

# Módulo 19: Controle de acesso



CyberOps Associate v1.0

Prof. Clemilson Oliveira

[clemilson.oliveira@edu.sc.senai.br](mailto:clemilson.oliveira@edu.sc.senai.br)



# Objetivos do módulo

**Título do módulo:** Controle de acesso

**Objetivo do módulo:** Explicar o controle de acesso como um método de proteção de uma rede.

Título do Tópico	Objetivo do Tópico
Conceitos de controle de acesso	Explique como os dados de rede de protocolos de controle de acesso.
Uso e operação AAA	Explicar como o AAA é usado para controlar o acesso à rede.

# 19.1 Conceitos de controle de acesso

# Segurançadas comunicações de controle de acesso: CIA

A segurança da informação trata da proteção da informação e dos sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição.

## Tríade CIA

A tríade da CIA consiste em três componentes da segurança da informação:

- **Confidencialidade** - Apenas indivíduos, entidades ou processos autorizados podem acessar informações confidenciais.
- **Integridade** - Refere-se à proteção de dados contra alterações não autorizadas.
- **Disponibilidade** - Os usuários autorizados devem ter acesso ininterrupto aos recursos e dados da rede de que necessitam.



# Controle de Acesso Segurança Zero Trust

- Zero Trust é uma abordagem abrangente para proteger todo o acesso em redes, aplicações e ambientes.
- Essa abordagem ajuda a proteger o acesso de usuários, dispositivos de usuário final, APIs, IoT, microsserviços, contêineres e muito mais.
- O princípio de uma abordagem de confiança zero é “nunca confiar sempre verificar”.
- Uma estrutura de segurança de confiança zero ajuda a impedir acesso não autorizado, conter violações e reduzir o risco de movimento lateral de um invasor através de uma rede.
- Em uma abordagem de confiança Zero, qualquer lugar em que uma decisão de controle de acesso seja necessária deve ser considerado um perímetro.

## Segurança de confiança zero(Cont.)

Os três pilares da confiança zero são força de trabalho, cargas de trabalho e local de trabalho.

- **Confiança zero para a Força de Trabalho** -Este pilar consiste em pessoas que acessam aplicativos de trabalho usando seus dispositivos pessoais ou gerenciados por empresas. Ele garante que apenas os usuários certos e dispositivos seguros possam acessar aplicativos, independentemente da localização.
- **Confiança zero para cargas de trabalho** -Esse pilar está preocupado com aplicativos que estão sendo executados na nuvem, em data centers e outros ambientes virtualizados que interagem entre si. Ele se concentra no acesso seguro quando uma API, um microsserviço ou um contêiner está acessando um banco de dados dentro de um aplicativo.
- **Confiança zero para o local de trabalho** - Este pilar se concentra no acesso seguro para todos os dispositivos, inclusive na Internet das Coisas (IoT), que se conectam a redes empresariais, como terminais de usuário, servidores físicos e virtuais, impressoras, câmeras e muito mais.

## Acesso Modelos de Controle de Acesso

- Uma organização deve implementar controles de acesso adequados para proteger seus recursos de rede, recursos do sistema de informações e informações.
- Um analista de segurança deve entender os diferentes modelos básicos de controle de acesso para ter uma melhor compreensão de como os invasores podem quebrar os controles de acesso.
- A tabela a seguir lista vários tipos de modelos de controle de acesso:

Modelos de controle de acesso	Descrição
Discretionary access control (DAC)	<ul style="list-style-type: none"><li>• Este é o modelo menos restritivo e permite que os usuários controlem o acesso aos seus dados como proprietários desses dados.</li><li>• Ele pode usar ACLs ou outros métodos para especificar quais usuários ou grupos de usuários têm acesso às informações.</li></ul>
Controle de acesso obrigatório (MAC)	<ul style="list-style-type: none"><li>• Isso se aplica ao controle de acesso mais rigoroso e é usado em aplicações militares ou de missão crítica.</li><li>• Ele atribui rótulos de nível de segurança às informações e permite que os usuários tenham acesso com base em sua autorização de nível de segurança.</li></ul>

# Modelos de controle de acesso de controle de acesso (Cont.)

Modelos de controle de acesso	Descrição
Role-based access control (RBAC)	<ul style="list-style-type: none"><li>• As decisões de acesso são baseadas nas funções e responsabilidades de um indivíduo dentro da organização.</li><li>• Diferentes funções recebem privilégios de segurança e indivíduos são atribuídos ao perfil RBAC para a função.</li><li>• Também conhecido como um tipo de controle de acesso não discricionário.</li></ul>
Controle de acesso baseado em atributos (ABAC)	Permite o acesso com base em atributos do objeto a ser acessado, o sujeito acessando o recurso e fatores ambientais sobre como o objeto deve ser acessado.
Rule-based access control (RBAC)	<ul style="list-style-type: none"><li>• A equipe de segurança de rede especifica conjuntos de regras ou condições associadas ao acesso a dados ou sistemas.</li><li>• Essas regras podem especificar endereços IP permitidos ou negados, ou determinados protocolos e outras condições.</li><li>• Também conhecido como RBAC Baseado em Regras.</li></ul>
Controle de acesso baseado em tempo (TAC)	Permite o acesso a recursos de rede com base na hora e no dia.



# 19.2 Uso e operação AAA

# AAA Operação AAA

- Uma rede deve ser projetada para controlar quem tem permissão para se conectar a ela e o que eles têm permissão para fazer quando estão conectados. Estes requisitos de design são identificados na política de segurança de rede.
- A política especifica como administradores de rede, usuários corporativos, usuários remotos, parceiros de negócios e clientes acessam recursos de rede.
- A política de segurança de rede também pode exigir a implementação de um sistema de contabilidade que rastreia quem iniciou sessão e quando e o que fizeram durante a sessão iniciada.
- O protocolo AAA (Authentication, Authorization and Accounting) fornece a estrutura necessária para habilitar a segurança de acesso escalável.

## AAA Operação AAA (Cont.)

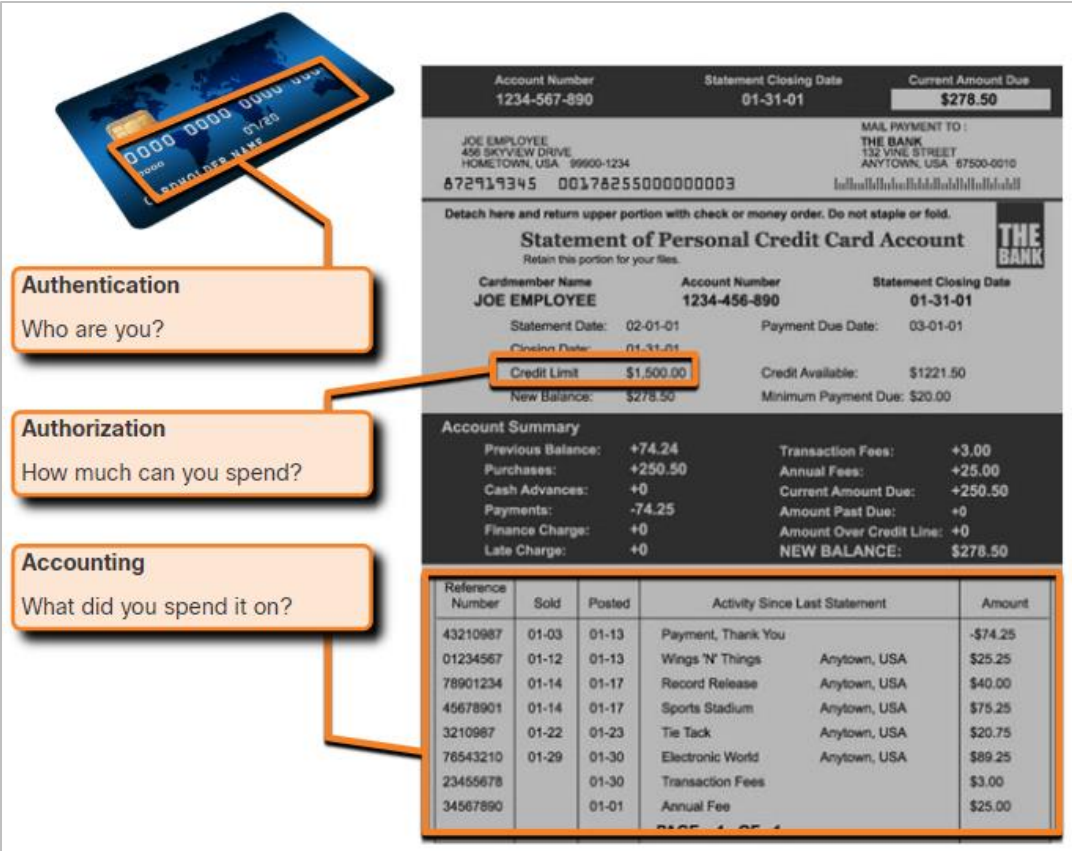
A tabela a seguir lista as três funções de segurança independentes fornecidas pela estrutura arquitetônica AAA:

Componente AAA	Descrição
Autenticação	<ul style="list-style-type: none"><li>A autenticação pode ser estabelecida usando combinações de nome de usuário e senha, perguntas e respostas de desafio, tokens e outros métodos.</li><li>A autenticação AAA fornece uma maneira centralizada de controlar o acesso à rede.</li></ul>
Autorização	<ul style="list-style-type: none"><li>Após a autenticação do usuário, os serviços de autorização determinam quais recursos o usuário pode acessar e quais operações ele tem permissão para executar.</li><li>Um exemplo é "O usuário pode acessar o servidor host XYZ usando apenas SSH."</li></ul>
Accounting (Contabilidade)	<ul style="list-style-type: none"><li>O accounting registra o que o usuário faz, incluindo o que é acessado, a quantidade de tempo em que o recurso é acessado e todas as alterações efetuadas.</li><li>O accounting rastreia como os recursos de rede são usados.</li><li>Um exemplo é "Servidor host acessado pelo usuário XYZ usando SSH por 15 minutos."</li></ul>

# Utilização e operação

## AAA Operação AAA (Cont.)

Esse conceito é semelhante ao uso de um cartão de crédito, conforme indicado na figura. O cartão de crédito identifica quem pode utilizá-lo, estipula um limite de uso e mantém o controle dos itens comprados pelo usuário, como mostrado na figura.



## Uso e operação AAAAutenticaçãoAAA

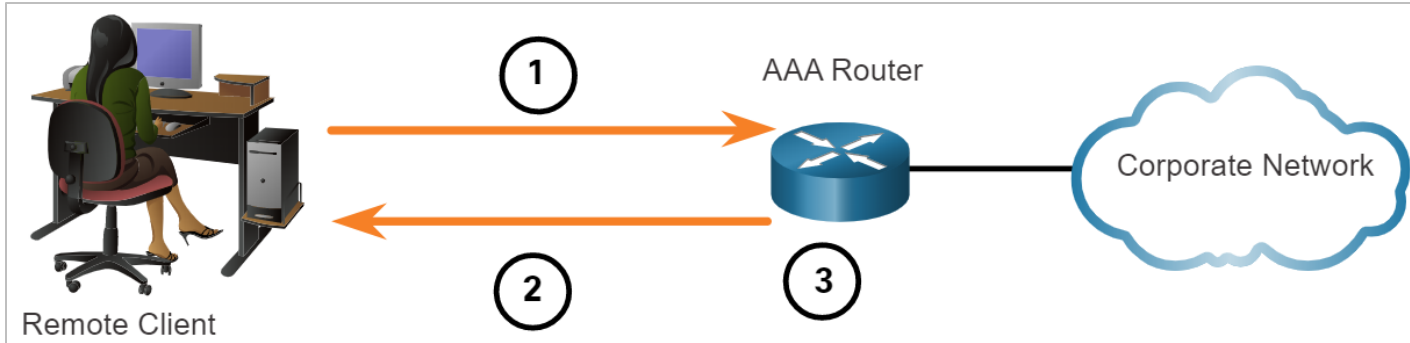
- A autenticação AAA pode ser usada para autenticar usuários para o acesso administrativo ou pode ser usada para autenticar usuários para o acesso à rede remota.
- A Cisco fornece dois métodos comuns para a implementação de serviços AAA:

### **Autenticação de AAA local**

- Este método é conhecido como autenticação autónoma porque autentica os utilizadores contra nomes de utilizador e palavras-passe armazenados localmente.
- A AAA local é ideal para redes pequenas.

## AAA Authentication (Condd.)

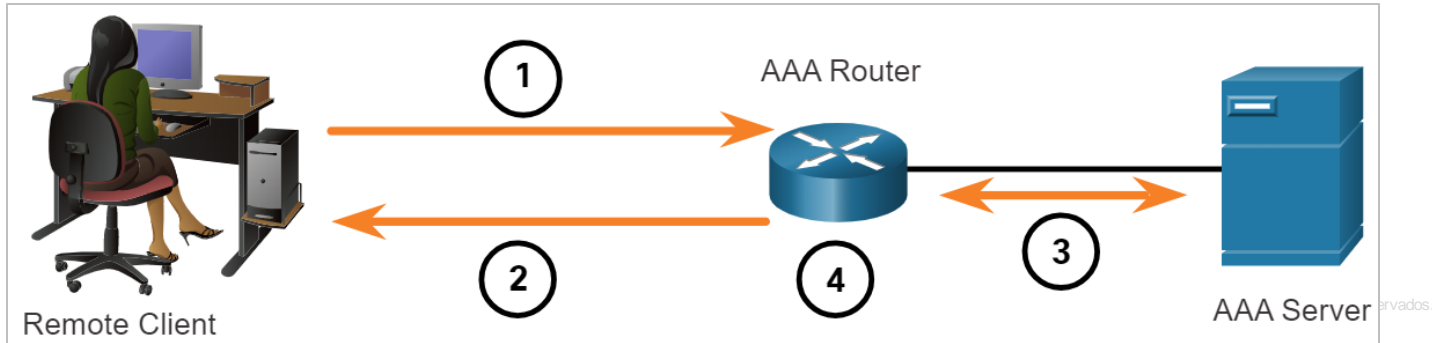
- O cliente estabelece uma conexão com o roteador.
- O roteador AAA solicita que o usuário forneça o nome de usuário e a senha.
- O roteador autenticou o nome de usuário e a senha usando o banco de dados local e o usuário tem acesso à rede com base nas informações do banco de dados local.



## Autenticação AAA (Cont.)

### Autenticação AAA baseada em servidor

- Esse método se autentica em um servidor AAA central que contém os nomes de usuário e senhas para todos os usuários. Isso é ideal para redes de médio a grande porte.
- O cliente estabelece uma conexão com o roteador.
- O roteador AAA solicita que o usuário forneça o nome de usuário e a senha.
- O roteador autentica o nome do usuário e a senha usando um servidor AAA.
- O usuário recebe acesso à rede com base nas informações no servidor AAA remoto.



## Autenticação AAA (Cont.)

### AAA centralizado

- O AAA centralizado é mais escalável e gerenciável do que a autenticação AAA local e, portanto, é a implementação AAA preferida.
- Um sistema AAA centralizado pode manter bancos de dados independentemente para autenticação, autorização e contabilidade.
- Ele pode aproveitar o Active Directory ou o Lightweight Directory Access Protocol (LDAP) para autenticação de usuário e associação de grupo, mantendo seus próprios bancos de dados de autorização e contabilidade.
- Os dispositivos se comunicam com o servidor AAA centralizado usando os protocolos RADIUS (Remote Authentication Dial-In User Service) ou Terminal Access Controller Access Control System (TACACS +).



## Autenticação AAA (Cont.)

A tabela a seguir lista as diferenças entre os dois protocolos:

Funções	TACACS+	RADIUS
Funcionalidade	Ele separa as funções de autenticação, autorização e contabilidade de acordo com a arquitetura AAA. Isso permite a modularidade da implementação do servidor de segurança.	Ele combina autenticação e autorização, mas separa a contabilidade, o que permite menos flexibilidade na implementação do TACACS+.
Padrão	Principalmente com suporte Cisco	Padrão aberto/RFC
Transporte	Porta TCP 49	Portas UDP 1812 e 1813, ou 1645 e 1646
Protocolo CHAP	Desafio bidirecional e resposta conforme usado no Challenge Handshake Authentication Protocol (CHAP)	Desafio unidirecional e resposta do servidor de segurança RADIUS para o cliente RADIUS

## Autenticação AAA (Cont.)

Funções	TACACS+	RADIUS
Confidencialidade	Criptografa todo o corpo do pacote, mas deixa um cabeçalho TACACS+ padrão.	Criptografa somente a senha no pacote de solicitação de acesso do cliente para o servidor. O restante do pacote é descriptografado, deixando o nome de usuário, os serviços autorizados e a contabilidade desprotegidos.
Personalização	Fornece autorização de comandos de roteador por usuário ou por grupo.	Não tem opção para autorizar comandos de roteador por usuário ou por grupo.
Accounting	Limitado	Abrangente

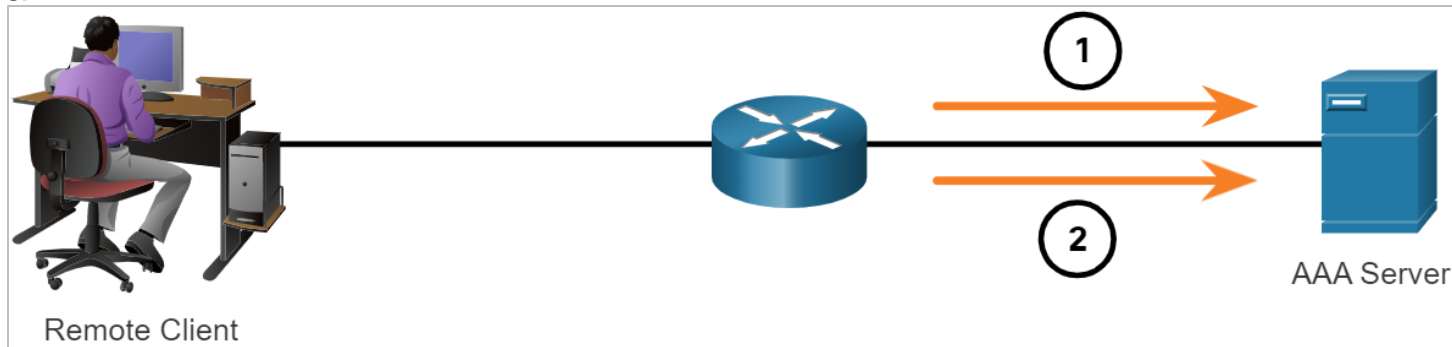
## Utilização do AAA e Operações

# Registros de ContabilidadeAAA

- O AAA centralizado também permite o uso do método de contabilidade.
- Os registros contábeis de todos os dispositivos são enviados para repositórios centralizados, o que simplifica a auditoria das ações do usuário.
- AAA Accounting coleta e relata dados de uso em registros AAA. Esses logs são úteis para auditoria de segurança.
- Os dados coletados podem incluir os horários de conexão inicial e final, comandos executados, número de pacotes e número de bytes.
- Um uso amplamente difundido da contabilidade é combiná-lo com a autenticação AAA. Isso ajuda a gerenciar o acesso a dispositivos de interrede pela equipe administrativa da rede.

## Utilização do AAA e Operação Registros de Contabilidade AAA (Cond.)

- Contabilidade fornece mais segurança do que apenas autenticação. Os servidores AAA mantêm um registro detalhado de exatamente o que o usuário autenticado faz no dispositivo.
- Isso inclui todos os comandos EXEC e de configuração emitidos pelo usuário.
- Quando um usuário realiza autenticação, o processo de contabilização AAA gera uma mensagem inicial para iniciar a contabilização.
- Quando o usuário termina, uma mensagem de parada é inserida e o processo contábil finaliza.



# Registro de contabilidade AAA(Cont.)

A tabela a seguir descreve os tipos de informações contábeis que podem ser coletadas:

Tipos de informações contábeis	Descrição
Contabilidade de Rede	Ele captura informações para todas as sessões PPP (Point-to-Point Protocol), incluindo contagens de pacotes e bytes.
Contabilidade de Conexão	Ele captura informações sobre todas as conexões de saída feitas a partir do cliente AAA, como por SSH.
Contabilidade EXEC	Ele captura informações sobre sessões de terminal EXEC do usuário no servidor de acesso à rede, incluindo nome de usuário, data, horas de início e parada e o endereço IP do servidor de acesso.
Contabilidade do Sistema	Ele captura informações sobre todos os eventos no nível do sistema.
Contabilidade de Comando	Ele captura informações sobre os comandos do shell EXEC para um nível de privilégio especificado, bem como a data e hora em que cada comando foi executado e o usuário que o executou.
Contabilidade de Recursos	Ele captura o suporte de registro 'start' e 'stop' para conexões que passaram pela autenticação do usuário.

# 19.3 Resumo do controle de acesso

# O que aprendi neste módulo?

- A tríade da CIA consiste nos três componentes principais da segurança da informação: confidencialidade, integridade e disponibilidade (availability).
- Zero Trust é uma abordagem abrangente para proteger todo o acesso em redes, aplicações e ambientes.
- O princípio da confiança zero é “nunca confiar, sempre verificar”. Os pilares da confiança são a confiança zero para a força de trabalho, a confiança zero para cargas de trabalho e a confiança zero para o local de trabalho.
- Numa abordagem de confiança zero, qualquer local em que seja necessária uma decisão de controle de acesso deve ser considerado um perímetro.
- Os métodos de controle de acesso incluem controle de acesso discricionário (DAC), controle de acesso obrigatório (MAC), controle de acesso baseado em função (RBAC), controle baseado em atributos (ABAC), acesso baseado em regras (RBAC) e controle de acesso baseado em tempo (TAC).
- Uma rede deve ser projetada para controlar quem tem permissão para se conectar a ela e o que eles têm permissão para fazer quando estão conectados, o que é especificado na diretiva de segurança de rede.

# O que aprendi neste módulo?

## (Continuação)

- Os sistemas AAA (Authentication, Authorization and Accounting) fornecem a estrutura necessária para permitir uma segurança escalável.
- A Cisco fornece dois métodos comuns de implementação de serviços AAA: Autenticação AAA local e Autenticação AAA baseada em servidor.
- O AAA centralizado é mais escalável e gerenciável do que o AAA local e é a implementação AAA preferida.
- Os dispositivos se comunicam com o servidor AAA centralizado usando os protocolos RADIUS (Remote Authentication Dial-In User Service) ou Terminal Access Controller Access Control System (TACACS +).
- O AAA centralizado também permite o uso do método contábil. AAA Accounting coleta e relata dados de uso em registros AAA.
- Vários tipos de informações contábeis que podem ser coletadas são contabilidade de rede, contabilidade de conexão, contabilidade EXEC, contabilidade de sistema, contabilidade de comando e contabilidade de recursos.



