Configurando AAA básico em um servidor de acesso

Índice

Introdução

Este documento explica como configurar as Autenticação, Autorização e Auditoria (AAA) em um roteador Cisco usando 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.

Nota: Leia por favor a seção na configuração geral AAA antes de continuar com a configuração de Cisco IOS®. A falha fazer assim pode conduzir ao misconfiguration e ao fechamento subsequente.

Antes de Começar

Convenções

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

técnicas Cisco.

Pré-requisitos

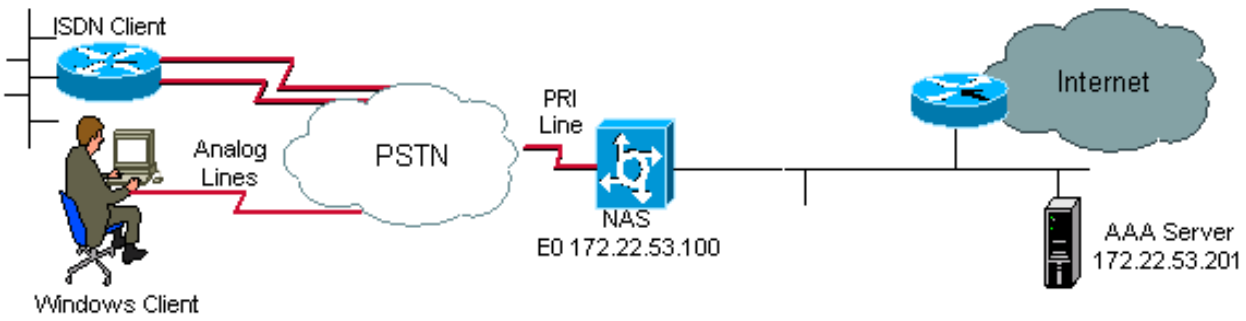
Para obter uma vista geral do AAA, e para detalhes completos sobre comandos aaa e opções, refere por favor o guia de configuração de segurança IO 12.2: Autenticação, autorização e relatório.

Componentes Utilizados

A informação neste documento é baseada na linha principal do Cisco IOS Software Release 12.1.

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 você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Diagrama de Rede



Configuração geral de AAA

Habilitando AAA

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

Nota: 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 relações (exceto a **linha engodo 0 da** linha de console). Se uma sessão de Telnet for aberta para o roteador após a ativação desse comando (ou se o tempo limite de uma conexão expirar e for necessária a reconexão), o usuário deverá ser autenticado usando a base de dados local do roteador. Para evitar o bloqueio por parte do roteador, recomendamos a definição de um nome de usuário e de uma senha no servidor de acesso antes de iniciar a configuração do AAA. Para isso:

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

Dica: Salvar sua configuração antes de configurar seus comandos aaa. Somente após ter concluído toda a configuração do AAA (e após ter certeza de que ela funcionando corretamente) é que você deverá salvar novamente a configuração. Isso permite a recuperação em caso de fechamentos inesperados (antes de salvar a configuração), recarregando o roteador.

Especificando 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 está usando o TACACS+, use o **comando tacacs-server host <IP address of the AAA server> <key>**.

Se você está usando o raio, use o **comando radius-server host <IP address of the AAA server> <key>**.

Configuração do servidor AAA

No servidor AAA, configurar os seguintes parâmetros:

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

Refira sua documentação do servidor AAA para o procedimento exato usado para configurar os parâmetros acima. Se o servidor AAA não for corretamente configurado, as solicitações do NAS ao AAA serão ignoradas pelo servidor AAA e a conexão poderá falhar.

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

Configurando a autenticação

A autenticação verifica usuários antes que o acesso esteja permitido à rede e aos serviços de rede (que estão 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 umas ou várias relações (no modo de configuração da interface).

A única exceção é a lista de métodos padrão (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 método definida cancela a lista do método padrão.

Os exemplos de autenticação abaixo utilizam autenticação RADIUS, de logon e por protocolo de ponto-a-ponto (PPP) (a mais utilizada) 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. Este processo continua até que haja uma comunicação bem sucedida com um método de autenticação listado, ou todos os métodos definidos na lista de método estão esgotados.

Éimportante notar que o Cisco IOS Software tenta a autenticação com o método de autenticação listado seguinte somente quando não há nenhuma resposta do método anterior. Se houver falha de autenticação em qualquer ponto desse ciclo, significando que o servidor AAA ou o banco de dados de nome de usuário local responde negando acesso ao usuário (indicado por FAIL), o processo de autenticação será interrompido e nenhum outro método de autenticação será usado.

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** autenticar os usuários que querem o acesso de exec no servidor de acesso (tty, vty, console e auxiliar).

Exemplo 1: Exec Access using Radius then Local

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

No comando acima:

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

Todos os usuários são autenticados usando o servidor Radius (o primeiro método). Se o servidor Radius não responde, a seguir o base de dados local do roteador está usado (o segundo método). Para autenticação local, defina o nome de usuário e a senha:

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

Devido ao fato de estarmos usando o padrão de lista no comando aaa authentication login, a autenticação de logon é automaticamente aplicada a todas as conexões de logon (como tty, vty, console e aux).

Nota: O servidor (Radius ou TACACS+) não responderá a uma solicitação de autenticação AAA enviada pelo servidor de acesso se não houver uma 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.

Nota: Com o exemplo acima, se não incluirmos a palavra-chave local, teremos:

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

Nota: Se a solicitação de autenticação não for respondida pelo servidor AAA, a autenticação falhará (desde que o roteador não tenha um método alternativo a ser tentado).

Nota: A palavra-chave de grupo fornece uma maneira de agrupar hosts de servidor existentes. O recurso permite que o usuário selecione um subconjunto dos hosts do servidor configurados e os use para um serviço específico. Para obter mais informações sobre destes recursos avançados,

refira o Grupo de servidores AAA do documento.

Exemplo 2: Acesso de console usando a senha de linha

Permite expandir a configuração a partir do Exemplo 1 de forma que o login do console apenas seja autenticado pela senha definida na linha con 0.

O CONSOLE da lista é definido e aplicado então para alinhar o engodo 0.

Configuramos:

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

No comando acima:

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

Depois de criada uma lista nomeada (neste exemplo, CONSOLE), ela deve ser aplicada a uma linha ou interface para que possa entrar em vigor. Isto é feito usando o comando login authentication list_name:

```
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 do CONSOLE cancela o padrão da lista do método padrão na linha engodo 0. Você precisa de incorporar a senha “Cisco” (configurado na linha engodo 0) para obter o acesso de console. A lista padrão é usada ainda no tty, vty e auxiliar.

Nota: Para ter o acesso de console autenticado por um nome de usuário local e por uma senha, use:

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

Nota: 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.

Nota: Para não ter nenhuma autenticação, use

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

Nota: 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 usando servidor AAA externo

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

Configuramos:

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

Somente a senha será pedida, o username é $enab15$. Daqui o username $enab15$ deve ser

definido no servidor AAA.

Se o servidor Radius não responder, a senha de habilitação configurada localmente no roteador precisará ser digitada.

Autenticação PPP

O comando aaa authentication ppp é usado autenticar uma conexão PPP. É usada tipicamente para autenticar o ISDN ou os usuários remotos análogos que querem alcançar o 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 que seja configurada para aceitar clientes do dialin PPP. Nós usamos um dialer rotary-group 0 mas a configuração pode ser definida na interface principal ou na interface de perfil do discador.

Nós configuramos

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

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

Exemplo 2: Autenticação de PPP utilizando uma lista específica

Para usar uma lista nomeada um pouco do que a lista padrão, configurar os comandos seguintes:

```
Router(config)# aaa authentication ppp ISDN_USER group radius Router(config)# int dialer 0
Router(config-if)# pp 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 servidor de acesso tem um cartão do modem interno (mica, Microcom ou porta seguinte). Vamos assumir que os comandos aaa authentication login e aaa authentication ppp estejam configurados.

Se um usuário de modem acessar primeiro o roteador usando uma sessão de exec do modo de caractere (por exemplo, usando Janela Terminal depois de Discar), o usuário será autenticado em uma linha tty. Para iniciar uma sessão de modo de pacote, os usuários devem digitar ppp default ou ppp. Desde que a autenticação de PPP é configurada explicitamente (com **autenticação ppp aaa**), o usuário é autenticado a nível PPP outra vez.

Para evitar essa segunda autenticação, pode-se utilizar 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
```

Nota: Se o cliente iniciar diretamente uma sessão PPP, a autenticação PPP será realizada diretamente, pois não há acesso de logon ao servidor de acessos.

Para obter mais informações sobre autenticação AAA, consulte os documentos do Manual de configuração de segurança do IOS 12.2: Configurando a autenticação e os Casos Práticos de Implementação do Cisco AAA.

Configurando autorização

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

Autorização AAA tem as mesmas regras que a autenticação:

1. Primeiro, defina uma lista nomeada de métodos de autorização.
2. Aplique então essa lista a umas ou várias relações (à exceção da lista do método 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 centra-se sobre os tipos do executivo e da autorização de rede.

Para obter mais informações sobre outros tipos de autorização, consulte o Manual de configuração de segurança do IOS da Cisco, versão 12.2.

Autorização de exec

O comando aaa authorization exec determina se o usuário tem permissão para executar um shell EXEC. Esta instalação pode retornar informações de perfil de usuário como autocomando, tempo-limite de ociosidade, tempo-limite de sessão, privilégio e lista de acesso e outros fatores por usuário.

A autorização de exec é realizada somente sobre linhas vty e tty.

O exemplo a seguir utiliza Radius.

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

Após a autenticação com:

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

Todos os usuários que queiram fazer login no servidor de acesso terão de ser autorizados usando o Radius (primeiro método) ou o banco de dados local (segundo método).

Configuramos:

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

Nota: No servidor AAA, Service-Type=1 (início de uma sessão) deve ser selecionado.

Nota: Com este exemplo, se o **palavra-chave local** não é incluído e o servidor AAA não responde, a seguir a autorização nunca será possível e a conexão falhará.

Nota: Nos exemplos 2 e 3 abaixo, nós não precisamos de adicionar o comando any no roteador mas de configurar somente o perfil no servidor de acesso.

Exemplo 2: Atribuição de Níveis de Privilégio de Execução do Servidor AAA

Baseado no exemplo 1, se um usuário que registre no servidor de acesso deve ser reservada incorporar diretamente o modo enable, configurar o seguinte par Cisco AV no servidor AAA:

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

Isto significa que o usuário entra diretamente no modo ativo.

Nota: Se o primeiro método falhar em responder, o banco de dados está sendo utilizado. No entanto, o usuário não passará diretamente para o modo de ativação, mas terá que digitar o comando enable e fornecer a senha de ativação.

Exemplo 3: Atribuindo Intervalo Ocioso do Servidor AAA

Para configurar um tempo limite de ociosidade (de modo que a sessão seja desconectada no caso de não haver tráfego após o tempo limite de ociosidade), use o atributo IETF Radius 28: Quietude-intervalo sob o perfil de usuário.

Autorização de rede

A comando aaa authorization network executa a autorização para todas as requisições de serviços relacionados à rede, como PPP, SLIP e ARAP. Esta seção concentra-se no PPP, que é o mais utilizado.

O servidor de AAA verifica se uma sessão PPP pelo cliente é permitida. Além disso, as opções do PPP podem ser solicitadas pelo cliente: rechamada, compressão, endereço IP de Um ou Mais Servidores Cisco ICM NT, e assim por diante. Essas opções devem ser configuradas no perfil do usuário no servidor AAA. Além disso, para um cliente específico, o perfil de AAA pode conter intervalo ocioso, lista de acesso e outros atributos por usuário cujo download será feito pelo software Cisco IOS e aplicados para esse cliente.

A autorização da mostra do exemplo seguinte usando o raio:

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

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

Inicialmente, os usuários são autenticados (como configurado anteriormente) usando:

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

em seguida, eles devem ser autorizados usando:

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

Nota: No servidor AAA, configure:

- Service-Type=7 (quadros configurados)
- Framed-Protocol = PPP

Exemplo 2: Aplicando atributos específicas de usuário

Você pode usar o servidor AAA para designar atributos por peer, 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

Assim como na autenticação, podemos configurar um nome de lista, em vez de usar o padrão:

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

Em seguida, esta lista é aplicada à interface:

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

Para obter mais informações sobre autenticação AAA, consulte os documentos do Manual de configuração de segurança do IOS 12.2: Configurando a autenticação e os Casos Práticos de Implementação do Cisco AAA.

Configurando relatório

O recurso de contabilização de AAA permite controlar os serviços que os usuários estão acessando e a quantidade de recursos da rede que estão consumindo.

A contabilidade AAA tem as mesmas regras que a authentication e autorização:

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

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). o contagem de pacote de informação, octects conta, tempo de sessão, horário de início e de parada.
- 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.

Para obter mais informações sobre outros tipos de autorização, consulte o Manual de configuração de segurança do IOS da Cisco, versão 12.2.

Os exemplos a seguir enfatizam como as informações podem ser enviadas ao servidor AAA.

Configurando exemplos de relatórios

Exemplo 1: Gerando os registros de contabilidade de início e de parada

Para cada sessão PPP de discagem, a informação de contabilidade está enviada ao servidor AAA

uma vez que o cliente é autenticado e após a disconexão usando a palavra-chave **start-stop**.

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

Exemplo 2: Gerando apenas registros de contabilidade de parada

Se informações contábeis tiverem de ser enviadas somente após a desconexão de um cliente, use a palavra-chave stop e configure a seguinte linha:

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

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

Até este ponto, a contabilidade AAA fornece o suporte de registro de início e parada para os atendimentos que passaram a autenticação de usuário.

Se a autenticação ou a negociação de PPP falham, não há nenhum registro da 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: Ativando o relatório de recurso completo

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 de contabilização são interligados usando um único ID de sessão da chamada.

Para obter mais informações sobre autenticação AAA, consulte os documentos do Manual de configuração de segurança do IOS 12.2: Configurando a autenticação e os Casos Práticos de Implementação do Cisco AAA.

Informações Relacionadas

- Suporte Técnico - Cisco Systems