

HyperFlexでのリモートトラブルシューティングのためのRADKitのセットアップ

内容

[はじめに](#)

[背景説明](#)

[RADKitとは](#)

[HXのRADKitが選ばれる理由](#)

[RADKitとIntersight](#)

[概要](#)

[接続図](#)

[コンポーネント](#)

[準備](#)

[実行手順の概要](#)

[ステップ 1: RADKitサービスのダウンロードとインストール](#)

[ステップ 2: RADKitサービスを開始し、初期セットアップ（ブートストラップ）を実行します](#)

[ステップ 3: RADKitサービスをRADKit Cloudに登録する](#)

[ステップ 4: デバイスとエンドポイントの追加](#)

[TAC SRでのRADKitの使用](#)

[1. RADKitサービスIDを入力します。](#)

[2. リモートユーザーの追加](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco HyperFlex環境のリモートトラブルシューティングを開始し、RADKit環境を準備する方法について説明します。

背景説明

このドキュメントの主な目的は、TACがRADKitをトラブルシューティングに利用できるように環境を準備する方法を説明することです。

RADKitとは

RADKネットワーク全体のオーケストレータです。機器に対処する根本的な新しい方法を体験できます。シスコのサービスが強化され、機能が拡張されます。

RADKitの詳細については、次のサイトを参照してください。 <https://radkit.cisco.com/>

HXのRADKitが選ばれる理由

Cisco HyperFlexは、ファブリックインターコネクト、UCSサーバ、ESXi、vCenter、およびSCVMの複数のコンポーネントで構成されます。多くの場合、異なるデバイスからの情報を収集して関連付ける必要があります。トラブルシューティングを行う際には、時間の経過とともに新しい情報が必要になる場合があります。この作業を（長い）WebExセッションで行うか、Intersightを通じて（大きな）サポートバンドルを取得することが、必ずしも最も効果的な方法とは限りません。TACエンジニアは、RADKitを使用して、トラブルシューティングプロセスで必要な情報をさまざまなデバイスやサービスから安全かつ制御された方法で要求できます。

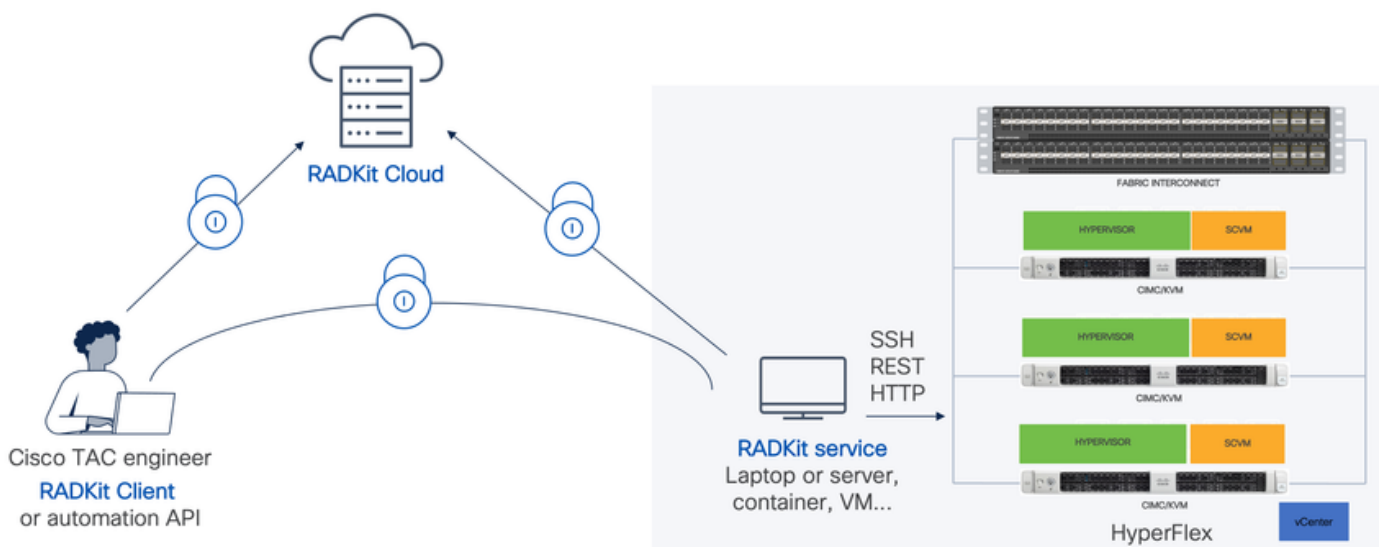
RADKitとIntersight

Intersightは、HyperFlexクラスタの主要な接続方法として引き続き機能し、ログの自動収集、テレメトリ、ハードウェアやその他の既知のアラートに対する環境の予防的なモニタリングなど、数多くのメリットを提供します。

多くのHXクラスタはIntersightに接続されていますが、Intersightは現在、主にHyperFlexクラスタの導入、メンテナンス、および監視を目的としています。Intersightはサポートバンドルとテレメトリ情報を収集する機能を提供します。これは通常、トラブルシューティングの開始点として適しています。ライブトラブルシューティングでは、従来のシナリオではTACエンジニアがWebExセッションを利用してRADKitを導入していました。これはIntersightに取って代わるものではありませんが、インタラクティブなセッションを使用するか、プログラムによる要求/応答シーケンスを利用して、トラブルシューティングに別のアプローチを追加します。

概要

接続図



コンポーネント

- **RADKit Service** : オンプレミスのRADkitサービスコンポーネントで、HX環境へのセキュア

なゲートウェイとして使用されます。お客様は、アクセス可能なデバイスと、アクセス可能なユーザを常に完全に制御できます。このサービスは、任意のLinux、MacOS、またはWindowsマシンでホストできます。

- RADKit Client:TACエンジニアがフロントエンドを使用して環境にアクセスします。プログラムによるトラブルシューティングとモニタリング、シスコ内部のツールを使用したデバイス出力の自動取得と分析、またはCLIを介したデバイスとの直接対話を使用します。
- RADKitクラウド：クライアントとサービス間のセキュアな転送を提供します。

準備

実行手順の概要

TACエンジニアがRADKitを活用してHX環境の接続とトラブルシューティングを行うには、次の手順が必要です。

1. RADKitサービスをダウンロードしてインストールします。Linux、MacOS、またはWindowsマシンにインストールできます。
2. RADKitサービスを開始し、初期セットアップ（ブートストラップ）を行います。Webインターフェイスを介してRADKitサービスをさらに管理するためのスーパー管理者アカウントを作成します。
3. RADKitサービスをRADKitクラウドに登録します。RADKitクラウドにRADKitサービスを登録し、環境を識別するサービスIDを生成します。
4. デバイスとエンドポイントを追加します。デバイスのリストを提供し、アクセスが必要なデバイスのクレデンシャルを保存します。

これらの手順に関するより詳細で一般的な説明については、次のサイトを参照してください。

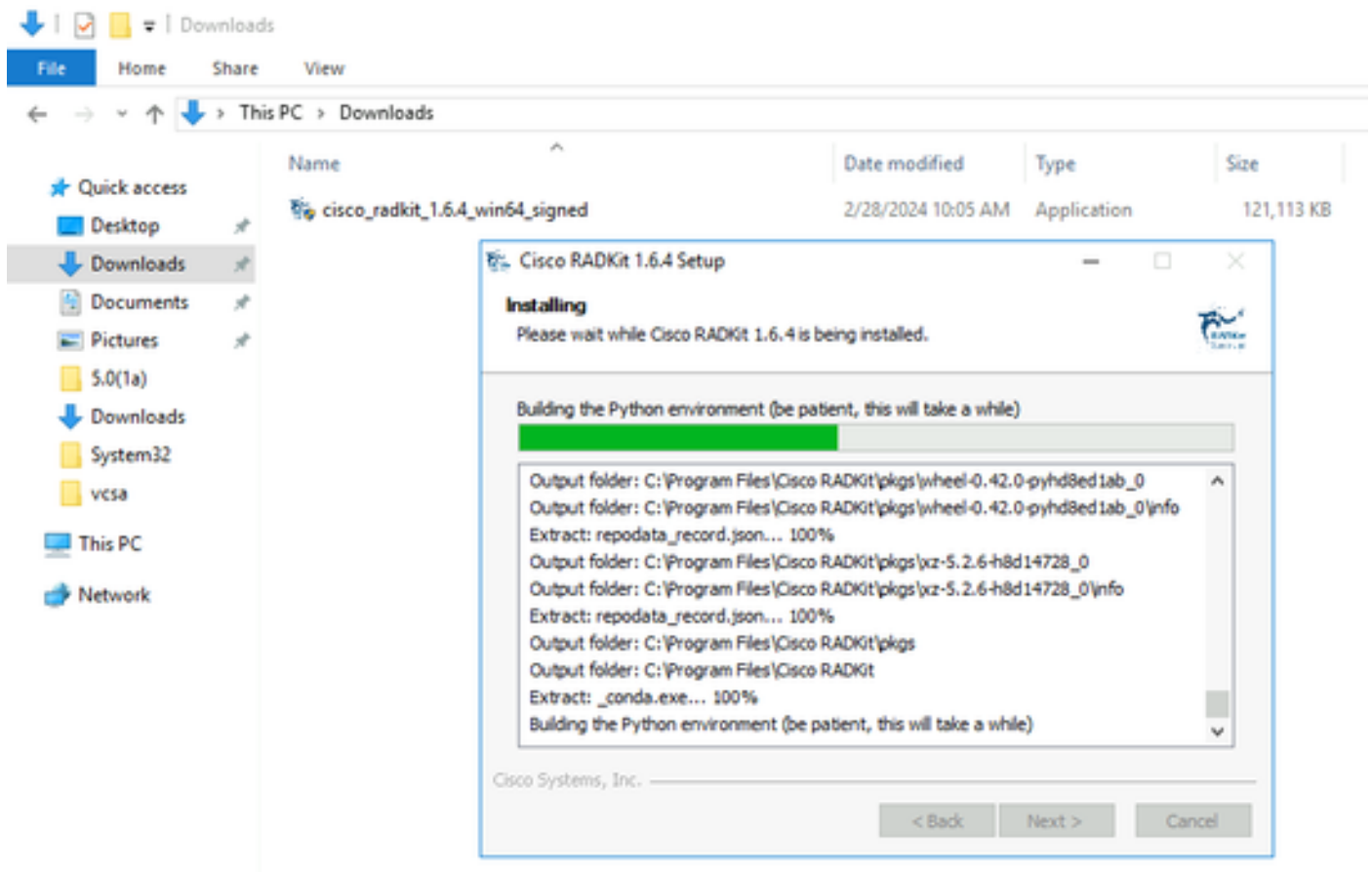
https://radkit.cisco.com/docs/pages/one_page_setup.html

ステップ 1：RADKitサービスのダウンロードとインストール

この手順の詳細は、RADKitサービスをインストールするために使用しているOSによって少し異なる場合がありますが、一般的にはプロセスは非常に似ています。OSの最新リリースは、

<https://radkit.cisco.com/downloads/release/>からダウンロードします。

システムのインストーラを実行し、プロンプトに従ってインストールが完了します。

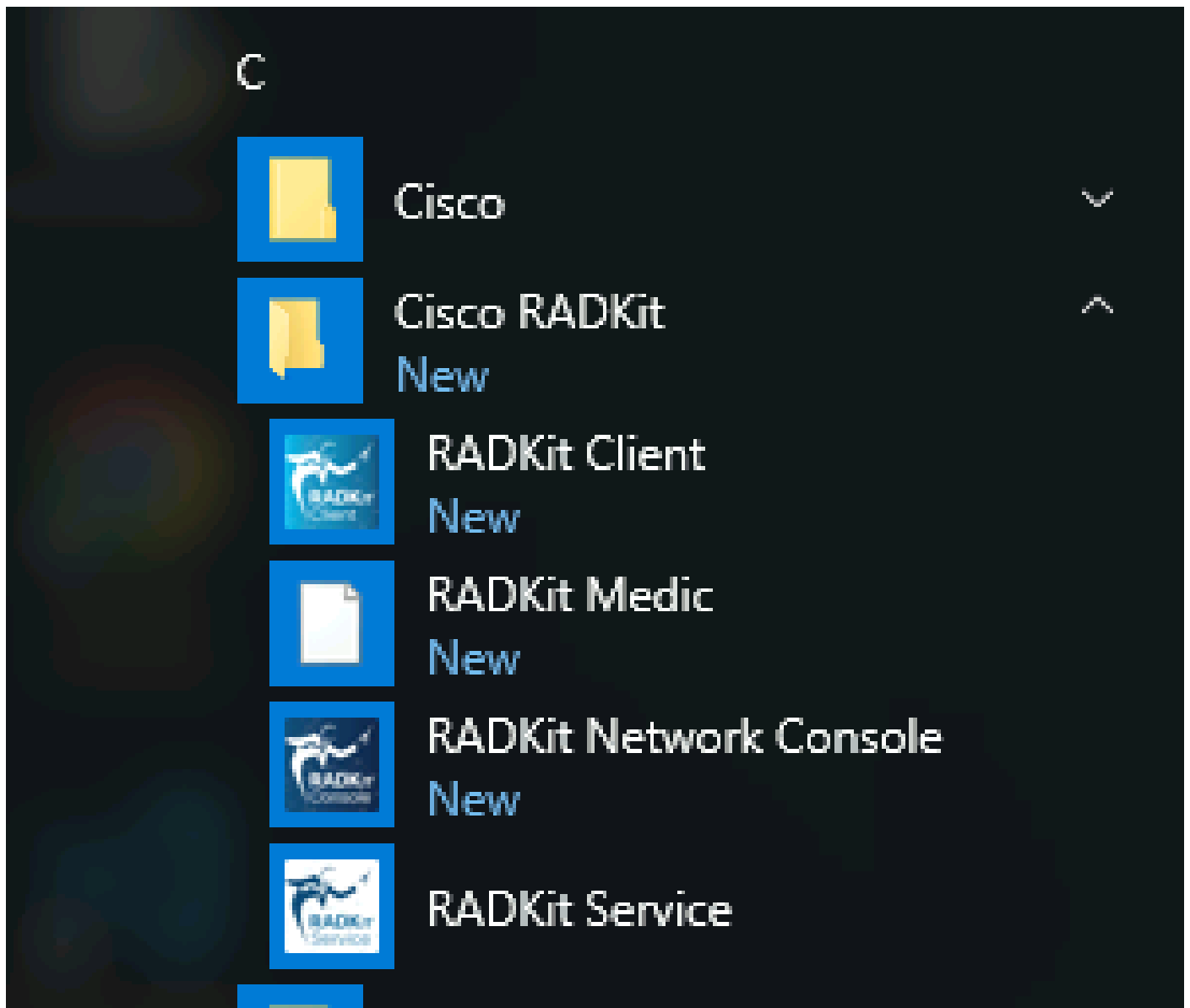


すべてのRADKitコンポーネントがインストールされたら、次の手順に進んで初期設定を行います。

ステップ 2 : RADKitサービスを開始し、初期セットアップ (ブートストラップ) を実行します

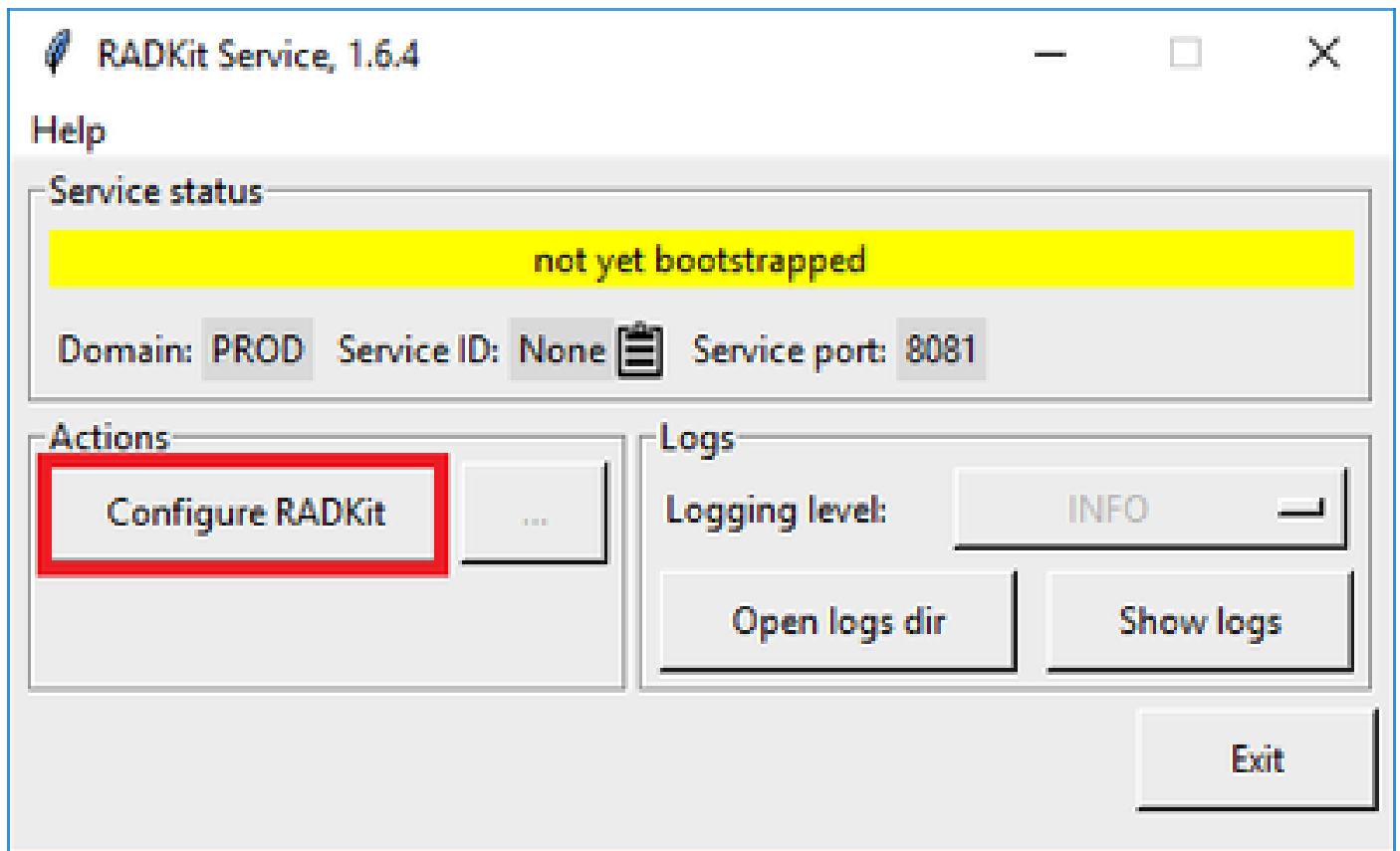
この手順では、Webインターフェイスを介してRADKitサービスをさらに管理するためのsuperadminアカウントを作成します。

スタートメニュー (Windowsの場合) またはアプリケーションフォルダ (macOSの場合) でRADKit Serviceを探して起動します。



RADKit Serviceを初めて起動する場合、起動に少し時間がかかることがあります（システムの速度によって約10～30秒）。後続の実行ははるかに速くなります。

起動が完了したら、[RADKit Service]ダイアログで、ステータスがnot yet bootstrappedに変わったら、「Configure RADKit」を押します。



Webブラウザが開き、RADKitサービスを管理できるWebベースの管理インターフェイスであるRADKitサービスWebUIが表示されます。

自己署名証明書を使用しているためにこのURLに接続すると、スキップできる証明書の警告が表示されることが予想されます。

superadminユーザはまだ存在しないため、WebUIはこのユーザのパスワードを作成するように要求します。



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

Submit

右側に表示されているパスワードの強度の要件に適合するパスワードを選択します。

このアカウントのパスワードは、秘密キーやデバイス資格情報などの秘密を保護するために使用されます。パスワードを紛失した場合、すべての秘密が失われ、RADKitサービスを再初期化する必要があります。パスワードは慎重に選択し、安全な場所に書き留めてください。必要に応じて後で変更できます。

superadminアカウントを作成した後、それを使用してWebUIにログインします。

 Remote Automation Development Kit
RADKit Service

Log in

Username *

superadmin

Password *

.....

Login

superadminアカウントが作成され、WebUIへのログインに成功したら、RADKitサービスがRADKitクラウドコンポーネントに登録されている次の手順に進むことができます。

ステップ 3 : RADKitサービスをRADKit Cloudに登録する

この手順では、RADKitクラウドにRADKitサービスを登録し、環境を識別するサービスIDを生成します。

superadminユーザでWebUIにログインした後（ステップ2を参照）、接続画面に移動します。

 Remote Automation Development Kit
Cisco RADKit Service

Domain: PROD Service ID: none

Connectivity

Devices

Remote

+ Add Device

☐

☐

☐

☐

o Edit Cart

+ Add

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

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

インターネットに接続するためにプロキシが必要な場合、詳細なセットアップ手順 (https://radkit.cisco.com/docs/pages/one_page_setup.html)を参照してください。

サービスを登録して、RADKit Cloudに接続できるようにする必要があります。これは、Cisco.com(CCO)アカウントを使用してService WebUI経由でログインすることで行われます。Enroll with SSOをクリックして次に進みます。

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

ステップ2の電子メールアドレスフィールドに、Cisco.com(CCO)アカウントに対応する電子メールアドレスを入力し、Submit as shown in the image:

Single Sign-On Enrollment



✓ Checking prerequisites

2 Email address

Provide email address for SSO login:

shimada@radkit.com

Submit

3 Connecting to the Access Service

RADKitサービスが認証のためにRADKitクラウドに接続すると、認証のためにCisco SSOサーバに移動する[CLICK HERE]リンクが表示されます。リンクをクリックすると、新しいブラウザタブまたはウィンドウが開きます。SSOへのログインには、前述の手順で入力した電子メールアドレスと同じ電子メールアドレスを使用してください。

✓ OAuth connect

5 Waiting for SSO

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

6 Requesting service certificate OTP

SSO認証が完了すると（すでに認証されている場合は即座に）、RADKit Accessの確認ページに移動します。ページ上の情報を読み、Acceptをクリックして、CCOアカウントに所有者として登録するRADKit Serviceを承認します。

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

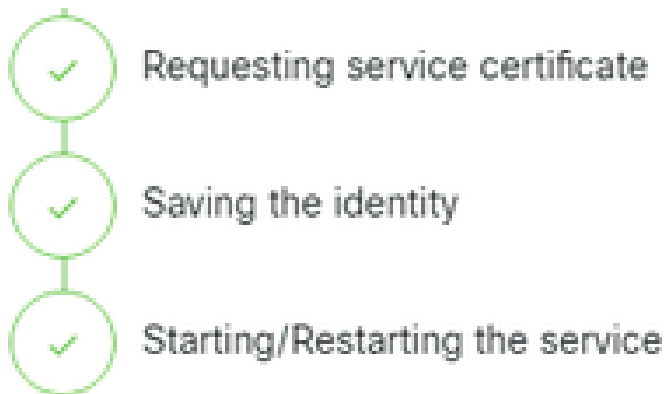
Deny

Log out all sessions

すると、Authentication result: Successという画面が表示されます。

Log out all sessions ボタンをクリックせず、SSOタブ/ウィンドウを閉じてRADKit Service WebUIに戻ります。

これはService enrolled with the identity: ...を示しています。次に示す一意の識別子は、RADKitサービスID (サービスシリアル番号とも呼ばれます) です。このスクリーンショットの例では、サービスIDdaxt9-kplb-5dwc yoursは異なります。



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

Close

Close をクリックしてダイアログを閉じ、Connectivity 画面に戻ります。

WebUI を更新すると、RADKit GUI の上部にサービス ID が表示され、次に示す接続ステータスも表示されます。



TAC エンジニアは、お客様の環境にあるデバイスにアクセスする必要がある場合、RADKit サービスを特定するためにこのサービス ID を必要とします。

これで、RADKit Cloud コンポーネントとの接続が確立され、その間にサービス ID が生成されました。次の手順では、RADKit を介して到達できるデバイスを追加します。

ステップ 4：デバイスとエンドポイントの追加

この手順では、RADKit 経由でアクセスできるデバイスのデバイスとクレデンシャルを追加します。HyperFlex の場合、理想的には、次のデバイスとそのクレデンシャルを追加する必要があります。

デバイス	デバイス タイプ	管理プロトコ ル	Credentials	転送 され た TCPポ ート	備考
------	-------------	-------------	-------------	-----------------------------	----

ハイパーバイザ (ESXiホスト)	Linux	ターミナル (SSH)	root		
ストレージコントローラ (SCVM)	HyperFlex	ターミナル (SSH)Swagger	admin ルート (有効)	443	イネーブルパスワードフィールドにルートパスワードを入力します。同意トークンが必要な場合に使用されます。Swaggerの場合:「Verify TLS Certificate」のチェックを外し、「Base URL」フィールドは空のままにします。
vCenter	Linux	ターミナル (SSH)	root		
UCSM	Generic	ターミナル (SSH)	admin		
インストーラ (オプション)	Linux	ターミナル (SSH)	root	443	
CIMC (エッジクラスタのみ)	Generic	ターミナル (SSH)	admin		
監視 (ストレッチクラスタのみ)	Linux	ターミナル (SSH)	root		
Intersight CVA/PCA (オプション)	Linux	ターミナル (SSH)	admin	443	

同じクラスタに属するデバイスを関連付けるために必要なので、デバイスはホスト名ではなくIPアドレスのみを使用して追加することが重要です。

これらのデバイスを追加するには、RADKit WebUIでDevices画面に移動します。

Remote Automation Development Kit

Cisco RADKit Service

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

Connectivity

Devices

Remote Users

+ Add Device

☐

☐

☐

☐

0 Edit Cart

+

-

☐	Active	Device Name	Hostname or IP Address	Device Type	In
No devices available					

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

上記の各デバイスに対して、Add Deviceをクリックして新しいエントリを作成します。クラスタ内のすべてのノードのIPアドレスを入力し、デバイスタイプを選択して、各デバイスタイプに応じた詳細を入力します。完了したら、をクリックAdd & closeして[デバイス]画面に戻るか、Add & continueをクリックして別のデバイスを追加します。

次に、エントリの例と、各デバイスタイプのエントリの設定を示します。

ESXiホストの例

Edit Device

Device Name^{*}(as it will appear in RADIUS)?

cluster2-node1-esxi

Management IP Address or Hostname[?]

172.16.2.11

Forwarded TCP ports [?]

Port ranges (eg. "1-1024,8888")

Device Type^{*}

LINUX

Jumphost Name

- Optional jumphost -

Description

Q Label search

?

RSAC status: **DISABLED**

Available Labels - 0 of 0 (click to add)

NO LABELS AVAILABLE

Selected Labels - 0 (click to delete)

Create newNone added

☒ Active (remotely manageable)

Available Management Protocols:
☒ Terminal ☐ Netconf ☐ Swagger ☐ HTTP ☐ SNMP

Terminal

Connection method:
☒ SSH (Password) ☐ SSH (Public key) ☐ Telnet

Username

root

Password

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

Port

22

☐ Allow connecting using obsolete/insecure SSH algorithms

☐ Use SSH Tunneling when using this device as a jumphost

☐ Enable Password [?]

Update

ストレージコントローラの例：

Edit Device



Device Name [⚠] (as it will appear in RadSec)

cluster2-node1-ecvm

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の例：

Edit Device

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

cluster2-vcenter

Management IP Address or Hostname*

172.16.0.22

Forwarded TCP ports ?

Port ranges (eg. "1-1024,8888")

Device Type*

LINUX

Jumphost Name

- Optional jumphost -

Description

Label search ?

RDAC 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

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

Port

22

☐ Enable Password ?

Update

UCSMの例：

Edit Device

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

cluster2-ucsm

Management IP Address or Hostname*?

172.16.2.201

Forwarded TCP ports ?

Port ranges (eg. "1-1024,8888")

Device Type*

Generic

Jumphost Name

- Optional jumphost -

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

Username

admin

Port

22

Allow connecting using obsolete/insecure SSH algorithms

☐

Use SSH Tunneling when using this device as a jumphost

☒

Password

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

Enable Password ?

☐

Update

TAC SRでのRADKitの使用

すべての準備が完了し、TACエンジニアにデバイスへのアクセスを提供する場合は、次の手順を実行できます。

エンジニアは、RADKitサービスIDと、お客様の環境または選択したデバイス（RBACを使用している場合）へのアクセスを、必要な時間だけ必要とします。

1. RADKitサービスIDを入力します。

まだTACケースをオープンしていない場合は、Cisco.comのSupport Case ManagerでUse RADKit for data collectionについて言及する機会があります。

☒ Use RADKit for data collection

RADKit Service ID 

axt9-kplb-5dwc

すでに未解決のサービスリクエストがある場合は、Support Case ManagerのCustomer Contact InformationセクションでRADKitサービスIDを追加できます。

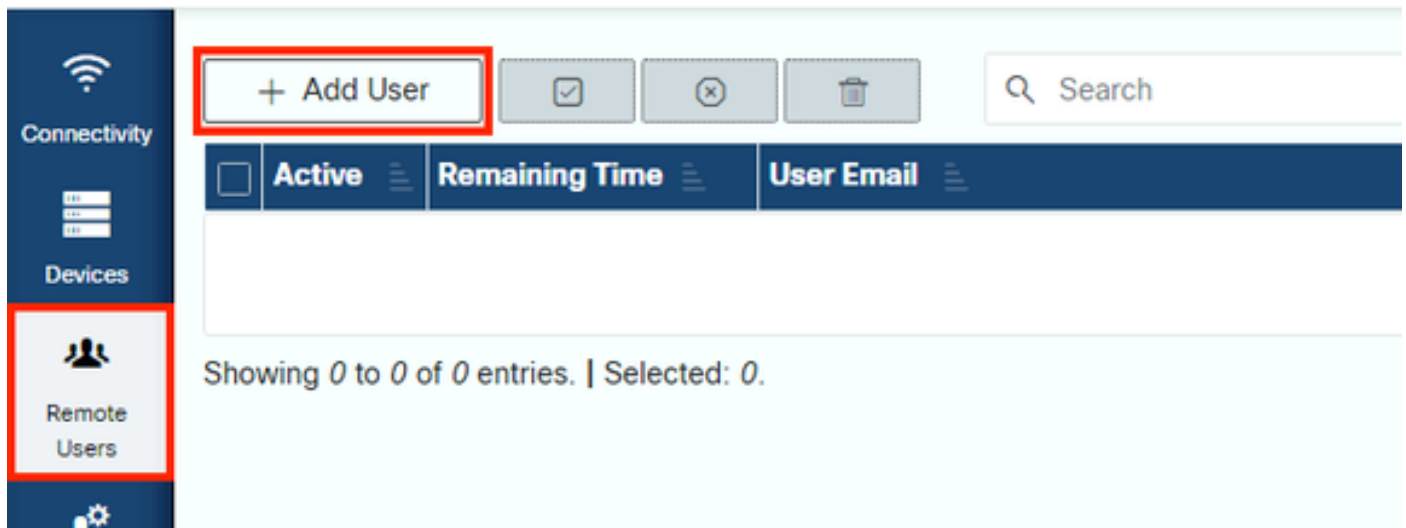


The screenshot shows the 'CUSTOMER CONTACT INFORMATION' section of the Support Case Manager. On the right, the 'Edit RADKit Service ID' section is visible. It includes a checkbox 'Use RADKit for data collection' which is checked. Below it, the 'RADKit Service ID' is displayed as 'axt9-kplb-5dwc'. A red box highlights the 'Add/Edit RADKit Service ID' link. At the bottom of this section are 'Save' and 'Cancel' buttons.

または、担当のケースを担当しているTACエンジニアにIDを伝えてください。

2. リモートユーザーの追加

ユーザがデバイスを使用して作業するには、明示的なアクセスを提供し、このアクセスが有効な期間を設定する必要があります。そのためには、RADKit WebUIでRemote Users画面に移動し、をクリックして新しいリモートユーザを作成します Add User.



TACエンジニアの@cisco.comの電子メールアドレスを入力します（誤字に注意してください）。必ず **Activate this user** チェックボックスと **Time slice** または **Manual** の設定に注意してください。

ユーザがアクティブな間は、RBACポリシーで許可されている限り、RADKitサービスを介して設定済みのデバイスにアクセスできます。

タイムスライスとは、ユーザが自動的に非アクティブになるまでの時間を表します。つまり、タイムスライスは時間に縛られたトラブルシューティングセッションを表します。ユーザのセッションは、そのユーザのタイムスライスの期間まで延長できます。ユーザを手動でアクティブ化/非アクティブ化する場合は、代わりに **Manual** を選択します。

ユーザは、タイムスライスが設定されているかどうかにかかわらず、常に手動でアクティブ化/非アクティブ化できます。ユーザが非アクティブになると、RADKitサービスを介したすべてのセッションが即座に切断されます。

終了したら、**Add & close** をクリックしてRemote Users画面に戻ります。

関連情報

- 一般的な質問の詳細と回答については、RADKitのWebサイト(<https://radkit.cisco.com/>)をご覧ください。
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。