Configurando o RADIUS com servidor Livingstone

Contents

Introduction

Este documento destina-se a auxiliar o usuário RADIUS pela primeira vez na configuração e depuração de uma configuração RADIUS para um servidor RADIUS Livingston. Não é uma descrição exaustiva dos recursos RADIUS do Cisco IOS®. A documentação do Livingston está disponível no site da Lucent Technologies.

A configuração do roteador é a mesma, independentemente do servidor utilizado. A Cisco oferece código RADIUS disponível comercialmente nos cursos NA, nos cursos UNIX ou no Cisco Access Registrar.

Esta configuração de roteador foi desenvolvida em um roteador que executa o Cisco IOS Software Release 11.3.3; A versão 12.0.5.T e posterior usa o **raio do grupo** em vez do **raio**, de modo que instruções como **aaa authentication login default radius enable** aparecem como **aaa authentication login default group radius enable**.

Consulte as informações RADIUS na documentação do Cisco IOS para obter detalhes sobre os comandos do roteador RADIUS.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Conventions

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

Autenticação

Conclua estes passos:

1. Certifique-se de compilar o código RADIUS no servidor UNIX. As configurações do servidor pressupõem que você use o código do servidor Livingston RADIUS. As configurações do roteador precisam funcionar com outro código de servidor, mas as configurações do servidor diferem. O código, radiusd, deve ser executado como raiz.
2. O código Livingston RADIUS vem com três arquivos de exemplo que devem ser personalizados para o seu sistema: clients.example, users.example e dictionary. Todos eles são normalmente encontrados no diretório raddb. Você pode modificar esses arquivos ou os arquivos de usuários e clientes no final deste documento. Todos os três arquivos precisam ser colocados em um diretório de trabalho. Teste para ter certeza de que o servidor RADIUS comece com os três arquivos:
   ```
   radiusd -x -d (directory_containing_3_files)
   ```
   Erros na inicialização precisam ser impressos na tela ou no diretório_content_3_files_logfile. Verifique para ter certeza de que o RADIUS foi iniciado, em outra janela de servidor:
   ```
   ps -aux | grep radiusd
   (or ps -ef | grep radiusd)
   ```
   Você vê dois processos radiosos.
3. Matar o processo radius:
   ```
   kill -9 highest_radiusd_pid
   ```
4. Na porta do console do roteador, comece a configurar o RADIUS. Entre no modo de ativação e digite **configure terminal** antes do conjunto de comandos. Essa sintaxe garante que você não seja bloqueado para fora do roteador inicialmente, já que o RADIUS não é executado no servidor:

   ```
   !--- 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. Permaneça conectado ao roteador através da porta de console enquanto você verifica para ter certeza de que ainda pode acessar o roteador por meio do Telnet antes de continuar. Como o radiusd não está em execução, a senha de ativação precisa ser aceita com qualquer ID de usuário.**Cuidado:** mantenha a sessão da porta do console ativa e permaneça no modo de ativação. Certifique-se de que esta sessão não exceda o tempo limite. Não se

afaste enquanto faz alterações de configuração.Execute estes comandos para ver a interação entre o servidor e o roteador no roteador:

```
terminal monitor
debug aaa authentication
```

6. Como raiz, inicie o RADIUS no servidor:

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

   Erros na inicialização são impressos na tela ou no diretório_content_3_files_logfile. Verifique se o RADIUS foi iniciado em outra janela do servidor:

   ```
   Ps -aux | grep radiusd
   (or Ps -ef | grep radiusd)
   ```

   Você precisa ver dois processos radiosos.
7. Os usuários do Telnet (vty) agora precisam se autenticar por meio do RADIUS. Com debug no roteador e no servidor, as etapas 5 e 6, faça Telnet no roteador a partir de outra parte da rede. O roteador produz um prompt de nome de usuário e senha ao qual você responde:

   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```

   Observe o servidor e o roteador onde você precisa ver a interação RADIUS, por exemplo, o que está sendo enviado para onde, respostas, solicitações e assim por diante. Corrija todos os problemas antes de continuar.
8. Se você também quiser que seus usuários se autentiquem por meio do RADIUS para entrar no modo de ativação, verifique se a sessão da porta de console ainda está ativa e adicione esse 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. Agora, os usuários precisam **habilitar** através do RADIUS. Com o debug sendo executado no roteador e no servidor, as etapas 5 e 6 fazem Telnet no roteador a partir de outra parte da rede. O roteador precisa produzir um prompt de nome de usuário e senha ao qual você responde:

   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```

   Quando você entra no modo enable, o roteador envia o nome de usuário $enable15$ e solicita uma senha, à qual você responde:

   ```
   shared
   ```

   Observe o servidor e o roteador onde você precisa ver a interação RADIUS, por exemplo, o que está sendo enviado para onde, respostas, solicitações e assim por diante. Corrija todos os problemas antes de continuar.
10. Verifique a autenticação dos usuários da porta de console por meio do RADIUS, estabelecendo uma sessão Telnet para o roteador, que precisa ser autenticada por meio do RADIUS. Permaneça conectado via Telnet no roteador e no modo de ativação até ter certeza de que pode fazer login no roteador através da porta do console, fazer logoff da sua conexão original com o roteador através da porta do console e, em seguida, reconectar-se à porta do console. A autenticação da porta do console para fazer login e habilitar por meio do uso de IDs de usuário e senhas na etapa 9 deve passar agora pelo RADIUS.
11. Enquanto você permanece conectado por meio de uma sessão Telnet ou pela porta de console e com o debug sendo executado no roteador e no servidor, as etapas 5 e 6 estabelecem uma conexão de modem com a linha 1. Os usuários de linha agora precisam fazer login e habilitar através do RADIUS. O roteador precisa produzir um prompt de nome de usuário e senha ao qual você responde:

    ```
    ciscousr (username from users file)
    ```

```
ciscopas (password from users file)
```

Quando você entra no modo enable, o roteador envia o nome de usuário $enable15$ e solicita uma senha, à qual você responde:

```
shared
```

Observe o servidor e o roteador onde você precisa ver a interação RADIUS, por exemplo, o que está sendo enviado para onde, respostas, solicitações e assim por diante. Corrija todos os problemas antes de continuar.

Relatório de adição

A adição de contabilidade é opcional.

1. A contabilização não ocorre a menos que seja configurada no roteador. Ative a contabilização 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. Inicie o RADIUS no servidor com a opção contábil:
   ```
   Start RADIUS on the server with the accounting option:
   ```
3. Para ver a interação entre o servidor e o roteador no roteador:
   ```
   terminal monitor
   debug aaa accounting
   ```
4. Acesse o roteador enquanto observa a interação entre o servidor e o roteador através da depuração e, em seguida, verifique o diretório contábil para arquivos de log.

Arquivos de teste

Este é o arquivo de teste do usuário:

```
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 de 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