Técnico em redes de computadores
UC3

Explicação: CHMOD

O comando chmod - Change Mode no Linux é usado para alterar as permissões de arquivos e diretórios. A importância das permissões configuradas é que podemos controlar quem poderá ler, escrever e executar um arquivo ou diretório em nosso servidor.

Imagine o seguinte cenário:

Temos diversos arquivos e diretórios que serão acessado por diversas pessoas com conhecimentos e setores diferentes, termos que configurá-los tanto arquivos e diretórios para determinar quem pode acessar e o que fazer com eles.

A configuração incorreta destes itens poderão causar um enorme prejuízo para a empresa e com certeza para o seu emprego também.

Dicas importantes:

Quando for responsável pela implantação deste tipo de servidor.

1 – Nunca realize os procedimentos diretamente no servidor em uso.

2 – Não acredite que é dono da razão e que não comete erros, teste quantas vezes forem necessários.

3 – Para garantir que esta tudo certo, solicite a outros da equipe ou não, que teste a funcionalidade do item implantado.

4 – Assim que implantado, execute um backup com maior frequência

1 – Criar diretórios e usuários para mudar permissões.

Iniciar o servidor srv_debian11

Criar o diretório senac.

```
mkdir /var/senac
```

Criar o diretório secretaria dentro do diretório senac.

```
mkdir /var/senac/secretaria
```

2 – Criando diversos outros diretórios.

Criar dentro de senac;

secretaria,

biblioteca,

enfermaria,

fotografia,

coordenacao,

ead e lab.

Listar o conteúdo: ls /var/senac

3 – Montar diretório dentro de outro existente.

mkdir lab/suporte = erro

cd /var/senac enter

ls

mkdir lab/suporte enter

4 - Montar diretório dentro de outro existente.

Exemplo.

Sair do diretório atual.

cd ..

mkdir lab teste

ls

Ele criou um diretório no diretório senac e não dentro do lab

Remover o diretório teste; rmdir teste

5 - Montar diretório dentro de outro inexistente.

mkdir -p secretaria/pagamentos

Para verificar os usuários do sistema

cat /etc/passwd

6 – Verificar os grupos ao criar e depois de apagar.

Vamos criar um grupo; addgroup computador

Exibir o grupo criado; cat /etc/group

Remover o grupo criado; groupdel computador

Exibir o grupo apagado; cat /etc/group

Digitar: cd /

7 – Listar permissões e verificar suas estruturas.

Listar as permissões dos diretórios; ls -lh ou ls –l

drwxr-xr-x 2 root root 4096 fev 20 10:17 Downloads

O primeiro item.

d = representa um diretório

- = representa um arquivo

L = representa um link simbólico (como se fosse um atalho de um arquivo ou pasta).

8 – Permissões correspondentes após a primeira letra.

d rwx r-x r-x

As 3 primeiras são permissões ao usuário dono deste arquivo ou pasta.

As 3 seguintes são permissões do grupo.

As 3 últimas são permissões para todos os outros.

9 – Significado de cada letra do conjunto (rwx).

r = read - Permissão de leitura e visualização do arquivo ou pasta

w - write - Permissão de escrita, podendo modificar ou alterar o arquivo ou diretório.

x - execute - um arquivo com esta permissão pode ser tratado com um programa dentro do sistema linux. Ex: script

10 – Entendendo as permissões da estrutura.

d 1º(rwx) 2º(r-x) 3º(r-x)

O 1º grupo de letras informam que o usuário dono pode ler, escrever e executar o arquivo ou pasta.

O 2º grupo de letras informam que o grupo pode ler, não pode escrever, ou seja, não pode modificar e pode executar o arquivo ou pasta.

11 – Entendendo as permissões da estrutura.

d 1º(rwx) 2º(r-x) 3º(r-x)

O 3º grupo de letras informam que o todos os outros pode ler, não pode escrever, ou seja, não pode modificar e pode executar o arquivo ou pasta.

O traço - significa que temos uma permissão negada.

12 - Convertendo as letras para números binários.

rwx r-x r-x

111 101 101

Convertendo número binários para decimais teríamos;

111= 7 101= 5 101= 5

13 – Verificando a tabela completa.

Permissão	Binário	Decimal
---	000	0
--x	001	1
-w-	010	2
-wx	011	3
r--	100	4
r-x	101	5
rw-	110	6
rwx	111	7

14 – Utilizando o comando CHMOD.

Criar um arquivo com o seu nome traço linux.

touch juscelino-linux

ls -l

Obs.: Não remover, mas se fosse remover o arquivo.

rm juscelino-linux

15 – Quais a permissões do arquivo criado.

Como padrão por motivo de segurança ele vem da seguinte forma;

- rw- r-- r--

No primeiro bloco

rw- = leitura, escrita e não execução por segurança para o dono.

No segundo e terceiro bloco.

r-- = Permissão de leitura e negação de escrita e execução para os grupos ou os outros.

16 - Direito a todos de execução do arquivo.

chmod +x juscelino-linux

ls -l

- rwx r-x r-x

Tirar o direito de todos executar o arquivo.

chmod -x juscelino-linux

ls -l

17 – Alterando local específico.

Devemos acrescentar as letras;

u = user

g = group

o = other

18 – Alterando local específico.

chmod u+x juscelino-linux para alterar o direito a executar do dono.

chmod g+x juscelino-linux para alterar o direito a executar do grupo.

chmod o+x juscelino-linux para alterar o direito a executar dos outros.

Para alterar a escrita ou leitura basta substituir a letra x.

chmod u+r ou u+w e o nome do arquivo.

19 – Usando através da tabela decimal.

Comando;

chmod 775 juscelino-linux

ls -l

- rwx rwx r-x

Dono total, grupos total e outros sem permissão de escrita.

20 – Calcular permissões pelo site.

No site abaixo, conseguimos de forma fácil calcular os resultados de permissão que desejamos para o arquivo ou pasta.

https://chmod-calculator.com/

Testar o site de diversas formas.

Fazer alteração diversas nas pastas que criamos.

21 – Verificação de dados de usuário e grupos .

Verificar os dados de qualquer usuário.

```
id juscelino
```

Para verificar os usuário criados.

```
cat /etc/passwd
```

Verificar os grupos criados.

```
cat /etc/group
```

Atividade:

No servidor srv-debian11

Realizar os procedimentos da tabela a seguir

Dentro do diretório na raiz chamado: jnminfo

Simular criação de uma estrutura de grupos e usuários.

Criar primeiro os grupos que serão associados aos departamentos da empresa, depois os usuários vinculados a eles.

Diretorios	Grupo principal	grupo secundário	usuários
ead	ead	empresa	joana, suely e marcia
Secretaria	Secretaria		carlos, mauro e jairo
coordenacao	coordenacao		silvana, samantha e luzia
biblioteca	biblioteca		Davi, Laura e Bernardo
enfermaria	enfermaria	empresa	Gabriel, Joaquim e Lorenzo
fotografia	fotografia		Miguel, Cecilia, Eloa
lab	lab	empresa	Helena, Laura e Luisa

Regras referentes ao acesso nos diretórios.

Grupo principal: dono total, grupo ler e escreve, outros somente ler.

Grupo secundário: dono tem direito total, grupo e outros somente de ler.

33 – Exemplo para facilitar a criação.

Exemplo para adicionar grupo
addgroup churrasco

Criando usuários e inserindo aos grupos.
adduser virginia --ingroup futebol
Nome completo;
Sala;
telefone;
fone;
outros;
S ou N;
adduser virginia ginastica