# 5.2 Lição 1

| | |
|---|---|
| **Certificação:** | Linux Essentials |
| **Versão:** | 1.6 |
| **Tópico:** | 5 Segurança e permissões de arquivos |
| **Objetivo:** | 5.2 Criação de usuários e grupos |
| **Lição:** | 1 de 1 |

## Introdução

Gerenciar usuários e grupos em uma máquina Linux é um dos principais aspectos da administração do sistema. De fato, o Linux é um sistema operacional multiusuário no qual vários usuários podem usar a mesma máquina ao mesmo tempo.

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 contendo informações básicas sobre os usuários

`/etc/group`
: um arquivo de quatro campos delimitados por dois pontos contendo informações básicas sobre os grupos

`/etc/shadow`
: um arquivo de nove campos delimitados por dois pontos contendo senhas de usuário criptografadas

`/etc/gshadow`
: um arquivo de quatro campos delimitados por dois pontos contendo senhas de grupo criptografadas

Todos esses arquivos são atualizados por um conjunto de ferramentas de linha de comando para gerenciamento de usuários e grupos, de que falaremos mais adiante nesta lição. Também existem aplicativos gráficos, específicos para cada distribuição Linux, com interfaces de gerenciamento mais simples e imediatas.

**Warning** Mesmo que os arquivos sejam em texto simples, não os edite diretamente. Sempre use as ferramentas fornecidas com sua distribuição.

### O Arquivo `/etc/passwd`

`/etc/passwd` é um arquivo legível por todos contendo uma lista de usuários em linhas separadas:

```
frank:x:1001:1001::/home/frank:/bin/bash
```

Cada linha consiste em sete campos delimitados por dois pontos:

Nome de usuário
: O nome usado quando o usuário se loga no sistema.

Senha
: A senha criptografada (ou um `x` no caso de senhas 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.

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`).

## O arquivo `/etc/group`

`/etc/group` é um arquivo legível por todos contendo uma lista de grupos em linhas separadas:

```
developer:x:1002:
```

Cada linha consiste em quatro campos delimitados por dois pontos:

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.

## O 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:$6$i9gjM4Md4MuelZCd$7jJa8Cd2bbADFH4dwtfvTvJLOYCCCBf/.jYbK1IMYx7Wh4fErXcc2xQVU2N1gb97yIYaiqH.jjJamm
zof2Jfr/:18029:0:99999:7:::
```

Cada linha consiste em nove campos delimitados por dois pontos:

Nome de usuário
: O nome usado quando o usuário se loga no sistema.

Senha criptografada
: A senha do usuário criptografada (se o valor for `!`, a conta está bloqueada).

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.

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.

## O 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.

Agora que vimos onde as informações de usuários e grupos são armazenadas, vamos falar sobre as ferramentas de linha de comando mais importantes para atualizar esses arquivos.

## Adicionando e removendo contas de usuário

No Linux, adicionamos uma nova conta de usuário com o comando `useradd` e excluímos uma conta de usuário com o comando `userdel`.

Se quiséssemos criar uma nova conta de usuário chamada `frank` com uma configuração padrão, executaríamos o seguinte:

```
# useradd frank
```

Após criar o novo usuário, definimos uma senha usando `passwd`:

```
# passwd frank
Changing password for user frank.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Ambos os comandos requerem autoridade de root. Quando executamos o comando `useradd`, as informações de usuário e grupo armazenadas nos bancos de dados de senha e de grupo são atualizadas para a conta de usuário recém-criada e, caso especificado, o diretório inicial do novo usuário é criado, bem como um grupo com o mesmo nome da conta de usuário.

Tip

Lembre-se de que sempre podemos usar o utilitário `grep` para filtrar os bancos de dados de senhas e grupos, exibindo apenas a entrada referente a um usuário ou grupo específico. Para o exemplo acima, usaríamos

```
cat /etc/passwd | grep frank
```

ou

```
grep frank /etc/passwd
```

para ver informações básicas sobre a conta `frank` recém-criada.

As opções mais importantes que se aplicam ao comando `useradd` são:

`-c`
Cria uma nova conta de usuário com comentários personalizados (por exemplo, nome completo)

`-d`
Cria uma nova conta de usuário com um diretório inicial personalizado.

`-e`
Cria uma nova conta de usuário com uma data específica na qual ela será desativada.

`-f`
Cria uma nova conta de usuário definindo o número de dias que o usuário tem para atualizar a senha após a expiração.

`-g`
Cria uma nova conta de usuário com um GID específico.

`-G`
Cria uma nova conta de usuário adicionando-a a diversos grupos secundários.

`-m`
Cria uma nova conta de usuário com seu diretório inicial.

`-M`
Cria uma nova conta de usuário sem seu diretório inicial.

`-s`
Cria uma nova conta de usuário com um shell de login específico.

`-u`
Cria uma nova conta de usuário com um UID específico.

Depois que a nova conta de usuário é criada, usamos os comandos `id` e `groups` para descobrir seu UID, GID e os grupos aos quais pertence.

```
# id frank
uid=1000(frank) gid=1000(frank) groups=1000(frank)
# groups frank
frank : frank
```

Tip

Lembre-se de verificar e, possivelmente, editar o arquivo `/etc/login.defs`, que define os parâmetros de configuração que controlam a criação de usuários e grupos. Por exemplo, você pode definir o intervalo de UIDs e GIDs que podem ser atribuídos a novas contas de usuário e grupo, especificar que não é necessário usar a opção `-m` para criar o diretório inicial do novo usuário e se o sistema deve criar automaticamente um novo grupo para cada novo usuário.

Se quiser excluir uma conta de usuário, pode usar o comando `userdel`. Esse comando atualiza, em particular, as informações armazenadas nos bancos de dados da conta, excluindo todas as entradas referentes ao usuário especificado. A opção `-r` também remove o diretório inicial do usuário e todo o seu conteúdo, juntamente com o spool de correio do usuário. Os arquivos que estiverem em outros locais deverão ser pesquisados e excluídos manualmente.

```
# userdel -r frank
```

Também neste caso, é preciso ter autoridade root para excluir contas de usuário.

## O diretório de esqueleto

Quando adicionamos uma nova conta de usuário e criamos seu diretório pessoal, este é preenchido com arquivos e pastas copiados do diretório de esqueleto (por padrão, `/etc/skel`). A idéia é simples: um administrador de sistema quer que os novos usuários tenham os mesmos arquivos e diretórios em seu diretório inicial. Portanto, se você deseja personalizar os arquivos e pastas que são criados automaticamente no diretório inicial das novas contas de usuário, adicione esses novos arquivos e pastas ao diretório de esqueleto.

**Tip** Note que os arquivos de perfil geralmente encontrados no diretório de esqueleto são arquivos ocultos. Portanto, se você deseja listar todos os arquivos e pastas do diretório de esqueleto que serão copiados para o diretório inicial dos usuários recém-criados, deve usar o comando `ls -Al`.

## Adicionando e excluindo grupos

Quanto ao gerenciamento dos grupos, os comandos `groupadd` e `groupdel` servem para adicionar e excluir grupos.

Para criar um novo grupo chamado `developer`, executaríamos o seguinte comando como root:

```
# groupadd -g 1090 developer
```

A opção `-g` deste comando cria um grupo com um GID específico.

Se quiser remover o grupo `developer`, você pode executar este comando:

```
# groupdel developer
```

**Warning** Lembre-se de que quando adicionamos uma nova conta de usuário, o grupo principal e os grupos secundários aos quais ela pertence devem existir antes de se iniciar o comando `useradd`. Além disso, não é possível excluir um grupo se este for o grupo principal de uma conta de usuário.

## O comando `passwd`

Este comando é usado principalmente para alterar a senha de um usuário. Qualquer usuário pode alterar sua senha, mas apenas o root pode alterar a senha de qualquer usuário.

Dependendo da opção de `passwd` usada, podemos controlar aspectos específicos do envelhecimento da senha:

`-d`
: Exclui a senha de uma conta de usuário (definindo assim uma senha vazia, transformando-a em uma conta sem senha).

`-e`
: Força a conta de usuário a alterar a senha.

`-l`
: Bloqueia a conta de usuário (a senha criptografada é prefixada com um ponto de exclamação).

`-u`
: Desbloqueia a conta de usuário (o ponto de exclamação é removido).

`-S`
: Exibe informações sobre o status da senha de uma conta específica.

Essas opções só estão disponíveis para o root. Para ver a lista completa de opções, consulte as páginas de manual.

# Exercícios Guiados

Indique a que arquivo se refere cada uma das entradas a seguir:

- `developer:x:1010:frank,grace,dave`
- `root:x:0:0:root:/root:/bin/bash`
- `henry:$1$.AbCdEfGh123456789A1b2C3d4.:18015:20:90:5:30::`
- `henry:x:1000:1000:User Henry:/home/henry:/bin/bash`
- `staff:!:dave:carol,emma`

Observe esta saída para responder às sete questões a seguir:

```
# cat /etc/passwd | tail -3
dave:x:1050:1050:User Dave:/home/dave:/bin/bash
carol:x:1051:1015:User Carol:/home/carol:/bin/sh
henry:x:1052:1005:User Henry:/home/henry:/bin/tcsh
# cat /etc/group | tail -3
web_admin:x:1005:frank,emma
web_developer:x:1010:grace,kevin,christian
dave:x:1050:
# cat /etc/shadow | tail -3
dave:$6$AbCdEfGh123456789A1b2C3D4e5F6G7h8i9:0:20:90:7:30::
carol:$6$q1w2e3r4t5y6u7i8AbcDeFgHiLmNoPqRsTu:18015:0:60:7:::
henry:!$6$123456789aBcDeFgHa1B2c3d4E5f6g7H8I9:18015:0:20:5:::
# cat /etc/gshadow | tail -3
web_admin:!:frank:frank,emma
web_developer:!:kevin:grace,kevin,christian
dave:!::
```

- Qual o identificador de usuário (UID) e identificador de grupo (GID) de `carol` ?
- Qual shell está configurado para `dave` e `henry` ?
- Qual o nome do grupo principal de `henry` ?
- Quem são os membros do grupo `web_developer` ? Quais deles são administradores do grupo?
- Qual usuário não pode se logar no sistema?
- Qual usuário deverá mudar a senha na próxima vez em que fizer login no sistema?
- Quantos dias devem se passar até que seja exigida uma alteração de senha para `carol` ?

# Exercícios Exploratórios

Trabalhando como root, use o comando `useradd -m dave` para adicionar uma nova conta de usuário. Quais as operações realizadas por esse comando? Suponha que `CREATE_HOME` e `USERGROUPS_ENAB` em `/etc/login.defs` estejam definidos como sim.

A conta de usuário `dave` foi criada; esse usuário pode fazer login no sistema?

Encontre o identificador de usuário (UID) e de grupo (GID) de `dave` e todos os membros do grupo `dave` .

Crie os grupos `sys_admin` , `web_admin` e `db_admin` e encontre seus identificadores de grupo (GIDs).

Adicione uma nova conta de usuário de nome `carol` com UID 1035 e defina `sys_admin` como grupo principal e `web_admin` e `db_admin` como grupos secundários.

Exclua as contas de usuário `dave` e `carol` e os grupos `sys_admin` , `web_admin` e `db_admin` criados anteriormente.

Execute o comando `ls -l /etc/passwd /etc/group /etc/shadow /etc/gshadow` e descreva a saída em termos de permissões de arquivos. Quais desses quatro arquivos estão em shadow por razões de segurança? Pressuponha que seu sistema usa senhas shadow.

Execute o comando `ls -l /usr/bin/passwd` . Qual bit especial é definido e o que ele significa?

# Resumo

Nesta lição, você aprendeu:

- Noções fundamentais de gerenciamento de usuários e grupos no Linux
- Gerenciar informações de usuários e grupos armazenados nos bancos de dados de senhas e grupos
- Manter o diretório de esqueleto
- Adicionar e remover contas de usuário
- Adicionar e remover contas de grupo
- Alterar a senha das contas de usuário

Os seguintes comandos foram discutidos nesta lição:

`useradd`
Cria uma nova conta de usuário.

`groupadd`
Cria uma nova conta de grupo.

`userdel`
Exclui uma conta de usuário.

`groupdel`
Exclui uma conta de grupo.

`passwd`

Altera a senha das contas de usuário e controla todos os aspectos do envelhecimento da senha.