0839- Linux - serviços de redes

João Silva

2022

Conteúdo

I Introdução **5**

0.1 Introdução . . . 7

1 Serviços de rede **9**

1.1 etc/rc.d/init.d/ . . . 9
1.1.1 Exercicio prático: . . . 9
1.2 Lista de portas e serviços no . . . 9
1.2.1 Exercício prático: . . . 10
1.3 Encerramento de um serviço ou porta . . . 10
1.3.1 Usando o kill . . . 10
1.3.2 Exercício prático: . . . 10
1.3.3 Exercício prático: . . . 10
1.4 XINET. . . . 10
1.4.1 Exercício prático: . . . 11
1.5 Arquivo /etc/xinetd.conf . . . 12
1.5.1 Exercício prático . . . 12
1.6 TCPWrappers . . . 13
1.6.1 /etc/hosts.allow . . . 13
1.6.2 /etc/hosts.deny . . . 13
1.6.3 Exercício prático . . . 13

2 NIS **15**

2.1 Tipos de servidor NIS . . . 15
2.1.1 Exercícios práticos . . . 16

3 DHCP **17**

3.1 Conceitos . . . 17
3.2 Iniciação do servidor DHCP . . . 17
3.3 Descrição dos principais parâmetros - lease time, range, mac address, routers, domain name . . . 17
3.3.1 Exercício prático: . . . 17
3.4 Name servers . . . 18
3.4.1 Arquivo /var/lib/dhcp/dhcpd. . . . 18
3.5 Configuração do range de uma rede . . . 19
3.6 Definição de informações para a rede TCP . . . 19
3.6.1 Exercício prático: . . . 19
3.7 Definição de IP e informações para uma máquina específica na rede através de seu endereço físico 20
3.8 Coexistência de mais de um servidor DHCP na rede . . . 20
3.8.1 Exercício prático: . . . 21
3.9 Configuração de um cliente para o acesso à rede DHCP . . . 21
3.10 Comando pump . . . 21
3.11 DHCP do Linux . . . 22
3.11.1 Exercício prático: . . . 22

4 DNS **23**

4.1 Zona, Domínios e Nós . . . 23
4.2 Servidores Matriz (root servers) . . . 23
4.3 Servidores DNS locais . . . 24
4.3.1 Exercício prático: . . . 24
4.4 FAPESP e Internic . . . 24
4.5 DNS e replicação de zonas . . . 24

4.6 BIND (named) - Berkeley Internet Name Domain 24
4.6.1 1.24.1 arquivo /etc/named.conf 25
4.6.2 Exercício prático: 25
4.6.3 Arquivo /var/named/named.ca 25

5 LOGS **27**
5.1 Arquivos de log do sistema 27
5.2 Pasta /var/log 27
5.2.1 Exercício prático 27
5.2.2 Exercício 28
5.2.3 Exercício prático 28
5.3 Syslogd 29
5.4 Arquivo syslog 29
5.4.1 Exercício prático 29
5.5 Apache 30
5.6 Sendmail 30
5.7 Bibliografia 31
5.8 Webgrafia 31

Parte I

Introdução

0.1 Introdução

Os serviços de rede em sistemas Linux são componentes fundamentais que permitem a comunicação entre diferentes dispositivos numa rede. Estes serviços permitem que as aplicações comuniquem entre si, transfiram arquivos, enviem e-mails e realizem outras operações que dependem da conectividade em rede.

Importa destacar que o conhecimento em serviços de rede é essencial a qualquer profissional trabalhe com com o sistema Linux, já que a utilização adequada destas ferramentas é fundamental para garantir a segurança, a eficiência e disponibilidade da rede e serviços oferecidos

Capítulo 1

Serviços de rede

Serviços de rede são programas que executam funções específicas na rede, como permitir a transferência de arquivos, envio de e-mails ou navegação na web. Alguns dos principais serviços de rede do Linux são DNS, DHCP, FTP, HTTP, SSH, SMTP e NTP.

Para iniciar e parar serviços de rede em Linux utilizam-se os comandos : **systemctl**, **service** e **chkconfig**.

Por exemplo, para iniciar o serviço SSH, executa-se o comando "systemctl start sshd"e para parar o serviço, executa-se o comando "systemctl stop sshd".

1.1 etc/rc.d/init.d/

A diretoria /etc/rc.d/init.d/ contém os scripts de inicialização e paragem de serviços de sistema executados durante o processo de boot ou encerramento do sistema.

Por exemplo, o script de inicialização do serviço Apache (httpd) está localizado em /etc/rc.d/init.d/httpd.

Os scripts em /etc/rc.d/init.d/ são geridos pelos utilitários de gestão de serviços como o systemd ou o SysV init. Estes utilitários podem ser usados para iniciar, parar ou reiniciar manualmente os serviços. Podem também controlar o inicio automático de determinado serviço durante o boot do sistema.

1.1.1 Exercicio prático:

Suponha que se deseja iniciar o serviço Apache através do script chamado "httpd"localizado em /etc/rc.d/init.d/, para iniciar o Apache teria de digitar o comando:

```
/etc/rc.d/init.d/httpd start
```

Este comando irá executar o script de inicialização do Apache localizado em /etc/rc.d/init.d/ com o parâmetro "start", que inicia o serviço Apache.

Agora veirificamos que o serviço foi iniciado corretamente através do comando,

```
systemctl status httpd
```

1.2 Lista de portas e serviços no

A pasta /etc/services contém uma lista de todos os serviços de rede disponíveis no sistema, juntamente com as portas correspondentes que cada serviço em execusão no sistema. Para visualizar a lista de serviços e portas em /etc/services, abra o arquivo com um editor de texto, como por exemplo o vi ou o nano. Poderá pesquisar por um serviço específico usando o comando "grep".

Por exemplo: "grep ssh /etc/services"mostra informações sobre o serviço SSH na lista.

A pasta /etc/services também pode ser utilizada para configurar serviços de rede no Linux, definindo portas personalizadas ou restringindo o acesso a determinados serviços na rede.

1.2.1 Exercício prático:

Para este exercício prático, identificaremos a porta padrão de determinado serviço de rede, por exemplo o ssh, e verificamos se está em execução.

Abra um terminal no Linux e escreva comando para abrir o arquivo /etc/services no editor nano:

```
sudo nano /etc/services
```

Procuramos pelo nome do serviço “ssh”:

```
ssh 22/tcp                      # Secure Shell Login
```

Conhecida aporta padrão executamos o comando netstat para verificar se o serviço está em executação:

```
sudo netstat -tlnp | grep 22
```

Este comando lista todas as conexões de rede em execução filtrando-as pelo número da porta 22

```
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1077/sshd
```

A coluna "0.0.0.0:22"indica que o serviço SSH está em execução na porta 22, e em todas as interfaces de rede.

1.3 Encerramento de um serviço ou porta

Para encerrar um serviço ou porta podem-se usam-se os comandos "kill"ou "systemctl stop".

1.3.1 Usando o kill

Identifique o ID do processo (PID) do serviço a encerrar através do comandos ps aux | grep <nome do serviço> ou "systemctl status <nome do serviço>

Use o comando "kill <PID>"para enviar o sinal para encerramento do processo do serviço

1.3.2 Exercício prático:

Para encerrar o serviço Apache com o comando kill executamos os passos:

```
ps aux | grep httpd
```

O resultado deste comando mostrará o PID do processo do serviço Apache. Suponhamos que o PID seria 1234, neste caso para encerraríamos o serviço com a seguinte instrução:

```
kill 1234
```

1.3.3 Exercício prático:

Para encerrar um serviço usando o comando systemctl stop, seriam os seguintes passos: Identificar o nome do serviço a encerrar. Utilizar o comando "systemctl stop <nome do serviço>"para interromper o serviço. Para encerrar o serviço Apache utilizar-se-ia o seguinte comando

```
systemctl stop httpd
```

Importante notar que o encerramento de um serviço poderá implicar a interrupção do funcionamento do sistema ou de outros serviços que dependam do serviço encerrado.

1.4 XINET.

O **xinetd (extended Internet daemon)** é um daemon que gere outros serviços de rede em um sistema Linux. É projetado para ser um super-servidor que pode iniciar vários servidores menores em resposta a solicitações de clientes. O xinetd é responsável por iniciar e parar os serviços de rede quando necessário, o que ajuda a economizar recursos de sistema e torna mais fácil gerir os serviços de rede num servidor.

Este daemon é configurado por meio de arquivos localizados em /etc/xinetd.d/. Cada arquivo de configuração corresponde a um serviço de rede específico, como FTP, Telnet, SSH, etc.

Os arquivos de configuração do xinetd têm uma sintaxe específica que especifica as opções de configuração para determinado serviço de rede.

Por exemplo, a configuração para o serviço Telnet seria:

```
# default: on
# description: The telnet server serves telnet sessions; it uses
# unencrypted username/password pairs for authentication.
service telnet
{
    socket_type     = stream
    wait            = no
    user            = root
    server          = /usr/sbin/in.telnetd
    log_on_failure  += USERID
}
```

Neste exemplo, o arquivo de configuração especifica que o serviço Telnet deve usar o tipo de socket "stream", não deve esperar por conexões adicionais antes de iniciar um novo processo, deve ser executado como root e deve usar o programa "in.telnetd"como servidor. Além disso, especifica que falhas de login devem ser registadas no log do sistema.

Para iniciar ou parar o daemon xinetd, utiliza-se o comando systemctl :

systemctl start xinetd

1.4.1 Exercício prático:

Para este exercício, vamos configurar um serviço de HTTP usando o xinetd no servidor Linux.

Verificar se o Apache está instalado:

sudo apt-get install apache2

Verifique o estado :

sudo systemctl status apache2

Edite o arquivo de configuração do xinetd para adicionar o serviço HTTP:

sudo nano /etc/xinetd.d/http

Adicione as seguintes linhas ao arquivo de configuração:

```
service http
{
    disable         = no
    flags           = REUSE
    socket_type     = stream
    protocol        = tcp
    user            = www-data
    wait            = no
    server          = /usr/sbin/apache2
    server\_args     = -DFOREGROUND
    log_on_failure  += USERID
```

```
}
```

Salve e reinicie o xinetd:

sudo systemctl restart xinetd

Verifique o funcionamento do Apache:
curl http://localhost

Para desativar o serviço HTTP, desative-o no arquivo de configuração do xinetd, alterando a linha "disable = yes":

```
service http
{
    disable         = yes
    flags           = REUSE
    socket_type     = stream
    protocol        = tcp
    user            = www-data
    wait            = no
    server          = /usr/sbin/apache2
    server_args     = -DFOREGROUND
    log_on_failure  += USERID
}
```

1.5 Arquivo /etc/xinetd.conf

O **arquivo /etc/xinetd.conf** é o arquivo principal de configuração xinetd. Usado para a configuração das as opções globais do xinetd, por exemplo o número máximo de conexões simultâneas permitidas e tempo limite para as conexões inativas. Este arquivo é lido pelo xinetd durante o início ou renicio do daemon.

Algumas das opções de configuração do /etc/xinetd.conf:

defaults: esta opção é usada para definir opções globais para todos os serviços geridos pelo xinetd

log_type: esta opção é usada para definir o nível de detalhe dos logs gerados pelo xinetd.

access_times: esta opção é usada para definir o horário de funcionamento dos serviços geridos pelo xinetd

umask: esta opção é usada para definir a permissão padrão para os arquivos criados pelos serviços geridos pelo xinetd.

Os serviços geridos pelo xinetd possuem um arquivo de configuração na pasta /etc/xinetd.d/.

1.5.1 Exercício prático

Para o exercício, vamos supor que queremos aumentar o número máximo de conexões simultâneas permitidas para os serviços geridos pelo xinetd.

Abra o ficheiro /etc/xinetd.conf e altere a opção defaults para definir o número máximo de conexões máximas em simultâneo igual a 100 para todos os serviçõe geridos pelo xinetd.

Na secção defaults adicione a opção “instances = 100”.

Se não existir , adicione-a à secção superior do arquivo. Reinicie o serviço xinetd

```
systemctl restart xinetd
```

1.6 TCPWrappers

TCP Wrappers é uma ferramenta de segurança de rede de sistemas Unix-like que permite controlar o acesso de rede de servidores e clientes. Funciona como uma camada intermédia entre serviços de rede e conexões de entrada, permitindo que as conexões sejam filtradas com base em endereços IP, nomes de hosts ou outras características.

É necessário adicionar uma linha ao arquivo de configuração do serviço (/etc/xinetd.d/ ou /etc/inetd.d/) para especificar o uso do TCP Wrappers

A habilitação do TCP Wrappers para o serviço SSH seria por exemplo adicionar uma linha ao arquivo de configuração do SSH :

```
tcp\_wrappers = yes
```

O TCP Wrappers utiliza a pasta /etc/xinetd.d para configurar os serviços que deseja gerir e arquivos hosts.allow e hosts.deny em conjunto para permitir ou negar o acesso de hosts a Estes serviços.

1.6.1 /etc/hosts.allow

Este arquivo contém a lista de serviços de rede e hosts com permissão para aceder aos serviços. Se um host não estiver listado no arquivo /etc/hosts.allow para determinado serviço, a conexão é rejeitada.

1.6.2 /etc/hosts.deny

Este arquivo contém uma lista de serviços de rede e hosts que estão proibidos de aceder aos serviços. Se um host estiver listado no arquivo /etc/hosts.deny para um determinado serviço, a conexão será rejeitada independentemente do que estiver listado no arquivo /etc/hosts.allow.

1.6.3 Exercício prático

Utilização do TCP Wrappers , xinetd e arquivos hosts.allow e hosts.deny no controlo de acesso ao serviço SSH :

Certificar se o xinetd está instalado e em execução.

Criamos a seguir o arquivo de configuração do serviço SSH em /etc/xinetd.d/ssh

```
# default: on
# description: SSH service
service ssh
{
    flags           = REUSE
    socket_type     = stream
    wait            = no
    user            = root
    server          = /usr/sbin/sshd
    log_on_failure  += USERID
    disable         = no
}
```

Adiciona-se a linha no fim do arquivo /etc/ssh/sshd_config para permitir o uso do TCP Wrappers para o serviço SSH

```
# enable TCP Wrappers
tcp_wrappers = yes
```

```
Ao arquivo /etc/hosts.allow e adicionamos para permitir conexões SSH apenas a hosts na rede 192.168.0.0
```

```
sshd: 192.168.0.0/24
```

Ao arquivo /etc/hosts.deny e adicionamos a seguinte linha para negar o acesso SSH a qualquer outro host

```
sshd: ALL
```

Capítulo 2

NIS

O **Network Information Service** (NIS) é um serviço de informação de rede permite aos utilizadores numa rede ter acesso aos arquivos e recursos noutras computadores.

É um serviço de diretório centralizado em ambientes UNIX e Linux de gestão de informações de conta de utilizador e grupo.

O servidor NIS armazena em servidor central, , informações de contas de utilizador e grupos, assim como arquivos de configuração do sistema /etc/password, /etc/group e /etc/hosts. Permite que sistemas compartilhem as mesmas informações de conta de utilizador e grupo, o que simplifica a administração e melhora a segurança, garantindo informações de conta consistentes e atualizadas em todos os sistemas.

Na autenticação, o cliente envia ao servidor NIS o seu nome de utilizador e palavra-chave para que seja verificado. O servidor NIS fornece o serviço centralizado na gestão de informações de contas de utilizador e grupos, e o cliente utiliza as informações para se autenticar no servidor.

O NIS é uma tecnologia muito utilizada, mas possui alguns inconvenientes, as palavras chave são transmitidas em texto simples, e pode ter um baixo desempenho na gestão de redes grandes e com muitos utilizadores Por estes motivos, atualmente as organizações e fazem a transição para serviços como LDAP ou Active Directory, mais seguros e com melhor desempenho.

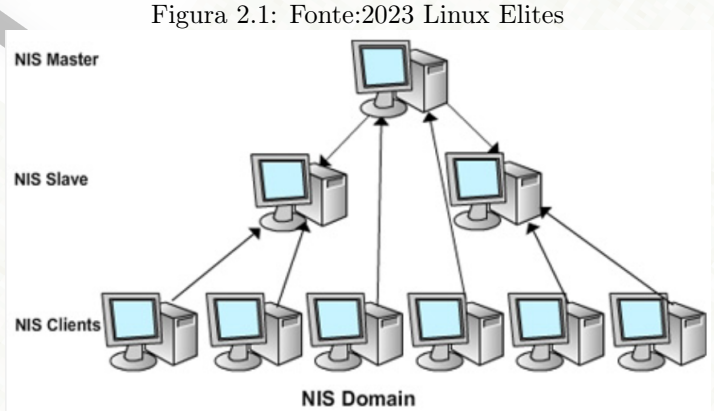
2.1 Tipos de servidor NIS

Os tipos de servidor NIS são:

Servidor Mestre : onde são armazenados todos os ficheiros

Servidor Escravo (secundário) : Usado para a gestão e armazenamento e útil em caso de falha do servidor mestre .Pode ter vários servidores secundários Nis se for necessário.

Figura 2.1: Fonte:2023 Linux Elites



2.1.1 Exercícios práticos

1. Questões:

1. O que significa NIS?
2. Qual o propósito do servidor NIS?
3. Que tipos de informações são armazenadas num servidor NIS?
4. Quais as vantagens em usar um servidor NIS?
5. Quais são as limitações na utilização de um servidor NIS?
6. Como se autentica o cliente NIS num servidor NIS?
7. Qual é a diferença entre cliente NIS e servidor NIS?
8. O servidor NIS pode gerir contas de clientes em sistemas Windows?

2. Instalação do NIS server: Siga os passos do documento específico fornecido pelo formador.

Capítulo 3

DHCP

3.1 Conceitos

O **DHCP (Dynamic Host Configuration Protocol)** é um protocolo de rede utilizado para atribuir dinamicamente endereços IP e outras informações de configuração aos dispositivos de uma rede. Os dispositivos obtém automaticamente as informações de configuração necessárias para se conectarem à rede, como o endereço IP, a máscara de rede, o gateway padrão e os servidores DNS.

O DHCP simplifica a administração da rede, evita erros de configuração, evita os conflitos de endereços, permitindo reutilização de endereços IP libertados pelos dispositivos que entretanto deixaram de usar a rede.

3.2 Iniciação do servidor DHCP

Para iniciar o servidor DHCP , é necessário ter instalado o servidor dhcpd no sistema operacional. Depois disso, o serviço é iniciado através do gestor de serviços, por exemplo o systemd em Linux.

Convém antes de iniciar o serviço, proceder à configuração do dhcpd, através da edição do arquivo localizado em /etc/dhcp/dhcpd.conf, para definir as opções de rede, como faixa de endereços IP disponíveis (range) , duração do aluguer de endereços IP (lease time), opções de DNS e outros parâmetros.

3.3 Descrição dos principais parâmetros - lease time, range, mac address, routers, domain name

Entre os principais parâmetros de configuração do servidor DHCP estão:

Lease Time: tempo de concessão de um endereço IP a determinado dispositivo. Tempos de expiração dos endereços atribuídos a cada dispositivo . Sempre que o tempo expira, os dispositivos tem de voltar a revalidar os endereços. O tempo de concessão pode ser configurado em segundos, minutos, horas ou dias.

Range●: faixa de endereços IP reservada para ser atribuída automaticamente aos dispositivos da rede. É importante que o range de endereços esteja dentro de uma sub-rede previamente configurada localmente.

MAC Address: endereço físico único do dispositivo. Quando o servidor DHCP atribui um endereço IP pode associa-lo ao endereço MAC do dispositivo, permitindo deste modo que o servidor saiba qual dispositivo está usar determinado endereço IP.

Routers: endereço IP do router padrão da rede. Quando o servidor DHCP fornece a configuração de rede a um dispositivo, pode incluir o endereço IP do router/gateway padrão da rede para que o dispositivo possa encaminhar o tráfego para a rede exterior.

Domain Name: nome de domínio DNS local.

3.3.1 Exercício prático:

```
Assinale a resposta que achar mais correta:

O que é o "lease time" no DHCP?
    a) O endereço IP atribuído a um dispositivo
    b) O tempo em que o endereço IP atribuído a um dispositivo será válido
    c) O nome de domínio atribuído a um dispositivo
    d) O endereço MAC do dispositivo

Resposta: b) O tempo em que o endereço IP atribuído a um dispositivo será válido

    Qual é a função do parâmetro "range" no DHCP?
    a) Definir o tempo de vida de um endereço IP atribuído a um dispositivo
    b) Definir o endereço IP do roteador padrão
    c) Definir o intervalo de endereços IP disponíveis para atribuição
    d) Definir o nome de domínio atribuído a um dispositivo

Resposta: c) Definir o intervalo de endereços IP disponíveis para atribuição

    O que é o "mac address" no DHCP?
    a) O endereço IP atribuído a um dispositivo
    b) O nome de domínio atribuído a um dispositivo
    c) O endereço físico exclusivo de um dispositivo
    d) O tempo em que o endereço IP atribuído a um dispositivo será válido

Resposta: c) O endereço físico exclusivo de um dispositivo

    Qual é a função do parâmetro "routers" no DHCP?
    a) Definir o tempo de vida de um endereço IP atribuído a um dispositivo
    b) Definir o endereço IP do roteador padrão
    c) Definir o intervalo de endereços IP disponíveis para atribuição
    d) Definir o nome de domínio atribuído a um dispositivo

Resposta: b) Definir o endereço IP do roteador padrão

    O que é o "domain name" no DHCP?
    a) O endereço IP atribuído a um dispositivo
    b) O nome de domínio atribuído a um dispositivo
    c) O endereço físico exclusivo de um dispositivo
    d) O tempo em que o endereço IP atribuído a um dispositivo será válido

Resposta: b) O nome de domínio atribuído a um dispositivo
```

3.4 Name servers

Name servers, também conhecidos como servidores de nomes, são computadores ou dispositivos de rede responsáveis por traduzir nomes de domínio em endereços IP. São Estenciais para o funcionamento da Internet, pois permitem que os utilizadores acedam aos sites e serviços da Internet usando nomes, fáceis de memorizar, em vez de terem de memorizar os respetivos endereços IP.

3.4.1 Arquivo /var/lib/dhcp/dhcpd.

O arquivo /var/lib/dhcp/dhcpd.leases é gerado pelo servidor DHCP para registar informações sobre os endereços IP atribuídos aos clientes que solicitam conexão à rede.

Quando um cliente se conecta e solicita um endereço IP, o servidor DHCP verifica se há um endereço disponível na faixa de endereços definida e, em seguida, atribui um endereço disponível ao cliente, assim como outras informações de configuração, gateway padrão, DNS e outras informações de rede.

O arquivo dhcpd.leases é atualizado sempre que um novo endereço IP é atribuído ou é libertado. Contém informações sobre os clientes conectados, endereço IP, o tempo de concessão (lease time), o endereço MAC

do cliente e outras. Este arquivo é útil aos administradores na monitorização da utilização de endereços IP e planearem, caso seja necessário, a alocação de novos endereços na rede.

Exercício prático:

```
1) O que é o arquivo /var/lib/dhcp/dhcpd.leases e qual a sua função no servidor DHCP?

2) Como é possível visualizar o conteúdo do arquivo /var/lib/dhcp/dhcpd.leases?

3) Quais informações importantes podem ser encontradas no arquivo /var/lib/dhcp/dhcpd.leases?
```

3.5 Configuração do range de uma rede

Para configurar o range de uma rede em um servidor DHCP edita-se o arquivo de configuração /etc/dhcpd.conf Pode-se especificar o intervalo de endereços IP disponíveis para distribuição, definido através dos parâmetros range ou pool.

Por exemplo, para configurar um range IP na rede 192.168.1.0/24, que permita a distribuição de 100 endereços IP, adicionamos as linhas ao arquivo de configuração /etc/dhcpd.conf:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.100 192.168.1.199;
}
```

Neste caso, a rede é definida pelo endereço 192.168.1.0, máscara de sub-rede 255.255.255.0 e a range de endereços IP disponíveis para distribuição começa em 192.168.1.100 e termina em 192.168.1.199.

3.6 Definição de informações para a rede TCP

Definição de informações de uma rede TCP envolve a atribuição de endereços IP e outras informações de rede necessárias para que os dispositivos se comuniquem entre si.

Envolve a atribuição de endereços IP, máscaras de sub-rede, gateways padrão, servidores DNS e informações adicionais de rede a cada dispositivo individualmente.

3.6.1 Exercício prático:

```
Suponha que está a configurar uma pequena rede TCP de uma sala de formação com 10 computadores.

Para começar a definir as informações da rede TCP, siga estes passos:

Intervalo de endereços IP: Decida qual intervalo de endereços IP deseja para a sua rede.
Por exemplo, o intervalo 192.168.100.1 a 192.168.1.200.

Gateway padrão: O gateway padrão é o endereço IP do router ou firewall que que
 estabelece a conexão com a rede exterior.
Por exemplo,  defina o endereço IP 192.168.1.1 como  gateway padrão.

Servidor DNS: Determine qual será o servidor DNS usado pela rede.
Por exemplo, defina o servidor DNS do seu provedor de Internet , por exemplo
 8.8.8.8, 8.8.4.4
Servidor DHCP: Decida se pretende utilizar um servidor DHCP para atribuir automaticamente endereços IP

Se sim, defina o intervalo de endereços IP que a ser atribuídos pelo servidor DHCP,
 atribua e configure o tempo de concessão (lease time)
para controlar o tempo cada dispositivo mantém seu endereço IP atribuído.
```

```
Por exemplo, defina os endereços IP de 192.168.1.100 a 192.168.1.200 e  tempo de
 concessão de 7 dias.
Nome da rede (SSID) e palavra-chave do Wi-Fi:
Por exemplo, o SSID como "formacao" e a senha como "fomacao#2022".
No servidor DHCP, teria de abrir o ficheiro de configuração "/etc/dhcp/dhcpd.conf"
 e adicionar as linhas

subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.200;
    option routers 192.168.1.1;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
    default-lease-time 86400;
    max-lease-time 604800;
}
```

Em que :
subnet: Define o endereço IP da sub-rede e a máscara de rede correspondente.

range: Define o intervalo de endereços IP disponíveis para atribuição pelo servidor DHCP.
option routers: Define o endereço IP do gateway padrão para a rede.

option domain-name-servers: Define os servidores DNS que os clientes devem usar para resolução de nomes.

default-lease-time: Define o tempo de concessão padrão para um endereço IP atribuído pelo servidor DHCP.

max-lease-time: Define o tempo máximo de concessão para um endereço IP atribuído pelo servidor DHCP.

3.7 Definição de IP e informações para uma máquina específica na rede através de seu endereço físico

Para definir um endereço IP específico de uma máquina usando seu endereço físico, é necessário indicar o endereço MAC dessa máquina no servidor DHCP através de uma reserva DHCP. Também conhecida como reserva de endereço IP.

Dessa forma, sempre que a máquina com o endereço MAC solicitar um endereço IP ao servidor DHCP, é automaticamente atribuído o endereço IP 192.168.1.10, garantindo que a máquina tenha sempre o mesmo endereço IP mesmo que outros dispositivos solicitem os seus endereços IP dinamicamente.

Por exemplo, para criar uma reserva de endereço IP para uma máquina com endereço MAC 00:11:22:33:44:55 e endereço IP 192.168.1.10 no servidor DHCP, teria de adicionar a seguinte ao ao arquivo de configuração do servidor:

```
host minha_maquina {
  hardware ethernet 00:11:22:33:44:55;
  fixed-address 192.168.1.10;
}
```

Neste exemplo, sempre que a máquina com endereço MAC 00:11:22:33:44:55 solicitar um endereço IP ao servidor DHCP, será atribuído o endereço IP 192.168.1.10.

3.8 Coexistência de mais de um servidor DHCP na rede

A coexistência de mais de um servidor DHCP na rede pode ser fonte de conflitos de IP e outras configurações, pois cada servidor poderá durante o processo atribuir diferentes valores de rede para para os mesmos parâmetros e mesmos clientes.

Para evitar conflitos, é importante que apenas um servidor DHCP esteja ativo na rede em determinado momento. Se houver mais de um servidor DHCP, é preciso garantir que eles estejam configurados de forma

adequada e coordenada, a evitando assim que os clientes recebam informações conflituantes.

Uma solução para evitar conflitos é a configuração de servidores DHCP para diferentes sub-redes, garantindo que apenas um servidor possa atribuir IPs na sua sub-rede. Outra solução é configurar cada servidor DHCP para atribuir IPs em faixas diferentes dentro da mesma sub-rede, com um intervalo de endereços diferente.

3.8.1 Exercício prático:

```
O que significa a coexistência de mais de um servidor DHCP na rede?
a) Significa que há vários routers na rede.
b) Significa que há vários servidores responsáveis pela atribuição de endereços IP.
c) Significa que há vários servidores de nomes na rede.
d) Significa que há vários servidores de arquivos na rede.

Qual é o principal problema da coexistência de mais de um servidor DHCP na rede?
a) A perda de informações de configuração.
b) A sobreposição de endereços IP.
c) A falta de segurança na rede.
d) A falta de atualização dos sistemas operacionais.

Qual é a solução recomendada para evitar conflitos entre servidores DHCP na rede?
a) Utilizar apenas um servidor DHCP na rede.
b) Configurar cada servidor DHCP com faixas de endereços IP diferentes.
c) Configurar cada servidor DHCP com o mesmo endereço IP.
d) Configurar cada servidor DHCP com o mesmo nome de domínio.

Respostas:

b) Significa que há vários servidores responsáveis pela atribuição de endereços IP.
b) A sobreposição de endereços IP.
b) Configurar cada servidor DHCP com faixas de endereços IP diferentes.
```


3.9 Configuração de um cliente para o acesso à rede DHCP

A configuração de um cliente para o acesso à rede via DHCP geralmente implica que placa de rede do cliente esteja configurada para receber um endereço IP automaticamente.

Para que o cliente possa aceder à rede via DHCP é necessário seguir os seguintes passos:

Configure a placa de rede para o protocolo DHCP.

Reinicie a interface de rede do cliente para que ele possa obter um endereço IP via DHCP. Poderá ser usado o comando ipconfig /release e, em seguida, ipconfig /renew em sistemas Windows ou sudo dhclient -r e, em seguida, sudo dhclient em sistemas Linux.

Verifique se o cliente tem um IP válido. Isto pode ser feito usando o comando ipconfig em sistemas Windows ou ifconfig em sistemas Linux. Certifique-se de que o endereço IP do cliente esteja dentro do range configurado no servidor DHCP.

Certifique as informações endereço do gateway padrão, servidor DNS e o domínio DNS atribuídos.

3.10 Comando pump

O **comando pump** é um cliente de DHCP disponível para sistemas Linux e Unix-like. É utilizado para obtenção dinâmica de um endereço IP a partir de um servidor DHCP da rede.

O pump pode ser executado no terminal e a sintaxe é:

```
pump [interface]
```

Em que [interface] é o nome da interface de rede que deseja configurar com o endereço IP atribuído pelo servidor DHCP. Se a interface for enp0s3 seria:

```
pump enp0s3
```

As informações obtidas do servidor DHCP são armazenadas em arquivos de configuração na pasta /var/lib/dhclient/.

Importante notar que o pump é já uma ferramenta obsoleta, foi substituído pelo dhclient em muitas das distribuições Linux. O dhclient é uma ferramenta mais moderna e flexível para configuração de cliente DHCP em sistemas Linux e Unix-like.

3.11 DHCP do Linux

O Linux é um sistema que suporta a implementação de um servidor DHCP por meio de vários pacotes de software, como o ISC DHCP e o Dnsmasq. O ISC DHCP é um pacote de software muito utilizado para implementar um servidor DHCP em sistemas operacionais Linux. O Dnsmasq é uma ferramenta de servidor DNS e DHCP leve e fácil de configurar que também é comummente usada em sistemas operacionais Linux.

3.11.1 Exercício prático:

Instalar e configurar o ISC – DHCP:

Abra um terminal (CTRL+ALT + T) e execute o comando abaixo para instalar o servidor DHCP:

```
sudo apt-get update

sudo apt-get install isc-dhcp-server
```

Edite o arquivo /etc/default/isc-dhcp-server e defina a interface de rede que o servidor DHCP utilizará para atribuir endereços IP. Pode editar o arquivo usando o editor nano:

```
sudo nano /etc/default/isc-dhcp-server
```

Defina a interface de rede, se a interface de rede for enp0s3 , adicione a seguinte linha ao arquivo:

```
INTERFACESv4="eth0"
```

Edite o arquivo /etc/dhcp/dhcpd.conf com as configurações para sua rede:

```
sudo nano /etc/dhcp/dhcpd.conf
```

Adicione as configurações de rede ao arquivo. Por exemplo, para atribuir endereços IP no intervalo 192.168.0.10 a 192.168.0.20, adicione as seguintes linhas:

```
subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.10 192.168.0.20;
}
```

Salve e feche o arquivo.

Reinicie o servidor DHCP:

```
sudo systemctl restart isc-dhcp-server

Verifique o estado do servidor DHCP:

sudo systemctl status isc-dhcp-server
```

Poderá a partir deste momento configurar os clientes para se conectarem à rede via DHCP, que fornecerá um endereço IP e outras informações de rede. Realize o teste com um cliente Windows e um cliente Linux.

Capítulo 4

DNS

O **Sistema de Nomes de Domínio** , na nomenclatura inglesa Domain Name System (DNS), é um sistema de nomes hierárquico e distribuído que tem como objetivo associar nomes de domínio a endereços IP . Permite que um utilizador aceda aos servidores web através de um nomes em vez de um endereços IP numéricos, processo denominado por resolução de nome.
Por padrão, o DNS usa o protocolo User Datagram Protocol (UDP) na porta 53 para servir as solicitações e as requisições.

O serviço é normalmente implementado pelo software Berkeley's Internet Name Daemon (BIND) que se encontra geralmente localizado no servidor DNS primário. O servidor DNS secundário é uma espécie de cópia de segurança do servidor DNS primário.

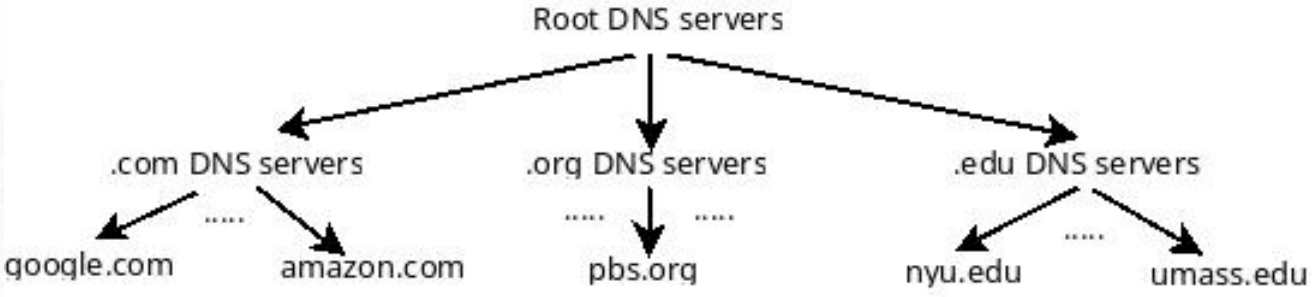
Existem centenas de servidores-raiz DNS (root servers) no mundo todo, agrupados em 13 zonas DNS raiz , dos quais dez estão localizados nos Estados Unidos da América, dois na Europa e um na Ásia. Para aumentar o número destes servidores foram instaladas réplicas pelo mundo, inclusive no Brasil desde 2003.

4.1 Zona, Domínios e Nós

O DNS usa uma estrutura em árvore, em que cada nó da árvore representa um domínio e seus subdomínios. A raiz da árvore é representada por um ponto ".". Cada domínio é dividido em subdomínios, cada nível é representado por um nome separado por um ponto.

A estrutura básica do DNS é composta por zonas, domínios e nós. Graficamente pode ser vista com uma árvore invertida , em que a raiz é representada por um ponto"." e os domínios representados pelos nós da árvore.

Figura 4.1: DNS



4.2 Servidores Matriz (root servers)

Os servidores Matriz (root servers) são servidores de nomes de domínio (DNS) que armazenam informações sobre servidores que gerem os TLDs (Top Level Domains), .com, .org, .edu, .net, .gov. entre outros. Podem-se registar nos TLD vários domínios .Nos domínios autoritativos encontram-se os servidores DNS de organizações.

Se determinado cliente pretende o endereço do site www.amazon.com .Como primeira aproximação, são executados os seguintes passos:

1. Cliente consulta o servidor DNS root sobre o servidor DNS .com
2. Cliente consulta o servidor DNS .com sobre o servidor DNS amazon.com
3. Cliente consulta o servidor DNS amazon.com para obter o endereço IP de www.amazon.com

4.3 Servidores DNS locais

Cada consulta é realizada ao servidor DNS local. O servidor DNS responde imediatamente às consultas a partir dos dados armazenados na cache DNS. Se o servidor DNS local tiver as informações de resolução de nomes armazenadas em cache, fornecerá uma resposta imediata. Caso contrário, consultará outro servidor DNS para obter as informações necessárias.

4.3.1 Exercício prático:

Cada fornecedor de internet possuí o seu próprio servidor DNS.Para saber o seu faça:
No Linux Ubuntu:

```
ifconfig
```

No windows :

```
ipconfig / all
```

No MacOS :

```
scutil -dns
```

4.4 FAPESP e Internic

A **FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo)** é uma das entidades responsáveis pela gestão do registo de domínios no Brasil. Tem objetivo promover e fomentar o desenvolvimento da pesquisa científica e tecnológica no Estado de São Paulo.

O **Internic (Internet Network Information Center)** é uma organização responsável pela gestão e coordenação dos recursos da Internet a nível global. Fundado em 1992, o Internic é uma parceria entre a National Science Foundation (NSF) e a Network Solutions, Inc., e tem como objetivo principal gerir o registo de domínios genéricos de topo (gTLDs) como .com, .net, .org. Atualmente, a gestão do registo de gTLDs é realizada pela ICANN (Internet Corporation for Assigned Names and Numbers), organização sem fins lucrativos responsável pela coordenação global do sistema de identificadores exclusivos na Internet.

4.5 DNS e replicação de zonas

A replicação de zonas é necessária porque as informações de DNS, de servidores físicos, são armazenadas em servidores DNS lógicos distribuídos por todo o mundo. Estes servidores mantém cópias consistentes das zonas para que consultas de DNS sejam corretas e rápidas.

4.6 BIND (named) - Berkeley Internet Name Domain

O **BIND (Berkeley Internet Name Domain)** é uma implementação do protocolo de Sistema de Nomes de Domínio (DNS). É um software em código aberto teve a sua origem nos anos 1980 na Universidade de Califórnia em Berkeley.

O BIND é dividido em dois principais componentes: o servidor de nomes (named) e a biblioteca de resolução (resolver library). O servidor de nomes (named) é responsável por servir solicitações de resolução de nomes de domínio e é configurado por meio de arquivos de zona. A biblioteca de resolução (resolver library) é usada pelos aplicativos do sistema para resolver nomes de domínio.

O BIND suporta várias configurações, primárias, secundárias e cache-only. Na configuração primária, o servidor de nomes é autoritativo para a zona. Na configuração secundária, o servidor recebe cópias de informações de zona do servidor primário e armazena-as em cache para atendendo a solicitações de resolução de nomes de domínio. Na configuração cache-only armazena em cache informações de resolução de nomes de domínio para consultas futuras.

4.6.1 1.24.1 arquivo /etc/named.conf

O arquivo /etc/named.conf é o arquivo de principal de configuração do servidor de DNS BIND . Contém as informações de configuração básicas , nomes de domínio pelos quais o servidor é responsável, as opções globais de configuração, as configurações de zona, as configurações de encaminhamento e opções avançadas.

O arquivo é dividido em seções, cada uma identificada por um bloco de início e fim delimitado por chaves . As secções incluem a secção options, que contém as opções globais de configuração do servidor, a secção zone, que contém as informações de configuração da zona DNS, e a secção logging, que controla o registo de mensagens de log pelo servidor BIND.

4.6.2 Exercício prático:

Suponha tem um domínio chamado formacao.com e que pretende configurar um servidor DNS para este domínio.

Abra o arquivo /etc/named.conf com o nano:

```
sudo nano /etc/named.conf
```

Adicione as linhas:

```
options {
    directory "/var/named";
    allow-query { any; };
    forwarders { 8.8.8.8; 8.8.4.4; };
    recursion yes;
};
```

Adicione as linhas para configurar a zona formacao.com:

```
zone "formacao.com" {
    type master;
    file "/var/named/formacao.com.zone";
};
```

Guarde e feche o arquivos

Crie o arquivo de zona /var/named/meusite.com.zone com o seguinte conteúdo:

```
$TTL 86400
@       IN      SOA     ns1.formacao.com. root.formacao.com. (
                        2022010101      ; serial
                        3600            ; refresh
                        1800            ; retry
                        604800          ; expire
                        86400           ; minimum
                        )
              IN      NS      ns1.formacao.com.
              IN      A       192.168.0.10
ns1           IN      A       192.168.0.10
```

Reinicie o serviço BIND

```
sudo systemctl restart named
```

4.6.3 Arquivo /var/named/named.ca

O arquivo named.ca é um arquivo de cache que contém os endereços IP dos servidores raiz do DNS (root servers) , responsáveis por fornecer informações sobre as zonas de domínio de nível superior (TLDs) para os servidores de nomes de domínio de nível inferior.

Capítulo 5

LOGS

5.1 Arquivos de log do sistema

Os arquivos de log do sistema são registos detalhados das atividades que ocorrem no sistema operacional. Podem ser úteis na resolução de problemas e diagnóstico de falhas no sistema. No Linux, a maioria dos arquivos de log é armazenada na pasta /var/log.

São arquivos frequentemente verificados para garantir que o sistema continue a funcionar e ao mesmo tempo, para permitir que se possa identificar eventuais falhas de sistema o mais cedo possível.

5.2 Pasta /var/log

Arquivos mais comuns encontrados da pasta /var/log são :

- **auth.log**: Contém informações de log relacionadas à autenticação de utilizadores e processos de autorização.
- **syslog:** Contém informações de log do sistema, incluindo mensagens de erro, avisos e outras informações importantes.
- **kern.log**: Contém informações de log do kernel do sistema, incluindo mensagens de erro, avisos e outras informações importantes relacionadas ao kernel.
- **messages**: Contém mensagens de erro, avisos e outras informações importantes do sistema que não estão incluídas em outros arquivos de log.
- **maillog**: Contém informações de log relacionadas ao servidor de e-mail, incluindo mensagens enviadas e recebidas.
- **secure**: Contém informações de log relacionadas à segurança do sistema, incluindo autenticação de utilizadores e falhas de segurança.
- **cron**: Contém informações de log relacionadas à execução de tarefas cron.
- **dmesg**: Contém informações de log relacionadas ao hardware do sistema, incluindo informações sobre dispositivos conectados e reconhecidos pelo kernel.

5.2.1 Exercício prático

Analisaremos o arquivo de log do sistema "auth.log"para ver quem fez login no sistema,

```
sudo nano /var/log/auth.log
```

Procure por “login”, e analise as linhas que cont-em informação relativas a nome de utilizador e hora de login

Para saber quem está atualmente conectado ao sistema , execute o seguinte comando :

```
who
```

Verá a lista de utilizadores atualmente conectados ao sistema

5.2.2 Exercício

Neste exercício iremos analisar o arquivo de log do sistema "/var/log/kern.log"em busca de eventuais problemas no sistema,

Tal como no exercício anterior, executamos o comando para abrir o arquivo kern.log:

```
sudo nano /var/log/kern.log
```

Procure por por mensagens de kernel. Por exemplo, linhas que contenham as palavras "kernel", "error"ou "warning".

Analise as mensagens de kernel , tente resolver o problema com base nas informações fornecidas no arquivo kern.log.

Ao terminar, salve as alterações no arquivo kern.log e saia do editor de texto.

Arquivo messages

O arquivo /var/log/messages é um arquivo de log do sistema no Linux que regista vários tipos de informações do sistema, informações de inicialização, mensagens de kernel, mensagens do serviço e outros eventos importantes do sistema. Este arquivo é frequentemente usado para depuração de problemas de sistema e verificação do estado do sistema.
Informações que podem ser encontradas no arquivo /var/log/messages,

- Mensagens de inicialização do sistema
- Mensagens de desligamento do sistema
- Informações de rede, como tentativas de conexão e desconexão
- Erros do kernel
- Mensagens de serviços do sistema, como o daemon do sistema de impressão ou servidor web
- Erros de hardware Por exemplo, mensagens em /var/log/messages relacionadas com erros de hardware são:
- Mensagens relacionadas a problemas de disco rígido, como falhas de leitura e gravação de dados, erros de leitura de setor ou falhas no SMART (Self-Monitoring, Analysis and Reporting Technology)
- Mensagens de erro do controlador de dispositivo, como mensagens relacionadas a problemas de driver de dispositivo, problemas de configuração do dispositivo ou problemas de comunicação do dispositivo com o sistema
- Mensagens relacionadas a problemas de memória, como falhas de leitura e gravação de memória, erros de alocação de memória ou problemas com o controlador de memória
- Mensagens relacionadas a problemas de alimentação ou temperatura, como problemas com a ventoinha do sistema, sobre-aquecimento do sistema ou falhas na fonte de alimentação
- Mensagens relacionadas a problemas com periféricos, como falhas do teclado, placa de rede ou outros dispositivos conectados ao sistema

5.2.3 Exercício prático

Procure por mensagens de erro falha (failed) , erro (error) e aviso (warning) no arquivo /var/log/messages, utilizando o comando de pesquisa **grep**

```
sudo grep -E '(error|failed|warning)' /var/log/messages
```

Este comando procura no arquivo /var/log/messages por todas as linhas que contenham as palavras-chave "error", "failed"ou "warning". O parâmetro -E ativa a interpretação de expressões regulares estendidas, que permitem procurar várias palavras-chave usando o operador OR (|). Tenha em atenção que deverá usar o comando acima com privilégios de administrador.

5.3 Syslogd

Syslogd é um daemon executado continuamente em segundo plano no sistema que coleta, processa e armazena mensagens de log geradas pelo sistema e pelos programas em execução no sistema. Mensagens de log podem incluir informações sobre o desempenho do sistema, erros, avisos, tentativas de acesso não autorizadas e muito mais. O syslogd é responsável por gerir os registos do sistema, encaminhando mensagens de log para os arquivos apropriados ou para outros servidores syslogd na rede.
O daemon syslogd é iniciado durante o boot do sistema e é controlado pelo arquivo de configuração /etc/syslog.conf. Este arquivo determina como são manipuladas , filtradas e armazenadas as mensagens de log.

As mensagens de log são geralmente armazenadas em arquivos em /var/log com nomes que correspondem aos diferentes tipos de mensagem. Por exemplo, mensagens de kernel são armazenadas em /var/log/kern.log, mensagens de sistema em /var/log/syslog e mensagens de autenticação em /var/log/auth.log.

O syslogd é também usado em conjunto com outros programas que geram mensagens de log como , servidores web, bases de dados e outros programas personalizados.

5.4 Arquivo syslog

O **arquivo syslog** é um arquivo de log que contém informações importantes sobre eventos do sistema, como mensagens do kernel, log de serviços do sistema e registos de programas em execução.

O arquivo syslog pode ser usado para diagnosticar problemas no sistema e encontrar informações sobre o comportamento dos programas em execução.

O conteúdo do arquivo syslog é formatado em linhas de registo, em que cada linha contem informações sobre um evento específico, data e hora, o nome do host que gerou a mensagem, o nome do programa que gerou a mensagem e a mensagem

5.4.1 Exercício prático

Vamos verificar se o syslogd está ativo no sistema através do comando,

```
systemctl status syslog
```

São exibidas também informações adicionais, como a versão do daemon syslogd instalado e quaisquer erros ou avisos registados.

Outra forma de verificar se o processo syslogd está em execução no sistema seria usar o comando :

ps aux | grep syslogd

Este comando exibe uma lista de todos os processos em execução no sistema que incluem a palavra-chave "syslogd". Se o syslogd estiver em execução, um ou mais processos serão exibidos na saída.

Em sistemas mais modernos, poderá obter uma mensagem de erro "syslog.service could not be found", ao tentar verificar se o sylog daemon está funcionamento. Pode acontecer que o daemon que gere o sistema de log no sistema tenha outro nome. Dependendo da distribuição Linux que usa, o daemon pode ter outra designação, rsyslog, syslog-ng ou outro nome.

N sentido, poderá encontrar serviço que gere o sistema de log no seu sistema através do comando :

```
systemctl list-units -type=service
```

Poderá então, verificar o estado do serviço com o comando:

```
sudo systemctl status <nome_do_serviço>
```

Outros arquivos de log de aplicativos
Além dos arquivos de log do sistema, existem outros arquivos de log de aplicativos específicos que podem ser úteis para depurar problemas ou monitorizar o desempenho do de determinado aplicativo. Alguns exemplos de arquivos de log de aplicativos em sistemas Linux:

Apache: O servidor web Apache mantém arquivos de log em /var/log/apache2/ em distribuições Debian e Ubuntu, ou /var/log/httpd/ em distribuições RHEL e CentOS. Os arquivos de log incluem access.log, que regista cada solicitação HTTP recebida pelo servidor, e error.log, que regista erros e avisos do servidor.

MySQL: O servidor de banco de dados MySQL mantém arquivos de log em /var/log/mysql/ em distribuições Debian e Ubuntu, ou /var/log/mysqld.log em distribuições RHEL e CentOS. Os arquivos de log incluem error.log, que regista erros do servidor, e slow_query.log, que regista consultas lentas.

Postfix: O servidor de email Postfix mantém arquivos de log em /var/log/mail.log em distribuições Debian e Ubuntu, ou /var/log/maillog em distribuições RHEL e CentOS. Os arquivos de log incluem mail.log, que regista o envio e receção de emails e eventuais erros.

SSH: O servidor SSH mantém um arquivo de log em /var/log/secure em distribuições baseadas em RHEL e CentOS, ou /var/log/auth.log em distribuições baseadas em Debian e Ubuntu. O arquivo de log regista tentativas de login, erros de autenticação e outras informações relacionadas com segurança.

5.5 Apache

O **diretoria /var/log/httpd** é usado para armazenar logs de acesso e erros do servidor web Apache. Quando o Apache serve uma página da web, regista informações sobre a solicitação no arquivo de log de acesso. Da mesma forma, se houver um erro ou problema durante o processamento da solicitação, o Apache regista informações detalhadas no arquivo de log de erros.

Os arquivos de log no diretoria/var/log/httpd geralmente são nomeados com base na data em que foram criados, como:

```
 "access_log-2021-01-01\"
```

e

```
"error_\log-2021-01-01\"
```

os podem ser mantidos por um período determinado pelo administrador do sistema antes de serem arquivados ou excluídos.

Os logs de acesso do Apache podem ser usados para monitorizar o tráfego da web, determinar o número de visitantes do site, identificar páginas populares e identificar possíveis problemas de segurança. Já os logs de erro podem ser usados para diagnosticar problemas de configuração do servidor, problemas de permissão de arquivo ou outras falhas no servidor web.

Os logs de acesso e erro do Apache podem ser personalizados pelo administrador do sistema para incluir ou excluir informações específicas, dependendo das necessidades do servidor. Em geral, é uma boa prática a revisão periódica dos logs do Apache para garantir que o servidor esteja a funcionar corretamente e para detetar quaisquer potenciais problemas.

5.6 Sendmail

A **diretoria /var/log/sendmail** contem os logs de envio de e-mails geridos pelo servidor Sendmail. O Sendmail é um dos mais antigos e ainda muito utilizados servidores de e-mail para sistemas Unix e Linux.

Esta diretoria contém arquivos de log que registam todas as atividades de envio de e-mails, como mensagens enviadas e recebidas, erros de entrega, tentativas de spam, conexões de clientes e muito mais.

Os arquivos de log na diretoria /var/log/sendmail são nomeados com base na data em que foram criados, como "sendmail-2021-01-01". Estes arquivos são normalmente mantidos por um período de tempo determinado pelo administrador do sistema antes de serem arquivados ou excluídos.

Os logs de envio de e-mails podem ser usados para ajudar a identificar problemas com o envio ou recebimento de e-mails, bem como para rastrear mensagens específicas.

5.7 Bibliografia

- Granjal, Jorge."Gestão de Sistemas e Redes em Linux ", 3.ª ed. FCA, 2013

5.8 Webgrafia

- https://www.inetdaemon.com/tutorials/networking/index.shtml "InetDaemon.COM", consultado em 2023
- https://bellard.org/jslinux/, "Run Linux in your browser", JSLinux, Bellard F., consultado em 2023
- https://pt.wikipedia.org/wiki/NIS, "Wikipédia NIS", consultado em 2023
- http://uw714doc.xinuos.com/en/NET_nis/nisC.mach_types.html,"NIS Domain", The SCO Group, consultado em 2023
- https://paginas.fe.up.pt/ mgi97018/, Remualdo P. , Silva L, consultado em 2023
- https://igsf.webnode.pt/ufcd-0839/, "Linux Serviços de Redes" , Faria I., consultado em 2023