Como configurar o Cisco VPN 3000 Concentrator para suportar a autenticação TACACS+ para contas de gerenciamento

Contents

Introduction

Este documento fornece instruções passo a passo para configurar os Cisco VPN 3000 Series Concentrators para suportar a autenticação TACACS+ para contas de gerenciamento.

Assim que um servidor TACACS+ é configurado no VPN 3000 Concentrator, os nomes de conta e as senhas configuradas localmente, como admin, config, isp e assim por diante, não são mais usados. Todos os logins do VPN 3000 Concentrator são enviados ao servidor TACACS+ externo configurado para verificação de usuário e senha.

A definição de um nível de privilégio para cada usuário no servidor TACACS+ determina as permissões no VPN 3000 Concentrator para cada nome de usuário TACACS+. Em seguida, faça a correspondência com o nível de acesso AAA definido sob o nome de usuário configurado localmente no VPN 3000 Concentrator. Este é um ponto importante porque assim que um servidor TACACS+ é definido, os nomes de usuário configurados localmente no VPN 3000 Concentrator não são mais válidos. No entanto, eles ainda são usados somente para corresponder o nível de privilégio retornado do servidor TACACS+ com o nível de acesso AAA sob esse usuário local. Em seguida, o nome de usuário TACACS+ recebe os privilégios que o usuário do VPN 3000 Concentrator configurado localmente definiu sob seu perfil.

Por exemplo, descrito em detalhes nas seções de configuração, um usuário/grupo TACACS+ é configurado para retornar um nível de privilégio TACACS+ de 15. Na seção Administrators do VPN 3000 Concentrator, o usuário administrador tem seu nível de acesso AAA também definido como 15. Este usuário tem permissão para modificar a configuração em todas as seções e para ler/gravar arquivos. Como o nível de privilégio TACACS+ e o nível de acesso AAA correspondem, o usuário TACACS+ recebe essas permissões no VPN 3000 Concentrator.

Como exemplo, se você decidir que um usuário precisa ser capaz de modificar a configuração, mas *não* ler/gravar arquivos, atribua a ele um nível de privilégio de 12 no servidor TACACS+. Você pode escolher qualquer número entre um e 15. Em seguida, no VPN 3000 Concentrator, escolha um dos outros administradores configurados localmente. Em seguida, defina seu nível de acesso AAA como 12 e defina as permissões desse usuário para poder modificar a configuração, mas não para ler/gravar arquivos. Devido ao nível de privilégio/acesso correspondente, o usuário obtém essas permissões ao fazer logon.

Os nomes de usuário configurados localmente no VPN 3000 Concentrator não são mais usados. No entanto, os Direitos de Acesso e os Níveis de Acesso AAA sob cada um desses usuários são usados para definir os privilégios que um usuário TACACS+ específico obtém quando você faz login.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Verifique se você tem conectividade IP com o servidor TACACS+ do VPN 3000 Concentrator. Se o servidor TACACS+ estiver em direção à interface pública, não se esqueça de abrir o TACACS+ (porta TCP 49) no filtro público .
- Verifique se o acesso de backup via console está operacional. É fácil bloquear acidentalmente todos os usuários fora da configuração quando você configura isso pela primeira vez. A única maneira de recuperar o acesso é através do console, que ainda usa os nomes de usuário e as senhas configurados localmente.

Componentes Utilizados

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

- Software Cisco VPN 3000 Concentrator versão 4.7.2.B (Alternativamente, qualquer versão do software do SO 3.0 ou posterior funciona.)
- Cisco Secure Access Control Server para servidores Windows versão 4.0 (como alternativa, qualquer versão de software 2.4 ou posterior funciona.)

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

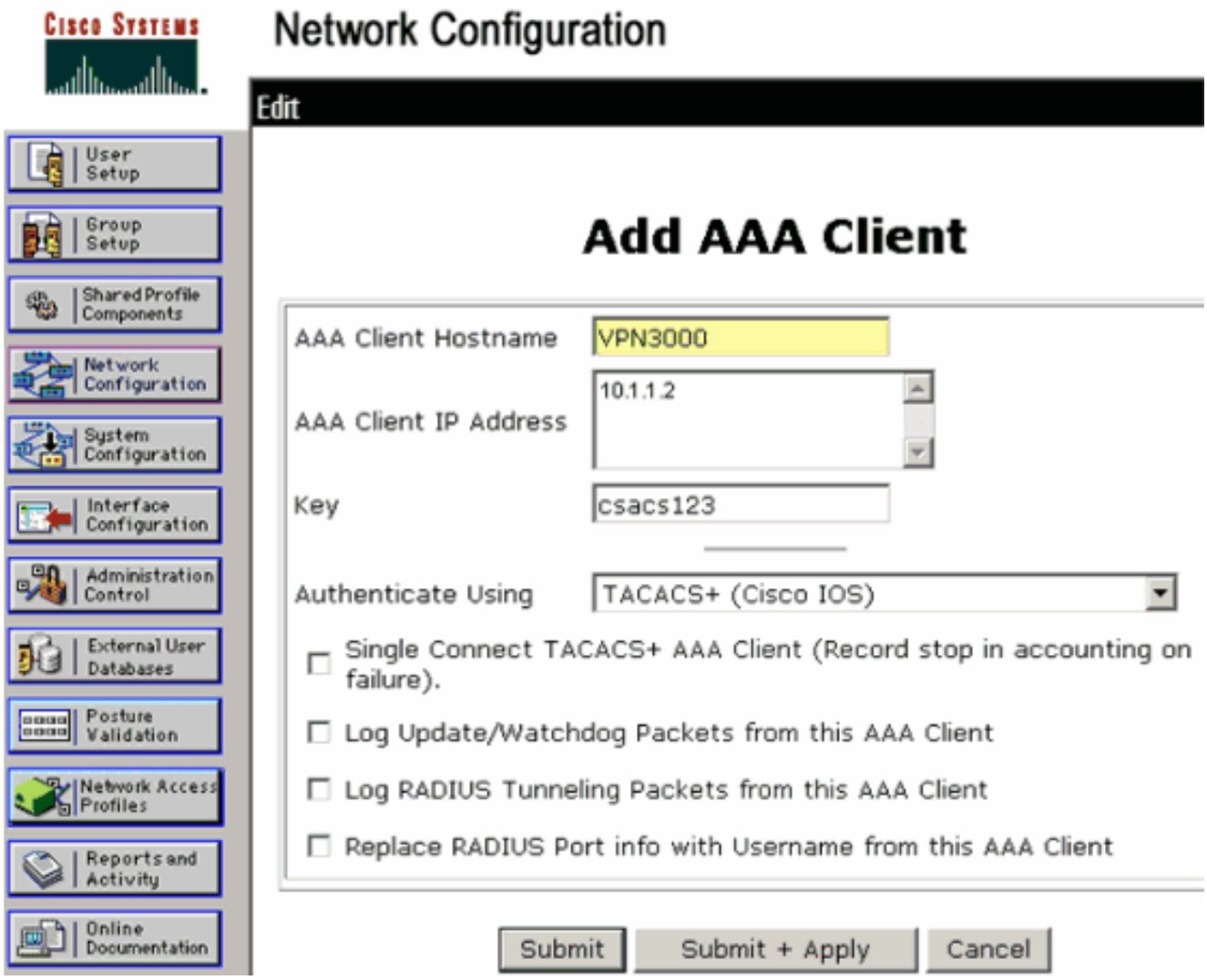
convenções de documentos.

Configurar o servidor TACACS+

Adicione uma entrada para o VPN 3000 Concentrator no servidor TACACS+

Conclua estes passos para adicionar uma entrada para o VPN 3000 Concentrator no servidor TACACS+.

1. Clique em **Network Configuration (Configuração de rede)** no painel esquerdo. Em AAA Clients, clique em Add Entry.
2. Na próxima janela, preencha o formulário para adicionar o VPN Concentrator como o cliente TACACS+. Este exemplo usa:AAA Client Hostname = **VPN3000**Endereço IP do cliente AAA = **10.1.1.2**Chave = **csacs123**Autenticar usando = **TACACS+ (Cisco IOS)**Clique em **Enviar + Reiniciar**.



Adicionar uma conta de usuário no servidor TACACS+

Conclua estes passos para adicionar uma conta de usuário no servidor TACACS+.

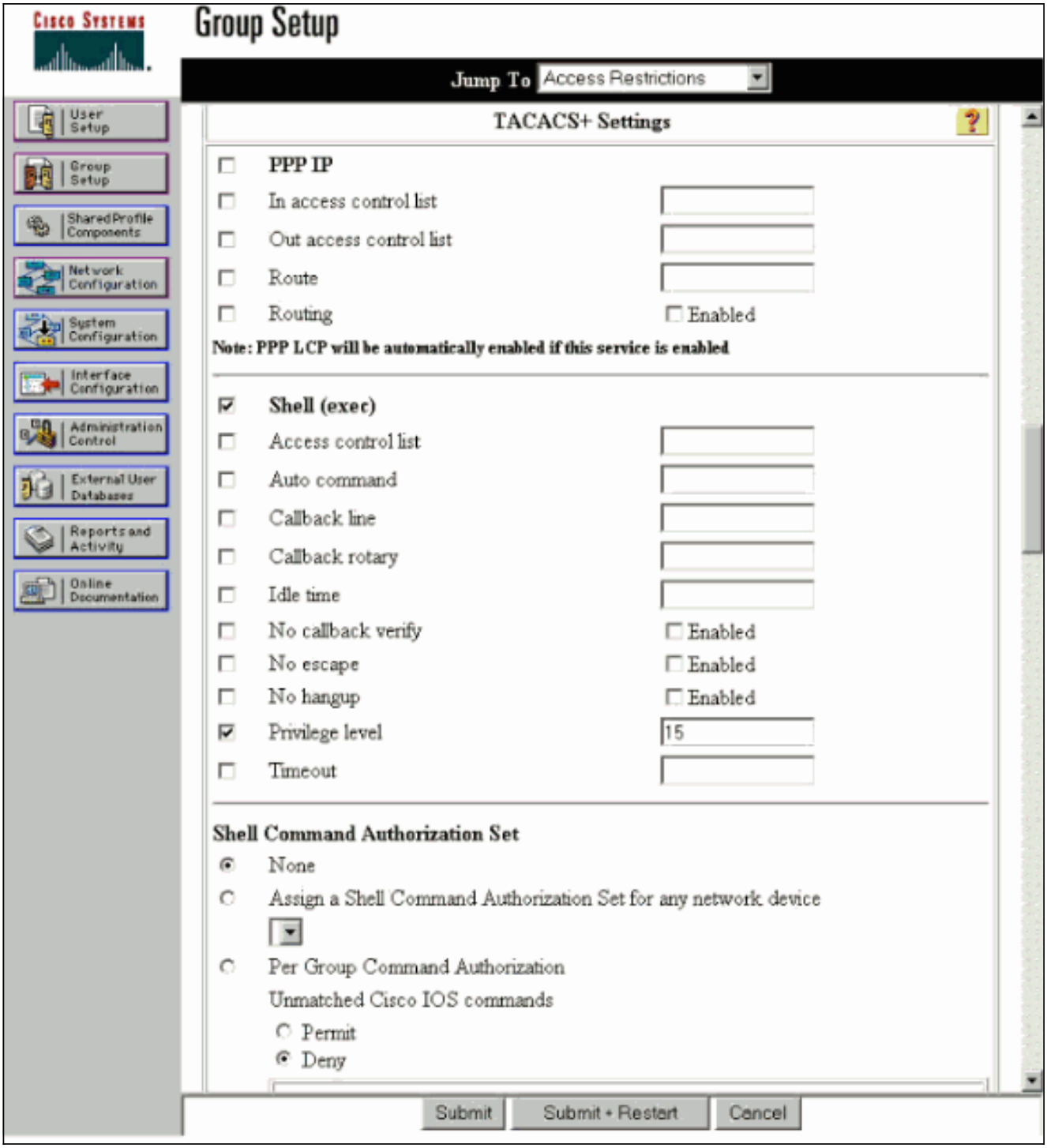
1. Crie uma conta de usuário no servidor TACACS+ que possa ser usada posteriormente para autenticação TACACS+. Clique em **User Setup** no painel esquerdo, adicione o usuário

"johnsmith" e clique em **Add/Edit** para fazer isso.
2. Adicione uma senha para esse usuário e atribua o usuário a um grupo ACS que contenha os outros administradores do VPN 3000 Concentrator.**Observação:** este exemplo define o nível de privilégio neste perfil de grupo ACS específico do usuário. Se isso for feito por usuário, escolha **Interface Configuration > TACACS+ (Cisco IOS)** e marque a caixa **User** para o serviço Shell (exec). Somente então as opções TACACS+ descritas neste documento estão disponíveis em cada perfil de usuário.

Edite o Grupo no Servidor TACACS+

Conclua estes passos para editar o grupo no servidor TACACS+.

1. Clique em **Group Setup (Configuração de grupo)** no painel esquerdo.
2. No menu suspenso, escolha o grupo ao qual o usuário foi adicionado na seção Adicionar uma conta de usuário no servidor TACACS+, que é Grupo 1 neste exemplo, e clique em **Editar configurações**.
3. Na próxima janela, certifique-se de que esses atributos estejam selecionados em TACACS+ Settings:**Shell (exec)Nível de privilégio = 15**Depois de concluir, clique em **Enviar + Reiniciar**.



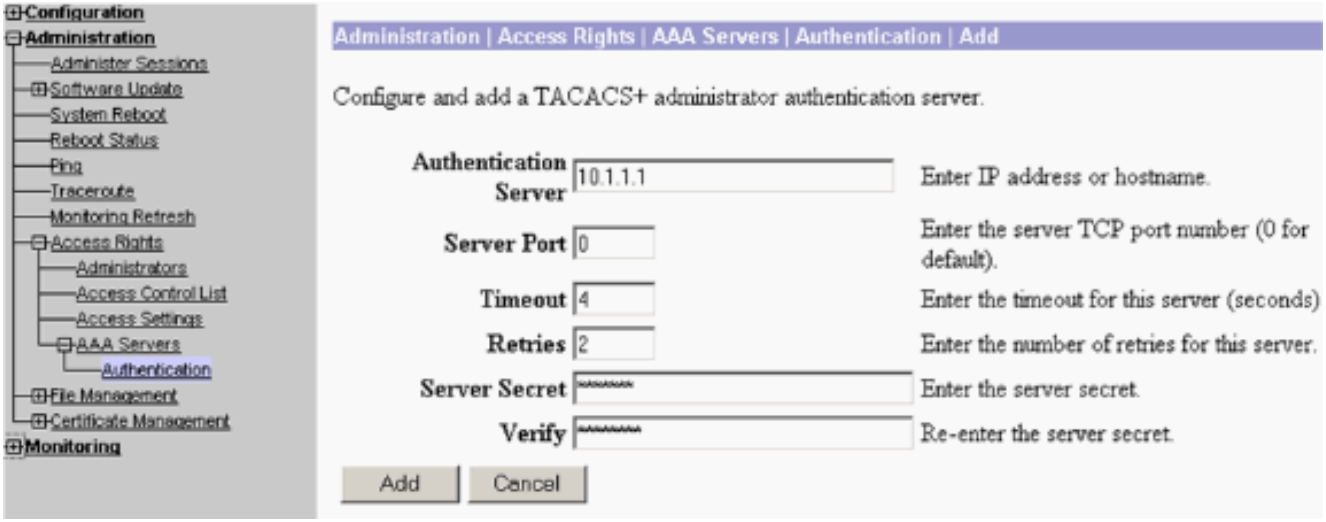
Configurar o VPN 3000 Concentrator

Adicione uma entrada para o servidor TACACS+ no VPN 3000 Concentrator

Conclua estes passos para adicionar uma entrada para o servidor TACACS+ no VPN 3000 Concentrator.

1. Escolha **Administration > Access Rights > AAA Servers > Authentication** na árvore de navegação no painel esquerdo e clique em **Add** no painel direito.Assim que você clicar em **Adicionar** para adicionar este servidor, o nome de usuário/senhas configurados localmente no VPN 3000 Concentrator não serão mais usados. Certifique-se de que o acesso de backup através do console funciona em caso de bloqueio.

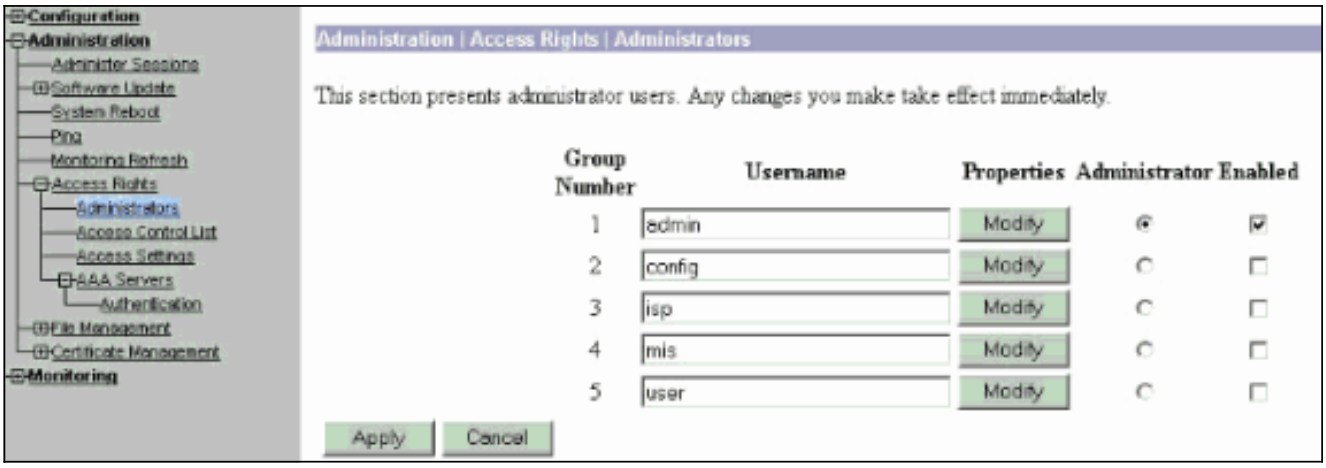
2. Na próxima janela, preencha o formulário conforme visto aqui:Servidor de autenticação = **10.1.1.1** (endereço IP do servidor TACACS+)Porta do servidor = **0** (padrão)Tempo limite = **4**Tentativas = **2**Segredo do servidor = **csacs123**Verificar = **csacs123**



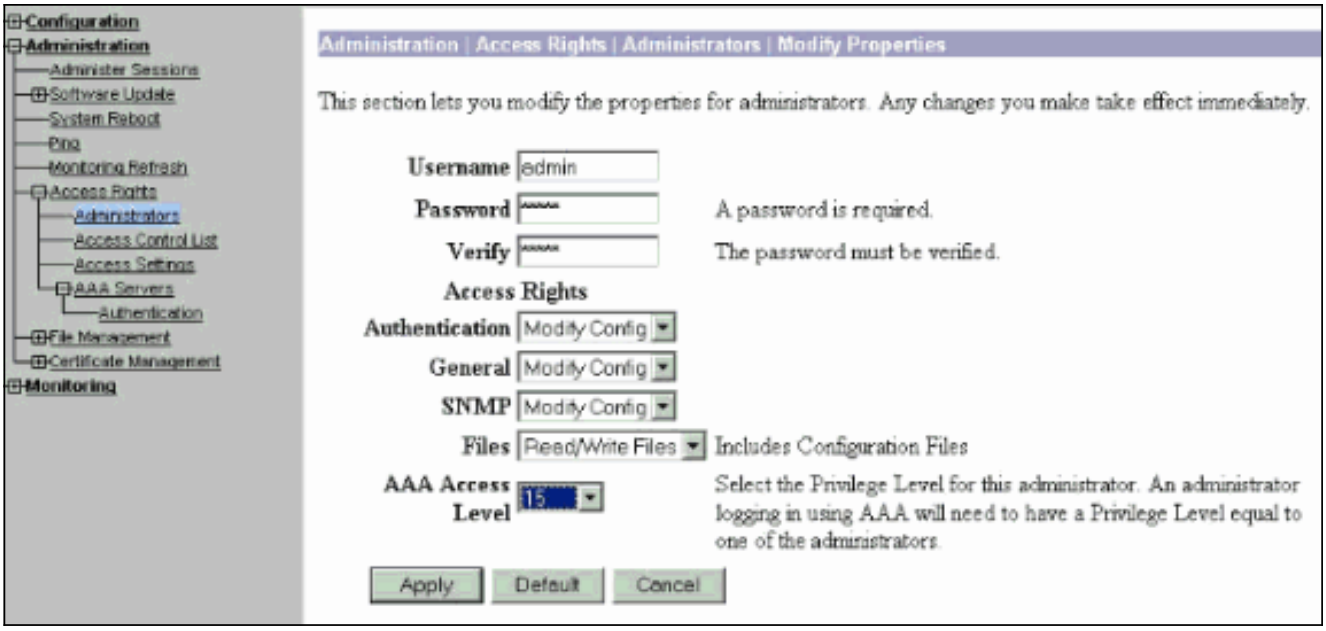
Modificar a conta do administrador no VPN Concentrator para autenticação TACACS+

Conclua estes passos para modificar a conta admin no VPN Concentrator para autenticação TACACS+.

1. Clique em **Modificar** para o administrador do usuário para modificar as propriedades deste usuário.



2. Escolha o nível de acesso AAA como **15**.Esse valor pode ser qualquer número entre um e 15. Observe que ele deve corresponder ao nível de privilégio TACACS+ definido no perfil de usuário/grupo no servidor TACACS+. O usuário do TACACS+, então, captura as permissões definidas sob esse usuário do VPN 3000 Concentrator para a modificação da configuração, leitura/gravação de arquivos e assim por diante.



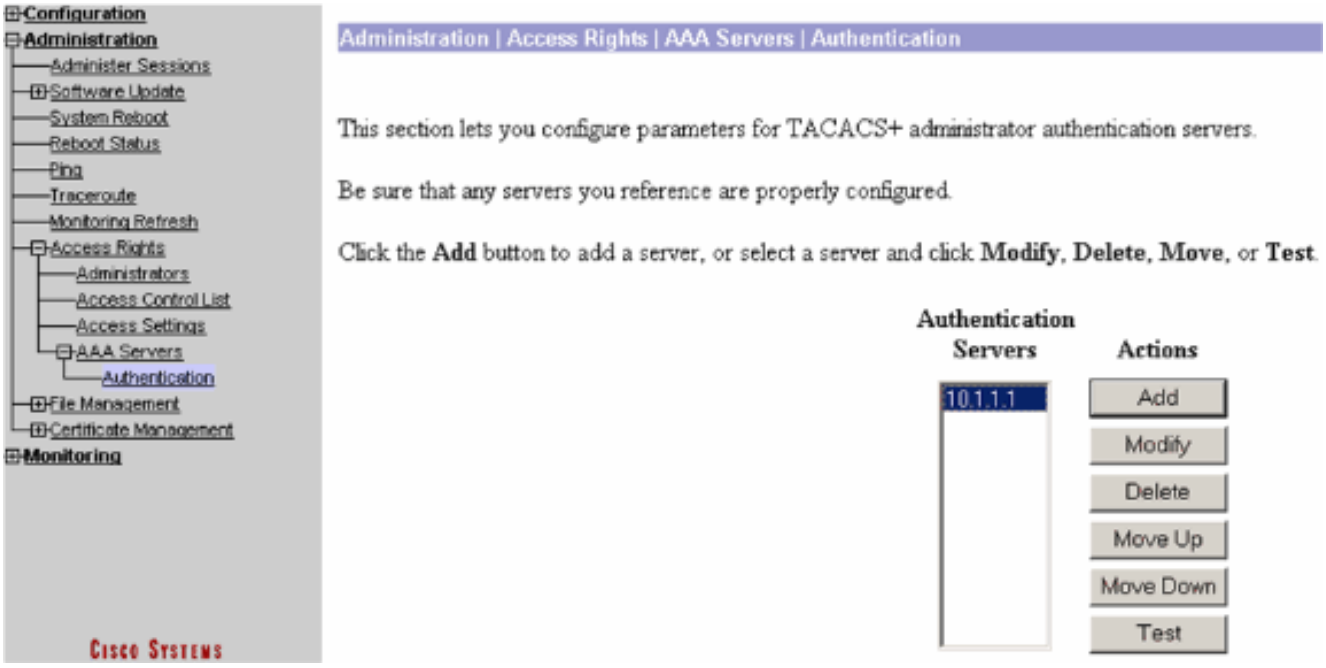
Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

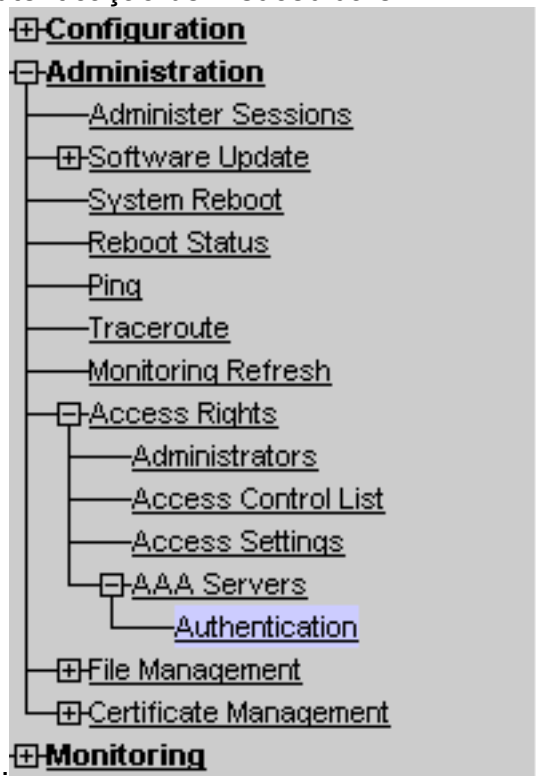
Conclua as etapas dessas instruções para solucionar problemas de sua configuração.

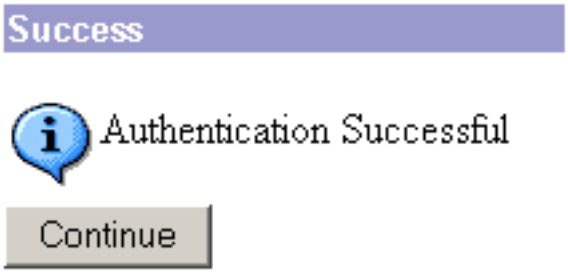
1. Para testar a autenticação:Para servidores TACACS+Escolha **Administration > Access Rights > AAA Servers > Authentication**.Selecione o servidor e clique em **Testar**.



Observação: quando o servidor TACACS+ é configurado na guia Administration (Administração), não há como configurar o usuário para autenticar no banco de dados local do VPN 3000. Você só pode recuar usando outro banco de dados externo ou servidor TACACS.Insira o nome de usuário e a senha TACACS+ e clique em **OK**.

Uma autenticação bem-sucedida é





exibida.

2. Se ele falhar, há um problema de configuração ou um problema de conectividade IP. Verifique se há mensagens relacionadas à falha no registro de tentativas com falha no servidor ACS.Se nenhuma mensagem for exibida neste registro, provavelmente há um problema de conectividade IP. A solicitação TACACS+ não chega ao servidor TACACS+. Verifique se os filtros aplicados à interface apropriada do VPN 3000 Concentrator permitem pacotes TACACS+ (porta TCP 49) de entrada e saída.Se a falha for exibida como serviço negado no registro, o serviço Shell (exec) não foi ativado corretamente no perfil de usuário ou grupo no servidor TACACS+.
3. Se a autenticação de teste for bem-sucedida, mas os logins no VPN 3000 Concentrator continuarem a falhar, verifique o Filterable Event Log através da porta de console.Se você vir uma mensagem semelhante:

```
65 02/09/2005 13:14:40.150 SEV=5 AUTH/32 RPT=2
User [ johnsmith ] Protocol [ HTTP ] attempted ADMIN logon.
Status: <REFUSED> authorization failure. NO Admin Rights
```

Essa mensagem indica que o nível de privilégio atribuído no servidor TACACS+ não tem nível de acesso AAA correspondente em nenhum dos usuários do VPN 3000 Concentrator. Por exemplo, johnsmith de usuário tem um nível de privilégio TACACS+ de 7 no servidor TACACS+, mas nenhum dos cinco administradores do VPN 3000 Concentrator tem um nível de acesso AAA de 7.

Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de suporte ao cliente do Cisco VPN 3000 Series
- Página de Suporte de Negociação IPSec/Protocolos IKE
- Página de Suporte do TACACS/TACACS+
- TACACS+ na Documentação do IOS
- Suporte Técnico e Documentação - Cisco Systems