Usuários e Grupos de Usuários

Administação de Sistemas Linux

Introdução

- O Linux é um sistema multiusuário, portanto, pode conter vários usuários registados no sistema.
- Um usuário é adicionado ao sistema sob forma de **conta de usuário**.
- Uma conta de usuário é uma coleção de dados e configurações que informam ao sistema quais arquivos e pastas este usuário pode aceder, quais alterações pode fazer no sistema e quais são suas preferências pessoais.
- As contas de usuário são entidades de segurança usadas para proteger e gerir o acesso aos recursos do sistema, permitindo que um usuário compartilhe um computador com outros usuários, enquanto mantém seus próprios arquivos e configurações.
- Um **grupo de usuário**, é um conjunto de contas de usuários. Com a utilização de grupos, a administração do acesso aos recursos da rede é simplificada, pois podemos atribuir as permissões a um grupo, ao invés de ter que configurarmos as permissões usuário por usuário.

Características das contas de usuário

Cada conta usuário poderá ter ...

Item	Descrição
Login	Nome do usuário para fins de *login (USERNAME)*
Password	Senha do usuário para aceder o sistema
UID	Número de Identificação do usuário
GID	Numero de Identificação do grupo
Comentários	Descrição do usuário (ex: nome completo)
Directório Inicial	Diretório inicial do usuário quando acede o sistema.

Cada grupo de usuário poderá ter ...

Item	Descrição
Nome	Nome do grupo
Password	Senha do grupo
GID	Número de Identificação do grupo
Lista de Usuários	Lista dos usuários que fazem parte do grupo

Tipos de contas de usuários

- No Linux, existem 4 tipos de contas usuários a saber: conta de superusuário, conta padrão, conta do sistema e contas de serviço .
  1. **A conta de superusuário**
     - No Linux, a conta do super-usuário é root, e tem UID = **0**(zero). O super-usuário também pode ser chamado de *administrador do sistema* e dispõe de acesso e controlo ilimitados sobre o sistema, incluindo sobre outros usuários.
     - O grupo padrão do superusuário tem o GID = **0**(zero) e também é chamado de root. O diretório inicial do superusuário é um diretório dedicado, de nível superior, /root, acessível apenas pelo próprio usuário root.

Tipos de contas de usuários

2. **Contas de usuário padrão**
   - Geralmente indicam uma conta de usuário “regular” (sem privilégios) e possuem com algumas excepções as seguintes propriedades:
     - UIDs iniciando em 1000 (4 dígitos), embora alguns sistemas legados possam iniciar em 500.
     - Um diretório inicial definido, geralmente um subdiretório de /home, dependendo da configuração local.
     - Um shell de login definido. No Linux, o shell padrão é geralmente o *Bourne Again Shell* (/bin/bash). Se uma conta de usuário não tiver um shell válido em seus atributos, o usuário não poderá abrir um shell interativo. Normalmente, /sbin/nologin é usado como um shell inválido.

Tipos de contas de usuários

3. **Contas do sistema**
   - As contas de sistema são tipicamente pré-criadas no momento da instalação do sistema. São destinadas a recursos, programas e serviços que não necessitam do super-usuários para executar.
   - As contas de sistema variam, mas dentre seus atributos temos:
     - Os UIDs normalmente são menores de 100 (2 dígitos) ou entre 500-1000 (3 dígitos).
     - Não têm nenhum diretório inicial dedicado ou têm um diretório que normalmente não está em /home.
     - Nenhum shell de login válido (tipicamente /sbin/nologin), com raras exceções. A maioria das contas de sistema no Linux nunca faz login e não precisa de um shell definido nos seus atributos.
     - Essas contas geralmente têm privilégios limitados ou, na maioria das dos casos, nenhum privilégio.

Tipos de contas de usuários

4. **Contas de serviço**
   - As contas de serviço são criadas tipicamente quando instalamos e configuramos serviços. Como no caso das contas de sistema, elas são destinadas aos recursos, programas e serviços que não serão executados como super-usuário.
   - As contas de sistema e de serviço são semelhantes e intercambiáveis. Embora não exista uma definição estrita, a principal diferença entre contas de sistema e de serviço está no UID/GID:
     - **Conta de sistema** - UID/GID <100 (2 dígitos) ou <500-1000 (3 dígitos);
     - **Conta de serviço** - UID/GID >1000 (4+ dígitos).

Arquivos de controlo de acesso

- As informações sobre usuários e grupos são armazenadas em quatro arquivos na árvore de diretórios /etc/:
  - **/etc/passwd** - um arquivo de sete campos delimitados por dois pontos e contém informações das contas dos usuários como: UID e GID, diretório inicial, shell etc. Apesar do nome, não armazena senha.
  - **/etc/group** - um arquivo de quatro campos delimitados por dois pontos e armazena informações básicas sobre todos os grupos de usuários no sistema, como nome do grupo, GID e membros
  - **/etc/shadow** - um arquivo de nove campos delimitados por dois pontos contendo senhas de usuário criptografadas e informações como data de expiração, quando a senha foi alterada pela ultima vez...
  - **/etc/gshadow -** um arquivo de quatro campos delimitados por dois pontos contendo senhas de grupo criptografadas e outras informações mais detalhadas sobre grupos como lista de usuários e de administradores do grupo

Arquivos de controlo de acesso

- Existem também arquivos relacionados com o aumento básico de privilégios em sistemas Linux, como nos comandos su e sudo. Por padrão, eles só estão acessíveis ao usuário root.
  - **/etc/sudoers** - Este arquivo controla quem e como se pode usar o comando sudo.
  - **/etc/sudoers.d** - Este diretório pode conter arquivos que complementam as configurações do arquivo sudoers.
- Embora /etc/sudoers seja um arquivo de texto, ele ão deve ser editado diretamente. Se for necessário fazer alterações em seu conteúdo, elas devem ser efetuadas através do utilitário visudo.

Arquivos de controlo de acesso

Arquivo /etc/passwd

- Contém uma lista de todas as contas dos usuários do sistema.
- Cada linha contém diversos campos, delimitados por dois pontos (:). Apesar do nome, o *hash one-way* das senhas não é armazenado neste arquivo atualmente.
- A sintaxe típica de uma linha nesse arquivo é:

NOME DE USUÁRIO:SENHA:UID:GID:GECOS:DIRECTORIO INICIAL:SHELL

- Onde:
  - NOME DE USUÁRIO - O nome usado quando o usuário se *loga* no sistema.
  - SENHA - A senha criptografada, quase sempre é ***x***, indicando que a senha está armazenada no arquivo /etc/shadow.
  - ID DE USUÁRIO (UID) - O número de identificação atribuído ao usuário no sistema.
  - ID DE GRUPO (GID) - O número do grupo principal do usuário no sistema.

Arquivos de controlo de acesso

Arquivo /etc/passwd

- ID DE GRUPO (GID) - O número do grupo principal do usuário no sistema.
- GECOS - Um campo de comentário opcional, usado para adicionar informações extras sobre o usuário (como o nome completo). O campo pode conter diversas entradas separadas por vírgula.
- DIRETÓRIO INICIAL - O caminho absoluto do diretório inicial do usuário.
- SHELL - O caminho absoluto do programa que é iniciado automaticamente quando o usuário efetua login no sistema (geralmente um shell interativo como /bin/bash).

- Exemplo:
  - Usuário root: **root:x:0:0:root:/root:/bin/bash**

Arquivos de controlo de acesso

Arquivo /etc/group

- O arquivo /etc/group contém uma lista de grupos do sistema.
- Os grupos são usados para aplicar permissões de acesso a recursos do sistema e também permitem a gestão e monitoramento de usuários.
- A sintaxe de cada linha é:

NOME DO GRUPO:SENHA DO GRUPO:GID: LISTA DE MEMBROS

- Onde:
  - NOME DO GRUPO - O nome do grupo.
  - SENHA DO GRUPO - A senha criptografada do grupo (ou um x se forem usadas senhas shadow).
  - ID DO GRUPO (GID) - O número de identificação atribuído ao grupo no sistema.
  - LISTA DE MEMBROS - Uma lista delimitada por vírgulas de usuários pertencentes ao grupo, exceto aqueles cujo grupo principal é este.

Arquivos de controlo de acesso

Arquivo /etc/shadow

- etc/shadow é um arquivo legível apenas pelo usuário root ou com privilégios de root e contém as senhas criptografadas dos usuários em linhas separadas:

  frank:6i9gjM4Md4MuelZCd$7jJa8Cd2bbADFH4dwtfvTvJLOYCCCBf/.jYbK1IMY x7Wh4fErXcc2xQVU2N1gb97yIYaiqH.jjJammzof2Jfr/:18029:0:99999:7:::

- Cada linha consiste em nove campos delimitados por dois pontos:
  - NOME - O nome usado quando o usuário efectua login no sistema.
  - SENHA CRIPTOGRAFADA - A senha do usuário criptografada (se o valor for **!** ou *, a conta está bloqueada). O comando **usermod -L** adiciona um símbolo **!** a este campo para bloquear a conta.
  - DATA DA ÚLTIMA ALTERAÇÃO DE SENHA - A data da última mudança de senha em número de dias desde 01/01/1970. Um valor de 0 indica que o usuário precisa trocar a senha em seu próximo acesso.

Arquivos de controlo de acesso

Arquivo /etc/shadow

- IDADE MÍNIMA DA SENHA - O número mínimo de dias que o usuário deve aguardar após uma alteração de senha para poder trocar a senha novamente.
- IDADE MÁXIMA DA SENHA - O número máximo de dias que devem passar antes que uma alteração de senha seja solicitada.
- PERÍODO DE AVISO DE SENHA - O número de dias para a expiração da senha, durante os quais o usuário é avisado de que a senha deve ser alterada.
- PERÍODO DE INATIVIDADE DA SENHA - O número de dias após a expiração de uma senha, durante os quais o usuário deve atualizá-la. Após esse período, se o usuário não alterar a senha, a conta é desativada.
- DATA DE EXPIRAÇÃO DA CONTA - A data, em número de dias desde 01/01/1970, na qual a conta do usuário será desativada. Um campo vazio indica que a conta do usuário nunca expirará.
- UM CAMPO RESERVADO - Um campo reservado para uso futuro.

Arquivos de controlo de acesso

Arquivo /etc/gshadow

- /etc/gshadow é um arquivo legível apenas pelo root e por usuários com privilégios de root que contém senhas criptografadas para grupos em linhas separadas:

  developer:$6$7QUIhUX1WdO6$H7kOYgsboLkDseFHpk04lwAtweSUQHipoxIgo83QNDxYtYwgmZTCU0qSCuCkErmyR263rvHiLctZVDR7Ya9Ai1::

- Cada linha consiste em quatro campos delimitados por dois pontos:
  - NOME DO GRUPO - O nome do grupo.
  - SENHA CRIPTOGRAFADA - A senha criptografada do grupo (é usada quando um usuário que não é membro do grupo deseja ingressar no grupo usando o comando newgrp — se a senha começar com **!**, ninguém tem permissão de acessar o grupo com newgrp).
  - ADMINISTRADORES DO GRUPO - Uma lista dos administradores do grupo delimitada por vírgulas (eles podem alterar a senha do grupo, bem como adicionar ou remover membros do grupo com o comando gpasswd)
  - MEMBROS DO GRUPO - Uma lista dos membros do grupo delimitada por vírgulas.

Usuários e grupos especiais

- Usuários e/ou grupos usados pelo sistema para executar tarefas específicas com privilégios restritos
  - **cupsys**: gestor de impressoras
  - **mail**: gerenciador de correio
  - **www-data**: servidor web
  - .....
- Grupos para controlo de privilégios
  - **cdrom**: controlo dos drives de cd ou dvd
  - **floppy** : controlo de drives de disquete
  - **áudio**: controlo de dispositivos de áudio
  - **admin**: concede permissões de administrador do sistema aos seus membros (via sudo)

Usuários e grupos especiais

- Os sistemas GNU/Linux são configurados para executar tarefas mínimas usando superusuário
  - Torne-se outro usuário
    - $ su [-] <nome_do_usuário>
- Execute um comando como super-usuário (somente usuários do grupo "sudo").
  - $ sudo ...
- Torne-se root permanentemente
  - $ sudo -s
  - $ sudo su