Fundamentos de Servidores Linux

Guia Introdutório Prático

SUMÁRIO

1. Objetivo da Apostila

Este material foi desenvolvido para apresentar os fundamentos de servidores Linux de forma simples e direta, especialmente para quem está começando. O conteúdo evolui passo a passo, desde os conceitos básicos até práticas essenciais do dia a dia em ambiente servidor.

Ao longo da apostila, são abordados temas como estrutura de diretórios, uso do terminal, permissões, usuários, processos, monitoramento e noções de rede, formando uma base sólida para atuação profissional.

Os exemplos utilizam, em sua maioria, comandos compatíveis com distribuições baseadas em Red Hat, como o ***Oracle Linux***, mas os conceitos também se aplicam a outras distribuições, com pequenas variações.

O guia pode servir tanto para aprendizado inicial quanto como apoio rápido nas atividades diárias com servidores Linux.

2. Introdução ao Linux em Ambiente de Servidor

O Linux é um sistema operacional amplamente utilizado em servidores devido à sua estabilidade, segurança e flexibilidade. Baseado no modelo de software livre, ele permite que organizações e profissionais adaptem o sistema conforme suas necessidades operacionais, sendo presença dominante em ambientes corporativos, data centers e infraestrutura de serviços online.

O núcleo do sistema (kernel) Linux foi criado por Linus Torvalds evoluiu com contribuições da comunidade global e de iniciativas ligadas à Free Software Foundation. Essa colaboração contínua resultou em um ecossistema robusto, confiável e amplamente documentado.

2.1. Linux no contexto de servidores

Em um ambiente de servidor, o Linux é utilizado para fornecer serviços de rede, hospedar aplicações, gerenciar usuários e garantir disponibilidade contínua de recursos. Diferentemente de sistemas voltados ao uso pessoal, servidores Linux são configurados para operar com foco em desempenho, controle administrativo e operação remota.

Características marcantes em servidores Linux:

- Operação estável por longos períodos
- Administração predominantemente via terminal
- Controle granular de permissões e acessos
- Alto nível de automação e personalização

2.2. Acesso e interação com o sistema

A administração de servidores Linux normalmente ocorre por meio de acesso remoto em modo texto, utilizando um interpretador de comandos (shell). Essa forma de interação permite controle preciso do sistema e execução eficiente de tarefas administrativas.

2.3. Importância no ambiente profissional

O domínio dos fundamentos do Linux é uma competência essencial para profissionais de infraestrutura, redes e operações de TI. A compreensão de sua estrutura e funcionamento permite administrar serviços, diagnosticar problemas e aplicar boas práticas de segurança em ambientes corporativos.

3. Organização do Sistema de Arquivos

O sistema de arquivos é a estrutura responsável por organizar, armazenar e gerenciar dados dentro do sistema operacional. No Linux, ele define como os arquivos são nomeados, armazenados no disco, protegidos e recuperados quando solicitados pelo usuário ou por um processo.

Diferentemente de alguns sistemas operacionais que utilizam múltiplas unidades identificadas por letras (como C:, D:, etc.), o Linux adota uma estrutura unificada, iniciada a partir de um único ponto chamado raiz, representado pelo símbolo '/'. Todos os arquivos e diretórios do sistema estão organizados a partir dessa raiz.

O sistema de arquivos também controla permissões de acesso, proprietários, grupos e metadados importantes, como data de modificação, tamanho e tipo de arquivo.

Entre os sistemas de arquivos mais utilizados no Linux estão:

- ext4

- xfs

- btrfs

Exemplo prático: Quando um administrador salva um arquivo chamado 'backup.sh' no diretório /home/admin, o sistema registra o local físico no disco, as permissões e o proprietário.

3.1. Hierarquia de Diretórios

O Linux segue o padrão Filesystem Hierarchy Standard (FHS), que define a organização dos diretórios do sistema. A estrutura começa no diretório raiz '/'.

Principais diretórios:

`/` → Diretório raiz do sistema

`/bin` → Comandos essenciais do sistema

`/boot` → Arquivos de inicialização

`/dev` → Dispositivos do sistema

`/etc` → Arquivos de configuração

`/home` → Diretórios pessoais dos usuários

`/lib` → Bibliotecas do sistema

`/mnt` → Ponto de montagem temporário

`/opt` → Programas adicionais

`/root` → Diretório do administrador

`/sbin` → Comandos administrativos

`/tmp` → Arquivos temporários

`/usr` → Programas de uso geral

`/var` → Logs e arquivos variáveis

Exemplo prático:

```
cd /var/log

ls
```

3.2. Localização de Arquivos Importantes

Arquivos de configuração geralmente estão em /etc.

Logs do sistema ficam em /var/log.

Diretórios pessoais estão em /home/usuario.

Arquivos de inicialização estão em /boot.

Exemplos de comandos:

```
cat /etc/passwd

tail -n 20 /var/log/syslog
```

3.3. Caminhos Absolutos e Relativos

Os caminhos indicam a localização de um arquivo dentro da estrutura do sistema. Eles podem ser absolutos ou relativos.

Caminho absoluto: começa a partir da raiz '/'.

/home/joao/relatorio.txt

Caminho relativo: depende do diretório atual em que o usuário está.

```
cat relatorio.txt
```

Símbolos especiais utilizados:

. → Diretório atual

.. → Diretório pai

```
cd ..
```

A compreensão correta da organização do sistema de arquivos é essencial para administração segura e eficiente de servidores Linux.

4. Uso do Terminal e Navegação no Sistema

O primeiro terminal que vamos ver é o shell é o interpretador de comandos do Linux. Ele atua como intermediário entre o usuário e o kernel, permitindo executar comandos, scripts e programas por meio da linha de comando.

Em servidores Linux, o uso do shell é predominante, pois muitos ambientes não possuem interface gráfica. O acesso normalmente ocorre via terminal local ou remotamente por meio de SSH.

Os shells mais comuns são:

- bash (padrão na maioria das distribuições)

- sh

- zsh

Quando um comando é digitado, o shell interpreta a instrução e solicita ao sistema que execute a ação correspondente.

Exemplo:

```
date
```

4.1. Navegação entre Diretórios

A navegação no sistema de arquivos é feita principalmente com o comando 'cd' (change directory).

Comandos básicos:

```
pwd
```

Exibe o diretório atual.

```
cd /var/log
```

Acessa um diretório utilizando caminho absoluto.

```
cd ..
```

Retorna ao diretório pai.

```
cd ~
```

Retorna ao diretório pessoal do usuário.

4.2. Visualização de Arquivos e Diretórios

Para listar arquivos e diretórios utiliza-se o comando 'ls'.

```
ls
```

Lista o conteúdo do diretório atual.

```
ls -l
```

Mostra detalhes como permissões, proprietário e tamanho.

```
ls -a
```

Exibe arquivos ocultos.

Para visualizar o conteúdo de arquivos:

```
cat arquivo.txt
```

Exibe todo o conteúdo do arquivo.

```
less arquivo.txt
```

Permite visualizar o conteúdo página por página.

```
more arquivo.txt
```

Outra forma de visualização paginada.

4.3. Criação, Cópia, Movimentação e Remoção

Comandos principais para manipulação de arquivos e diretórios:

```
mkdir novo_diretorio
```

Cria um novo diretório.

```
touch arquivo.txt
```

Cria um arquivo vazio.

```
cp arquivo.txt /home/usuario/
```

Copia um arquivo para outro local.

```
cp -r pasta1 pasta2
```

Copia um diretório e seu conteúdo.

```
mv arquivo.txt novo_nome.txt
```

Move ou renomeia arquivo.

```
rm arquivo.txt
```

Remove arquivo.

```
rmdir pasta
```

Remove diretório vazio.

```
rm -r pasta
```

Remove diretório com conteúdo.

É importante utilizar o comando 'rm' com cautela, pois a exclusão é permanente em ambiente servidor.

5. Gerenciamento Básico de Usuários

No Linux, usuários são entidades que representam pessoas ou serviços que acessam o sistema. Cada usuário possui um identificador único (UID), senha e permissões específicas.

Grupos são conjuntos de usuários utilizados para facilitar o controle de acesso a arquivos e recursos. Cada grupo possui um identificador chamado GID.

Esse modelo permite aplicar o princípio do menor privilégio, garantindo que cada conta possua apenas os acessos necessários.

5.1. Criação e Remoção de Usuários

Para criar um usuário:

```
useradd nome_usuario
```

Para criar usuário já com diretório pessoal:

```
useradd -m nome_usuario
```

Para remover um usuário:

```
userdel nome_usuario
```

Para remover usuário e seu diretório pessoal:

```
userdel -r nome_usuario
```

Para criar um grupo:

```
groupadd nome_grupo
```

5.2. Alteração de Senhas

A senha pode ser definida ou alterada com o comando:

```
passwd nome_usuario
```

O sistema solicitará a nova senha e sua confirmação. As senhas são armazenadas de forma criptografada.

5.3. Diretórios Pessoais

Cada usuário possui um diretório pessoal geralmente localizado em /home/nome_usuario. Esse diretório armazena arquivos, configurações e dados individuais.

Exemplo de verificação dos diretórios de usuários:

```
ls /home
```

O diretório do usuário root é uma exceção e está localizado em /root.

O gerenciamento adequado de usuários é essencial para manter a segurança e organização em servidores Linux.

6. Processos e Operação do Sistema

No Linux, um processo é um programa em execução. Sempre que um comando, aplicação ou serviço é iniciado, o sistema cria um processo correspondente na memória.

Cada processo possui um identificador único chamado PID (Process ID), além de informações como usuário proprietário, consumo de CPU e memória.

Serviços essenciais do sistema, como servidor web ou banco de dados, também funcionam como processos em execução contínua.

6.1. Visualização e Controle de Processos

Para listar processos ativos:

```
ps aux
```

Para monitorar processos em tempo real:

```
top
```

Outra alternativa moderna de monitoramento:

```
htop
```

Para encerrar um processo pelo PID:

```
kill PID
```

Para forçar o encerramento de um processo:

```
kill -9 PID
```

O uso adequado desses comandos permite controlar aplicações travadas ou processos que estejam consumindo recursos excessivos.

6.2. Inicialização e Desligamento do Sistema

A maioria das distribuições Linux modernas utiliza o systemd como sistema de inicialização e gerenciamento de serviços.

Para reiniciar o sistema:

```
reboot
```

Para desligar o sistema imediatamente:

```
shutdown -h now
```

Para agendar desligamento:

```
shutdown -h +10
```

O desligamento correto é fundamental para evitar corrupção de dados e garantir integridade do sistema.

6.3. Monitoramento Básico do Sistema

O monitoramento é uma atividade contínua na administração de servidores Linux. Ele permite acompanhar consumo de recursos, identificar gargalos e antecipar falhas.

Para verificar uso de memória:

```
free -h
```

Para verificar espaço em disco:

```
df -h
```

Para visualizar informações gerais do sistema:

```
uname -a
```

Uso de CPU em tempo real:

```
top
```

Tempo ligado e carga média do sistema:

```
uptime
```

Tamanho ocupado por diretório específico:

```
du -sh /diretorio
```

Listar dispositivos de armazenamento:

```
lsblk
```

Verificar interfaces de rede:

```
ip addr
```

Listar portas abertas:

```
ss -tuln
```

Testar conectividade:

```
ping 8.8.8.8
```

Acompanhar logs em tempo real:

```
tail -f /var/log/syslog
```

Visualizar logs via systemd:

```
journalctl -xe
```

Estatísticas de CPU e memória a cada 5 segundos:

```
vmstat 5
```

Estatísticas de uso de disco (requer pacote sysstat):

```
iostat
```

O uso combinado desses comandos permite uma visão clara da saúde do servidor, auxiliando na identificação rápida de problemas de desempenho ou conectividade.

7. Fundamentos de Rede em Servidores Linux

Todo servidor Linux precisa estar corretamente identificado na rede por meio de endereço IP, nome de host (hostname) e máscara de rede. Essas informações permitem que o sistema seja localizado e acessado por outros dispositivos.

Para visualizar o endereço IP configurado:

```
ip addr
```

Para verificar o nome do host:

```
hostname
```

Para visualizar informações detalhadas do hostname:

```
hostnamectl
```

7.1. Configurações Básicas de Conectividade

As configurações de rede podem ser definidas de forma dinâmica (DHCP) ou estática. Em servidores, é comum utilizar IP fixo para garantir estabilidade na comunicação.

Para verificar rota padrão configurada:

```
ip route
```

Para configurar IP temporariamente (exemplo):

```
ip addr add 192.168.1.100/24 dev eth0
```

Para reiniciar serviço de rede (systemd):

```
systemctl restart NetworkManager
```

7.2. Testes de Comunicação

Para testar conectividade com outro host:

```
ping 192.168.1.1
```

Para testar resolução de nomes (DNS):

```
nslookup google.com
```

Para testar conexão com porta específica:

```
telnet 192.168.1.10 80
```

Para verificar caminho até um destino:

```
traceroute 8.8.8.8
```

7.3. Noções de Serviços de Rede

Serviços de rede são aplicações que permitem comunicação entre sistemas, como servidores web, servidores de arquivos, bancos de dados e serviços de autenticação.

Para verificar portas abertas no sistema:

```
ss -tuln
```

Para verificar status de um serviço:

```
systemctl status nome_do_servico
```

Para iniciar ou parar um serviço:

```
systemctl start nome_do_servico

systemctl stop nome_do_servico
```

O entendimento básico de rede é fundamental para administração de servidores, pois praticamente todos os serviços dependem de conectividade estável e corretamente configurada.

8. Manutenção e Boas Práticas

Manter o sistema organizado é essencial para facilitar a administração e evitar falhas operacionais. Arquivos devem ser armazenados em diretórios apropriados, respeitando a hierarquia padrão do Linux.

Evite armazenar arquivos críticos em diretórios temporários e mantenha separação clara entre dados, configurações e arquivos de usuários.

Verificar utilização de espaço em disco:

```
df -h
```

Verificar tamanho de diretórios específicos:

```
du -sh /diretorio
```

8.1. Atualizações e Cuidados Gerais

Manter o sistema atualizado é uma das principais práticas de segurança. Atualizações corrigem falhas, vulnerabilidades e melhoram o desempenho.

Em sistemas baseados em Red Hat / Oracle Linux:

```
dnf update
```

Em sistemas Debian/Ubuntu:

```
apt update && apt upgrade
```

Antes de atualizações críticas, recomenda-se realizar backup e verificar compatibilidade com aplicações em produção.

8.2. Registro de Eventos do Sistema

O sistema registra eventos e mensagens importantes em arquivos de log, que auxiliam na identificação de erros e auditoria.

Visualizar logs recentes:

```
tail -f /var/log/messages
```

Em sistemas com systemd:

```
journalctl -xe
```

A análise periódica dos logs permite detectar comportamentos anormais ou falhas antes que impactem os serviços.

8.3. Rotinas Básicas de Administração

A administração de servidores envolve tarefas recorrentes, como verificação de recursos, monitoramento de serviços e conferência de backups.

Verificar status de um serviço:

```
systemctl status nome_do_servico
```

Reiniciar serviço:

```
systemctl restart nome_do_servico
```

Agendar tarefas automáticas:

```
crontab -e
```

A adoção de rotinas periódicas garante estabilidade, segurança e continuidade operacional do ambiente.

9. Introdução à Segurança em Linux

A segurança em servidores Linux baseia-se em princípios como o menor privilégio, atualizações constantes e controle rigoroso de acessos. O objetivo é reduzir a superfície de ataque e proteger dados e serviços.

O princípio do menor privilégio determina que cada usuário ou serviço deve possuir apenas as permissões estritamente necessárias para executar suas funções.

Exemplo de verificação de usuários conectados:

```
who
```

Verificar tentativas de login no sistema:

```
last
```

9.1. Controle de Acesso

O controle de acesso é realizado por meio de usuários, grupos e permissões de arquivos.

Visualizar permissões de um arquivo:

```
ls -l arquivo.txt
```

Alterar permissões:

```
chmod 640 arquivo.txt
```

Alterar proprietário:

```
chown usuario:grupo arquivo.txt
```

Em ambientes corporativos, também pode ser utilizado firewall para restringir acessos externos.

Verificar status do firewall (exemplo com firewalld):

```
systemctl status firewalld
```

9.2. Boas Práticas Operacionais

Entre as boas práticas estão manter o sistema atualizado, utilizar senhas fortes, realizar backups periódicos e monitorar logs regularmente.

Atualizar sistema (Oracle Linux / Red Hat):

```
dnf update
```

Verificar logs de segurança:

```
tail -f /var/log/secure
```

Evitar exposição desnecessária de serviços e manter apenas portas essenciais abertas.

Verificar portas abertas:

```
ss -tuln
```

9.3. Uso Consciente de Privilégios Administrativos

O usuário root possui controle total sobre o sistema. O uso constante dessa conta pode aumentar riscos de segurança.

Trocar para usuário administrador temporariamente:

```
su -
```

Executar comando com privilégio administrativo:

```
sudo comando
```

O uso do sudo é recomendado para tarefas administrativas pontuais, mantendo o registro das ações executadas.

A adoção dessas práticas contribui para um ambiente mais seguro, estável e adequado ao uso profissional.

10. Encerramento e Próximos Passos

Ao longo desta apostila foram apresentados os fundamentos essenciais para administração básica de servidores Linux. Foram abordados conceitos estruturais do sistema, organização de diretórios, uso do terminal, permissões, gerenciamento de usuários, processos, monitoramento, rede, manutenção e segurança.

O domínio desses conceitos permite compreender como o sistema operacional funciona internamente e como os recursos são organizados e controlados.

Entre os principais comandos estudados, destacam-se ferramentas para navegação, manipulação de arquivos, gerenciamento de usuários, monitoramento de processos e verificação de rede.

Exemplo de rotina básica combinando comandos aprendidos:

```
df -h

free -h

ss -tuln

systemctl status sshd
```

Esse conjunto simples de verificações já permite ao administrador avaliar espaço em disco, uso de memória, portas abertas e status de serviços críticos.

10.1. Caminhos para Aprofundamento

Após a compreensão dos fundamentos, o próximo passo é aprofundar conhecimentos em áreas específicas da administração de sistemas.

Alguns temas recomendados para continuidade dos estudos incluem:

- Gerenciamento avançado de serviços com systemd

- Configuração de servidores web (Apache ou Nginx)

- Implementação de servidores de banco de dados

- Hardening de segurança e firewall avançado

- Virtualização e containers (Docker)

- Automação com Shell Script

Exemplo de verificação de serviços habilitados na inicialização:

```
systemctl list-unit-files --type=service
```

O aprofundamento técnico amplia a capacidade de atuação profissional e prepara o administrador para ambientes corporativos mais complexos.

10.2. Aplicação Prática no Ambiente Profissional

No ambiente corporativo, servidores Linux são utilizados para hospedar aplicações, bancos de dados, serviços de autenticação, armazenamento de arquivos e sistemas críticos.

A aplicação prática envolve atividades como configuração de usuários, monitoramento contínuo, atualização do sistema, análise de logs e resolução de incidentes.

Exemplo de verificação de logs para análise de falhas:

```
journalctl -xe

tail -f /var/log/messages
```

Além do conhecimento técnico, é fundamental desenvolver boas práticas como documentação de procedimentos, realização periódica de backups e planejamento de contingência.

A experiência prática consolida o aprendizado teórico e contribui para o desenvolvimento de autonomia e segurança na administração de servidores.

Este guia representa o ponto de partida para a formação em administração de sistemas Linux, servindo como base sólida para evolução profissional na área de infraestrutura e tecnologia da informação.