



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Instituto de Ciências Exatas e de Informática

Projeto de infraestrutura de redes: Anymalhas

Davi Coelho Peixoto

Fernanda Belmont Rivlis

Lucas Dias de Melo

Márcia Delmare de Oliveira Peixoto

Pedro Miranda

Valdeir Carlos Mendes

Orientador: Fábio Leandro Rodrigues Cordeiro

PROJETO DE INFRAESTRUTURA DE REDE:

ANYMALHAS

Belo Horizonte

2024

1. INTRODUÇÃO

1.1 A empresa de manufatura Anymalhas

Este segmento pode ser entendido como toda e qualquer empresa, independente do porte, que transforma matéria prima em um produto ou parte de um produto que ainda será montado.

Atualmente, o setor da indústria no Brasil é responsável por 20,2% dos empregos formais, além de representar 20,9% do PIB nacional.

A Anymalhas é uma empresa brasileira de manufatura têxtil, fundada em 1990, que se especializou na produção de fios e tecidos para diversos segmentos do mercado.

Possui sua Matriz, na região central e industrial de Belo Horizonte, Minas Gerais, onde possui escritórios e a produção. Na sua Matriz, a empresa faz a administração de vendas, marketing, recursos humanos e concentra suas operações. Para a produção dos fios e tecidos, são utilizados diversos materiais como: algodão, poliéster, linho, lã, lã PET reciclada e acrílico.

Além da matriz, a empresa possui três filiais nas cidades de Arcos, Campo Belo e Lavras, todas localizadas a aproximadamente 200 km de Belo Horizonte. Essas filiais funcionam como centro de produção.

A Anymalhas possui cerca de 129 funcionários e conta com 62 máquinas, utilizando a tecnologia para otimizar o processo de produção.

Ser a melhor para trabalhar e para vestir, se destacando como uma empresa criativa e sustentável.

1.1.1 Missão

Ser uma empresa com horizontes globais, que se destaca pela criatividade e sustentabilidade, alicerçada em um ambiente de inovação, melhoria contínua e excelência operacional, atendendo à indústria têxtil com as melhores soluções em fios e estabelecendo-se como referência em inovação e gestão de pessoas. Seu compromisso é oferecer produtos exclusivos que agreguem valor à vida dos clientes empresariais, contribuindo para expressar o estilo próprio de cada um.

1.1.2 Valores

Oferecer soluções inovadoras e integradas para a cadeia têxtil, de forma sustentável, com entusiasmo e relacionamento de confiança.

1.1.3 Produção

A empresa é especializada na produção de fios e diversos tipos de tecidos, destinados à confecção de roupas, estofados, tecidos técnicos e industriais, decoração de interiores etc. A produção é dividida basicamente em quatro etapas:

1. Fiação: envolve a transformação das fibras, naturais ou sintéticas, em fios. As fibras naturais são as de origem animal, como a lã e a seda, e as de origem vegetal, como o algodão, a juta e o linho. Já as sintéticas são obtidas a partir de polímeros sintéticos, como o elastano, a poliamida e o poliuretano, e englobam, por exemplo, o náilon e o poliéster.

2. Tecelagem: formação dos tecidos têxteis através do entrelaçamento de fios no tear, de forma longitudinal (urdume) e transversal (trama).

3. Malharia: entrelaçamento de fios têxteis, feito com agulhas, sempre no mesmo sentido, ou seja, todos na trama (horizontal) ou todos no urdume (teia).

4. Beneficiamento: tratamentos adicionais aos tecidos, como tingimento, estamparia, impermeabilização, resistência a altas temperaturas e cortes, processos para melhorar as propriedades ou o apelo estético do tecido.

A manufatura também é conhecida como “segundo setor”, e ao longo dos anos teve seus processos aprimorados com foco em otimização para produção em larga escala. Após a Revolução Industrial, o processo “manual” foi ficando cada vez mais automatizado, dando seu lugar para máquinas que fazem o mesmo trabalho, potencialmente sem erros e com maior velocidade

Máquinas inteligentes de produção otimizam o processo de fabricação têxtil, garantindo maior eficiência, qualidade e flexibilidade na criação de diferentes tipos de tecidos. As máquinas de fiação, de tecelagem e de tricô, ao serem conectadas a uma infraestrutura de rede, permitem um monitoramento e controle centralizado em tempo real, facilitando a detecção e correção de falhas.

1.1.4 Serviços Oferecidos

A Anymalhas possui serviços voltados para o atendimento e suporte às empresas, com o objetivo de atender às necessidades específicas de cada empresa.

Entre os serviços oferecidos, destacam-se: suporte na escolha de produtos, consultoria

técnica especializada, atendimento ao cliente, plataformas de pedidos online e e-commerce (B2B) e serviço de entrega e logística. Este último, em parceria com fornecedores logísticos, de forma terceirizada.

1.2 Análise, planejamento e prototipação da solução

1.2.1 Infraestrutura de Rede

1.2.1.1 Infraestrutura de rede da matriz (Belo Horizonte)

A matriz da Anymalhas, localizada em Belo Horizonte, conta com uma infraestrutura de rede projetada para atender todas as operações da empresa. Nessa unidade estão concentrados os escritórios centrais responsáveis pela gestão da maioria dos setores, além de abrigar parte da produção de têxteis.

A matriz emprega cerca de 61 funcionários e utiliza 50 máquinas ligadas a rede, além de 2 tablets para uso local e 10 note-books para eventuais trabalhos remotos dos funcionários.

SETOR	Nº DE FUNCIONÁRIOS	FUNÇÃO	QUANTIDADE DE COMPUTADORES
Diretoria	3	Diretor, Assessor, Auxiliar	3
Marketing	4	Gerente, Designer, Gestor de Tráfego, Auxiliar	4
Recursos Humanos	4	Gerente de RH, 2 Auxiliares de RH	3
Departamento Pessoal	4	Gerente, Controle de Ponto, Folha de Pagamento, Legislação Trabalhista	3

Financeiro	3	Gerente, Auxiliares	3
Compras	5	Gerente, Compradores	5
Comercial	6	Gerente, Vendedores	6
Contabilidade	3	Gerente, Contador, Auxiliar	3
Fiscal	5	Gerente, Analista, Responsáveis pelas Entradas, Saídas e Legislação	5
Logística	6	Gerente, Analista, Conferentes	
T.I.	7	Gerente, Gestor de Projetos, Desenvolvedor, Analista de Dados, Analista de Segurança e 2 Suportes	7
Produção	13	Supervisor de Produção, 2 Técnicos em Fiação, 2 Técnicos em Tecelagem, 2 Técnicos em Tricô, 2 Coloristas, 2 Inspecionadores de Qualidade Têxtil, 2 Técnicos de Manutenção e Máquinas	5
Estratégico	1	Especialista de Mercado	1

1.2.1.2 Infraestrutura de rede das filiais (Arcos, Campo Belo e Lavras)

As três filiais da Anymalhas, localizadas respectivamente nas cidades de Arcos, Campo Belo e Lavras, possuem uma infraestrutura de rede semelhante, focada principalmente no setor de produção. Embora o número de dispositivos conectados à rede seja menor em comparação à matriz, com um total de 15 máquinas ligadas à cabo e 5 notebooks para eventuais trabalhos

remotos na filial 1 e 6 máquinas ligadas à cabo e 3 notebooks para eventuais trabalhos remotos nas filiais 2 e 3. Essa estrutura garante uma conectividade eficiente entre as unidades, promovendo a integração das operações e assegurando um fluxo produtivo contínuo. Cada filial emprega 61 colaboradores, o que reforça a importância de manter uma rede confiável para suportar suas atividades diárias.

Os setores que cada filial da Anymalhas possui com seus respectivos funcionários e o número de computadores conectados à rede são:

SETOR	Nº DE FUNCIONÁRIOS	FUNÇÃO	QUANTIDADE DE COMPUTADORES
Recursos Humanos	2	Gerente de RH e Auxiliar de RH	2
Financeiro	2	Analista Financeiro, Auxiliar Financeiro	2
Fiscal	3	Responsáveis pelas Entradas, Saídas e Legislação	3
Logística	3	Gerente, conferentes	3
Produção	13	Supervisor de Produção, 2 Técnicos em Fiação, 2 Técnicos em Tecelagem, 2 Técnicos em Tricô, 2 Coloristas, 2 Inspetores de Qualidade Têxtil, 2 Técnicos de Manutenção e Máquinas	5

Tanto a matriz quanto as filiais possuem um Centro de Processamento de Dados (CPD), onde estão acomodados racks, servidores e equipamentos de rede (roteadores e switches), firewalls, servidores e cabeamento estruturado. Nos setores estão alocadas as máquinas (PCs e note-books), conectados via cabeamento ou rede wireless.

A topologia de rede utilizada é a topologia em barramento, também conhecida como linear. Neste tipo de topologia, todos os dispositivos são ligados a um único cabo, chamado de barramento. Os dados são enviados por este barramento e todos os dispositivos os recebem, mas apenas o destino processa as informações.

1.2.2 Prototipação da Solução

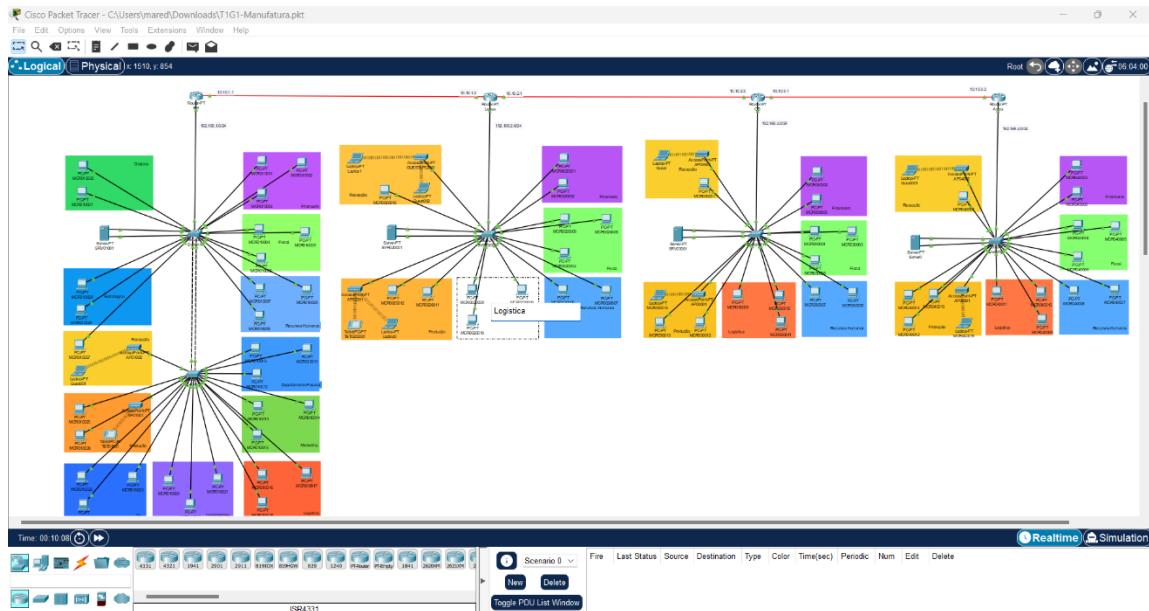
Para a prototipação da solução, foi utilizada a ferramenta de simulação de rede Cisco Packet Tracer. Esta ferramenta permite a criação, configuração e teste de redes virtuais em um ambiente simulado, facilitando a visualização e o ajuste de configurações antes da implementação real. Conforme o plano de infraestrutura, foram adicionados os dispositivos necessários (roteadores, switches e computadores), que foram configurados com seus respectivos IPs, tanto fixos quanto por meio de DHCP. Em seguida, foram simulados diferentes tipos de tráfego de rede para observar o comportamento e o desempenho da rede. Por fim, foram previamente mapeados os serviços que serão instalados e configurados *on-premise* e/ou *on cloud* na etapa seguinte: DNS, Email, Web, FTP, AD e DHCP.

Para a prototipação da infraestrutura de rede foi utilizada a ferramenta Cisco Packet Tracer, onde a partir do planejamento da rede (definição de objetivos da rede, número de dispositivos, tipos de conexões, segurança, etc.) foi criado um diagrama visual da rede.

Através do Cisco Packet Tracer, foi realizada a configuração dos dispositivos (roteadores e Switches), com seus respectivos IPs, tanto fixos quanto por meio de DHCP, conforme o plano de infraestrutura. Também foi feita a simulação do tráfego de rede com o objetivo de verificar se a configuração atendia aos requisitos.

Por fim, foram previamente mapeados os seguintes servidores que serão implementados na etapa seguinte: DNS, Email, WEB, FTP, Database, Serviço de diretório (AD) e DHCP.

Figura 1 – Protótipo da infraestrutura de rede



2. PREPARAÇÃO DO AMBIENTE EM NUVEM E VIRTUALIZAÇÃO LOCAL

Nesta etapa do projeto, foi realizado o mapeamento e implantação dos servidores *on cloud* e *on-premise* para o devido atendimento do planejamento inicial.

2.1 Serviços *on cloud*

A hospedagem de servidores em nuvem é uma tecnologia que permite executar sites, aplicativos, bancos de dados e outros serviços em servidores virtuais na nuvem, em vez de depender de hardware físico específico. Isso oferece várias vantagens como flexibilidade, escalabilidade e eficiência de custos.

Para a hospedagem *on cloud*, foi utilizada a play de serviço da Amazon Web Services (AWS). A AWS é uma plataforma cloud computing, que oferece várias funcionalidades para ajudar empresas a desenvolver e gerenciar suas aplicações de forma eficiente e escalável.

Na figura a seguir podemos observar o painel EC2 da AWS, mostrando três instâncias (WEBMAIL e WEB) na região us-east-1a. As instâncias do tipo t2.micro estão em execução com status variando entre inicializando e executando. O painel fornece detalhes como ID da instância, DNS público e IP elástico, permitindo o monitoramento e controle das máquinas virtuais.

Figura 2 – painel EC2 da AWS

The screenshot shows the AWS Management Console with the EC2 service selected. The left sidebar includes links for Painel, Visualização Global do EC2, Eventos, Instâncias (selected), Types de instância, Modelos de execução, Solicitações spot, Savings Plans, Instâncias reservadas, Hosts dedicados, Reservas de capacidade, Images, AMIs, Catalogo de AMIs, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Rede e segurança, Security groups, IPs elásticos, Placement groups, Pares de chaves, Interfaces de rede, CloudShell, and Comentários.

The main content area displays the 'Instâncias' (Instances) table with the following data:

	Name	ID da Instância	Estado da Inst...	Tipo de Inst...	Verificação de stat...	Status do alarm...	Zona de dispon...	DNS IPv4 público	Endereço IP...	IP elástico	IPs IPv6
<input type="checkbox"/>	WEBMAIL	i-09f26896324d607e8	Executando	t3.small	Initializando	Exibir alarms +	us-east-1a	ec2-3-223-106-189.co...	3.223.106.189	3.223.106.189	-
<input type="checkbox"/>	i-07e1422ee4fc65862	i-07e1422ee4fc65862	Executando	t3.micro	Initializando	Exibir alarms +	us-east-1a	ec2-3-89-206-52.com...	3.89.206.52	-	-
<input type="checkbox"/>	WEB	i-0b548bf97c0e6d4ef	Executando	t3.micro	Initializando	Exibir alarms +	us-east-1a	ec2-3-214-198-62.com...	3.214.198.62	3.214.198.62	-

A modal window titled 'Selecionar uma instância' is open at the bottom left, with the instruction 'Selecione a instância que deseja executar'.

2.1.1 Servidores hospedados em nuvem

▫ DNS

Um servidor DNS (Domain Name System) é um banco de dados hierárquico distribuído que armazena endereços IP e outros dados, e os procura por nome. Quando um usuário digita um endereço URL no navegador, o provedor de acesso repassa a solicitação para o DNS, que encontra o IP do servidor que armazena o site. Para esse serviço foi utilizado o Route 53 da AWS.

Na figura 3 é possível ver a configuração da zona hospedada `anymalhas.com` no serviço Route 53 da AWS. Na seção de registros, aparecem entradas de DNS como tipos A, NS, SOA e CNAME, cada uma com suas políticas e valores específicos, incluindo IPs e nomes de servidores. Essa tela permite gerenciar os registros de DNS para o domínio, facilitando o roteamento de tráfego para os serviços correspondentes.

Figura 3 - zonas de hospedagem

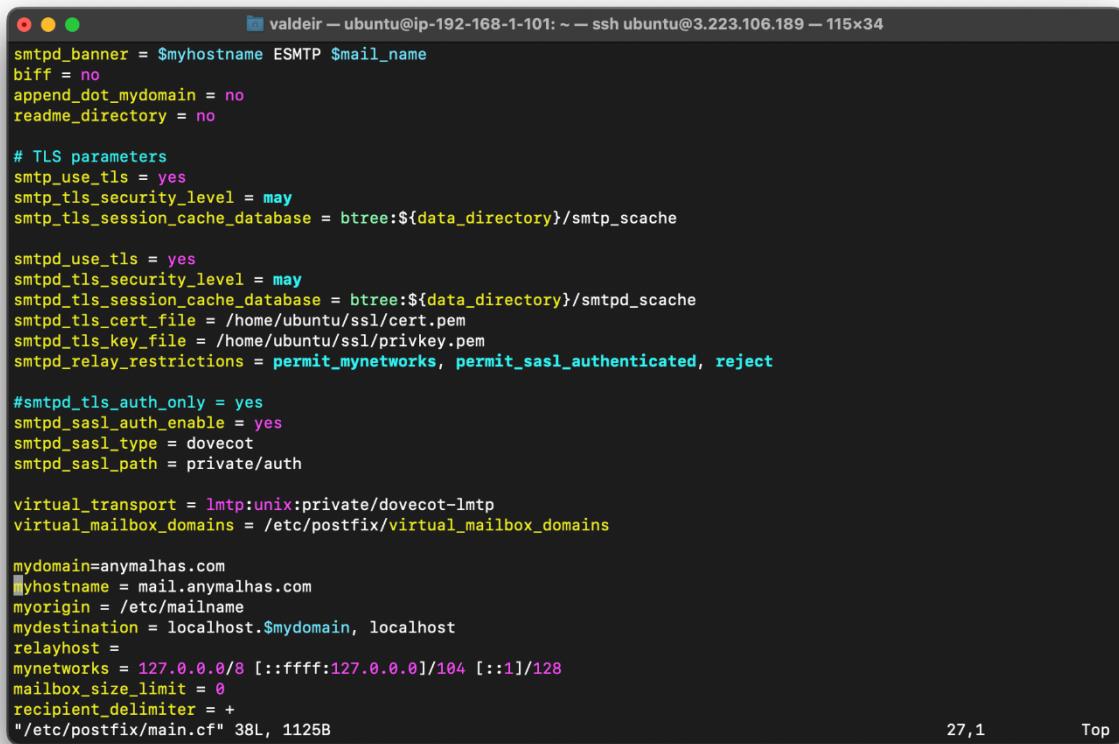
Nome do registro	Tipo	Propriedade	Valor/roteador de tráfego para	TTL (segundos)	ID de versão	Avaliação
anymalhas.com	A	Simples	-	300	-	-
anymalhas.com	MX	Simples	-	300	-	-
anymalhas.com	NS	Simples	-	172800	-	-
anymalhas.com	SOA	Simples	-	900	-	-
mail.anymalhas.com	A	Simples	-	300	-	-
webmail.anymalhas.com	A	Simples	-	300	-	-
www.anymalhas.com	CNAME	Simples	-	300	-	-

□ E-mail com Webmail

Um servidor de e-mail é um sistema que permite o envio, recebimento e armazenamento de mensagens eletrônicas. Ele é responsável por: gerenciar o fluxo de mensagens entre provedores de e-mail e a internet; processar e entregar e-mails recebidos aos destinatários; controlar a segurança e impedir que outras pessoas tenham acesso aos e-mails e documentos. Utilizando uma instância EC2 foi instalado e configurado servidores de SMTP, POP3 e um webmail.

A figura 4 mostra um arquivo de configuração do servidor de e-mail Postfix onde várias configurações estão definidas para gerenciar o serviço SMTP e segurança TLS. As configurações incluem `smtp_use_tls` e `smtp_tls_security_level` para habilitar o uso de TLS, além dos caminhos para os arquivos de certificado e chave SSL. Também estão especificados detalhes como o domínio `anymalhas.com`, nome do host `mail.anymalhas.com` e as restrições de retransmissão para maior segurança.

Figura 4 – configuração gerenciamento serviço SMTP e segurança TLS



The screenshot shows a terminal window titled "valdeir" running on an Ubuntu system. The command "ssh ubuntu@3.223.106.189" is visible at the top. The window displays the configuration file for the Postfix SMTP service, specifically /etc/postfix/main.cf. The configuration includes various parameters related to TLS (TLS parameters, certificate files, and security levels), virtual transports (lmtp), and virtual mailbox domains. The configuration file is color-coded for readability, with keywords in blue and values in black. The terminal window has a dark background and light-colored text. In the bottom right corner of the terminal window, there is a status bar with the number "27,1" and the word "Top".

```
valdeir - valdeir@ip-192-168-1-101: ~ - ssh ubuntu@3.223.106.189 - 115x34
smtpd_banner = $myhostname ESMTP $mail_name
biff = no
append_dot_mydomain = no
readme_directory = no

# TLS parameters
smtp_use_tls = yes
smtp_tls_security_level = may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_use_tls = yes
smtpd_tls_security_level = may
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtpd_tls_cert_file = /home/ubuntu/ssl/cert.pem
smtpd_tls_key_file = /home/ubuntu/ssl/privkey.pem
smtpd_relay_restrictions = permit_mynetworks, permit_sasl_authenticated, reject

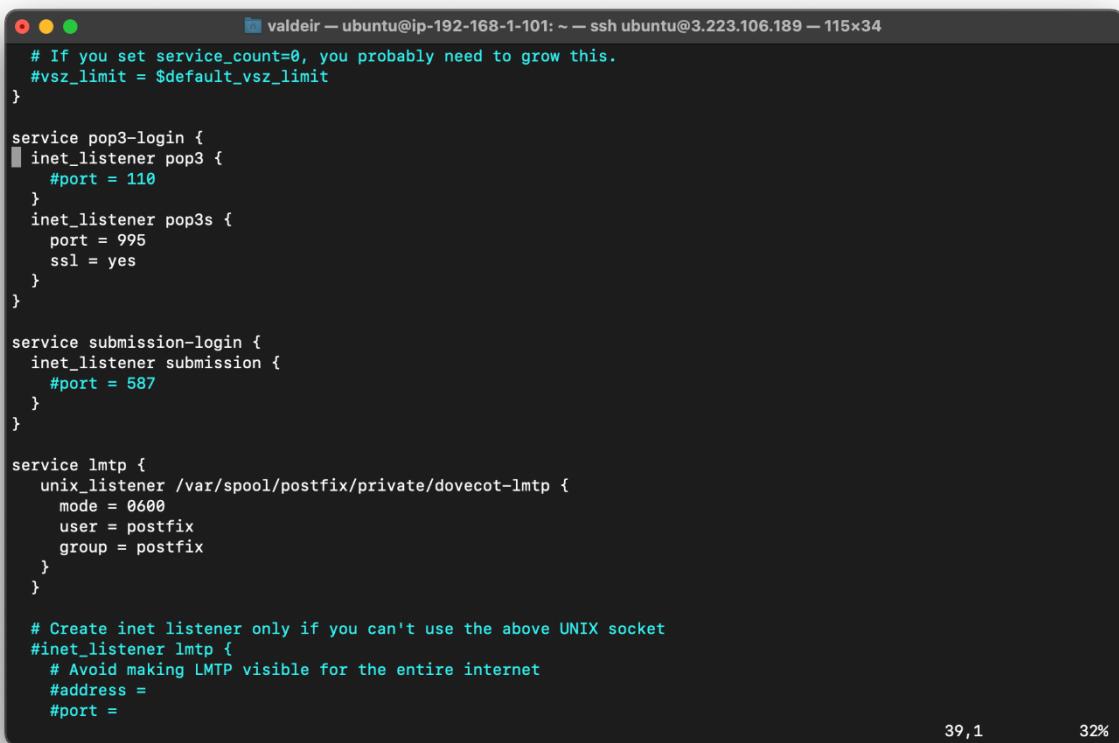
#smtpd_tls_auth_only = yes
smtpd_sasl_auth_enable = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth

virtual_transport = lmtp:unix:private/dovecot-lmtp
virtual_mailbox_domains = /etc/postfix/virtual_mailbox_domains

mydomain=anymalhas.com
myhostname = mail.anymalhas.com
myorigin = /etc/mailname
mydestination = localhost.$mydomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [:ffff:127.0.0.0]/104 [:1]/128
mailbox_size_limit = 0
recipient_delimiter = +
"/etc/postfix/main.cf" 38L, 1125B
```

Na figura 5, a seguir, é apresentada a configuração do Dovecot utilizada para gerenciar serviços de e-mail como POP3 e LMTP. As portas para POP3 seguro (POP3S) e envio de e-mails estão definidas, com POP3S na porta 995 e a submissão na 587. O serviço LMTP está configurado com um unix_listener para integrar-se ao Postfix, definindo características específicas do usuário e grupo.

Figura 5 – configuração serviços de e-mail



```
# If you set service_count=0, you probably need to grow this.
#vsz_limit = $default_vsz_limit
}

service pop3-login {
inet_listener pop3 {
    #port = 110
}
inet_listener pop3s {
    port = 995
    ssl = yes
}
}

service submission-login {
inet_listener submission {
    #port = 587
}
}

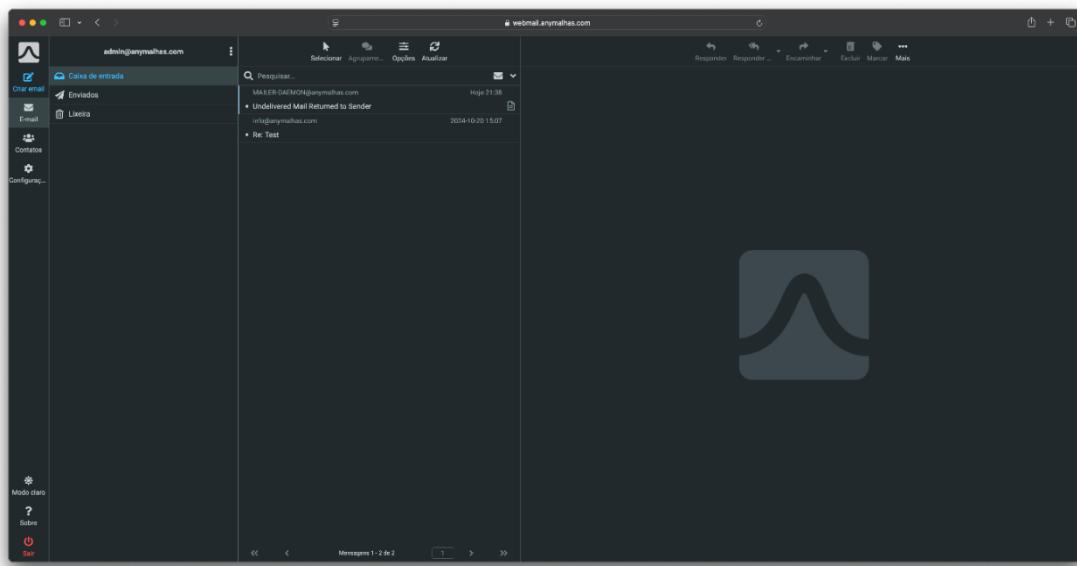
service lmtp {
unix_listener /var/spool/postfix/private/dovecot-lmtp {
    mode = 0600
    user = postfix
    group = postfix
}
}

# Create inet listener only if you can't use the above UNIX socket
#inet_listener lmtp {
#    # Avoid making LMTP visible for the entire internet
#    #address =
#    #port =
```

39,1 32%

A figura 6 mostra a interface de um cliente de webmail(Roudcube), acessando a conta admin@anymalhas.com. Na coluna da esquerda há pastas como caixa de entrada e enviados. No centro uma lista de e-mails exibe duas mensagens, incluindo uma de MAILER-DAEMON e outra de info @anymalhas.com. A interface oferece opções para gerenciar e-mails como responder, encaminhar e excluir, facilitando o uso do correio eletrônico pela web.

Figura 6 – Interface de um cliente de webmail Roudcube



WEB

Um servidor Web é um sistema que armazena, processa e entrega conteúdos e serviços para os usuários da internet. Quando um usuário digita uma URL ou clica em um link, o servidor web recebe a solicitação, processa e envia a página desejada para o navegador. Utilizando uma instância EC2 foi instalado e configurado o Apache 2 juntamente com PHP na versão 8.2

Na figura 7, no terminal é apresentado um trecho da configuração do PHP em um servidor. A opção expose_php é definida como Off o que impede a exibição de que o PHP está instalado no servidor. Há também limites de recursos especificados, como max_execution_time de 30 segundos que definem o tempo máximo de execução de cada script e max_input_time de 60 segundos que limitam o tempo para processar dados de entrada. Outras configurações incluem o nível máximo de aninhamento de variáveis max_input_nesting_level e o número máximo de variáveis de entrada permitidas max_input_vars configurado como 1000.

Figura 7 – configuração do PHP em um servidor

```
; Decides whether PHP may expose the fact that it is installed on the server
; (e.g. by adding its signature to the Web server header). It is no security
; threat in any way, but it makes it possible to determine whether you use PHP
; on your server or not.
; https://php.net/expose-php
expose_php = Off

;;;;;;;;;;
; Resource Limits ;
;;;;;;;;;

; Maximum execution time of each script, in seconds
; https://php.net/max-execution-time
; Note: This directive is hardcoded to 0 for the CLI SAPI
max_execution_time = 30

; Maximum amount of time each script may spend parsing request data. It's a good
; idea to limit this time on production servers in order to eliminate unexpectedly
; long running scripts.
; Note: This directive is hardcoded to -1 for the CLI SAPI
; Default Value: -1 (Unlimited)
; Development Value: 60 (60 seconds)
; Production Value: 60 (60 seconds)
; https://php.net/max-input-time
max_input_time = 60

; Maximum input variable nesting level
; https://php.net/max-input-nesting-level
;max_input_nesting_level = 64

; How many GET/POST/COOKIE input variables may be accepted
;max_input_vars = 1000
```

▫ Banco de Dados

Bancos de dados são conjuntos de arquivos relacionados, normalmente contendo registros sobre pessoas, lugares ou informações em geral. Esses conjuntos são coleções organizadas de dados, que podem estar inter-relacionados ou não, com o objetivo de armazenar informações essenciais para empresas. De fato, os bancos de dados tornaram-se a principal fonte de dados para sistemas de informação e segurança.

Para uso dessa ferramenta optou-se por utilizar o serviço RDS da AWS com SGBD MySQL instalado, pois já abstrai grande parte da instalação e configuração. Além disso, alterações podem ser feitas utilizando o console de gerenciamento sem a necessidade de utilizar linhas de comando.

Na figura 8, captura de parte do painel do RDS mostrando as propriedades do banco. Na imagem é exibido o painel do Amazon RDS, onde estão as propriedades de um banco de dados chamado "mail", configurado com o mecanismo MySQL Community. O resumo mostra detalhes como a classe de instância db.t4g.micro, o status disponível, a utilização de CPU 2,67%, e a região us-east-1c. Na seção segurança e conexão, o endpoint e a porta 3306 são especificados, juntamente com as subredes e grupos de segurança associados.

Figura 8 – Propriedades de base de dados do RDS.

Identificador de banco de dados	Status	Função	Mecanismo	Recomendações
mail	Disponível	Instância	MySQL Community	2 Informativa

Endpoint	Redes	Segurança
mail.cev6paqwsblk.us-east-1.rds.amazonaws.com	Zona de disponibilidade: us-east-1c VPC: my-vpc (vpc-09bf4410f1a19a06a) Grupo de sub-redes: default-vpc-09bf4410f1a19a06a Sub-redes: subnet-0fa15b6710cd9f5f subnet-000294eb97c761ea subnet-075d44443061af982b subnet-0b058789957565189 subnet-009ef4711beab2142 subnet-03acb422b118d8e38	Grupos de segurança da VPC: default (sg-063117283fd36ed94) Ativo Publicamente acessível: Sim Autoridade de certificação: rds-ca-rsa2048-g1 Data da autoridade de certificado: May 25, 2061, 20:54 (UTC-03:00) Data de expiração do certificado da instância de banco de dados: October 12, 2025, 09:52 (UTC-03:00)

FTP

- Configuração do servidor FTP na AWS Ubuntu

File Transfer Protocol (FTP) é um protocolo utilizado para transferir arquivos entre computadores em uma rede que utiliza o TCP/IP como a internet. Ele permite que usuários autorizados façam upload e download de arquivos de um servidor FTP facilitando a transferência de dados entre diferentes dispositivos.

Para estabelecer uma conexão FTP é necessário um cliente FTP e um servidor FTP. O cliente envia uma solicitação ao servidor que responde com as credenciais necessárias.

O FTP é simples de configurar e utilizar, especialmente com clientes FTP como Filezilla. Além disso, suporta grandes volumes de dados e é amplamente utilizado para transferência de arquivos grandes.

Na figura 9, este terminal de comando no sistema operacional Ubuntu, o usuário está executando várias instruções de instalação e configuração de pacotes. Comandos como sudo apt-get install vsftpd, sudo apt install vim, e sudo apt install net-tools são usados para instalar pacotes específicos, incluindo o servidor FTP vsftpd e os editores de texto vim e nano. Ao final, o comando sudo ufw status exibe o status do firewall UFW (Uncomplicated Firewall), mostrando que as portas 20/tcp e 21/tcp estão configuradas para permitir conexões de qualquer origem,

diminuindo configurações para serviços de FTP.

Figura 9 - Atualização dos pacotes e instalação do vsFTPd

```
ubuntu@ip-172-31-45-175:~$ sudo apt-get update
Fetched 4786 kB in 5s (1013 kB/s)
Reading package lists... Done
ubuntu@ip-172-31-45-175:~$ sudo apt-get install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
vsftpd is already the newest version (3.0.5-0ubuntu3).
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
ubuntu@ip-172-31-45-175:~$ sudo apt install vim -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
vim is already the newest version (2:9.1.0016-lubuntu7.3).
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
ubuntu@ip-172-31-45-175:~$ sudo apt install nano -y
E: Invalid operation instal
ubuntu@ip-172-31-45-175:~$ sudo apt install -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
ubuntu@ip-172-31-45-175:~$ sudo apt install traceroute -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
traceroute is already the newest version (1:2.1.5-1).
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
ubuntu@ip-172-31-45-175:~$ sudo apt install net-tools -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
net-tools is already the newest version (2.18-0.lubuntu4).
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
ubuntu@ip-172-31-45-175:~$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.original
ubuntu@ip-172-31-45-175:~$ sudo ufw status
Status: active

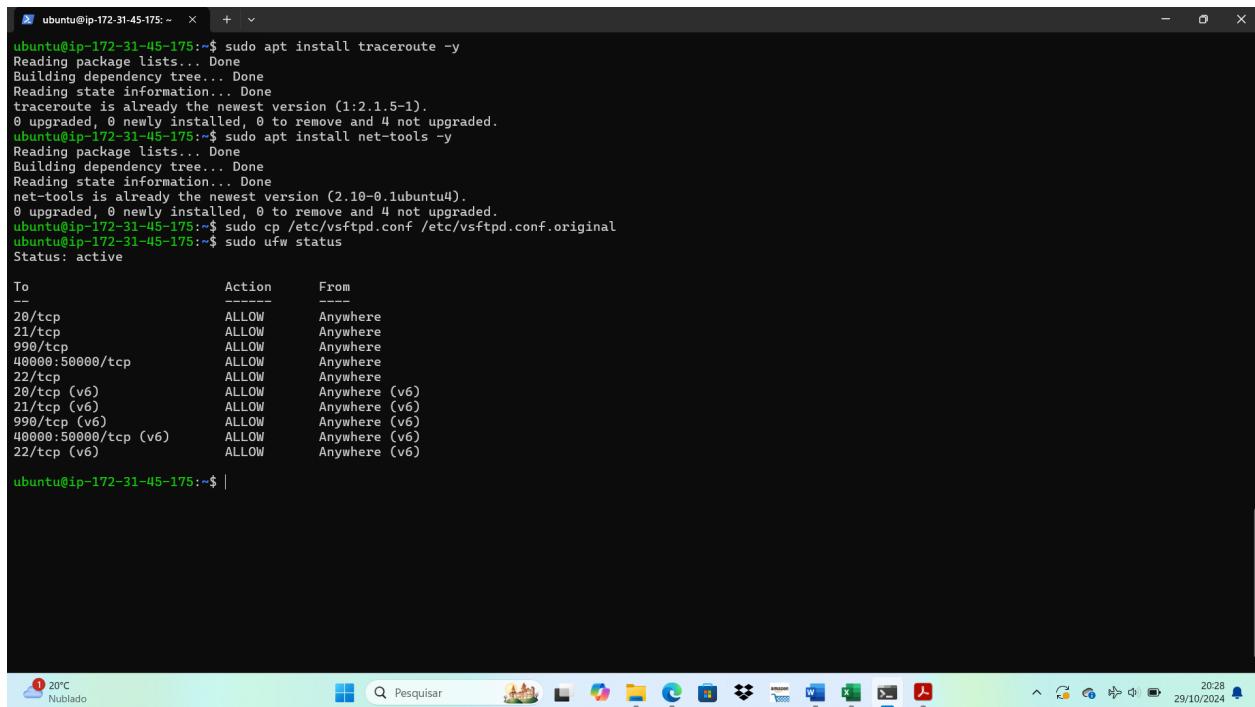
To                         Action      From
--                         --          --
20/tcp                     ALLOW       Anywhere
21/tcp                     ALLOW       Anywhere

20°C
Nublado
20:26
29/10/2024
```

- Configuração do Firewall

A figura 10 mostra o processo de configuração do firewall para permitir o tráfego de FTP no servidor. A partir do terminal, podemos ver a execução de comandos utilizando *ufw*, o firewall padrão para sistemas Ubuntu, que está ativo e configurado para permitir conexões nas portas específicas para FTP (20/tcp e 21/tcp) e outras portas necessárias para a comunicação de dados. As regras configuradas estabelecem permissões para tráfego tanto para IPv4 quanto para IPv6, abrangendo as conexões de controle de dados. Esta configuração é essencial para garantir que o servidor FTP possa receber e responder às requisições externas de forma segura, sem bloquear o tráfego legítimo necessário para o funcionamento do serviço FTP.

Figura 10: Permitindo Tráfego FTP do firewall



A screenshot of a Windows desktop environment. At the top is a black terminal window titled 'ubuntu@ip-172-31-45-175: ~'. The window contains a series of terminal commands and their outputs:

```
ubuntu@ip-172-31-45-175:~$ sudo apt install traceroute
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
traceroute is already the newest version (1:2.1.5-1).
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
ubuntu@ip-172-31-45-175:~$ sudo apt install net-tools -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
net-tools is already the newest version (2.10-0.lubuntu4).
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
ubuntu@ip-172-31-45-175:~$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.original
ubuntu@ip-172-31-45-175:~$ sudo ufw status
Status: active

To                         Action      From
--                         --          --
20/tcp                      ALLOW      Anywhere
21/tcp                      ALLOW      Anywhere
990/tcp                     ALLOW      Anywhere
40000:50000/tcp             ALLOW      Anywhere
22/tcp                      ALLOW      Anywhere
20/tcp (v6)                  ALLOW      Anywhere (v6)
21/tcp (v6)                  ALLOW      Anywhere (v6)
990/tcp (v6)                ALLOW      Anywhere (v6)
40000:50000/tcp (v6)        ALLOW      Anywhere (v6)
22/tcp (v6)                  ALLOW      Anywhere (v6)

ubuntu@ip-172-31-45-175:~$ |
```

The desktop taskbar at the bottom shows various icons for system notifications, weather (20°C, Nublado), search, and other applications.

- Criação do Diretório

A Figura 11 apresenta o processo de criação do diretório para um usuário no servidor FTP. Nesta sequência de comandos, observa-se a criação de um diretório específico para armazenar os arquivos FTP do usuário, em um caminho definido como /home/any/ftp/files. Após garantir que o diretório existe, um arquivo de exemplo (sample.txt) é criado dentro dele para verificar a funcionalidade de upload e download no servidor FTP. A configuração desse diretório e o uso de permissões adequadas são passos importantes para organizar o espaço de armazenamento e assegurar que o usuário tenha acesso aos arquivos necessários sem comprometer a segurança do sistema.

Figura 11 - Criando o diretório do usuário

The screenshot shows a Windows terminal window with a blue title bar. The title bar displays the path "ubuntu@ip-172-31-45-175: ~" and the window number "+ 1". The main area of the window contains a command-line session:

```
990/tcp          ALLOW      Anywhere
40000:50000/tcp ALLOW      Anywhere
22/tcp          ALLOW      Anywhere
20/tcp (v6)      ALLOW      Anywhere (v6)
21/tcp (v6)      ALLOW      Anywhere (v6)
990/tcp (v6)    ALLOW      Anywhere (v6)
40000:50000/tcp (v6) ALLOW      Anywhere (v6)
22/tcp (v6)      ALLOW      Anywhere (v6)

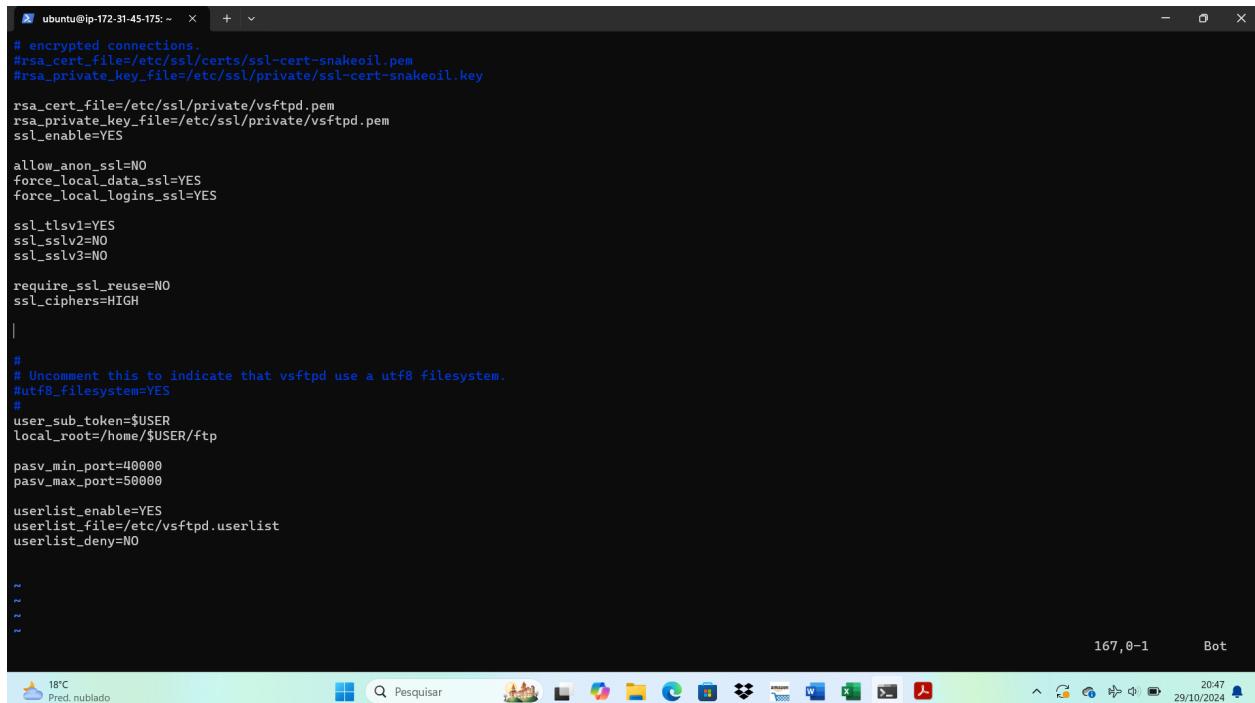
ubuntu@ip-172-31-45-175:~$ [200~sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.bkp~
[200~sudo: command not found
ubuntu@ip-172-31-45-175:~$ sudo useradd any
useradd: user 'any' already exists
ubuntu@ip-172-31-45-175:~$ sudo passwd any
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-45-175:~$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.bkp
ubuntu@ip-172-31-45-175:~$ sudo vim /etc/vsftpd.conf
ubuntu@ip-172-31-45-175:~$ sudo mkdir /home/any/ftp
mkdir: cannot create directory '/home/any/ftp': File exists
ubuntu@ip-172-31-45-175:~$ sudo chown nobody:nogroup /home/any/ftp
ubuntu@ip-172-31-45-175:~$ sudo chmod a-w /home/any/ftp
ubuntu@ip-172-31-45-175:~$ sudo ls -la /home/any/ftp
total 12
dr-xr-xr-x 3 nobody nogroup 4096 Oct 20 18:23 .
drwxr-xr-x 4 root root 4096 Oct 20 18:17 ..
drwxr-xr-x 2 any any 4096 Oct 20 20:59 files
-rw-r--r-- 1 root root 0 Oct 20 19:51 teste.txt
ubuntu@ip-172-31-45-175:~$ sudo mkdir /home/any/ftp/files
mkdir: cannot create directory '/home/any/ftp/files': File exists
ubuntu@ip-172-31-45-175:~$ sudo chown any:any /home/any/ftp/files
ubuntu@ip-172-31-45-175:~$ echo "vsftpd sample file" | sudo tee /home/any/ftp/files/sample.txt
vsftpd sample file
ubuntu@ip-172-31-45-175:~$ |
```

The taskbar at the bottom of the window shows the date and time as "29/10/2024 20:42".

- Configuração do Servidor

A Figura 12 mostra a configuração do servidor FTP vsftpd para habilitar conexões seguras e definir diversas opções de segurança. Nesta configuração, as linhas configuram certificados SSL para criptografar a conexão, usando caminhos específicos para o certificado e a chave privada. A opção `ssl_enable=YES` ativa o SSL, enquanto parâmetros como `force_local_data_ssl=YES` e `force_local_logins_ssl=YES` garantem que todos os dados e logins sejam transmitidos com segurança. A configuração também inclui os detalhes de compatibilidade de codificação e o limite de portas para conexões passivas (`pasv_min_port=30000` e `pasv_max_port=30000`). Essas medidas de segurança são fundamentais para proteger a transferência de dados sensíveis através do FTP, prevenindo acessos não autorizados e interceptações de dados.

Figura 12 - Configurando o vsftpd



```
# encrypted connections
#rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
#rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key

rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES

allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES

ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO

require_ssl_reuse=NO
ssl_ciphers=HIGH

#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
#
user_sub_token=$USER
local_root=/home/$USER/ftp

pasv_min_port=40000
pasv_max_port=50000

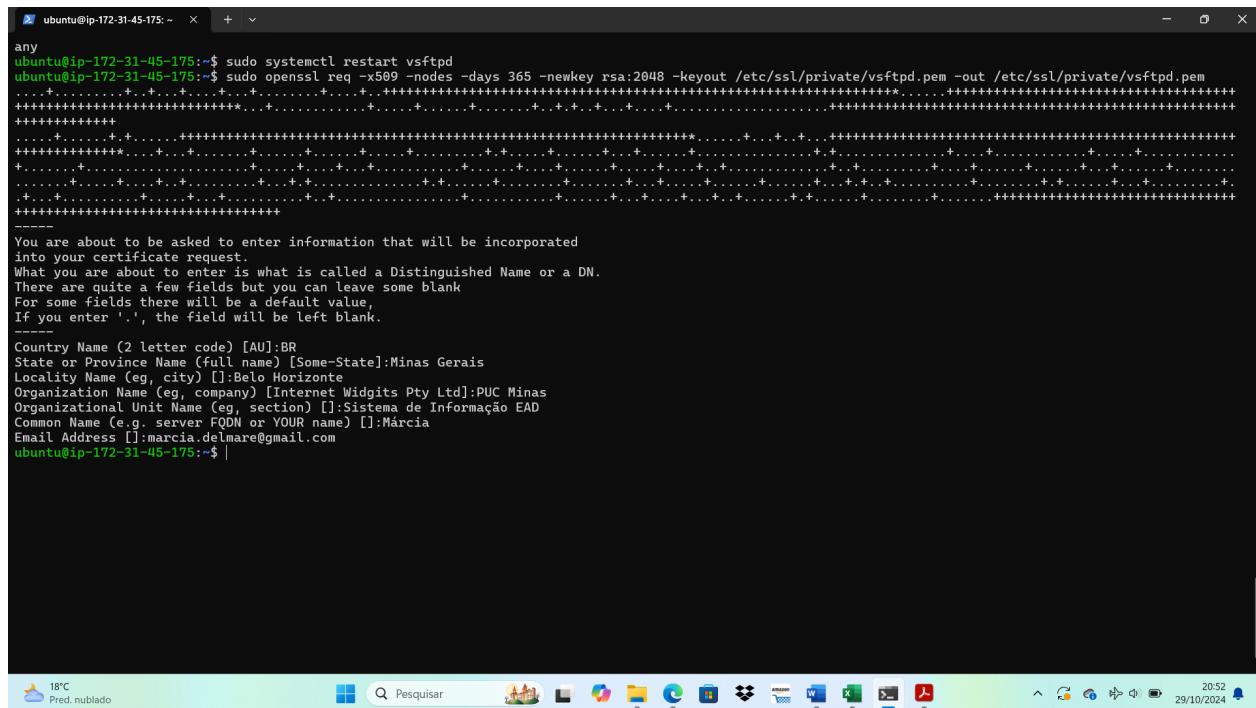
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO

~
~
~
```

- Criando o Certificado de Segurança

A Figura 13 ilustra o processo de criação de um certificado de segurança para o servidor FTP usando o comando openssl. Esse comando gera um certificado autofirmado com criptografia RSA de 2048 bits, que é válido por 365 dias. Durante o processo, informações como país, estado, cidade, nome da organização e endereço de e-mail são solicitadas para preencher o conteúdo do certificado. Esse certificado será usado para habilitar conexões seguras no vsftpd, permitindo que os dados transmitidos entre o cliente e o servidor sejam criptografados, o que é essencial para proteger informações sensíveis contra interceptações.

Figura 13 - Criando o certificado de Segurança



The screenshot shows a terminal window on an Ubuntu system. The command entered is:

```
any
ubuntu@ip-172-31-45-175:~$ sudo systemctl restart vsftpd
ubuntu@ip-172-31-45-175:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem
```

Followed by a series of asterisks (*). The terminal then prompts for certificate information:

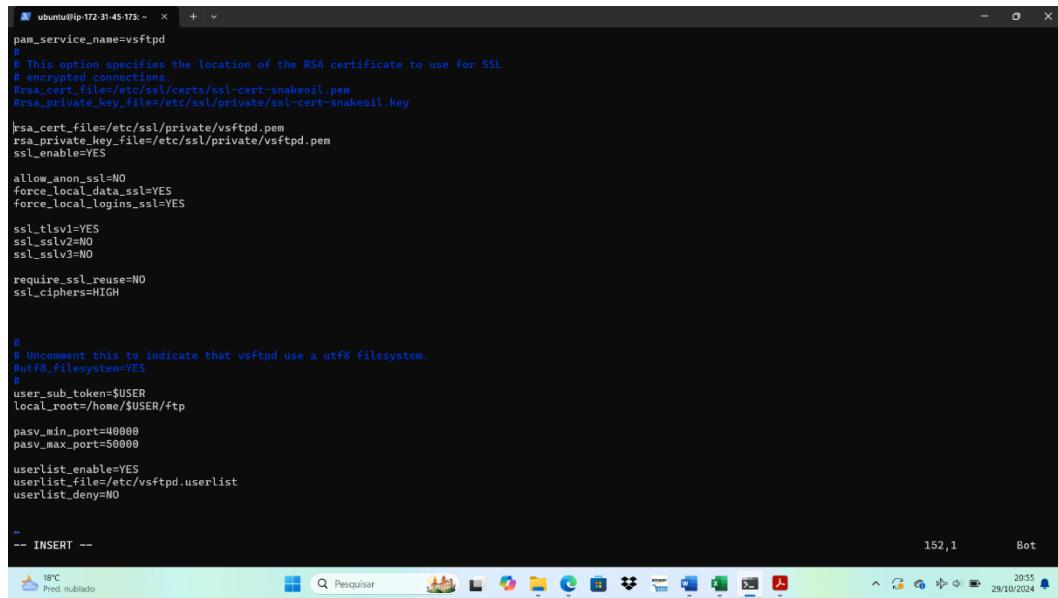
```
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [AU]:BR  
State or Province Name (full name) [Some-State]:Minas Gerais  
Locality Name (eg, city) []:Belo Horizonte  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PUC Minas  
Organizational Unit Name (eg, section) []:Sistema de Informação EAD  
Common Name (e.g. server FQDN or YOUR name) []:Marcia  
Email Address []:marcia.delmare@gmail.com
```

The command `ubuntu@ip-172-31-45-175:~$` is shown at the bottom.

- Configurando e Habilitando o certificado de segurança

A Figura 14 mostra a configuração do servidor vsftpd para habilitar o certificado de segurança TLS/SSL, essencial para conexões seguras. O arquivo de configuração especifica o caminho do certificado e da chave privada criados previamente, e o parâmetro `ssl_enable=YES` ativa o suporte para conexões SSL/TLS. Com opções como `force_local_data_ssl=YES` e `force_local_logins_ssl=YES`, o servidor exige que todos os dados e logins utilizem SSL, reforçando a segurança da transmissão de dados. Outras configurações definem detalhes de codificação e compatibilidade, além de limitar o intervalo de portas para conexões passivas. Essa configuração protege a comunicação no FTP contra acessos não autorizados e garante a integridade dos dados.

Figura 14 - Configurando e habilitando o certificado de Segurança TLS/SSL



```
ubuntu@ip-172-31-45-175: ~ + pam_service_name=vsftpd
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
#rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
#rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES

allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES

ssl_tlsv1=YES
ssl_tlsv2=NO
ssl_sslv3=NO

require_ssl_reuse=NO
ssl_ciphers=HIGH

#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
#
user_sub_token=$USER
local_root=/home/$USER/ftp

pasv_min_port=40000
pasv_max_port=50000

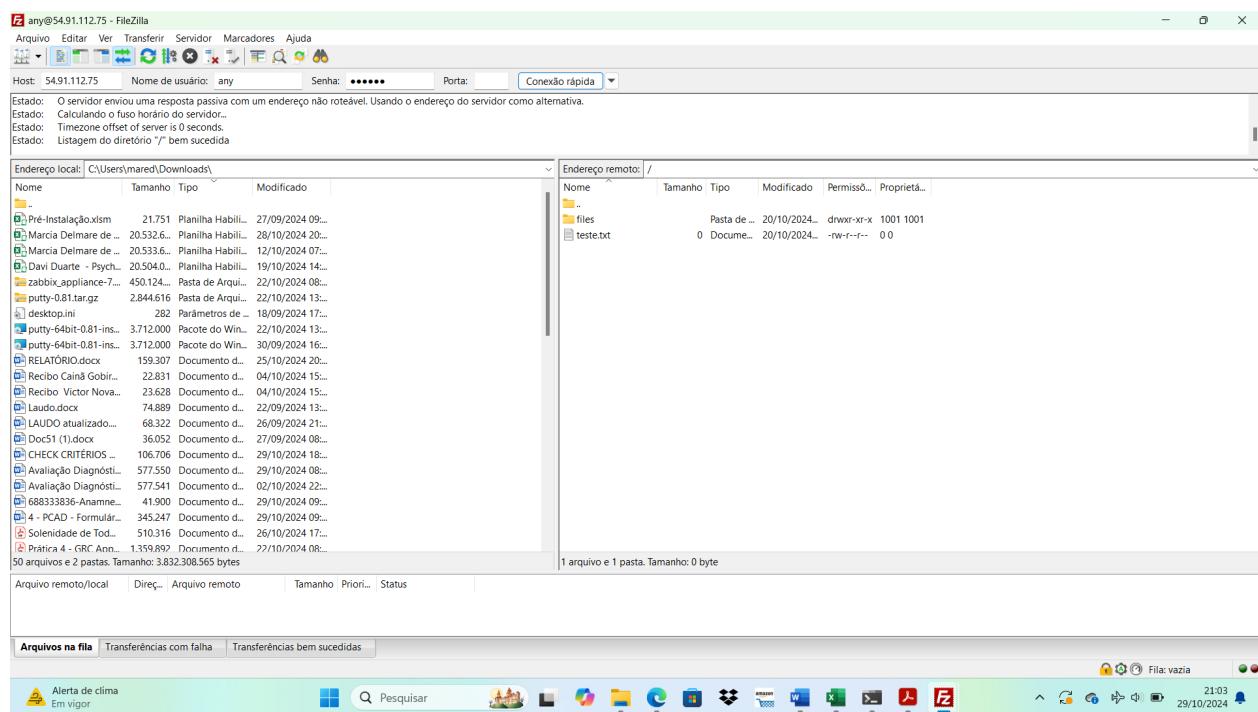
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO

-- INSERT --
```

- Teste de conexão com o servidor FTP

A Figura 15 ilustra o teste de conexão com o servidor FTP utilizando o software FileZilla. Nesta interface é possível observar que o cliente FileZilla se conecta ao servidor FTP pelo endereço IP especificado e exibe os arquivos e diretórios disponíveis para o usuário. Na seção à direita, o diretório remoto *files* e o arquivo *sample.txt* podem ser visualizados indicando que a configuração do servidor e a criação de diretórios foram realizadas com sucesso. Esse teste é fundamental para verificar se o servidor FTP responde corretamente às conexões e se os usuários conseguem acessar e gerenciar arquivos conforme o esperado, garantindo a funcionalidade do serviço de transferência de arquivos.

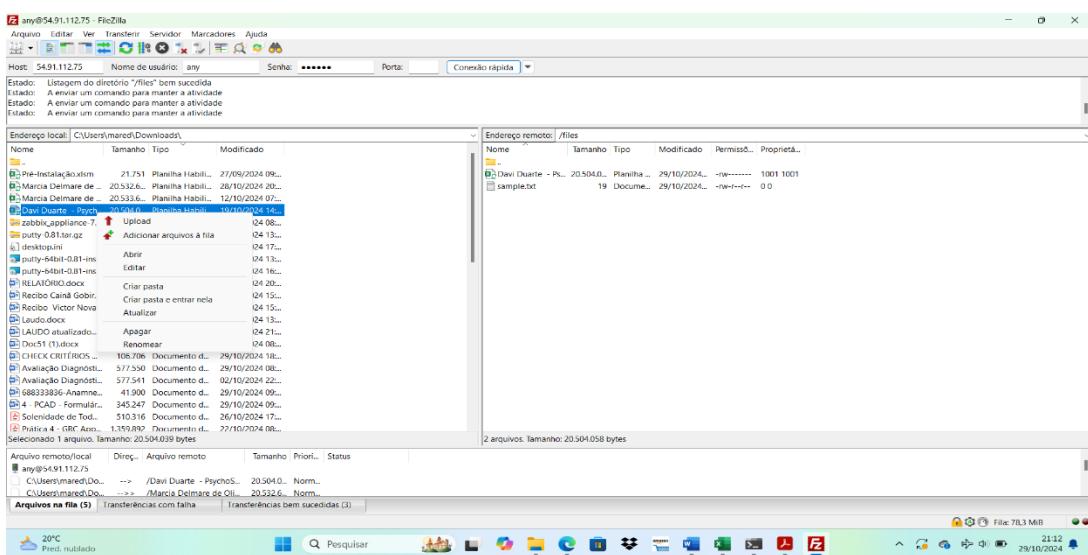
Figura 15 – Testando conexões com o filezilla



- Upload de arquivos para o servidor FTP

A Figura 16 apresenta o processo de upload de arquivos para o servidor FTP utilizando o FileZilla. Na tela, observa-se que o usuário selecionou um arquivo na área local (lado esquerdo) e o transferiu para o diretório remoto files (lado direito), onde já se encontra o arquivo sample.txt. O status de transferência indica que o envio foi realizado com sucesso, confirmando que o servidor FTP está configurado corretamente para receber uploads. Esse teste de upload é essencial para verificar a capacidade do servidor de aceitar arquivos de clientes remotos, garantindo a funcionalidade e a confiabilidade do serviço de FTP para transferências de dados.

Figura 16 - upload de arquivos

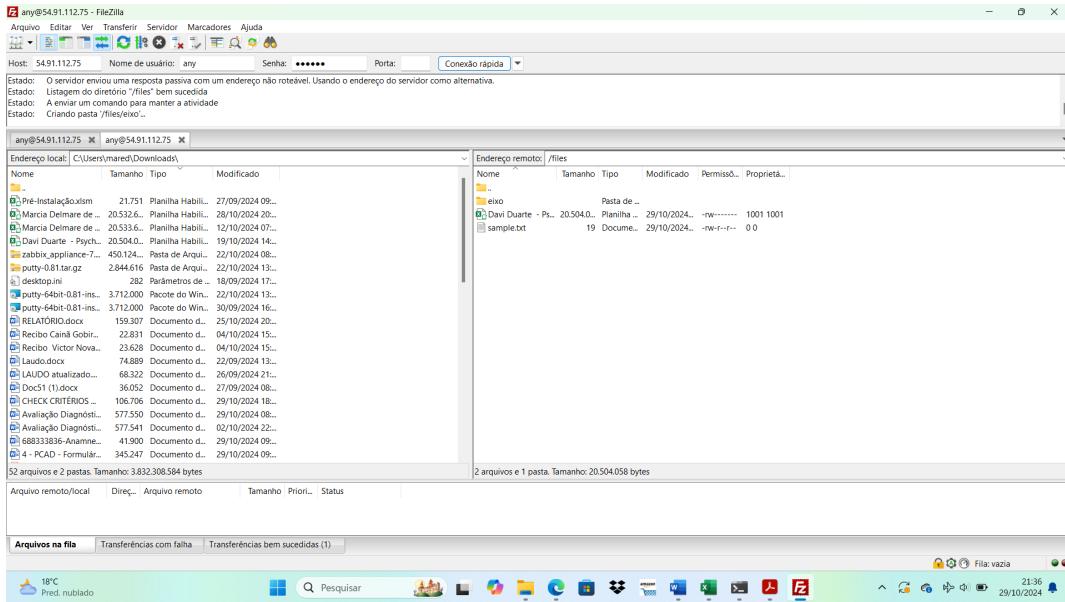


- Criação de pastas

A Figura 17 ilustra o processo de criação de pastas no servidor FTP usando o FileZilla.

Na interface, observa-se que o usuário criou uma pasta denominada *Dani Duarte* no diretório remoto *files*. Esse procedimento demonstra a funcionalidade do servidor FTP em permitir que usuários organizem arquivos e pastas de acordo com suas necessidades no ambiente remoto. A criação de diretórios é essencial para estruturar o armazenamento de dados e facilitar o acesso e a organização de arquivos, especialmente em ambientes colaborativos onde múltiplos usuários podem estar acessando o servidor FTP simultaneamente.

Figura 17 - Criando pastas



2.1.2 Endereços dos servidores hospedados em nuvem

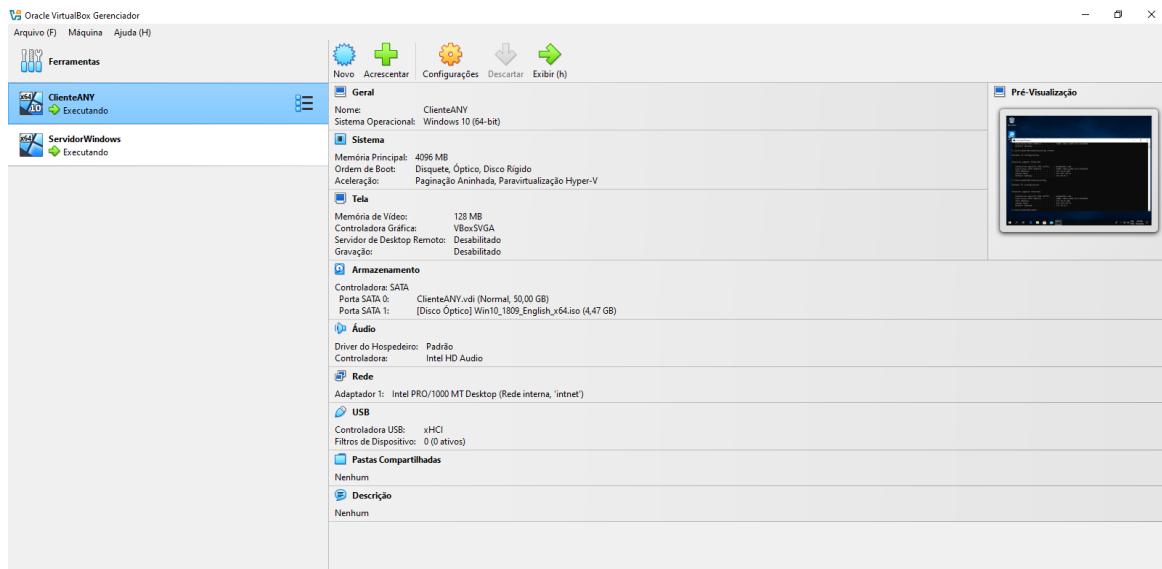
SERVIDOR	NOME/MAQUINA	IP/HOST	USUÁRIO DE ACESSO
DNS	Route 53		-
Email	WEBMAIL	3.223.106.189	ubuntu
WEB	WEB	3.214.158.62	ubuntu
FTP	Srv Ubuntu	54.91.112.75	ubuntu
Database	mail (RDS)	mail.cev6qaqwsbkq.us-east-1.rds.amazonaws.com	admin

2.2 Servidores instalados on-premise

Para o mapeamento e implantação dos serviços *on-premise*, foi utilizado o Virtualizador de Sistemas Operacionais Oracle VirtualBox. A virtualização local é o processo de criar um ambiente de computação simulado em um computador. Isso permite que um único computador execute múltiplos sistemas operacionais ou aplicativos de forma independente.

Active Directory (AD) é um serviço de diretório desenvolvido pela Microsoft que fornece um local centralizado para gerenciar e organizar recursos em um ambiente de rede. Serve como um repositório para armazenar informações sobre contas de usuário, computadores, grupos e outros recursos de rede.

Figura 18 – Oracle virtualbox gerenciamento ClientANY



- Server Manager

As imagens abaixo mostram duas telas do Server Manager:

Na figura 19, temos a visão geral de *All Servers*, onde o servidor DC está listado com informações de endereço IPv4, status de gerenciamento (online) e eventos recentes, como erros e avisos de sistema. Esta visão permite ao administrador monitorar rapidamente o estado e os alertas de todos os servidores de forma eficiente.

Figura 19 – exibição de todos os servidores

The screenshot shows the Windows Server Manager interface. The left sidebar has a 'Local Server' section selected. The main area displays two tables: 'SOURCES' and 'EVENTS'. The 'SOURCES' table lists one server named 'DC' with IP '10.0.2.15,172.16.0.1'. The 'EVENTS' table lists several system events, including errors and warnings related to the disk.

Server Name	ID	Severity	Source	Log	Date and Time
DC	6008	Error	EventLog	System	10/20/2024 7:45:53 PM
DC	34	Warning	disk	System	10/20/2024 7:45:52 PM
DC	34	Warning	disk	System	10/20/2024 7:45:52 PM
DC	34	Warning	disk	System	10/20/2024 7:45:52 PM
DC	41	Critical	Microsoft-Windows-Kernel-Power	System	10/20/2024 7:45:50 PM
DC	6008	Error	EventLog	System	10/20/2024 4:21:50 PM
DC	34	Warning	disk	System	10/20/2024 4:21:48 PM

A figura 20 exibe a seção *Local Server*, que fornece detalhes específicos sobre o

The screenshot shows the Windows Server Manager interface with the 'Local Server' section selected. The main area displays a 'PROPERTIES' table for the local computer 'DC'. It shows details like computer name, domain, firewall status, operating system version, and hardware information.

Computer name	DC	Last installed updates	Never
Domain	anymalhas.com	Windows Update	Downloaded
		Last checked for updates	Today at
Microsoft Defender Firewall	Public: On	Microsoft Defender Antivirus	Real-Time
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) (00454-00)
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	
interna	172.16.0.1, IPv6 enabled		
Operating system version	Microsoft Windows Server 2022 Standard Evaluation	Processors	AMD Ryzen
Hardware information	innoteck GmbH VirtualBox	Installed memory (RAM)	4 GB

servidor DC. Nesta seção, podemos ver propriedades de configuração, como o nome do computador, grupo de trabalho, status do firewall, endereços IP e informações sobre atualizações e segurança. Esse painel é útil para ajustes detalhados e configurações específicas no servidor local, permitindo um controle mais aprofundado sobre seu funcionamento e segurança.

Figura 20 – exibição do servidor local

- Gerenciamento de contas de usuários e computadores

As imagens seguintes mostram o console "Active Directory Users and Computers", utilizado para gerenciar contas de usuários e computadores dentro de um domínio:

Na figura 21 vemos a estrutura do domínio *anymalhas.com*, onde o usuário "*Davi Coelho*" está registrado na unidade organizacional "*Departamento de TI*". Esta visualização permite o gerenciamento de permissões e políticas de segurança aplicadas aos usuários.

Figura 21 – exibição do usuário registrado

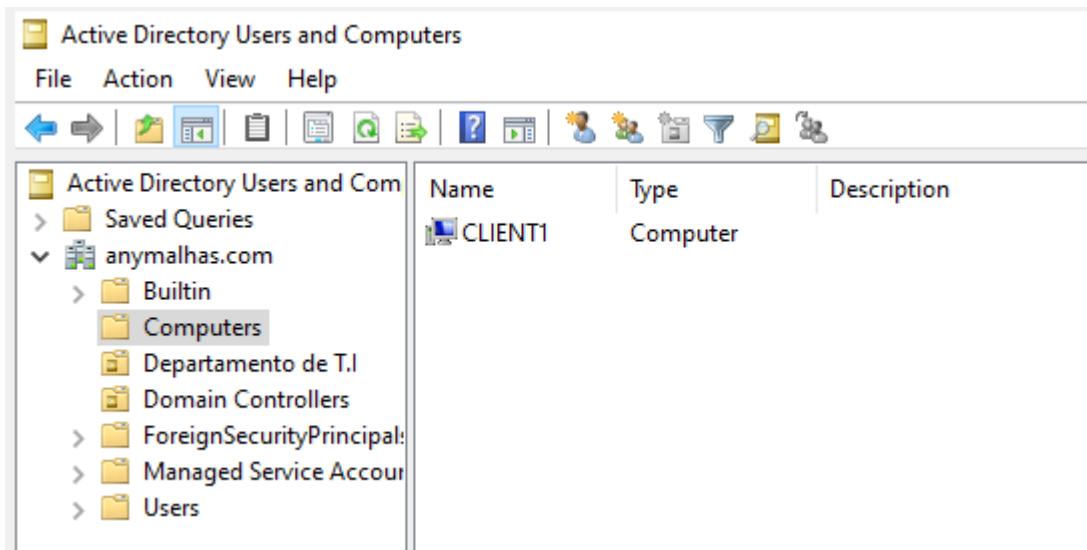
The screenshot shows the Windows Server Management Console window titled "Active Directory Users and Computers". The left pane displays the navigation tree for the domain "anymalhas.com", with the "Computers" container expanded to show "Departamento de TI" which is selected. The right pane lists users with a single entry: "Davi Coelho" (User). The interface includes a toolbar with various icons and a menu bar with "File", "Action", "View", and "Help".

Name	Type	Description
Davi Coelho	User	

A figura 22 exibe um computador chamado "CLIENT1", também registrado no domínio.

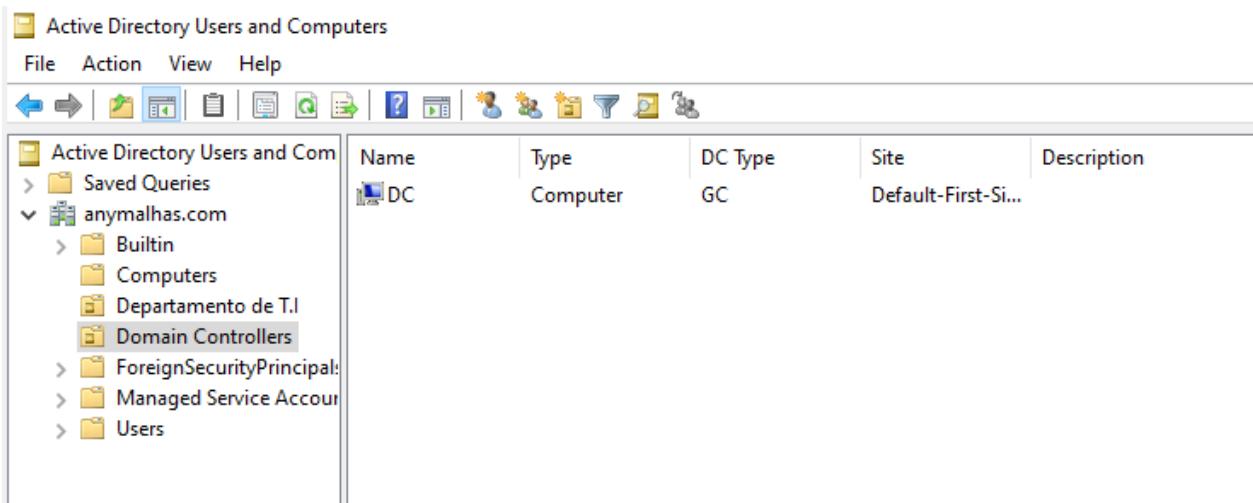
Esta configuração permite ao administrador gerenciar o acesso e as políticas aplicáveis a este dispositivo específico:

Figura 22 – exibição do registro de computadores no domínio



Na figura 23, o servidor "DC" (Controlador de Domínio) está listado sob "Domain Controllers". Ele possui o tipo "GC" (Global Catalog), o que significa que ele contém uma cópia parcial de todos os objetos do Active Directory, facilitando buscas e login de usuários em redes grandes. O gerenciamento através do Active Directory centraliza o controle sobre usuários e dispositivos:

Figura 23 – exibição do controlador de domínio



- DNS Manager e o Group Policy Management.

Em seguida, as imagens mostram duas ferramentas de gerenciamento de rede: o DNS Manager e o Group Policy Management:

Na figura 24, o DNS Manager exibe a configuração de zonas de pesquisa direta para o domínio *anymalhas.com*. Vemos várias entradas de registros, incluindo o registro de Autoridade de Origem (SOA), registros de servidor de nomes (NS) e registros de host (A e AAAA) para dispositivos como "CLIENT1" e "dc". Estes registros são essenciais para a resolução de nomes, permitindo que dispositivos no domínio localizem outros recursos pela rede através de nomes amigáveis, em vez de endereços IP:

Figura 24 – configuração de zonas de pesquisa

A figura 25 apresenta o console de Group Policy Management com uma política configurada para "Bloquear painel de controle". Esta política, aplicada ao domínio

anymalhas.com, restringe o acesso ao painel de controle dos usuários, o que é uma prática comum para aumentar a segurança e evitar alterações indesejadas nas configurações do sistema. A configuração "Prohibit access to Control Panel and PC settings" está habilitada, limitando o controle dos usuários sobre essas áreas. Esse gerenciamento centralizado de políticas facilita a aplicação de restrições e configurações de segurança de forma consistente em toda a rede:

Figura 25 - console de Group Policy Management

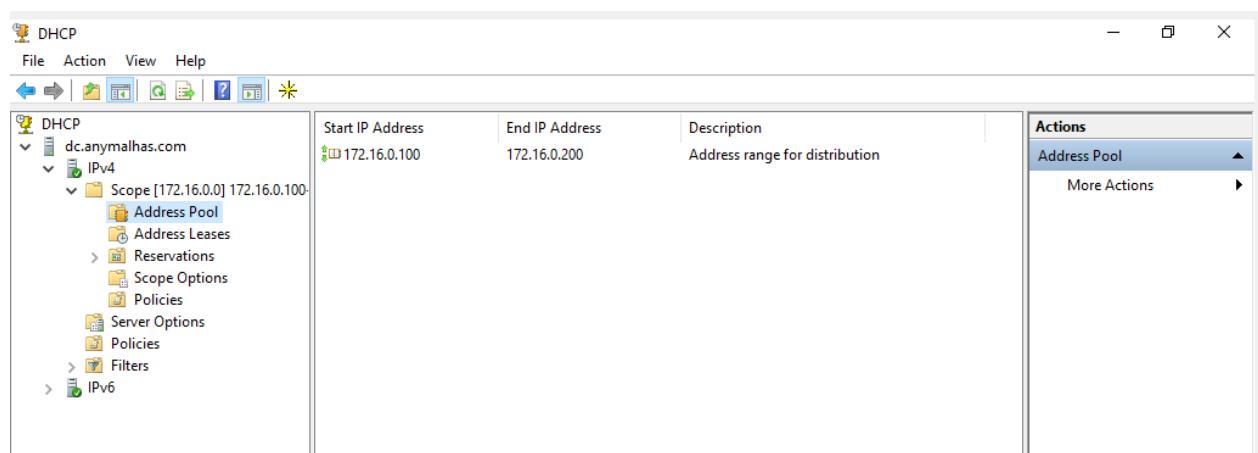
▫ **DHCP**

Um servidor DHCP (Dynamic Host Configuration Protocol) é responsável por atribuir automaticamente endereços IP e outras configurações de rede a dispositivos conectados. Isso elimina a necessidade de configuração manual de cada dispositivo, facilitando a administração da rede e garantindo que não haja conflitos de endereços IP.

As imagens mostram o console de gerenciamento do DHCP para o domínio *anymalhas.com*.

Na figura 26, vemos a configuração do escopo do DHCP, que define uma faixa de endereços IP, de 172.16.0.100 a 172.16.0.200, destinada à distribuição automática de endereços IP para dispositivos na rede. Esta faixa é configurada para facilitar a atribuição dinâmica de IPs, garantindo que cada dispositivo receba um endereço válido dentro do intervalo especificado sem a necessidade de configuração manual.

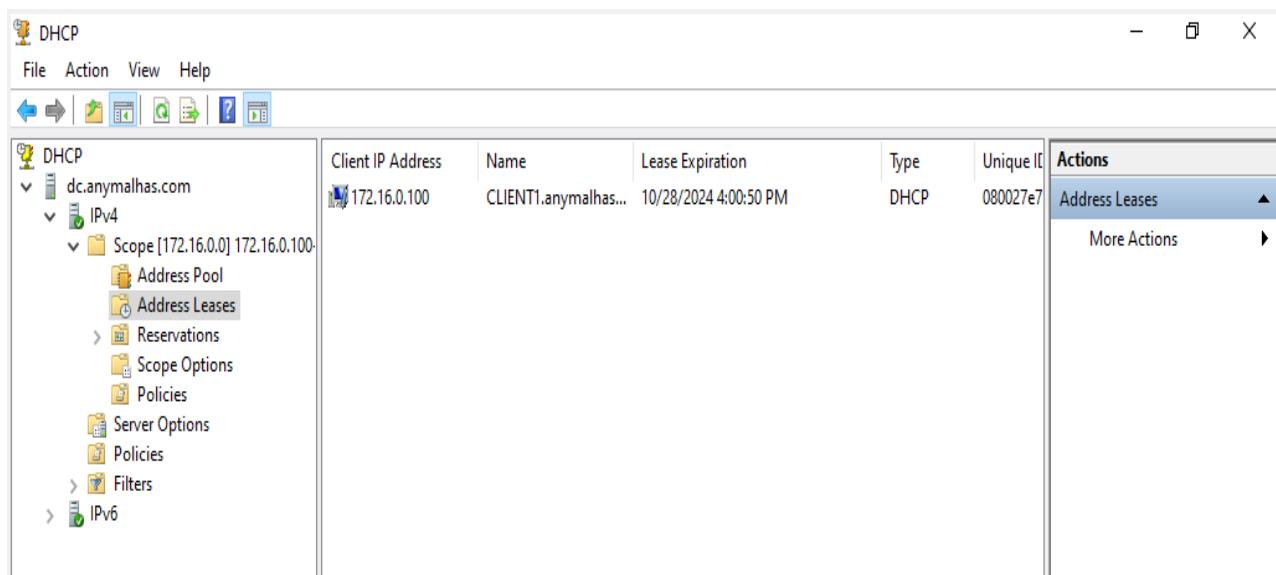
Figura 26 - configuração do escopo do DHCP



A figura 27 exibe uma concessão de IP ativa, onde o dispositivo "CLIENT1" recebeu o

endereço 172.16.0.100 com uma data de expiração do lease. Esta concessão permite que o dispositivo mantenha o IP por um período específico antes que o servidor DHCP precise renová-lo. O uso do DHCP automatiza o gerenciamento de endereços IP na rede, reduzindo o trabalho manual e minimizando erros na configuração de rede.

Figura 27 – concessão de IP



3. MONITORAMENTO

O monitoramento de redes são processos que envolvem a supervisão de uma rede de computadores, com o objetivo de garantir o funcionamento adequado de seus componentes:

Estratégia de segurança cibernética: permite identificar e resolver problemas na rede, como falhas e interrupções que podem afetar o desempenho e a disponibilidade.

Monitoramento de redes: é uma etapa do gerenciamento de redes, e é realizado por meio de protocolos como o SNMP (Protocolo simples de gerenciamento de rede), ICMP (Protocolo de mensagens de controle da Internet) e WMI (Instrumentação de gerenciamento do Windows).

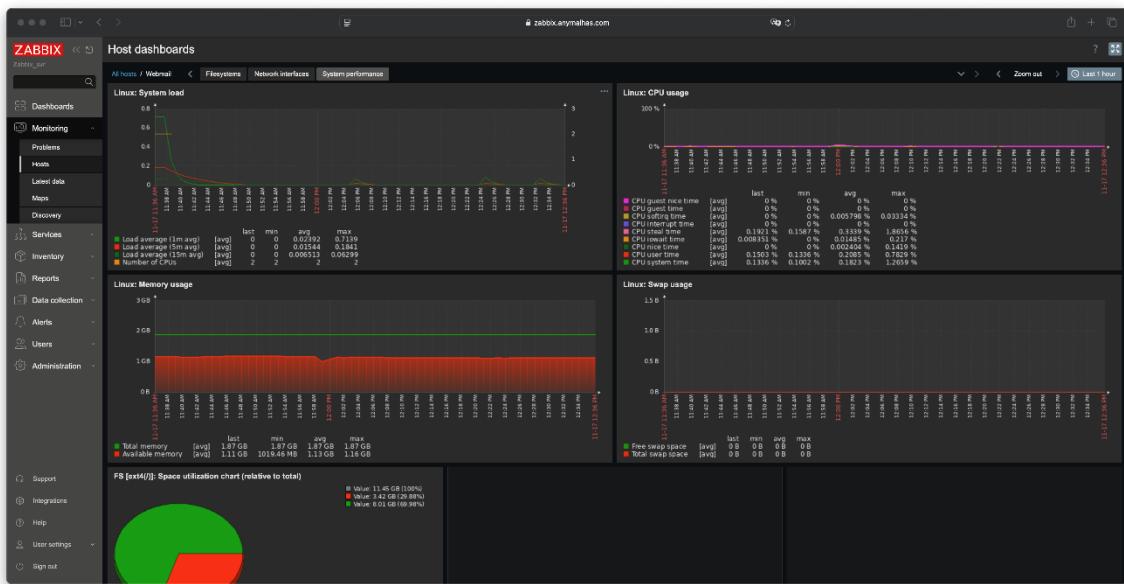
3.1 Monitoramento dos servidores *on cloud*

Para monitorar as máquinas que estão em nuvem foi instanciada uma nova máquina com sistema operacional Ubuntu na versão 22.4 e nela instalado o zabbix na sua última versão (7.0.5) disponível. Esta é responsável por monitorar as outras instâncias onde estão instalados os serviços de E-mail, Web e FTP através do zabbix-Agent instalado nas máquinas.

3.1.1 Webmail

Para garantir o funcionamento dos serviços é possível acompanhar o estado da máquina, onde está o servidor de e-mail, e agir em tempo hábil diante de qualquer anomalia que vier a surgir. A seguir na Figura 28 a captura do painel web do Zabbix exibindo o dashboard de monitoramento do host de webmail.

Figura 28 – Captura contendo host dashboard Zabbix



3.1.2 Webserver

Seguindo as mesmas premissas do webmail a seguir podemos ver uma captura do host webserver na Figura 29. A imagem exibe o dashboard do Zabbix, uma ferramenta de monitoramento de desempenho, destacando métricas relacionadas ao sistema de discos do host. As seções apresentadas incluem taxas de leitura e gravação do disco, tempo médio de espera das requisições e a utilização do disco, incluindo filas de processamento. Esses gráficos fornecem uma visão em tempo real da saúde e eficiência do armazenamento, permitindo identificar gargalos ou picos de utilização que possam impactar a performance geral do sistema.



Figura 29 – Captura contendo host dashboard Zabbix

3.1.3 FTP

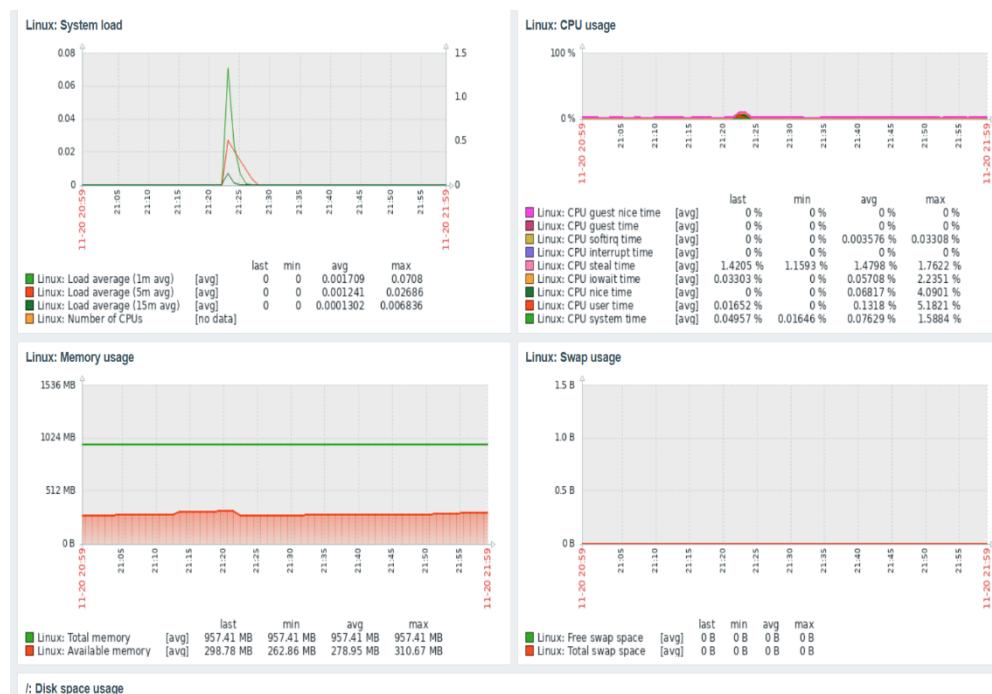
Em seguida, temos a captura do painel do Zabbix, exibindo o gráfico de monitoramento do host FTP. Este gráfico mostra picos esporádicos no tempo de CPU softirq, com uma média de 0,00351% e um máximo de 0,0311%. Mostra também flutuações no tempo de CPU steal, variando entre aproximadamente 0,8% e 1,8%. Esses gráficos são úteis para monitorar e analisar o desempenho da CPU e a alocação de recursos para o processo FTP em um sistema Linux, como o uso de memória e espaço em disco. Triggers são configuradas para alertar quando essas métricas atingem certos limiares.

Figura 30 – Captura contendo host graph Zabbix do servidor FTP



Temos também na próxima captura o dashboard do host FTP zabbix, exibindo métricas importantes para garantir que o serviço esteja funcionando corretamente. Esses elementos são apresentados em widgets que podem ser personalizados e organizados conforme necessário.

Figura 31: Dashboard host FTP Zabbix



3.2 Monitoramento dos servidores locais

Para monitorar os servidores locais foi instanciada uma nova máquina com sistema operacional Red hat e nela instalado o zabbix na sua última versão (7.0.5) disponível, esta é responsável por monitorar a instância do servidor AD/DNS.

3.2.1 Servidor AD/DNS

Podemos ver uma captura do host do servidor AD/DNS na Figura 32 e Figura 33.

As imagens exibem os dashboards do Zabbix, contendo métricas de desempenho do sistema de discos do host, como taxas de leitura e gravação, tempo médio de espera e utilização, incluindo filas de processamento. Esses gráficos oferecem uma visão em tempo real da eficiência do armazenamento, ajudando a identificar gargalos ou picos que possam afetar a performance do sistema.

Figura 32 – Captura contendo host dashboard Zabbix do servidor AD/DNS

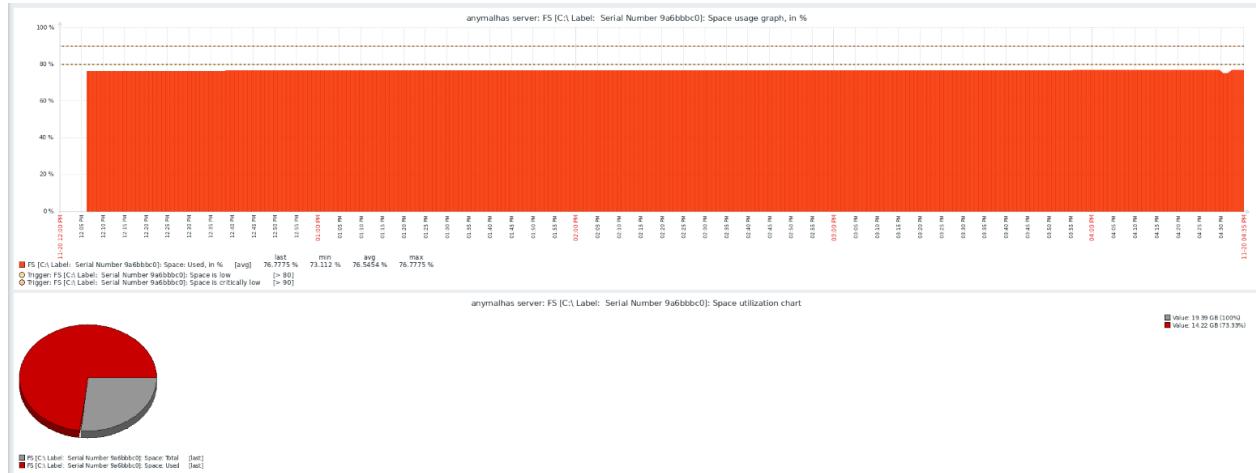
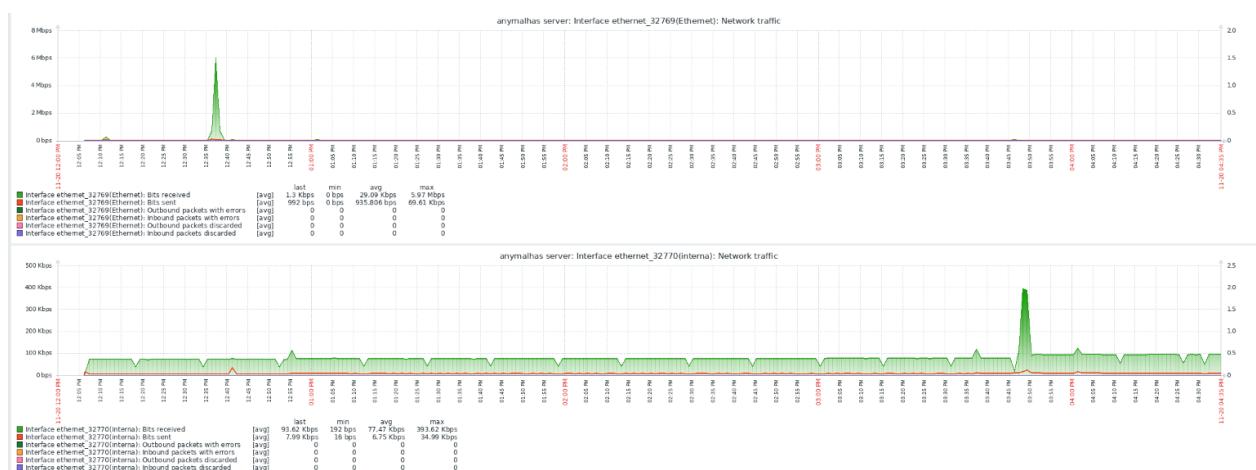


Figura 33 – Captura contendo host dashboard Zabbix do servidor AD/DNS



4. SEGURANÇA

4.1 Política de segurança da informação (PSI)

A Política de Segurança da Informação (PSI) é um documento estratégico que estabelece diretrizes e controles fundamentais para proteger os ativos de informação, garantindo a confidencialidade, integridade e disponibilidade dos dados. Na Anymalhas, foi elaborada uma PSI abrangente, com o objetivo de instituir normas claras e práticas seguras que promovam a proteção de informações sensíveis, sistemas corporativos e dispositivos utilizados nas operações da empresa. O documento define regras específicas para controle de acesso, classificação de informações, uso seguro da internet, correio eletrônico, redes sem fio, dispositivos móveis e repositórios digitais. Além disso, a PSI detalha as responsabilidades atribuídas a todos os níveis da organização, incluindo colaboradores, gestores e terceiros, assegurando a aplicação efetiva das medidas de segurança e a conformidade com as legislações vigentes, como a LGPD.

4.2 Cartilha de Segurança

A Cartilha de Segurança para Internet é um documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças, verifique a seguir nas Figuras 34 e 35 a cartilha da Anymalhas.

Figura 34 – Reprodução de uma parte da Cartilha de segurança



A imagem mostra uma reprodução de uma parte da Cartilha de Segurança da Anymalhas. A parte visível inclui o logo da Anymalhas (uma silhueta de montanha), o título "Cartilha de segurança da informação", uma subseção "Senhas" com dicas sobre a criação e gerenciamento de senhas fortes, uma seção "Softwares" com dicas sobre a segurança de downloads, uma seção "E-mail" com dicas para evitar clica-bait e spam, e uma seção "Internet" com dicas para não usar redes públicas. O fundo da cartilha é escuro, com destaque para os tópicos e suas respectivas listas de recomendações.

Senhas

- Utilize senhas fortes, uma quantidade de no mínimo 12 caracteres combinando letras maiúsculas, minúsculas, números e caracteres especiais;
- Tenha senhas diferentes para contas distintas, principalmente para conta de e-mail principal que usa para se cadastrar em outros serviços;
- Mantenha as informações de recuperação de senhas sempre atualizadas;
- Não compartilhe suas senhas com ninguém;
- Evite anotar suas senhas, se tiver dificuldade de recordá-las utilize algum software específico para guardá-las protegidas por uma senha “mestre”;
- Ative o multifator de autenticação;

Softwares

- Baixe e instale softwares apenas de fornecedores conhecidos e verificados;
- Não utilize software pirata estes podem vir acompanhados de surpresas indesejáveis;
- Mantenha o antivírus sempre atualizado;

E-mail

- Não clique em links de remetentes desconhecidos;
- Marque mensagens suspeitas como spam/black list

Internet

Não utilize redes públicas (Wi-Fi em shoppings, aeroportos, etc.) caso haja necessidade

Figura 35 – Reprodução de outra parte da Cartilha de segurança

A imagem mostra uma cartilha de segurança dividida em três seções principais:

- Dispositivos Removíveis**: Descreve a importância de não utilizar mídias removíveis em computadores públicos e a necessidade de varredura com antivírus.
- Redes Sociais**: Fornecerá dicas para evitar a divulgação de informações confidenciais e citar a fonte de imagens.
- Informações Pessoais**: Orienta sobre a evitação de divulgar informações pessoais em sites desconhecidos e o uso seguro de HTTPS.
- Websites**: Dicas para inserir informações pessoais em sites e navegar com segurança.
- Sessões**: Recomenda não deixar sessões abertas em dispositivos de terceiros.
- Legislação**: Alerta para a importância de ficar atento às leis que regem a área.

O layout inclui ícones correspondentes a cada seção: uma lupa para Redes Sociais, um globo para Informações Pessoais, uma cadeado para Legislação e um QR code para acesso à política completa.

4.3 Vulnerabilidades

4.3.1 Ambiente on cloud

Com o crescimento e expansão dos negócios surge a necessidade de disponibilizar serviços na internet, tornando-os acessíveis em qualquer parte do globo. Em contrapartida, o novo ambiente está exposto a novos tipos de vulnerabilidades talvez não encontradas anteriormente. A seguir foram listadas as vulnerabilidades encontradas nos servidores hospedados em nuvem.

4.3.1.1 Webmail

A instância, na qual o webmail está instalado, está com a porta padrão (22) de SSH (Secure Shell) habilitada e exposta publicamente na internet sem nenhum tipo de filtro de IP. Algum conhecimento geral, falhas na aplicação poderiam ser exploradas para executar ataques. Uma alternativa seria substituir a porta usada por alguma outra não corriqueira para dificultar a ação de agentes mal-intencionados.

Este mesmo host também conta com serviços de SMTP e IMAP habilitados e com porta padrão exposta, sem nenhum tipo de filtro ou Proxy, estando sujeito a ataques de força bruta que poderiam causar sérios danos a reputação do negócio. Acessível também através da web, o painel do webmail não possui nenhuma proteção contra-ataques de força bruta ou negação.

4.3.1.2 Web Server

Além de compartilhar as mesmas vulnerabilidades relacionadas ao SSH presentes no item anterior, este importante serviço do negócio onde está hospedado o site da empresa, também não possui nenhuma proteção contra-ataques de negação (DDoS). Um ataque assim poderia deixar um dos principais meios de visibilidade e comunicação da empresa indisponível.

4.3.1.3 Monitoramento

Esta instancia possui o sistema de monitoramento Zabbix instalado, uma importante ferramenta para acompanhar a saúde dos outros serviços presentes no mesmo ambiente, porém foi detectado que a máquina possui também vulnerabilidade relacionada aos serviços de SSH e HTTP que ocorrem nas outras, acompanhando também esta ferramenta foi levantada uma nova vulnerabilidade nas demais maquinas, tendo em vista que para seu funcionamento, foi exposta uma nova porta sem nenhum tipo de filtro em todas as instancias monitoradas.

4.3.1.4 Database(RDS)

Um serviço fornecido pela AWS, mas com tipo de conexão arcaica feita através de senha e com a porta padrão exposto, um ataque de força bruta poderia indisponibilizar ou no pior dos casos conseguir acessar os dados contidos ali, acarretando graves prejuízos financeiros e de reputação para os negócios ao ter que responder questões relacionadas a LGPD (Lei geral de proteção de dados).

4.3.1.5 FTP

O servidor de FTP apresenta vulnerabilidades de segurança, como a suscetibilidade a ataques de força bruta, devido ao uso de conexões remotas que requerem autenticação por nome de usuário e senha. Além disso, este servidor também não apresenta proteção contra ataques de negação de serviço (DoS), podendo ser alvo de tais ataques que visam sobrecarregar o servidor e torná-lo indisponível.

4.3.2 Ambiente on-promise

Em um ambiente local (on-promise), os recursos são implantados internamente e na

infraestrutura de TI da empresa. A empresa é responsável por manter a solução e todos os seus processos relacionados. No entanto, esse tipo de ambiente, assim como o on cloud, pode apresentar várias vulnerabilidades como as que serão listadas adiante.

4.3.2.1 Active Directory e Servidor DNS

O servidor contém instalados e habilitados serviços de SNMP, porém conta com conexão aberta sem filtro. Em conjunto, a conexão pública da instância é um fator de risco para o sistema. O serviço pode ser acessado de qualquer endereço IP por padrão, um ataque remoto pode explorar o serviço SNMP.

Está sendo utilizada a versão SNMP 2.0, a qual utiliza strings que são enviadas em texto claro pela rede. Um invasor pode interceptar o tráfego de rede e obter acesso a informações.

Está configurado o uso da porta 161, porém sem firewalls para restringir o acesso à porta. Também não foi estabelecido limite de tráfego SNMP somente para a rede interna.

REFERENCIAIS

AMATO NETO, João. Manufatura Classe Mundial. São Paulo: Atlas, 2012. ISBN 978-85-224-6789-0.

SLACK, Nigel; CHAMBERS, Stuart; JOHNSTON, Robert. Gestão da Produção e Operações. 7^a ed. São Paulo: Atlas, 2013. ISBN 978-85-224-6789-0

TANENBAUM, Andrew S.; WETHERALL, David J. Redes de Computadores. 5^a ed. São Paulo: Pearson, 2011. ISBN 978-85-7605-888-9.

WERNER, Jorge. Infraestrutura de Redes de Computadores. Indaiatuba: UNIASSELVI, 2020. 2 ed. 211 p. ISBN 978-65-663-059-5.