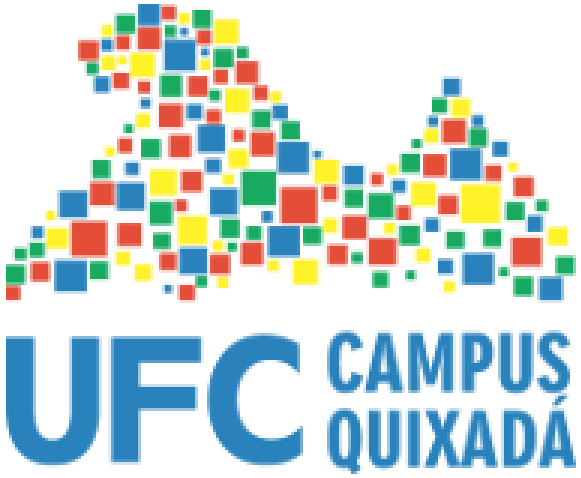

Manipulação de Contas e Permissões

Prof. Michel Sales Bonfim

Disciplina: Administração de Sistemas Operacionais Linux

Manipulação de Contas de Usuários

Gerenciamento de Usuários no Linux

- O gerenciamento de usuários no Linux é uma tarefa importante para a segurança do sistema operacional.

- No Linux, cada usuário tem uma conta com atributos que o identificam. Esses atributos permitem que o usuário tenha uma senha, seja membro de um grupo, defina um shell e conceda permissões para executar programas ou editar arquivos.

Superusuário

- No Linux, temos dois tipos de usuários: o "usuário" e o "administrador“.
- O administrador é conhecido como **superusuário** ou **root.**
- O **root** é o usuário com maior nível de autorização dentro do **Linux**.
  - Gerenciamento de usuários (criação, remoção, etc).
  - Configurações especiais do sistema.
- Para acessar o sistema como root, pode-se utilizar o login inicial ou o comando **su** (caso já esteja logado com outro usuário)

su

- Este comando permite mudar de usuário em um ambiente shell.

```
su [opções][usuário]
```

Onde

usuário é o nome do usuário que passará a usar um determinado ambiente.

Opções:

-c, --command COMMAND : um comando é executado usando os privilégios do usuário especificado.

-s, --shell SHELL : define o ambiente **shell** a ser usado com o usuário especificado.

- Caso o nome do usuário não seja fornecido, assume-se que o objetivo é se tornar o usuário root.
- No Ubuntu, usa-se o comando **sudo** quando se deseja executar comandos com os privilégios de outro usuário. Portanto, deve-se usar **sudo** antes de **su** caso o objetivo seja se tornar o usuário root.

Verificando todos os usuários e todos os grupos

- Os dados do usuário são colocados no arquivo **/etc/passwd** após sua criação e os dados do grupo são colocados no arquivo **/etc/group**.

- **OBSERVAÇÃO**: Caso esteja usando senhas ocultas (shadow passwords), as senhas dos usuários serão colocadas no arquivo **/etc/shadow** e as senhas dos grupos no arquivo **/etc/gshadow**.
  - Isto aumenta mais a segurança do sistema porque somente o usuário root pode ter acesso a estes arquivos.

/etc/passwd

Usuário:**Senha**:**UID**:**GID**:**Comentário**:**Home**:**Shell**

- **Usuário**: login do usuário.
- **Senha**: Valor da senha do usuário em texto claro. Caso seja incluído um "x", indica que a senha está guardada em outro local (/etc/shadow).
- **User ID:** Indica o identificador do usuário.
- **Group ID padrão**: é o grupo de login do usuário. Todos os arquivos do sistema são de propriedade de um usuário e de um grupo.
- **Comentário**: este campo guarda informações do usuário, podendo ser seu nome, telefone, e-mail, etc.
- **Home**: Diretório home do usuário
- **Shell**: por padrão esta é /bin/bash (Bourne Again Shell). Contas que não precisam ou não devem (por medidas de segurança) ter uma shell de login possuem neste campo /bin/false

/etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
ubuntu:x:1000:1000:ubuntu,,,:/home/ubuntu:/bin/bash

/etc/group

`Grupo:Senha:GID:Comentário:Usuários`

- **Grupo**: Nome do grupo.
- **Senha**:Valor da senha do grupo em texto claro. Caso seja incluído um "x", indica que a senha está guardada em outro local (/etc/gshadow).
- **Group ID**: É o identificador numérico e único do grupo
- **Comentário**: Este campo guarda informações do grupo.
- **Usuários**: Indica uma de usuários pertencentes ao grupo.

Exemplo:

```
general:x:502:juan,shelley,bob
```

/etc/shadow

```
ubuntu:$1$BJxvA4uP$Lap0ybTdV1F6cvj1PMBGF:12060:0:99999:7:::
```

- **Nome do usuário:** É o nome de login do usuário, igual ao referido no arquivo /etc/passwd.
- **Senha criptografada:** geralmente utiliza-se um algoritmo Hash (MD5 ou SHA-512)
- **Última mudança de senha:** este número representa o número de dias decorridos entre 1 de janeiro de 1970 e a última alteração da senha.
- **Número de dias para que a mudança de senha seja permitida:** tipicamente este número é zero, permitindo que o usuário mude sua senha quando desejar.
- **Número de dias após o qual a senha deve ser alterada:** caso a alteração da senha não seja forçada, este número será 99999.
- **Número de dias antes da expiração da senha no qual o usuário será avisado:** tipicamente o usuário é avisado com uma semana de antecedência.
- **Número de dias entre a expiração da senha e a desativação da conta:** caso não se queira desativação automática da conta, este campo é deixado em branco ou com o valor 1.
- **Dia da desativação da conta:** dias decorridos entre 1 de Janeiro de 1970 e a data em que a conta será desativada. Um valor em branco (ou 1) neste campo suspende desativação automática.
- **Campo reservado:** para uso futuro.

/etc/gshadow

```
Grupo:Senha Criptografada:Administradores:Usuários
```

- **Grupo**: Nome do grupo.
- **Senha**: Senha do grupo. Necessária caso queira que usuários não membros do grupo acessem as suas permissões, através do comando **newgrp**.
- **Administradores:** Inclui uma lista de administradores do grupo. Podem alterar a senha ou os membros do grupo.
- **Usuários**: Indica uma lista de usuários pertencentes ao grupo. Deve incluir a mesma lista do /etc/group

- Exemplo:

```
sambashare:!::ubuntu
```

adduser

- Adiciona um usuário ou grupo no sistema.

```
adduser [opções] [usuário/grupo]
```

Onde:

usuário/grupo: Nome do novo usuário que será adicionado ao sistema.

Opções:

--group Cria um novo grupo ao invés de um novo usuário. A criação de grupos também pode ser feita pelo comando addgroup.

Observações:

Ao se criar o novo usuário, será criada os seguintes elementos:

- Um UID.
- DIretório com o nome no usuário no diretório /home.
- Um grupo com o mesmo nome do usuário (Grupo primário).

login, logout, exit

- **login**
  - Este comando abre uma nova sessão para um usuário. Esta nova sessão assume o perfil do usuário com todas as características associadas a ele.
- **logout**
  - Tem como função desconectar um usuário de uma determinada sessão.
- **exit**
  - No modo gráfico, o comando **exit** fecha a janela na qual o usuário digitou o comando;
  - No modo texto, o comando **exit** encerra a sessão do usuário (volta para a tela inicial onde é feita a identificação dos usuários).

id

- Mostra a identificação atual do usuário, grupo primário e outros grupos que pertence.

```
id [opções] [usuário]
```

Onde:

usuário É o usuário que desejamos ver a identificação, grupos primários e complementares.

Opções:

-g Mostra somente a identificação do grupo primário.

-u Mostra somente a identificação do usuário (user ID).

users

- Mostra os nomes de usuários usando atualmente o sistema.

```
users
```

groups

- Mostra os grupos que o usuário pertence.

```
groups [usuário]
```

lastlog

- Mostra o último login dos usuários cadastrados no sistema.

```
lastlog [opções]
```

Opções:

-u [nome] Mostra somente detalhes sobre o usuário [nome].

last

- Mostra uma listagem de entrada e saída de usuários no sistema.

```
last [opções]
```

Opções:

-R Não mostra o campo HostName.

-a Mostra o hostname na última coluna. Será muito útil se combinada com a opção -d.

-d Usa o DNS para resolver o IP de sistemas remotos para nomes DNS.

logname

- Mostra seu login (username).

```
logname
```

chfn

- Muda os dados inseridos durante o cadastro do novo usuário.

```
chfn [opções] [usuário]
```

Onde:

usuário Nome do usuário.

Opções:

-f [nome] Adiciona/altera o nome completo do usuário.

-r [nome] Adiciona/altera o número da sala do usuário.

-w [tel] Adiciona/altera o telefone de trabalho do usuário.

-h [tel] Adiciona/altera o telefone residencial do usuário.

-o [outros] Adiciona/altera outros dados do usuário.

usermod

- Modifica dados da conta do usuário.

```
usermod [opções] [usuário]
```

Onde:

usuário Nome do usuário.

Opções:

-d diretório [-m]	cria um novo diretório home para o usuário. A opção -m faz com que os arquivos do diretório atual do usuário seja movido para o novo diretório.
-g grupo :	altera o GID do grupo padrão do usuário para o valor especificado.
-G grupo1[,grupo2, ...]	define o GID dos outros grupos aos quais o usuário pertence.
-l nome	altera o nome de identificação do usuário (o usuário não pode estar logado).
-s shell	altera o shell do usuário.
-u uid	altera o número de UID do usuário.

passwd

- Modifica os parametros de senha de usuário.

```
passwd [opções] [usuário]
```

Onde:

usuário: Nome do usuário que terá sua senha alterada.

Opções:

-x [dias] Especifica o número máximo de dias que a senha poderá ser usada. Após terminar o prazo, a senha deverá ser modificada.

Observações:

Você deve ser o dono da conta para poder modificar a senhas. O usuário root pode modificar/apagar a senha de qualquer usuário.

Configurando expiração de senhas

- Em /etc/login.defs, você pode ajustar os seguintes parâmetros para refletir sua política ou controle de segurança:

- PASS_MAX_DAYS: Quantos dias a senha fica ativa antes de expirar.
- PASS_MIN_DAYS: Quantos dias uma senha deve ficar ativa antes de poder ser alterada por um usuário.
- PASS_WARN_AGE: O número de dias que um aviso é emitido ao usuário antes de uma expiração iminente da senha.

chage

- Muda as informações de expiração de senha de um usuário.

```
chage [opções] LOGIN
```

Opções:

-l, --list	exibe informação sobre idade da conta
-E, --expiredate mm/dd/aa	define data de expiração de conta.
-I, --inactive INATIVO	define senha inativa após expiração para INATIVO
-m, --mindays MIN_DIAS	define número mínimo de dias antes da troca de senha para MIN_DIAS
-M, --maxdays MAX_DIAS	define número máximo de dias antes da troca de senha para MAX_DIAS
-W, --warndays NUM_DIAS	define dias para aviso de expiração

chage

- Exemplos

chage -M 90 usuário	senha válida por 90 dias
chage -W 5 usuário	usuário começara ser alertado 5 dias antes da data limite
chage -I 3 usuário	após 3 dias da data limite o usuário ainda pode alterar a senha, após esse período somente o administrador do sistema poderá alterar

addgroup

- Adiciona um novo grupo de usuários no sistema.

```
addgroup [opções] [grupo]
```

Onde:

grupo: Nome do novo grupo de usuários que será adicionado ao sistema.

Opções:

Adicionar usuário a um grupo

- Criar usuário **teste.**
- Criar grupo **grupoteste.**
- Adicionar o usuário **teste** ao grupo **grupoteste.**
- Duas formas:
  - Editar arquivo /etc/group
  - Utilizar o comando adduser
    - `adduser teste grupoteste`

gpasswd

- Modifica parâmetros e senha de grupo. Um usuário somente pode alterar a senha de seu grupo, mas o superusuário (root) pode alterar a senha de qualquer grupo de usuário, inclusive definir o administrador do grupo.

```
gpasswd [opção] GRUPO
```

Opções:

-a, --add USUÁRIO adiciona o USUÁRIO ao GRUPO

-d, --delete USUÁRIO remove USUÁRIO do GRUPO

-r, --remove-password remove a senha do GRUPO

-R, --restrict restringe acesso dos membros ao GRUPO

-M, --members USUÁRIO,... ajusta a lista de membros do GRUPO

-A, --administrators ADMIN,... ajusta a lista de administradores para o GRUPO

newgrp

- Altera a identificação de grupo do usuário. Para retornar a identificação anterior, digite **exit** e tecle **Enter**.

```
newgrp - [grupo]
```

Onde:

- Se usado, inicia um novo ambiente após o uso do comando newgrp (semelhante a um novo login no sistema), caso contrário, o ambiente atual do usuário é mantido.

grupo Nome do grupo ou número do grupo que será incluído.

- Quando este comando é usado, é pedida a senha do grupo que deseja acessar. Caso a senha do grupo esteja incorreta ou não exista senha definida, a execução do comando é negada.

groupdel

- Apaga um grupo do sistema.

```
groupdel [grupo]
```

Observações:

Tenha certeza que não existem arquivos/diretórios criados com o grupo apagado através do comando find.

Você não pode remover o grupo primário de um usuário. Remova o usuário primeiro.

userdel

- Apaga um usuário do sistema.

```
userdel [-r] [usuário]
```

Onde:

-r Apaga também o diretório HOME do usuário.

Observações:

Note que uma conta de usuário não poderá ser removida caso ele estiver no sistema.

Operações Manuais

- Como transformar um usuário em administrador?
- Como bloquear um usuário?
- Como remover a senha de um usuário?

Controle de Permissões em Diretórios e Arquivos

Permissões de Acesso

- A segurança no sistema GNU/Linux é baseada em permissões de acesso.
- Protegem o sistema de arquivos contra o acesso indevido de usuários ou programas não autorizados.
- A ideia básica é definir os tipos de acesso a arquivos e diretórios para 3 entidades:
  - Proprietário;
  - Grupo;
  - Outros usuários.

Tipos de Acesso

- **r – read**
  - **Arquivo:** permite ler um arquivo**.**
  - **Diretório:** permite listar o conteúdo de um diretório (ls).
- **w – write**
  - **Arquivo:** permissão de gravação para arquivos.
  - **Diretório:** permite a gravação de arquivos e diretórios dentro dele.
- **x – execute**
  - **Arquivo:** permite executar um arquivo (caso seja um excutável).
  - **Diretório:** permite acessar um diretório (cd).

Tipos de Acesso

-rwxr-xr-- 1 gleydson user 8192 2011-02-31 16:00 teste

Primeiro Caracter (-) : identifica o tipo do arquivo (arquivo ou diretório). Nesse caso, é um arquivo (-), para ser diretório, o valor seria "d".

Segundo ao Quarto Caracter (rwx) : indica a permissão de acesso do dono do arquivo (gleydson). Nesse caso, o dono tem permissão de leitura (r), gravação (w) e execução (x).

Quinto ao Sétimo Caracter (r-x) : indica a permissão de acesso ao grupo do arquivo (user). Nesse caso, o grupo tem permissão de leitura (r) e execução (x).

Oitavo ao Décimo Caracter (r--) : indica a permissão de acesso para os outros usuários. Nesse caso, os outros usuários têm apenas a permissão de leitura (r).

chmod

- Muda a permissão de acesso a um arquivo ou diretório.

```
chmod [opções] [permissões] [diretório/arquivo]
```

Onde:

 # diretório/arquivo: Diretório ou arquivo que terá sua permissão mudada.

 # opções:

-v, --verbose Mostra todos os arquivos que estão sendo processados.

-R, --recursive Muda permissões de acesso do diretório/arquivo no diretório atual e subdiretórios.

 # permissões (ugoa+-=rwx) -> Modo Amigável!!!!!

ugoa Controla que nível de acesso será mudado. Especificam, em ordem, usuário (u), grupo (g), outros (o), todos (a).

+-= + coloca a permissão, - retira a permissão do arquivo e = define a permissão exatamente como especificado.

rwx r permissão de leitura do arquivo. w permissão de gravação. x permissão de execução (ou acesso a diretórios).

chmod (Exemplos)

- **chmod g+r ***
- **chmod o-r teste.txt**
- **chmod uo+x teste.txt**
- **chmod a+x teste.txt**
- **chmod a=rw teste.txt**

chmod (Exemplos)

- **chmod g+r *** Permite que todos os usuários que pertençam ao grupo dos arquivos (g) tenham (+) permissões de leitura (r) em todos os arquivos do diretório atual.
- **chmod o-r teste.tx**t Retira (-) a permissão de leitura (r) do arquivo teste.txt para os outros usuários (usuários que não são donos e não pertencem ao grupo do arquivo teste.txt).
- **chmod uo+x teste.txt** Inclui (+) a permissão de execução do arquivo teste.txt para o dono e outros usuários do arquivo.
- **chmod a+x teste.txt** Inclui (+) a permissão de execução do arquivo teste.txt para o dono, grupo e outros usuários.
- **chmod a=rw teste.txt** Define a permissão de todos os usuários exatamente (=) para leitura e gravação do arquivo teste.txt.

chmod (Exemplos)

- **cteste1.dat:** permissões totais. Ou seja, leitura, escrita e execução para o dono, grupo e outros

- **cteste2.txt**: Leitura e escrita para o dono, leitura para o grupo e leitura para os outros

- **cteste3.doc**: Leitura e escrita para o dono e leitura para o grupo

chmod

- Permissões: Modo máscara binária ou modo octal
- Flexível - especifica diretamente a permissão do dono, grupo e outros.
- Valores:
  - 4 = Ler (**r**ead)
  - 2 = Gravar (**w**rite)
  - 1 = Executar (**e**xecute)

chmod

User (owner)			Group			Other		
r	w	x	r	w	x	r	w	x
4	2	1	4	2	1	4	2	1

- **Associação (Soma):**
  - **0 -** Nenhuma permissão de acesso. Equivalente a -rwx.
  - **1** - Permissão de execução (x).
  - **2** - Permissão de gravação (w).
  - **3** - Permissão de gravação e execução (wx). Equivalente a permissão 2+1
  - **4** - Permissão de leitura (r).
  - **5** - Permissão de leitura e execução (rx). Equivalente a permissão 4+1
  - **6** - Permissão de leitura e gravação (rw). Equivalente a permissão 4+2
  - **7 -** Permissão de leitura, gravação e execução. Equivalente a +rwx (4+2+1).

chmod (Exemplos)

- chmod 777 teste.txt
- chmod 755 teste.txt
- chmod 751 teste.txt

chmod (Exemplos)

- **oteste1.dat:** permissões totais. Ou seja, leitura, escrita e execução para o dono, grupo e outros

- **oteste2.txt**: Leitura e escrita para o dono, leitura para o grupo e leitura para os outros

- **oteste3.doc**: Leitura e escrita para o dono e leitura para o grupo

chgrp

- Muda o grupo de um arquivo/diretório.

```
chgrp [opções] [grupo] [arquivo/diretório]
```

Onde:

 # grupo Novo grupo do arquivo/diretório.

 # arquivo/diretório Arquivo/diretório que terá o grupo alterado.

 # opções

-v, --verbose Mostra todas as mensagens e arquivos sendo modificados.

-R, --recursive Altera os grupos de arquivos/sub-diretórios do diretório atual.

chown

- Muda dono de um arquivo/diretório. Opcionalmente pode também ser usado para mudar o grupo.

```
chown [opções] [dono.grupo] [diretório/arquivo]
```

Onde:

 # dono.grupo Nome do dono.grupo que será atribuído ao diretório/arquivo. O grupo é opcional.

 # diretório/arquivo Diretório/arquivo que o dono.grupo será modificado.

 # opções

-v, --verbose Mostra os arquivos enquanto são alterados.

-R, --recursive Altera dono e grupo de arquivos no diretório atual e sub-diretórios.