

Conectividade em Sistemas
CiberFísicos

TDE 2

Usuários, Grupos e Permissões no Sistema de Arquivos



Atividades deste TDE

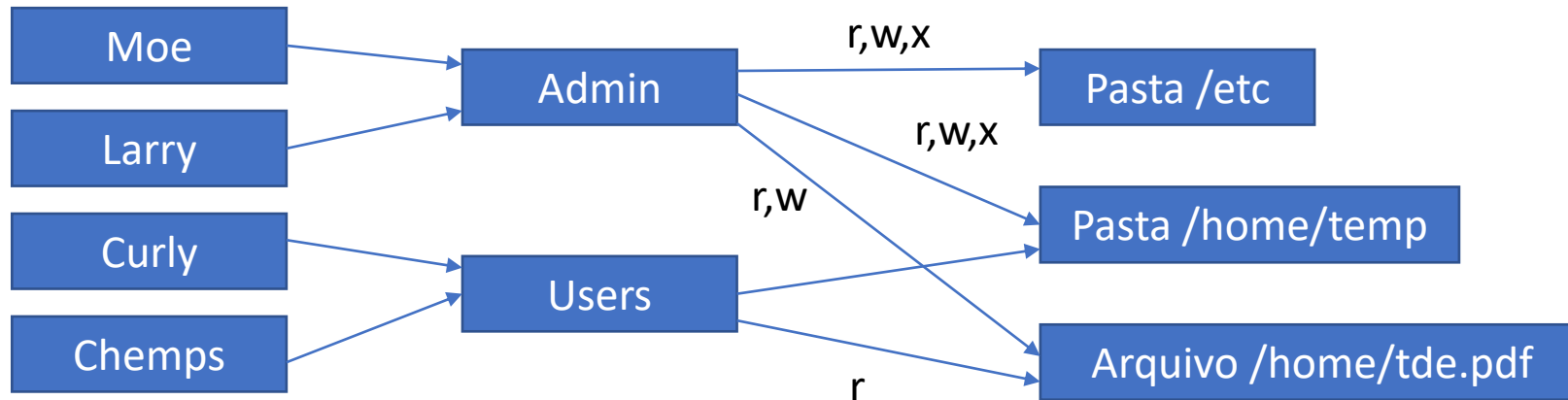
1. Ler alguns aspectos teóricos que estão apresentados nos primeiros slides.
2. Fazer os exercícios práticos conforme indicado
3. A entrega da atividade corresponde ao relatório solicitado no final deste roteiro com a resposta as **PERGUNTAS** formuladas durante o roteiro.

Permissões

- Um sistema operacional pode ser acessado pelo próprio usuário logado ou por usuários remotos, através de aplicações como SSH, Servidores Web e aplicações de Transferência de Arquivos
- É necessário controlar quais usuários tem permissões para acessar arquivos e pastas no sistema de arquivos
- O Linux define três tipos de acesso:
 - Ler (r)
 - Escrever (w)
 - Executar (x)

Usuários e Grupos

- As permissões pode ser atribuídas para cada usuário
- Contudo é mais fácil agrupar os usuários em grupos, e atribuir permissões ao grupo



Usuários e Grupos Pré-Criados

- Os programas e serviços do sistema operacional também recebem permissões através de grupos
- Por isso o sistema cria vários grupos automaticamente
- Você pode ver todos os grupos criados com o comando abaixo:
 - `cat /etc/group | cut -d: -f1`
- Você pode ver todos os usuários criados com o comando abaixo:
 - `cat /etc/passwd | cut -d: -f1`

Exercício1: Informações do Usuário

- Verifique as informações do seu usuário (conectividade) usando o comando a seguir:
 - id conectividade
- O comando traz as seguintes [informações](#):
 - uid = identificador do usuário
 - gid = identificador do grupo primário do usuário (inserido quando ele é criado)
 - grupos = lista de grupos secundários ao qual o usuário pertence
- **PERGUNTA 1:**
 - Indique a quais grupos o usuário conectividade pertence
 - Ele é administrador do sistema?

DAC: Discretionary Access Control

- O Linux implementa um modelo de permissões denominado DAC
- Nesse modelo, o usuário que criar um arquivo é seu proprietário, e pode determinar quais outros usuários também terão acesso.
- Cada arquivo do sistema está associado a um conjunto de permissões, que podem ser verificadas com o comando abaixo;

`ls -l`

- As permissões são representadas pelo conjunto de 10 caracteres da primeira coluna.

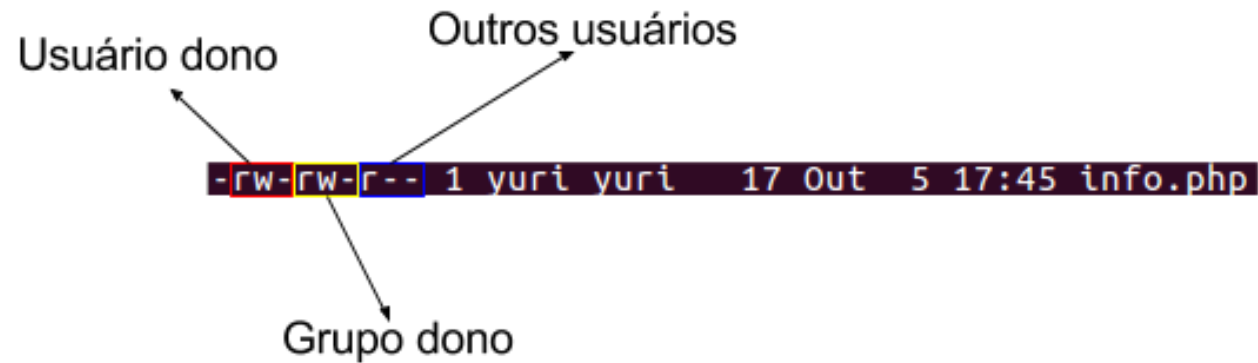
Diagram illustrating the components of the permissions string in the output of the `ls -l` command:

```
ls -l -rw-rw-r-- 1 yuri yuri 17 Out 5 17:45 info.php
```

The permissions string `-rw-rw-r--` is highlighted, and arrows point to its components:

- Usuário dono** (User permissions): `-rw`
- Grupo dono** (Group permissions): `-rw`
- Outros usuários** (Other users permissions): `-r--`

Permissões



- O primeiro caractere indica se o objeto listado é um arquivo (-) ou um diretório (d)
- Os nove caracteres restantes nos mostram as permissões do usuário dono, grupo dono e outros usuários respectivamente
- Observe que as permissões se aplicam aos usuários logados no sistema. Verifique o usuário logado com o comando abaixo:
 - `users`

Exercício 2: Permissão de Execução

1. Usando o gedit, crie o arquivo teste.sh conforme indicado abaixo:
#!/bin/bash
echo "bem vindo"
 2. Verifique as permissões do arquivo:
 - ls -l teste.sh
 3. Verifique se você consegue executar o script:
 - ./testes.sh
 4. Adicione a permissão de execução:
 - chmod u=rwx,g=rw,o=r teste.sh
 - ls -l testes.sh
 5. Verifique novamente se a execução é possível
-
- **PERGUNTA 2:**
 - Indique quais permissões o comando chmod modificou comparando o resultado do comando **ls -l** nos passos 2 e 4.

Exercício 3: Criação de Usuários

1. Crie um novo usuário e defina sua senha como **1234**
 - `sudo useradd convidado -s /bin/bash`
 - `sudo passwd convidado`
 2. OBS. Não confunda as senhas. A senha solicitada pelo sudo é do usuário conectividade.
 3. Altere o usuário logado para convidado:
 - `su convidado`
 4. Verifique se ele consegue:
 - ler o arquivo: `cat teste.sh`
 - executar o arquivo: `./testes.sh`
 - apagar o arquivo: `rm teste.sh`
 - renomear o arquivo: `mv teste.sh teste2.sh`
- **PERGUNTA 3:**
 - Explique os resultados do passo 4 analisando as permissões do arquivo com `ls -l teste.sh`.

Exercício 4: Permissões em Pastas

1. OBS. Para voltar ao usuário conectividade digite exit
2. Crie a estrutura de pastas com os comandos ao lado:
3. Mude o usuário novamente para convidado e verifique se ele consegue:
 - copiar o arquivo teste.sh para a pasta privada: cp ../teste.sh publico/teste2.sh
 - copiar o arquivo teste.sh para a pasta publica: cp ../teste.sh privado/teste2.sh
 - executar o arquivo teste.sh na pasta pública: cd publico e ./teste.sh

```
mkdir arquivos
cd arquivos
mkdir publico
mkdir privado
cp ../teste.sh publico/teste.sh
chmod u=rwx,g=rx,o=r privado
chmod -R g+rx publico
ls -l
sudo adduser convidado conectividade
id convidado
```

- **PERGUNTA 4:**

- Explique os resultados do passo 3 analisando as informações do usuário convidado (**id convidado**) e as permissões das pastas obtidas com **ls -l**.

Entrega do TDE

- Responda as quatro perguntas e entregue apenas o relatório