Configuration de l'intégration Cisco RADKit dans FMC

Table des matières

Introduction

Ce document décrit la fonctionnalité Cisco RADKit Integration dans FMC ajoutée dans la version 7.7.

Fond

Problème rencontré par les administrateurs de pare-feu

- Le Remote Automation Development Kit (RADKit), développé par Cisco, est un orchestrateur à l'échelle du réseau conçu pour offrir aux utilisateurs la possibilité d'accéder de manière sécurisée et de dépanner les périphériques réseau. https://radkit.cisco.com/
- Le Cisco Secure Firewall Management Center (FMC) gère et exploite les périphériques Secure Firewall Threat Defense (FTD). Un seul contrôleur FMC peut gérer plusieurs périphériques sur différents sites.
- Bien qu'il soit possible pour les utilisateurs d'installer RADKit séparément et d'y intégrer leurs FMC et FTD, l'intégration du service RADKit dans le FMC et l'intégration du ou des FMC et de tous les périphériques gérés (FTD) de manière automatisée serait une meilleure expérience pour les utilisateurs finaux.

Scénario

Voici quelques-unes des fonctionnalités clés dont les utilisateurs pourraient bénéficier après l'intégration de RADKit dans le FMC :

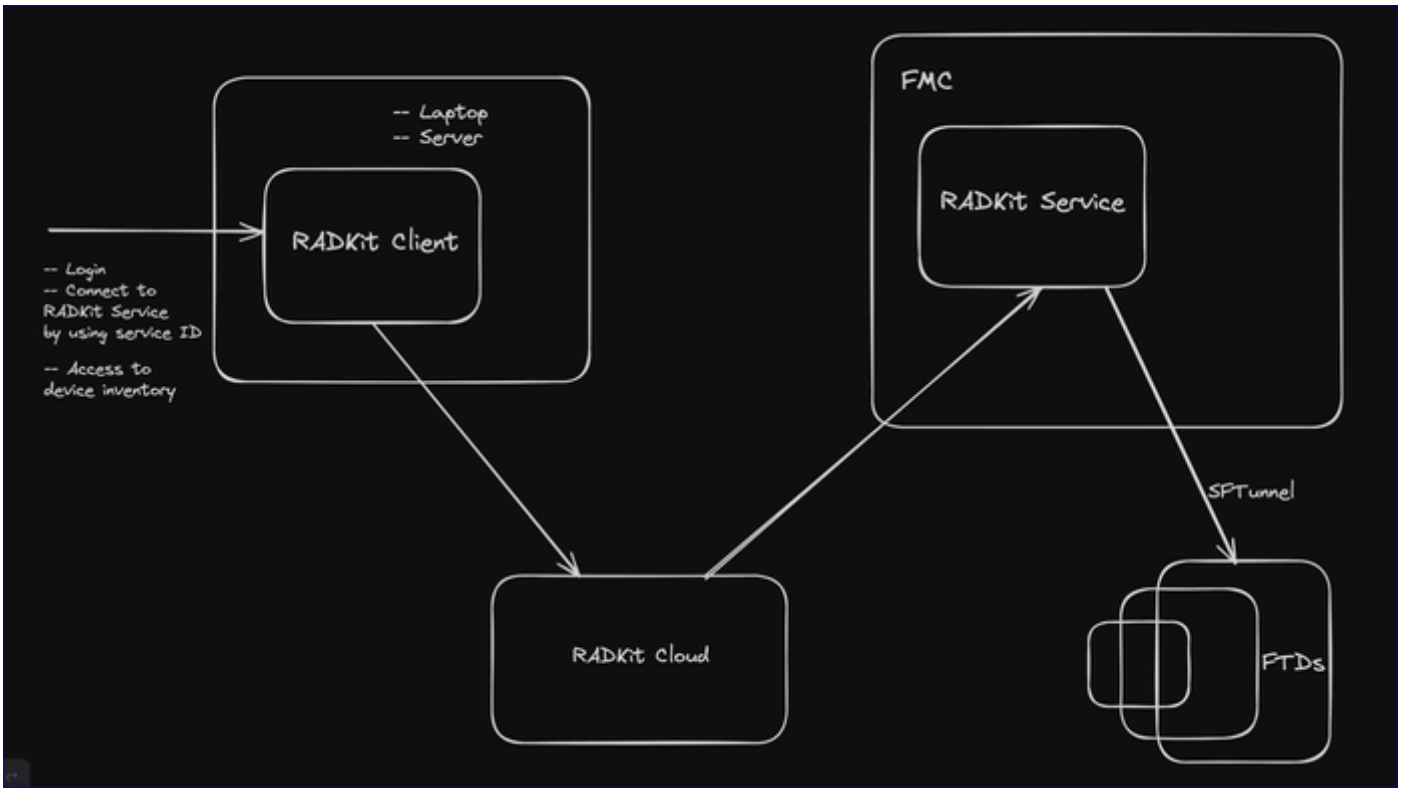
- Possibilité d'accéder aux FMC/FTD à distance depuis l'interface de ligne de commande du client RADKit.
- Possibilité de fournir un accès contrôlé aux FMC/FTD à toute personne qui en a besoin (par exemple, un ingénieur du centre d'assistance technique Cisco).
- Exploitez les fonctionnalités d'automatisation pour collecter des données et diagnostiquer les problèmes à partir du client RADKit (les scripts qui exécutent des commandes sur plusieurs périphériques peuvent être créés et utilisés à partir du client RADKit).

Nouveautés - Solution

- À partir de Secure Firewall 7.7.0, le service Remote Automation Development Kit (RADKit) est intégré à FMC.
- Les utilisateurs peuvent activer ou désactiver le service RADKit à la demande, l'inscrire dans le cloud RADKit et créer des autorisations d'utilisateurs distants pour accéder à des périphériques spécifiques à partir du client RADKit pour une durée d'accès planifiée.
    - Les autorisations peuvent être modifiées ou révoquées.
- Il est également possible de fournir un accès sudo aux périphériques pour un dépannage avancé.

Intégration du service RADKit dans le diagramme FMC

Ce schéma montre comment RADKit permet la communication entre le client RADKit de l'utilisateur (ingénieur TAC) et les périphériques FTD de production :



Notions de base Plates-formes prises en charge, licences

Applications et gestionnaires

FTD		ASA	
FMC and FTD Platforms: All		Not supported	
FMC on 7.7.0 FMC REST API	Yes Yes	ASA CLI 9.23.1	No
FTD Supported Versions *(lowest version FMC on 7.7.0 can manage is 7.2)*	7.7.0 only	ASDM 7.23.1	No
Snort Support (Snort 3 is the only Snort version supported in 7.7)	Snort 3 Snort 2 (only for devices on 7.2.x..7.6.x)	CSM 4.30	No
FDM on 7.7.0	No		

Autres aspects du soutien

Platforms	
FTD	
Licenses Required	No licensing requirements for this feature.
Works in Evaluation Mode	Yes
IP Addressing	IPv4 IPv6
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes
Other (only routed mode | transparent mode), etc.	No Special Notes
Internet access for the RADKit cloud enrollment required	Access to prod.radkit-cloud.cisco.com

Dépendances pour le fonctionnement de la fonctionnalité

- La version minimale est Secure Firewall 7.7.0.
- Pour la connexion au service RADKit hébergé dans FMC, le client RADKit doit être installé à partir de https://radkit.cisco.com/downloads/release/ sur l'ordinateur de l'ingénieur du support.
- La version préférée du client RADKit est 1.6.10 ou supérieure.
- Les versions plus anciennes de RADKit Client peuvent être utilisées car le service RADKit est rétrocompatible avec les versions plus anciennes de RADKit Client.

Description des fonctionnalités et procédure pas à pas

Présentation des fonctionnalités

- L'intégration du service RADKit dans FMC permet aux administrateurs de périphériques de fournir aux utilisateurs distants (ingénieurs du TAC Cisco) un accès à des périphériques FMC et FTD spécifiques de leur réseau à des fins de dépannage et d'automatisation. RADKit est beaucoup plus efficace pour le dépannage que le partage d'écran, il ne nécessite pas de contrôler l'ordinateur de l'utilisateur, est un moyen plus sûr de travailler sur un réseau et complète bien Webex.
- Cela améliore l'expérience du support technique, car les administrateurs de périphériques n'ont pas à installer et configurer le service RADKit séparément. Cela réduit également le temps d'assistance des ingénieurs du TAC Cisco pour la résolution des problèmes d'assistance.

Configuration Steps: Aperçu

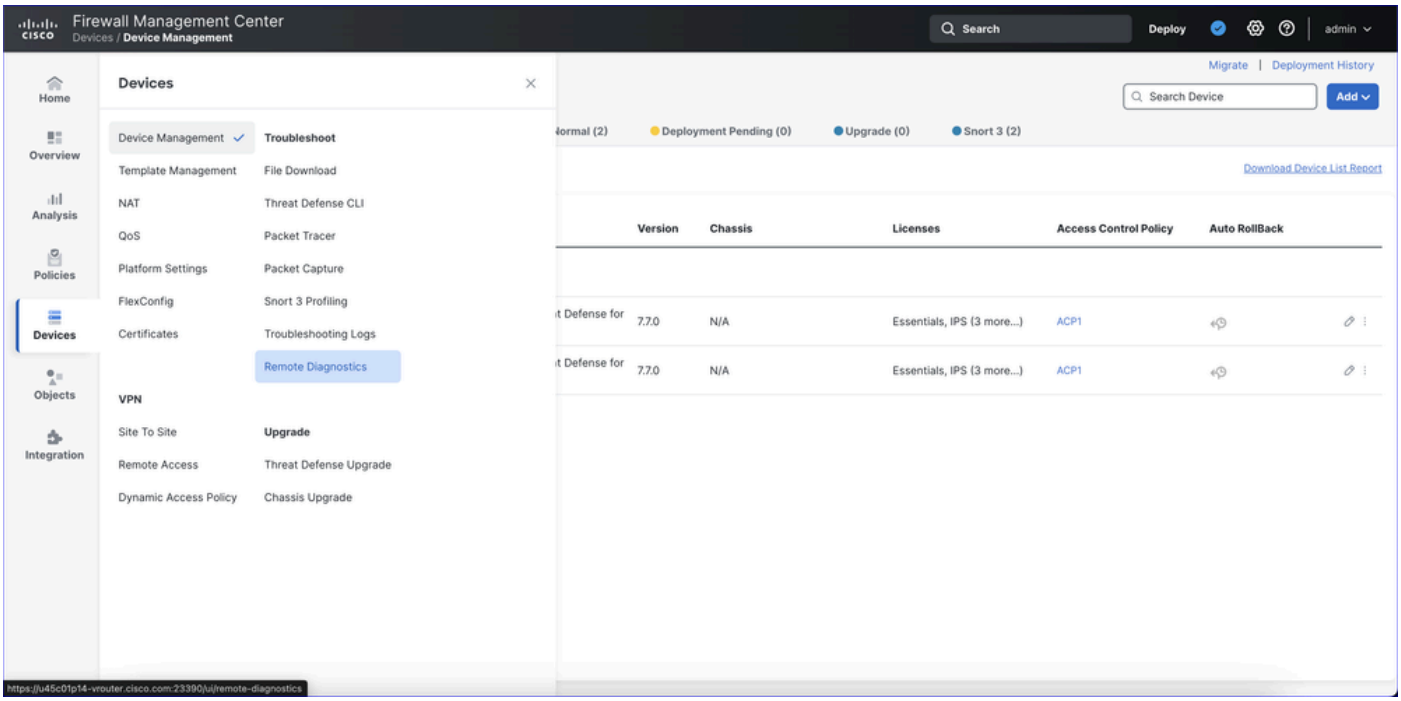
1. Administrateur de périphérique (utilisateur administrateur FMC) : Activez et inscrivez le service RADKit et configurez les autorisations sur l'interface utilisateur graphique FMC.

2. Assistance Cisco TAC/Cisco : Installez le client RADKit sur leur ordinateur, accédez aux périphériques et dépannez-les à partir du client RADKit.

Utilisateur admin FMC : Procédure pas à pas de Firewall Management Center

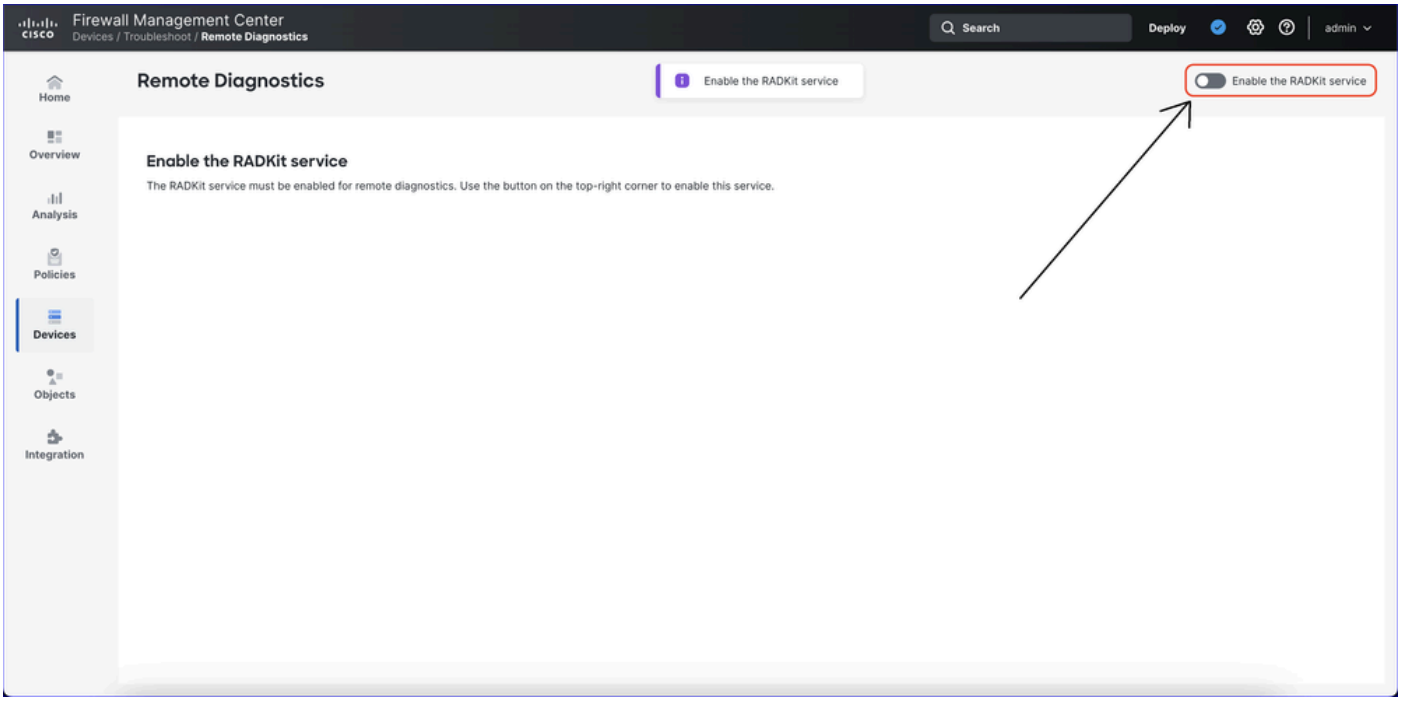
Menu Diagnostics à distance

- Un nouvel élément de menu "Diagnostics à distance" a été ajouté pour cette fonctionnalité sous Périphériques -> Dépannage.
- Les utilisateurs Administrateur, Administrateur réseau et Maintenance disposent d'autorisations de lecture/écriture sur la page.
- Les utilisateurs Analyste de sécurité, Analyste de sécurité (lecture seule) et Approbateur de sécurité disposent d'autorisations en lecture seule sur la page.



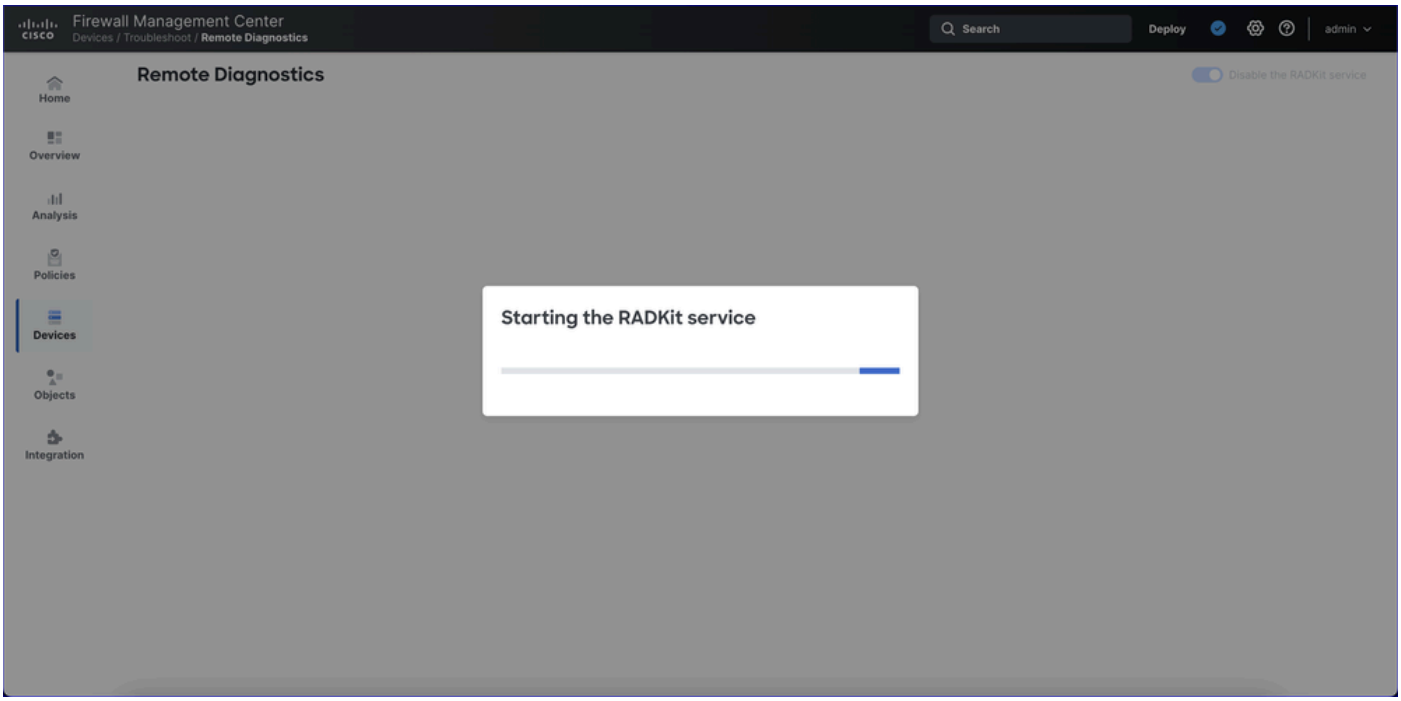
Page Diagnostics à distance initiaux

Il s'agit de la page Diagnostics à distance initiale. Le service RADKit peut être activé en activant le commutateur « Activer le service RADKit » :



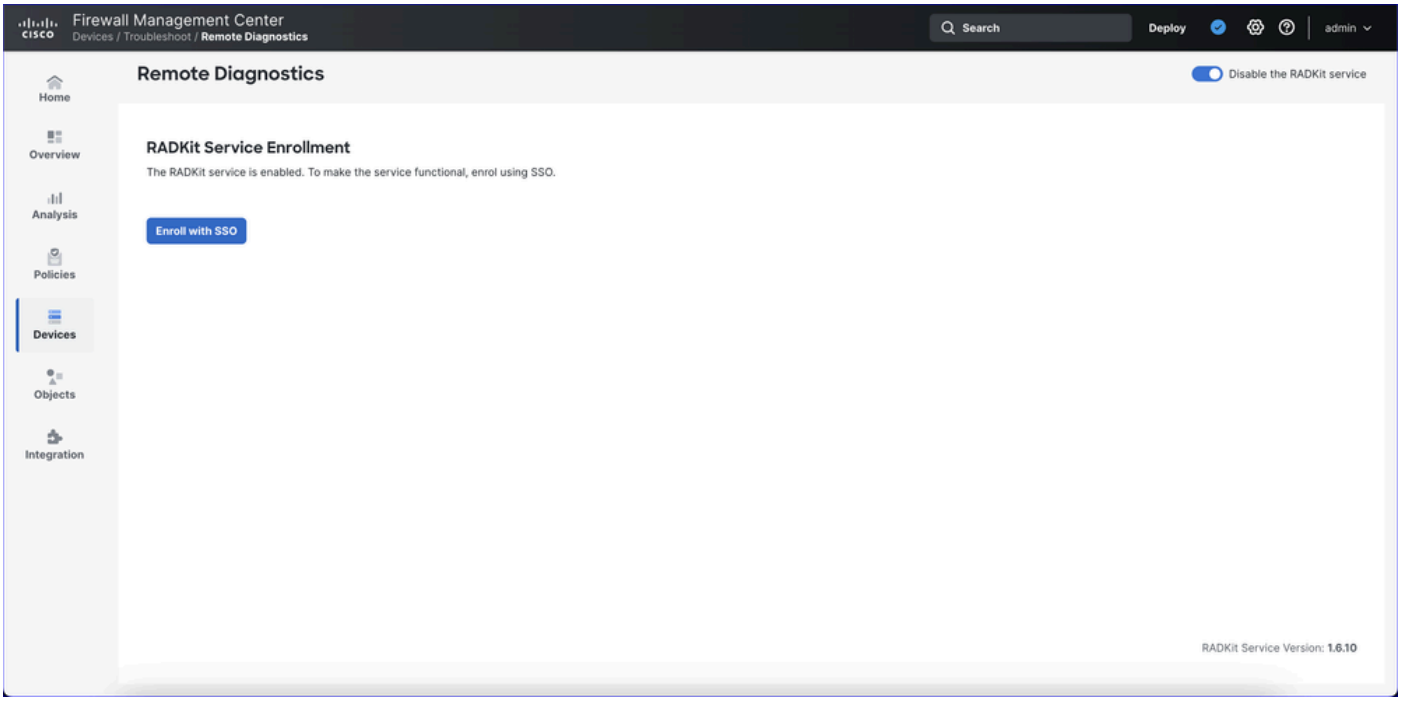
Démarrage du service RADKit

Après avoir activé le service RADKit, une barre de progression apparaît jusqu'à ce que le service RADKit soit démarré :



Service RADKit activé

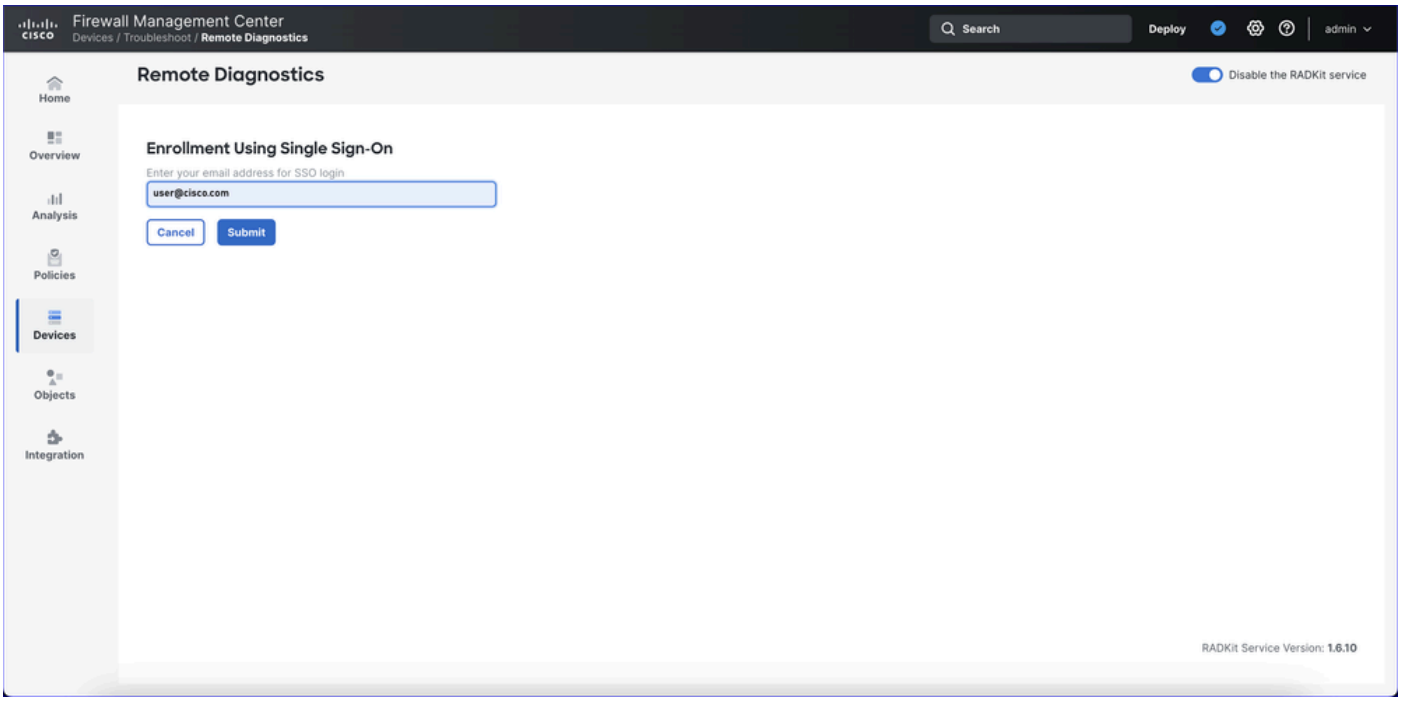
- Lorsque le processus d'activation du service RADKit est terminé, cette page s'affiche :



L'étape suivante consiste à vous inscrire dans le cloud RADKit en cliquant sur le bouton « S'inscrire avec SSO ».

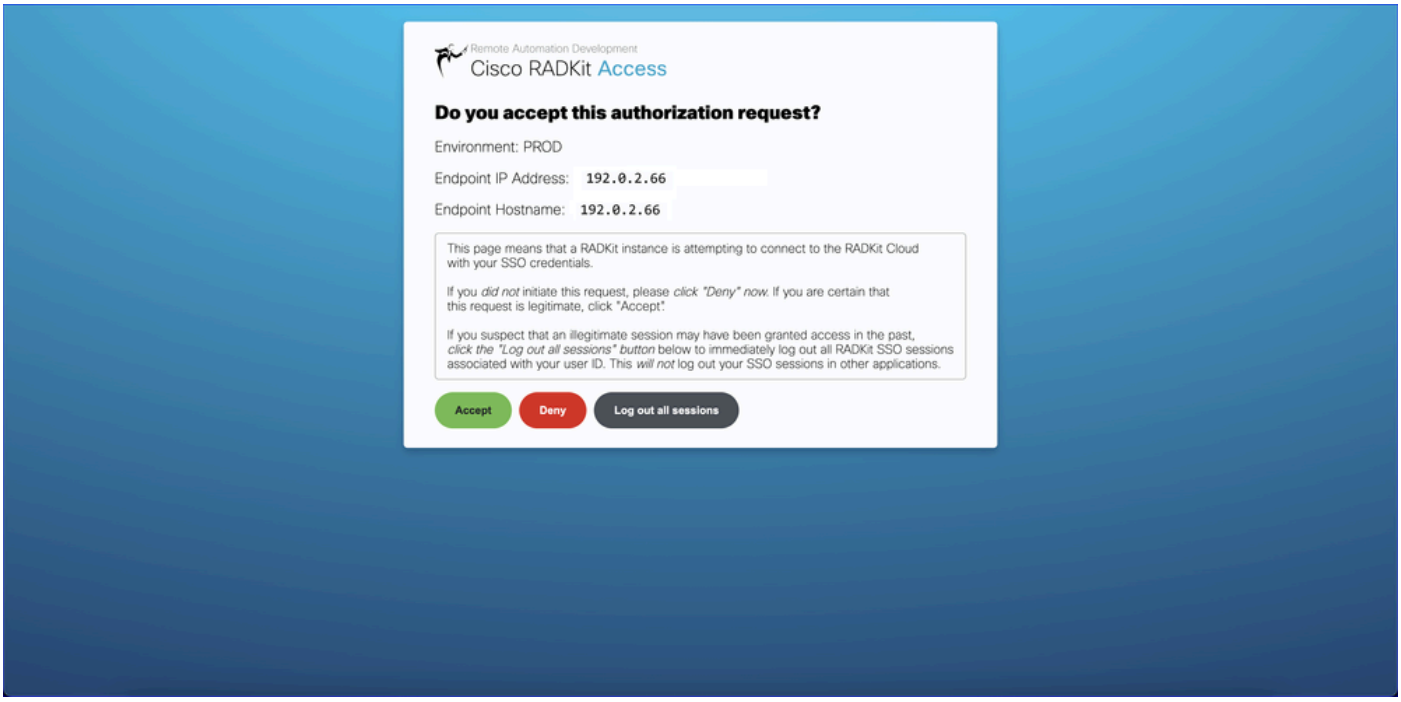
S'inscrire avec SSO - Saisir une adresse e-mail

L'étape 1 du processus d'inscription consiste à saisir l'adresse e-mail de l'utilisateur pour l'inscription au cloud RADKit :



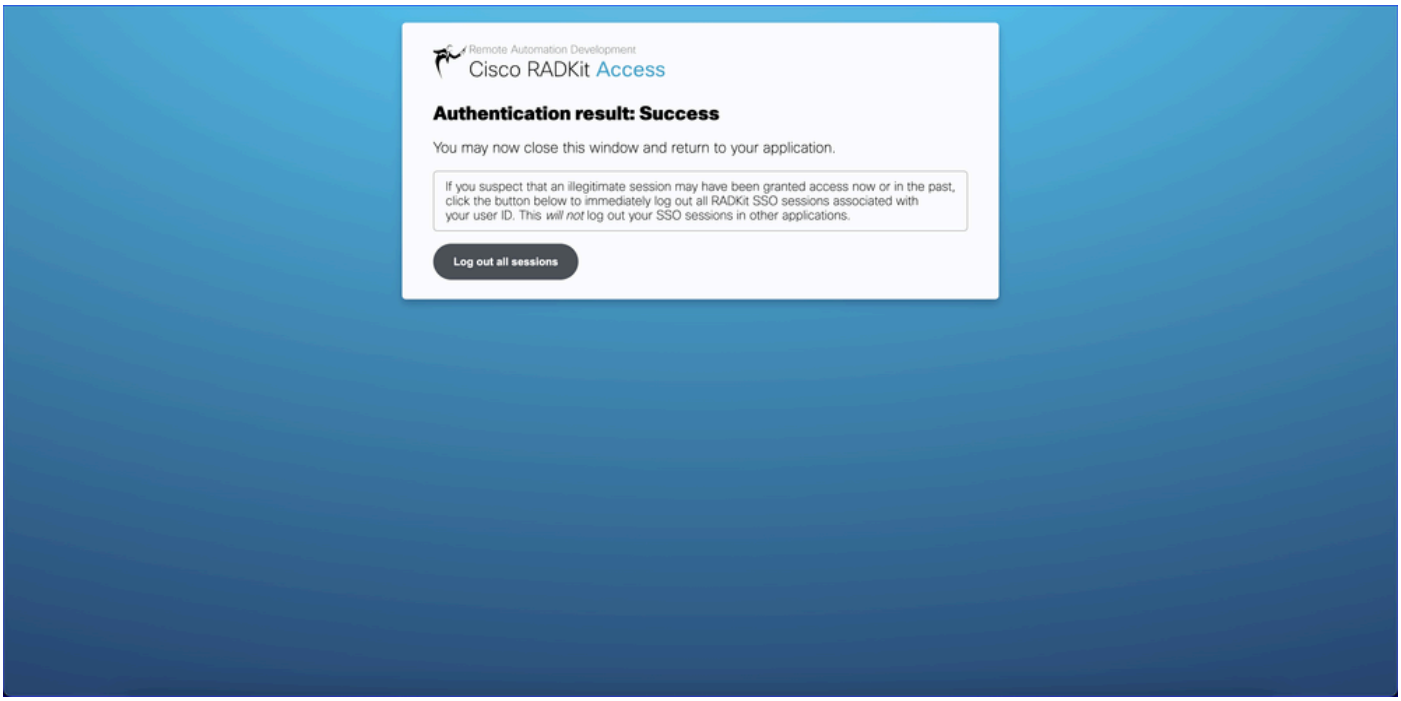
S'inscrire avec SSO - Accepter la demande d'autorisation

Un nouvel onglet de navigateur (ou une nouvelle fenêtre, selon les paramètres du navigateur) s'ouvre. Cliquez sur le bouton Accepter.



Inscription avec SSO - Authentification réussie

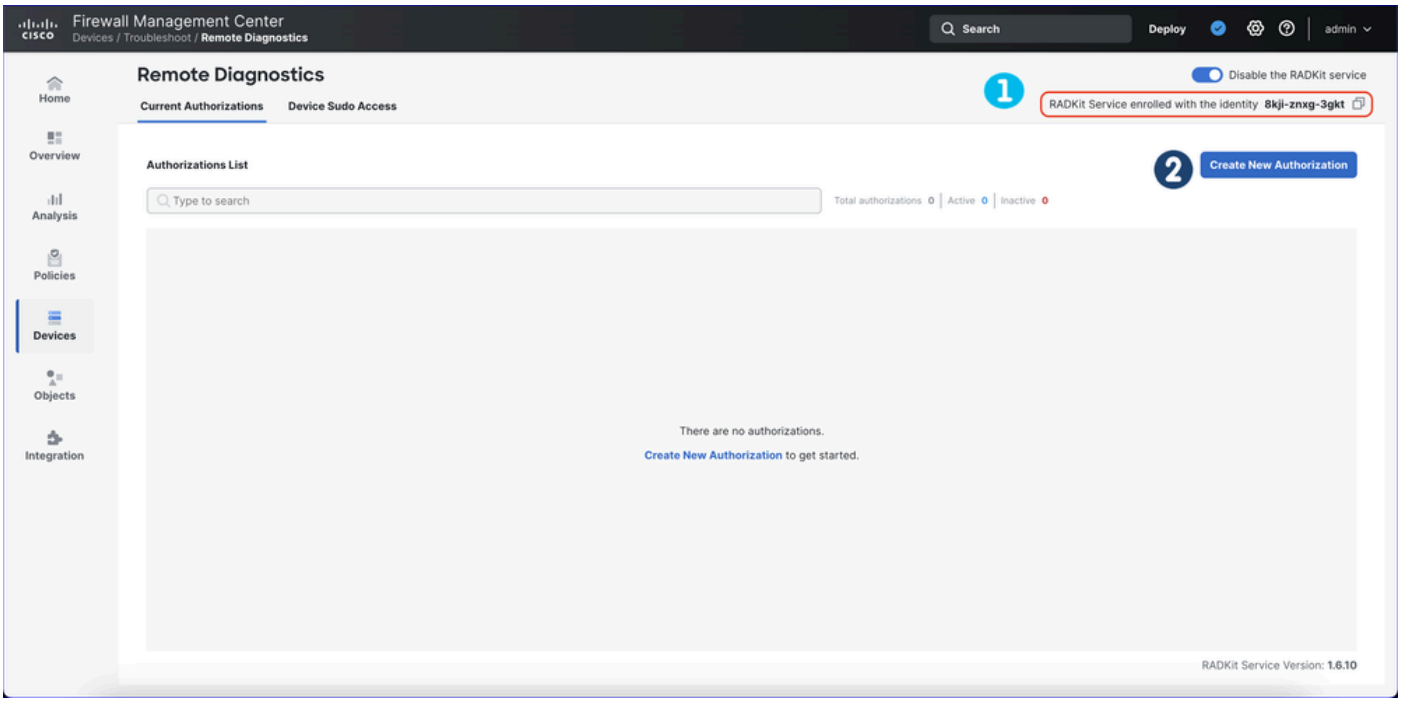
Une fois l'authentification réussie, l'utilisateur peut fermer l'onglet du navigateur et revenir à la page Diagnostics à distance FMC.



Service RADKit inscrit

Le service RADKit est inscrit avec l'ID de service spécifié (dans cet exemple, l'ID est 8kji-znxg-3gkt). L'ID peut être copié dans le Presse-papiers. Adressez-le à l'ingénieur du centre d'assistance technique Cisco afin qu'il puisse se connecter au service RADKit à partir du client RADKit.

L'étape suivante consiste à créer une autorisation en cliquant sur le bouton « Create New Authorization » :

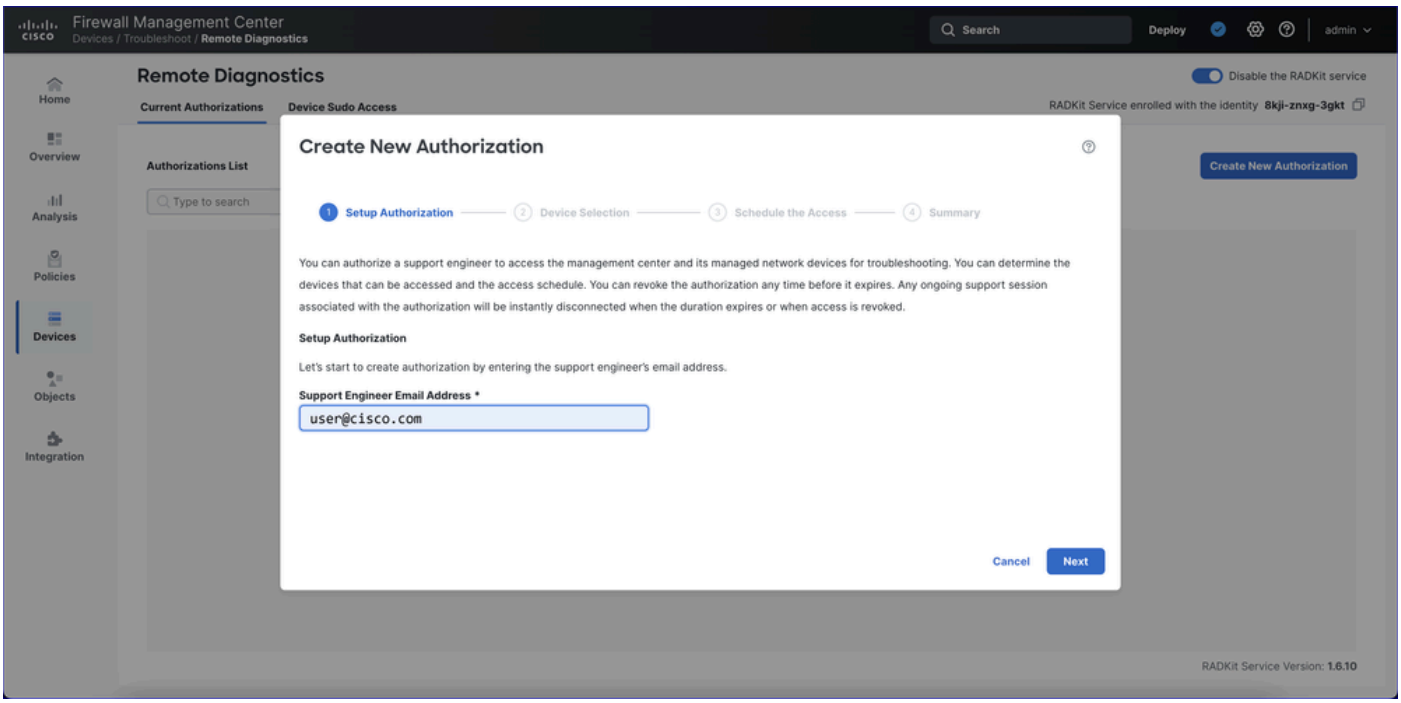


Créer une nouvelle autorisation : Étape 1

- Pour créer une nouvelle autorisation, la première étape consiste à ajouter l'adresse e-mail

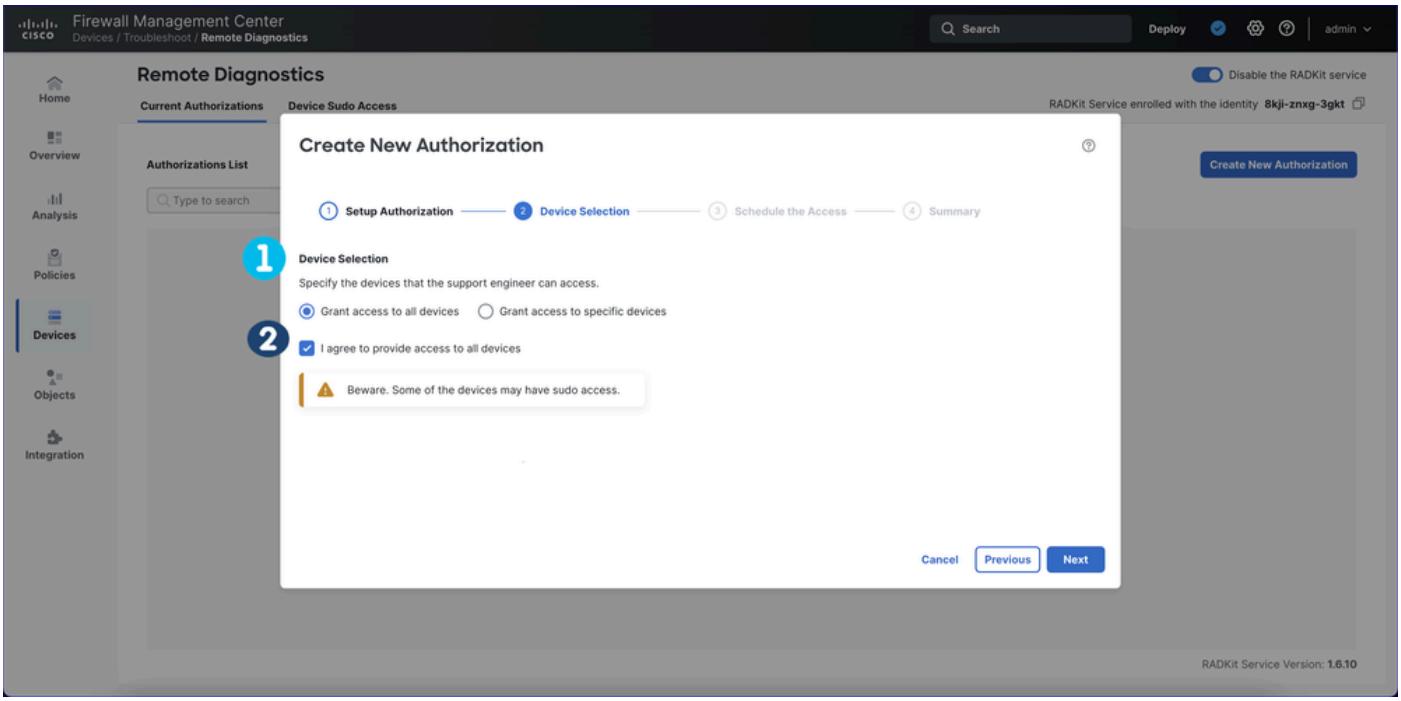
de l'ingénieur du support technique.

- La création d’une nouvelle autorisation s’effectue en quatre étapes. La progression le long des étapes est indiquée en haut.



Créer une nouvelle autorisation : Étape 2

- Étape 1 : Spécifiez les périphériques auxquels l'ingénieur du support technique peut accéder. Ou, comme dans cet exemple, accordez l'accès à tous les périphériques.
- Étape 2 : Cochez la case d'option pour tous les périphériques ou pour des périphériques spécifiques. Pour des périphériques spécifiques, des FMC et/ou des FTD peuvent être sélectionnés. Notez l'avertissement que l'accès sudo peut fournir à certains périphériques dans l'onglet Device Sudo Access. Le bouton Suivant n'est pas activé tant que la case n'est pas cochée.
- L'accès Sudo est fourni par périphérique dans l'onglet Device Sudo Access plus tard (pas lors de la création d'une autorisation).

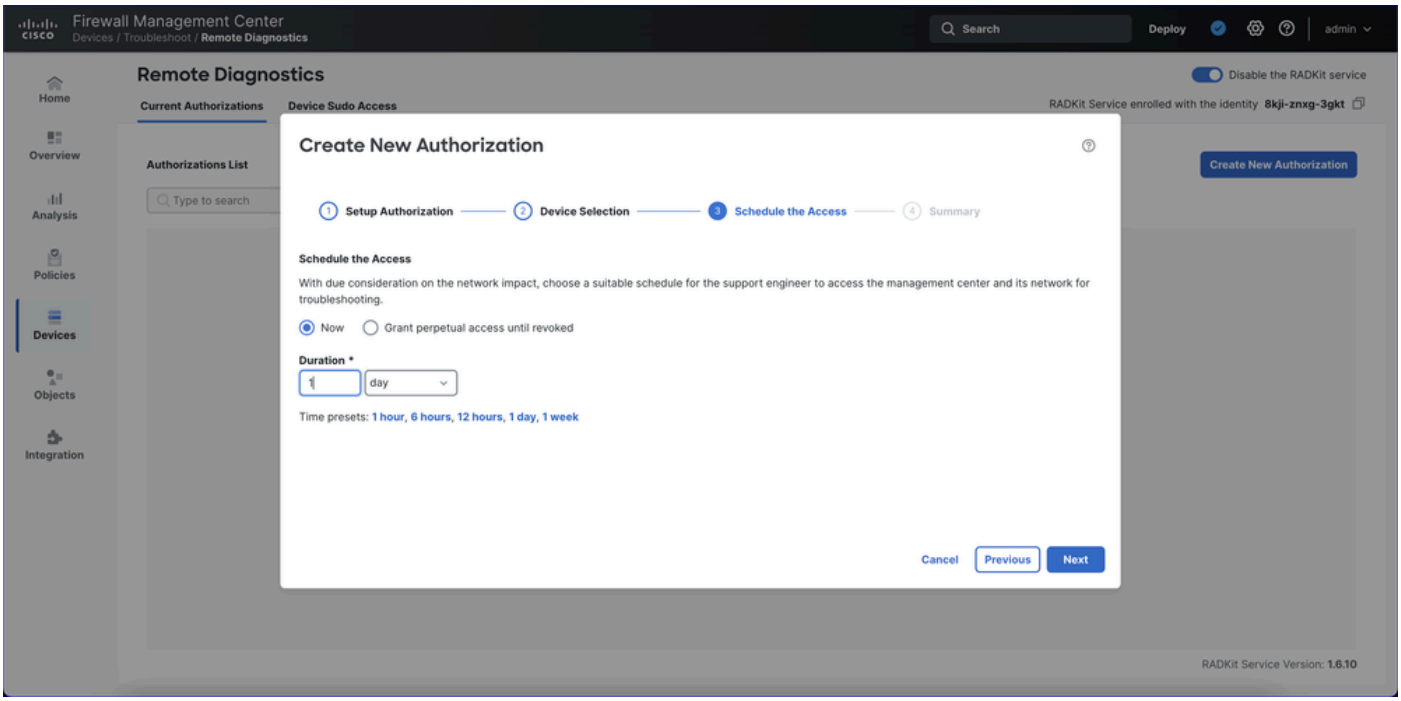


Remarques sur les périphériques de prélèvement

- Seuls les périphériques d'une version prise en charge (par exemple, dans la version initiale, seuls les périphériques 7.7.0) peuvent être sélectionnés.
- Les périphériques qui sont désactivés et inaccessibles ne peuvent pas être sélectionnés. RADKit utilise sftunnel (TCP 8305) pour accéder aux périphériques.
  - Si un problème de connectivité sftunnel survient, il ne fonctionne pas, mais il est toujours affiché dans l'inventaire RADKit.
  - Si un périphérique est hors tension, il n'est pas visible du tout.
- S'il existe des FMC dans une paire haute disponibilité, seul le principal/actif peut être ajouté.
- Les périphériques sont ajoutés à l'inventaire RADKit lors de la création/modification d'une autorisation. Lorsque des périphériques sont radiés de FMC, ils sont supprimés de l'« inventaire » des périphériques.

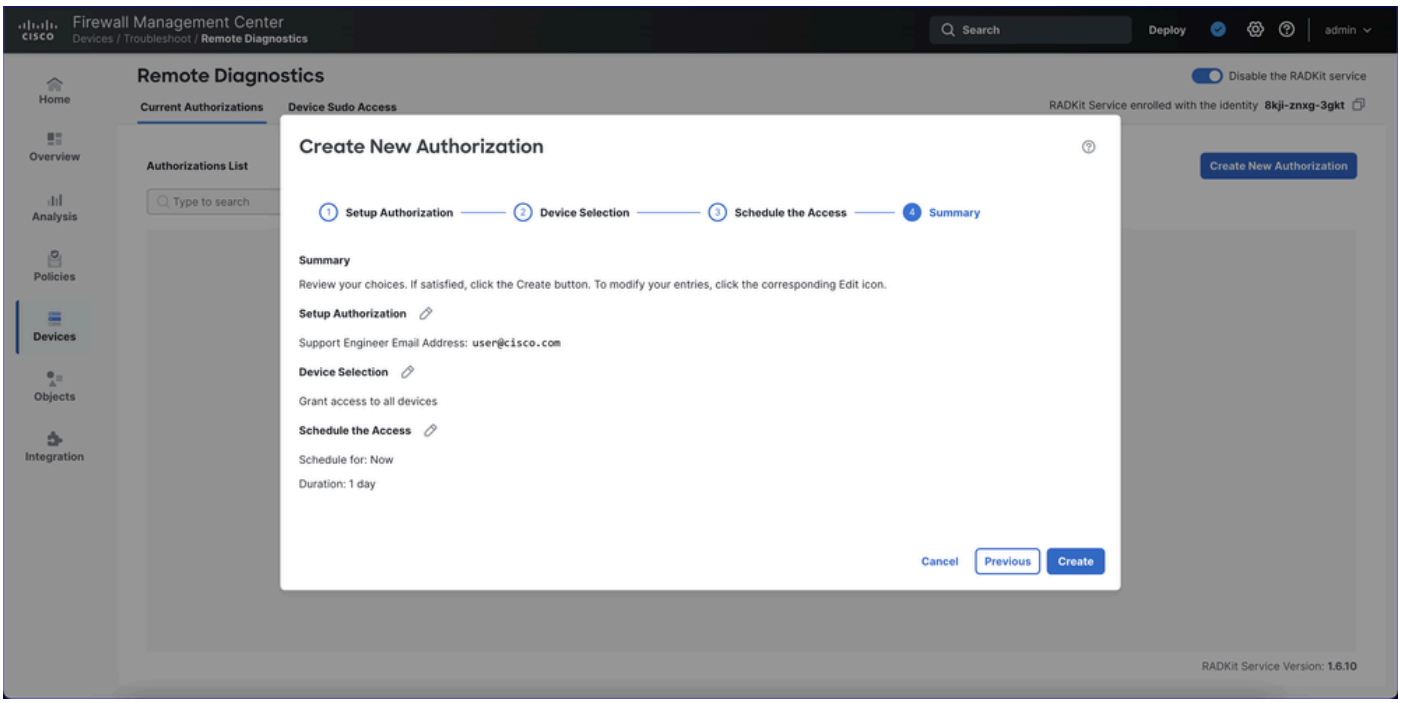
Créer une nouvelle autorisation : Étape 3

- Étape 3 : Spécifiez la durée pendant laquelle l'ingénieur du support technique peut accéder aux périphériques.
- Sélectionnez "Maintenant" et spécifiez une durée, ou,
- Sélectionnez "Accorder un accès permanent jusqu'à révocation".
- La durée par défaut est de 1 jour. Toute durée peut être définie ; il existe également des valeurs de durée prédéfinies.



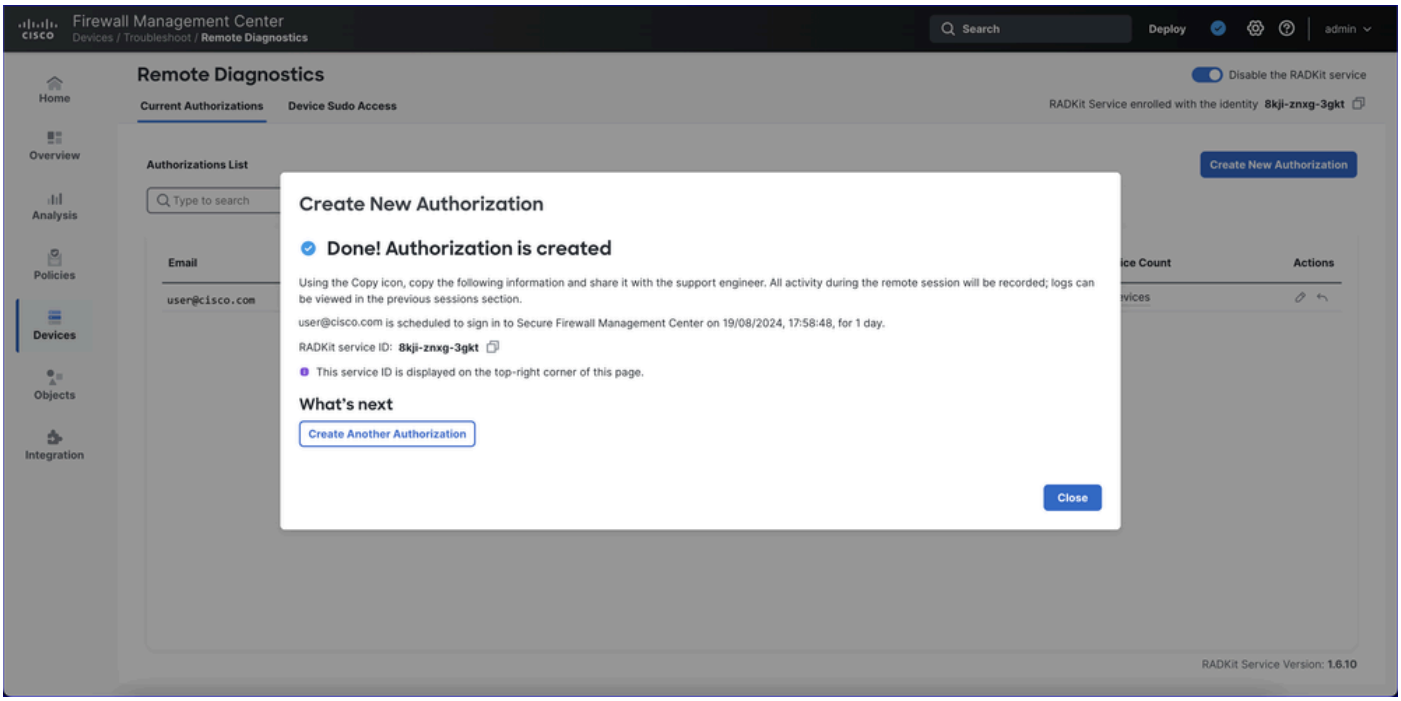
Créer un résumé d'autorisation

La dernière étape est le résumé de l'autorisation. Ici, un utilisateur peut vérifier et modifier la configuration.



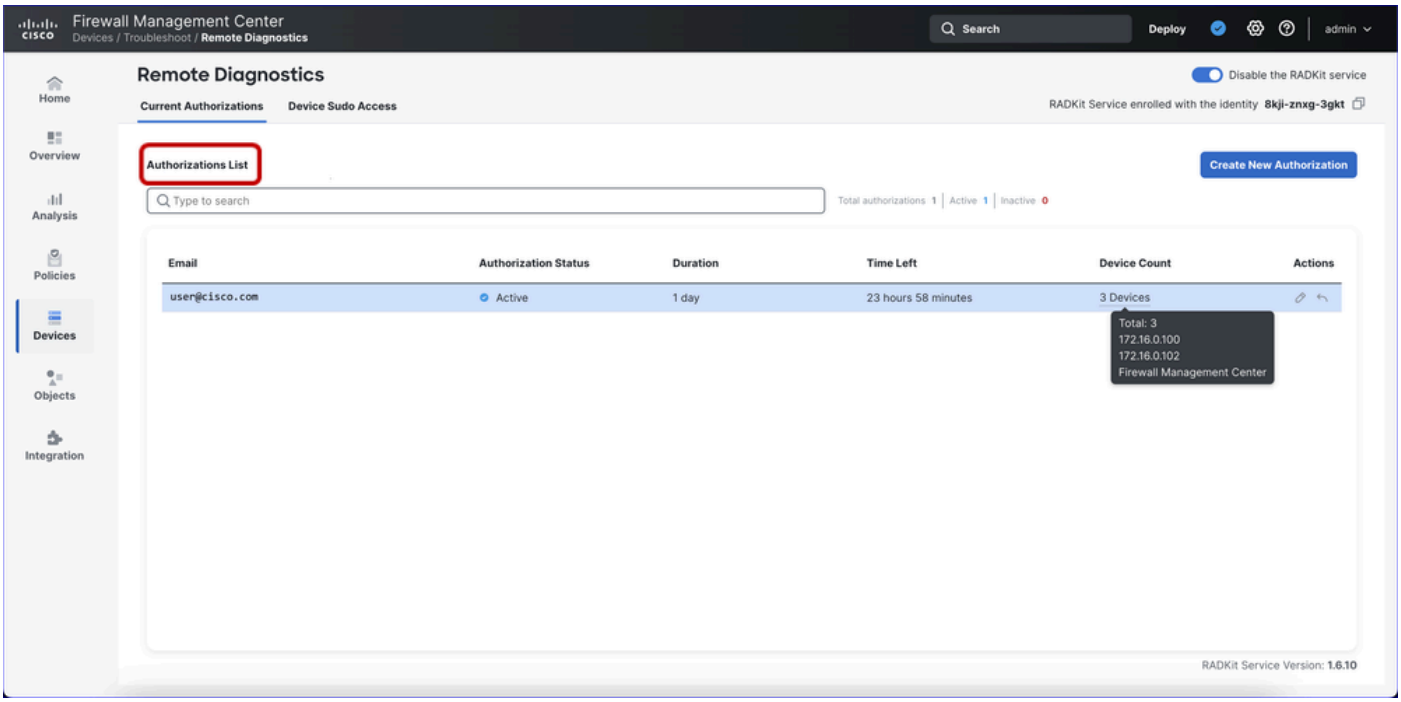
Création d'autorisation terminée

Un écran de confirmation s'affiche une fois la création de l'autorisation terminée :



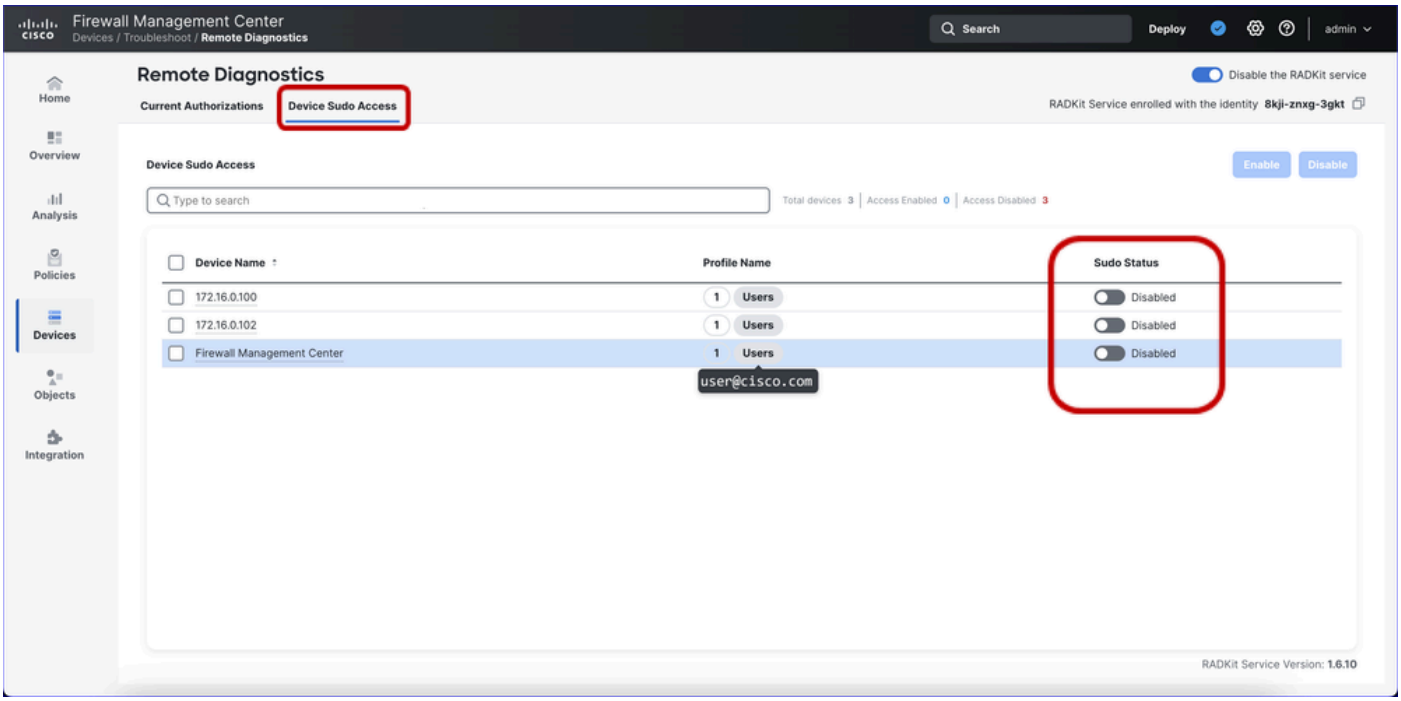
Liste Des Autorisations Actuelles, Y Compris Retrait

- La liste des autorisations actuelles s'affiche dans l'onglet Autorisations actuelles.
- Les actions (colonne d'extrême droite) sont Revoke access et Edit authorization.



Liste d'accès Sudo

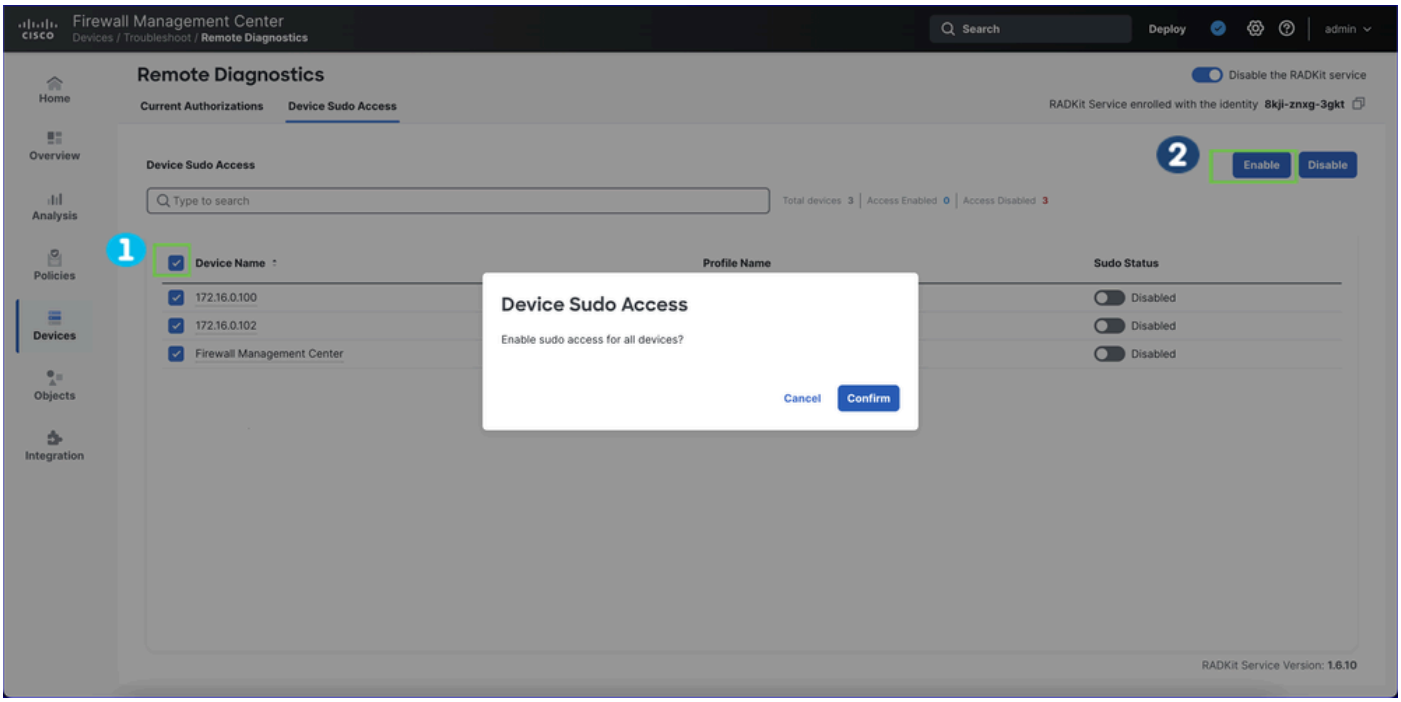
- La liste des périphériques avec des paramètres d'accès sudo est présentée dans l'onglet Device Sudo Access.
- Utilisez la bascule dans la colonne de droite pour activer l'accès sudo. Il est désactivé par défaut.
- En outre, l'accès sudo activé/désactivé en masse est disponible.



Confirmer l'activation de l'accès sudo aux périphériques

1. L'accès sudo peut être activé pour tous ou seulement pour certains périphériques spécifiques en sélectionnant les périphériques puis en cliquant sur le bouton "Activer".

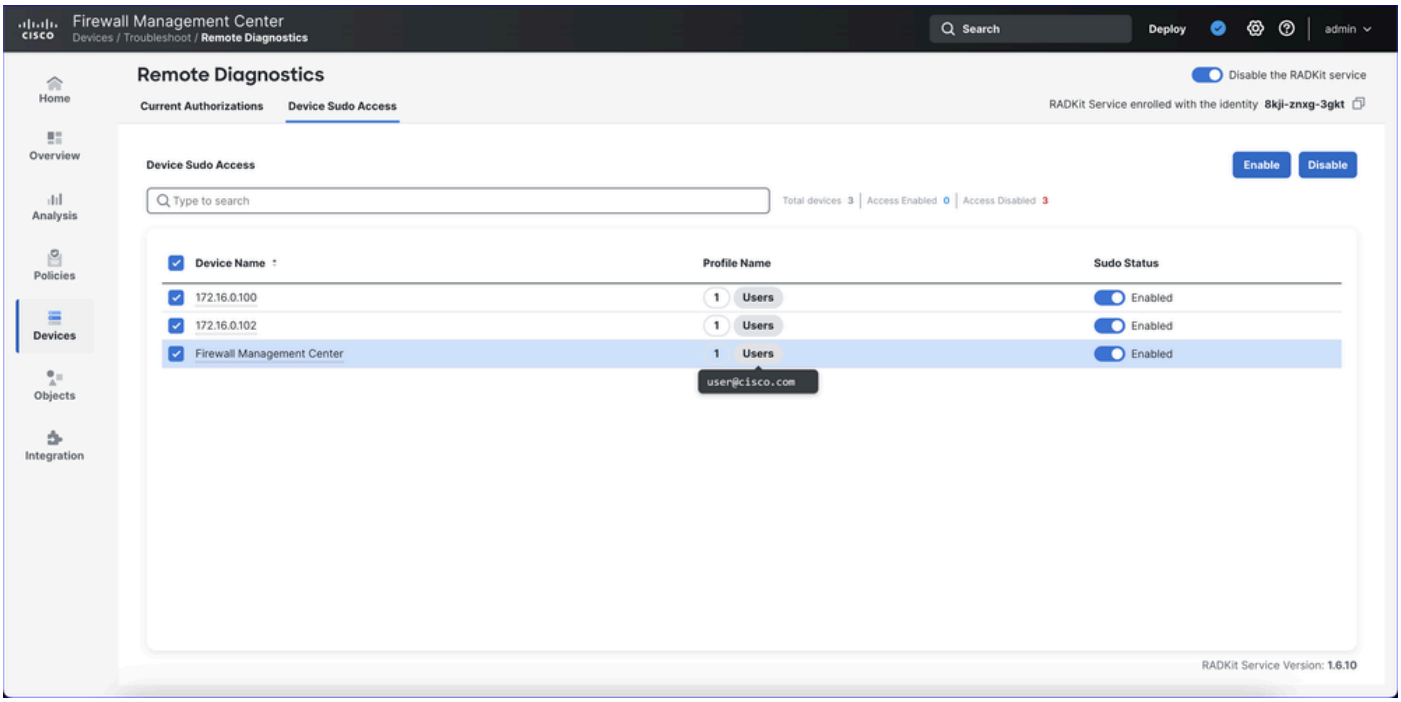
2. Lors de l'activation, une boîte de dialogue de confirmation s'affiche et vous devez cliquer sur Confirmer.



Périphériques Sudo Access activés

- Après avoir activé ou désactivé l'accès sudo pour un périphérique, la colonne État sudo à droite de la page est mise à jour.

- L'ingénieur de support est capable d'exécuter sudo su sur le périphérique ; c'est sans mot de passe. L'ingénieur du support n'a pas besoin d'avoir le mot de passe racine.



Autres remarques

- Seuls les périphériques du domaine auquel l'utilisateur FMC a accès sont visibles et peuvent être autorisés pour un accès à distance.
- Si les FMC sont en haute disponibilité :
  - Le service RADKit ne peut être activé que sur le routeur actif/principal.
  - Le FMC secondaire ne peut pas être ajouté actuellement en tant que périphérique accessible à partir du client RADKit.
- L'autorisation ne peut être accordée que pour un seul ingénieur d'assistance à la fois.
  - Si vous avez besoin de l'accès d'un autre ingénieur de support, créez une autre autorisation pour l'ingénieur supplémentaire. L'ID de service est identique.

API REST FMC

API REST du service RADKit

Pour prendre en charge les opérations de création et de lecture sur le service RADKit, ces nouvelles URL ont été introduites :

- GET : /api/fmc_troubleshoot/v1/domain/{domainUUID}/radkit/services
  - Récupère toutes les données du service RADKit du FMC.
- GET : /api/fmc_troubleshoot/v1/domain/{domainUID}/radkit/services/{id}
  - Récupère/récupère les données du service RADKit à partir de l'ID spécifié.
- POST : /api/fmc_troubleshoot/v1/domain/{domainUUID}/radkit/services
  - Crée le service RADKit sur le FMC (activer/désactiver le service).

Modèle de service RADKit

Le modèle de service RADKit comprend :

- type
- id
- status (état)
- estInscrit
- serviceId
- version


```
{
  "type": "RADKitService",
  "id": "DummyContainerId",
  "status": "RUNNING",
  "isEnrolled": true,
  "serviceId": "8kji-znxg-3gkt",
  "version": "1.6.10"
}
```


Assistance Cisco : Utilisation du client RADKit

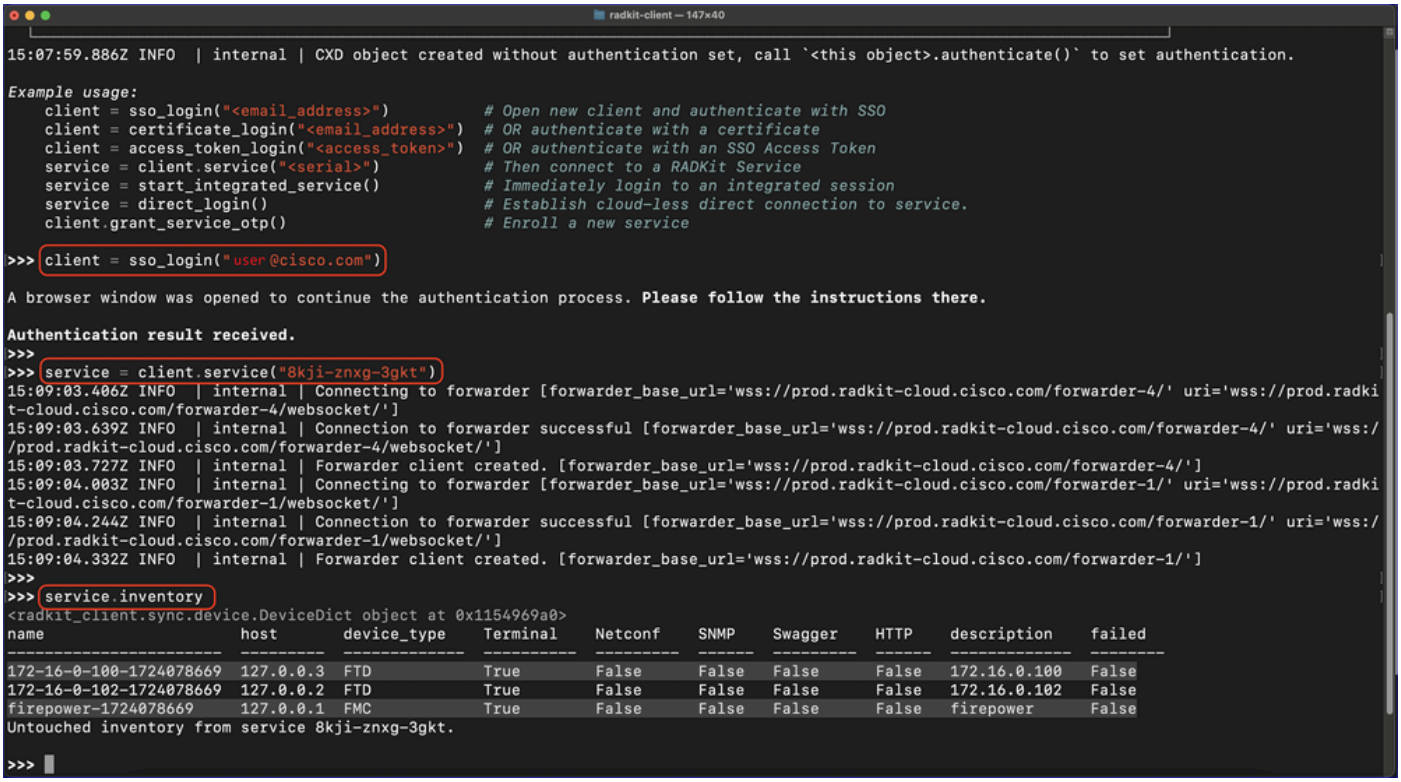
Côté assistance : Installation du client RADKit

- Pour accéder aux FMC/FTD, le client RADKit doit être installé sur le support.
  - Le client fonctionne sur les systèmes d'exploitation Windows, Mac et Linux.
- Le support peut avoir accès à plusieurs périphériques depuis plusieurs utilisateurs. Chaque autorisation RADKit possède son propre « inventaire » de périphériques.
  - Pour chaque inventaire de périphérique utilisateur auquel le support souhaite accéder, l'ID de service RADKit est nécessaire.
  - Pour un inventaire unique, l'accès est possible à la fois pour le FMC et ses FTD gérés à partir du client RADKit, comme spécifié par l'utilisateur lors de l'autorisation d'accès.

Obtention et installation du client RADKit

Le client RADKit peut être installé localement à partir de https://radkit.cisco.com/downloads/release/ puis lancé à partir du terminal avec la commande : radkit-client

Les programmes d'installation sont disponibles pour Windows, MacOS et Linux.



Capture d'écran du client RADKit avec les commandes de connexion (détails sur la section suivante).

Commandes de connexion du client RADKit

- Utilisez l'adresse e-mail saisie par l'utilisateur lors de l'autorisation dans FMC.
- Connexion du client RADKit et connexion aux commandes Service ID spécifiées. L'ID de service RADKit, dans cet exemple 8abc-znxg-3abc, doit correspondre à ce que l'administrateur du pare-feu voit dans FMC.

<#root>

>>>

client = sso_login("user@cisco.com")

A browser window was opened to continue the authentication process.

Please follow the instructions there.

```
Authentication result received.


>>>
service = client.service("8abc-znxg-3abc")


15:09:03.639Z INFO  | internal | Connection to forwarder successful [forwarder_base_url='wss://prod.rad
15:09:03.727Z INFO  | internal | Forwarder client created. [forwarder_base_url='wss://prod.radkit-cloud
15:09:04.244Z INFO  | internal | Connection to forwarder successful [forwarder_base_url='wss://prod.rad
15:09:04.332Z INFO  | internal | Forwarder client created. [forwarder_base_url='wss://prod.radkit-cloud
```

Commande RADKit Client Service Inventory

Commande permettant de répertorier l'inventaire auquel l'utilisateur distant (ingénieur TAC Cisco) est autorisé à accéder :

<#root>

```
>>>
service.inventory


<radkit_client.sync.device.DeviceDict object at 0x1154969a0>
name                      host       device_type    Terminal    Netconf    SNMP    Swagger    HTTP    de
------------------------  ---------  -------------  ----------  ---------  ------  ---------  ------  --
172-16-0-100-1724078669   127.0.0.3  FTD            True        False      False   False      False   17
172-16-0-102-1724078669   127.0.0.2  FTD            True        False      False   False      False   17
firepower-1724078669      127.0.0.1  FMC            True        False      False   False      False   fi
Untouched inventory from service 8kji-znxg-3gkt.
```

Il existe une commande de filtre pour les périphériques de l'inventaire (section suivante). Utilisez le nom dans la colonne de gauche pour démarrer une session interactive avec le périphérique (commande sur la section suivante).

Conseil : Si l'inventaire est obsolète, vous pouvez le mettre à jour à l'aide de la commande : **>>>** service.update_inventory()

Client RADKit : Filtrer les périphériques

Commande de filtrage des périphériques de l'inventaire :

<#root>

```
>>>
ftds = service.inventory.filter(attr='name',pattern='172-16-0’)


>>>
ftds


<radkit_client.sync.device.DeviceDict object at 0x111a93130>
name host device_type Terminal Netconf SNMP Swagger HTTP description failed
---------------------- --------- ------------ ---------- --------- ------ --------- ------ ----------
172-16-0-100-1724078669 127.0.0.3 FTD True False False False False 172.16.0.100 False
172-16-0-102-1724078669 127.0.0.2 FTD True False False False False 172.16.0.102 False
2 device(s) from service 8kji-znxg-3gkt.
```

Commande de session interactive du périphérique client RADKit

Lancement d’une session interactive pour un périphérique (dans ce cas un FMC) avec le nom « firepower-1724078669 » tiré de la commande précédente « service.inventory » :

<#root>

```
>>>
service.inventory["firepower-1724078669"].interactive()


08:56:10.829Z INFO | internal | Starting interactive session (will be closed when detached)
08:56:11.253Z INFO | internal | Session log initialized [filepath='/Users/use/.radkit/session_logs/clie

Attaching to firepower-1724078669 ...
Type: ~. to terminate.
~? for other shortcuts.
When using nested SSH sessions, add an extra ~ per level of nesting.

Warning: all sessions are logged. Never type passwords or other secrets, except at an echo-less passwor


Copyright 2004-2024, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v82.17.0 (build 170)
Cisco Secure Firewall Management Center for VMware v7.7.0 (build 1376)
```

Commandes d'exécution du client RADKit sur les périphériques

Exécutez les commandes sur les périphériques !

<#root>

```
>>>
result = ftds.exec(['show version', 'show interface'])


>>>
>>>
result.status


<RequestStatus.SUCCESS: 'SUCCESS'>

>>>
>>>
result.result['172-16-0-100-1724078669']['show version'].data | print


> show version
-------------------[ firepower ]--------------------
Model : Cisco Secure Firewall Threat Defense for VMware (75) Version 7.7.0 (Build 1376)
UUID : 989b0f82-5e2c-11ef-838b-b695bab41ffa
LSP version : lsp-rel-20240815-1151
VDB version : 392
----------------------------------------------------
```

Obtenir des détails supplémentaires à partir des périphériques

Considérant cet inventaire :

<#root>

```
>>>
service.inventory


[READY] <radkit_client.sync.device.DeviceDict object at 0x192cdb77110>
name                          host      device_type   Terminal   Netconf   SNMP   Swagger   HTTP   desc
----------------------------- --------- ------------ ---------- --------- ------ --------- ------ ----
10-62-184-69-1743156301       127.0.0.4 FTD           True       False     None   False     False  10.6
fmc1700-1-1742391113          127.0.0.1 FMC           True       False     None   False     False  FMC1
ftd3120-3-1743154081          127.0.0.2 FTD           True       False     None   False     False  FTD3
ftd3120-4-1743152281          127.0.0.3 FTD           True       False     None   False     False  FTD3
```

Pour obtenir les détails 'show version' à partir des périphériques FTD :

<#root>

>>>

command = "show version"

>>>

ftds = service.inventory.filter("device_type","FTD").exec(command).wait()

>>>
>>>

 # Print the results

>>>

for key in ftds.result.keys():

...

print(key)

...

ftds.result.get(key).data | print

...

<- Press Enter twice

```
ftd3120-3-1743154081
> show version
-------------------[ FTD3100-3 ]--------------------
Model : Cisco Secure Firewall 3120 Threat Defense (80) Version 7.7.0 (Build 89)
UUID : 123a456a-cccc-bbbb-aaaa-a123456abcde
LSP version : lsp-rel-20250327-1959
VDB version : 404
----------------------------------------------------

>
10-62-184-69-1743156301
> show version
-----------------[ KSEC-FPR1010-10 ]-----------------
Model : Cisco Firepower 1010 Threat Defense (78) Version 7.7.0 (Build 89)
UUID : 123a456a-cccc-bbbb-aaaa-a123456abcde
LSP version : lsp-rel-20250327-1959
VDB version : 404
----------------------------------------------------

>
ftd3120-4-1743152281
> show version
-------------------[ FTD3100-4 ]--------------------
Model : Cisco Secure Firewall 3120 Threat Defense (80) Version 7.7.0 (Build 89)
UUID : 123a456a-cccc-bbbb-aaaa-a123456abcde
LSP version : lsp-rel-20250327-1959
VDB version : 404
```

```
-------------------------------------------------

>
```

Autre approche :

<#root>

```
>>> # Get the FTDs. This returns a DeviceDict object:
...
ftds = service.inventory.filter("device_type","FTD")


>>> # Access the dictionary of devices from the _async_object attribute
...
devices_obj = ftds.__dict__['_async_object']


>>> # Extract the 'name' from each AsyncDevice object
...
names = [device.name() for device in devices_obj.values()]


>>> # Get the 'show version' output from all FTD devices:
...
command = "show version"

...
show_ver_ftds = []

...
for name in names:

...
ftd = service.inventory[name]

...
req = ftd.exec(command)

...
req.wait(30)
 # depending on the number of devices you might need to increase the timeout value
...
show_ver_ftds.append(req.result.data)
```

```
>>> # Print the inventory device name + 'show version' output from each device:
...
for name, show_version in zip(names, show_ver_ftds):


...
print(f"Inventory name: {name}")


...
print(show_version[2:-2]) # Remove the leading '> ' and trailing ' \n>'


...
print("\n")


Inventory name: ftd3120-3-1743154081
show version
-------------------[ FTD3100-3 ]--------------------
Model : Cisco Secure Firewall 3120 Threat Defense (80) Version 7.7.0 (Build 89)
UUID : 123a456a-cccc-bbbb-aaaa-a123456abcde
LSP version : lsp-rel-20250327-1959
VDB version : 404
----------------------------------------------------


Inventory name: ftd3120-4-1743152281
show version
-------------------[ FTD3100-4 ]--------------------
Model : Cisco Secure Firewall 3120 Threat Defense (80) Version 7.7.0 (Build 89)
UUID : 123a456a-cccc-bbbb-aaaa-a123456abcde
LSP version : lsp-rel-20250327-1959
VDB version : 404
----------------------------------------------------


Inventory name: 10-62-184-69-1743156301
show version
----------------[ KSEC-FPR1010-10 ]-----------------
Model : Cisco Firepower 1010 Threat Defense (78) Version 7.7.0 (Build 89)
UUID : 123a456a-cccc-bbbb-aaaa-a123456abcde
LSP version : lsp-rel-20250327-1959
VDB version : 404
----------------------------------------------------
```

Obtention de fichiers à partir de périphériques

- Par le biais du client RADKit, un ingénieur du centre d'assistance technique Cisco peut envoyer des messages SSH aux périphériques et effectuer diverses opérations, notamment la génération de fichiers de dépannage.

Assistance Cisco : Console RADKit

Utilisation de la console réseau RADKit

- Au lieu d'utiliser le client RADKit, un ingénieur de support TAC Cisco peut utiliser la console réseau RADKit. La console réseau fait partie du client RADKit.
- La console réseau RADKit est une fonctionnalité qui fournit une interface de ligne de commande (CLI) simple pour les fonctions de base du client RADKit. Il est destiné à être utilisé pour une connectivité rapide à une instance de service RADKit, l'établissement de sessions interactives et le téléchargement/chargement de fichiers sans tracas et avec une formation minimale.
- Démarrez la console réseau à l'aide de la ligne de commande : radkit-network-console
- Consultez la documentation de RADKit pour plus de détails.

Mises à niveau et rétrocompatibilité

Mise à niveau vers 7.7 et à partir de 7.7

- Le service RADKit a été ajouté à Secure Firewall 7.7.0.
    - Les périphériques mis à niveau vers la version 7.7.0+ disposent de la configuration requise pour le service RADKit.

Expérience avec les FTD non pris en charge

- Les FMC et les FTD doivent disposer de la version 7.7.0 minimum pour que cette fonctionnalité fonctionne (les FTD dont la version est antérieure à 7.7 ne peuvent pas être ajoutés à une autorisation FMC RADKit 7.7).
- Les FTD enregistrés qui ne figurent pas sur la version 7.7.0 ne sont pas disponibles pour le prélèvement en vue de l'activation de l'autorisation.

Dépannage

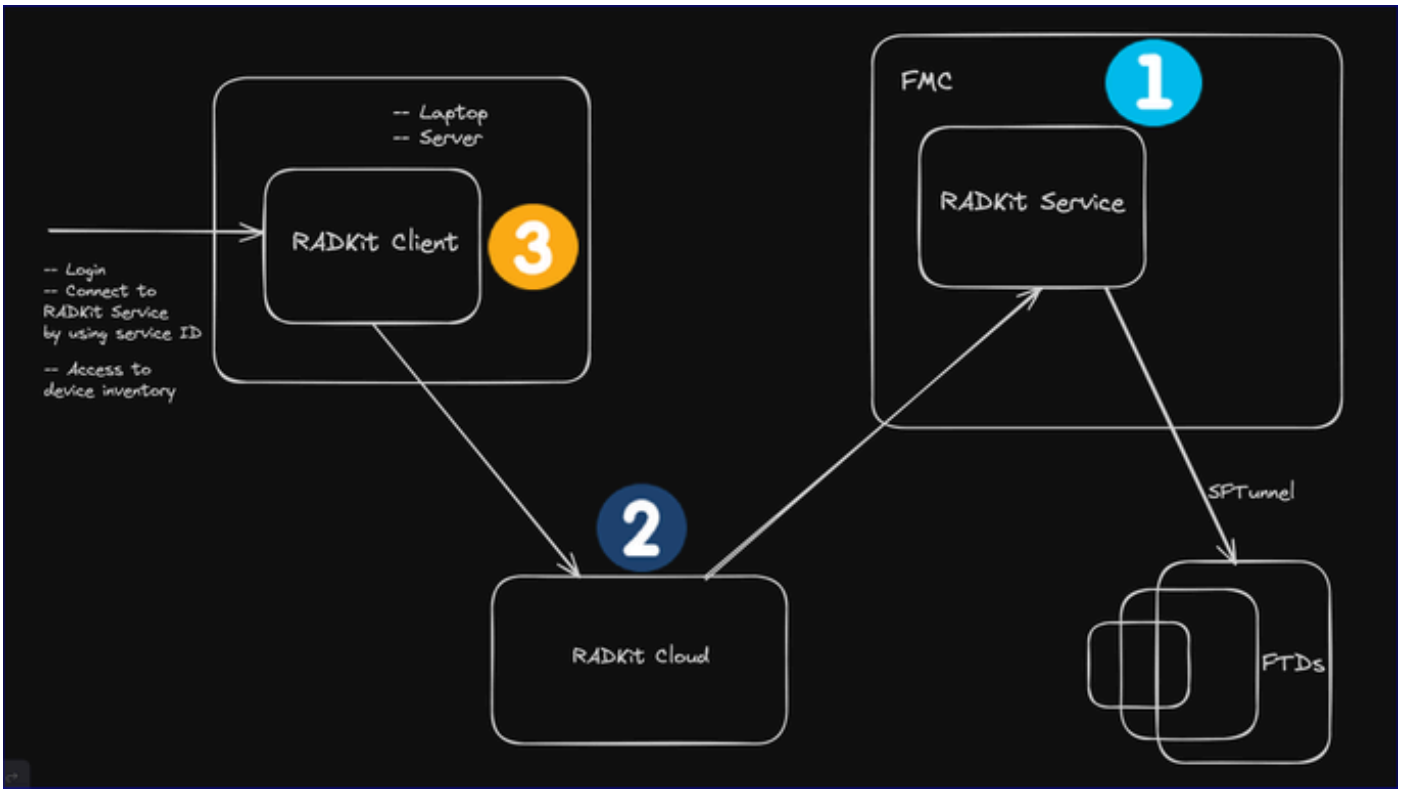
Présentation des diagnostics

Points de dépannage

1. Utilisez les outils de développement de navigateur et les journaux FMC pour voir ce qui se passe dans FMC.

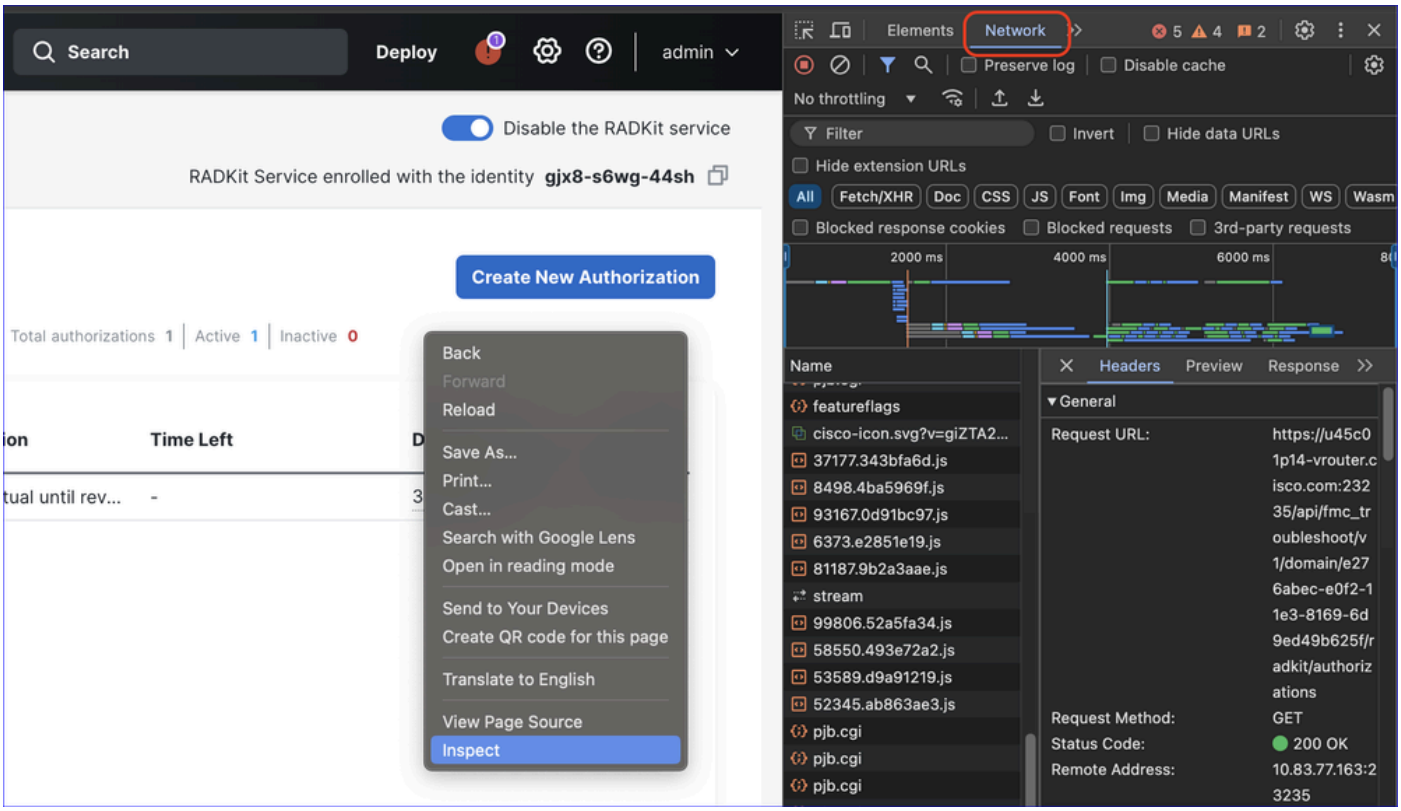
2. Pour les problèmes de communication entre le service RADKit sur FMC, le cloud RADkit et le client RADKit, consultez la journalisation du client RADKit.

3. Client RADKit.



Procédure de dépannage : Outils de développement du navigateur

- L'onglet Developer Tools, Network du navigateur affiche les appels d'API qui ont été exécutés sur la page, ceci peut être utilisé lors du dépannage de problèmes sur FMC. Vous pouvez le lancer en cliquant avec le bouton droit sur la page, puis en cliquant sur Inspecter.
- Vérifiez le code d'état de l'appel API et l'aperçu de la réponse dans l'onglet Réseau.



API intermédiaires RADKit Service Go

Go Middleware pour l'intégration RADKit utilise des appels d'API qui ne sont pas disponibles publiquement via l'explorateur d'API FMC. Le journal Go Middleware API est disponible à l'adresse /var/log/auth-daemon.log. Fonctionnalités de Go Middleware :

- Inscrivez le service RADKit dans le cloud RADKit avec le processus d'authentification unique.
- Récupère la liste de toutes les autorisations d'utilisateurs RADKit distants et des périphériques associés.
- Récupérer une autorisation d'utilisateur RADKit à distance spécifique et les périphériques associés en utilisant un e-mail.
- Créer une autorisation utilisateur RADKit distante et accorder des autorisations d'accès aux périphériques (tous les périphériques ou une liste de périphériques sélectionnés) pour une période spécifiée.
- Modifier une autorisation utilisateur RADKit distante.
- Supprimer une autorisation utilisateur RADKit distante.

Journaux de dépannage du service RADKit

- Journaux FMC généraux : pigtail à partir d'une session FMC ssh.
- Accédez aux API middleware : /var/log/auth-daemon.log
- Journaux contenant les données des processus RADKit et auth-daemon :

/var/log/process_stdout.log

/var/log/process_stderr.log

Tous ces journaux sont inclus dans les dépannages FMC/FTD.

- Journaux de service RADKit internes : /var/lib/radkit/logs/service/
- Journaux des opérations effectuées à partir du client RADKit sur les périphériques (FMC et FTD) : /var/lib/radkit/session_logs/service

Journaux à envoyer au TAC Cisco

- Captures d'écran des erreurs.
- Description du problème.
- Étapes à reproduire.
- Pigtail et /var/log/auth-daemon.log extraient les journaux contenant les erreurs.

Contrôle des accès

La consignation des personnes auxquelles l’accès a été accordé pendant combien de temps et des personnes auxquelles il a été accordé se trouve dans les journaux d’audit de FMC.

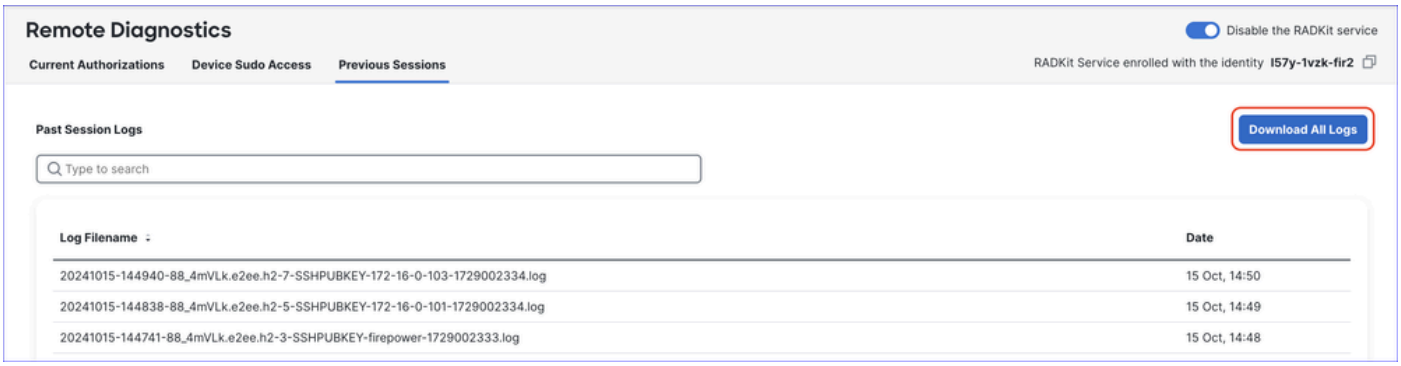
Journaux de session RADKit

Les journaux de session RADKit pour les opérations effectuées à partir du client RADKit sur les périphériques (FMC et FTD) sont présents sur FMC à l'adresse /var/lib/radkit/session_logs/service :

- Les journaux proviennent du service RADKit.
- Ces journaux sont inclus dans une offre de dépannage.
- Les journaux sont également accessibles depuis l'interface utilisateur (voir la section suivante).
- Il existe plusieurs fichiers journaux de session ; une par session.

Journaux des sessions précédentes RADKit

Les journaux des sessions RADKit pour les opérations de périphérique effectuées à partir du client RADKit sont disponibles pour téléchargement sous forme d'archive contenant tous les journaux dans l'onglet Sessions précédentes en cliquant sur le bouton « Download All Logs ».



Exemple de problème avec la procédure pas à pas de dépannage

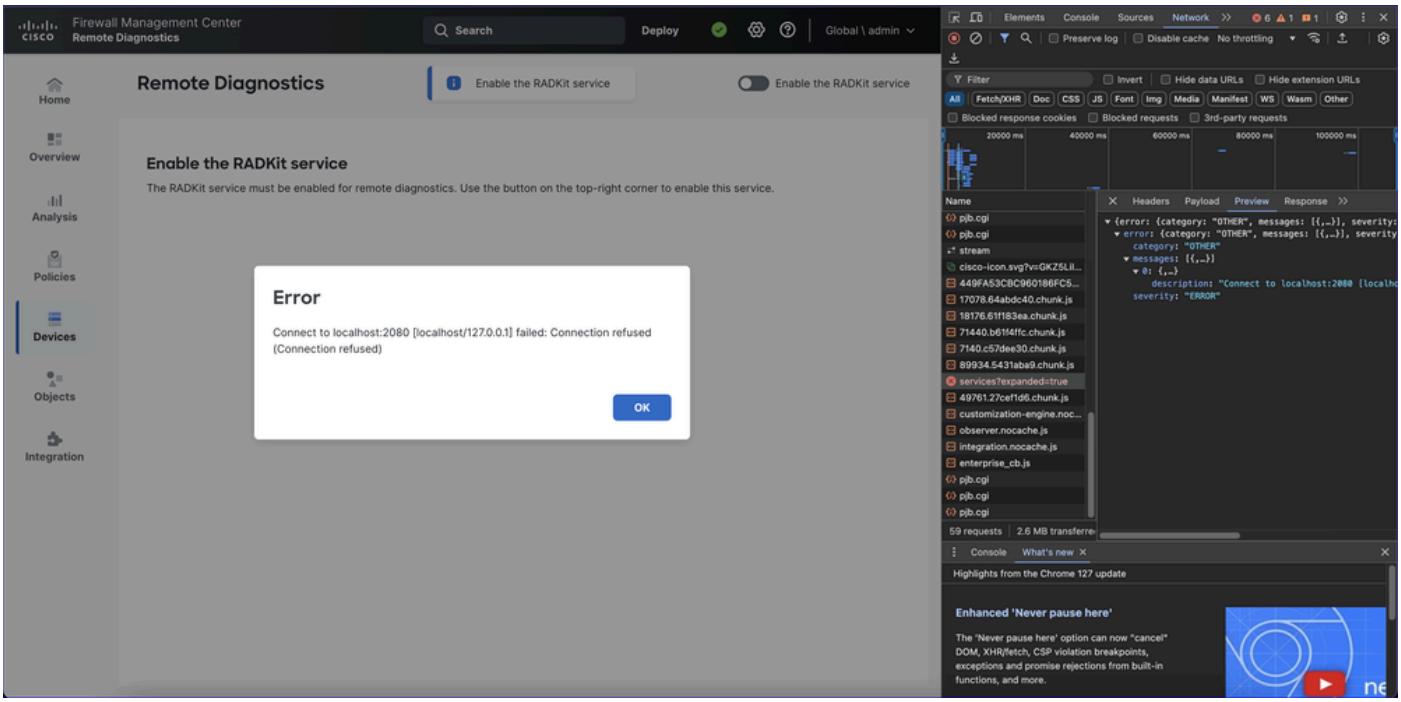
Exemple de dépannage

En cas d'erreur du type « Échec de la connexion à localhost : 2080 [localhost/127.0.0.1] : Connexion refusée (Connexion refusée) », essayez de redémarrer le démon auth à partir d'une session FMC SSH :

<#root>

root@firepower:~$

sudo pmtool restartbyid auth-daemon



Télémétrie

La sortie de télémétrie a été ajoutée pour cette fonctionnalité :

```
"remoteDiagnostics" : {
   "isRemoteDiagnosticsEnabled": 0 // 0 = false , 1 = true
}
```

Forum aux questions

FAQ: Connexion et inscription

Q. L'inscription fonctionne-t-elle avec un proxy si FMC n'a pas d'accès direct à Internet ?

R. Oui, si le proxy a accès à prod.radkit-cloud.cisco.com qui est utilisé pour le processus d'inscription.

Q. Un utilisateur peut-il utiliser son propre IDp pour ce service ?

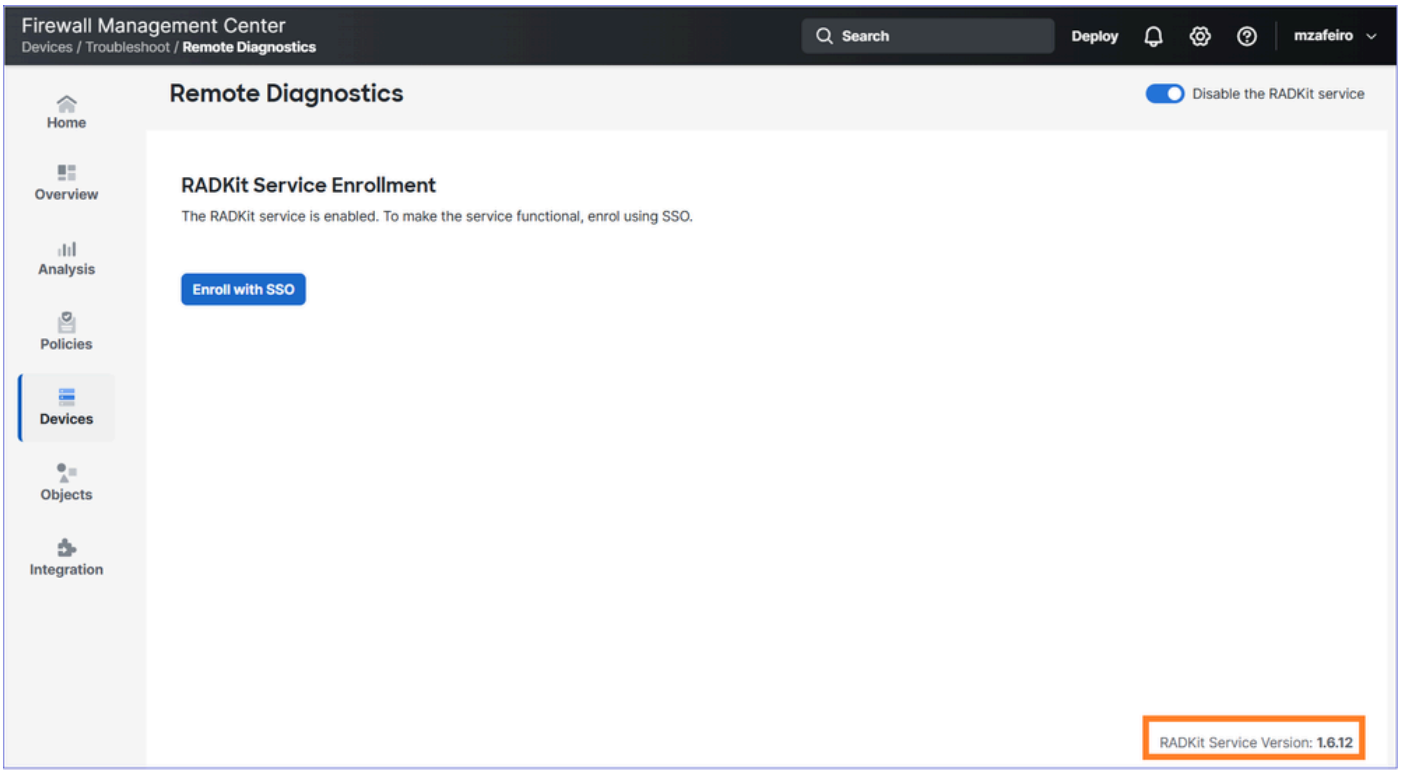
R. Seul Cisco SSO est accepté sur le cloud RADKit. Il est possible d'associer votre compte d'entreprise à un compte Cisco, afin que l'inscription au service RADKit soit possible avec un e-mail non Cisco.

FAQ: Versions RADKit

Q. Quelle version de RADkit est incluse dans FMC dans la version 7.7 ? Comment savoir quelle version de RADKit est incluse dans FMC ? Est-ce quelque chose qui peut être mis à jour sans mise à niveau FMC ?

A.

- La version de RADKit fournie avec 7.7.0 est 1.6.12.
- La version du service RADKit s'affiche au bas de la page Diagnostics à distance FMC : "Version du service RADKit : 1.6.12."



- RADKit est fourni avec les correctifs/packages de mise à niveau FMC. La mise à niveau du service RADKit dans FMC séparément n'est pas prise en charge.

FAQ: Other (autre)

Q. Les périphériques externes non gérés par le FMC peuvent-ils être inclus ?

R. Seuls les périphériques gérés par le FMC peuvent être ajoutés à l'inventaire RADKit, puis peuvent être accessibles via une autorisation.

Q. La configuration RADKit est-elle sauvegardée dans le cadre de la sauvegarde FMC ?

A.

- La configuration n'est pas sauvegardée dans le cadre de la sauvegarde FMC.
- Il n'est pas sauvegardé car nous prévoyons que, généralement, l'accès permanent ne sera

pas fourni ; l'accès est généralement limité dans le temps.

Références

Liens utiles:

- Guide de configuration FMC - RADKit
- https://radkit.cisco.com/
- https://radkit.cisco.com/docs/index.html
- https://radkit.cisco.com/downloads/release/
- https://github.com/Cisco-RADKit/Intro

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.