

Configuration de RADKit dans un environnement de collaboration

Table des matières

[Introduction](#)

[Exigences](#)

[Composants utilisés](#)

[Terminologie](#)

[Architecture RADKit](#)

[Installation de RADKit](#)

[Service RADKit \(côté utilisateur\)](#)

[Intégration](#)

[Ajouter des périphériques](#)

[Autoriser les utilisateurs distants](#)

[Client RADkit \(côté TAC\)](#)

[Connexion](#)

[Accès SSH](#)

[Accès GUI](#)

[Proxy HTTP](#)

[Transfert de port](#)

[Collecte des journaux](#)

[RTMT](#)

[API SOAP](#)

[Exemples d'utilisation RADKit](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes de configuration de RADKit et montre la configuration nécessaire pour commencer à l'utiliser avec les produits de collaboration.

Exigences

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

- Connaissances de base de tout produit de collaboration VOS
- Connaissances de base de l'accès CLI/SSH

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Cisco Unified Communications Manager 12.5 et 14.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

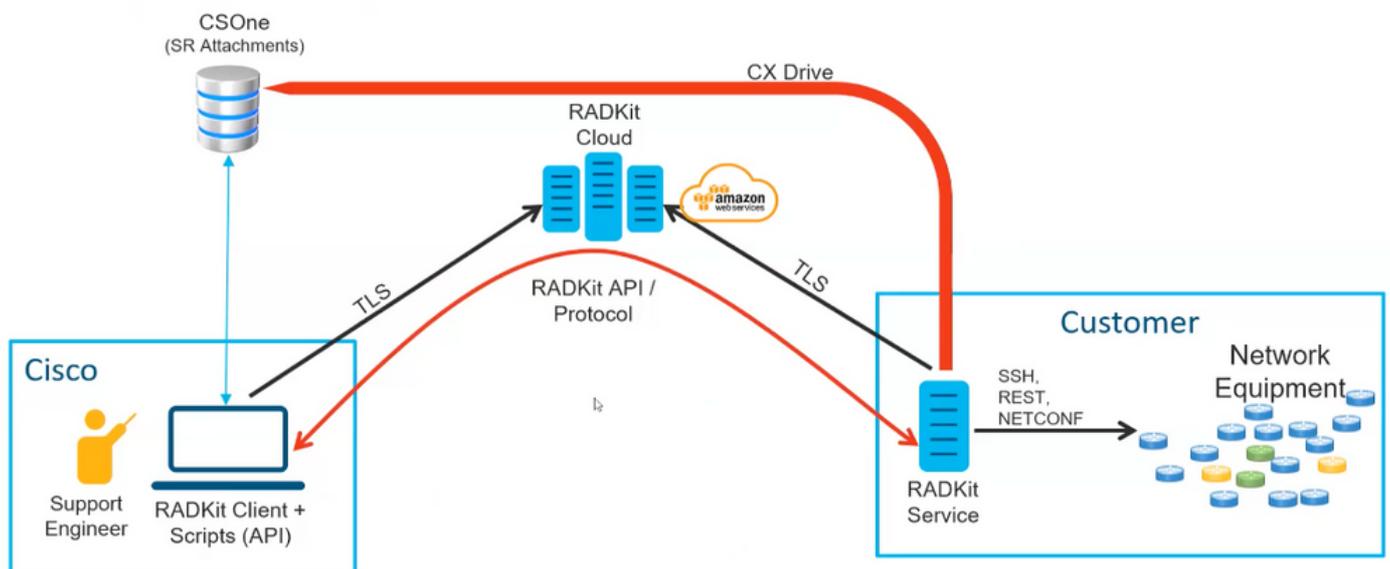
Terminologie

RADKit : Il s'agit d'un connecteur permettant aux ingénieurs et partenaires du TAC Cisco d'accéder à distance et en toute sécurité aux périphériques des utilisateurs. Il prend en charge plusieurs protocoles pour interagir avec des périphériques, tels que SSH ou HTTP/HTTPS.

Service RADKit : C'est le côté serveur. Il est géré et entièrement géré par l'utilisateur. Du côté du serveur, l'utilisateur contrôle qui peut accéder aux périphériques et pendant combien de temps. Le service Radkit doit être connecté aux périphériques du réseau pour pouvoir y accéder.

Client RADKit : C'est le côté client. Il s'agit du PC utilisé pour se connecter aux périphériques du réseau utilisateur.

Architecture RADKit



Architecture RADKit

Installation de RADKit

Étape 1. Accédez à <https://radkit.cisco.com> et cliquez sur Downloads, puis accédez au dossier release.

Cisco Remote Automation Development Kit (RADKit)

CISCO RADKit. FROM NETOPS TO DEVOPS.

RADKit is a network-wide orchestrator.
Experience a radical new way of addressing
your equipment, boost your Cisco Services,
and expand your capabilities.



INDEX OF /DOWNLOADS/

[../](#)

[nonrelease/](#)

[release/](#)

03-Mar-2023 18:10

-

04-Apr-2023 11:45

-

Étape 2. Cliquez sur la dernière version.

INDEX OF /DOWNLOADS/RELEASE/

[../](#)

[1.3.9/](#)

11-Jan-2023 13:11

-

[1.4.6/](#)

10-Mar-2023 15:05

-

[1.4.7/](#)

24-Mar-2023 13:00

-

[1.4.8/](#)

11-Apr-2023 16:05

-

[1.4.9/](#)

11-Apr-2023 16:05

-

Étape 3. Téléchargez le fichier approprié en fonction de votre système d'exploitation.

INDEX OF /DOWNLOADS/RELEASE/1.4.9/

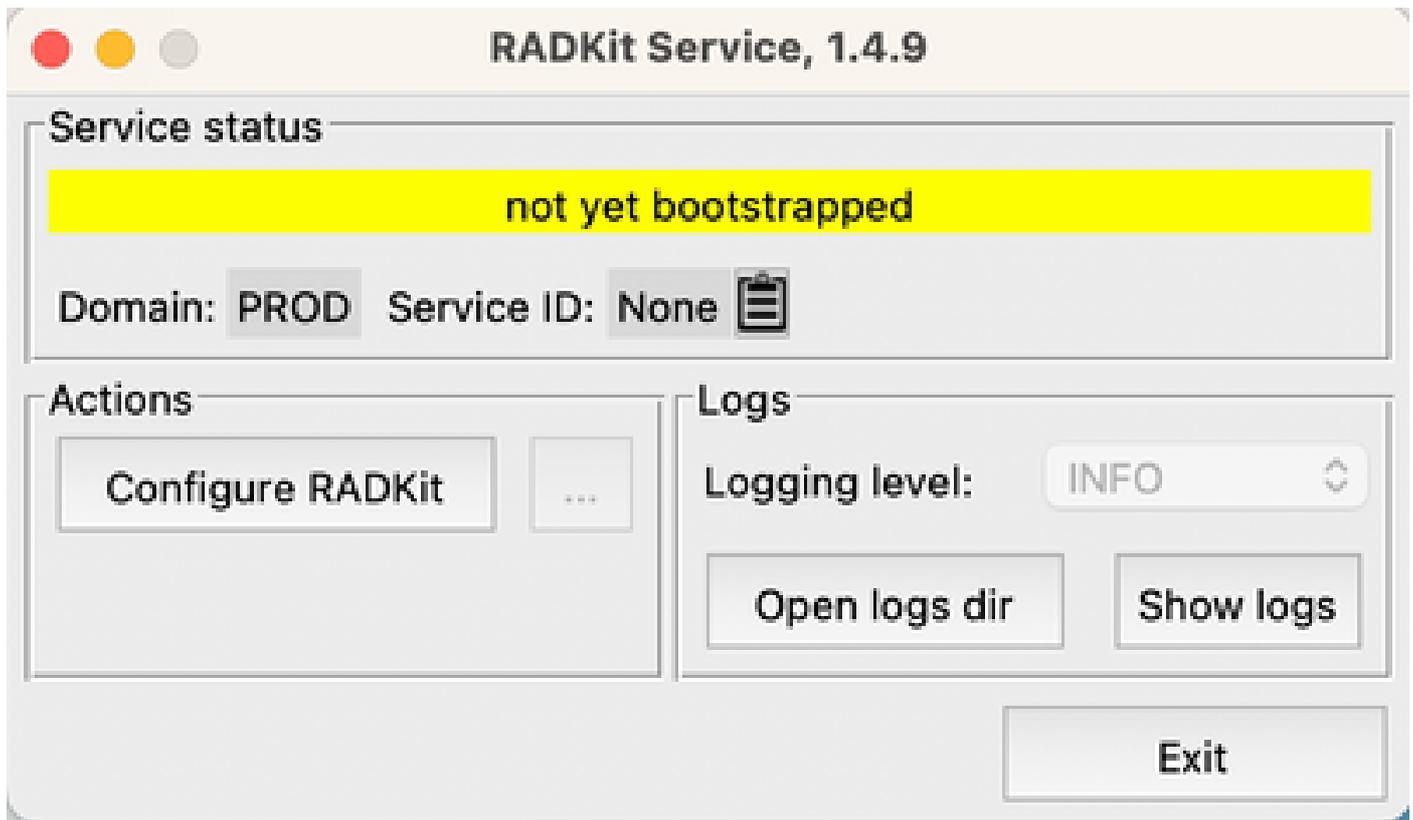
../		
docs/	04-Apr-2023 11:45	-
cisco_radkit_1.4.9_doc_html.tgz	04-Apr-2023 11:43	8003863
cisco_radkit_1.4.9_macos_arm64_signed.pkg	11-Apr-2023 10:41	74142354
cisco_radkit_1.4.9_macos_x86_64_signed.pkg	11-Apr-2023 10:41	77265560
cisco_radkit_1.4.9_pip_linux.tgz	04-Apr-2023 11:49	146189048
cisco_radkit_1.4.9_pip_macos.tgz	04-Apr-2023 11:49	37257192
cisco_radkit_1.4.9_pip_win.tgz	04-Apr-2023 11:49	35385652
cisco_radkit_1.4.9_win64_signed.exe	04-Apr-2023 13:18	104692424

Étape 4. Exécutez le programme d'installation sur le PC ou le serveur. Dans le cadre de l'installation, Radkit doit installer trois applications : Radkit Service, Radkit Client et Radkit Network Console.

Service RADKit (côté utilisateur)

Intégration

Étape 1. Pour commencer à configurer le service RADKit, accédez à Applications et localisez RADKit Service. La première fois que vous exécutez, il affiche un message "not yet bootstrapped".



Étape 2. Cliquez sur Configure RADKit, le navigateur apparaît automatiquement avec l'URL <https://localhost:8081/bootstrap>.

- Créez un mot de passe pour l'utilisateur superadmin et cliquez sur Submit.
- Ce nom d'utilisateur et ce mot de passe superadmin sont demandés chaque fois que le service est démarré ou configuré.

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 1 lowercase letter
- Minimum 1 uppercase letter
- Minimum 1 number
- Minimum 1 symbol
- Minimum 8 characters

Étape 3. Une fois que vous avez cliqué sur Submit, le navigateur vous redirige vers <https://localhost:8081/#/connectivity/>.

Sous Connectivity > Service Enrollment, il existe deux méthodes d'authentification :
Authentification unique et mot de passe à usage unique.

Single Sign-On Enrollment



1 Checking prerequisites

2 Email address • • •

Provide email address for SSO login:

Submit

3 Connecting to the Access Service

4 OAuth connect

5 Waiting for SSO

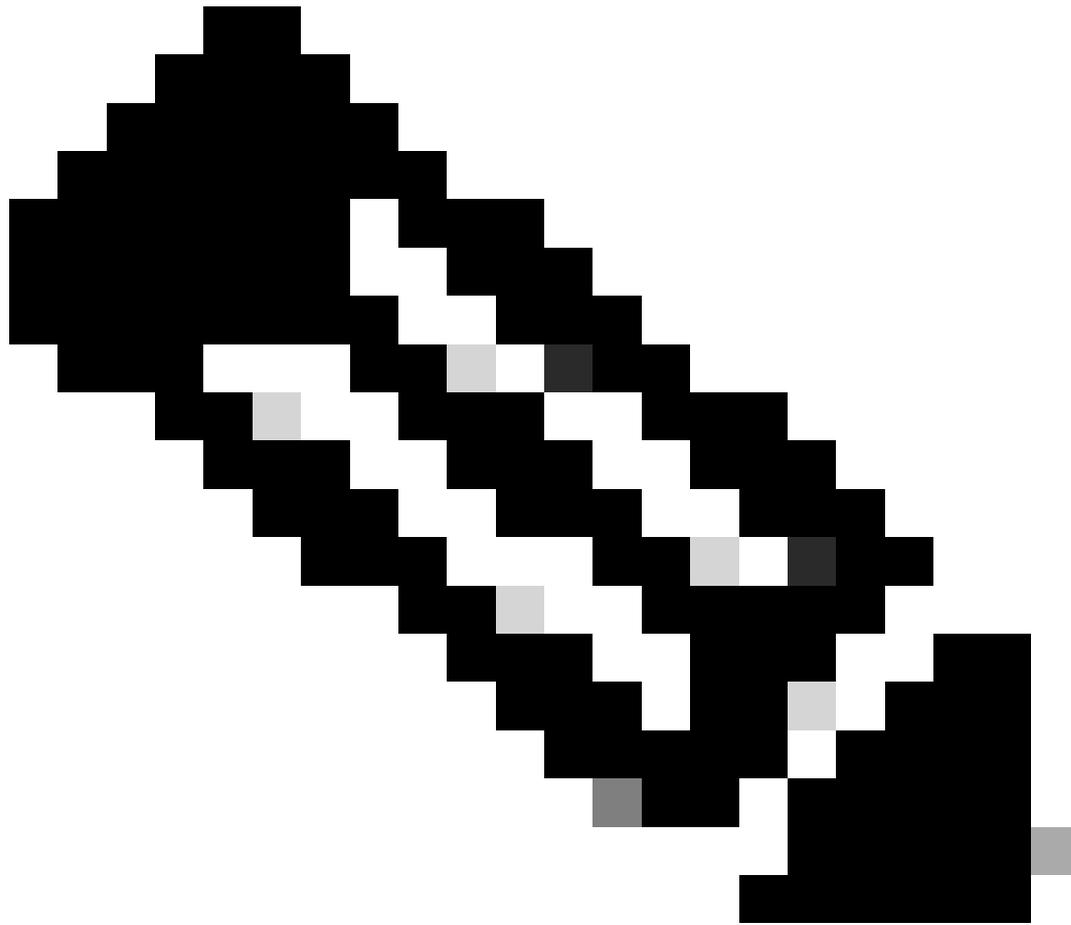
6 Requesting service certificate OTP

7 Requesting service certificate

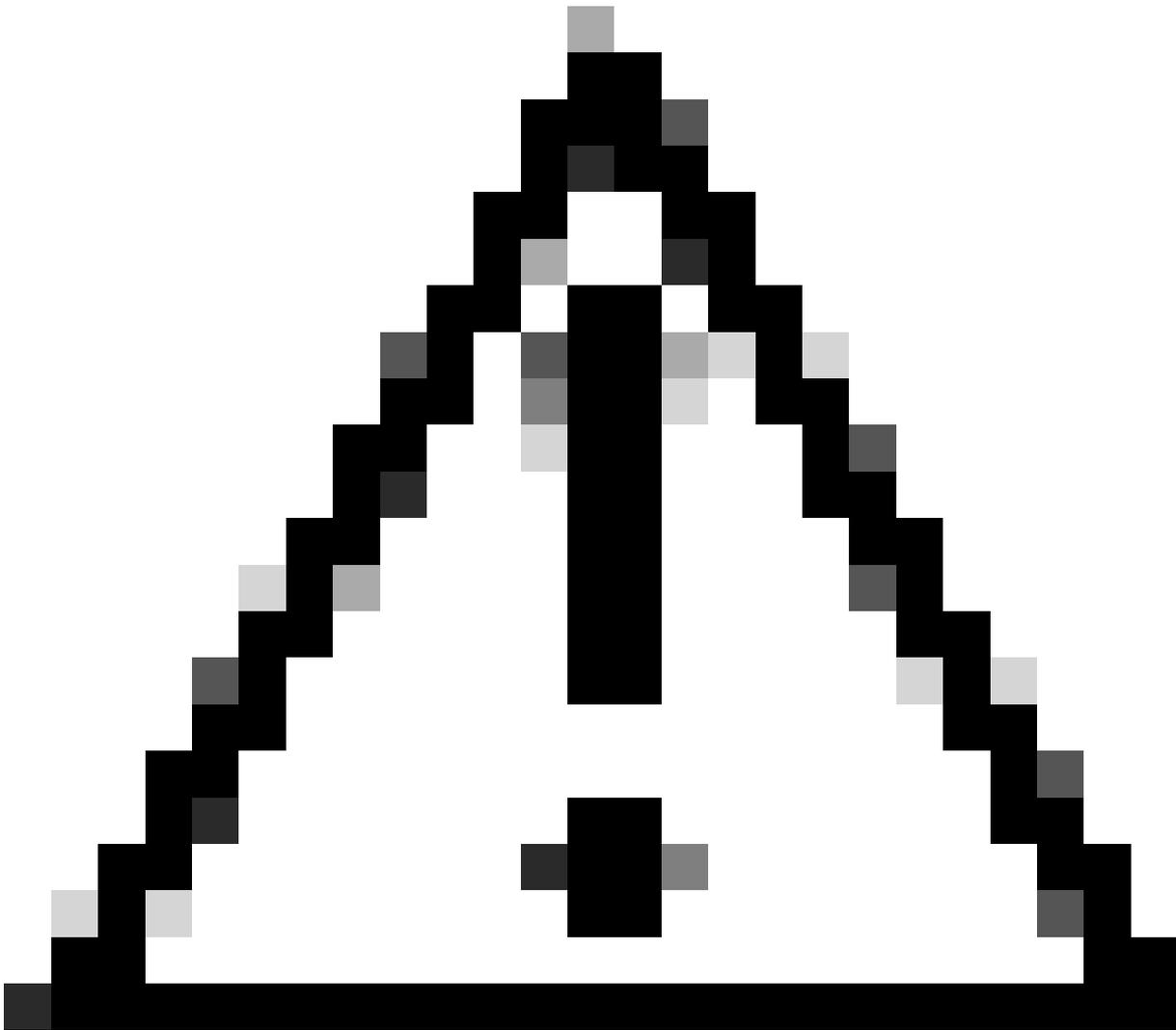
Étape 5. Terminez l'Assistant et suivez les étapes jusqu'à ce qu'il affiche « Service inscrit avec une nouvelle identité : xxxx-xxxx-xxxx », et lorsque vous cliquez sur Close, le service apparaît comme Connected.

Service enrolled with new identity: k331-0evx-s94g

Close



Remarque : Un compte Cisco est nécessaire pour activer le service RADKit.



Mise en garde :

- Si le serveur sur lequel le service RADKit est exécuté nécessite la définition d'un proxy, outre la définition du proxy sur le serveur/PC lui-même, une variable d'environnement doit également être définie pour que le service RADKit fonctionne
RADKIT_CLOUD_CLIENT_PROXY_URL=<http://proxy.example.com:80>.

Ajouter des périphériques

Étape 1. Accédez à Devices et cliquez sur Add Device.

Add New Device



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

cesavilacum

Device Type*

CUCM

Management IP Address or Hostname*?

10.88.247.197

Jumphost Name

- Optional jumphost -

Forwarded TCP ports ?

443;8443

Description

Label search

RBAC status: **ENABLED**

Available Labels - 2 of 2 (click to add)

active SR697039480

Selected Labels - 0 (click to delete)

Create new None added

Active (remotely manageable)

Available Management Protocols:

Terminal Netconf Swagger HTTP SNMP

Étape 3. Pour chaque protocole de gestion, configurez les paramètres appropriés et cliquez sur Add & Close.

Terminal

Connection method:

SSH 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 ?

Étape 4. Une fois ajouté, le périphérique doit être affiché dans la liste des périphériques ; il peut être activé/désactivé pour l'accès à distance.

Remote Automation Development
Cisco RADKit Service

Domain: PROD Serial: k331-0evx-s94g

CONNECTED

+ Add Device

0 Edit Tray

Search

Active	Device Name	Hostname or IP Address	Device Type	In tray	Description	Actions
<input checked="" type="checkbox"/>	cesavilaCUCM	10.88.247.197	UNKNOWN			

Showing 1 to 1 of 1 entries. | Selected: 0.

Page size 15 25 50 100 250

Autoriser les utilisateurs distants

Étape 1. Afin d'accorder à l'utilisateur l'accès aux périphériques configurés dans le service RADKit, accédez à Utilisateurs distants et sélectionnez Ajouter des utilisateurs.

Remote Automation Development
Cisco RADKit Service

Domain: PROD Serial: k331-0evx-s94g

CONNECTED

+ Add User

Search

Active	Remaining Time	User Email	Full Name	Description	Actions
 No Users Available					

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

Page size 15 25 50 100 250

Étape 2 : configuration des informations utilisateur :

- Adresse électronique
- Nom complet (facultatif)
- Activez l'utilisateur.
- Spécifiez si l'activation doit être contrôlée manuellement ou définissez un délai pour accorder l'accès à cet utilisateur.

Add New User



User Email*
cesavila@cisco.com

Full Name
Cesar Avila

Description

Activate this user

USER ACCESS POLICY

Manual

Time slice (h/m):
24 00

Clear form Add & close Add & continue

Étape 3. Sélectionnez Ajouter et fermer.

Client RADkit (côté TAC)

Connexion

Étape 1. Sur le PC client, accédez à Applications et localisez RADkit Client.

Étape 2 : création d'une instance de client avec votre connexion SSO

```
<#root>
```

```
>>>
```

```
client = sso_login("cesavila@cisco.com")
```

```
cesavila — radkit-client — 117x32

Example usage:
client = sso_login("<email_address>")           # Open new client and authenticate with SSO
client = certificate_login("<email_address>")     # OR authenticate with a certificate
client = access_token_login("<access_token>")    # OR authenticate with an SSO Access Token
service = client.service("<serial>")           # Then connect to a RADKit Service
service = start_integrated_service()            # Immediately login to an integrated session
client.grant_service_otp()                      # Enroll a new service

>>> client = sso_login("cesavila@cisco.com")
```

Étape 3. Acceptez la demande d'autorisation SSO ouverte automatiquement sur votre navigateur.



Do you accept this authorization request?

Environment: PROD

Client IP address: 128.107.241.164

Client hostname: N/A

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



Authentication result: Success

You may now close this window and return to your application.

If you suspect that an illegitimate session may have been granted access now or in the past, click the 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.

Log out all sessions

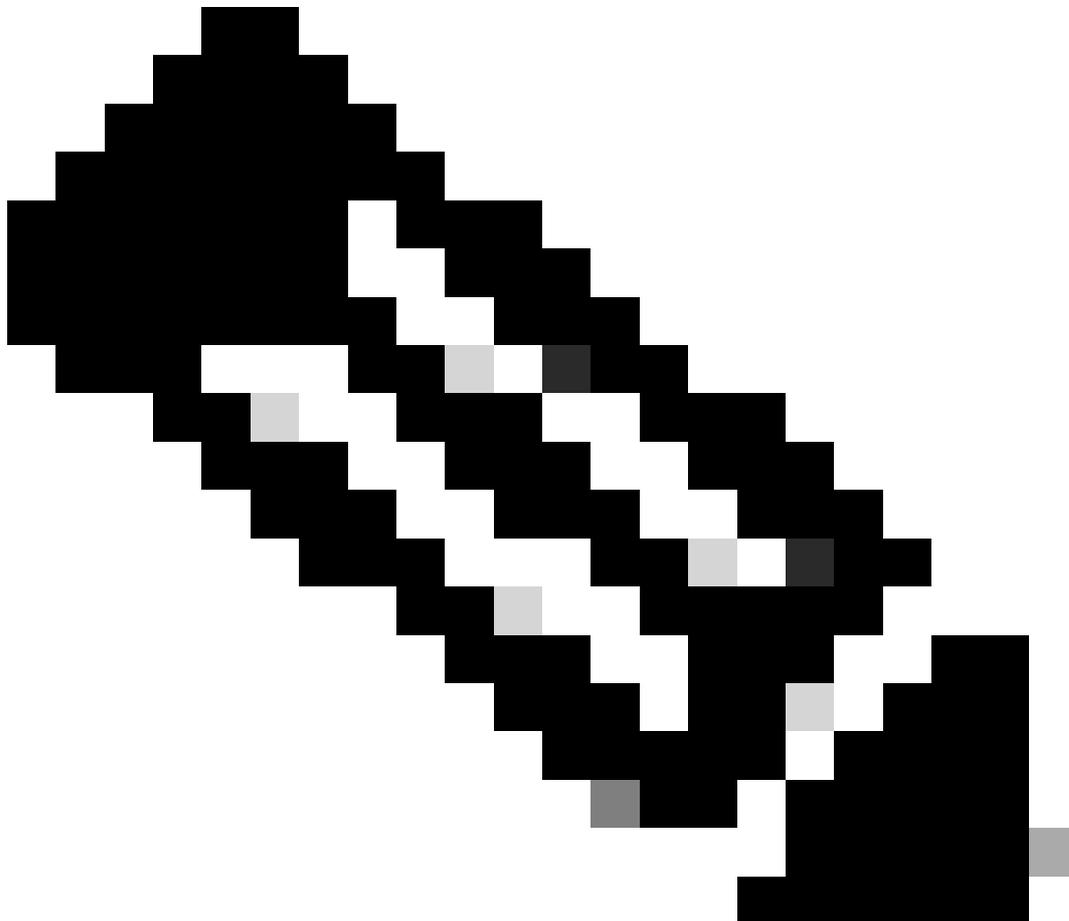
Étape 4. Créez une instance de service à l'aide du numéro de série généré par l'utilisateur à partir de la phase RADKit Service - Onboarding.

<#root>

>>>

```
service = client.service("k331-0evx-s94g")
```

```
>>> service = client.service("k331-0evx-s94g")
05:16:36.349Z INFO | internal | Connecting to forwarder [uri='wss://prod.radkit-cloud.cisco.com/forwarder-2/websocket/']
05:16:37.153Z INFO | internal | Connection to forwarder successful [uri='wss://prod.radkit-cloud.cisco.com/forwarder-2/websocket/']
05:16:39.523Z INFO | internal | Connecting to forwarder [uri='wss://prod.radkit-cloud.cisco.com/forwarder-3/websocket/']
05:16:40.333Z INFO | internal | Connection to forwarder successful [uri='wss://prod.radkit-cloud.cisco.com/forwarder-3/websocket/']
```



Remarque : service est une variable qui peut être n'importe quoi.

Étape 5 : vérification des périphériques disponibles pour l'accès

```
<#root>
```

```
>>>
```

```
service.inventory
```

```
>>> service.inventory
<radkit_client.sync.device.DeviceDict object at 0x10d7728e0>
name          host          device_type  Terminal  Netconf  Swagger  HTTP  description  failed
-----
cesavilacucm  10.88.247.197 UNKNOWN    True      False    False    True  -----
False
```

Pour actualiser la liste d'inventaire, utilisez la commande `update_inventory`.

```
<#root>
```

```
>>> service.update_inventory().wait()
```

Accès SSH

Étape 1 : création d'un objet à partir de la liste d'inventaire

```
<#root>
```

```
>>> cucm = service.inventory['cesavilacucm']
```

```
>>> service.inventory
<radkit_client.sync.device.DeviceDict object at 0x10d7728e0>
name          host          device_type  Terminal  Netconf  Swagger  HTTP  description  failed
-----
cesavilacucm  10.88.247.197 UNKNOWN    True      False    False    True  -----
False
Untouched inventory from service k331-0evx-s94g.
>>>
>>> cucm = service.inventory["cesavilacucm"]
```

Étape 2 : Démarrez la session SSH avec la commande interactive.

```
<#root>
```

```
>>> cucm.interactive()
```

```
>>> cucm.interactive()
05:35:23.882Z INFO | internal | starting interactive session (will be closed when detached)
05:35:24.765Z INFO | internal | Session log initialized [filepath='/Users/cesavila/.radkit/session_logs/client/202304-cesavilacucm.log']
{
  Attaching to cesavilacucm ...
  Type: ~. to detach.
  ~? for other shortcuts.
  When using nested SSH sessions, add an extra ~ per level of nesting.

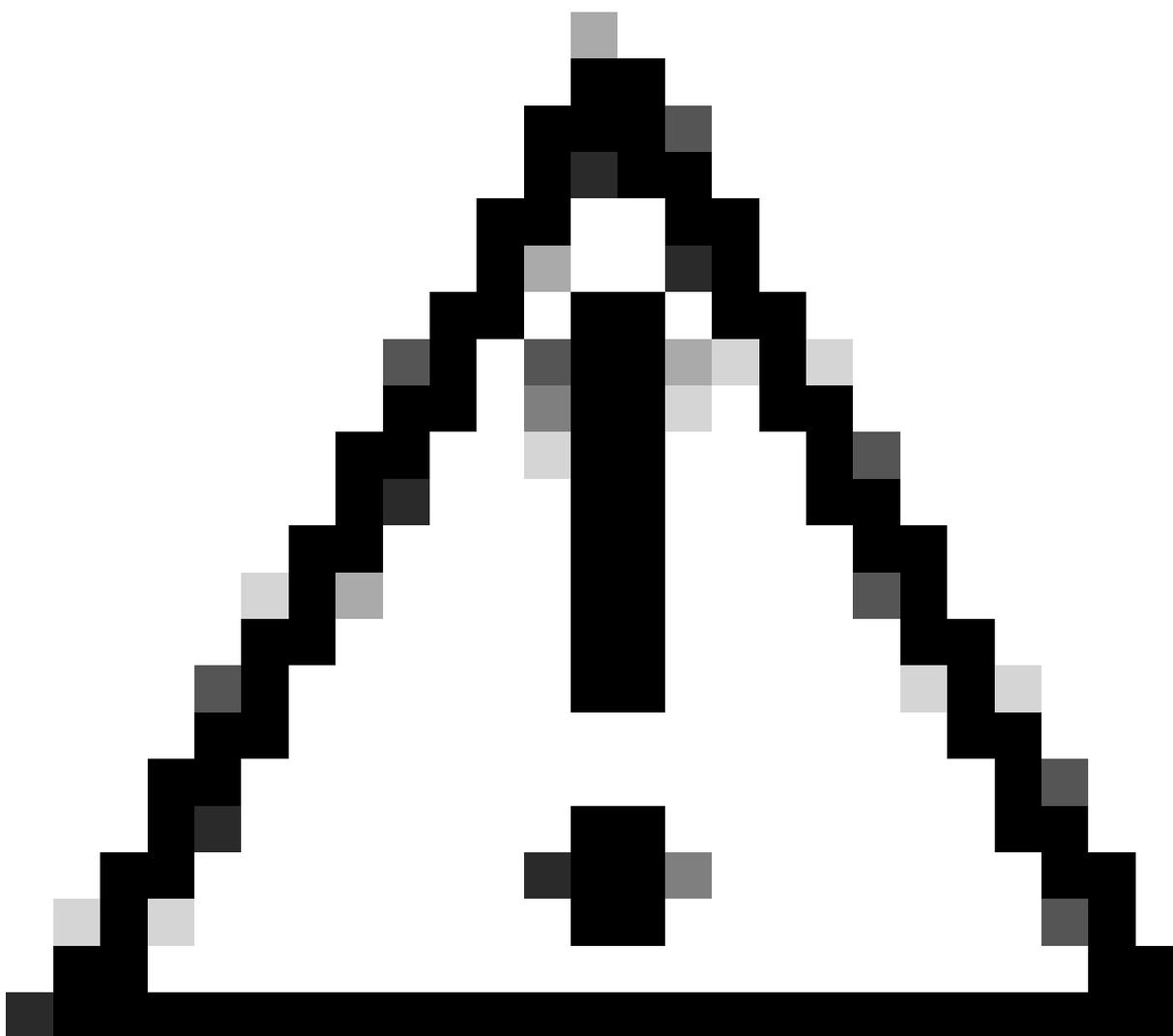
Command Line Interface is starting up, please wait ...

Welcome to the Platform Command Line Interface

VMware Installation:
  2 vCPU: Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz
  Disk 1: 200GB, Partitions aligned
  4096 Mbytes RAM
  WARNING: DNS unreachable
  WARNING: Ungraceful shutdown detected - A rebuild of this node is highly recommended
  to ensure no negative impact(such as configuration or file system corruption). For
  rebuild instructions, see the installation guide.

admin:|
```

Étape 3. Vous pouvez maintenant gérer le périphérique normalement.



Mise en garde :

- Soyez toujours conscient de notre responsabilité lorsque vous travaillez dans un environnement utilisateur.
- RADKit doit être utilisé comme outil de collecte de données.
- N'effectuez jamais de modifications sans l'autorisation de l'utilisateur.
- Documentez toutes vos conclusions dans les notes de cas.

Accès GUI

- Proxy HTTP

Étape 1 : assurez-vous que les informations d'identification HTTP sont ajoutées au service RADKit sur la configuration du périphérique.

Étape 2 : démarrage du proxy HTTP sur le client Radkit et définition du port local utilisé pour la connexion au proxy

<#root>

```
>>> http_proxy = client.start_http_proxy(4001)
```

```
>>>
>>> http_proxy = client.start_http_proxy(4001)
22:24:19.981Z WARNI | HTTP proxy is NOT PROTECTED by username/password
>>> █
```

Étape 3. Dans le navigateur Web, accédez à <https://localhost:4001> et sélectionnez le service auquel vous souhaitez vous connecter.

The screenshot shows a web browser window with the address bar set to 'localhost:4001'. The page content includes the Cisco logo and the text 'RADKit Client Proxy'. Below this, the word 'Services' is displayed in a large font. Underneath, it says 'Choose any of the following services:' followed by a numbered list: '1. r7nz-6n40-x3su' and '2. ckt7-tv6c-uale'. The first service is highlighted with a red rectangular box.

Étape 4. Cliquez sur l'option Go to Web Page sur le périphérique approprié pour vous connecter à

sa page Web.

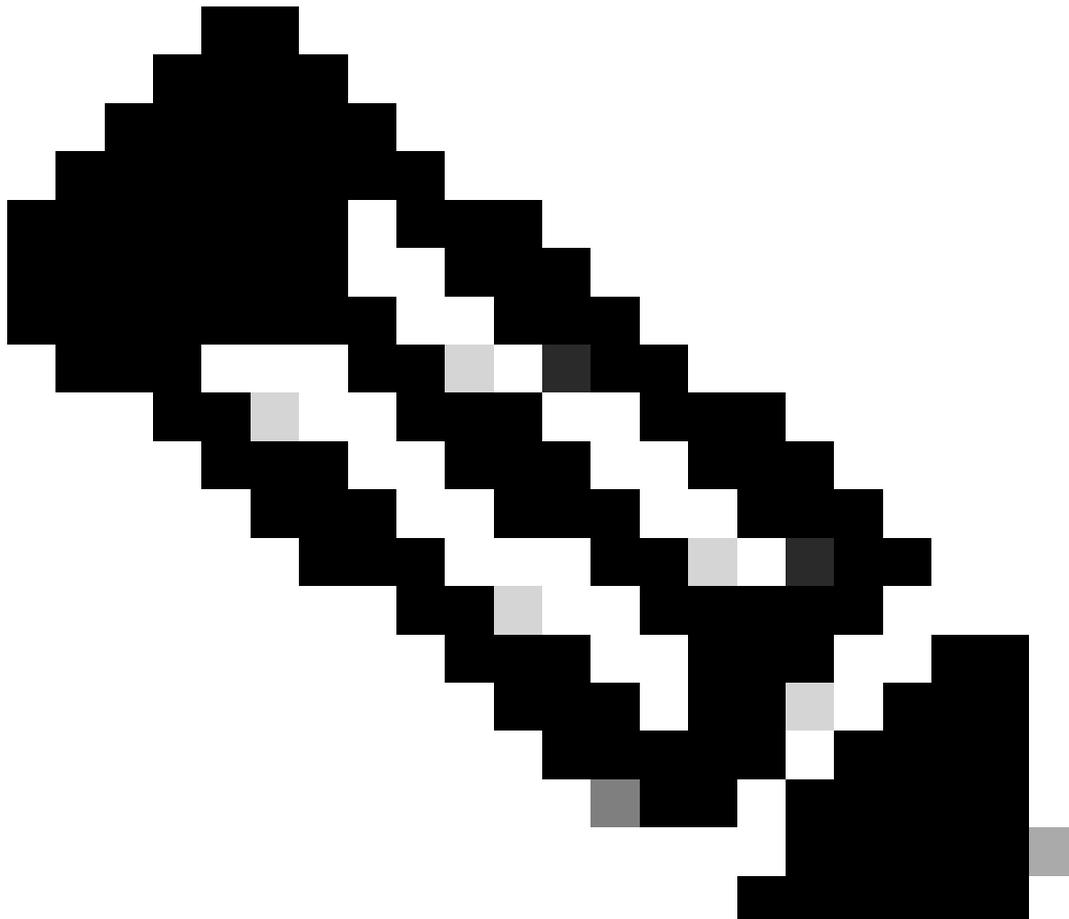
localhost:4001/service/r7nz-6n40-x3su

Technical Services... iCloud - Buscar mi... Cisco Internal www.cisco.com/cj/... Cisco General BUFF Dedicated Instance WxC Calling Voice

RADKit Client Proxy

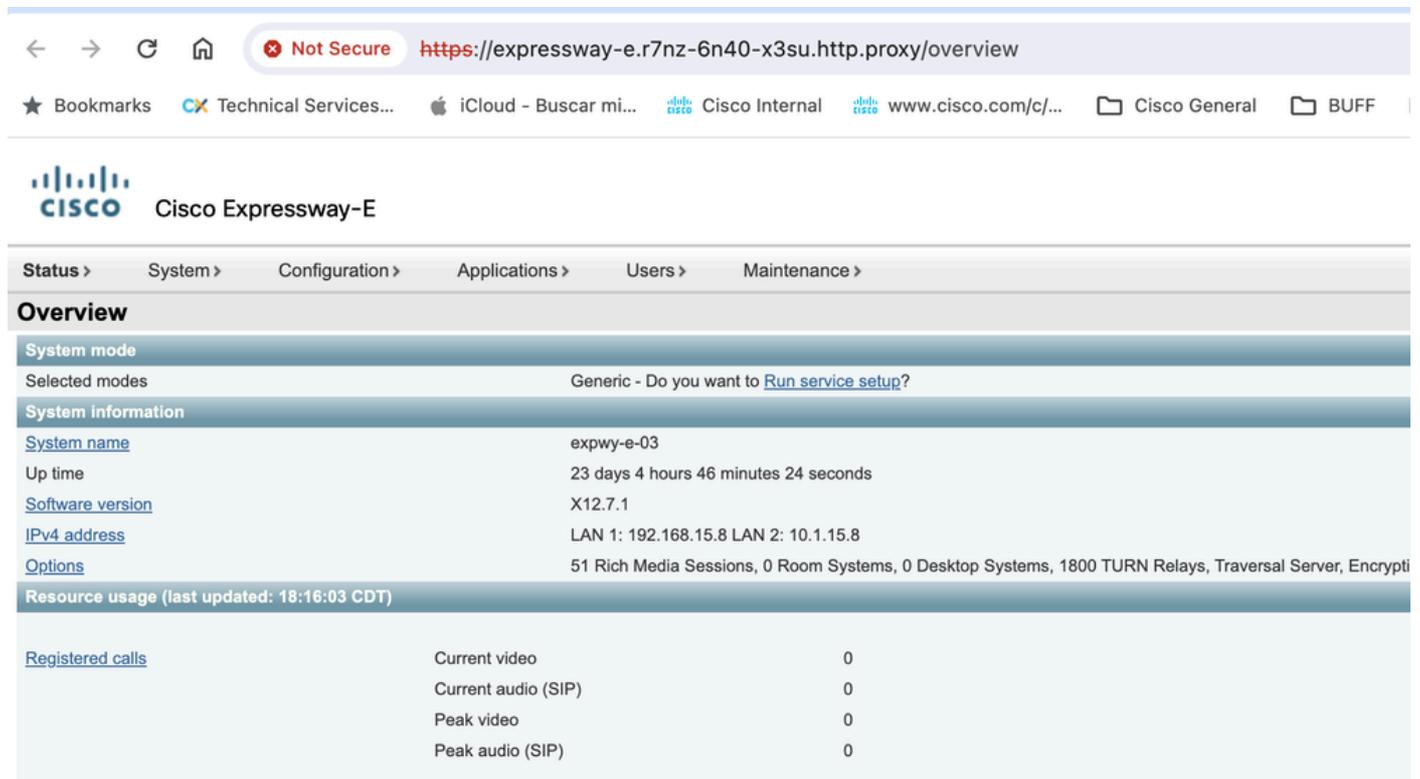
Service ID: r7nz-6n40-x3su

Device name	TCP port forwards	Supports HTTP	Reset Session
expressway-c	443;8443	Go to web page	<input type="button" value="Reset"/>
expressway-e	443;8443	Go to web page	<input type="button" value="Reset"/>
cucmhq	443;8443	Go to web page	<input type="button" value="Reset"/>



Remarque : la première fois que le proxy HTTP est configuré sur un client RADKit, il est recommandé de cliquer sur l'option Reset pour chaque périphérique avant d'essayer d'ouvrir la page Web Device.

Étape 5. La page Web s'affiche.



← → ↻ 🏠 ⓧ Not Secure https://expressway-e.r7nz-6n40-x3su.http.proxy/overview

★ Bookmarks CX Technical Services... 🍏 iCloud - Buscar mi... 📶 Cisco Internal 📶 www.cisco.com/c/... 📁 Cisco General 📁 BUFF

CISCO Cisco Expressway-E

Status > System > Configuration > Applications > Users > Maintenance >

Overview

System mode

Selected modes: Generic - Do you want to [Run service setup?](#)

System information

[System name](#): expwy-e-03

Up time: 23 days 4 hours 46 minutes 24 seconds

[Software version](#): X12.7.1

[IPv4 address](#): LAN 1: 192.168.15.8 LAN 2: 10.1.15.8

[Options](#): 51 Rich Media Sessions, 0 Room Systems, 0 Desktop Systems, 1800 TURN Relays, Traversal Server, Encryption

Resource usage (last updated: 18:16:03 CDT)

Registered calls	
Current video	0
Current audio (SIP)	0
Peak video	0
Peak audio (SIP)	0

- Transfert de port

Étape 1 : vérification des ports TCP Forwarded configurés pour le périphérique

```
<#root>
```

```
>>> cucm.forwarded_tcp_ports
```

```
>>> cucm.forwarded_tcp_ports
'443;8443'
>>> █
```

Étape 2 : configuration d'un port local à mapper avec le port de destination du périphérique, vous devez utiliser le port local pour accéder à l'interface utilisateur graphique du périphérique.

```
<#root>
```

```
>>> cucm.forward_tcp_port(local_port=8443, destination_port=443)
```

```
>>>
>>> cucm.forward_tcp_port(12443,443)
[RUNNING] <radkit_client.sync.port_forwarding.TCPPortForwarder object at 0x10ceb3d60>
-----
status          RUNNING
serial          None
device_name     cesavilacucm
local_port      12443
destination_port 443
#active         0
#failed         0
#closed         0
#total          0
bytes up        0
bytes down      0
exception       None
-----
```

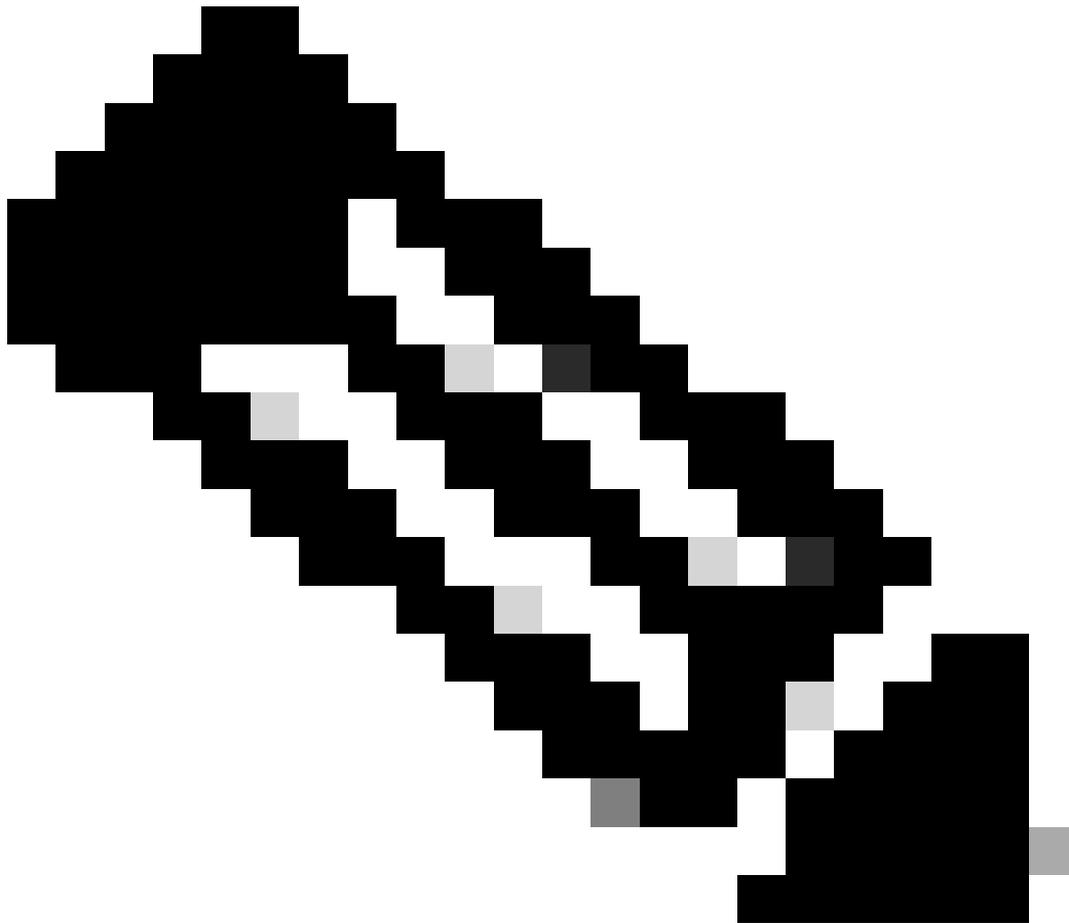
Étape 3. Ouvrez votre navigateur et tapez l'URL avec le port configuré à l'étape 2 : <https://localhost:8443>.

L'interface utilisateur graphique du périphérique est désormais accessible.



The screenshot shows a web browser window with the address bar displaying "Not Secure https://localhost:8443". The browser's bookmark bar includes "Bookmarks", "Technical Services...", "iCloud - Buscar mi...", "Cisco Internal", "www.cisco.com/c/...", and "Cisco General". The main content area features the Cisco logo at the top. Below the logo, there are two sections:

- Installed Applications**
 - Cisco Unified Communications Manager
 - Cisco Unified Communications Self Care Portal
 - Cisco Prime License Manager
 - Cisco Unified Reporting
 - Cisco Unified Serviceability
- Platform Applications**
 - Disaster Recovery System
 - Cisco Unified Communications OS Administration



Remarque : Pour accéder à l'interface utilisateur graphique du produit, vous avez toujours besoin des informations d'identification pour pouvoir vous connecter. Par conséquent, il est recommandé à l'utilisateur de créer un compte d'utilisateur en lecture seule pour y accéder.

Collecte des journaux

- RTMT

Étape 1 : vérifiez que le port 8443 est répertorié dans les ports TCP Forwarded configurés pour le périphérique.

```
<#root>
```

```
>>> cucm.forwarded_tcp_ports
```

```
>>> cucm.forwarded_tcp_ports
'443;8443'
>>> █
```

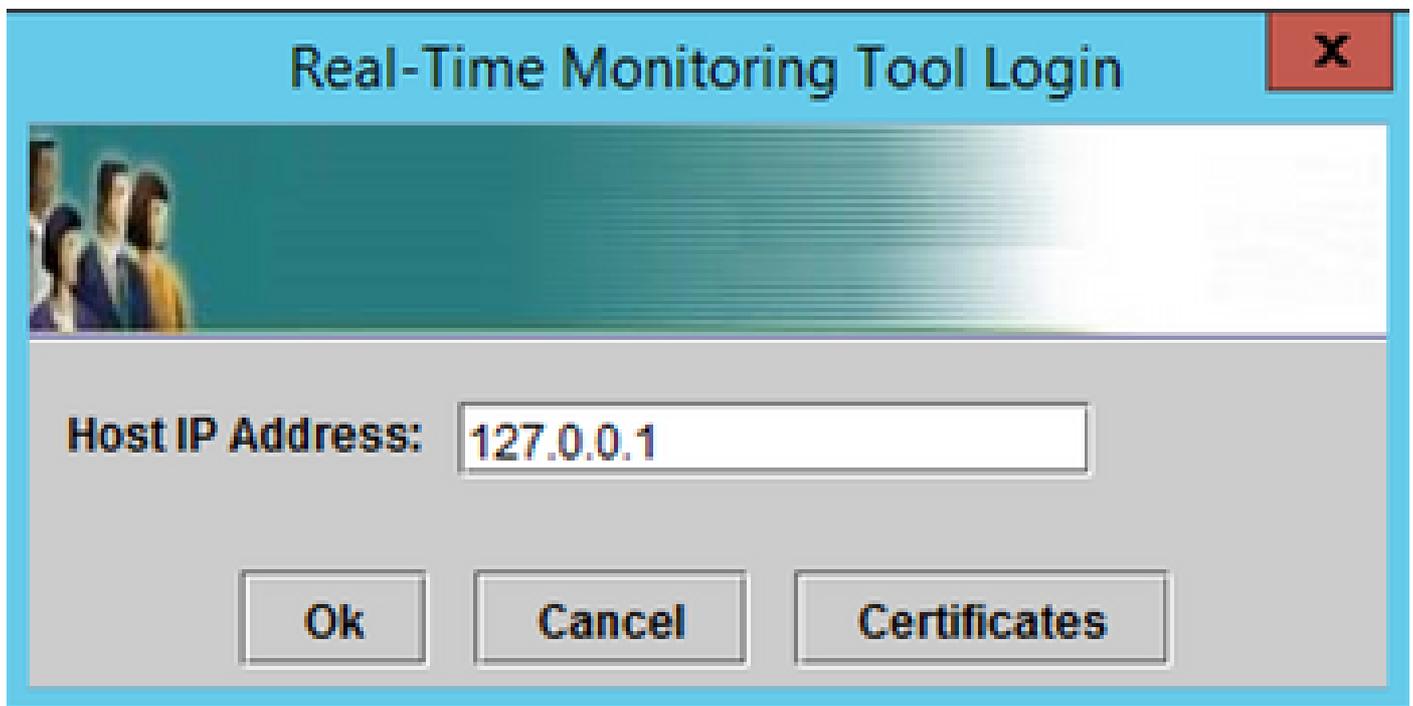
Étape 2 : configurez le même port 8443 comme port local à mapper avec le port 8443 comme port de destination du périphérique.

<#root>

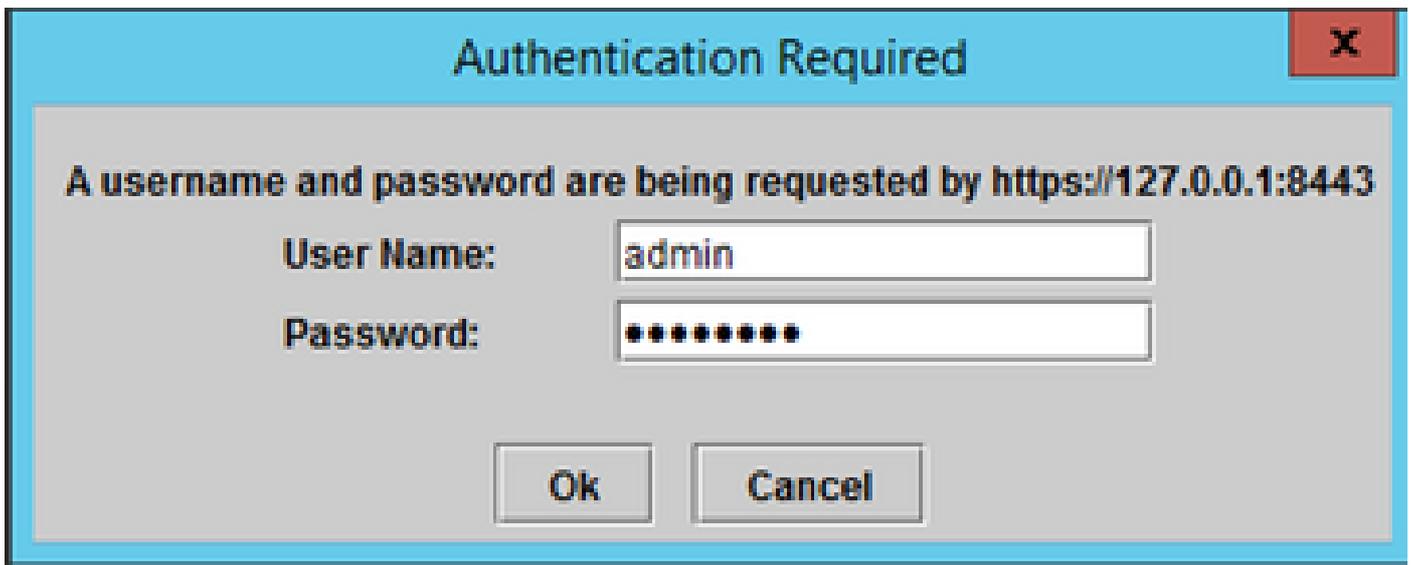
```
>>> cucm.forward_tcp_port(local_port=8443, destination_port=8443)
```

```
>>> cucm.forward_tcp_port(8443,8443)
[RUNNING] <radkit_client.sync.port_forwarding.TCPPortForwarder object at 0x1077defa0>
-----
status          RUNNING
serial          None
device_name     cesavilacum
local_port      8443
destination_port 8443
#active         0
#failed         0
#closed         0
#total          0
bytes up        0
bytes down      0
exception       None
-----
```

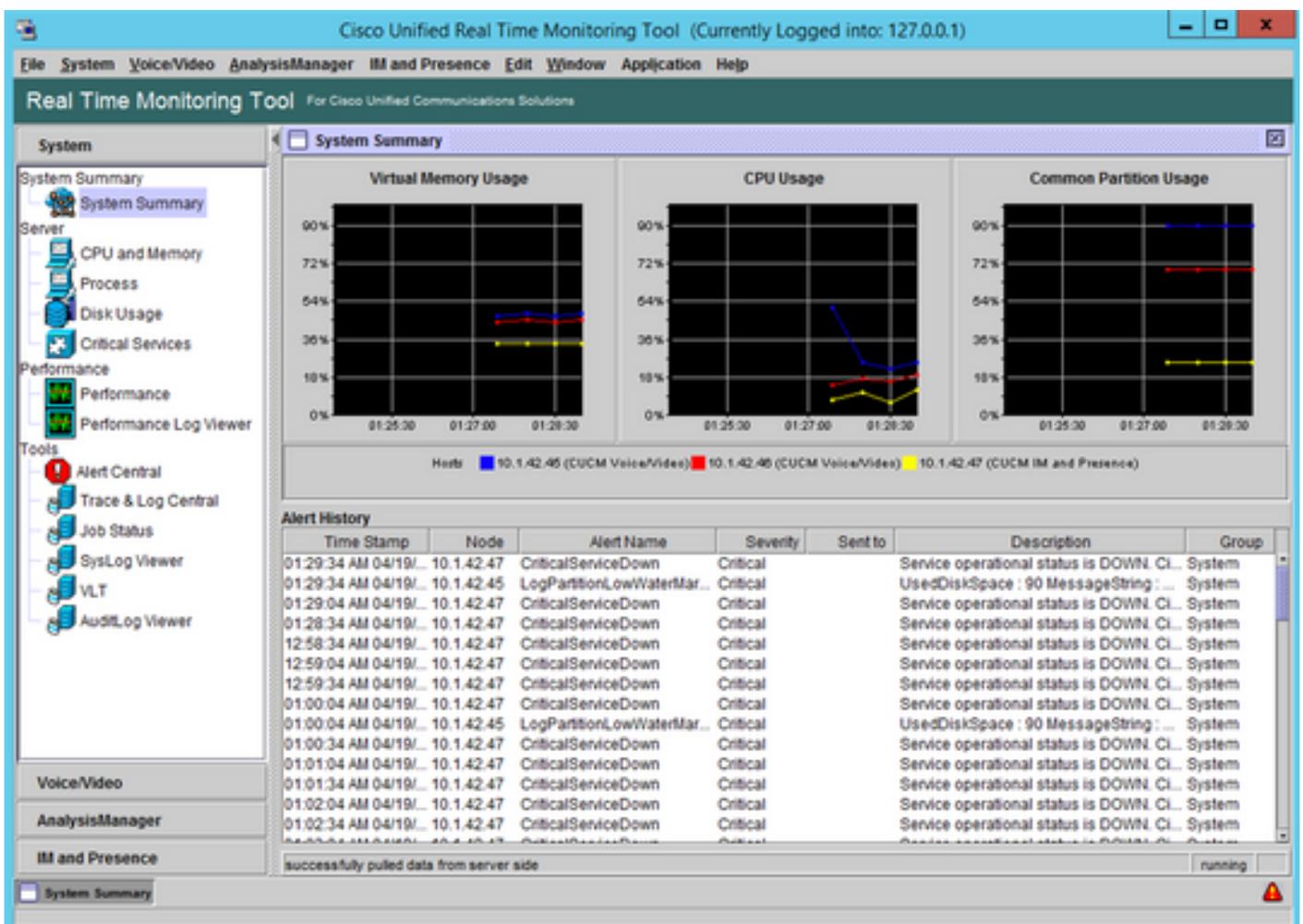
Étape 3. Ouvrez RTMT et tapez 127.0.0.1 dans l'adresse IP de l'hôte. Il utilise automatiquement le port 8443.



Étape 4. Connectez-vous avec les informations d'identification correctes.



Étape 5 : RTMT s'affiche.



Étape 6. Accédez à AnalysisManager dans le panneau de gauche.

Cisco Unified Real Time Monitoring Tool (Currently Logged into: localhost)

File System Voice/Video AnalysisManager IM and Presence Edit Window Application Help

Real Time Monitoring Tool

For Cisco Unified Communications Solutions

System

System Summary

- System Summary
- Server
 - CPU and Memory
 - Process
 - Disk Usage
 - Critical Services
- Performance
 - Performance
 - Performance Log Viewer
- Tools
 - Alert Central
 - Trace & Log Central
 - Job Status
 - SysLog Viewer
 - VLT
 - AuditLog Viewer

Voice/Video

AnalysisManager

IM and Presence

System Summary

System Summary

Virtual Memory Usage

CPU Usage

Common Partition Usage

Hosts: 10.1.42.45 (CUCM Voice/Video) 10.1.42.46 (CUCM Voice/Video) 10.1.42.47 (CUCM IM and Presence)

Alert History

Time Stamp	Node	Alert Name	Severity	Sent to	Description	Group
09:16:41 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:17:11 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:17:41 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:18:11 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:18:11 PM 0...	10.1.42...	LogPartitionLowWaterM...	Critical		UsedDiskSpace : 90 MessageString...	System
09:18:41 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:19:11 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:19:41 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:20:11 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:20:41 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:21:11 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System
09:21:41 PM 0...	10.1.42...	CriticalServiceDown	Critical		Service operational status is DOWN...	System

successfully pulled data from server side running

Étape 7. Cliquez sur Nodes and Add pour configurer les détails du périphérique à ajouter à l'aide de localhost et du port TCP transféré.

Real Time Monitoring Tool For Cisco Unified Communications Solutions

- System
- Voice/Video
- AnalysisManager
 - Inventory
 - Nodes**
 - Node Groups
 - Call Record Repositories
 - Trace File Repositories
 - Trace Templates
 - Tools
 - Analyze Call Path
 - Collect Traces Now
 - Schedule Trace Collection
 - Schedule Trace Settings and Collection
 - Set Trace Levels
 - View Configuration
 - Administration
 - Import
 - Job Status
 - Upload Files
- IM and Presence

Nodes	
Name	Node Type

Add Edit Delete Discover Test Connectivity Refresh



Add Node

Node Type* CUCM Voice/Video

IP/Host Name* 127.0.0.1

Transport Protocol* HTTPS

Port Number* 8443

User Name* admin

Password*

Confirm Password*

Description

Associated Call Record Repositories

Associated Trace File Repositories

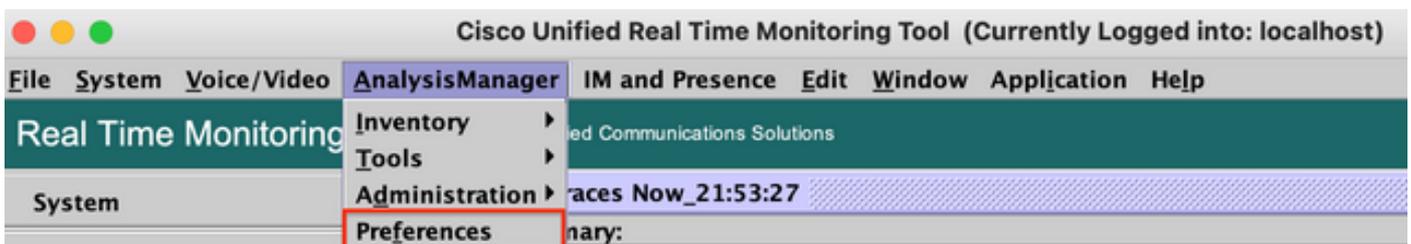
Associated Group AllNodes

Advanced...

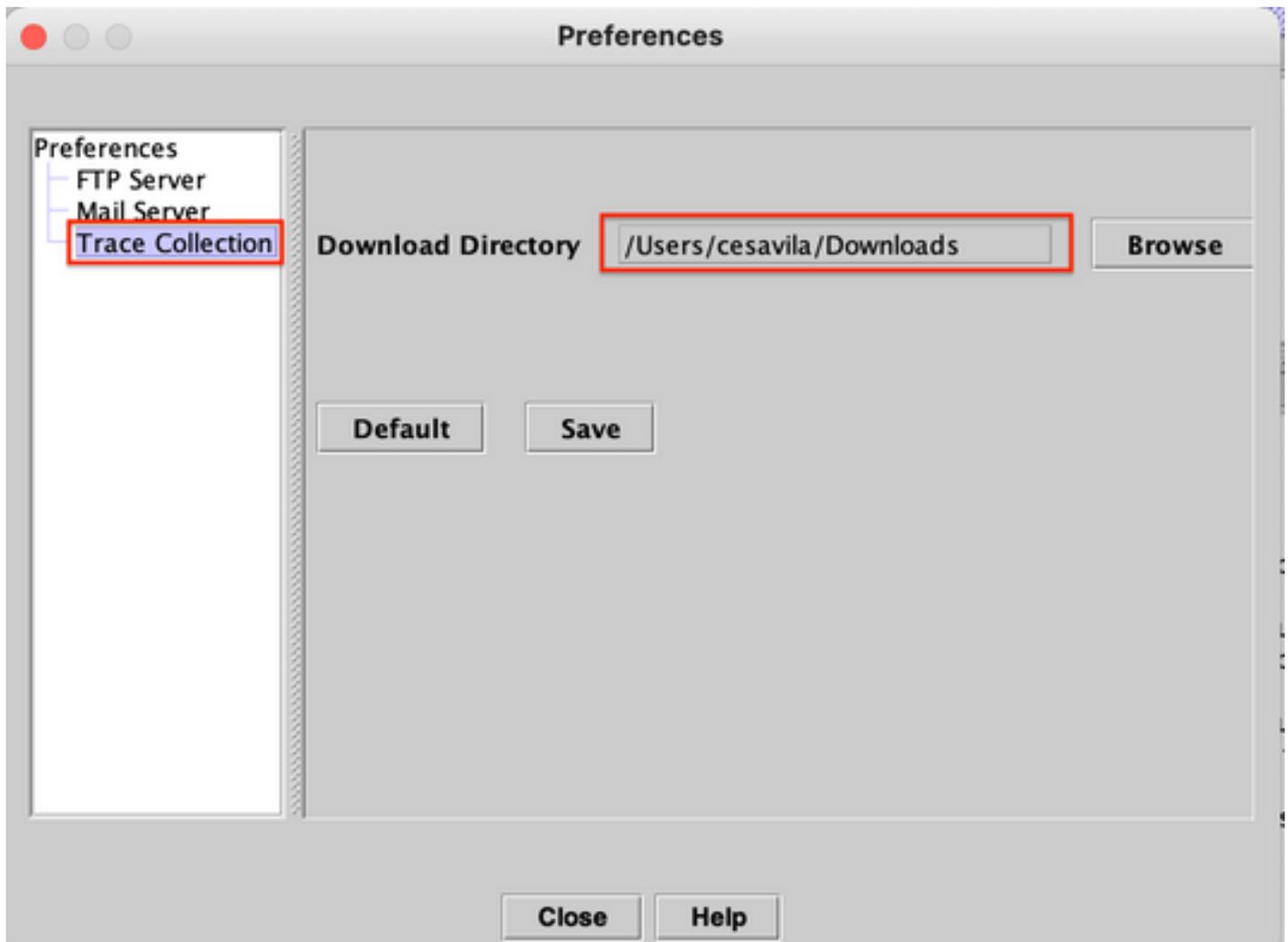
* Required Fields

Save Cancel

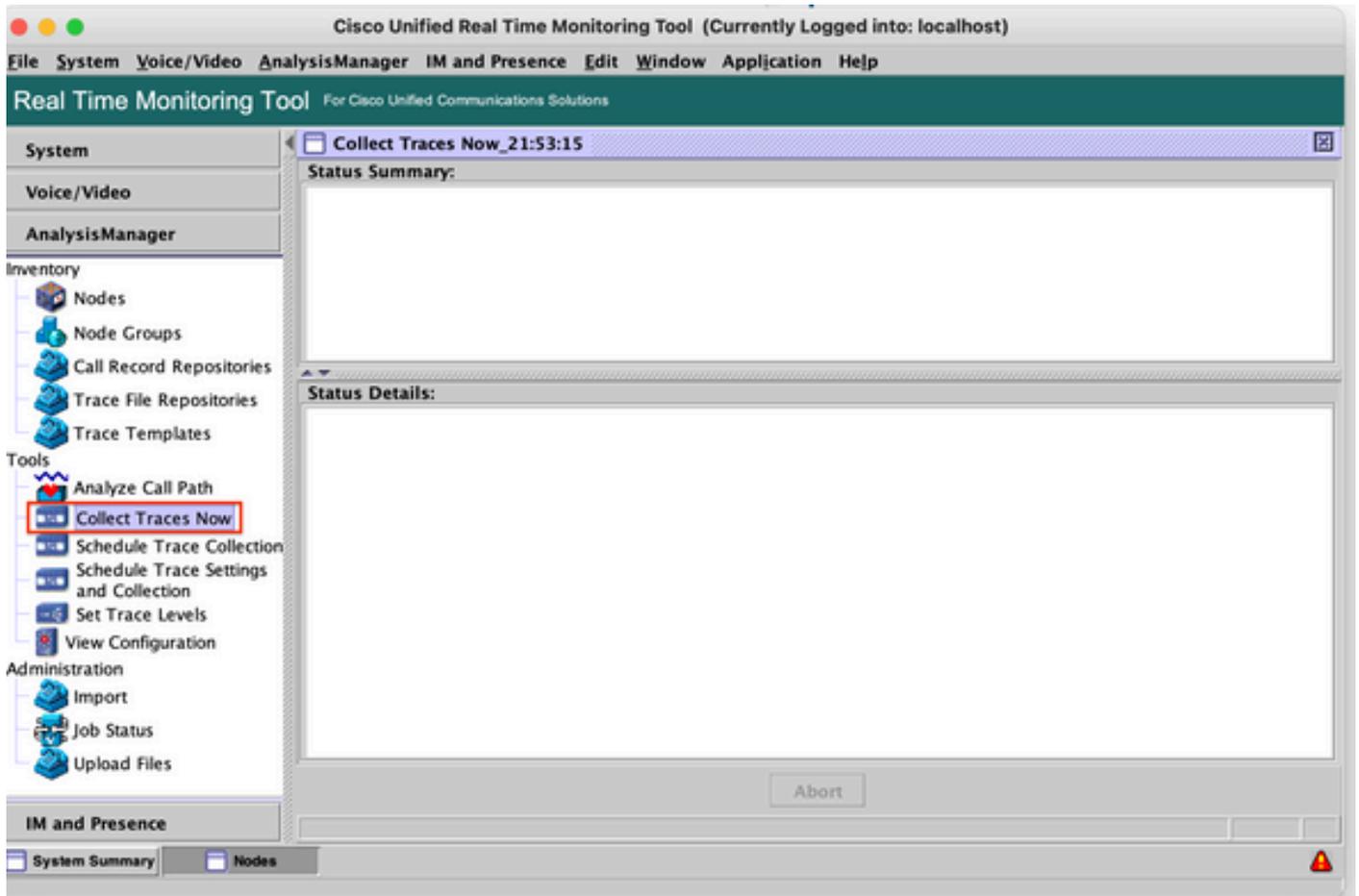
Étape 8. Cliquez sur Analysis Manager dans le menu en haut et sélectionnez Préférences.



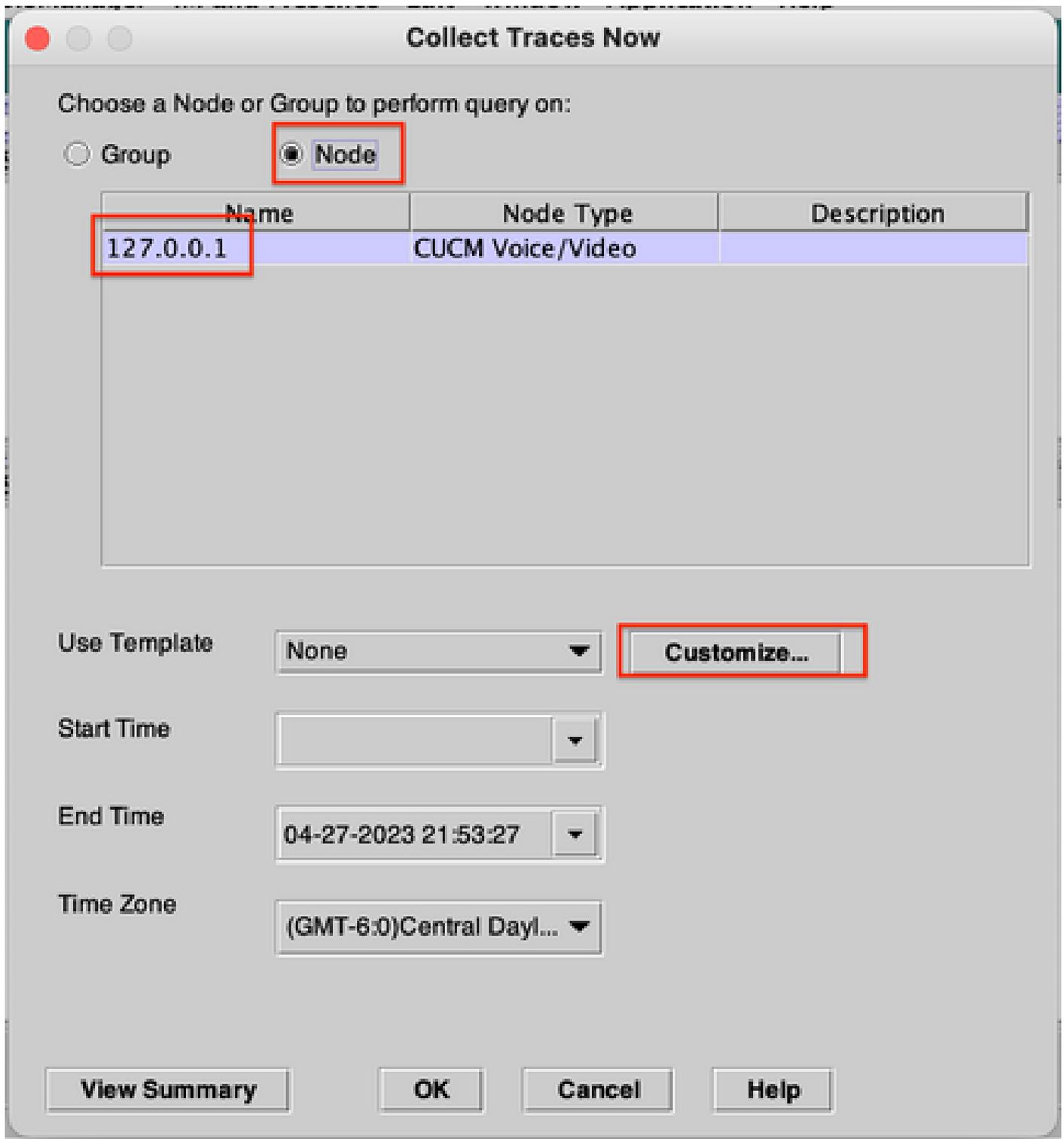
Étape 9. Accédez à Trace Collection et sélectionnez le dossier correct pour télécharger les journaux, cliquez sur Save, puis sur Close.



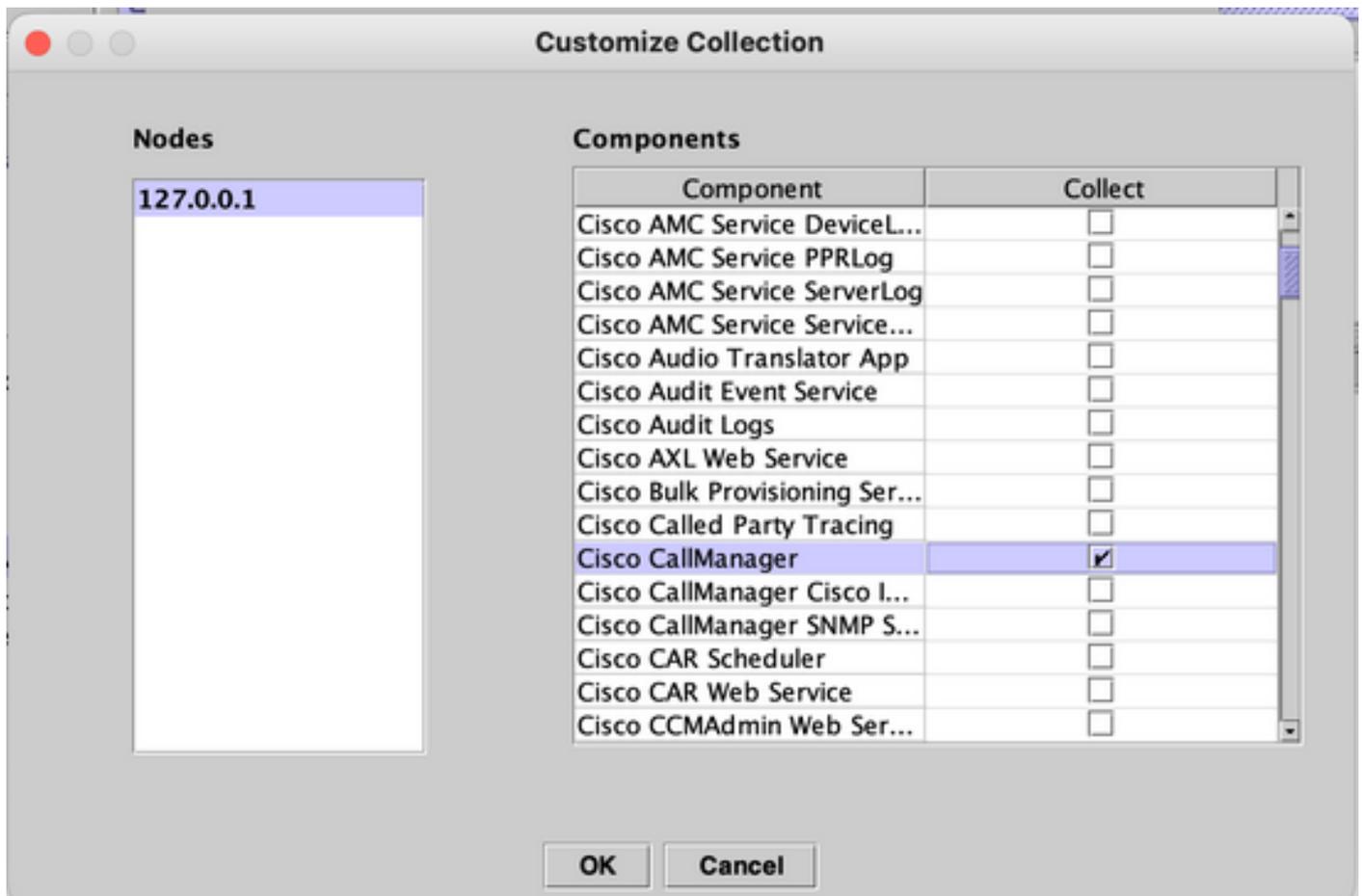
Étape 10. Accédez à Collecter les traces maintenant.



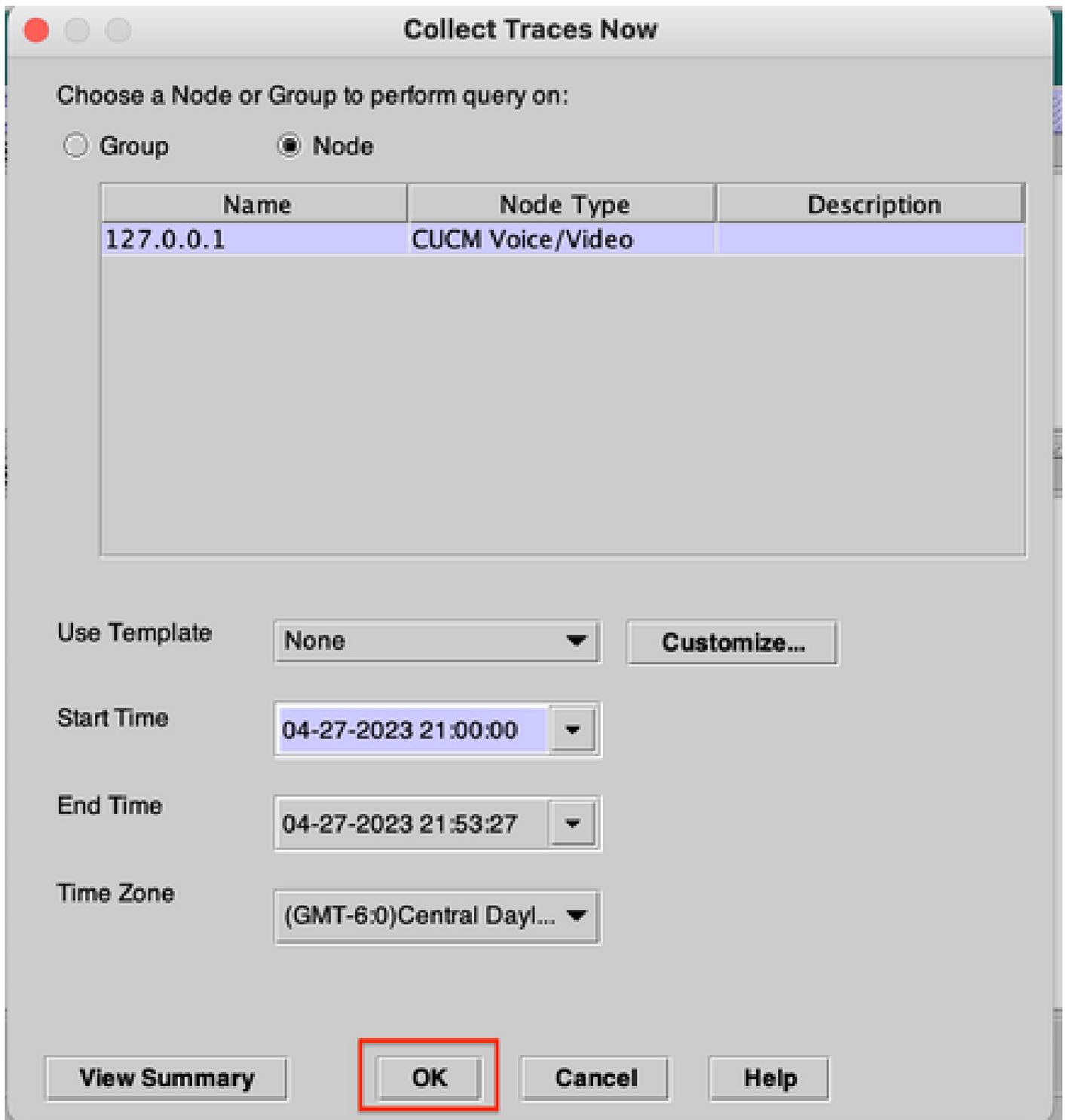
Étape 11. Sélectionnez l'option Noeud, sélectionnez le périphérique qui a été ajouté à l'étape 7 et cliquez sur Personnaliser.



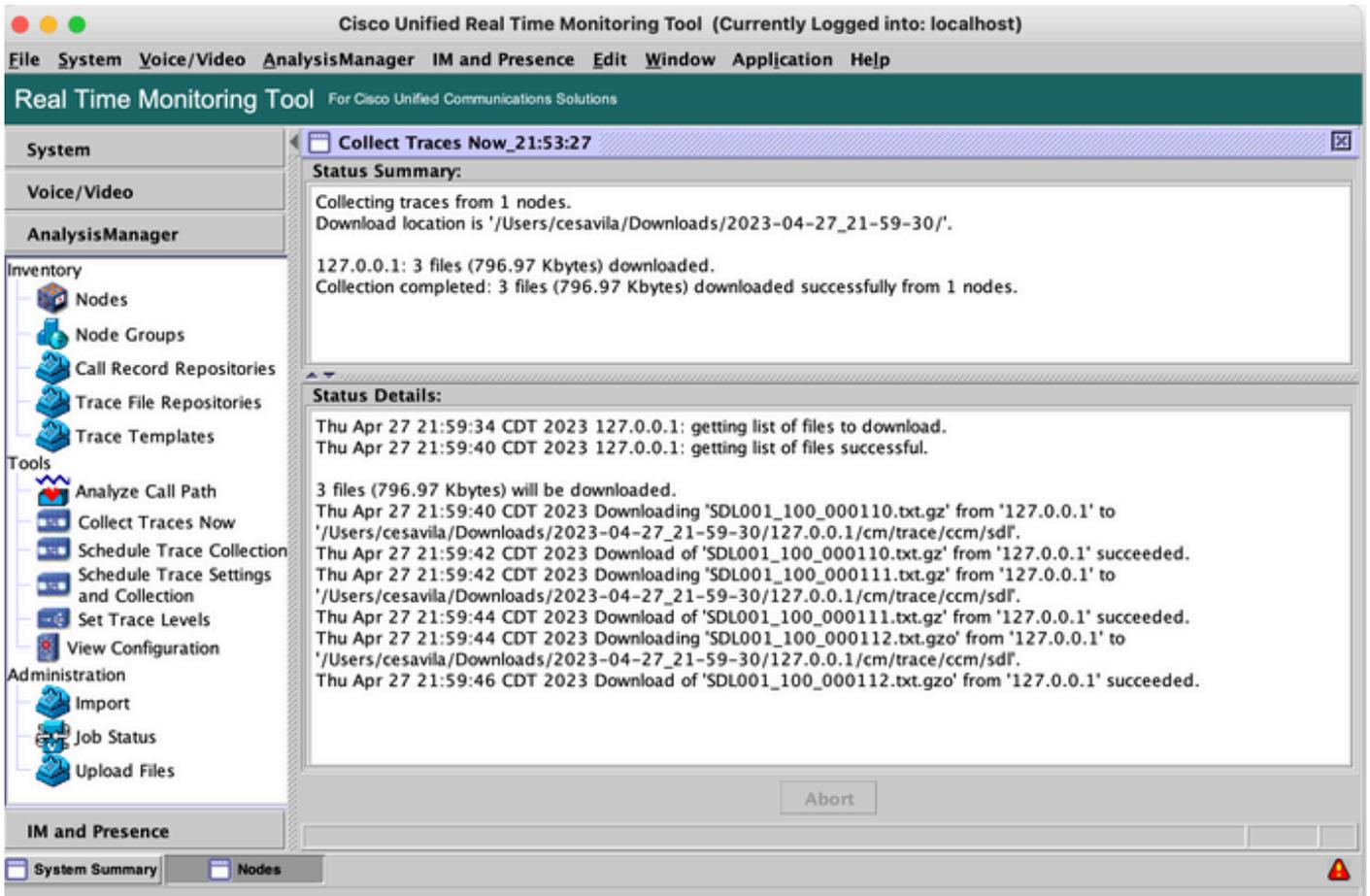
Étape 12. Sélectionnez les journaux à collecter auprès du périphérique et cliquez sur OK.



Étape 13. Sélectionnez enfin Heure de début et Heure de fin des journaux à collecter, puis cliquez sur OK.



Étape 14. Les fichiers sont téléchargés sur le PC local (RADKit Client PC).



- API SOAP

L'API SOAP est actuellement prise en charge pour CUCM. En outre, Swagger est pris en charge pour CMS, Expressway, CVP, etc.

Étape 1 : assurez-vous que les informations d'identification HTTP sont ajoutées au service RADKit sur la configuration du périphérique.

Étape 2 : exécutez la commande HTTP Post sur le client RADKit, spécifiez le chemin d'accès à la ressource, le corps de la requête avec les paramètres et les en-têtes nécessaires.

```
>>>
... r = cucm.http_post('/logcollectionsevice2/services/LogCollectionPortTypeService', content = '''<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/so
... ap/envelope/" xmlns:soap="http://schemas.cisco.com/ast/soap">
... <soapenv:Header/>
... <soapenv:Body>
... <soap:FileName>/var/log/active/cm/trace/ccm/sdl/SDL002_100_000819.txt.gz</soap:FileName>
... </soapenv:Body>
... </soapenv:Envelope>''', headers = {'Content-Type': 'text/xml; charset=utf-8', "SOAPAction": "GetOneFile"}, postprocessors = ['cucm-extract'])
>>>
```

Remarque : L'option de post-processeurs 'cucm-extraction' est utilisée pour supprimer les en-têtes de réponse HTTP afin de pouvoir enregistrer le journal dans un fichier.

```
>>> r
[SUCCESS] HttpResponse(device_name='cucmsiteb', method='POST', url='/logcollectionsservice2/services/LogCollectionPortTypeService', status_code=200)
-----
identity      cesavila@cisco.com
service_id    ckt7-tv6c-uale
device_name   cucmsiteb
method        POST
url           /logcollectionsservice2/services/LogCollectionPortTypeService
status_code   200 OK
content       b'\x1f\x8b\x08\x00\x00\x00\x00\x04\x03\xd4[\x8f\xdaF\x14~G\xe2?\x9c\xbe%\x95\x81\xc1\x170N\xa9\xca\x1aH\xac,\xae\xae\xcd\xf6\xa6\xd6\x1a\xdb\x03
X16\xb1\xc7\xc9n\xb5?\xbeg\xcc%\xf6n\xd8\x90\xaaUU\xb4f\x99\xe3\xb9|s\xae\xdf\x0cQ\xd4...'
-----
```

Étape 3. Enregistrez le contenu dans un fichier pour que le fichier de trace soit enregistré sur le PC local.

<#root>

```
>>> content = r.content
>>> with open('SDL002_100_000819.txt.gz', 'wb') as file:
    file.write(content)
```

Exemples d'utilisation RADKit

Comme cela a été souligné, RADKit fournit une connexion sécurisée aux périphériques réseau, y compris les serveurs de collaboration, sans avoir besoin d'être sur un WebEx. L'idée est de simplifier certains des défis liés à la collecte de données en fournissant un accès à la demande aux périphériques requis.

En ce qui concerne plus particulièrement les déploiements de solutions de collaboration, RADKit peut actuellement s'avérer très utile pour de nombreux problèmes tels que :

- Problèmes de réplication DB.
- Procédures de régénération de certificat.
- Vérification de l'état du système
- Validation de la configuration dans GUI / CLI.
- Collecte des journaux via l'interface Web (par exemple, CER, Expressway, CIMC, etc.).
- Journaux de débogage via CLI sur les passerelles vocales.

Informations connexes

- Page principale de RADKit <https://radkit.cisco.com/>
- Page d'assistance RADKit externe <https://community.cisco.com/t5/radkit-discussions/bd-p/disc-radkit>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.