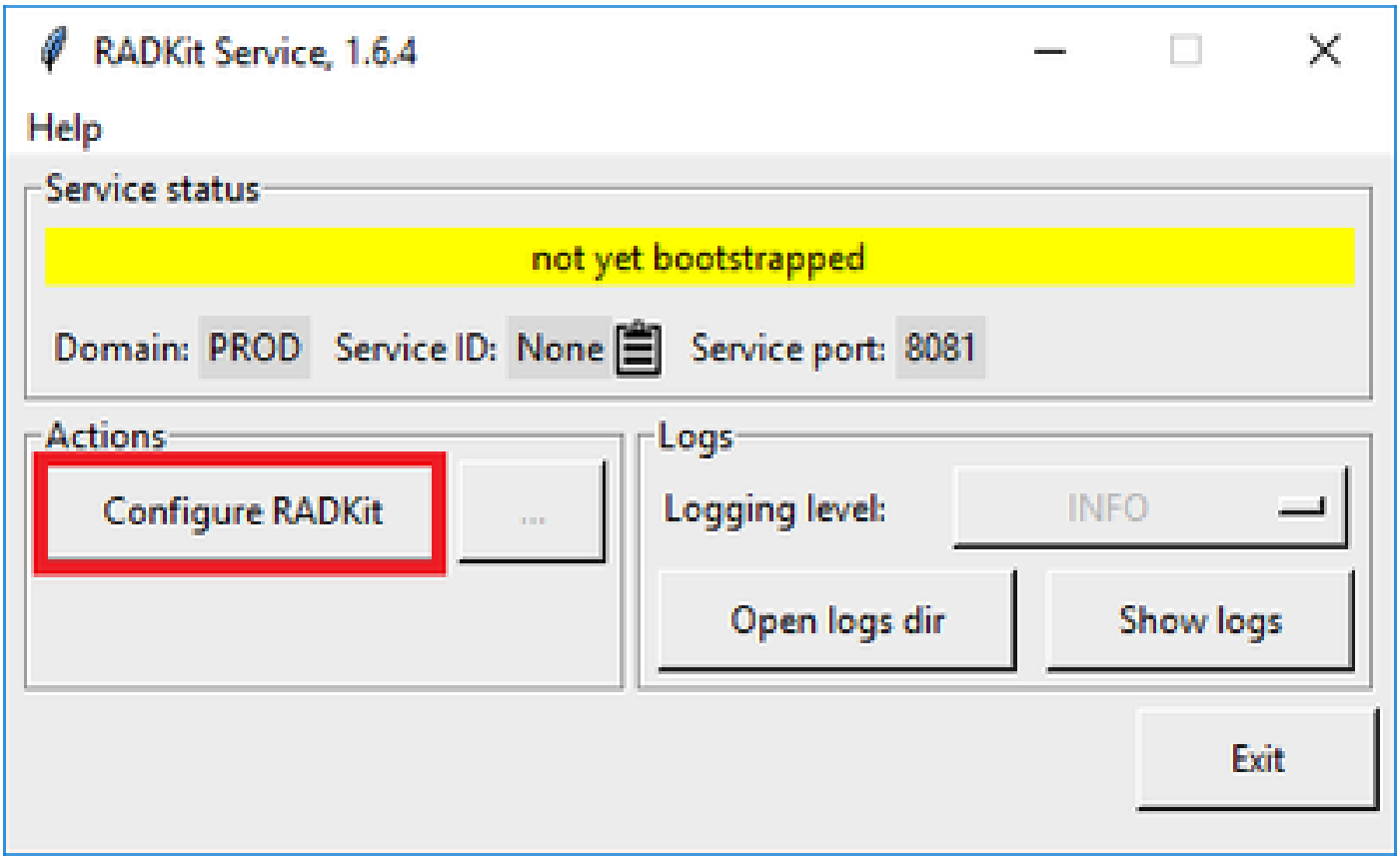
步驟 2.啟動RADKit服務並執行初始設定（啟動）

在此步驟中，請建立一個superadmin帳戶，以便透過Web介面進一步管理RADKit服務。

在「開始」選單（在Windows上）或「應用程式」資料夾（在macOS上）中找到RADKit Service並啟動它：

第一次啟動時，可能需要一些時間才能啟動RADKit服務（約10到30秒，取決於系統的速度）。後續的運行速度會快得多。

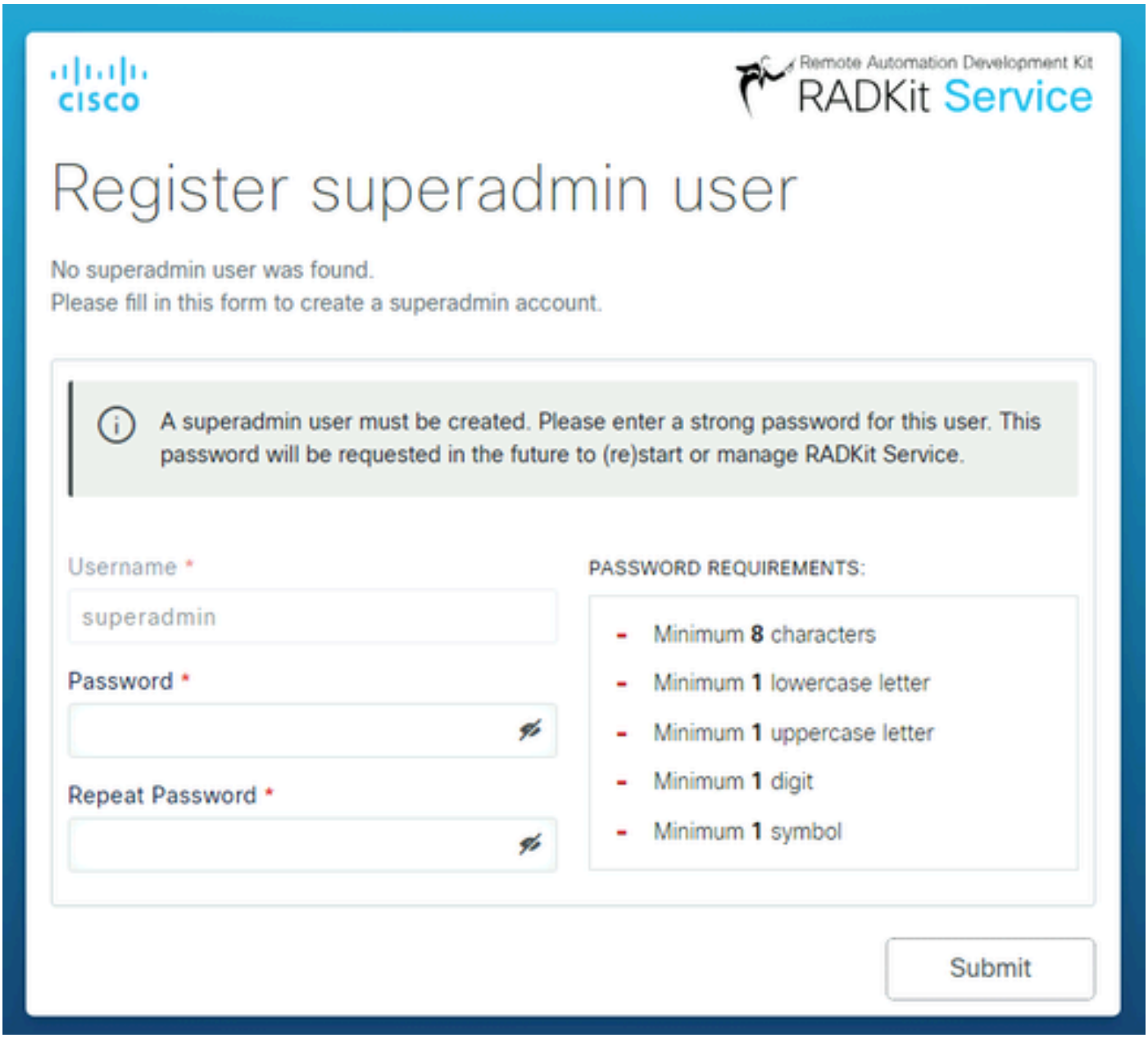
啟動完成後，在RADKit Service對話方塊中，當狀態更改為not yet bootstrapped press Configure RADKit ：



這將打開您的Web瀏覽器，並進入RADKit服務WebUI，這是一個基於Web的管理介面，允許您管理RADKit服務。

當使用自簽名證書連線到此URL時，將會收到證書警告，您可以跳過該警告。

由於superadmin使用者尚不存在，WebUI將要求您為此使用者建立密碼：



選擇符合右側顯示的密碼強度要求的密碼。

此帳戶的密碼將用於保護私鑰和裝置憑據等機密；如果丟失密碼，所有機密都將丟失，並且需要重新初始化RADKit服務，因此請謹慎選擇密碼並將其寫入安全位置。稍後可視需要加以變更。

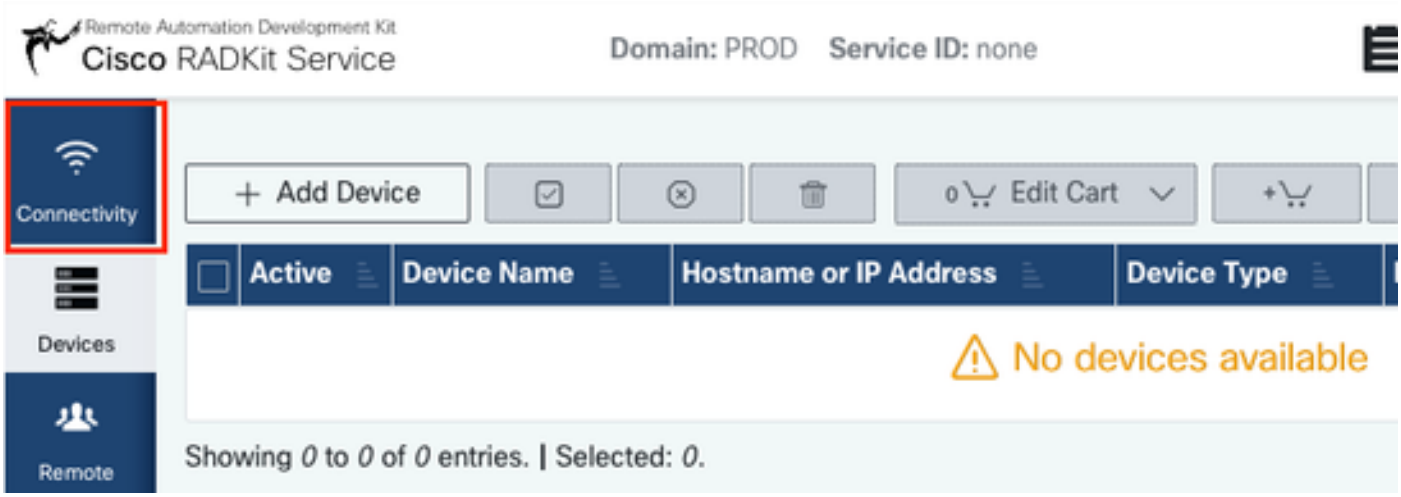
建立superadmin帳戶後，請使用它登入WebUI：

建立superadmin帳戶並成功登入到WebUI後，您可以繼續執行下一步，即向RADKit雲元件註冊RADKit服務。

步驟 3.使用RADKit Cloud註冊RADKit服務

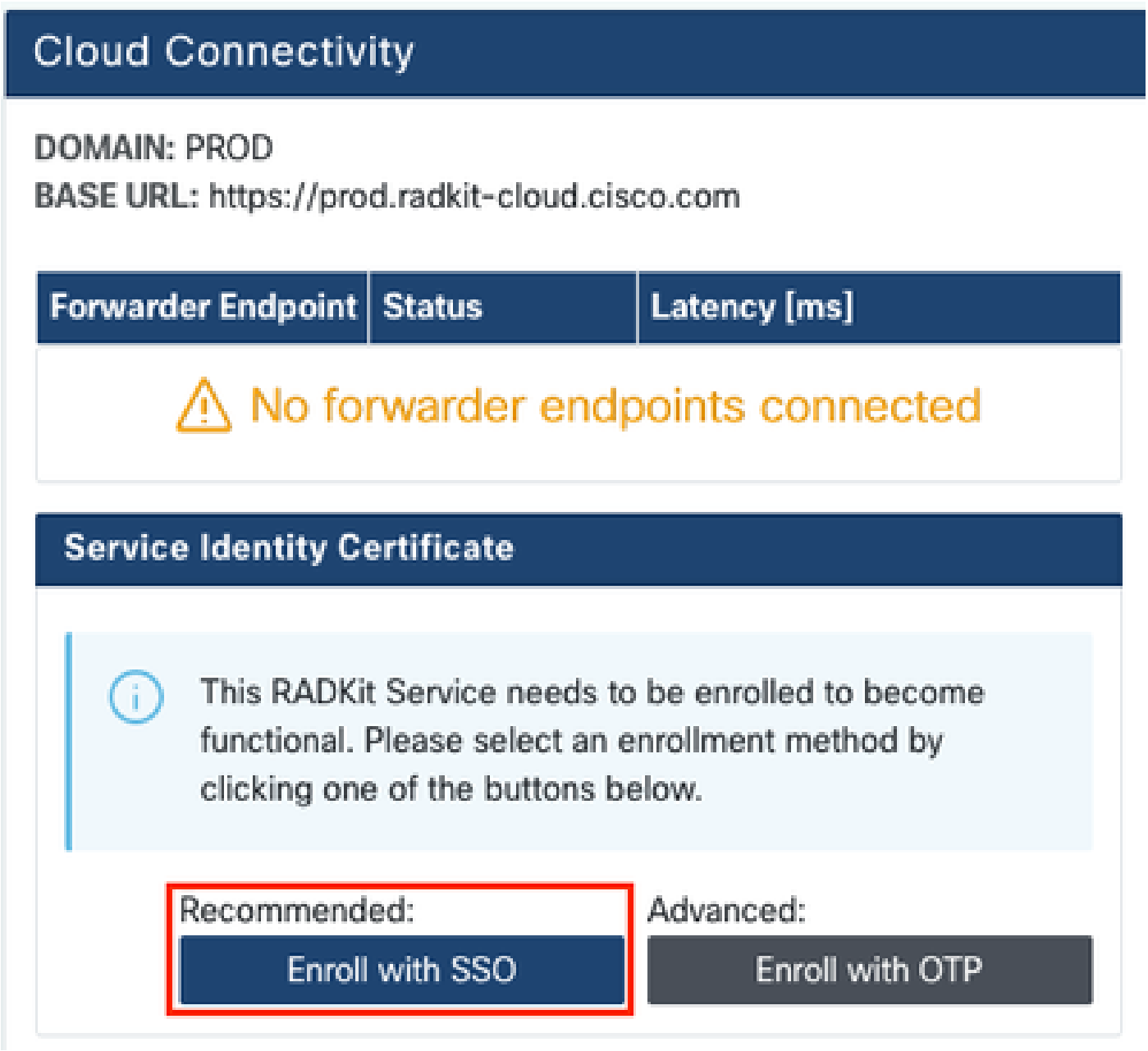
在此步驟中，請向RADKit雲註冊RADKit服務，並生成服務ID以辨識您的環境。

使用superadmin使用者登入WebUI後（請參閱第2步），導航到connectivity螢幕：

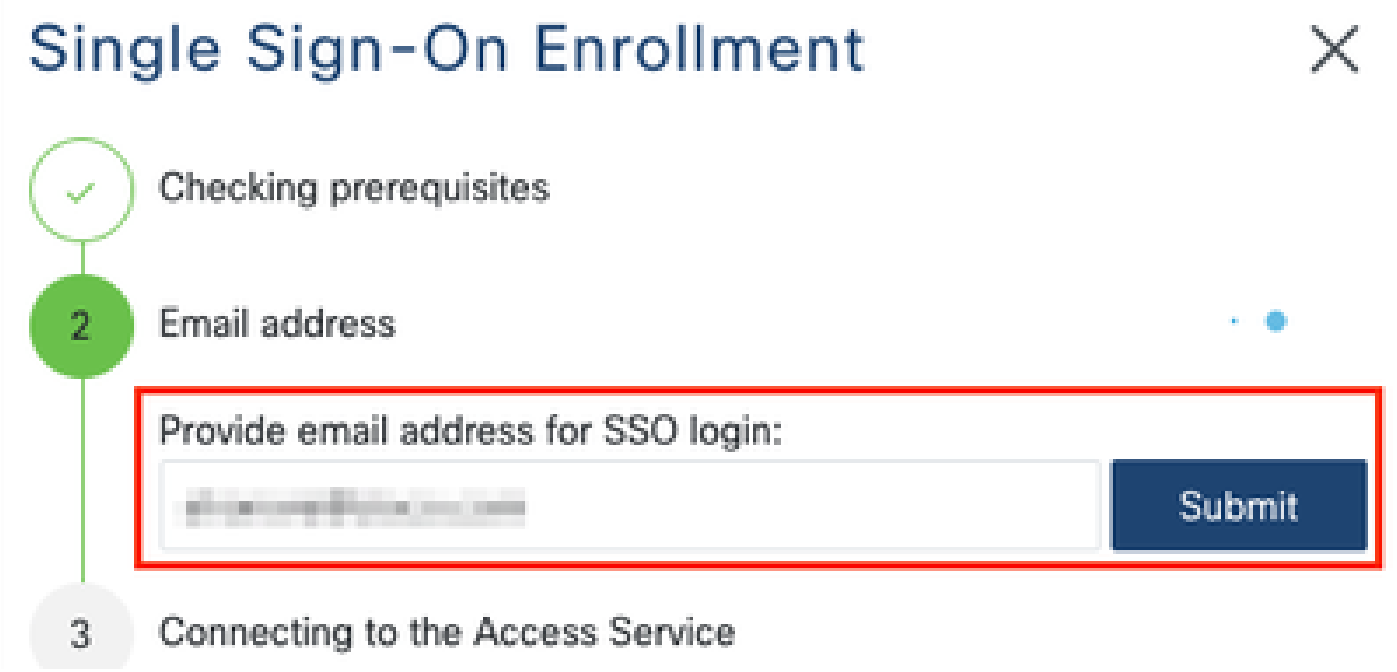


如果您需要Proxy來連線到網際網路，請參考此處提供的詳細設定說明：https://radkit.cisco.com/docs/pages/one_page_setup.html

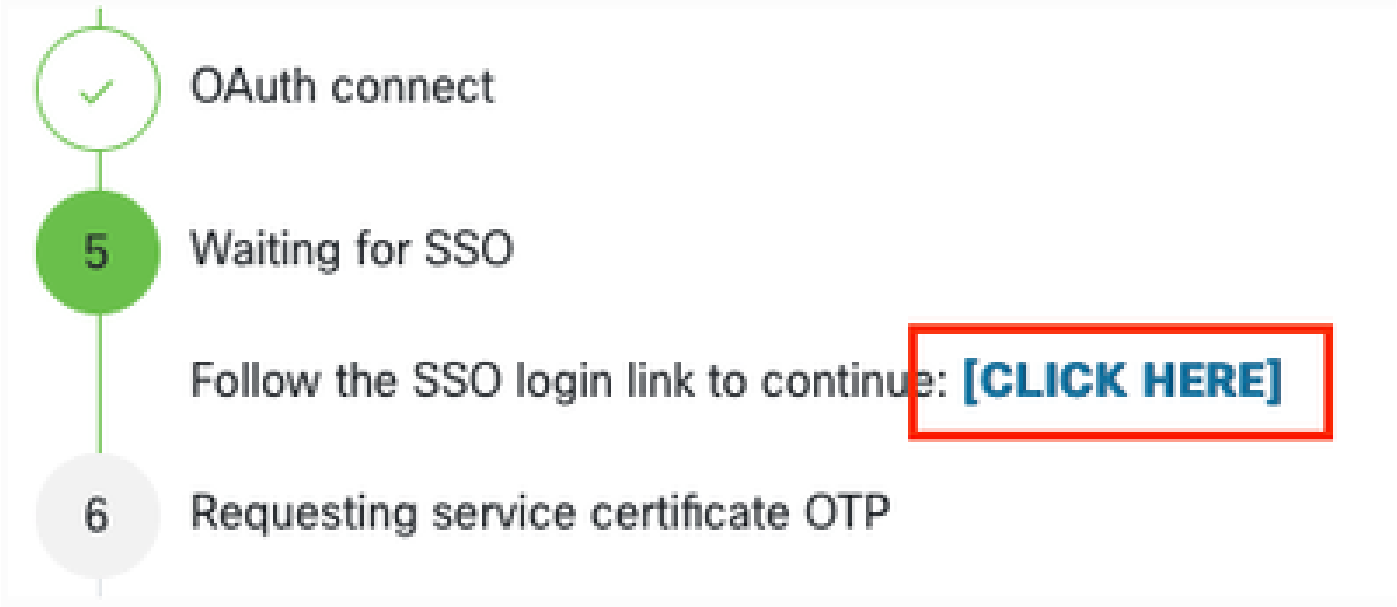
現在，您需要註冊該服務，使其連線到RADKit Cloud。這可透過使用您的Cisco.com (CCO)帳戶透過服務WebUI登入來完成。點選Enroll with SSO以繼續：



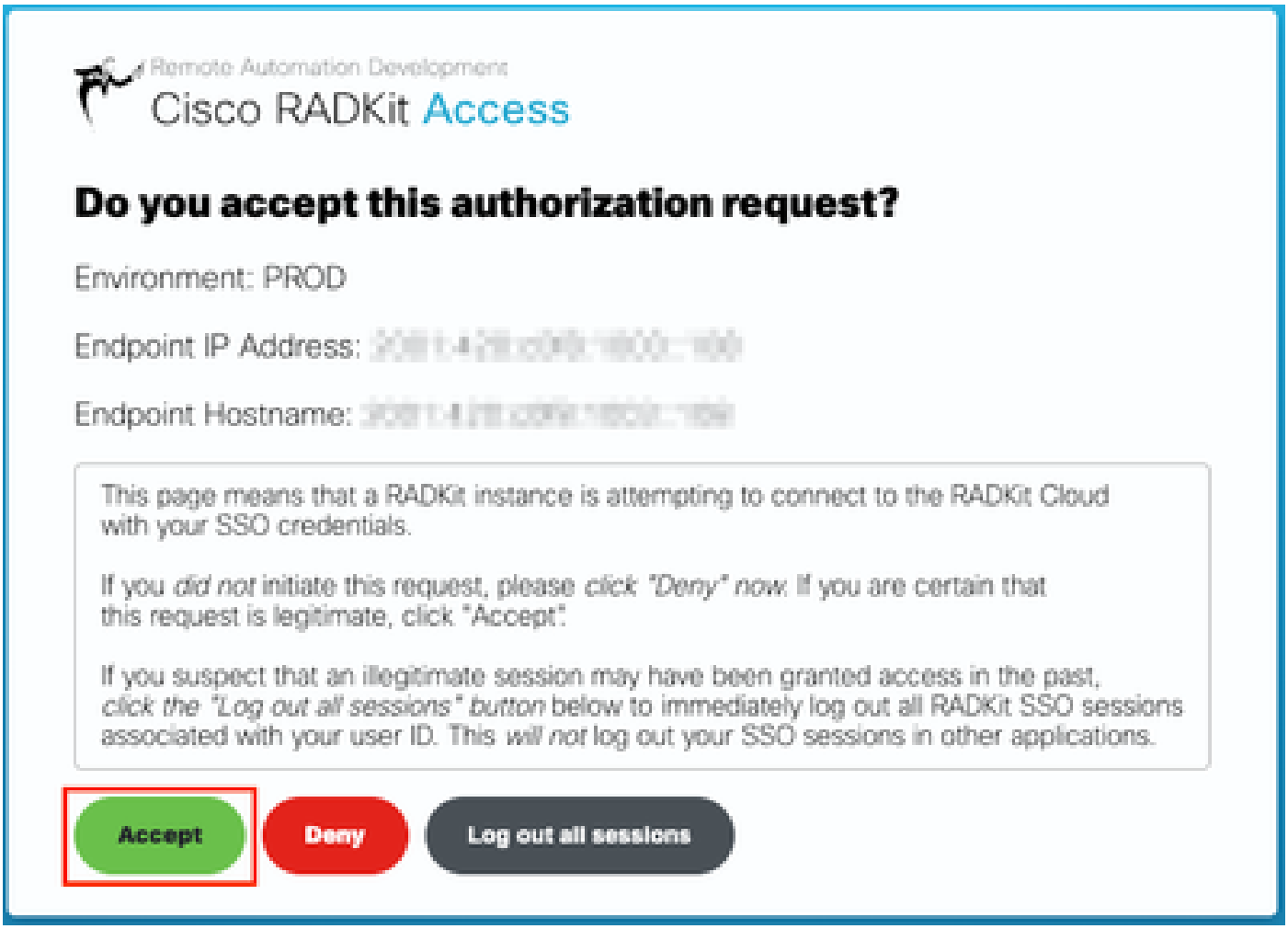
在Step 2的email address欄位中輸入與您的Cisco.com (CCO)帳戶對應的電子郵件地址。然後按一下Submit as shown in the image：



RADKit Service連線到RADKit Cloud進行授權之後，它會顯示[CLICK HERE]一個連結，該連結將帶您連線到Cisco SSO伺服器進行身份驗證。按一下連結以繼續；它將在新的瀏覽器標籤/視窗中開啟。請確保使用與之前所提及步驟中輸入的電子郵件地址相同的電子郵件地址登入SSO：



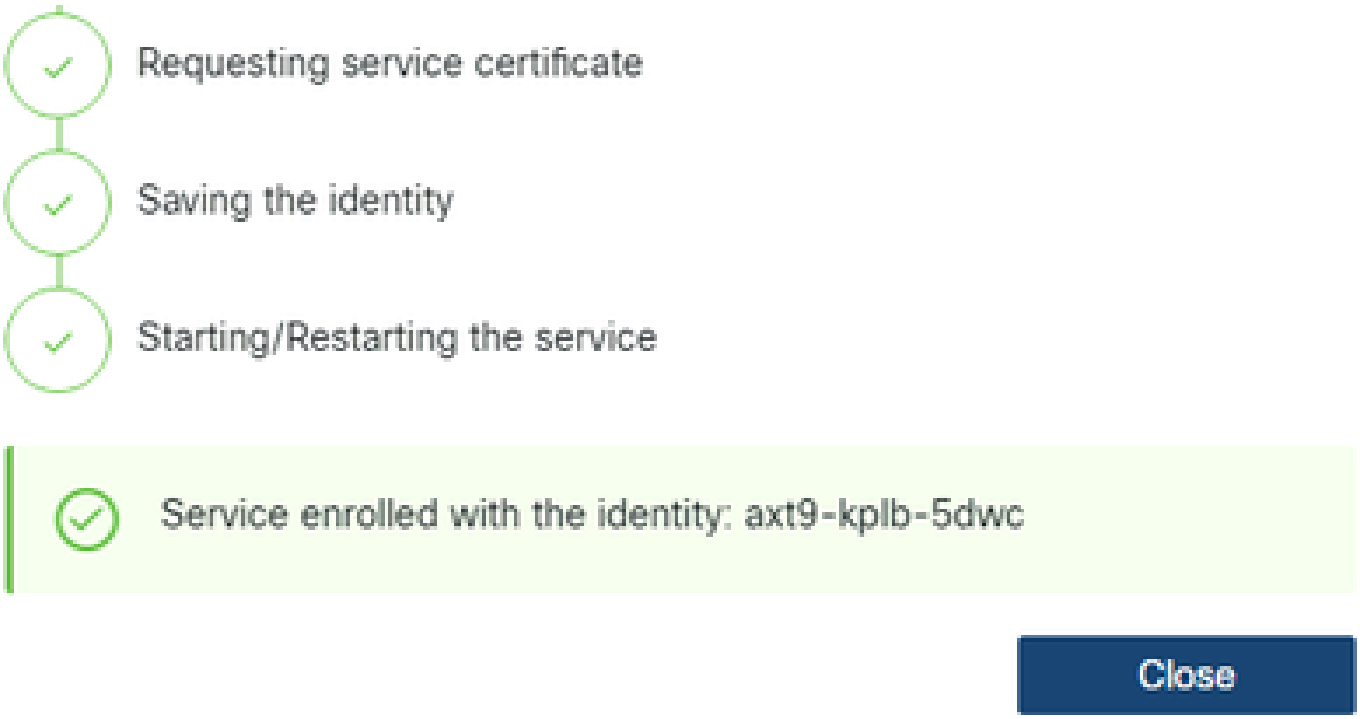
SSO身份驗證完成後（或者如果您已經過身份驗證，則立即進入RADKit Access確認頁面）。閱讀頁面上的資訊，然後按一下Accept授權RADKit服務以您的CCO帳戶作為所有者註冊。



然後您會看到一個顯示Authentication result: Success（這是您尋找快取缺失可以使用的隱藏命令）的螢幕。

請勿按一下Log out all sessions按鈕，只需關閉SSO頁籤/窗口並返回RADKit服務WebUI。

此圖顯示Service enrolled with the identity: …。後面的唯一識別符號是您的RADKit服務ID，也稱為服務序列號。在示例螢幕截圖中，服務ID是您axt9-kplb-5dwc的將會不同。



按一下Close關閉對話方塊並返回Connectivity螢幕。

刷新WebUI後，您的服務ID和連線狀態將顯示在RADKit GUI的頂部，如下所示：

每當TAC工程師需要訪問您環境中的任何裝置時，他們都需要此服務ID來辨識您的RADKit服務。

現在，已與RADKit Cloud元件建立連線，並在建立連線時生成服務ID，下一步是增加可以透過RADKit訪問的裝置。

步驟 4.增加裝置和終端

在此步驟中，為可以透過RADKit訪問的裝置增加裝置及其憑證。對於HyperFlex，這意味著理想情況下需要增加以下裝置及其憑據：

裝置	裝置型別	管理協定	憑證	轉發的TCP埠	備註
虛擬機器監控程式（ESXi主機）	Linux	終端(SSH)	根		
儲存控制器	HyperFlex	終端	管理員	443	在啟用密碼欄位中輸入根密碼。當需要同

(SCVM)		(SSH)Swagger	root (enable)		意令牌時，將使用此選項。對於Swagger：取消選中「驗證TLS證書」，並將「基本URL」欄位留空
vCenter	Linux	終端(SSH)	根		
UCSM	一般	終端(SSH)	管理員		
安裝程式（選擇性）	Linux	終端(SSH)	根	443	
CIMC （僅適用於邊緣群集）	一般	終端(SSH)	管理員		
見證（僅適用於延伸叢集）	Linux	終端(SSH)	根		
Intersight CVA/PCA（可選）	Linux	終端(SSH)	管理員	443	

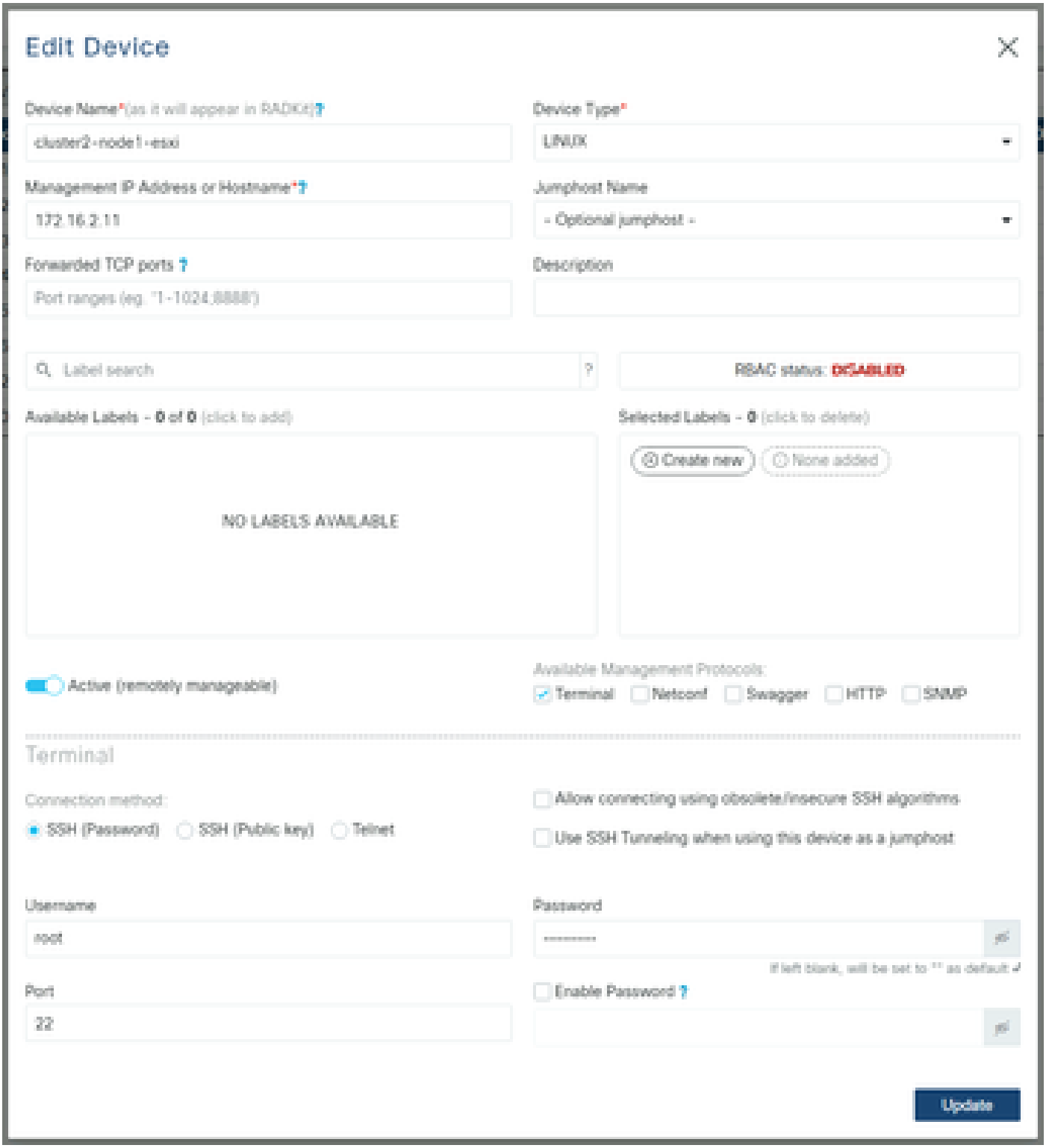
增加裝置時，務必僅使用裝置的IP地址而非主機名，因為這樣才能使屬於同一集群的裝置相互關聯。

要增加這些裝置，請在RADKit WebUI中導航到「裝置」螢幕：

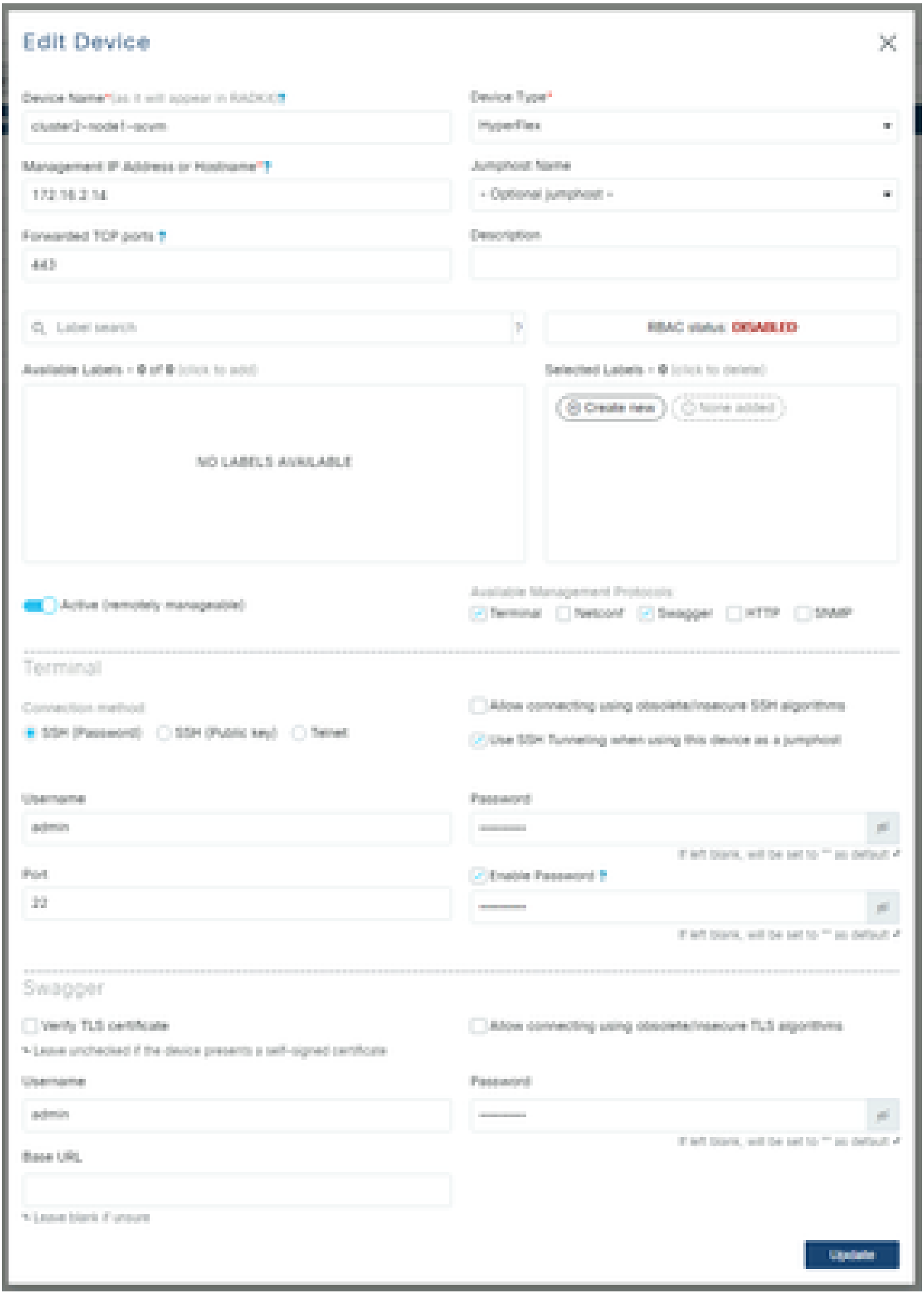
對於上面列出的每個裝置，透過按一下Add Device建立新條目。輸入IP位址、選取裝置型別，並根據叢集中所有節點的每種裝置型別提供詳細資訊。完成後，按一下Add & close返回「裝置」螢幕，或按一下Add & continue增加另一裝置。

您可以在此處找到每個裝置型別的示例條目及其配置：

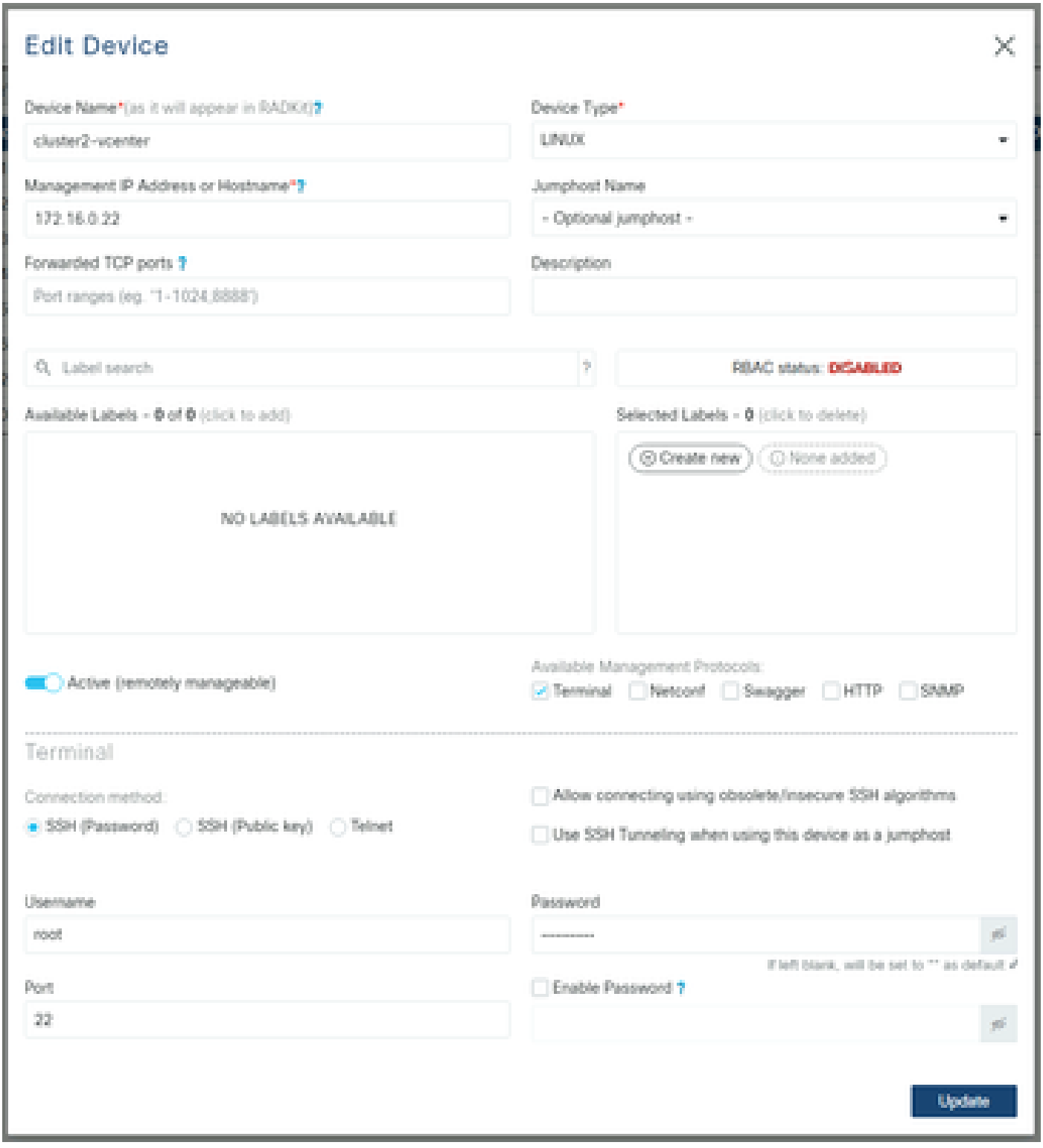
ESXi主機示例：



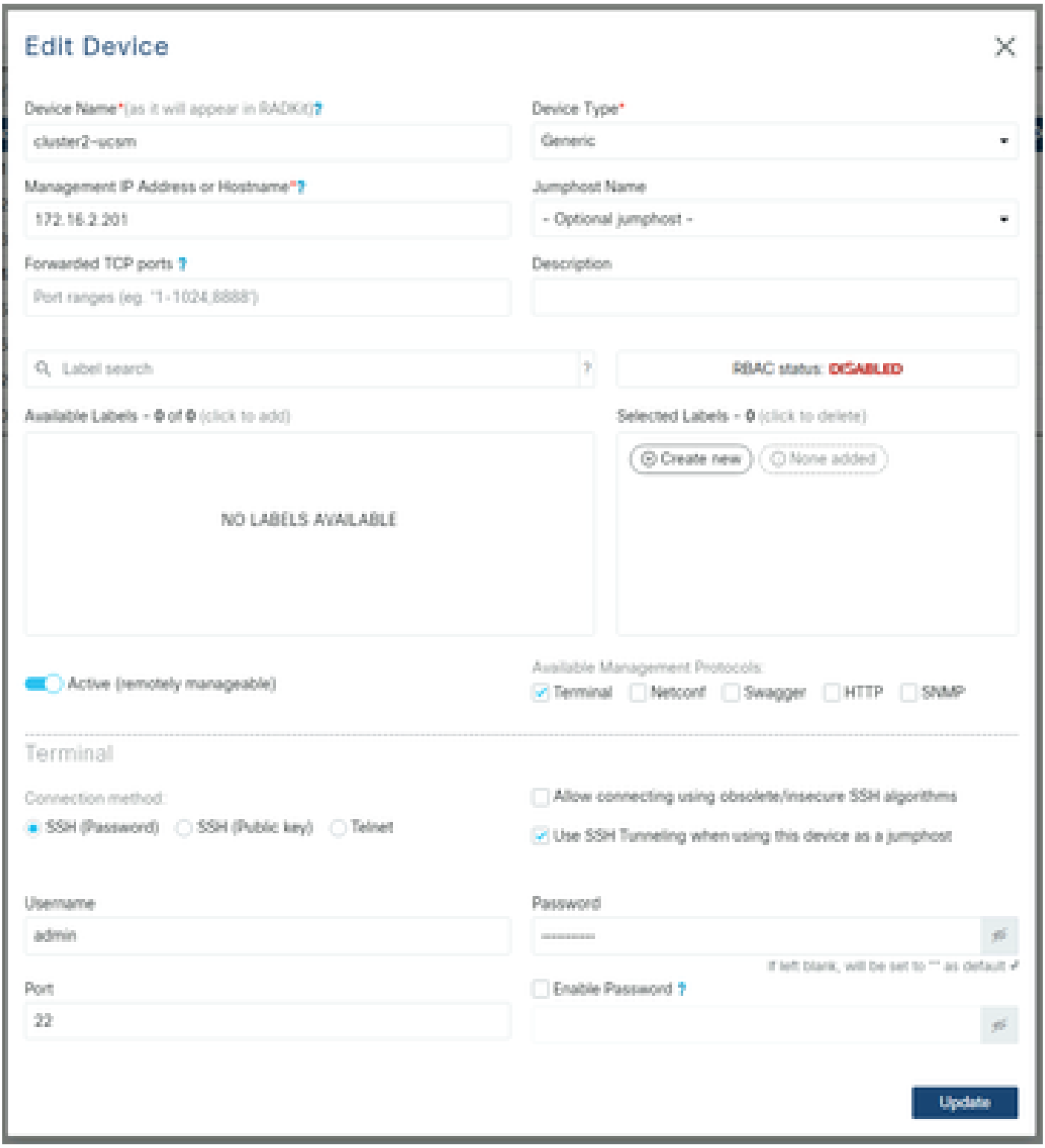
儲存控制器的範例：


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

vCenter示例：



UCSM示例：



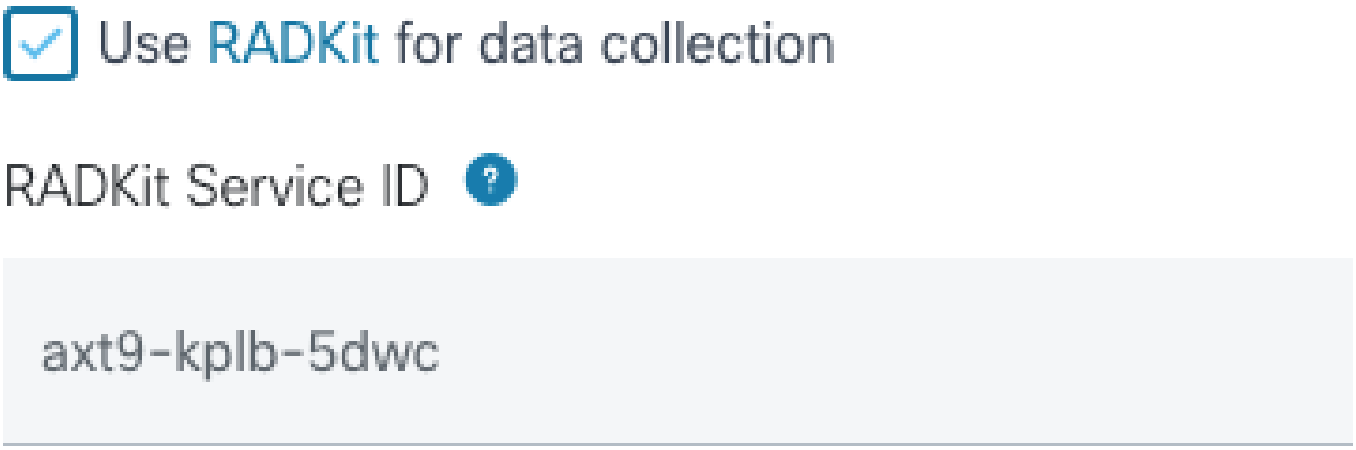
在TAC SR上使用RADKit

如果所有準備工作都完成，並且您想向TAC工程師提供裝置訪問許可權，您可以完成以下步驟。

工程師需要您的RADKit服務ID以及訪問您的環境或所選裝置（使用RBAC時）所需的時間。

1. 提供RADKit服務ID

如果您尚未提交TAC支援請求，則可以在Cisco.com上的支援請求管理器中提及Use RADKit for data collection：

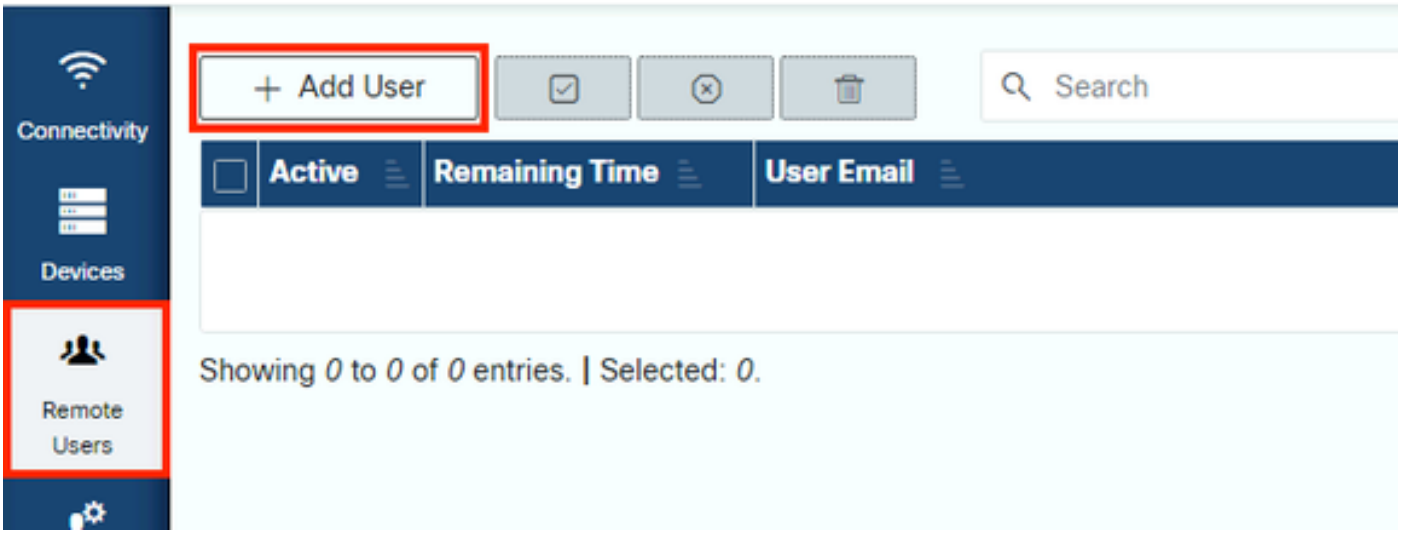


如果您已經有一個未結服務請求，您可以在支援案例管理器中增加RADKit服務ID以及客戶聯絡資訊部分：

或者直接將您的ID告知正在處理您的案例的TAC工程師。

2. 增加遠端使用者

在任何使用者能夠使用您的裝置之前，您需要提供顯式訪問並配置一個時間範圍，以便此訪問仍然有效。為此，在RADKit WebUI中，導航到Remote Users螢幕，並透過按一下 Add User.



輸入TAC工程師的@cisco.com電子郵件地址（請小心錯別字）。請務必注意Activate this user覈取方塊以及Time slice或Manual 設定。

使用者處於活動狀態時，可以透過RADKit服務訪問已配置的裝置，前提是這些裝置已啟用且RBAC策略允許這些裝置。

時間片段代表使用者自動停用之前的時間量；換句話說，時間片段代表有時限的疑難排解工作階段。使用者的會話可以延長到該使用者的時間片段的持續時間。如果您希望手動啟用/停用使用者，請選擇Manual。

無論使用者是否配置了時間片，都可以手動啟用/停用使用者。當使用者被停用時，他們透過RADKit服務的所有會話會立即斷開。

完成後，按一下Add & close返回到「Remote Users」螢幕。

相關資訊

- 更多資訊和常見問題解答位於RADKit網站：https://radkit.cisco.com/
- **思科技術支援與下載**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。