



Título do Curso:

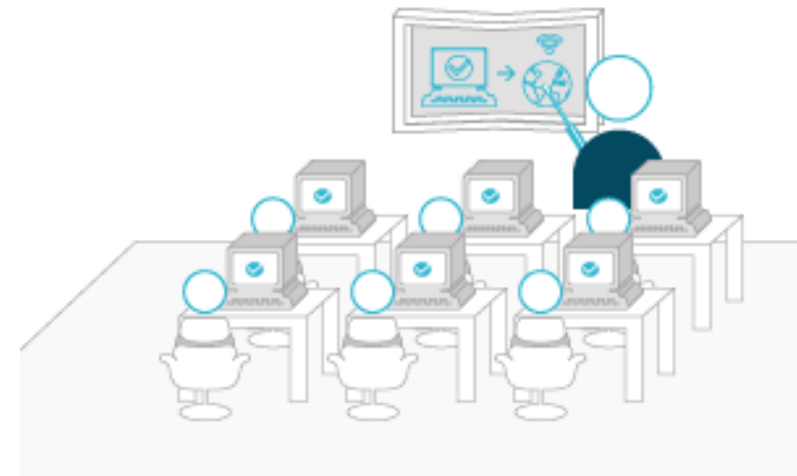
Administração de Sistemas
GNU/Linux



Conteúdo do curso

ADMINISTRAÇÃO DE SISTEMAS GNU/LINUX

- ✓ Tópico 1: Introdução ao sistema operacional GNU/Linux.
- ✓ Tópico 2: Introdução ao Shell e comandos básicos.
- ✓ Tópico 3: Manipulação de conteúdos com comandos no Shell.
- ✓ Tópico 4: Comandos para gerenciamento do sistema e do Hardware.
- ✓ Tópico 5: Editor de Texto VI.
- **Tópico 6: Administração de usuários e grupos.**
- Tópico 7: Gerenciamento de permissões.
- Tópico 8: Gerenciamento de processos.
- Tópico 9: Sistemas de arquivos e particionamento.
- Tópico 10: Expressões regulares.
- Tópico 11: Introdução ao Shell Script.
- Tópico 12: Gerenciamento de Pacotes.
- Tópico 13: Agendamento de tarefas (cron) e Backup.





DGP

Tecnologia da Informação

Tópico 6

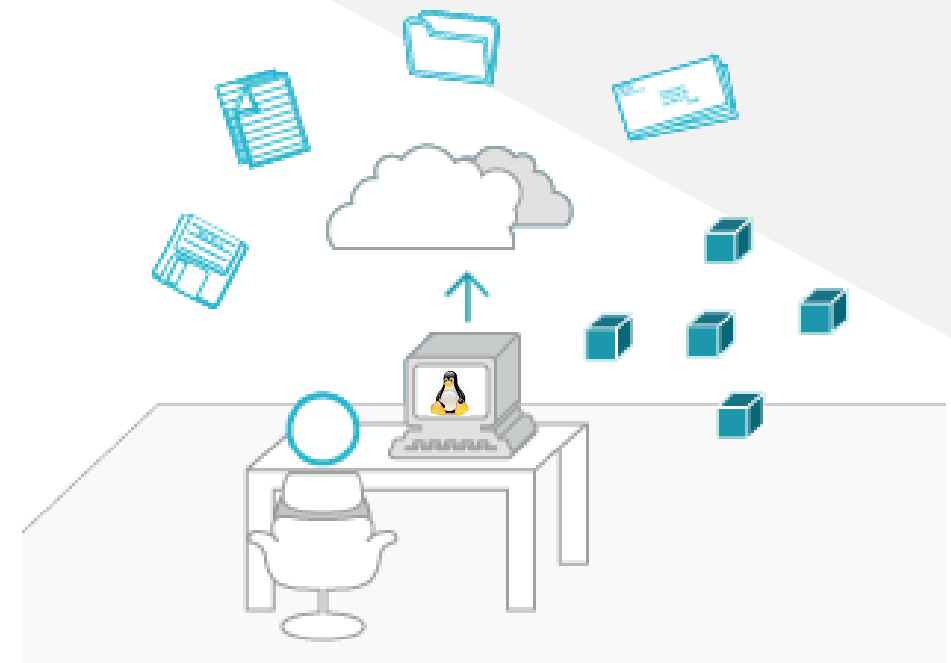
Administração de usuários e grupos.



Administração de

Usuários e Grupos.

- Neste slide teremos comandos que nos auxiliam no gerenciamento de usuários e grupos, bem como conceitos e elevação de privilégios:
 - Comandos para Gerenciamento de usuários e grupos;
 - Arquivos de Administração de Usuários e Grupos;
 - Conceitos e Elevação de privilégios.



Comandos para Gerenciamento de usuários e grupos

Tópico 6: Administração de
usuários e grupos.



Comandos para Gerenciamento de usuários e grupos

- Da mesma forma que em um sistema operacional Microsoft, podemos administrar privilégios de usuários com a criação de usuários e grupos, nos sistemas GNU/Linux temos alguns comandos que permitem a administração de usuários e grupos de forma intuitiva:

- `useradd` → Cria/adiciona um usuário ao sistema:

- Ex.: `useradd <opções> [nome_usuario]`

```
[root@server ~]# useradd aluno
```

- Observe que após criar o usuário, seu diretório pessoal foi criado em “/home”:

```
[root@server ~]# ls /home/  
aluno
```

- Observe a nova linha (com os dados do usuário) inserida no arquivo “/etc/passwd”:

```
aluno:x:1004:1004:/:/home/aluno:/bin/bash
```



Comandos para Gerenciamento de usuários e grupos

- userdel → Remove um usuário do sistema:

- Ex.: `userdel <opções> [nome_usuario]`

```
[root@server ~]# userdel aluno
```

- OBS.: Ao excluir a conta, o diretório pessoal do mesmo não é excluído. Para esta finalidade devemos utilizar o parâmetro “-r” ou o “-f” (caso algum arquivo em seu diretório pessoal possua outra conta como proprietário)

- usermod → Altera as propriedades de um usuário:

- Ex.: `usermod <opções> [usuário]`

```
[root@server ~]# usermod -G 0 aluno
```

- No exemplo acima, estamos adicionando o usuário em um grupo que possui o identificador 0.
 - **PERGUNTA: Qual grupo do sistema possui identificador 0?**



Comandos para Gerenciamento de usuários e grupos

- usermod → Continuação... Com o “usermod” podemos:
 - Modificar o grupo primário do usuário → Ex.: `usermod -g grupo [usuário]`
 - Inserir diversos grupos secundários → Ex.: `usermod -G grupo [usuário]`
- ```
[root@server ~]# usermod -G root,bin,disk aluno
```
- Modificar o shell padrão do usuário → Ex.: `usermod -s /bin/false [usuário]`
  - Entre outras possibilidades...
- No sistema Linux, podemos definir um grupo primário para um usuário e diversos grupos suplementares (característica dos sistemas POSIX).
    - Geralmente trabalhamos com diversos grupos para facilitar a atribuição de permissões no acesso a arquivos e outros recursos em rede.
      - ***“Permissões” será o próximo tema do curso.***





# Comandos para Gerenciamento de usuários e grupos

- groupadd → Cria/Adiciona um grupo no sistema:

- Ex.: `groupadd <opções> [nome_grupo]`

```
[root@server ~]# groupadd gestores
```

- Observe a nova linha no arquivo “/etc/group”:

```
gestores:x:1005:
```

- groupdel → Remove um grupo no sistema:

- Ex.: `groupdel [nome_grupo]`

```
[root@server ~]# groupdel gestores
```

- OBS.1: Caso este grupo tenha algum usuário como membro, o grupo será removido da mesma forma.
- **PERGUNTA:** Caso o grupo seja “proprietário” de um determinado arquivo, o que acontece se o mesmo for excluído?



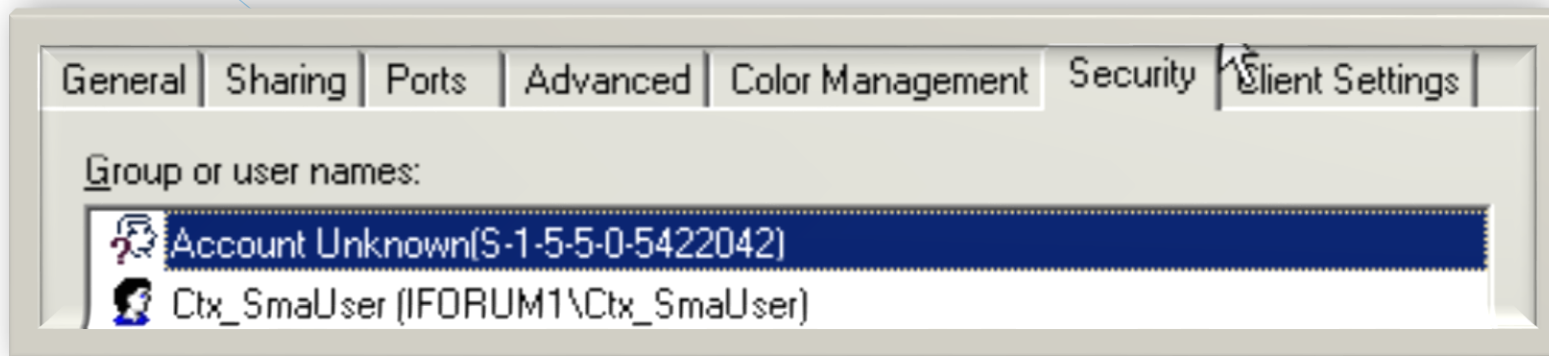
# Comandos para Gerenciamento de usuários e grupos

- groupdel → continuação...
  - *PERGUNTA: O que acontece ao remover um usuário ou grupo que for “proprietário” de um determinado arquivo?*

```
[root@server ~]# ls -l
-rw-r--r-- 1 root gestores 1241 Mar 24 18:40 lista

[root@server ~]# groupdel gestores
[root@server ~]# ls -l
-rw-r--r-- 1 root 1005 1241 Mar 24 18:40 lista
```

- Ocorre o mesmo na plataforma **Micro\$oft**...





# Comandos para Gerenciamento de usuários e grupos

- groupmod → Modifica um grupo no sistema:
  - Ex.: `groupmod <opções> [nome_grupo]`

```
[root@server ~]# groupmod
Usage: groupmod [-g gid [-o]] [-n name] group
[root@server ~]# groupadd setores
[root@server ~]# groupmod -n dptos setores
[root@server ~]# tail -n 1 /etc/group
dptos:x:1005:
[root@server ~]# _
```

O parâmetro “-n” altera o nome do grupo.  
Ex.: `groupmod -n <novo-nome> <antigo>`

- groups → Exibe a lista de grupos que determinado usuário é membro:
  - Ex.: `groups <usuário>`

```
[root@server ~]# groups
root bin daemon sys adm disk wheel
```

```
[root@server ~]# groups aluno
aluno : aluno root bin disk
```

- OBS.: Caso não seja informado o nome do usuário, será exibida a lista de grupos que o usuário “logado” pertence.



# Comandos para Gerenciamento de usuários e grupos

- passwd → Define a senha de acesso de um usuário:
  - Ex.: `passwd <nome_usuario>`

```
[root@server ~]# passwd aluno
Changing password for user aluno.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

- OBS.: Caso não seja informado o nome do usuário, será solicitada uma nova senha para a conta que estiver “logada” no momento.
- Falando em senhas, qual a finalidade dos arquivos a seguir?
  - `/etc/passwd`
  - `/etc/group`
  - `/etc/shadow`



# Arquivos de Administração de Usuários e Grupos

Tópico 6: Administração de  
usuários e grupos.

# Arquivos de Administração de Usuários e Grupos



- Arquivo “/etc/passwd” →
  - Contém as contas de usuários e suas propriedades:

```
aluno:x:1004:1004:~/home/aluno:/bin/bash
```

- Cada linha possui até 7 informações referentes a um usuário, sendo:
  - 1º Campo = Login (Nome da credencial/usuário utilizado para o Logon);
  - 2º Campo = Representa a “senha” do usuário (leia o próximo slide);
  - 3º Campo = UID (User Identifier – Número único para identificar o usuário);
  - 4º Campo = GID (Group Identifier – Identificador numérico do grupo primário ao qual o usuário pertence);
  - 5º Campo = Comentário (Aceita diversos tipos de caracteres e espaços, onde podemos informar o nome completo ou outras informações);
  - 6º Campo = Diretório Home (Caminho do diretório padrão do usuário);
  - 7º Campo = Shell (Define qual Shell será executado pelo usuário após o logon).

# Arquivos de Administração de Usuários e Grupos



- Arquivo “/etc/passwd” →
  - Continuação...:

```
aluno:x:1004:1004:~/home/aluno:/bin/bash
```

- Curiosidades:
  - O Segundo campo (senha), pode possuir três caracteres, sendo o “x” para informar que a senha está contida no arquivo “/etc/shadow”, o “\*” para informar que a conta está desabilitada, ou sem informações “::” para definir que a conta está “sem senha”;
  - O UID “0” representa o usuário “root” (porém, pode ser atribuído a outro usuário);
  - O intervalo de UID de 1-99 são reservados para contas pré-definidas;
  - O intervalo de UID de 100-999 (ou 100-499, dependendo da distribuição), são reservados para contas administrativas de usuários e grupos, portanto, ao criar uma conta, o sistema sempre utilizará um UID após este intervalo.

# Arquivos de Administração de Usuários e Grupos



- Arquivo “/etc/group” →
  - Contém as contas de grupo e quais os usuários são membros de cada um deles:

```
[root@server ~]# usermod -G dptos aluno
[root@server ~]# usermod -G dptos root
[root@server ~]# tail -n 1 /etc/group
dptos:x:1005:aluno,root
```

- Cada linha possui até 4 informações referentes a um grupo, sendo:
  - 1º Campo = Nome do grupo;
  - 2º Campo = Representa a “senha” do grupo (pouco usual, armazenada no arquivo “/etc/gshadow”);
  - 3º Campo = GID (Group Identifier – Identificador numérico do grupo);
  - 4º Campo = Usuários membros do grupo (separados por vírgula).



# Arquivos de Administração de Usuários e Grupos



- Arquivo “/etc/shadow” →
  - Contém as senhas criptografadas, após serem definidas pelo comando “**passwd**”:

```
aluno:!!:15438:0:99999:7:::
```

Usuário criado, antes de definir a senha (observe o “!!” – 2º campo)

```
aluno:1h1AA7S24$20fbYsUuUbYZyVAgOCZ6h1:15438:0:99999:7:::
```

Usuário criado e senha definida.

- Cada linha possui até 8 informações referentes a um usuário, sendo:
  - 1º Campo = Login (Nome do usuário utilizado para o Logon);
  - 2º Campo = Senha criptografada (algoritmo “MD5-based” [\$1], método “salt” – vide link\*);
  - 3º Campo = Última mudança da senha (Lastchanged – Dia em que a senha foi alterada, considerando a quantidade de dias corridos a partir de 01/01/1970);
  - 4º Campo = “Minimum Password Age” (Tempo mínimo de dias em que o usuário deve aguardar pra mudar a senha, após uma alteração da mesma);
  - 5º Campo = “Maximum Password Age” (Tempo em dias que a senha será considerada válida - O valor 99999 representa que a senha não expira);

# Arquivos de Administração de Usuários e Grupos



- Arquivo “/etc/shadow” →
  - Continuação...:

```
aluno:!!:15438:0:99999:7:::
```

Usuário criado, antes de definir a senha (observe o “!!” – 2º campo)

```
aluno:1h1AA7S24$20fbYsUuUbYZyVAgOCZ6h1:15438:0:99999:7:::
```

Usuário criado e senha definida.

- Cada linha possui até 8 informações referentes a um usuário, sendo:
  - 6º Campo = Warn (Número de dias que antecede a expiração da senha, onde um alerta será enviado ao usuário durante o Logon);
  - 7º Campo = Inactive (Informa que a conta será desativada após “X” dias em que a senha expirar);
  - 8º Campo = Expire (Dia em que a senha será automaticamente expirada, considerando a quantidade de dias corridos a partir de 01/01/1970);
- O comando “**chage**” pode ser utilizado para definir estas informações (contidos no arquivo “/etc/shadow”) sobre as senhas dos usuários.

# Conceitos e Elevação de privilégios

Tópico 6: Administração de usuários e grupos.



# Conceitos – UID e GID

- Os identificadores UID e GID são tratados pelo sistema de forma transparente e atribuídos sequencialmente aos usuários e grupos criados;
- Geralmente, ao criar uma conta de usuário, uma conta de grupo com o mesmo nome é criada e vinculada ao usuário (ambos com o mesmo número para UID e GID, caso disponível);
- Em algumas distribuições, todas as contas de usuário criadas são vinculadas em um grupo de nome “users” de GID 500 ou 1000;
- O comando “id” permite visualizar os grupos e o GID de todos os grupos vinculados a uma conta de usuário.
  - id → Exibe os grupos e GID vinculados a conta “logada” ou especificada:
  - Ex.: `id <usuário>`

```
[root@server ~]# id aluno
uid=1004(aluno) gid=1004(aluno) groups=1004(aluno),1005(dptos) context=root:syste
m_r:unconfined_t:SystemLow-SystemHigh
```



# Elevação de privilégios

- Por razões de segurança, comandos mais “nocivos” de administração do sistema, não podem ser executados por um usuário comum no Linux.
  - Ex.: “shutdown”; “reboot”; “init”; “halt” (exceto CentOS); “useradd”; “fdisk”; entre outros.
- Para prover maior segurança, alguns administradores não permitem que o usuário “root” tenha permissões para Logon remoto;
- Desta forma, precisamos acessar remotamente com um usuário comum e utilizar comandos para possibilitar a elevação de privilégios e consequentemente, administrar o sistema como se fosse o usuário “root”;



# Elevação de privilégios

- **su** → Possibilita que um usuário altere o UID e GID utilizado no momento para o UID e GID de um usuário a ser especificado:

- Ex.: **su** <opções> <usuário>

```
[guilherme@server ~]$ su
Password:
[root@server guilherme]#
```

```
[root@server guilherme]# pwd
/home/guilherme
[root@server guilherme]# whoami
root
```

Observe que o usuário permanece no mesmo diretório que estava, porém, possui privilégio de root (está logado como se fosse o root).

- OBS.: Caso não seja informado o nome do usuário, será considerado o “**root**”.
- OBS.: Podemos utilizar o comando “su -” para carregar todo o perfil do “**root**”.

- **sudo** → Permite ao usuário logado executar algum comando com privilégios de “**root**” ou do usuário especificado (parâmetro “-u”):

- Ex.: **sudo** <opções> <usuário>

- OBS.: Podemos configurar no arquivo “/etc/sudoers” quais usuários possuem determinado nível de privilégios e quais comandos o mesmo poderá executar sem solicitar a senha do usuário “**root**”.



# Comodidade!?

## Criando usuários com “adduser”

- Em algumas distribuições Linux, temos um “wizard” para criação de usuários através do comando “**adduser**”:
  - adduser → Inicia um “wizard” solicitando diversas informações do usuário a ser criado, como login, nome, senha, telefone, endereço, grupos, UID, etc:

```
root@darkstar:~# adduser
Login name for new user []: guilherme
User ID ('UID') [defaults to next available]:
Initial group [users]:
Additional groups (comma separated) []: vendas,ti,marketing
```

```
Home directory [/home/guilherme]
Shell [/bin/bash]
Expiry date (YYYY-MM-DD) []:
```

**OBS.:** Apenas o comando “adduser” foi executado (primeira linha) e os demais itens foram solicitados para preenchimento, como um formulário.

**OBS.2:** Basta pressiona [Enter] para utilizar os valores padrão [descritos entre colchetes]



# Comodidade!?

## Criando usuários com “adduser”

- adduser → continuação...:

```
Creating new account...
Changing the user information for guilherme
Enter the new value, or press ENTER for the default
 Full Name []: Guilherme Rodrigues
 Room Number []:
 Work Phone []:
 Home Phone []:
 Other []:
Changing password for guilherme
Enter the new password (minimum of 5, maximum of 127 characters)
Please use a combination of upper and lower case letters and numbers.
New password:
Re-enter new password:
Password changed.
Account setup complete.
```

- OBS.: Conforme citado anteriormente, apenas algumas distribuições possuem este “wizard”, em outras distribuições, o “**adduser**” é um link simbólico do convencional “**useradd**”:

```
[root@mail ~]# which adduser
/usr/sbin/adduser
[root@mail ~]# ls -l /usr/sbin/adduser
lrwxrwxrwx 1 root root 7 Jul 19 2010 /usr/sbin/adduser -> useradd
```





# No próximo slide...

- Tópico 7: Gerenciamento de permissões.
  - Conceitos sobre permissões de acesso;
  - Permissões padrão (*file mode*);
  - Permissões avançadas (*special modes*).



# Referências

- BONAN, Adilson Rodrigues. **LINUX – Fundamentos, Prática & Certificação LPI**. Editora: Alta Books. RJ. 2010;
- PEREIRA, Guilherme Rodrigues. **Slides para aula expositiva**. Centro Universitário UNA.
- SILVA, Gleydson Mazioli. **Guia Foca GNU/Linux**. Disponível em: <https://guiafoca.org/>



**DGP**

Tecnologia da Informação

**Obrigado!**



Guilherme Rodrigues