IMD0043 – Redes de Computadores
Prof. Silvio Costa Sampaio

Relatório referente ao trabalho de instalação e configurações de serviços da camada de aplicação (DNS, FTP, Correio Eletrônico).

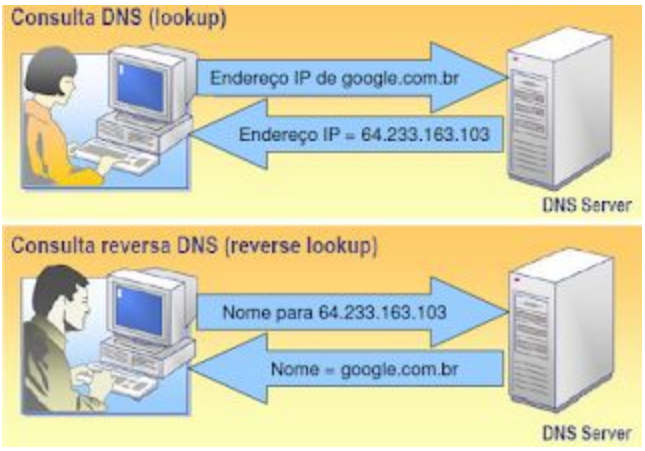
Eucharlis Vieira Duarte
Ewerton Leandro de Sousa
Paulo Victor dos Santos Araújo

A proposta do trabalho é criar um servidor de DNS, WEB/SSL, WEBMAIL, FTP e SSH na mesmo ambiente virtual, onde decidimos usar o sistema operacional Lubunto na versão 16.04 em uma máquina virtual do Virtual Box. A seguir discursamos sobre o conceito de cada serviço e como fazer sua instalação no ambiente citado.

Domain Name System - DNS

O Sistema de Nomes de Domínio, mais conhecido pela nomenclatura em Inglês Domain Name System (DNS), é um sistema hierárquico e distribuído de gestão de nomes para computadores, serviços ou qualquer máquina conectada à Internet ou a uma rede privada. Faz a associação entre várias informações atribuídas a nomes de domínios e cada entidade participante. A sua utilização mais convencional associa nomes de domínios mais facilmente memorizáveis a endereços IP numéricos, necessários à localização e identificação de serviços e dispositivos, processo esse denominado por: resolução de nome.

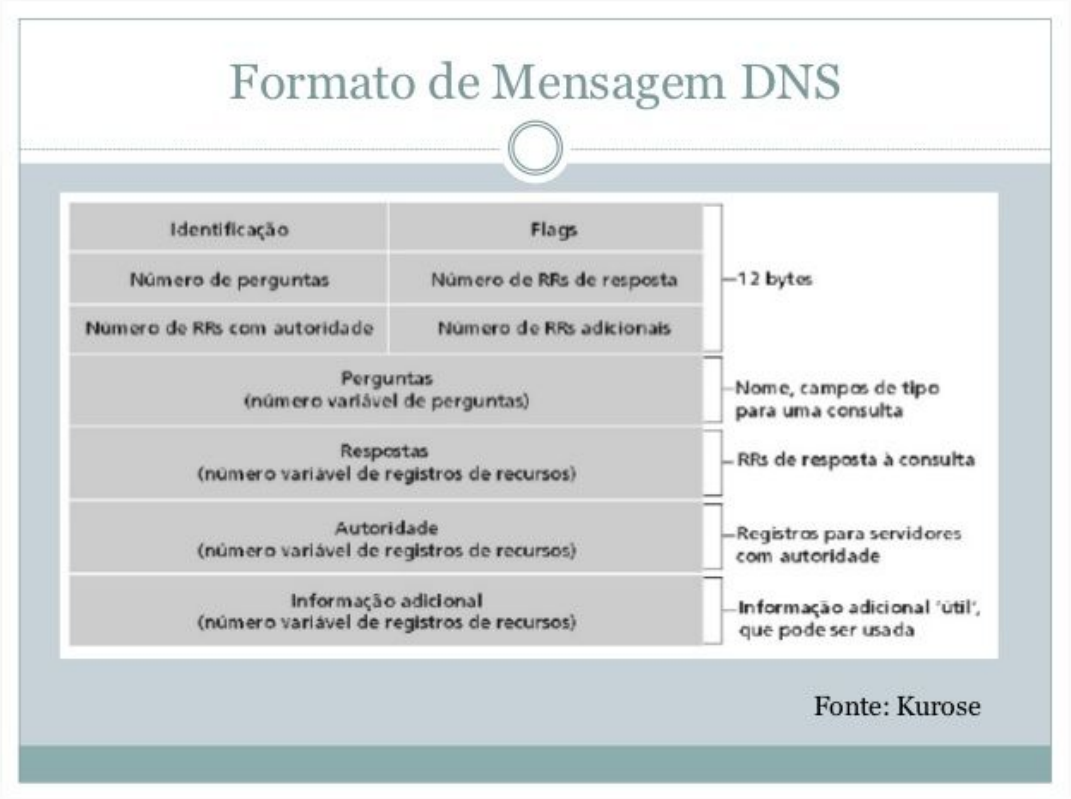
O DNS apresenta uma arquitetura cliente/servidor, podendo envolver vários servidores DNS na resposta a uma única consulta. O servidor DNS resolve nomes para os endereços IP e de endereços IP para os nomes respectivos, permitindo a localização de hosts num determinado domínio.



O DNS assim como alguns outros serviços funcionam em ambos os protocolos da camada de transporte tanto o TCP como o UDP. O TCP é um protocolo orientado a conexão e requer dados sejam consistentes no destino e UDP é um protocolo sem conexão e não requer dados sejam consistentes ou não é necessário uma conexão seja estabelecida com o host para consistência de dados.

DNS usa TCP para a transferência de zona e UDP para consultas de nome tanto regular (primário) ou inversa. UDP pode ser usado para trocar informações de pequenas enquanto TCP deve ser usada para trocar informações maiores que 512 bytes. Se um cliente não obtiver

resposta do DNS que ele deve transmitir novamente os dados usando TCP após 3-5 segundos do intervalo.



Esse formato possui um cabeçalho de tamanho fixo (12 bytes) e uma área de dados variável. Os principais campos são: identificação (usado para numerar a mensagem DNS), parâmetros (informam o tipo da mensagem, isto é, se é uma pergunta ou outro). Nas respostas, constam o nome do domínio, o tipo de dado da resposta, a classe do dado da resposta, o tempo de vida, os dados em si (o endereço IP solicitado) e assim por diante.
Vale ressaltar que o DNS é um protocolo que atua na camada de aplicação no modelo TCP/IP. Pedidos DNS são repassados à camada de Transporte através da porta 53 e usa-se o protocolo UDP para estes pedidos.

Soluções de DNS
Foi pesquisado algumas opções de servidor DNS disponível no mercado:

- Bind
- djbDNS
- Microsoft DNS
- MaraDNS

Tabela comparativa entre os servidor de DNS disponíveis no mercado.

Características x Servidor	BIND	djbDNS	Microsoft DNS	MaraDNS
Criador	Internet Systems Consortium	Daniel J. Bernstein	Microsoft Corporation	Sam Trenholme
Documentação/Site	www.isc.org	http://cr.yp.to	www.microsoft.com	www.maradns.org
Custo	Free	Free	MSRP $999	Free
OpenSource	Sim	Não	Não	Sim
Tipo de Licença	BSD	License-free software	Comercial	BSD
Interface	CLI	CLI	CLI e GUI [0]	CLI
Facilidade Administração	Difícil	Média [5]	Fácil	Fácil
Tamanho Instalador	4Mb [9]	200Kb	2Mb	1.2Mb [9]
Suporte/Atualização	Alta	Baixa	Alta	Alta
Portabilidade	Alta (Mac, 'NIX, Windows...)	Baixa (Unix Like)	Baixa (apenas Windows)	Alta (idem)
Autoritativo	Sim	Sim [1]	Sim	Sim
Pesquisa Recursiva	Sim	Sim [1]	Sim	Sim
Modo Slave	Sim	Parcial [2]	Sim	Parcial [10]
Caching	Sim	Sim	Sim	Sim
DNSSec	Sim	Não	Parcial [3]	Não
TSIG	Sim	Não	Sim	Não
Suporte IPV6	Sim	Sim	Sim [4]	Parcial
WildCard	Sim	Sim	Não	Sim
Suporte a Views	Sim	Sim	Não	Não
Segurança	Média	Alta [6]	Baixa	Alta
Rotação - Round-Robin	Sim	Sim	Sim	Sim
Multi-Threading/Processor	Sim [7]	Sim [7]	Sim [7]	Sim [7]
Processamento/Memória	Médio [8]	Baixo [8]	Alto [8]	Baixíssimo [11]
Performance Cache/Queries	Boa	Ótima	Boa	Excelente [12]
Sender Policy Framework	Sim	Sim	Sim	Sim [14]
Suporte a Split DNS	Sim	Sim	Sim	Sim
Transferência Incremental	Sim	Sim	Sim	Parcial [13]
Atualização Dinâmica	Sim	Sim	Sim	Sim

Tabela 01 - Distribuição de recursos X aplicação (servidor)

Devido a vasta documentação disponível na internet e a escolha do sistema operacional ter sido um Linux, distribuição Lubuntu, foi escolhido o Bind versão 9.

Configuração do Bind versão 9

Para a instalação do Bind9 foi utilizado o gerenciador de pacote padrão do Debian e também disponível nas distribuições baseada em Debian como o Lubuntu.

$sudo apt install bind9

Após a instalação foi iniciado a configuração do Bind9 pela criação das zonas de domínio regular e reversa.

Arquivo /etc/bind/named.conf.default-zones

```
zone “teobaldo.net” {
  type master;
  file /etc/bind/db.teobaldo.net;
}

zone “2.0.10.in-addr.arpa” {
  type master;
  file  /etc/bind/db.teobaldo.net.rev;
}
```

Configuração de dominio

- DOMAIN.NAME. - O nome do domínio ao qual o registro SOA pertence. Observe o ponto final (.). Isso significa que nenhum sufixo deve ser anexado ao nome.
- IN - A classe do registro DNS. IN significa "Internet".
- SOA - O tipo de registro DNS, o Start of Authority neste exemplo.
- Hostname.Domain.Name. - O "campo de origem" precisa conter o nome do host do servidor de nomes principal dessa zona, o host no qual os dados autoritativos residem.
- Mailbox.Domain.Name. - O email do responsável pelo (serviço de nome) deste domínio. Para converter esse campo em um endereço de e-mail utilizável, substitua o primeiro ponto (.) por um @ (arroba).
- Serial number - O número de série da versão atual do banco de dados DNS desse domínio. O número de série é o meio pelo qual outros servidores de nomes percebem que seu banco de dados foi atualizado. Este número de série começa em 1 e deve ser um número inteiro crescente monotonicamente.
- Refresh - Diz ao servidor de nomes secundário com que frequência pesquisar o servidor de nomes principal e com que frequência verificar uma alteração do número de série. Esse intervalo afeta quanto tempo leva para as alterações de DNS feitas no servidor de nome principal se propagarem.
- Retry - O intervalo por segundo no qual o servidor de nome secundário tenta se reconectar ao servidor de nome principal, caso ele falhe ao se conectar no intervalo de atualização.
- Expire - O número de segundos após o qual um servidor de nomes secundário precisa "expirar" os dados do servidor de nomes principal, se ele não conseguir se reconectar ao servidor de nomes principal.
- TTL - O valor padrão que se aplica a todos os registros no banco de dados DNS em um servidor de nomes. Cada registro de recurso DNS pode ter um valor TTL configurado. O TTL padrão do registro SOA é usado apenas se um registro de recurso específico não tiver um valor explícito configurado. Este valor é fornecido por servidores de nomes oficiais (servidores de nomes primários e secundários para uma zona específica) quando respondem a consultas DNS.

```
DOMAIN.NAME.    IN      SOA     Hostname.Domain.Name. Mailbox.Domain.Name. (
                        1       ;    serial number
```

86400 ; refresh in seconds (24 hours)
7200 ; retry in seconds (2 hours)
2592000 ; expire in seconds (30 days)
345600) ; TTL in seconds (4 days)

Tipos de registros

Existem diversos tipos diferentes de registros DNS disponíveis, no entanto, abaixo será mostrado apenas o que significam os mais comuns de serem encontrados durante o gerenciamento de um domínio:

- A – O A, também conhecido por hostname, é o registro central de um DNS, ele vincula um domínio ou subdomínio a um endereço IP direto. Os registros de DNS do tipo A são a razão final da existência do sistema de resolução de nomes, e o tipo de registros que dá nome ao serviço. Este é, hoje, um dos dois tipos de registros que se destinam a fazer o que o nome diz… resolver nomes.
- AAAA – A internet cresceu de tal forma que o número de IPs inicialmente disponíveis está praticamente esgotado e já não permite acompanhar o crescimento da rede. Para ultrapassar este problema foi criado um novo conjunto de endereços, designados com o nome IPv6. Sendo assim, registros AAAA executam a mesma função de A, porém, para um endereço IPv6.
- NS – Name Server (Servidor de Domínio), especifica servidores DNS para o domínio ou subdomínio. Pelo menos, dois registros NS devem ser definidos para cada domínio. Geralmente, um principal e outro secundário.
- CNAME – Significa Canonical NAME. Especifica um apelido (alias) para o hostname (A). É uma forma de redirecionamento.
- MX – Sigla para Mail eXchanger. Aponta o servidor de e-mails. Pode-se especificar mais de um endereço, formando-se assim uma lista em ordem de prioridade para que haja alternativas no caso de algum e-mail não puder ser entregue. Na prática, quando temos um email do tipo email@example.com, devemos perguntar ao servidor de NS do domínio example.com qual é o servidor de email do domínio, isto é, qual o MX do domínio, e em seguida, enviar o email para esse servidor.
- PTR – PoinTeR, aponta o domínio reverso a partir de um endereço IP.
- SOA – Start Of Authority. Indica o responsável por respostas autoritárias a um domínio, ou seja, o responsável pelo domínio. Também indica outras informações úteis como número serial da zona, replicação, etc.
- TXT – Refere-se a TeXT, o qual permite incluir um texto curto em um hostname. Técnica usada para implementar o SPF. Atualmente, uma das informações mais comuns – mas ainda não comum o suficiente – que podemos encontrar neste tipo de registros são as chaves públicas dos servidores de email, que podem ser utilizadas para validar que um email enviado como se tivesse origem num domínio aí tem de facto origem.
- SPF – Sender Policy Framework, é uma tentativa de controle de falsos e-mails. Permite ao administrador de um domínio definir os endereços das máquinas autorizadas a enviar mensagens neste domínio.

- SRV – Abreviação de SeRVice, permite definir localização de serviços disponíveis em um domínio, inclusive seus protocolos e portas. Este tipo de registros servem para indicar que servidores suportam cada tipo de serviço baseado no domínio para o endereçamento, isto é, em que o tipo de conta seja do tipo <utilizador>@<dominio.com>, com exceção do domínio que, sendo deste tipo (o endereçamento do email é do tipo acima), utiliza os domínio do tipo MX.
- Outros– Implementações diversas de serviços implementam frequentemente alterações ao DNS para suportar outros tipos de registos, uns mais comuns do que outros, mas os registos acima são os mais comuns, e os que são suportados pelos RFCs recomendados pelo IEEE, o organismo responsável pela gestão dos RFCs que definem a maioria dos protocolos base da Internet.

Configuração do dominio: teobaldo.net

Arquivo /etc/bind/db.teobaldo.net

```
$TTL 86400 ;(24 horas)
@ IN SOA teobaldo.net. ewerton.teobaldo.net. {
  1    ;Serial
  604800   ;Refresh (7 dias)
  86400    ;Retry   (24 horas)
  2419200 ;Expire (28 dias)
  86400)   ;Negative Cache TTL (24 horas)
;
@       IN   NS   localhost.
www     IN   A    10.0.2.15
ftp     IN   A    10.0.2.15
smtp    IN   A    10.0.2.15
pop     IN   A    10.0.2.15
imap    IN   A    10.0.2.15
ssh     IN   A    10.0.2.15
mail    IN   A    10.0.2.15
```

Arquivo /etc/bind/db.teobaldo.net.rev

```
$TTL 86400  ;(24 horas)
@ IN SOA teobaldo.net. ewerton.teobaldo.net. {
  1    ;Serial
  604800   ;Refresh (7 dias)
  86400    ;Retry   (24 horas)
  2419200 ;Expire (28 dias)
  86400)   ;Negative Cache TTL (24 horas)
;
     IN   NS   teobaldo.net.
1    IN   PTR    www.teobaldo.net.
2    IN   PTR    ftp.teobaldo.net.
```

```
3   IN   PTR    smtp.teobaldo.net.
4   IN   PTR    pop.teobaldo.net.
5   IN   PTR    imap.teobaldo.net.
6   IN   PTR    ssh.teobaldo.net.
7   IN   PTR    mail.teobaldo.net.
```

Configurar a estação para utilizar o Bind9 instalado na propria máquina.
Arquivo /etc/resolvconf/resolv.conf.d/head

```
nameserver 10.0.2.15
```

Script de instalação e configuração:

```
#!/bin/bash

# Instalação do Bind9
echo "Instalando o Bind 9"
sudo apt install bind9

# Configuração da zona do dominio
echo "Criando zona do dominio"
echo "zone \"teobaldo.net\" {" >> /etc/bind/named.conf.default-zones
echo "   type master;" >> /etc/bind/named.conf.default-zones
echo "   file \"/etc/bind/db.teobaldo.net\";" >> /etc/bind/named.conf.default-zones
echo "};" >> /etc/bind/named.conf.default-zones

# Configuração do dominio
echo "Criando dominio"
echo "\$TTL 86400" >> /etc/bind/db.teobaldo.net
echo "@ IN SOA teobaldo.net. root.teobaldo.net. (" >> /etc/bind/db.teobaldo.net
echo "   1   ;Serial" >> /etc/bind/db.teobaldo.net
echo "   604800   ;Refresh" >> /etc/bind/db.teobaldo.net
echo "   86400   ;Retry" >> /etc/bind/db.teobaldo.net
echo "   2419200   ;Expire" >> /etc/bind/db.teobaldo.net
echo "   86400)   ;Negative Cache TTL" >> /etc/bind/db.teobaldo.net
echo ";" >> /etc/bind/db.teobaldo.net
echo "@          IN   NS   localhost." >> /etc/bind/db.teobaldo.net
echo "www  IN   A      10.0.2.15" >> /etc/bind/db.teobaldo.net
echo "ftp  IN   A      10.0.2.15" >> /etc/bind/db.teobaldo.net
echo "smtp IN   A      10.0.2.15" >> /etc/bind/db.teobaldo.net
echo "pop  IN   A      10.0.2.15" >> /etc/bind/db.teobaldo.net
echo "imap IN   A      10.0.2.15" >> /etc/bind/db.teobaldo.net
echo "mail IN   A      10.0.2.15" >> /etc/bind/db.teobaldo.net
echo "ssh  IN   A      10.0.2.15" >> /etc/bind/db.teobaldo.net
```

```
#Configurar arquivo HOSTS
echo "127.0.0.1 localhost" > /etc/hosts
echo "10.0.2.15 usuario-VirtualBox" >> /etc/hosts
echo  " " >> /etc/hosts
echo "# The following lines are desirable for IPv6 capable hosts" >> /etc/hosts
echo "::1         ip6-localhost ip6-loopback" >> /etc/hosts
echo "fe00::0 ip6-localnet" >> /etc/hosts
echo "ff00::0 ip6-mcastprefix" >> /etc/hosts
echo "ff02::1 ip6-allnodes" >> /etc/hosts
echo "ff02::2 ip6-allrouters" >> /etc/hosts

#Configurando DNS local na máquina
echo "nameserver 10.0.2.15" >> /etc/resolvconf/resolv.conf.d/head
echo " " >> /etc/resolvconf/resolv.conf.d/head
sudo service resolvconf restart

#Reiniciar o bind
echo "Restart servidor dns e aplicando configurações..."
/etc/init.d/bind9 restart

#Teste
echo "######## Vamos testa agora!! ########"
echo "Checar arquivo de configurações"
named-checkzone www /etc/bind/db.teobaldo.net
echo "Testa se o servidor foi configurado corretamente!!!"
```

Apache 2 e OpenSSL

O Apache é um servidor de código aberto e que alimenta cerca de 46% de todos os sites hospedados na internet. O nome oficial dele é Apache HTTP Server. E ele é mantido pela Apache Software Foundation.

O Apache permite que donos de sites mostrem e mantenham seus conteúdos na internet – daí o nome de “servidor de internet”. Ele é um dos mais antigos e confiáveis servidores de internet. A sua primeira versão, por exemplo, foi lançada em 1995, há mais de 20 anos.

Quando alguém visita um site, esse visitante entra em um domínio na barra de endereço por um navegador. Em seguida, o servidor entrega os arquivos solicitados atuando como se fosse um como um entregador de encomendas, só que virtual.

Embora estejamos chamando o Apache de servidor de internet, ele não é um servidor físico. Ele é um software que é executado em um servidor. O trabalho dele é estabelecer uma conexão entre o servidor e os navegadores de sites (Firefox, Google Chrome, etc.) enquanto puxa e entrega arquivos entre eles (estrutura cliente-servidor).

O Apache é um software multiplataforma. Portanto, ele funciona tanto em servidores Unix quanto em servidores Windows. Assim, você está amparado pelo uso dos dois lados, independente qual deles queira usar.

Quando um visitante quer carregar uma página no seu site, por exemplo, a página inicial ou a página “Sobre nós”, o navegador dele envia um pedido para o seu servidor e o Apache devolve uma resposta com todos os arquivos solicitados (texto, imagens, etc.).

O servidor e o cliente se comunicam pelo protocolo HTTP. E o Apache é responsável por facilitar e assegurar a comunicação entre os dois lados.

O Apache é altamente personalizável e ele tem uma estrutura baseada em módulos. Esses módulos permitem que os administradores dos servidores ativem ou desativem novas funcionalidades.

O Apache tem módulos para segurança, cache, reescrita de URL, autenticação de senhas e mais. Para sua instalação e execução basta rodar os comandos:

```
$ sudo apt-get update
$ sudo apt-get install apache2
$ sudo apt-get install php
$ sudo apt-get install phpmyadmin
$ sudo apt-get install nmap
```

Acessando o diretório /etc/apache2/sites-availabel/, vai encontrar os 3 arquivos de configurações que já vem com as configurações padrão do apache2. Com isso ja conseguirá rodar suas páginas HTML no navegador, basta apenas incluir os arquivos HTML na pasta /var/www/html e digitar o diretório localhost no navegador.

Certificado digital

É um documento criptografado que contém informações necessárias para identificação de uma pessoa física ou entidade jurídica. Qualquer conteúdo eletrônico que foi assinado digitalmente tem garantia de autenticidade de origem. Por exemplo: ao receber uma requisição, verifica-se os campos do certificado digital, a partir desses dados pode-se ter certeza que a origem da requisição é confiável e autêntica. Um certificado digital é emitido por uma Autoridade Certificadora (AC), uma entidade confiável do ponto de vista jurídico. No entanto, isso não impede que você mesmo crie um certificado digital para fins particulares. O certificado digital é transmitido através de uma conexão segura, que usa um protocolo de transmissão específico para transmitir dados criptografados: o SSL (Secure Socket Layer). Você só poderá usar um certificado digital se a aplicação (navegador da web, cliente de e-mail, etc) que você estiver utilizando implementar o suporte a conexões seguras.

OpenSSL

É uma implementação de código aberto dos protocolos SSL e TLS. A biblioteca (escrita na linguagem C) implementa as funções básicas de criptografia e disponibiliza várias funções utilitárias. Também estão disponíveis wrappers que permitem o uso desta biblioteca em várias outras linguagens. Para a instalação do openssl basta rodar os comandos:

$sudo apt install openssl
$sudo openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
$sudo a2enmod ssl

VsFTP (Servidor FTP)

FTP é a sigla para File Transfer Protocol, um termo que, traduzido para o português, significa Protocolo de Transferência de Arquivos.
Ele é basicamente um tipo de conexão que permite a troca de arquivos entre dois computadores conectados à internet. Com ela, você pode enviar qualquer coisa para uma outra máquina ou armazená-los em um servidor FTP, ficando ela sempre disponível para o usuário acessar.

Um servidor FTP é o servidor que oferece um serviço de acesso a um disco rígido ou servidor de arquivos criados através de um protocolo FTP. É ele que armazena as informações ou dados enviados por um usuário e que estarão acessíveis por qualquer membro da internet.
Servidores FTP são muito usados quando se trabalha com grandes volumes de dados compartilhados pela rede. E eles são bastante úteis para gerenciar essas informações entre diversos clientes que solicitam o acesso a eles. Instalação e configuração do Vsftpd:

$sudo apt-get install vsftpd
$sudo ufw status (verificar se o firewall está ativo e bloqueando as portas 20 e 21)
É necessário ter um usuário criado (sudo adduser [FULANO])
No arquivo /etc/vsftpd.conf é preciso fazer as configurações para dar permissão de leitura e escrita.
/etc/vsftpd.userlist criar o arquivo com nome de usuários que poderão acessar os dados
$sudo systemctl restart vsftpd

OpenSSH (Servidor SSH)

O SSH (Secure SHell) é um protocolo que permite a você acessar virtualmente o servidor como se você estivesse em um terminal (no prompt do DOS, por exemplo). Se você preferir, considere como o SSH como um computador controlando outro computador.
A diferença entre o telnet e o SSH está na segurança. Toda a transmissão de dados no SSH é criptografada. Assim, os riscos de alguém "bisbilhotar" o que você está fazendo no servidor (às vezes você precisa transmitir senhas para acessar outros sistemas ou programas) é virtualmente zero. Fora isso, tudo o que você faz no telnet pode ser feito pelo SSH.

Quando você conecta via terminal remoto com seu servidor, você está controlando aquele servidor a partir de seu sistema operacional. Qualquer comando que você digitar é executado no servidor (e não no seu PC) e você opera de acordo com os paramêtros de comandos do servidor. Para acessar o protocolo SSH é necessário um programa que conecte na porta 22. Dica:Usamos o programa PUTTY para fazer a conexão. Instalando ssh:

$sudo apt-get install openssh-server

Conclusão

Apesar de algumas dificuldades encontradas no decorrer do projeto, conseguimos implementar quase todos os servidores, ficando pendente apenas o servidor webmail, que tivemos uma grande dificuldade de implementá-lo e por isso acabamos desviando o foco para os outros, e a configuração do ssl. No mais todos os outros serviços estão validados e pronto na máquina virtual criada.

Referências

- https://www.dicas-l.com.br/sysadmin/sysadmin_20071123.php
- https://pt.wikipedia.org/wiki/Sistema_de_Nomes_de_Dom%C3%ADnio
- http://dboanarede.blogspot.com/2015/05/dns-domain-name-system.html
- https://blog.remontti.com.br/1397
- https://www.techemportugues.com/2016/03/20/dns-aprenda-configurar-um-servidor-bind9/
- https://www.cisco.com/c/en/us/support/docs/ip/domain-name-system-dns/12684-dns-resource.html
- https://www.vivaolinux.com.br/artigo/Tutorial-de-instalacao-e-configuracao-do-Apache-no-Linux
- https://pt.wikipedia.org/wiki/OpenSSL
- https://ajudadoprogramador.com.br/artigo/certificado-auto-assinado-no-linux
- https://www.hostinger.com.br/tutoriais/ftp-o-que-e-como-funciona
- https://www.cybernetfx.com/clientes/index.php?rp=/knowledgebase/71/O-que-e-e-como-usar-SSH.html