# Permissões de arquivo no Linux

## Descrição do projeto

Através de comandos Linux, foram realizadas alterações nas permissões de arquivos e diretórios no ambiente de trabalho do usuário researcher2. O objetivo era ajustar as permissões de acesso para garantir maior segurança e controle sobre os dados armazenados no diretório projects.

## Verifique os detalhes do arquivo e do diretório

Para identificar as permissões e outros detalhes dos arquivos e diretórios no sistema, utilizei o comando ls com a opção -la. Essa opção lista os conteúdos do diretório de forma detalhada, incluindo arquivos ocultos.

researcher2@0e5ba9455086:~$ ls

projects

researcher2@0e5ba9455086:~$ cd projects/

researcher2@0e5ba9455086:~/projects$ ls -la

total 32

drwxr-xr-x 3 researcher2 research\_team 4096 Nov 20 22:33 .

drwxr-xr-x 3 researcher2 research\_team 4096 Nov 20 23:01 ..

-rw--w---- 1 researcher2 research\_team 46 Nov 20 22:33 .project\_x.txt

drwx--x--- 2 researcher2 research\_team 4096 Nov 20 22:33 drafts

-rw-rw-rw- 1 researcher2 research\_team 46 Nov 20 22:33 project\_k.txt

-rw-r----- 1 researcher2 research\_team 46 Nov 20 22:33 project\_m.txt

-rw-rw-r-- 1 researcher2 research\_team 46 Nov 20 22:33 project\_r.txt

-rw-rw-r-- 1 researcher2 research\_team 46 Nov 20 22:33 project\_t.txt

## Descreva a sequência de permissões

Os 10 caracteres que indicam as permissões de um arquivo podem ser interpretados da seguinte forma:

1. **Primeiro caractere:** Indica o tipo (ex.: d para diretórios, - para arquivos regulares).
2. **Próximos três caracteres:** Representam as permissões de **leitura** (r), **escrita** (w) e **execução** (x) para o **usuário** proprietário.
3. **Três caracteres seguintes:** Representam as permissões de leitura, escrita e execução para o **grupo**.
4. **Últimos três caracteres:** Representam as permissões de leitura, escrita e execução para **outros**.

Por exemplo, o arquivo project\_k.txt tinha inicialmente a string de permissões -rw-rw-rw-. Isso significa que:

* **Usuário, grupo e outros** tinham permissão para **ler** (r) e **escrever** (w), mas ninguém tinha permissão de **execução** (x).

## Alterar permissões de arquivo

O próximo passo foi ajustar as permissões dos arquivos para atender às políticas de segurança definidas. Utilizei o comando chmod para realizar as alterações necessárias.

**Atualizar permissões do arquivo project\_k.txt**

researcher2@0e5ba9455086:~/projects$ chmod 664 project\_k.txt

researcher2@0e5ba9455086:~/projects$ ls -l

total 20

drwx--x--- 2 researcher2 research\_team 4096 Nov 20 22:33 drafts

-rw-rw-r-- 1 researcher2 research\_team 46 Nov 20 22:33 project\_k.txt

Aqui, removi as permissões de escrita para outros. Após a alteração, o arquivo passou a ter permissões -rw-rw-r--.

**Exemplo 2: Atualizar permissões do arquivo project\_m.txt**

researcher2@0e5ba9455086:~/projects$ chmod 600 project\_m.txt

researcher2@0e5ba9455086:~/projects$ ls -l

total 20

-rw------- 1 researcher2 research\_team 46 Nov 20 22:33 project\_m.txt

Nesse caso, removi todas as permissões de grupo e outros, deixando o arquivo acessível apenas pelo usuário proprietário.

## Alterar permissões de arquivo em um arquivo oculto

Foi solicitado que o arquivo oculto .project\_x.txt fosse configurado para leitura apenas para o usuário e o grupo, removendo todas as permissões de outros.

researcher2@0e5ba9455086:~/projects$ chmod 440 .project\_x.txt researcher2@0e5ba9455086:~/projects$ ls -la

-r--r----- 1 researcher2 research\_team 46 Nov 20 22:33 .project\_x.txt

## Alterar permissões de diretório

Por fim, as permissões do diretório drafts foram ajustadas para garantir que apenas o usuário proprietário tivesse acesso completo.

researcher2@0e5ba9455086:~/projects$ chmod 700 drafts researcher2@0e5ba9455086:~/projects$ ls -l

drwx------ 2 researcher2 research\_team 4096 Nov 20 22:33 drafts

## Resumo

Utilizando os comandos do Linux, foi possível verificar e atualizar as permissões dos arquivos e diretórios no diretório **projects**, atendendo às políticas de segurança definidas. A análise inicial foi realizada com o comando ls -la, e as alterações foram aplicadas utilizando chmod. Isso garantiu que os arquivos e diretórios estivessem protegidos de acessos não autorizados.