Curitiba, 23, março de 2024.

**Disciplina**: Administração de Sistemas Linux

**Professor:** Jhonatan Geremias

**Estudante: Marcos Vinicius Maximo da SIlva**

**Atividade Prática / Relatório 2**

**Sistemas de Arquivos e Permissões no Linux**

# **Descrição da Atividade:**

Nesta atividade, os estudantes irão explorar e aprender sobre os sistemas de arquivos e o gerenciamento de permissões no ambiente Linux. Como pré-requisito para esta atividade, o estudante deve ter acesso a uma máquina com o sistema operacional Linux.

**Especificação:**

Esta atividade consiste na leitura do material de apoio e na realização da atividade práticas/teóricas. A atividade está estruturada em duas etapas, primeiramente visa explorar os comandos para manipular os sistemas de arquivos no Linux, na sequência focamos no gerenciamento de permissões no Linux. Ao longo da atividade o estudante deve coletar os *printscreens* contendo todos os comandos solicitados para gerar seu relatório. Para auxiliar o estudante no desenvolvimento da atividade está sendo disponibilizado os links abaixo.

[Guia Foca - Linux](https://www.guiafoca.org/#download)

[Documentação Ubuntu](https://help.ubuntu.com/)

**Entrega:**

Esta atividade deverá ser realizada individual, entregue no Canvas até o dia **31/03/2024** (data prevista para o último encontro deste módulo).

Atenção: As atividades além de compor a nota do estudante serão utilizadas para contabilizar a presença da disciplina.

**Atividade 1 – Sistema de Arquivos Linux**

1. Inicie a máquina virtual Linux.
2. Abra um terminal no sistema operacional Linux.
3. Verifique a lista de discos rígidos atualmente disponíveis (utilizar o comando fdisk -l). Executar o comando com privilégios de “sudo”
4. Efetue um *printscreen* contendo cada um dos discos (caso necessário adicionar mais de *printscreen*).

Texto

Descrição gerada automaticamente

1. Analisando a saída do comando “fdisk -l”, quantos discos e partições você possui nesta máquina virtual?

**Discos:**

/dev/loop0

/dev/loop1

/dev/loop2

/dev/loop3

/dev/loop4

/dev/loop5

/dev/loop6

/dev/loop7

/dev/vda

**Partições:**

/dev/vda1

/dev/vda2

/dev/vda3

Há 9 discos e 3 partições.

1. Execute o comando “df -h”.
2. Efetue um *printscreen* com a saída do comando*.*Texto

   Descrição gerada automaticamente com confiança média
3. Descreva para que é utilizado o comando “df -h”.

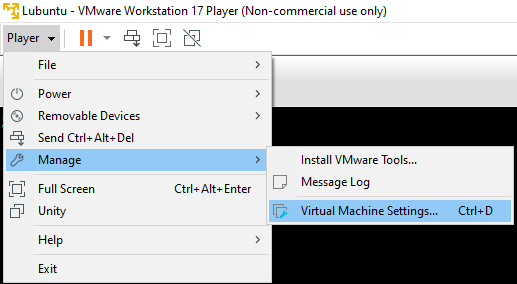
É usado para exibir informações sobre o espaço em disco disponível em cada sistema de arquivos montado no sistema.

1. Execute o comando “blkid”. Executar o comando com privilégios de “sudo”.
2. Efetue um *printscreen* com a saída do comando*.* Texto

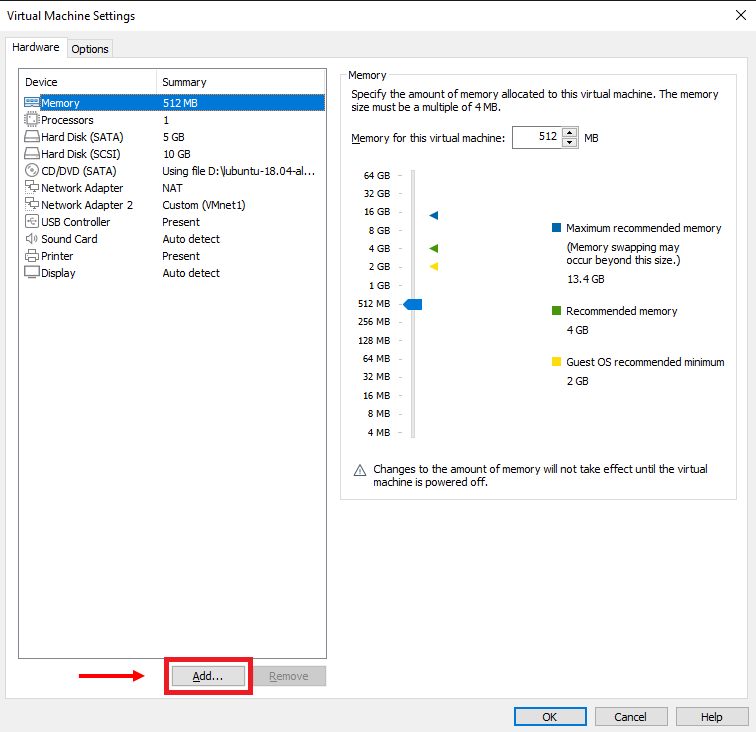
   Descrição gerada automaticamente
3. Analisando a saída do comando “blkid”, qual o tipo de sistema de arquivos utilizado para /dev/sda1?

O tipo de sistema de arquivos utilizado para /dev/vda1 é "vfat".

1. Adicione um novo disco na máquina virtual.
   1. Para o VMWare Player, acessar as configurações da máquina virtual.



* 1. Adicione um novo dispositivo de hardware, clique na opção “Add...”.

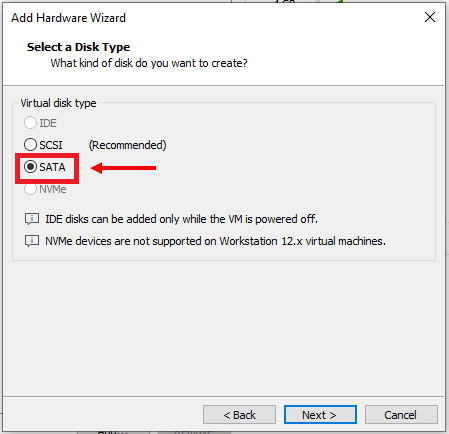


* 1. Selecionar a opção “Hard Disk” e clicar em “Next”.

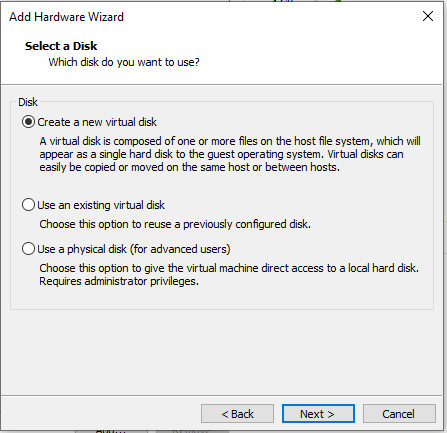
Interface gráfica do usuário

Descrição gerada automaticamente

* 1. Selecionar o tipo da tecnologia do disco rígido “SATA”.



* 1. Selecionar a opção “Create a new virtual disk” e clicar em “Next”.



* 1. Definir um tamanho para o disco, então clicar em “Next”.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

* 1. Definir o nome para o disco, o ideal é deixar o nome fornecido por *default*, então clicar em “Finish”.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

* 1. Nas configurações da máquina virtual clicar em “Ok” e retornar para máquina virtual

1. Crie a tabela de partição para o novo disco fornecido.
2. Utilizar a ferramenta gparted.
   1. A tabela de partição deve ser definida como GPT.
   2. Adicionar o *printscreen* do procedimento acima.

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

* 1. A ferramenta deve ser executada com privilégios de “sudo”.

1. Formate o novo disco com o sistema de arquivo ext4.
2. Execute o comando “blkid”. Executar o comando com privilégios de “sudo”.
3. Efetue um *printscreen* com a saída do comando*.*Texto

   Descrição gerada automaticamente
4. Verifique se o novo disco foi adicionado.
5. Crie um diretório com o seu nome no diretório “/”
   1. Ex: mkdir /jhonatan
6. Agora você deve montar a partição do novo disco no diretório com o seu nome, utilizar o comando “mount”.
7. Execute o comando “df -h”.
8. Efetue um *printscreen* com a saída do comando*.*

Texto

Descrição gerada automaticamente

1. Acesse a partição e crie um arquivo dentro, “arquivo.txt”.
2. Desmontar a partição utilizando o comando umount.
3. Execute o comando “df -h”.
4. Efetue um *printscreen* com a saída do comando*.*

Texto

Descrição gerada automaticamente

1. Abaixo forneça a entrada necessária que deve ser adicionada no arquivo /etc/fstab para montar o disco automaticamente.
   1. Forneça apenas a entrada conforme a sua configuração.
   2. Como esta configuração se não for realizada corretamente pode gerar problema na inicialização não é necessário executar ela na prática.

**Atenção**: Nos itens 4, 9 e 13, você deve executar o comando com privilégios de “sudo”.

**Material de Apoio – Permissões Básicas Linux**

As permissões básicas no Linux são: leitura, escrita e execução. Tais permissões são concedidas aos usuários considerando três blocos, proprietário, grupo e outros. As permissões são definidas na figura abaixo:



Para alterar as permissões básicas no Linux utilizamos o comando chmod, este comando pode ser utilizado de forma nominal ou por representação binária. A proposta desta atividade consiste em demostrar como definir as permissões no Linux utilizando a máscara binária. Segue a sintaxe do comando chmod:

chmod <máscara> <objeto>

Para alterar as permissões de um objeto (arquivo ou diretório) é necessário ter privilégios sobre ele. Assim, para obter os privilégios de superusuário podemos utilizar o comando “sudo” antecedendo o comando que queremos executar, este comando vai fornecer os privilégios necessários, será solicitado que você forneça a senha do usuário para elevar os privilégios.

sudo chmod <máscara> <objeto>

Para modificar as permissões utilizando a representação binária você deve atribuir a nova permissão utilizando uma máscara numérica. Basicamente, a máscara é composta por três dígitos consecutivos (ex.: 000). Nesta máscara cada dígito deve ser considerado individualmente. O primeiro dígito refere-se a permissão do usuário ([**0**]00), na sequência o próximo dígito é utilizado para definir a permissão do grupo (0[**0**]0) e o último dígito é utilizado para definir a permissão de outros (00[**0**]).

A representação da máscara binária é apresentada na tabela abaixo, deve-se utilizar o valor decimal na permissão desejada:

|  |  |  |
| --- | --- | --- |
| 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 |

Deste modo, você define as permissões de maneira individual para cada um dos dígitos, atribuindo o valor decimal. Por exemplo, se você quer definir o usuário com permissão de leitura, escrita e execução o primeiro dígito deve receber o valor 7; definir o grupo com permissão de leitura e execução o segundo dígito deve receber o valor 5; definir outros com a permissão de leitura o terceiro dígito deve receber o valor 4. Assim, como resultado teremos uma máscara formada pela sequência desses números, ou seja 754, esta máscara deve ser utilizada com o comando chmod.

chmod 754 arquivo.txt

A maneira mais simples de você recordar como aplicar essas permissões é lembrar o valor das três permissões básicas de leitura, escrita e execução. Para o valor da permissão de execução é 1, a escrita é o seu dobro, tem o valor é 2, e a leitura é o seu dobro temos o valor é 4. Diante disto, é só somar o valor que você precisa. Por exemplo a permissão anterior: usuário com permissão de leitura=4, escrita=2 e execução=2, é só somar os valores das permissões 4+2+1=7, aqui temos a permissão do usuário; grupo com permissão de leitura=4 e execução=1, é só somar os valores 4 + 1 = 5; por fim a permissão para outros como a permissão é apenas permissão de leitura adicionamos apenas o valor 4. Assim, como resultado teremos a mesma máscara formada pela sequência desses números, ou seja 754.

Então, para reforçar vamos utilizar um segundo exemplo: usuário com permissão de escrita e execução; grupo com permissão de leitura e execução, outros com permissão de leitura e escrita.

* Usuário: escrita (2) e execução (1), 2 + 1 = **3**;
* Grupo: leitura (4) e execução (1), 4 + 1 = **5**;
* Outros: leitura (4) e escrita (2), 4 + 2 = **6**;

Assim, como resultado teremos uma máscara formada pela sequência desses números, ou seja 356, esta máscara deve ser utilizada com o comando chmod.

chmod 356 arquivo.txt

**Atividade 2 – Permissões Representação Binária:**

1. Verifique qual o seu diretório corrente.
2. Acesse o diretório home do usuário. (cd ~)
3. Crie o diretório “lnx\_pasta”.
4. Acesse o diretório “lnx\_pasta”.
5. Crie os arquivos “arquivo1.txt”, “arquivo2.txt” e “arquivo3.txt”.
6. Liste os arquivos e diretórios e verifique as permissões concedidas.
7. Adicione a permissões no arquivo “arquivo1.txt”, usuário: escrita e execução; grupo: leitura e escrita, outros: leitura. (Utilizar a representação binária).
8. Adicione a permissões no arquivo “arquivo2.txt”, usuário: leitura e execução; grupo: leitura; outros: sem nenhuma permissão. (Utilizar a representação binária).
9. Adicione a permissões no arquivo “arquivo3.txt”, usuário: leitura e escrita; grupo: leitura e execução, outros: execução. (Utilizar a representação binária).
10. Adicione a permissões no diretório “lnx\_pasta”, usuário: leitura, escrita e execução; grupo: leitura e escrita, outros: execução. (Utilizar a representação binária).
11. Liste os arquivos e diretórios e verifique as permissões concedidas.
12. Efetue um *printscreen* contendo todos os comandos anteriores para compor seu relatório.

Interface gráfica do usuário, Texto

Descrição gerada automaticamente com confiança médiaTexto

Descrição gerada automaticamente

**Alterar o Proprietário e Grupo do Objeto**

Para alterar o proprietário e grupo de um objeto (diretório e arquivo) é utilizado o comando chown. Segue a sintaxe do comando:

chown <usuário>:<grupo> <objeto>

Antes de efetivamente utilizar o comando chown, vou mostrar outros dois outros comandos um para criar um usuário e outro comando para criar um outro grupo.

useradd <usuário>

Como exemplo, vamos criar um usuário “user\_ctic”:

useradd user\_ctic

Por sua vez, o comando para criar um grupo é groudadd. Segue a sintaxe do comando:

groupadd <grupo>

Como exemplo, vamos criar um grupo “grupo\_ctic”:

groupadd grupo\_ctic

Agora sim, vamos utilizar o comando chown para modificar o proprietário de um arquivo:

chown user\_ctic:grupo\_ctic arquivo1.txt

Para modificar o proprietário de um diretório a sintaxe é a mesma, acrescenta-se apenas a opção de recursividade:

chown -R user\_ctic:grupo\_ctic pasta1

**Atividade 3 - Modificar Proprietário/Grupo:**

1. Verifique qual o seu diretório corrente.
2. Acesse o diretório home do usuário. (cd ~)
3. Acesse o diretório “lnx\_pasta”.
4. Liste os arquivos e diretórios e verifique o proprietário do arquivo.
5. Crie um usuário chamado user\_lnx.
6. Crie um grupo chamado grupo\_lnx.
7. Altere o proprietário do arquivo “arquivo1.txt” para “user\_lnx” e grupo para “grupo\_lnx”.
8. Altere o proprietário do diretório “lnx\_pasta” para “user\_lnx” e grupo para “grupo\_lnx”.
9. Liste os arquivos e diretórios e verifique o proprietário do arquivo.
10. Efetue um printscreen contendo todos os comandos anteriores para compor seu relatório.Texto

    Descrição gerada automaticamenteUma imagem contendo Interface gráfica do usuário

    Descrição gerada automaticamenteTexto

    Descrição gerada automaticamente

**Atenção:** No item 10 é necessário que no *printscreen* os comandos estejam legíveis.