

# Configurando o RADIUS com servidor Livingstone

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Autenticação](#)

[Relatório de adição](#)

[Arquivos de teste](#)

[Informações Relacionadas](#)

## Introdução

Este documento é pretendido ajudar a primeira vez ao usuário RADIUS na fundação e na eliminação de erros uma configuração RADIUS a um servidor RADIUS Livingston. Não é uma descrição exaustiva de recursos de RADIUS de Cisco IOS®. A documentação livingston está disponível do site do LUCENT TECHNOLOGIES.

A configuração de roteador é a mesma não importa o que o server é usado. Cisco oferece o código radius disponível no comércio em Couscouses NA, mistura Unix, ou Cisco Access Registrar.

Esta configuração de roteador foi desenvolvida em um roteador que executasse o Cisco IOS Software Release 11.3.3; Libere 12.0.5.T e um **raio de grupo** mais atrasado dos usos em vez do **raio**, assim que as indicações tais como o **raio padrão da autentificação de login aaa permitem** aparecem como o **habilitado para radius do grupo padrão da autentificação de login aaa**.

Refira a [informação radius na](#) documentação IOS Cisco para detalhes em comandos router do RAO.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

## Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

## Autenticação

Conclua estes passos:

1. Certifique-se que você compilou o código radius no servidor Unix. As configurações do servidor supõem que você usa o código de servidor RADIUS Livingston. As configurações de roteador precisam de trabalhar com o outro código de server mas as configurações do servidor diferem. O código, radiusd, deve ser executado como a raiz.
2. O código dos radius livingston vem com três arquivos de amostra que devem ser personalizada para seu sistema: clients.example, users.example, e dicionário. Estes são todos encontrados geralmente no diretório do raddb. Você pode alterar estes arquivos ou os usuários e os arquivos dos clientes na extremidade deste documento. Todos os três arquivos precisam de ser colocados em um diretório de funcionamento. Teste para ter certeza os começos do servidor Radius com os três arquivos:

```
radiusd -x -d
```

(directory\_containing\_3\_files) Erros na necessidade startup de ser imprimido à tela ou ao directory\_containing\_3\_files\_logfile. Verifique no RAIO de ordem para ter certeza começado, de uma outra janela de servidor:

```
ps -aux | grep radiusd
```

(or ps -ef | grep radiusd) Você vê dois processos do radiusd.

3. Mate o processo do raio:

```
kill -9 highest_radiusd_pid
```
4. Na porta de Console de roteador, comece configurar o RAIO. Incorpore o modo enable e o tipo **configura o terminal** antes do comando set. Esta sintaxe assegura-se de que você não esteja travado fora do roteador inicialmente, dado que o RAIO não é executado no server:

```
!--- Turn on RADIUS aaa new-model enable password whatever !--- These are lists of authentication methods, !--- that is, "linmethod", "vtymethod", "conmethod" 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 radiusd !--- not being started, the enable password will be !--- accepted because it is in each list. aaa authentication login default radius enable aaa authentication login linmethod radius enable aaa authentication login vtymethod radius enable aaa authentication login conmethod radius enable !--- Point the router to the server, that is, !--- #.#.#.# is the server IP address. radius-server host #.#.#.# !--- Enter a key for handshaking !--- with the RADIUS server: radius-server key cisco 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 password whatever 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. Remain entrou ao roteador através da porta de Console quando você verificar em ordem para ter certeza que você pode ainda alcançar o roteador com o telnet antes que você continue. Porque o radiusd não está sendo executado, a senha da possibilidade precisa de ser aceita com todo o userid. **Cuidado:** Mantenha a sessão de porta de Console ativa e permaneça no modo enable. Assegure-se de que esta sessão não cronometre para fora. Não se trave para fora quando você fizer alterações de configuração. Emita estes comandos a fim ver o server à interação de roteador no roteador:

```
terminal monitor
debug aaa authentication
```

6. Como a raiz, comece o RAIO no server:

```
radiusd -x -d (directory_containing_3_files)Os
```

erros na partida são imprimidos à tela ou ao `directory_containing_3_files_logfile`. Verifique para ter certeza o RAIIO começado de uma outra janela de servidor:  
`Ps -aux | grep radiusd`  
(or `Ps -ef | grep radiusd`) Você precisa de ver dois processos do radiusd.

7. Os usuários (vty) do telnet agora têm que autenticar através do RAIIO. Com debugar no roteador e o server, as etapas 5 e o 6, telnet no roteador de outro parte da rede. O roteador produz uma alerta do nome de usuário e senha a que você responde:  
`ciscousr (username from users file)`  
`ciscopas (password from users file)` Olhe o server e o roteador onde você precisa de ver a interação de radius, por exemplo, o que está sendo enviada onde, respostas, e pedidos, e assim por diante. Corrija todos os problemas antes que você continue.
8. Se você igualmente quer seus usuários autenticar através do RAIIO para obter no modo enable, certifique-se que sua sessão de porta de Console é ainda active e se adicionar deste comando ao roteador.  
*!--- For enable mode, list "default" looks to RADIUS !--- then enable password if RADIUS not running.* `aaa authentication enable default radius enable`
9. A necessidade de usuários tem que agora **permitir** através do RAIIO. Com debugar entrar no roteador e o server, as etapas 5 e o 6, telnet no roteador de outro parte da rede. O roteador precisa de produzir uma alerta do nome de usuário e senha a que você responde:  
`ciscousr (username from users file)`  
`ciscopas (password from users file)` Quando você incorpora o modo enable, o roteador envia `username $enable15$` e pede uma senha, a que você responde:`shared` Olhe o server e o roteador onde você precisa de ver a interação de radius, por exemplo, o que está sendo enviada onde, respostas, e pedidos, e assim por diante. Corrija todos os problemas antes que você continue.
10. Verifique para ver se há a autenticação de seus usuários da porta de Console através do RAIIO pelo estabelecimento de uma sessão de Telnet ao roteador, que necessidades de autenticar através do RAIIO. Permaneça em telnet no roteador e 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, e reconecta então à porta de Console. A autenticação de porta de Console a entrar e permitir com o uso dos `userid`s e as senhas na etapa 9 precisam agora de ser através do RAIIO.
11. Quando você permanecer conectado através ou de uma sessão de Telnet ou a porta de Console e com debuga ir no roteador e o server, as etapas 5 e o 6, estabeleça uma conexão de modem para alinhar 1. linhas necessidade de usuários têm que agora entrar e permitir através do RAIIO. O roteador precisa de produzir uma alerta do nome de usuário e senha a que você responde:  
`ciscousr (username from users file)`  
`ciscopas (password from users file)` Quando você incorpora o modo enable, o roteador envia `username $enable15$` e pede uma senha, a que você responde:`shared` Olhe o server e o roteador onde você precisa de ver a interação de radius, por exemplo, o que está sendo enviada onde, respostas, e pedidos, e assim por diante. Corrija todos os problemas antes que você continue.

## Relatório de adição

Os relatórios de adição são opcionais.

1. A contabilidade não ocorre a menos que configurado no roteador. Permita a contabilidade no roteador como neste exemplo:  
`aaa accounting exec default start-stop radius`

```
aaa accounting connection default start-stop radius
aaa accounting network default start-stop radius
aaa accounting system default start-stop radius
```

2. Comece o RAIIO no server com a opção da contabilidade: Start RADIUS on the server with the accounting option:
3. A fim ver o server à interação de roteador no roteador: terminal monitor  
debug aaa accounting
4. Alcance o roteador quando você observar o server e a interação de roteador com debugar, e verifique então o diretório da contabilidade para ver se há arquivos de registro.

## Arquivos de teste

Este é o arquivo de teste dos usuários:

```
ciscousr      Password = "ciscopas"
              User-Service-Type = Login-User,
              Login-Host = 1.2.3.4,
              Login-Service = Telnet
```

```
$enable15$   Password = "shared"
              User-Service-Type = Shell-User
```

Este é o arquivo de teste dos clientes:

```
# 1.2.3.4 is the ip address of the client router and cisco is the key
1.2.3.4      cisco
```

## Informações Relacionadas

- [Remote Authentication Dial-In User Service \(RADIUS\)](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)