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

Índice

Introdução

Este documento fornece instruções passo a passo a fim configurar o Concentradores Cisco VPN série 3000 para apoiar a autenticação TACACS+ para contas de gerenciamento.

Assim que um server TACACS+ estiver configurado no VPN 3000 concentrator, os nomes da conta localmente configurados e as senhas tais como o admin, configuração, isp, estiverem usadas e assim por diante já não. Todos os inícios de uma sessão ao VPN 3000 concentrator são enviados ao server externo configurado TACACS+ para o usuário e a verificação de senha.

A definição de um nível de privilégio para cada usuário no server TACACS+ determina as permissões no VPN 3000 concentrator para cada username TACACS+. Então, fósforo que acima com do nível de acesso AAA definiu sob o username localmente configurado no VPN 3000 concentrator. Este é um ponto importante porque assim que um server TACACS+ for definido, os nomes de usuário localmente configurados no VPN 3000 concentrator são já não válidos. Mas, são usados ainda a fim combinar somente acima do nível de privilégio retornado do server TACACS+, com o nível de acesso AAA sob esse usuário local. O username TACACS+ é atribuído então os privilégios que o usuário localmente configurado do VPN 3000 concentrator definiu sob seu perfil.

Por exemplo, descrito em detalhe nas seções de configuração, um usuário TACACS+/grupo é configurado para retornar um nível de privilégio TACACS+ de 15. Sob a seção dos administradores do VPN 3000 concentrator, o usuário admin tem seu nível de acesso AAA ajustado igualmente a 15. É permitido a este usuário alterar a configuração sob todas as seções, e aos arquivos de leitura/gravação. Porque o nível de privilégio TACACS+ e o nível de acesso AAA combinam, o usuário TACACS+ é dado aquelas permissões no VPN 3000 concentrator.

Como um exemplo, se você decide que um usuário precisa de poder alterar a configuração, mas os arquivos não de leitura/gravação, atribuem-lhes um nível de privilégio de 12 no server TACACS+. Você pode escolher qualquer número entre um e 15. Então, no VPN 3000 concentrator, escolha um dos outros administradores localmente configurados. Em seguida, ajuste seu nível de acesso AAA a 12, e ajuste as permissões neste usuário a fim poder alterar a configuração, mas não aos arquivos de leitura/gravação. Devido ao privilégio/nível de acesso de harmonização, o usuário obtém aquelas permissões quando entram.

Os nomes de usuário localmente configurados no VPN 3000 concentrator são usados já não. Mas, os direitos de acesso e níveis de acesso AAA sob cada um daqueles usuários é usado a fim definir os privilégios que um usuário particular TACACS+ obtém quando você entra.

Pré-requisitos

Requisitos

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

- Assegure-se de que você tenha a conectividade IP ao server TACACS+ do VPN 3000 concentrator. Se seu server TACACS+ é para a interface pública, não esqueça abrir o TACACS+ (porta TCP 49) no filtro público.
- Assegure-se de que o acesso alternativo através do console esteja operacional. É fácil travar acidentalmente todos os usuários fora da configuração quando você configura primeiramente este. A única maneira de recuperar o acesso é através do console, que ainda usa os nomes de usuário e senha localmente configurados.

Componentes Utilizados

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

- Software Release 4.7.2.B do Cisco VPN 3000 Concentrator (alternativamente, alguma liberação do 3.0 ou trabalhos mais atrasados do OS Software.)
- Liberação 4.0 dos server do Cisco Secure Access Control Server para Windows (alternadamente, alguma liberação de 2.4 ou trabalhos mais atrasados do software.)

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

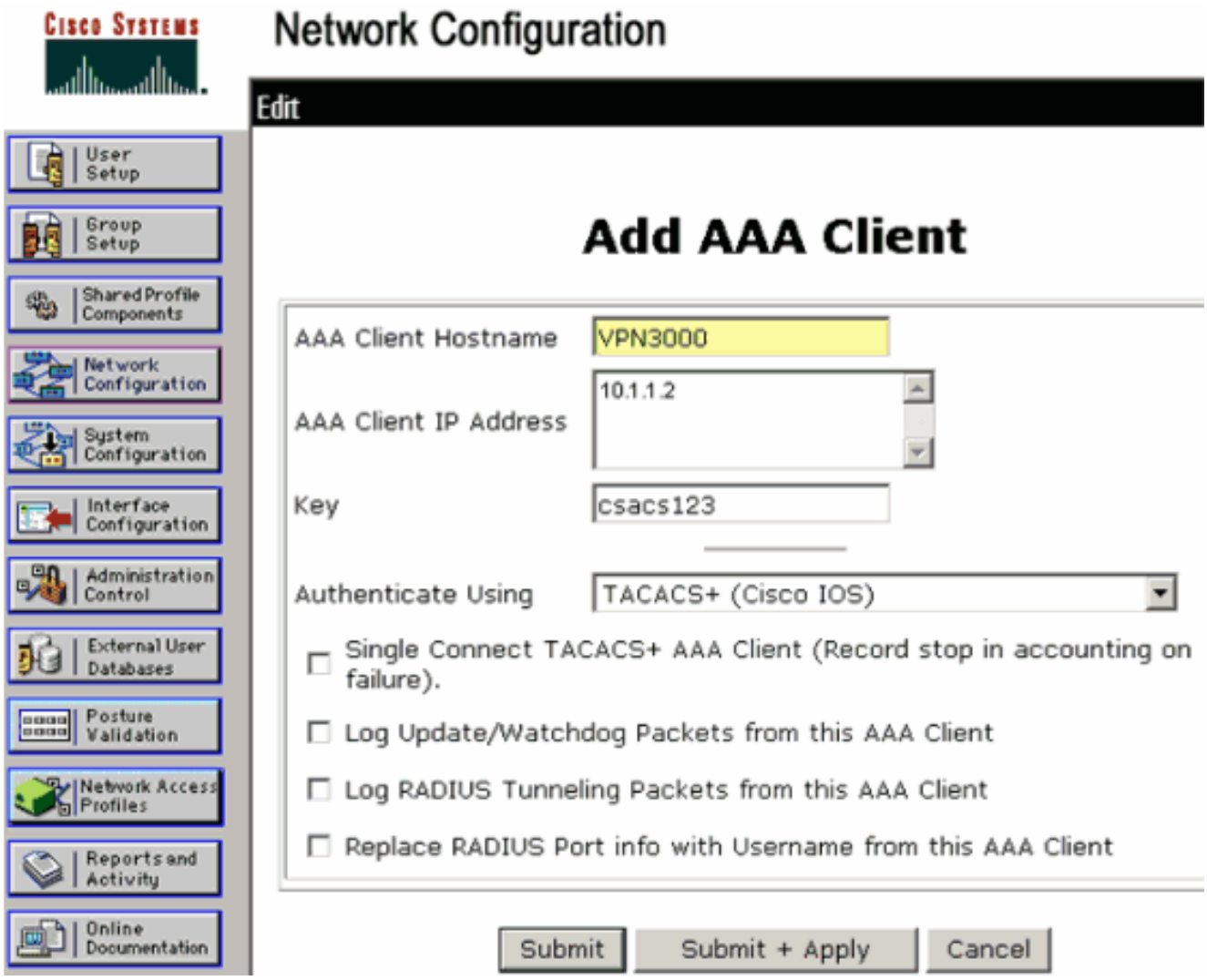
convenções de documentos.

Configurar o server TACACS+

Adicionar uma entrada para o VPN 3000 concentrator no server TACACS+

Termine estas etapas a fim adicionar uma entrada para o VPN 3000 concentrator no server TACACS+.

1. Clique a **configuração de rede no** painel esquerdo. Em AAA Clients, clique em Add Entry.
2. Na próxima janela, complete o formulário para adicionar o concentrador VPN como o cliente TACACS+. Este exemplo usa-se:Nome de host do cliente AAA = **VPN3000**Endereço IP de Um ou Mais Servidores Cisco ICM NT = **10.1.1.2 do** cliente de AAAChave = **csacs123**Autentique usando-se = **TACACS+ (o Cisco IOS)**Clique **Submit + Restart**.



Adicionar uma conta de usuário no server TACACS+

Termine estas etapas a fim adicionar uma conta de usuário no server TACACS+.

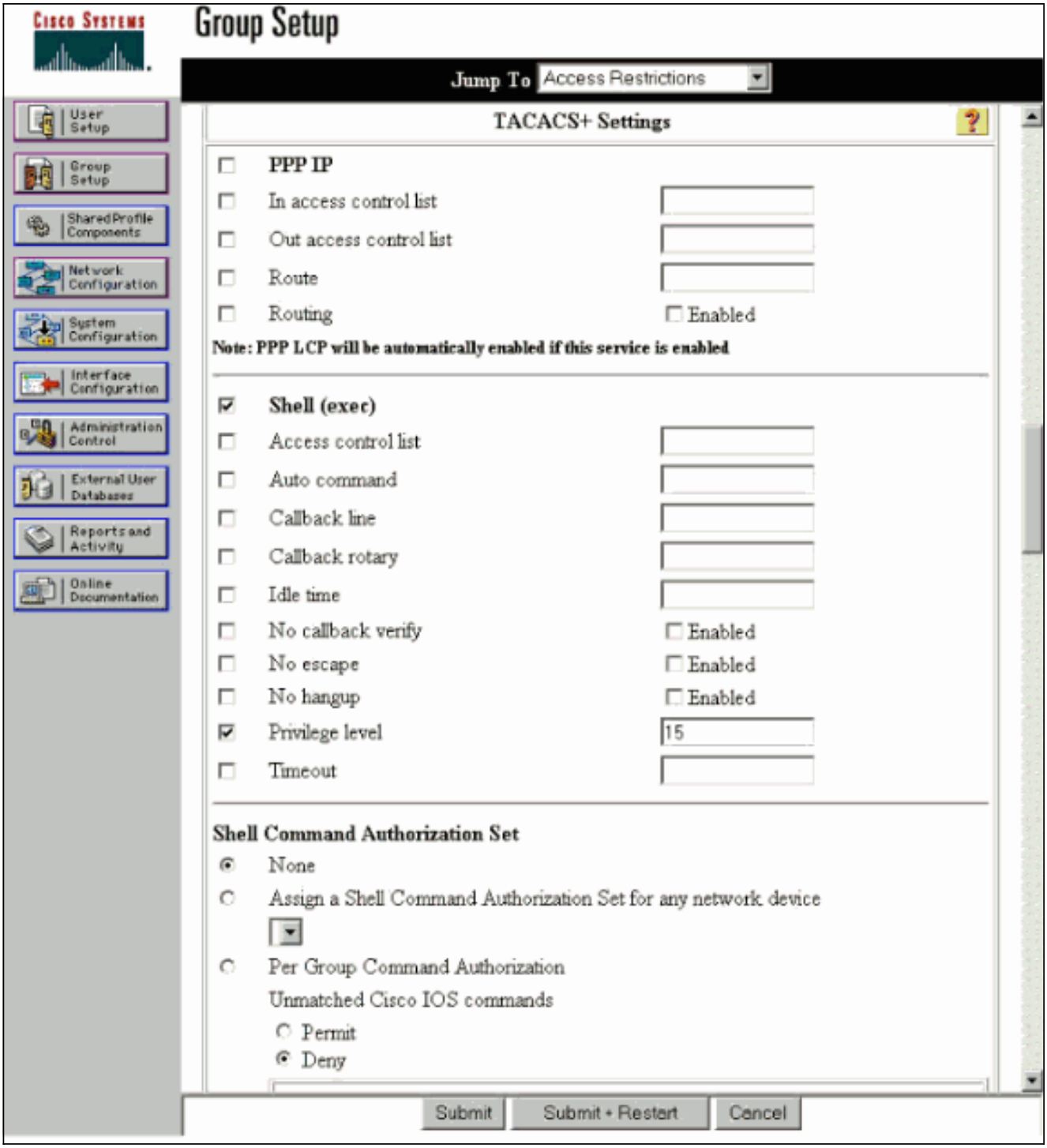
1. Crie uma conta de usuário no server TACACS+ que pode mais tarde ser usado para a autenticação TACACS+. Clique a **instalação de usuário no** painel esquerdo, adicionar o

usuário “johnsmith” e o clique **adiciona/edita** a fim fazer este.
2. Adicionar uma senha para este usuário, e atribua o usuário a um grupo ACS que contenha os outros administradores do VPN 3000 concentrator.**Nota:** Este exemplo define o nível de privilégio sob este perfil de grupo do usuário particular ACS. Se este deve ser feito em uma base do usuário per., escolha **Interface Configuration > Tacacs+ (Cisco IOS)** e verifique a caixa do **usuário** para ver se há o serviço do shell (exec). Somente são então as opções TACACS+ descritas neste inferior disponível do documento cada perfil de usuário.

Edite o grupo no server TACACS+

Termine estas etapas para editar o grupo no server TACACS+.

1. Clique a **instalação de grupo no** painel esquerdo.
2. Do menu suspenso, escolha o grupo que o usuário foi adicionado adicionar uma conta de usuário na seção do server TACACS+, que é grupo1 neste exemplo, e o clique **edita ajustes**.
3. Na próxima janela, certifique-se de que estes atributos estão selecionados sob ajustes TACACS+:**Shell (exec)Privilege level=15**Uma vez que feito, clique **Submit + Restart**.



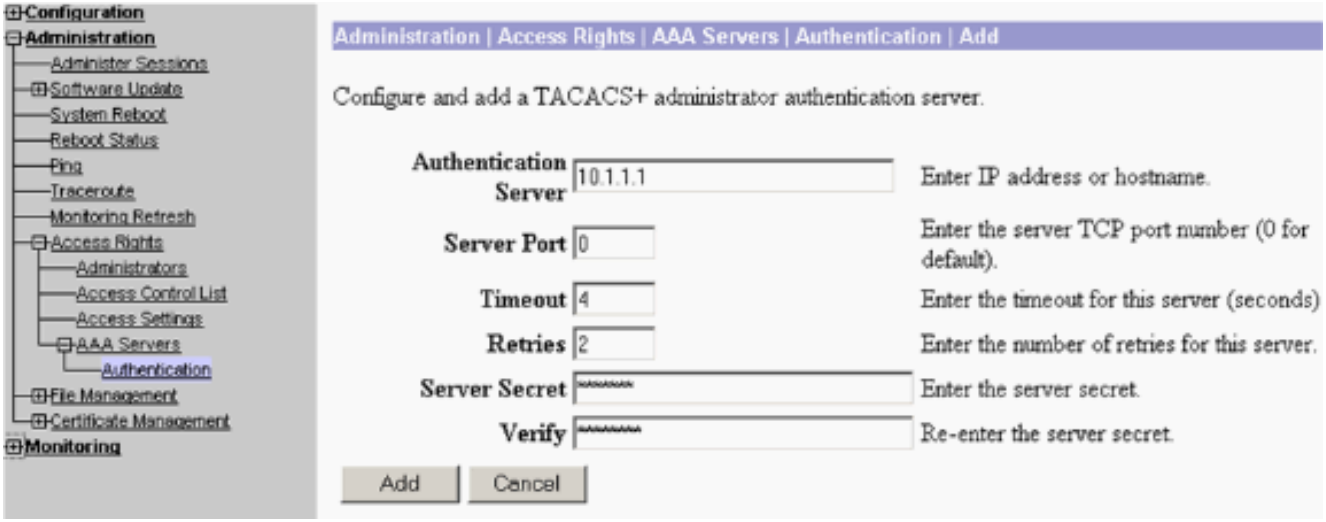
Configurar o VPN 3000 Concentrator

Adicionar uma entrada para o server TACACS+ no VPN 3000 concentrator

Termine estas etapas a fim adicionar uma entrada para o server TACACS+ no VPN 3000 concentrator.

1. Escolha o **Administração > Direitos de Acesso > Servidores AAA > Autenticação na** árvore de navegação no painel esquerdo, e clique-o então **adicionam no** painel direito.Assim que você clique **adicionar** a fim adicionar este server, o username localmente configurado/senhas no VPN 3000 concentrator está usado já não. Assegure o acesso alternativo através dos trabalhos do console em caso de um fechamento.

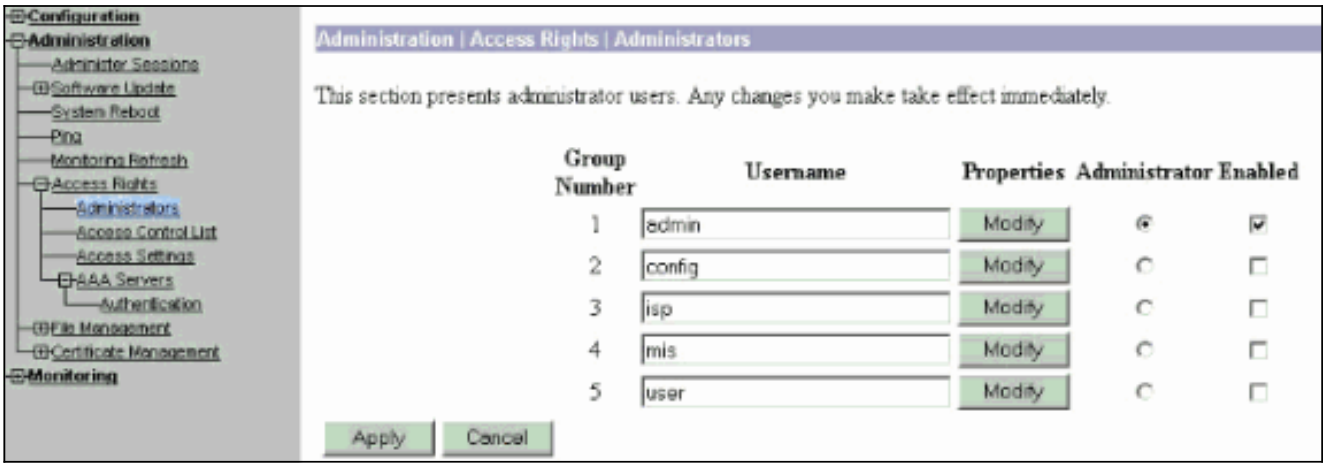
2. Na próxima janela, complete o formulário como visto aqui:Authentication Server = **10.1.1.1** (endereço IP de Um ou Mais Servidores Cisco ICM NT do server TACACS+)Porta de servidor = **0** (padrão)Intervalo = **4**Retries = **2**Segredo de servidor = **csacs123**Verifique = **csacs123**



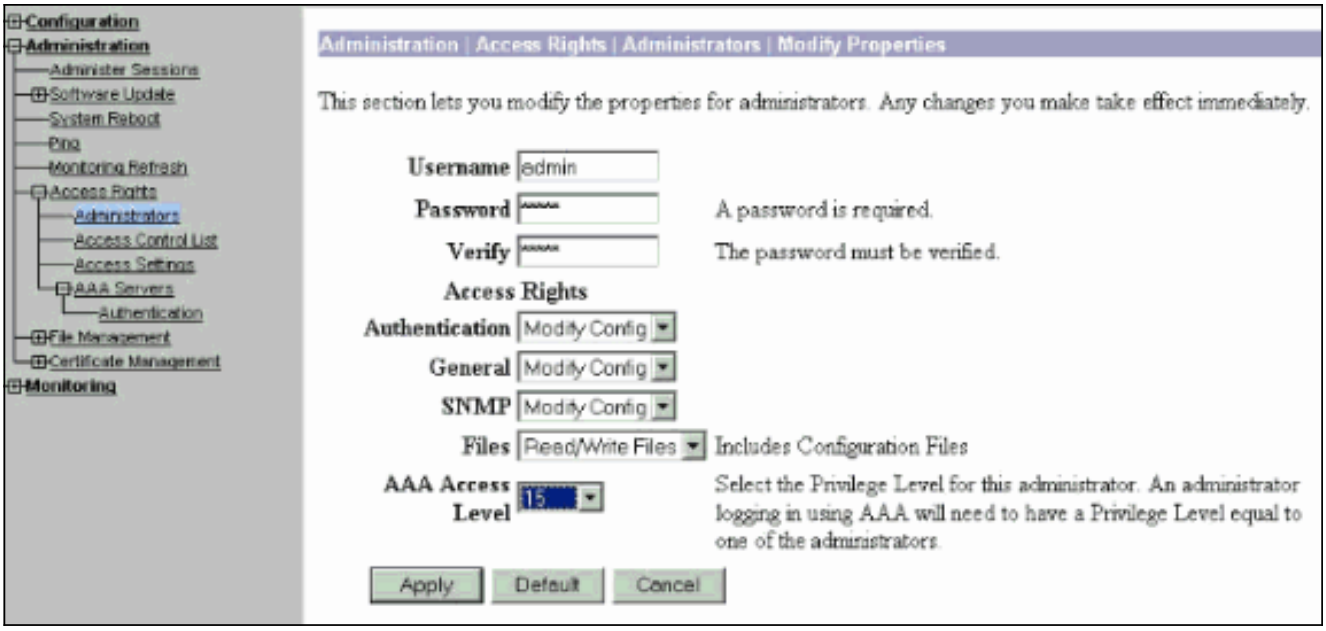
Altere a conta admin no concentrador VPN para a autenticação TACACS+

Termine estas etapas para alterar a conta admin no concentrador VPN para a autenticação TACACS+.

1. O clique **altera** para o usuário admin a fim alterar as propriedades deste usuário.



2. Escolha o nível de acesso AAA como **15**.Este valor pode ser qualquer número entre um e 15. Note que deve combinar o nível de privilégio TACACS+ definido sob o usuário/perfil de grupo no server TACACS+. O usuário TACACS+ pegara então as permissões definidas sob este usuário do VPN 3000 concentrator para a alteração da configuração, arquivos da leitura/escrita, e assim por diante.



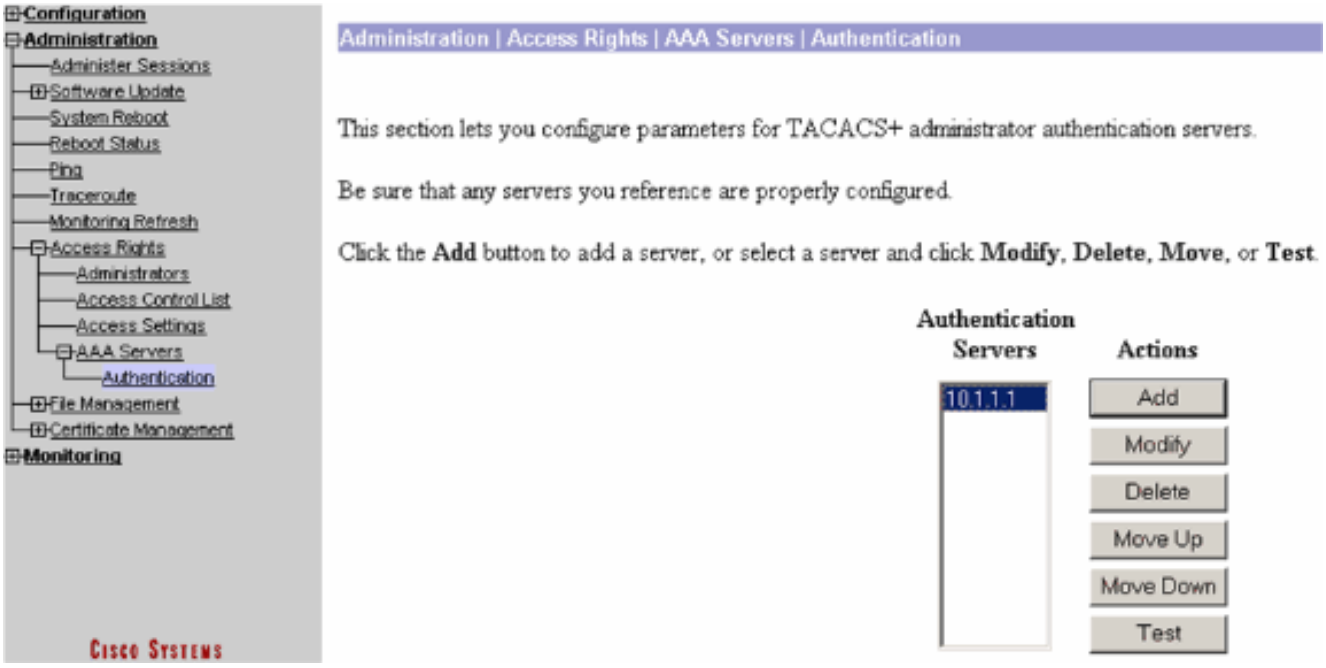
Verificar

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

Troubleshooting

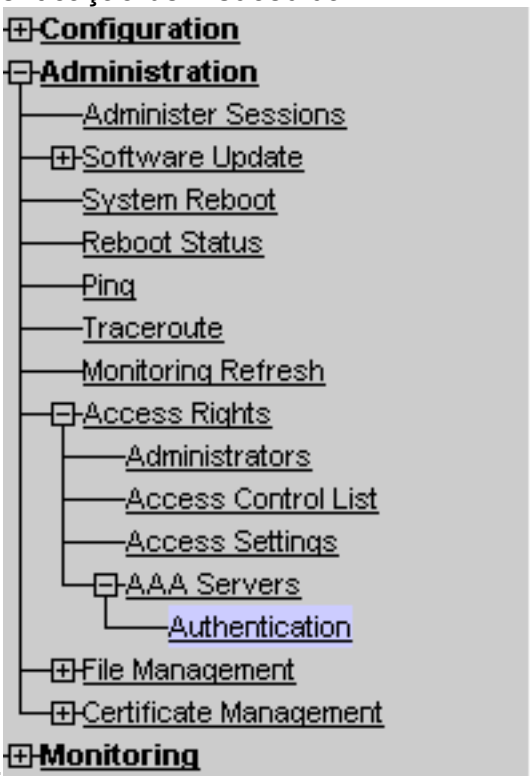
Termine as etapas nestas instruções a fim pesquisar defeitos sua configuração.

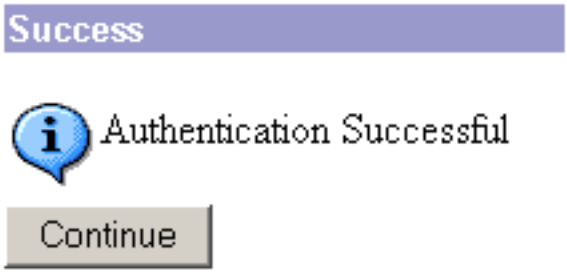
1. A fim testar a autenticação:Para server TACACS+Escolha o **Administração > Direitos de Acesso > Servidores AAA > Autenticação**.Selecione seu server, e clique então o **teste**.



Nota: Quando o server TACACS+ é configurado na aba da administração, não há nenhuma maneira de estabelecer o usuário para autenticar no base de dados local VPN3000. Você pode somente reserva usando um outro base de dados externo ou servidor de TACACS.Incorpore o nome de usuário e senha TACACS+ e clique a **APROVAÇÃO**.

Uma autenticação bem sucedida





aparece.

2. Se falha, há um problema de configuração ou um problema de conectividade IP. Verifique o fazer logon das falhas de tentativa o servidor ACS para ver se há mensagens relativas à falha.Se nenhuma mensagem aparece neste log então há provavelmente um problema de conectividade IP. O pedido TACACS+ não alcança o server TACACS+. Verifique que os filtros aplicados à relação apropriada do VPN 3000 concentrator permitem pacotes TACACS+ (porta TCP 49) dentro e para fora.Se os indicadores da falha como o serviço negaram no log, a seguir o serviço do shell (exec) não foi permitido corretamente sob o usuário ou o perfil de grupo no server TACACS+.
3. Se a autenticação de teste é bem sucedida, mas os inícios de uma sessão ao VPN 3000 concentrator continuam a falhar, verifique o log filtrável de eventos através da porta de Console.Se você vê uma mensagem similar:
   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` Esta mensagem indica que o nível de privilégio atribuído no server TACACS+ não tem nenhum nível de acesso de harmonização AAA sob alguns dos usuários do VPN 3000 concentrator. Por exemplo, o johnsmith do usuário tem um nível de privilégio TACACS+ de 7 no server TACACS+, mas nenhuns dos cinco administradores do VPN 3000 concentrator têm um nível de acesso AAA do 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