Grupos da autorização do comando shell ACS no exemplo de configuração IO e ASA/PIX/FWSM

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Grupos do comando authorization
Adicionar um grupo da autorização do comando shell
Cenário 1: Privilégio para o acesso de leitura/gravação ou o acesso direto
Cenário 2: Privilégio para o acesso somente leitura
Cenário 3: Privilégio para o acesso restrito
Associe a autorização do comando shell ajustada ao grupo de usuário
Associe a autorização do comando shell ajustada (acesso de leitura/gravação) ao grupo de usuário (o admin group)
Associe a autorização do comando shell ajustada (acesso de leitura apenas) ao grupo de usuário (o grupo de leitura apenas)
Associe a autorização do comando shell ajustada (Restrict_access) ao usuário
Configuração do IOS Router
Configuração ASA/PIX/FWSM
Troubleshooting
Erro: comando authorization falhado
Informações Relacionadas

Introdução

Este documento descreve como configurar os grupos da autorização do shell no Serviço de controle de acesso Cisco Secure (ACS) para clientes de AAA, tais como o Roteadores do ® do Cisco IOS ou o Switches e os dispositivos do Cisco Security (ASA/PIX/FWSM) com o TACACS+ como o protocolo da autorização.

Nota: O ACS expresso não apoia o comando authorization.

Pré-requisitos

Requisitos

Este documento supõe que as configurações básicas estão ajustadas em clientes de AAA e em ACS.

No ACS, escolha **Interface Configuration > Advanced Options**, e assegure-se de que a caixa de verificação dos **atributos do usuário per. TACACS+/RADIUS** esteja verificada.

Componentes Utilizados

A informação neste documento é baseada no Serviço de controle de acesso Cisco Secure (ACS) essas corridas a versão de software 3.3 e mais atrasado.

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.

Convenções

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

Grupos do comando authorization

Os grupos do comando authorization fornecem um mecanismo central para controlar a autorização de cada comando que é emitido em todo o dispositivo de rede dado. Esta característica aumenta extremamente a escalabilidade e a viabilidade exigidas para ajustar limitações da autorização.

No ACS, os grupos da autorização do comando default incluem grupos da autorização do comando shell e a autorização do comando pix ajusta-se. Os aplicativos de gerenciamento do dispositivo Cisco, tais como o Centro de gerenciamento do CiscoWorks para firewalls, podem instruir o ACS para apoiar tipos ajustados da autorização do comando adicional.

Nota: Os grupos da autorização do comando pix exigem que o pedido de autorização do comando tacacs+ identifica o serviço como o *pixshell*. Verifique que este serviço esteve executado no OS da versão de PIX que seus Firewall usam; se não, use grupos da autorização do comando shell para executar o comando authorization para dispositivos de PIX. Refira configurar uma autorização do comando shell ajustada para um grupo de usuário para mais informação.

Nota: Até à data da versão do PIX OS 6.3, o serviço do pixshell não foi executado.

Nota: Os dispositivos do Cisco Security (ASA/PIX) não permitem atualmente que o usuário seja colocado diretamente no modo enable durante o início de uma sessão. O usuário deve manualmente participar no modo enable.

A fim oferecer mais controle de sessões de telnet administrativo dispositivo-hospedadas, um dispositivo de rede que use o TACACS+ pode pedir a autorização para cada linha de comando antes que execute. Você pode definir um conjunto de comandos que é permitido ou negado para a execução por um usuário particular em um dispositivo dado. O ACS aumentou mais esta capacidade com estas características:

- **Grupos Nomeados reusáveis do comando authorization** — Sem diretamente mencionar qualquer usuário ou grupo de usuário, você pode criar um conjunto nomeado das autorizações de comando. Você pode definir diversos grupos do comando authorization que traçam perfis diferentes do acesso. Por exemplo:Um grupo do comando authorization do *help desk* podia permitir o acesso aos comandos de nível elevado da consultação, tais como a **corrida da mostra**, e nega todos os comandos configuration.*Todo o* grupo do comando authorization dos *engenheiros de rede* podia conter uma lista limitada de comandos permitidos para todo o engenheiro de rede na empresa.*Uma rede local projeta o* comando authorization que o grupo poderia permitir comandos all (e para incluir comandos de configuração de endereço IP).
- **Granularidade fina da configuração** — Você pode criar associações entre grupos Nomeados do comando authorization e grupos de dispositivo de rede (NDGs). Assim, você pode definir perfis diferentes do acesso para usuários segundo que dispositivos de rede alcançam. Você pode associar o mesmo grupo Nomeado do comando authorization com o mais de um NDG e usá-lo para mais de um grupo de usuário. O ACS reforça a integridade de dados. Os grupos Nomeados do comando authorization são mantidos no base de dados interno ACS. Você pode usar as características alternativas ACS e da restauração a alternativo e à restauração elas. Você pode igualmente grupos da autorização do comando replicate aos ACS secundários junto com outros dados de configuração.

Para os tipos ajustados do comando authorization que apoiam aplicativos de gerenciamento do dispositivo Cisco, os benefícios são similares quando você usa grupos do comando authorization. Você pode grupos da autorização do comando apply aos grupos ACS que contêm usuários do aplicativo do Gerenciamento de dispositivos a fim reforçar a autorização de vários privilégios em um aplicativo do Gerenciamento de dispositivos. Os grupos ACS podem corresponder aos papéis diferentes dentro do aplicativo do Gerenciamento de dispositivos, e você pode aplicar grupos diferentes do comando authorization a cada grupo, como aplicáveis.

O ACS tem três fases sequenciais da filtração do comando authorization. Cada pedido do comando authorization é avaliado na ordem alistada:

1. **Comando match** — O ACS determina se o comando que é processado combina um comando alistado no grupo do comando authorization. Se o comando não é combinado, o comando authorization está determinado pelo ajuste ímpar dos comandos: *permit or deny*. Se não, se o comando é combinado, a avaliação continua.
2. **Fósforo do argumento** — O ACS determina se os argumentos do comando apresentados combinam os argumentos do comando alistados no grupo do comando authorization.Se nenhum argumento não é combinado, o comando authorization está determinado por se a opção ímpar de Args da licença está permitida. Se os argumentos ímpares são permitidos, o comando estão autorizados e as extremidades da avaliação; se não, o comando não é autorizado e extremidades da avaliação.Se todos os argumentos são combinados, a avaliação continua.
3. **Política do argumento** — Uma vez que o ACS determina que os argumentos nos argumentos do comando match no grupo do comando authorization, ACS determinam se cada argumento do comando está permitido explicitamente. Se todos os argumentos são permitidos explicitamente, o ACS concede o comando authorization. Se nenhuns argumentos não são permitidos, o ACS nega o comando authorization.

Adicionar um grupo da autorização do comando shell

Esta seção inclui estas encenações que descrevem como adicionar um comando authorization ajustado:

- Cenário 1: Privilégio para o acesso de leitura/gravação ou o acesso direto
- Cenário 2: Privilégio para o acesso somente leitura
- Cenário 3: Privilégio para o acesso restrito

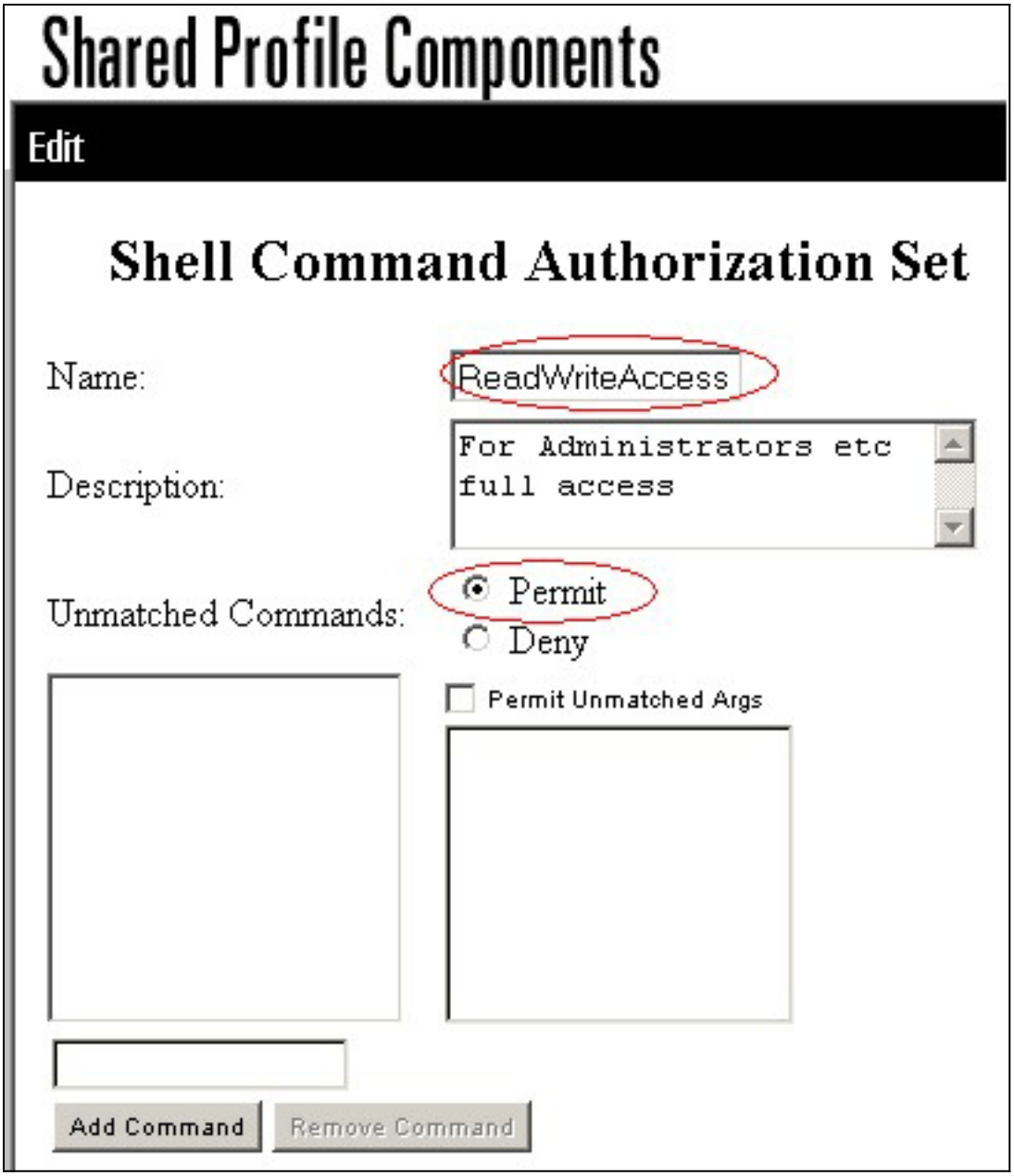
Nota: Refira adicionar uma seção de conjunto do comando authorization do Guia do Usuário para o Serviço de controle de acesso Cisco Secure 4.1 para obter mais informações sobre de como criar grupos do comando authorization. Refira a edição de um comando authorization ajustado e a supressão de um comando authorization ajustado para obter mais informações sobre de como editar e de grupos da autorização do comando delete.

Cenário 1: Privilégio para o acesso de leitura/gravação ou o acesso direto

No este as encenações, usuários são concedidas o acesso de leitura/gravação (ou completo).

Na área ajustada da autorização do comando shell do indicador dos componentes de perfil compartilhado, configurar estes ajustes:

1. No campo de nome, entre em **ReadWriteAccess** como o nome de conjunto do comando authorization.
2. No campo de descrição, incorpore uma descrição para o grupo do comando authorization.
3. Clique o botão de rádio da **licença**, e clique-o então **submetem-se**.

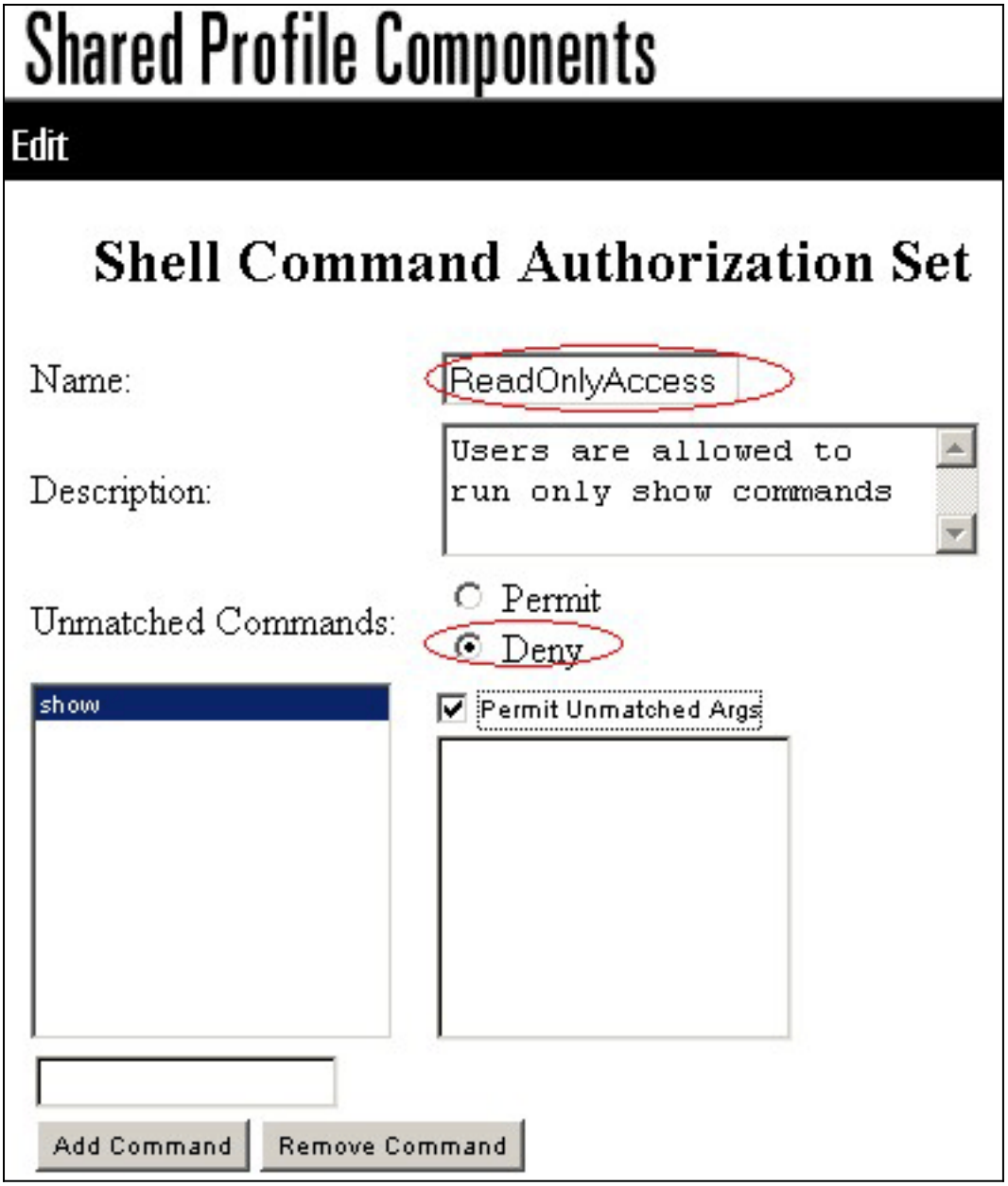


Cenário 2: Privilégio para o acesso somente leitura

No este as encenações, usuários podem usar somente **comandos show**.

Na área ajustada da autorização do comando shell do indicador dos componentes de perfil compartilhado, configurar estes ajustes:

1. No campo de nome, entre em **ReadOnlyAccess** como o nome do grupo do comando authorization.
2. No campo de descrição, incorpore uma descrição para o grupo do comando authorization.
3. Clique o botão de rádio da **negação**.
4. Inscreva o **comando show no** campo acima do botão de comando Add, e clique então o **comando Add**.
5. Verifique a caixa de verificação **ímpar de Args da licença**, e o clique **submete-se**

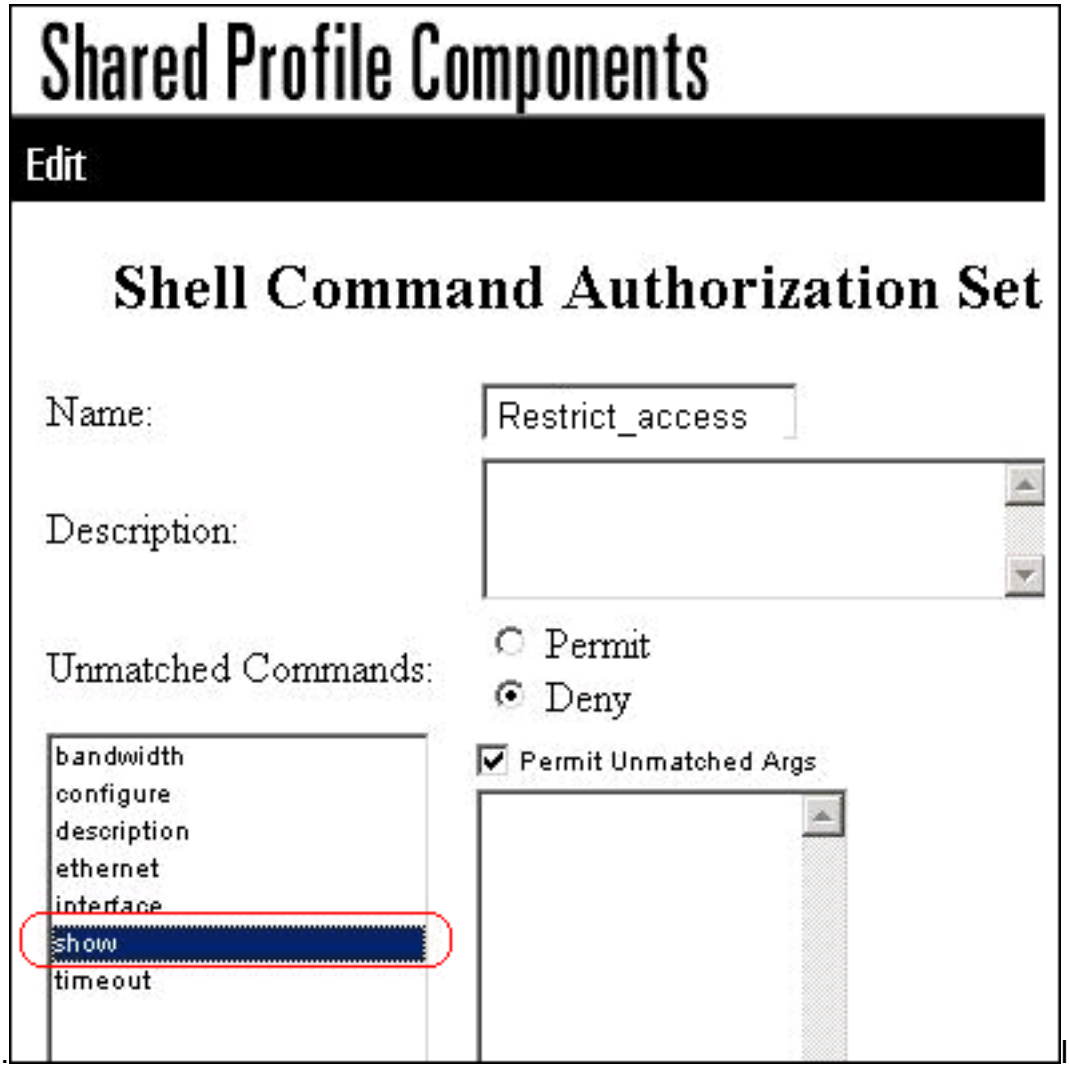


Cenário 3: Privilégio para o acesso restrito

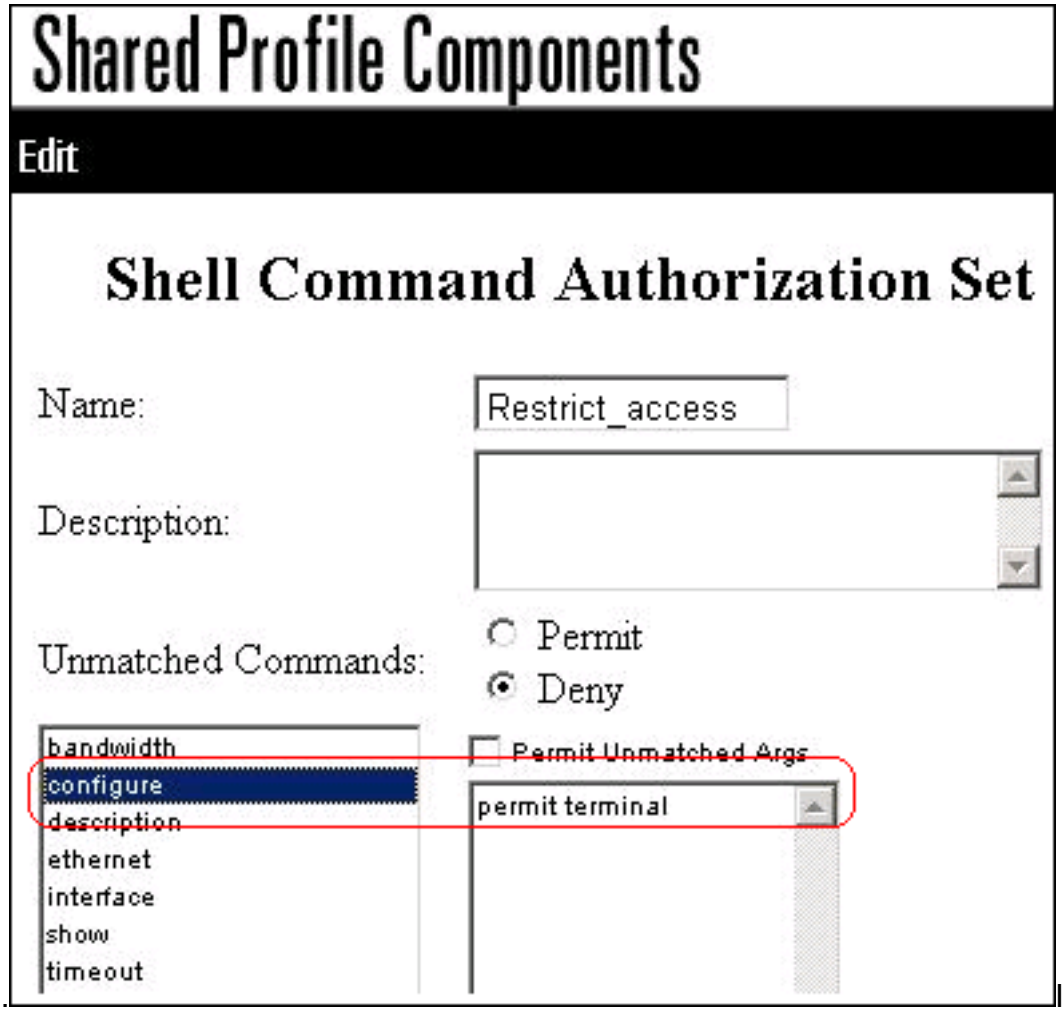
Nesta encenação, os usuários podem usar comandos seletivos.

Na área ajustada da autorização do comando shell do indicador dos componentes de perfil compartilhado, configurar estes ajustes:

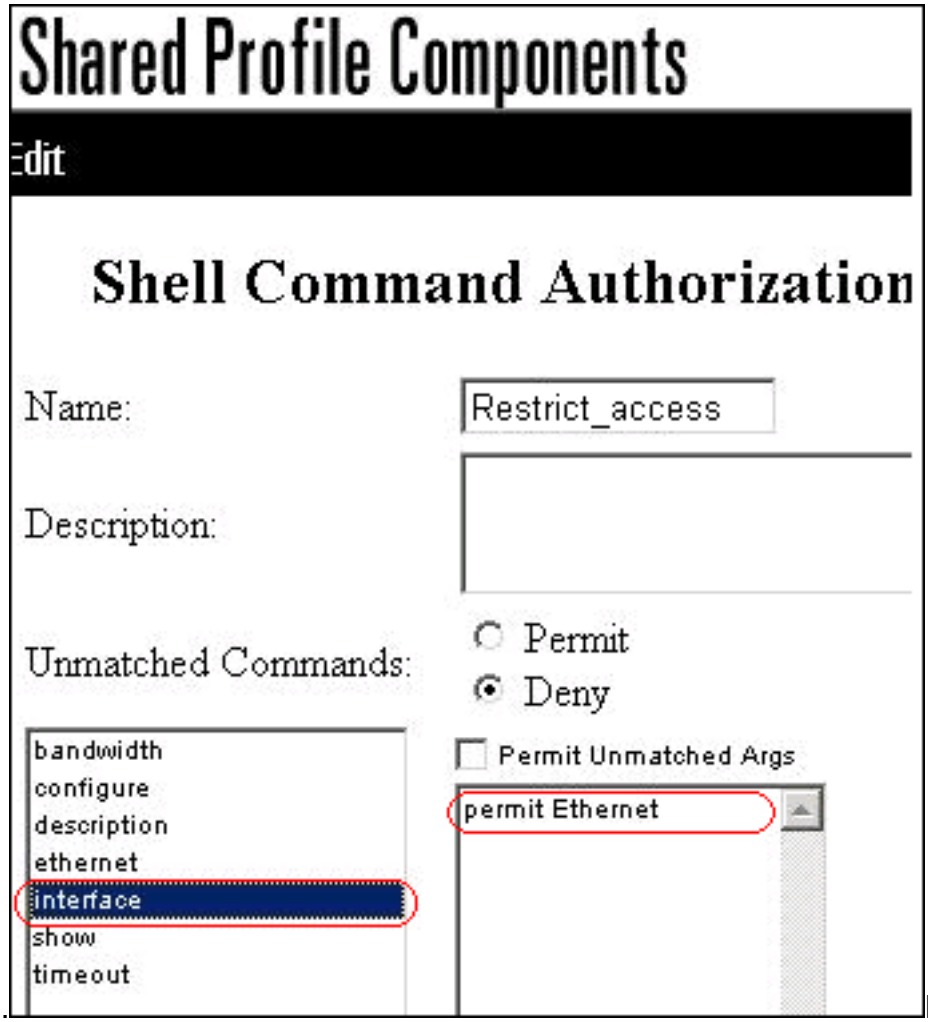
1. No campo de nome, entre em **Restrict_access** como o nome do grupo do comando authorization.
2. Clique o botão de rádio da **negação**.
3. Incorpore os comandos que você quer permitir nos clientes de AAA.No campo situado acima do botão de comando Add, inscreva o **comando show**, e clique o **comando**



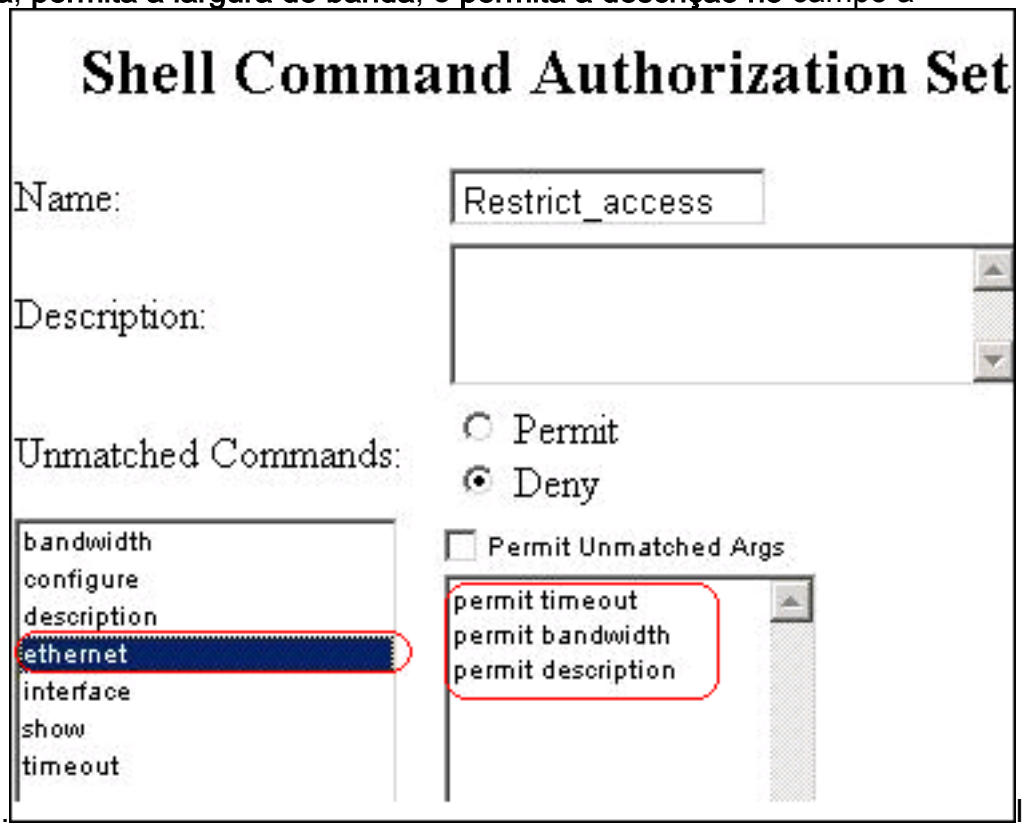
Add.Inscreva o **comando configure**, e clique o **comando Add**.Selecione o **comando configure**, e entre no **terminal da licença no** campo à



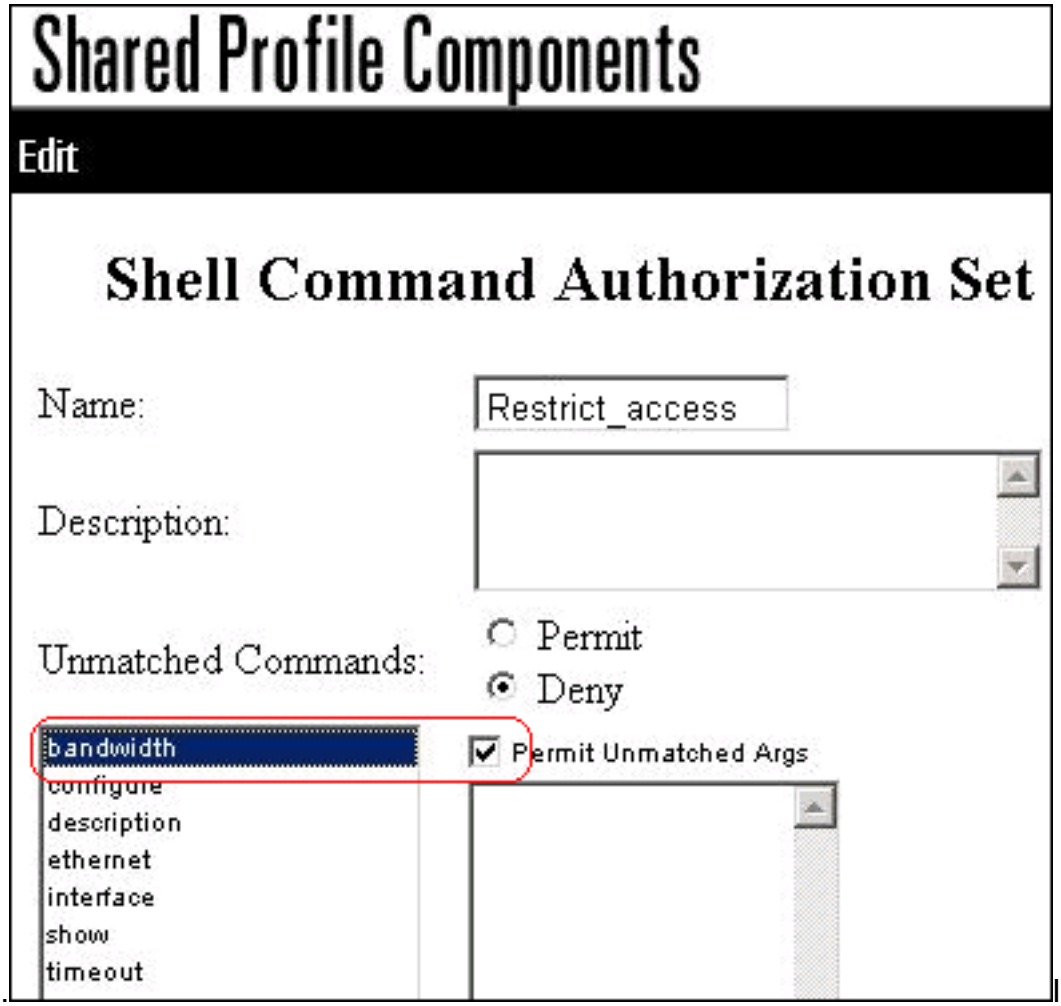
direita.Inscreva o **comando interface**, e clique o **comando Add**.Selecione o **comando interface**, e incorpore **Ethernet da licença ao** campo à



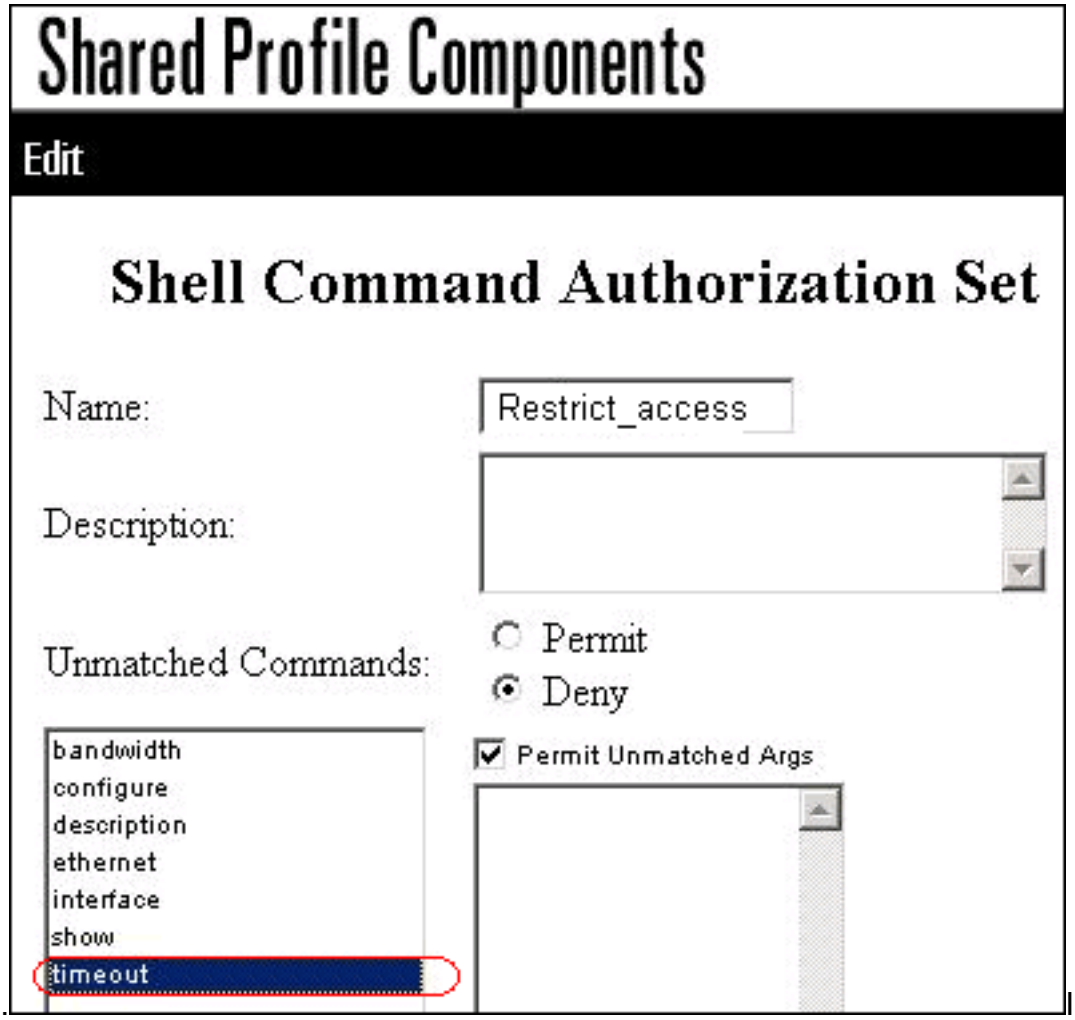
direita.Inscreva o **comando ethernet**, e clique o **comando Add**.Selecione o **comando interface**, e incorpore o **intervalo da licença**, **permita a largura de banda**, e **permita a descrição no** campo à



direita.Inscreva o **comando bandwidth**, e clique o **comando**

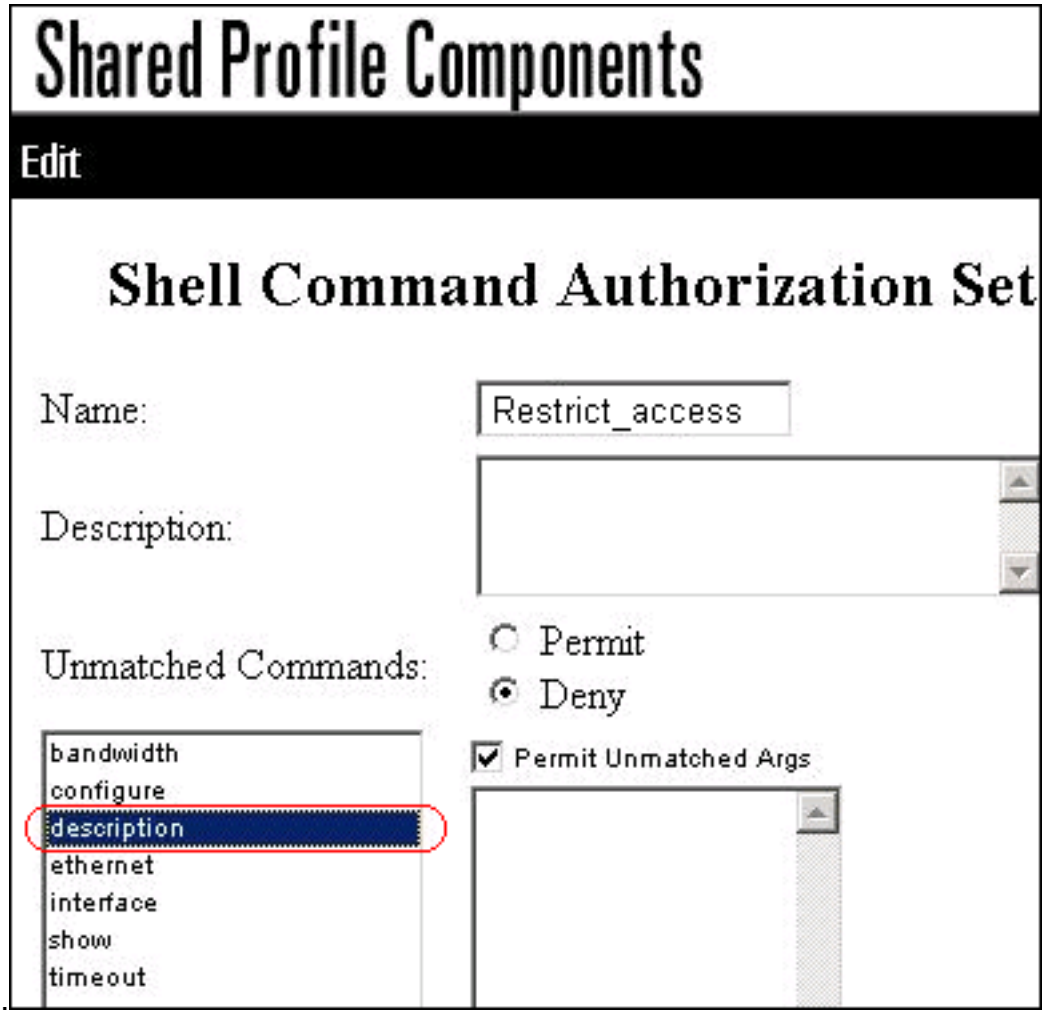


Add. Inscreva o **comando timeout**, e clique o **comando**



Add. Inscreva o **comando description**, e clique o **comando**

Add.



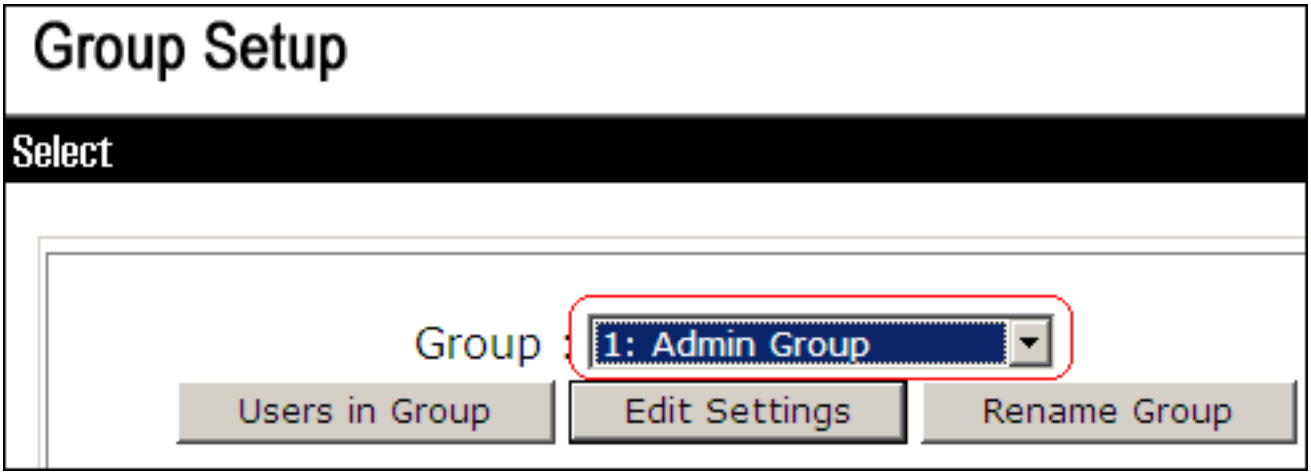
4. Clique em Submit.

Associe a autorização do comando shell ajustada ao grupo de usuário

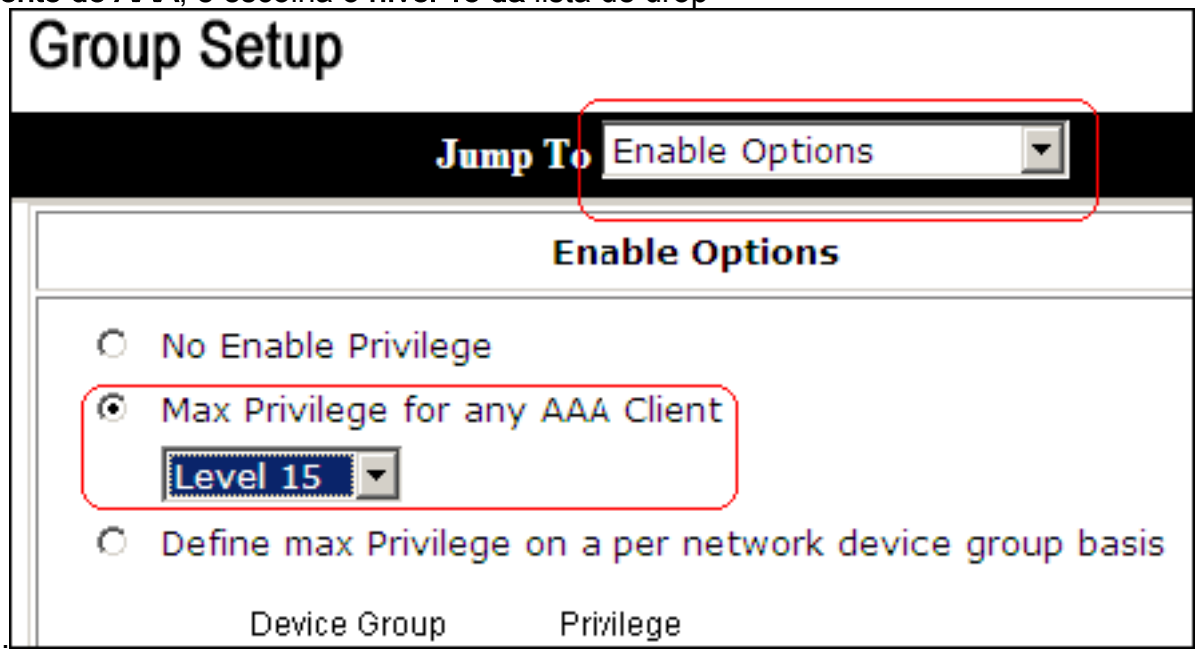
Refira configurar uma autorização do comando shell ajustada para uma seção do grupo de usuário do Guia do Usuário para o Serviço de controle de acesso Cisco Secure 4.1 para obter mais informações sobre de como configurar a configuração ajustada da autorização do comando shell para grupos de usuário.

Associe a autorização do comando shell ajustada (acesso de leitura/gravação) ao grupo de usuário (o admin group)

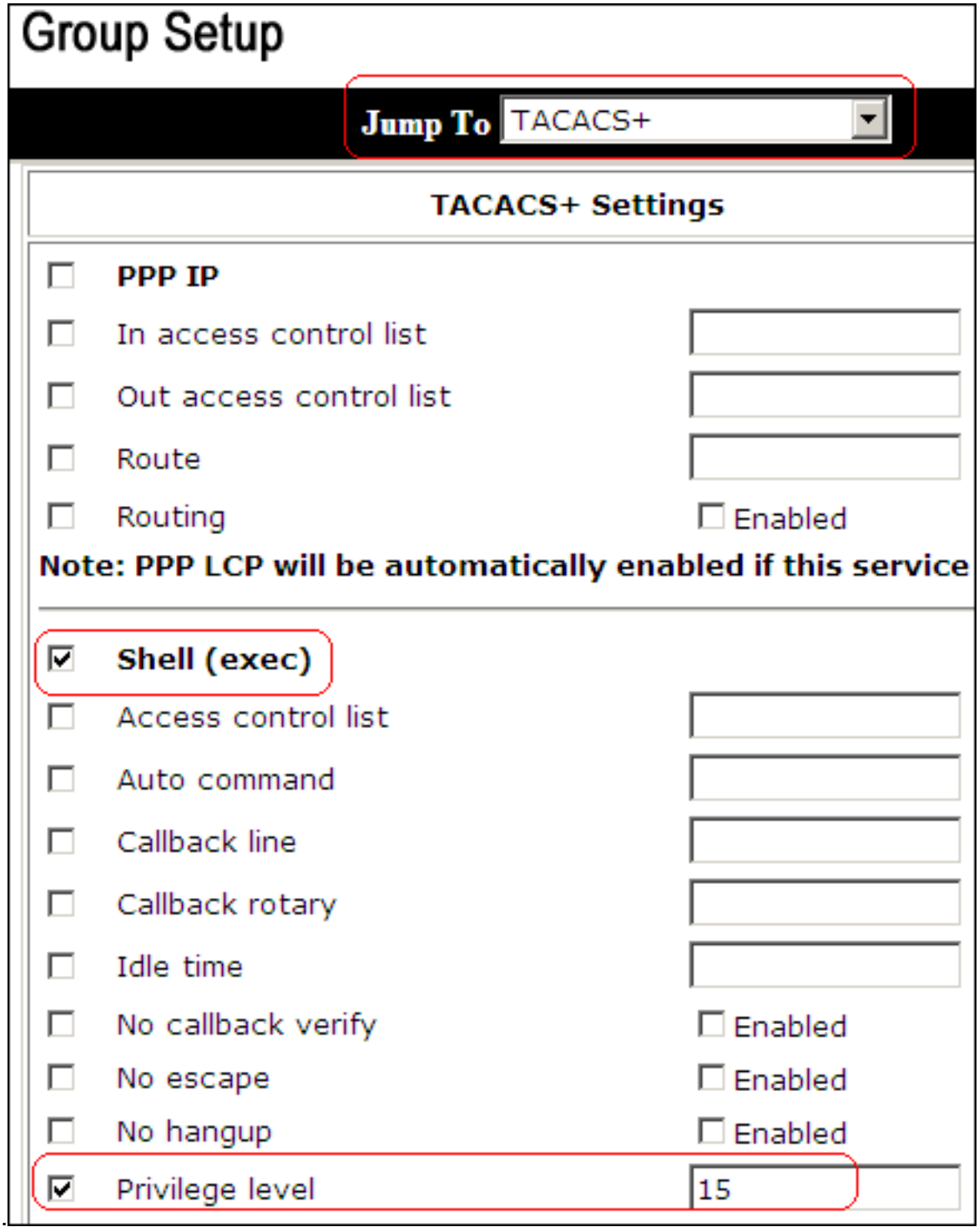
1. Na janela de ACS, clique a **instalação de grupo**, e escolha o **admin group da** lista de drop-down do
grupo.



2. O clique **edita ajustes**.
3. Do salto à lista de drop-down, escolha **permitem opções**.
4. Na área das opções da possibilidade, clique o **privilégio máximo para todo o** botão de rádio do **cliente de AAA**, e escolha o **nível 15 da** lista de drop-down.

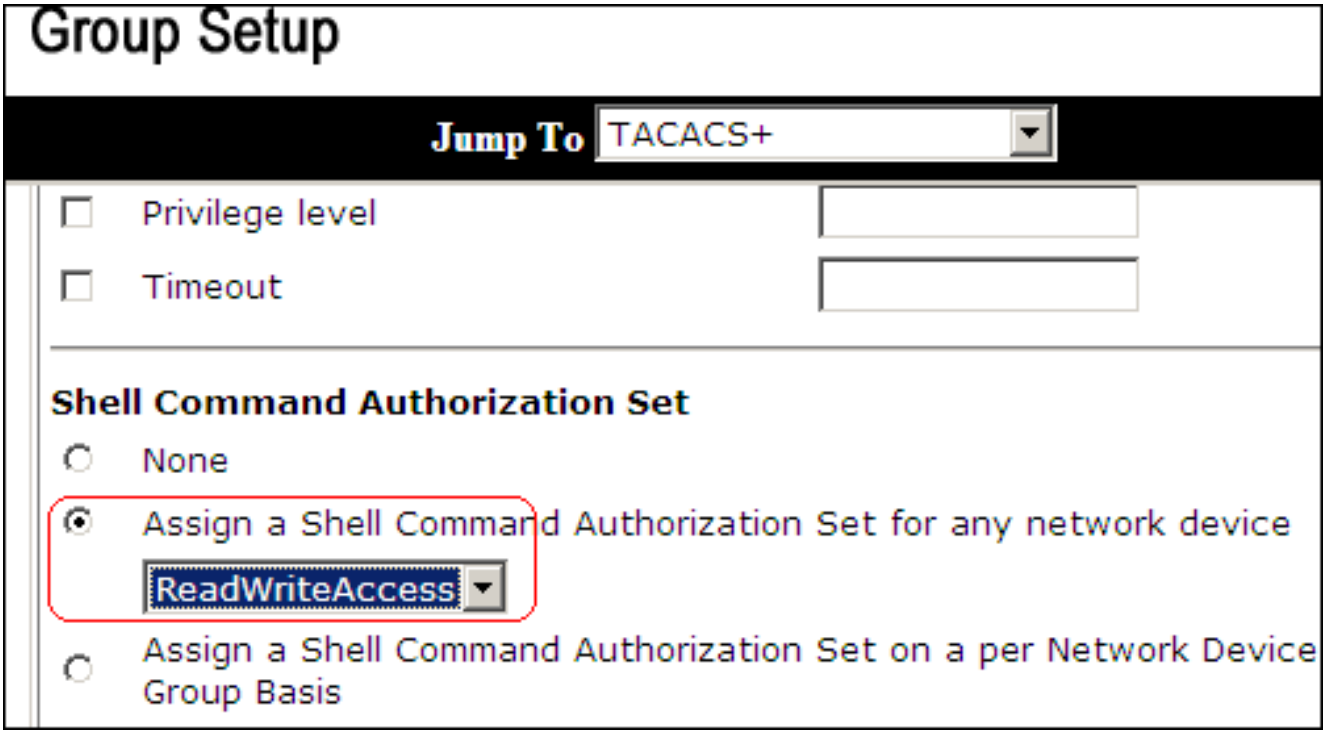


5. Do salto à lista de drop-down, escolha o **TACACS+**.
6. Na área dos ajustes TACACS+, verifique a caixa de verificação do **shell (exec)**, verifique a caixa de verificação do **nível de privilégio**, e incorpore **15 ao** campo do nível de



privilégio.

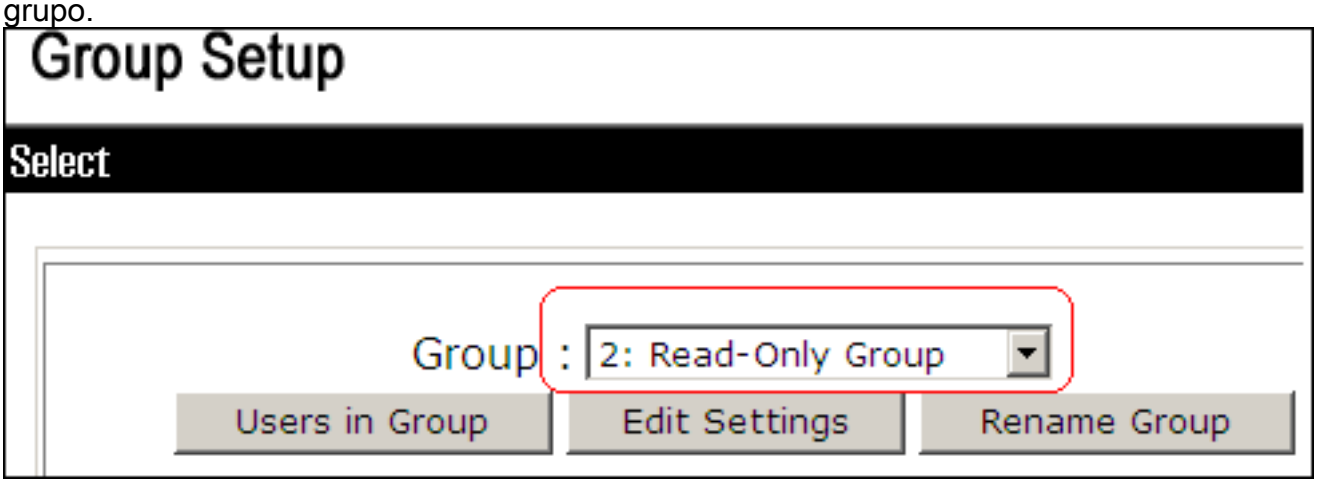
7. Na área ajustada da autorização do comando shell, clique a **atribuição uma autorização do comando shell ajustada para todo o** botão de rádio do **dispositivo de rede**, e escolha **ReadWriteAccess da** lista de drop-down.



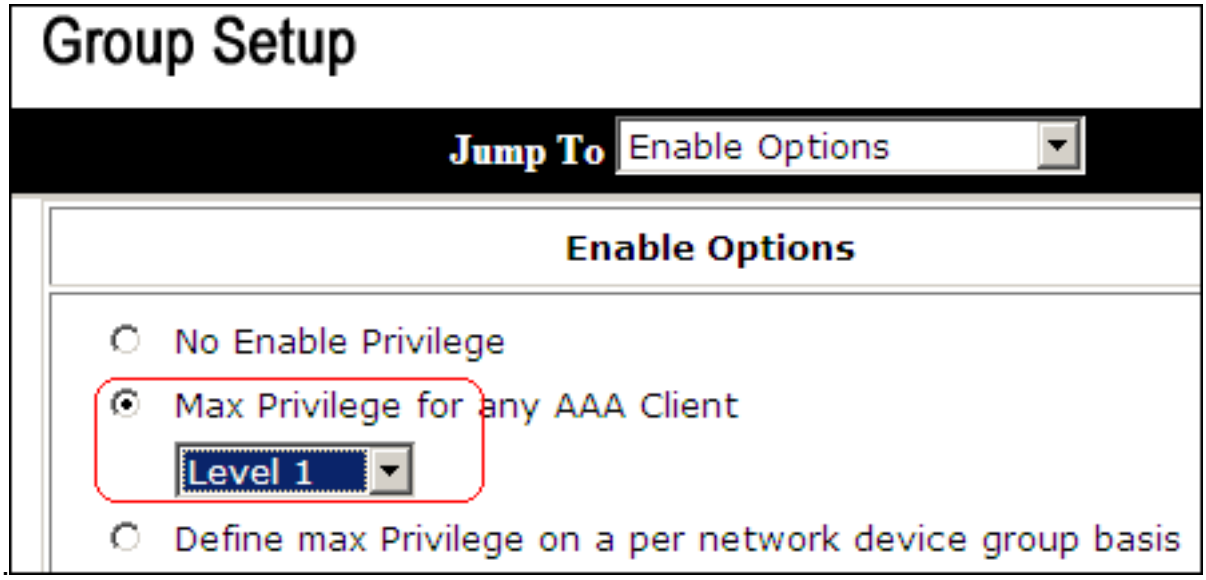
8. O clique **submete-se**

Associe a autorização do comando shell ajustada (acesso de leitura apenas) ao grupo de usuário (o grupo de leitura apenas)

1. Na janela de ACS, clique a **instalação de grupo**, e escolha o **grupo de leitura apenas da** lista de drop-down do grupo.

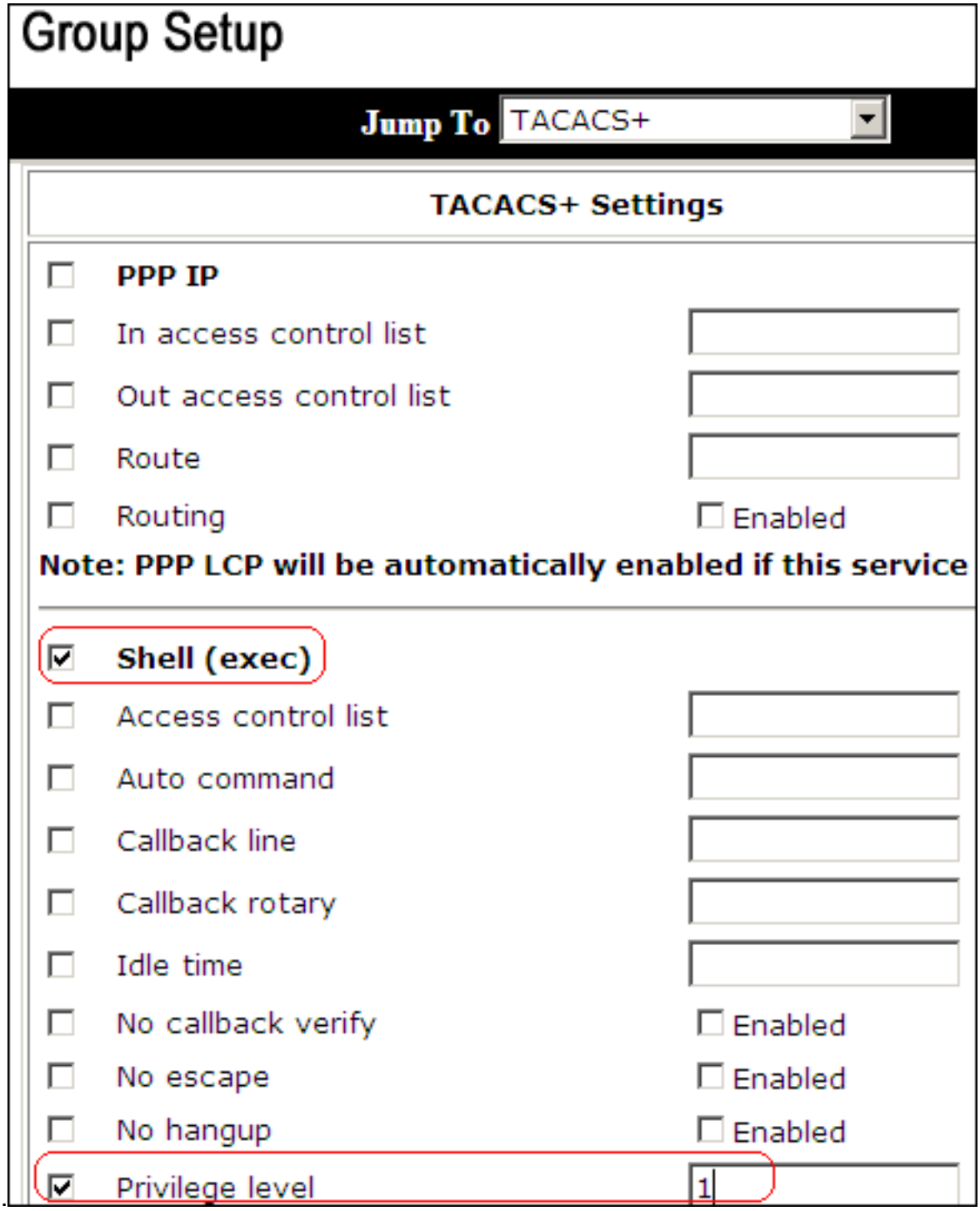


2. O clique **edita ajustes**.
3. Do salto à lista de drop-down, escolha **permitem opções**.
4. Na área das opções da possibilidade, clique o **privilégio máximo para todo o** botão de rádio do **cliente de AAA**, e escolha o **nível 1 da** lista de drop-

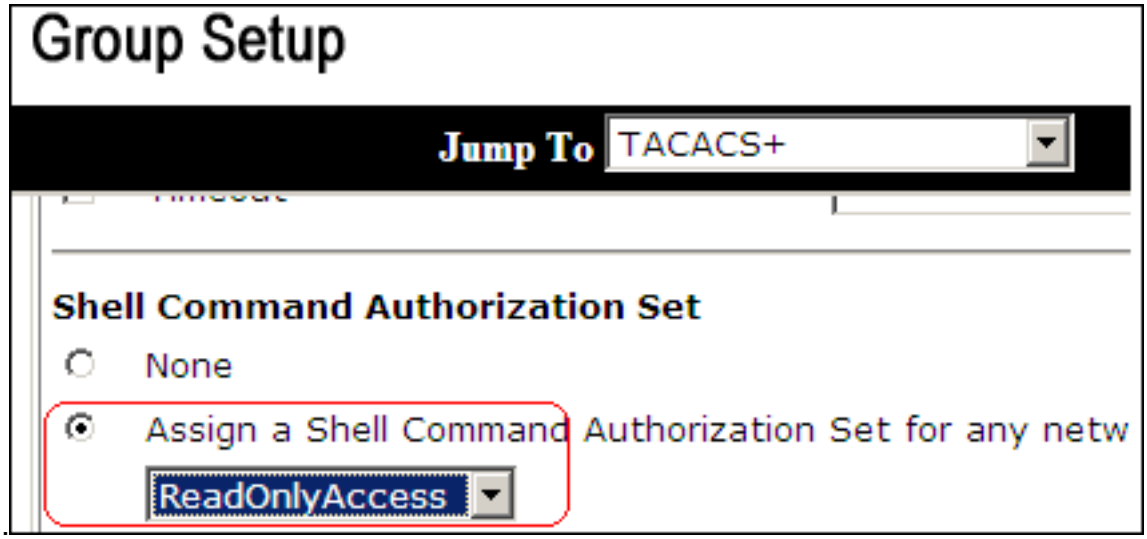
down. 

5. Na área dos ajustes TACACS+, verifique a caixa de verificação do **shell (exec)**, verifique a caixa de verificação do **nível de privilégio**, e incorpore **1 ao** campo do nível de

privilégio.



6. Na área ajustada da autorização do comando shell, clique a **atribuição uma autorização do comando shell ajustada para todo o** botão de rádio do **dispositivo de rede**, e escolha **ReadOnlyAccess da** lista de drop-

down. 

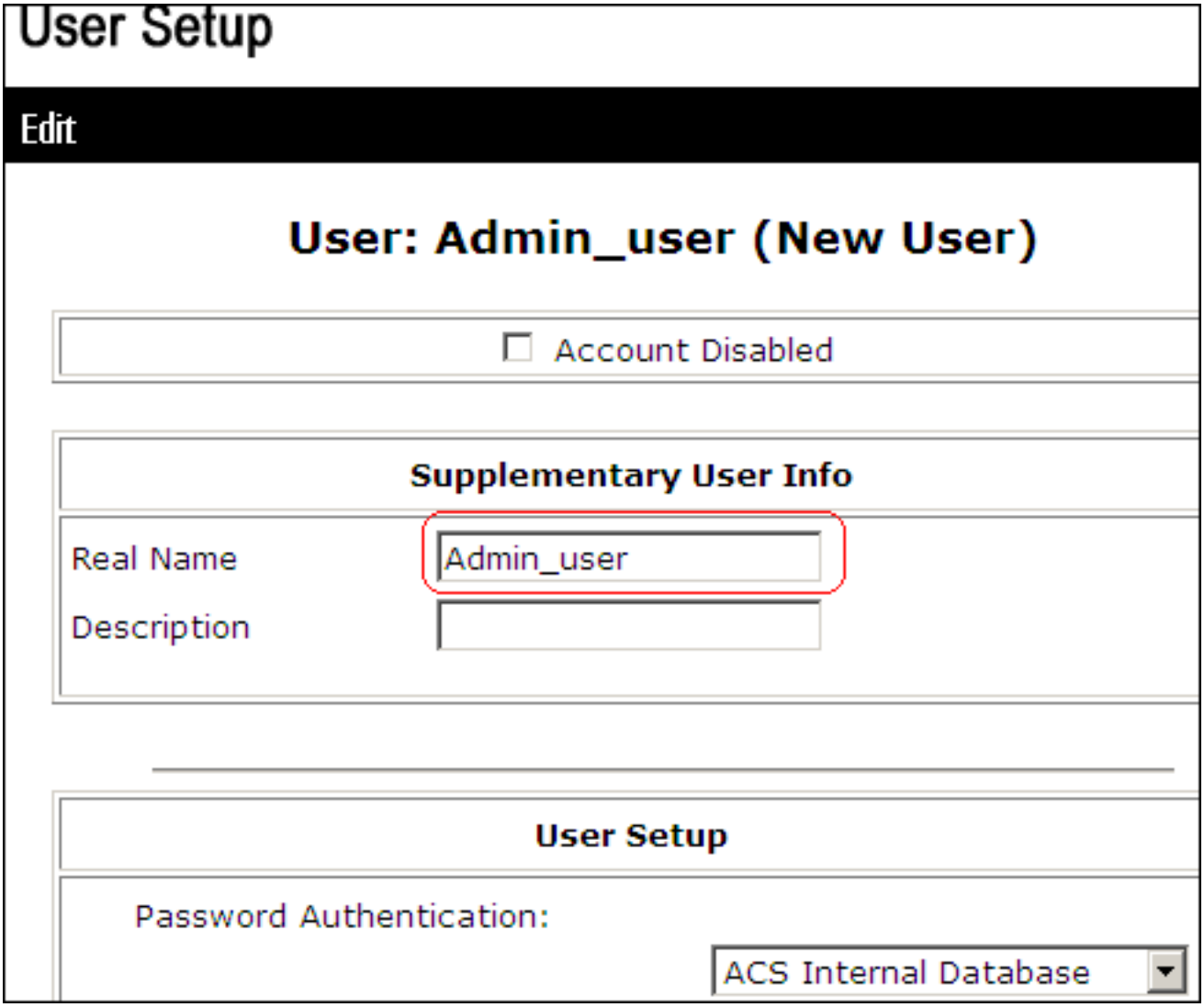
7. O clique **submete-se**

Associe a autorização do comando shell ajustada (Restrict_access) ao usuário

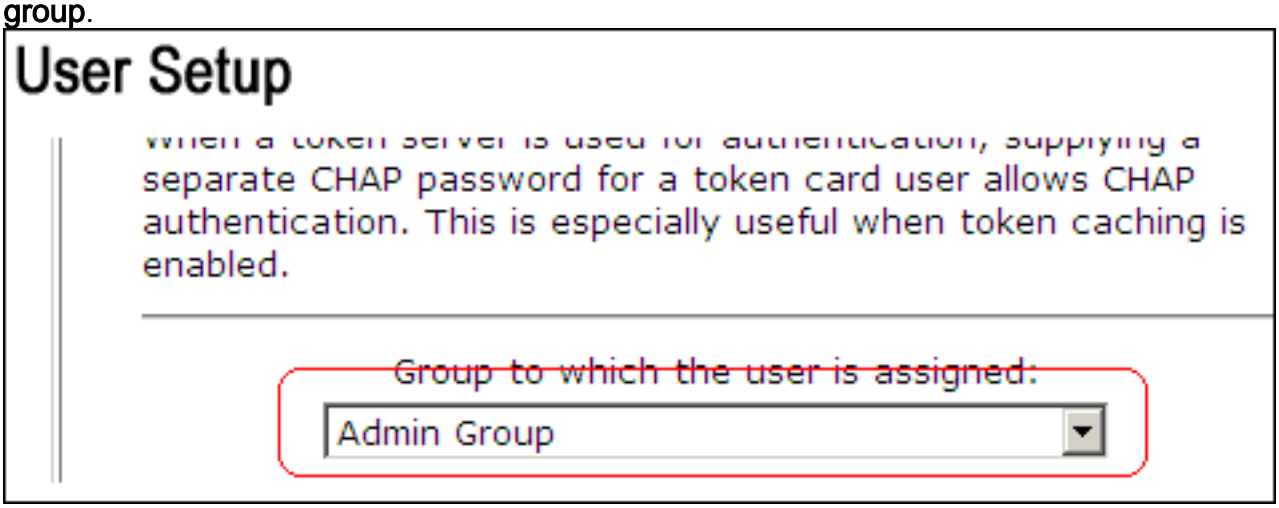
Refira configurar uma autorização do comando shell ajustada para uma seção do usuário do Guia do Usuário para o Serviço de controle de acesso Cisco Secure 4.1 para obter mais informações sobre de como configurar a configuração ajustada da autorização do comando shell para usuários.

Nota: Os ajustes do nível de usuário cancelam ajustes do grupo-nível no ACS, que significa se o usuário tem a autorização do comando shell ajustada nos ajustes do nível de usuário, a seguir cancela os ajustes do grupo-nível.

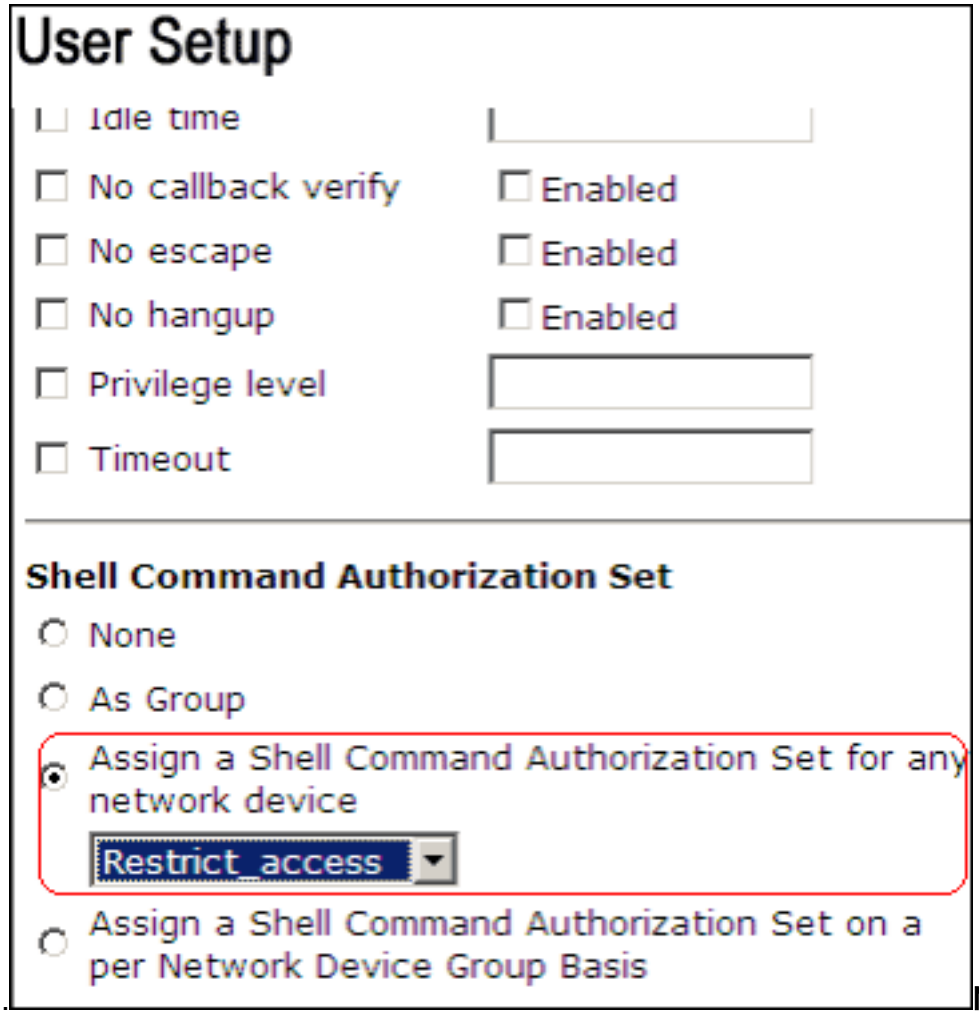
1. **O > Add da instalação de usuário do** clique**/edita** a fim criar um novo usuário nomeado *Admin_user* para ser parte de admin
   group.



2. Do grupo a que o usuário é atribuído a lista de drop-down, escolha o **admin group**.



3. Na área ajustada da autorização do comando shell, clique a **atribuição uma autorização do comando shell ajustada para todo o** botão de rádio do **dispositivo de rede**, e escolha **Restrict_access da** lista de drop-down.**Nota:** Nesta encenação, este usuário é parte de admin group. O grupo da autorização do shell de *Restrict_access* é aplicável; o grupo *de leitura/gravação da* autorização do shell do *acesso* não é



aplicável. **Nota:** Na seção TACACS+ (Cisco) da área da configuração da interface, assegure-se de que a opção do **shell (exec)** esteja selecionada na coluna do usuário.

Configuração do IOS Router

Além do que sua configuração do pré-ajuste, estes comandos são exigidos em um IOS Router ou em um interruptor a fim executar o comando authorization através de um servidor ACS:

```
aaa new-model
aaa authorization config-commands
aaa authorization commands 0 default  group tacacs+ local
aaa authorization commands 1 default  group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
tacacs-server host 10.1.1.1
tacacs-server key cisco123
```

Configuração ASA/PIX/FWSM

Além do que sua configuração do pré-ajuste, estes comandos são exigidos em ASA/PIX/FWSM a fim executar o comando authorization através de um servidor ACS:

```
aaa-server authserver protocol tacacs+
aaa-server authserver host 10.1.1.1
aaa authorization command authserver
```

Nota: Não é possível usar o protocolo de raio a fim restringir o acesso de usuário ao ASDM para finalidades de leitura apenas. Desde que os pacotes de informação de RADIUS contêm a authentication e autorização ao mesmo tempo, todos os usuários que são autenticados no

servidor Radius têm um nível de privilégio de 15. Você pode conseguir este com o TACACS com a aplicação de grupos do comando authorization.

Nota: ASA/PIX/FWSM tomam um muito tempo executar cada comando datilografado mesmo se o ACS é não disponível executar o comando authorization. Se o ACS é não disponível e o ASA tem o comando authorization configurado, o ASA ainda pedirá o comando authorization para cada comando.

Troubleshooting

Erro: comando authorization falhado

Problema

Depois que você entra ao Firewall com o TACACS que registra, os comandos não trabalham. Quando você incorpora um comando, este erro está recebido: `comando authorization falhado`.

Solução

Siga estes passos para resolver esse problema:

1. Assegure-se de que o nome de usuário correto esteja usado e que todos os privilégios exigidos estão atribuídos ao usuário.
2. Se o nome de usuário e os privilégios estão corretos, verifique que o ASA tem a Conectividade com o ACS e que o ACS é ativo.

Nota: Este erro pode igualmente ocorrer se a autorização do comando configurado do administrador equivocadamente para o local, assim como TACACS, usuários. Neste caso, execute uma recuperação de senha a fim resolver a edição.

Informações Relacionadas

- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Página de suporte segura do Access Control Server do controle de Cisco
- Suporte Técnico e Documentação - Cisco Systems