1.Introdução ao controle de acesso em contas e sistemas

1.1 Controle de acesso

O controle de acesso é um conjunto de políticas, procedimentos e tecnologias que garantem que apenas pessoas autorizadas tenham permissão para acessar recursos, sistemas ou dados específicos. Ele envolve a autenticação, que verifica a identidade do usuário, e a autorização, que determina quais ações ou recursos o usuário tem permissão para utilizar.

O objetivo principal é proteger informações sensíveis e recursos críticos, reduzindo o risco de acessos não autorizados ou uso inadequado, fortalecendo assim a segurança de um ambiente digital.

2.Controle de acesso discricionário (DAC)

Também conhecido como Discretionary Access Control (DAC), é um modelo de controle de acesso que permite que os proprietários de recursos digitais determinem quem pode acessar esses recursos e quais ações podem ser realizadas sobre eles. O DAC funciona da seguinte maneira:

- **Proprietários e recursos:** Em um sistema DAC, cada recurso digital (como arquivos, pastas ou objetos) tem um proprietário. O proprietário é geralmente a pessoa que criou o recurso ou aquele a quem foi atribuído o controle sobre ele.
- **Permissões de acesso:** Cada recurso possui um conjunto de permissões que determinam quais ações podem ser executadas sobre ele. As permissões comuns incluem leitura (read), gravação (write), execução (execute) e exclusão (delete).
- **Lista de controle de acesso (ACL):** Uma ACL é associada a cada recurso e contém informações sobre os usuários ou grupos autorizados a acessar o recurso e suas permissões. Cada entrada na ACL inclui o nome do usuário ou grupo e as permissões associadas.
- **Proprietário e controle:** O proprietário do recurso tem controle total sobre as permissões e pode alterá-las conforme necessário. Ele pode conceder ou revogar acesso a outros usuários ou grupos, conforme sua discricionariedade.

2.1 Controle de acesso baseado em função (RBAC)

O Controle de Acesso Baseado em Função (Role-Based Access Control - RBAC) é um modelo de controle de acesso que se baseia na atribuição de funções específicas aos usuários e, em seguida, concede permissões de acesso com base nessas funções. Veja como o RBAC funciona:

- **Funções:** No RBAC, as funções são criadas com base nas responsabilidades e cargos dentro de uma organização. Cada função descreve um conjunto específico de tarefas ou ações que os usuários desse papel podem executar.
- **Usuários:** Cada usuário é atribuído a uma ou mais funções com base em suas responsabilidades e necessidades de acesso. Os usuários podem pertencer a diferentes funções, dependendo de suas funções na organização.

- **Permissões:** As permissões de acesso são associadas às funções, não diretamente aos usuários. Cada função tem um conjunto de permissões que define quais ações podem ser executadas em recursos específicos.
- **Recursos:** Os recursos incluem ativos digitais, como arquivos, pastas, bancos de dados, aplicativos ou qualquer objeto que precise de controle de acesso. Cada recurso pode ter permissões diferentes associadas a ele.

2.2 Controle de acesso obrigatório (MAC)

O Controle de Acesso Obrigatório (Mandatory Access Control - MAC) é um modelo de controle de acesso que impõe restrições de segurança com base em políticas definidas pelo sistema, em vez de depender das decisões discricionárias dos proprietários de recursos ou dos próprios usuários. Veja o funcionamento do MAC:

- **Políticas de segurança:** No MAC, as políticas de segurança são definidas pelo administrador do sistema ou pela organização. Essas políticas determinam quais usuários ou processos podem acessar recursos e que tipo de operações podem ser executadas.
- **Rótulos de segurança:** Cada recurso e usuário/processo é atribuído um rótulo de segurança, que é uma etiqueta que descreve seu nível de confidencialidade e integridade. Geralmente, esses rótulos são representados por níveis de classificação, como "Alto", "Médio" e "Baixo".
- **Regra de acesso:** Às regras de acesso definem as permissões com base nos rótulos de segurança. Uma regra típica no MAC pode ser: "Os usuários com rótulo 'Alto' podem acessar recursos com rótulo 'Alto' ou 'Médio', mas não 'Baixo'."
- **Aplicações de políticas:** O sistema MAC aplica automaticamente as políticas definidas, sem considerar a discricionariedade dos usuários. Se um usuário ou processo não tiver a combinação de rótulos de segurança necessária, o acesso será negado.

2.3 Controle de acesso baseado em atributos (ABAC)

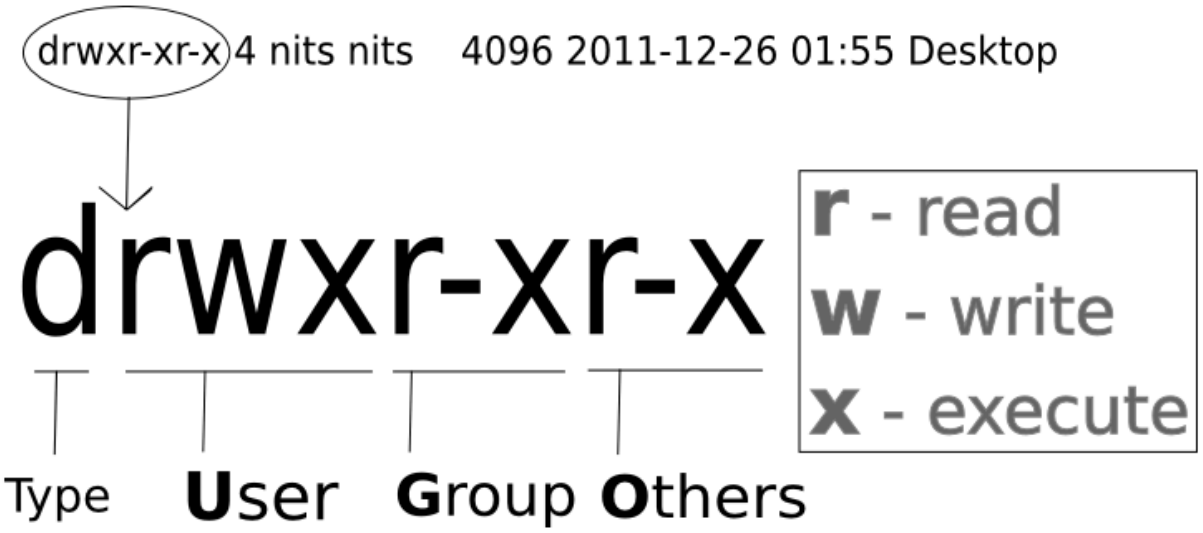
O Controle de Acesso Baseado em Atributos (Attribute-Based Access Control - ABAC) é um modelo de controle de acesso que toma decisões de autorização com base em atributos de entidades, recursos e condições, em vez de depender de funções ou permissões estáticas:

- **Atributos:** O ABAC utiliza atributos para definir características específicas de entidades, recursos e contexto. Os atributos podem incluir informações como a função de um usuário, o local, a data e hora, a classificação de segurança de um documento, entre outros.
- **Entidades:** As entidades no ABAC podem ser usuários, grupos, aplicativos ou qualquer coisa que precise de acesso a recursos. Cada entidade é associada a um conjunto de atributos que a descrevem.
- **Recursos:** Os recursos são os ativos digitais ou físicos que precisam ser protegidos. Cada recurso é associado a um conjunto de atributos que o descrevem, incluindo sua classificação de segurança.
- **Políticas de autorização:** As políticas de autorização são definidas com base em regras que relacionam atributos de entidades, recursos e contexto.

2.4 Permissões do sistema de arquivos

As permissões do sistema de arquivos, como "Read (r)", "Write (w)" e "Execute (x)", junto com os comandos "chmod" e "chown", determinam quais ações os usuários podem realizar em um arquivo ou diretório. Elas são fundamentais para o controle de acesso em sistemas Unix-like. Veja como esses elementos funcionam:

- **Leitura (read - r):** Permite a visualização do conteúdo de um arquivo ou lista de arquivos em um diretório. Com essa permissão, os usuários podem abrir e ler o conteúdo do arquivo, mas não podem modificá-lo.
- **Escrita (write - w):** Permite a modificação e criação de novos arquivos em um diretório. Se aplicada a um arquivo, permite a edição e exclusão do conteúdo do arquivo. Sem essa permissão, os usuários podem apenas visualizar o conteúdo, mas não alterá-lo.
- **Execução (execute - x):** Permite que um arquivo seja executado como um programa ou script. Para diretórios, permite a navegação no diretório e acesso a arquivos e subdiretórios dentro dele. Sem essa permissão, os usuários não podem executar programas ou acessar o conteúdo de diretórios.
- **Comando (chmod):** comando "chmod" é usado para modificar as permissões de um arquivo ou diretório. Pode ser usado em conjunto com diferentes opções para adicionar, remover ou definir permissões específicas. Exemplo: "chmod +x arquivo.sh" adiciona permissão de execução ao arquivo "arquivo.sh".
- **Comando (chown):** O comando "chown" é usado para alterar o proprietário de um arquivo ou diretório. Pode ser usado para atribuir um novo proprietário a um arquivo ou diretório. Exemplo: "chown novo_usuario arquivo.txt" atribui o arquivo "arquivo.txt" ao "novo_usuario".



2.5 Gerenciamento de acesso privilegiado (PAM)

O Gerenciamento de Acesso Privilegiado (Privileged Access Management - PAM) é uma abordagem de segurança que se concentra em proteger e gerenciar o acesso a contas e recursos privilegiados em sistemas de computador e redes. O PAM é crucial para reduzir o risco de ameaças internas e externas, garantindo que apenas as pessoas autorizadas tenham acesso a informações e recursos críticos.

Veja como é implantado o PAM:

- **Identificação de contas privilegiadas:** O primeiro passo no PAM é identificar e listar todas as contas e recursos que são considerados privilegiados em um ambiente de TI. Isso inclui contas de administrador, sistemas, servidores, bancos de dados e outros recursos que podem causar um grande impacto se forem comprometidos.
- **Políticas de acesso:** Com base nas contas e recursos identificados, as políticas de acesso são estabelecidas para determinar quem pode acessar essas contas privilegiadas. As políticas geralmente são definidas com base em cargos, responsabilidades e princípios de menor privilégio, onde o acesso é concedido somente quando necessário.
- **Gerenciamento de credenciais:** O PAM envolve o gerenciamento seguro das credenciais associadas às contas privilegiadas. Isso inclui senhas, chaves de acesso, certificados e outros meios de autenticação. As senhas costumam ser armazenadas de forma criptografada e protegida contra acesso não autorizado.
- **Autenticação multifator (MFA):** Uma prática comum no PAM é a implementação de autenticação multifator (MFA) para contas privilegiadas. O MFA requer que os usuários forneçam duas ou mais formas de autenticação para acessar uma conta, tornando-a mais segura.
- **Monitoramento de atividades:** O PAM inclui a capacidade de monitorar e registrar todas as atividades de acesso privilegiado. Isso ajuda a identificar e responder rapidamente a qualquer atividade suspeita ou não autorizada.
- **Rotação de senhas:** As senhas das contas privilegiadas são regularmente trocadas (rotacionadas) para evitar o uso indevido. A rotação de senhas ajuda a minimizar o risco de senhas comprometidas e garante que apenas as pessoas autorizadas tenham acesso.
- **Controle de sessões:** O PAM permite que as organizações controlem e registrem as sessões de acesso privilegiado com capacidade de encerrar sessões não autorizadas e restringir o tempo de acesso.
- **Aprovação e revisão:** As atividades relacionadas ao PAM são frequentemente revisadas e auditadas para garantir que as políticas de acesso estejam sendo seguidas e sejam eficazes. As revisões ajudam a identificar problemas de segurança e aprimorar as políticas de PAM conforme necessário.

3.Serviço de diretório

Os serviços de diretório, como o Lightweight Directory Access Protocol (LDAP) e os diretórios no formato X.500, são sistemas que permitem armazenar, organizar e recuperar informações de forma hierárquica. O LDAP é uma implementação mais leve e amplamente utilizada dos diretórios X.500.

3.1 LDAP
É um protocolo de aplicação que define como as informações são acessadas e gerenciadas em um diretório. Ele foi projetado para ser uma versão mais simples e eficiente do padrão X.500 e é amplamente utilizado em ambientes de rede para consultas e autenticação.

3.2 Diretórios X.500
Os diretórios no formato X.500 são sistemas de gerenciamento de diretórios que seguem o padrão X.500, que define como as informações são armazenadas, organizadas e acessadas. Os diretórios X.500 são geralmente utilizados em ambientes corporativos ou governamentais para armazenar informações como registros de funcionários, contatos, endereços de email, entre outros.

3.3 Hierarquia
Tanto o LDAP quanto os diretórios X.500 usam uma estrutura hierárquica para organizar as informações. A hierarquia é semelhante à estrutura de diretórios de um sistema de arquivos, com entradas de diretório pai e filho.

3.4 Nome distinto (DN)
O DN é uma identificação única e hierárquica atribuída a cada entrada no diretório. Ele fornece uma maneira de localizar e identificar exclusivamente uma entrada no diretório. Um DN geralmente consiste em uma série de componentes (atributos) que descrevem a posição da entrada na hierarquia do diretório.

3.5 Árvore de diretórios
A estrutura de diretórios é organizada em uma árvore, onde o nó raiz representa o diretório principal. Cada nó na árvore representa uma entrada no diretório e pode conter informações como nomes, endereços, telefones, etc. Os nós podem ser organizados em contêineres (organizações, grupos) e folhas (entidades individuais).

3.6 LDAP como interface
O LDAP atua como a interface de comunicação entre os clientes e o diretório. Os clientes LDAP enviam solicitações para o servidor LDAP para recuperar, adicionar, atualizar ou excluir informações no diretório.

3.7 Consultas LDAP
Os clientes LDAP podem realizar consultas de pesquisa no diretório para localizar informações específicas. As consultas são baseadas em filtros que especificam quais entradas no diretório devem ser retornadas com base em critérios específicos.

4.Autenticação
Além de consultas, o LDAP é comumente usado para autenticação, permitindo que os sistemas verifiquem as credenciais dos usuários em um diretório centralizado.

4.1 Elementos em sistemas de gerenciamento de diretórios

Atributos como Common Name (CN), Organizational Unit (OU), Organization (O), Country (C) e Domain Component (DC) são elementos fundamentais usados em sistemas de gerenciamento de diretórios, como o Lightweight Directory Access Protocol (LDAP) e os diretórios X.500, para identificar, classificar e organizar informações:

- **Common name (CN):** É um atributo que representa o nome comum de uma entidade, como um usuário ou um recurso, em um diretório. Em contextos de autenticação e certificados digitais, o CN é frequentemente usado para identificar um indivíduo ou uma entidade de forma única.
- **Organizational Unit (OU):** Em português "Unidade Organizacional", é um atributo que descreve uma subdivisão ou departamento dentro de uma organização. É usado para organizar e classificar entidades de maneira hierárquica. Por exemplo, em uma estrutura de diretório, você pode ter uma OU chamada "Vendas" para agrupar usuários e recursos relacionados a vendas.
- **Organization (O):** Em português "Organização", é um atributo que descreve a organização ou empresa à qual uma entidade pertence. Ele ajuda a categorizar entidades com base em sua afiliação organizacional. Por exemplo, pode ser usado para distinguir entre diferentes empresas em um diretório LDAP.
- **Country (C):** Em português "País", é um atributo que indica o país de origem ou localização de uma entidade. É frequentemente representado como um código de duas letras conforme a norma ISO 3166-1. O atributo C é útil em contextos globais para identificar a localização geográfica das entidades.
- **Domain Component (DC):** Em português "Componente de Domínio", é usado para representar domínios em um ambiente de diretório. Em sistemas LDAP, é comum usá-lo para representar partes de nomes de domínio (por exemplo, "dc=exemplo, dc=com"). Ele ajuda a criar uma estrutura de diretório que reflete a estrutura de domínio de uma organização.

5.Federação

Refere-se a um modelo em que várias organizações ou serviços concordam em compartilhar informações de autenticação e autorização para permitir o acesso a recursos em suas respectivas redes ou sistemas:

- **Identidade e atributos:** Cada organização participante em uma federação mantém suas próprias identidades de usuários e atributos associados a essas identidades. Isso inclui informações como nome, endereço de email, funções, etc.
- **Provedores de identidade (IdPs):** As organizações participantes, conhecidas como Provedores de Identidade (IdPs), são responsáveis por autenticar seus usuários e fornecer informações de atributos associados a esses usuários.
- **Provedores de serviço (SPs):** São as organizações ou sistemas que oferecem recursos ou serviços aos usuários autenticados. Os SPs dependem do IdP para autenticar os usuários.

- **Federação:** É um acordo formal entre os IdPs e SPs que estabelece como a autenticação e a autorização serão compartilhadas e confiadas entre as organizações participantes. Isso envolve a definição de padrões e protocolos comuns para comunicação segura.
- **SAML (Security Assertion Markup Language):** É um protocolo amplamente utilizado para implementar a Federação. Ele permite que os IdPs forneçam afirmações de autenticação e atributos aos SPs em um formato seguro. Essas afirmações SAML podem incluir informações como quem é o usuário autenticado e quais são suas atribuições.
- **Processo de autenticação e autorização:** Quando um usuário tenta acessar um serviço ou recurso em um SP, o SP redireciona o usuário para o IdP apropriado para autenticação. O IdP autentica o usuário e, em seguida, gera uma afirmação SAML que contém informações sobre o usuário. O IdP envia essa afirmação SAML de volta para o SP. O SP verifica a afirmação SAML e concede ou nega o acesso ao recurso com base nas informações fornecidas.
- **Benefícios da federação:** A Federação permite que organizações compartilhem recursos e serviços sem a necessidade de criar contas separadas para os usuários em cada sistema. Ela simplifica o gerenciamento de identidades e o acesso a recursos em um ambiente distribuído. Também aumenta a segurança, pois a autenticação é gerenciada pelas organizações que conhecem melhor seus usuários.
- **Controle de acesso granular:** A Federação pode ser configurada para fornecer controle de acesso granular, permitindo que organizações definam quais atributos específicos são compartilhados com SPs e quais recursos estão disponíveis para cada usuário.

6.SAML

É um padrão de segurança baseado em XML projetado para trocar informações de autenticação e autorização entre diferentes domínios de segurança. Ele permite que uma entidade IdP emita afirmações sobre a identidade e atributos de um usuário autenticado, que são consumidas por outra entidade.

Componentes:

- **Afirmação (assertion):** São declarações sobre a identidade do usuário, como seu nome, papel ou nível de acesso.
- **Provedor de identidade (IdP):** É responsável por autenticar o usuário e emitir afirmações SAML.
- **Provedor de serviço (SP):** É a aplicação ou serviço que confia nas afirmações SAML do IdP para conceder acesso ao usuário.
- **Pacotes SAML (SAML artifacts):** São os documentos XML que contêm afirmações e informações relacionadas.
- **Protocolos SAML:** Define como as solicitações e respostas SAML são transmitidas, como o SAML Single Sign-On (SSO) e o SAML Single Logout (SLO).

6.1 Fluxo de autenticação SAML

- Um usuário acessa uma aplicação ou serviço (SP).
- O SP redireciona o usuário para o IdP apropriado.
- O IdP autentica o usuário e emite uma afirmação SAML, geralmente em forma de token XML, que é assinado digitalmente para garantir sua integridade.
- O usuário é redirecionado de volta para o SP com a afirmação SAML.
- O SP verifica a assinatura digital do token SAML e concede acesso ao usuário com base nas informações contidas na afirmação.

7.SOAP

É um protocolo de comunicação baseado em XML usado para trocar mensagens entre aplicativos em uma rede. Ele fornece uma maneira padrão de estruturar, enviar e receber informações entre sistemas heterogêneos, independentemente da plataforma ou linguagem de programação.

Componentes:

- **Envelope SOAP:** É o elemento raiz de uma mensagem SOAP que define a estrutura geral da mensagem.
- **Header SOAP:** Contém informações de metadados opcionais sobre a mensagem, como autenticação, segurança ou transações.
- **Body SOAP:** Contém os dados da mensagem, que podem ser comandos, respostas ou informações de serviço.
- **Protocolo de transporte:** O SOAP pode ser usado em vários protocolos de transporte, como HTTP, SMTP, FTP, etc., para transmitir mensagens pela rede.

7.1 Funcionamento do SOAP

- Um aplicativo cliente cria uma mensagem SOAP que encapsula uma solicitação ou dados a serem enviados para um serviço.
- A mensagem SOAP é enviada através de um protocolo de transporte para o serviço.
- O serviço recebe a mensagem SOAP, extrai os dados relevantes do corpo (Body) da mensagem e processa a solicitação.
- O serviço pode criar uma resposta em formato SOAP e enviá-la de volta ao cliente.
- O cliente recebe a resposta SOAP, extrai os dados do corpo da mensagem e processa a resposta conforme necessário.

8.RESTful OAuth

O RESTful OAuth (também conhecido como OAuth) é um protocolo de autorização amplamente utilizado para permitir que aplicativos de terceiros acessem recursos protegidos em nome de um usuário, sem a necessidade de compartilhar suas credenciais de autenticação. O OAuth segue um conjunto de padrões e fluxos que permitem a autorização segura para aplicativos, sites e serviços.

Componentes:

- **Cliente:** O aplicativo ou serviço que deseja acessar recursos protegidos em nome de um usuário.
- **Proprietário dos recursos:** O usuário que possui os recursos protegidos (por exemplo, uma conta de usuário em uma rede social).
- **Servidor de autorização:** O servidor que emite tokens de acesso após a autenticação bem-sucedida do usuário e sua autorização.
- **Servidor de recursos:** O servidor que hospeda os recursos protegidos que o cliente deseja acessar.

8.1 Registro do cliente
O cliente precisa ser registrado no servidor de autorização. O registro inclui informações como o nome do cliente, o tipo de aplicativo, os URLs de redirecionamento e a chave secreta compartilhada (client secret) para autenticação.

8.2 Fluxo OAuth
Existem vários fluxos OAuth, incluindo o Fluxo de Autorização de Código (Authorization Code Flow), o Fluxo Implícito (Implicit Flow), o Fluxo de Credenciais de Cliente (Client Credentials Flow) e outros. Cada fluxo é adequado para diferentes cenários de uso.

8.3 Fluxo de autorização de código
Neste fluxo, o cliente redireciona o usuário para o servidor de autorização, onde o usuário faz login e concede permissão ao cliente. O servidor de autorização retorna um código de autorização para o cliente. O cliente usa o código de autorização para solicitar um token de acesso do servidor de autorização.

8.4 Token de acesso
O token de acesso é um artefato essencial no OAuth. Ele é usado pelo cliente para acessar os recursos protegidos no servidor de recursos em nome do usuário. O token de acesso é de curta duração e pode ser revogado a qualquer momento.

8.5 Intercâmbio do código por um token de acesso
O cliente envia o código de autorização e sua chave secreta para o servidor de autorização. O servidor de autorização valida o código e, se correto, emite um token de acesso para o cliente.

8.6 Acesso a recursos protegidos
O cliente usa o token de acesso para acessar os recursos protegidos no servidor de recursos. O servidor de recursos verifica a validade do token de acesso e concede ou nega o acesso.

8.7 Escopo
O escopo é um parâmetro que permite que o cliente especifique quais recursos ele deseja acessar e com quais permissões. O usuário autoriza o escopo durante o processo de autorização.

8.8 Renovação de token
Os tokens de acesso podem expirar após um curto período. O cliente pode solicitar um novo token de acesso usando um token de atualização (refresh token) obtido durante a autorização inicial, sem a necessidade de autenticar novamente o usuário.

9.OpenID Connect (OIDC)
É um protocolo de autenticação e autorização construído em cima do OAuth 2.0, projetado para permitir que aplicativos e serviços autentiquem usuários e obtenham informações sobre eles. O OIDC é amplamente utilizado em cenários de autenticação e autorização seguras, especialmente em aplicativos da web e móveis.

Atores envolvidos:

- **Provedor de Identidade (IdP):** Este é o servidor que lida com a autenticação e a emissão de tokens de identificação.
- **Cliente:** O aplicativo ou serviço que deseja autenticar os usuários e obter informações sobre eles.
- **Usuário Final:** O usuário que está tentando acessar o aplicativo ou serviço.

9.1 Registro do cliente
O cliente (aplicativo ou serviço) precisa se registrar com o provedor de identidade (IdP). O registro inclui informações sobre o cliente, como nome, redirecionamentos de URL e chaves de segurança compartilhadas (client secret).

9.2 Autenticação do usuário
Quando o usuário tenta acessar o aplicativo, o cliente redireciona o usuário para o servidor de autenticação do provedor de identidade. O servidor de autenticação autentica o usuário por meio de um processo de login, que pode envolver senhas, autenticação multifator (MFA) ou outros métodos.

9.3 Emissão do token de identificação
Após a autenticação bem-sucedida, o servidor de autenticação emite um token de identificação (ID token). O ID token é um token JWT (JSON Web Token) que contém informações sobre o usuário, como nome, endereço de email e outras afirmações.

9.4 Redirecionamento de volta ao cliente
O servidor de autenticação redireciona o usuário de volta para o cliente junto com o ID token. O ID token é passado por meio de uma solicitação segura para o cliente.

9.5 Verificação do token de identificação
O cliente verifica a assinatura digital do ID token para garantir sua autenticidade e integridade. Ele também verifica o emissor do token (issuer) para confirmar que o token foi emitido pelo IdP correto.

9.6 Autorização adicional
Além do ID token, o cliente pode solicitar um token de acesso para acessar recursos protegidos em nome do usuário. A solicitação pode incluir escopos que definem as permissões específicas que o cliente deseja obter.

9.7 Solicitação de token de acesso
O cliente faz uma solicitação ao IdP para obter um token de acesso, apresentando o ID token como prova da autenticação do usuário. O IdP valida a solicitação e, se aprovada, emite um token de acesso ao cliente.

9.8 Acesso a recursos protegidos
O cliente pode usar o token de acesso para acessar recursos protegidos no servidor de recursos, como dados do usuário ou outras informações. O servidor de recursos verifica a validade do token de acesso antes de conceder ou negar o acesso.

9.9 Renovação e expiração de tokens
Os tokens de identificação e acesso têm prazos de validade limitados. O cliente pode solicitar a renovação desses tokens quando expiram, ou o usuário pode ser redirecionado para autenticação novamente.

9.10 Segurança
O OIDC implementa medidas de segurança, como a verificação de tokens e o uso de HTTPS, para garantir a confidencialidade e a integridade das informações durante a autenticação e a autorização.

9.11 Compartilhamento de informações do usuário
O OIDC permite que o cliente obtenha informações do usuário, como nome, endereço de email e outros atributos, para personalizar a experiência do usuário ou cumprir requisitos de negócios.

9.12 Controles de gerenciamento de identidade
Em uma rede privada, a identidade digital de um usuário é representada por uma conta. O administrador de rede é responsável por garantir a integridade do servidor que hospeda as contas, enquanto cada usuário tem a responsabilidade de proteger as credenciais associadas à sua conta, de modo que apenas eles possam autenticar-se e utilizá-la.

Nos casos em que a rede é pública ou como uma camada adicional de proteção em redes privadas, a conta pode ser identificada também por algum material criptográfico. Essa identificação criptográfica adiciona uma camada adicional de segurança ao processo de autenticação e autorização, tornando mais difícil para invasores obterem acesso não autorizado a uma conta.

10.Certificados e smart card

A infraestrutura de chave pública (PKI) permite o gerenciamento de identidades digitais, em que uma autoridade de certificação (CA) emite certificados para sujeitos validados, como usuários e servidores. Esses certificados contêm a chave pública do sujeito e são assinados pela chave pública da AC. As chaves públicas permitem que terceiros verifiquem o certificado e a assinatura, garantindo a confiança na identidade do sujeito.

O par de chaves consiste na chave pública, que é incluída no certificado e pode ser divulgada amplamente, e na chave privada, que está vinculada à chave pública e deve ser mantida em segredo pelo proprietário. A chave privada pode ser armazenada no computador, seja no sistema de arquivos ou em um chip de plataforma confiável (TPM). Além disso, a chave privada e o certificado de um usuário podem ser armazenados em um cartão inteligente ou em uma chave USB, permitindo que o usuário se autentique em diferentes computadores e dispositivos móveis.

Essa abordagem com certificados e cartões inteligentes oferece uma camada adicional de segurança, uma vez que a chave privada é protegida fisicamente e pode ser transportada facilmente pelo usuário. Dessa forma, é possível autenticar-se de maneira segura e confiável em diferentes ambientes, sem a necessidade de expor a chave privada diretamente ao sistema em que se está autenticando.

11.Tokens

Em um sistema em que os usuários precisam autenticar-se em várias aplicações, seria inconveniente ter que fazer o processo de autenticação repetidamente. Para resolver esse problema, é comum utilizar um sistema de autenticação única, no qual o usuário autentica-se em um provedor de identidade (IdP) e recebe um token criptográfico.

Esse token funciona como uma prova de autenticação do usuário e pode ser apresentado às aplicações compatíveis, permitindo que o usuário obtenha autorizações e acesso às funcionalidades dessas aplicações sem a necessidade de autenticar-se novamente. No entanto, é importante estar ciente de que o uso de tokens também apresenta um risco de segurança: um ator malicioso pode capturar e reproduzir o token, obtendo acesso não autorizado às aplicações.

12.Provedores de identidade

Os provedores de identidade são os serviços responsáveis pelo fornecimento de contas de usuário e pelo processamento de solicitações de autenticação. Em uma rede privada, esses diretórios de identidade e serviços de autorização de aplicativos podem ser operados localmente, em um mesmo local. No entanto, atualmente, a maioria das redes utiliza serviços em nuvem de terceiros.

Essa abordagem de gestão federada de identidade simplifica o processo de autenticação e autorização, ao mesmo tempo em que aumenta a conveniência para o usuário. Além disso, proporciona maior segurança, pois os provedores de identidade são especializados em

gerenciar e proteger as informações de identidade dos usuários, aplicando medidas de segurança robustas.

13.Verificação de antecedentes e políticas de integração

A gestão de identidade e acesso (IAM) envolve tanto procedimentos e tecnologias de TI/segurança quanto políticas de Recursos Humanos (RH). As políticas de gerenciamento de pessoal são aplicadas em três fases:

- **Recrutamento:** Consiste em localizar e selecionar pessoas para ocupar cargos específicos. As questões de segurança nessa fase incluem a triagem de candidatos e a realização de verificações de antecedentes.
- **Operação:** Geralmente, é o departamento de RH que gerencia a comunicação de políticas e treinamentos para os funcionários (embora em organizações maiores possa haver um departamento separado para treinamento e desenvolvimento pessoal). Portanto, é crucial que os gestores de RH desenvolvam programas de treinamento que transmitam aos funcionários a importância da segurança.
- **Término ou separação:** Quando um funcionário deixa a empresa voluntariamente ou involuntariamente, o processo de término é delicado e apresenta várias implicações de segurança.

14.Verificação de antecedentes

A verificação de antecedentes consiste em avaliar se uma pessoa é realmente quem ela diz ser e se ela não está ocultando atividades criminais, falência ou conexões que a tornem inadequada ou arriscada. Funcionários que trabalham em ambientes de alta confidencialidade ou com acesso a transações de alto valor obviamente precisarão passar por um grau maior de escrutínio.

Para algumas ocupações, especialmente cargos federais que exigem uma autorização de segurança, as verificações de antecedentes são obrigatórias. Algumas verificações de antecedentes são realizadas internamente, enquanto outras são realizadas por terceiros externos.

15.Processo de integração (onboarding)

No contexto de Recursos Humanos, o processo de integração, conhecido como onboarding, consiste em receber um novo funcionário na organização. O mesmo princípio se aplica à contratação de novos fornecedores ou contratados. Alguns dos mesmos controles e processos são utilizados na criação de contas de clientes e convidados. Como parte do onboarding, as áreas de TI e RH se unem para criar uma conta de acesso ao sistema de computador para o usuário, atribuir as devidas permissões e garantir que as credenciais da conta sejam conhecidas apenas pelo usuário legítimo.

Essas funções devem estar integradas para evitar a criação de vulnerabilidades de configuração acidentais, como a criação de uma conta de usuário por parte de TI para um

funcionário que na realidade nunca foi contratado. Alguns dos outros aspectos e processos envolvidos no onboarding incluem:

- **Transmissão segura de credenciais:** Criar e enviar uma senha inicial ou emitir um cartão inteligente de forma segura. Esse processo precisa ser protegido contra possíveis ações maliciosas por parte do pessoal administrativo. Contas recém-criadas com senhas simples ou padrões representam uma porta de entrada facilmente explorável.
- **Alocação de ativos:** Fornecer computadores ou dispositivos móveis para o usuário ou permitir o uso de dispositivos pessoais (BYOD).
- **Treinamento/políticas:** Agendar treinamentos adequados de conscientização de segurança e certificações relevantes para o cargo ocupado.

16.Acordo de confidencialidade

Um Acordo de Confidencialidade, também conhecido como NDA (Non-Disclosure Agreement), estabelece os termos e condições em relação à confidencialidade das informações. Esses termos podem estar incorporados ao contrato de trabalho do funcionário ou serem um documento separado. Quando um funcionário ou contratado assina um NDA, ele está declarando que não compartilhará informações confidenciais com terceiros.

O NDA é uma medida de proteção importante para garantir que informações sensíveis e estratégicas da empresa sejam mantidas em sigilo. Por meio desse acordo, os funcionários se comprometem legalmente a não divulgar informações confidenciais a pessoas ou entidades não autorizadas.

Essa medida visa proteger os interesses comerciais da empresa, garantindo que segredos comerciais, dados confidenciais, estratégias de negócio e outras informações sensíveis não sejam divulgados indevidamente, preservando a vantagem competitiva e a privacidade da organização.

17.Políticas de pessoal para gerenciamento de privilégios

Os departamentos de Recursos Humanos (RH) e Tecnologia da Informação (TI) devem colaborar para garantir um gerenciamento eficaz de privilégios. As políticas de pessoal para gerenciamento de privilégios têm como objetivo minimizar o risco de ameaças internas.

Essas políticas são estabelecidas para definir como os privilégios de acesso a sistemas, dados e recursos são atribuídos aos funcionários, levando em consideração fatores como suas responsabilidades, cargos e necessidades específicas para realizar suas atividades de trabalho. Isso é feito de forma a garantir que cada funcionário tenha apenas os privilégios necessários para desempenhar suas funções, evitando a atribuição excessiva de permissões que possam resultar em riscos de segurança.

Além disso, essas políticas buscam estabelecer diretrizes claras para a revogação ou alteração de privilégios quando necessário, como em casos de mudança de função, transferência ou

término de contrato. Dessa forma, o gerenciamento de privilégios visa reduzir a possibilidade de uso inadequado ou abuso de acesso aos recursos da empresa por parte dos funcionários.

18.Separação de funções

A separação de funções é um meio de estabelecer controles e equilíbrios contra a possibilidade de que sistemas ou procedimentos críticos possam ser comprometidos por ameaças internas. As funções e responsabilidades devem ser divididas entre os indivíduos para evitar conflitos éticos ou abuso de poder.

A separação de funções significa que os funcionários devem estar sujeitos a políticas de segurança:

- **Procedimentos operacionais padrão:** Garantem que um funcionário não tenha desculpas para não seguir o protocolo ao realizar esses tipos de operações críticas.
- **Autoridade compartilhada:** Autoridade compartilhada significa que nenhum usuário tem permissão para executar ou realizar alterações por conta própria. Pelo menos duas pessoas devem autorizar a mudança. Um exemplo disso é separar a responsabilidade de compra (realizar o pedido) da autorização de pagamento. Outro exemplo é que uma solicitação para criar uma conta deve ser sujeita a aprovação e supervisão.

Essa abordagem garante que nenhum indivíduo tenha controle absoluto sobre uma função crítica, diminuindo os riscos de abuso, erros ou fraudes. Ao dividir as tarefas entre diferentes pessoas e estabelecer controles e autorizações adequadas, a organização cria um ambiente mais seguro, onde várias camadas de proteção são aplicadas para evitar possíveis incidentes de segurança.

Isso fortalece a governança e a integridade dos processos internos, mitigando a possibilidade de danos causados por ameaças internas.

19.Menor privilégio

O princípio do "menor privilégio" significa que um usuário recebe apenas os direitos necessários para desempenhar sua função, sem privilégios extras. Isso visa mitigar riscos caso a conta seja comprometida e caia sob o controle de um ator malicioso. A "expansão de autorização" ocorre quando um usuário adquire cada vez mais direitos, seja diretamente ou por ser adicionado a grupos de segurança e funções.

O princípio do menor privilégio deve ser garantido por meio de uma análise cuidadosa dos fluxos de trabalho da empresa para avaliar quais privilégios são necessários e por meio de auditorias regulares de contas.

Ao aplicar o princípio do menor privilégio, é essencial restringir o acesso aos recursos e informações somente àqueles que são essenciais para o desempenho das atividades do usuário. Dessa forma, se ocorrer uma violação de segurança ou um ataque cibernético, o

impacto será limitado, pois o usuário terá acesso apenas a recursos específicos, reduzindo as possibilidades de danos e movimentação lateral dentro do sistema.

Além disso, é importante realizar análises regulares das contas de usuário para identificar qualquer expansão indevida de privilégios. Isso envolve revisar as permissões atribuídas a cada usuário, verificar se elas ainda são necessárias e remover qualquer acesso desnecessário.

Essas auditorias periódicas garantem que os privilégios estejam alinhados com as necessidades reais dos usuários e ajudam a evitar a acumulação excessiva de direitos, que pode criar brechas de segurança e aumentar o risco de abusos ou violações.

20.Rotação de cargos

A rotação de cargos (ou rotação de tarefas) significa que nenhuma pessoa é permitida a permanecer no mesmo cargo por um longo período. Por exemplo, os gerentes podem ser movidos para diferentes departamentos periodicamente, ou os funcionários podem desempenhar mais de uma função, alternando entre elas ao longo do ano.

Rotacionar indivíduos em diferentes cargos, como administrador de firewall ou especialista em controle de acesso, ajuda uma organização a garantir que não esteja excessivamente dependente de uma única pessoa, pois o conhecimento institucional vital é compartilhado entre funcionários confiáveis. A rotação de cargos também ajuda a prevenir abuso de poder, reduz o tédio e aprimora as habilidades profissionais dos indivíduos.

A rotação de cargos traz uma série de benefícios para a organização. Ao mudar os funcionários de posição ou permitir que desempenhem diferentes funções, é possível evitar que uma única pessoa acumule poder excessivo ou se torne indispensável em uma determinada área. Isso reduz o risco de dependência excessiva de um indivíduo e ajuda a mitigar os impactos negativos que poderiam ocorrer se essa pessoa deixasse a organização repentinamente.

Além disso, a rotação de cargos também traz vantagens individuais. Ao ter a oportunidade de desempenhar diferentes funções, os funcionários têm a chance de expandir suas habilidades, adquirir novos conhecimentos e experiências em áreas diferentes. Isso pode contribuir para o desenvolvimento profissional e aumentar a motivação e o engajamento dos colaboradores.

21.Licença obrigatória

A licença obrigatória significa que os funcionários são obrigados a tirar suas férias, durante as quais outra pessoa assume suas responsabilidades. A política típica de licença obrigatória requer que os funcionários tirem pelo menos uma semana de férias por ano (no Brasil é um mês), de forma a ficarem afastados do trabalho por pelo menos cinco dias consecutivos.

Durante esse período, os funcionários responsáveis pela auditoria corporativa e segurança têm tempo para investigar e descobrir quaisquer discrepâncias na atividade dos funcionários.

A licença obrigatória é uma medida importante para garantir a integridade e segurança dos processos organizacionais. Ao forçar os funcionários a tirarem férias regulares, a empresa cria uma oportunidade para detectar possíveis fraudes, erros ou comportamentos inadequados que possam passar despercebidos durante o dia a dia do trabalho.

Durante a ausência do funcionário, outras pessoas podem assumir suas responsabilidades, o que permite uma revisão independente das atividades e uma identificação mais fácil de possíveis problemas.

Além disso, a licença obrigatória também traz benefícios para os próprios funcionários. Tirar férias regulares é essencial para o bem-estar e saúde mental dos colaboradores, pois proporciona descanso, relaxamento e a oportunidade de desconectar-se do trabalho. Isso contribui para reduzir o estresse e a exaustão, aumentando a produtividade e a satisfação no trabalho quando os funcionários retornam das férias.

22.Políticas de offboarding

O Offboarding (ou entrevista de saída) é o processo de garantir que um funcionário deixe a empresa de forma adequada e organizada. Esse procedimento também é aplicado quando um projeto que envolve contratados ou terceiros é encerrado.

Em termos de segurança, várias etapas devem ser cumpridas durante o offboarding:

- **Gerenciamento de contas:** Desativar a conta do usuário e suas permissões. Garantir que quaisquer ativos de informação criados ou gerenciados pelo funcionário, mas de propriedade da empresa, sejam acessíveis (por meio de chaves de criptografia ou arquivos protegidos por senha).
- **Ativos da empresa:** Recuperar dispositivos móveis, chaves, cartões inteligentes, mídias USB, entre outros. O funcionário deverá confirmar (e, em alguns casos, comprovar) que não retém cópias de quaisquer ativos de informação.
- **Ativos pessoais:** Limpar dispositivos de propriedade do funcionário de dados e aplicativos corporativos. Em alguns casos, o funcionário poderá manter alguns ativos de informação (como e-mails pessoais ou informações de contato), dependendo das políticas em vigor.

A saída de certos tipos de funcionários deve acionar processos adicionais para reforçar a segurança dos sistemas de rede. Isso inclui funcionários com conhecimento detalhado dos sistemas e procedimentos de segurança, além de acesso a credenciais de contas compartilhadas ou genéricas.

23.Segurança em tipos de contas

Nos sistemas operacionais, dispositivos de rede e produtos de diretório de rede, são utilizados diferentes tipos de contas como base de um sistema de gerenciamento de privilégios. Alguns

desses tipos de contas incluem usuário padrão, usuário administrativo, contas de grupos de segurança e contas de serviço.

24.Gestão de credenciais

A gestão de credenciais é o processo de administrar e controlar as identidades digitais e as formas de autenticação utilizadas por usuários em sistemas e redes. Ela envolve a criação, distribuição, armazenamento e revogação de credenciais, que podem incluir senhas, cartões inteligentes, certificados digitais, tokens ou identificação biométrica.

A gestão de credenciais é essencial para garantir a segurança e o acesso adequado aos recursos de uma organização. Isso envolve a implementação de políticas e práticas que garantam que apenas usuários autorizados tenham acesso aos sistemas, aplicativos e dados relevantes.

Além disso, a gestão de credenciais visa proteger as informações confidenciais contra acessos não autorizados e prevenir ataques cibernéticos.

As atividades de gestão de credenciais incluem a criação de contas de usuário, atribuição de privilégios adequados, atualização regular de senhas, monitoramento de atividades suspeitas, revogação de credenciais quando necessário e implementação de medidas de segurança para proteger as credenciais armazenadas.

Uma boa gestão de credenciais é fundamental para manter a integridade e a segurança dos sistemas de uma organização, reduzindo os riscos de violações de dados e comprometimento da infraestrutura de TI.

25.Contas de convidados

Contas de convidados são contas de usuário criadas em sistemas ou redes para permitir que usuários temporários ou externos acessem recursos específicos sem terem uma conta permanente. Essas contas são projetadas para fornecer acesso limitado e controlado a pessoas que não fazem parte da organização ou que não possuem uma conta regular no sistema.

As contas de convidados são úteis em várias situações, como quando uma pessoa precisa acessar um aplicativo ou serviço por um curto período de tempo, quando visitantes ou fornecedores precisam utilizar recursos específicos da organização ou quando um usuário externo deseja testar ou experimentar um sistema.

Geralmente, as contas de convidados possuem restrições de privilégios e permissões, permitindo apenas o acesso a recursos necessários para a tarefa ou serviço em questão. Elas são configuradas de forma a proteger a segurança do sistema, limitando o acesso a informações sensíveis e restringindo a capacidade de fazer alterações ou executar ações que possam comprometer a integridade ou a confidencialidade dos dados.

As contas de convidados podem ter um período de validade definido, após o qual são desativadas automaticamente, evitando assim que permaneçam ativas por um longo período de tempo sem necessidade. Além disso, é importante monitorar e auditar as atividades das contas de convidados para garantir que não sejam usadas indevidamente ou para fins maliciosos.

26.Contas de administrador ou Root

Contas de administrador ou root são contas de usuário que possuem os mais altos privilégios em um sistema de computador ou rede. Essas contas têm controle total sobre o sistema, permitindo que realizem tarefas como instalação e remoção de software, modificação de configurações do sistema, gerenciamento de permissões de arquivos e diretórios, e outras atividades que exigem acesso privilegiado.

A conta de administrador é geralmente criada durante a instalação do sistema operacional ou do software e possui poderes especiais que a diferenciam das contas de usuário comuns. Em sistemas baseados em Unix e Linux, a conta de administrador é conhecida como "root", enquanto em sistemas Windows é chamada de "conta de administrador".

As contas de administrador ou root são essenciais para a administração e manutenção de sistemas, pois permitem realizar alterações críticas e executar tarefas avançadas que são necessárias para o funcionamento adequado do sistema.

No entanto, devido aos seus amplos privilégios, essas contas também apresentam riscos significativos para a segurança, uma vez que podem ser exploradas por usuários mal-intencionados ou por malware.

26.1 Serviços de conta

Os serviços de conta de sistema, serviço local e serviço de rede são tipos de contas de usuário usadas no contexto de sistemas operacionais Windows para executar serviços e processos em um computador. Cada um desses serviços tem características específicas e é usado para diferentes finalidades.

26.2 Conta de sistema

A conta de sistema é uma conta interna do sistema operacional que possui os mais altos privilégios. É usada para executar serviços e processos do próprio sistema operacional. A conta de sistema tem acesso completo a recursos do sistema e geralmente é invisível para os usuários.

Ela é responsável por executar serviços críticos do sistema, como o Gerenciador de Controle de Serviços (Service Control Manager) e o subsistema do Windows. Essa conta é geralmente usada para garantir a estabilidade e segurança do sistema operacional.

26.3 Conta de serviço local

A conta de serviço local é uma conta de usuário pré-configurada que possui privilégios limitados. Ela é usada para executar serviços que não precisam acessar recursos de rede. A conta de serviço local tem permissões restritas em relação ao sistema e não possui acesso a recursos em outros computadores na rede. Essa conta é útil para executar serviços que operam somente localmente, como serviços de impressão ou serviços de auditoria de eventos.

26.4 Conta de serviço de rede

A conta de serviço de rede é outra conta de usuário pré-configurada, porém com privilégios um pouco mais elevados do que a conta de serviço local. Ela é usada para executar serviços que precisam acessar recursos de rede, como compartilhamentos de arquivos ou bancos de dados em outros computadores.

A conta de serviço de rede possui permissões para se comunicar com outros dispositivos na rede, mas não possui privilégios administrativos no computador local. Essa conta é comumente utilizada para executar serviços de servidores que requerem acesso a recursos compartilhados em uma rede.

27.Contas e credenciais compartilhadas

As contas e credenciais compartilhadas são aquelas que são utilizadas por múltiplos usuários para acessar um recurso compartilhado. Em vez de criar uma conta de usuário separada para cada indivíduo, uma única conta é criada e as credenciais (como nome de usuário e senha) são compartilhadas entre eles.

Essas contas são geralmente usadas para facilitar o acesso a recursos compartilhados, como pastas de rede, servidores FTP, bancos de dados ou sistemas de gerenciamento de conteúdo. No entanto, o uso de contas e credenciais compartilhadas pode apresentar desafios de segurança, pois torna difícil rastrear ações individuais e controlar o acesso.

28.Contas genéricas

As contas genéricas são aquelas criadas para fins específicos ou funções de trabalho em uma organização. Elas não estão vinculadas a usuários individuais, mas são usadas por vários indivíduos para executar tarefas comuns.

As contas genéricas facilitam a delegação de responsabilidades e a colaboração, mas é importante garantir que o acesso a essas contas seja restrito apenas aos usuários autorizados e que sejam aplicadas medidas de segurança adequadas.

29.Contas de equipamento

As contas de equipamento são usadas por dispositivos ou equipamentos específicos para acessar recursos ou executar determinadas tarefas em um ambiente de rede. Essas contas são associadas a um dispositivo em vez de um usuário individual.

Essas contas são necessárias para que os dispositivos possam autenticar-se e acessar os recursos necessários para executar suas funções. É importante proteger as credenciais de conta de equipamento para evitar o acesso não autorizado aos dispositivos e recursos associados.

30.Chaves do SSH

Secure Shell (SSH) Keys, ou Chaves do Protocolo Secure Shell, são um método de autenticação e criptografia utilizado para estabelecer conexões seguras em sistemas de rede. O SSH é um protocolo amplamente utilizado para acessar servidores remotos de forma segura, permitindo a execução de comandos, transferência de arquivos e gerenciamento remoto de sistemas.

As chaves do SSH consistem em pares de chaves criptográficas: uma chave privada e uma chave pública. A chave privada é mantida em segredo pelo usuário e serve para descriptografar as informações criptografadas.

A chave pública, por sua vez, é compartilhada com os servidores remotos que se deseja acessar. Quando um usuário tenta se conectar a um servidor remoto, o cliente SSH utiliza a chave privada correspondente à chave pública armazenada no servidor para autenticar e estabelecer uma conexão segura.

A principal vantagem das chaves do SSH em relação às senhas convencionais é a segurança aprimorada. As chaves são criptografadas e mais difíceis de serem comprometidas por ataques de força bruta. Além disso, as chaves do SSH eliminam a necessidade de inserir senhas manualmente, o que torna o processo de autenticação mais conveniente e menos suscetível a ataques de phishing.