Configurar a autenticação TACACS+ no switch Arista com ISE

Contents

Introdução

Este documento descreve como integrar o Cisco ISE TACACS+ com um switch Arista para AAA centralizado de acesso de administrador.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolo Cisco ISE e TACACS+.
- Switches Arista

Componentes Utilizados

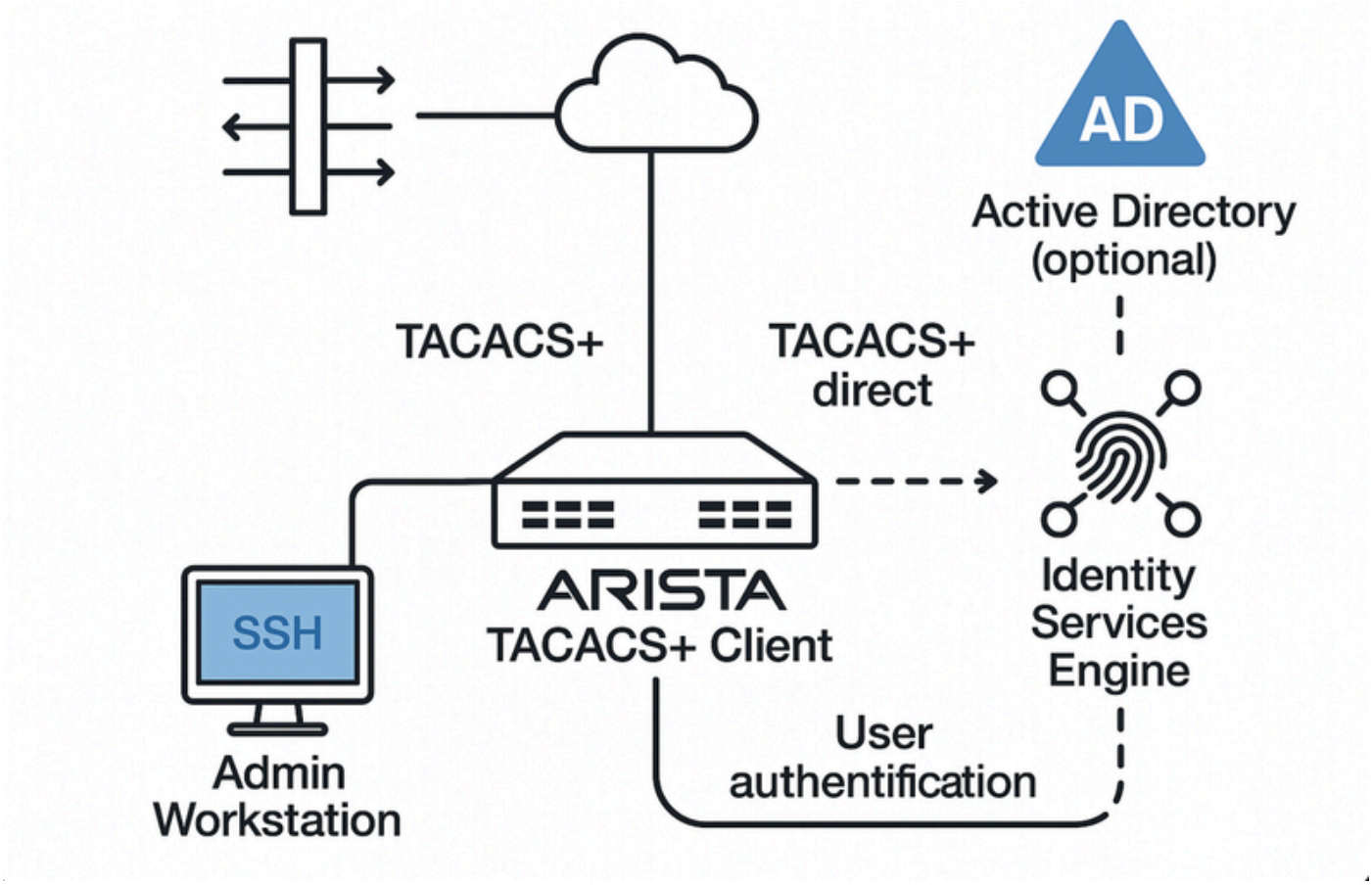
As informações neste documento são baseadas nestas versões de software e hardware:

- Versão da imagem do software do switch Arista: 4,33,2F
- Cisco Identity Services Engine (ISE) versão 3.3 Patch 4

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando

Diagrama de Rede

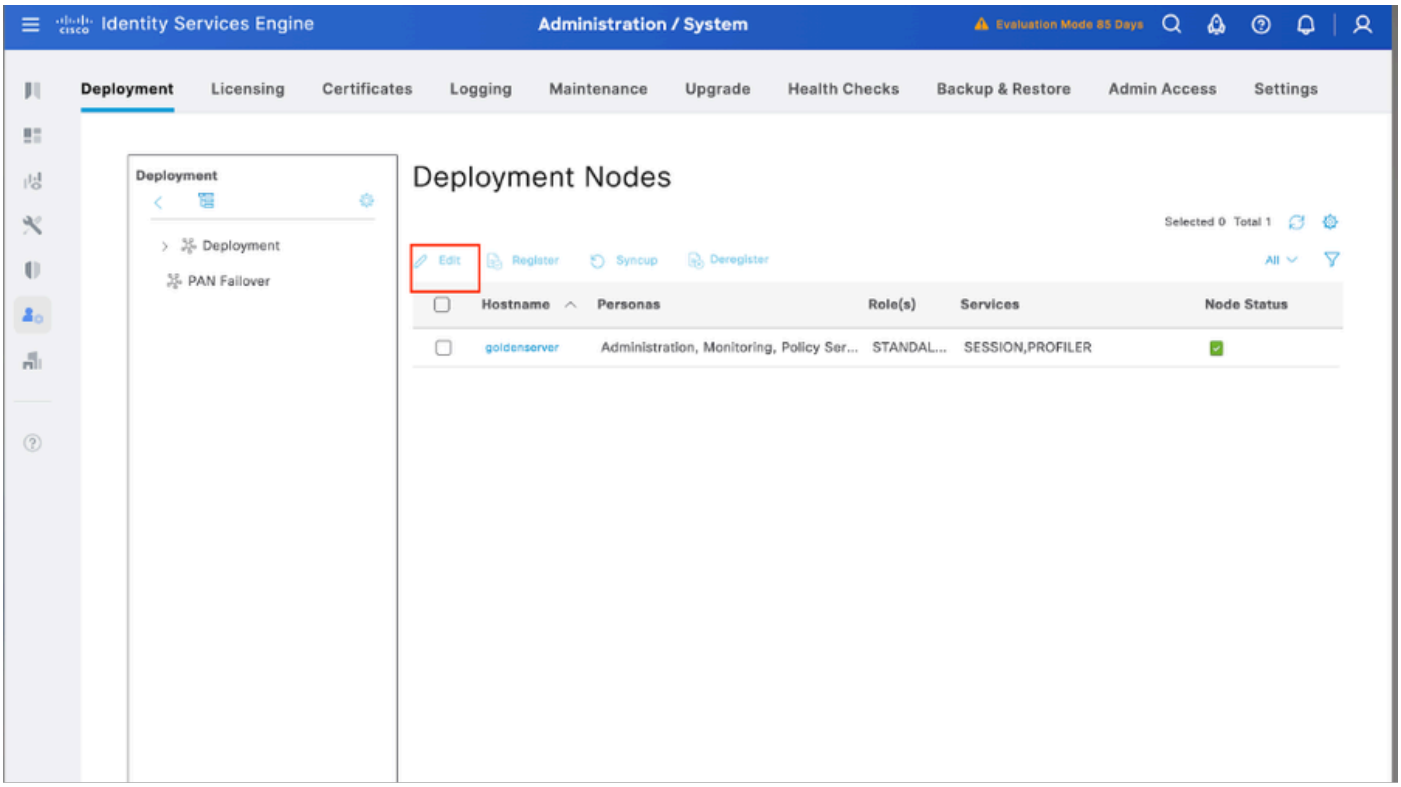


Configurações

Configuração TACACS+ no ISE

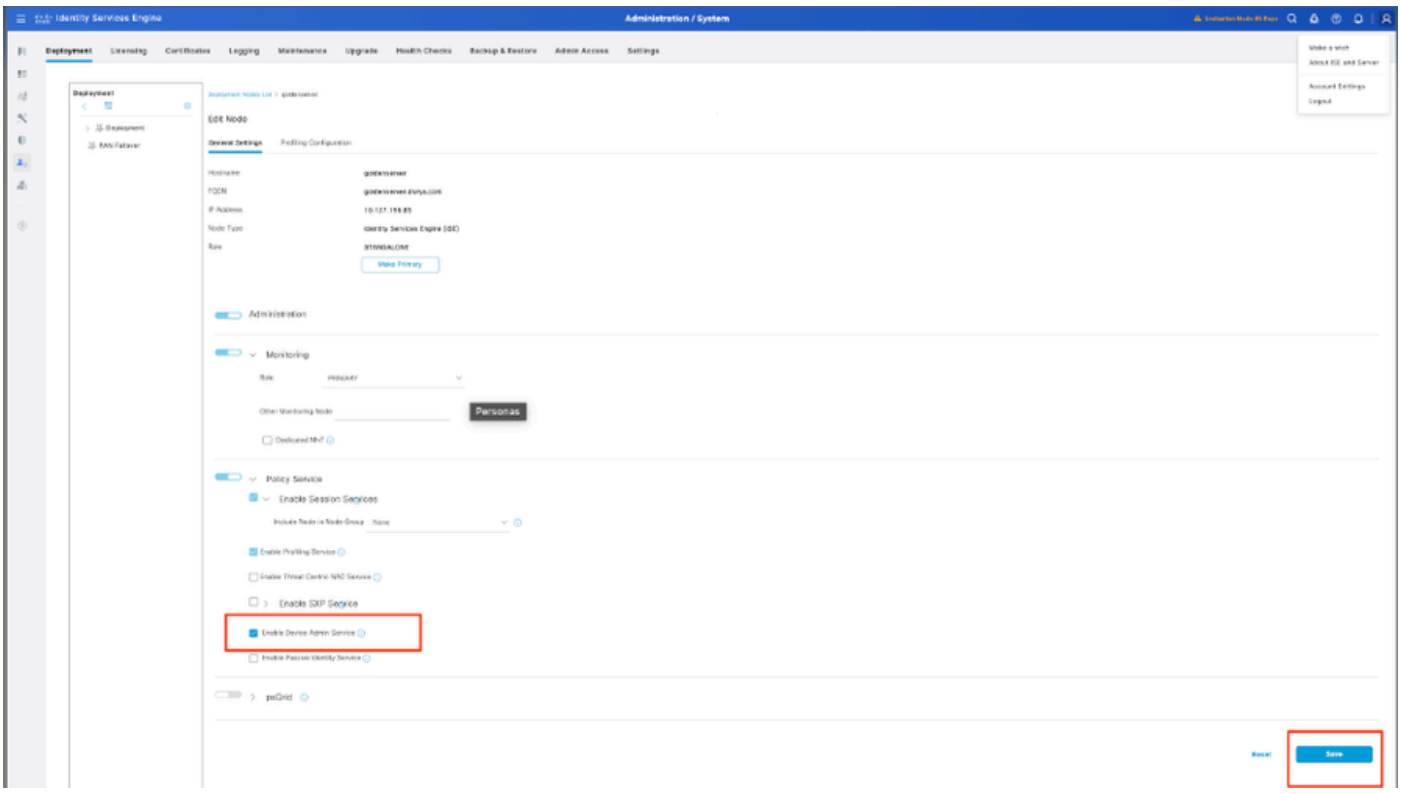
Etapa 1. A etapa inicial é verificar se o Cisco ISE tem os recursos necessários para lidar com a autenticação TACACS+. Para fazer isso, confirme se o Policy Service Node (PSN) desejado tem o recurso Device Admin Service habilitado.

Navegue até Administration > System > Deployment, selecione o nó apropriado onde o ISE processa a autenticação TACACS+ e clique em Edit para revisar sua configuração.



Etapa 2. Role para baixo para localizar o recurso Device Administration Service. Observe que a habilitação desse recurso exige que a persona do Serviço de política esteja ativa no nó, junto com as licenças TACACS+ disponíveis na implantação.

Marque a caixa de seleção para ativar o recurso e salve a configuração.

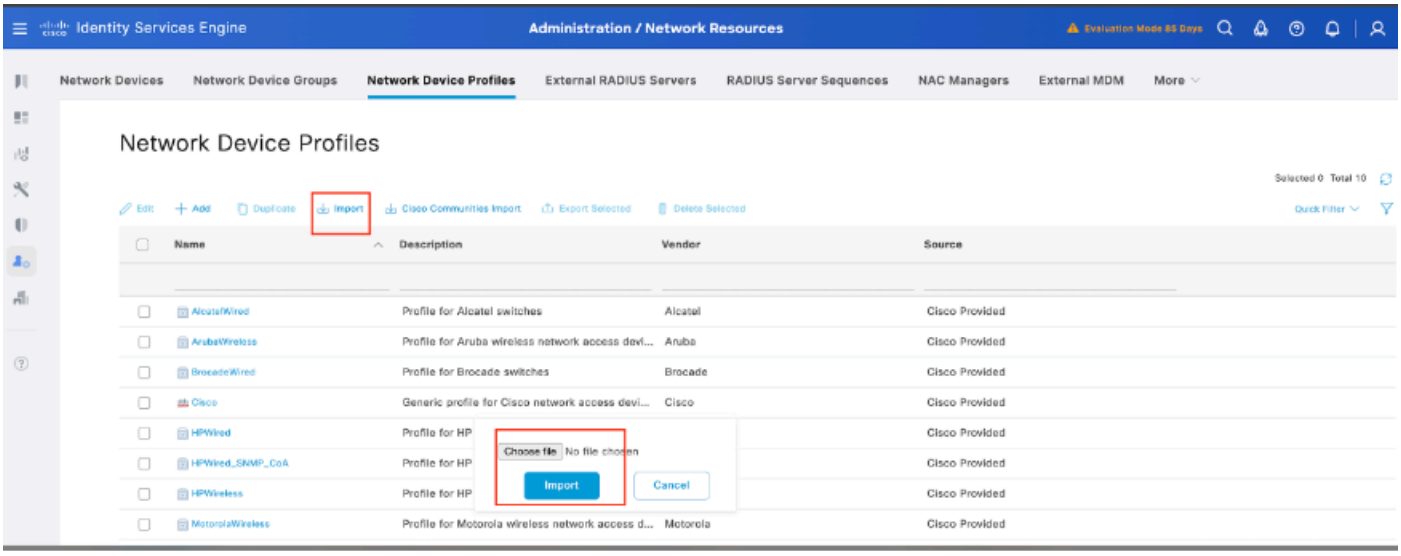


Etapa 3. Obter o perfil do dispositivo de rede Arista para o Cisco ISE.

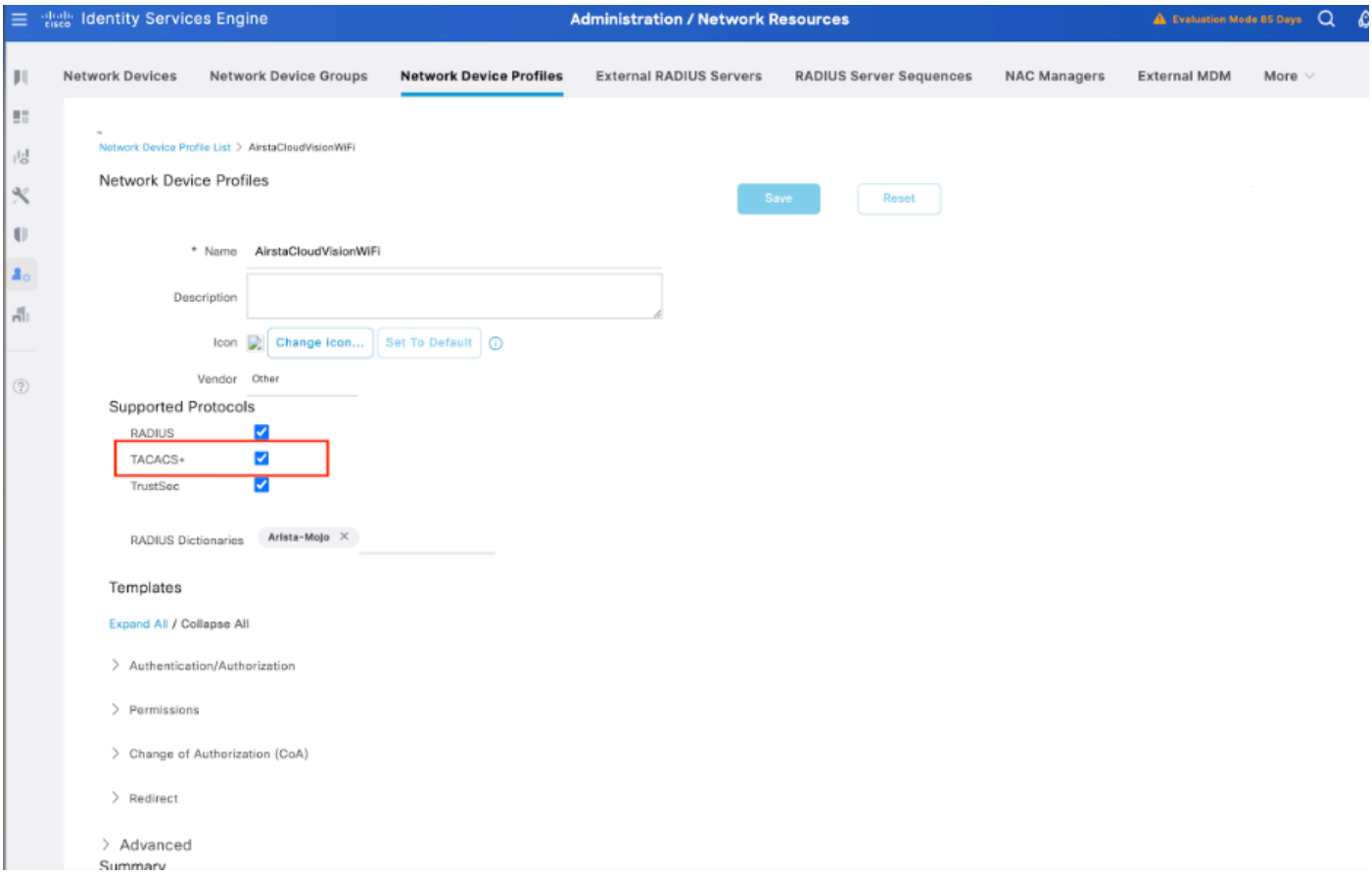
A Comunidade Cisco compartilhou um perfil NAD dedicado para dispositivos Arista. Esse perfil, juntamente com os arquivos de dicionário necessários, pode ser encontrado no artigo Arista CloudVision WiFi Dictionary e NAD Profile for ISE Integration. O download e a importação desse perfil para a configuração do ISE facilita uma integração mais tranquila

Etapas para importar o perfil Arista NAD para o Cisco ISE:

1. Faça o download do perfil:
    - Obtenha o perfil Arista NAD no link da Comunidade Cisco fornecido acima. Comunidade Cisco
2. Acesse o Cisco ISE:
    - Faça login no console administrativo do Cisco ISE
3. Importar o perfil NAD:
    - Navegue até Administration > Network Resources > Network Device Profiles.
    - Clique no botão Importar
    - Carregue o arquivo de perfil Arista NAD baixado.

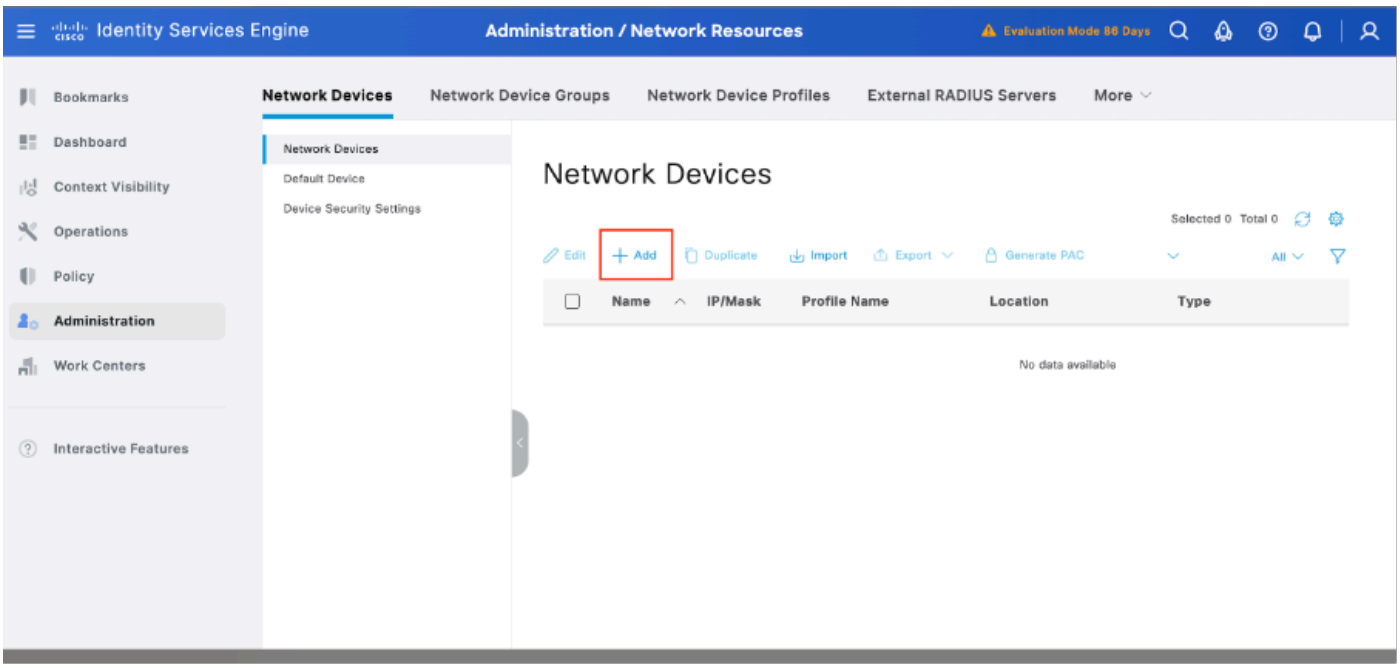


Após a conclusão do upload, navegue para a opção Edit e ative o TACACS+ como um protocolo suportado.



Passo 2: Adicione o switch Arista como um dispositivo de rede.

1. Navegue até Administração > Recursos de rede > Dispositivos de rede> +Adicionar:

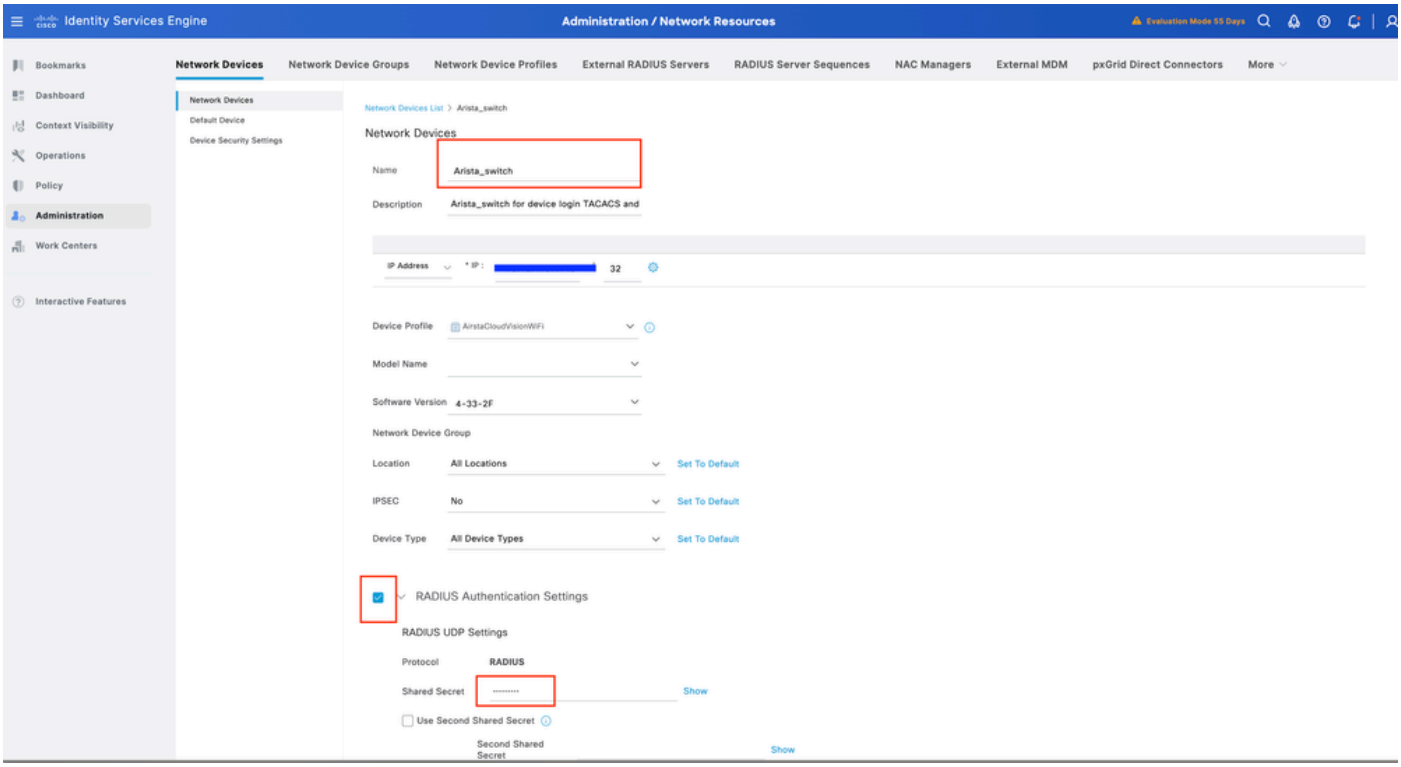


2.Clique em Adicionar e insira estes detalhes:

- Endereço IP: <Switch-IP>
- tipo de dispositivo: Escolha outro com fio
- Perfil do dispositivo de rede: selecione AirstaCloudVisionWiFi.

- Configurações de autenticação RADIUS:
  - Ative a autenticação RADIUS.
  - Insira o Shared Secret (deve corresponder à configuração do switch).

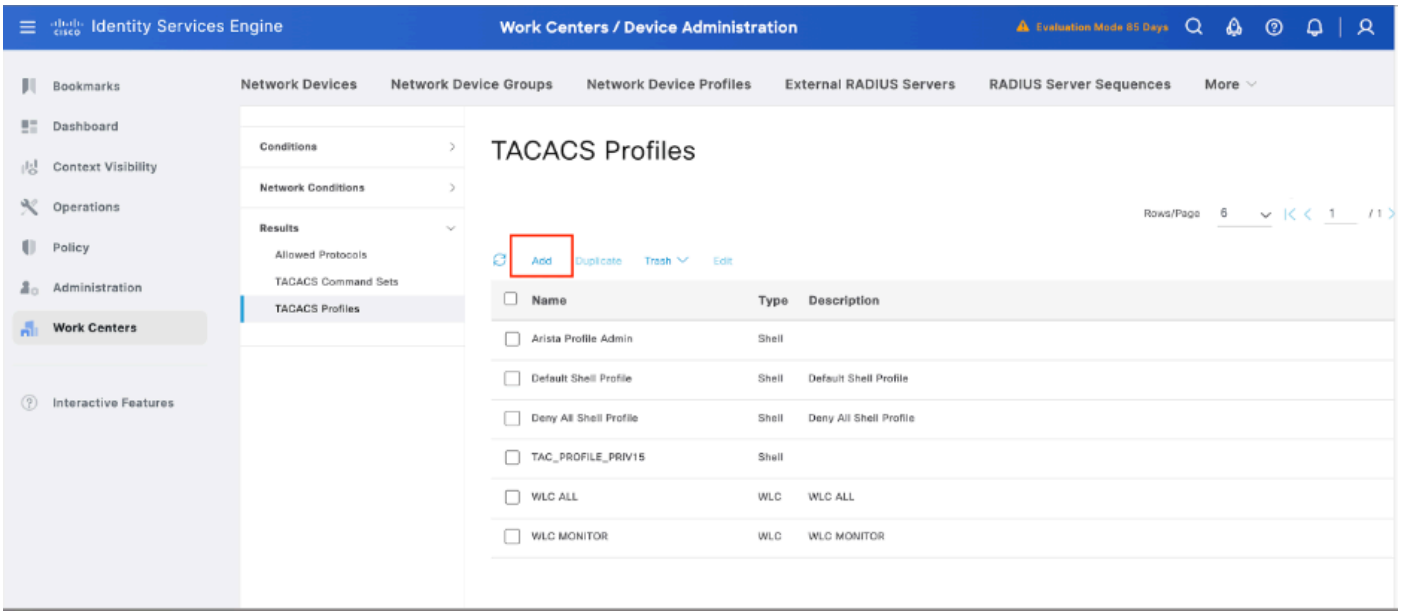
3. Clique em Salvar:



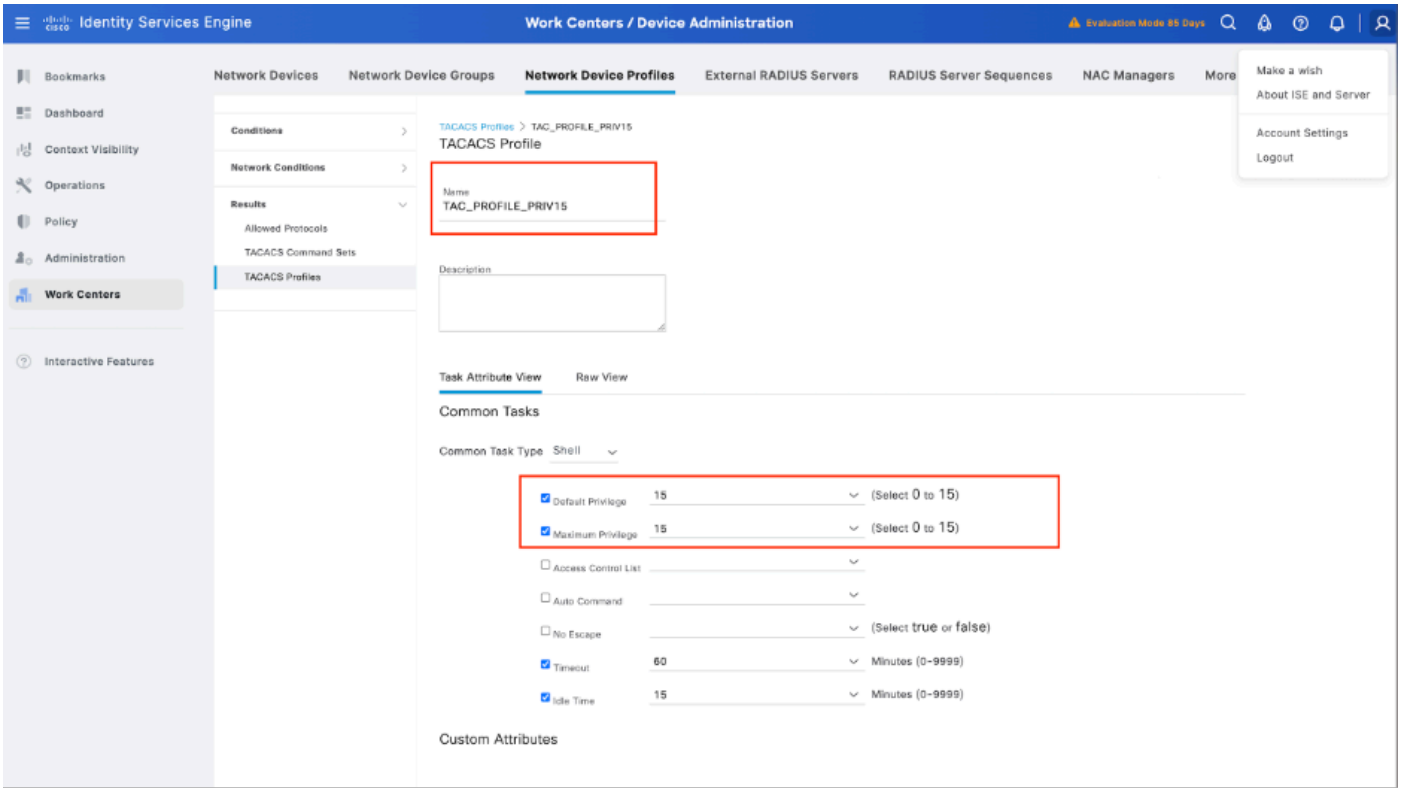
Etapa 3. Validar o novo dispositivo é mostrado em Dispositivos de rede:

Etapa 4. Configurar o perfil TACACS.

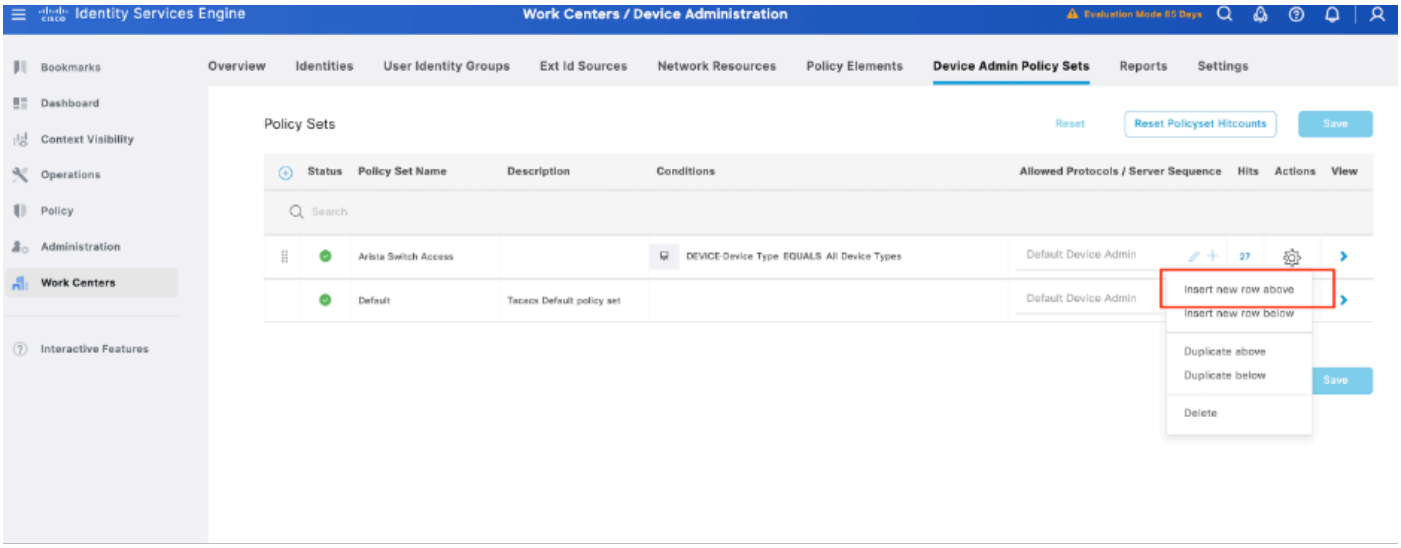
Crie um perfil TACACS, navegue até o menu Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Perfis TACACS e selecione Adicionar:



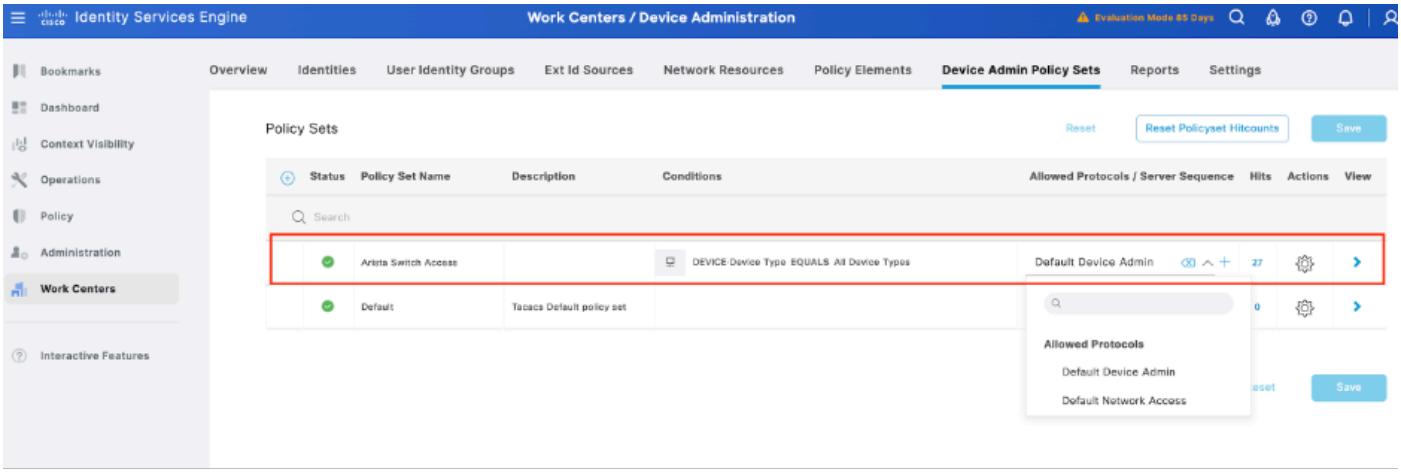
Insira um Nome, marque a caixa de seleção Privilégio Padrão e defina o valor como 15. Além disso, selecione Privilégio Máximo, defina seu valor como 15 e clique em Enviar:



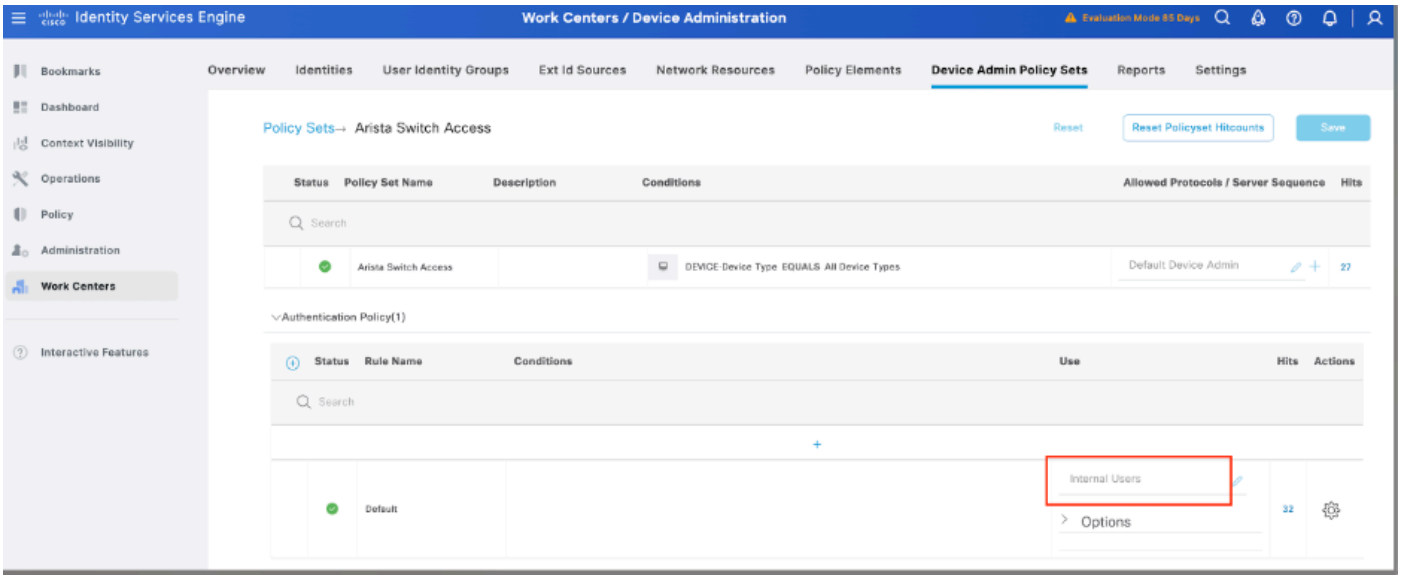
Etapa 5. Crie um Device Admin Policy Set a ser usado para seu Arista Switch, navegue para o menu Work Centers > Device Administration > Device Admin Policy Sets, em seguida, de um conjunto de políticas existente selecione o ícone de engrenagem para, em seguida, selecione Insert new row above.



Etapa 6. Nomeie este novo Conjunto de políticas, adicione condições dependendo das características das autenticações TACACS+ que estão em andamento no switch Arista e selecione Allowed Protocols > Default Device Admin, salve sua configuração.

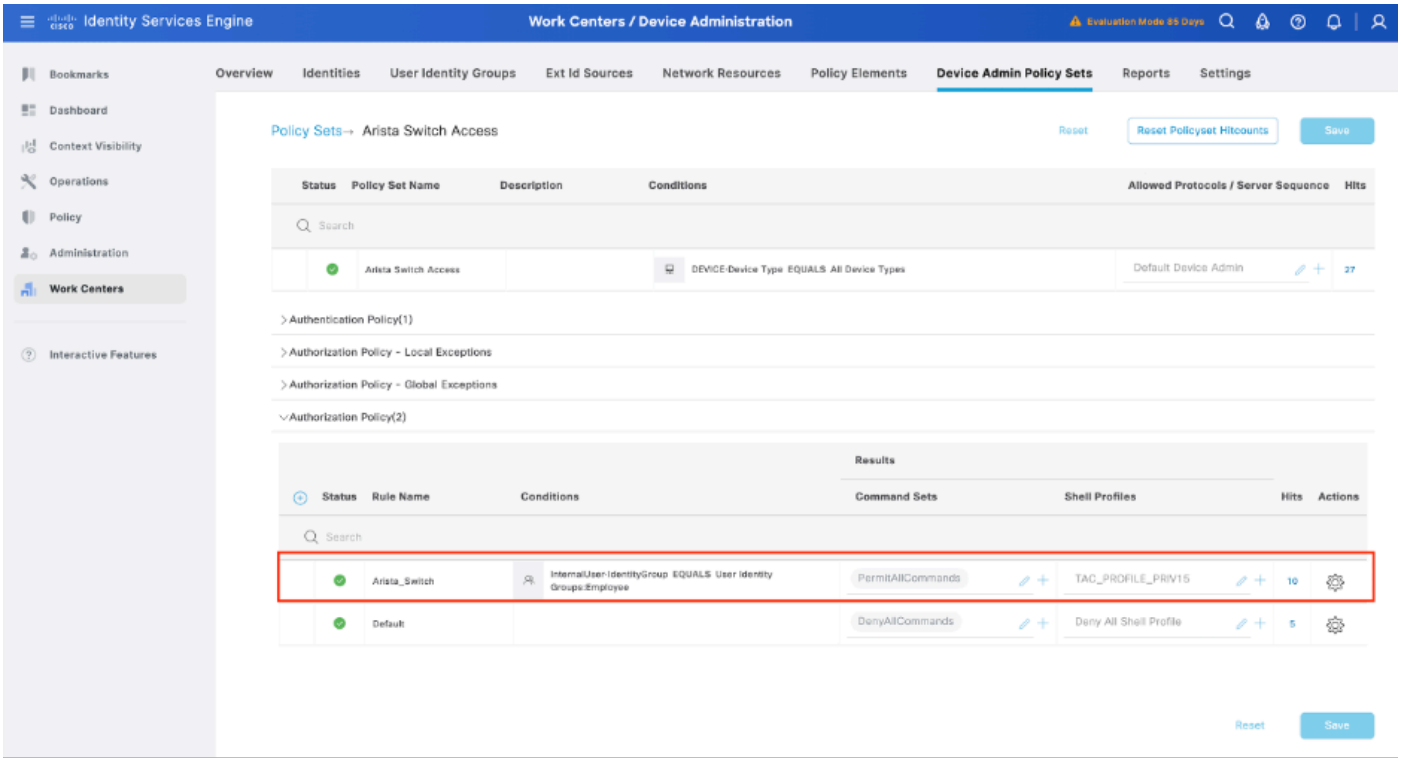


Etapa 7. Selecione na opção > view e, em seguida, na seção Authentication Policy, selecione a fonte de identidade externa que o Cisco ISE usa para consultar o nome de usuário e as credenciais para autenticação no switch Arista. Neste exemplo, as credenciais correspondem a Usuários internos armazenados no ISE.



Etapa 8. Role para baixo até a seção chamada Authorization Policy to Default policy, selecione o ícone de engrenagem e insira uma regra acima.

Etapa 9. Nomeie a nova Regra de Autorização, adicione condições referentes ao usuário que já está autenticado como membro do grupo e, na seção Perfis de shell adicione o perfil TACACS que você configurou anteriormente, salve a configuração.



Configurar o switch Arista

Etapa 1. Ativar a autenticação TACACS+

Faça login no switch Arista e entre no modo de configuração:

configurar

```
!
tacacs-server host <ISE-IP> key <TACACS-SECRET>
!
aaa group server tacacs+ ISE_TACACS
  server <ISE-IP>
!
aaa authentication login default group ISE_TACACS local
aaa authorization exec default group ISE_TACACS local
aaa accounting commands 15 default start-stop group ISE_TACACS
!
Fim
```

Etapa 2. Salvar a configuração

Para persistir a configuração nas reinicializações:

```
# write memory
```

OU

```
# copy running-config startup-config
```

Verificar

Revisão do ISE

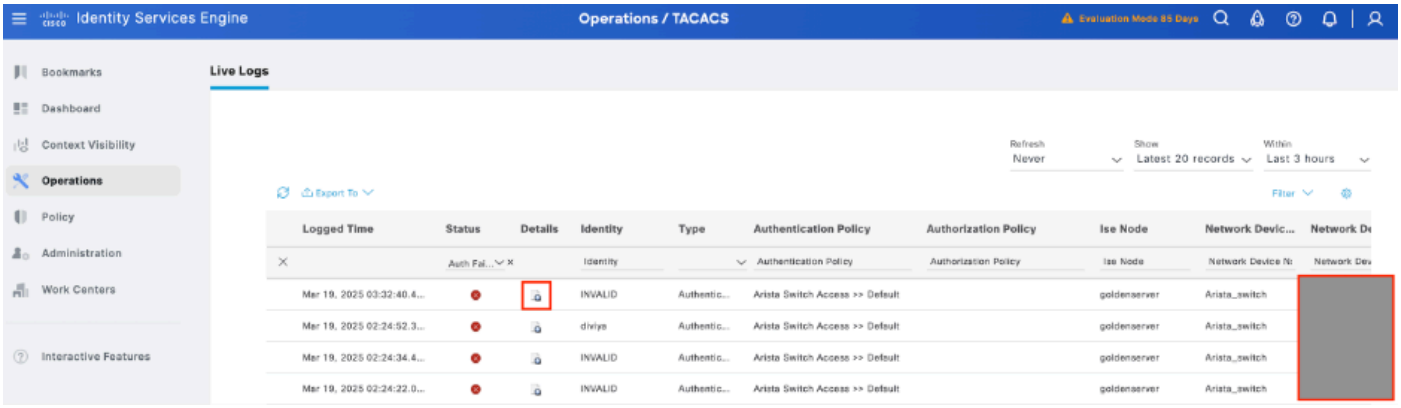
Etapa 1. Revise se se a capacidade de serviço TACACS+ está em execução, isso pode ser verificado em:

- GUI: Verifique se você tem o nó listado com o serviço DEVICE ADMIN em > Sistema > Implantação.
- CLI: Execute o comando show ports | incluir 49 para confirmar que há conexões na porta TCP que pertencem ao TACACS+

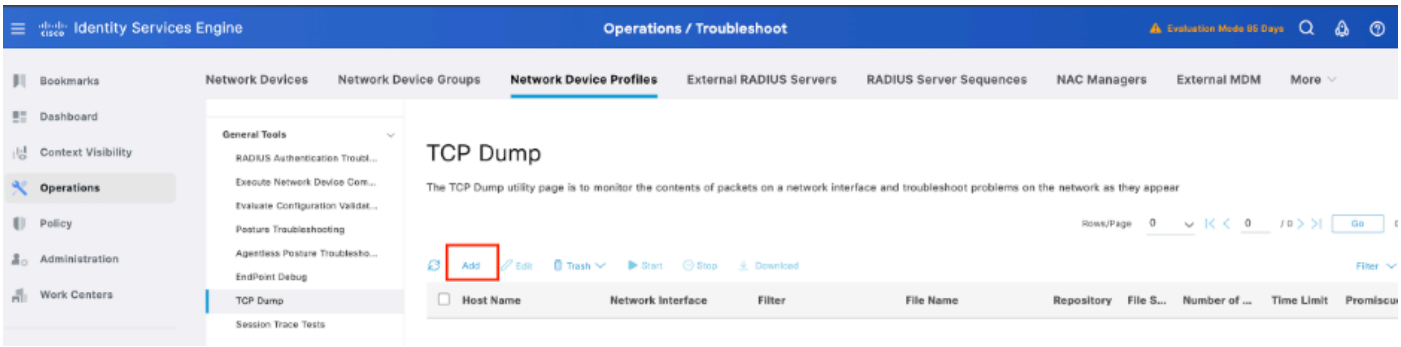
Etapa 2. Confirme se há registros em tempo real referentes a tentativas de autenticação

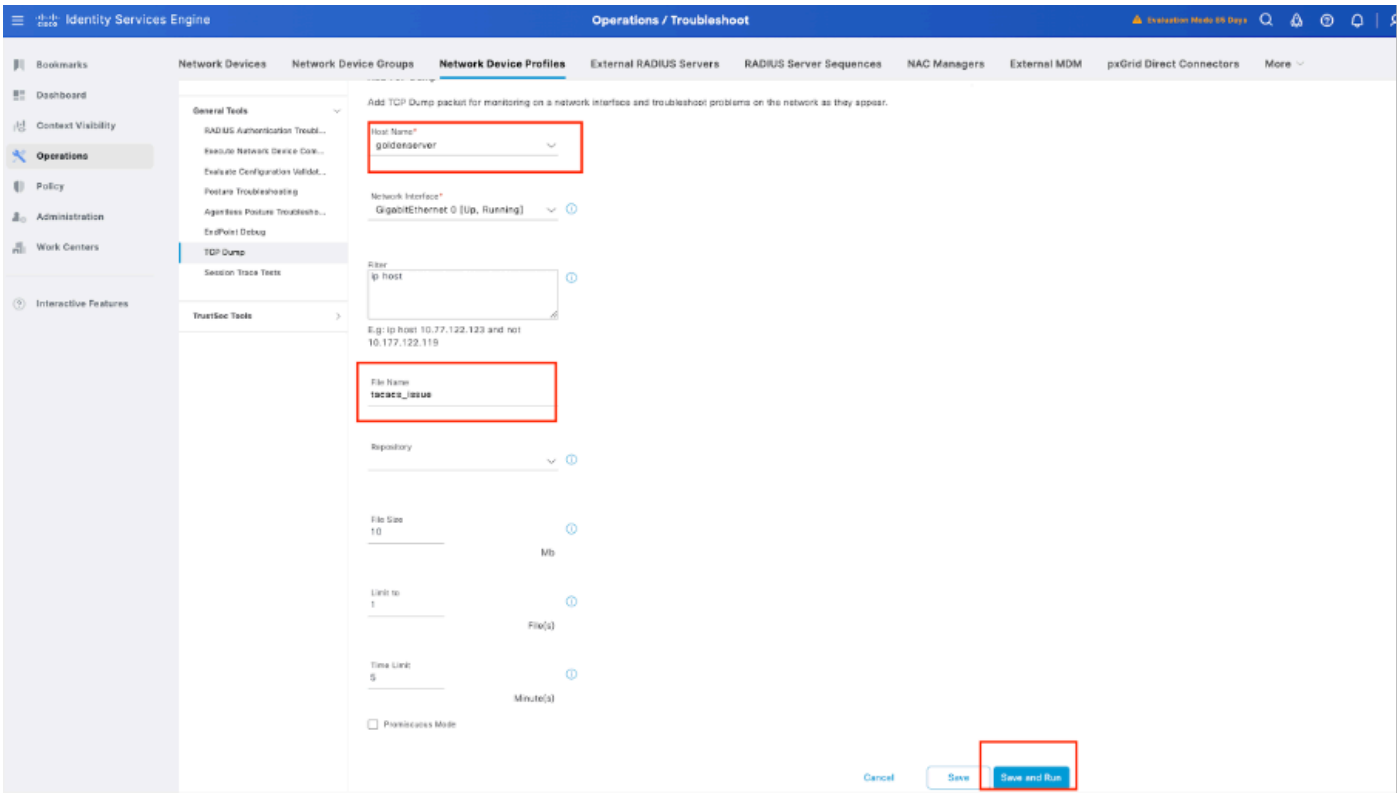
TACACS+ : isso pode ser verificado no menu Operations > TACACS > Live logs,

Dependendo do motivo da falha, você pode ajustar sua configuração ou tratar da causa da falha.

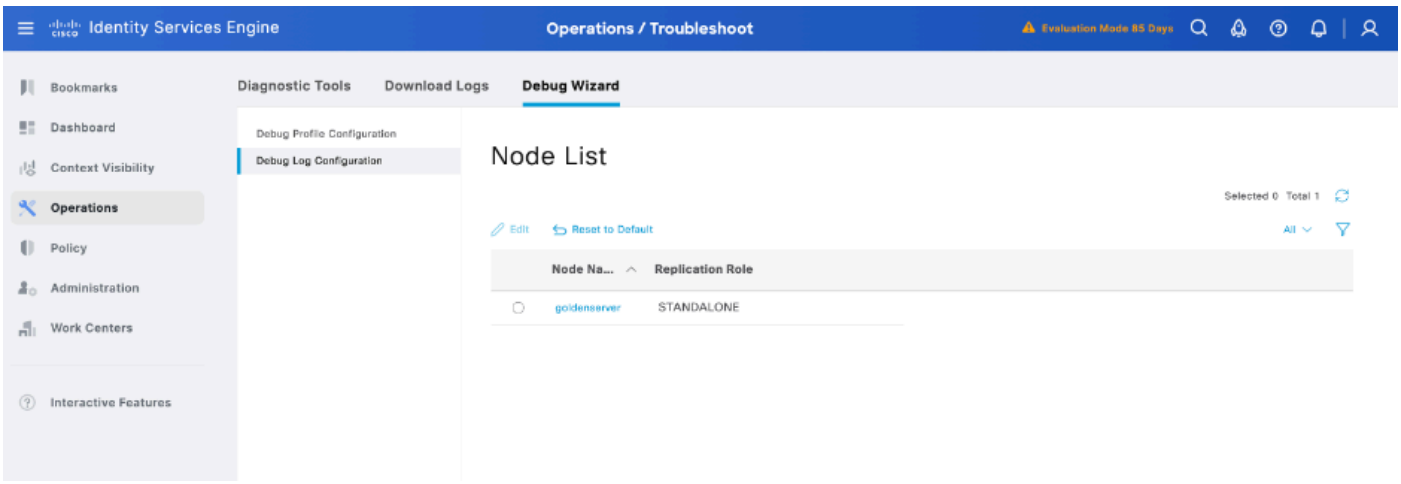


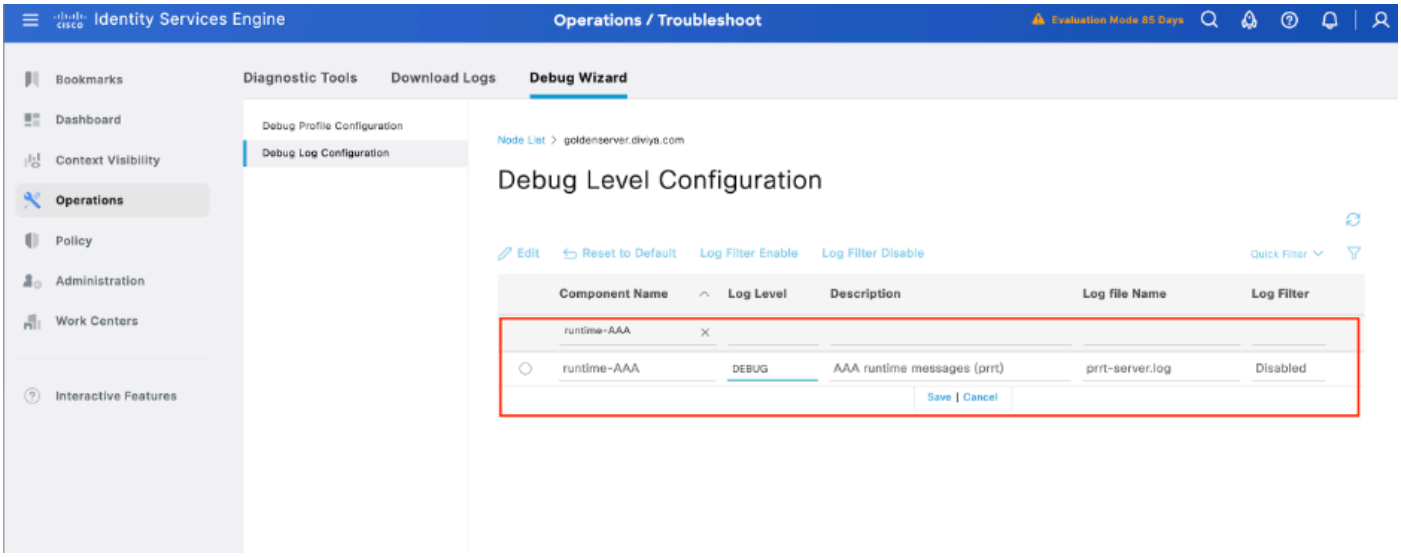
Etapa 3. Caso você não veja nenhum Livelog, continue para capturar um pacote. Navegue até o menu Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump , selecione Add:





Etapa 4. Ative o componente runtime-AAA na depuração dentro do PSN de onde a autenticação está sendo executada em Operações > Solução de problemas > Assistente de depuração > Configuração do log de depuração, selecione o nó PSN e, em seguida, selecione o botão Editar:





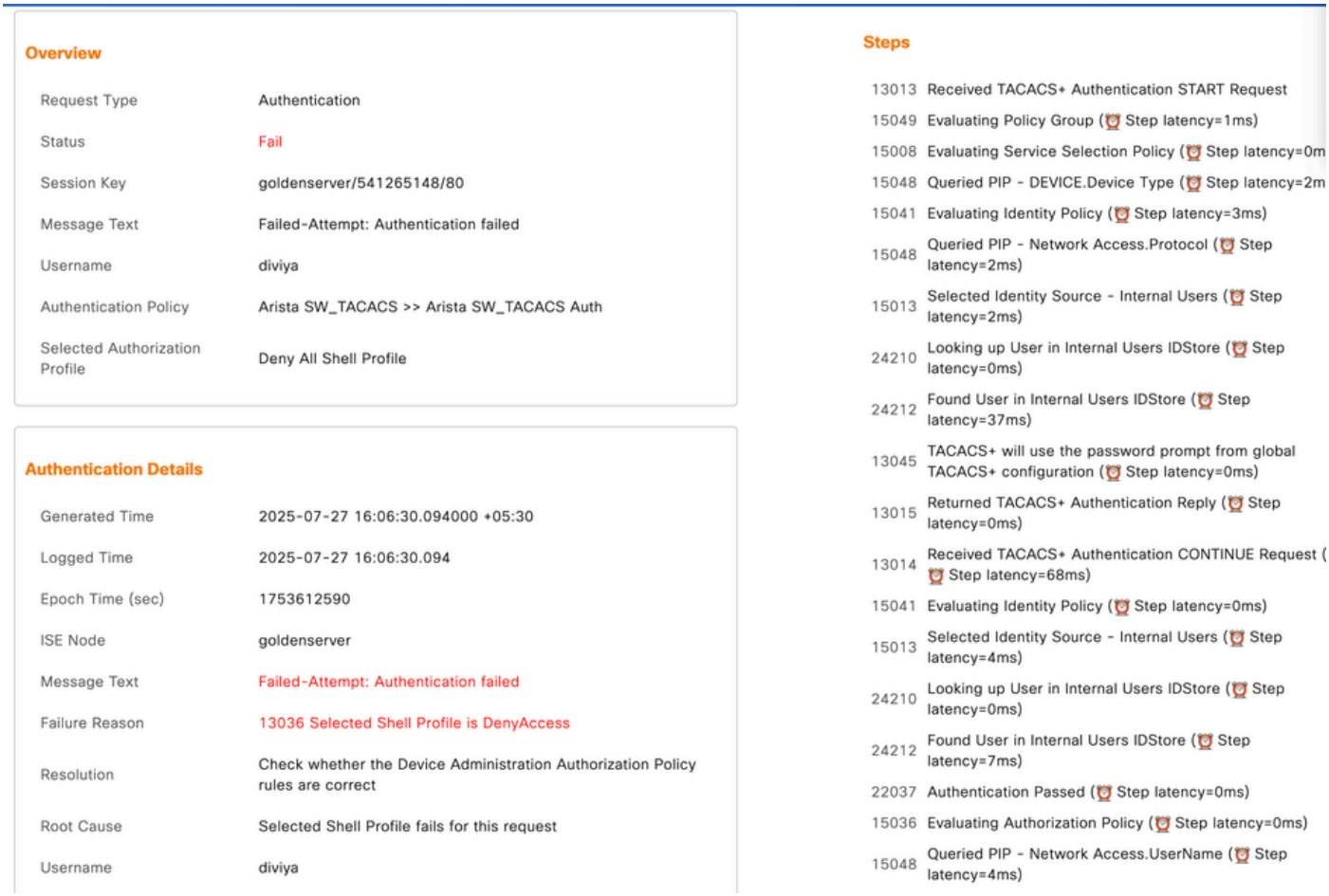
Identifique o componente runtime-AAA, defina seu nível de registro como debug, reproduza o problema e analise os registros para investigação adicional.

Troubleshooting

Problema 1

A autenticação TACACS+ entre o Cisco ISE e o switch Arista (ou qualquer dispositivo de rede) falha com a mensagem de erro:

"13036 perfil de shell selecionado é DenyAccess"



Overview

Request Type	Authentication
Status	Fail
Session Key	goldenserver/541265148/80
Message Text	Failed-Attempt: Authentication failed
Username	diviya
Authentication Policy	Arista SW_TACACS >> Arista SW_TACACS Auth
Selected Authorization Profile	Deny All Shell Profile

Authentication Details

Generated Time	2025-07-27 16:06:30.094000 +05:30
Logged Time	2025-07-27 16:06:30.094
Epoch Time (sec)	1753612590
ISE Node	goldenserver
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13036 Selected Shell Profile is DenyAccess
Resolution	Check whether the Device Administration Authorization Policy rules are correct
Root Cause	Selected Shell Profile fails for this request
Username	diviya

Steps

13013 Received TACACS+ Authentication START Request
15049 Evaluating Policy Group (Step latency=1ms)
15008 Evaluating Service Selection Policy (Step latency=0m
15048 Queried PIP - DEVICE.Device Type (Step latency=2m
15041 Evaluating Identity Policy (Step latency=3ms)
15048 Queried PIP - Network Access.Protocol (Step latency=2ms)
15013 Selected Identity Source - Internal Users (Step latency=2ms)
24210 Looking up User in Internal Users IDStore (Step latency=0ms)
24212 Found User in Internal Users IDStore (Step latency=37ms)
13045 TACACS+ will use the password prompt from global TACACS+ configuration (Step latency=0ms)
13015 Returned TACACS+ Authentication Reply (Step latency=0ms)
13014 Received TACACS+ Authentication CONTINUE Request (Step latency=68ms)
15041 Evaluating Identity Policy (Step latency=0ms)
15013 Selected Identity Source - Internal Users (Step latency=4ms)
24210 Looking up User in Internal Users IDStore (Step latency=0ms)
24212 Found User in Internal Users IDStore (Step latency=7ms)
22037 Authentication Passed (Step latency=0ms)
15036 Evaluating Authorization Policy (Step latency=0ms)
15048 Queried PIP - Network Access.UserName (Step latency=4ms)

O erro "13036 perfil de shell selecionado é DenyAccess" no Cisco ISE geralmente significa que, durante uma tentativa de administração de dispositivo TACACS+, a política de autorização correspondeu a um perfil de shell definido como DenyAccess. Geralmente, isso não é resultado de um perfil de shell configurado incorretamente em si, mas indica que nenhuma das regras de autorização configuradas correspondeu aos atributos de usuário de entrada (como associação de grupo, tipo de dispositivo ou local). Como resultado, o ISE volta para uma regra padrão ou uma regra de negação explícita, resultando no acesso negado.

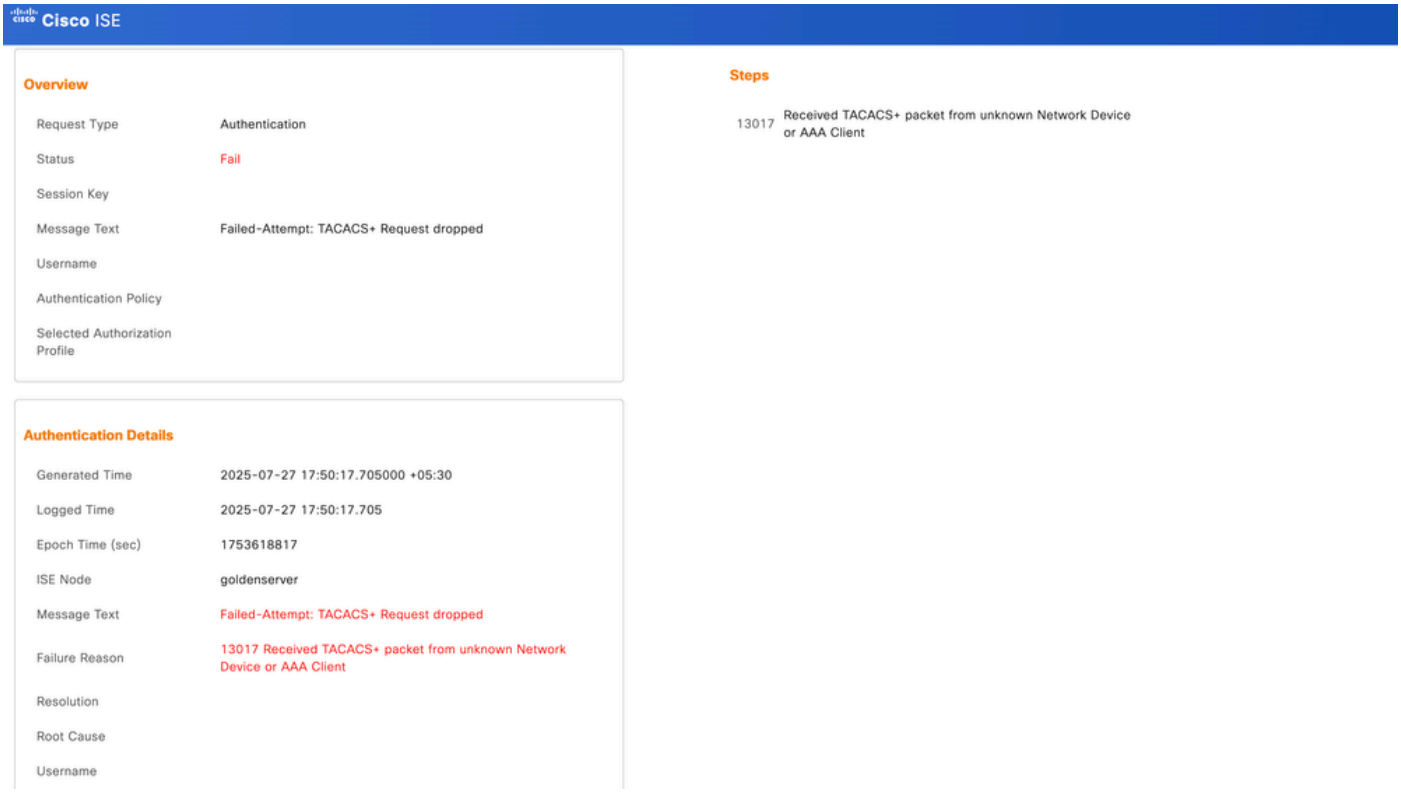
Possíveis causas

- Revise as regras da política de autorização no ISE. Confirme se o usuário ou dispositivo corresponde à regra correta que atribui o perfil de shell desejado, como um que permita acesso apropriado.
- Verifique se o AD ou o mapeamento do grupo de usuários interno está correto e se as condições da política, como associação do grupo de usuários, tipo de dispositivo e protocolo, estão especificadas com precisão.
- Use os logs ao vivo do ISE e os detalhes da tentativa com falha para ver exatamente qual regra é correspondida e por quê.

Problema 2

A autenticação TACACS+ entre o Cisco ISE e o switch Arista (ou qualquer dispositivo de rede) falha com a mensagem de erro:

"13017 pacote TACACS+ recebido de dispositivo de rede desconhecido ou cliente AAA"



Possíveis causas

- O motivo mais comum é que o endereço IP do switch não é adicionado como um dispositivo de rede no ISE (em Administração > Recursos de rede > Dispositivos de rede).
- Certifique-se de que o endereço IP ou intervalo corresponda exatamente ao IP de origem que está sendo usado pelo switch Arista para enviar pacotes TACACS+.
- Se o switch usar uma interface de gerenciamento, verifique se o IP exato (não apenas uma sub-rede/intervalo) foi adicionado ao ISE.

Solução

- Vá para Administração > Recursos de rede > Dispositivos de rede na GUI do ISE.
- Verifique se o endereço IP de origem exato no switch Arista está usando para comunicação TACACS+ (geralmente o IP da interface de gerenciamento).
- Especifique o segredo compartilhado (ele deve corresponder ao que está definido no switch Arista).

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.