Configurar a autorização do comando de autenticação TACACS+ do ISE 2.0

Contents

Introduction

Este documento descreve como configurar a Autenticação TACACS+ e a Autorização de Comando com base na associação de grupo do Microsoft Ative Diretory (AD).

Informações de Apoio

Para configurar a Autenticação TACACS+ e a Autorização de Comando com base na associação de grupo do Microsoft Ative Diretory (AD) de um usuário com o Identity Service Engine (ISE) 2.0 e posterior, o ISE usa o AD como um armazenamento de identidade externo para armazenar recursos como usuários, máquinas, grupos e atributos.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O roteador Cisco IOS está totalmente operacional
- Conectividade entre o roteador e o ISE.
- O servidor ISE é inicializado e tem conectividade com o Microsoft AD

Componentes Utilizados

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

- Cisco Identity Service Engine 2.0
- Software Cisco IOS® versão 15.4(3)M3
- Microsoft Windows Server 2012 R2

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

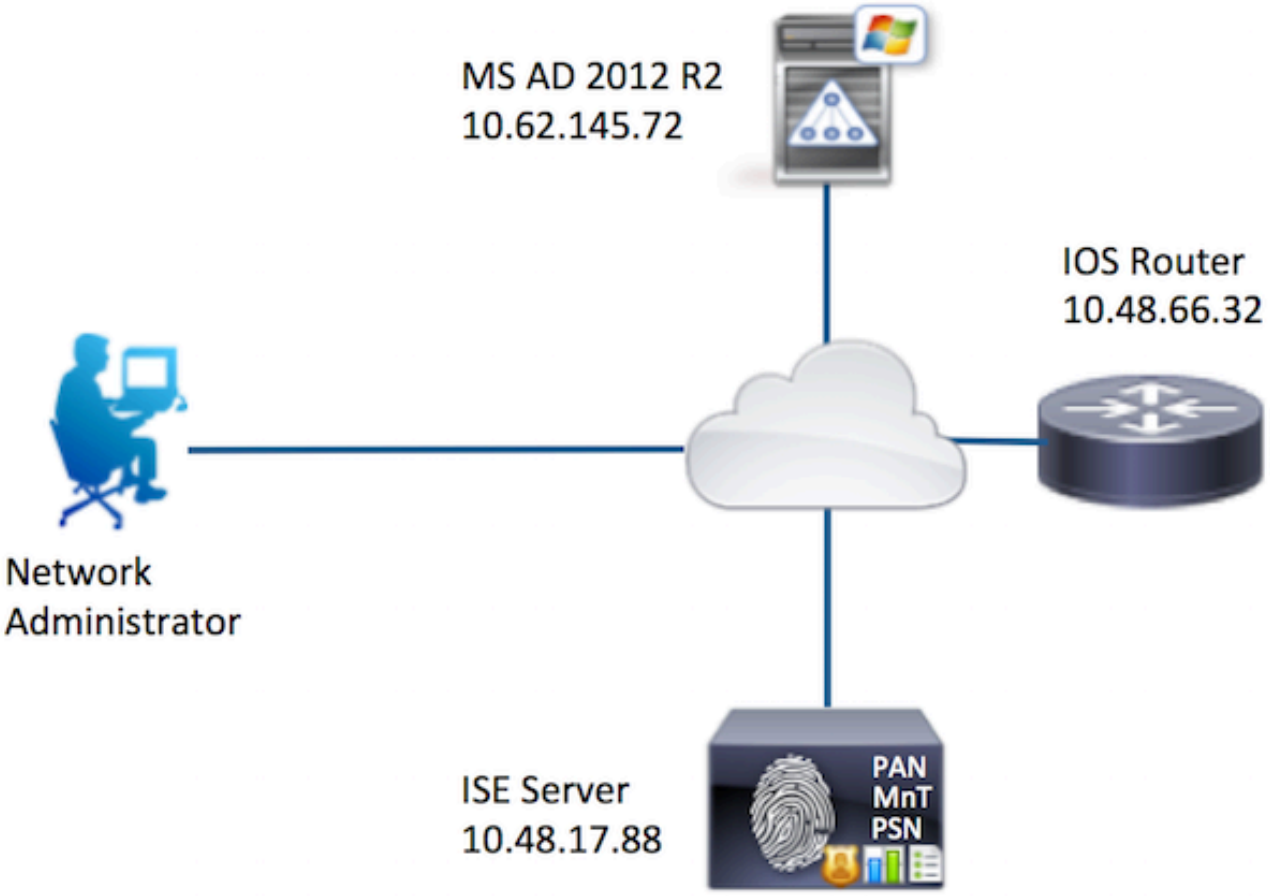
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

O objetivo da configuração é:

- Autenticar usuário telnet via AD
- Autorize o usuário telnet para que ele seja colocado no modo EXEC privilegiado após o login
- Verificar e enviar todos os comandos executados ao ISE para verificação

Diagrama de Rede

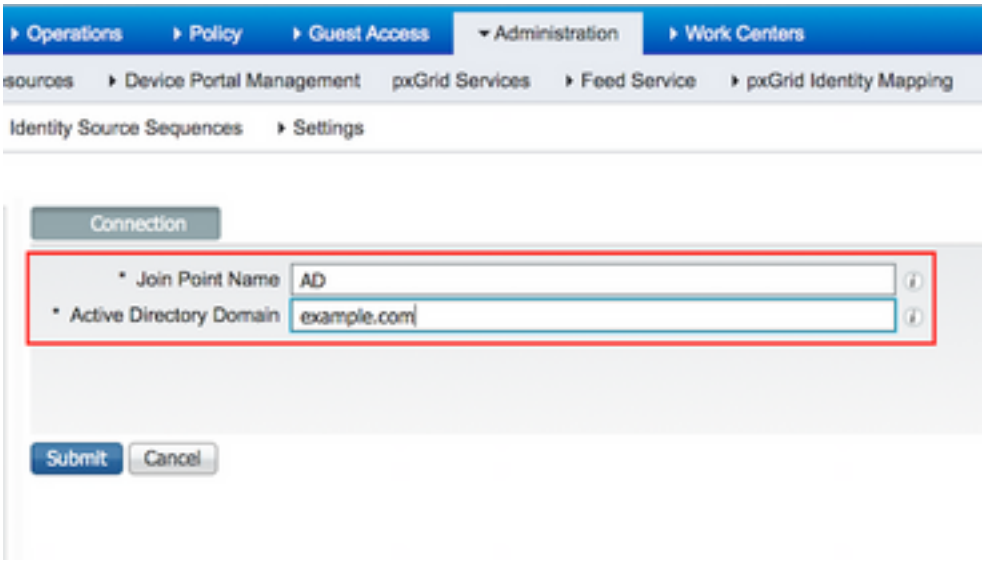


Configurações

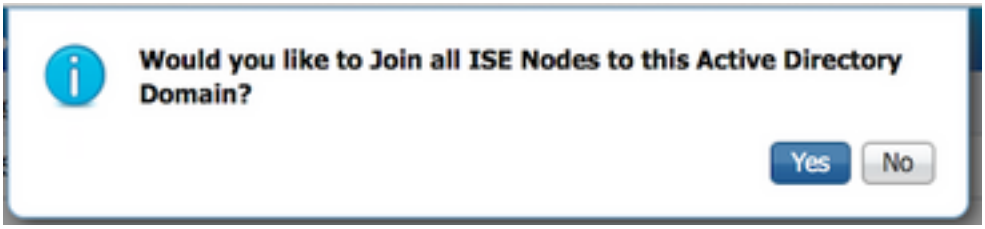
Configurar o ISE para autenticação e autorização

Junte o ISE 2.0 ao Ative Diretory

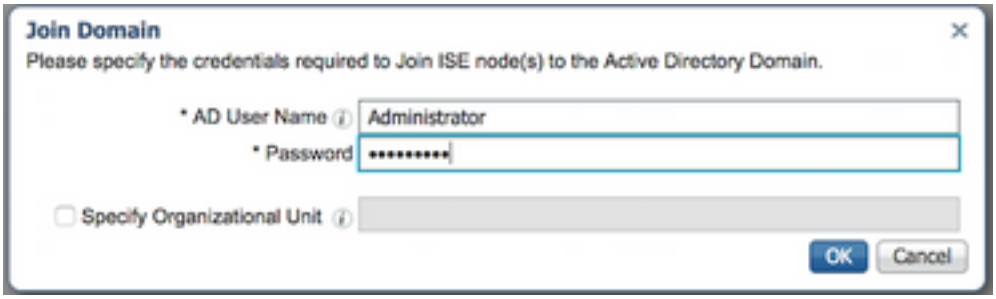
1. Navegue até **Administração > Gerenciamento de identidades > Repositórios de identidades externos > Ative Diretory > Adicionar**. Forneça o Join Point Name (Nome do ponto de ingresso), Ative Diretory Domain (Domínio do Ative Diretory) e clique em **Submit (Enviar).**



2. Quando for solicitado a Ingressar em todos os Nós do ISE neste Domínio do Ative Diretory, clique em **Sim.**



3. Forneça o Nome de usuário e a Senha do AD e clique em **OK**.

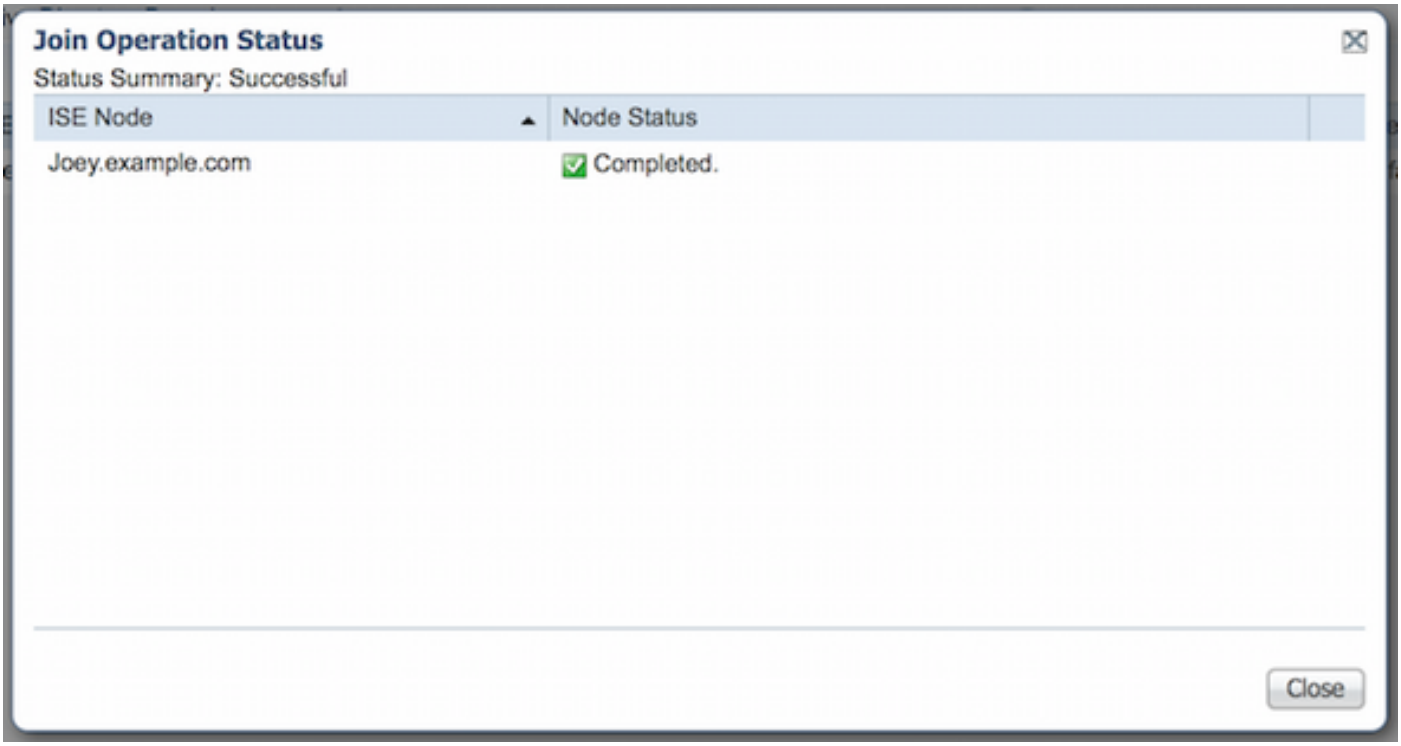


A conta do AD necessária para acesso ao domínio no ISE pode ter um destes:

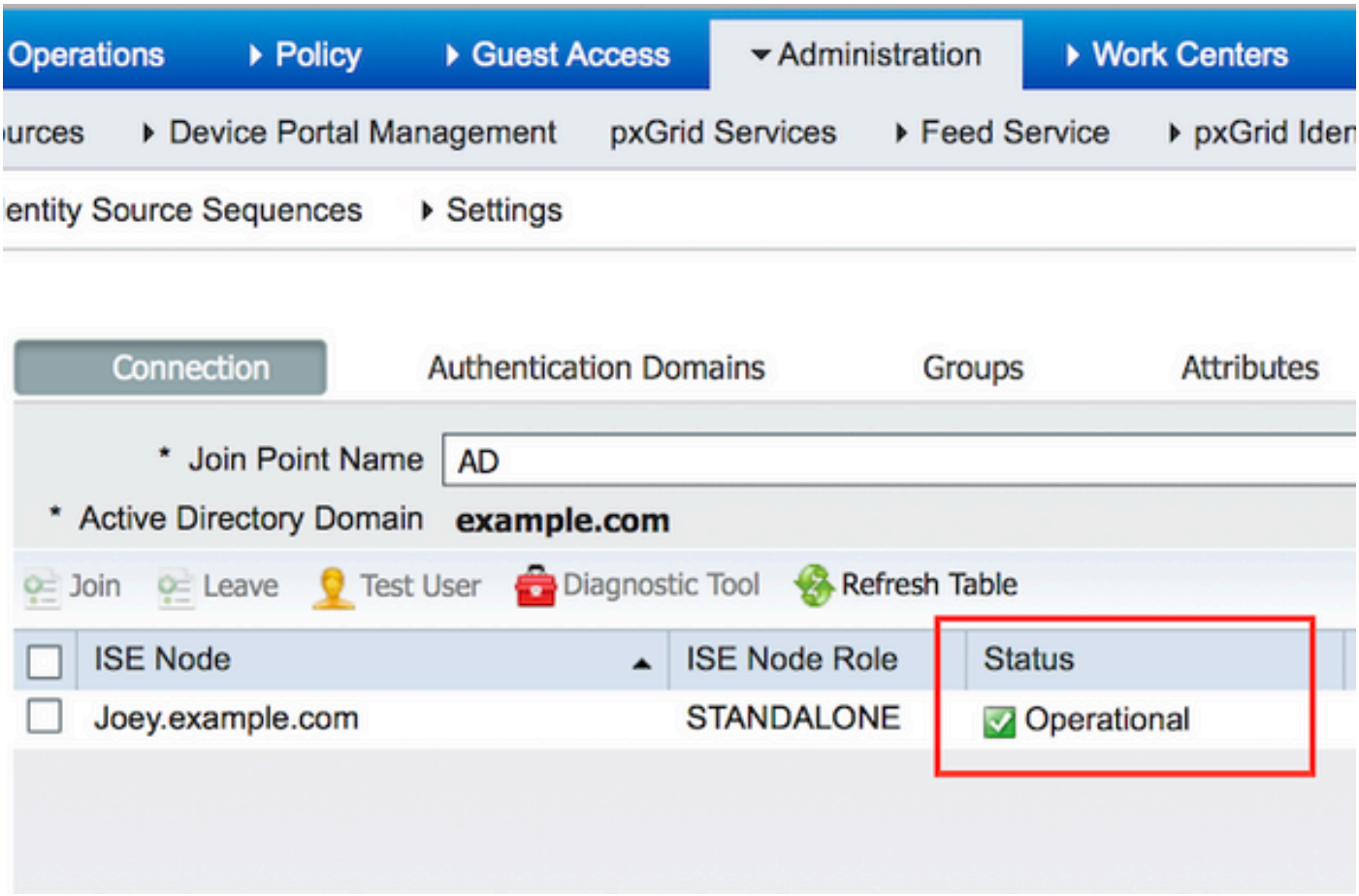
- Adicionar estações de trabalho ao domínio do direito do usuário no respectivo domínio
- Criar Objetos do Computador ou Excluir Objetos do Computador no respectivo contêiner de computadores onde a conta da máquina do ISE é criada antes de ela ingressar na máquina do ISE para o domínio

Note: A Cisco recomenda desabilitar a política de bloqueio para a conta do ISE e configurar a infraestrutura do AD para enviar alertas ao administrador se uma senha incorreta for usada para essa conta. Quando a senha incorreta é inserida, o ISE não cria nem modifica sua conta de máquina quando necessário e, portanto, possivelmente nega todas as autenticações.

4. Revise o Status da Operação. O Status do Nó deve aparecer como Concluído. Clique em Close.



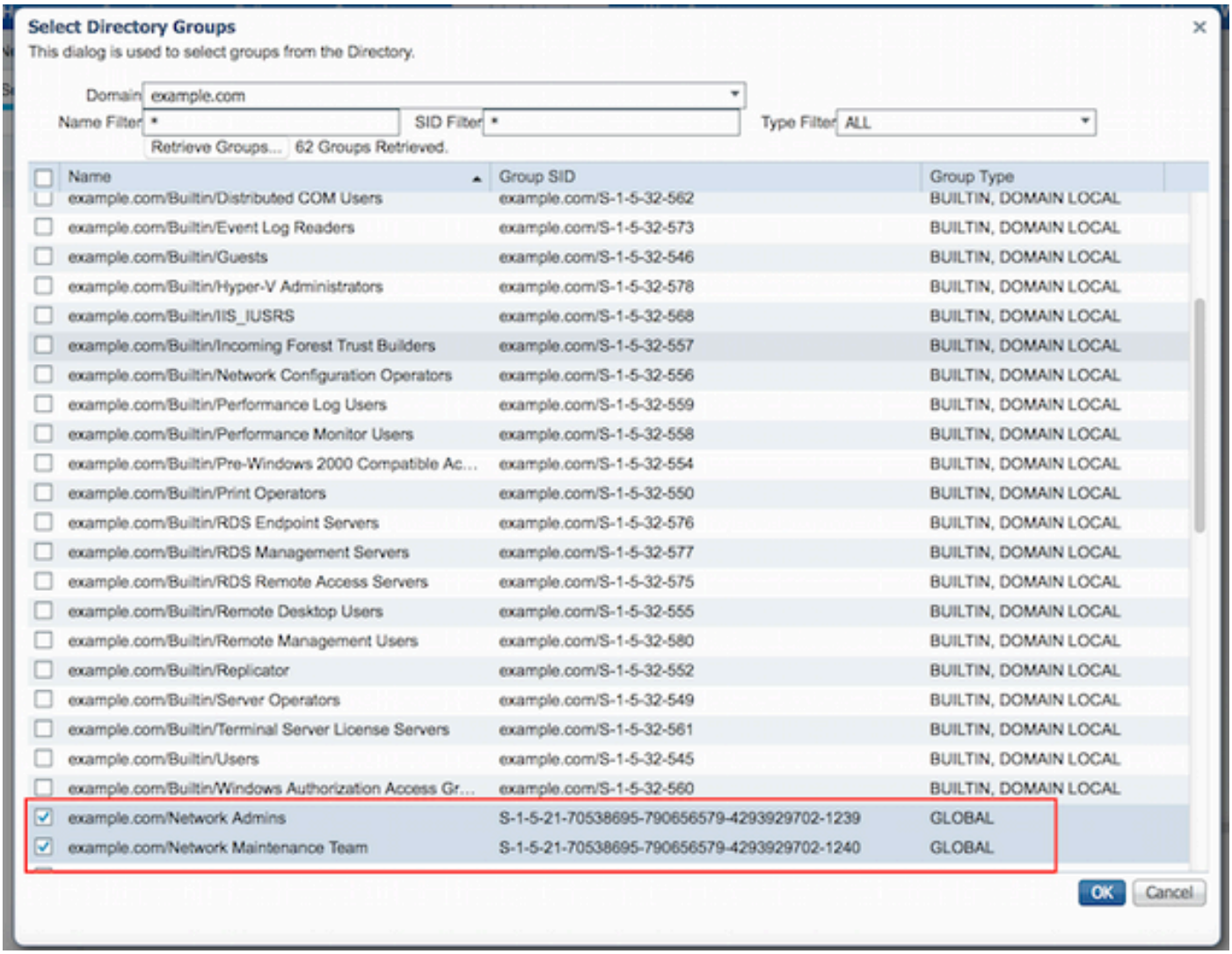
5. O status do AD é Operacional.



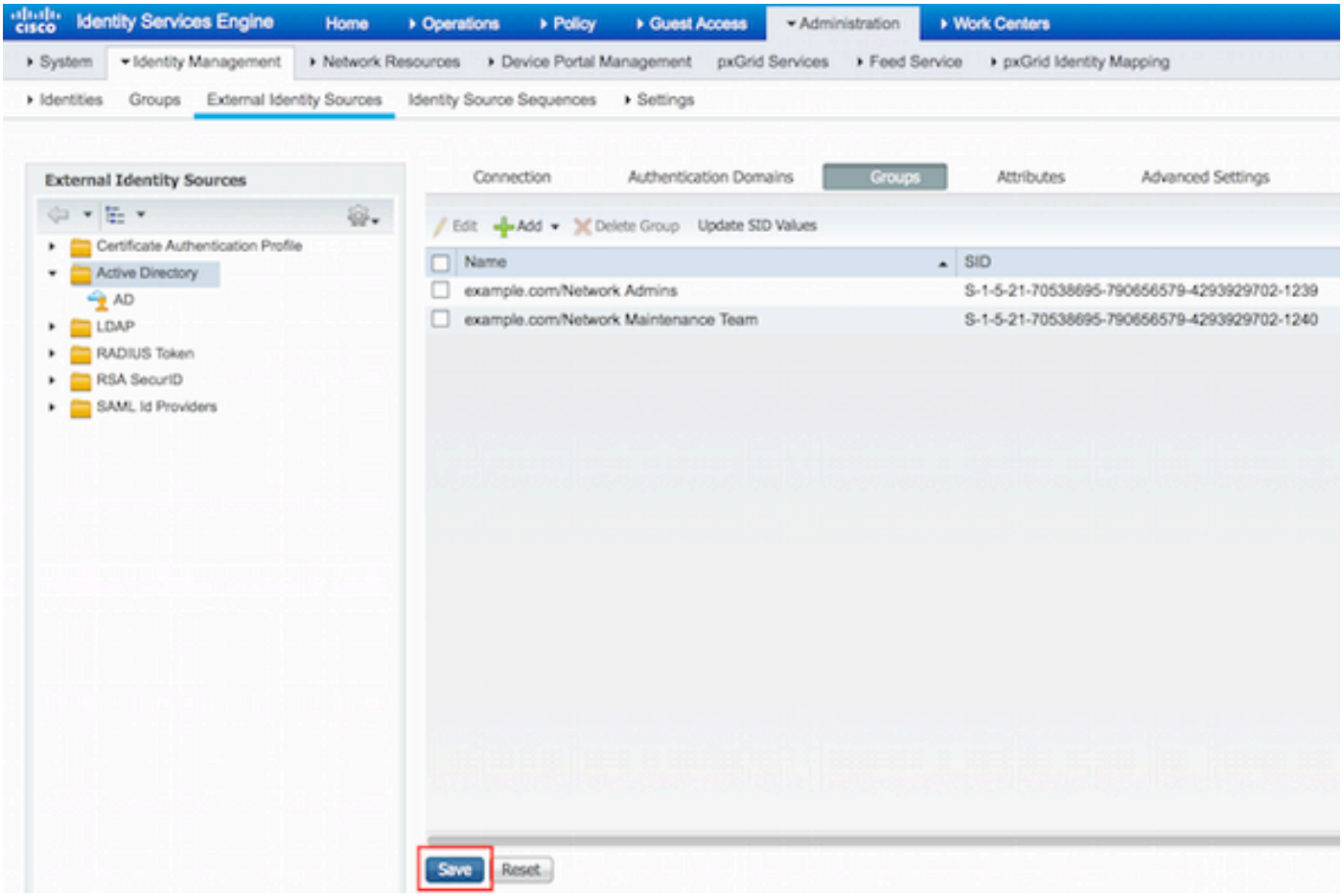
6. Navegue até **Groups > Add > Select Groups From Diretory > Retrieve Groups.** Marque as caixas de seleção **Administradores de rede** Grupo AD e **Equipe de manutenção de rede** Grupo AD, como mostrado nesta imagem.

> **Note**: O usuário admin é membro do grupo AD de administradores de rede. Este usuário tem privilégios de acesso total. Este usuário é membro do Grupo AD da Equipe de

Manutenção de Rede. Este usuário pode executar apenas comandos show.

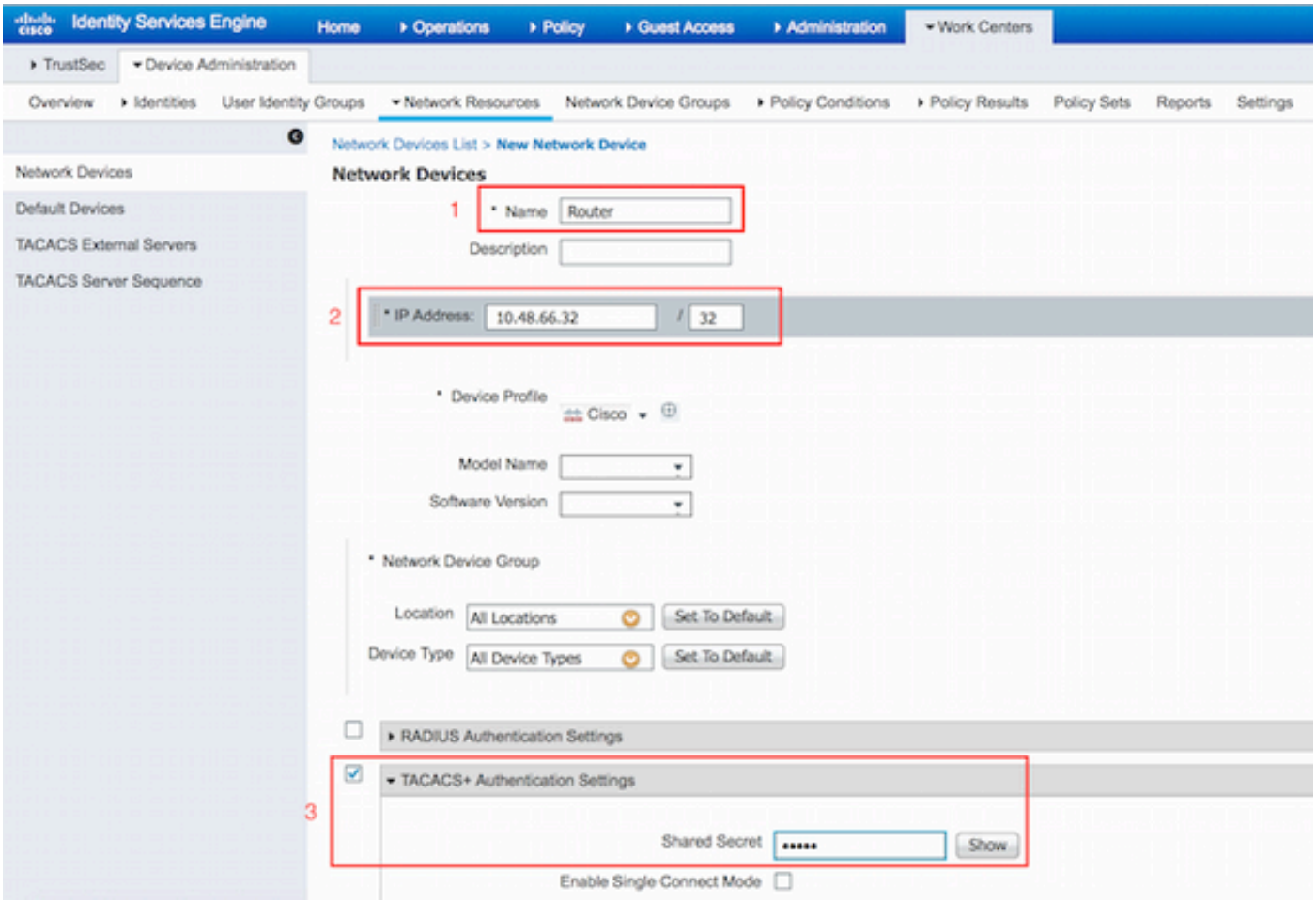


7. Clique em **Salvar** para salvar os Grupos do AD recuperados.



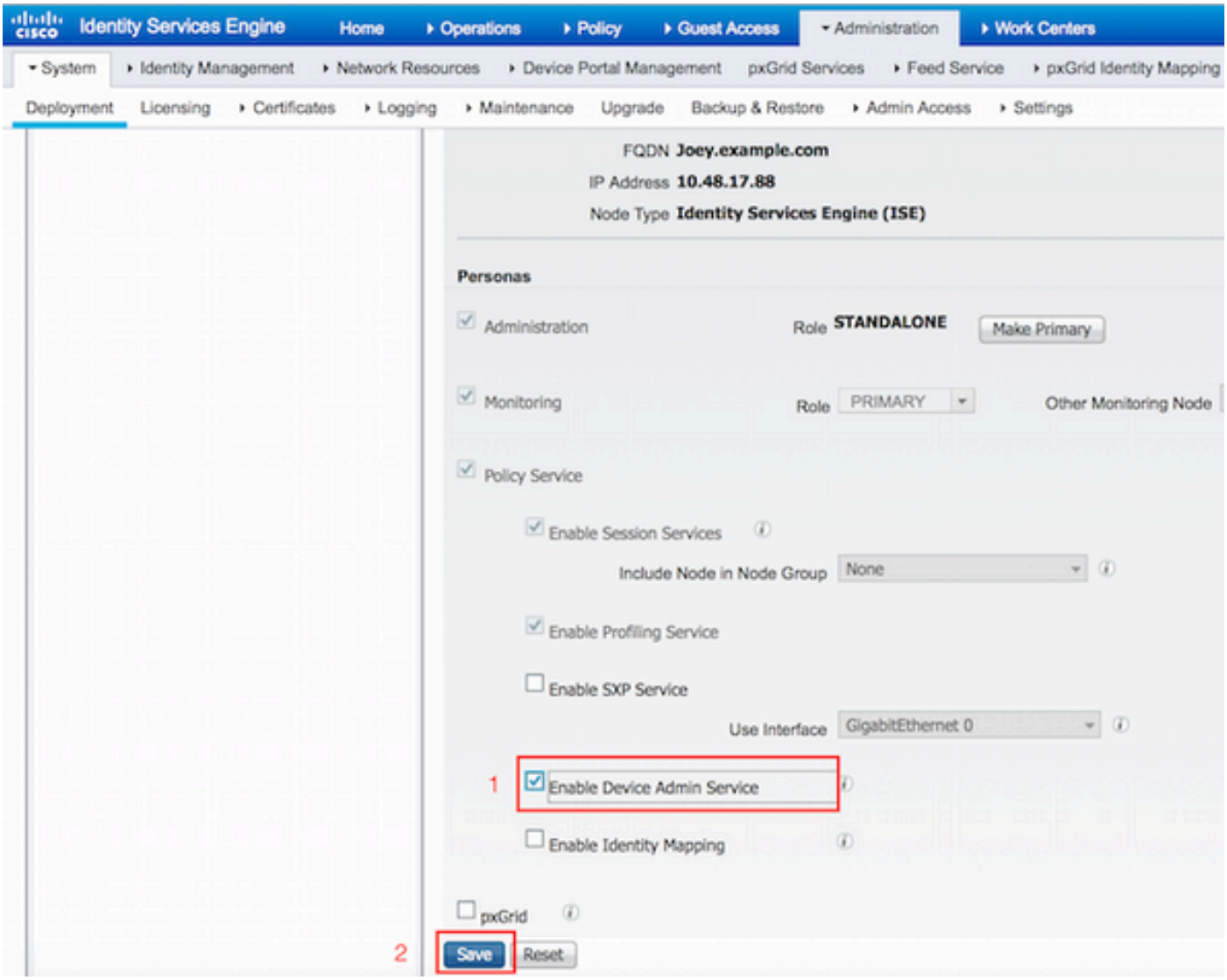
Adicionar dispositivo de rede

Navegue até **Centros de trabalho > Administração de dispositivos > Recursos de rede > Dispositivos de rede**. Clique em Add. Forneça Name, IP Address, marque a caixa de seleção **TACACS+ Authentication Settings** e forneça Shared Secret key.



Habilitar Serviço de Administração de Dispositivo

Navegue até **Administração > Sistema > Implantação.** Escolha o Nó necessário. Marque a caixa de seleção **Enable Device Admin Service** e clique em **Save.**

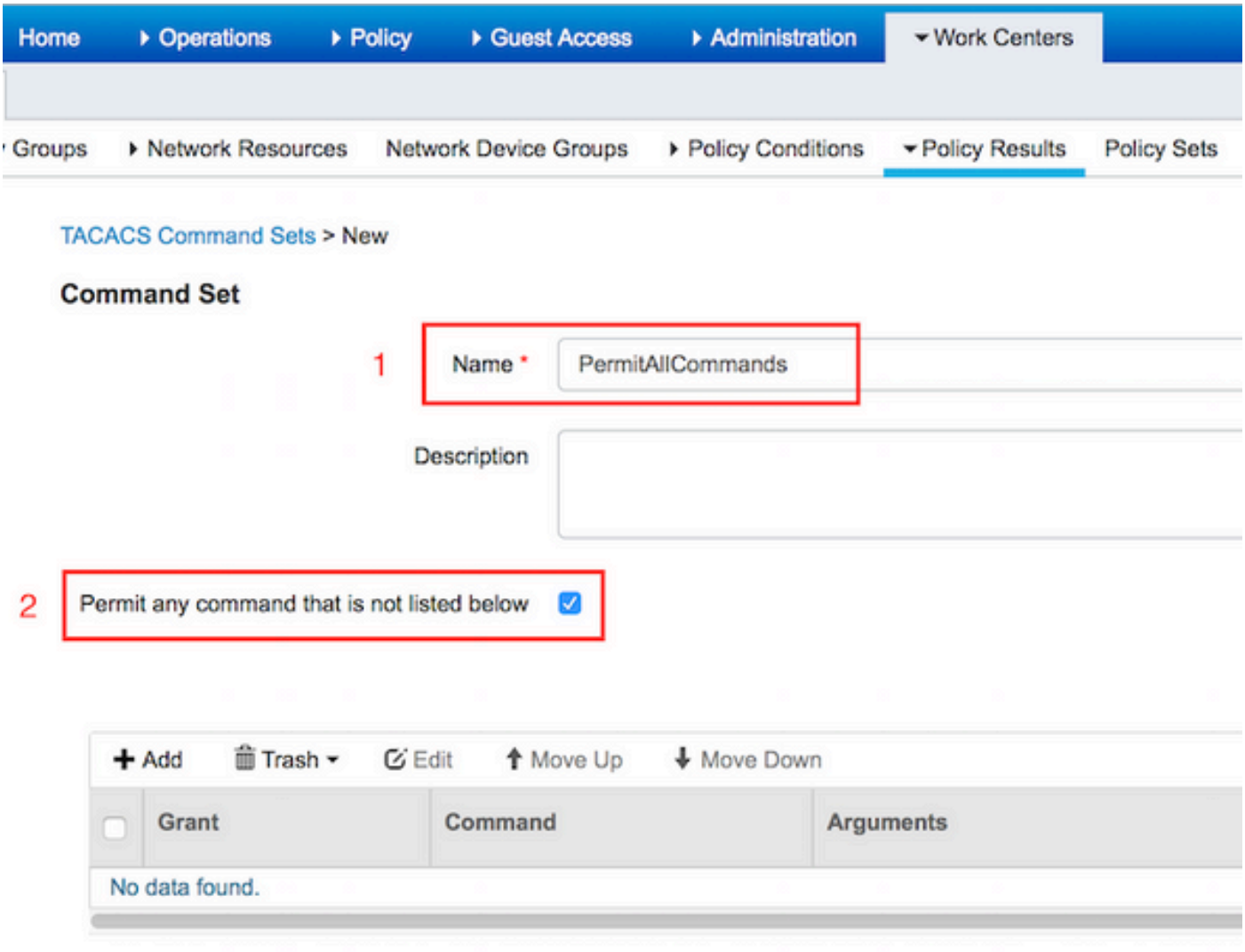


Note: Para o TACACS, você precisa ter licenças separadas instaladas.

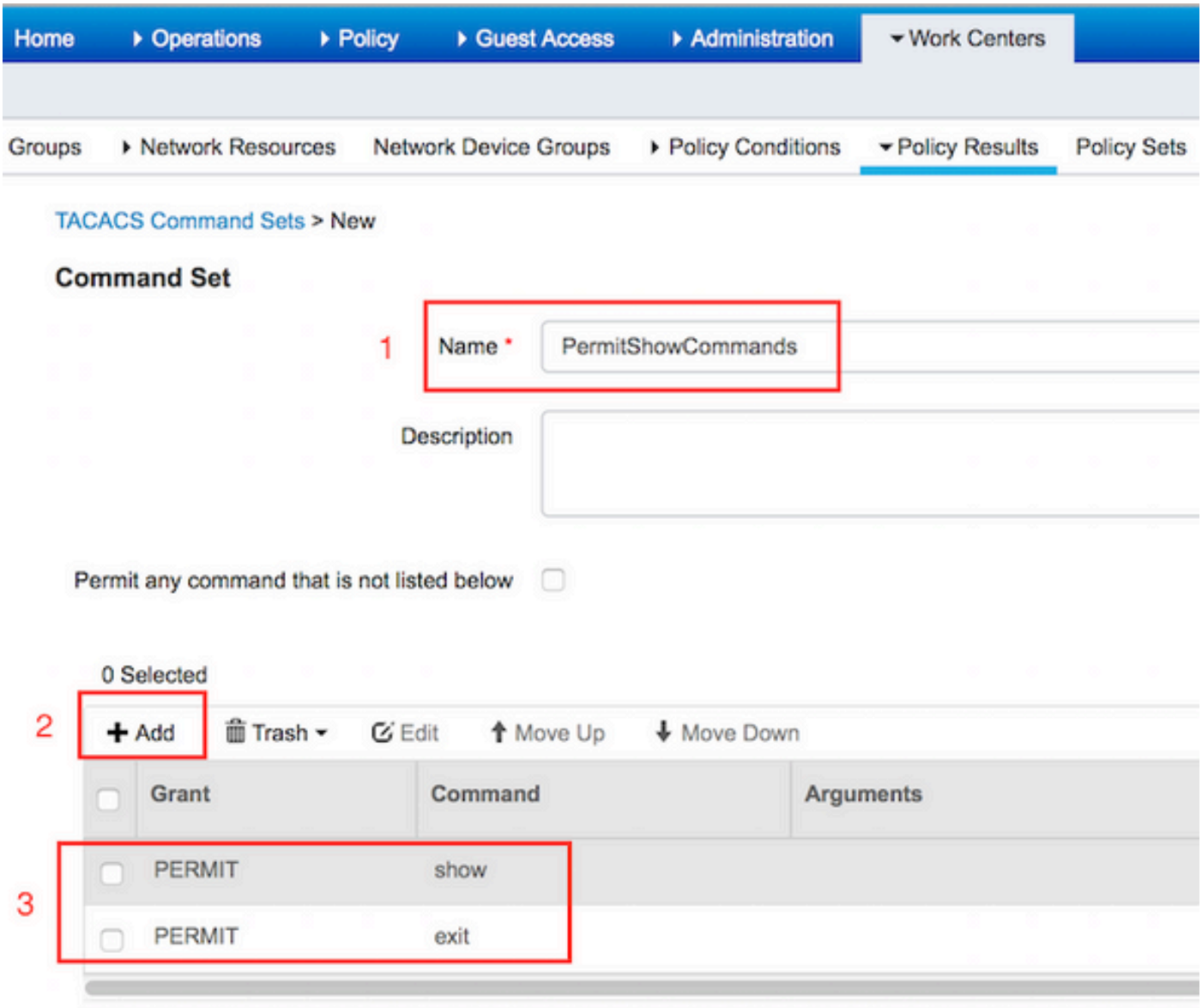
Configurar conjuntos de comandos TACACS

Dois conjuntos de comandos estão configurados. Primeiro **PermitAllCommands** para o administrador do usuário, que permite todos os comandos no dispositivo. Segundo **PermitShowCommands** para usuário que permite apenas comandos show.

1. Navegue até **Centros de trabalho > Administração de dispositivo > Resultados de política > Conjuntos de comandos TACACS.** Clique em Add. Forneça o nome **PermitAllCommands**, escolha a caixa de seleção **Permit any command** que não esteja listada e clique em **Enviar.**

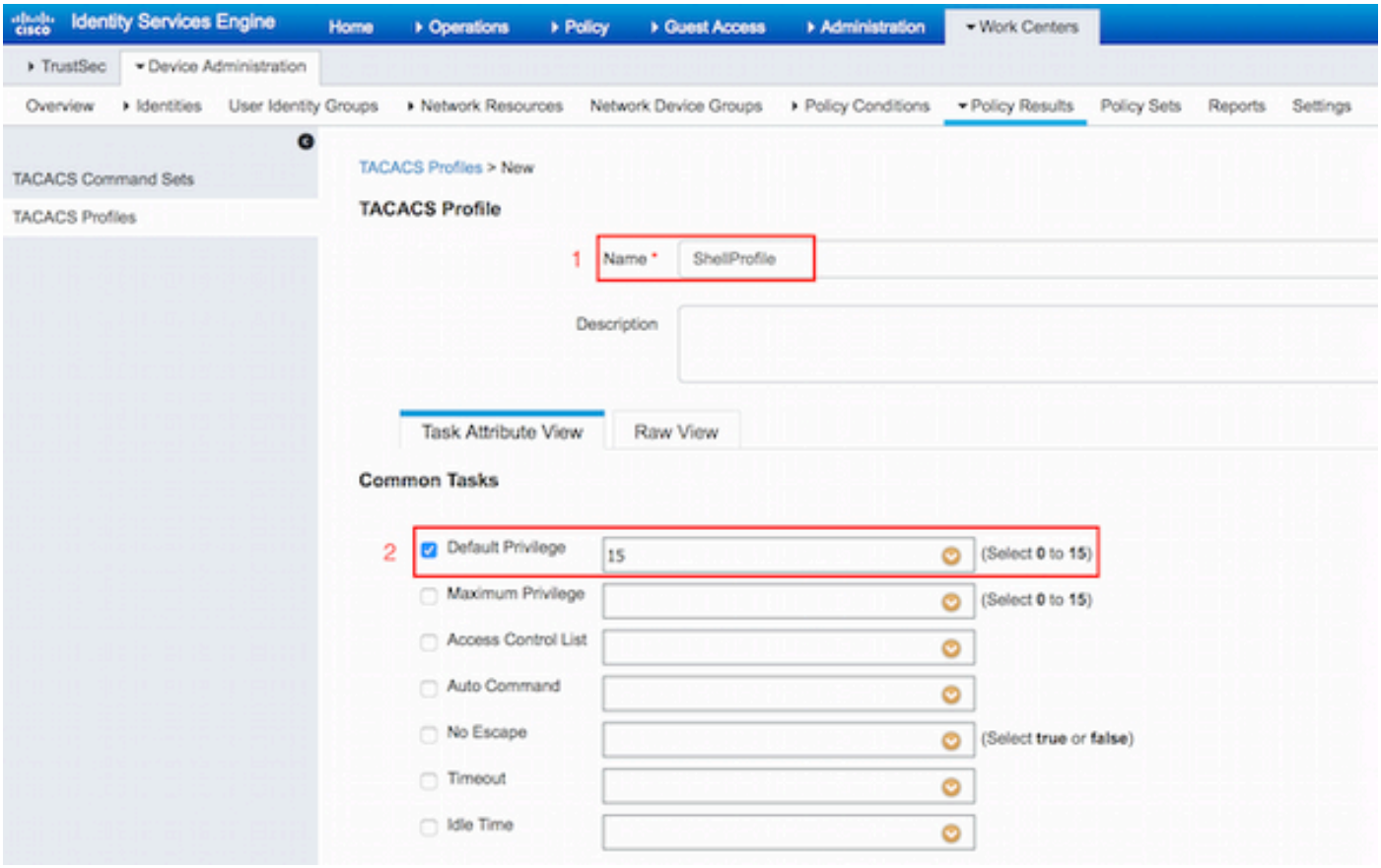


2. Navegue até **Centros de trabalho > Administração de dispositivo > Resultados de política > Conjuntos de comandos TACACS.** Clique em Add. Forneça os comandos Name **PermitShowCommands**, clique em **Add** e permit **show** e **exit**. Por padrão, se Argumentos for deixado em branco, todos os argumentos serão incluídos. Clique em Submit.



Configurar perfil TACACS

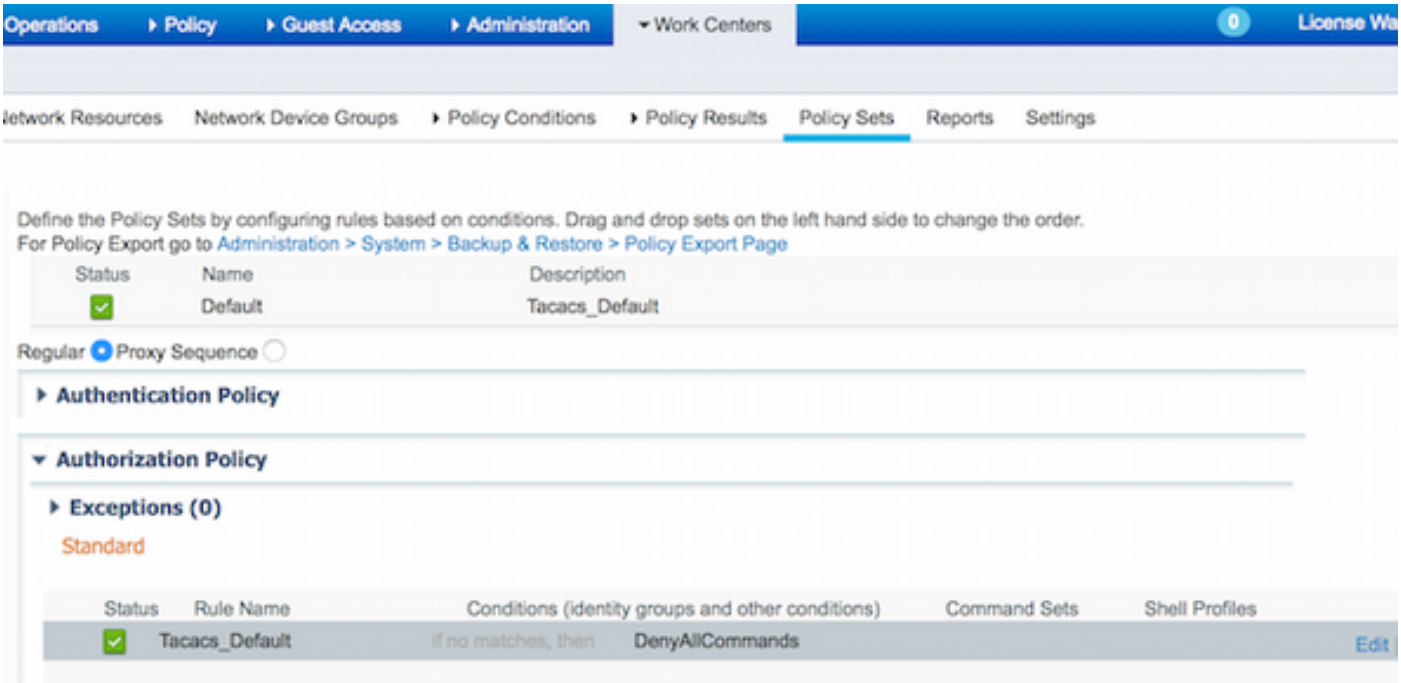
Um único perfil TACACS é configurado. O perfil TACACS é o mesmo conceito que o perfil Shell no ACS. A execução real do comando é feita através de conjuntos de comandos. Navegue até **Centros de trabalho > Administração de dispositivo > Resultados de política > Perfis TACACS.** Clique em Add. Forneça o nome ShellProfile, marque a caixa de seleção **Privilégio padrão** e insira o valor 15. Clique em **Enviar.**



Configurar política de autorização TACACS

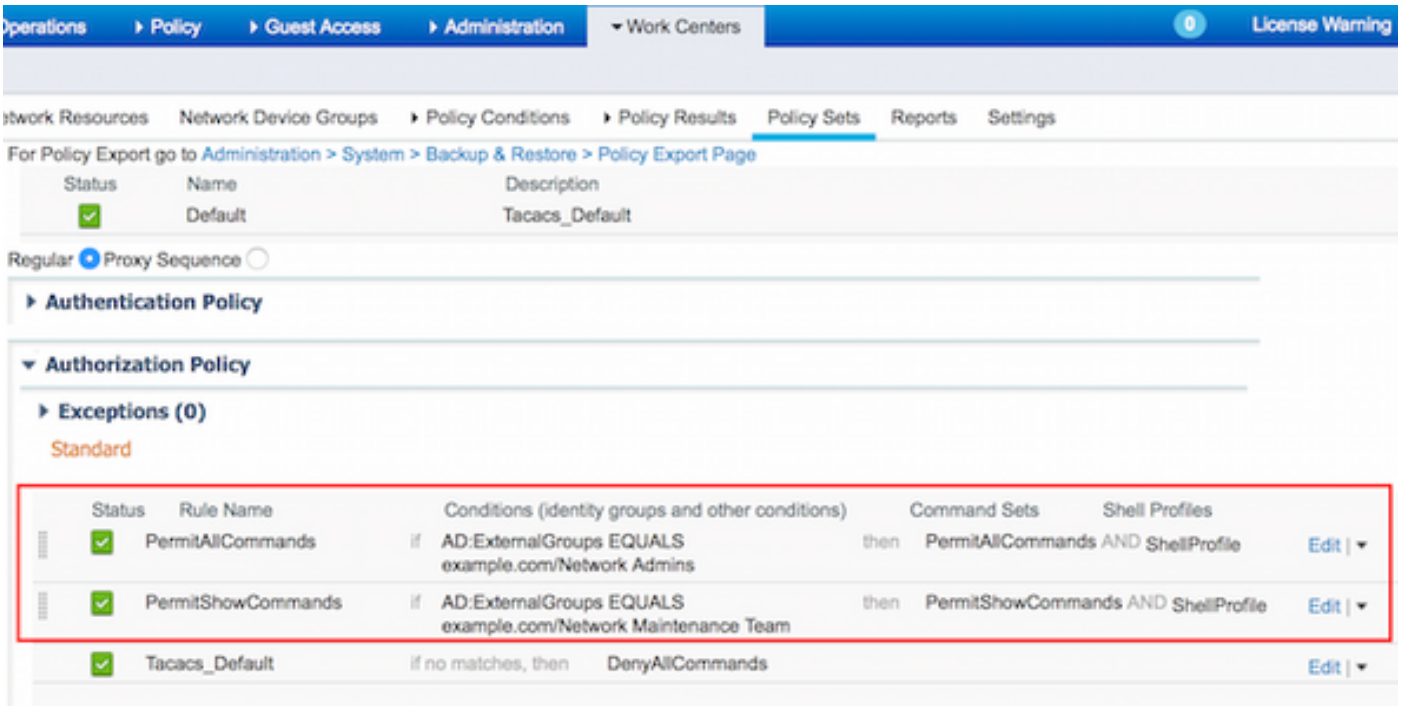
Por padrão, a política de autenticação aponta para All_User_ID_Stores, que inclui o AD, de modo que não é alterado.

Navegue até **Centros de trabalho > Administração de dispositivos > Conjuntos de diretivas > Padrão > Política de autorização > Editar > Inserir nova regra acima.**



Duas regras de autorização são configuradas; A primeira regra atribui o perfil TACACS ShellProfile e o comando Set PermitAllCommands com base na associação do grupo AD de

administradores de rede. A segunda regra atribui o perfil TACACS ShellProfile e o comando Set PermitShowCommands com base na associação do Grupo AD da Equipe de Manutenção de Rede.



Configurar o Cisco IOS Router para Autenticação e Autorização

Conclua estas etapas para configurar o Cisco IOS Router para Autenticação e Autorização.

1. Crie um usuário local com privilégio total para fallback com o comando **username**, conforme mostrado aqui.

```
username cisco privilege 15 password cisco
```

2. Ative aaa new-model. Defina o ISE do servidor TACACS e coloque-o no grupo ISE_GROUP.

```
aaa new-model

tacacs server ISE
 address ipv4 10.48.17.88
 key cisco
aaa group server tacacs+ ISE_GROUP
 server name ISE
```

Note: A chave do servidor corresponde àquela definida no ISE Server anteriormente.

3. Teste a acessibilidade do servidor TACACS com o comando test **aaa** como mostrado.

```
Router#test aaa group tacacs+ admin Krakow123 legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

A saída do comando anterior mostra que o servidor TACACS está acessível e que o usuário foi autenticado com êxito.

4. Configure o login e ative as autenticações e, em seguida, use as autorizações de exec e command conforme mostrado.

```
aaa authentication login AAA group ISE_GROUP local
aaa authentication enable default group ISE_GROUP enable
aaa authorization exec AAA group ISE_GROUP local
aaa authorization commands 0 AAA group ISE_GROUP local
aaa authorization commands 1 AAA group ISE_GROUP local
aaa authorization commands 15 AAA group ISE_GROUP local
aaa authorization config-commands
```

> **Note**: A lista de métodos criada é denominada AAA, que é usada posteriormente, quando atribuída à linha vty.

5. Atribua listas de métodos à linha vty 0 4.

```
line vty 0 4
 authorization commands 0 AAA
 authorization commands 1 AAA
 authorization commands 15 AAA
 authorization exec AAA
 login authentication AAA
```

Verificar

Verificação do roteador Cisco IOS

1. Faça Telnet para o Roteador IOS Cisco como administrador que pertence ao grupo de acesso completo no AD. O grupo Administradores de Rede é o grupo no AD que é mapeado para os comandos ShellProfile e PermitAllCommands definidos no ISE. Tente executar qualquer comando para garantir acesso total.

```
Username:admin
Password:

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes
Router(config-isakmp)#exit
Router(config)#exit
Router#
```

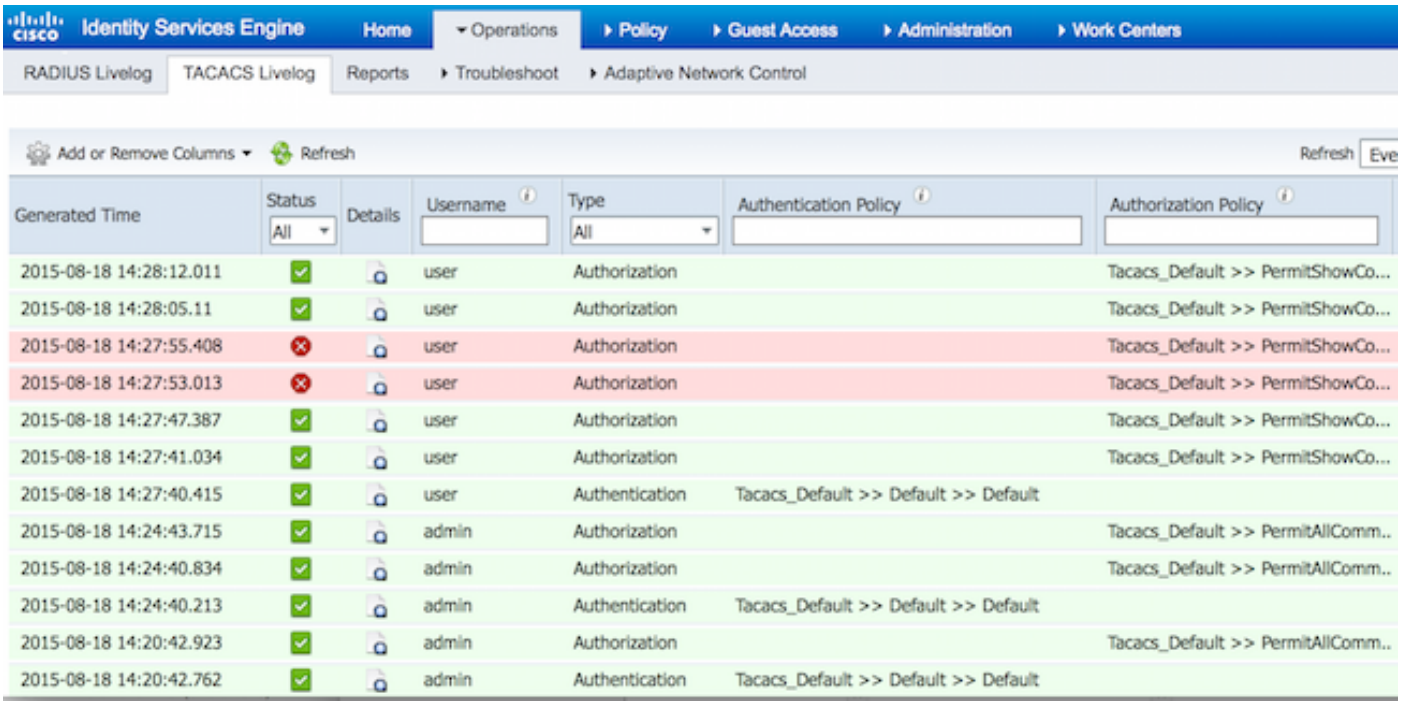
2. Faça Telnet para o Cisco IOS Router como usuário que pertence ao grupo de acesso limitado no AD. O grupo Equipe de Manutenção de Rede é o grupo no AD que é mapeado para os comandos ShellProfile e PermitShowCommands definidos no ISE. Tente executar qualquer comando para garantir que somente comandos show possam ser emitidos.

```
Username:user
Password:

Router#show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.48.66.32     YES NVRAM  up                    up
```

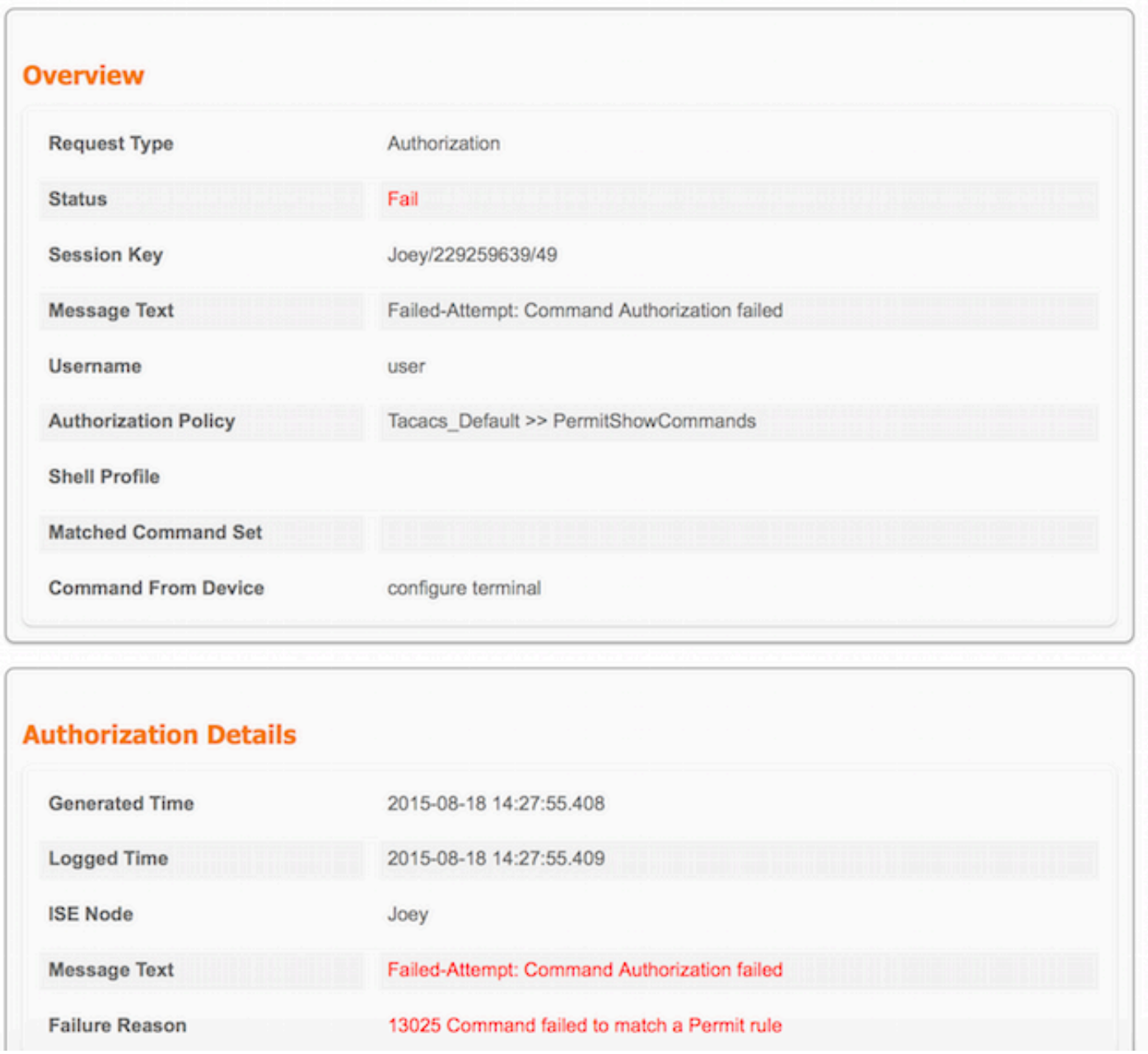
```
Router#ping 8.8.8.8
Command authorization failed.

Router#configure terminal
Command authorization failed.

Router#show running-config | include hostname
hostname Router
Router#
```

Verificação do ISE 2.0

1. Navegue até **Operations > TACACS Livelog.** Verifique se as tentativas feitas foram vistas.



2. Clique nos detalhes de um dos relatórios em vermelho. Um comando com falha executado anteriormente pode ser visto.



Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229259639/49
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> PermitShowCommands
Shell Profile	
Matched Command Set	
Command From Device	configure terminal

Authorization Details

Generated Time	2015-08-18 14:27:55.408
Logged Time	2015-08-18 14:27:55.409
ISE Node	Joey
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule

Troubleshoot

Erro: Falha do comando 13025 ao corresponder a uma regra de permissão

Verifique os atributos SeletedCommandSet para verificar se os Conjuntos de Comandos esperados foram selecionados pela política de Autorização.

Informações Relacionadas

Suporte Técnico e Documentação - Cisco Systems

Notas da versão do ISE 2.0

Guia de instalação de hardware do ISE 2.0

Guia de atualização do ISE 2.0

Guia da ferramenta de migração ACS para ISE

Guia de integração do Ative Diretory do ISE 2.0

Guia do administrador do mecanismo ISE 2.0

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.