ISE 2.0: Exemplo de configuração da autenticação TACACS+ e do comando authorization ASA CLI

Índice

Introdução

Este original descreve como configurar a autenticação TACACS+ e o comando authorization na ferramenta de segurança adaptável de Cisco (ASA) com o motor do serviço da identidade (ISE) 2.0 e mais atrasado. O ISE usa a loja local da identidade para armazenar recursos tais como usuários, grupos, e valores-limite.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O Firewall ASA é plenamente operacional

- Conectividade entre o ASA e o ISE
- O server ISE é amarrado

Componentes Utilizados

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

- Motor 2.0 do serviço da identidade de Cisco
- Software Release 9.5(1) de Cisco ASA

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

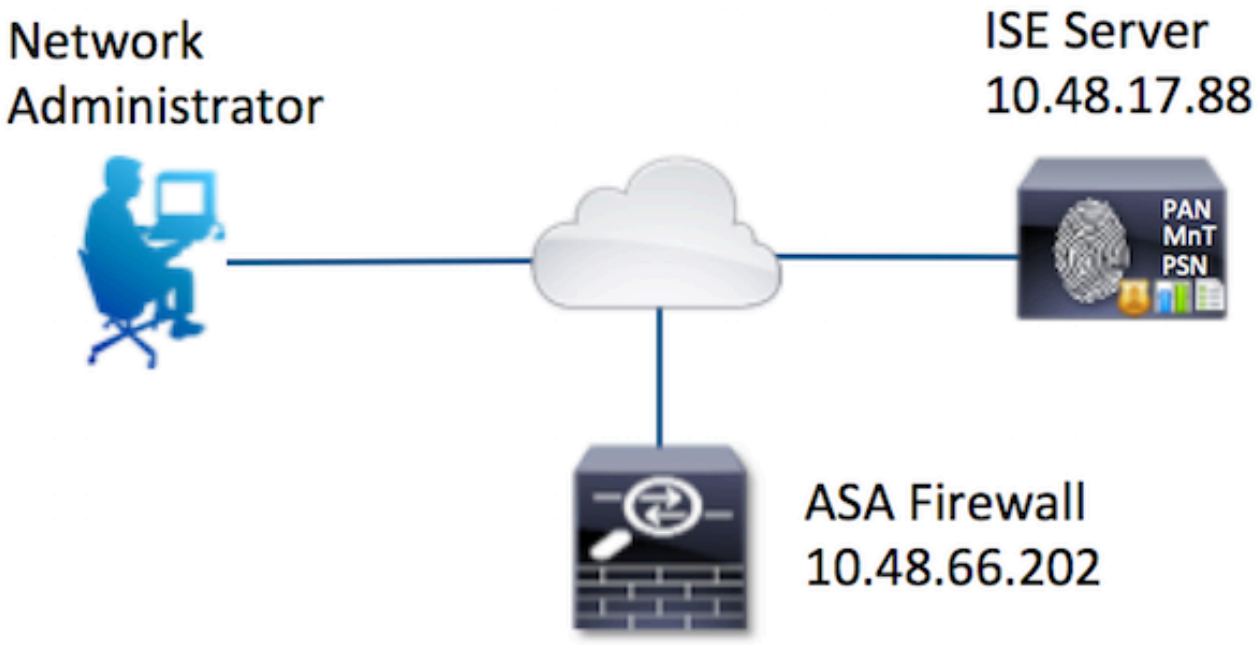
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

O alvo da configuração está a:

- Autentique o usuário do ssh através da loja interna da identidade
- Autorize o usuário do ssh assim que será colocada no modo de exec privilegiado após o início de uma sessão
- Verifique e envie cada comando executado ao ISE para a verificação

Diagrama de Rede



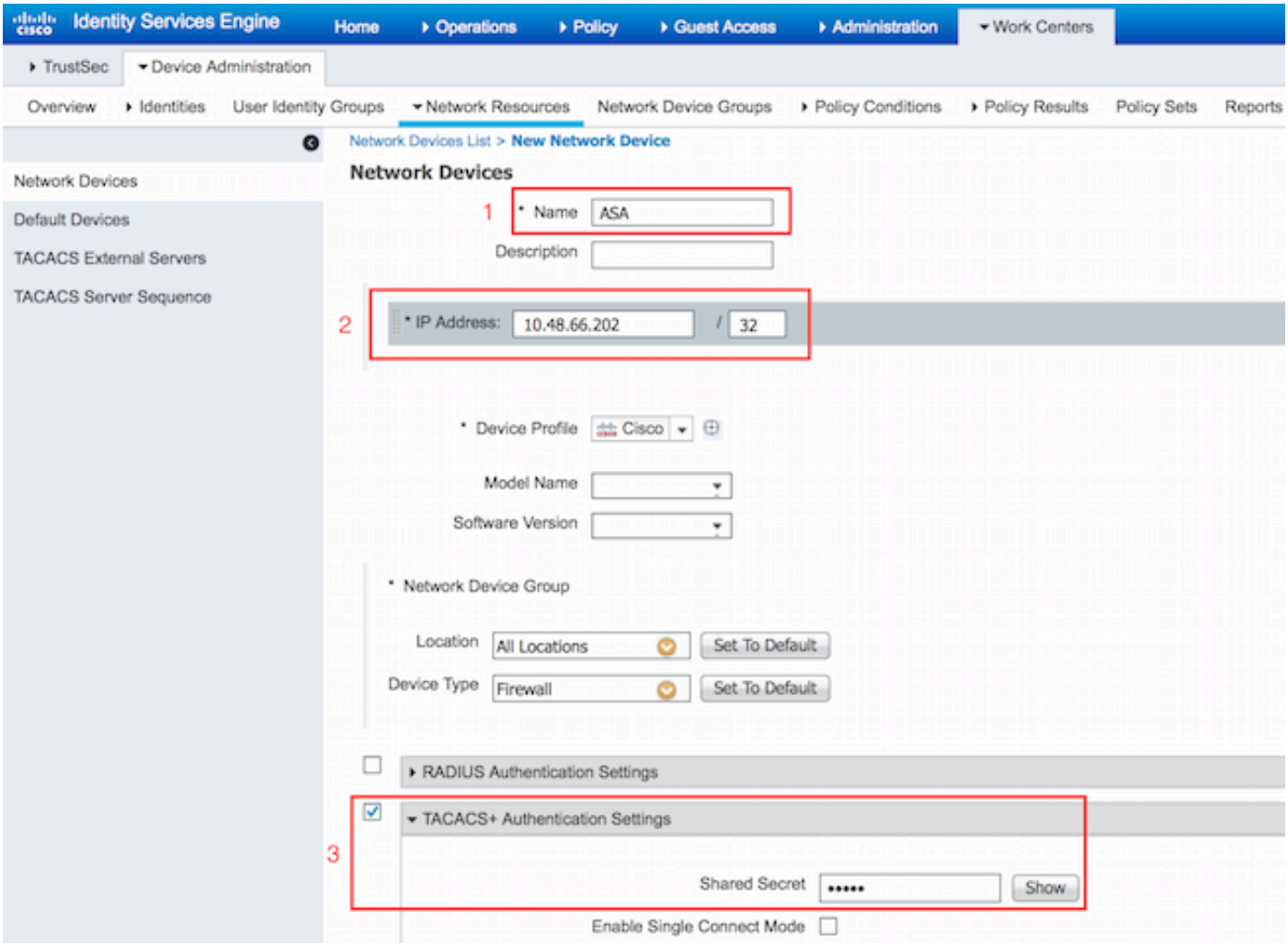
Configurações

Configurar o ISE para a authentication e autorização

Dois usuários são criados. **O administrador do** usuário é parte de um grupo local da identidade de **Admins da rede no** ISE. Este usuário tem privilégios completos CLI. **O usuário do** usuário é parte de um grupo local da identidade da **equipe da manutenção de rede no** ISE. É permitido a este usuário fazer somente comandos show e sibilo.

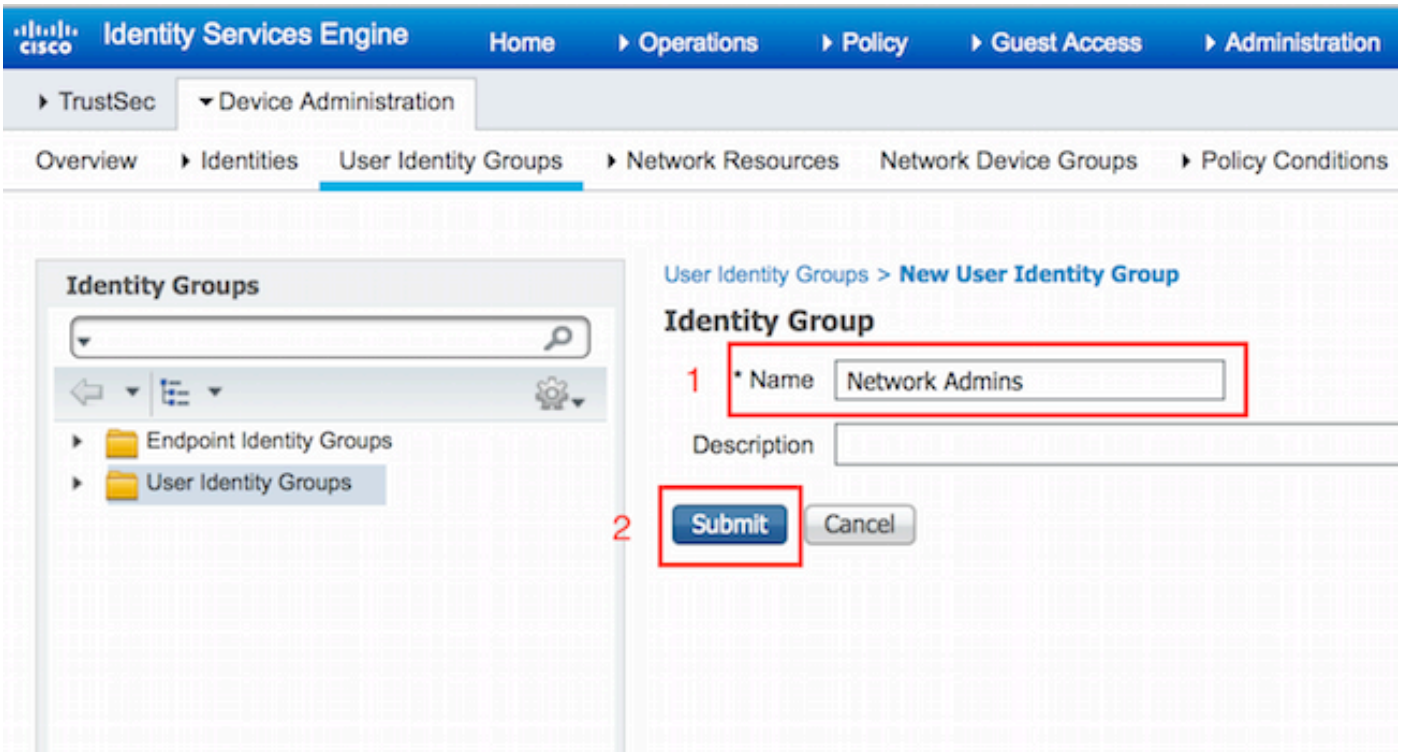
Adicionar o dispositivo de rede

Navegue aos **centros de trabalho > à administração > aos recursos de rede > aos dispositivos de rede do dispositivo.** Clique em Add. Forneça o nome, IP address, selecione a caixa de seleção dos **ajustes da autenticação TACACS+** e forneça a **chave secreta compartilhada**. Opcionalmente o tipo de dispositivo/lugar pode ser especificado.



Configurando grupos da identidade do usuário

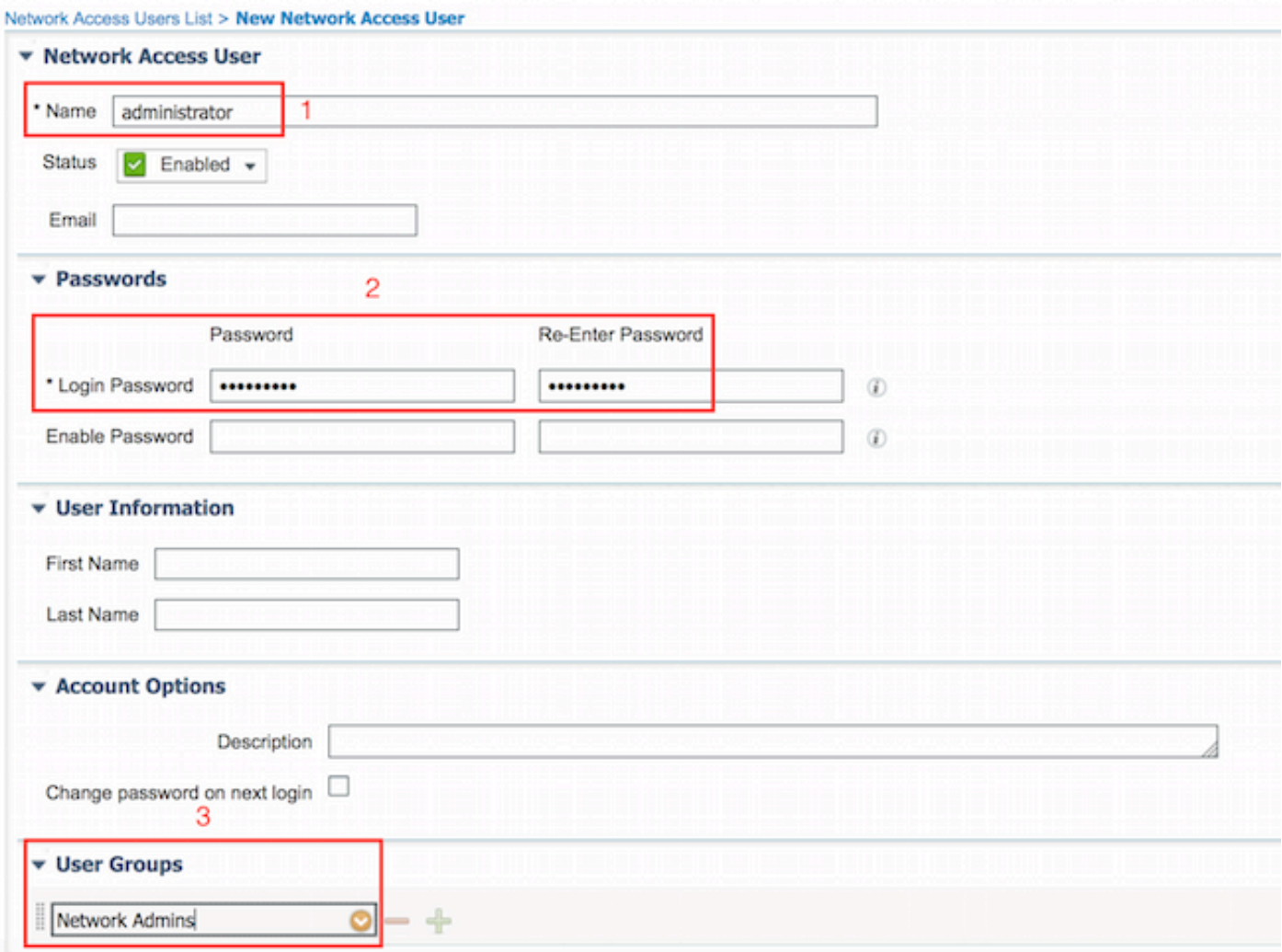
Navegue aos **grupos da identidade dos centros de trabalho > da administração > do usuário do dispositivo.** Clique em Add. Forneça o nome e o clique **submete-se.**



Repita a mesma etapa para configurar o grupo da identidade do usuário da **equipe da manutenção de rede**.

Configurando usuários

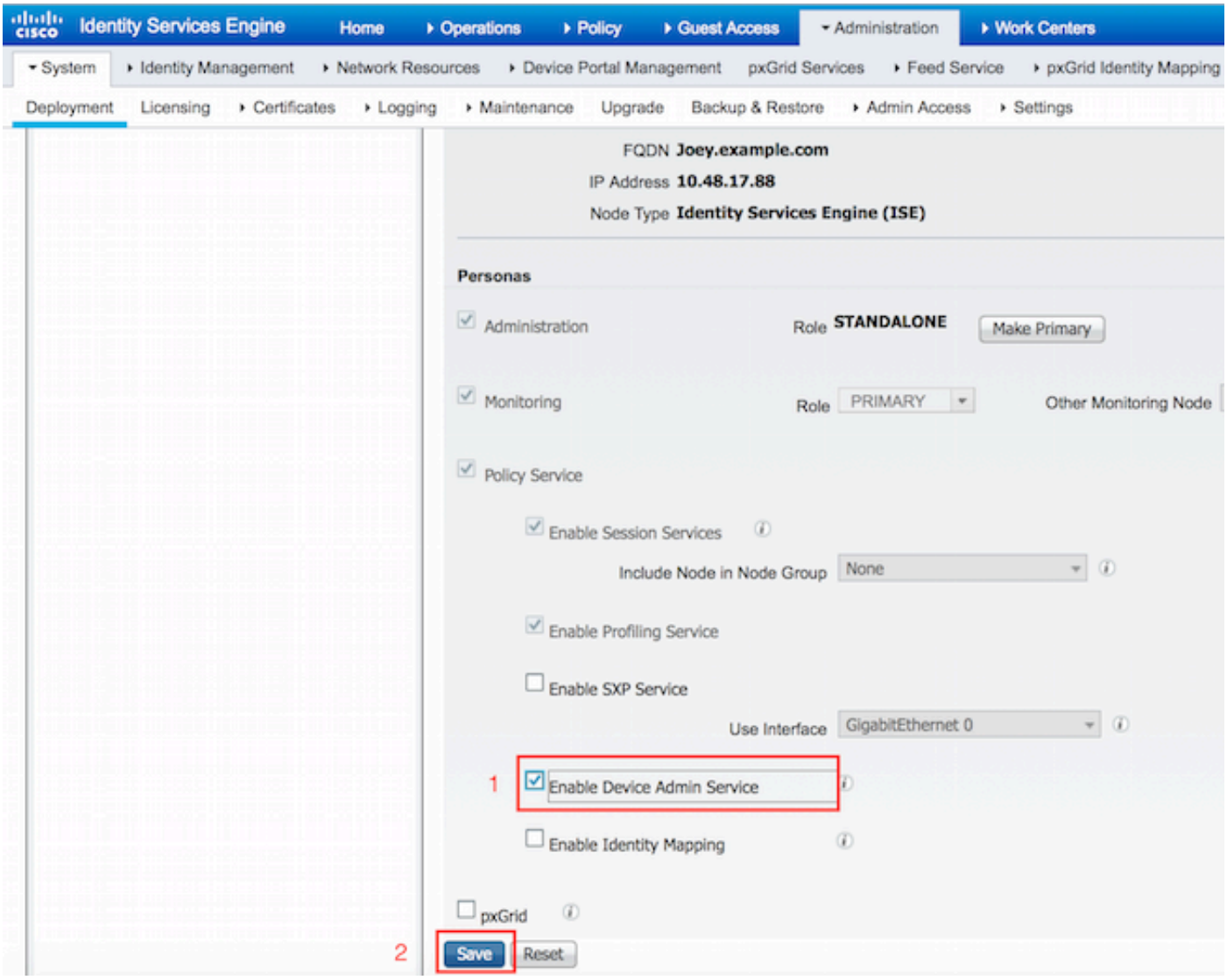
Navegue aos **centros de trabalho > à administração > às identidades > aos usuários do dispositivo.** Clique em Add. Forneça o nome, a senha de login especifica o grupo de usuário e o clique **submete-se**.



Repita as etapas para configurar o **usuário do** usuário e para atribuir o grupo da identidade do usuário da **equipe da manutenção de rede**.

Permita o serviço Admin do dispositivo

Navegue à **administração > ao sistema > ao desenvolvimento.** Select exigiu o nó. Seleto **permita a** caixa de seleção do **serviço Admin do dispositivo** e clique a **salvaguarda.**

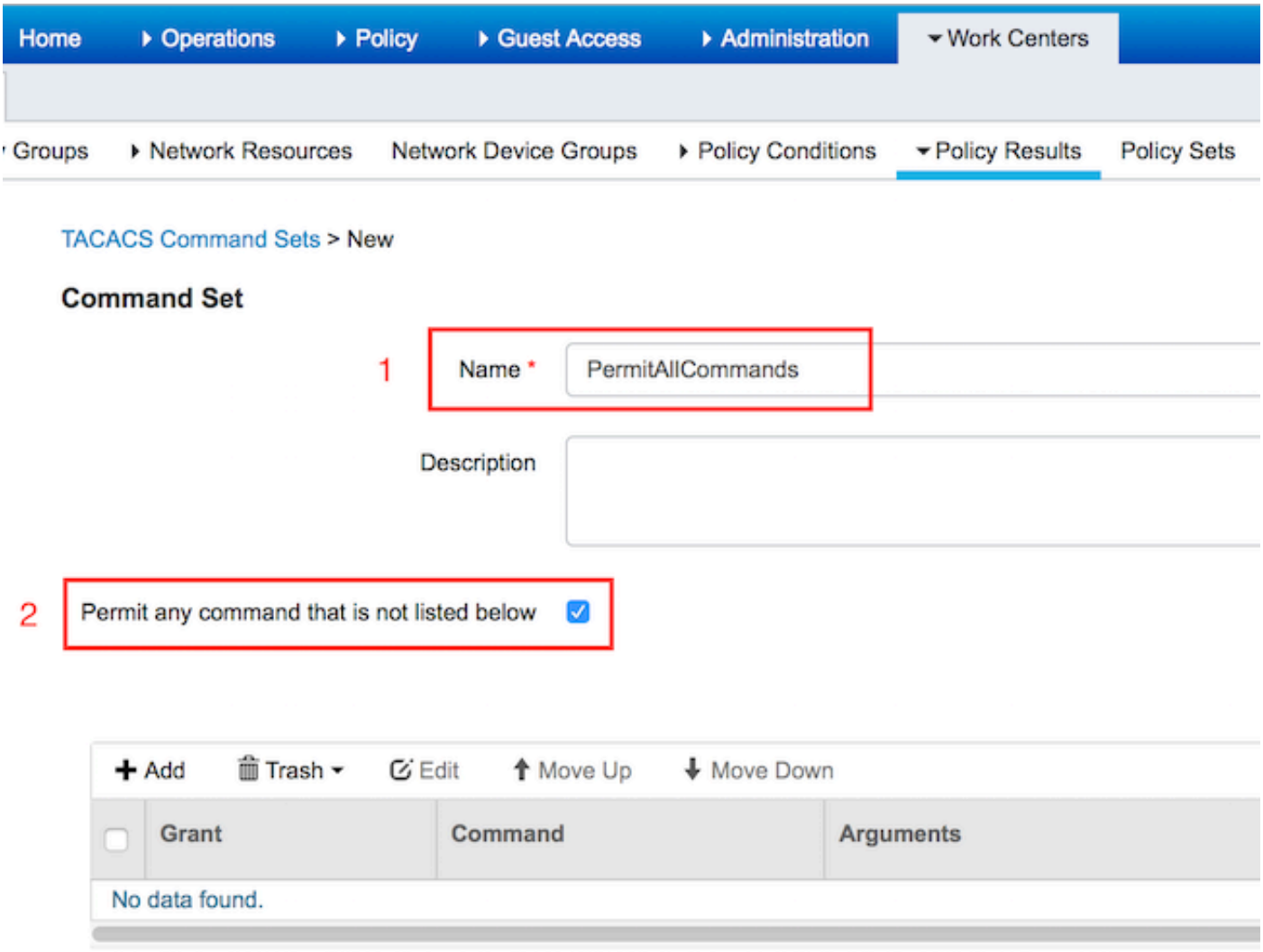


Nota: Para o TACACS você precisa de ter a licença separada instalada.

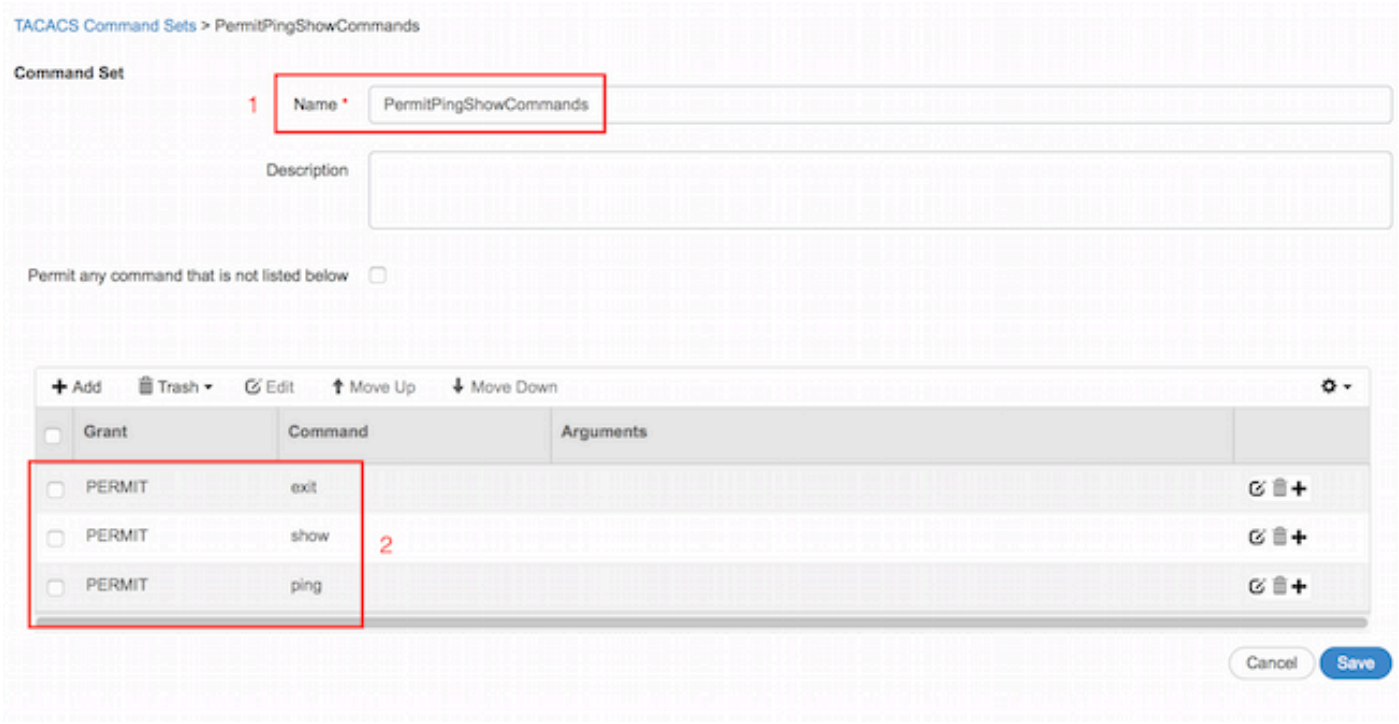
Configurando grupos do comando tacacs

Dois conjuntos de comandos são configurados. Primeiro **PermitAllCommands** para o **usuário do administrador** que permitem comandos all no dispositivo. Em segundo **PermitPingShowCommands** para o usuário do **usuário** que permitem somente a mostra e os comandos ping.

1. Navegue aos **centros de trabalho > à administração > à política do dispositivo resulta > grupos do comando tacacs.** Clique em Add. Forneça o nome **PermitAllCommands, o comando permit any** seleto **que não é** caixa de seleção **abaixo listada** e o clique **se submete.**

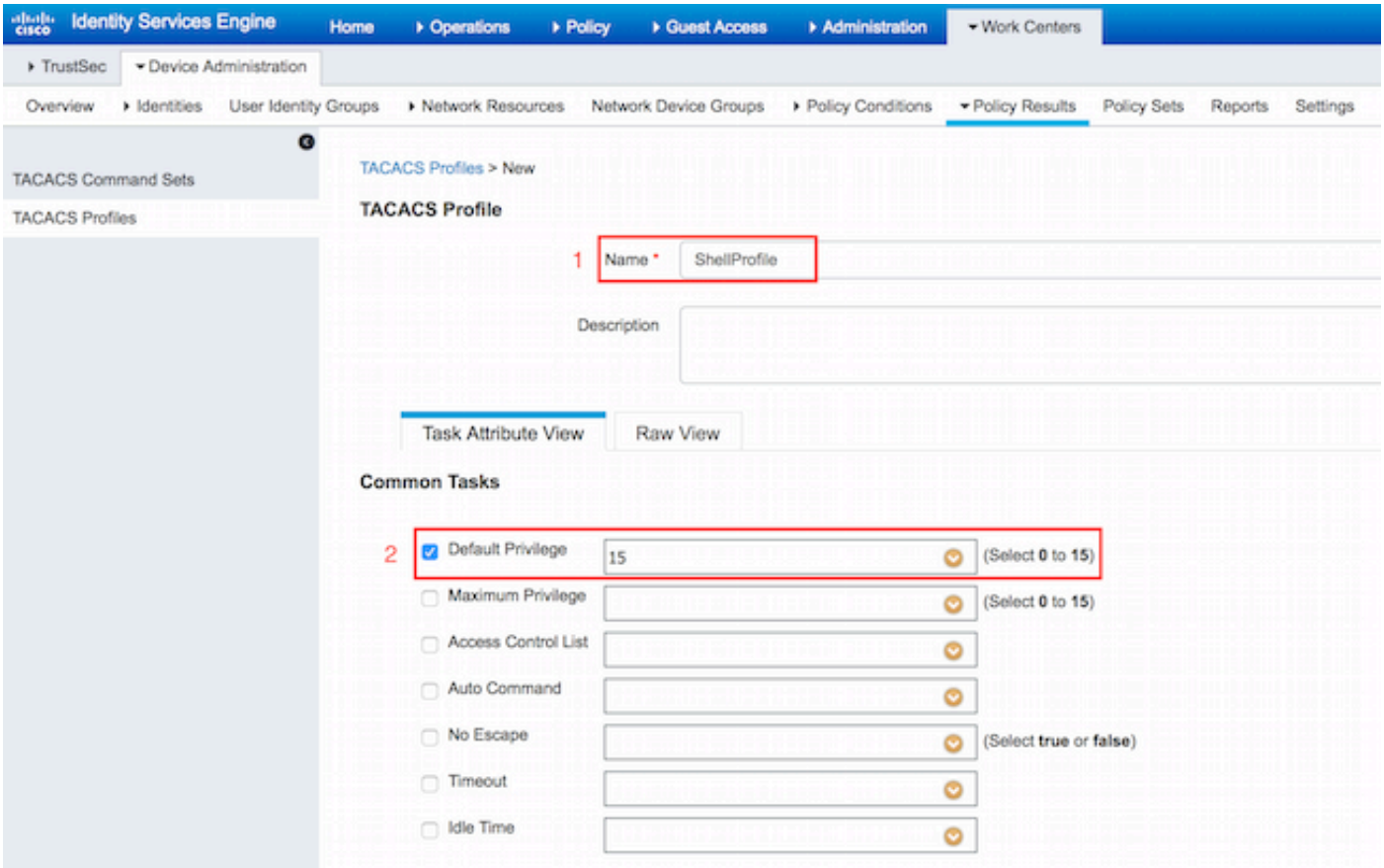


2. Navegue aos **centros de trabalho > à administração > à política do dispositivo resulta > grupos do comando tacacs.** Clique em Add. Forneça o nome **PermitPingShowCommands,** clique **adicionam** e permitem a **mostra, o sibilo** e os **comandos exit**. À revelia se os argumentos são deixados vazio, todos os argumentos são incluídos. Clique em Submit.



Configurando o perfil TACACS

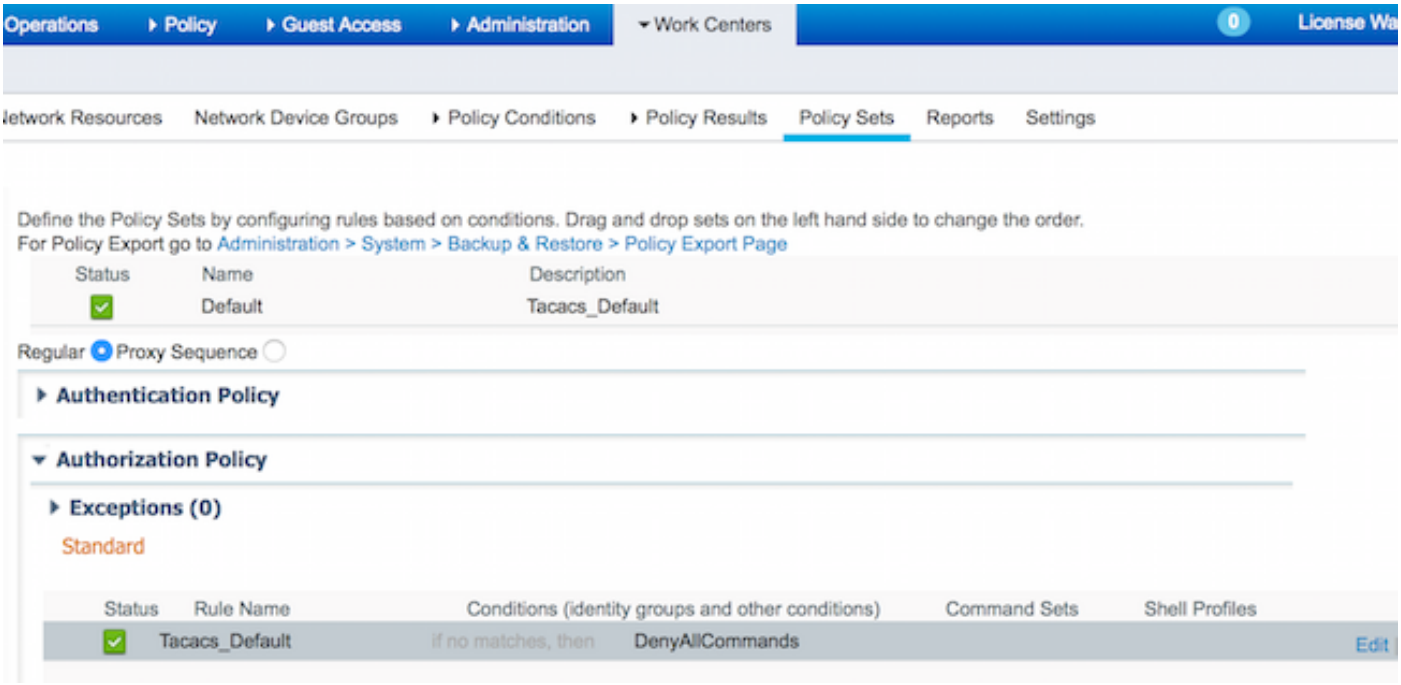
O único perfil TACACS será configurado. A aplicação real do comando será feita através dos conjuntos de comandos. Navegue aos **centros de trabalho > à administração > à política do dispositivo resulta > perfis TACACS.** Clique em Add. Forneça o nome **ShellProfile,** selecione a caixa de seleção do **privilégio padrão** e incorpore o valor de 15. Clique em Submit.



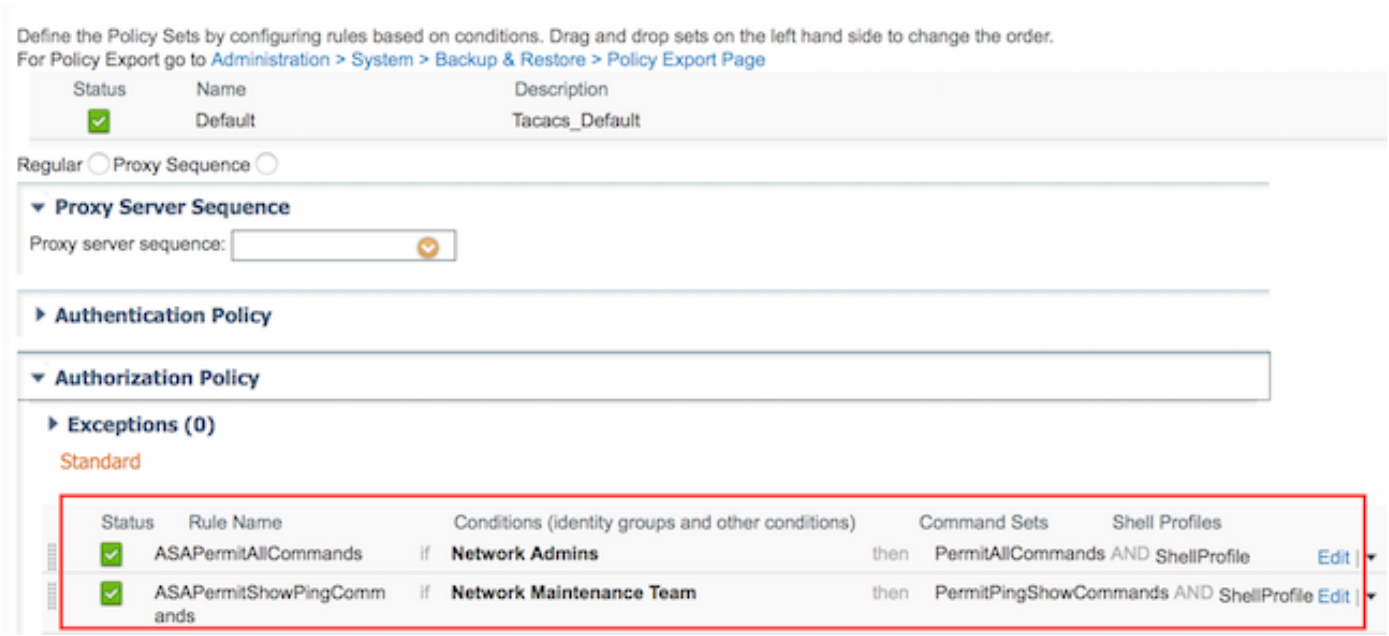
Configurando a política da autorização TACACS

A política de autenticação aponta à revelia a All_User_ID_Stores, que inclui a loja local também, assim que é deixado inalterado.

Navegue aos **grupos dos centros de trabalho > da administração > da política do dispositivo > à política do padrão > da autorização > editam > regra nova da inserção acima.**



O rulesare de duas autorizações configurado, primeira regra atribui o perfil **ShellProfile** TACACS e o comando set **PermitAllCommands** baseado na membrasia do clube da identidade do usuário de **Admins da rede**. A segunda regra atribui o perfil **ShellProfile** TACACS e o comando set **PermitPingShowCommands** baseado na membrasia do clube da identidade do usuário da **equipe da manutenção de rede**.



Configurar o Firewall de Cisco ASA para a authentication e autorização

1. Crie um usuário local com o privilégio completo para a reserva com o **comando username** como mostrado aqui

```
ciscoasa(config)# username cisco password cisco privilege 15
```

2. Defina o servidor de TACACS ISE, especifique a relação, o IP address do protocolo, e a chave dos **tacacs**.

```
ciscoasa(config)# username cisco password cisco privilege 15
```

> Nota: A chave de servidor deve combinar esse define no server ISE mais cedo.

3. Teste o reachability do servidor de TACACS com o **comando aaa do** teste como mostrado.

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

A saída do comando precedente mostra que o servidor de TACACS é alcançável e o usuário esteve autenticado com sucesso.

4. Configurar a autenticação para o ssh, a autorização de exec e as autorizações de comando como mostrado abaixo. Com o **executivo que da autorização aaa o Authentication Server auto-o permite** será colocado no modo de exec privilegiado automaticamente.

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

> Nota: Com os comandos acima, a autenticação é feita no ISE, usuário é colocada diretamente no modo do privilégio e o comando authorization ocorre.

5. Permita shh na relação do mgmt.

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

Verificar

Verificação do Firewall de Cisco ASA

1. Ssh ao Firewall ASA como o **administrador** que pertence ao grupo da identidade do usuário do acesso direto. O grupo de **Admins da rede** é traçado a **ShellProfile** e a comando set de **PermitAllCommands no** ISE. Tente executar o comando any assegurar o acesso direto.

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh administrator@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# configure terminal
ciscoasa(config)# crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)# encryption aes
ciscoasa(config-ikev1-policy)# exit
```

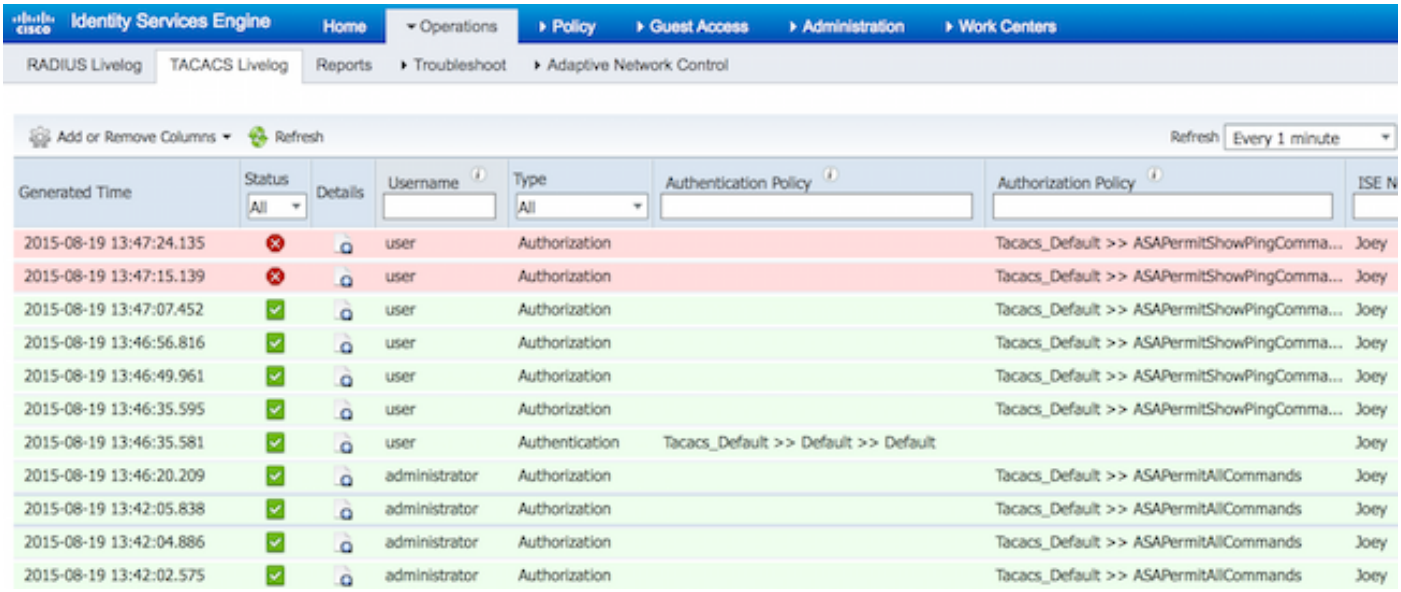
```
ciscoasa(config)# exit
ciscoasa#
```

2. Ssh ao Firewall ASA como o **usuário** que pertence ao grupo limitado da identidade do usuário do acesso. O grupo da **manutenção de rede** é traçado a **ShellProfile** e a comando set de **PermitPingShowCommands no** ISE. Tente executar o comando any assegurar-se de que somente a mostra e os comandos ping possam ser emitidos.

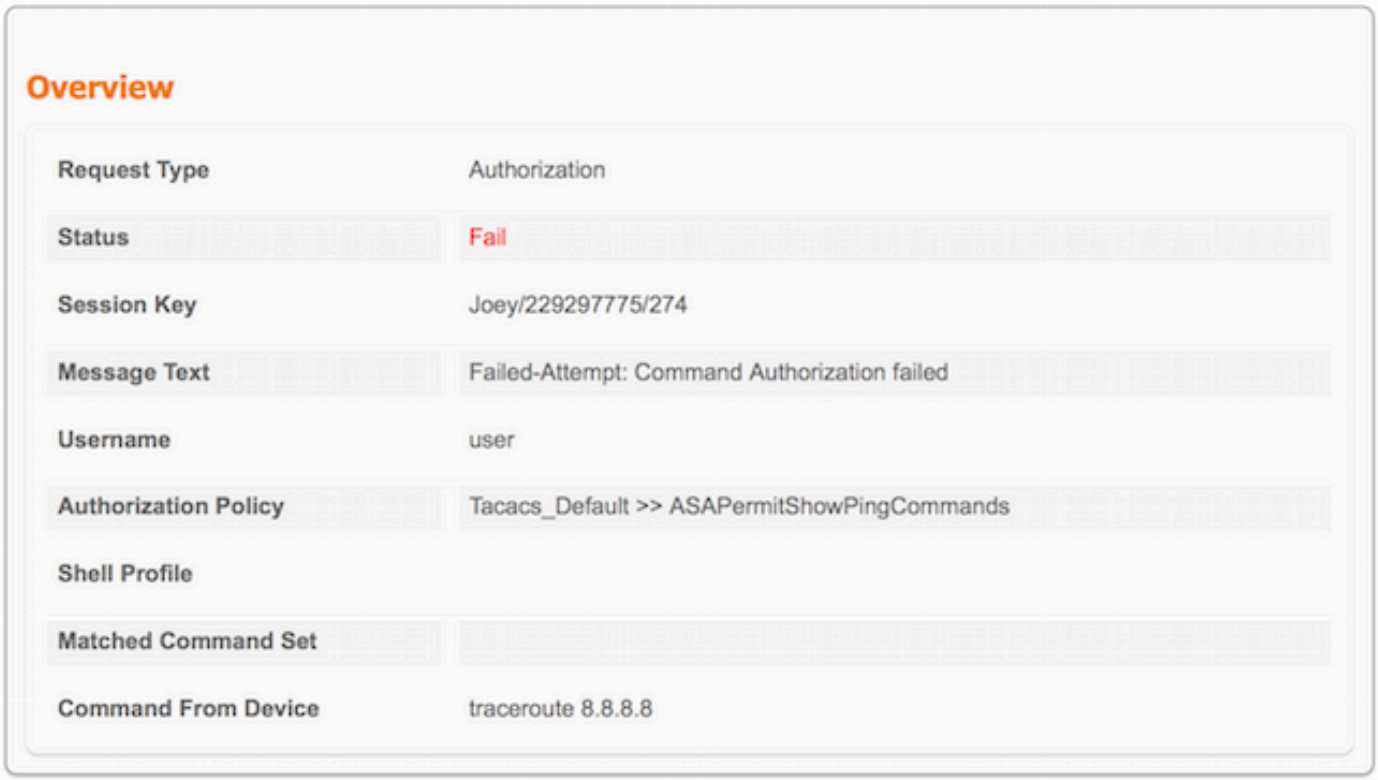
```
EKORNEYC-M-K04E:~ ekorneyc$ ssh user@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# show version | include Software
Cisco Adaptive Security Appliance Software Version 9.5(1)
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
ciscoasa# configure terminal
Command authorization failed
ciscoasa# traceroute 8.8.8.8
Command authorization failed
```

Verificação ISE 2.0

1. Navegue às **operações > ao TACACS Livelog.** Assegure-se de que as tentativas feitas acima estejam consideradas.



2. Clique sobre os detalhes de um dos relatórios vermelhos, mais adiantado executado comando falhado pode ser visto.



Troubleshooting

Erro: Falha de tentativa: Comando authorization falhado

Verifique os atributos de SelectedCommandSet para verificar que os grupos do comando expected estiveram selecionados pela política da autorização

Informações Relacionadas

Suporte Técnico e Documentação - Cisco Systems

Release Note ISE 2.0

Guia de instalação de hardware ISE 2.0

Guia da elevação ISE 2.0

ACS ao guia da ferramenta da migração ISE

Guia da integração do ative directory ISE 2.0

Guia do administrador do motor ISE 2.0