Estratégia CONCURSOS

Aula 00 (Prof. Celson unior)

Sistemas Operacionais p/ UFPE (Técnico de Tecnologia da Informação/Sistemas) - Pós-Edital

Professor: Celson Carlos Martins Junior, Diego Carvalho, Equipe Informática e TI

Esclarecimentos Iniciais 3
1 – Sistema Operacional Linux 5
1.1 Conceitos iniciais 6
1.2 Características do Linux 9
1.3 Interface Gráfica 10
1.4 Resolução de questões 11
2 – Gerenciamento Linux 19
2.1 Gerenciamento de Processos 19
2.2 Processos em background 21
2.3 Gerenciamento de Pacotes 23
2.4 Gerenciamento de Usuários 25
2.5 Gerenciamento de Dispositivos 29
2.6 Gerenciamento de Rede 33
2.7 Resolução de Questões 34
3 – Sistemas de Arquivos Linux 52
3.1 Permissões de Acesso 54
3.2 Permissões Especiais 56
3.3 Arquivos e diretórios Linux 56
3.4 Ext 59
3.5 NFS 60
3.6 Logical Volume Manager 61
3.7 Resolução de questões 63
4 – Comandos de Linha Linux 87
4.1 Shell Linux 87
4.2 Navegação em diretórios Linux 88
4.3 Manipulação de Arquivos Linux 89
4.4 Shell Script Linux 95
4.5 Resolução de questões 96
5 – Gerenciamento de Serviços Linux 119

5.1 Serviços de Rede 119
5.2 NIS 122
5.3 DHCP 123
5.4 SMB/CIFS 124
5.5 Segurança Linux 126
5.6 Resolução de Questões 129
6.0 Gabarito 134

ESCLARECIMENTOS INICIAIS

Pessoal, o objetivo desta aula é entendermos os conceitos e noções básicas de administração de sistemas Linux.

Este assunto tem tido presença quase certa nas últimas provas da banca, portanto seu entendimento é essencial.

Nessa aula, resolveremos muitas questões, incluindo questões recentes da banca sobre o tópico desta aula.

Pessoal, antes de iniciar nosso assunto propriamente dito, precisamos esclarecer alguns pontos.

Nossa abordagem será **descritiva**, ou seja, iremos conhecer o Linux descrevendo suas principais funcionalidades e características, sempre recorrendo às questões de concursos para nos balizar.

Além de entender as noções básicas, um dos nossos objetivos é auxiliá-los a identificar o "modus operandi" da banca e verificar quais conceitos são mais abordados.

Atenção, como não há questões suficientes de apenas uma banca para cobrir todos os tópicos previstos no edital, iremos nos valer de questões de diversas bancas.

Para facilitar nossa vida, no decorrer do texto, os conceitos preferidos da banca foram acompanhados com um dos logos do Estratégia abaixo:





Nosso objeto de estudo é o sistema operacional Linux, com foco em suas características principais. Iremos abordar: suas **funções principais**, **gerenciamento**; **sistemas de arquivos**; **comandos de linha**.

Precisamos destacar que são valiosas fontes de auxílio as páginas de manual (manpages) do próprio sistema Linux e o Guia Foca GNU/Linux (http://www.guiafoca.org).

Recomendamos que em caso de dúvidas sobre algum ponto não abrangido no curso, recorram a estes recursos.

Um ponto de ressalva, é que os editais possivelmente por vezes podem prever distribuições Linux específicas.

Em função disto, também abordaremos alguns tópicos relativos à distribuição Linux **Red Hat Enterprise Linux**. Basearemos os tópicos específicos sobre Red Hat no site da distribuição, e em materiais de elaboração da própria fabricante.

Apesar disso, a expectativa é que o examinador aborde tópicos mais genéricos, ok?

Para padronizar nosso entendimento, os comandos serão exibidos no seguinte formato:

```
#
```

Os utilitários e arquivos de configuração serão citados em ***negrito e itálico***, no seguinte formato: ***/caminho/utilitário***

Sem mais delongas, vamos a nossa aula, Ok. ☺ Mas, antes de iniciar nosso assunto propriamente dito, precisamos esclarecer alguns pontos.

1 – Sistema Operacional Linux

Pessoal, um Sistema Operacional é um conjunto de softwares cujo objetivo é facilitar o uso dos recursos de um sistema computacional. Um Sistema Operacional possui um conjunto de funções nobres reservadas ao seu núcleo, chamado kernel.

Como veremos na nossa aula, a grande maioria dos conceitos atinentes a Sistemas Operacionais também se aplicam quando estamos falando do Linux.

O Linux tanto pode ser visto puramente como um Sistema Operacional, ou como uma plataforma, haja vista sua imensa versatilidade.

O Linux se originou dos sistemas Unix, e deles herdou várias características. O Unix é um sistema operacional comercial multiusuário e multitarefa, disponível para diversas plataformas.

E você pode me perguntar: professor, qual a importância de saber essa descendência do Linux? Respondo com toda a franqueza: pessoal, o Linux e os Unix´s permanecem presentes em vários ambientes computacionais importantes. Compreender bem sistemas Linux é um passo para compreender Unix, e vice-versa.

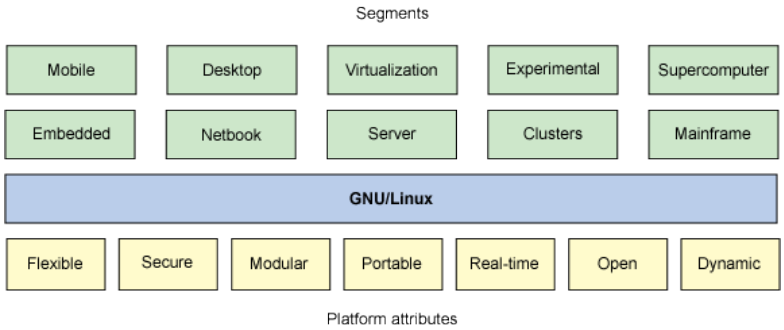
A proposta do Linux é oferecer todas as funcionalidades de um Unix, porém a um menor custo. Seu licenciamento é feito sob uma licença opensource, a GPL (GNU Public License), o que significa que seu código fonte pode ser adaptado e redistribuído, desde que sejam observados os termos desta licença.

Podemos encontrar o Linux em várias áreas da computação como em desktops, notebooks, servidores, clusters, mainframes, supercomputadores, portáteis, tablets, soluções de virtualização, etc.

Em virtude dessa heterogeneidade de plataformas em que o Linux pode ser utilizado, foi estabelecido um padrão chamado **Linux Standard Base** (LSB) para padronizar as diversas distribuições Linux, de forma a permitir que um software desenvolvido para uma distribuição possa ser compatível com as demais. Podemos dizer que as várias distribuições do Linux são interoperáveis em virtude do LSB, para integração com outros o Linux dispões de outros recursos.

1.1 CONCEITOS INICIAIS

O sistema operacional Linux é composto por um kernel e uma coleção de aplicativos de usuário (como bibliotecas, gerenciadores de janela e aplicativos), como a figura abaixo exemplifica.

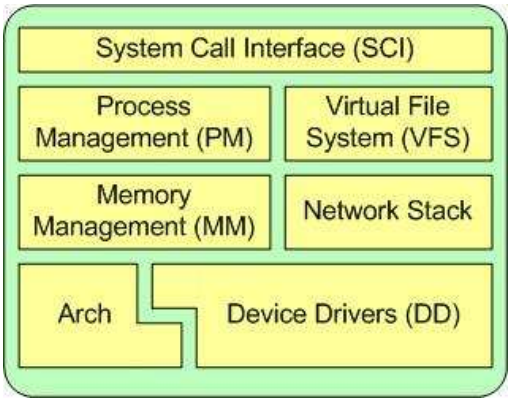


O **Kernel é o núcleo do Linux**, é a parte mais próxima ao hardware e responsável por lidar com sua complexidade e diversidade. Ele possibilita intermediar a comunicação entre aplicações e usuários, lidar com os dispositivos e processos, gerenciar os recursos como memória e disco, entre outros.

Outra importante característica do Linux é o fato de ele ser **multitarefa**. Vários programas/processos podem ser executados simultaneamente, e o kernel do Linux se encarrega de garantir recursos adequados para sua execução.

Linux é um sistema **multiusuário** e suporta conexões simultâneas de diversos usuários, diretamente ou por terminais virtuais. É possível maximizar a utilização da capacidade de processamento e armazenamento das informações. Para tanto, o Linux possui recursos de segurança para permitir o isolamento das atividades de cada usuário.

Vamos agora olhar o Linux sob a perspectiva de seus componentes, para entender melhor seu funcionamento. A figura abaixo exemplifica, em alto nível, as partes principais da arquitetura do Linux.



A **System Call Interface** (SCI) é uma camada que fornece os meios para que usuários realizem chamadas de função. As chamadas de sistema são meios de comunicação dos processos com o núcleo do Linux. As chamadas de sistema permitem aos programas dos usuários a passagem do controle da execução para o sistema operacional.

O Linux é focado no Gerenciamento de processos e na execução de processos. O kernel do Linux realiza o gerenciamento de recursos; por exemplo, se o recurso é memória ou dispositivo de hardware, o kernel gerencia e arbitra o acesso ao recurso entre vários processos concorrentes. Nesse aspecto, temos que recordar dos conceitos de gerenciamento de processos que vimos nas aulas anteriores.

Outro recurso importante que é gerenciado pelo kernel do Linux é a memória. O Linux inclui os meios para **gerenciar a memória** disponível, bem como os mecanismos de memória virtual.

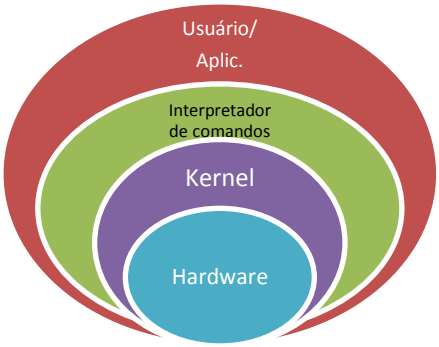
O **sistema de arquivos virtual** (VFS) é outro aspecto relevante do kernel do Linux, porque fornece uma interface de abstração comum para sistemas de arquivos. O VFS fornece uma camada de comunicação entre a Interface de Chamada de Sistema e os diversos sistemas de arquivos suportados pelo kernel.

A **pilha de rede** do Linux segue uma arquitetura em camadas, modelada independentemente dos próprios protocolos, e fornece uma interface para uma variedade de protocolos de rede, permitindo gerenciar conexões e mover dados entre terminais, de maneira padronizada.

Em virtude de o Linux ter como propósito ser multiplataforma, ele dispõe de uma imensa variedade de drivers de dispositivos, nativos no código-fonte do kernel do Linux, o que torna o sistema mais flexível para suportar uma grande diversidade de dispositivos de hardware.

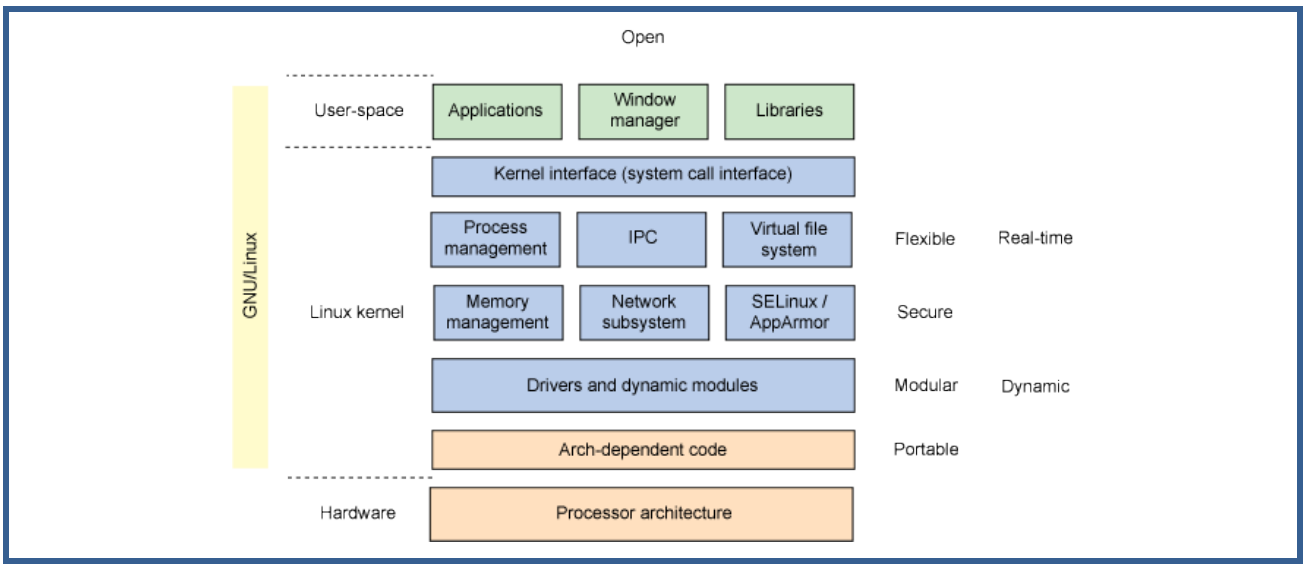
TOME NOTA!

Somando-se a essas características, precisamos saber que a **arquitetura do Linux é divida em camadas**, conforme a figura abaixo. Essa divisão proporciona maior independência do hardware utilizado nesse sistema, entre outras diversas características, que veremos a seguir.



Uma das características primordiais do Linux é sua **modularidade**. Por exemplo, o módulo de driver do kernel Linux suporta que módulos sejam carregados dinamicamente sem afetar o desempenho, permitindo uma plataforma mais *dinâmica*.

A figura abaixo exemplifica a modularidade do Linux, e apresenta as partes principais do sistema.



1.2 CARACTERÍSTICAS DO LINUX



Outras características do Linux são:

✓ **Portabilidade** - o Linux é portável, ou seja, pode ser adaptado facilmente para ser executado em diferentes arquiteturas de hardware. Talvez essa seja a característica mais importante desse Sistema Operacional, que permitiu sua adoção por centenas de fabricantes diferentes e intensificou sua expansão.

✓ **Estrutura hierárquica de diretórios** - o sistema de armazenamento de informações do Linux possui estrutura hierárquica. Grande parte dos sistemas Linux trabalha com FHS. FHS é sigla para **Filesystem Hierarchy Standard** (padrão para sistema de arquivos hierárquico), e define os principais diretórios de um sistema Linux. A estrutura hierárquica facilita a localização e a manipulação de informações.

✓ **Pipelines** - o uso de pipelines ou pipes é um recurso que permite conectar a saída de um comando com a entrada de outro. Essa é uma das mais conhecidas e versáteis características do Linux e é utilizada para a execução de comando ou funções mais complexas, como scripts shell que iremos ver adiante. A figura abaixo dá uma ideia da concatenação de comandos, se usarmos o recurso de pipe para encadear comandos.



✓ **Suporte a sistemas de arquivos externos** de qualquer sistema operacional, permitindo, por exemplo, *flexibilidade* e modularidade.

✓ **Memória virtual** – o Linux trabalha com recursos de memória virtual, permitindo a execução de programas cujo tamanho venha a ser superior à capacidade da memória física. O sistema gerencia a memória, mantendo em memória apenas as partes efetivamente em execução, e as demais em memória virtual.

✓ **Distribuições** – em virtude da diversidade de plataformas e de necessidades, normalmente surgem várias distribuições Linux, com propostas, objetivos, e plataformas distintas. Segundo o site www.distrowatch.org, existem aproximadamente 1.000 distribuições Linux no mundo. Atualmente, as distribuições mais populares são Debian, Ubuntu, Red Hat Enterprise Linux, CentOS, Fedora, OpenSuse e o sistema operacional Android.

1.3 INTERFACE GRÁFICA

Uma característica peculiar do Linux é que o ambiente gráfico não é parte nativa do kernel. Ele é fornecido por um servidor e gerenciador de janelas.

▪ O servidor de janelas predominante no Linux é X-Window, X11 ou simplesmente X. É ele quem possibilita o emprego de uma interface gráfica, com o conceito de janelas.

X-Window é um **protocolo** padrão para interfaces gráficas nos sistemas Linux. Ele permite acesso remoto e pode ser iniciado através da linha de comandos utilizando, por exemplo, o comando startx.

O servidor X é o programa que provê a interface gráfica para os usuários e permite a execução de programas e aplicações gráficas. O servidor captura as entradas de dados por meio do teclado e do mouse e as relaciona com as respectivas telas gráficas.

Além dessas peculiaridades, outra característica marcante do Linux é que ele permite escolher o gerenciador de desktop que será utilizado. Os gerenciadores **GNOME e KDE** são os mais comumente utilizados, e são bastante semelhantes, ambos se propõem a realizar as mesmas funções e são manipulados de forma bastante semelhante.

O principal objetivo da resolução de questões é, sem dúvida, consolidar o entendimento sobre os conceitos.

Mas além disso, devem ter sempre em mente é que a resolução de questões das bancas

permite observarmos como as bancas abordam os tópicos e quais são os pontos preferidos do examinador.

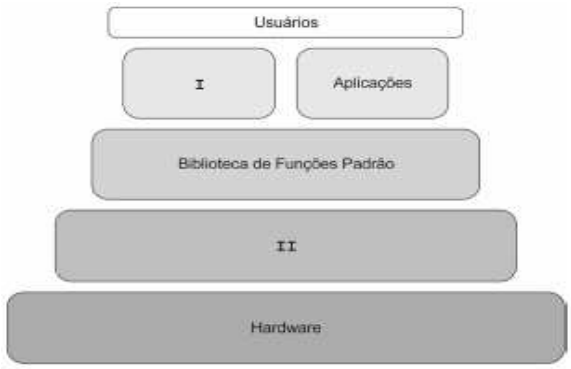
Observar as tendências da banca é muito importante para facilitar e otimizar nossos estudos.



Antes, porém, vamos ao que nos interessa: resolução de questões!!!!

1.4 RESOLUÇÃO DE QUESTÕES

1. **(2017 - FCC - TRF - 5ª REGIÃO - Técnico Judiciário - Informática)** - Considere a figura abaixo que mostra a arquitetura do sistema operacional Linux



a) I representa a camada responsável pela interface entre o hardware e as aplicações. Dentre suas funções encontram-se gerenciamento de I/O, manutenção do sistema de arquivos, gerenciamento de memória e swapping, controle da fila de processos, etc.
b) II representa a camada que permite o acesso a recursos através da execução de chamadas feitas por processos. Tais chamadas são geradas por funções padrão suportadas pelo kernel. Dentre suas funções estão habilitar funções padrão como open, read, write e close e manter a comunicação entre as aplicações e o kernel.
c) I é um processo que executa funções de leitura de comandos de entrada de um terminal, interpreta-os e gera novos processos, sempre que requisitados. É conhecido também como interpretador de comandos.
d) II é um processo que realiza modificações no shell, permitindo que funcionalidades do Linux sejam habilitadas ou desabilitadas, conforme a necessidade. Tal processo gera ganho de performance, pois à medida que customiza o shell, o usuário torna o Linux enxuto e adaptável.

e) I é um processo que realiza modificações no kernel, permitindo que funcionalidades do Linux sejam habilitadas ou desabilitadas, conforme a necessidade. Tal processo gera ganho de performance, pois à medida que customiza o kernel, o usuário torna o Linux enxuto e adaptável.

Comentários:

I representa o **shell** ou interpretador de comandos, processo que executa funções de leitura de comandos de entrada de um terminal, interpreta-os e gera novos processos, sempre que requisitados.
II representa o **kernel**, camada responsável pela interface entre o hardware e as aplicações.

Gabarito: C

---

2. **(FGV - 2014 - SUSAM - Analista de Sistemas)** - Assinale a opção que indica características do sistema operacional Linux.

a) Monousuário, monotarefa e monoplataforma
b) Multiusuário, monotarefa e monoplataforma.
c) Monousuário, multitarefa e monoplataforma.
d) Monousuário, monotarefa e multiplataforma.
e) Multiusuário, multitarefa e multiplataforma.

Comentários:

O Linux é multitarefa. Vários programas/processos podem ser executados simultaneamente, e o kernel do SO se encarrega de garantir recursos de processamento e memória adequados para sua execução.
Linux é um sistema multiusuário, suporta conexões simultâneas de diversos usuários, diretamente ou por terminais virtuais. O Sistema Operacional possui ferramentas de segurança para permitir o isolamento das atividades de cada usuário. Além disso, o Linux permite que cada usuário detenha permissões específicas sobre seus arquivos.
O Linux é portável, ou seja, pode ser adaptado para ser executado em diferentes arquiteturas de hardware. Essa é a característica que permitiu a adoção por centenas de fabricantes diferentes e intensificou a expansão do Linux.

Gabarito: E

---

3. **(2012 - ESAF - MI - Analista de Sistemas)** - As camadas de um sistema Linux são:

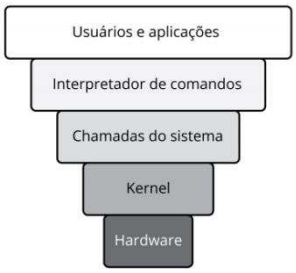
a) usuário, servidor utilitário padrão, biblioteca- padrão, shell Linux, software.
b) usuário, programas utilitários padrão, biblioteca- padrão, sistema operacional Linux, hardware.

c) interface, programas operacionais padrão, biblioteca DDL, sistema operacional Linux, hardware.
d) administrador, servidores e clientes, arquivo-padrão, sistema operacional DMS, hardware.
e) usuário, programas utilitários verificadores, biblioteca da aplicação, arquitetura Linux, software.

Comentários:

Para fins didáticos, a arquitetura do Linux é divida em camadas, conforme a figura abaixo. Na prática, essa divisão não é rígida, sendo considerada uma abstração para facilitar decisões arquiteturais. Essa divisão proporciona maior independência do hardware, entre outras diversas características.

As principais camadas são: usuário e programas, bibliotecas-padrão, sistema operacional Linux (que tem o interpretador de comandos, o kernel e as systems calls como partes), e hardware.



Gabarito: B

---

4. **(ESAF – 2012 - MI - Analista de Sistemas)** - São categorias dos programas utilitários padrão do Linux:

a) comandos para extensão de diretórios para arquivos, filtros de linha, processamento de texto, administração de rede.
b) comandos para manipulação de arquivos e diretórios, filtros, processamento de texto, administração de sistema.
c) comandos para manutenção de programas utilitários, manipuladores de diretórios, armazenamento de texto, administração de sistema.
d) comandos para manipulação do sistema operacional, filtros, processamento de imagens, auditoria de sistema.
e) instruções para manipulação de strings, filtros no domínio da frequência, processamento de texto, operadores de sistema.

Comentários:

O Linux possui uma imensa diversidade de utilitários e comandos de linha, a questão citou algumas categorias. As alternativas A e C estão equivocadas, pois não existem utilitários de comandos para extensão de diretórios para arquivos ou comandos para manutenção de programas utilitários.
Do mesmo modo, a alternativa E não procede, pois não existem utilitários no Linux de filtros no domínio da frequência. A alternativa D pode suscitar dúvidas, mas foi dada como errada pela Banca, que adota o critério da alternativa mais certa.
Os comandos para manipulação de arquivos e diretórios (***cd***, ***ls***, ***mkdir***, entre outros), filtros (pipes |, grep, egrep), processamento de texto (***cat, tac, tail, head)***, administração de sistema são as categorias corretas de utilitários.

Gabarito: B

---

5. **(ESAF – 2012 - MI - Nível Superior)** - A estrutura do núcleo do Linux contém os componentes:

a) E/S, Gerenciador de periféricos, Gerenciador de programa.
b) Gerenciador de TCP/IP, Gerenciador de memória virtual, Gerenciador de processo.
c) E/S, Gerenciador de memória, Gerenciador de processo.
d) E/S, Gerenciador de sinais, Gerenciador de escalonamento de CPU.
e) Gerenciador de sistema operacional, Gerenciador de memória principal, Gerenciador de processador.

Comentários:

O Linux obrigatoriamente deve dispor de recursos para cumprir as tarefas nobres reservadas ao núcleo de um sistema operacional: gerenciador de Entrada e Saída, Gerenciador de memória, Gerenciador de processos. Vimos estes tópicos em nossa aula sobre conceitos de SO, lembram ainda?

Gabarito: C

---

6. **(2012 – ESAF – MDIC - Analista de Comércio Exterior)** - A estrutura do núcleo do Linux contém componentes:

a) De entrada e saída. Gerenciador de memória. Gerenciador de processo.
b) De hardware. Gerenciador de tarefas. Gerenciador de processo.
c) De entrada e saída. Avaliador de memória. Gerenciador de projeto.
d) De entrada e saída. Alocador de memória virtual. Direcionador de processo.

e) De entradas de software. Gerenciador de memória. Multiprocessador.

Comentários:

A banca por vezes se dá ao trabalho de apenas trocar a ordem das alternativas. A questão aborda quais as funções básicas de um sistema operacional. O Linux obrigatoriamente deve dispor de recursos para cumprir as tarefas nobres reservadas ao núcleo de um sistema operacional: gerenciador de Entrada e Saída, Gerenciador de memória, Gerenciador de processos. Nosso gabarito alternativa A.

Gabarito: A

---

7. **(CETAP – 2010 - AL-RR - Analista de Sistemas)** - Nos últimos anos, o sistema Linux tem sido cada vez mais adotado tanto para uso pessoal quanto para uso corporativo. Com relação ao sistema Linux, indique a alternativa CORRETA.

a) O Linux é um sistema operacional, portanto deve funcionar em conjunto com o sistema Microsoft Windows.
b) O acesso às funções do sistema Linux é feito somente através de linhas de comandos.
c) O Linux oferece funcionalidades para gerenciamento e acesso a arquivos, pastas e programas.
d) O Linux é um sistema utilitário para compactação de arquivos no formato ZIP.
e) O Linux é um software proprietário utilizado como alternativa ao Microsoft Word, Excel e Power Point.

Comentários:

Pessoal, o Linux não possui qualquer dependência com outro Sistema operacional. Ele é uma alternativa livre, e possui a grande maioria de aplicativos com fins similares aos encontrados na plataforma Microsoft. O Linux é um Sistema operacional multiusuário, multitarefa e portável. Não há qualquer dependência em seu funcionamento de outros sistemas operacionais, como o Windows, e seu uso pode ser efetivado por linha de comando ou por uma interface gráfica. As alternativas A e B estão equivocadas. Também estão equivocadas as alternativas D e E, o Linux é um Sistema operacional, não é um utilitário de compactação ou uma suite de escritório.
São ofertados aplicativos de gerenciamento e acesso a arquivos ou pastas no Linux, como o Nautilus da Distribuição Ubuntu. Alternativa correta letra C.

Gabarito: C

---

8. **(CESPE – 2009 - PC-RN - Delegado de Polícia)** - O sistema operacional Linux não é

a) capaz de dar suporte a diversos tipos de sistema de arquivos.
b) um sistema monousuário.
c) um sistema multitarefa.
d) capaz de ser compilado de acordo com a necessidade do usuário.
e) capaz de suportar diversos módulos de dispositivos externos.

Comentários:

O Linux é multitarefa. Vários programas/processos podem ser executados simultaneamente, e o kernel do SO se encarrega de garantir recursos de processamento e memória adequados para sua execução.

Linux é um sistema multiusuário, suporta conexões simultâneas de diversos usuários, diretamente ou por terminais virtuais. O Sistema Operacional possui ferramentas de segurança para permitir o isolamento das atividades de cada usuário. Além disso, o Linux permite que cada usuário detenha permissões específicas sobre seus arquivos.

O Linux é portável, ou seja, pode ser adaptado para ser executado em diferentes arquiteturas de hardware. É possível compilá-lo seus códigos fonte para execução em outras plataformas. Ele tem suporte a vários sistemas de arquivos, como Ext2, Ext3, ReiserFs e HFS.

A letra B é a única alternativa equivocada, o Linux é um sistema multiusuário, e não monousuário como afirma o item.

Gabarito: B

---

9. **(2011 - FCC - NOSSA CAIXA DESENVOLVIMENTO - Analista de Sistemas)** - É INCORRETO afirmar que, no GNU/Linux,

a) somente o que é usado durante o processamento é carregado para a memória, que é totalmente liberada logo após a finalização do programa/dispositivo.
b) drivers dos periféricos e recursos do sistema podem ser carregados e removidos completamente da memória RAM a qualquer momento.
c) o suporte é nativo às redes TCP/IP e não depende de camadas intermediárias para funcionar.
d) a cada nova versão do kernel diminui substancialmente a necessidade de se reiniciar o sistema após modificar a configuração de qualquer periférico ou parâmetro de rede.
e) sistemas operacionais como Windows, MacOS, DOS ou outro sistema Linux podem ser executados por meio de sistemas de virtualização, tais como Xen e VMware.

Comentários:

No Linux, somente o que é usado durante o processamento é carregado para a memória, fazendo uso de técnicas modernas de gerenciamento de memória. Os drivers dos dispositivos podem ser carregados e removidos da memória RAM a qualquer momento fazendo uso do comando modeprob, por exemplo. O suporte é nativo às redes TCP/IP. E o Linux, como hospedeiro ou convidado, é totalmente compatível com soluções de virtualização. O erro da alternativa D, é afirmar que necessariamente as novas versões de kernel reduzem a necessidade de reboot do sistema, após a modificação de qualquer periférico**.**

Gabarito: D

---

10. (2013 - ESAF – STN - Analista de Finanças e Controle) - São formas de instalação de programas no Linux:

a) usar um operador para instalar pacotes próprios da edição em uso. Usar programas com instaladores próprios, destinados a funcionar em várias distribuições. Instalar o programa a partir do código- objeto.
b) usar um gerenciador para instalar pacotes próprios da distribuição em uso. Usar programas com instaladores próprios, destinados a funcionar em várias distribuições. Instalar o programa a partir do código-fonte.
c) usar um gerenciador para excluir a distribuição em uso. Usar programas com instaladores proprietários, destinados a funcionar em uma única distribuição. Instalar o programa a partir do código-fonte.
d) usar um gerenciador para instalar pacotes próprios da edição em uso. Usar programas com instaladores proprietários, destinados a restringir a quantidade de distribuições. Instalar o programa a partir do código- fonte.
e) usar um gerenciador para instalar pacotes próprios da distribuição em uso. Usar programas com um instalador genérico, destinados a funcionar em distribuições de mineração de dados. Instalar o programa a partir do código-objeto.

Comentários:

Pessoal, questão simples e introdutória que aborda as possíveis formas de instalação de aplicativos no Linux. A opção correta é a letra B: com **gerenciador de pacotes**, o APT por exemplo; com **instaladores** próprios dos aplicativos; a partir do **código-fonte** (atenção, não é código-objeto).

Gabarito: B

---

11. **(2014 - CESPE - Polícia Federal - Agente de Polícia Federal)** - As rotinas de inicialização GRUB e LILO, utilizadas em diversas distribuições Linux, podem ser acessadas por uma interface de linha de comando.

Comentários:
GRUB e LILO são dois gerenciadores de boot utilizados para configurar a inicialização de um sistema Linux. Ambos podem ser acessados por uma interface de linha de comando.

Gabarito: Certa

---

12. **(2014 - CESPE - TJ-SE - Conhecimentos Básicos - Cargos 3,8)** - No Linux, ambientes gráficos são executados por meio de um servidor, geralmente Xwindows ou X11, o qual fornece os elementos necessários para uma interface gráfica de usuário.

Comentários:
No Linux, podemos fazer uso de dois ambientes para interagir com o sistema operacional: o ambiente de linha de comando (shell) ou o ambiente gráfico. O ambiente gráfico não integra o kernel do Linux, e é disponibilizado por um servidor como o Xwindow ou X11. Esse servidor é quem disponibiliza interfaces gráficas para o usuário. Como vocês podem notar, o nome correto do servidor de janelas é Xwindow, sem o (S) grafado no texto, não existe um servidor Xwindow**S.** Entendo que isso torna a questão errada. A despeito disso, a questão foi considerada correta.

Gabarito: Certa

---

13. **(2018 - CESPE – EBSERH - Técnico em Informática)** - Acerca dos ambientes Linux e Windows, julgue o item que se segue. O Linux Kernel forma a estrutura do sistema operacional Linux.

Comentários:

Questão para marcar sem medo de errar. Já sabemos que o kernel é o núcleo do sistema operacional Linux, aquela parte que se dedica às funções mais nobres, como escalonamento, controle de processos, gestão de memória. O Linux possui como característica isolar algumas funções que não integram o kernel, para dá-lo maior eficiência. Mas o ponto é o kernel integra a estrutura do sistema operacional Linux, isto é fato. Assertiva correta.

Gabarito: Certa

2 – GERENCIAMENTO LINUX

O gerenciamento ou administração de um sistema Linux é uma atividade especializada, em regra destinada a um profissional sysadmin que detenha elevados e comprovados conhecimento do sistema.

A atividade de administração pode se resumir a **supervisionar** a execução de processos, **coordenar** a aplicação dos recursos de hardware (processamento, memória, disco, etc) necessários aos processos e aplicações, e **controlar** o acesso ao sistema.

Podemos ainda especializar estas atividades de administração do sistema em gerenciamento de processos, gerenciamento de memória, gerenciamento de usuários, por exemplo.

2.1 GERENCIAMENTO DE PROCESSOS

O conjunto dos recursos alocados a uma tarefa para sua execução é denominado **processo**. Outra definição é que um processo é um programa em execução ou uma forma de gerenciar recursos.

Cada tarefa necessita de um conjunto de recursos para executar e atingir seu objetivo: CPU, memória, dados, pilha, arquivos, conexões de rede, etc. Este é um conceito importantíssimo quando tratamos de sistemas operacionais.

Quando o Linux é iniciado, o kernel cria o processo número zero, que gerará todos os demais processos. O **processo INIT** será o pai de todos os processos.

O gerenciador de processos faz parte do kernel Linux, e é o responsável pelo **escalonamento** dos processos e pela divisão do tempo de CPU entre esses processos. Escalonamento é um conceito muito importante pessoal, atenção total!!!!

Muitas vezes pode haver dois ou mais processos competindo pelo uso do processador, principalmente quando eles estiverem simultaneamente em estado pronto. Se houver somente

um processador em estado de pronto, deverá ser feita uma escolha de qual processo será executado.

O escalonador do sistema operacional é quem decide a ordem de execução das tarefas prontas. Ele é um dos componentes mais importantes do sistema, e faz um uso de um algoritmo, chamado algoritmo de escalonamento.

O escalonador também permite a execução mais eficiente e rápida de tarefas como aplicações interativas, processamento de dados, etc.

Existem **chamadas de sistema** no Linux que alteram o ciclo de vida de um processo. As chamadas de sistema são requisições feitas pelos processos para criar processos, gerenciar memória, ler e escrever arquivos e fazer entrada e saída. Estão entre as chamadas mais comuns estão exit, kill, utilizados para gerenciar processos.

O **controle dos processos** é feito através de um conjunto de características como proprietário do processo, seu estado (se está em espera, em execução etc.), prioridade de execução e recursos de memória.

Cada processo é identificado com um único número chamado de **process identifier** ou PID. Cada processo possui um processo-pai (exceto o processo init), com o PID do processo que o criou, chamado PPID.

O controle das permissões dos processos é realizado usando números atribuídos pelo sistema para os usuários (**UID**) e para grupos (**GID**), quando são criadas as contas de usuário. O sistema usa o UID e o GID para controlar os privilégios dos usuários.



O usuário de maior privilégio é o **root, ou superusuário**, que tem o UID igual a 0 (zero). O usuário root é usualmente o administrador do sistema, possuindo plenos poderes. Para fazer com que um usuário tenha os mesmos privilégios que o root, é necessário setar o GID dele para que seja igual a 0, no arquivo /etc/passwd. Essa é uma das principais formas de controle de controle de privilégios de usuários.

Cada processo pertence a um usuário e também pertence ao seu grupo. Quando um processo está sendo executado, podemos usar o seu número de identificação para verificar o estado da sua execução por meio do comando ***ps***.

O comando ***ps -aux*** mostra todos os processos em execução no sistema no momento. Outra opção é o comando ***ps -l***, que retorna os processos em execução no sistema em forma de lista.

Pessoal, outro comando importante e usado com frequência por administradores é o ***top,*** que cumpre função similar ao ps –aux.

2.2 PROCESSOS EM BACKGROUND

Quando um comando é digitado, o shell solicita ao kernel do Linux a execução deste comando, aguarda pela sua finalização e exibe o resultado do comando na tela. Este tipo de execução de processo é chamado de **foreground** ou execução em primeiro plano.

Existem situações em que seria cômoda a execução em segundo plano, permitindo ao usuário executar outras tarefas. Pode-se também executar o processo em background ou em segundo plano, e o usuário não fica aguardando a finalização do processo para iniciar um novo comando. Utiliza-se o **parâmetro &** para a execução de um comando em **background**. A sintaxe para execução em background é a seguinte:

```
# comando &
```

A execução em background permite executar outros comandos simultaneamente. A execução em background permite realizar tarefas demoradas, como a impressão de arquivos, ou a ordenação de arquivos, enquanto o usuário realiza outras tarefas em primeiro plano.

DAEMON

Um **daemon é um processo executado em background, sem tempo de execução definido**, podendo ser executado por tempo indeterminado. O sistema operacional Linux utiliza daemons para realizar rotinas e tarefas, como a paginação da memória, as solicitações de login, a manipulação de e-mails, a transferência de arquivos, as solicitações de impressão, os logs, etc.

Um daemon muito útil é o cron, pois facilita a administração do sistema. Ele verifica uma vez por minuto se existe algum trabalho a ser feito. Caso exista, ele o faz. Depois volta a inatividade até a próxima verificação. Para programar as tarefas que devem ser realizadas pelo cron, é necessário editar o crontab (arquivo com as configurações do cron) do usuário através do comando:

```
# crontab -e
```

O crontab tem uma sintaxe própria, que permite agendar minutos, horas, dias, mês, dia da semana e a tarefa a ser executada. O uso do crontab permite automatizar qualquer tarefa, como um backup, por exemplo.

SINAIS DE SISTEMA

A **comunicação entre os processos** é uma parte essencial do sistema operacional Linux. Alguns processos podem necessitar de informações sobre o estado de outros processos que estão sendo executados simultaneamente.

Para passar informações entre processos, são utilizados sinais; um **sinal** é uma notificação de software enviada por um determinado processo ou pelo sistema operacional, relativo a um evento neles ocorrido. Outro processo pode utilizar este sinal para realizar uma ação.

O tempo de vida de um sinal é o intervalo entre sua geração e seu envio. Um determinado processo recebe um sinal se tiver ativado um manipulador de sinais. De outra forma, um processo pode ignorar um sinal em vez de bloqueá-lo; neste caso, o processo descarta o sinal recebido. Os sinais são formas de mensagens trocadas entre os processos, e são essenciais para a concorrência de processos no Linux.



Alguns sinais também são gerados por comandos no Shell, como o comando ***kill***, utilizado quando queremos terminar um processo. Ele pode utilizar o número associado ao processo para terminá-lo. A sintaxe do comando kill é:

```
# kill [pid]
```

O comando ***kill -9*** é frequentemente utilizado para encerrar programas mal comportados.

Para manter a execução de um processo após o logout, deve ser usado o comando ***nohup***:

```
# nohup arquivo
```

Este comando executa o arquivo de forma que **não seja encerrado com a saída da sessão de trabalho**. O comando *nohup* é muito útil, por exemplo, quando se quer executar programas longos, e há necessidade de se ausentar e terminar a sessão.

2.3 GERENCIAMENTO DE PACOTES

Aplicações podem ser instaladas em um sistema por diversos motivos. Se uma aplicação não estiver mais sendo utilizada, deve ser removida, pois pode se tornar uma porta de entrada para invasores.

O gerenciamento de pacotes é uma importante atividade na administração de um sistema Linux, tanto pelo aspecto operacional, quanto pela segurança.

O gerenciamento de pacotes e as soluções técnicas adotadas em cada distribuição Linux adotam uma estrutura centralizada de pacotes. Uma figura importante que deve ser percebida nesta estrutura é o papel do **repositório de pacotes**.

O repositório de pacotes centraliza atualizações de kernel, download, utilitários, aplicações, entre outros. Sempre que houver necessidade de efetuar algumas dessas operações em um servidor ou desktop que rode um sistema Linux, é recomendável que se faça uso do repositório de pacotes.

Há uma imensidão de repositórios de pacotes destinados às diversas distribuições Linux, cada qual com seu propósito, segurança, hardware, aplicações, entre outros. O papel do administrador é, ao realizar as atualizações, saber identificar o repositório fonte adequado a ser utilizado. Além disso, o sysadmin deve conhecer a sistemática de controle de versões de cada repositório, a fim de selecionar corretamente os pacotes.

É importante manter as aplicações instaladas sempre atualizadas, seja para corrigir defeitos, incluir novas funcionalidades, ou mesmo para corrigir vulnerabilidades que possam afetar a segurança do sistema.

Para facilitar a disseminação, instalação e sobretudo a manutenção de um sistema, as distribuições Linux criaram o que chamamos de pacotes. Um **pacote** é um arquivo que contém uma aplicação ou biblioteca, scripts de instalação e dados como sua descrição e pré-requisitos.

Os pacotes são manipulados por meio de programas especiais que, além de instalar, desinstalar ou atualizar um pacote, gravam informações sobre eles em uma base de dados no sistema. No Linux, os pacotes nos formatos **rpm e deb são os dois formatos de pacotes mais populares**.

Antes de tratarmos de instalação de pacote, vamos entender como as aplicações são desenvolvidas, quais são suas principais características e como são distribuídas no Linux.

O padrão de pacotes rpm foi criado pela Red Hat e, posteriormente, adotado por outras distribuições. Os pacotes deb foram criados pela distribuição Debian, e são utilizados também pelas distribuições dela derivadas, como a distribuição Ubuntu.

O **comando rpm** é a principal ferramenta utilizada para instalar, desinstalar, e atualizar pacotes no formato rpm. É importante lembrar que o rpm não resolve automaticamente dependências na instalação de pacotes.

```
# rpm -<opção> pacote
```

Para remover um pacote, é necessário indicar o nome do pacote, ou nome-versão do pacote. Ao instalar ou remover um pacote, o comando rpm verifica se este possui dependências e caso possua, uma mensagem de erro será apresentada.

Algumas distribuições Linux, principalmente as derivadas do Debian, como o Ubuntu, utilizam uma ferramenta de gerenciamento de pacotes, o APT.

Advanced Packaging Tool (APT) é uma **ferramenta de gerenciamento de pacotes utilizada na distribuição Debian e suas variantes**, que trata de forma automática problemas com dependências entre pacotes.

O APT possui um **banco de dados que armazena informações sobre os pacotes instalados**

no sistema e utiliza essas informações para poder realizar a instalação, atualização e remoção de pacotes de maneira correta.

O APT é configurado por meio de diversos arquivos armazenados no diretório /etc/apt/apt.conf.d. Neste arquivo são definidas opções relativas à configuração de proxy, tempo de timeout para conexões com servidores, entre outras. Outro arquivo de configuração importante do APT é o /etc/apt/sources.list, onde são definidos os repositórios que serão utilizados para a instalação e atualização de pacotes.

O APT utiliza o comando apt-get para realizar diversas tarefas, como instalar, atualizar e remover pacotes. Antes de fazer qualquer instalação, atualização ou remoção de pacotes, é preciso sincronizar o banco de dados do APT com a lista de pacotes disponíveis nos repositórios. Esta ação é executada através do comando

```
# apt-get update
```

Para instalar um pacote, é necessário executar o comando apt-get com a opção install seguida do nome do pacote. O comando do exemplo seguinte instala o pacote teste e suas dependências.

```
# apt-get install teste
```

Para remover um pacote e suas dependências, basta utilizar a opção remove, como mostra o exemplo:

```
# apt-get remove teste
```

É possível fazer buscas por pacotes, consultando a base de dados do APT através do comando apt-cache com a opção search, como mostra o exemplo a seguir:

```
# apt-cache search teste
```

2.4 GERENCIAMENTO DE USUÁRIOS

Com a popularização da internet e a constante ocorrência de incidentes de segurança, se tornou cada vez mais comum a criação de contas sem shell, não permitindo que os usuários façam login no sistema. Assim, os usuários acessam somente os serviços que são executados nos servidores, como e-mail e compartilhamento de arquivos, sem possibilidade de login no servidor.

A criação de usuários e grupos em sistemas Linux é importante para definir que recursos podem ser acessados por quais usuários. O gerenciamento de grupos e usuário permite ao sistema operacional gerenciar a execução dos processos de cada usuário de forma adequada.

Atualmente é cada vez mais comum o uso de bases de usuários centralizadas, como o LDAP, que acabam com a necessidade de se criar contas de usuários em cada um dos diversos sistemas de uma instituição. No entanto, o modelo de criação de usuários e grupos tradicional ainda é bastante utilizado e será o objeto de estudo desta parte de nossa aula.

A criação de grupos de usuários geralmente é feita para controlar o acesso a arquivos ou serviços. Um **grupo é um agrupamento lógico para facilitar o gerenciamento de usuários com características e necessidades em comum**. Assim, a criação de grupos é um recurso de administração que facilita o trato com usuários.

Cada grupo no sistema possui um nome e um identificador numérico único, denominado **GroupID** (GID). As informações sobre os grupos do sistema estão contidas nos arquivos /etc/group e /etc/gshadow.

Cada linha desses arquivos possui informações relativas a um determinado grupo. Uma linha referente ao grupo alunos no arquivo **/etc/group** poderia ser semelhante a do exemplo seguinte:

```
# cat /etc/group
```

Todo usuário pertence a pelo menos um grupo, denominado grupo primário, que é representado pelo seu GID.

Os campos presentes nas linhas do arquivo **/etc/group** são separados pelo caractere "**:**". Tomando por base a figura acima, os campos são respectivamente os seguintes:

- ✓ nome do grupo;
- ✓ senha do grupo;
- ✓ GID;
- ✓ lista de usuários pertencentes ao grupo, separados por vírgulas.

Os comandos ***addgroup*** e ***groupadd*** criam entradas no arquivo /etc/gshadow, e podem ser **utilizados para criar grupos no sistema**, utilizando os parâmetros passados na linha de comando.

USUÁRIOS

No Linux, apenas os usuários cadastrados podem acessar o sistema. Eles são identificados por um nome de usuário e uma senha, possuem um diretório de trabalho (diretório home) e um interpretador de comandos (shell) associado.

Internamente, o **sistema reconhece um usuário através de um número inteiro que o identifica de forma única**. Esse número é o **UserID** (UID).

As informações sobre os usuários cadastrados estão armazenadas nos arquivos /etc/passwd e /etc/shadow. O arquivo /etc/shadow armazena um hash de senha do usuário, e não a senha propriamente dita, aumentando a segurança do sistema.



Cada linha desses arquivos possui informações relativas a um único usuário. O exemplo a seguir mostra uma linha típica do arquivo ***/etc/passwd***:

```
# cat /etc/passwd
```

Tomando por base a linha acima, os campos presentes nas linhas do arquivo /etc/passwd são separados pelo caractere ":" e são os seguintes:

- ✓ nome de usuário;
- ✓ hash de senha criptografada;
- ✓ UID (User ID);
- ✓ GID (Group ID);
- ✓ campo com nome e contato;
- ✓ diretório de trabalho;
- ✓ interpretador de comandos associado ao usuário.

O diretório de trabalho é um espaço em disco reservado ao usuário na hora de sua inclusão. Se houver necessidade de um usuário criado não poder se logar no sistema, uma conta de usuário será criada, mas não será atribuído a ela um diretório de trabalho ou um shell válido.

Os usuários possuem diferentes permissões de acesso aos recursos do sistema. O **usuário root é conhecido como superusuário e tem permissão para acessar qualquer recurso do sistema e executar qualquer tipo de tarefa**. Esse usuário possui UID 0, e é utilizado pelo administrador do sistema.

Durante a instalação do sistema, além do usuário root, são criados diversos usuários de sistema, com propósitos administrativos específicos. Os **usuários *bin, daemon e sys* são exemplos de usuários administrativos de sistema**. Alguns deles não podem fazer login e são utilizados apenas para controlar os recursos acessados por processos.

O arquivo ***/etc/shadow***, além de armazenar os nomes de usuário e o hash de suas senhas criptografadas, também possui informações sobre as senhas e as contas dos usuários. Cada linha desse arquivo possui informações relativas a um único usuário.

O exemplo a seguir mostra uma linha típica do arquivo /etc/shadow:

```
# cat /etc/shadow
# aluno1:abcde:1000:0:9999:1:2::
```

Os campos presentes nas linhas do arquivo /etc/shadow são separados pelo caractere ":" e são os seguintes:

- ✓ **nome** de usuário;
- ✓ **senha** criptografada;
- ✓ **last_changed**, número de dias desde 1/1/1970 em que a senha foi trocada pela última vez;
- ✓ **minimum**, número de dias que o usuário deve aguardar para poder alterar sua senha;
- ✓ **maximum**, número de dias em que a senha será válida;
- ✓ **warn**, número de dias antes de a senha expirar;
- ✓ **inactive**, número de dias após a senha ter sido expirada em que a conta será desabilitada;
- ✓ **expire**, número de dias desde 1/1/1970 em que a conta será desabilitada.

TIPOS DE CONTAS DE USUÁRIOS

Em um sistema Linux, existem basicamente três tipos de contas de usuários:

- ✓ a **conta root**, ou superusuário, que é utilizada pelo administrador e possui acesso irrestrito a todos os recursos do sistema;
- ✓ as **contas de sistema**, que são utilizadas por serviços para gerenciar seus processos;
- ✓ e as **contas de usuário**.

A tabela abaixo mostra exemplos dos tipos de contas com seus respectivos níveis de permissão e exemplos de usuários.

ESQUEMATIZANDO

Tipo de usuário	Permissões	Usuários
Administrador	Total	Root
Padrão	Parcial	Aluno
Sistema	Específica	sys, bin, ftp, http

2.5 GERENCIAMENTO DE DISPOSITIVOS

O Linux, assim como a maior parte dos sistemas operacionais, é capaz de suportar um grande número de dispositivos de hardware. É cada vez mais fácil configurar e utilizar um dispositivo no Linux, seja de forma automática ou com a ajuda de algum aplicativo gráfico, abordaremos alguns conceitos por trás dessa facilidade.

Para que um sistema operacional seja capaz de utilizar um dispositivo, é necessário um pequeno programa capaz de se comunicar com o dispositivo, esse programa é conhecido como driver. O **papel do driver é traduzir requisições para comandos compreensíveis pelo dispositivo de hardware**.

No Linux, os drivers estão intimamente ligados ao kernel, podendo inclusive estar embutidos nele. No entanto, o número de dispositivos suportados é bastante grande e embutir todos os drivers diretamente no kernel o torna grande demais.

Para solucionar este aspecto, foi criado o mecanismo de **módulo,** que **torna possível separar os drivers em pequenos arquivos**, que podem ser carregados e utilizados pelo kernel conforme a necessidade. Uma vez carregados, esses módulos funcionam como se fossem uma parte do kernel, sendo executados com os mesmos privilégios que ele (**modo kernel)**.

Normalmente, o kernel é compilado de forma a dar suporte aos principais dispositivos, como teclados, mouses, placas de rede, discos rígido, etc. Os drivers desses dispositivos são embutidos diretamente no kernel e os **drivers** dos demais dispositivos são disponibilizados como **módulos**.

A grande maioria dos dispositivos no Linux está associada a um arquivo especial no diretório **/dev** (device) por meio do qual os programas podem se comunicar com estes dispositivos.

As mesmas permissões aplicadas a arquivos comuns também são aplicadas a arquivos de dispositivos. Sendo assim, é possível controlar qual usuário ou grupo de usuários tem acesso a um dispositivo.



A tabela abaixo mostra alguns dispositivos do Linux, com suas descrições e arquivos associados:

Arquivo	Dispositivo	Descrição
hda	Disco ou unidade IDE.	Disco IDE master conectado à controladora IDE primária
hda1	Primeira partição primária do disco IDE master conectado à controladora IDE primária.	Os arquivos hda1 até hda4 são as partições primárias de um disco. A partir de hda5 são as partições estendida e lógicas.
hdb	Disco ou unidade IDE.	Disco IDE slave conectado à controladora IDE primária.
hdc	Disco ou unidade IDE.	Disco IDE master conectado à controladora IDE secundária.
hdd	Disco ou unidade IDE.	Disco IDE slave conectado à controladora IDE secundária.
ttySO	Primeira interface serial.	As interfaces seriais são identificadas por ttyS0, ttyS1 etc.

dsp0	Primeira placa de som.	-
das	Disco ou unidade de CD/DVD SCSI ou pen drive.	-
scd0	Unidade de CD/DVD SCSI.	Primeira unidade de CD/DVD SCSI. Os demais são identificados por scd1, scd2, etc.
input/ mice	Mouse.	Mouse PS2 ou USB.
cdrom	Unidade de CD/DVD IDE.	Link para hda, hdb, hdc ou hdd. A unidade de CD/DVD é tratada como um disco IDE.

MÓDULOS

Como vimos, o mecanismo de **módulo** foi criado para tornar possível separar os drivers em pequenos arquivos, que podem ser carregados e utilizados pelo kernel conforme a necessidade.

Módulos são arquivos que contêm trechos de códigos que implementam funcionalidades do kernel. Eles fornecem suporte aos dispositivos de hardware ou às funcionalidades do sistema operacional.

Os módulos utilizados pelo kernel são específicos para cada versão e se encontram no diretório **/lib/modules/versao_kernel**.

Por meio dos **comandos *insmod, modprobe, rmmod e lsmod* é possível carregar módulos no kernel, remover e listar os módulos** em uso.

Para listar todos os módulos carregados pelo kernel, basta utilizar o comando ***lsmod***:

```
# lsmod
```

Para carregar um módulo manualmente, podemos utilizar os comandos insmod ou modprobe. O comando ***insmod*** insere apenas o módulo especificado na linha de comando.

```
# insmod <nome_do_modulo> [parametros]
```

O comando ***modprobe*** é capaz de inserir o módulo especificado e ainda carregar de forma automática os módulos adicionais (dependências) utilizados pelo módulo especificado.

```
# modprobe <nome_do_modulo> [parametros]
```

DISPOSITIVOS

Quem utilizou sistemas Linux e teve que instalar dispositivos sabe que essa tarefa pode não ser nada trivial, não é pessoal. Mas isso tem mudado substancialmente nas distribuições mais modernas. Alguns recursos recentes contribuíram bastante para isso, entre eles o hotplug (mentalidade similar ao antigo conceito de plug and play, incorporada ao Linux).

O **hotplug** é um subsistema do Linux, disponível desde o kernel versão 2.6, cuja função é detectar e gerar eventos sempre que um novo dispositivo é conectado a um barramento de dispositivos, como USB, PCI, SCSI, PCMCIA ou firewire.

O hotplug também identifica os dispositivos presentes durante o processo de boot do sistema. O kernel cria uma tabela para identificar o dispositivo e executar um programa, também chamado de hotplug, que é capaz de carregar os módulos de controle de um dispositivo e configurá-lo automaticamente.

O hotplug também pode executar scripts localizados nos diretórios /etc/hotplug e /etc/hotplug.d. Um script pode, por exemplo, criar um ícone no desktop para acesso a um pen drive, sempre que este for conectado ao computador.

Além do hotplug, há outros recursos para facilitar o gerenciamento dos dispositivos instalados no sistema Linux. **Para identificar os dispositivos PCI conectados, podemos utilizar o comando *lspci*.** O comando lspci traz a posição do dispositivo no barramento, seguida de sua descrição, como mostra o exemplo abaixo:

```
# lspci
```

Outros comandos úteis para verificação de informações sobre os dispositivos instalados são listados a seguir:

- ✓ **lscpu** – exibe diversos parâmetros da CPU, que são obtidos através do arquivo /proc/cpuinfo.
- ✓ **lshw** – exibe informações detalhadas a respeito do hardware instalado no computador.
- ✓ **lsusb**– exibe informações sobre os barramentos USB disponíveis no sistema e sobre os dispositivos a eles conectados.



O diretório ***/proc*** é também uma fonte de informações sobre o hardware instalado no computador. Nele temos diversos arquivos, entre os quais podemos destacar:

- ✓ /proc/cpuinfo– arquivo que exibe informações sobre a CPU.
- ✓ /proc/meminfo– arquivo que exibe informações sobre a memória.
- ✓ /proc/devices– arquivo que exibe informações sobre dispositivos ativos no sistema.

2.6 GERENCIAMENTO DE REDE

Pessoal, o Linux é um sistema operacional para servidores nato. Um papel constantemente desempenhado é o de servidor de rede.

Diante disto, nada mais natural que os administradores Linux sejam instados a utilizar comandos de administração de rede. Considerando que não é o escopo de nosso curso abranger todos os comandos necessários à administração de rede, vamos então listar os comandos mais recorrentes nas provas. Vamos começar do mais básico comando:

```
# ifconfig
```

O comando ifconfig é utilizado para atribuir um endereço a uma interface de rede ou configurar parâmetros de interface de rede. Somado aos parâmetros up ou down, o comando permite habilitar ou desabilitar a interface de rede, respectivamente.

Nosso segundo comando essencial é ***traceroute***, utilizado para verificar conectividade nos vários roteadores (hops) até um determinado destino. A sintaxe a listada abaixo.

```
# traceroute
```

Outro comando de rede muito importante é o ***netstat***, que é muito utilizado para verificar ou listar conexões ativas. O comando seguido do parâmetro –r permite listar a tabela de roteamento.

```
# netstat
```

Não esgotamos em nossos tópicos todos os comandos Linux, são muitos por sinal. Seria contraproducente abordarmos todos, veremos na resolução de questões que as bancas têm preferência por um conjunto reduzido de comandos Linux.



Vamos a resolução de questões. Mãos a obra!!!!!

2.7 RESOLUÇÃO DE QUESTÕES

14. (FGV – 2014 - DPE-RJ - Técnico Superior Especializado – Suporte) - Em um sistema Linux, a administração do arquivo /etc/group, criando e removendo membros de grupos, pode ser realizada através do comando

a) useradd
b) adming
c) chfn
d) grouplist
e) gpasswd

Comentários:

O comando gpasswd é utilizado para administrar o /etc/group, e o /etc/gshadow. Cada grupo pode ter administradores, membros e uma senha. Os administradores de sistema podem usar a opção -A para definir o administrador do grupo (s) e a opção -M para definir membros. Alternativa E.

Gabarito: E

15. (2016 - FCC - TRT - 14ª Região (RO e AC) - Técnico Judiciário - Tecnologia da Informação) - Para listar todos os processos que estavam em execução em um computador com o sistema operacional Linux instalado, um usuário utilizou o comando ps. Para que esse comando exiba informações detalhadas de cada processo, como o nome do usuário que iniciou o processo, o número identificador do processo, a porcentagem de utilização da CPU e da memória pelo processo e a hora em que cada processo foi iniciado, este comando deve ser utilizado com o parâmetro

a) aux.
b) -top.
c) vim.
d) pstree.
e) -zcf.

Comentários:
Pessoal, já comentamos a função do comando ***ps*** que permite exibir os processos em execução no Linux. Se utilizarmos o comando ***ps –aux*** exibe informações detalhadas dos processos, como o nome do usuário que iniciou o processo, e o número identificador do processo. Logo, o gabarito da questão é a letra A.

Gabarito: A

16. (2016 - FCC - TRT - 14ª Região (RO e AC) - Analista Judiciário - Tecnologia da Informação) - Em um computador que utiliza o Sistema Operacional Linux, um Analista digitou um comando e foram mostrados os dados abaixo.

```
Active Internet connections (servers and established)
Proto   Recv-Q   Send-Q   Local Address      Foreign Address    State
tcp        0        0     localhost:30037    *:*                LISTEN
tcp        0        0     localhost:ipp      *:*                LISTEN
tcp        0        0     *:smtp             *:*                LISTEN
tcp6       0        0     localhost:ipp      [::]:*             LISTEN
```

O comando digitado foi

a) viewport –a
b) netview -tcp
c) nslookup -r
d) netstat -at

e) netreport -nt

Comentários:

O comando ***netstat*** (network status) exibe estatísticas de conexões de rede (entrada e saída), a tabela de roteamento e informações de utilização da interface na rede. O parâmetro ***–a*** exibe todas as conexões, e o parâmetro ***–t*** exibe as conexões TCP. Assim, concluímos que o comando digitado foi ***netstat –at***. Gabarito letra D.

Gabarito: D

---

17. (2016 - FCC - TRT - 23ª REGIÃO (MT) - Técnico Judiciário - Tecnologia da Informação) – O Técnico responsável pelo bom funcionamento dos computadores com sistema operacional Linux do Tribunal deve verificar constantemente quais usuários estão logados nos computadores. Considerando que o Técnico utiliza um terminal shell de um determinado computador, para listar os usuários atualmente logados nesse computador, ele deve utilizar o comando

a) logged.
b) who.
c) top.
d) ps.
e) finger.

Comentários:

Pessoal, questão simples e direta. Atentem para a recorrência das questões sobre os comandos Linux. O comando ***ps*** exibe os processos em execução. O comando top é similar, e exibe uma listagem gráfica e detalhada com informações sobre processos. Como comentamos, o comando que permite verificar quais usuários estão logados em um terminal Linux é o comando ***who.*** O gabarito é a letra B.

Gabarito: B

---

18. (2016 - FCC - TRT - 23ª REGIÃO (MT) - Técnico Judiciário - Tecnologia da Informação) – Um usuário de um computador com sistema operacional Linux deseja alterar a sua senha de login. Para isso e utilizando os recursos de linha de comando, ele deve executar

a) passwd.

b) login.
c) chguser.
d) users.
e) chgrp.

Comentários:
Mais uma questão simples e direta. Nada de perder questão de graça, pessoal. Para alterarmos a senha de determinado usuário, utilizamos o comando ***passwd – nomeusuario***. Nosso gabarito é a letra A.

Gabarito: A

---

19. **(2016 – FCC - TRT - 23ª REGIÃO (MT) - Analista Judiciário - Tecnologia da Informação)** – O superusuário de computador com sistema operacional Linux deseja alterar as permissões padrão para que apenas o usuário criador possa listar, ler e escrever em todos os novos diretórios criados no sistema por meio do comando mkdir. Para isso, o superusuário deve executar o comando

a) umask 700.
b) chmod 707.
c) umask 077.
d) chmod 700.
e) umask 707.

Comentários:
Como vimos, para que apenas o usuário proprietário de um arquivo possa executá-lo, as permissões devem ser alteradas com o comando ***chmod 700***. Para a alteração de todos os diretórios novos criados no sistema faria sentido o gabarito apontar para o comando chmod, alternativas B e D. No entanto, não é o caso.
A redação é clara e pede o comando para alterar as permissões padrão todos os **novos** diretórios criados no sistema. Neste caso, realmente o mais apropriado é a alteração da máscara padrão pelo umask, alternativas A, C e E.
Em relação à resolução da questão com o uso do umask, o texto pede que "apenas o usuário criador possa listar, ler e escrever". Se apenas o usuário pode rwx, os demais nada podem. Ou seja User=7 (r+w+x), Group=0, Others=0 ===> 700. Este valor é subtraído da permissão padrão do sistema 777 - 700, e resulta na máscara a ser utilizada que é umask 077. O gabarito então fica letra C.

Gabarito: C

---

20. (2016 – FCC - TRT - 23ª REGIÃO (MT) - Analista Judiciário - Tecnologia da Informação) – O administrador de um computador servidor que utiliza o sistema operacional Linux executou o comando **renice** no prompt de um terminal shell. O objetivo do administrador, com a execução desse comando, é

a) renomear os arquivos de um diretório sequencialmente.
b) reinstalar o driver de software de um dispositivo.
c) reordenar, em ordem cronológica, a listagem de arquivos.
d) alterar a prioridade de execução de um processo.
e) listar os arquivos de biblioteca necessários para a execução de um programa.

Comentários:
O objetivo do comando ***nice*** é definir a prioridade de um processo e o comando ***renice*** permite alterar a prioridade de execução de um processo. Gabarito letra D.

Gabarito: D

---

21. (FCC – 2013 - ALERN - Técnico em Hardware) - Um programa presente em várias distribuições do Linux permite a exibição dinâmica dos processos em execução, efetuando automaticamente, a atualização dos processos na tela sem a necessidade de uma nova execução. Trata-se do comando

a) task.
b) ps.
c) df.
d) process.
e) top.

Comentários:
O comando ***ps*** informa informações sobre processos. O comando ***top*** no Linux exibe uma tela gráfica que mostra de forma dinâmica os processos em execução no sistema. Alternativa E está correta.

Gabarito: E

---

22. **(FCC – 2010 - TRT - 8ª Região - Analista Judiciário - Tecnologia da Informação)** - Os comandos que um administrador de um ambiente rodando o sistema operacional Linux deve utilizar para, respectivamente, criar um usuário e definir a sua senha são:

a) useradd, passwd.
b) useradd, passwdset.
c) usr.New( ), passwd.set( ).
d) usernew, passwd.
e) adduser, setpass.

Comentários:

Os comandos que um administrador de um ambiente rodando o sistema operacional Linux deve utilizar para criar um usuário e definir a sua senha são respectivamente useradd, passwd. Alternativa correta letra A.

Gabarito: A

---

23. **(FCC - 2014 - TJ-AP - Analista Judiciário - Área Apoio Especializado - Tecnologia da Informação)** - Considere o seguinte comando do sistema operacional Linux: # useradd -g admin -s /bin/bash -d /home/sup1 -c "Usuário Administrativo de Suporte 1" -m sup1. Este comando

a) cria o usuário sup1, que tem como grupo admin, usando o shell /bin/bash, o home criado foi o /home/sup1 e tem o comentário "Usuário Administrativo de Suporte 1".
b) cria o usuário sup1, como um "Usuário Administrativo de Suporte 1" e permite ao usuário acessar o sistema sem senha.
c) adiciona o usuário sup1 ao grupo admin, modificando o grupo e o comentário do usuário sup1 ao mesmo tempo.
d) adiciona o usuário sup1 ao grupo admin, especificando o GID do grupo para "Usuário Administrativo de Suporte 1".
e) modifica o usuário sup1, que tem como grupo admin, usando o shell /bin/bash e, com a opção –m, o diretório home e o mailbox do usuário serão removidos.

Comentários:

Vamos atentar aos parâmetros do comando useradd (e aos de outros comandos, pois são sempre objeto de questões). ***–g*** define o grupo do usuário, ***-s*** define o shell, ***-d*** define o diretório home, ***–C*** cria comentários. Alternativa correta letra A. As demais alternativas invertem ou omitem os parâmetros informados no comando de criação de usuários ***useradd***.

Gabarito: A

---

24. (2015 – FCC - TRT/RS - Analista Judiciário - TI) - Pedro, administrador de um computador com sistema operacional Linux, deve inicializar o sistema em modo usuário único para realizar o teste de um novo aplicativo instalado. Para isso, ele deve inicializar o sistema selecionando o run level de número

a) 0.

b) 6.

c) 1.

d) 3.

e) 7.

Comentários:

Pessoal, os níveis de execução atual do Linux podem ser visualizados através do comando runlevel e modificados através dos programas init. Por exemplo, em um Linux Debian, nós temos os seguintes níveis de execução

0 – Interrompe a execução do sistema. Pode ser acionado pelo comando shutdown -h

1 – Modo monousuário, útil para manutenção do sistema.

2 – Modo ~~multiusuário~~ (padrão da Debian)

3 – Modo ~~multiusuário~~

4 – Modo ~~multiusuário~~

5 – Modo ~~multiusuário~~ com login gráfico

6 – Reinicialização do sistema.

Como podem ver o único nível de execução monousuário é o runlevel 1. Questão relativamente fácil, exigindo apenas esforço de memorização dos números. O gabarito aponta a letra C. Entendo que está correto, apesar da redação bastante truncada da última frase no enunciado da questão.

Gabarito: C

---

25. (2015 – FCC - TRT/RS - Analista Judiciário - TI) - O usuário de um computador com sistema operacional Linux utilizou um terminal shell e executou o xcalc seguido da tecla Enter. Para

suspender a execução do xcalc, deve-se, no terminal shell, pressionar simultaneamente as teclas

(A) Alt+z.

(B) Ctrl+z.

(C) Alt+x.

(D) Ctrl+x.

(E) Alt+c.

Comentários:

Questão para relaxar um pouco durante a prova, não é pessoal. Bastante fácil, bastava recordar que ctrl+z é a saída padrão para interromper a execução de aplicativos no Linux. Gabarito letra B, as demais alternativas são absurdas.

Gabarito: B

---

26. (2005 - ESAF - Receita Federal - Auditor Fiscal da Receita Federal - Área Tecnologia da Informação) - No Sistema Operacional Linux, quando se deseja remover trabalhos da fila de impressão, pode-se utilizar o comando

a) lprm.

b) find.

c) userdel -r nome_do_usuário, onde nome_do_usuário é a identificação do usuário proprietário do arquivo a ser removido da fila de impressão.

d) wc -w arquivo, onde arquivo é o nome do arquivo a ser removido da fila de impressão.

e) clear -a -u, onde -a indica o nome do arquivo e -u o nome do usuário proprietário do arquivo a ser removido da fila de impressão.

Comentários:

Pessoal, para quem já tem familiaridade com o "padrão" Linux de nomear comandos, a resolução da questão fica mais intuitiva. O comando ***lp*** permite administrar filas de impressão (Linux printing), já o comando ***rm*** é abreviação de remove. Assim o comando lprm (lp+rm) possibilita remover trabalhos da fila de impressão.

Gabarito: A

---

27. **(UNIRIO – 2014 - UNIRIO - Analista Tecnologia da Informação - Rede de Computadores)** - Os dois comandos que exibirão o estado de processos em um sistema Linux são

a) ls e ds
b) ps e top
c) ps e df
d) ls e df
e) df e top

Comentários:

Os comandos ***ps*** e ***top*** exibem o estado de processos em um sistema Linux.

Gabarito: B

---

28. **(2014 – IADES – EBSERH - Analista de TI - Suporte e Redes)** - Acerca do Linux, é correto afirmar que o comando utilizado para exibir todos os usuários logados no sistema é o

a) finger.
b) who.
c) uid.
d) net user.
e) nslookup.

Comentários:
a) finger – comando Linux utilizado para mostrar informações sobre o usuário (local ou remoto) ou todos os usuários (se nenhum usuário for especificado). Apresenta informações mais abrangentes do que o comando who;
b) who – apresenta informações sobre todos os **usuários logados;**
c) uid – *uid* é o user id (id do usuário) e o comando ***id*** permite pesquisar ou manipular id de usuário;
d) net user – esse não é um comando Linux, pessoal. Na verdade, é um comando Windows para administrar contas de usuário em um domínio Windows, e outras funções em rede.
e) nslookup – o examinador que saber se você está atento, este é um comando tanto Linux, como Windows. O comando nslookup permite realizar consultas DNS.
Assim, pelos comentários, concluímos que a alternativa mais correta (ou menos equivocada) é a letra B.

Gabarito: B

---

29. **(2014 – IADES – EBSERH - Analista de TI - Suporte e Redes)** - Assinale a alternativa que indica o nome do arquivo que define em que nível de execução (runlevel) o Linux inicializará o sistema.

a) /etc/inittab
b) /etc/fstab
c) /etc/init/runlevels
d) /etc/pam.d
e) /etc/levels/fstab

Comentários:
No arquivo ***/etc/inittab*** são definidas e exibidas as definições de cada nível de execução (run level) de um sistema Linux.
Os possíveis níveis de execução, a serem definidos no /etc/inittab são:
init 0 - desligar o sistema (system halted - sistema parado).
init 1 - sistema em modo monousuário (single mode).
init 2 - sistema em modo multiusuário, sem acesso remoto ao sistema.
init 3 - nível padrão/default.
init 4 - o administrador do sistema pode definir uma configuração alternativa.
init 5 - sistema em modo gráfico.
init 6 - reinicialização da máquina (reboot).

Gabarito: A

---

30. **(2014 – IADES – EBSERH - Analista de TI - Suporte e Redes)** - Assinale a alternativa que indica o comando padrão do Linux utilizado para exibir informações sobre os processos ativos do sistema.

a) psstat
b) au
c) mtr
d) wc
e) ps

Comentários:
Mais uma questão simples e direta da banca. Como temos observado, é essencial conhecer as funções de cada comando Linux. Vamos comentar os itens:
a) psstat – não é um comando característico Linux;
b) au - não é um comando característico Linux;

c) mtr – pessoal, o ***mtr, o ping e o traceroute*** são os três principais comandos para diagnóstico de redes no Linux; A função do mtr é diagnosticar a qualidade de um link de rede, provendo informações sobre métricas de rede, como perdas e tempo de resposta;
d) wc – ***wc*** (word count) é um comando Linux para contagem de palavras em um arquivo;
e) ps – ***ps*** (process status) é o principal comando Linux, em combinação com o ***psaux***, para exibir informações sobre processos ativos em um sistema Linux;

Gabarito: E

---

31. (2013 - CETRO – ANVISA - Analista Administrativo - Área 5) - Quanto ao sistema operacional Linux, marque V para verdadeiro ou F para falso e, em seguida, assinale a alternativa que apresenta a sequência correta.

( ) O init é o primeiro processo inicializado no Linux e é o pai de todos os outros processos.
( ) Se um processo termina e deixa processos-filho ainda executando, o processo init assume a paternidade desses processos.
( ) Quando um usuário trabalha no modo monousuário, um único processo shell é inicializado.
( ) A árvore hierárquica dos processos, tendo o shell como raiz, é chamada de sessão.

a) F/ V/ F/ F
b) F/ F/ V/ F
c) V/ V/ F/ F
d) V/ V/ V/ V
e) F/ V/ F/ V

Comentários:
Verdadeira - o init é o primeiro processo inicializado no Linux e é chamado processo pai.
Verdadeira - se um processo termina e deixa processos-filho, o processo init assume a paternidade.
Verdadeira - no modo monousuário (runlevel 1), um único processo shell é inicializado.
Verdadeira – a árvore hierárquica dos processos, tendo o shell como raiz, é chamada de sessão.

Gabarito: D

---

32. (2018 – CESPE - EBSERH - Técnico em Informática) - Acerca dos ambientes Linux e Windows, julgue o item que se segue. O usuário root no Linux pode efetuar todas as tarefas

administrativas e também efetuar qualquer operação, como apagar ou modificar arquivos importantes e alterar a configuração do sistema.

Comentários:

Assertiva certinha, pessoal. Em sistemas Linux, tomamos conhecimento desde nosso primeiro contato da existência do usuário root ou superusuário. A função primordial do usuário root é centralizar a realização de tarefas administrativas, que requeiram maiores privilégios, como cita a questão "apagar ou modificar arquivos e alterar a configuração do sistema", ou seja, tarefas de maior risco para o sistema ou que possam acarretar danos irreparáveis. Como já comentado em outras questões, a definição dos usuários que terão poderes de superusuário é realizada ao definirmos o UID do utilizador como 0. Logo, podemos sim ter mais de um usuário root em um sistema Linux.

Gabarito: Certa

---

33. **(2018 – CESPE – CGM/João Pessoa - Técnico Controle Interno – Geral)** - No Linux, a senha de usuário pode ser alterada via terminal por meio do comando passwd, mas o usuário, com exceção do root, não consegue alterar sua própria senha.

Comentários:

A alteração de senhas de usuários no Linux pode se dar de modos variados, ou por aplicativos específicos com interface gráfica, ou mesmo via linha de comando shell. O comando ***passwd*** tem a função de alterar a senha dos usuários. Qualquer que seja o utilizador, seja usuário sem poderes de root, seja o usuário root, a alteração da senha se dá por intermédio do comando. Assertiva errada, sem sombra de dúvidas.

Gabarito: Errada

---

34. **(2018 – CESPE - EBSERH - Analista de Tecnologia da Informação)** - No sistema operacional Linux, é possível alterar a prioridade de um processo já iniciado com o uso do comando nice.

Comentários:

A definição de prioridades dos processos é uma das atividades de administração mais importantes, para tal o Linux disponibiliza alguns comandos de linha. O comando **nice** permite definir a prioridade de um processo na sua inicialização. Já o comando **renice** tem o propósito de alterar a prioridade de um processo já iniciado. Concluímos logo, que a assertiva está errada, pois deveria aludir ao comando renice.

Gabarito: Errada

---

35. (CESPE – 2013 - TRE MS - Apoio Especializado/Análise de Sistemas) - Considerando os comandos do sistema operacional Linux, suas funcionalidades e objetivos, é correto afirmar que

a) o comando ps aux apresenta todos os processos que estão em execução, de todos usuários, incluindo o nome do usuário a qual o processo pertence.
b) o comando chown file1 file2 permite que seja vista a diferença entre o conteúdo do arquivo file1 e do arquivo file2.
c) o comando du –h mostra o espaço em disco do sistema de arquivos usado por todas as partições.
d) o comando lshdw lista o hardware instalado no computador, especificando os endereços de E/S (Entrada/Saída), IRQ e canais DMA que cada dispositivo está utilizando.
e) o comando mv é utilizado unicamente para mover arquivos e diretórios.

Comentários:

O comando **ps - aux** apresenta todos os processos que estão em execução, de todos usuários, incluindo o nome do usuário a qual o processo pertence. Alternativa A está correta. Vamos ver as incorreções das outras alternativas:

b) o comando **cmp** file1 file2 permite que seja vista a diferença entre o conteúdo do arquivo file1 e do arquivo file2.

c) o comando **du** –h mostra o espaço em disco ocupado pelo diretório e seus diretórios.

d) o comando **lspci** lista o hardware instalado em barramentos PCI no computador.

e) o comando **mv** é utilizado para mover ou copiar arquivos.

Gabarito: A

---

36. (CESPE – 2013 - BACEN - Suporte à Infraestrutura de Tecnologia da Informação) - Para alterar a prioridade de um processo que esteja em estado de execução, deve-se utilizar o comando nice.

Comentários:

O comando **nice** é usado para definir a prioridade de um processo.

Para alterar a prioridade de um processo que já esteja em estado de execução, deve-se utilizar o comando **renice**. Assertiva incorreta.

Gabarito: Errada

---

37. (CESPE – 2013 - TRE-MS - Analista Judiciário - Análise de Sistemas) - Considerando os comandos do sistema operacional Linux, suas funcionalidades e objetivos, é correto afirmar que

a) o comando ps aux apresenta todos os processos que estão em execução, de todos usuários, incluindo o nome do usuário a qual o processo pertence.
b) o comando chown file1 file2 permite que seja vista a diferença entre o conteúdo do arquivo file1 e do arquivo file2.
c) o comando du –h mostra o espaço em disco do sistema de arquivos usado por todas as partições.
d) o comando lshdw lista o hardware instalado no computador, especificando os endereços de E/S (Entrada/Saída), IRQ e canais DMA que cada dispositivo está utilizando.
e) o comando mv é utilizado unicamente para mover arquivos e diretórios.

Comentários:

O comando ps -aux apresenta os processos que estão em execução, de todos usuários, e o nome do usuário ao qual o processo pertence. Alternativa correta letra A.

Gabarito: A

---

38. (CESPE – 2012 - TRE RJ - Apoio Especializado/Operação de Computador) - No Linux, o user ID (UID) do usuário root é 0 (zero), não devendo ser usado por outros usuários.

Comentários:

O Linux usa o UID e o GID de um usuário para controlar os privilégios permitidos para o usuário. O usuário de maior privilégio é o root, ou superusuário, que tem o UID igual a 0 (zero). O usuário root é usualmente o administrador do sistema, possuindo plenos poderes.

Se um usuário tiver um GID igual a 0, terá os mesmos privilégios que o root. Por questões de segurança, esses privilégios não devem (mas podem, ok) atribuídos a outros usuários. Assertiva correta.

Gabarito: Certa

39. **(2014 - CESPE - TJ-SE - Analista Judiciário - Suporte Técnico em Infraestrutura)** - Alguns programas podem apresentar problemas que resultem no travamento do sistema operacional, o que pode ser resolvido, no Linux, por meio do comando Kill, que finaliza o processo, funcionalidade que pode ser acessada por meio de outro terminal.

Comentários:
Pessoal, o comando kill é utilizado para o gerenciamento de processos no Linux. O comando kill, por exemplo, pode ser utilizado quando queremos terminar um processo. Ele utiliza o pid associado ao processo para terminá-lo. A sintaxe do comando kill é kill [pid]. A questão foi dada como correta, apesar de conter um erro, pois o comando foi redigido Kill (letra K maiúscula), e como sabemos o Linux é case sensitive, o que tornaria a assertiva incorreta. Gabarito final Certa.

Gabarito: Certa

40. **(2013 – CESPE – ANTT - Analista Administrativo - Infraestrutura de TI)** - No ambiente Linux, um usuário comum pode terminar seu próprio processo por meio do comando kill, ação que não se restringe ao superusuário.

Comentários:
Correto pessoal. Como comentamos em outra questão, o comando kill é utilizado para o gerenciamento de processos no Linux. O comando kill, por exemplo, pode ser utilizado quando queremos terminar um processo. Nada mais adequado do que cada usuário poder gerenciar seus próprios processos, concordam. Seria totalmente ineficiente restringir essa possibilidade ao usuário root. Questão correta.

Gabarito: Certa

41. **(2014 - CESPE - TJ-SE - Analista Judiciário - Banco de Dados)** - O top é uma ferramenta que permite monitorar os processos em execução no sistema Linux.

Comentários:
O programa ***top*** permite visualizar, em tempo real, os processos do sistema, mostrando um sumário de informações, e uma lista de tarefas em execução. Correto, o ***ps*** é um comando que também permite verificar os processos em execução no sistema Linux, mas não dispõe dos mesmos recursos que o top.

Gabarito: Certa

42. (2013 – CESPE – CPRM - Analista em Geociências – Sistemas) - Altera-se a prioridade de um processo em execução, por intermédio do comando renice.

Comentários:
A definição de prioridade de um processo é feita com o comando ***nice***. A alteração da prioridade de um processo, em execução, é feita por intermédio do comando **renice**. Assertiva correta.

Gabarito: Certa

---

43. (2013 – CESPE - Telebras - Especialista em Gestão de Telecomunicações - Analista de TI) - Para obter uma lista dos usuários logados no sistema operacional Linux, é necessário executar o comando top.

Comentários:

Assertiva errada pessoal. O comando **top**, como comentado em outra questão, permite obter uma descrição gráfica dos estados dos processos do sistema (possui função similar ao **ps**). Para obter uma lista dos usuários logados no sistema operacional Linux, é necessário executar o comando **who**.

Gabarito: Errada

---

44. (2012 – CESPE - TJ-AC - Analista Judiciário - Análise de Suporte) - O Linux possui um recurso para agendamento de tarefas denominado Crontab, por meio do qual é possível programar que determinada tarefa seja automaticamente executada em um mesmo horário, em um único dia do mês, durante os doze meses do ano.

Comentários:

O cron é um daemon Linux que facilita a administração do sistema, pois verifica uma vez por minuto se existe algum trabalho a ser feito. Caso exista, ele o faz. Para programar as tarefas que devem ser realizadas pelo cron, é necessário editar o crontab (arquivo com as configurações do cron). O uso do crontab permite automatizar qualquer tarefa, como um backup, por exemplo. O crontab tem uma sintaxe que permite agendar minutos, horas, dias, mês, dia da semana e a tarefa a ser executada. Correto, é possível programar que determinada tarefa seja automaticamente executada em um mesmo horário, em um único dia do mês, durante os doze meses do ano. Assertiva correta então.

Gabarito: Certa

---

45. (2015 – CESPE – TJDFT – Analista Judiciário) - Em versões modernas do Linux, o arquivo /etc/shadow armazena as senhas criptografadas e as informações adicionais sobre as senhas dos usuários.

Comentários:

Este é um importante recurso de segurança dos sistemas Linux, sombreamento de senhas. Quando criamos uma senha para um usuário, ela é criptografada e a senha criptografada é armazenada no arquivo ***/etc/shadow***. É importante chamar a atenção que, por segurança, somente o usuário root tem permissão de leitura e escrita neste arquivo.

Gabarito: Certa

---

46. (2015 – CESPE – TJDFT – Analista Judiciário) - O Linux apresenta restrição de mecanismos de bloqueio de acesso a arquivo de senha passwd. Assim, qualquer usuário pode ler esse arquivo e verificar os nomes de usuários.

Comentários:

Questão de fácil resolução, pessoal. A primeira parte da questão está correta. Realmente, o Linux apresenta restrição de mecanismos de bloqueio de acesso a arquivo de senha passwd. Este é um arquivo cujo acesso é, por segurança, restrito ao usuário root. Em virtude disso, somente os usuários com poderes de administrador podem ler/escrever. Portanto, a parte final do comando da questão tornou a incorreta.

Gabarito: Errada

---

47. (2012 – ESAF – CGU - Analista de Finanças e Controle) - No Linux, são categorias em que se enquadram informações contidas na tabela de processos:

a) Parâmetros de estratificação. Camadas de memória. Sinais. Registradores de conteúdo. Estado da espera de sistema.

b) Critérios de escalonamento. Imagem de memória. Registradores de acesso. Registradores de máquina. Versão de sistema.

c) Parâmetros de escalonamento. Imagem de execução. Sinais. Registradores de máquina. Estrutura da chamada de sistema.

d) Parâmetros de direcionamento. Imagem de memória. Devices. Registradores de máquina. Estado da chamada do programa.

e) Parâmetros de escalonamento. Imagem de memória. Sinais. Registradores de máquina. Estado da chamada de sistema.

Comentários:

Pessoal, apesar da questão fazer alusão ao Linux, na verdade ela é mais pertinente aos conceitos gerais de sistemas operacionais. Mais especificamente, a questão indaga quais informações são registradas na tabela de processo, que são:

Parâmetros de escalonamento: prioridade, tempo de CPU;

Imagem da memória: ponteiros, dados, pilha, tabelas de página;

Sinais: sinais sendo informados;

Demais informações de estado do sistema: estado, PID, PPID, identificação de grupo e usuário;

Basicamente, estas são as informações indispensáveis para que o sistema consiga interromper a execução de um processo (preempção) e possa posteriormente dar continuidade a seu processamento.

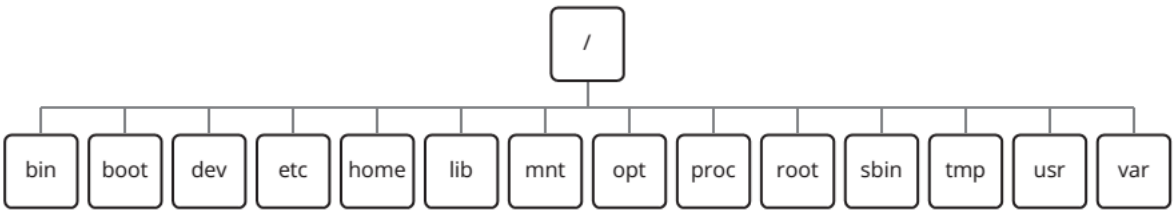
Gabarito: E

3 – Sistemas de Arquivos Linux

Como vimos, o **sistema de arquivos do Linux possui estrutura hierárquica, como decorrência do FHS**. A estrutura hierárquica torna mais fácil a localização e a manipulação de informações distribuídas por essa estrutura.



Atenção!!! No tocante a este tópico, existem pequenas variações de distribuição para distribuição, apesar do padrão FHS.



Vamos agora conhecer um pouco da função de cada diretório padrão da estrutura do Linux.

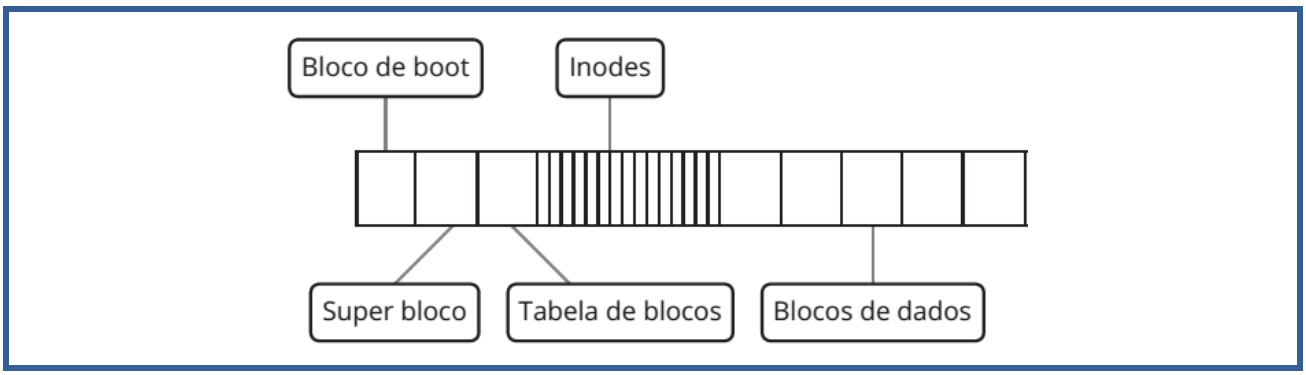
/	**diretório-raiz e origem da árvore hierárquica de diretórios**
/bin	binários do sistema utilizado pelos usuários
/boot	arquivos de inicialização do sistema
/dev	arquivos de dispositivos de entrada e saída
/etc	arquivos de configuração, scripts de inicialização de serviços, entre outros **Atenção!!! para o *./etc/fstab* importante arquivo de configuração de pontos de montagem.**
/home	diretórios pessoais dos usuários do Linux
/lib	bibliotecas compartilhadas pelos programas e pelo sistema
/mnt	diretório utilizado como ponto de montagens para dispositivos removíveis
/opt	diretório utilizado para instalar pacotes opcionais, que não fazem parte da distribuição
/proc	diretório virtual que contém o sistema de arquivos do kernel
/root	diretório pessoal do usuário root

/sbin	comandos de administração do sistema, utilizados pelo usuário root
/tmp	arquivos temporários do sistema e de programas
/usr	programas de uso geral do sistema
/var	arquivos de tamanho variável, como cache, logs, etc

Atributos de arquivos

No Linux os objetos manipulados pelo Sistema Operacional são armazenados na forma de arquivos, incluindo diretórios, dispositivos de hardware e conexões de rede.

Para identificar o tipo do arquivo, o Linux consulta as informações contidas em um índice, chamado ***inode***, que contém informações sobre blocos do sistema de arquivos.



Os arquivos possuem diversos atributos, que são armazenados na estrutura de arquivos correspondentes.

Resumindo

Entre esses atributos, podemos destacar:

Nome	**nome do arquivo.**
Localização	local onde o arquivo está armazenado no disco.
Tamanho	tamanho do arquivo em bytes.
Ligações	nomes pelos quais o arquivo é conhecido.
Propriedade	usuário dono (owner) do arquivo.
Grupo	grupo de usuários que pode ter acesso ao arquivo.

Tipo	tipo do arquivo.
Criação	data de criação do arquivo.
Modificação	data de modificação do arquivo.
Acesso	data do último acesso ao arquivo.
Permissão	permissões de acesso ao arquivo.

Todas essas informações e atributos dos arquivos são mantidas pelo sistema na medida em que os arquivos são criados e utilizados. Os diversos utilitários usam essas informações para processar e lidar com arquivos.

O Linux é um sistema projetado para ser multiusuário. Para suportar operações em ambientes com múltiplos usuários, o Linux dispõe de mecanismos que lidam com os atributos dos arquivos e restringem o acesso a arquivos e diretórios, baseados na identificação do usuário que solicita o acesso, e as permissões de acesso atribuídas a cada arquivo e diretório. Vamos a seguir ver a permissão de arquivos, que nesse sentido desempenha papel principal.

Permissões de arquivos

No Linux, todo arquivo ou diretório é associado a um usuário que é chamado de dono (owner). O usuário que inicialmente cria o arquivo é o dono do arquivo.

Cada arquivo ou diretório pode ser associado a um **grupo**, que é atribuído ao arquivo quando este é criado. Um grupo é um conjunto de usuários, a que cada usuário pode pertencer.

O usuário que cria o arquivo ou diretório determina o grupo que pode acessá-lo. Esse grupo associado ao arquivo ou diretório é o grupo primário do usuário que os criou. Tanto o dono como o grupo de um arquivo podem ser alterados, após essa definição inicial.

3.1 Permissões de Acesso



As **permissões de acesso**, conhecidas como modos de acesso, determinam as operações que um usuário, seu grupo, ou outras pessoas podem realizar em um arquivo. A seguir estão os três tipos básicos de permissão que podem ser aplicadas a um arquivo ou diretório.

- r (**read**): acesso apenas para leitura.
- w (**write**): acesso para leitura e gravação.
- x (**execute**): permite executar o arquivo.

Por exemplo, um arquivo que tenha as permissões rw pode ter seu conteúdo lido e escrito por um usuário, mas não pode ser executado por esse usuário, pois o arquivo não tem a permissão de execução x.

As permissões habilitam a execução de ações diferentes em arquivos e diretórios. Arquivos ou diretórios podem ter uma ou mais permissões.

As permissões também podem ser representadas por grupos de rwx, que de acordo com a sua posição podem representar as permissões do dono (primeiro conjunto), do grupo (segundo conjunto) e dos outros (terceiro conjunto).

ESQUEMATIZANDO

Dono	Grupo	Outros
Rwx	Rwx	Rwx
421	421	421

Cada grupo possui três bits, o **primeiro bit** do grupo é associado à permissão de leitura. O **segundo bit** do grupo indica a permissão de escrita. E o **terceiro bit** do grupo indica a permissão de execução.

Se um bit do grupo tiver o valor 0, indica ausência de permissão e, se tiver o valor 1, indica a presença da permissão.

A variação de cada conjunto de bits em um grupo representa o privilégio de realizar um determinado conjunto de ações, por exemplo:

- ✓ 7 - permite leitura, escrita e execução (rwx);
- ✓ 6 - permite leitura e escrita (rw);
- ✓ 4 - permite somente leitura (r);
- ✓ 3 - permite escrita e execução (wx);
- ✓ 2 - permite somente escrita (w);

- ✓ 1 - permite somente execução (x)

Se tivermos, por exemplo, um arquivo que tem permissão 764, significa que:

- ✓ 7 – leitura(4), escrita(2) e execução(1) = (7) para o **dono** (u);
- ✓ 6 - permite leitura(4) e escrita (2) = (6) para o **grupo** (g);
- ✓ 4 - permite leitura (r) = (4) para os **outros** (o).

3.2 PERMISSÕES ESPECIAIS

Além das permissões padrão, é possível também dispor no Linux das permissões especiais que veremos um resumo neste ponto. As permissões especiais são bits que podem ser setados e visam estender funções de permissionamento não previstas nas permissões padrão.

As permissões especiais podem ser de três tipos: suid, sgid e sticky bits.

O **bit suid** "Set User ID" quando está ativado o arquivo é executado com as permissões do dono e não com as permissões de quem executou. Por exemplo, um arquivo executável onde o dono é o root e o bit SUID está ativado, sempre roda com as permissões do root, ou seja, qualquer usuário pode executa-lo com privilégios de administrador. Identificamos se o bit suid está ativado por um “s” na permissão de execução (x) do dono.

O **bit sgid** "Set Group ID" quando está ativado o arquivo é executado com as permissões do grupo e não com as permissões de quem executou. Identificamos se o bit suid está ativado por um “s” na permissão de execução (x) do grupo.

O **sticky bit** é uma de permissão de acesso que pode ser atribuída a diretórios e arquivos em sistemas Linux. Ele indica que o arquivo ou diretório deve receber algum tratamento especial, nesse caso, os arquivos criados dentro do diretório apenas podem ser renomeados ou apagados pelo dono do arquivo, do diretório ou pelo superusuário, mesmo que possua outras permissões.

3.3 ARQUIVOS E DIRETÓRIOS LINUX

Vamos agora entender alguns tipos de arquivos existentes no Linux.

Arquivo comum

A estrutura básica que o Linux utiliza para armazenar informações é o arquivo. Nos arquivos são armazenados todos os tipos de dados, desde textos até instruções em código de máquina. Todos os tipos de informações necessárias para a operação do sistema são armazenados em arquivos.

Internamente, o sistema identifica os arquivos por números, mas para uma pessoa na prática, essa identificação perde o sentido. Dessa forma, o sistema permite a identificação dos arquivos através de nomes.

O nome do arquivo pode ter qualquer sequência de até 256 caracteres, suficiente para descrever o conteúdo do arquivo. Para um sistema com milhares de arquivos, é pouco provável que não sejam escolhidos nomes que já estejam sendo utilizados por outros arquivos.

Arquivos de dispositivos

O sistema de arquivos estende o conceito de arquivo para tratar os dispositivos de entrada e saída, como impressoras, ou outros tipos que podem ser instalados em um Sistema Linux.

Os arquivos de dispositivos são manipulados como arquivos especiais do sistema. Os arquivos de dispositivos podem ser de dois tipos:

- Arquivos de dispositivos **orientados a caractere**: realizam suas transferências de dados byte a byte, são exemplos as portas seriais orientadas a caractere.

- Arquivos de dispositivos **orientados a blocos de caracteres**: realizam transferências de dados em blocos de tamanho que pode variar entre 512 bytes e 32 Kbytes. Os discos rígidos e as unidades de fita são exemplos de dispositivos orientados a bloco.

Alguns dispositivos só podem ser acessados no modo caractere, como terminais e impressoras, pois não têm recursos para o acesso bloco a bloco.

Outros dispositivos permitem o acesso bloco a bloco, como discos e fitas, mas podem, também, ser acessados caractere a caractere, dependendo da operação efetuada. Por exemplo: na formatação de um disco, os blocos ainda não existem, logo, o acesso inicial a esse dispositivo deve ser orientado a caractere. Após a formatação inicial, o acesso é feito bloco a bloco.

Por convenção, **todos os dispositivos de Entrada e Saída no Linux recebem nomes individuais de arquivo e são agrupados no diretório /dev**, abreviatura de devices.

Diretório

Um diretório é um contêiner ou uma representação lógica utilizada nos sistemas de arquivos dos sistemas operacionais. Um diretório desempenha a mesma função que uma gaveta em armário, permitindo agrupar arquivos num lugar comum onde possam ser facilmente encontrados.

O diretório dá ao usuário flexibilidade para agrupar arquivos de forma lógica. Por exemplo, ao criar arquivos com as notas de um aluno, é possível agrupar esses arquivos em diretórios, com as notas por disciplina, por exemplo.

Existem diversos sistemas de arquivos, cada um organizando a seu modo os diretórios. Os tipos mais comuns de sistemas de arquivos são organizados na forma de diretório único ou de diretório em árvore.

O Linux utiliza a organização hierárquica ou em forma de árvore. Para o Sistema Operacional Linux, um **diretório** é um arquivo especial que contém uma listagem de nomes de arquivos e seus *inodes* (nó índice) correspondentes.

O diretório desempenha a função de um catálogo: dado o nome de um arquivo, o Sistema Operacional consulta seu diretório e obtém o número do *inode* correspondente ao arquivo.

Com o número do *inode*, o sistema de arquivos pode examinar suas tabelas internas para determinar onde está armazenado o arquivo e disponibilizá-lo ao usuário.

Os **diretórios podem ter nomes compostos por até 256 caracteres**. **Cada usuário do Linux tem seu diretório *home*, que geralmente possui o mesmo nome do usuário.**

Links

Vamos supor que o arquivo /home/professor/notas contenha informações de notas dos alunos de um professor e todos os alunos precisem acessar este arquivo. Imagine o trabalho que daria copiar este arquivo para o diretório home de cada aluno e mantê-los atualizados.

Com os links simbólicos criamos um link em cada diretório home dos alunos, que aponta para o arquivo original localizado no diretório /home/professor/notas, reduzindo o trabalho e mantendo o acesso às informações sempre atualizadas. Cada aluno pode criar seus links com nomes diferentes em seu diretório home, apontando para o mesmo arquivo original.

Ao criar um arquivo do tipo link em seu diretório home, o usuário evita a digitação de todo o caminho do arquivo, por exemplo, manipulando-o diretamente através de seu diretório home. O comando para a criação de um arquivo do tipo link possui a sintaxe:

```
# ln –[opções] origem [destino]
```

Onde origem ou destino podem ter um nome de arquivo ou o caminho completo do arquivo na estrutura hierárquica do diretório.

3.4 EXT

Ext3

Sistemas de arquivos padrão utilizados no Linux, sendo a versão atual o ext4. A partir da versão ext3, já possui suporte a journaling.

É o mais comum sistemas de arquivos no Linux, muitas distribuições o utilizaram como padrão e também temos aplicações especificamente desenhadas para Ext3.

O Ext3 é o sistema de arquivos Linux mais familiar para maioria dos administradores Linux. Suas principais desvantagens são:

- ✓ Tempo de reparo (fsck) pode ser extremamente longo;
- ✓ Escalabilidade limitada (tamanho máximo de arquivos 16TB).

EXT4

É o sistema de arquivos sucessor do ext3. Suas principais características são:

- ✓ Uso de extents;
- ✓ Fsck mais rápido (aproximadamente 10x mais rápido que ext3);
- ✓ Muito similar e relativamente familiar para usuários ext3.

XFS

É um sistema de arquivos Linux desenvolvido para suportar quantidades massivas de dados (suporta sistemas de arquivos de ate 9 Exabytes). Suas principais características são:

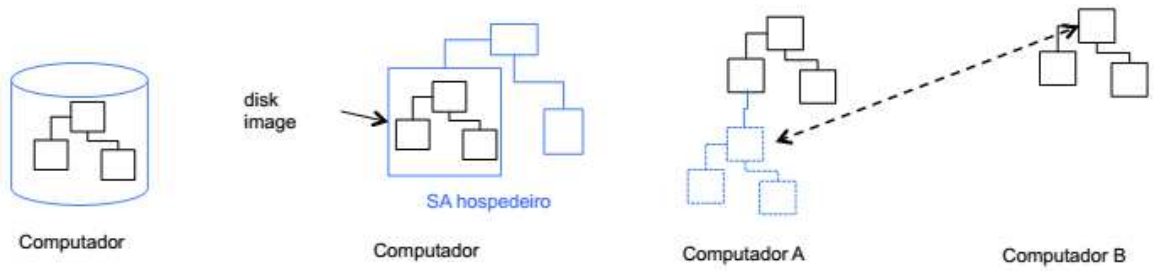
- ✓ Alta performance para grandes quantidades de dados;

- ✓ Muitos anos de uso em grandes ambientes (>16TB);
- ✓ A maior parte de seus metadados é organizado em árvores B+.

3.5 NFS

Um sistema de arquivos pode estar contido em uma partição de um disco local, ou então estar em um arquivo de um sistema de arquivos hospedeiro, ou ainda em partição no disco de outro computador e acessível pela rede.

As figuras abaixo exemplificam essa diversidade de locais nos quais os sistemas de arquivos podem estar localizados.

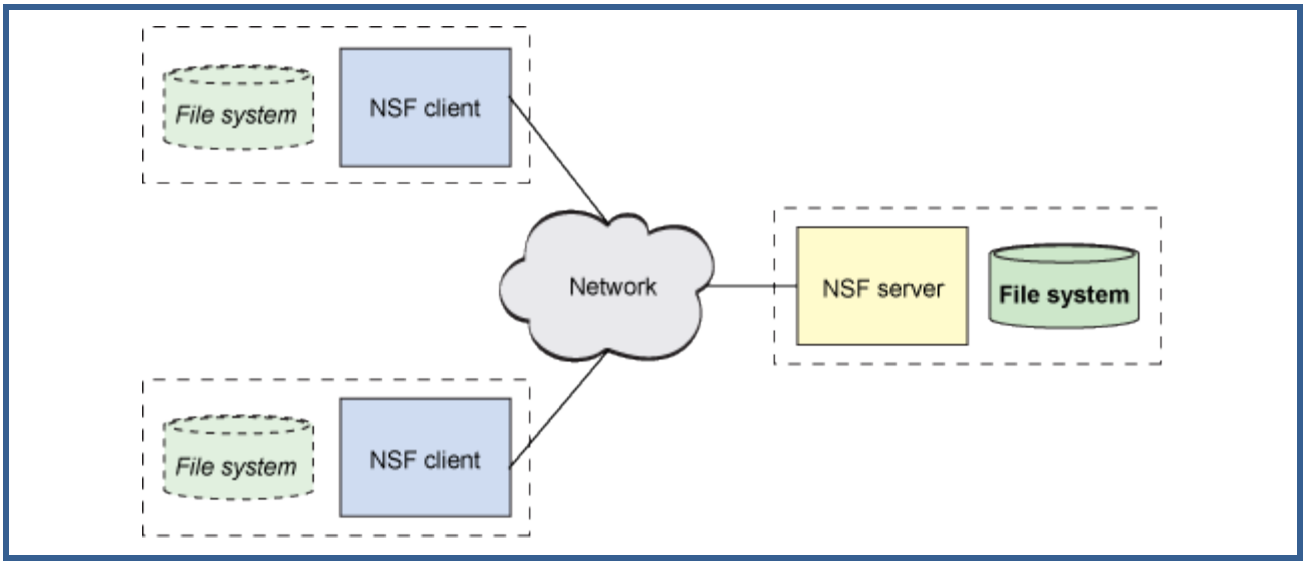


Um **sistema de arquivos remoto ou de rede** é uma abstração em rede de um sistema de arquivos que permite que um cliente remoto o acesse pela rede de uma forma semelhante a um sistema de arquivos local.

Embora não tenha sido o primeiro desse tipo de sistema, o NFS cresceu e evoluiu para o sistema de arquivos de rede mais poderoso e mais amplamente usado em sistemas Linux (e Unix Like).

O NFS permite o compartilhamento de um sistema de arquivos comum entre os usuários e oferece a centralização de dados para minimizar o armazenamento necessário.

O NFS segue o modelo computacional cliente/servidor, como ilustra a figura abaixo.



O servidor implementa o sistema de arquivos e o armazenamento compartilhados aos quais os clientes se conectam. Os clientes implementam a interface com o usuário para o sistema de arquivo compartilhado, disposto no espaço no arquivo do cliente.

No Linux, o sistema de arquivo virtual (VFS) determina para qual armazenamento uma solicitação é destinada e qual sistema de arquivos deve ser usado para satisfazer a solicitação.

Por esse motivo, o NFS é um sistema de arquivos conectável como qualquer outro. A única diferença com o NFS é que as solicitações de entrada/de saída podem não ser atendidas localmente, tendo, em vez disso, que atravessar a rede para sua conclusão.

O NFS não é um sistema de arquivos no sentido tradicional, mas um protocolo para acessar sistemas de arquivos remotamente.

As versões mais antigas do NFS usavam o protocolo UDP, mas atualmente o TCP é o mais comumente usado para dar uma maior confiabilidade.

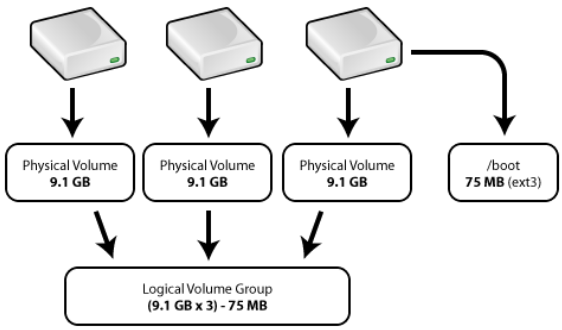
3.6 Logical Volume Manager

O Gerenciamento de Volumes Lógicos (LVM) é uma maneira mais flexível de criar, excluir, redimensionar e expandir partições do sistema de arquivos.

Ao invés de abrigar as informações sobre as partições na tabela de partições, o LVM escreve suas próprias informações em separado e mantém o controle sobre a localização das partições, quais dispositivos são partes delas e o tamanho de cada uma. Se faltar espaço, é só adicionar no LVM outros discos rígidos.

O LVM permite alocar espaço do disco rígido em volumes lógicos que podem ser facilmente redimensionados, ao contrário das partições.

Com o LVM, o disco rígido ou conjunto de discos rígidos é alocado em um ou mais volumes físicos, sendo que um volume físico não pode ultrapassar mais de um disco. O grupo de volume lógico é dividido em volumes lógicos.





A estruturação de um LVM cria os seguintes containeres lógicos:

- ✓ PV (**Phisical Volume**) - Corresponde ao disco rígido/partição ou dispositivo de bloco que será adicionado ao LVM. Os aplicativos que manipulam o volume físico, começam com as letras pv*.
- ✓ VG (**Volume Group**) - Corresponde ao agrupamento de PVs que fazem parte do LVM. O que deve ficar bem claro sobre os VGs é que sua função é agrupar os PVs. Do VG alocamos os espaços para criação dos volumes lógicos. Os aplicativos que manipulam o grupo de volume, começam com as letras vg*.
- ✓ LV (**Logical Volume**) - Corresponde a cada partição lógica criada no VG pelo LVM para gravação de dados. Ao invés de ser identificada por nomes de dispositivos, podem ser usados nomes comuns para se referir as partições. O Volume lógico é a área onde o sistema de arquivo é criado para gravação de dados.

- ✓ PE (**Physical Extends**, ou extensão física) – é uma divisão do espaço disponível no volume físIco (PV).
- ✓ LE (**Logical Extends**, ou extensões lógicas) - é uma divisão de espaço do volume lógico (LV), corresponde aos PE (Physical Extends) alocados.

O LVM diferencia-se dos demais esquemas de particionamento modernos, pois permite que os discos sejam divididos em partições de tamanho variável, e essa divisão pode ser realizada com um sistema em funcionamento.



3.7 RESOLUÇÃO DE QUESTÕES

48. (2017 - Quadrix - COFECI - Assistente de TI) – Quanto à nomeação de arquivos, as extensões são partes obrigatórias dos nomes dos arquivos nos sistemas Unix.

Comentários:
É comum nos sistemas operacionais Windows associar a extensão de um arquivo a uma característica (executável ou instalável) ou associação a um programa. Uma peculiaridade do Linux é que as extensões são mais flexíveis e não se prestam somente a este fim, por conta disto extensões não são obrigatórias na maioria dos sistemas Linux. Assertiva errada.

Gabarito: Errada

---

49. (2016 - FCC - TRT - 23ª REGIÃO (MT) - Técnico Judiciário - Tecnologia da Informação) – Bento, administrador de um servidor com sistema operacional Linux, escreveu um shell script para automatizar o processo de backup do sistema. Para que apenas Bento possa executar o shell script criado, as permissões devem ser alteradas utilizando o comando chmod com o parâmetro

a) 707.
b) 660.
c) 700.
d) 006.

e) 077.

Comentários:
As permissões de um arquivo são alteradas através do comando ***chmod*** (change mode). Cada uma das nove permissões (ler, escrever e executar; para o dono, para o grupo e para os outros) pode ser individualmente concedida ou negada com esse comando. Como vimos, o primeiro algarismo é que define as permissões para o dono do arquivo. Lembrando que o sistema de permissões "*rwx*" do Linux é substituível pelo equivalente numérico:

R	w	x
4	2	1

Para que apenas o usuário proprietário de um arquivo possa executá-lo, as permissões devem ser alteradas com o comando ***chmod 700***.

Gabarito: C

---

50. (2016 – FCC - TRT - 23ª REGIÃO (MT) - Analista Judiciário - Tecnologia da Informação) – Uma partição NFS remota deve ser montada em um computador com sistema operacional Linux. Para especificar, no comando **mount**, que a partição é NFS, deve-se utilizar a opção:

a) –n.
b) –f.
c) –i.
d) –s.
e) –t.

Comentários:
Vale a pena lembrar que os comandos e parâmetros no Linux buscam ser intuitivos. Então, para memorizar ou recordar a função de um parâmetro, tente associá-lo a ao propósito indagado. O Comando ***mount*** permite definir como uma partição deve ser montada em um sistema operacional Linux. Os parâmetros podem ser: ***-a*** (monta todos os sistemas de arquivos em /etc/fstab), ***-h ou --help*** (exibe as opções do mout). O parâmetro ***–t*** define o tipo de sistema de arquivo que será montado, por exemplo, ext3, nfs ou ntfs. Assim, o gabarito da questão é a letra E.

Gabarito: E

51. (FCC – 2012 - TRT6 - Apoio Especializado/Tecnologia da Informação) - Filesystem Hierarchy Standard (FHS) é a padronização da organização do sistema de arquivos do sistemas Linux à qual aderem as principais distribuições. De acordo com a FHS, arquivos executáveis que precisam estar disponíveis em single user mode, arquivos cujo conteúdo varia ao longo da operação do sistema e arquivos de configuração do sistema devem localizar-se, respectivamente, em

a) /boot, /tmp e /usr/share.
b) /usr/bin, /tmp e /usr/local.
c) /bin, /opt e /usr/local.
d) /boot, /usr e /etc.
e) /bin, /var e /etc.

Comentários:

A correlação correta consta da alternativa E:

/bin - arquivos executáveis binários;

/var - arquivos variáveis ao longo da operação do sistema;

/etc - arquivos de configuração do sistema.

Gabarito: E

52. (FCC – 2013 - DPE SP - Engenheiro de Redes) - O administrador de um servidor, com sistema operacional Linux, deseja configurar uma nova interface de rede instalada no servidor. Para isso ele deve verificar se o driver de dispositivo da nova interface está disponível no sistema operacional. Por padrão, os drivers de dispositivo no sistema operacional Linux são instalados no diretório

a) /bin.
b) /etc.
c) /lib.
d) /dev.
e) /sys.

Comentários:

A correlação correta consta da alternativa D.

As alternativas A, B, C e E estão equivocadas e a relação correta é apresentada abaixo:

/bin - arquivos executáveis binários;

a) /etc- arquivos de configuração do sistema;

b) /lib – bibliotecas compartilhadas;

c) /sys – sistema de arquivos virtual.

Gabarito: D

---

53. (FCC – 2013 - TRT5 - Apoio Especializado/Tecnologia da Informação) - Arquivos em Linux são protegidos atribuindo-se a cada um deles um código de proteção de 9 bits. O código de proteção consiste em campos de 3 bits, um grupo para qualquer usuário, outro para o usuário do arquivo e um para o grupo ao qual o usuário pertence. Cada campo possui um bit de permissão de leitura, um bit de permissão de escrita e outro de permissão de execução. Por exemplo, o código de proteção de um arquivo definido como "-wxr-xr--" significa que:

a) membros do grupo e o proprietário podem ler, executar e escrever no arquivo e outros usuários podem apenas ler.
b) membros do grupo podem escrever e executar o arquivo, qualquer usuário pode ler e executar o arquivo e o dono do arquivo pode apenas ler o conteúdo do arquivo.
c) qualquer usuário pode escrever e executar o arquivo, o proprietário pode ler e executar o arquivo e membros do grupo podem apenas ler o arquivo.
d) o proprietário pode escrever e executar o arquivo, membros do grupo podem ler e executar o arquivo e qualquer usuário pode ler o arquivo.
e) o proprietário pode ler, escrever e executar o arquivo, membros do grupo podem ler e escrever no arquivo e qualquer usuário pode ler e executar o arquivo.

Comentários:

A questão apresenta um permissionamento -wxr-xr-- (354), cujo leitura é a seguinte:

- ✓ -wx (3)=> proprietários do arquivo podem escrever e executar;
- ✓ r-x (5)=> membros do mesmo grupo do proprietário podem somente ler e executar;
- ✓ r--(4) => outros (qualquer usuário) podem somente ler

Gabarito: D

---

54. (2012 - FCC - TRT6 - Apoio Especializado/Tecnologia da Informação) - Filesystem Hierarchy Standard (FHS) é a padronização da organização do sistema de arquivos do sistemas Linux à qual aderem as principais distribuições. De acordo com a FHS, arquivos executáveis que

precisam estar disponíveis em single user mode, arquivos cujo conteúdo varia ao longo da operação do sistema e arquivos de configuração do sistema devem localizar-se, respectivamente, em

a) /boot, /tmp e /usr/share.
b) /usr/bin, /tmp e /usr/local.
c) /bin, /opt e /usr/local.
d) /boot, /usr e /etc.
e) /bin, /var e /etc.

Comentários:

A correlação correta consta da alternativa E:

/bin - arquivos executáveis binários;

/var - arquivos variáveis ao longo da operação do sistema;

/etc- arquivos de configuração do sistema.

Gabarito: E

---

55. **(VUNESP – 2015 - TCE-SP - Agente da Fiscalização Financeira - Infraestrutura de TI e Segurança da Informação)** - Nos sistemas operacionais Linux, o diretório raiz do sistema é identificado pelo caractere

a) \ (barra inclinada para a esquerda).
b) / (barra inclinada para a direita).
c) $ (sinal de dólar).
d) # (cerquilha).
e) : (dois pontos).

Comentários:

Nos sistemas operacionais Linux, o diretório raiz do sistema é identificado pela barra inclinada para a direita (/). A estrutura de diretórios é hierárquica (FHS) e toda ela deriva do diretório raiz.

Gabarito: B

---

56. **(UFPR – 2010 - UFPR - Analista de Tecnologia da Informação)** - Sobre estrutura de diretório do Linux, assinale a alternativa correta.

a) /etc - Contém os arquivos que virtualizam todos os dispositivos de entrada/saída.
b) /dev - Contém os arquivos de configuração específicos da máquina.
c) /Bin - Contém as bibliotecas compartilhadas necessárias aos programas e aos módulos de kernel.
d) /mnt - Contém os arquivos para a área de swap.
e) /var - Contém logs, filas de impressão e outros arquivos alterados dinamicamente pelo sistema.

Comentários:

As alternativas A, B, C e D estão equivocadas. As finalidades corretas são descritas abaixo:

a) /etc - arquivos de configuração, scripts de inicialização de serviços, entre outros;
b) /dev - arquivos de dispositivos de entrada e saída;
c) /bin - binários do sistema utilizado pelos usuários;
d) /mnt - diretório utilizado como ponto de montagens para dispositivos removíveis.

Gabarito: E

---

57. (FUMARC – 2014 - AL-MG - Analista de Sistemas) - Qual é pasta padrão em que ficam armazenados os logs de sistemas operacionais GNU/LINUX?

a) /log
b) /sys/log
c) /var/log
d) /tmp/log

Comentários:

O diretório /var armazena arquivos de tamanho variável, como cache, logs, etc. Os logs do Linux por padrão são armazenados em /var/log.

Gabarito: C

---

58. (VUNESP – 2010 - CREMESP - Administrador de Banco de Dados) - No sistema operacional Linux, o diretório /etc/skel tem a função de armazenar

a) a estrutura de dispositivos montados e em uso pelo sistema operacional.
b) as configurações de processo e aplicações gerenciados pelo sistema.
c) o modelo de configuração de ambiente para os usuários criados.
d) os dados criptografados do arquivo original /etc/ passwd.
e) os dados de proxy e cookie para o acesso à rede Internet.

Comentários:

Já pensou se para cada usuário criado fosse necessário redefinir a configuração das variáveis de ambiente. O Linux facilita a vida ao permitir criar um esqueleto com as configurações de variáveis de ambiente. No Linux, o diretório /etc/skel (skeleton) guarda o modelo de configuração de ambiente para os usuários criados. Alternativa C correta.

Vamos aos erros das demais alternativas:

a) a estrutura de dispositivos montados e em uso pelo sistema operacional fica em /mnt.
b) as configurações de processos e aplicações gerenciados pelo sistema são guardadas em /proc.
d) os dados criptografados de senhas /etc/ shadow.
e) os dados de proxy e cookie para o acesso à rede Internet ficam em /var/log/squid, por exemplo.

Gabarito: C

---

59. **(VUNESP – 2014 - Câmara Municipal de São José dos Campos - SP - Analista Legislativo - Analista de Sistemas)** - No sistema operacional Linux, a configuração de controle de acesso definida pelo sticky bit é

a) ignorada quando aplicada diretamente a arquivos.
b) utilizada para identificar diretórios remotos acessados via NFS.
c) aplicável apenas a partições do tipo ext3 e ext4.
d) utilizada pelo SELinux para estabelecer suas políticas de controle de acesso.
e) aplicada a todos os arquivos e diretórios que pertencem ao usuário “root”.

Comentários:

O sticky bit é uma permissão de acesso que pode ser atribuída a diretórios e arquivos em sistemas Linux. Ele indica que o arquivo ou diretório deve receber algum tratamento especial pelo sistema operacional. Essa permissão geralmente é aplicada a diretórios. Nesse caso, os arquivos criados dentro do diretório apenas podem ser renomeados ou apagados pelo dono do arquivo, do diretório ou pelo superusuário. Embora exista uma concordância sobre a funcionalidade dessa permissão quando aplicada a diretórios, quando ela é aplicada a arquivos sua função varia de

acordo com o sistema operacional utilizado. Os sistemas Linux, por exemplo, ignoram o sticky bit em arquivos.

Gabarito: A

---

60. (2013 – IADES – EBSERH - Analista de Tecnologia da Informação - Suporte e Redes) - O FHS (Filesystem Hierarchy Standard) é uma referência para a organização dos flesystems Unix. Essa referência prevê que haverá um diretório, volátil, pois os dados poderão ser apagados durante o boot do sistema, para o armazenamento temporário de arquivos; e um outro para configurações gerais do sistema. Esses dois diretórios são, respectivamente,

a) /var/tmp e /bin
b) /tmp e /var/tmp
c) /etc e /bin
d) /tmp e /etc
e) /etc e /tmp

Comentários:
Pessoal, como vimos, o FHS (Filesystem Hierarchy Standard) é a principal referência para a organização dos flesystems em sistemas Linux. Segundo o FHS, o armazenamento temporário de arquivos é realizado no diretório ***/tmp***; já o diretório para configurações gerais do sistema é o ***/etc***. Assim, a alternativa que apresenta respectivamente e corretamente os diretórios é a letra D.

Gabarito: D

---

61. (2011 – IADES - PG-DF - Analista Jurídico - Analista de Sistemas) - As permissões de acesso a arquivos em um sistema operacional de rede, como o Linux, obedecem aos direitos de usuário, de grupo e outros. Analisando as permissões dos arquivos, assinale a alternativa que apresenta um arquivo com direito de execução para qualquer usuário do sistema.

a) -rw-rw-rw- 1 ricardo suporte 706113 2010-10-04 16:02 manual.pdf
b) drwxr-x--- 2 maria copa 4096 2010-10-11 16:45 Documentos
c) -rwxr--r-- 1 pedro drh 1458 2010-11-17 10:40 calculo.sh
d) crw------- 1 root root 4, 1 2011-02-21 09:27 tty1
e) -rwxr-xr-x 54 jose users 4096 2011-02-28 11:45 planilha.xls

Comentários:
A questão solicita que assinalemos a alternativa que apresenta um arquivo com direito de execução para qualquer usuário do sistema. Para identificar qual alternativa corresponde ao

solicitado temos que ter em mente dois pontos: cada permissão é constituída de três caracteres (parâmetros) **r** (read), **w** (write) e **x** (execute); é possível atribuir um grupo de permissões ao **owner** (primeiro grupo de três caracteres), ao **grupo** do proprietário (segundo grupo de três caracteres) e a **outros** (terceiro grupo de três caracteres). Além disso, temos que lembrar que o primeiro caractere à esquerda do grupo de permissões indica o tipo do arquivo (no caso o – indica que se trata de um arquivo comum, se tivéssemos um d, seria um diretório). Assim, a única opção que apresenta um arquivo com direito de execução para qualquer usuário do sistema é a letra E: rw**x**r-**x**r-**x.**

Gabarito: E

---

62. (2011 – IADES - PG-DF - Analista Jurídico - Analista de Sistemas) - Um determinado documento, gravado em um disco da rede de computadores de um órgão público, possui os seguintes atributos: -rw-r--r-- 1 root root 1789 2010-07-20 10:47 passwd. Analise as permissões de acesso a esse arquivo e assinale a alternativa correta.

a) O dono do arquivo pode ler, gravar e executar o arquivo, ao passo que os demais usuários têm somente permissão de leitura.
b) O dono do arquivo, seu grupo e todos os demais usuários da rede podem ler e copiar o conteúdo desse arquivo.
c) O grupo de trabalho a que pertence esse arquivo tem apenas permissão de leitura e execução sob o mesmo.
d) Todos os usuários da rede podem executar esse arquivo, porém somente o dono tem permissão de gravação/alteração.
e) Nenhum outro usuário da rede, exceto o dono, pode executar esse arquivo e somente o dono e grupo podem lê-lo.

Comentários:
A questão informa as permissões do arquivo (-rw-r--r--). Podemos notar que o owner, group e others tem permissão de leitura. Assim, nada os impede de copiar o arquivo. Assim, a alternativa B é a correta.

Gabarito: B

---

63. (2013- CETRO – ANVISA - Analista Administrativo - Área 5) - Assinale a alternativa que apresenta o valor numérico da permissão utilizando o chmod de "-rwxrwxrwx" no sistema operacional Linux.

a) 625.

b) 125.
c) 777.
d) 888.
e) 327.

Comentários:
Pessoal, relembrando a parte teórica já vista, o sistema de permissões "*rwx*" do Linux é substituível pelo equivalente numérico:

R	w	x
4	2	1

Então, para um chmod atribuindo "-rwxrwxrwx", teríamos a seguinte equivalente numérica

Rwx	rwx	rwx
4+2+1=7	4+2+1=7	4+2+1=7

Gabarito: C

---

64. **(2018 - CESPE - STJ - Técnico Judiciário - Suporte Técnico)** - Acerca dos ambientes de servidores Windows e Linux, julgue o próximo item. Em Linux, as partições são conceitualmente distintas e separadas umas das outras, entretanto /dev/sda é o arquivo de dispositivo de bloco do disco, essencialmente uma imagem do disco inteiro. Assim, comandos em nível de usuário podem acessar o disco diretamente por meio desse arquivo.

Comentários:

O diretório /dev no Linux tem a função muito peculiar de permitir o acesso direto aos dispositivos por outras aplicações. Este diretório /dev é organizado em subdiretórios especializados destinados a cada tipo de dispositivo específico. Por exemplo, o subdiretório /dev/sda, citado na questão, aponta para o disco. Logo, percebemos que está correta a assertiva chave na questão "comandos em nível de usuário podem acessar o disco diretamente por meio desse arquivo".

Gabarito: Certa

---

65. **(CESPE – 2013 - TRT10 - Apoio Especializado/Tecnologia da Informação)** - Em todas as instalações do Linux, o /boot funciona como um sistema de arquivo próprio, sem formatação básica, que armazena o kernel do Linux.

Comentários:

Pessoal, sobre esta questão um ponto importante é não confundam o processo de boot do Linux com o seu diretório /boot.

O processo de boot começa após o computador ser ligado, com a BIOS carregando o setor de Boot (os primeiros 512 bytes do disco) para a memória, setor conhecido como MBR (Master Boot Record).

Na MBR fica localizado o gerenciador de Boot, o Grub (Grand Unified Bootloader) ou o LILO (Linux Loader). O processo de boot termina após a inicialização (/etc/init.tab) integral do sistema.

O diretório /boot armazena os arquivos de inicialização do sistema Linux. Sua formatação é realizada no decorrer do processo de instalação do sistema.

Gabarito: Errada

---

66. **(CESPE – 2013 - TRT10 - Apoio Especializado/Tecnologia da Informação)** - Se o disco for compartilhado, o ponto de montagem-padrão do Linux corresponde ao diretório /win, local em que se instala o sistema Windows.

Comentários:

Quando conectamos um dispositivo - usb, DVD, etc – em um sistema Linux ele é um dispositivo como qualquer outro. Ficará disponível em /dev/nome_dispositivo , mas não poderá ser lido ou modificado.

Para possa ser acessado, é necessário que seja montado. O ponto de montagem é a pasta no sistema onde o conteúdo do dispositivo estará disponível para que possa ser lido ou alterado.

Nas distribuições Linux mais atuais, a montagem de dispositivos é feita automaticamente. Em distribuições antigas, é necessário montar o dispositivo usando o comando "mount". E desmontar com o comando "umount".

O ponto de montagem-padrão do Linux corresponde ao diretório /mnt.

Gabarito: Errada

---

67. **(CESPE - 2012 - TRE RJ - Apoio Especializado/Análise de Sistemas)** - O /etc/config é o arquivo de configuração do Linux que inicia o boot normal do sistema, ao ler os scripts de inicialização e carregar os módulos de software especificados.

Comentários:

O /etc/init.tab é o arquivo de configuração do Linux, utilizado como base para o processo de boot do sistema.

Gabarito: Errada

---

68. **(CESPE – 2013 - TRT10 - Apoio Especializado/Tecnologia da Informação)** - Os diretórios /etc e /lib contêm, respectivamente, os arquivos de configuração dos sistemas do tipo Linux e os arquivos de bibliotecas do sistema.

Comentários:

A tabela abaixo apresenta um resumo dos principais diretórios do Linux:

/	diretório-raiz e origem da árvore hierárquica de diretórios
/bin	binários do sistema utilizado pelos usuários
/boot	arquivos de inicialização do sistema
/dev	arquivos de dispositivos de entrada e saída
/etc	arquivos de configuração, scripts de inicialização de serviços, entre outros
/home	diretórios pessoais dos usuários do Linux
/lib	bibliotecas compartilhadas pelos programas e pelo sistema
/mnt	diretório utilizado como ponto de montagens para dispositivos removíveis
/opt	diretório utilizado para instalar pacotes opcionais, que não fazem parte da distribuição
/proc	diretório virtual que contém o sistema de arquivos do kernel

/root	diretório pessoal do usuário root
/sbin	comandos de administração do sistema, utilizados pelo usuário root
/tmp	arquivos temporários do sistema e de programas
/usr	programas de uso geral do sistema
/var	arquivos de tamanho variável, como cache, logs, etc

A assertiva está correta, o diretório /etc contém os principais arquivos de configuração e o /lib armazena as bibliotecas do Linux.

Gabarito: Certa

---

69. (CESPE – 2013 - PCF/Área 3) - No Linux, os usuários são cadastrados no sistema no arquivo /home, que guarda uma entrada para cada usuário, incluindo-se o diretório e o shell.

Comentários:

No Linux os usuários criados constam do arquivo /etc/passwd, nesse arquivo podemos identificar o diretório home e o shell do usuário. As senhas criptografadas são armazenadas no arquivo /etc/shadow. O diretório /home é o diretório padrão dos usuários, no qual são armazenados arquivos e demais informações de usuários. Assertiva incorreta.

Gabarito: Errada

---

70. (CESPE – 2014 - TJ-SE - Analista Judiciário - Suporte Técnico em Infraestrutura) - No diretório /dev/, são encontrados diversos dispositivos de hardware instalado no Linux.

Comentários:

O diretório /dev armazena arquivos de dispositivos de entrada e saída.

Gabarito: Certa

---

71. **(CESPE – 2012 - TRE RJ - Apoio Especializado/Operação de Computador)** - No Linux, em um arquivo com permissões 764, os usuários do mesmo grupo que o proprietário podem ler, escrever e executar o arquivo.

Comentários:

As permissões de acesso, ou modos de acesso, determinam as operações que um usuário pode realizar em um arquivo. Os três tipos básicos de permissão que podem ser aplicadas a um arquivo ou diretório são:

r (read): permite acesso apenas para leitura.

w (write): permite acesso para leitura e gravação.

x (execute): permite executar o arquivo.

As permissões também podem ser representadas por grupos de rwx, que de acordo com a sua posição pode representar as permissões do dono (primeiro conjunto), do grupo (segundo conjunto) e dos outros (terceiro conjunto).

Cada número corresponde a três bits, sendo o primeiro deles associado à permissão de leitura, o segundo à permissão de escrita e o terceiro à permissão de execução. Se o bit tiver o valor 0, indica ausência de permissão e, se tiver o valor 1, indica a presença da permissão.

Rwx	Rwx	Rwx
421	421	421
Dono	Grupo	Outros

7 - permite leitura, escrita e execução (rwx);

6 - permite leitura e escrita (rw);

4 - permite somente leitura (r);

3 - permite escrita e execução (wx);

2 - permite somente escrita (w);

1 - permite somente execução (x)

A questão informa que o arquivo tem permissão 764, logo:

- ✓ 7 - leitura, escrita e execução (rwx) para o dono (u);
- ✓ 6 - permite leitura e escrita (rw) para o grupo (g);
- ✓ 4 - permite leitura (r) para os outros (o).

Os usuários do mesmo grupo que o dono dos arquivos podem somente ler e escrever. Assertiva incorreta.

Gabarito: Errada

---

72. (CESPE – 2013 - BACEN - Área 1 - Análise e Desenvolvimento de Sistemas) - Em sistemas Unix, a proteção de arquivos é efetuada pelo controle dos campos dono, grupo e universo, compostos de três bits (rwx), que definem se um usuário pode ler, escrever ou executar o arquivo.

Comentários:
Assertiva correta, conforme visto na explicação nas questões anteriores.

Gabarito: Certa

---

73. (2010 – CESPE - TRT - 21ª Região (RN) - Analista Judiciário - Tecnologia da Informação) - No Linux, o diretório raiz, que é representado pela barra /, e o diretório representado por /dev servem para duas funções primordiais ao funcionamento do ambiente: o primeiro é onde fica localizada a estrutura de diretórios e subdiretórios do sistema; o segundo é onde ficam os arquivos de dispositivos de hardware do computador em que o Linux está instalado.

Comentários:
Confere pessoal. É a partir do diretório **/** ou diretório raiz que é criada toda a estrutura de diretórios do Linux. O diretório /dev é onde ficam os arquivos de dispositivos de hardware.

Gabarito: Certa

---

74. (2014 – CESPE - TJ-SE - Analista Judiciário - Suporte Técnico em Infraestrutura) - Na estrutura de arquivos do sistema operacional, o diretório /var/ contém o spool de impressora.

Comentários:

O diretório /var é o diretório por excelência das estruturas variáveis do sistema. O spool de impressora é uma fila que armazena os arquivos que a serem impressos. Por sua natureza variável, o spool fica no diretório /var, em /var/spool. Questão Correta.

Gabarito: Certa

---

75. (2015 – CESPE - TRE-GO - Analista Judiciário) - No Linux, todo arquivo executável tem como extensão o sufixo .exe.

Comentários:
Errado. Pessoal, vimos que a possibilidade de execução de um arquivo é denotada pela presença da letra x, nas permissões de arquivo, para o dono, para o grupo e para outros: **rwx** rwx **rwx**. Não é a presença de um sufixo .exe que determina se um arquivo será executável ou não.

Gabarito: Errada

---

76. (2012 – CESPE - TRE-RJ - Cargos de Nível Superior) - No Linux, o diretório /bin contém programas do sistema que são utilizados pelos usuários, não sendo necessário, para que esses programas sejam executados, que eles possuam a extensão .exe.

Comentários:
Atenção para a diferença com o diretório **/sbin** que contém arquivos executáveis necessários para o boot e somente podem ser executados pelo usuário root.
O diretório **/bin** contém programas do sistema que são utilizados pelos usuários.
A possibilidade de execução no sistema Linux não depende de extensão .exe, e sim da permissão de execução. Portanto, para que esses programas sejam executados, não é necessário que eles possuam a extensão .exe.

Gabarito: Certa

---

77. (2015 - FCC - TRT/MG - Analista Judiciário - Adaptada) - As versões Ext2, Ext3 e Ext4 dos sistemas de arquivos utilizados Linux apresentam a inclusão de novos recursos e a ampliação da capacidade de armazenamento no decorrer da evolução. O que de fato diferencia o Ext2 do Ext3 é a inclusão

(A) da capacidade de formatar e gerenciar adequadamente mídias removíveis como pen drives e cartões SD.

(B) do recurso de alocação do mesmo dado em blocos múltiplos para aumentar a velocidade de acesso ao dado.

(C) da alocação postergada, o que reduz a quantidade de acessos físicos ao disco, reduzindo o tempo de acesso.

(D) do journaling, que aumenta a confiabilidade e elimina a necessidade da checagem do sistema de arquivos após uma parada repentina.

(E) da checagem rápida FSCK sem que haja a necessidade de checar a tabela de alocação.

Comentários:

a) **Alternativa Errada** – Ext2 ou Ext3 não permitem gerenciar mídias. Não é um diferencial entre Ext2 e Ext3.

b) **Alternativa Errada** – do recurso de alocação do mesmo dado em blocos múltiplos para aumentar a velocidade de acesso ao dado. Essa é uma caracteristica do Ext2.

c) **Alternativa Errada** – da alocação postergada, o que reduz a quantidade de acessos físicos ao disco, reduzindo o tempo de acesso. Não é um diferencial entre Ext2 e Ext3.

d) **Certa** - Ext2 não possui journaling. Certa.

e) **Alternativa Errada** – da checagem rápida FSCK sem que haja a necessidade de checar a tabela de alocação. Ext2 e Ext3 possuem checagem rápida.

Gabarito: D

---

78. (2015 – FCC - TRT/RS - Analista Judiciário - TI) - A possibilidade de compartilhar arquivos entre diferentes sistemas operacionais é fundamental para aumentar a produtividade computacional. A montagem automática de uma partição com sistema de arquivos CIFS, durante o boot do servidor com sistema operacional Linux, deve ser configurada no arquivo

(A) /etc/fstab.

(B) /boot/mount.

(C) /etc/mount.

(D) /boot/inittab.

(E) /etc/initd.

Comentários:

Questão bastante simples pessoal. O arquivo ***/etc/fstab*** permite configurar a montagem de uma partição, durante o boot de um servidor Linux. A coluna tipo do arquivo permite definir o sistema de arquivos e a coluna de opções permite indicar o tipo de montagem. Gabarito letra A.

Gabarito: A

---

79. (Quadrix – 2012 - DATAPREV - Engenheiro de Segurança do Trabalho) - Considere o sistema operacional Linux e assinale a alternativa correta.

a) O usuário pode escolher a interface gráfica que deseja usar, como o Bash, por exemplo.
b) Os diretórios particulares dos usuários são criados dentro do diretório /home por padrão.
c) Não há necessidade de se ter uma "conta de usuário" para se logar em um computador com Linux.
d) A interface texto padrão do Linux é o Gnome, por meio da qual os comandos do sistema são digitados e executados.
e) O Linux formata o HD em NTFS, que é mais seguro que a formatação em ext3 do Windows.

Comentários:

No Linux, Os diretórios particulares dos usuários são criados dentro do diretório /home por padrão. A alternativa B está correta.

Vamos entender o erro das demais alternativas.

c) O Bash é um interpretador de comandos que pode ser utilizado no Linux, e não uma interface gráfica.

d) O Linux pode ter, por exemplo, dois tipos de contas root e usuário comum, sendo ambas contas de usuário. Por segurança, em regra, a conta de root só é utilizada para tarefas de administração, visto que possui o maior privilégio. É necessária uma conta de usuário comum para as tarefas corriqueiras e para evitar acidentes.

e) A interface gráfica do Linux pode ser, por exemplo, Gnome ou KDE.

f) Não é possível a formatação do sistema de arquivos Linux em NTFS, que é um sistema de arquivos proprietário da Microsoft, destinado aos sistemas Windows. O Linux utiliza, por exemplo, ext3, reiserfs.

Gabarito: B

---

80. (VUNESP – 2013 - UNESP - Assistente de Suporte Acadêmico) - No Linux, por padrão, para deixar um arquivo como oculto, é preciso que o nome do arquivo seja iniciado por;

a) .
b) @
c) *
d) $
e) !

Comentários:

Os arquivos cujos nomes são iniciados por (.) ficam ocultos aos usuários normais. Alternativa correta letra A.

Gabarito: A

---

81. (2005 - FCC - TRE-MG - Técnico Judiciário - Programação de Sistemas) - Um arquivo oculto, que não aparece nas listagens normais de diretórios, no GNU/Linux, é identificado por

a) um ponto (.) no início do nome.
b) um hífem (-) no início do nome.
c) um underline (_) no início do nome.
d) uma extensão .hid.
e) uma extensão .occ.

Comentários:

Se um arquivo inicia seu nome com um ponto, ele não aparecerá nas **listagens regulares**, ficará oculto. Para que sejam exibidos, o comando de listagem deve ter referência expressa definindo isto. Gabarito letra A.

Gabarito: A

---

82. (CESPE – 2014 - TJ-SE - Analista Judiciário - Suporte Técnico em Infraestrutura) - No Linux, a notação ~ é utilizada para acessar o diretório /root/ do sistema.

Comentários:

No Linux, a notação ~ é utilizada para acessar o diretório /home do sistema.

Gabarito: Errada

---

83. (2012 – CESPE - TJ-RO - Analista Judiciário - Análise de Sistemas – Desenvolvimento) - A respeito do sistema operacional Linux, assinale a opção correta.

a) Por meio do comando sudo finger /dev/hda, pode-se gerenciar a partição do dispositivo /dev/hda, bem como excluí-la ou alterar seu tamanho.
b) Enquanto o diretório /bin contém o mínimo de arquivos necessários para funcionar e serem manuseados pelo administrador, o diretório /dev fornece informações sobre o kernel e os processos que estão sendo executados.
c) Para ocultar um arquivo, basta renomeá-lo inserindo um ponto (.) no início de seu nome.
d) Os três tipos de restrição de acesso a arquivos e diretórios são read, write e execute. No comando chmod, estes tipos são referenciados, respectivamente, por 0, 3 e 7.
e) Mediante o comando sudo cat /etc/passwd /etc/group, realiza-se uma junção de todos os arquivos, entre os conteúdos textuais dos diretórios /etc/passwd e /etc/group.

Comentários:
a) **Errada** – um comando usado gerenciar partições é o mkfs, a edição também pode ser feita configurando-se o arquivo /etc/fstab.
b) O diretório /bin contém o mínimo de arquivos necessários para funcionar e serem manuseados pelo administrador, **correta essa parte inicial da assertiva**. **Errado o trecho seguinte,** o diretório /dev fornece informações sobre os **dispositivos instalados no sistema**.
c) **Correto** - Para ocultar um arquivo, basta nomeá-lo ou renomeá-lo inserindo um ponto (.) no início de seu nome.
d) **Errada** - Os três tipos de restrição de acesso a arquivos e diretórios são read, write e execute. No comando chmod, estes tipos são referenciados, respectivamente, **por 4, 2 e 1**.
e) **Errada** - Mediante o comando sudo cat /etc/passwd /etc/group, realiza-se uma **listagem** ou junção dos conteúdos textuais dos diretórios /etc/passwd e /etc/group.

Gabarito: C

---

84. (2013 - CESPE – IBAMA - Analista Ambiental) - Um arquivo oculto no sistema operacional GNU/Linux é identificado por um ponto no início do seu nome, como, por exemplo, no código .bashrc.

Comentários:
Pessoal, conforme comentários questões anteriores, um arquivo cujo nome se inicia por um ponto (.) é um arquivo oculto nas listagens regulares.

Gabarito: Certa

---

85. (2015 – ESAF – Ministério do Planejamento – Analista de Planejamento) - O LVM (Logic Volume Manager) é muito utilizado em servidores Linux por oferecer uma capacidade de ajuste dinâmico de seus volumes. Analise as seguintes afirmações sobre LVM e classifique-as como Verdadeiras (V) ou Falsas (F) e, em seguida, assinale a opção correta.

I. Quando se cria uma partição do disco destinada a uso via LVM, esta partição será um PV (Physical Volume) e fará parte de algum VG (Volume Group), enquanto os LV (Logical Volume) são "fatias" de algum VG.

II. A capacidade total de armazenamento de um VG (Volume Group) é a soma das capacidades dos PVs (Physical Volume) associados a ele.

III. A principal vantagem do LVM é que se pode redimensionar VGs (Volume Group) e PVs (Physical Volume), aumentando ou diminuindo seus tamanhos.

IV. Para refazer o desenho de partições é necessário fazer backup dos dados, apagar as partições, criar um novo layout de partições, formatar as partições, reinstalar o sistema operacional e depois ainda fazer o restore dos dados.

As afirmações I, II, III e IV são, respectivamente,

a) V, V, V, V.

b) V, F, V, F.

c) V, V, F, F.

d) F, V, F, V.

e) F, F, F, F.

Comentários:

Pessoal, para facilitar a assimilação do conteúdo, vamos comentar item a item:

I. Correta. O PV (Physical Volume) comporta algum VG (Volume Group), que pode comportar os LV (Logical Volume).

II. Correta!

III. Errada! Os Physical Volume não são passíveis de redimensionamento, estão limitados ao espaço físico disponível no PV.

IV. Errada! A principal característica do LVM é a flexibilidade, pois no redimensionamento de partições não é necessário fazer backup dos dados.

As alternativas I e II estão corretas, e nosso gabarito é a letra C.

Gabarito: C

---

86. (2014 - CESPE - TJ-SE - Técnico Judiciário - Programação de Sistemas) - O administrador de um servidor Linux dispõe de uma solução cluster em que os discos estejam sendo acessados por meio de LVM (logical volume manager) para facilitar o gerenciamento destes discos. Em face dessa situação, é correto afirmar que o comando pvchng - n xpto - t 100G permitirá aumentar o espaço lógico do volume xpto para 100 GB.

Comentários:
Errado. O comando utilizado para aumentar o espaço lógico do volume é lvextend –L [tamanho] xpto.

Gabarito: Errada

---

87. (2014 - CESPE - TJ-CE - Analista Judiciário) - A instalação de um novo disco em um computador com o sistema operacional Linux requer a observância e o cumprimento de alguns procedimentos em virtude dos padrões de interfaces utilizados, bem como das diversas distribuições Linux existentes. Acerca desse assunto, assinale a opção correta.

a) A partição de swap deve ser criada em um único disco. A divisão do espaço de swap entre vários discos prejudica o desempenho do sistema, o que provoca lentidão no acesso aos dados.
b) Os sistemas de arquivos modernos estão isentos de se tornarem inconsistentes devido à alta compatibilidade com os discos existentes no mercado
c) A conversão de um sistema de arquivos em ext2 para ext3 é permitida, devendo-se, nesse caso, alterar a entrada correspondente em /etc/init.d/linux.conf.
d) Para que um novo disco adicionado seja acessível, o Linux criará automaticamente os arquivos de dispositivos em /dev logo após a conexão do disco, tarefa esta não permitida a um usuário, mesmo na modalidade manual.
e) Um dos benefícios do LVM (Logical Volume Manager) é ajustar o tamanho dos volumes lógicos sem que haja necessidade de interromper o funcionamento do sistema

Comentários:
Pessoal, um dos benefícios do LVM é ajustar o tamanho dos volumes lógicos sem que haja necessidade de interromper o funcionamento do sistema. Gabarito letra E.

Gabarito: E

---

88. (2016 – FAURGS – HCPA – Analista TI) - Ao ser criado um arquivo em um diretório compartilhado por usuários de diferentes grupos primários, pretende-se que esse arquivo faça parte do mesmo grupo do diretório e não do grupo primário de quem o criou. Entre as alternativas abaixo, qual combinação corresponde aos campos de bit de tipo e bits de permissão desse diretório, para que isso ocorra?

a) drwsrwsr-x
b) drwxrwxr-x
c) drwxr-xr-x
d) lrwxrwxrwx
e) -rwxrwxr--

Comentários:
A questão informa que o arquivo deve fazer parte do mesmo grupo do diretório e não do grupo primário de quem o criou. Depreende-se que devemos recorrer ao uso de permissões especiais, suid, sgid e sticky bits.
O bit suid "**Set User ID**" quando está ativado o arquivo é executado com as permissões do dono e não com as permissões de quem executou. Por exemplo, um arquivo executável onde o dono é o root e o bit SUID está ativado, sempre roda com as permissões do root, ou seja, qualquer usuário pode executa-lo com privilégios de administrador. Identificamos se o bit suid está ativado por um "s" na permissão de execução (x) do dono.
O bit sgid "**Set Group ID**" quando está ativado o arquivo é executado com as permissões do grupo e não com as permissões de quem executou. Identificamos se o bit suid está ativado por um "s" na permissão de execução (x) do grupo.
O **sticky bit** é uma de permissão de acesso que pode ser atribuída a diretórios e arquivos em sistemas Linux. Ele indica que o arquivo ou diretório deve receber algum tratamento especial, nesse caso, os arquivos criados dentro do diretório apenas podem ser renomeados ou apagados pelo dono do arquivo, do diretório ou pelo superusuário, mesmo que possua outras permissões.

Gabarito: A

---

89. (2016 – FAURGS – HCPA – Analista TI) - Em relação às características do sistema de arquivos Ext3 ou Ext4 do sistema operacional GNU/Linux, assinale a alternativa correta.

a) O Linux é case insensitive, ou seja, não diferencia letras maiúsculas de letras minúsculas em nomes de arquivos e diretórios.
b) Os programas executáveis no Linux são aqueles que possuem a extensão .exe ou .bin.
c) Os arquivos ocultos possuem nomes que iniciam com o caractere ponto.
d) O comando gzip permite reunir vários arquivos em um único arquivo, mantendo a hierarquia e os atributos originais desses arquivos.
e) Ao criar várias partições em um mesmo disco rígido, é necessário que todas essas partições sejam formatadas com o mesmo sistema de arquivos.

Comentários:
a) **Errada -** O Linux é case **sensitive**, diferencia letras maiúsculas de letras minúsculas em nomes de arquivos e diretórios, comandos, etc.

b) **Errada -** Os programas executáveis no Linux são aqueles que possuem permissão de execução.

c) **Certa** - Os arquivos ocultos possuem nomes que iniciam com o caractere ponto.

d) **Errada -** O comando gzip permite compactar arquivos.

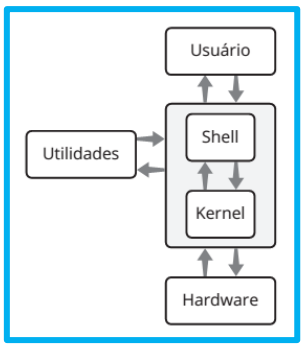
e) **Errada -** Ao criar várias partições em um mesmo disco rígido, não é necessário que todas as partições utilizem o mesmo sistema de arquivos. É possível partições ext2, ext3 e reiserfs conviverem em um mesmo disco.

Gabarito: C

4 – COMANDOS DE LINHA LINUX

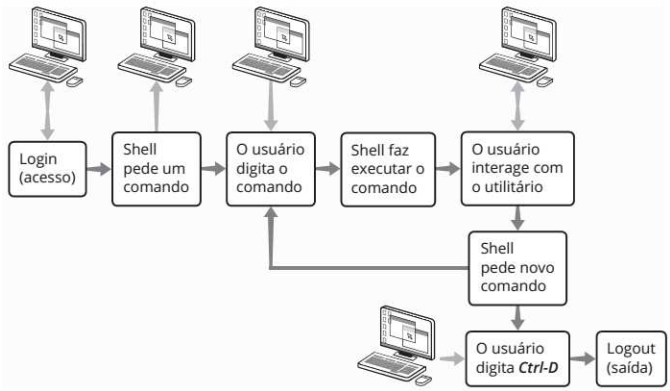
4.1 SHELL LINUX

O Shell é o **interpretador de comandos** do Linux, é ele quem viabiliza a interação do usuário com o kernel do Linux. O interpretador suporta várias funcionalidades, como a manipulação de arquivos, a execução de sequências de comandos predefinidos, entre outras, facilitando a execução de tarefas complexas.



O interpretador de comandos **não faz parte do kernel do sistema**, mas constitui uma ponte entre o usuário e o sistema operacional. Através dele o usuário requisita ações ao sistema, utilizando-se de comandos. Podemos observar a atuação do Shell quando abrimos um terminal ou console e executamos comandos como ls, cat, touch, mkdir, cp, rm, mv, etc.

A interação do usuário com o Shell é como um diálogo. O Shell mostra um *prompt* na tela do terminal, aguardando uma entrada do usuário. Assim que um comando é digitado, o Shell o executa. Quando o comando foi completado, o Shell solicita nova entrada ao usuário, mostrando novamente o cursor, de modo que se possa continuar digitando comandos e interagindo com o Shell. A figura abaixo mostra a sequência em um diálogo do usuário com o Shell:



Existem vários shells, os mais comuns são da família Bourne, dentre eles o Bourne Shell(sh) e o Bourne Again Shell(bash). O Bash Shell é o shell mais usado nas distribuições Linux.

A diferença entre os diversos shells existentes está basicamente nas funcionalidades incorporadas e na sintaxe dos comandos, que podem ser simples ou mais complexas. Uma tela similar à mostrada abaixo, é exibida quando se loga em um sistema Linux. O sinal de *prompt* sinaliza a espera de comandos pelo shell.

```
#
```

4.2 NAVEGAÇÃO EM DIRETÓRIOS LINUX

Existem dois tipos especiais de diretórios utilizados para a navegação na estrutura de diretórios do Linux:

- ✓ **Ponto** (“.”), representa o diretório corrente.
- ✓ **Dois pontos** (“..”), representa o nível acima do diretório corrente.

Conforme vimos anteriormente, os diretórios do Linux são organizados hierarquicamente, em uma estrutura em árvore.

O diretório que fica um nível imediatamente acima do diretório corrente é chamado de diretório-pai (parent directory).

O diretório que fica no nível hierárquico mais alto ou no topo da árvore de diretórios é o **diretório-raiz**, representado pela barra normal ("**/**").

Essa estrutura em árvore permite que **possa haver arquivos ou diretórios com os mesmos nomes**, diferenciados pelo sistema devido aos caminhos diferentes percorridos na estrutura de diretório.

Cada caminho é representado por uma sequência de diretórios separados pelo caractere /(**barra**). Essa sequência representa o nome do caminho (path name) do arquivo ou diretório.

Existem dois tipos de caminhos: o **absoluto**, que se iniciam sempre no diretório-raiz, e o **relativo**, que são baseados no diretório corrente, em vez de se utilizar o diretório-raiz como início do caminho.

Para a navegação nos diretórios, os dois principais comandos são *pwd* e *cd*.

O primeiro passo para navegar na estrutura é saber o local onde estamos. O comando ***pwd*** (print working directory) é utilizado para mostrar o diretório corrente, retornando o caminho completo de identificação desse diretório. O comando pwd é um dos mais simples do Linux, pois não tem opções nem entrada e só produz uma linha de saída.

O comando ***cd*** (change dir) é o outro comando utilizado para navegação na árvore de diretórios. Ele tem a função de mudar a localização do usuário para outro diretório. No exemplo abaixo, o comando cd é utilizado para navegar até o diretório /home/aluno:

```
# cd /home/aluno
```

4.3 Manipulação de Arquivos Linux

Para listar os arquivos do diretório corrente, é utilizado o comando ***ls***. As regras utilizadas nos demais comandos também podem ser aplicadas ao comando ls. O comando ls lista o conteúdo do diretório atual. Sua sintaxe é a seguinte:

```
# ls
```

Uma das opções mais utilizadas pelo usuário é a opção -l, para listar arquivos e diretórios no formato "longo". Esse comando retornar a listagem do diretório atual com seguintes detalhes: Tipo do arquivo, permissões, número de links, dono do arquivo, grupo do arquivo, tamanho em bytes, data da última alteração e nome.

```
# ls –l   (lista o atual diretório, com mais detalhes)
```



Para alterar o dono ou o grupo do arquivo, são utilizados os comandos ***chown***(change owner) e ***chgrp***(change group), respectivamente:

```
# chown dono arquivo
# chgrp  grupo arquivo
```

As permissões de um arquivo também podem ser alteradas através do comando ***chmod*** (change mode). Cada uma das nove permissões (ler, escrever e executar; para o dono, para o grupo e para os outros) pode ser individualmente concedida ou negada com esse comando. O sinal de + atribui, e o sinal de – retira a permissão informada em seguida (rwx).

A seguir, são apresentados alguns exemplos de uso do comando chmod.

```
# chmod +r arquivo (concede acesso de leitura ao arquivo)
# chmod g -w arquivo (retira ou nega acesso de escrita ao grupo)
```

O comando ***touch*** é utilizado para atualizar os horários de acesso e de modificação de um arquivo existente.

Caso esse arquivo não exista, será criado um arquivo com a data e hora especificadas no comando, cuja sintaxe é:

```
# touch [opções] arquivo
```

Quando o usuário faz login em um sistema Linux, ele é automaticamente direcionado para o seu diretório home, onde tem permissão para criar arquivos e diretórios.

Caso haja necessidade de criar outros diretórios, o usuário pode fazer uso de comandos do Linux para isso. Para a criação de diretórios, é utilizado o comando ***mkdir***, cuja sintaxe é:

```
# mkdir -[opções] nome_diretorio
```

A cópia de arquivos pode ser necessária por diversos motivos, como, por exemplo, fazer uma cópia de um arquivo para outro computador. A cópia de arquivos pode ser feita com o comando ***cp***, cuja sintaxe é:

```
# cp - [opções] origem destino_do_arquivo
```

Pode-se omitir o nome, se quisermos manter o mesmo nome da origem. Para copiar diretórios, deve ser utilizada a opção –r do comando cp, que faz cópias recursivas. Existe uma versão para **cópias seguras chamada scp, que faz uso o protocolo ssh.**

O comando utilizado para remover arquivos é o ***rm*** e as mesmas regras vistas para o comando cp, se aplicam ao comando rm, cuja sintaxe é:

```
# rm - [opções] nome_do_arquivo
```

A remoção de arquivos deve ser feita com **atenção**, pois nem sempre será solicitada, pelo sistema, a confirmação do usuário para a execução da remoção. Da mesma forma que, para a cópia, a remoção de todos os arquivos, inclusive os diretórios, pode ser feita utilizando o comando ***rm*** com a opção ***-r***.

Diretórios sem conteúdo também podem ser removidos com o comando ***rmdir***.

O comando ***mv*** pode ser utilizado de duas formas: para mover arquivos da origem para o destino ou para renomear arquivos, trocando apenas seu nome, mantendo-o no diretório original.

Sintaxe do comando mv:

```
# mv - [opções] origem destino
```

O comando ***rename*** pode ser utilizado para renomear arquivos, mas com a funcionalidade adicional de trocar partes de nomes, sendo muito útil quando utilizado com caracteres-curinga. No exemplo abaixo, as terminações de todos os arquivos do diretório corrente são trocadas de .htm para .html.

```
# rename .htm .html *.htm
```

O comando ***find*** é utilizado para fazer buscas por arquivos e diretórios, fornecendo como resultado o caminho completo para o(s) arquivo(s) e diretório(s) encontrado(s).

É possível, também, utilizar caracteres-curinga para ampliar a pesquisa a um conjunto de nomes que atendam a uma especificação múltipla. Formato do comando:

```
# find [caminho] [expressão]
```

O comando find faz uma busca pela expressão definida como parâmetro, em todos os diretórios e subdiretórios especificados também como parâmetros no campo caminho, retornando os resultados da busca, caso existam.

Podemos utilizar, ainda, o comando ***locate***, que faz buscas por arquivos, consultando um banco de dados que contém os arquivos criados pelo usuário. Para forçar a atualização desse banco de dados, utilizamos o comando ***updatedb***.

O comando ***locate*** tem sintaxe simples e funciona como se houvesse caracteres antes e depois do nome do arquivo, isto é, procura-se o nome do arquivo isoladamente ou como parte de um nome. Por exemplo, para achar os arquivos concurso e concurso_provas, podemos utilizar o seguinte comando:

```
# locate concur
```

O comando ***cat*** pode ser utilizado para criar um arquivo, mesmo sendo sua **função principal a de concatenar arquivos**.



TOME NOTA!

Como a sua saída padrão é a tela do monitor, ao executar o comando a seguir, o conteúdo do arquivo será mostrado na tela:

```
# cat arquivos
```

O comando ***cat*** exibe o texto continuamente, se o tamanho do texto ultrapassar o número de linhas da tela do monitor, ele continuará mostrando o arquivo até o final, sem pausas, a tela só para de rolar quando todo o conteúdo do arquivo for exibido.

Para evitar o problema de visualização de arquivos maiores que o número de linhas da tela, devemos utilizar os comandos ***more*** ou ***less***, que listam o arquivo dando uma pausa na listagem quando ela preenche toda a tela.

A sintaxe desses comandos pode ser vista abaixo:

```
# more [opções] [-num] [arquivo]
```

```
# less [opções] [arquivo]
```

Com o utilitário chamado ***wc***, podemos **contar os caracteres, palavras e as linhas contidos em um arquivo texto**. A sintaxe do comando é:

```
# wc [opções] [arquivo]
```

Para exibir o conteúdo inicial e final de arquivos texto, existem dois comandos: o head e o tail, respectivamente.



O comando ***head*** permite que visualizemos as primeiras linhas de um arquivo. Sua sintaxe é:

```
# head [opções] [arquivo1 arquivo 2 ...]
```

O inverso do comando head é o comando ***tail***, que mostra as últimas linhas de um arquivo. Sintaxe do comando tail:

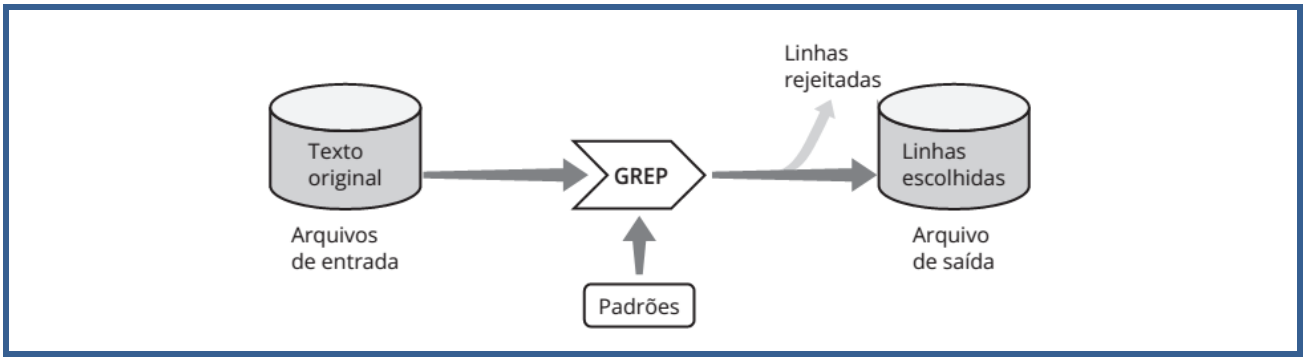
```
# tail [opções] [arquivo1 arquivo 2 ...]
```

O comando ***tail*** é muito utilizado na visualização de arquivos longos, como por exemplo um log de servidor.

A pesquisa e seleção de conteúdos de arquivos no Linux é uma operação muito comum, e pode ser utilizada para encontrar uma determinada informação.

Por exemplo, se quisermos encontrar no arquivo de alunos do nosso exemplo todos aqueles que residem no mesmo estado, na mesma cidade ou na mesma rua, podemos utilizar comandos do Linux que realizam a pesquisa de conteúdo.

O comando ***grep*** é um utilitário de seleção e pesquisa de arquivos. **Esse comando, em combinação com pipes, é muito utilizado em shell script**. A Figura 4.5 mostra o funcionamento do comando grep.



O usuário especifica um padrão que será utilizado pelo grep para fazer a pesquisa nos arquivos de entrada. Esse utilitário examina as linhas do arquivo, verificando se cada uma contém o padrão especificado. Quando o padrão é encontrado, a linha é copiada para o arquivo de saída, ou para a tela do terminal. Se a linha não contém o padrão, é rejeitada, isto é, não é copiada no arquivo de saída.

Quando o comando grep termina de pesquisar os arquivos de entrada, o arquivo de saída vai conter todas as linhas que contêm os padrões desejados. A sintaxe do comando grep é:

```
# grep [opções] padrão [arquivo1]
```

O comando ***cmp*** compara os arquivos e mostra a posição em que aparece a primeira diferença. O exemplo a seguir compara dois arquivos, e informa que eles têm um caractere diferente na posição 1 da linha 1:

```
# cmp [arquivo1] [arquivo2]

# arquivo1 arquivo2 differ: char 1, line1
```

O conteúdo de um arquivo pode ser ordenado antes de ser processado. O comando ***sort*** recebe as linhas de um ou mais arquivos de entrada e a seguir as processa, produzindo um arquivo de saída que contém as linhas em ordem classificada. Sintaxe do comando sort:

```
# sort [opções] [arquivo]
```

Vamos agora ao comando mais necessário ao administrador Linux novato ;-). O comando para encerrar programas mal comportados na interface gráfica.

```
# ctrl + z
```

Pessoal, nesse ponto da aula precisamos fazer uma ressalva importante. Como notaram, não explicamos todos os comandos do Linux, pois não era nossa proposta. Foram abordados

apenas aqueles mais recorrentes em provas, ok.

Caso surjam dúvidas, vocês podem recorrer às páginas ***man*** do próprio Linux, ou podem me encaminhar.

4.4 SHELL SCRIPT LINUX

Shell Script é uma linguagem de programação baseada no conceito de interpretação, que pode ser utilizada na linha de comando do shell linux. Os programas escritos nessa linguagem são chamados de scripts, e são muito poderosos.

Shell Script pode ser usado com o objetivo de automatizar sequências de tarefas que serão repetidas várias vezes, transformando essas tarefas em arquivos executáveis especiais. Podemos escrever as sequências de comandos do sistema operacional, tal como fazemos no Shell, e até adicionar lógica de programação (if, do, while, etc).

Por exemplo, uma das atividades rotineiras de um administrador de sistemas Linux é realizar operações de backup, mantendo cópias de segurança dos arquivos importantes. Se tal atividade for realizada periodicamente, é interessante que seja criado um programa para automatizar essa tarefa. Podemos automatizar essa atividade, recorrendo a um shell script.

No Shell, os programas são interpretados, e por essa característica são chamados de scripts. Assim, os **scripts nada mais são do que programas contendo sequências de comandos que são interpretados pelo Shell, linha após linha**.

O script é um arquivo executável, com diretrizes na linha inicial que diz qual Shell deverá interpretar aquela sequência de comandos quando o arquivo for executado. Essa linha deve ser a **primeira linha do script e começa com os caracteres *#!,*** denominados shebang. Após estes caracateres, é seguido do caminho na árvore de diretórios (pacth) no qual o Shell será encontrado.



O sistema de arquivos do Linux identifica um script através do conteúdo dos seus dois primeiros bytes.

Para indicar o shell bash como o interpretador, supondo que o interpretador bash esteja no diretório /bin, devemos ter a primeira linha como:

```
#!/bin/bash
```

Importante sabermos que poderá ser utilizado qualquer shell disponível no sistema Linux.

Supondo que vamos fazer um backup bem simples com os seguintes passos:

- ✓ usar, por exemplo, arquivos .log gerados na pasta /var/log/;
- ✓ compactar os arquivos, gerando um arquivo denominado bk com extensão .tar;
- ✓ colocar os arquivos em um diretório chamado backup.

Podemos então, criar um arquivo chamando, por exemplo, "scriptBackup", e nele colocar os comandos necessários para realizar o backup dos arquivos:

```
#!/bin/bash
# cd /home/usuário/backup
# tar cvf bk.tar /var/log/*.log
```



Atenção, pessoal!!!! Vamos agora passar a resolução de questões sobre comandos Linux. Observem que este é um dos tópicos mais recorrentes nas questões de concursos.

Não esqueçam de observar os tópicos prediletos da banca!!! Busquem otimizar os estudos.

4.5 RESOLUÇÃO DE QUESTÕES

90. (2017 – FGV - MPE-BA - Analista Técnico - Tecnologia) - Pode ser utilizado no sistema operacional Linux para listar o conteúdo do diretório corrente, de modo que seja possível conferir o tamanho e a data de criação de cada arquivo ou pasta, inclusive dos arquivos ocultos, o seguinte comando:

a) ls -1

b) ls -lha

c) ls -ld

d) ls -sa

e) ls –ltr

Comentários:

O comando ls lista os arquivos do diretório corrente, e pode ser utilizado em conjunto com vários parâmetros para especificar melhor a listagem a ser realizada. O comando da questão informa que a listagem deve apresentar o tamanho e a data de criação de cada arquivo ou pasta, inclusive dos arquivos ocultos. Para tanto, o comando ls deve vir acompanhado dos parâmetros **l** (longo), **h** (apresentar tamanho em formato compreensível humano k, Kb ou mb) e **a** (exibe na listagem os arquivos ocultos). Alternativa correta letra B.

Gabarito: B

---

91. (2017 – FGV - MPE-BA - Analista Técnico - Tecnologia) - O sistema operacional Linux oferece várias ferramentas de linha de comando úteis para o dia a dia do administrador de sistemas. A ferramenta mais adequada para fazer o rastreamento das portas que estão abertas no sistema operacional é::

a) uname;

b) top;

c) nmap;

d) arp;

e) finger.

Comentários:

a) **Errada –** uname exibe informações do sistema;

b) **Errada –** top exibe informações sobre os processos em execução;

c) **Certa** - nmap é uma ferramenta, não oriunda exclusivamente de sistemas Linux, destinada a mapear portas de sistemas operacionais;

d) **Errada –** arp é um comando para exibir informações da tabela arp, que informa endereços físicos (MAC);

e) **Errada –** finger é um comando Linux, em desuso, que apresenta informações de usuários logados no sistema.

Alternativa correta letra C.

Gabarito: C

---

92. (2017 – FGV - SEPOG – RO - Analista em Tecnologia da Informação e Comunicação) - Assinale a opção que indica o comando que pode ser utilizado para incluir um usuário em um grupo em um sistema operacional Linux:

a) chgrp
b) chown
c) groupad
d) su
e) usermod

Comentários:
a) **Errada –** chgrp altera o grupo a que pertence um arquivo;
b) **Errada –** chown altera o proprietário de um arquivo;
c) **Errada –** groupad inclui um novo grupo;
d) **Errada –** su concede poderes de outro usuário ao usuário corrente;
e) **Certa –** usermod permite modificar um usuário;
Alternativa correta letra E.

Gabarito: E

---

93. (2010 – FCC - TCM-CE - Analista de Controle Externo - Inspeção de Obras Públicas) - Remove arquivos no Linux o comando

a) pwd
b) mkdir
c) cd
d) rm
e) tar

Comentários:

O comando rm remove arquivos, e o comando rmdir remove diretórios vazios. Alternativa correta letra D.

Gabarito: D

---

94. (2013 - FCC – DPE SP - Engenheiro de Redes) - Deseja-se verificar o conteúdo da tabela de roteamento de um servidor com sistema operacional Linux. Um dos comandos que podem ser utilizados para apresentar o conteúdo da tabela de roteamento é o

a) netstat.
b) nettab.
c) routing.
d) table.
e) traceroute.

Comentários:

O comando netstat - exibe informações sobre as conexões de rede (de saída e de entrada), tabelas de roteamento e uma gama de informações sobre as estatísticas da utilização da interface na rede. O comando traceroute exibe informações sobre rotas em uma conexão TCP/IP. As demais alternativas não fazem sentido.

Gabarito: A

---

95. (2013 - FCC – ALERN - Técnico em Hardware) - Uma ferramenta muito utilizada em sistemas operacionais Linux permite a exibição da utilização do espaço por arquivos. Analise o seguinte comando efetuado com este utilitário: du –ahc. A execução deste comando com os parâmetros informados irá apresentar

a) todos os arquivos da pasta atual, exceto arquivos ocultos e armazenados em cache.
b) todas as pastas do sistema, incluindo arquivos ocultos e armazenados em cache.
c) a taxa de compactação dos arquivos juntamente com informações sobre a memória heap.
d) apenas os arquivos que contenham os atributos hidden e compacted.
e) apresentar todos os arquivos, com valores descritos de forma mais legível e com um total ao final.

Comentários:

O comando ***du*** exibe informações sobre uso de disco (**d**isk **u**se). O parâmetro **–a** apresenta todos os arquivos, **-h** apresenta informações em formato amigável, **-c** totaliza o espaço usado pelo diretório e seus subdiretórios. Alternativa correta letra E.

Gabarito: E

---

96. (2012 – FCC - TRE-SP - Técnico Judiciário - Operação de Computador) - No sistema Linux, para se executar um arquivo texto contendo comandos de interpretador como um script é necessário que o arquivo

a) seja compilado.
b) possua permissão de execução.
c) esteja no diretório /usr/bin
d) tenha a extensão .exe
e) tenha a extensão .bat

Comentários:
Pessoal, a questão está se referindo a um script shell que vimos na parte teórica. Como vimos, a possibilidade de execução de um arquivo não é decorrente de o arquivo ter uma extensão .exe. Para os arquivos comuns serem executados no Linux, é necessário que tenham permissão de execução. Gabarito letra B.

Gabarito: B

---

97. (2016 – FCC – ELETROBRAS/ELETROSUL - Informática) - Um profissional de TI da Eletrosul trabalha em computadores com os sistemas operacionais Unix e Linux. Foi solicitado a ele utilizar comandos para realizar as seguintes tarefas. Considerando os sistemas operacionais indicados, os comandos I, II e III são, correta e respectivamente:

I. No sistema operacional Unix, atualizar a data de acesso do arquivo dados.txt, mas caso este arquivo não exista, não permitir que seja criado um arquivo novo vazio.
II. No sistema operacional Linux Red Hat, criar uma lista (no arquivo listagem) de todos os softwares instalados.
III. No sistema operacional Linux CentOS, calcular e exibir o espaço total do diretório corrente em megabytes.

a)

I – Unix	II– Linux Red Hat	III– Linux CentOS
touch -c dados.txt	rpm -q -a > listagem	du –h

b)

I – Unix	II– Linux Red Hat	III– Linux CentOS
du -h dados.txt	touch -c listagem	rpm -q -a

c)

I – Unix	II– Linux Red Hat	III– Linux CentOS
rpm -q -a > dados.txt	du -h listagem	touch –c

d)

I – Unix	II– Linux Red Hat	III– Linux CentOS
touch dados.txt	rpm -c > listagem	du -m

e)

I – Unix	II– Linux Red Hat	III– Linux CentOS
rpm -c dados.txt	du -c >listagem	touch –m

Comentários:

I. No sistema operacional Unix, o comando utilizado para atualizar a data de acesso do arquivo dados.txt, é touch -c dados.txt. O parâmetro definido como **–c ou --no-create** especifica ao Unix para não criar quaisquer arquivos.

II. No sistema operacional Linux Red Hat, para criar uma listagem de todos os softwares instalados utiliza-se o comando **rpm -q –a ou -qa**. Para que esta listagem seja salva em arquivo, a saída do comando é direcionada para a saída em arquivo pelo > listagem, em vez da saída padrão (stdout). Se quisermos verificar se o pacote dde servidor http está instalado, podemos utilizar um comando similar, conjugado com o grep para pesquisar: **rpm -qa | grep httpd**

III. No CentOS, o comando utilizado para calcular e exibir o espaço utilizado pelo diretório corrente, em formato acessível, é o **du -h**. Lembrando que o comando du equivale a disk usage, e o parâmetro –h equivale a formato humano.

Gabarito: A

98. (2016 - FCC - ELETROBRAS-ELETROSUL - Informática) - Um profissional de TI está usando um computador com sistema operacional Linux que utiliza no shell o interpretador de comandos bash. Ele está logado como usuário teste e criou o seguinte arquivo shell script:

1 - **#!/bin/bash**
2 - **echo 'Eletrosul- Centrais Elétricas S.A.'**
3 - **$ variavel= 'Eu estou logado como usuário $user'**
4 - **$ echo $variavel**

Considerando que 1, 2, 3 e 4 indicam as linhas do arquivo e que este tenha sido salvo com o nome exemplo, é correto afirmar:

a) Para o arquivo ser executável, é necessário acionar o comando $ chmod +x exemplo. Depois disto o arquivo poderá ser executado com ./exemplo.
b) A linha 1 indica que todas as outras linhas abaixo deverão ser executadas pelo compilador sh, que se localiza em /bin/bash.
c) Após ser executado, o arquivo imprimirá na tela apenas frase "Eletrosul – Centrais Elétricas S. A." utilizando o comando echo.
d) Ao acionar o comando file arquivo é possível ver que a definição dele é Bourne-Again Shell Script, que se refere ao bash script.
e) As linhas 3 e 4 farão com que seja impresso na tela Eu estou logado como usuário $teste.

Comentários:
Vamos comentar as linhas do arquivo, para facilitar o entendimento:

#!/bin/bash
Esta linha inicial informa ao interpretador de comandos bash que o arquivo deverá ser tratado como um arquivo binário.

echo 'Eletrosul- Centrais Elétricas S.A.'
Nesta linha, o comando ***echo*** exibirá no terminal a mensagem entre as aspas simples.

$ variavel= 'Eu estou logado como usuário $user'
Este comando cria uma variável e nela armazena a string entre as aspas simples.

$ echo $variavel
O comando ***echo*** exibe o conteúdo armazenado na variável echo.

Vamos ao ponto indagado na questão. Como comentado, para tornar um arquivo executável, é necessário alterar as permissões do arquivo, utilizando o comando ***chmod.*** *Por segurança, um*

*arquivo em um sistema Linux necessita de permissão para execução. A*o utilizarmos o parâmetro ***+x*** somado ao comando chmod o script bash poderá ser executado.

Gabarito: A

---

99. (2015 – FCC - TRT/RS - Analista Judiciário - TI) - O administrador de um computador com sistema operacional Linux deseja desativar as interfaces de rede para verificar o funcionamento da nova configuração do sistema operacional. O comando que permite desativar a interface eth0 é:

(A) ifconfig –s eth0

(B) ifdown eth0

(C) ifconfig –a eth0

(D) shutdown eth0

(E) ifconfig –x eth0

Comentários:

Pessoal, questão bem fácil. Entre as opções, o comando que permite desativar a interface eth0 é ***ifdown eth0***, para ativar a interface ifup eth0. Observem que o ifconfig também permite (a depender da distribuição Linux) desativar a interface com o comando ***ifconfig eth0 down***, mas esta alternativa não consta entre as opções. A alternativa correta que nos restou é a letra B.

Gabarito: B

---

100. (2015 – FCC - TRT/RS - Analista Judiciário - TI) - O administrador de um computador com sistema operacional Linux deseja visualizar o estado das funções de rede de computadores. Executando o comando netstat, para visualizar a tabela de roteamento, deve-se utilizar a opção

a) -r

b) -l

c) -t

d) -i

e) -x

Comentários:

No linux, podemos ver a tabela de roteamento usando um dos seguintes comandos: ***netstat -r ou route -n*** ou ***cat /proc/net/route.*** O gabarito apontou a letra A, e este realmente é nosso gabarito.

Gabarito: A

---

101. (2005 - ESAF - Receita Federal - Auditor Fiscal da Receita Federal) - No sistema operacional Linux, o comando

a) pwd mostra a senha de sua conta.

b) mkdir destrói um diretório.

c) shutdown -r +5 faz com que o sistema reinicie após cinco minutos.

d) who mostra a versão do Linux e a quantidade de memória do computador.

e) ls lista os usuários conectados na máquina via rede.

Comentários:

a) **Errada** - pwd (Print Working Directory) identifica o diretório corrente;

b) **Errada** – mkdir (make dir) constrói, cria um diretório;

c) **Correta**! – o comando shutdown reinicia o sistema, conforme os parâmetros informados;

d) **Errada** – mostra informações dos usuários logados no sistema; o comando que exibe informações sobre o sistema é o uname;

e) **Errada** – ls (list), comando equivalente ao comando dir do Windows, lista os arquivos relativos a um diretório.

Gabarito: C

---

102. (2012 – ESAF – Ministério Integração - Ana Sist - Informática e Redes) - No ambiente Linux é correto afirmar que:

a) cp copia um ou mais linhas de comando.
b) cat cataloga vários arquivos na biblioteca padrão.
c) make executa arquivos e constrói um octal.
d) mdir constrói um diretório de imagens.
e) head extrai as primeiras linhas de um arquivo.

Comentários:

Alternativa correta letra E, o comando head exibe as primeiras linhas do arquivo. As demais alternativas estão incorretas:

a) cp - copia um arquivo.

b) cat – exibe o conteúdo de um arquivo.

c) make – em conjunto com configure e install, permitem compilar e instalar programas.

d) mkdir - constrói um diretório.

Gabarito: E

---

103. (2012 - ESAF - MI - Analista de Sistemas) - No ambiente Linux é correto afirmar que:

a) cp copia um ou mais linhas de comando.

b) cat cataloga vários arquivos na biblioteca padrão.

c) make executa arquivos e constrói um octal.

d) mdir constrói um diretório de imagens.

e) head extrai as primeiras linhas de um arquivo.

Comentários:

Comentando item a item as alternativas

a) Errada! O comando ***cp*** permite a cópia de um arquivo, seu propósito não é copiar linhas de comando.

b) Errada! O comando ***cat*** permite visualizar uma arquivo texto, por exemplo. Não tem relação alguma com a catalogação de arquivos.

c) Errada! O comando **make,** em parceria com o comando configure e install, permite a instalação a partir de código fonte.

d) Errada! O comando ***mkdir*** (make dir) permite a criação de um diretório.

e) Correta! O comando ***head*** permite visualizar as linhas iniciais de um arquivo, e em parceira com o comando ***tail*** que permite visualizar as linhas finais do arquivo, é bastante útil para a visualização e manipulação de arquivos longos, como arquivos de log.

Gabarito: E

---

104. (2014 - NCE-UFRJ – UFRJ - Técnico) - No Sistema Operacional Linux, o comando ls é utilizado para:

a) listar diretórios e arquivos
b) listar aplicativos em execução
c) excluir diretórios
d) criar um diretório seguro.
e) criar um arquivo.

Comentários:

No linux, o comando *ls* é utilizado para listar o conteúdo diretório corrente. Relação correta das demais alternativas:

b) *ps* ou *top* - listar aplicativos em execução
c) *rmdir* - excluir diretórios
d) *chmod* - criar um diretório seguro (configuração de permissões).
e) *touch* - criar um arquivo.

Gabarito: A

---

105. (2014 – UNIRIO - UNIRIO - Analista Tecnologia da Informação - Desenvolvimento de Sistemas) - Com relação ao sistema operacional Linux, é CORRETO afirmar que o comando

a) pwd é usado para mostrar a versão utilizada do sistema operacional.
b) du exibe um resumo do espaço livre em disco.
c) chmod muda o dono de um diretório.
d) mkdir cria permissões para um diretório.
e) who mostra quem está logado no sistema.

Comentários:

Função correta dos comandos:

a) *pwd* - usado para mostrar o diretório corrente.
b) *du* - exibe um resumo do espaço utilizado em disco pelo diretório e seus subdiretórios.
c) *chmod* – change mode, muda as permissões de um arquivo ou diretório.
d) *mkdir* - cria um diretório.

A alternativa E está correta. O comando *who* mostra as informações sobre o usuário logado no sistema. Pode ser utilizado com os comandos ***whoami*** e ***w***.

Gabarito: E

---

106. (2013 - FUNCAB - SUDECO – Contador) - No sistema operacional Linux, o comando que NÃO está relacionado a manipulação de arquivos é:

a) kill
b) cat
c) rm
d) cp
e) ftp

Comentários:

O comando *kill* é utilizado para envio de sinais aos processos. Alternativa correta letra A. Função correta dos demais comandos de manipulação de arquivos são:

b) cat – exibe o conteúdo de um arquivo;
c) rm – excluir um arquivo;
d) cp – copia um arquivo;
e) ftp – não é um comando, e sim um protocolo de transferência de arquivos (File Transfer Protocol).

Gabarito: A

---

107. (2010 - CESGRANRIO - IBGE - Analista de Sistemas) - No sistema operacional Linux, o comando

a) ifconfig é usado para configurar e exibir dispositivos de rede.
b) netstat - r permite configurar as tabelas de roteamento do sistema operacional.
c) bind verifica a configuração do DNS.
d) wc - l retorna o número de vezes que um determinado usuário se conectou ao seu computador.
e) dhcpd permite obter informações sobre um endereço IP a partir de um servidor DHCP.

Comentários:

Alternativa A está correta. O comando ifconfig é usado para configurar e exibir dispositivos de rede. Função correta dos demais comandos:

b) **netstat** - exibe informações sobre as conexões de rede (de saída e de entrada), tabelas de roteamento e uma gama de informações sobre as estatísticas da utilização da interface na rede.

c) **named-checkconf** - verifica a configuração do DNS.

d) **wc** - retorna o número de linhas de um arquivo.

e) **dhcpd** – daemon do servidor DHCP.

Gabarito: A

---

108. (2014 – IADES - CONAB - Tecnologia da Informação) - No Linux, o comando responsável por alterar as permissões de leitura, escrita e execução de um arquivo é o

a) filech.
b) chmod.
c) free.
d) change.
e) file.

Comentários:
Pessoal, como veremos esta questão ilustra bem o estilo de questões da banca, no que se trata dos comandos do sistema operacional Linux. São questões simples, que exigem apenas o conhecimento da função de um comando Linux. Na questão, o comando Linux utilizado para alterar as permissões de um arquivo é o ***chmod.*** A alteração das permissões de leitura, escrita e execução, respectivamente, é realizada utilizando-se o comando em conjunto com os parâmetros r, w e x (como comentamos na parte teórica, acompanhando-se o parâmetro de + habilita-se, e de – desabilita-se a operação). Gabarito letra B.

Gabarito: B

---

109. (2014 – IADES - TRE-PA - Técnico Judiciário - Programador de Computador) - O comando tail, no sistema operacional Linux, é utilizado para exibir as últimas linhas de um arquivo texto. Assinale a alternativa que apresenta qual comando gera a exibição das dez últimas linhas do arquivo /etc/candidato.

a) tail – 10/etc/candidato.
b) tail – u 10/etc/candidato.
c) tail – ult 10/etc/candidato.
d) tail – n 5/etc/candidato.
e) tail/etc/candidato.

Comentários:
Pessoal, a dupla de comandos ***head*** e ***tail*** é utilizada em sistemas Linux para visualizar realizar diagnósticos em logs de sistema. Haja vista que, em regra, os logs são arquivos de grande extensão, a facilidade provida pelos comandos é permitir visualizar as linhas iniciais e finais, respectivamente. Por padrão, o tail visualiza apenas as 10 linhas iniciais do arquivo. Em conjunto com o parâmetro –n, o tail permite definir a quantidade de linhas do arquivo a ser visualizada. A alternativa menos errada é a letra E, apesar de dispor de um erro crasso, pois ao omitir o espaço entre o tail e os parâmetros definidores do arquivo /etc/candidato, o comando está semanticamente incorreto. Nosso gabarito, letra E.

Gabarito: E

---

110. (2015 – CETRO – AMAZUL - Analista de desenvolvimento de sistemas) - Assinale a alternativa que apresenta a função do comando cat no Linux.

a) Serve para limpar a tela do terminal.
b) Finaliza processos.
c) Exibe o que há dentro de determinado arquivo.
d) Mostra informações sobre o sistema.
e) Mostra qual o tipo de arquivo.

Comentários:
Pessoal, atenção para o perfil da banca e o tipo de questão favorita. O comando cat é um dos mais utilizados pelos sysadmin de Linux. Sua função é basicamente exibe o conteúdo de arquivos texto. Por exemplo, ***cat texto.txt***, exibe o conteúdo do arquivo texto.txt. Um comando similar é o comando ***tac***, que também exibe o conteúdo de arquivos, porém exibe inicialmente a parte final do arquivo.

Gabarito: E

---

111. (2015 - CETRO – AMAZUL - Analista de desenvolvimento de sistemas) - Assinale a alternativa que apresenta a função da linha de comando :psaux, digitada no terminal do sistema operacional Linux.

a) Exibe data e hora atual do sistema.
b) Lista os processos em execução.
c) Verifica a quantidade de memória.
d) Procura por pastas e arquivos.
e) Acessa o manual de uso.

Comentários:
O comando ***ps*** lista os processos em execução em um sistema Linux. Os parâmetros –aux definem que a exibição deve ser de todos os arquivos.

Gabarito: B

---

112. (2013- CETRO – ANVISA - Analista Administrativo - Área 5) - Considere os comandos do sistema operacional Linux para correlacionar as colunas abaixo e, em seguida, assinale a alternativa que apresenta a sequência correta.

1.	modprobe.	( )	Exibe os usuários conectados e o que estão executando.
2.	ping.	( )	Adicione ou remove módulos carregáveis do *kernel*.
3.	arp.	( )	Envia requisições ICMP para um determinado host.
4.	w.	( )	Permite descobrir o endereço MAC de um host da rede.

a) 4/ 1/ 2/ 3
b) 2/ 1/ 4/ 3
c) 1/ 4/ 3/ 2
d) 2/ 3/ 1/ 4
e) 3/ 2/ 1/ 4

Comentários:
Pessoal, bastante atenção para memorizar os comandos Linux mais frequentes nas provas. Em provas para cargos gerais, os comandos citados nesta questão não são frequentes, porém são bons candidatos em provas para cargos especializados, analista em redes, por exemplo. Vamos comentar a função de cada comando Linux: **Modprobe** – adiciona ou remove módulos no kernel Linux; **Ping** – envia requisições ICMP; **Arp** – permite descobrir endereços MAC de interfaces de rede; **W** – exibe os usuários conectados;
Nosso gabarito é a alternativa A.

Gabarito: A

---

113. (2018 – CESPE – CGM/João Pessoa - Técnico Controle Interno – Geral) - Acerca dos conceitos de organização e de gerenciamento de arquivos, dos procedimentos e dos aplicativos para segurança da informação, julgue o item subsequente. No sistema operacional Linux, é possível criar arquivos sem nenhum conteúdo.

Comentários:

A criação de arquivos no Linux pode se dar de várias formas: **>nomearquivo**; **utilizando editor de texto, como vi, vim, ou gedit**; **utilizando comando touch nomearquivo**. Nas formas citadas é possível cria-los sem conteúdo. Assertiva certa!!!

Gabarito: Certa

---

114. (2018 – CESPE – EBSERH - Técnico em Informática) - Acerca dos ambientes Linux e Windows, julgue o item que se segue. No Linux, o comando wc -w RELATORIO.TXT apresenta a quantidade de palavras existentes no arquivo RELATORIO.TXT.

Comentários:

Pessoal, devem saber, que um dos pontos preferidos do examinador, no que atine ao Linux, são os comandos de linha. Temos diversas categorias de comandos de linha, e uma em especial é muito importante: edição de arquivos texto. O comando ***wc***, literalmente word count, é muito importante na edição e análise de arquivos, permite contar caracteres, palavras e linhas de um arquivo, respetivamente com os parâmetros ***–d, -w, -l***. Concluímos então que a assertiva está correta.

Gabarito: Certa

---

115. (CESPE – 2014 - FUB - Conhecimentos Básicos - Todos os Cargos de Nível Superior) - No ambiente Linux, os comandos executados por um usuário são interpretados pelo programa shell.

Comentários:

No ambiente Linux, os comandos executados por um usuário são interpretados pelo interpretador de comandos do shell, por exemplo, ash, bash ou sh.

Gabarito: Certa

---

116. (2007 - CESPE - TCU - Analista de Controle Externo - Tecnologia da Informação) - No Linux, o comando ifconfig permite habilitar ou desabilitar o protocolo ARP para determinada interface.

Comentários:

Ifconfig [-] arp - Habilita ou desabilita o uso do protocolo ARP para uma interface.

Gabarito: Certa

---

117. (2007 - CESPE - TCU - Analista de Controle Externo - Tecnologia da Informação) - A checagem do sistema de arquivos permite verificar se a estrutura para armazenamento de arquivos, diretórios, permissões, conectividade e superfície do disco estão funcionando corretamente. No Linux, o comando fsck permite checar e, eventualmente, reparar o sistema de arquivos.

Comentários:

Questão antiga pessoal, mas acho que vale a pena resolvermos, pois é de um dos últimos concursos para a área de TI do TCU. Vamos ver o ponto da questão então. No Linux, o comando **fsck** permite verificar se toda a estrutura para armazenamento de arquivos, diretórios, permissões, conectividade e superfície do disco estão funcionando corretamente, e em caso de falhas, permite reparar o sistema de arquivos. Assertiva correta.

Gabarito: Certa

---

118. (2014 - CESPE - TJ-SE - Analista Judiciário - Suporte Técnico em Infraestrutura) - Em um comando Shell Script do Linux, é possível combinar diversos comandos em sequência utilizando-se apenas o comando +.

Comentários:

Em Shell Script, é possível combinar comandos de duas formas: um comando sendo executado por vez, de forma independente, utilizamos ponto e virgula (;);
Comandos executados concorrentemente, é utilizado o caractere **&** entre os comandos. Neste caso o último comando só será executado se o primeiro for bem sucedido.
Não é utilizado o caractere +, assertiva errada.

Gabarito: Errada

---

119. (2014 - CESPE - TJ-SE - Técnico Judiciário - Programação de Sistemas) - O administrador de um servidor Linux verificou que uma máquina estava muito lenta. Nessa situação, para averiguar se a causa deste problema é a quantidade de processos em

execução e para visualizar o quanto cada processo está exigindo da CPU, o administrador poderá utilizar o seguinte comando: tail -lh /bin/proc.

Comentários:
Tail é um comando Linux para listar arquivos texto, muito comum seu uso, ou do comando head, para listar o final ou início de arquivos muito longos, como um arquivo de log. Os comandos utilizados para listar quantidade de processos em execução e para visualizar o quanto cada processo está exigindo da CPU são o comando ***ps*** ou o comando ***top***. Assertiva errada.

Gabarito: Errada

---

120. (2014 - CESPE - MTE - Contador) - No Linux, o comando cat arq1 >> arq2 | less lista o conteúdo dos arquivos arq1 e arq2 com paginação das telas.

Comentários:
Para melhorar o entendimento, segmentemos o comando em três partes:
a) cat arq1 >> arq2 - insere o conteúdo do arquivo "arq1" ao final do arquivo "arq2"
b) | (pipe) – recebe o resultado dos comandos à esquerda e os repassa como entrada para os comandos à sua direita
c) more ou less – permitem visualizar arquivos texto que ultrapassarem uma tela, com rolagem da tela e navegação do conteúdo.
De fato, mesmo assim ainda pode restar confuso o entendimento. O que deve ser ressaltado para compreender a questão é que após o operador >> resultar na inserção do conteúdo do arq1 ao fim de arq2, o arquivo conjunto resultante não é submetido ao comando less combinado com o | pipe. Assertiva errada então.

Gabarito: Errada

---

121. (2012 - CESPE - TJ-AC - Analista Judiciário - Análise de Suporte) - Para exibir as últimas 20 linhas de um arquivo, em Linux, com nome teste.txt, é necessário executar o comando head -20 teste.txt.

Comentários:
Para exibir as últimas 20 linhas de um arquivo, em Linux, com nome teste.txt, é necessário executar o comando **tail** –n 20 teste.txt. O comando **head** –n 20 teste.txt lista as 20 primeiras linhas do arquivo. Assertiva errada.

Gabarito: Errada

---

122. (2012 - CESPE - TJ-AC - Analista Judiciário - Análise de Suporte) - No Linux, a execução do comando du -h permite visualizar se um ponto de montagem está com suporte à leitura e gravação.

Comentários:
O comando "du" é utilizado para saber o espaço utilizado (disk use) em disco, por pastas ou arquivos. Um comando para visualizar informações sobre pontos de montagem pode ser o cat /etc/fstab.

Gabarito: Errada

---

123. (2015 – Cespe – Tribunal de Contas da União – Auditor TI) - No Linux, o comando ls -lRash sort –s lista, em ordem decrescente de tamanho, os arquivos existentes em determinado diretório, incluindo os arquivos ocultos e os presentes em seus subdiretórios

Comentários:

Pessoal, questão do TCU com nível alto de dificuldade, para os ninjas. Para resolver a questão, é necessário lembrar os parâmetros do comando ls:

-l = listar formato longo;

-R = listagem recursiva diretórios e subdiretorios;

-a = listar arquivos ocultos;

-s = lista o tamanho (size) do arquivo;

-S = lista ordenada por tamanho

-h = formato humano;

O ponto da questão era diferenciar -s (somente lista por tamanho) de -S (listagem ordenada por tamanho). Assim, a assertiva está errada pois o parâmetro ***–s*** utilizado no comando lista os arquivos existentes no diretório e seus respectivos tamanhos, mas a listagem não é ordenada por tamanho.

Gabarito: Errada

---

124. (2015 – Cespe – Tribunal de Contas da União – Auditor TI) - No Linux, o comando chmod u+w xyz permite a escrita no arquivo xyz pelo proprietário, enquanto o comando

chmod ug=rw,o=r xpto permite a leitura e a escrita no arquivo xpto pelo proprietário e pelo grupo, além de permitir a leitura aos demais usuários.

Comentários:

Questão bastante tranquila pessoal. Vimos o comando **chmod**. O comando chmod ug=rw,o=r xpto altera a permissão de leitura e a escrita no arquivo xpto pelo proprietário e pelo grupo, e permite a leitura aos demais usuários. Assertiva correta!

Gabarito: Certa

---

125. (2015 – CESPE - TRE-PI, cargo de Analista Judiciário – Analise de sistemas) - Assinale a opção que apresenta o comando que um usuário deve utilizar, no ambiente Linux, para visualizar, em um arquivo de texto (nome-arquivo), apenas as linhas que contenham determinada palavra (nome-palavra).

A) pwd nome-arquivo | locate nome-palavra

B) find nome-palavra | ls -la nome-arquivo

C) cat nome-arquivo | grep nome-palavra

D) lspci nome-arquivo | find nome-palavra

E) cd nome-arquivo | search nome-palavra

Comentários:

a) **Errada!** O comando pwd (print working directory) informa o nome do diretório atual.

b) **Errada!** O comando find possui função de pesquisa segundo algum critério, mas não permite a visualização de conteúdo de um arquivo texto.

c) **Correta!** o comanto ***cat*** permite visualizar o conteúdo de um arquivo texto. Outro comando com finalidade similar é o comando ***tac***, que permite a visualização do arquivo, iniciando a exibição do final do arquivo. Utilizando ambos os comando conjuntamente (uso do | pipe) com o comando grep é possível filtrar apenas as linhas que correspondam ao critério determinado (nome-palavra).

d) **Errada!** O comando lspci permite listar dispositivos conectados a interfaces PCI.

e) **Errada!** O comando cd (change directory) se presta a alterar o diretório de trabalho no terminal Linux.

Gabarito: C

---

126. (2015 – CESPE - TRE-PI, cargo de Analista Judiciário – Analise de sistemas) – Assinale a opção que apresenta os comandos utilizados no console de Linux respectivamente para: comparar conteúdo de dois arquivos ASCII, procurar por trecho de texto dentro de arquivos e mudar as proteções de um arquivo.

a) pine / ls / mv

b) cf / find / rmdir

c) diff / grep / umask

d) comp / find / tail

e) file / cp / chgrp

Comentários:

Os comandos utilizados no console de Linux respectivamente para:

a) comparar conteúdo de dois arquivos ASCII = ***diff***
b) procurar por certo padrão de texto dentro de arquivos = ***grep***
c) mudar as proteções de um arquivo = **umask**

O gabarito apontou corretamente a alternativa com os seguintes comandos ***diff / grep / umask***.

Gabarito: C

---

127. (2015 – CESPE - TRE-PI, cargo de Analista Judiciário – Operação de computadores) – Assinale a opção que apresenta o comando, no sistema operacional Linux, que deve ser utilizado para determinar quanto espaço em disco está sendo ocupado por um diretório e seus subdiretórios.

a) pwd

b) file

c) du

d) head

e) lshw

Comentários:

Vejamos a alternativa que atende ao comando da questão.

a) **Errada!** O comando pwd (print working directory) informa o nome do diretório atual.

b) **Errada!** O comando file indica o tipo de arquivo ou diretório informado pelo usuário conforme os padrões do sistema operacional, entre os vários tipos de retorno, exemplos: ASCII, text, C, Program source, directory, etc.

c) **Correta!** O comando du (disk use) indica o espaço utilizado por arquivos ou diretórios em disco.

d) **Errada!** Comando head exibe as primeiras linhas de um arquivo, enquanto o comando tail exibe as linhas finais do arquivo indicado. Conjuntamente, são bastante úteis para a visualização de arquivos longos, como logs.

e) **Errada!** O comando lshw (listen hardware) apresenta informações da configuração do hardware do sistema: memória, cache, placa mãe, CPU.

Gabarito: C

---

128. (2005 - ESAF - Receita Federal - Auditor Fiscal da Receita Federal - Área Tecnologia da Informação) - No Sistema Operacional Linux, para recuperar-se um BackUp criado com o comando TAR, deve-se utilizar a opção

a) TAR -file
b) TAR -c
c) TAR -v
d) TAR -x
e) TAR –history

Comentários:
Questão de fácil resolução, pessoal. Como assevera o comando da questão, o comando TAR tem a principal finalidade comprimir e descompactar arquivos. O parâmetro –x (e**x**tract) permite recuperar um arquivo de backup. Assim, nosso gabarito é a alternativa D.

Gabarito: D

---

129. (2014 – FAURGS – TJRS – Técnico Informática) - O administrador de um servidor baseado em Linux deseja:

I - saber a quantidade de memória física da máquina.

II - saber quais usuários estão "logados" atualmente no sistema.

III - listar o conteúdo do arquivo de configuração do servidor Apache, instalado na máquina.

Assinale, dentre as opções abaixo, aquela que apresenta, respectivamente, os comandos para realizar as operações desejadas.

a) top, who e touch

b) top, who e cat

c) top, pwd e ls

d) swapon, pwd e cat

e) swapon, who e ls

Comentários:

I – O comando **top** é utilizado para verificar a quantidade de memória física da máquina.

II - O comando **who** é utilizado para saber quais usuários estão "logados" atualmente no sistema.

III - O comando **ls** é utilizado para listar os arquivos de determinado diretório. Já para exibir o conteúdo de um arquivo de configuração, utilizamos o comando ***cat***.

Assim, nosso gabarito é a alternativa B.

Gabarito: B

5 – GERENCIAMENTO DE SERVIÇOS LINUX

Neste tópico, vamos abordar as atividades de gerenciamento de serviços de rede, serviços de arquivos, e aspectos segurança.

5.1 SERVIÇOS DE REDE

DNS - DOMAIN NAME SYSTEM

O DNS é um serviço de resolução de nomes da pilha de protocolos TCP/IP. Sua estrutura é hierárquica e baseada no conceito de espaço de nomes de domínios, árvores e florestas.

O DNS permite organizar as redes em agrupamentos lógicos, que veremos em seguida, e nomear servidores, computadores e equipamentos de rede em geral (tais como roteadores,hubs, switchs).

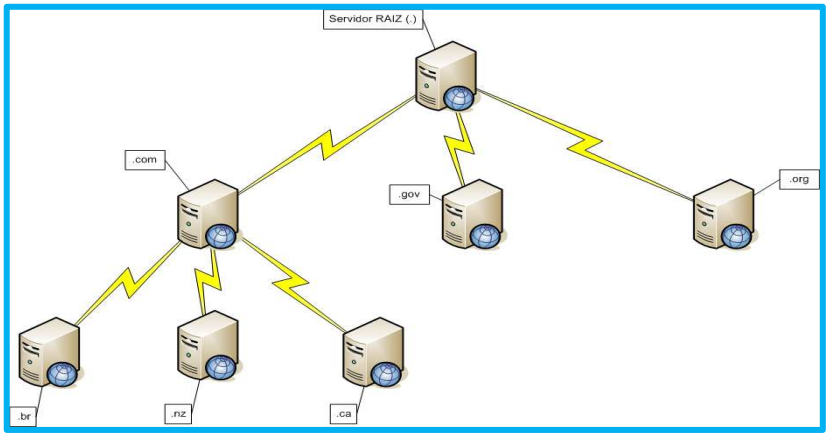
Mas por que a necessidade de um serviço de nomes?

Primeiramente por que em uma rede baseada no protocolo TCP/IP toda comunicação é feita pelo endereço IP. Porém, é muito mais intuitivo para nós o trabalho com nomes do que com números, além do fato de não ser produtivo se tivéssemos que consultar uma tabela de números IP para cada acesso a um recurso da rede.



O papel do DNS é identificar o endereço IP associado ao nome informado pelo usuário. Por exemplo, se nós digitarmos http://www.estrategiaconcursos.com.br/, para acessarmos nossa querida aula de Sistemas Operacionais, não precisamos saber o endereço IP do servidor do **Estratégia Concursos**. O papel do DNS é resolver e retornar o endereço IP associado à URL que informamos.

O DNS também pode ser conceituado como um grande banco de dados distribuído pelos servidores DNS do mundo, que proporciona a identificação dos nomes de domínios da Internet.



A figura acima exemplifica a organização hierárquica do DNS. O principal domínio, o domínio root, ou o domínio de mais alto nível é nomeado com um ponto (.). No segundo nível são definidos os domínios superiores ou de topo (Top level domains). Alguns domínios são exemplificados na Tabela abaixo.

Domínio	Descrição
.com	organizações comerciais
.gov	organizações governamentais
.edu	instituições educacionais
.org	organizações não comerciais
.net	Diversos
.mil	instituições militares

Após o nível anterior, existe um segundo nível hierárquico por distribuição geográfica, por exemplo .com.br para o Brasil.

O nome completo de um domínio é o nome completo do caminho até chegar ao domínio root (.). O nome completo de um equipamento na rede é conhecido como Full Qualified Domain Name (FQDN).

Como vimos, o DNS é baseado em conceitos como domínios e árvores, organizados de forma hierárquica. Além dos conceitos temos alguns componentes importantes do DNS, que são os seguintes:

✓ **Espaço de nomes:** espaço de nomes hierárquico e contínuo de um determinado domínio.

✓ **Servidores DNS:** contém o banco de dados de mapeamento entre os nomes DNS e o respectivo número IP, e respondem às consultas de nomes envidas por um usuário.

✓ **Registros do DNS (Resource Records):** cada entrada do banco de dados do DNS, com um mapeamento entre um nome e uma informação associada ao nome.

✓ **Cliente DNS:** Conhecidos como resolvedores (resolvers), são os softwares responsáveis por receber um pedido de resolução de nome e encaminhar esta consulta para um servidor DNS.

✓ **Cache DNS:** mapeamento mantido nos servidores e usuários para acelerar o processo de resolução DNS, mantém as últimas ou mais frequentes consultas.

Quando os mapeamentos são gravados no cache do servidor DNS, é associado com cada informação um parâmetro chamado **Time-To-Live** (TTL), que determina quanto tempo a informação será mantida no cache. O valor padrão do parâmetro TTL é 3600 segundos.

As informações sobre o DNS são armazenadas em **zona DNS** com informações sobre computadores, serviços e endereços IP para um conjunto de equipamentos. Basicamente uma zona é um arquivo com informações no servidor DNS.

Uma zona DNS é dita chamada **primária** no momento de sua criação com as informações do domínio. As zonas **secundárias** contém uma cópia integral dos registros da zona primária. As zonas secundárias somente podem ser criadas se já existir uma zona primária.

O envio e recebimento das atualizações de DNS entre zona primária e zona secundária é feito através do mecanismo de **transferência de zona**. A transferência de zona pode ser **completa** (AXFR) ou **parcial** (IXFR).

Se a zona DNS contiver informações para mapear um nome para endereço IP, será chamada **zona direta.** A **zona reversa** mapeia um endereço IP para um nome associado ao endereço IP, e é utilizada quando o usuário, por exemplo, quer saber quem responde por um determinado endereço IP que está acarretando problemas na rede.

Vamos conhecer agora uma importante informação: os **tipos de Registros DNS**.

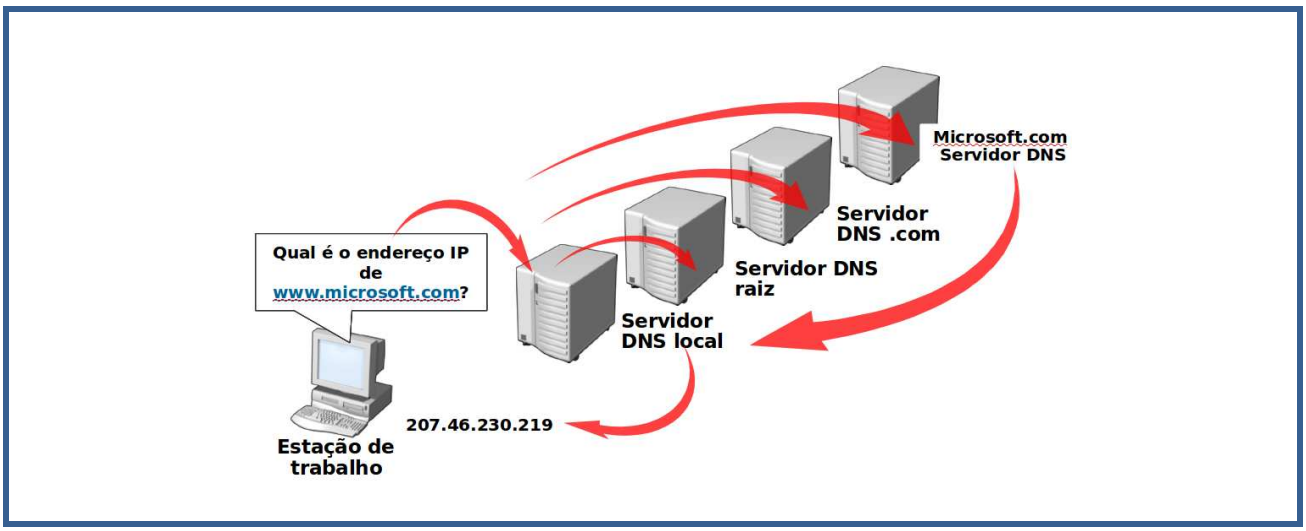
✓ **A -** Mapeamento de um nome DNS para um endereço IP versão 4, de 32 bits.
Exemplos: host1.estrategia.com.br IN A 10.10.10.1
✓ **AAAA -** Mapeamento de um nome DNS para um endereço IP versão 6, de 128 bits.
Exemplo:
ipv6_ host1.estrategia.com.br. IN AAAA 2001:db8:1:2:3:4:567:89ab
✓ **CNAME** - Canonical name (CNAME): Mapeia um alias (apelido) ou nome DNS alternativo. Exemplo:
www.estrategia.com.br. CNAME srv01.estrategia.com.br.
✓ **MX -** Mail exchanger (MX): informações utilizadas pelos servidores de e-mail, para o roteamento de mensagens.
✓ **NS –** Servidor de nomes (Name Server), relaciona um nome DNS com o servidor autoridade para o nome DNS.

✓ **PTR** - Pointer (PTR) utilizado em zonas reversas, para fazer o mapeamento reverso entre um número IP e um nome.

✓ **SOA** - Start of authority (SOA) define o nome da zona e o nome do servidor que é a autoridade para a referida zona. Contém também a definição características básicas da zona, como o valor do TTL. É sempre o primeiro registro da zona.

✓ **SRV** – mapeia um serviço ao respectivo servidor.

Quando a consulta chega ao servidor DNS, se ele não puder responder a solicitação usando informações de uma zona local do DNS e nem informações contidas no cache do servidor DNS, continuará o processo de pesquisa usando o processo de recursão (recursion).



A **recursão** consiste em o servidor DNS recorrer a outros servidores da hierarquia para responder a consulta do usuário. O processo de recursão é ilustrado na figura abaixo.

Nós podemos ter dois tipos de Servidor DNS. O servidor DNS **autoritativo** é responsável por manter os mapas referentes a uma zona local e responder a requisições vindas de máquinas de todo o mundo, que precisarem resolver nomes de domínio da zona sobre a qual este servidor tem autoridade;

O servidor DNS **recursivo** é responsável por receber as consultas DNS dos clientes locais e consultar os servidores externos, de modo a obter respostas às consultas efetuadas.

5.2 NIS

Pessoal, assim como vimos que nas redes Windows, à medida que aumenta o número de máquinas aumenta a complexidade de administração, a mesma conclusão se aplica às redes Linux. É preciso um recurso que facilite a administração, similar ao Active Directory.

Em sistemas Linux temos o OpenLDAP e também o NIS. Ambos cumprem papéis na

administração de usuários. Neste tópico iremos abordar o NIS.

No Linux, como em qualquer outro sistema operacional, existe a possibilidade de realizar logon (autenticação) de usuários. Esse papel é desempenhado pelo servidor NIS, que tem a função de informar aos clientes da rede os usuários disponíveis.

Quando um cliente NIS envia uma solicitação para um servidor NIS, ele verifica se o usuário e a senha estão corretos, caso não estejam, ele rejeita a autenticação, caso estejam corretos ele informa os programas, arquivos e configurações daquele usuário como se ele tivesse na sua máquina real.

O Network Information Service (Serviço de Informações de Rede) ou NIS (originalmente chamado de Yellow Pages, "páginas amarelas") é um protocolo de serviço de diretório cliente-servidor para distribuição de dados de configuração de sistema em uma rede de computadores.

O NIS é baseado em Chamadas de Procedimento Remoto (RPC) que utilizam um padrão de representação de dados externo. Em seu funcionamento há três tipos de ambientes NIS: master servers, slave servers e clients.

Os servidores concentram as informações do repositório para dos hosts. Os master servers possuem uma cópia do repositório, enquanto os slave servers armazenam um espelhamento das informações de forma a garantir redundância e disponibilidade das informações em caso de falha dos servidores master. Já os clients acessam e fazem uso das informações disponibilizadas pelos servidores.

A base de dados NIS é criada a partir de tabelas oriundas dos arquivos /etc/passwd, /etc/shadow e /etc/group.

5.3 DHCP

Administrar manualmente endereços IP não é uma tarefa trivial e conflitos de endereços de rede podem causar enormes transtornos, que não são fáceis de detectar e sanar.

O **Dynamic Host Configuration Protocol** (DHCP) é um protocolo de atribuição dinâmica de endereço, que constitui um recurso de redes indispensável em redes de qualquer extensão, e que facilita a administração de endereços IP da rede.

O DHCP facilita a execução de tarefas administrativas remotamente, e permite adicionar outras funções e papéis ao servidor que dependam do DHCP. O servidor DHCP de um domínio precisa ligar-se a um Active Directory e precisa estar em um servidor seja membro de um domínio.

Os servidores DHCP podem trabalhar com agrupamentos lógicos dos endereços, para facilitar a administração. O **escopo** é um agrupamento administrativo de endereços IP em uma rede que use o serviço DHCP. Um escopo tem as seguintes propriedades:

- ✓ Um intervalo de endereços IP usados para ofertas de concessão de serviço DHCP.
- ✓ Uma máscara de sub-rede.
- ✓ Um nome de escopo.
- ✓ Valores de duração da concessão.
- ✓ Outras opções do escopo DHCP, como servidor do Sistema de Nomes de Domínio (DNS), endereço IP do gateway, e endereço do servidor do serviço WINS.

Uma **reserva DHCP** é um recurso opcional que pode ser usado para garantir que um cliente DHCP sempre receba o mesmo endereço IP.

Um **superscopo** é um grupo de escopos correlacionados que pode ser criado para atender redes que trabalhem conjuntamente. Um servidor DHCP com um superscopo engloba vários escopos menores, que podem ser estabelecidos para várias redes simultaneamente.

Um recurso do Windows relacionado à atribuição de endereços IP é chamado **Automatic Private IP Addressing** (APIPA). Em redes que trabalham com DHCP, o APIPA é atribuído caso uma estação não possa receber um endereço IP de um servidor DHCP.

5.4 SMB/CIFS

SMB/CIFS

Pessoal, como devem saber, o cenário corporativo mais comum é termos várias soluções de TI heterogêneas e que requerem um esforço de integração. Neste aspecto, um importante esforço despendido é para integrar sistemas Linux e sistemas Windows. Muito provavelmente, o cenário que irão encontrar é de predominância do Linux (ou Unix Like) no ambiente de servidores, e de sistemas Windows na plataforma de desktops.

Neste ponto surge a necessidade de trabalhar com tecnologias que permitam integrar os dois ambientes. Podemos falar das tecnologias de integração em diversos níveis, protocolos de rede, troca de arquivos, etc. Nesse item vamos sobre o SMB/CIFS e o SAMBA, duas importantes tecnologias de integração.

O Server Message Block (SMB) é um protocolo de compartilhamento de arquivos em rede que permite que os aplicativos de um computador leiam e gravem em arquivos e solicitem serviços dos programas do servidor em uma rede de computadores.



O protocolo SMB pode ser usado sobre o protocolo TCP/IP ou outros protocolos de rede. Utilizando o protocolo SMB, um aplicativo (ou o usuário de um aplicativo) pode acessar arquivos ou outros recursos em um servidor remoto. Isso permite que os aplicativos leiam, criem e atualizem arquivos no servidor remoto. Ele também **pode se comunicar com qualquer programa do servidor que esteja configurado para receber uma solicitação de um cliente SMB**.

O Common Internet File System (CIFS) é o protocolo padrão para compartilhar arquivos através de redes internas ou externa. O CIFS também é um protocolo de compartilhamento de arquivos nativo do Windows, e é uma adaptação do SMB.

O CIFS define uma série de comandos usados para passar informações entre computadores em rede. O protocolo CIFS complementa o HTTP, proporcionando compartilhamento de arquivos e transferência de arquivos.

O **uso mais comum do SMB/CIFS é o compartilhamento de arquivos em uma LAN**. Ele permite que o cliente manipule arquivos como se estes estivessem em sua máquina local.

O protocolo SMB/CIFS envia pacotes do cliente para o servidor. Cada pacote é baseado em uma requisição de algum tipo, como a abertura ou leitura de um arquivo. O servidor então recebe este pacote checa-o para ver se a requisição é válida, ou seja, verifica se o cliente possui as permissões apropriadas para efetuar a requisição e finalmente executa a requisição e retorna um pacote de resposta ao cliente. O cliente então analisa o pacote de resposta para determinar se a requisição inicial foi completada com sucesso.

O SMB/CIFS é um protocolo de rede de alto nível. No modelo OSI ele pode ser classificado na camada de Aplicação/Apresentação. O SMB/CIFS depende de outros protocolos para o transporte (TCP/UDP).

Apesar do compartilhamento de arquivos ser a principal proposta do SMB/CIFS existem outras funções associadas a ele. A maioria das implementações de SMB/CIFS são capazes de determinar outros servidores SMB/CIFS na rede (navegação), compartilhar impressoras e até mesmo fornecer técnicas de autenticação.

O protocolo SMB/CIFS é extremamente utilizado pelos sistemas operacionais Microsoft Windows. Podemos dizer que o núcleo de rede nativo da Microsoft seja baseado nos serviços do SMB/CIFS.

A maioria dos sistemas Linux possuem uma implementação cliente/servidor do SMB/CIFS via **Samba**. O que faz com que o protocolo SMB/CIFS seja um protocolo comum para o compartilhamento de arquivos disponível.

O Samba é um servidor que em ambientes Linux permite compartilhar arquivos e acessar compartilhamentos em ambientes Windows. Ele é dividido em dois módulos, o **servidor Samba** propriamente dito e o **smbclient**, o cliente que permite acessar compartilhamentos em outras máquinas.

Após a instalação do Samba, o servidor Linux se comporta como uma máquina Windows, compartilhando arquivos e impressoras e executando outras funções, como autenticação de usuários. É possível até configurar o Samba para tornar-se um controlador de domínio, em redes mistas.

5.5 SEGURANÇA LINUX

Pessoal, apesar de ser considerado um sistema bastante seguro, o Linux também está sujeito a vulnerabilidades e ataques de segurança.

Existe uma infinidade de fatores que podem comprometer a segurança de servidores que utilizem sistemas operacionais Linux. Normalmente, a literatura especializada recomenda diversos procedimentos visando garantir a segurança. Vamos ver os três mais comumente presentes em provas, o Hardening, as recomendações de segurança e a proteção de logs.

LOGS

Todo sistema operacional gera eventos que, na maioria das vezes ocorrem a intervalos irregulares. Por exemplo, um servidor de arquivos gera eventos como a finalização de uma escrita em disco, a abertura de um arquivo etc. Muitos desses eventos possuem um grau de importância relativamente baixo e sendo assim não precisam ser armazenados.

Todas as ações executadas pelas aplicações que estão ativas em um sistema Linux podem ser registradas em arquivos, geralmente localizados no diretório /var/log.

Um arquivo de log contém, normalmente, os seguintes registros: data e hora em que ocorreu o evento, nome do servidor que gerou o evento, nome do programa que gerou o evento e a mensagem emitida pelo programa.

Tais informações são de extrema importância para o administrador de sistemas, auxiliando-o não só no monitoramento das atividades executadas pelos programas, como também na solução e prevenção de incidentes de segurança e falhas de software e hardware.

O **daemon syslogd é responsável pelo controle dos registros de eventos do sistema operacional e das aplicações**. A principal desvantagem do syslogd é que ele não criptografa os dados que transporta, podendo gerar problemas de segurança se os registros forem armazenados em um servidor remoto, já que estes podem ser facilmente interceptados e alterados. O arquivo de configuração ***/etc/syslog.conf*** controla os registros que serão armazenados pelo syslogd por meio de regras específicas.

Alguns arquivos de log do sistema apresentam-se no formato binário, visando aumentar a segurança dos dados neles armazenados. Dessa forma, torna-se mais complicada a alteração de um determinado registro presente nesses arquivos.

É recomendada a configuração das permissões de acesso desses arquivos para o valor 644, definindo o usuário root como o dono dos arquivos.

Arquivo /var/log/lastlog

Arquivo binário que registra o horário do último acesso (ou tentativa de acesso) feito por cada um dos usuários do sistema. Seu conteúdo muda a cada login efetuado e é visualizado toda vez que um determinado usuário efetua login, ou quando os comandos finger ou lastlog são executados.

No Linux, esses registros devem ser explicitamente habilitados, configurando no arquivo /etc/login.defs.

Arquivo /var/log/utmp

Arquivo binário que registra informações relacionadas a usuários locais que se encontram logados no sistema. Para ter acesso aos dados contidos nesse arquivo, podem ser utilizados os comandos w, who e finger.

Arquivo /var/log/wtmp

Arquivo binário que registra informações sobre as últimas sessões abertas e encerradas pelos usuários. Para ter acesso aos dados contidos nesse arquivo é necessária a execução do comando last.

HARDENING

O Hardening é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com o objetivo tornar um sistema Linux preparado para enfrentar tentativas de ataque.

Normalmente, o Hardening é uma atividade complexa e abrangente que é realizada por especialistas em segurança em um determinado domínio, por exemplo um servidor Linux que atue como servidor web requer um especialista em Hardening de servidores web.

No processo de Hardening, além dos aspectos relativos as peculiaridades de um sistema Linux, são observadas boas práticas e recomendações que visam reduzir a área de um servidor Linux que pode se sujeitar a ataques.

RECOMENDAÇÕES DE SEGURANÇA

Em conjunto com o Hardening, são seguidas algumas recomendações básicas de segurança, que não são obrigatórias, mas devem ser seguidas pelo administrador de sistemas, nos casos em que ele julgar necessário, a fim de tornar seus sistemas mais seguros.

Sincronização - Manter os relógios de todos os servidores da rede sincronizados por meio do protocolo Network Time Protocol (NTP), para evitar inconsistências nos horários dos registros dos eventos gerados pelos diversos servidores, facilitando possíveis auditorias em casos de incidentes de segurança.

Proteção de logs - Recompilar o syslogd, modificando o nome e a localização do arquivo /etc/syslog.conf, para dificultar possíveis tentativas de apagar registros de invasões.

Instalar um servidor dedicado ao armazenamento de registros de eventos gerados por todos os servidores da organização, desativando qualquer outro serviço desse servidor.

Fazer um backup diário do servidor de logs para garantir a integridade, a autenticidade e a disponibilidade dos arquivos de log.

Módulos de segurança – utilizar módulos especializados em segurança, como o Linux Intrusion Detection System. O LIDS é um patch para o kernel do Linux que adiciona funcionalidades de segurança como: Mandatory Access Control (MAC); detecção de port scanners; proteção contra acessos a arquivos e diretórios (inclusive para o usuário root) e proteção extra para processos, módulos e interfaces.

Com LIDS é possível restringir qualquer tipo de acesso ao sistema; qualquer tentativa de acesso não autorizada em sistemas protegidos por ele é reportada através de e-mails e registros nos arquivos de log.

Pessoal, essas recomendações que citamos são apenas exemplificativas. É importante saberem que esta é uma área bastante abrangente. Existem normativos e boas práticas bem extensos que tratam do tema, como por exemplo.

Vale ressaltar que este não é um tópico recorrente em provas de concursos, somente é mais exigido para provas de cargos especializados em segurança, ok.

Vale lembrar que abordamos outros aspectos indiretamente ligados a segurança nos demais tópicos dessa aula, como permissões de acesso, sombreamento de senhas em /etc/shadow, sistema de arquivos, etc.

Neste ponto da aula, recorremos a conteúdo elaborado pelo www.cert.br, que é a principal referência utilizada pelas bancas de concurso, e que indicamos para aqueles que desejarem se aprofundar no assunto.



Não esqueçam de observar quais os tópicos prediletos da banca!!! Busquem otimizar os estudos.

5.6 RESOLUÇÃO DE QUESTÕES

130. (2012 – ESAF – CGU - Analista de Finanças e Controle) - É um mecanismo de Hardening do Servidor Linux:

a) minimizar software instalado.
b) instalar apenas softwares padronizados internacionalmente.
c) instalar versões antigas do sistema operacional e fazer logo em seguida o upgrade do sistema.
d) não fazer upgrades frequentes, o que pode comprometer a segurança do sistema.
e) manter instalados todos os serviços, mesmo os que sejam aparentemente desnecessários.

Comentários:

Pessoal, hardening (termo em inglês, que pode ser traduzido como ajuste, endurecimento) é um processo de ajuste de uma instalação de um sistema operacional, para colocação em produção, no qual se objetiva reduzir a superfície de ataque do sistema operacional. A alternativa A apresenta

claramente uma técnica de hardening, reduzir a quantidade de software àquela necessária a sua atividade primordial. As demais alternativas estão equivocadas.

Gabarito: A

---

131. (2014 – IADES – EBSERH - Analista de TI - Suporte e Redes) - O CUPS é o sistema de impressão usado atualmente na maioria dos sistemas Linux. A adição de novas impressoras pode ser feita através da sua interface web, que em sua configuração padrão, armazena as informações das impressoras na pasta

a) /etc/printers
b) /etc/cups/printers
c) /etc/cups/ppd
d) /dev/prn
e) /dev/interfaces/printers

Comentários:
O CUPS (Common Unix Printing System) é um sistema de impressão para sistemas Linux e permite ser configurado pelo navegador web. O CUPS permite ao administrador adicionar, remover, gerenciar impressoras. É possível configurar o driver de dispositivo que o CUPS fornece para as impressoras ao editar arquivos de texto no formato **PostScript Printer Description** (PPD). O CUPS armazena as informações dos drivers das impressoras na pasta /etc/cups/ppd. Gabarito letra C.

Gabarito: C

---

132. (2014 – IADES - TRE-PA - Técnico Judiciário - Operação de Computador) - Programas maliciosos de computador podem colocar em risco a integridade dos sistemas que nele rodam e também podem proporcionar acesso indevido a informações sigilosas que ele contenha. Em sistemas Linux, é correto afirmar que os hackers costumam utilizar um software de invasão chamado

a) rootkit.
b) spyware.
c) vírus.
d) malware.
e) keylogger.

Comentários:

Questão de fácil resolução, pessoal. Rootkits são um conjunto de artefatos maliciosos utilizados em hackerismo para comprometer e manter um sistema Linux. Segundo a definição do SANS Institute, "*A rootkit is a **collection of tools** (programs) that a **hacker uses to mask intrusion and obtain administrator-level access** to a computer or computer network*". O principal diferencial no uso de um rootkit é a amplitude do comprometimento propiciado, pois um rootkit age no nível do kernel, manipulando e alterando as funcionalidades dos comandos de root, daí provém seu nome. A única alternativa compatível é portanto a letra A.

Gabarito: A

---

133. (2014 – IADES - TRE-PA - Técnico Judiciário - Operação de Computador) - Um servidor Linux pode hospedar o serviço de resolução de nomes de uma rede de computadores. Conhecido por DNS, esse serviço é indispensável em uma rede que possua conexão com a internet. O nome de um pacote que implementa o DNS, muito utilizado em sistemas operacionais Linux, é

a) Firefox.
b) Apache.
c) Squid.
d) Postfix.
e) BIND.

Comentários:
Questão bastante ilustrativa da natureza das questões da banca. Simples e direta: definir um comando ou pacote responsável por uma função. Dentre as alternativas, a única que corresponde a um pacote Linux que implementa o DNS e é utilizado em sistemas operacionais Linux, é a alternativa E: bind. O ***bind*** (Berkeley Internet Name Daemon) é uma referência na implementação do protocolo DNS (Domain Name System). Nosso gabarito é a letra E.

Gabarito: E

---

134. (2013 - CESPE - TRT - 17ª Região (ES) - Analista Judiciário - Tecnologia da Informação) - Para configurar em um host Linux o servidor DNS (domain name system) cujo endereço IP é 8.8.8.8, deve-se editar o arquivo /etc/resolv.conf e adicionar uma entrada no formato ServerDNS 8.8.8.8.

Comentários:
Pessoal, questão sobre DNS, o qual vimos na parte teórica. Atentem que o arquivo para editar a configuração do servidor DNS é o /etc/resolv.conf.

Para configurar em um host Linux o servidor DNS, cujo endereço IP é 8.8.8.8, deve-se editar o arquivo /etc/resolv.conf e adicionar uma entrada no formato nameserver 8.8.8.8.
O erro da assertiva está somente no trecho final, em vez de ServerDNS, o registro DNS correto é **nameserver**.

Gabarito: Errada

---

135. (2013 – CESPE - TRT - 8ª Região (PA e AP) - Analista Judiciário - Tecnologia da Informação) - Assinale a opção em que é apresentado o protocolo do Windows responsável por compartilhar discos e impressoras em uma rede interna entre computadores Linux e Windows.

a) Telnet
b) SMB (server message block)
c) TCP/IP
d) FTP (file transfer protocol)
e) BitTorrent

Comentários:
O Server Message Block (SMB) é um protocolo de compartilhamento de arquivos em rede. O protocolo SMB pode ser usado sobre o protocolo TCP/IP ou outros protocolos de rede. Utilizando o protocolo SMB, um aplicativo (ou o usuário de um aplicativo) pode acessar arquivos ou outros recursos em um servidor remoto. Isso permite que os aplicativos leiam, criem e atualizem arquivos no servidor remoto. Ele também pode se comunicar com qualquer programa do servidor que esteja configurado para receber uma solicitação de um cliente SMB. Além disso, o SMB é responsável por compartilhar discos e impressoras em uma rede interna entre computadores Linux e Windows.

Gabarito: B

---

136. (2013 – CESPE – SERPRO - Analista – Redes) - O protocolo IPv6 é desabilitado por padrão no Kernel 2.6 do Linux. Para habilitar essa funcionalidade, é necessário manipular o arquivo sysctl.conf em /etc.

Comentários:
A partir das versões 2.2.x, o suporte ao IPv6 passou a ser compilado junto ao kernel, entretanto ainda não vinha habilitado por padrão. Atualmente, a maioria das distribuições Linux já vem com o suporte ao IPv6 compilado e habilitado. Questão errada.

Gabarito: Errada

---

137. (2015 – Cespe – Tribunal de Contas da União – Auditor TI) - No Linux, o aplicativo Pacemaker possibilita criar nuvens com os recursos de manipulação de arquivos, de acordo com a arquitetura GRID.

Comentários:

Pessoal, apesar da questão se referir a Linux, também está afeita às soluções de Cloud Computing. Na verdade, o Pacemaker não é uma solução de computação em nuvem. Pacemaker é um orquestrador/gerenciador de recursos para clusters (e não para Grids) de HA que integra algumas distribuições Linux, como Debian e Red Hat. Ele não possibilita a criação de nuvens. Assertiva errada.

Gabarito: Errada

GABARITO

1.	C	39.	CERTA	77.	D	115.	CERTA
2.	E	40.	CERTA	78.	A	116.	CERTA
3.	B	41.	CERTA	79.	B	117.	CERTA
4.	B	42.	CERTA	80.	A	118.	ERRADA
5.	C	43.	ERRADA	81.	A	119.	ERRADA
6.	A	44.	CERTA	82.	ERRADA	120.	ERRADA
7.	C	45.	CERTA	83.	C	121.	ERRADA
8.	B	46.	ERRADA	84.	CERTA	122.	ERRADA
9.	D	47.	E	85.	C	123.	ERRADA
10.	B	48.	ERRADA	86.	ERRADA	124.	CERTA
11.	CERTA	49.	C	87.	E	125.	C
12.	CERTA	50.	E	88.	A	126.	C
13.	CERTA	51.	E	89.	C	127.	C
14.	E	52.	D	90.	B	128.	D
15.	A	53.	D	91.	C	129.	B
16.	D	54.	E	92.	E	130.	A
17.	B	55.	B	93.	D	131.	C
18.	A	56.	E	94.	A	132.	A
19.	C	57.	C	95.	E	133.	E
20.	D	58.	C	96.	B	134.	ERRADA
21.	E	59.	A	97.	A	135.	B
22.	A	60.	D	98.	A	136.	ERRADA
23.	A	61.	E	99.	B	137.	ERRADA
24.	C	62.	B	100.	A		
25.	B	63.	C	101.	C		
26.	A	64.	CERTA	102.	E		
27.	B	65.	ERRADA	103.	E		
28.	B	66.	ERRADA	104.	A		
29.	A	67.	ERRADA	105.	E		
30.	E	68.	CERTA	106.	A		
31.	D	69.	ERRADA	107.	A		
32.	CERTA	70.	CERTA	108.	B		
33.	ERRADA	71.	ERRADA	109.	E		
34.	ERRADA	72.	CERTA	110.	E		
35.	A	73.	CERTA	111.	B		
36.	ERRADA	74.	CERTA	112.	A		
37.	A	75.	ERRADA	113.	CERTA		
38.	CERTA	76.	CERTA	114.	CERTA		

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.



Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.