

在HyperFlex上设置RADKit以进行远程故障排除

目录

[简介](#)

[背景信息](#)

[什么是RADKit？](#)

[为什么选择适用于HX的RADKit？](#)

[RADKit vs. Intersight](#)

[简要概述](#)

[连接图](#)

[组件](#)

[准备](#)

[要遵循的步骤概述](#)

[步骤1: 下载并安装RADKit服务](#)

[第二步：启动RADKit服务并执行初始设置（引导程序）](#)

[第三步：使用RADKit云注册RADKit服务](#)

[第四步：添加设备和终端](#)

[在TAC SR上使用RADKit](#)

[1. 提供RADKit服务ID](#)

[2. 添加远程用户](#)

[相关信息](#)

简介

本文档介绍如何开始和准备RADKit环境，以便对Cisco HyperFlex环境进行远程故障排除。

背景信息

本文档的主要目的是说明如何准备您的环境以供TAC使用，从而利用RADKit进行故障排除。

什么是RADKit？

RADKit是一个全网络协调器。体验一种全新的设备寻址方式，提升您的思科服务并扩展服务能力。

有关RADKit的详细信息，请访问：<https://radkit.cisco.com/>

为什么选择适用于HX的RADKit？

Cisco HyperFlex由多个组件组成：交换矩阵互联、UCS服务器、ESXi、vCenter和SCVM。在许多情况下，需要收集来自不同设备的信息，并对信息进行关联。在进行故障排除时，随着时间的推移可能需要新的信息，而通过（长）WebEx会话或通过通过Intersight获取（大）支持捆绑包并不总是

最有效的方法。通过使用RADKit，TAC工程师可以在故障排除过程中以安全可控的方式从各种设备和服务请求所需信息。

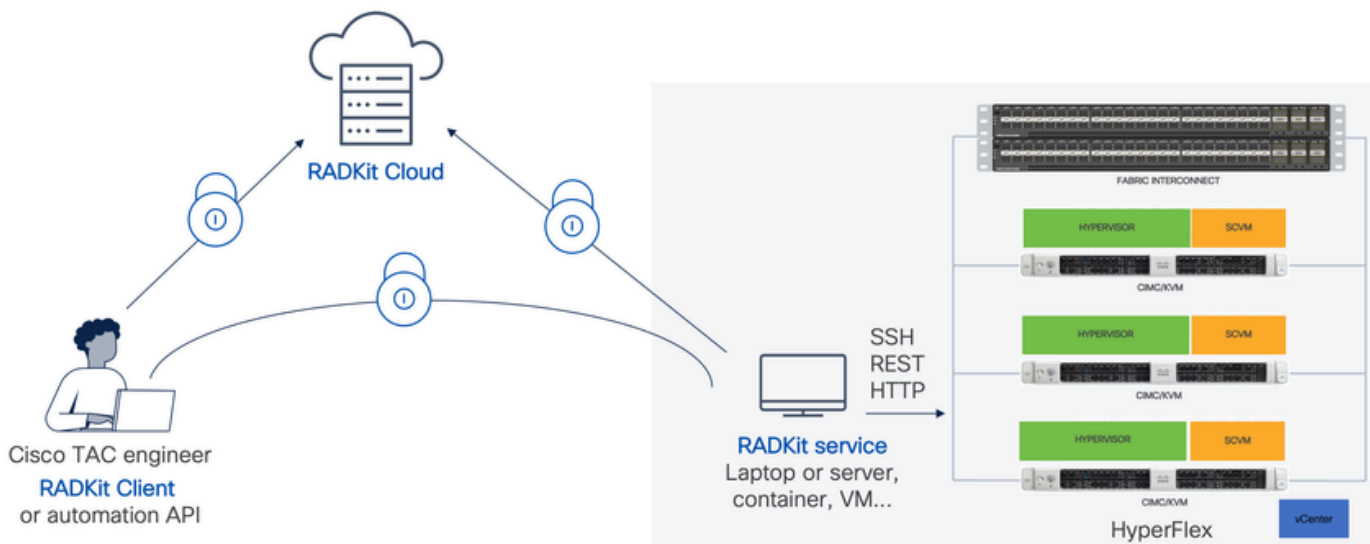
RADKit vs. Intersight

Intersight仍然是HyperFlex集群的主要连接方法，可提供许多优势，例如自动日志收集、遥感勘测，以及对您的环境进行主动监控以发现硬件和其他已知警报。

虽然许多HX集群与Intersight连接，但Intersight目前主要用于部署、维护和监控HyperFlex集群。Intersight确实允许收集支持捆绑包和遥测信息，这通常是故障排除的良好起点。对于实时故障排除，在经典场景中，TAC工程师会使用WebEx会话RADKit。它不会取代Intersight，但会添加不同的故障排除方法，无论是使用交互式会话还是利用编程请求-响应序列。

简要概述

连接图



组件

- RADKit服务：本地RADKit服务组件，用作通往HX环境的安全网关。作为客户，您完全可以控制哪些设备可以访问，以及哪些人可以在何时访问这些设备。此服务可在任何Linux、MacOS或Windows计算机上托管。
- RADKit客户端：由TAC工程师用于访问您的环境的前端，使用编程故障排除和监控、自动检索和分析使用思科内部工具或通过CLI直接与设备进行交互的设备输出。
- RADKit云：在客户端和服务之间提供安全传输。

准备

要遵循的步骤概述

在TAC工程师利用RADKit来连接您的HX环境并进行故障排除之前，需要执行以下步骤：

1. 下载并安装RADKit服务。它可以安装在任何Linux、MacOS或Windows计算机上。
2. 启动RADKit服务并执行初始设置（引导程序）。创建超级管理员帐户，以通过网络界面进一步管理RADKit服务。
3. 向RADKit云注册您的RADKit服务。向RADKit云注册RADKit服务，并生成服务ID以识别您的环境。
4. 添加设备和终端。提供设备列表并为可能需要访问的设备存储凭证。

有关这些步骤的详细说明/一般说明，请参阅

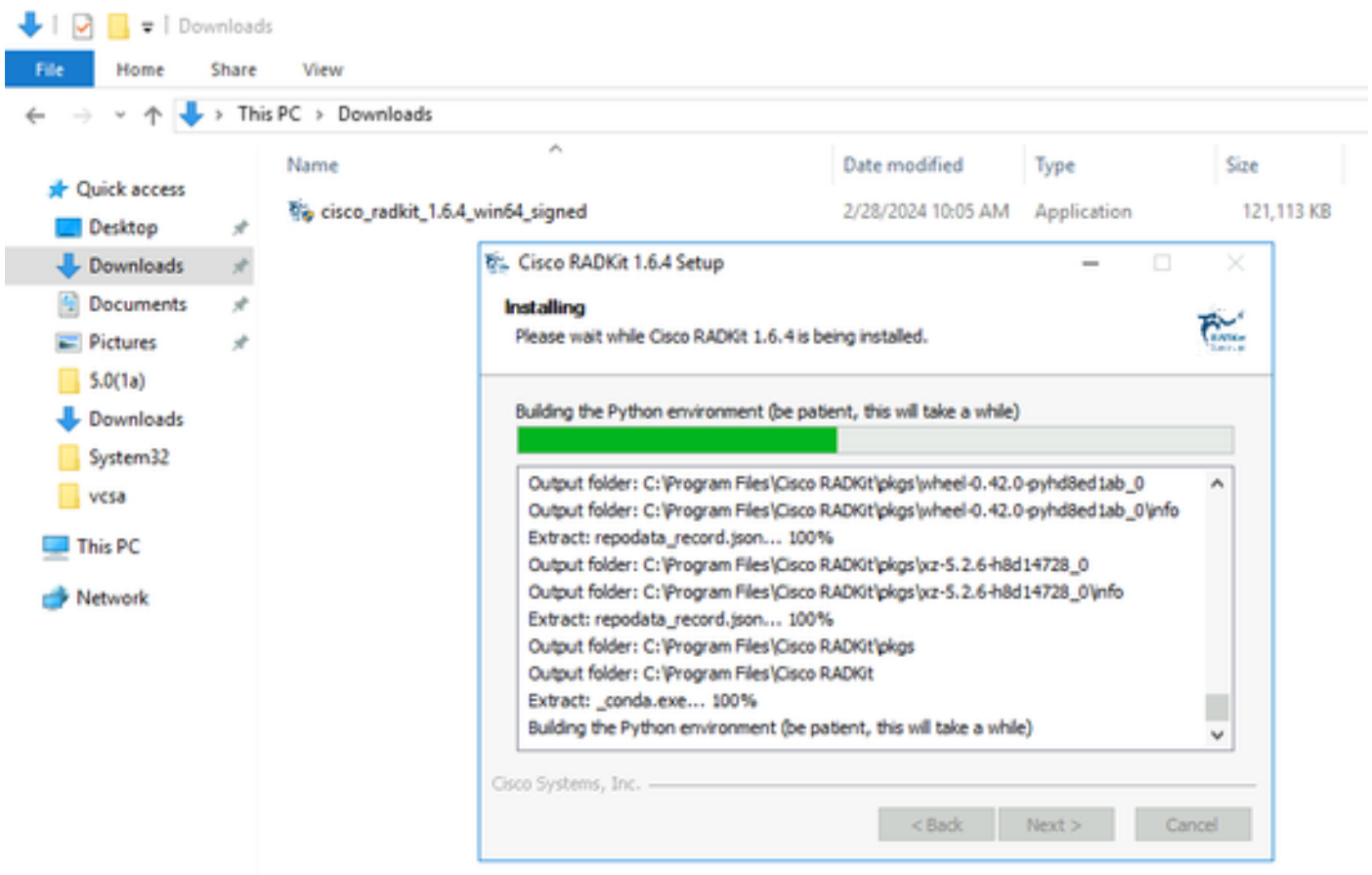
: https://radkit.cisco.com/docs/pages/one_page_setup.html

步骤1:下载并安装RADKit服务

此步骤中的详细信息可能略有不同，具体取决于用于安装RADKit服务的操作系统，但一般而言，该过程非常相似。从此处下载适用于您的OS的最新版本

: [https://radkit.cisco.com/downloads/release/。](https://radkit.cisco.com/downloads/release/)

运行系统的安装程序并按照提示操作，直到安装完成：

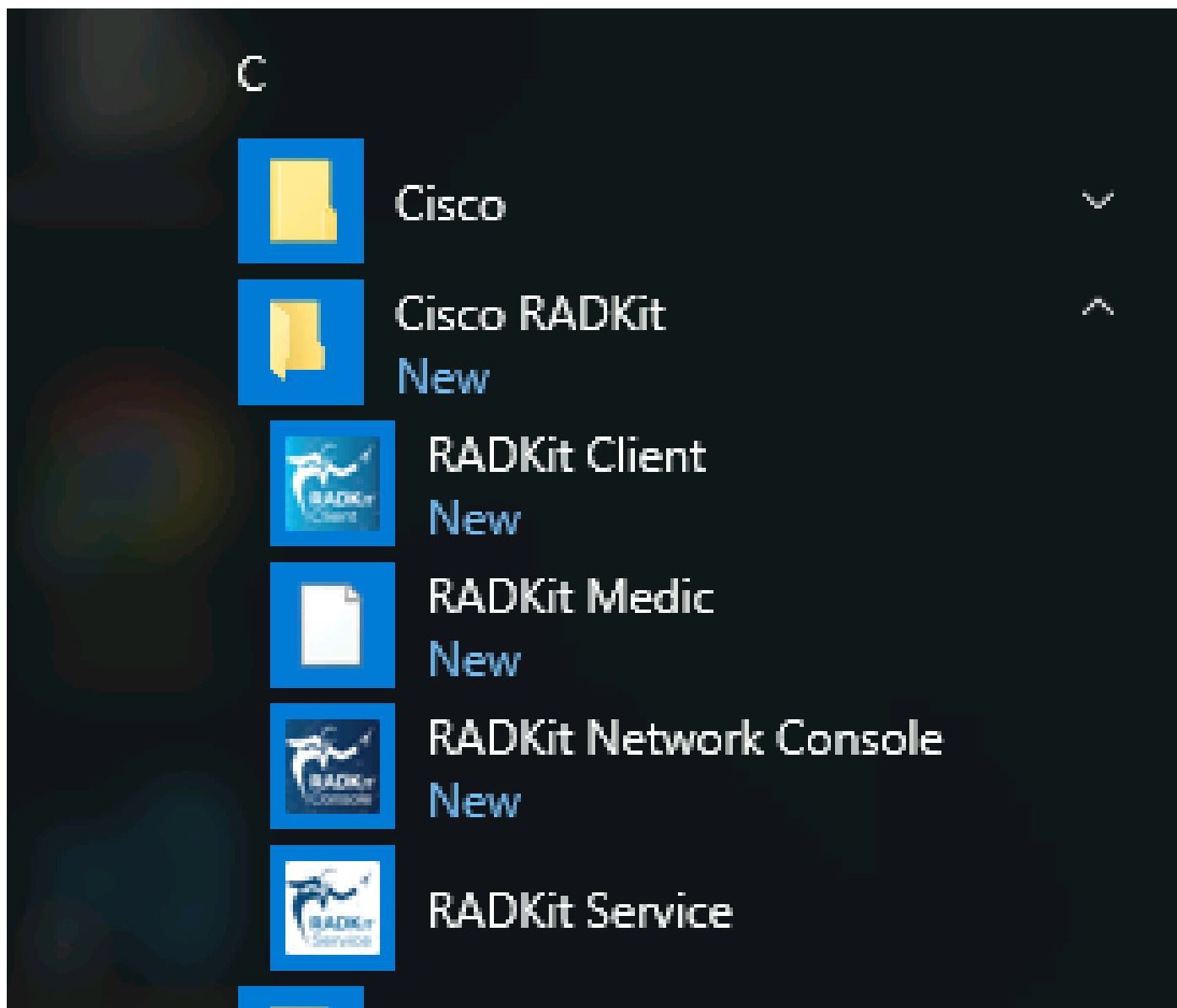


安装完所有RADKit组件后，您可以继续进行下一步，完成初始设置。

第二步：启动RADKit服务并执行初始设置（引导程序）

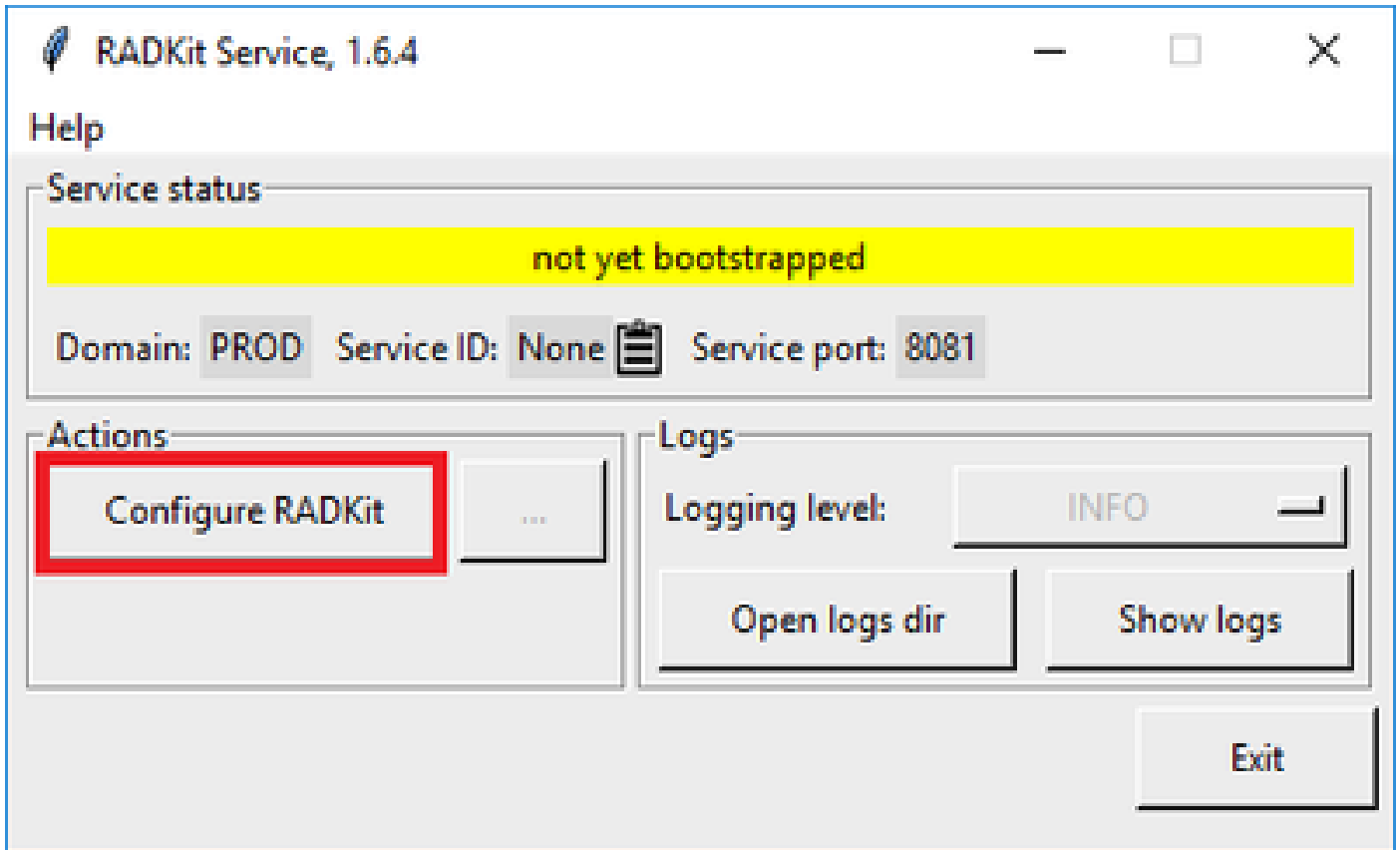
在此步骤中，创建一个superadmin帐户，以便通过网络界面进一步管理RADKit服务。

在“开始”菜单（在Windows上）或“应用程序”文件夹（在macOS上）中找到RADKit Service并启动它：



第一次启动它时，可能需要一些时间才能启动RADKit服务（大约10到30秒，具体取决于系统速度）。后续运行速度会快得多。

启动完成后，在RADKit Service对话框中，当状态更改为not yet bootstrapped时，请按Configure RADKit：



这将打开您的Web浏览器，并转到RADKit服务WebUI，这是一个基于Web的管理界面，允许您管理RADKit服务。

当连接到此URL时，会收到证书警告，您可以跳过该警告，因为此URL正在使用自签名证书。

由于superadmin用户尚不存在，WebUI将请求您为此用户创建密码：

Register superadmin user

No superadmin user was found.
Please fill in this form to create a superadmin account.



A superadmin user must be created. Please enter a strong password for this user. This password will be requested in the future to (re)start or manage RADKit Service.

Username *

Password *

Repeat Password *

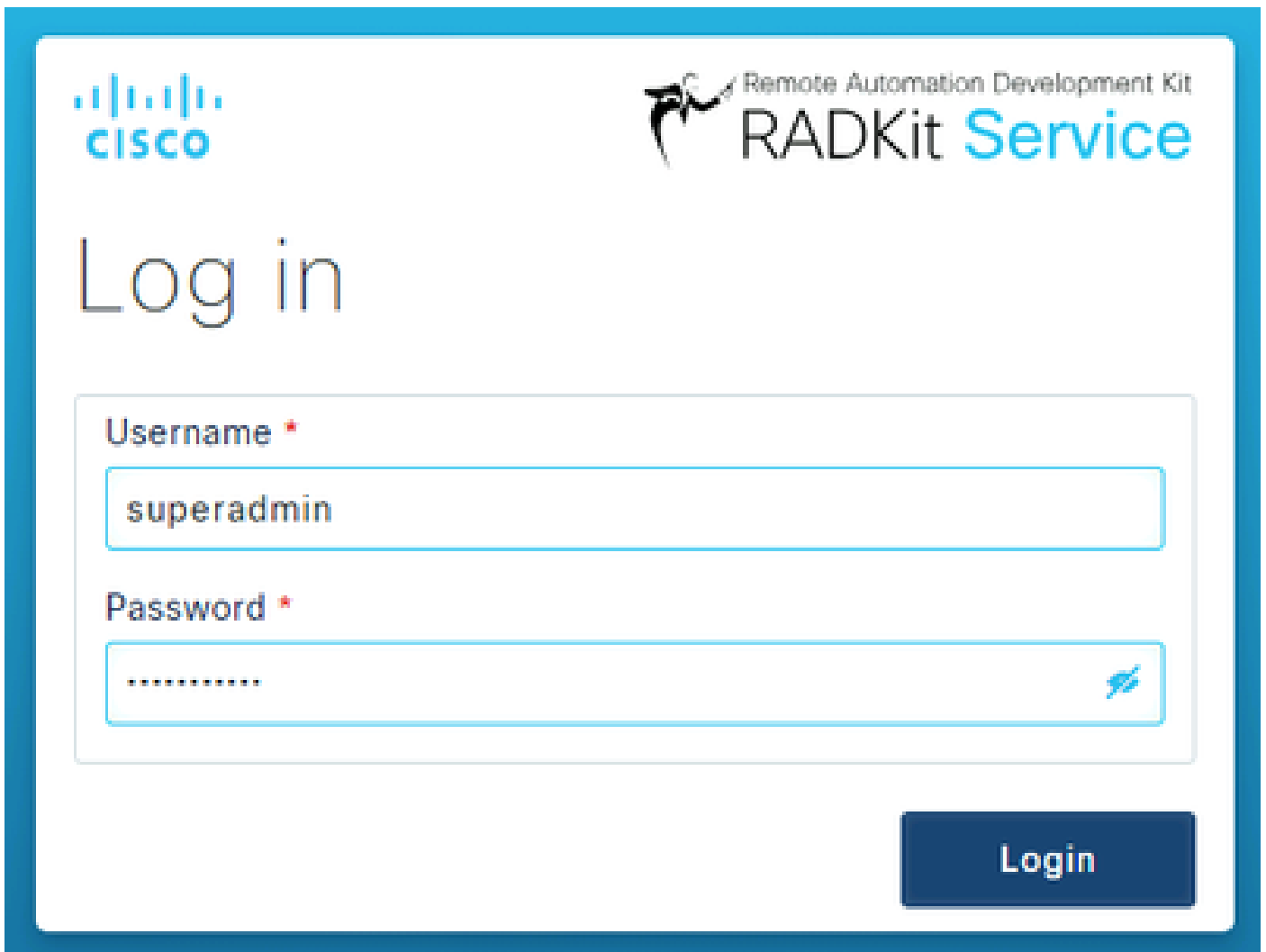
PASSWORD REQUIREMENTS:

- Minimum **8** characters
- Minimum **1** lowercase letter
- Minimum **1** uppercase letter
- Minimum **1** digit
- Minimum **1** symbol

选择符合右侧显示的密码强度要求的密码。

此帐户的密码将用于保护私钥和设备凭证等机密；如果丢失这些机密，所有机密都将丢失，需要重新初始化RADKit服务，因此请仔细选择并在安全位置将其记下。可以根据需要稍候进行更改。

创建superadmin帐户后，使用它登录WebUI：

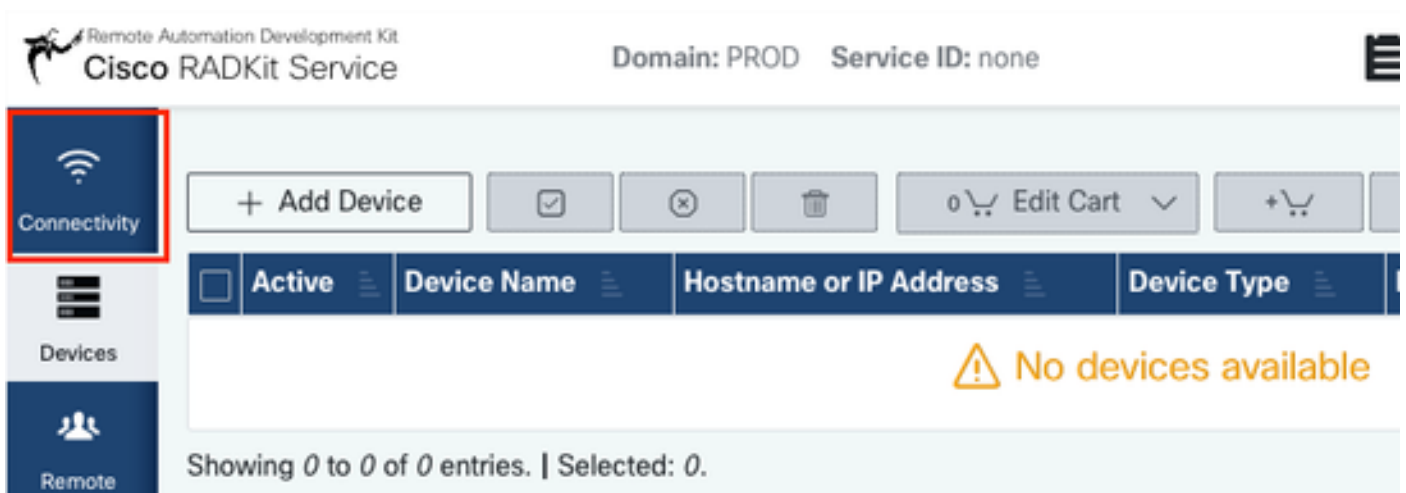


创建superadmin帐户并成功登录到WebUI后，您可以继续执行下一步，将RADKit服务注册到RADKit云组件。

第三步：使用RADKit云注册RADKit服务

在此步骤中，向RADKit云注册RADKit服务，并生成服务ID以识别您的环境。

使用superadmin用户登录WebUI后（请参阅第2步），导航到connectivity屏幕：



如果您需要代理连接互联网，请参阅此处提供的详细设置说明：https://radkit.cisco.com/docs/pages/one_page_setup.html

现在，您需要注册该服务，使其连接到RADKit云。这可通过使用您的Cisco.com (CCO)帐户通过服务WebUI登录来完成。点击Enroll with SSO以继续：

Cloud Connectivity

DOMAIN: PROD

BASE URL: <https://prod.radkit-cloud.cisco.com>

Forwarder Endpoint	Status	Latency [ms]
 No forwarder endpoints connected		

Service Identity Certificate



This RADKit Service needs to be enrolled to become functional. Please select an enrollment method by clicking one of the buttons below.

Recommended:

Enroll with SSO

Advanced:

Enroll with OTP

在第2步的email address字段中输入与您的Cisco.com (CCO)帐户对应的电子邮件地址。并单击Submit as shown in the image：

Single Sign-On Enrollment



1 Checking prerequisites

2 Email address

Provide email address for SSO login:

example@your.com

Submit

3 Connecting to the Access Service

RADKit Service连接到RADKit Cloud进行授权后，它会显示[CLICK HERE]一个链接，该链接会将您引导至思科SSO服务器进行身份验证。单击链接继续；它将在新的浏览器选项卡/窗口中打开。确保使用与之前所述步骤中输入的电子邮件地址相同的电子邮件地址登录SSO：

4 OAuth connect

5 Waiting for SSO

Follow the SSO login link to continue: [\[CLICK HERE\]](#)

6 Requesting service certificate OTP

在SSO身份验证完成后（或直接进行，如果已进行身份验证），您将进入RADKit Access确认页面。阅读页面上的信息，然后单击Accept授权RADKit服务以作为所有者通过您的CCO帐户注册。

Do you accept this authorization request?

Environment: PROD

Endpoint IP Address: 208.1.4.28:208.1.4.28

Endpoint Hostname: 208.1.4.28:208.1.4.28

This page means that a RADKit instance is attempting to connect to the RADKit Cloud with your SSO credentials.

If you *did not* initiate this request, please click "Deny" now. If you are certain that this request is legitimate, click "Accept".

If you suspect that an illegitimate session may have been granted access in the past, click the "Log out all sessions" button below to immediately log out all RADKit SSO sessions associated with your user ID. This will not log out your SSO sessions in other applications.

Accept



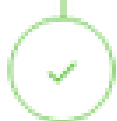
Deny

Log out all sessions

然后您将看到显示Authentication result: Success (已在上一步创建)的屏幕。

请勿点击Log out all sessions按钮，只需关闭SSO选项卡/窗口并返回到RADKit Service WebUI即可。

此处显示Service enrolled with the identity: ...。后面的唯一标识符就是您的RADKit服务ID，也称为服务序列号。在示例屏幕截图中，服务ID是您的axt9-kplb-5dwc，则不同。

-  Requesting service certificate
-  Saving the identity
-  Starting/Restarting the service

 Service enrolled with the identity: axt9-kplb-5dwc

Close

单击Close关闭对话框并返回到Connectivity屏幕。

刷新WebUI后，您的服务ID以及连接状态将显示在RADKit GUI的顶部，如下所示：



每当TAC工程师需要访问您环境中的任何设备时，他们都需要此服务ID来标识您的RADKit服务。

现在已与RADKit Cloud组件建立连接，并在建立连接时生成服务ID，在下一步中，添加可通过RADKit访问的设备。

第四步：添加设备和终端

在此步骤中，为可以通过RADKit访问的设备添加设备及其凭证。对于HyperFlex，这意味着理想情况下，需要添加这些设备及其凭证：

设备	设备类型	管理协议	凭证	转发的TCP端口	备注
虚拟机监控程序 (ESXi主机)	Linux	终端(SSH)	根		

存储控制器 (SCVM)	HyperFlex	终端 (SSH) Swagger	admin root (enable)	443	在enable password字段中输入根密码。当需要同意令牌时，将使用此命令。对于Swagger：取消选中“验证TLS证书”(Verify TLS Certificate)，并将“基本URL”(Base URL)字段留空
vCenter	Linux	终端(SSH)	根		
UCSM	通用	终端(SSH)	admin		
安装程序 (可选)	Linux	终端(SSH)	根	443	
CIMC (仅适用于边缘集群)	通用	终端(SSH)	admin		
见证 (仅适用于扩展群集)	Linux	终端(SSH)	根		
Intersight CVA/PCA (可选)	Linux	终端(SSH)	admin	443	

添加设备时必须仅使用设备的IP地址，而不使用主机名，因为要关联属于同一集群的设备，必须执行此操作。

要添加这些设备，请在RADKit WebUI中导航到Devices屏幕：



对于上面列出的每个设备，通过点击Add Device创建新条目。输入IP地址，选择设备类型，并根据集群中所有节点的每种设备类型提

供详细信息。完成后，点击Add & close返回到Devices屏幕，或点击Add & continue以添加其他设备。

您可以在此处找到每个设备类型的示例条目及其配置：

ESXi主机示例：

Edit Device [Close]

Device Name* (as it will appear in RADICSS)

Device Type*

Management IP Address or Hostname*

Jumphost Name

Forwarded TCP ports

Description

Label search ?

PSAC status: **DISABLED**

Available Labels - 0 of 0 (click to add)

Selected Labels - 0 (click to delete)

NO LABELS AVAILABLE

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

Password

If left blank, will be set to "" as default

Port

Enable Password ?

存储控制器示例：

Edit Device



Device Name (as it will appear in RedBox)

cluster2-node1-rcvm

Device Type

HyperFlex

Management IP Address or Hostname

172.16.2.14

Jumpshot Name

- Optional jumpshot -

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 jumpshot

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

* Leave unchecked if the device presents a self-signed certificate

Allow connecting using obsolete/insecure TLS algorithms

Username

admin

Password

If left blank, will be set to "" as default

Base URL

* Leave blank if unused

Update

vCenter示例：

Edit Device ✕

Device Name* (as it will appear in RADIUS) [?](#)

Device Type*

Management IP Address or Hostname* [?](#)

Jumphost Name

Forwarded TCP ports [?](#)

Description

[?](#) RBAC status: **DISABLED**

Available Labels - 0 of 0 (click to add)

NO LABELS AVAILABLE

Selected Labels - 0 (click to delete)

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

Password

If left blank, will be set to "" as default [?](#)

Port

Enable Password [?](#)

UCSM示例：

Edit Device ✕

Device Name* (as it will appear in RADKit) ?

Device Type*

Management IP Address or Hostname* ?

Jumphost Name

Forwarded TCP ports ?

Description

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

Password

If left blank, will be set to "" as default ?

Port

Enable Password ?

Update

在TAC SR上使用RADKit

如果所有准备工作都已完成，并且您希望向TAC工程师提供设备访问权限，您可以完成以下步骤。

工程师需要您的RADKit服务ID以及访问您的环境或所选设备（使用RBAC时）所需的时间。

1. 提供RADKit服务ID

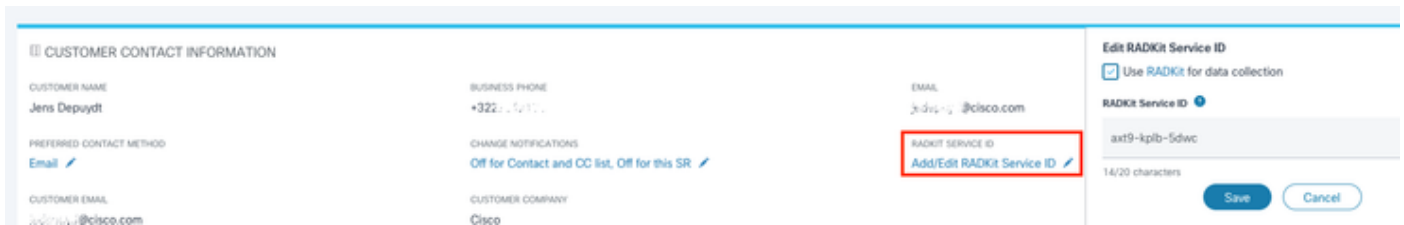
如果您尚未提交TAC支持请求，则可以在Cisco.com上的支持请求管理器中提及Use RADKit for data collection：

Use RADKit for data collection

RADKit Service ID

axt9-kplb-5dwc

如果您已经有一个未结服务请求，您可以在支持案例管理器中添加RADKit服务ID，并包含“客户联系信息”部分：

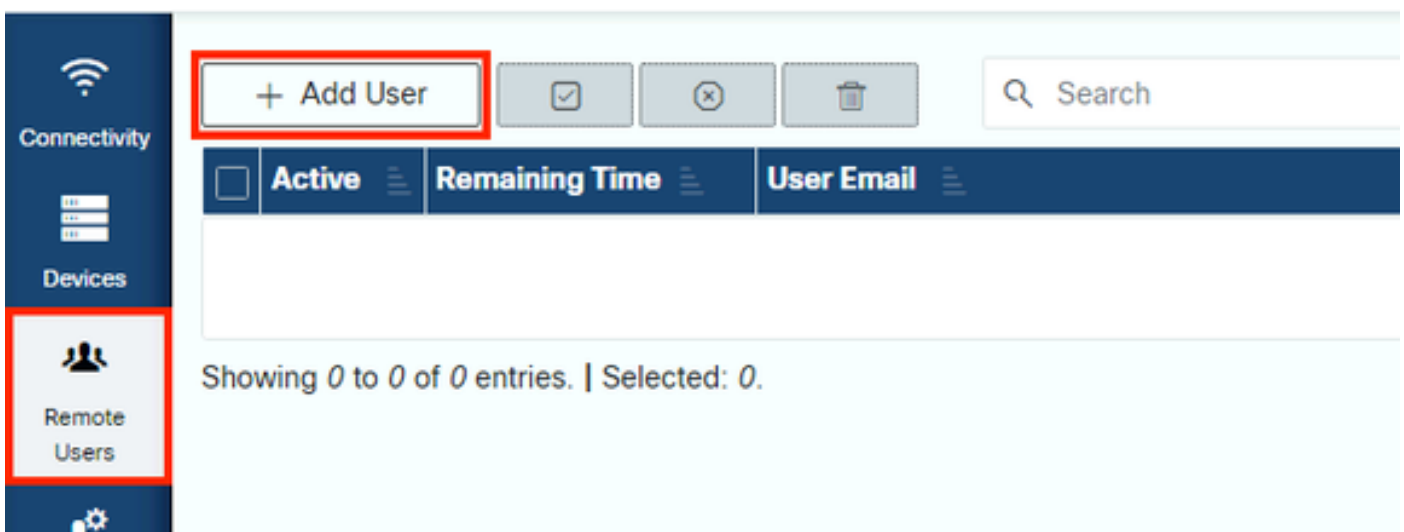


The screenshot shows the 'CUSTOMER CONTACT INFORMATION' section with fields for Customer Name (Jens Depuydt), Business Phone (+322 11111), Email (j.d@cisco.com), Preferred Contact Method (Email), and Customer Email (j.d@cisco.com). The Customer Company is Cisco. The 'Edit RADKit Service ID' panel on the right shows the 'Use RADKit for data collection' checkbox checked, the 'RADKit Service ID' field containing 'axt9-kplb-5dwc', and 'Save' and 'Cancel' buttons. A red box highlights the 'Add/Edit RADKit Service ID' link.

或者，只需将您的ID告知正在处理您的案例的TAC工程师。

2. 添加远程用户

在任何用户能够使用您的设备之前，您需要提供明确的访问权限并配置一个时间范围，以便此访问权限保持有效。为此，请在RADKit WebUI中，导航到Remote Users屏幕，并通过单击创建一个新的远程用户 Add User.



The screenshot shows the 'Remote Users' management interface. The left sidebar has 'Connectivity', 'Devices', and 'Remote Users' (highlighted with a red box). The main area has a '+ Add User' button (highlighted with a red box), a search bar, and a table with columns 'Active', 'Remaining Time', and 'User Email'. The table is currently empty, showing 'Showing 0 to 0 of 0 entries. | Selected: 0.'

输入TAC工程师的@cisco.com电邮地址（请注意输入错误）。请务必注意Activate this user复选框和Time slice或Manual 设置。

当用户处于活动状态时，用户可以通过RADKit服务访问已配置的设备，前提是这些设备已启用且RBAC策略允许这些设备。

时间片表示用户自动停用的时间量；换句话说，时间片表示有时限的故障排除会话。用户的会话可以延长到该用户的时间片持续时间。如果您倾向于手动激活/停用用户，请选择Manual。

无论用户是否配置了时间片，都可以手动激活/停用用户。当用户被停用时，其通过RADKit服务的所有会话会立即断开。

完成后，点击Add & close返回到Remote Users屏幕。

相关信息

- 有关常见问题的详细信息和答案，请访问RADKit网站：<https://radkit.cisco.com/>
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。