

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Autenticação](#)

[Adicionar a autorização](#)

[Adicionar relatório](#)

[Arquivo de teste](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve como configurar um roteador Cisco para autenticação com o TACACS+ que executa em UNIX. [O TACACS+ não oferece tantas características como o, comercialmente disponível, Cisco Secure ACS for Windows ou o Cisco Secure ACS UNIX.](#)

O software TACACS+ fornecido previamente pelo Cisco Systems foi interrompido e é apoiado já não pelo Cisco Systems.

Hoje, você pode encontrar muitas versões do freeware disponíveis TACACS+ quando você procura “pelo freeware TACACS+” em seu Engine de busca dos internet favorita. Cisco não recomenda especificamente nenhuma aplicação particular do freeware TACACS+.

O Serviço de controle de acesso Cisco Secure (ACS) está disponível para a compra através das vendas Cisco e dos canais de distribuição regulares no mundo inteiro. O Cisco Secure ACS for Windows inclui todos os componentes necessários necessários para uma instalação independente em uma estação de trabalho de Microsoft Windows. A solution engine do Cisco Secure ACS é enviada com uma licença do software instalada do Cisco Secure ACS. Visite [Cisco que pede o Home Page \(clientes registrados somente\)](#) para colocar uma ordem.

Nota: Você precisa uma conta CCO com um contrato de serviço associado obter a versão de teste de 90-dia para o [Cisco Secure ACS for Windows](#).

A configuração de roteador neste documento foi desenvolvida em um roteador que executasse o Software Release 11.3.3 de Cisco IOS®. O Cisco IOS Software Release 12.0.5.T e Mais Recente usa o **TACACS+ de grupo** em vez de **tacacs+**, assim que as indicações tais como o **TACACS+ padrão da autenticação de login aaa** permitem aparecem enquanto o **grupo padrão tacacs+ da autenticação de login aaa** permite.

Refira a [documentação do Cisco IOS Software](#) para informações mais completas sobre dos comandos router.

[Pré-requisitos](#)

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no Cisco IOS Software Release 11.3.3 e no Cisco IOS Software Release 12.0.5.T e Mais Recente.

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.

Autenticação

Conclua estes passos:

1. Certifique-se de você ter compilado o código TACACS+ (TAC+) no servidor Unix. As configurações do servidor aqui supõem que você usa o código de server de Cisco TAC+. As configurações de roteador devem trabalhar mesmo se o código de server é código de servidor Cisco. O TAC+ deve ser executado como a raiz; SU a enraizar caso necessário.
2. Copie o [test_file na](#) extremidade deste documento, coloque-o no server TAC+, e nomeie-o **test_file**. Verifique para ter certeza os começos **tac_plus_executable** do demônio com o **test_file**. Neste comando, - As verificações da opção **P** para compilam erros mas não começam o demônio: Você pôde ver os índices de test_file enrolar para baixo o indicador, mas você não deve ver que as mensagens tais como não podem encontrar o arquivo, texto não criptografado esperado--texto não criptografado, OU inesperado encontrado}. Se há uns erros, verifique trajetos a test_file, verifique novamente sua datilografia, e contraprova antes que você continue.
3. Comece configurar o TAC+ no roteador. Incorpore o **modo enable** e o tipo **configura o terminal** antes do comando set. Esta sintaxe de comando assegura-se de que você não esteja travado fora do roteador inicialmente, fornecendo o **tac_plus_executable** não esteja sendo executado:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list. !          aaa authentication login linmethod tacacs+ enable  aaa authentication login vtymethod tacacs+ enable  aaa authentication login conmethod tacacs+ enable  !  !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
```

vtymethod

4. Teste para ter certeza você pode ainda alcançar o roteador com telnet e através da porta de Console antes que você continue. Porque o **tac_plus_executable** não está sendo executado, a senha da **possibilidade** deve ser aceita. **Nota:** Mantenha a sessão de porta de Console ativa e permaneça no modo enable. Esta sessão não deve cronometrar para fora. O acesso ao roteador é limitado neste momento, e você precisa de poder fazer alterações de configuração sem travar-se para fora. Emita estes comandos ver a interação de servidor a roteador no roteador:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod
```

5. Como a raiz, comece o TAC+ no server: !--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod

6. Verifique para ter certeza o TAC+ começado: !--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod
- OU !--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4

```
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-  
timeout 0 0 login authentication vtymethod
```

Se o TAC+ não começa, é geralmente um problema com sintaxe no test_file. Retorne a etapa 1 para corrigir isto.

7. Datilografe o `tail -f /var/tmp/tac_plus.log` para ver a interação do roteador-à-server no server.**Nota:** - A opção `d 16` na etapa 5 envia a saída de todas as transações a `/var/tmp/tac_plus.log`.

8. Os usuários do telnet (VTY) devem agora ter que autenticar com o TAC+.Com debugar entrar no roteador e no server (etapas 4 e 7), telnet no roteador de outro parte da rede.O roteador produz uma alerta do nome de usuário e senha, a que você responde:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list. !  
aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod0
```

Os usuários agora têm que permitir com o TAC+.

9. Se você igualmente quer seus usuários autenticar com o TAC+ a fim obter no modo enable, certifique-se que sua sessão de porta de Console é ainda active e se adicionar deste comando ao roteador:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list. !  
aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
```

vtymethodOs usuários agora têm que permitir com o TAC+.

10. Com debugar entrar no roteador e no server (etapas 4 e 7), telnet no roteador de outro parte da rede. O roteador produz uma alerta do nome de usuário e senha, a que você responde:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list. !  
aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
```

Quando você incorporar o modo enable, as requisições de roteador uma senha, a

que você responde: *!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---*
tac_plus_executable not being started, the *!--- enable password is accepted because !---*
 it is in each list. *! aaa authentication login linmethod tacacs+ enable*
aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod
tacacs+ enable ! !--- Point the router to the server, where #.#.# !--- is the server
IP address. ! tacacs-server host #.#.# line con 0 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed
38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out
to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
 vtymethod

Olhe o server e o roteador onde você deve ver a interação TAC+? o que é enviado onde, respostas, pedidos, e assim por diante. Corrija todos os problemas antes que você continue.

11. Derrube o processo TAC+ no server quando ainda conectado à porta de Console para ter certeza que seus usuários podem ainda alcançar o roteador se o TAC+ está para baixo: *!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---*
tac_plus_executable not being started, the *!--- enable password is accepted because !---*
 it is in each list. *! aaa authentication login linmethod tacacs+ enable*
aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod
tacacs+ enable ! !--- Point the router to the server, where #.#.# !--- is the server
IP address. ! tacacs-server host #.#.# line con 0 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed
38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out
to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
 vtymethod
- OU *!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---*
tac_plus_executable not being started, the *!--- enable password is accepted because !---*
 it is in each list. *! aaa authentication login linmethod tacacs+ enable*
aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod
tacacs+ enable ! !--- Point the router to the server, where #.#.# !--- is the server
IP address. ! tacacs-server host #.#.# line con 0 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed
38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out
to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
 vtymethod
- Repita o telnet e permita-o da etapa precedente. O roteador então realiza que o processo TAC+ não está respondendo e permite que os usuários entrem e permitam com as senhas padrão.
12. Verifique para ver se há a autenticação de seus usuários da porta de Console com o TAC+. A fim fazer isto, traga acima o server TAC+ outra vez (etapas 5 e 6), e estabeleça uma sessão de Telnet ao roteador (que deve autenticar com o TAC+). Remain conectou com o telnet no roteador no modo enable até que você esteja certo que você pode entrar ao roteador através da porta de Console. A saída de sua conexão original ao roteador através da porta de Console, reconecta então à porta de Console. Autenticação de porta de Console a entrar e permitir usando o usuário - os ids e as senhas (mostrados na etapa 10) devem agora ser com o TAC+.
13. Quando você permanecer conectado através ou de uma sessão de Telnet ou a porta de Console e com debuga ir no roteador e no server (etapas 4 e 7), estabeleça uma conexão

de modem para alinhar 1.A linha usuários agora tem que entrar e permitir com o TAC+.O roteador produz uma alerta do nome de usuário e senha, a que você responde:!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod

Quando você incorporar o modo enable, as requisições de roteador uma senha.Resposta:!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod

Olhe o server e o roteador onde você vê a interação TAC+? o que é enviado onde, respostas, pedidos, e assim por diante. Corrija todos os problemas antes que você continue.Os usuários agora têm que permitir com o TAC+.

Adicionar a autorização

Adicionar a autorização é opcional.

À revelia, há três níveis de comando no roteador:

- o nível de privilégio 0 que inclui o desabilitação, permite, retira, ajuda, e saída
- a alerta do nível de privilégio 1 - normal em nível em um telnet - diz o Roteador>
- a alerta do nível de privilégio 15 - permita o nível - diz o router-

Desde que os comandos disponíveis dependem do conjunto de recursos IO, versão do Cisco IOS, modelo do roteador, e assim por diante, não há uma lista abrangente dos comandos all a níveis 1 e 15. Por exemplo, a **rota IPX da mostra** não está atual em um conjunto de recursos IP somente, o **transporte nat da mostra IP** não está no Cisco IOS Software Release 10.2.x porque o NAT não foi introduzido naquele tempo, e o **ambiente da mostra** não está atual nos modelos do roteador sem fonte de alimentação e monitoramento de temperatura. Os comandos disponíveis em um roteador particular a nível particular podem ser encontrados quando você incorpora a? na alerta no roteador quando a esse nível de privilégio.

A autorização da porta de Console não foi adicionada como uma característica até que a identificação de bug Cisco [CSCdi82030](#) ([clientes registrados somente](#)) esteve executada. A autorização da porta de Console é fora à revelia diminuir a probabilidade que você se torna travado acidentalmente fora do roteador. Se um usuário tem o acesso físico ao roteador através

do console, a autorização da porta de Console não é extremamente eficaz. Contudo, a autorização da porta de Console pode ser girada sobre a linha engodo 0 em uma imagem que a identificação de bug Cisco [CSCdi82030](#) ([clientes registrados somente](#)) esteve executada dentro com o comando:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication
methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the
methods !--- listed on the same lines are the methods !--- in the order to be tried. As used
here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !-
-- enable password is accepted because !--- it is in each list.          !          aaa
authentication login linmethod tacacs+ enable  aaa authentication login vtymethod tacacs+
enable  aaa authentication login conmethod tacacs+ enable  !  !--- Point the router to the
server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut
transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password
whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0
login authentication vtymethod
```

1. O roteador pode ser configurado para autorizar comandos com o TAC+ de todo ou alguns níveis. Esta configuração de roteador permite que todos os usuários tenham a autorização do por-comando estabelecida no server. Aqui nós autorizamos comandos all com o TAC+, mas se o server está para baixo, nenhuma autorização é necessária.

```
!--- Turn on TAC+. aaa new-
model enable password whatever !--- These are lists of authentication methods. !---
"linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods
!--- listed on the same lines are the methods !--- in the order to be tried. As used here,
if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--
- enable password is accepted because !--- it is in each list.          !          aaa
authentication login linmethod tacacs+ enable  aaa authentication login vtymethod tacacs+
enable  aaa authentication login conmethod tacacs+ enable  !  !--- Point the router to
the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line
con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging.
exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod
modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0
4 password whatever !--- No time-out to prevent being locked out !--- during debugging.
exec-timeout 0 0 login authentication vtymethod
```

2. Quando o server TAC+ for executado, telnet no roteador com **authenuser** userid. Porque o authenuser tem o serviço padrão = a licença em test_file, este usuário deve poder executar todas as funções. Quando no roteador, incorpore o modo **enable**, e gire sobre a eliminação de erros da autorização:

```
!--- Turn on TAC+. aaa new-model enable password whatever !---
These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and
!--- so on are names of lists, and the methods !--- listed on the same lines are the
methods !--- in the order to be tried. As used here, if !--- authentication fails due to
the !--- tac_plus_executable not being started, the !--- enable password is accepted
because !--- it is in each list.          !          aaa authentication login linmethod
tacacs+ enable  aaa authentication login vtymethod tacacs+ enable  aaa authentication
login conmethod tacacs+ enable  !  !--- Point the router to the server, where #.#.#.# !--
- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !---
No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login
authentication conmethod line 1 8 login authentication linmethod modem InOut transport
input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever
!--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login
authentication vtymethod
```

3. Telnet no roteador com **authoruser** userid e na senha de operador. Este usuário não pode fazer o **traceroute** e uma **saída de dois comandos show** (veja o [test file](#)). Olhe o server e o roteador onde você deve ver a interação TAC+ (o que é enviado onde, respostas, pedidos, e assim por diante). Corrija todos os problemas antes que você continue.
4. Se você quer configurar um usuário para um comando automático, elimine o usuário transitório comentado-para fora no [test file](#), e põe um destino do endereço IP válido no lugar

do **#####**. Pare e ligue o server TAC+. No roteador: *!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list. !* aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where ##### !--- is the server IP address. !* tacacs-server host ##### line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod*

Telnet ao roteador com transeunte e senha transitória useríd. O telnet ##### executa e o usuário transitório é enviado ao outro lugar.

Adicionar relatório

Os relatórios de adição são opcionais.

A referência ao arquivo de contabilidade está em test_file? arquivo de contabilidade = /var/log/tac.log. Mas a contabilidade não ocorre a menos que configurado no roteador (fornecido o roteador executa uma versão de Cisco IOS Software mais tarde de 11.0).

1. Permita a contabilidade no roteador: *!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list. !* aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where ##### !--- is the server IP address. !* tacacs-server host ##### line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod*

Nota: A contabilidade AAA não faz a contabilidade do por-comando em algumas versões. Uma ação alternativa é usar a autorização do por-comando e registrar a ocorrência no arquivo de contabilidade. (Refira a identificação de bug Cisco [CSCdi44140](#).) Se você se usa uma imagem em que esta fixada é usada [Cisco IOS Software Release 11.2(1.3)F, 11.2(1.2), 11.1(6.3), 11.1(6.3)AA01, 11.1(6.3)CA em setembro 24, 1997] você pode igualmente permitir a comando-contabilidade.

2. Quando o TAC+ for executado no server, incorpore este comando no server ver as entradas que entram no arquivo de contabilidade: *!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list. !* aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where ##### !--- is the server IP address. !* tacacs-server host ##### line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem*


```
InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
timeout 0 0 login authentication vtymethod
Então log e fora do roteador, telnet fora do
roteador, e assim por diante. Caso necessário, no roteador entre:!--- Turn on TAC+. aaa new-
model enable password whatever !--- These are lists of authentication methods. !---
"linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods
!--- listed on the same lines are the methods !--- in the order to be tried. As used here,
if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--
- enable password is accepted because !--- it is in each list. ! aaa
authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+
enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to
the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line
con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging.
exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod
modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0
4 password whatever !--- No time-out to prevent being locked out !--- during debugging.
exec-timeout 0 0 login authentication vtymethod
```

[Arquivo de teste](#)

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication
methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the
methods !--- listed on the same lines are the methods !--- in the order to be tried. As used
here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !-
-- enable password is accepted because !--- it is in each list. ! aaa
authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+
enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the
server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut
transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password
whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0
login authentication vtymethod
```

Nota: Este Mensagem de Erro é gerado se seu servidor de TACACS não é alcançável: %AAAA-3-DROPACCTSNDFAIL: o registro de contabilidade deixado cair, envia ao server falhado: sistema-início. Verifique que o server TACACS+ é operacional.

[Informações Relacionadas](#)

- [TACACS+ de segurança de acesso de usuário único à rede](#)
- [Terminal Access Controller Access Control System \(TACACS+\)](#)
- [Cisco Secure Access Control Server for Windows](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)