Configurar a integração do Cisco RADKit no FMC

Contents

- Introdução
  - Background
  - Descrição do recurso e passo a passo
  - APIs REST do FMC
  - Obtenha detalhes adicionais dos dispositivos
  - Suporte da Cisco: Console RADKit
  - Atualizações e compatibilidade com versões anteriores
- Troubleshooting
  - Visão Geral do Diagnóstico
  - Logs de sessão RADKit
  - Exemplo de problema com Troubleshooting de Passo a Passo
  - Telemetria
- FAQ

Introdução

Este documento descreve o recurso Integração do Cisco RAIDit no FMC adicionado na versão 7.7.

Background

Problemas enfrentados pelos administradores do firewall

- O Remote Automation Development Kit (RADKit), desenvolvido pela Cisco, é um orquestrador em toda a rede projetado para fornecer aos usuários a possibilidade de acessar de maneira segura e solucionar problemas de dispositivos de rede. https://radkit.cisco.com/
- O Cisco Secure Firewall Management Center (FMC) gerencia e opera dispositivos Secure Firewall Threat Defense (FTD). Um único FMC pode gerenciar vários dispositivos em vários locais.
- Embora os utilizadores possam instalá-lo separadamente e integrar os seus CVP e DTF no CVP, a criação do serviço RADKit no CVP e a integração do(s) CVP e de todos os dispositivos geridos (DTF) de forma automatizada constituiria uma melhor experiência para os utilizadores finais.

Caso de uso

Alguns dos principais recursos dos quais os usuários podem se beneficiar após a integração do RADKit no FMC incluem:

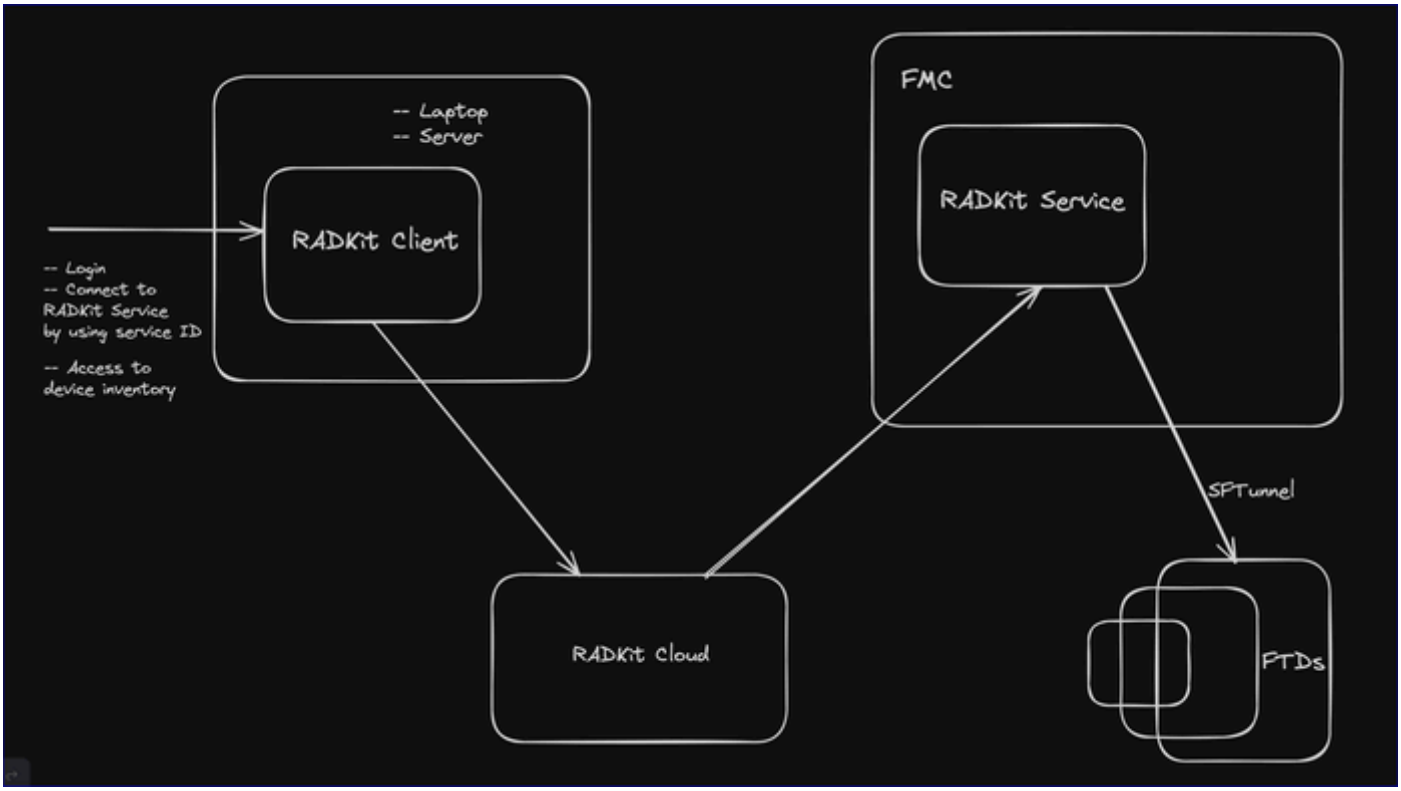
- Capacidade de acessar os FMCs/FTDs remotamente da CLI do cliente RADKit.
- Capacidade de fornecer acesso controlado aos FMCs/FTDs a qualquer pessoa que precise deles (por exemplo, um engenheiro do Cisco TAC).
- Aproveite os recursos de automação para coletar dados e diagnosticar problemas do cliente RADKit (os scripts que executam comandos em vários dispositivos podem ser criados e usados a partir do cliente RADKit).

O que há de novo - Solução

- A partir do Secure Firewall 7.7.0, o serviço Remote Automation Development Kit (RADKit) é integrado ao FMC.
- Os usuários podem ativar ou desativar o serviço RADKit sob demanda, inscrevê-lo na nuvem RADKit e criar autorizações de usuários remotos para acessar dispositivos específicos do cliente RADKit por uma duração de acesso programada.
    - É possível editar ou revogar autorizações.
- Há também uma opção para fornecer acesso sudo a dispositivos para solução de problemas avançada.

Integração de serviço RADKit no diagrama FMC

Este diagrama mostra como o RADKit permite a comunicação do cliente RADKit do usuário (engenheiro do TAC) com os dispositivos FTD de produção:



Conceitos básicos: Plataformas suportadas, licenciamento

Aplicativos e gerentes

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		

Outros aspectos do suporte

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

Dependências para o recurso operar

- A versão mínima é o Secure Firewall 7.7.0.
- Para se conectar ao serviço RADKit hospedado no FMC, o cliente RADKit precisa ser instalado de https://radkit.cisco.com/downloads/release/ no computador do engenheiro de suporte.
- A versão preferida para o cliente RADKit é a 1.6.10 ou posterior.
- Versões mais antigas do RADKit Client poderiam ser usadas porque o RADKit Service é compatível com versões mais antigas do RADKit Client.

Descrição do recurso e passo a passo

Visão geral do recurso

- A integração do Serviço RADKit no FMC permite que os administradores de dispositivos forneçam aos usuários remotos (engenheiros do Cisco TAC) acesso a dispositivos FMC e FTD específicos em sua rede para fins de solução de problemas e automação. RADKé muito mais eficiente para a solução de problemas do que o compartilhamento de tela, não exige o controle do computador do usuário, é uma maneira mais segura de trabalhar em uma rede e complementa bem o Webex.
- Isso melhora a experiência do suporte técnico, pois os administradores de dispositivos não precisam instalar e configurar o serviço RADKit separadamente. Além disso, isso reduz o tempo de suporte para os engenheiros do Cisco TAC resolverem problemas de suporte.

Configuration Steps: Overview

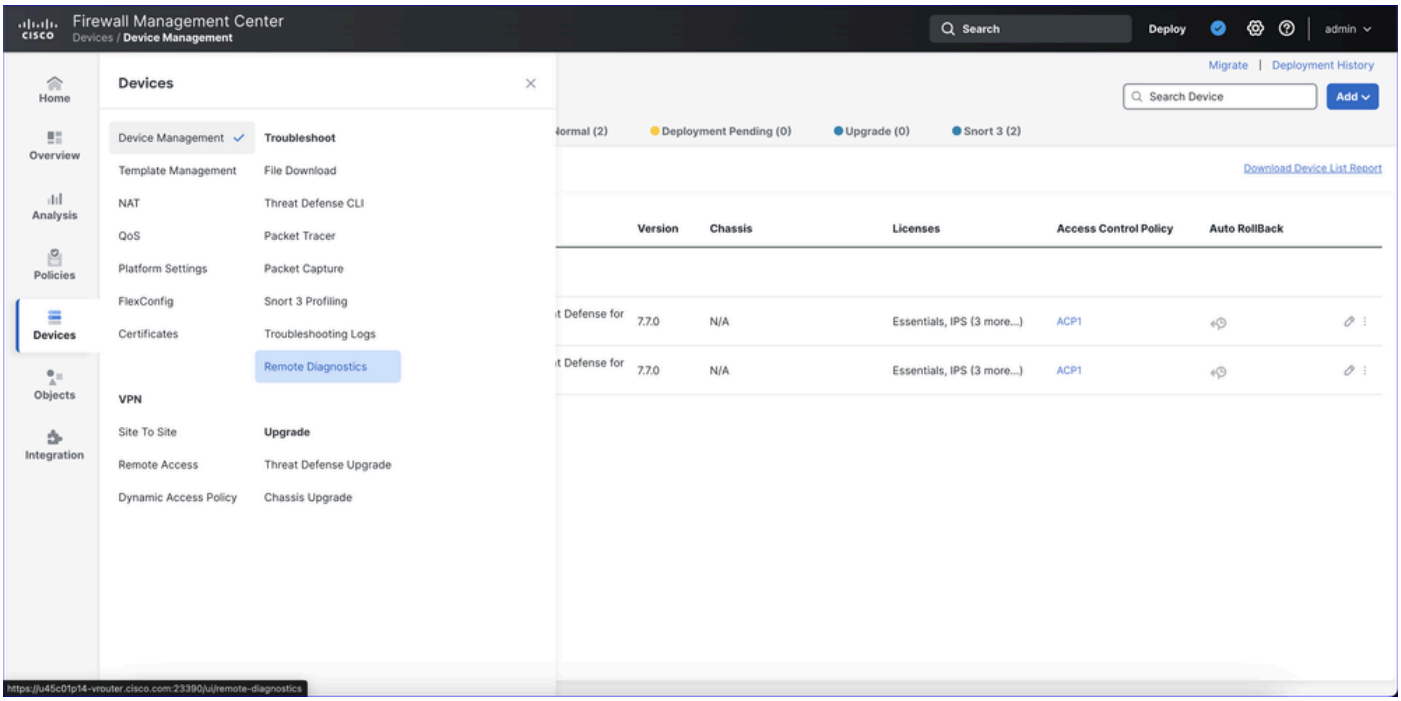
1. Administrador do dispositivo (utilizador administrador do CVP): Habilite e registre o serviço RADKit e configure autorizações na GUI do FMC.

2. Cisco TAC/Suporte da Cisco: Instale o RADKit Client no computador, acesse e solucione problemas dos dispositivos do RADKit Client.

Usuário administrador do FMC: Passo a passo do Firewall Management Center

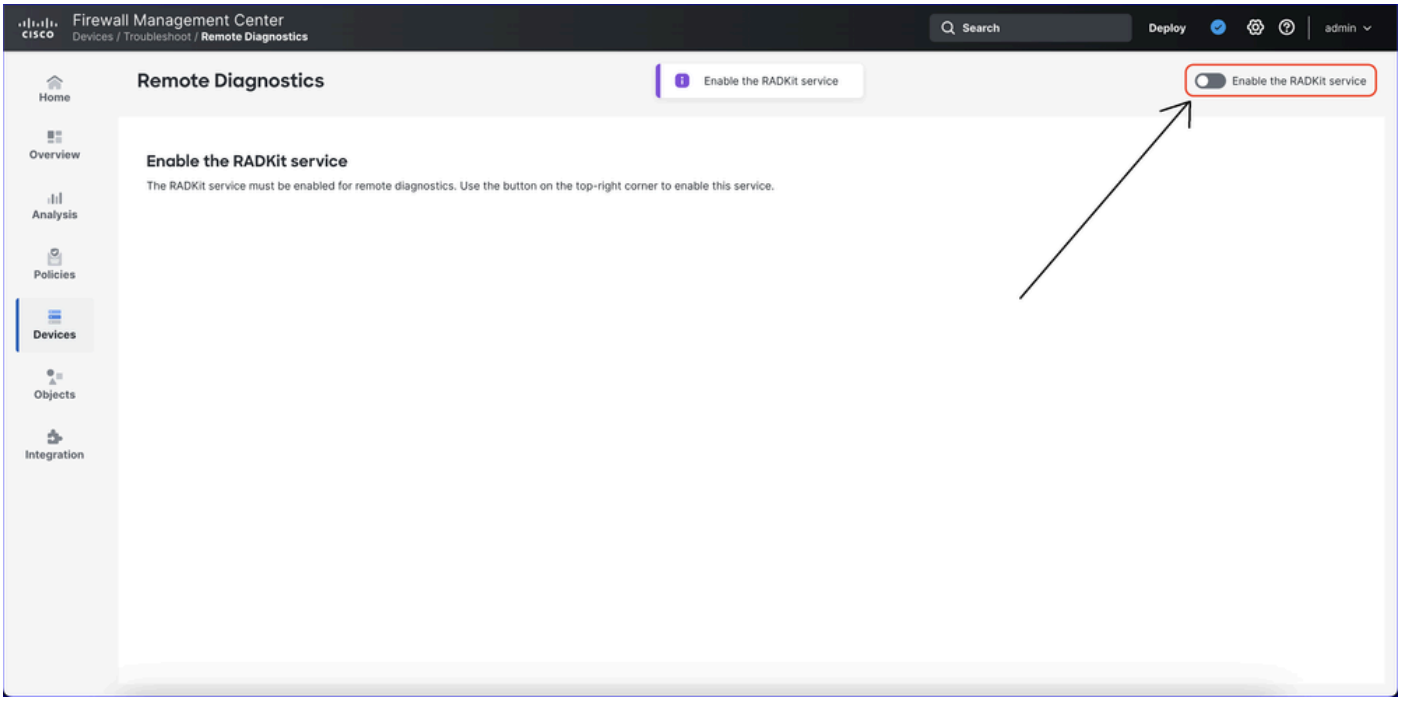
Menu de Diagnóstico Remoto

- Um novo item de menu "Diagnóstico remoto" foi adicionado para este recurso em Dispositivos -> Solução de problemas.
- Os usuários Administrador, Administrador de rede e Manutenção têm permissões de leitura/gravação na página.
- Os usuários Analista de segurança, Analista de segurança (somente leitura) e Aprovador de segurança têm permissões somente leitura para a página.



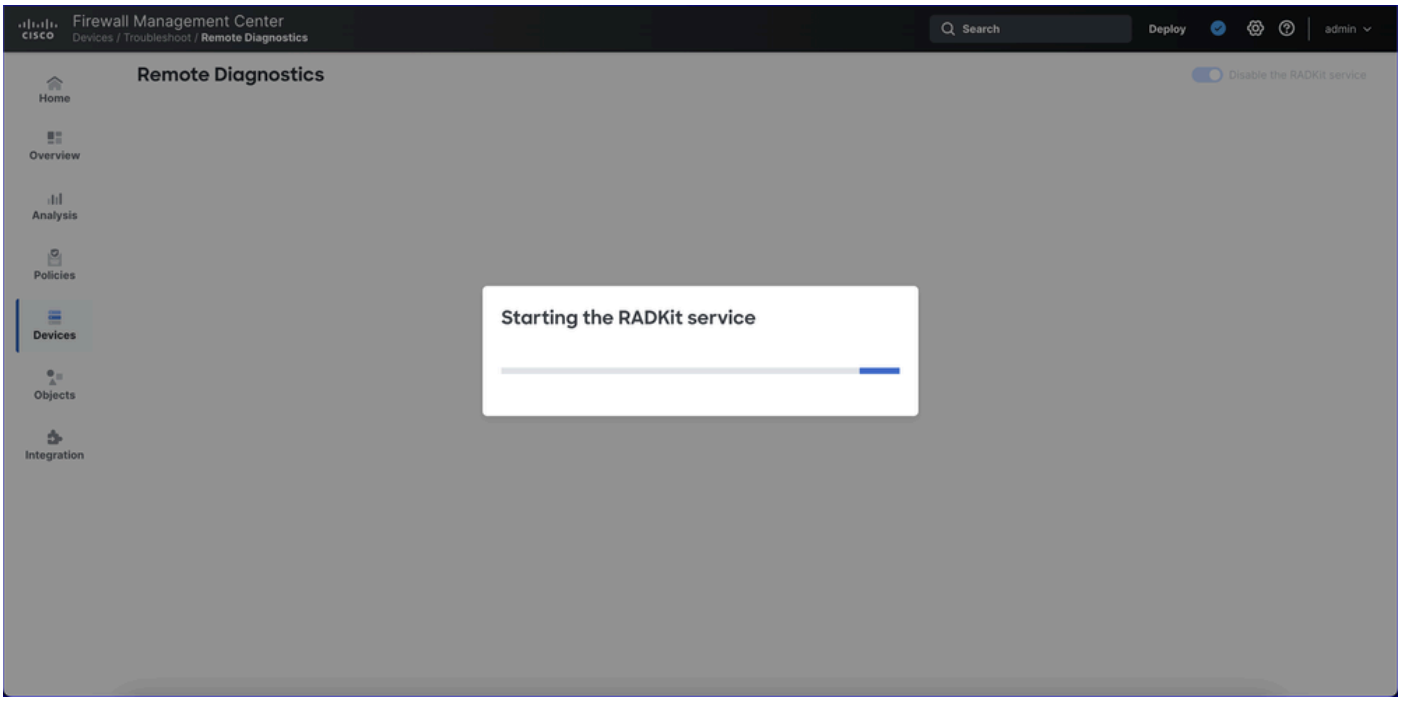
Página Diagnóstico remoto inicial

Esta é a página inicial do Remote Diagnostics. O serviço RADKit pode ser ativado alternando o switch "Enable the RADKit service":



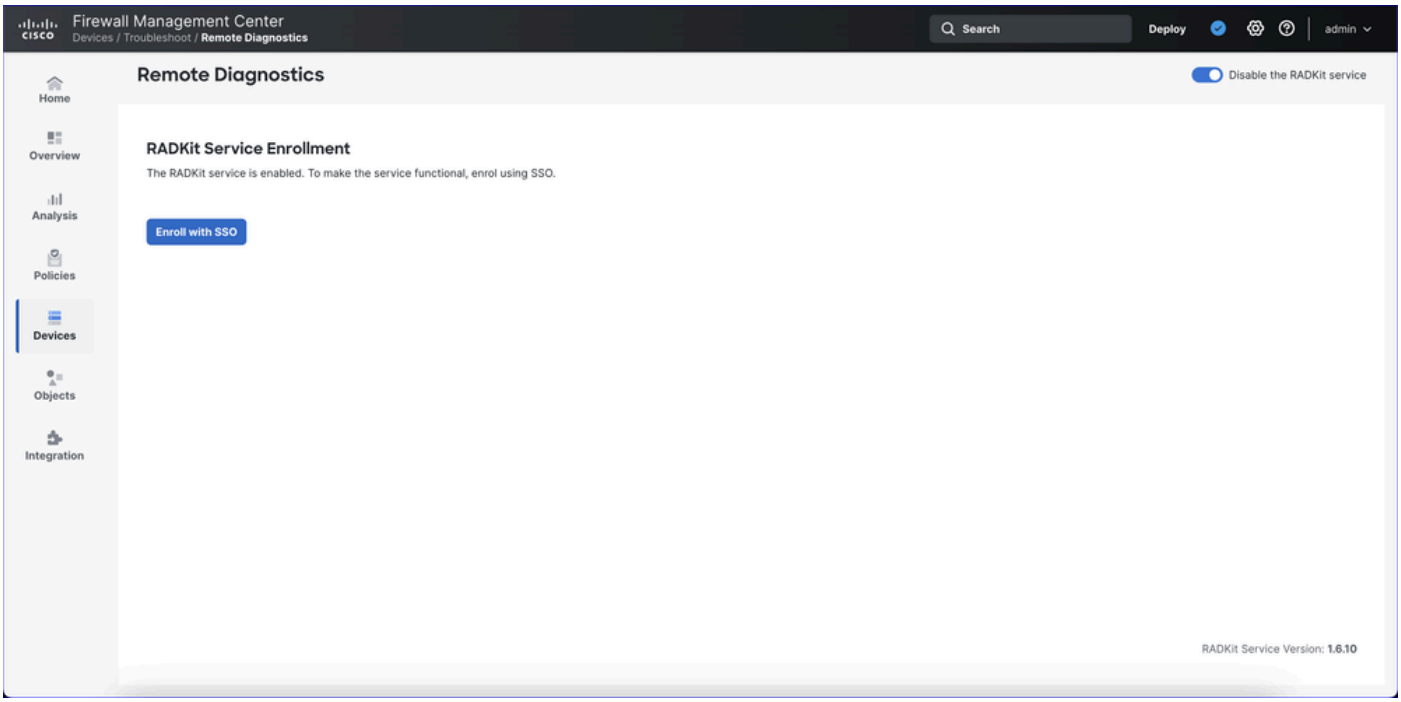
Serviço RADKit iniciando

Depois de ativar o serviço RADKit, uma barra de progresso é exibida até que o serviço RADKit seja iniciado:



Serviço RADKit habilitado

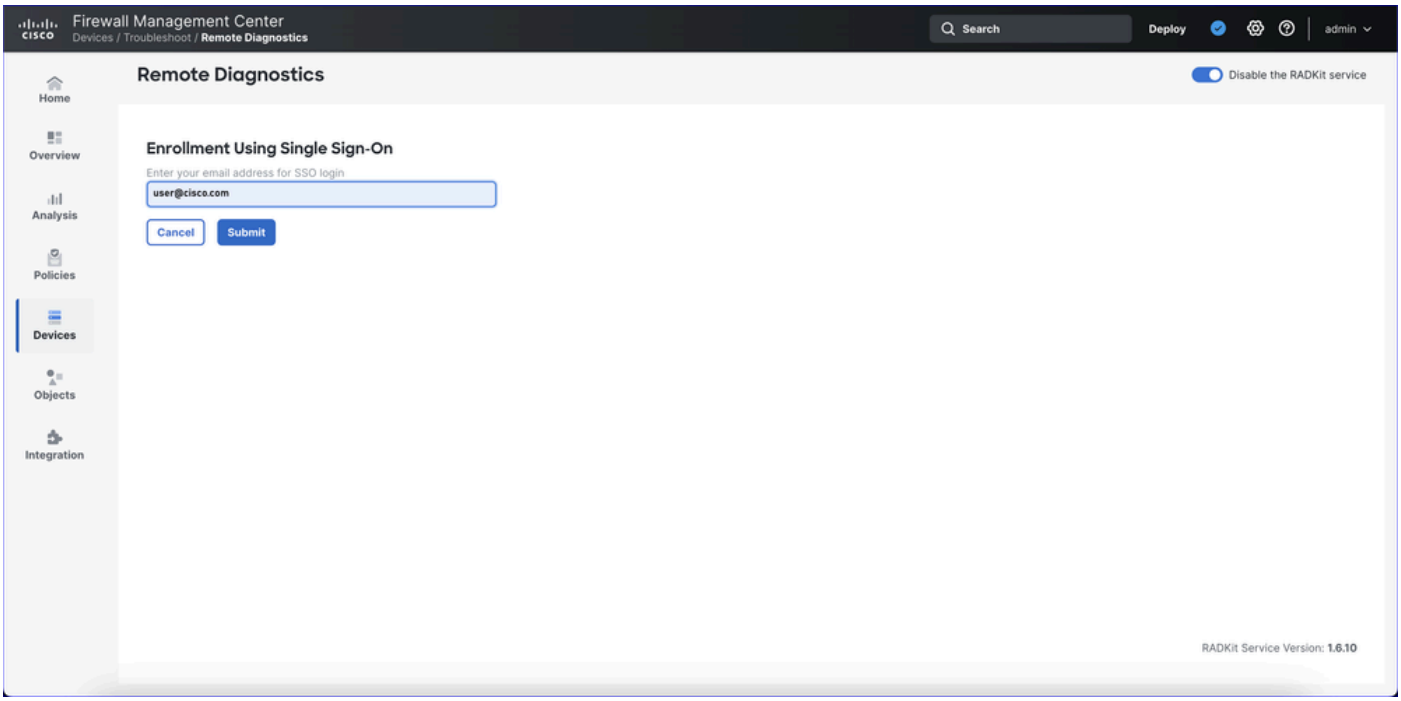
- Quando o processo de ativação do serviço RADKit estiver concluído, esta página será mostrada:



A próxima etapa é a inscrição na nuvem RADKit clicando no botão "Inscrever-se com SSO".

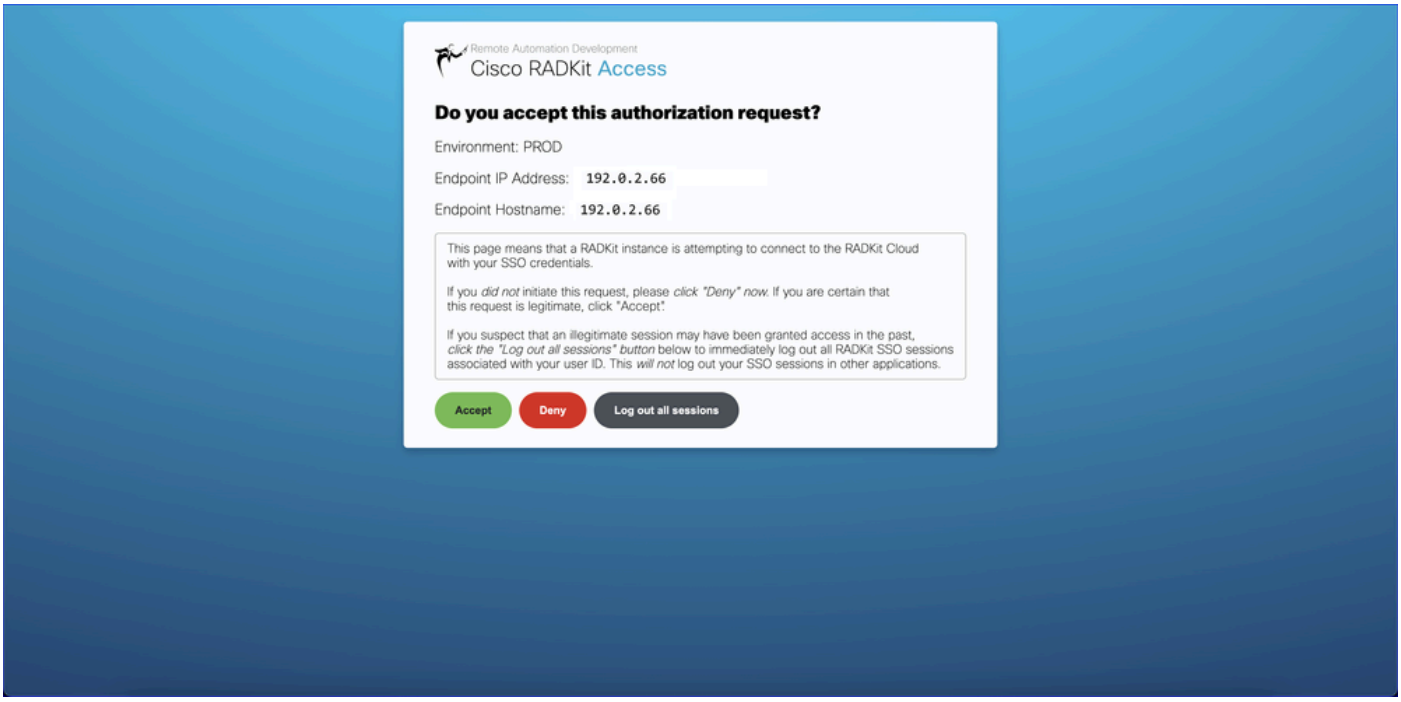
Inscreva-se no SSO - Insira o endereço de e-mail

A etapa 1 do processo de inscrição consiste em inserir o endereço de e-mail do usuário para a inscrição em nuvem do RADKit:



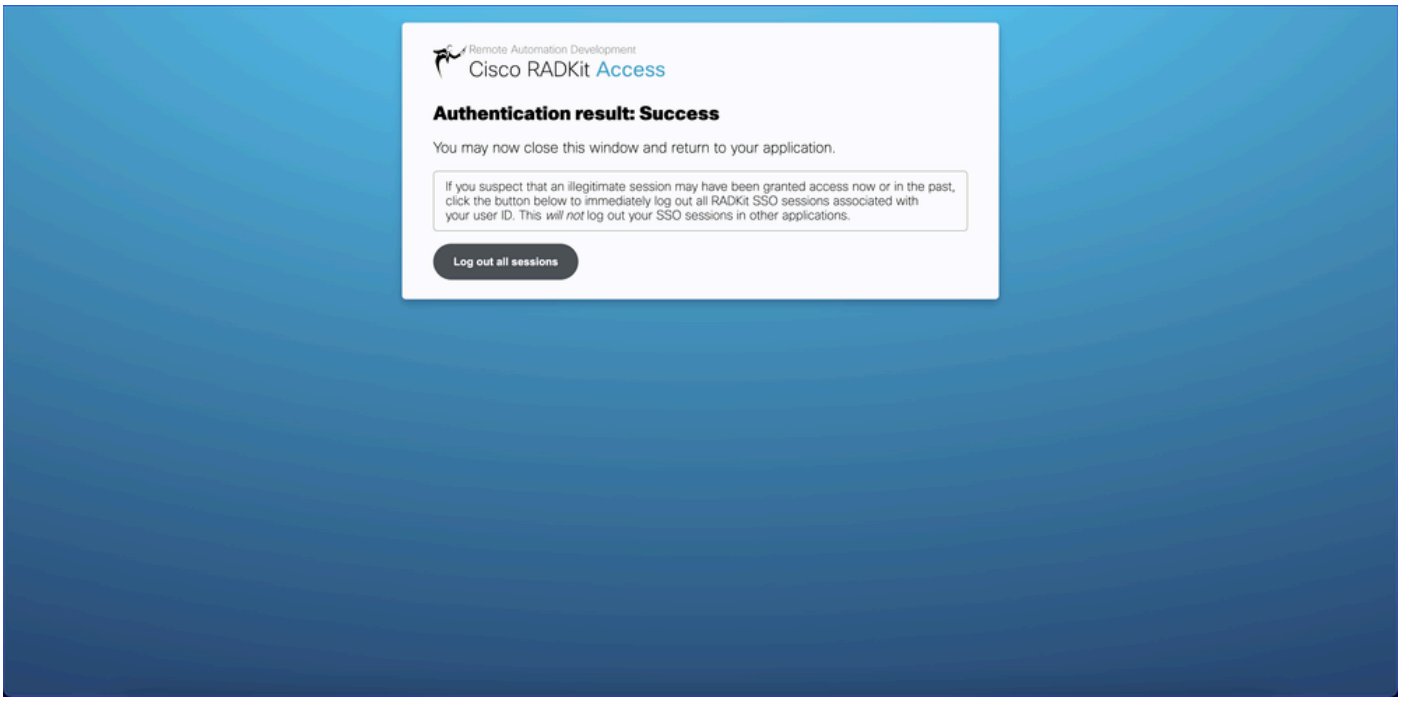
Inscreva-se no SSO - Aceite a solicitação de autorização

Uma nova guia do navegador (ou janela, dependendo das configurações do navegador) é aberta. Clique no botão Aceitar.



Inscreva-se no SSO - Autenticação Bem-sucedida

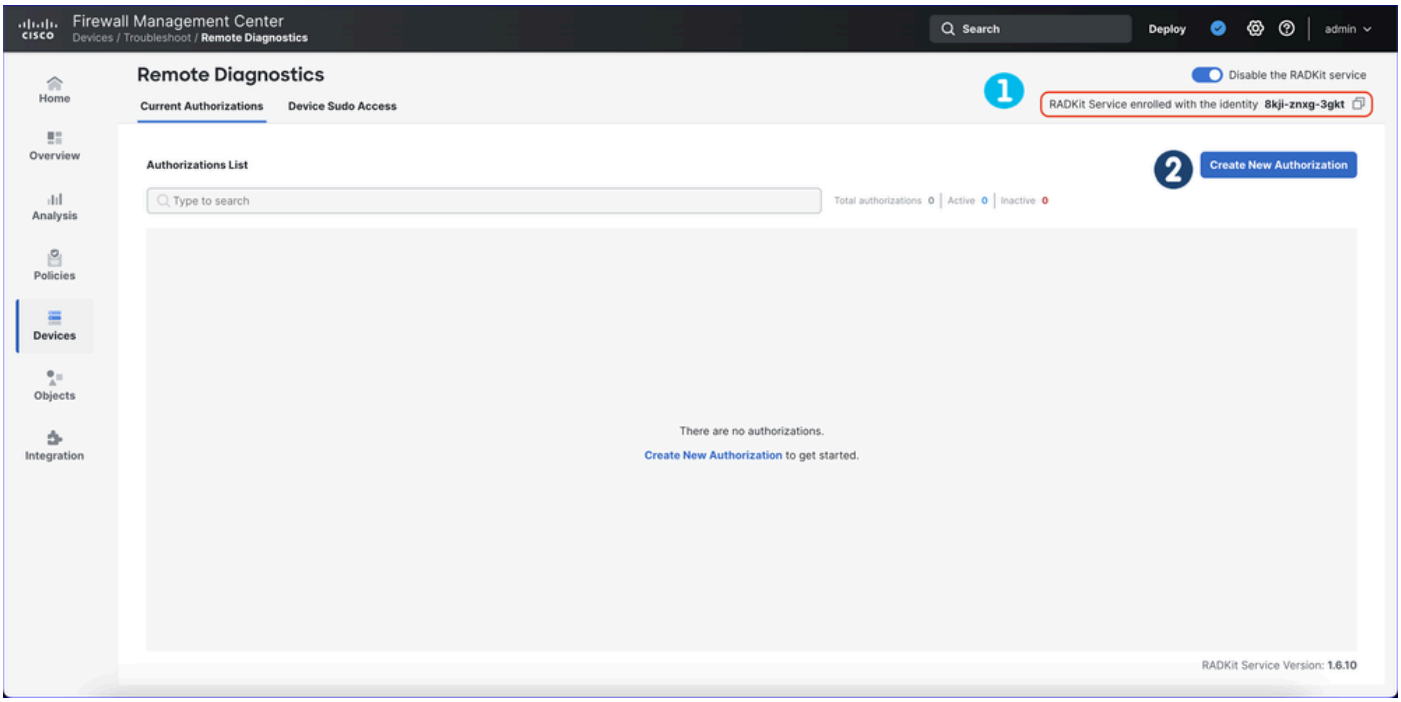
Após a autenticação bem-sucedida, o usuário pode fechar a guia do navegador e retornar à página Remote Diagnostics do FMC.



Serviço RADKit inscrito

O serviço RADKit é registrado com o ID de serviço especificado (neste exemplo, o ID é 8kji-znxg-3gkt). A ID pode ser copiada para a área de transferência. Entregue-o ao engenheiro do Cisco TAC para que ele possa se conectar ao serviço RADKit a partir do cliente RADKit.

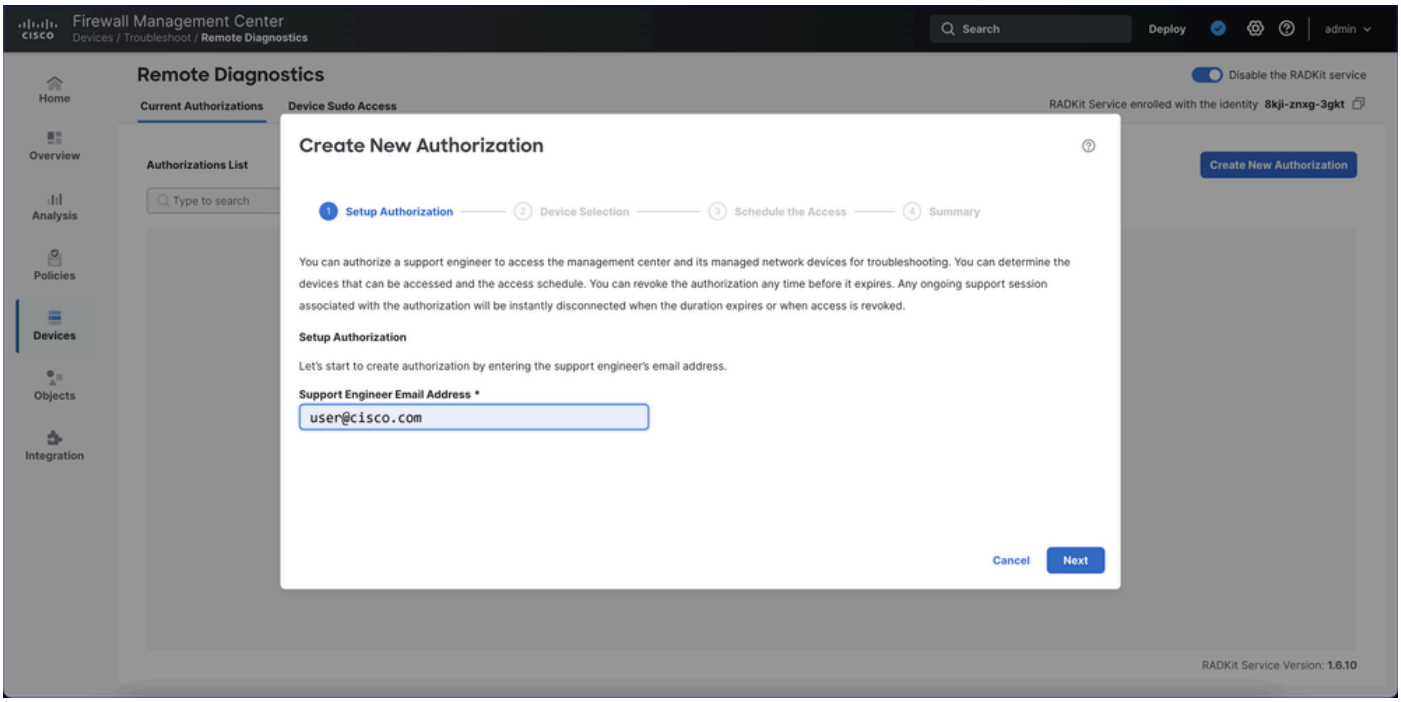
A próxima etapa é criar uma autorização clicando no botão "Criar nova autorização":



Criar nova autorização: Passo 1

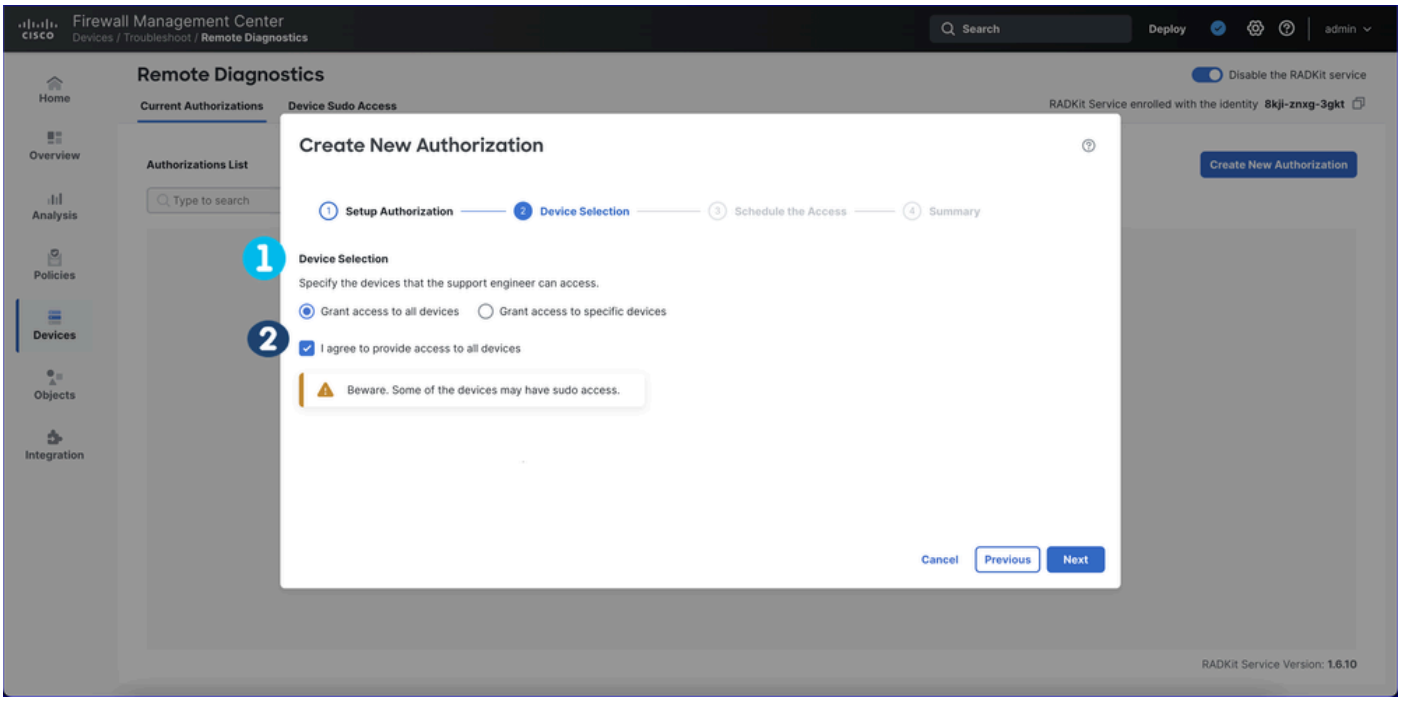
- Para criar uma nova autorização, a primeira etapa é adicionar o endereço de e-mail do engenheiro de suporte.

- Há quatro etapas para criar uma nova autorização. O progresso ao longo das etapas é mostrado na parte superior.



Criar nova autorização: Passo 2

- Passo 1: Especifique os dispositivos que o engenheiro de suporte pode acessar. Ou, como neste exemplo, conceda acesso a todos os dispositivos.
- Passo 2: Verifique o botão de opção de todos os dispositivos ou de dispositivos específicos. Para dispositivos específicos, podem ser escolhidos o CVP e/ou o DTF. Observe o aviso que o acesso sudo pode fornecer a alguns dispositivos na guia Acesso Sudo ao Dispositivo. O botão Avançar não será habilitado até que a caixa de seleção seja marcada.
- O acesso ao Sudo é fornecido por dispositivo na guia Acesso ao Sudo do Dispositivo posteriormente (não durante a criação de uma autorização).

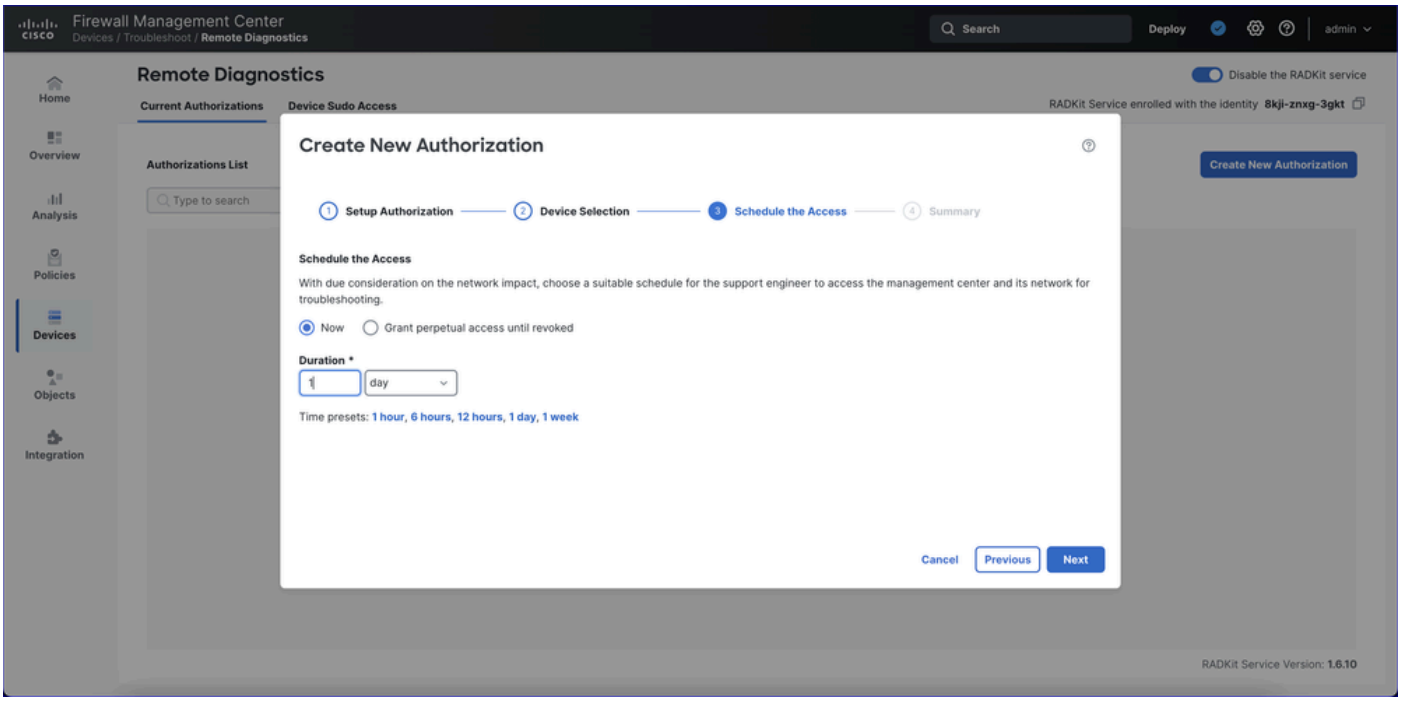


Notas sobre dispositivos de seleção

- Somente os dispositivos em uma compilação suportada (por exemplo, na versão inicial, somente os dispositivos 7.7.0) podem ser selecionados.
- Os dispositivos que estão desativados e inalcançáveis não são selecionáveis. RADKit depende de sftunnel (TCP 8305) para acessar os dispositivos.
  - Se houver um problema de conectividade de túnel, ele não funcionará, mas ainda será mostrado no inventário RADKit.
  - Se um dispositivo for desligado, ele não será visto.
- Se houver FMCs em um par HA, somente o Ativo/Primário poderá ser adicionado.
- Os dispositivos são adicionados ao inventário RADKit durante a criação/edição de uma autorização. Quando o registro dos dispositivos no FMC é cancelado, eles são removidos do "inventário" de dispositivos.

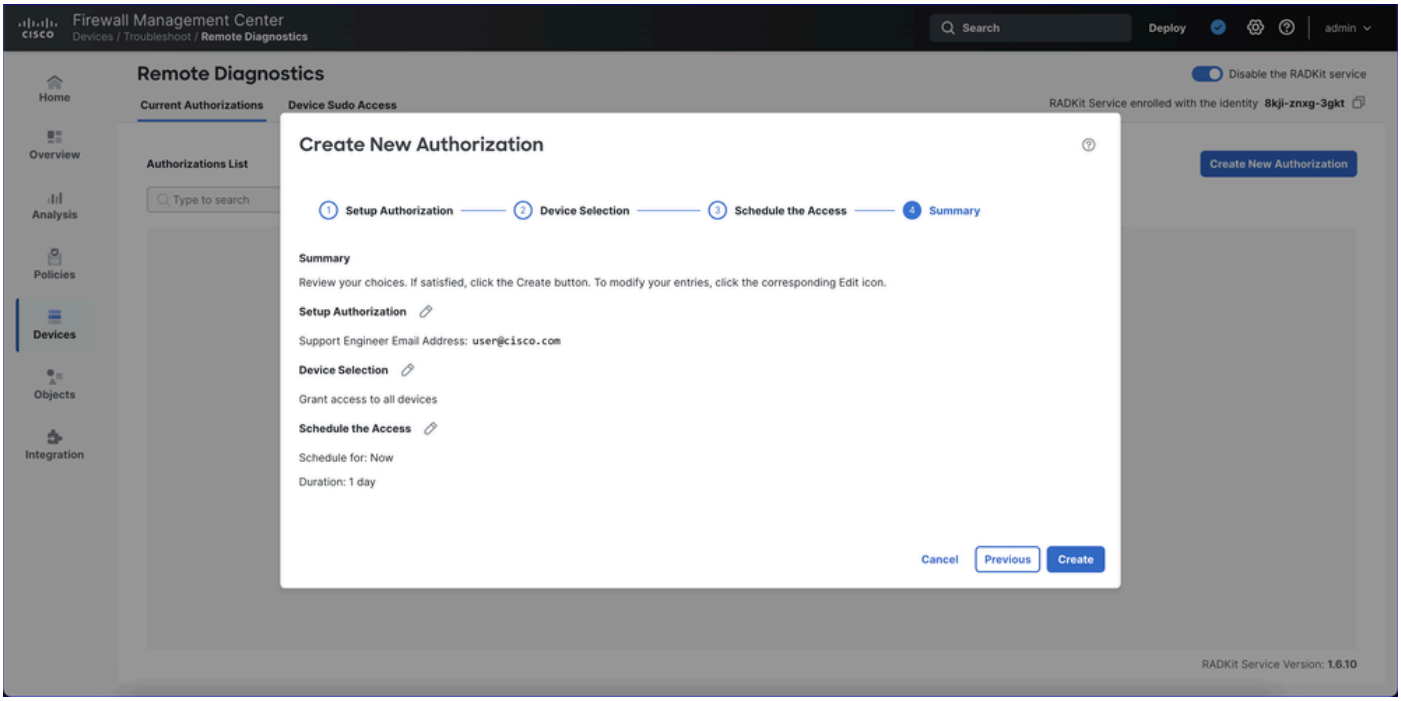
Criar nova autorização: Etapa 3

- Passo 3: Especifique a duração do acesso do engenheiro de suporte aos dispositivos.
- Escolha "Agora" e especifique uma duração, ou
- Selecione "Conceder acesso permanente até ser revogado".
- A duração padrão é 1 dia. Qualquer duração pode ser definida; há também alguns valores de duração predefinidos.



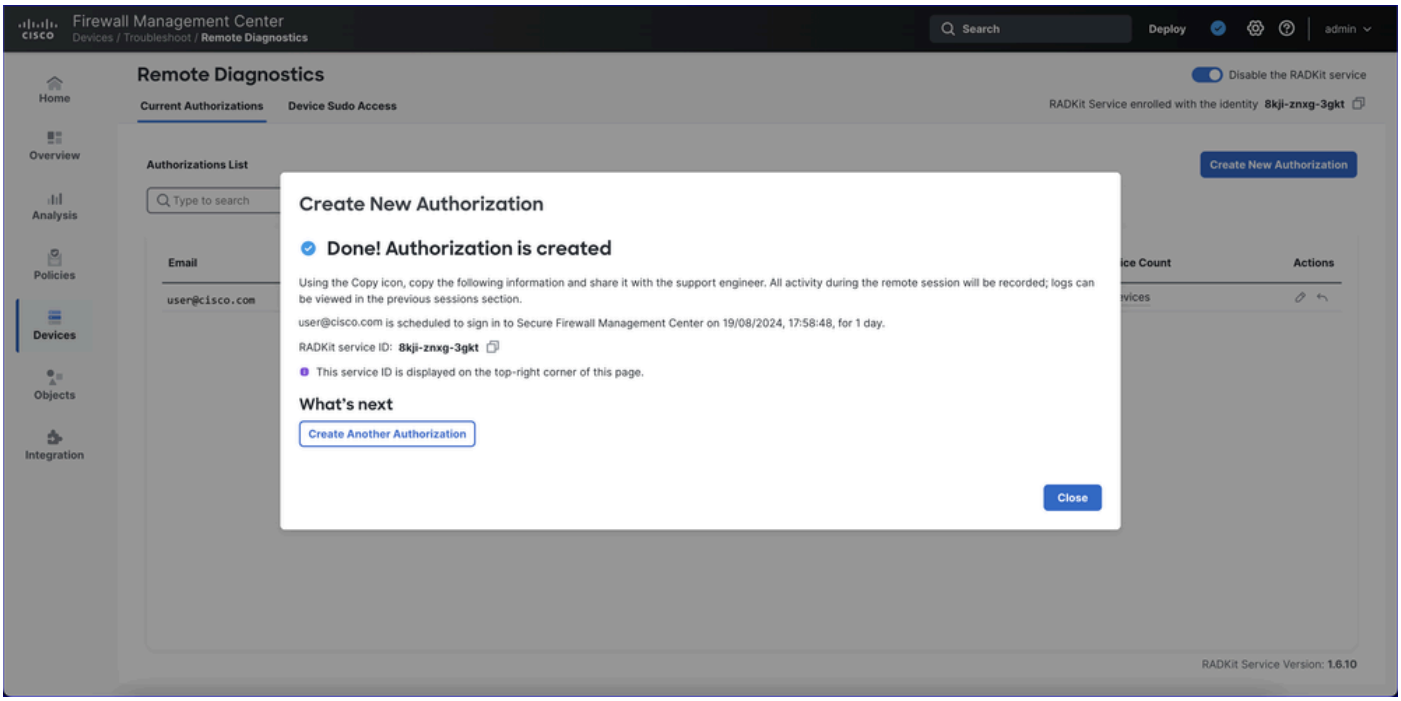
Criar Novo Resumo de Autorização

A etapa final é o resumo da autorização. Aqui, um usuário pode revisar e editar a configuração.



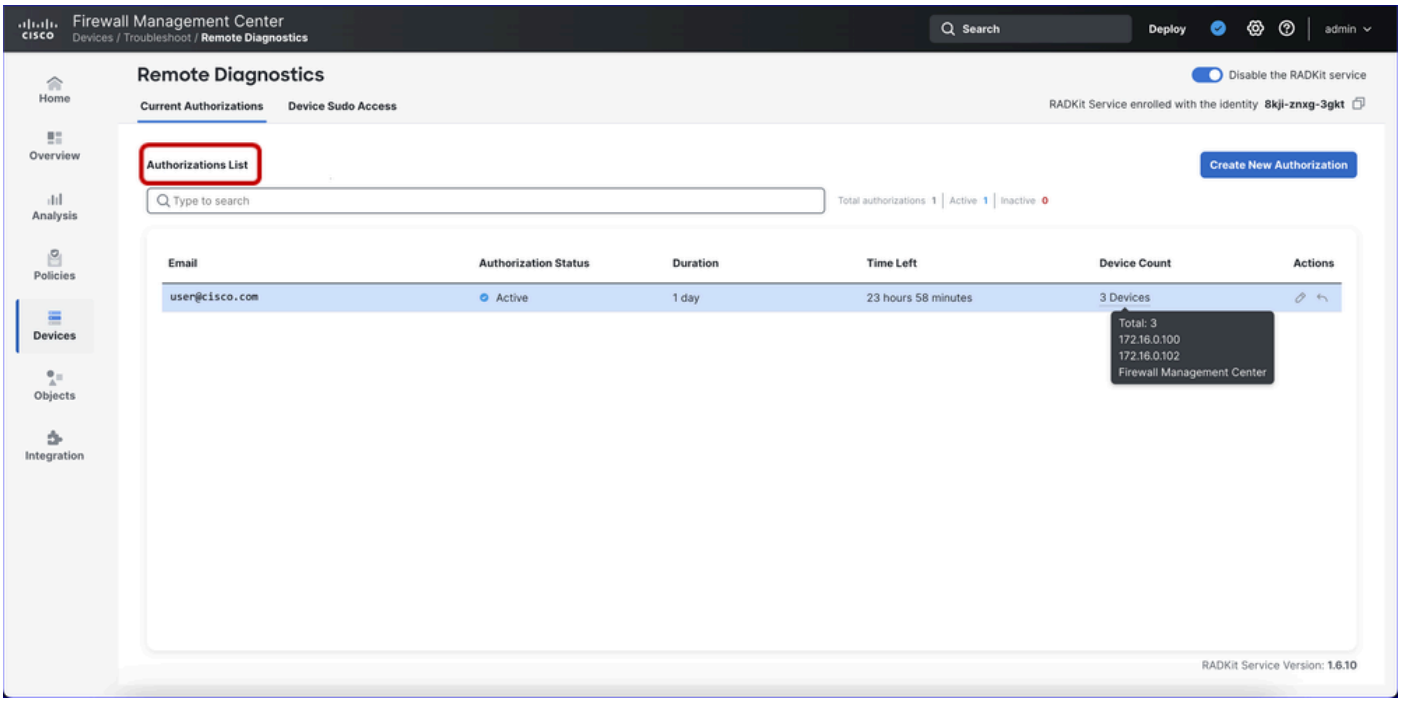
Criação de nova autorização concluída

Uma tela de confirmação será exibida após a conclusão da criação da autorização:



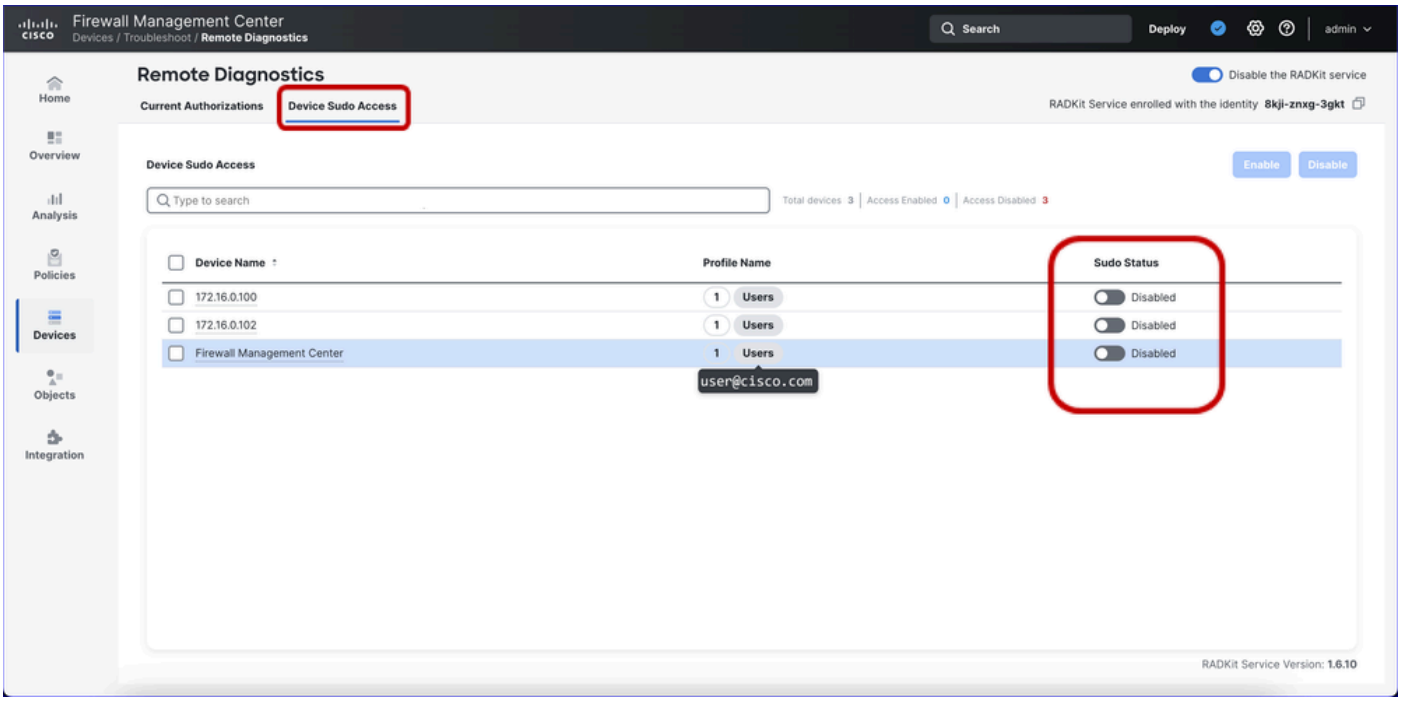
Lista de Autorizações Atuais, Incluindo Revogar

- A lista de autorizações atuais é exibida na guia Autorizações Atuais.
- As Ações (coluna da extrema direita) são Revogar acesso e Editar autorização.



Lista de Acesso Sudo do Dispositivo

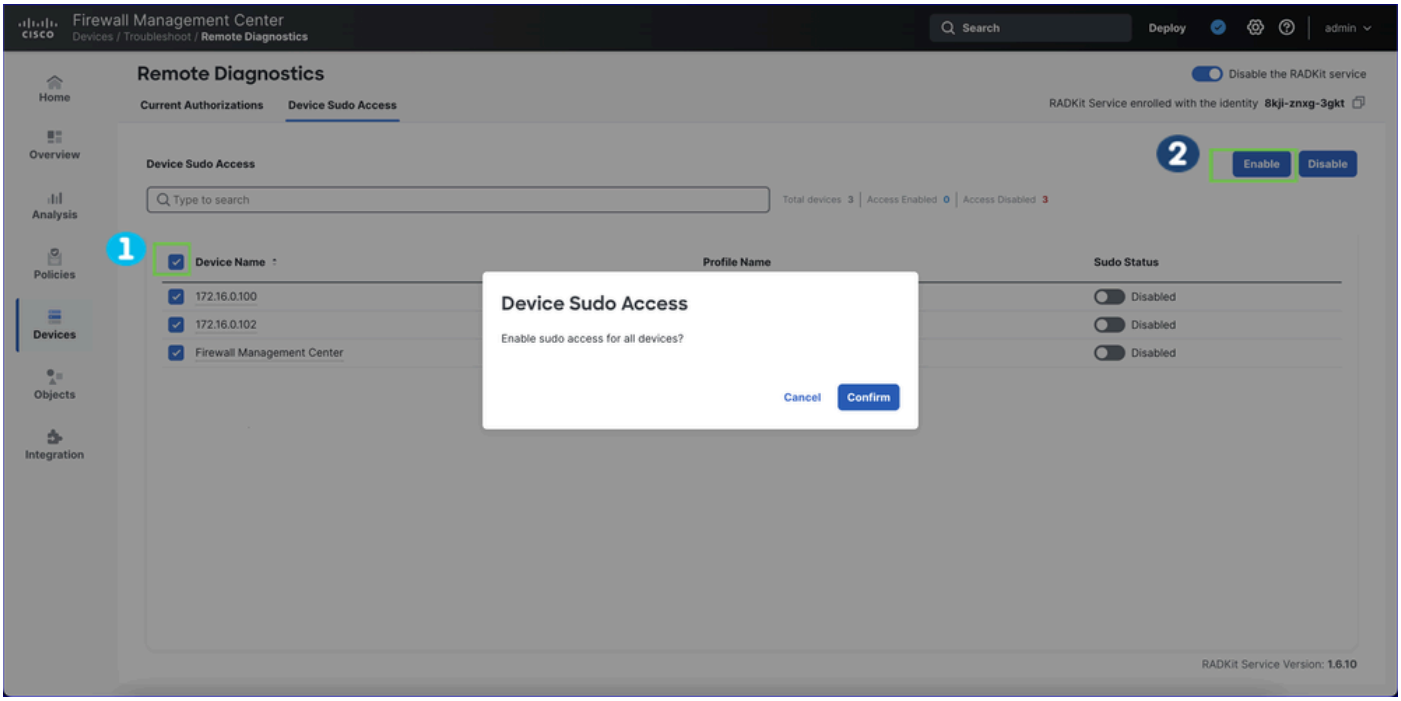
- A lista de dispositivos com configurações de acesso sudo é apresentada na guia Acesso Sudo ao Dispositivo.
- Utilize a tecla de alternância na coluna da direita para ativar o acesso sudo. Está desativado por padrão.
- Além disso, habilitar/desabilitar o acesso sudo em massa está disponível.



Confirmar ativação do acesso ao sudo dos dispositivos

1. O acesso ao Sudo pode ser ativado para todos ou apenas para alguns dispositivos específicos, selecionando os dispositivos e clicando no botão "Enable".

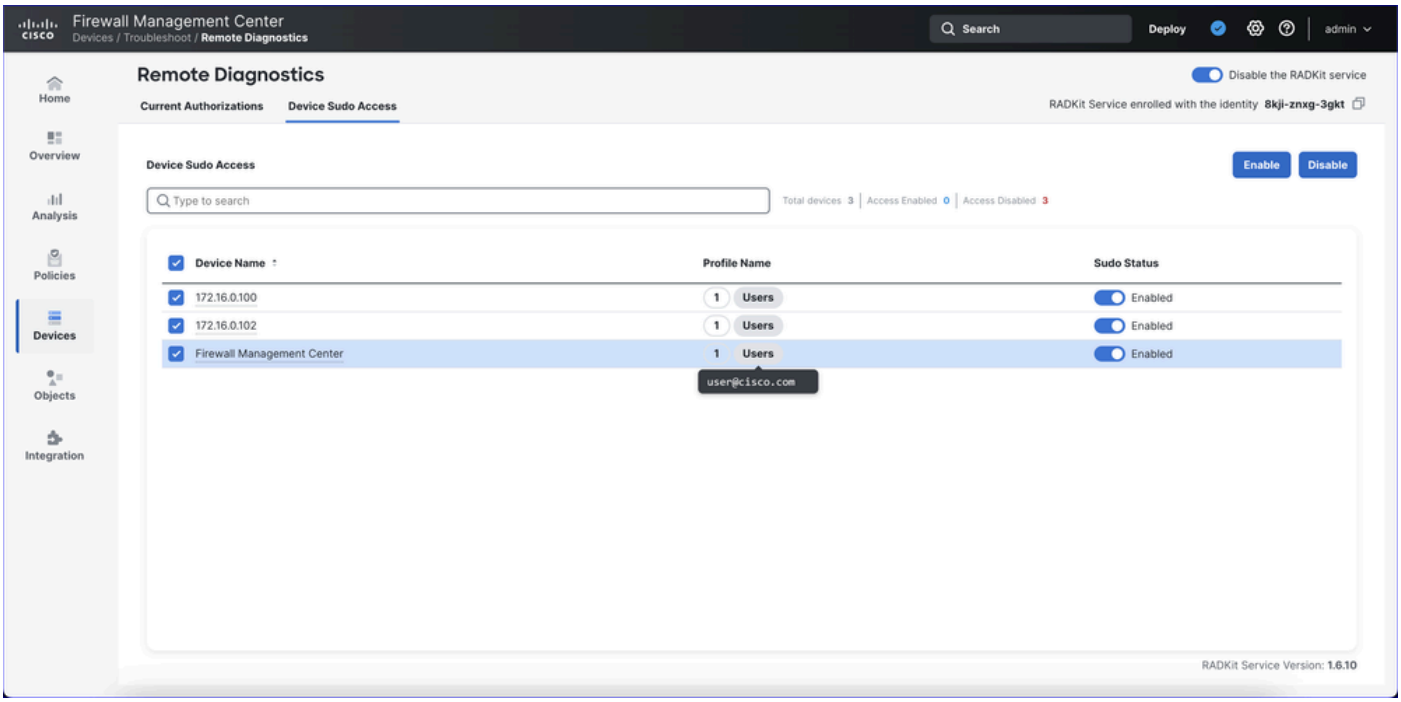
2. Ao ativar, uma caixa de diálogo de confirmação é exibida e é necessário clicar em Confirmar.



Acesso Sudo a Dispositivos Habilitado

- Depois de ativar ou desativar o acesso sudo para um dispositivo, a coluna Status do sudo à direita da página é atualizada.
- O engenheiro de suporte é capaz de executar sudo su no dispositivo; isto não tem senha. O

engenheiro de suporte não precisa ter a senha raiz.



Outras observações

- Apenas os dispositivos no domínio ao qual o usuário do FMC tem acesso são visíveis e podem ser autorizados para acesso remoto.
- Se os CVP estiverem em HA:
  - O serviço RADKit só pode ser ativado no modo Ativo/Primário.
  - O FMC secundário não pode ser adicionado atualmente como um dispositivo a ser acessado do cliente RADKit.
- A autorização só pode ser feita para um engenheiro de suporte de cada vez.
  - Se você precisar de outro engenheiro de suporte para ter acesso, crie outra autorização para o engenheiro adicional. A ID do serviço seria a mesma.

APIs REST do FMC

APIs REST do serviço RADKit

Para suportar operações de criação e leitura no serviço RADKit, estes novos URLs foram introduzidos:

- GET: /api/fmc_troubleshoot/v1 /domain/{domainUUID}/radkit/services
  - Recupera todos os dados do serviço RADKit do FMC.
- GET: /api/fmc_troubleshoot/v1/domain/{domainUID}/radkit/services/{id}
  - Obtém/recupera os dados do serviço RADKit da ID especificada.
- POST: /api/fmc_troubleshoot/v1/domain/{domainUID}/radkit/services
  - Cria o serviço RADKit no FMC (habilitar/desabilitar o serviço).

Modelo de serviço RADKit

O modelo de serviço RADKit consiste em:

- tipo
- id
- status
- estáInscrito
- serviceId
- versão


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


Suporte da Cisco: Uso do cliente RADKit

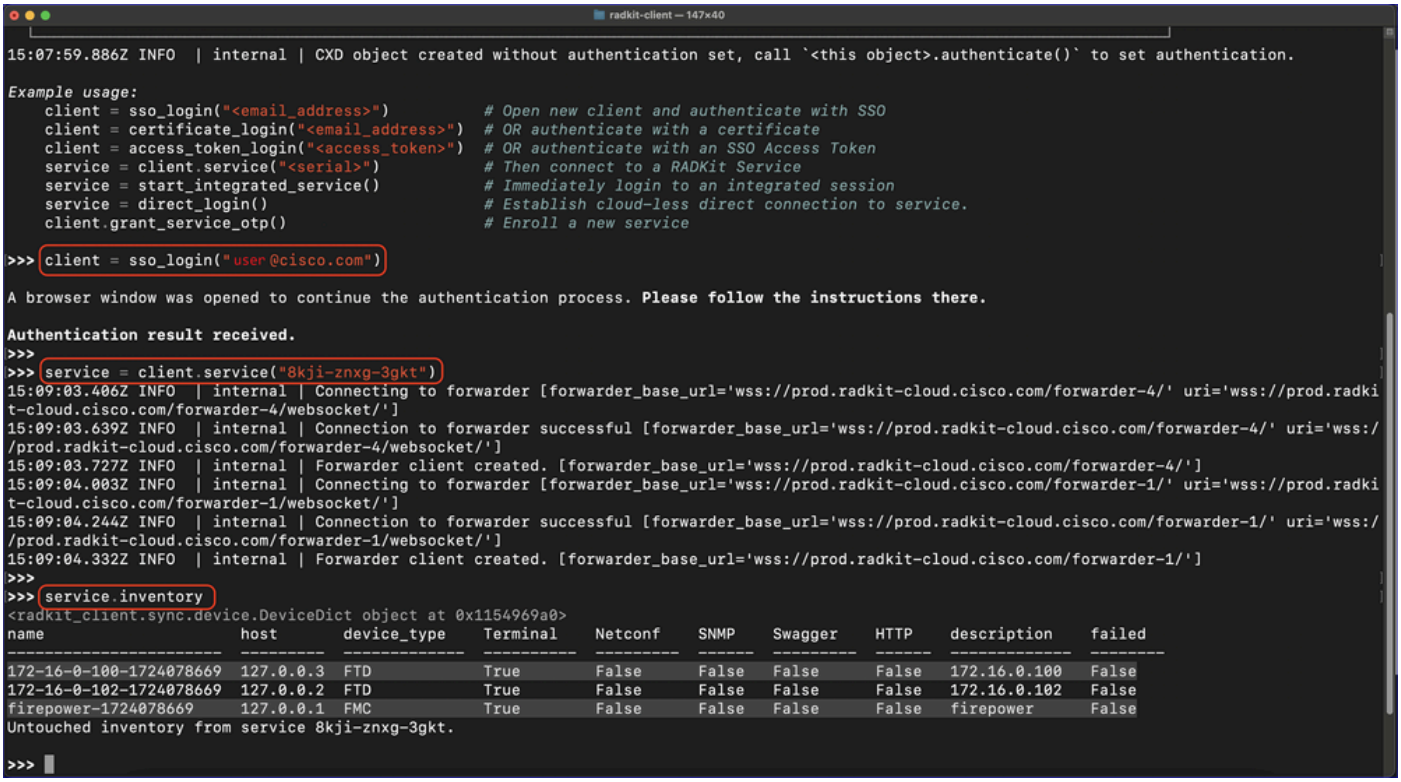
Lado de suporte: Instalar o cliente RADKit

- Para acessar o FMC/FTD, o suporte precisa ter o cliente RADKit instalado.
  - O cliente funciona em sistemas operacionais Windows, Mac e Linux.
- O suporte pode acessar vários dispositivos de vários usuários. Cada autorização RADKit tem seu próprio "inventário" de dispositivos.
  - Para cada inventário de dispositivo de usuário que o suporte deseja acessar, a ID de serviço RADKit é necessária.
  - Para um único inventário, o acesso é possível para o FMC e seus FTDs gerenciados do cliente RADKit, conforme especificado pelo usuário ao autorizar o acesso.

Obtenha e instale o cliente RADKit

O cliente RADKit pode ser instalado localmente a partir de https://radkit.cisco.com/downloads/release/ e, em seguida, iniciado a partir do terminal com o comando: radkit-client

Os instaladores estão disponíveis para Windows, MacOS e Linux.



Captura de tela do cliente RADKit com comandos de login (detalhes na próxima seção).

Comandos de login do cliente RADKit

- Usar o endereço de email que o usuário inseriu durante a autorização no FMC.
- O cliente RADKit efetua login e conecta-se aos comandos de ID de serviço especificados. A ID de serviço RADKit, neste exemplo 8abc-znxg-3abc, deve corresponder ao que o administrador do firewall vê no 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
```

Comando RADKit Client Service Inventory

Comando para listar o inventário que o usuário remoto (engenheiro do Cisco TAC) está autorizado a acessar:

```
<#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.
```

Há um comando de filtragem para os dispositivos no inventário (próxima seção). Use o nome na coluna à esquerda para iniciar uma sessão interativa com o dispositivo (comando na próxima seção).

Tip: Se o inventário estiver desatualizado, você poderá atualizá-lo usando o comando: **>>>** service.update_inventory()

Cliente RADKit: Filtrar Dispositivos

Comando para filtrar dispositivos no inventário:

```
<#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.
```

Comando de sessão interativa do dispositivo do cliente RADKit

Início de uma sessão interativa para um dispositivo (neste caso, um FMC) com o nome "firepower-1724078669" retirado do comando anterior "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)
```

Comandos de execução do cliente RADKit em dispositivos

Execute os comandos nos dispositivos!

```
<#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
----------------------------------------------------
```

Obtenha detalhes adicionais dos dispositivos

Considerando este inventário:

<#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
```

Para obter detalhes de 'show version' nos dispositivos de 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
----------------------------------------------------

>
```

Método alternativo:

<#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
----------------------------------------------------
```

Obtendo arquivos de dispositivos

- Por meio do cliente RADKit, um engenheiro do Cisco TAC pode executar SSH para dispositivos e várias operações, incluindo a geração de arquivos de solução de problemas.

Suporte da Cisco: Console RADKit

Usando o console de rede RADKit

- Como alternativa ao uso do cliente RADKit, um engenheiro de suporte do Cisco TAC pode usar o console de rede RADKit. O Network Console faz parte do cliente RADKit.

- O RADKit Network Console é um recurso que fornece uma interface de linha de comando (CLI) simples para funções básicas do cliente RADKit. Ele deve ser usado para conectividade rápida com uma instância do serviço RADKit, estabelecendo sessões interativas e fazendo download/upload de arquivos sem problemas e com treinamento mínimo.
- Inicie o Network Console usando a linha de comando: radkit-network-console
- Consulte a documentação do RADKit para obter mais detalhes.

Atualizações e compatibilidade com versões anteriores

Atualização para 7.7 e de 7.7 para cima

- O serviço RADKit é adicionado ao Secure Firewall 7.7.0.
    - Os dispositivos atualizados para a versão 7.7.0+ têm a configuração necessária para o serviço RADKit.

Experiência com FTDs sem suporte

- Os FMC e os FTD devem ter a versão mínima 7.7.0 para que esta funcionalidade funcione (os FTD com uma versão inferior a 7.7 não podem ser acrescentados a uma autorização FMC RADKit 7.7).
- Os FTDs registrados que não estão na versão 7.7.0 não estão disponíveis para seleção para habilitação de autorização.

Troubleshooting

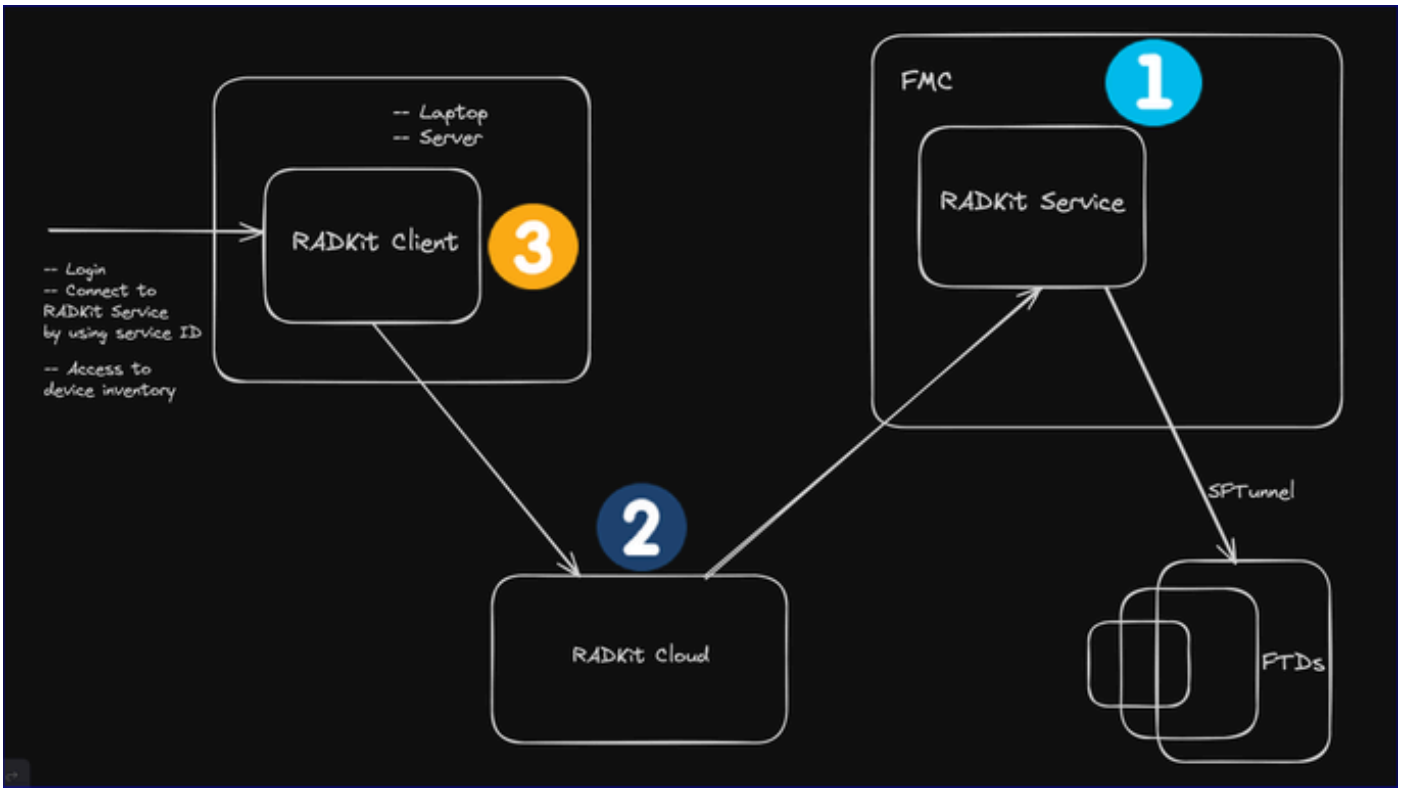
Visão Geral do Diagnóstico

Pontos de Troubleshooting

1. Use as ferramentas Browser Development e os logs do FMC para ver o que está acontecendo no FMC.

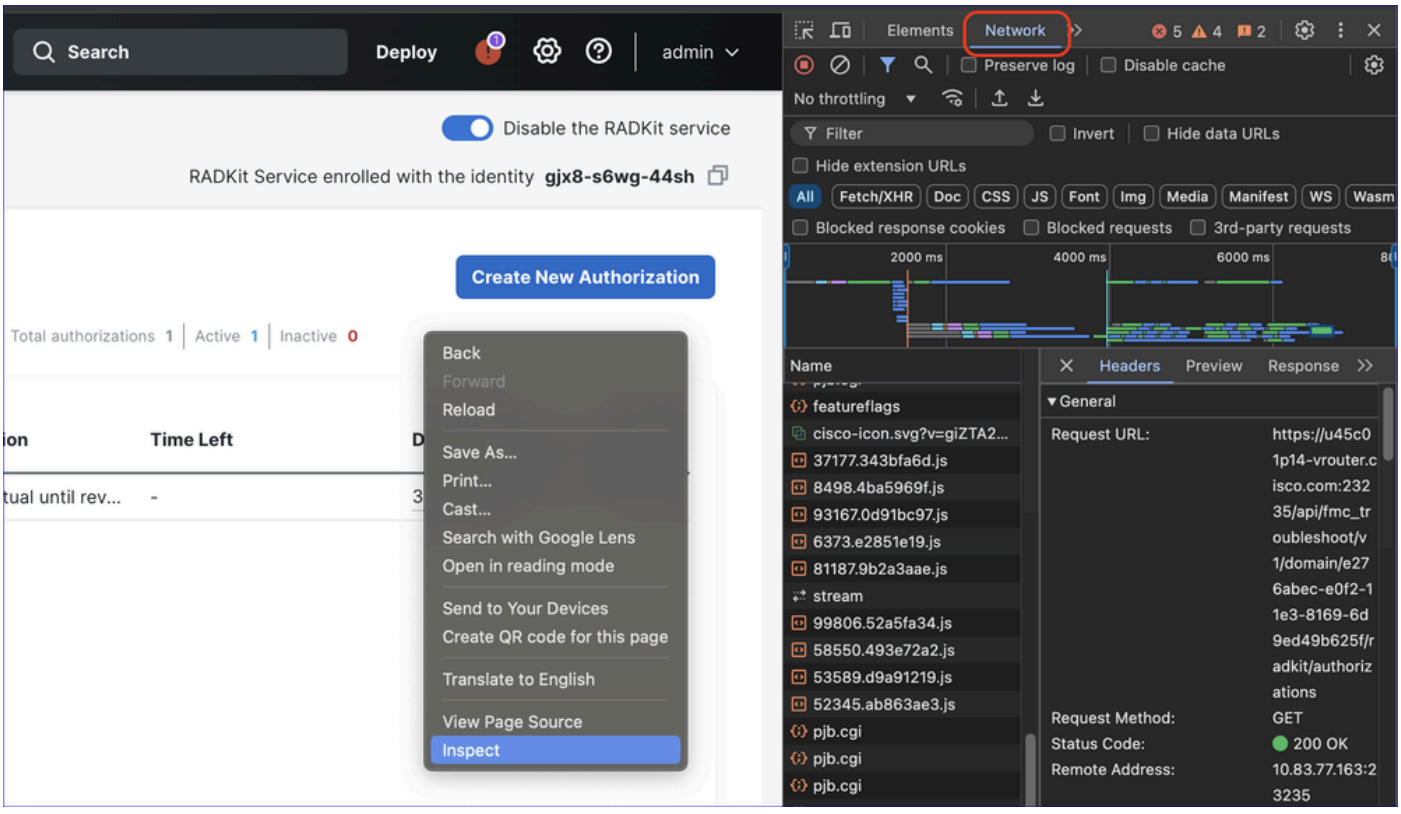
2. Para problemas de comunicação entre o serviço RADKit no FMC, o RADkit Cloud e o cliente RADKit, consulte o registro do cliente RADKit.

3. Cliente RADKit.



Como solucionar problemas: Ferramentas para desenvolvedores do navegador

- A guia do navegador Developer Tools, Network mostra as chamadas de API que foram executadas na página; isso pode ser usado ao solucionar problemas no FMC. Isso pode ser iniciado clicando com o botão direito do mouse na página e depois clicando em Inspecionar.
- Verifique o código de status da chamada da API e a visualização da resposta na guia Rede.



APIs de middleware de Go do serviço RADKit

Go Middleware para a integração RAKIit usa chamadas de API que não estão disponíveis publicamente através do FMC API explorer. O registro Go Middleware APIs está disponível em /var/log/auth-daemon.log. A funcionalidade que o Go Middleware executa inclui:

- Inscreva o serviço RADKit na nuvem RADKit com o processo Single Sign On.
- Busque uma lista de todas as autorizações de usuários remotos RADKit e dispositivos associados.
- Busque uma autorização de usuário RADKit remota específica e os dispositivos associados usando um e-mail.
- Crie uma autorização de usuário RADKit remota e conceda permissões para acessar dispositivos (todos os dispositivos ou uma lista de dispositivos selecionados) por um período de tempo especificado.
- Modificar uma autorização de usuário RADKit remota.
- Excluir uma autorização de usuário RADKit remota.

Registros para Troubleshooting do Serviço RADKit

- Registros gerais do FMC: comando pigtail de uma sessão ssh do FMC.
- APIs Go Middleware: /var/log/auth-daemon.log
- Logs que contêm RADKit e auth-daemon processam dados:

/var/log/process_stdout.log

/var/log/process_stderr.log

Todos esses registros estão incluídos nas soluções de problemas do FMC/FTD.

- Logs de serviço RADKit internos: /var/lib/radkit/logs/service/
- Registros para as operações realizadas do cliente RADKit em dispositivos (FMCs e FTDs): /var/lib/radkit/session_logs/service

Registros para enviar ao Cisco TAC

- Capturas de tela de erros.
- Descrição do problema.
- Etapas para reprodução.
- Extratos de log Pigtail e /var/log/auth-daemon.log contendo os erros.

Monitorando o acesso

O registro de quem recebeu acesso durante quanto tempo e de quem recebeu o acesso consta dos registros de auditoria do CVP.

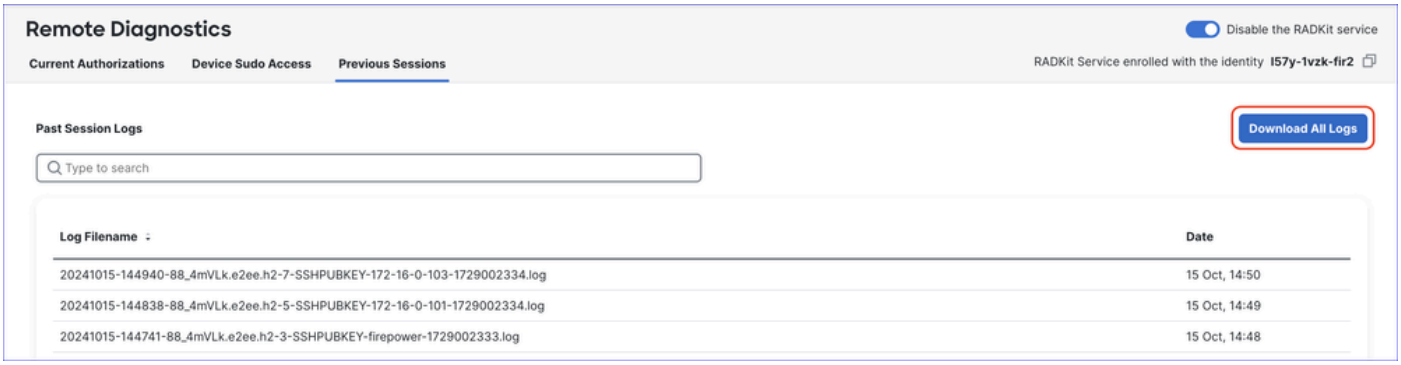
Logs de sessão RADKit

Os registros de sessão RADKit para as operações realizadas do cliente RADKit em dispositivos (FMCs e FTDs) estão presentes no FMC em /var/lib/radkit/session_logs/service:

- Os registros são do próprio serviço RADKit.
- Esses registros estão incluídos em um pacote de solução de problemas.
- Os logs também podem ser acessados pela interface do usuário (consulte a próxima seção).
- Há vários arquivos de log de sessão; um por sessão.

RADKit Logs de sessões anteriores

Os registros de sessões do RADKit para as operações do dispositivo executadas a partir do cliente RADKit estão disponíveis para download como um arquivo contendo todos os registros na guia Previous Sessions, clicando no botão "Download All Logs".



Exemplo de problema com Troubleshooting de Passo a Passo

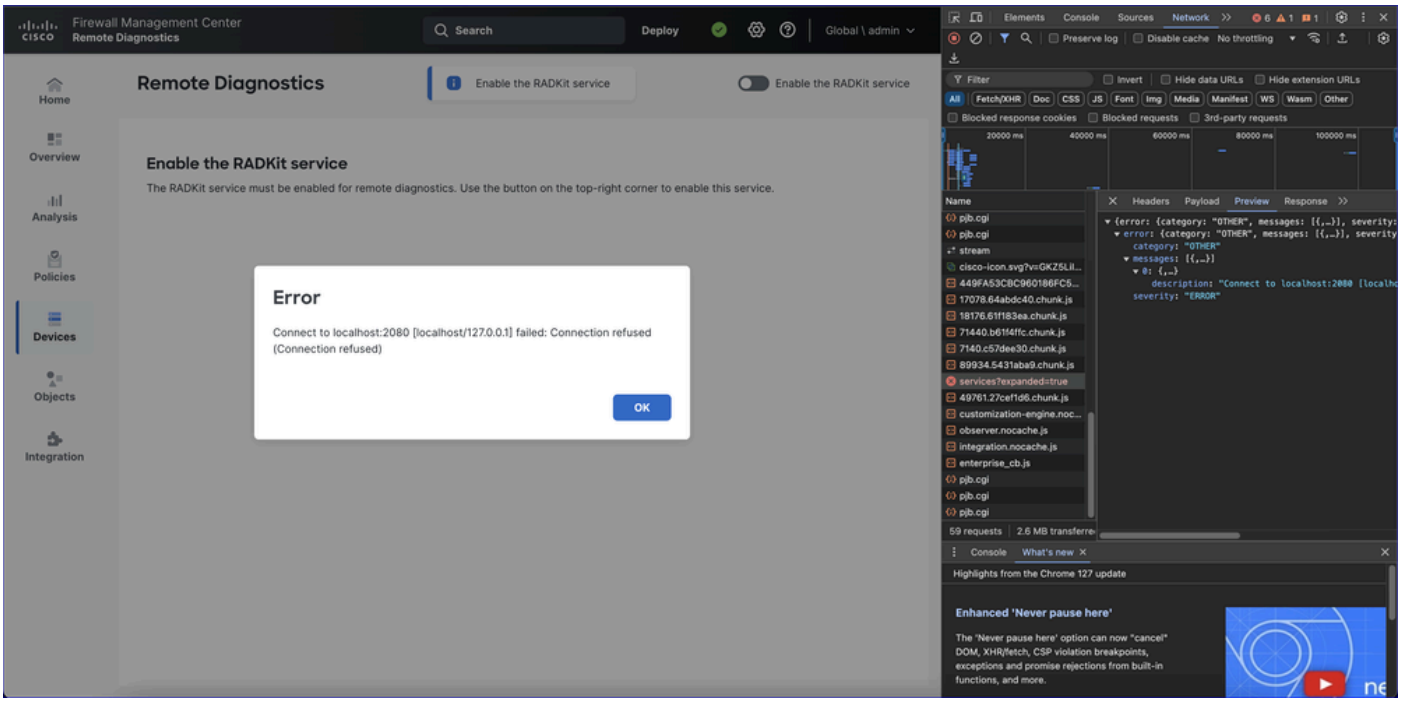
Exemplo de Troubleshooting

Em caso de erro como "Connect to localhost:2080 [localhost/127.0.0.1] failed: Connection rejected (Connection refused)", tente reiniciar o auth-daemon de uma sessão FMC SSH:

<#root>

root@firepower:~$

sudo pmtool restartbyid auth-daemon



Telemetria

A saída de telemetria foi adicionada para este recurso:

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

FAQ

Perguntas freqüentes: Login e inscrição

P. A inscrição funciona com proxy se o FMC não tiver acesso direto à Internet?

R. Sim, se o proxy tiver acesso a prod.radkit-cloud.cisco.com, que é usado para o processo de inscrição.

P. Um usuário pode usar seu próprio IdP para esse serviço?

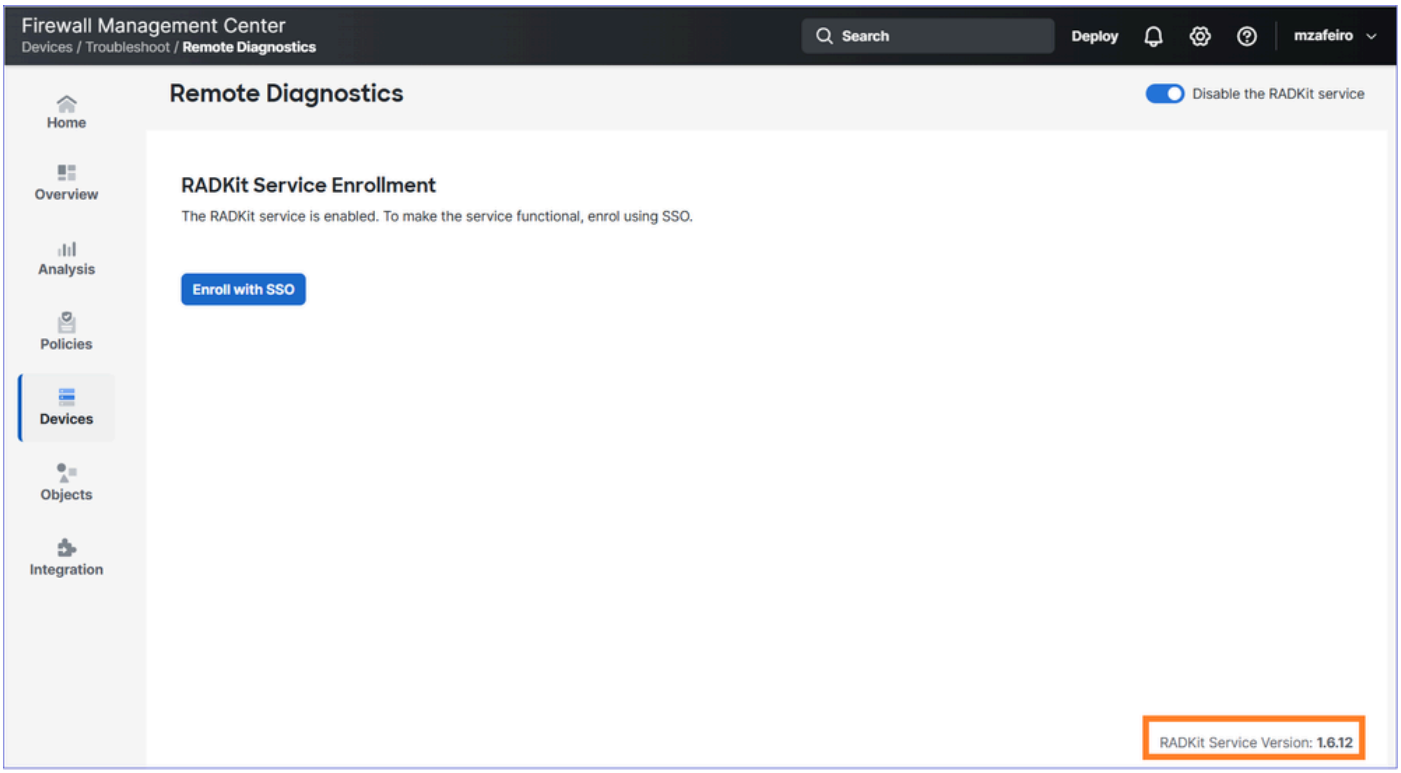
R. Somente o Cisco SSO é aceito na nuvem RADKit. Há uma opção para associar a conta da sua empresa a uma conta da Cisco, para que a inscrição de serviço RADKit seja possível com um e-mail que não seja da Cisco.

Perguntas freqüentes: Versões RADKit

P. Que versão do RADkit está incluída no FMC na versão 7.7? Como podemos saber qual versão do RADKit está incluída no FMC? Isso pode ser atualizado sem uma atualização do FMC?

A.

- A versão do RADKit que vem com 7.7.0 é 1.6.12.
- A versão do serviço RADKit é exibida na parte inferior da página FMC Remote Diagnostics: "Versão do serviço RADKit: 1.6.12."



- O RADKit vem com pacotes/hotfixes de atualização do FMC. A atualização do serviço RADKit no FMC separadamente não é suportada.

Perguntas freqüentes: Outro

P. Os dispositivos externos - não gerenciados pelo FMC - podem ser incluídos?

R. Somente os dispositivos gerenciados pelo FMC podem ser adicionados ao inventário do RADKit e, em seguida, podem ser acessados através de uma autorização.

P. É feito backup da configuração do RADKit como parte do backup do FMC?

A.

- O backup da configuração não é feito como parte do backup do FMC.
- Não há suporte porque esperamos que, em geral, o acesso perpétuo não seja oferecido; normalmente, o acesso é limitado.

Referências

Links úteis:

- Guia de configuração do 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

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.