

Configuração RADKit para solução de problemas remota no HyperFlex

Contents

[Introdução](#)

[Informações de Apoio](#)

[O que é RADKit?](#)

[Por que RADKit para HX?](#)

[RADKit versus Intersight](#)

[Visão geral de alto nível](#)

[Diagrama de conectividade](#)

[Componentes](#)

[Preparação](#)

[Visão geral das etapas a serem seguidas](#)

[Etapa 1. Faça o download e instale o serviço RADKit](#)

[Etapa 2. Inicie o serviço RADKit e faça a configuração inicial \(Bootstrap\)](#)

[Etapa 3. Inscreva seu serviço RADKit na nuvem RADKit](#)

[Etapa 4. Adicionar dispositivos e endpoints](#)

[Usando RADKit em um TAC SR](#)

[1. Fornecer ID de Serviço RADKit](#)

[2. Adicionar Usuário Remoto](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como começar e preparar um ambiente RADKit para a solução remota de problemas em um ambiente Cisco HyperFlex.

Informações de Apoio

O objetivo principal deste documento é explicar como preparar seu ambiente para uso pelo TAC para aproveitar o RADKit para solução de problemas.

O que é RADKit?

RADKit é um orquestrador em toda a rede. Experimente uma nova forma radical de endereçar seu equipamento, impulsionar os serviços da Cisco e expandir seus recursos.

Mais informações sobre o RADKit podem ser encontradas aqui: <https://radkit.cisco.com/>

Por que RADKit para HX?

O Cisco HyperFlex consiste em vários componentes: interconexões em malha, servidores UCS, ESXi, vCenter e SCVMs. Em muitos casos, as informações de diferentes dispositivos precisam ser coletadas e correlacionadas. Durante a solução de problemas, novas informações podem ser necessárias ao longo do tempo e fazer isso em uma (longa) sessão do WebEx ou buscando pacotes de suporte (grandes) pela Intersight nem sempre é a maneira mais eficaz. Usando o RADKit, um engenheiro do TAC pode solicitar as informações necessárias durante o processo de solução de problemas, a partir de vários dispositivos e serviços, de forma segura e controlada.

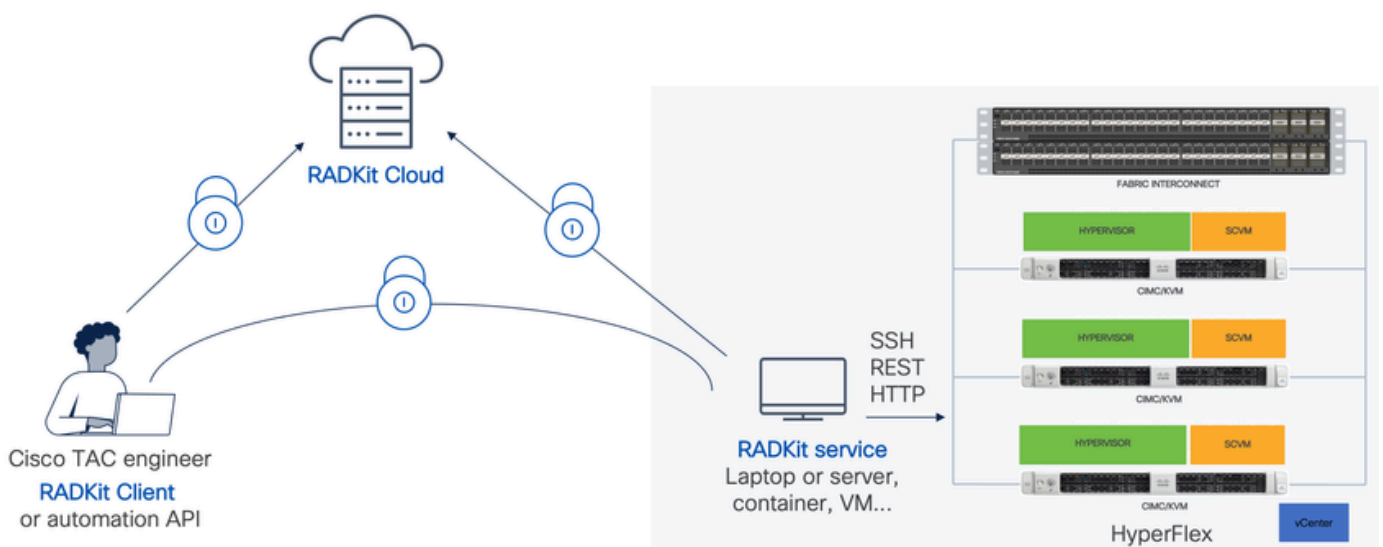
RADKit versus Intersight

A Intersight continua sendo o principal método de conectividade para clusters HyperFlex, fornecendo vários benefícios, como coleta automática de registros, telemetria e monitoramento pró-ativo do seu ambiente para hardware e outros alertas conhecidos.

Embora muitos clusters HX estejam conectados à Intersight, a Intersight atualmente se destina principalmente à implantação, manutenção e monitoramento de seus clusters HyperFlex. A Intersight permite coletar pacotes de suporte e informações de telemetria, o que geralmente é um bom ponto de partida para a solução de problemas. Para a solução de problemas ao vivo, em que, em um cenário clássico, um engenheiro do TAC utilizaria uma sessão do WebEx, o RADKit é implantado. Ele não substitui a Intersight, mas adiciona uma abordagem diferente à solução de problemas, seja usando uma sessão interativa ou aproveitando sequências programáticas de solicitação-resposta.

Visão geral de alto nível

Diagrama de conectividade



Componentes

- Serviço RADKit: componente de serviço RADkit no local, que é usado como um gateway seguro para seu ambiente HX. Como cliente, você mantém controle total sobre quais dispositivos estão acessíveis e quem pode acessá-los em determinado momento. Esse serviço pode ser hospedado em qualquer máquina Linux, MacOS ou Windows.
- Cliente RADKit: front-end usado pelo engenheiro do TAC para obter acesso ao seu ambiente, usando solução de problemas e monitoramento programáticos, recuperação automatizada e análise de saídas de dispositivos usando ferramentas internas da Cisco ou interação direta com os dispositivos por meio da CLI.
- Nuvem RADKit: fornece transporte seguro entre o cliente e o serviço.

Preparação

Visão geral das etapas a serem seguidas

Estas etapas são necessárias antes que um engenheiro do TAC possa aproveitar o RADKit para conectar e solucionar problemas do ambiente HX:

1. Baixe e instale o serviço RADkit. Ele pode ser instalado em qualquer computador Linux, MacOS ou Windows.
2. Inicie o serviço RADKit e faça a configuração inicial (bootstrap). Crie uma conta de superadministrador para gerenciar ainda mais o serviço RADKit por meio de uma interface da Web.
3. Inscreva seu serviço RADKit na nuvem RADKit. Registre seu serviço RADKit na nuvem RADKit e gere uma ID de serviço para identificar seu ambiente.
4. Adicione dispositivos e endpoints. Forneça uma lista de dispositivos e armazene credenciais para dispositivos que possam precisar ser acessados.

Uma explicação mais detalhada/genérica dessas etapas pode ser encontrada aqui:

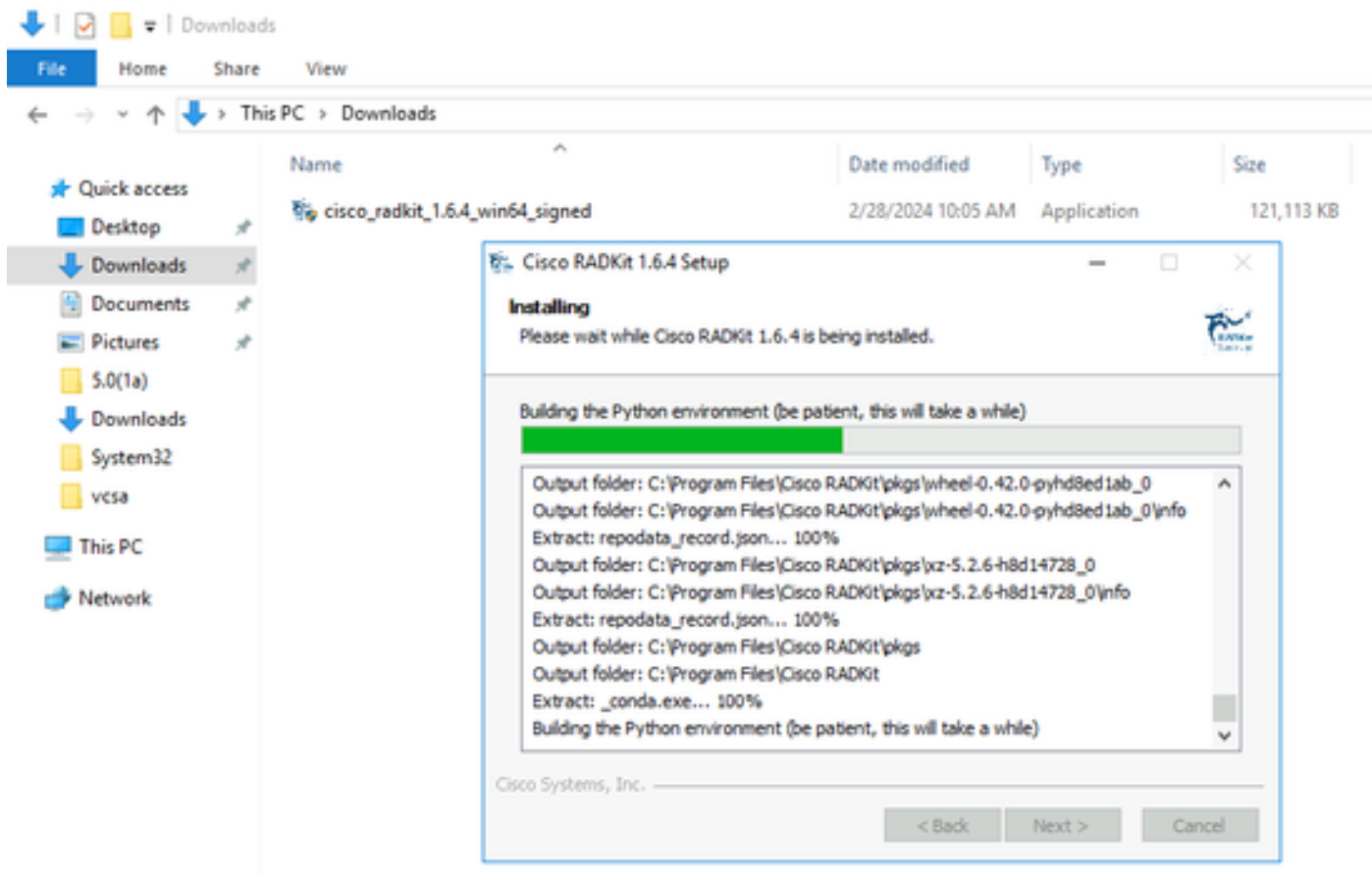
https://radkit.cisco.com/docs/pages/one_page_setup.html

Etapa 1. Faça o download e instale o serviço RADKit

Os detalhes nesta etapa podem ser um pouco diferentes, dependendo do sistema operacional que você está usando para instalar o serviço RADKit, mas, em geral, o processo é muito semelhante. Faça o download da versão mais recente para o seu SO aqui:

<https://radkit.cisco.com/downloads/release/>.

Execute o instalador do sistema e siga os avisos até que a instalação seja concluída:



Depois que todos os componentes RADKit estiverem instalados, você poderá passar para a próxima etapa da configuração inicial.

Etapa 2. Inicie o serviço RADKit e faça a configuração inicial (Bootstrap)

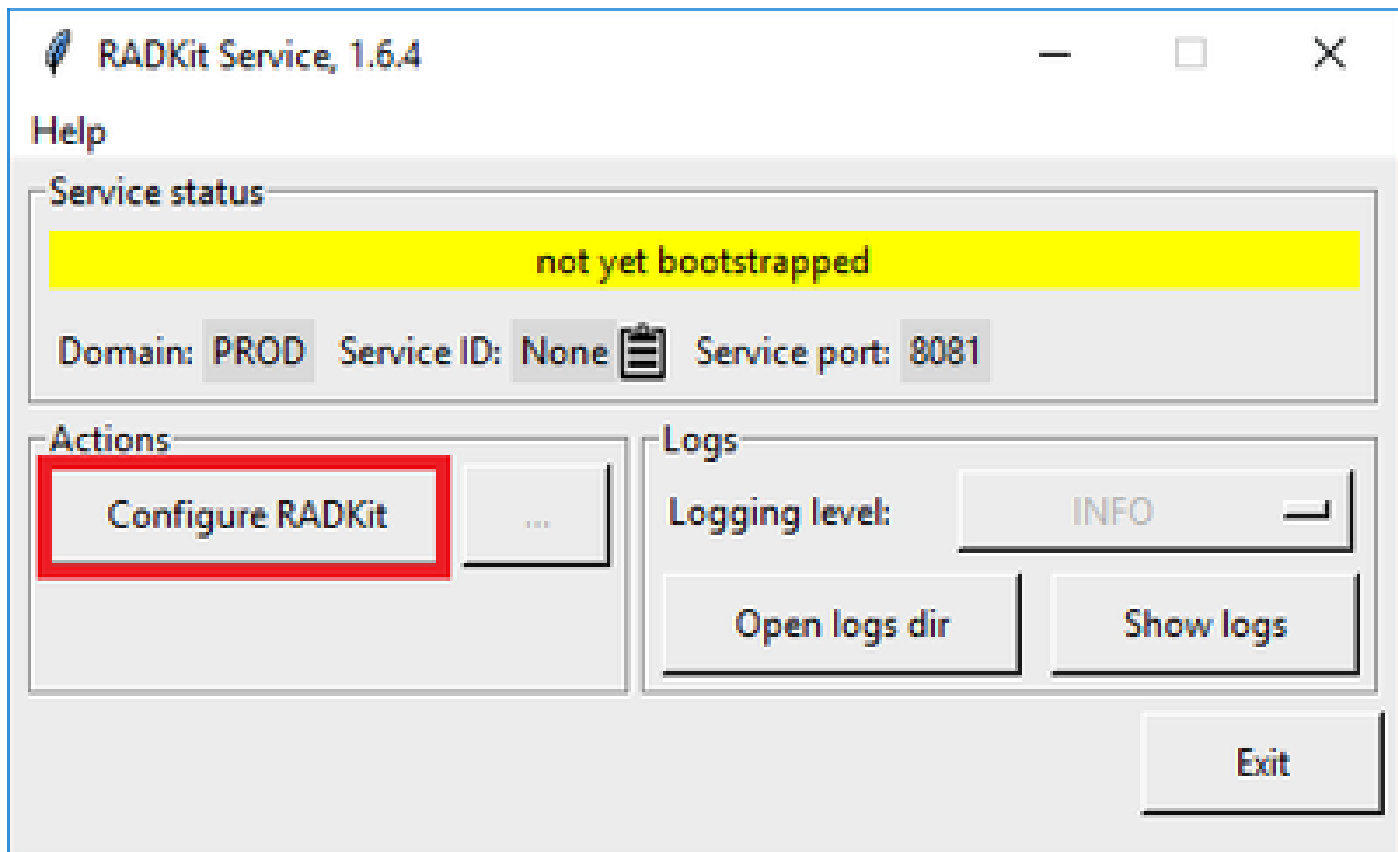
Nesta etapa, crie uma conta superadmin para gerenciar ainda mais o serviço RADKit por meio de uma interface da Web.

Localize RADKit Service o menu Iniciar (no Windows) ou a pasta Aplicativos (no macOS) e inicie-o:



Na primeira vez que você iniciá-lo, pode demorar um pouco para que o Serviço RADKit seja iniciado (cerca de 10 a 30 segundos, dependendo da velocidade do sistema). As execuções subsequentes serão muito mais rápidas.

Após a conclusão da inicialização, na caixa de diálogo Serviço RADKit, uma vez que o status seja alterado para not yet bootstrapped pressioneConfigure RADKit :



Isso abre seu navegador da Web e o direciona para a WebUI do serviço RADKit, uma interface de gerenciamento baseada na Web que permite gerenciar o serviço RADKit.

Espera-se obter um aviso de certificado, que você pode ignorar, ao conectar-se a esta URL, pois ela está usando um certificado autoassinado.

Como um usuário superadmin ainda não existe, a WebUI solicitará que você crie uma senha para este usuário:

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

Selecione uma senha que atenda aos requisitos de força de senha exibidos à direita.

A senha desta conta será usada para proteger segredos, como chaves privadas e credenciais de dispositivo; se você perdê-la, todos os segredos serão perdidos e o Serviço RADKit precisará ser reinicializado, então escolha-a cuidadosamente e anote-a em um local seguro. Ele pode ser alterado posteriormente, conforme necessário.

Depois de criar a conta superadmin, use-a para fazer login na WebUI:



Log in

Username *

superadmin

Password *

.....



Login

Depois que a conta superadmin tiver sido criada e você tiver feito login com êxito na WebUI, você poderá continuar para a próxima etapa em que seu serviço RADKit está registrado com o componente de nuvem RADKit.

Etapa 3. Inscreva seu serviço RADKit na nuvem RADKit

Nesta etapa, registre seu serviço RADKit na nuvem RADKit e gere uma ID de serviço para identificar seu ambiente.

Depois de fazer login na WebUI com o usuário superadmin (consulte a etapa 2), navegue até a tela de conectividade:

Remote Automation Development Kit
Cisco RADKit Service

Domain: PROD Service ID: none

Connectivity

+ Add Device

o Edit Cart

Active	Device Name	Hostname or IP Address	Device Type
⚠ No devices available			

Showing 0 to 0 of 0 entries. | Selected: 0.


Caso você precise de um proxy para se conectar à Internet, consulte as instruções detalhadas de configuração disponíveis aqui:

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


Agora você precisa inscrever o serviço para permitir que ele se conecte à nuvem RADKit. Isso é feito fazendo login através da WebUI de serviço usando sua conta Cisco.com (CCO). Clique Enroll with SSO para continuar:

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: **Advanced:**

Enroll with SSO **Enroll with OTP**

Insira o endereço de e-mail correspondente à sua conta Cisco.com (CCO) no campo de endereço de e-mail na Etapa 2. e clique em Submit as shown in the image:

Single Sign-On Enrollment



✓ Checking prerequisites

2 Email address

Provide email address for SSO login:

XXXXXXXXXX@XXXX.XXX.XXX

Submit

3 Connecting to the Access Service

Depois que o serviço RADKit se conecta à nuvem RADKit para obter autorização, ele mostra um [CLICK HERE] link que o leva ao servidor Cisco SSO para autenticação. Clique no link para continuar; ele será aberto em uma nova guia/janela do navegador. Certifique-se de usar o mesmo endereço de e-mail para fazer login no SSO, como o que você inseriu na etapa mencionada anteriormente:

✓ OAuth connect

5 Waiting for SSO

Follow the SSO login link to continue: **[CLICK HERE]**

6 Requesting service certificate OTP

Depois que a autenticação SSO estiver concluída (ou imediatamente, se você já tiver sido autenticado), você será direcionado para uma página de confirmação de acesso RADKit. Leia as informações que estão na página e clique em Accept para autorizar o serviço RADKit a se inscrever com sua conta CCO como proprietário.

Do you accept this authorization request?

Environment: PROD

Endpoint IP Address: 208.1.4.28:2049-1800-1800

Endpoint Hostname: 208.1.4.28:2049-1800-1800

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

Em seguida, você chega a uma tela que diz Authentication result: Success .

Não clique no botão Log out all sessions; em vez disso, basta fechar a guia/janela SSO e retornar à WebUI do serviço RADKit.

Isso mostra Service enrolled with the identity: O identificador exclusivo a seguir é o ID de serviço do RADKit, também conhecido como Número de série do serviço. Na captura de tela do exemplo, a ID do serviço é axt9-kplb-5dwc sua será diferente.

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

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

Close

Clique Close para fechar a caixa de diálogo e retornar à Connectivity tela.

Após atualizar a WebUI, sua ID de serviço é exibida na parte superior da GUI do RADKit, junto com o status de conectividade como visto aqui:



Sempre que um engenheiro do TAC precisar acessar qualquer um dos dispositivos em seu ambiente, ele precisará dessa ID de serviço para identificar o serviço RADKit.

Agora que uma conectividade foi estabelecida com o componente de nuvem RADKit e gerou uma ID de serviço, na próxima etapa, adicione os dispositivos que podem ser acessados por meio do RADKit.

Etapa 4. Adicionar dispositivos e endpoints

Nesta etapa, adicione os dispositivos e suas credenciais para os dispositivos que podem ser acessados por meio do RADKit. Para o HyperFlex, isso significa que, de preferência, esses dispositivos e suas credenciais precisam ser adicionados:

Dispositivo	tipo de dispositivo	Protocolos de gerenciamento	Credenciais	Portas TCP encaminhadas	Lembretes
Hipervisor (hosts ESXi)	Linux	Terminal (SSH)	root		

Controlador de armazenamento (SCVM)	HyperFlex	Terminal (SSH)Swagger	admin root (enable)	443	Digite a senha raiz no campo enable password. Isso será usado quando um token de consentimento for necessário. Para Swagger: desmarque "Verificar certificado TLS" e deixe o campo URL base vazio
vCenter	Linux	Terminal (SSH)	root		
UCSM	GENÉRICO	Terminal (SSH)	admin		
Instalador (opcional)	Linux	Terminal (SSH)	root	443	
CIMC (somente para clusters de borda)	GENÉRICO	Terminal (SSH)	admin		
Testemunha (apenas para clusters ampliados)	Linux	Terminal (SSH)	root		
Intersight CVA/PCA (opcional)	Linux	Terminal (SSH)	admin	443	

É importante adicionar os dispositivos somente usando seu endereço IP e não seu nome de host, pois isso é necessário para correlacionar os

dispositivos que pertencem ao mesmo cluster.

Para adicionar esses dispositivos, na WebUI do RADKit, navegue até a tela Devices:



Remote Automation Development Kit
Cisco RADKit Service

Domain: PROD Service ID: axt9-kplb-5dwc

+ Add Device

o Edit Cart

Active Device Name Hostname or IP Address Device Type In

No devices available

Showing 0 to 0 of 0 entries. | Selected: 0.

Para cada um dos dispositivos listados acima, crie uma nova entrada clicando em Add Device . Insira o endereço IP, selecione o tipo de dispositivo e forneça detalhes, dependendo de cada tipo de dispositivo, para todos os nós no cluster. Ao terminar, clique em Add & close para voltar à tela Dispositivos ou Add & continue para adicionar outro dispositivo.

Aqui você pode encontrar entradas de exemplo e suas configurações para cada tipo de dispositivo:

Exemplo para hosts ESXi:

Edit Device ✕

Device Name* (as it will appear in RADIC8) ?

Device Type*

Management IP Address or Hostname* ?

Jumphost Name

Forwarded TCP ports ?

Description

?

PSAC 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 ?

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

Update

Exemplo para controladores de armazenamento:

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

Exemplo para o vCenter:

Edit Device ✕

Device Name* (as it will appear in RADIX) [?](#)
cluster2-vcenter

Device Type*
Linux

Management IP Address or Hostname* [?](#)
172.16.0.22

Jumphost Name
- Optional jumphost -

Forwarded TCP ports [?](#)
Port ranges (eg. "1-1024,8888")

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
root

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

Port
22

Enable Password [?](#)

[Update](#)

Exemplo de UCSM:

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

Usando RADKit em um TAC SR

Se toda a preparação for feita e você quiser fornecer acesso aos seus dispositivos para um engenheiro do TAC, você pode passar por essas etapas.

Um engenheiro precisa de sua ID de serviço RADKit e acesso ao seu ambiente ou a dispositivos selecionados (ao usar RBAC) pelo tempo necessário.

1. Fornecer ID de Serviço RADKit

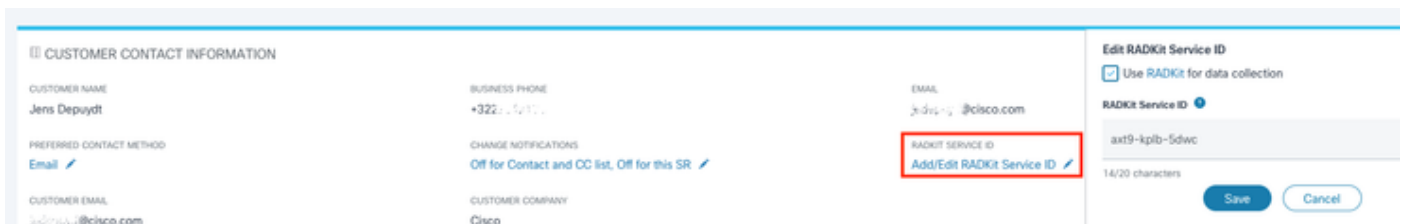
Se você ainda não abriu um caso de TAC, tem a oportunidade de mencionar Use RADKit for data collection no Support Case Manager em Cisco.com:

Use RADKit for data collection

RADKit Service ID 

axt9-kplb-5dwc

Caso você já tenha uma solicitação de serviço aberta, poderá adicionar a ID de serviço RADKit no Gerenciador de caso de suporte com a seção Informações de contato do cliente:

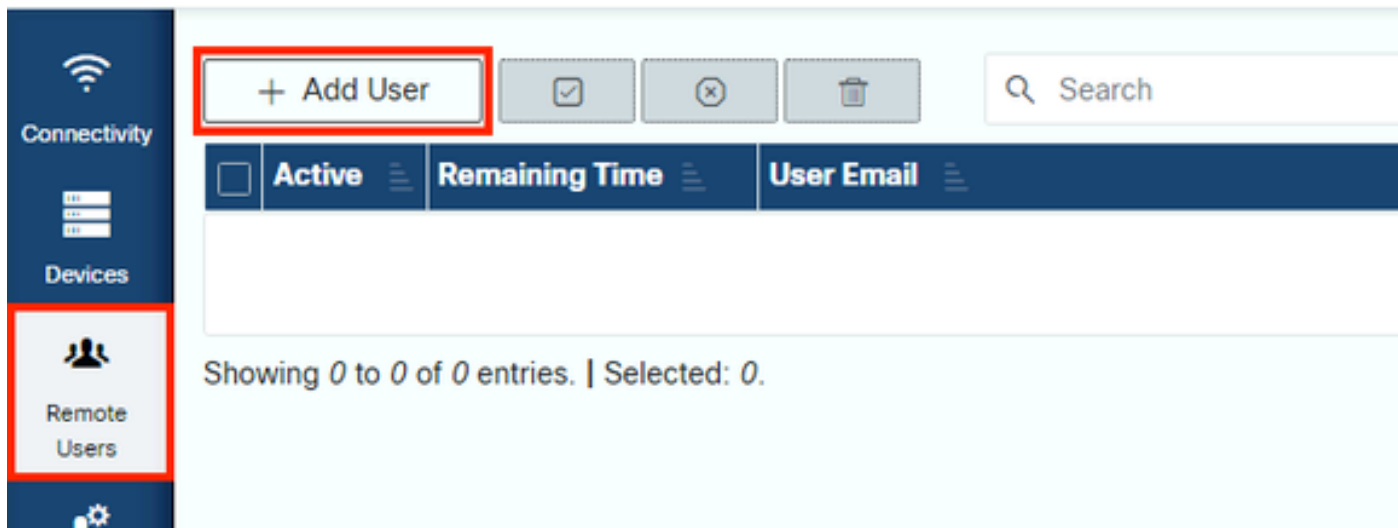


The screenshot shows a web interface for managing a support case. On the left, under 'CUSTOMER CONTACT INFORMATION', there are fields for 'CUSTOMER NAME' (Jens Depuydt), 'BUSINESS PHONE' (+322 11111), 'EMAIL' (jens.depuydt@cisco.com), 'PREFERRED CONTACT METHOD' (Email), and 'CUSTOMER EMAIL' (jens.depuydt@cisco.com). In the center, there are 'CHANGE NOTIFICATIONS' (Off for Contact and CC list, Off for this SR) and 'CUSTOMER COMPANY' (Cisco). On the right, there is a section for 'Edit RADKit Service ID' with a checked box for 'Use RADKit for data collection' and a 'RADKit Service ID' field containing 'axt9-kplb-5dwc'. A red box highlights the 'Add/Edit RADKit Service ID' link. Below the field are 'Save' and 'Cancel' buttons.

Ou simplesmente mencione sua identificação para o engenheiro do TAC que está trabalhando em seu caso.

2. Adicionar Usuário Remoto

Antes que qualquer usuário possa trabalhar com seus dispositivos, você precisa fornecer acesso explícito e configurar um período para o qual esse acesso permanece válido. Para fazer isso, na WebUI do RADKit, navegue até a tela Remote Users e crie um novo usuário remoto clicando em Add User.



Insira o endereço de e-mail @cisco.com do engenheiro do TAC (tenha cuidado com erros de digitação). Preste atenção à caixa **Activate this user** de seleção e às **Time slice** configurações ou **Manual** do .

Enquanto o usuário estiver ativo, ele terá acesso aos dispositivos configurados através do Serviço RADKit, desde que esses dispositivos estejam habilitados e que a política RBAC permita.

A fatia de tempo representa a quantidade de tempo após a qual o usuário será automaticamente desativado; em outras palavras, uma fatia de tempo representa uma sessão de solução de problemas com limite de tempo. A sessão do usuário pode ser estendida até a duração da fatia de tempo para esse usuário. Se preferir ativar/desativar usuários manualmente, selecione **Manual**.

Os usuários sempre podem ser ativados/desativados manualmente, independentemente de terem uma fatia do tempo configurada ou não. Quando um usuário é desativado, todas as suas sessões através do Serviço RADKit são desconectadas instantaneamente.

Ao concluir, clique **Add & close** para voltar à tela **Usuários remotos**.

Informações Relacionadas

- Mais informações e respostas para perguntas comuns podem ser encontradas no site da RADKit: <https://radkit.cisco.com/>
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.