Configurar AAA básico em um servidor de acesso

Contents

Introduction

Este documento descreve como configurar a Autenticação, Autorização e Contabilização (AAA - Authentication, Authorization, and Accounting) em um roteador Cisco com protocolos Radius ou TACACS+.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Componentes Utilizados

As informações neste documento são baseadas na linha principal do Cisco IOS® Software Release 12.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento explica como configurar a Autenticação, Autorização e Contabilização (AAA - Authentication, Authorization, and Accounting) em um roteador Cisco com protocolos Radius ou TACACS+. O objetivo deste documento não é cobrir todos os recursos AAA, mas explicar os comandos principais e fornecer alguns exemplos e diretrizes.

> **Note**: Leia a seção sobre Configuração Geral AAA antes de prosseguir com a configuração do Cisco IOS. Deixar de fazer isso pode resultar em erro de configuração e bloqueio subsequente.

Para obter mais informações, consulte Authentication, Authorization and Accounting Configuration Guide.

Diagrama de Rede

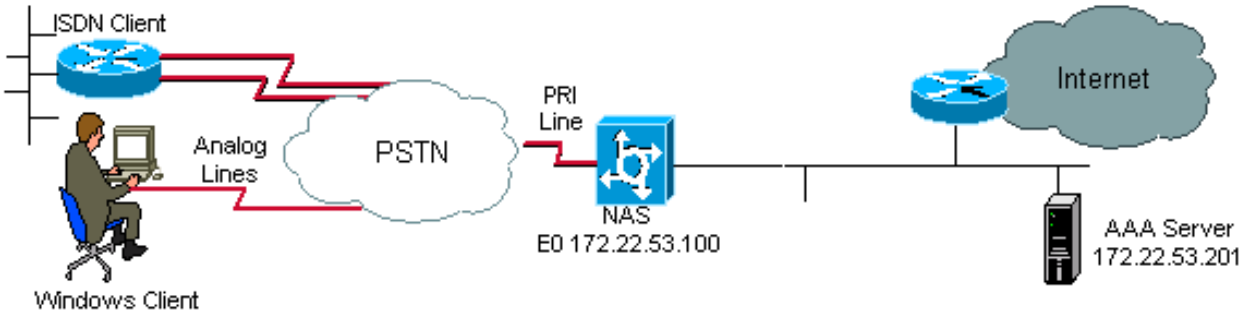

Diagrama de Rede

Configuração geral de AAA

Ativar AAA

Para habilitar o AAA, é necessário configurar o comando aaa new-model na configuração global.

> **Note**: Até que este comando esteja habilitado, todos os outros comandos AAA estarão ocultos.

> **aviso:** O comando **aaa new-model aplica imediatamente a autenticação local a todas as linhas e interfaces (com exceção da linha de console line con 0).** Se uma sessão telnet for aberta para o roteador após a ativação desse comando (ou se o tempo limite de uma conexão for excedido e for necessário reconectar), o usuário deverá ser autenticado com o banco de dados local do roteador. É recomendável definir um nome de usuário e uma senha no servidor de acesso antes de iniciar a configuração AAA, para que você não seja bloqueado no roteador. Veja o próximo exemplo de código.

```
Router(config)#username xxx password yyy
```

> **Tip**: Antes de configurar os comandos AAA, save sua configuração. Você pode save a configuração novamente somente após ter concluído sua configuração AAA (e estiver satisfeito que ela funciona corretamente). Isso permite que você se recupere de bloqueios inesperados, pois pode reverter qualquer alteração com uma recarga do roteador.

Especifique o servidor AAA externo

Na configuração global, defina o protocolo de segurança utilizado com o AAA (Radius, TACACS+). Se você não quiser usar esses dois protocolos, use o banco de dados local no roteador.

Se você usa TACACS+, use o comando **tacacs-server host <endereço IP do servidor AAA> <chave>**.

Se você usar Radius, use o comando **radius-server host <endereço IP do servidor AAA> <chave>**.

Configuração do servidor AAA

No servidor AAA, configure os próximos parâmetros:

- O nome do servidor de acesso.
- O endereço IP que o servidor de acesso usa para comunicar-se com o servidor AAA.**Note**: Se ambos os dispositivos estiverem na mesma rede Ethernet, por padrão, o servidor de acesso usa o endereço IP definido na interface Ethernet quando ele envia o pacote AAA. Esse problema é importante quando o roteador tem várias interfaces (e, portanto, vários endereços).
- A mesma chave exata <key> configurada no servidor de acesso.**Note**: A chave diferencia maiúsculas de minúsculas.
- O protocolo usado pelo servidor de acesso (TACACS+ ou Radius).

Consulte a documentação do servidor AAA para obter o procedimento exato usado para configurar os parâmetros anteriores. Se o servidor AAA não estiver configurado corretamente, as solicitações AAA do NAS podem ser ignoradas pelo servidor AAA e a conexão pode falhar.

O servidor AAA precisa ser de IP praticável no servidor de acesso (realize um teste de ping para verificar a conectividade).

Configuração de autenticação

A autenticação verifica os usuários antes que tenham acesso à rede e aos serviços de rede (que são verificados com autorização).

Para configurar a autenticação AAA:

1. Primeiro defina uma lista nomeada de métodos de autenticação (no modo de configuração global).
2. Aplique essa lista a uma ou mais interfaces (no modo de configuração de interface).

A única exceção é a lista de métodos padrão (que é chamada de **default**). A lista de métodos padrão é aplicada automaticamente a todas as interfaces, exceto aquelas que tenham uma lista de métodos nomeada explicitamente definida. Uma lista de métodos definida substitui a lista de métodos padrão.

Esses exemplos de autenticação usam autenticação Radius, login e PPP (Point-to-Point Protocol) para explicar conceitos como métodos e listas nomeadas. Em todos os exemplos, TACACS+ pode ser substituído por Radius ou autenticação local.

O Cisco IOS Software usa o primeiro método listado para autenticar usuários. Se aquele método falhar em responder (indicado por um ERRO), o software Cisco IOS seleciona o próximo método de autenticação listado na lista de métodos. Esse processo continua até que haja uma comunicação bem-sucedida com um método de autenticação listado ou que todos os métodos definidos na lista de métodos sejam esgotados.

Éimportante observar que o software Cisco IOS tenta realizar a autenticação com o próximo método de autenticação listado, somente quando não há resposta do método anterior. Se a autenticação falhar em qualquer ponto desse ciclo, ou seja, se as respostas do servidor AAA ou do banco de dados de nome de usuário local forem para negar o acesso do usuário (indicado por uma FALHA), o processo de autenticação será interrompido e nenhum outro método de autenticação será tentado.

Para permitir uma autenticação de usuário, você deve configurar o nome de usuário e a senha no servidor AAA.

Autenticação de login

Você pode usar o comando **aaa authentication login para autenticar os usuários que desejam acesso exec no servidor de acesso (tty, vty, console e aux).**

Exemplo 1: Acesso Exec com Radius e Local

```
Router(config)#aaa authentication login default group radius local
```

No comando anterior:

- A lista nomeada é a padrão (default).
- Existem dois métodos de autenticação (raio de grupo e local)

Todos os usuários são autenticados com o servidor Radius (o primeiro método). Se o servidor Radius não responder, o banco de dados local do roteador será usado (o segundo método). Para autenticação local, defina o nome de usuário e a senha:

```
Router(config)#username xxx password yyy
```

Como o padrão de lista no comando **aaa authentication login** é usado, a autenticação de logon é aplicada automaticamente para todas as conexões de logon (como tty, vty, console e aux).

> **Note**: O servidor (Radius ou TACACS+) não pode responder a uma solicitação de **autenticação AAA** enviada pelo servidor de acesso se não houver conectividade IP, se o servidor de acesso não estiver definido corretamente no servidor AAA ou se o servidor AAA não estiver definido corretamente no servidor de acesso.

> **Note**: Se você usar o exemplo anterior, sem a palavra-chave **local**, o resultado será:

```
Router(config)#aaa authentication login default group radius
```

> **Note**: Se o servidor AAA não responder à solicitação de autenticação, a autenticação falhará (já que o roteador não tem um método alternativo para tentar).

> **Note**: A palavra-chave **group** fornece uma maneira de agrupar os hosts do servidor atual. O recurso permite que o usuário selecione um subconjunto dos hosts do servidor configurados e os use para um serviço específico.

Exemplo 2: Acesso de console usado com senha de linha

Expanda a configuração do Exemplo 1 para que o login do console seja autenticado apenas pela senha definida na linha con 0.

O CONSOLE da lista é definido e aplicado a line con 0.

Configuração:

```
Router(config)#aaa authentication login CONSOLE line
```

No comando anterior:

- a lista nomeada é CONSOLE.
- Há somente um método de autenticação (linha).

Quando uma lista nomeada (neste exemplo, CONSOLE) é criada, ela deve ser aplicada a uma linha ou interface antes de ser executada. Isso é feito com o comando login authentication comando:

```
Router(config)#line con 0
Router(config-line)#exec-timeout 0 0
Router(config-line)#password cisco
Router(config-line)#login authentication CONSOLE
```

A lista CONSOLE substitui a lista de métodos padrão **default** na linha con 0. Após esta configuração na linha con 0, você precisa digitar a senha **cisco** para obter acesso ao console. A lista padrão ainda é usada em tty, vty e aux.

> **Note**: Para que o acesso ao console seja autenticado por um nome de usuário e senha locais, use o próximo exemplo de código:

```
Router(config)#aaa authentication login CONSOLE local
```

Nesse caso, um nome de usuário e uma senha devem ser configurados no banco de dados local do roteador. A lista também deve ser aplicada à linha ou interface.

> **Note**: Para não ter autenticação, use o próximo exemplo de código:

```
Router(config)#aaa authentication login CONSOLE none
```

Nesse caso, não há autenticação para obter acesso ao console. A lista também deve ser aplicada à linha ou interface.

Exemplo 3: Habilitar o acesso de modo usado com o servidor AAA externo

Você pode emitir a autenticação para entrar no modo de habilitação (privilégio 15).

Configuração:

```
Router(config)#aaa authentication enable default group radius enable
```

Somente a senha pode ser solicitada; o nome de usuário é $enab15$. Portanto, o nome de usuário $enab15$ deve ser definido no servidor AAA.

Se o servidor Radius não responder, a senha de ativação configurada localmente no roteador pode ter que ser inserida.

Autenticação PPP

O comando **aaa authentication ppp é usado para autenticar uma conexão PPP.** Geralmente, é usado para autenticar usuários remotos ISDN ou analógicos que desejam acessar a Internet ou um escritório central através de um servidor de acesso.

Exemplo 1: Método de autenticação PPP único para todos os usuários

O servidor de acesso tem uma interface ISDN configurada para aceitar clientes de discagem PPP. Usamos um **dialer rotary-group 0**, mas a configuração pode ser feita na interface principal ou na interface do perfil do discador.

Configuração:

```
Router(config)#aaa authentication ppp default group radius local
```

Esse comando autentica todos os usuários PPP com Radius. Se o servidor Radius não responder, o banco de dados local será usado.

Exemplo 2: Autenticação PPP usada com uma lista específica

Para usar uma lista nomeada em vez da lista padrão, configure estes comandos:

```
Router(config)#aaa authentication ppp ISDN_USER group radius

Router(config)#interface dialer 0
Router(config-if)#ppp authentication chap ISDN_USER
```

Nesse exemplo, a lista é ISDN_USER, e o método é Radius.

Exemplo 3: PPP iniciado a partir de sessão no modo de caractere

O access-server tem uma placa de modem interna (Mica, Microcom ou Next Port). Suponha que os comandos **aaa authentication login** e **aaa authentication ppp** estejam configurados.

Se um usuário do modem acessar primeiro o roteador com uma sessão exec do modo de caractere (por exemplo, com Janela do terminal após discagem), o usuário será autenticado em uma linha tty. Para iniciar uma sessão de modo de pacote, os usuários devem digitar ppp default ou ppp. Como a autenticação do PPP é explicitamente configurada (com o **PPP de autenticação de AAA), o usuário é autenticado no nível de PPP novamente.**

Para evitar essa segunda autenticação, use a palavra-chave **if-needed**:

```
Router(config)#aaa authentication login default group radius local
Router(config)#aaa authentication ppp default group radius local if-needed
```

> **Note**: Se o cliente inicia uma sessão PPP diretamente, a autenticação PPP é executada diretamente, pois não há acesso de login ao servidor de acesso.

Configurar autorização

A autorização é o processo pelo qual você pode controlar o que um usuário pode fazer.

Autorização AAA tem as mesmas regras que a autenticação:

1. Primeiro, defina uma lista nomeada de métodos de autorização.
2. Em seguida, aplique essa lista a uma ou mais interfaces (exceto a lista de métodos padrão).
3. O primeiro método listado é usado. Se ela não responder, o segundo método é usado e assim por diante.

As listas de método são específicas para o tipo de autorização solicitado. Este documento se concentra nos tipos de autorização Exec e Network.

Para obter mais informações sobre outros tipos de autorização, consulte o Guia de Configuração de Segurança do Cisco IOS .

Autorização de exec

O comando aaa authorization exec determina se o usuário tem permissão para executar um shell EXEC. Esse recurso pode retornar informações de perfil do usuário, como informações de comando automático, timeout de ociosidade, timeout de sessão, privilégio e lista de acesso e outros fatores por usuário.

A autorização do exec é executada apenas nas linhas vty e tty.

O próximo exemplo usa Radius.

Exemplo 1: Mesmos Métodos de Autenticação Exec para Todos os Usuários

Quando autenticado com:

```
Router(config)#aaa authentication login default group radius local
```

Todos os usuários que desejarem efetuar login no servidor de acesso devem ser autorizados com Radius (primeiro método) ou banco de dados local (segundo método).

Configuração:

```
Router(config)#aaa authorization exec default group radius local
```

Note: No servidor AAA, Service-Type=1 (login) deve ser selecionado.

Note: Neste exemplo, se a palavra-chave **local** não estiver incluída e o servidor AAA não responder, portanto, a autorização não será possível e a conexão poderá falhar.

Note: Nos próximos Exemplos 2 e 3, você não precisa adicionar nenhum comando no roteador. Você só precisa configurar o perfil no servidor de acesso.

Exemplo 2: Atribua níveis de privilégio de exec do servidor AAA

Com base no Exemplo 1, configure o próximo par Cisco AV no servidor AAA para que um usuário possa fazer login no servidor de acesso e entrar diretamente no modo enable:

```
shell:priv-lvl=15
```

Agora o usuário pode ir diretamente para o modo de ativação (enable mode).

Note: Se o primeiro método falhar em responder, o banco de dados está sendo utilizado. No entanto, o usuário não pode ir diretamente para o modo de ativação, mas precisa inserir o comando de ativação e fornecer a senha de ativação.

Exemplo 3: Atribua Idle-Timeout do servidor AAA

Para configurar um timeout de ociosidade (de modo que a sessão seja desconectada no caso de nenhum tráfego após o timeout de ociosidade) use o atributo IETF Radius 28: Idle-Timeout no perfil do usuário.

Autorização de rede

O **aaa authorization network** executa a autorização para todas as solicitações de serviço relacionadas à rede, como PPP, SLIP e ARAP. Esta seção se concentra no PPP, que é o mais comumente usado.

O servidor de AAA verifica se uma sessão PPP pelo cliente é permitida. Além disso, as opções do PPP podem ser solicitadas pelo cliente: retorno de chamada, compactação, endereço IP e assim por diante. Essas opções devem ser configuradas no perfil do usuário no servidor AAA. Além disso, para um cliente específico, o perfil AAA pode conter timeout de ociosidade, lista de acesso e outros atributos por usuário que podem ser baixados pelo software Cisco IOS e aplicados a esse cliente.

Os próximos exemplos mostram a autorização com Radius.

Exemplo 1: Mesmos métodos de autorização de rede para todos os usuários

O servidor de acesso é usado para aceitar conexões de discagem PPP.

Os usuários são autenticados (como foi configurado anteriormente) com:

```
Router(config)#aaa authentication ppp default group radius local
```

Use o comando seguinte para autorizar os usuários:

```
Router(config)#aaa authorization network default group radius local
```

Note: No servidor AAA, configure: **Service-Type=7** (enquadrado) e **Framed-Protocol=PPP**.

Exemplo 2: Aplicar Atributos Específicos do Usuário

Você pode usar o servidor AAA para atribuir atributos por usuário, como endereço IP, número de retorno de chamada, valor de timeout de ociosidade do discador ou lista de acesso, etc. Em tal implementação, o NAS faz o download dos atributos adequados do perfil de usuário do servidor de AAA.

Exemplo 3: Autorização PPP com uma lista específica

Semelhante à autenticação, configure um nome de lista em vez de um padrão:

```
Router(config)#aaa authorization network ISDN_USER group radius local
```

Em seguida, aplique esta lista à interface:

```
Router(config)#interface dialer 0
Router(config-if)#ppp authorization ISDN_USER
```

Configuração de Contabilização

O recurso de contabilização AAA permite que você rastreie os serviços que os usuários acessam e a quantidade de recursos de rede que eles consomem.

A auditoria de AAA tem as mesmas regras que a autenticação e a autorização:

1. Você deve primeiro definir uma lista nomeada de métodos de contagem.
2. Em seguida, aplique essa lista a uma ou mais interfaces (exceto a lista de métodos padrão).
3. O primeiro método listado é utilizado e, se ele não responder, o segundo é utilizado, e assim por diante.

- A contabilização da rede fornece informações de todas as sessões de PPP, Slip e AppleTalk Remote Access Protocol (ARAP). contagem de pacotes, contagem de octetos, tempo de sessão, hora de início e de término.
- A contabilidade Exec fornece informações sobre sessões de terminal EXEC (uma sessão telnet por exemplo) do servidor de acesso à rede: Tempo da sessão, horário de início e de término.

Os próximos exemplos focalizam como as informações podem ser enviadas ao servidor AAA.

Exemplos de Configuração de Contabilização

Exemplo 1: Gerar Registros de Contabilização Inicial e Final

Para cada sessão PPP de discagem, as informações de contabilização são enviadas ao servidor AAA depois que o cliente é autenticado e depois da desconexão com a palavra-chave **start-stop**.

```
Router(config)#aaa accounting network default start-stop group radius local
```

Exemplo 2: Gerar Somente Registros Contábeis de Parada

Se as informações de relatório tiverem que ser enviadas somente depois que um cliente tiver se desconectado, use a palavra-chave **stop** e configure a próxima linha:

```
Router(config)#aaa accounting network default stop group radius local
```

Exemplo 3: Gerar registros de recursos para falhas de autenticação e negociação

Até esse ponto, a auditoria de AAA oferece suporte ao registro de início e de término para chamadas que passaram pela autenticação de usuário.

Se ocorrer uma falha na autenticação ou na negociação de PPP, não haverá registro de autenticação.

A solução é utilizar o relatório de parada de falha do recurso AAA:

```
Router(config)#aaa accounting send stop-record authentication failure
```

Éenviado um registro de parada para o servidor AAA.

Exemplo 4: Habilitar Contabilização de Recursos Completos

Para habilitar a contabilização completa de recursos, que gera tanto um registro de início na configuração de chamada quanto um registro de interrupção ao término da chamada, configure:

```
Router(config)#aaa accounting resource start-stop
```

Esse comando foi apresentado no Cisco IOS Software Release 12.1(3)T.

Com este comando, um registro de contabilidade de iniciar-parar configuração e desconexão de chamada controla o progresso da conexão entre o recurso e o dispositivo. Um registro de contabilidade de início e parada de autenticação do usuário separado controla o progresso do gerenciamento de usuários. Esses dois conjuntos de registros contábeis estão interligados com uma ID de sessão exclusiva para a chamada.

Informações Relacionadas

- Suporte Técnico - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.