

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Instituto de Ciências Exatas e de Informática

Projeto da Infraestrutura de Rede da Secretaria de Saúde∗

Felipe Moreira de Oliveira1 Guilherme Augusto Pessoa de Castro2

João Paulo Maia de Paula3  
Rafael Henrique de Souza Pereira4

Thiago Vinicius Costa Lara5

**Resumo**

Este relatório técnico detalha o planejamento e a implementação da infraestrutura de rede para uma Secretaria de Saúde no município Alfa, conectando o edifício-sede da Secretaria, um Hospital Regional e seis Unidades de Pronto Atendimento (UPAs). O objetivo deste documento é fornecer informações abrangentes sobre a infraestrutura de rede distribuída nesse território, abordando a topologia da rede, os protocolos utilizados para comunicação entre as unidades, o hardware e software de rede em cada local, além do gerenciamento, desempenho e segurança da rede. Ao entender completamente essa infraestrutura, é possível realizar uma manutenção eficaz e implementar melhorias para aumentar sua robustez e desempenho.  
**Palavras-chave:** Cisco Packet Tracer. Gerenciamento de Rede. Infraestrutura de Rede. Zabbix. DHCP. AD. DNS.



∗Artigo apresentado como pré-requisito para aprovação no 5º período do curso de Bacharel em Sistemas de Informação.

1Aluno da Graduação em Sistemas de Informação. 2Aluno da Graduação em Sistemas de Informação. 3Aluno da Graduação em Sistemas de Informação. 4Aluno da Graduação em Sistemas de Informação. 5Aluno da Graduação em Sistemas de Informação.

**Abstract**

This technical report details the planning and implementation of the network infrastructure for a Health Department in Alpha city, connecting the headquarters of the Department, a Regional Hospital, and six Emergency Care Units (UPAs). The purpose of this document is to provide comprehensive information about the distributed network infrastructure in this territory, covering the network topology, protocols used for communication between the units, network hardware and software at each location, as well as network management, performance, and security. Understanding this infrastructure thoroughly is essential for effective maintenance and implementing improvements to enhance its robustness and performance.

**Keywords:** Cisco Packet Tracer. Network Management. Network Infrastructure. Zabbix.

DHCP. AD. DNS.

1. **INTRODUÇÃO**

Este documento delineia o projeto de infraestrutura de rede que será instaurado na Secretaria de Saúde do município Alfa, visando aprimorar a experiência e satisfação dos usuários em serviços de saúde de variados níveis de complexidade. O cerne deste projeto é facilitar uma comunicação eficaz e segura entre a sede da Secretaria, um Hospital Regional e seis Unidades de Pronto Atendimento (UPAs), estrategicamente situadas em distintas regiões da cidade.

O enfoque do trabalho será no planejamento, na criação de protótipos, na implementação e na documentação detalhada da infraestrutura de rede. Esta abordagem tem como objetivo assegurar os pilares de confiabilidade, segurança e escalabilidade da rede. Tal infraestrutura permitirá que a Secretaria de Saúde não apenas aperfeiçoe os serviços atuais, mas também contemple a expansão futura do número de hospitais regionais e UPAs, atendendo assim à crescente demanda por atendimento médico no município de Alfa.

Para construir uma infraestrutura de rede robusta e resiliente, serão adotadas soluções avançadas de monitoramento e gestão de rede. Este esforço visa maximizar a disponibilidade da rede e minimizar os períodos de inatividade, garantindo uma prestação de serviços de saúde contínua e eficiente.

**1.1. Serviços e Infraestrutura**

Os serviços a serem disponibilizados para os usuários são:

* Agendamento de exames e consultas online (Servidor Web);
* Acessar o resultado dos exames realizados.
* Acesso à internet via wifi da UPA ou Hospital Regional.

**1.2. Recursos e serviços**

Para a Secretaria, o hospital regional e as upas, serão utilizados os seguintes recursos.

* Videoconferência.
* Sistema de gestão hospitalar atual.
* Sistema de Gestão Hospitalar Legado (Consulta).
* Sistema de Laboratório.
* Sistema de Imagem (RIS/PACS).
* Sistema de Controle de Acesso.
* Sistemas Administrativos.
* Firewall.
* Sistema de Controle de Ponto.
* Acessar o e-mail e a intranet.
* Antivírus.
* Servidor Active Directory.
* Servidor de Banco de Dados (centralizado na Secretaria de Saúde).
* Servidor de Aplicação - Web (centralizado na Secretaria de Saúde).
* Servidores Proxy (centralizado na Secretaria de Saúde).
* Servidor de arquivos - FTP.
* Servidor DHCP.
* Servidor de Impressão (centralizado na Secretaria de Saúde).
* Firewall.
* Servidor DNS (centralizado na Secretaria de Saúde).
* Storage NAS ou DAS (centralizado na Secretaria de Saúde).

**1.3. Equipamentos**

**1.3.1. Secretaria de Saúde**

400 desktop.

4 Impressora de Rede.

9 Switch de 48 portas.

25 Access Points.

2 roteador.

**1.3.2. Hospital Regional**

208 desktop.

20 Impressora de Rede.

35 Switch de 48 portas.

105 Access Points.

2 roteador.

**1.3.3. UPA**

50 desktop.

5 Impressora de Rede.

12 Switch de 48 portas.

36 Access Points.

2 roteador.

1. **DESENVOLVIMENTO**
   1. **Etapa 1 - Análise, Planejamento e Prototipação da Solução**

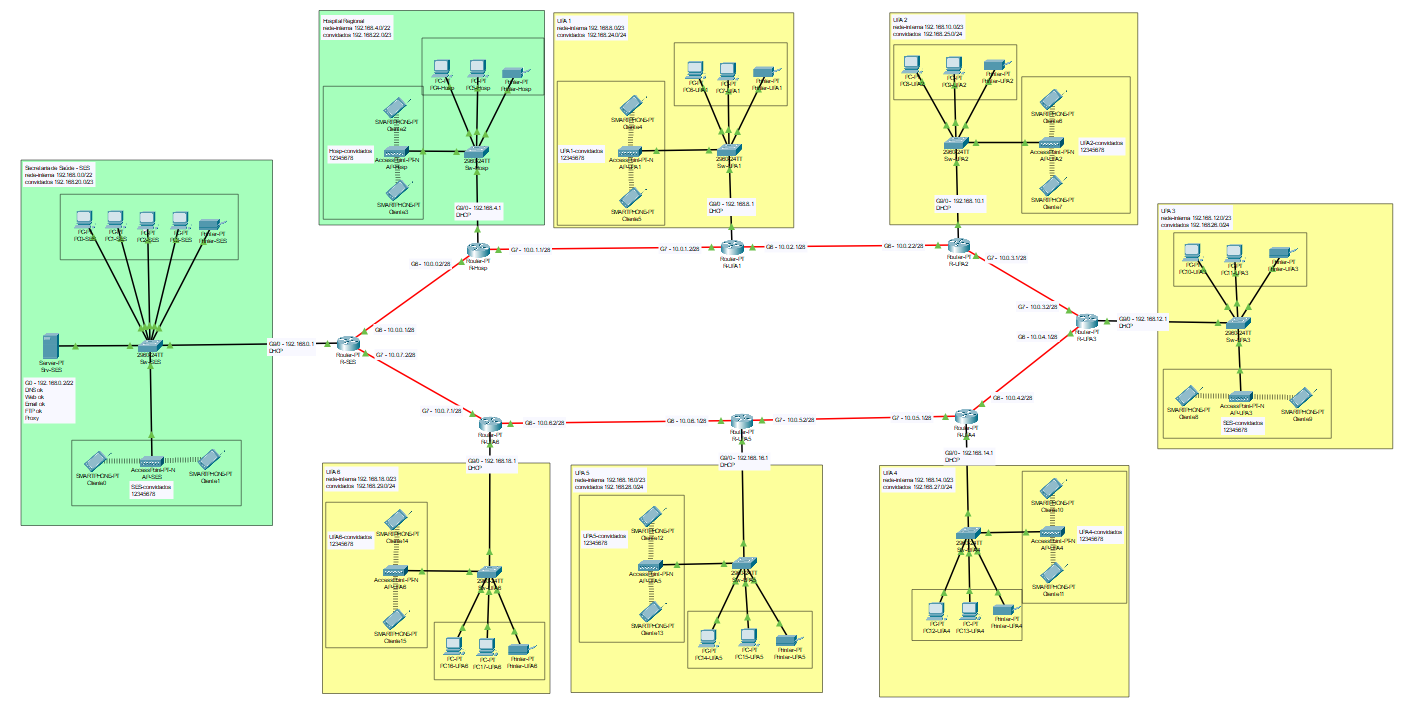
O processo de planejamento foi elaborado levando em consideração os critérios essenciais de eficiência, escalabilidade e segurança da infraestrutura de rede. Isso se deve ao entendimento de que alterações na configuração das unidades são inevitáveis, seja por meio de uma expansão das capacidades existentes ou por uma readequação necessária da infraestrutura para atender a novas demandas. Para o estágio de prototipagem, optamos pela utilização do Cisco Packet Tracer, uma ferramenta avançada de modelagem e configuração de redes, reconhecida por sua eficácia em simular cenários de rede complexos com precisão e flexibilidade.

A rede da Secretaria de Saúde é conectada com o Hospital Regional e as UPAs por meio da implementação de topologia no formato Anel.

Essa topologia apresenta algumas características positivas para o nosso modelo de negócio, tais como:

* Unidirecionalidade: cada dispositivo recebe dados do dispositivo anterior e os encaminha para o próximo dispositivo;
* Autonomia: Cada nó é responsável por receber dados, amplificá-los (se necessário) e encaminhá-los para o próximo nó.
* Confiabilidade: Se um dispositivo falhar ou um cabo for desconectado em algum ponto do anel, a comunicação ainda pode ocorrer, pois os dados podem contornar o ponto de falha no anel.
* Latência previsível: a latência tende a ser previsível e uniforme já que o caminho dos dados ao redor do anel é fixo, o que impacta positivamente no sistema de gestão hospitalar que permite o controle dos processos em tempo real.
* Menor Largura de banda: A largura de banda total disponível pode ser menor, pois todos os dispositivos compartilham o mesmo meio de comunicação.
* Protocolos específicos: há a possibilidade de implementar um protocolo especial, como por exemplo o Token Ring, que controla o acesso ao meios de transmissão para evitar colisões de dados.

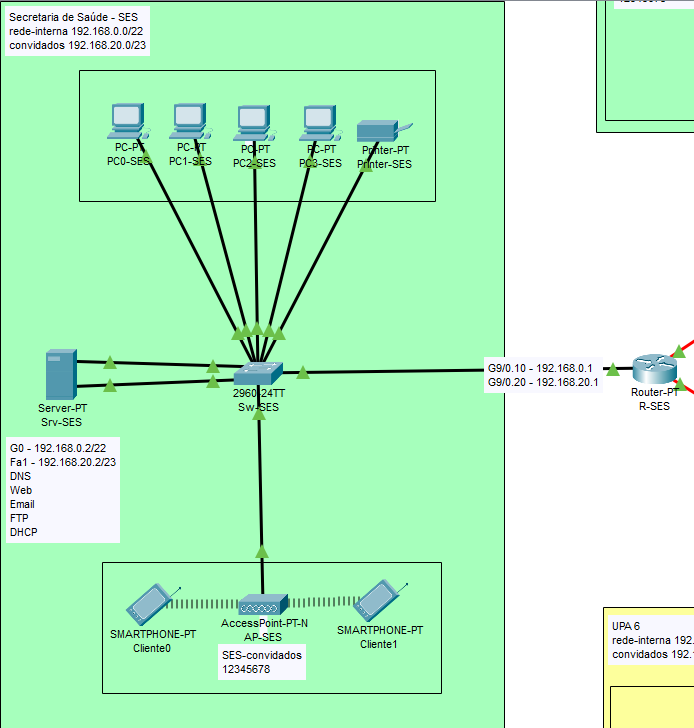
**Figura 1: Estrutura da rede utilizando o Packet Tracer.**

******

**Fonte: Elaborado pelos autores no Cisco Packet Tracer (2023).**

Nas próximas figuras iremos mostrar as configurações gerais de cada uma das distintas unidades, a saber: Secretaria de Saúde, Hospital Regional e UPA padrão.

**Figura 2: Estrutura da rede da Secretaria de Saúde utilizando o Packet Tracer.**



**Fonte: Elaborado pelos autores no Cisco Packet Tracer (2023).**

**Tabela 1: Planilha de IPS da rede - Packet Tracer.**

|  | Planilha de IP's | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| VLAN 10 | Nome | IP address | Subnet Mask | IP Gateway | IP Range | DHCP IP |
|  | Secretaria de Saúde | 192.168.0.0 | 255.255.252.0 | 192.168.0.1 | 0.1 a 3.254 | 192.168.0.2 |
|  | Hospital Regional | 192.168.4.0 | 255.255.252.0 | 192.168.4.1 | 4.1 a 7.254 | 192.168.4.1 |
|  | UPA 1 | 192.168.8.0 | 255.255.254.0 | 192.168.8.1 | 8.1 a 9.254 | 192.168.8.1 |
| rede-interna | UPA 2 | 192.168.10.0 | 255.255.254.0 | 192.168.10.1 | 10.1 a 11.254 | 192.168.10.1 |
|  | UPA 3 | 192.168.12.0 | 255.255.254.0 | 192.168.12.1 | 12.1 a 13.254 | 192.168.12.1 |
|  | UPA 4 | 192.168.14.0 | 255.255.254.0 | 192.168.14.1 | 14.1 a 15.254 | 192.168.14.1 |
|  | UPA 5 | 192.168.16.0 | 255.255.254.0 | 192.168.16.1 | 16.1 a 17.254 | 192.168.16.1 |
|  | UPA 6 | 192.168.18.0 | 255.255.254.0 | 192.168.18.1 | 18.1 a 19.254 | 192.168.18.1 |
| VLAN 20 |  |  |  |  |  |  |
|  | Secretaria de Saúde | 192.168.20.0 | 255.255.254.0 | 192.168.20.1 | 20.1 a 21.254 | 192.168.20.2 |
|  | Hospital Regional | 192.168.22.0 | 255.255.254.0 | 192.168.22.1 | 22.1 a 23.254 | 192.168.22.1 |
|  | UPA 1 | 192.168.24.0 | 255.255.255.0 | 192.168.24.1 | 24.1 a 24.254 | 192.168.24.1 |
| clientes | UPA 2 | 192.168.25.0 | 255.255.255.0 | 192.168.25.1 | 25.1 a 25.254 | 192.168.25.1 |
|  | UPA 3 | 192.168.26.0 | 255.255.255.0 | 192.168.26.1 | 26.1 a 26.254 | 192.168.26.1 |
|  | UPA 4 | 192.168.27.0 | 255.255.255.0 | 192.168.27.1 | 27.1 a 27.254 | 192.168.27.1 |
|  | UPA 5 | 192.168.28.0 | 255.255.255.0 | 192.168.27.1 | 28.1 a 28.254 | 192.168.27.1 |
|  | UPA 6 | 192.168.29.0 | 255.255.255.0 | 192.168.29.1 | 29.1 a 29.254 | 192.168.29.1 |

**Fonte: Elaborado pelos autores (2023).**

**2.2 - Etapa 2 - Configuração dos Ambientes On-Premise e On-Cloud**

O processo de implantação da infraestrutura de rede adotou um modelo híbrido, com a configuração na rede própria da Secretaria de Saúde (On-premise) e utilização da Amazon Web Services - AWS (On-cloud).

**Endereço dos servidores configurados:**

FTP: 3.94.110.38

usuário: aluno

senha: aluno

HTTP: 54.205.123.47

Banco de Dados:

Nome do usuário principal: admin.

Senha: hospitalpuc.

Endpoint: hospitalpuc.croavsxysbvv.us-east-1.rds.amazonaws.com

AD (On-premise): ses.com.br (192.168.0.2/22)

usuario: Administrador

senha: privada

DNS (On-premise): SRV-SES (192.168.0.2/22)

Servidor de Impressão (CUPS) (On cloud):

54.235.4.13:631

DHCP (On-premise):

Start IP 192.168.0.21

End IP: 192.168.3.254

Proxy (On cloud)

54.221.159.110:3128

usuário SES

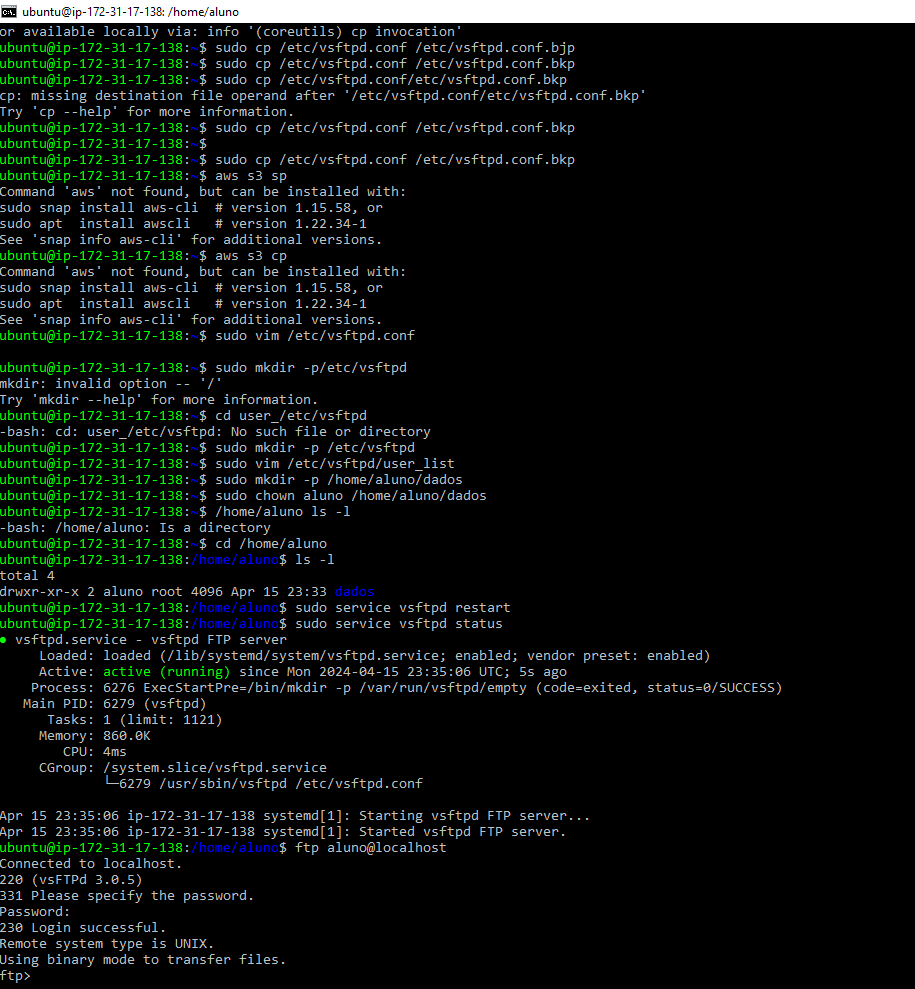
senha 1234

**2.2.1. Configuração do File Transfer Protocol (FTP)**

Nesse modelo cliente-servidor, o servidor centralizado na Secretaria de Saúde irá hospedar os arquivos que serão acessados pela secretaria, pelo Hospital Regional e pelas 06 (seis) Unidades de Pronto Atendimento (UPA) localizadas em diversos pontos do município. O servidor FTP (File Transfer Protocol) é um tipo de servidor utilizado para transferir arquivos entre computadores em uma rede, como a Internet. Ele funciona como um repositório centralizado onde os usuários podem fazer upload e download de arquivos de e para o servidor, possuindo backup dos dados e permitindo a documentação dos arquivos da Secretaria de Saúde de acordo com a permissão de cada usuário.

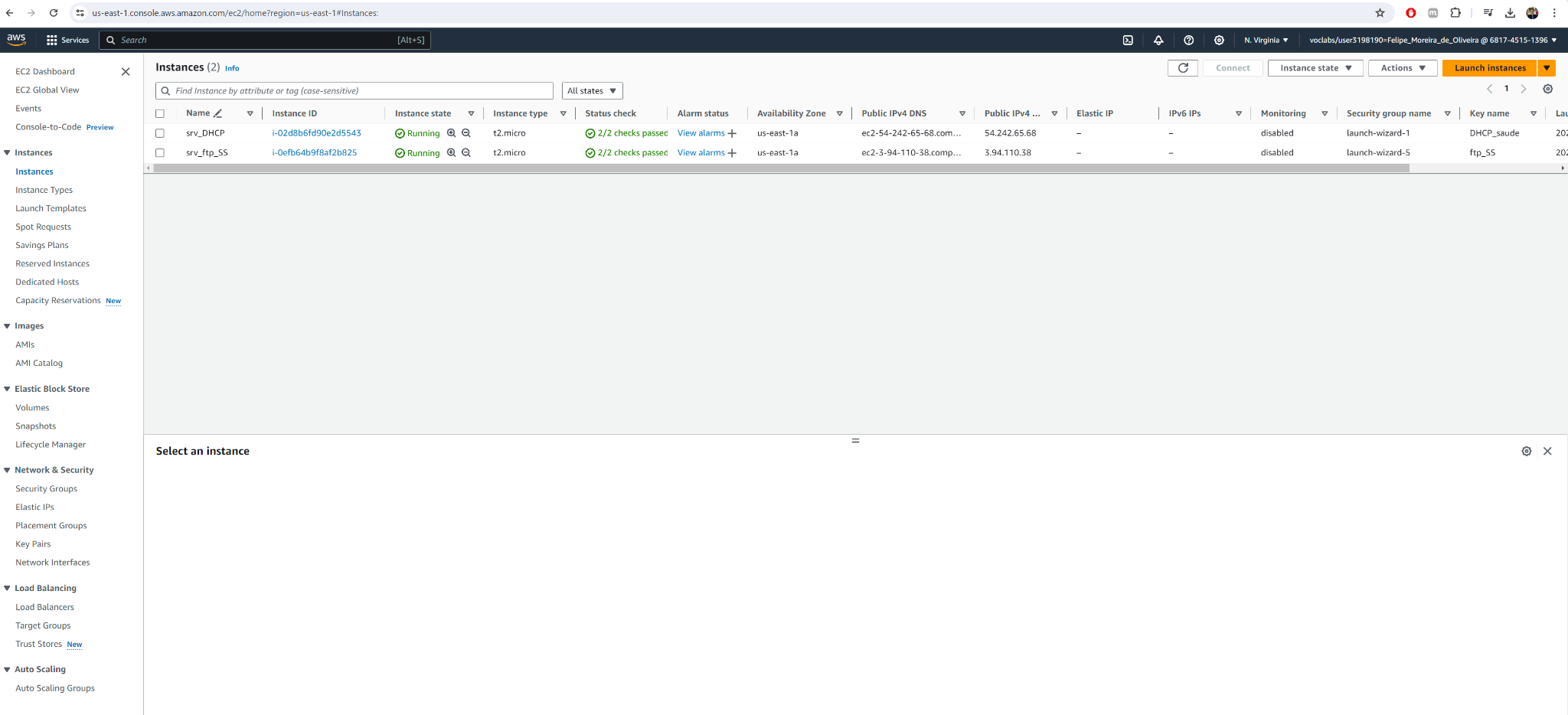
Os prints abaixo mostram a configuração bem sucedida do servidor FTP (on cloud) realizada na AWS e que foi testada no Filezilla.

**Figura 3: Configuração do servidor FTP**



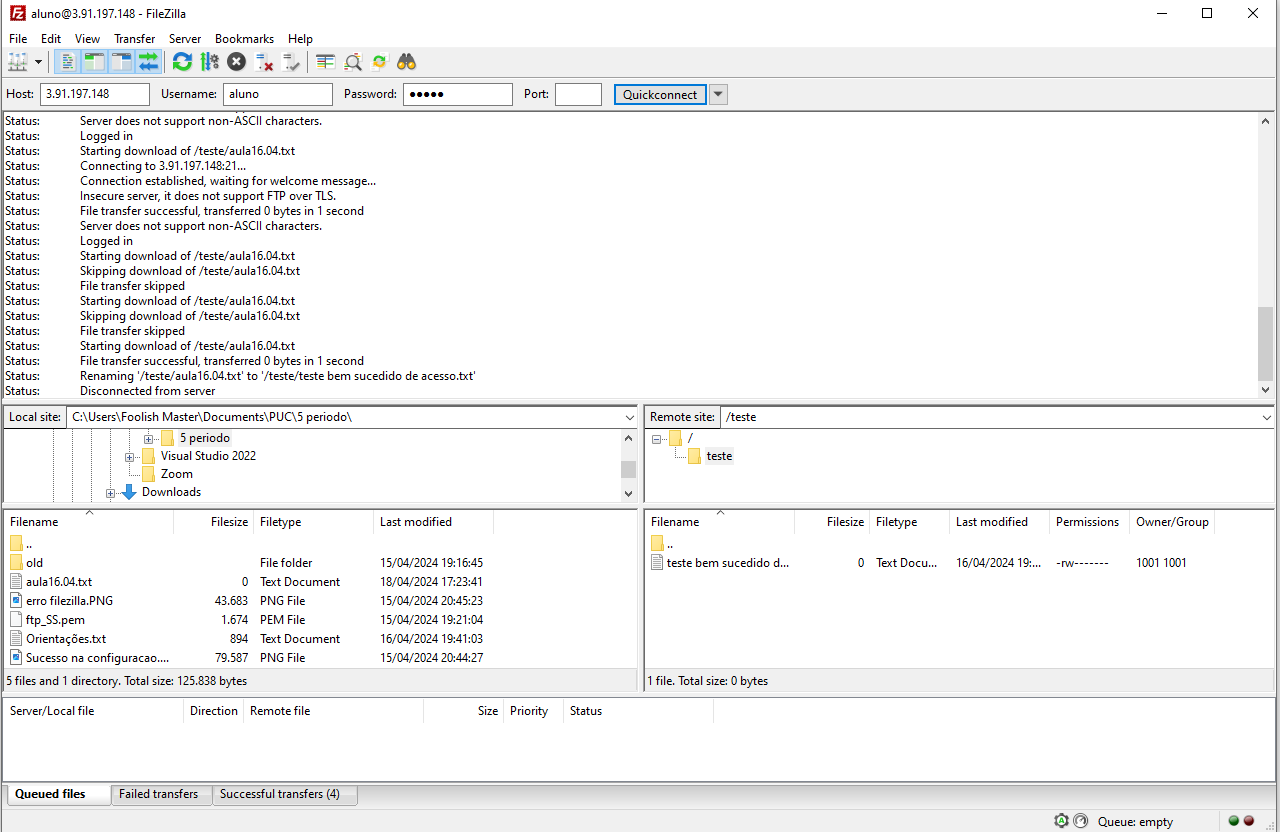
Fonte: Configuração realizada pelos autores seguindo tutorial Instalação FTP e Servidor Web + AWS

**Figura 4: Configuração do servidor FTP na AWS**



Fonte: Configuração realizada pelos autores na AWS - Amazon Inc. (2023)

**Figura 5: Conexão ao servidor FTP utilizando o Filezilla**



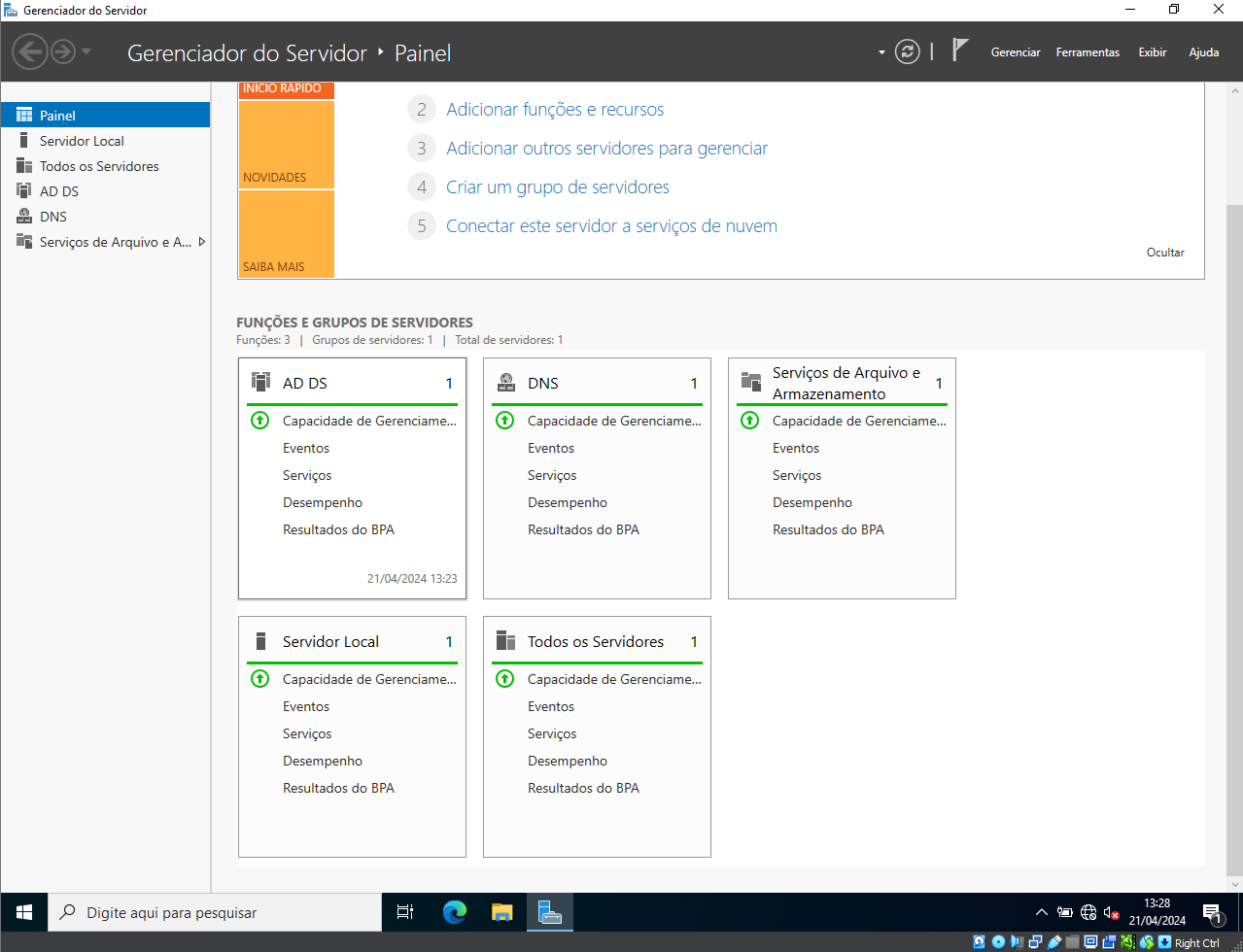
Fonte: Teste de acesso realizado no Filezilla (2023)

Os testes foram realizados com o usuário: aluno e a senha: aluno no ip dinâmico: 3.94.110.38, que foi registrado no teste acima demonstrado no Filezilla..

**2.2.2 Configuração do Active Directory (AD) e DNS (Domain Name System):**

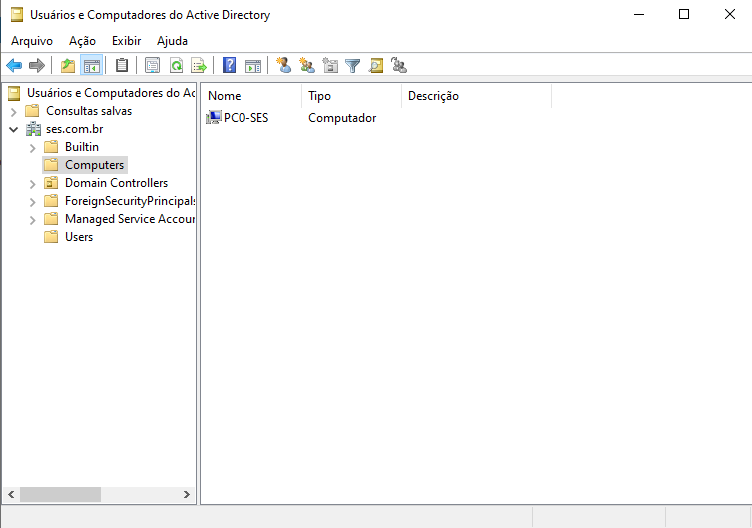
Optou-se por disponibilizar o serviço de AD na infraestrutura física da Secretaria de Saúde. Para ser levado a efeito, foi criado o domínio “ses.com.br”, NetBIOS SES, e disponibilizando-o para todas as UPAs e para o Hospital. Assim, será possível ter o controle das atividades de todas as máquinas inseridas na rede interna. A plataforma escolhida foi o Windows Server 2022:

**Figura 6: Configuração do AD**



Fonte: Elaboração própria dos autores

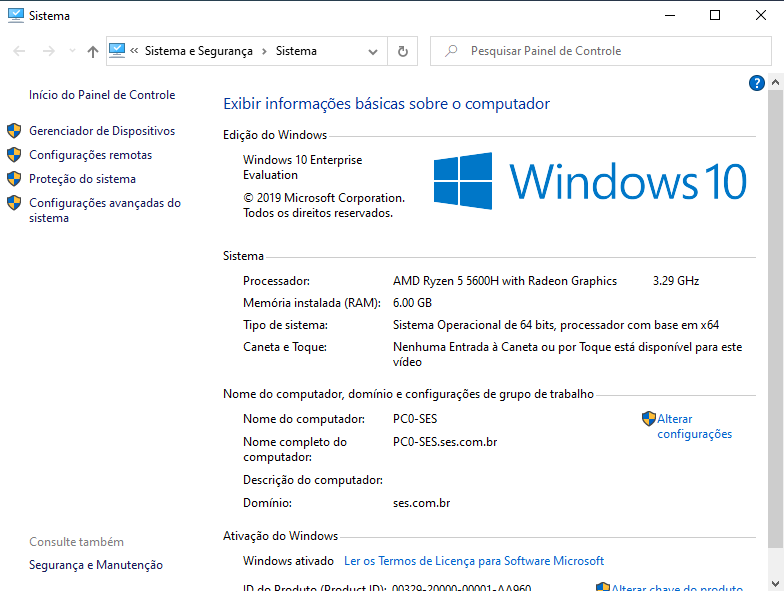
**Figura 7: Configuração do AD**



Fonte: Elaboração própria dos autores

Foi incluído um host no domínio sem problemas, como se pode ver abaixo:

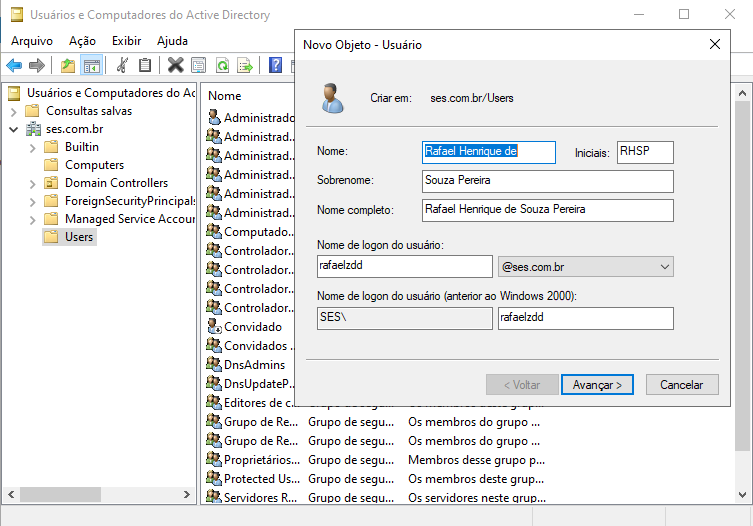
**Figura 8: Configuração do AD - inclusão de host no domínio**



Fonte: Elaboração própria dos autores

Foi criado um usuário no AD:

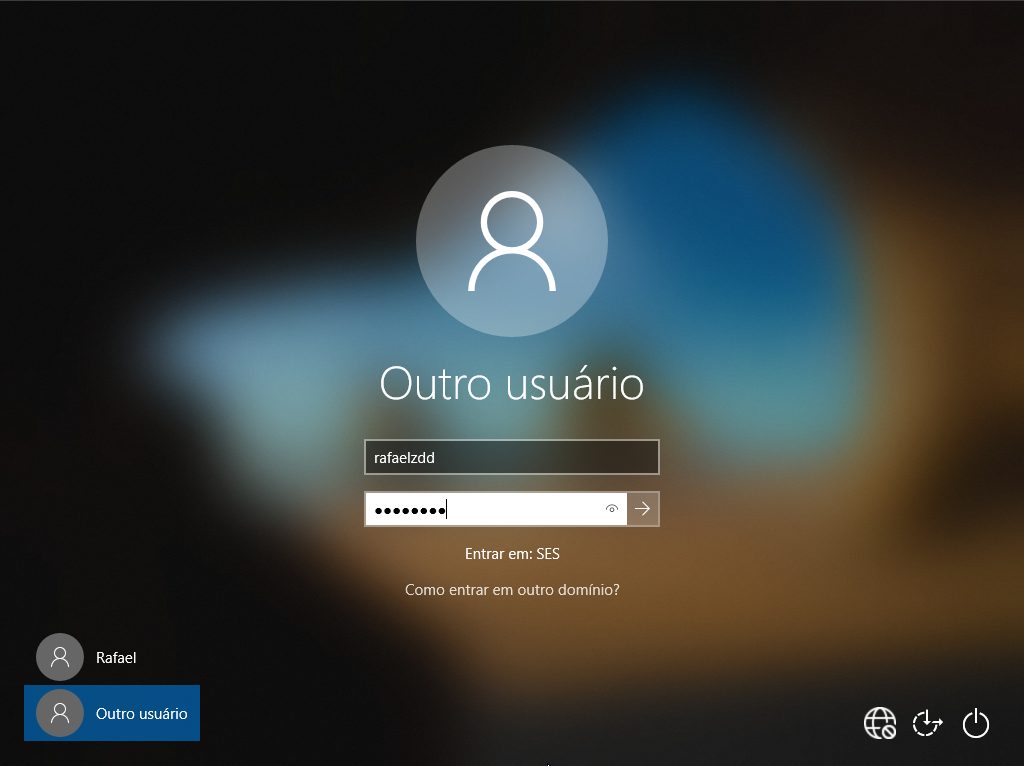
**Figura 9: Configuração do AD - Criação de Usuários**



Fonte: Elaboração própria dos autores

O usuário logou no host normalmente:

**Figura 10: Configuração do AD - Logar no Host**

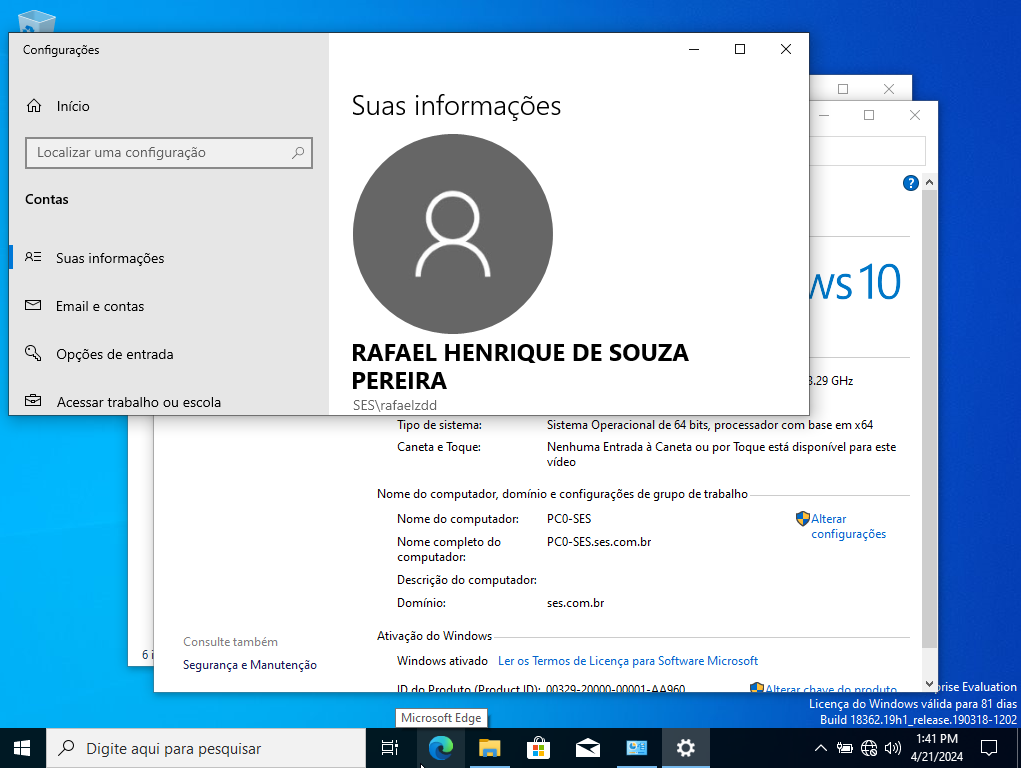


Fonte: Elaboração própria dos autores

**Figura 11: Configuração do AD - login bem sucedido**



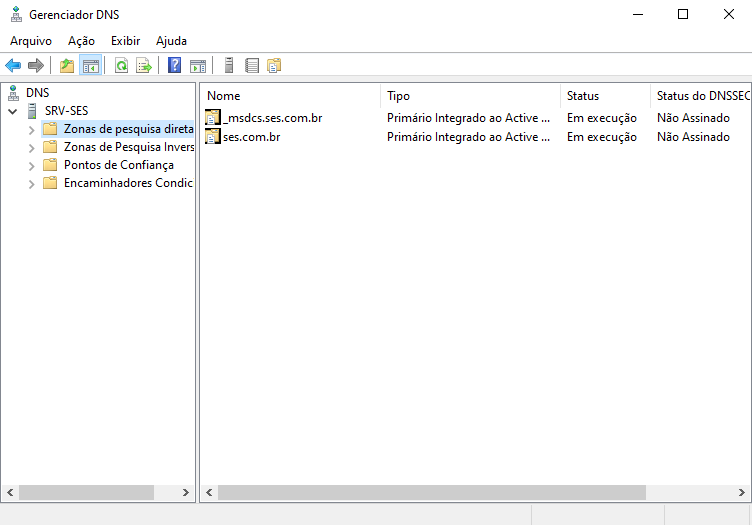
Fonte: Elaboração própria dos autores

**Figura 12: Configuração do AD - Usuário Logado**

Fonte: Elaboração própria dos autores

O serviço de DNS foi implementado de forma suplementar ao de AD, na mesma plataforma Windows Server 2022:

**Figura 13: Implementação de DNS**



Fonte: Elaboração própria dos autores

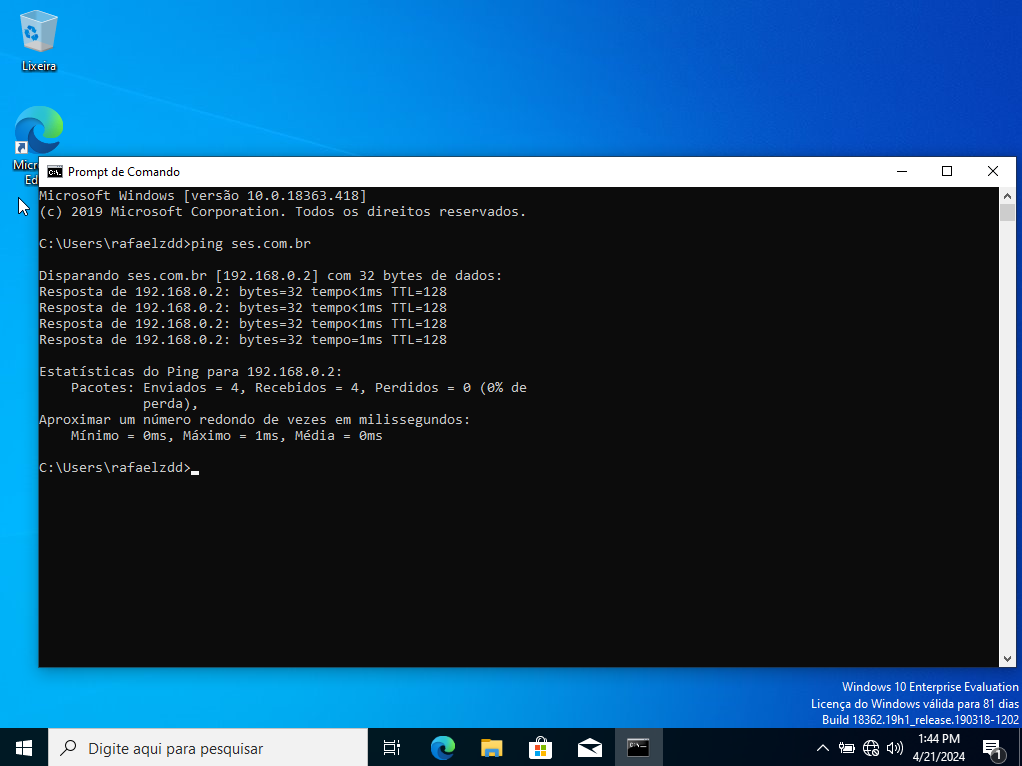
Os testes de conectividade e de resolução de nome foram realizados com sucesso:

**Figura 14: Implementação de DNS - teste de conectividade**



Fonte: Elaboração própria dos autores

**Figura 15: Implementação de DNS - teste de conectividade realizado**



Fonte: Elaboração própria dos autores

**2.2.3 - Configuração dos Ambientes On-Cloud- servidor HTTP - AWS**

Para a criação do servidor HTTP foi criada uma instância na AWS utilizando a plataforma Ubuntu/Linux. Quando digitado o endereço de IPv4 público da máquina virtual no navegador, podemos nos conectar a esse ambiente Figura 15.

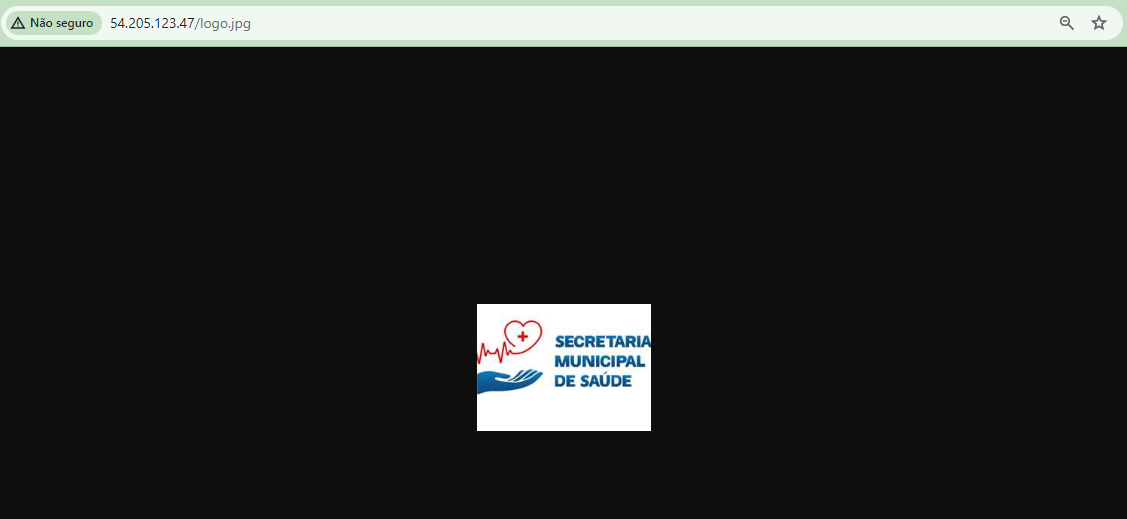
**Figura 16: Conexão ao servidor HTTP.**



Fonte: Elaboração própria dos autores

Após a configuração, foi efetuado o upload de uma imagem de nome logo.jpg para a máquina. Essa imagem simula, de maneira bem simplificada, um web site (Figura 16).

**Figura 17: Conexão ao servidor HTTP - acessando arquivos.**



Fonte: Elaboração própria dos autores

**2.2.4 - Configuração dos Ambientes On-Cloud- Banco de dados - AWS**

Para a configuração do banco de dados, utilizou-se do serviço de gerenciamento de banco de dados relacional da AWS, o ADS.

Os detalhes das configurações mais relevantes estão descritos abaixo.

Tipo do banco: MYSQL.

Nome do usuário principal: admin.

Senha: hospitalpuc.

Endpoint: hospitalpuc.croavsxysbvv.us-east-1.rds.amazonaws.com.

Armazenamento: 20 gb com escalabilidade automática.

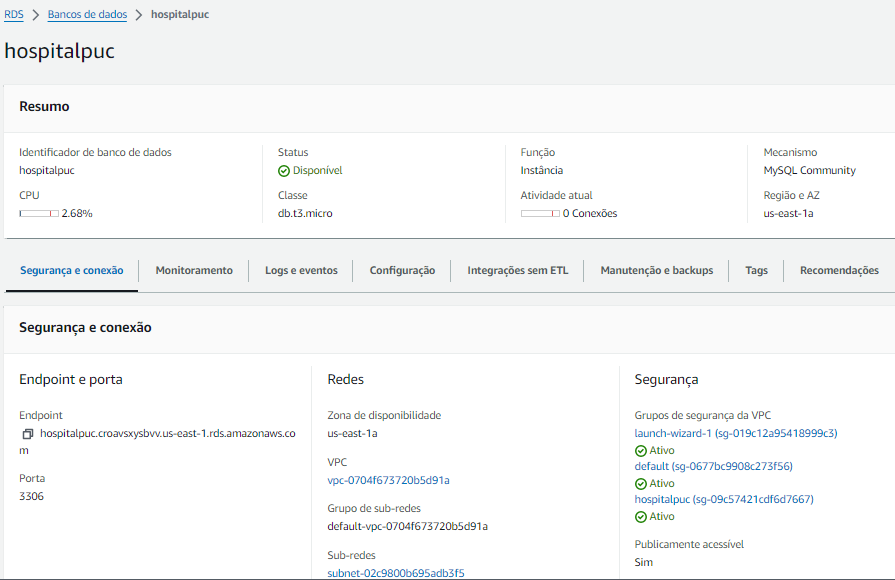
Tipo de rede: IPv4.

Grupo de segurança: implantado.

Nome do grupo de segurança: hospitalpuc.

A Figura 17 mostra a descrição do banco.

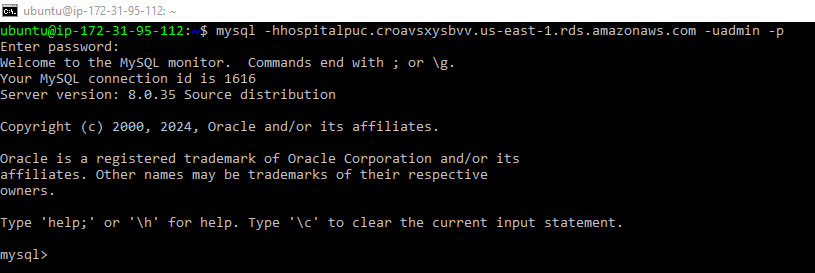
**Figura 18: Banco de dados AWS.**



Fonte: Elaboração própria dos autores

O próximo passo foi conectar o banco de dados à máquina virtual criada no ítem anterior, Figura 18.

**Figura 19: Conexão da máquina ao banco de dados.**

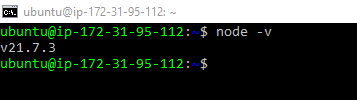


Fonte: Elaboração própria dos autores

**2.2.5 - Configuração dos Ambientes On-Cloud- Configuração da aplicação - AWS**

Em nosso trabalho foi utilizado como plataforma Back-end, o Node.Js. A Figura 19 abaixo mostra a última versão instalada no computador virtual.

**Figura 20: Versão do Node.Js instalado na máquina virtual.**

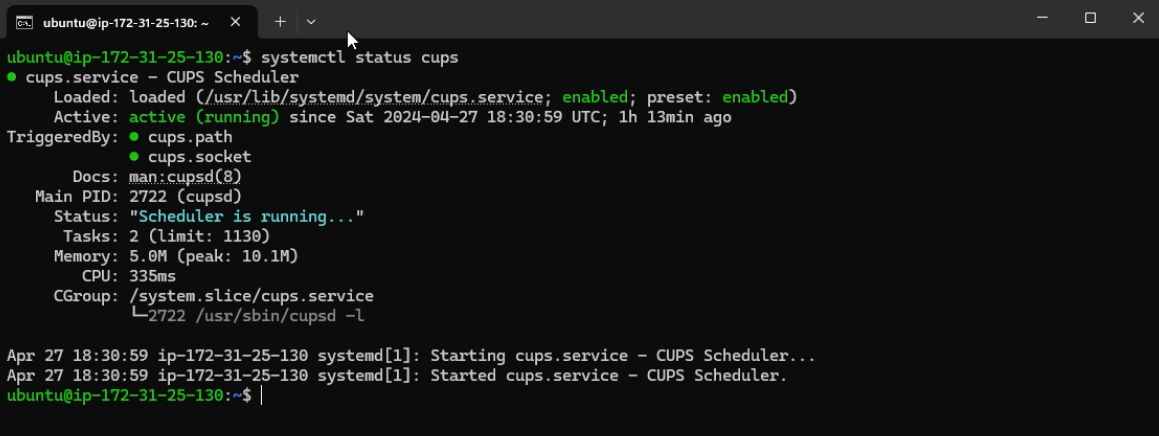


Fonte: Elaboração própria dos autores

Assim, o sistema está pronto para receber uma aplicação em Node.Js.

**2.2.6 - Configuração dos Ambientes On-Cloud- Servidor de impressão - AWS**

Foi escolhido o servidor de impressão Common UNIX Printing System (CUPS) para funcionar em uma máquina virtual hospedada na AWS. Como o domínio SES é em Windows, também foi necessário instalar o Samba para realizar a compatibilidade.

**Figura 21: Configuração do CUPS na AWS**

Fonte: Elaboração própria dos autores

Após feita a instalação e ativação do serviço, a customização pode ser feita via GUI utilizando o browser (acesso via porta 631 no IP público da VM da AWS):

**Figura 22: Customização do UNIX na AWS**



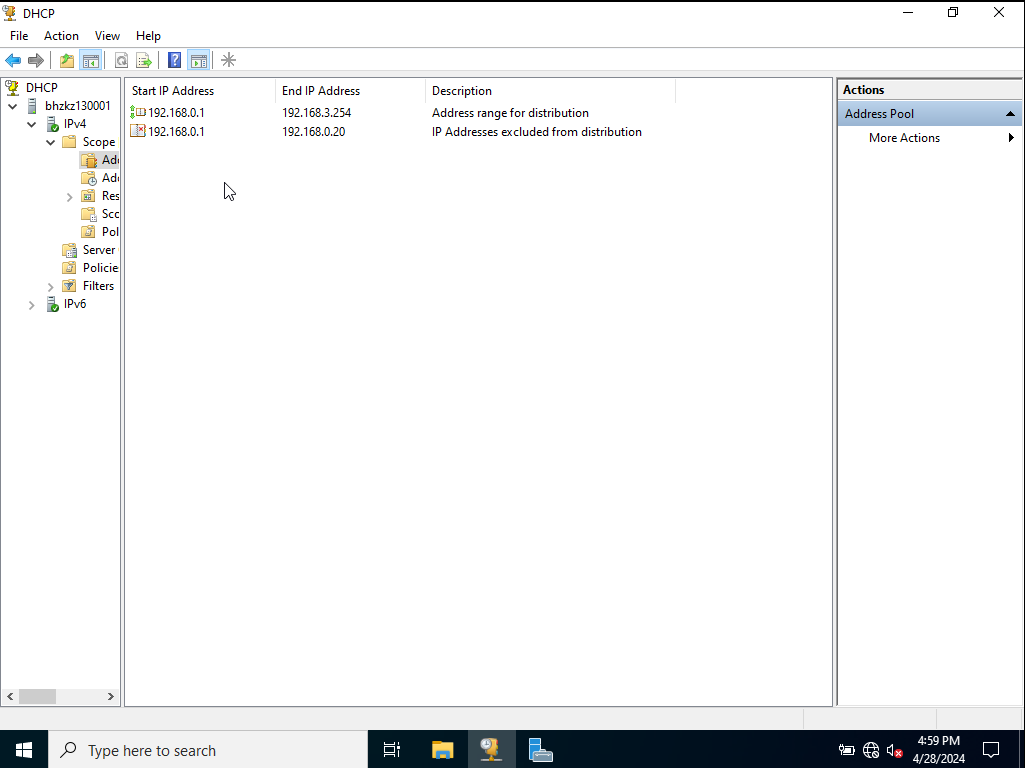
Fonte: Elaboração própria dos autores

**2.2.7 - Configuração dos ambientes On-Premises: Servidor DHCP**

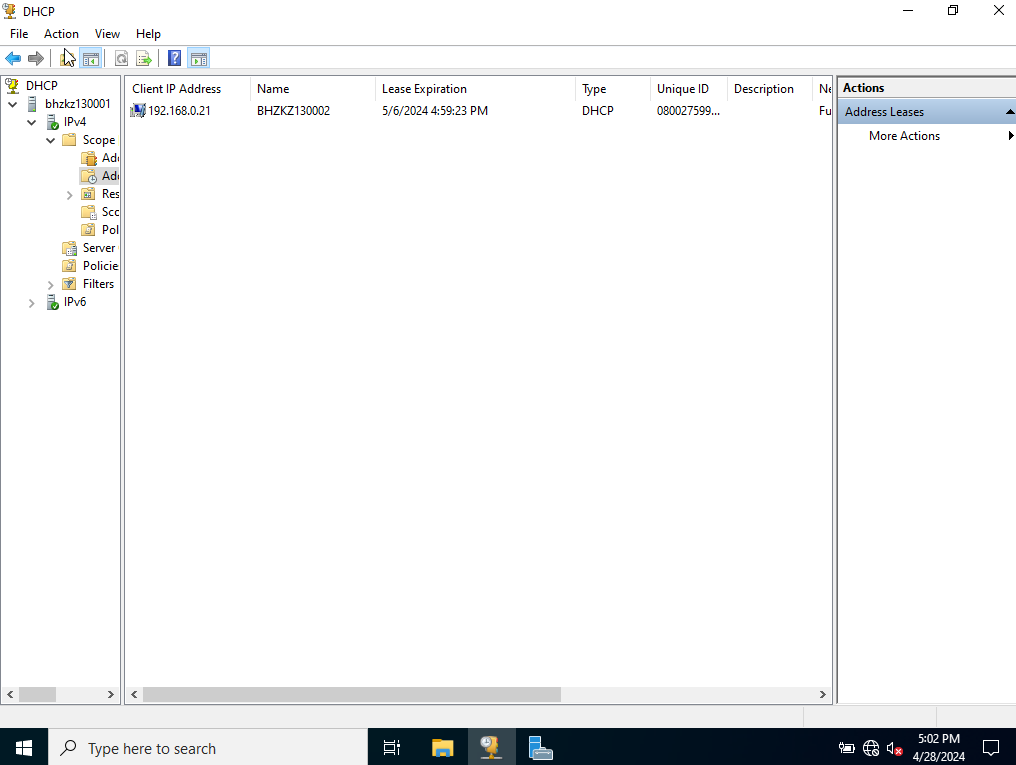
Para a configuração do serviço de DHCP (Dynamic Host Configuration Protocol) na Secretaria Estadual de Saúde foi escolhida a utilização de um servidor com sistema operacional Windows Server 2022 Standard.

Respeitando-se a Tabela 1: Planilha de IPS da rede - Packet Tracer, foi criado, após a instalação do serviço DHCP, uma zona de exclusão de IP’s para a faixa 192.168.0.1 a 192.168.0.20. Desta forma, o servidor DHCP irá distribuir IP’s para a rede corporativa a partir do IP 192.168.0.21.

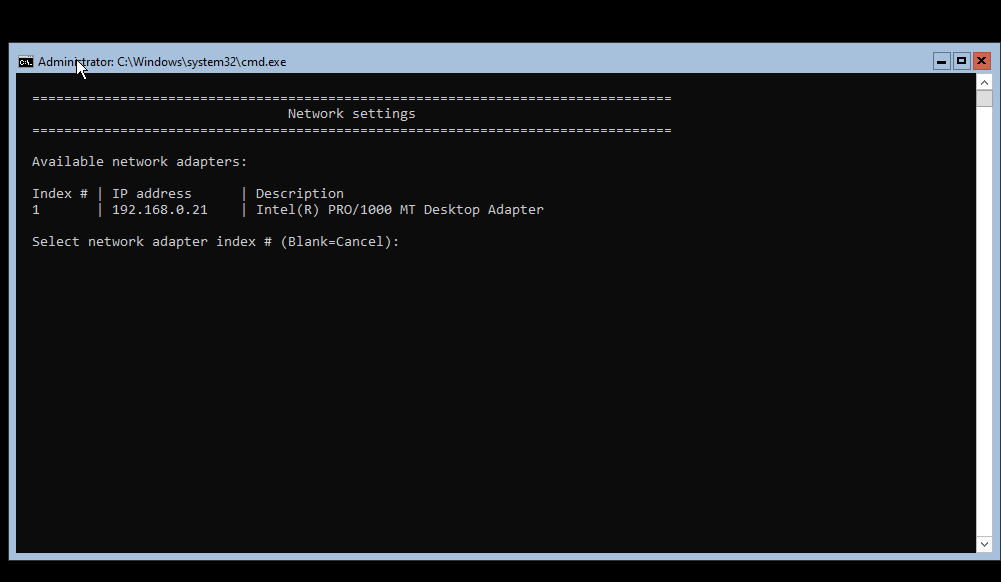
As figuras abaixo mostram o serviço DHCP em funcionamento e também a distribuição de um IP fora da faixa de exclusão para um servidor da rede:

**Figura 23: Faixa de distribuição e exclusão de IP’s:**

Fonte: Elaboração própria dos autores

**Figura 24: Distribuição de IP para servidor BHZKZ130002 no DHCP**

Fonte: Elaboração própria dos autores

**Figura 25: Distribuição de IP para servidor BHZKZ130002 no Servidor:**

Fonte: Elaboração própria dos autores

**2.2.8 - Configuração dos Ambientes On-Cloud- Proxy - AWS**

Para a instalação e configuração do serviço de Proxy foi escolhido a utilização de um servidor com sistema operacional UBUNTU hospedado no ambiente virtual da AWS. A sua configuração, utilizando o serviço SQUID, seguiu os passos abaixo:

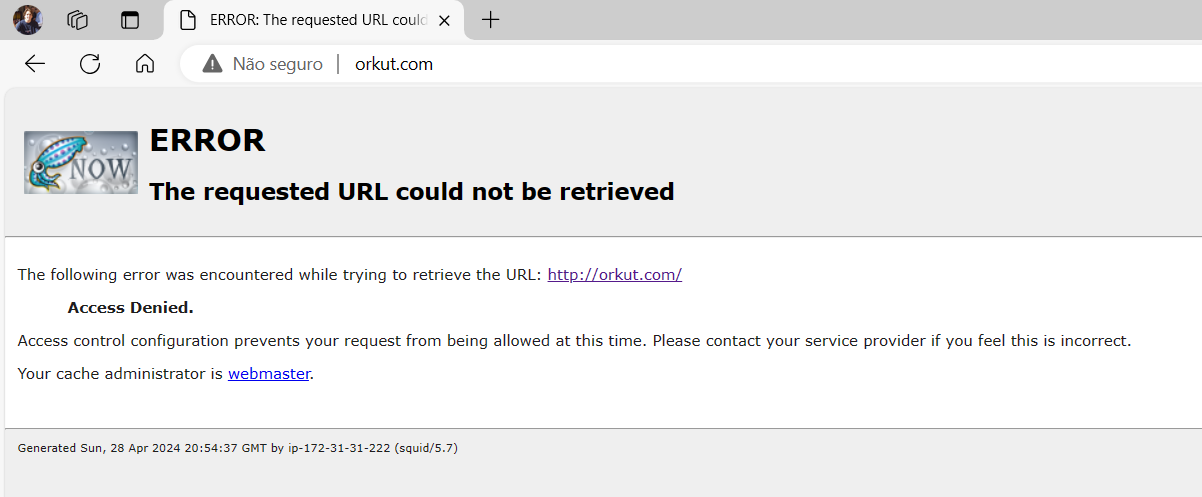
* $ sudo apt update (atualiza bibliotecas do ubuntu)
* $ sudo apt install squid -y (instala o Squid)
* $ sudo systemctl status squid (verifica o status do serviço do SQUID)
* $ sudo ss -pnltu | grep -i 3128 (Verifica se o SQUID está respondendo pela porta 3128).
* $ sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.bak (Faz backup do arquivo de configuração padrão do SQUID)
* $ sudo vi /etc/squid/squid.conf (Abre o arquivo squid.conf)
* Os seguintes parâmetros foram incluídos no arquivo de configuração do SQUID:
  + acl blocksites dstdomain /etc/squid/blocksites.txt (Cria arquivo com lista de sites bloqueados)
  + http\_access deny blocksites (Nega o acesso aos sites constantes no arquivo blocksites.txt
* $ cat /etc/squid/blocksites.txt (Criação do arquivo com a lista de sites bloqueados)
* Lista de sites bloqueados:
  + .facebook.com
  + .globo.com
  + .orkut.com
* $ sudo systemctl restart squid (Reinicia o serviço do SQUID)

Criação do serviço de autenticação dentro do servidor SQUID:

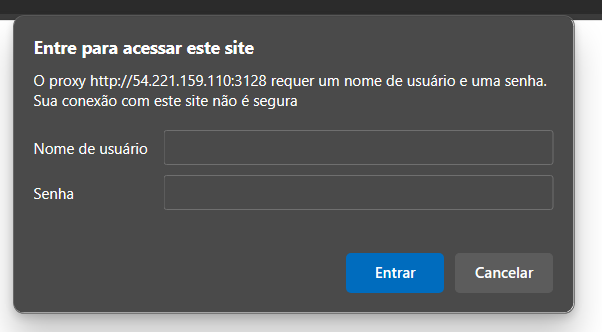
* $ sudo apt install apache2-utils -y (instala o apache)
* $ sudo touch /etc/squid/passwords (cria o arquivo de usuário e senha para autenticação no Proxy)
* $ sudo chmod 777 /etc/squid/passwords (Abre o arquivo de usuários e senhas)
* $ sudo htpasswd -c /etc/squid/passwords ses (Cria o usuário SES com a senha 1234)
* $ sudo vi /etc/squid/squid.conf (Abre o arquivo de configuração do SQUID para inserção de parâmetros de autenticação. Os parâmetros inseridos foram os abaixo:
  + auth\_param basic program /usr/lib/squid/basic\_ncsa\_auth /etc/squid/passwords
  + auth\_param basic realm Squid proxy-caching web server
  + auth\_param basic credentialsttl 24 hours
  + auth\_param basic casesensitive off
  + acl authenticated proxy\_auth REQUIRED
  + acl blocksites dstdomain /etc/squid/blocksites.txt
  + http\_access deny blocksites
  + http\_access allow authenticated
  + # And finally deny all other access to this proxy
  + http\_access deny all
  + dns\_v4\_first on
  + forwarded\_for delete
  + via off
* $ sudo systemctl restart squid (Reinicia o Serviço do SQUID)

Após esta configuração o proxy está configurado para utilização. Este proxy bloqueará os sites do facebook.com, orkut.com e globo.com e permitirá acesso, mediante autenticação, aos demais sites. Todo o tráfego de internet passará pelo proxy e os usuários da rede terão o mesmo IP público que o IP do Proxy Server.

As imagens abaixo demonstram o Proxy Server em funcionamento:

**Figura 26: Servidor Proxy negando acesso ao site www.orkut.com**

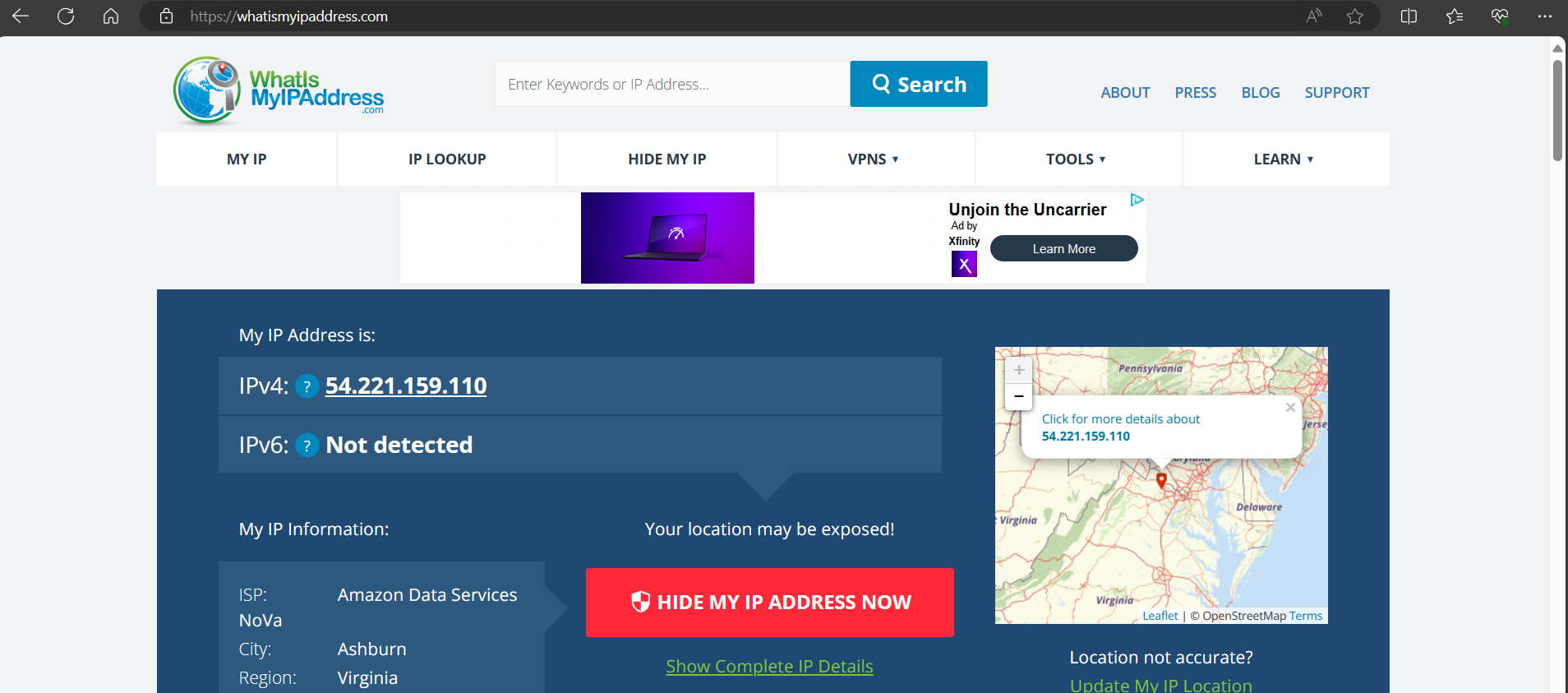
Fonte: Elaboração própria dos autores

**Figura 27: Servidor proxy solicitando usuário e senha para tráfego na internet:**

Fonte: Elaboração própria dos autores

Utilizando-se o site Whats is My IP Address (https://whatismyipaddress.com/) verifica-se que o IP público de navegação do computador conectado ao proxy é o mesmo do proxy server, confirmando que o tráfego de internet está passando por este servidor:

**Figura 28: IP público de navegação**



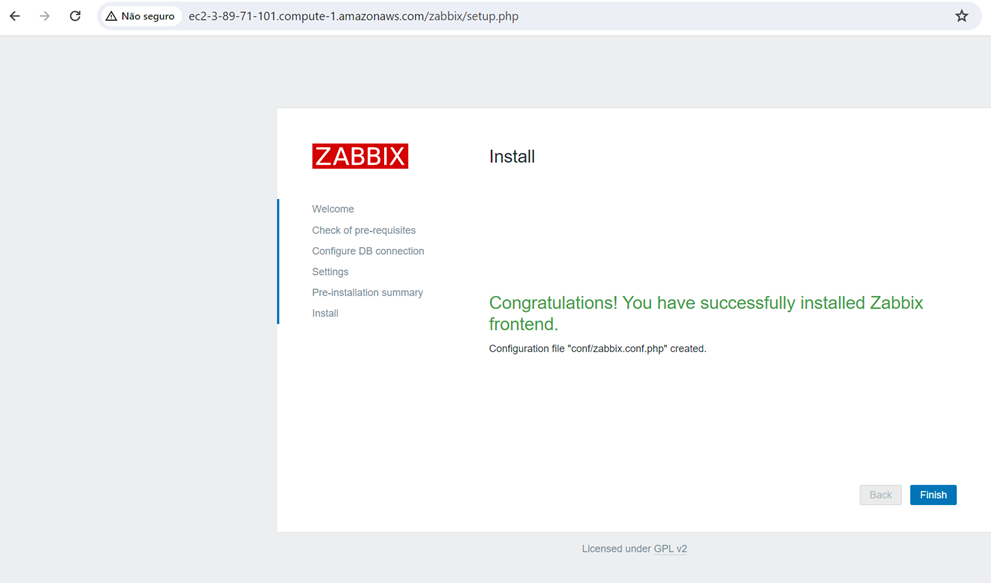
Fonte: Elaboração própria dos autores

**3. Etapa 3 - Gerência e Monitoramento dos Ambientes On-Cloud e On-Premise**

Existem diversas ferramentas de gerenciamento e monitoração de redes, tais como Auvik, SolarWinds, Paessler PRTG Network Monitor e o Zabbix.. Esta última ferramenta foi a escolhida e será utilizada para se obter o status da rede em tempo real, verificando a utilização da CPU, o volume de tráfego (dados lidos e escritos), bem como os horários de picos de utilização da rede, permitindo ainda obter o rastreamento de anomalias ou interrupções no cabeamento ou equipamentos utilizados pela rede da Secretaria de Saúde. Considerando o perfil híbrido da infraestrutura da secretaria, o Zabbix foi configurado para realizar tanto o monitoramento dos servidores que ficam localizados na Secretaria de Saúde quanto nos servidores que ficam na nuvem da AWS.

**3.1 - Monitoramento local/Nuvem**

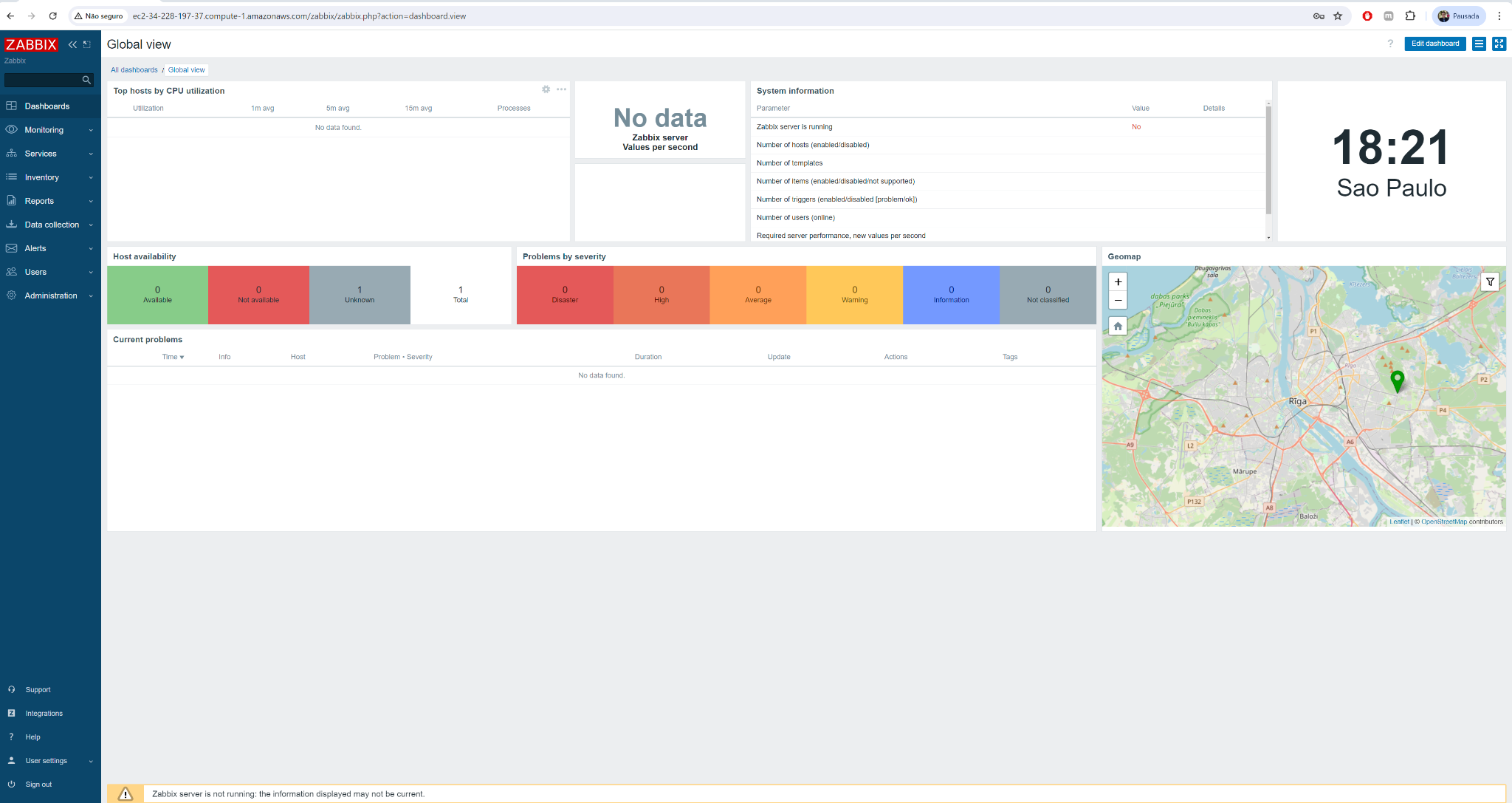
Foi realizada a instalação no servidor Apache, com o banco de dados MYSQL de forma bem sucedida, conforme a Figura 29.

**Figura 29: Instalação bem sucedida do frontend do Zabbix**

**Fonte: Zabbix**

O login foi realizado com sucesso, conforme a Figura 30.

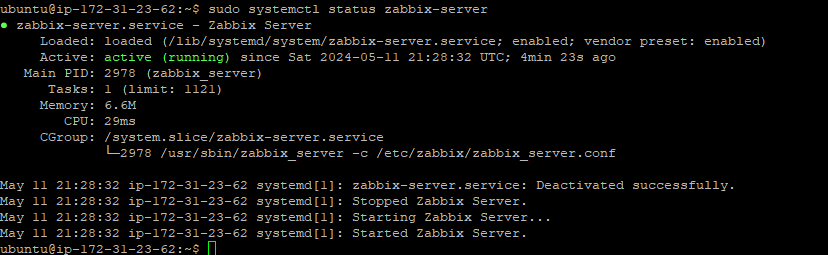
**Figura 30: Acesso ao Zabbix**

****

**Fonte: Zabbix**

O servidor apareceu com o parâmetro “Zabbix server is running” com o value “NO”, o que nos levou à consulta: sudo systemctl status zabbix-server, que mostrou que o servidor estava ativo executando conforme status abaixo:

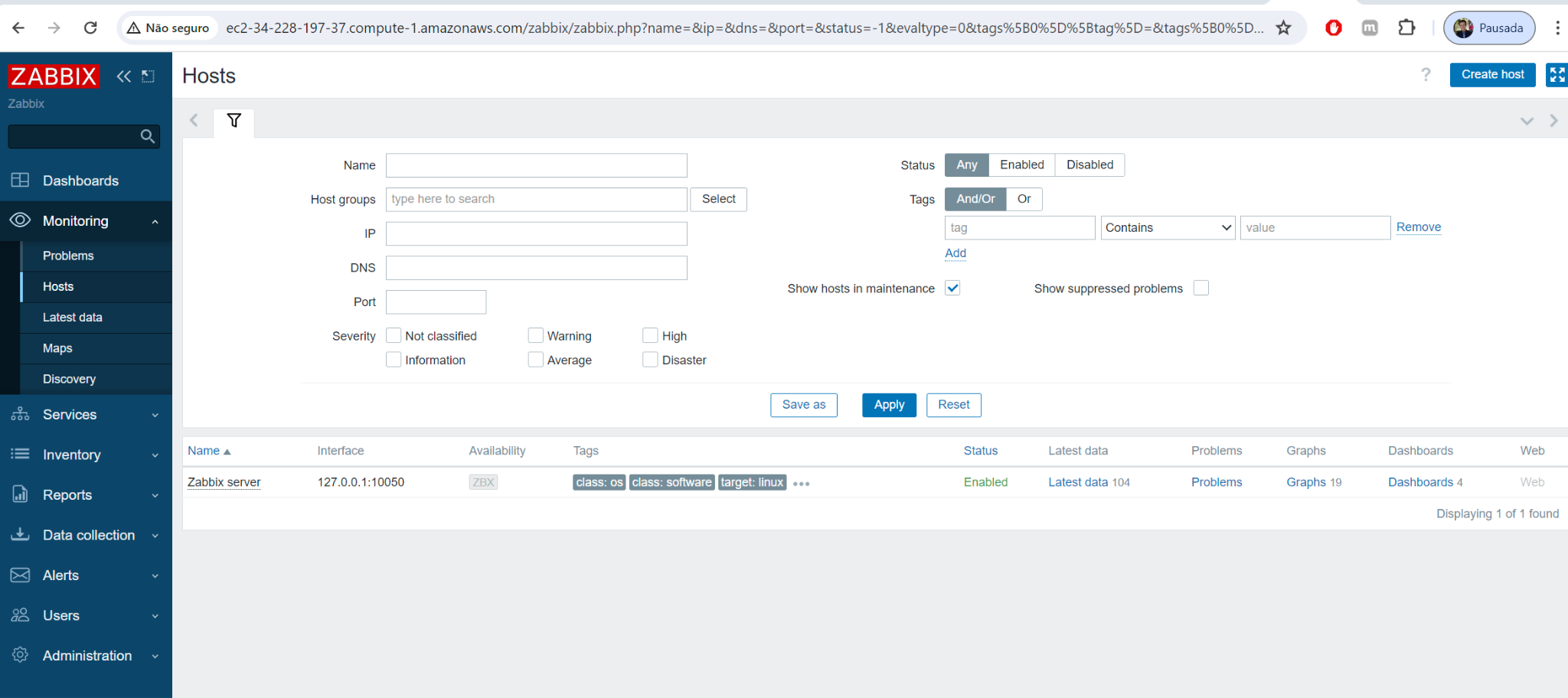
**Figura 31: Teste do servidor Zabbix**

****

**Fonte: Zabbix**

Foram registrados 70 itens monitorados no Zabbix conforme print abaixo:

**Figura 32: Servidor de FTP no Zabbix da AWS**

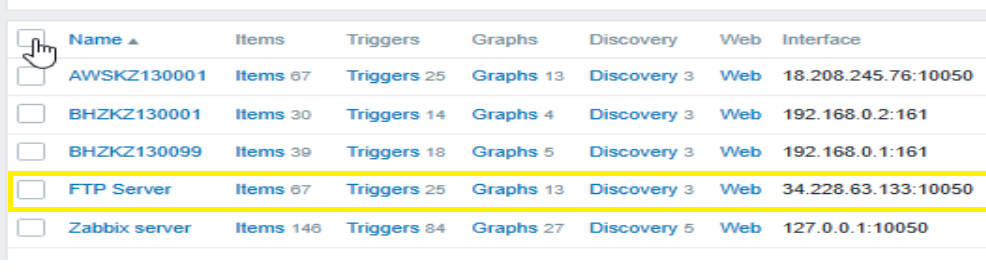


**Fonte: Elaboração própria**

Apesar de criar um novo Host no Zabbix para monitorar o servidor FTP e ter instalado o agent Zabbix nesse servidor, não foi possível monitorar os dados através do Zabbix na AWS. Desta forma, foi escolhido fazer o monitoramento dentro do servidor on premises.

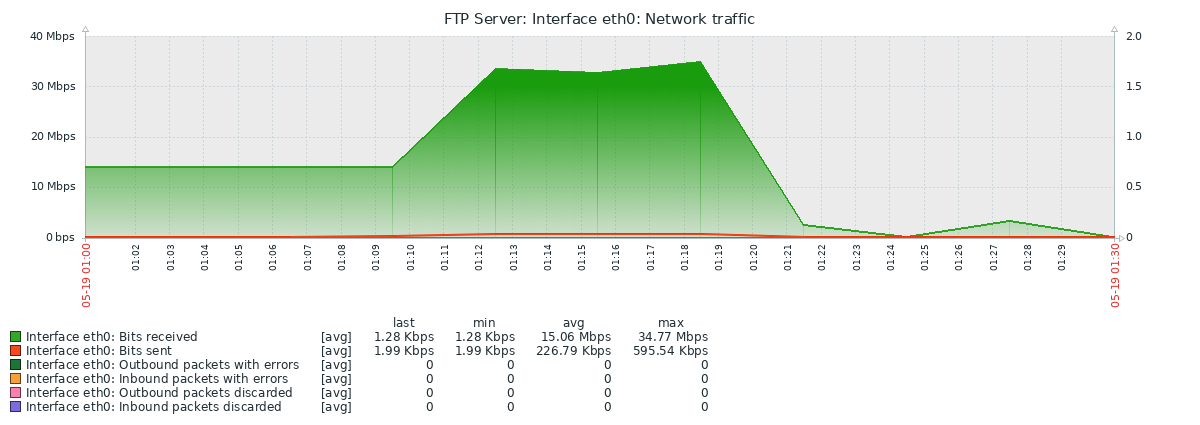
No ambiente on premise foram registrados 67 (sessenta e sete) itens de monitoramento conforme demonstrado abaixo:

**Figura 33: Servidor de FTP no Zabbix On Premise**

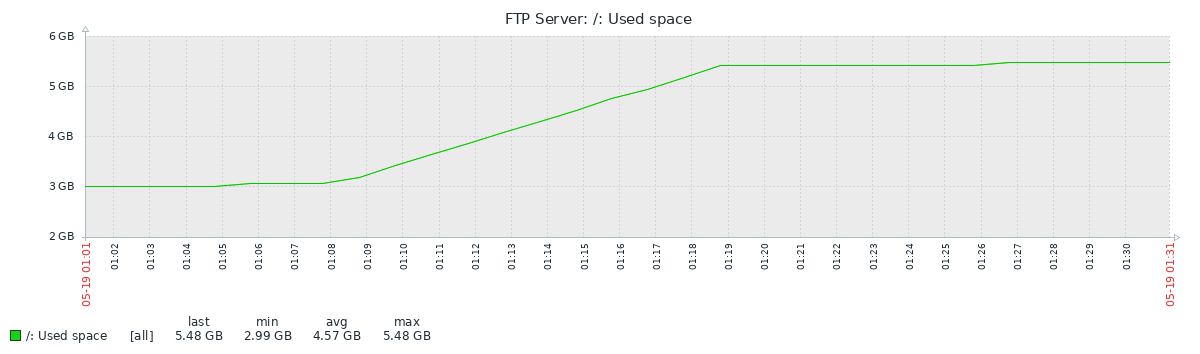


**Fonte: Elaboração própria/Zabbix**

Através da liberação de portas e configuração do Agent no servidor de FTP, foi possível fazer o monitoramento. Foi enviado arquivos via FTP para o servidor de aproximadamente 2,4 GB. Abaixo algumas imagens de monitoramento retiradas do zabbix agent on premise:

**Figura 34: Tráfego de internet do servidor FTP**

**Fonte: Elaboração própria/Zabbix**

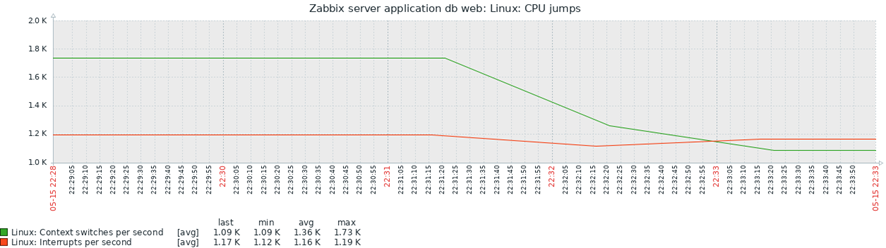
**Figura 35: Evolução do espaço em disco no servidor FTP**

**Fonte: Elaboração própria/Zabix**

Com essas imagens podemos ver que o monitoramento conseguiu demonstrar o desempenho do servidor durante o recebimento de um arquivo de 2.4 GB.

**3.2 - Monitoramento do servidor Web, banco de dados e de aplicação - Cloud**

Para o monitoramento desse servidor foi necessária a instalação dos agentes e servidor Zabbix na máquina virtual EC2 da AWS. Essa máquina é a mesma utilizada nos itens **2.2.3**, **2.2.4** e **2.2.5**, a qual faz o papel de servidor de banco de dados, web e de aplicação. Portanto, essa máquina faz tanto o papel de servidor e agente de monitoramento, pois monitora ela mesma. Abaixo, são mostradas algumas imagens de monitoramento da máquina por um tempo de cinco minutos.

**Figura 36: Monitoramento de saltos do CPU**

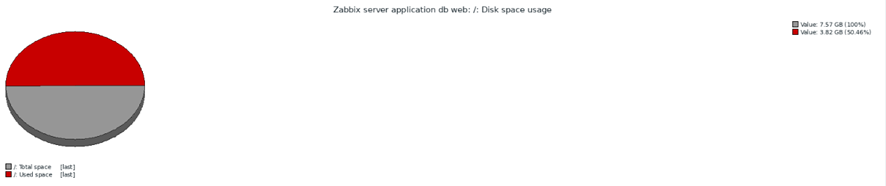
**Fonte: Zabbix**

**Figura 37: Monitoramento do tráfego da rede.**



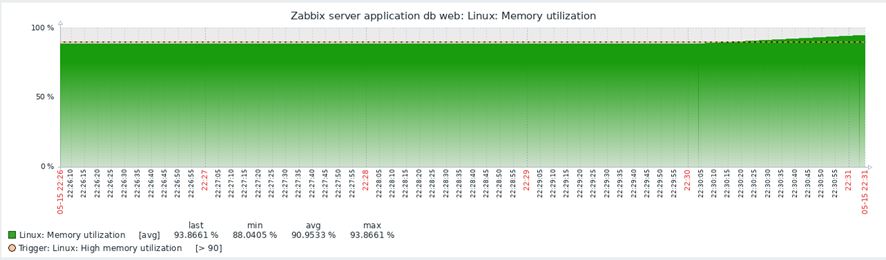
**Fonte: Zabbix**

**Figura 38: Monitoramento do espaço usado no disco.**



**Fonte: Zabbix**

**Figura 39: Monitoramento da utilização da memória.**

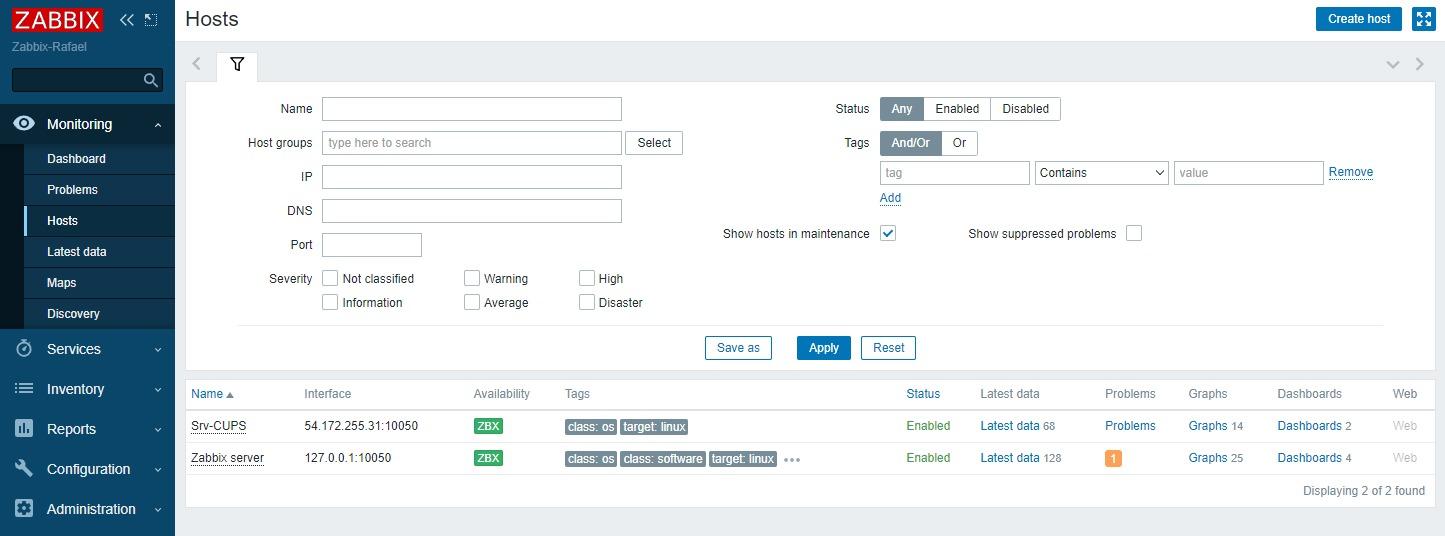


**Fonte: Zabbix**

**3.3 - Monitoramento do servidor de impressão - Cloud**

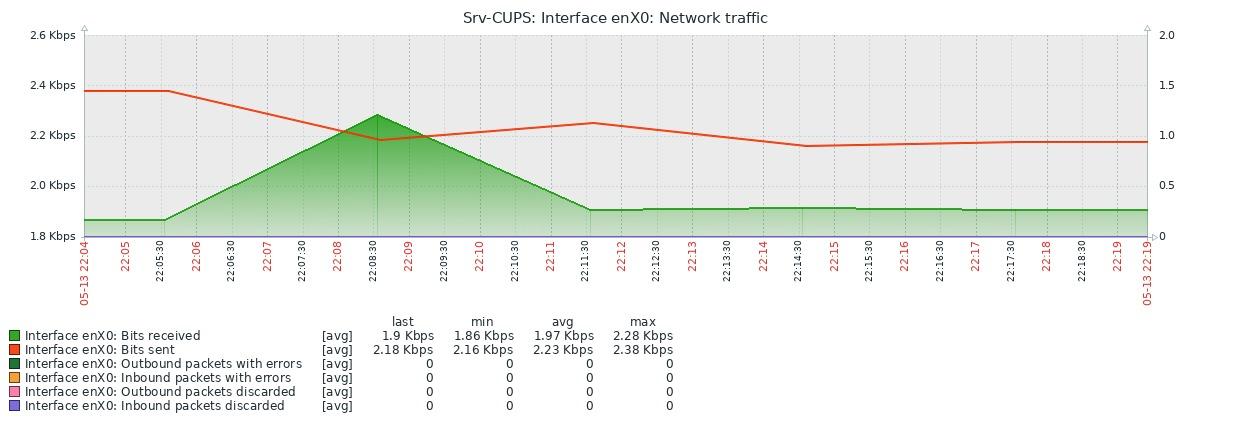
A fim de monitorar o servidor CUPS, foi instanciada uma máquina virtual na AWS com o objetivo de executar o Zabbix Server. O método de monitoramento escolhido foi o Zabbix Agent, o qual foi devidamente instalado e configurado na máquina cliente (host). O Template aplicado foi o Linux by Zabbix Agent.

**Figura 40: Inclusão do host (Srv-CUPS)**

****

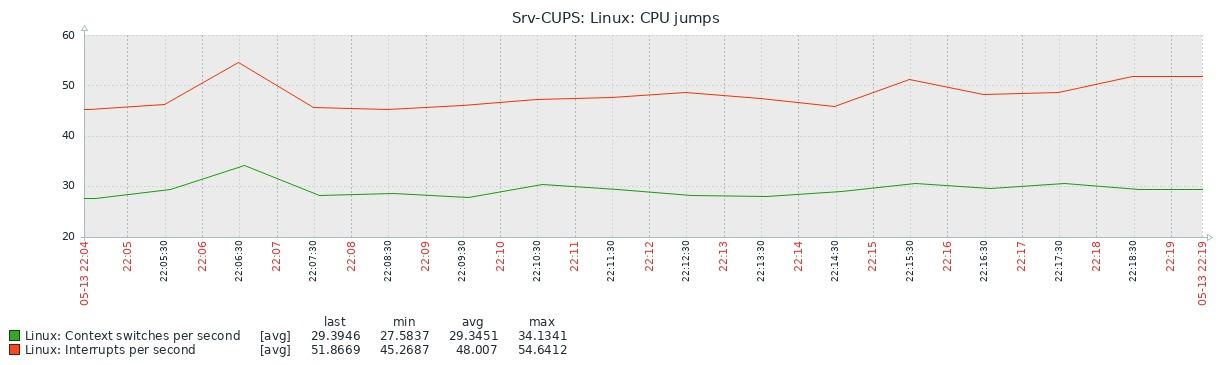
**Fonte: Zabbix**

**Figura 41: Tráfego de rede na interface enX0**

****

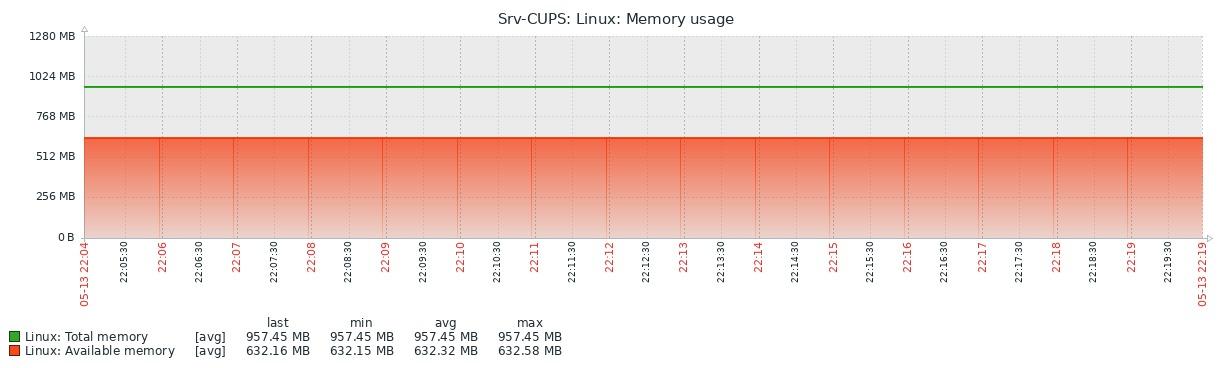
**Fonte: Zabbix**

**Figura 42: Saltos de CPU**

****

**Fonte: Zabbix**

**Figura 43: Uso de memória**

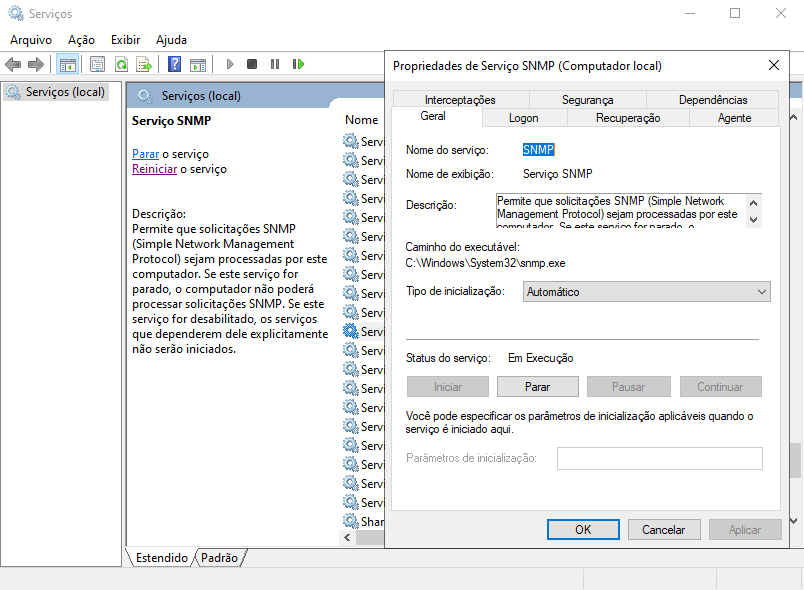
****

**Fonte: Zabbix**

**3.4 - Monitoramento do servidor de AD e DNS - On Premise**

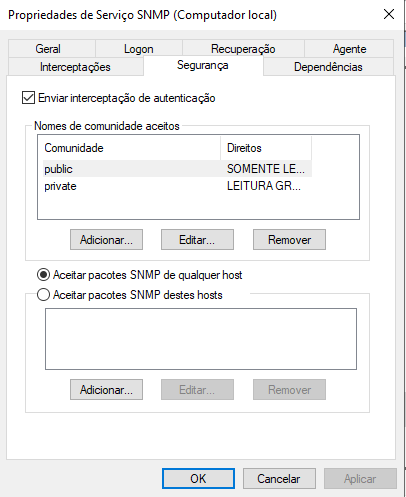
Os servidores de AD e DNS foram colocados no ar por uma mesma máquina Windows Server 2022, instalada em ambiente On Premise, por meio do Hipervisor tipo 2 Oracle VM VirtualBox. O método de monitoramento escolhido foi o protocolo SNMP, tendo o serviço sido configurado conforme se verifica nas imagens seguintes:

**Figura 44: Serviço SNMP ativado**

****

**Fonte: Srv-SES**

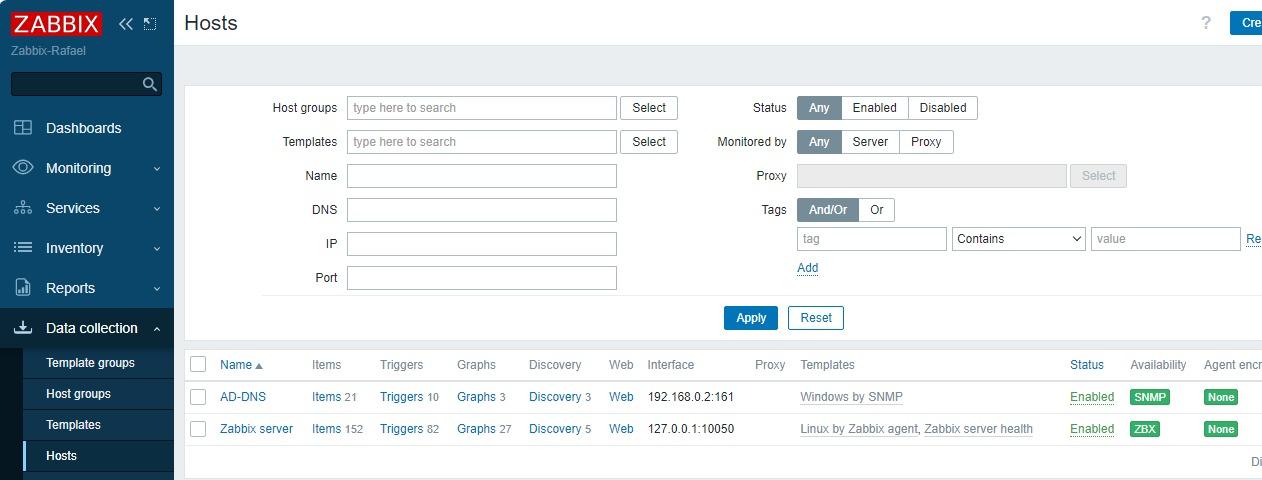
**Figura 45: Configuração da comunidade**

****

**Fonte: Srv-SES**

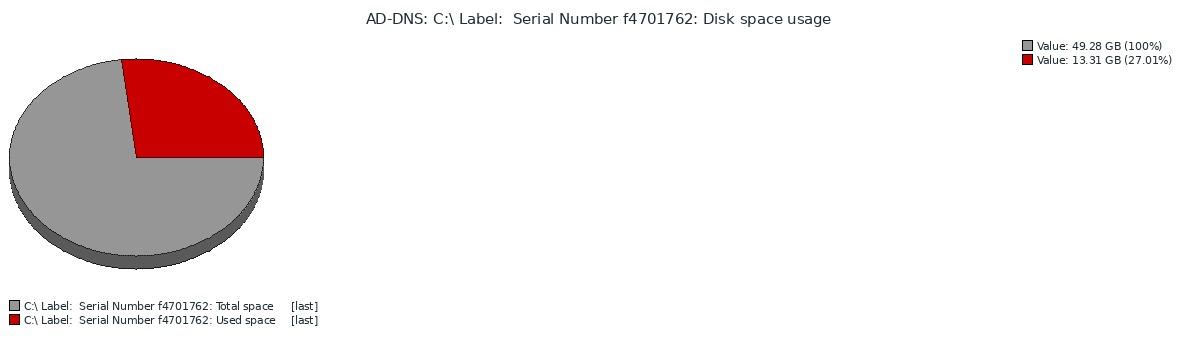
Uma vez configurado, foi criada uma máquina virtual de Zabbix Server no VirtualBox para a inclusão do Srv-SES como host. O template escolhido foi o Windows by SNMP:

**Figura 46: Inclusão do host (Srv-SES)**



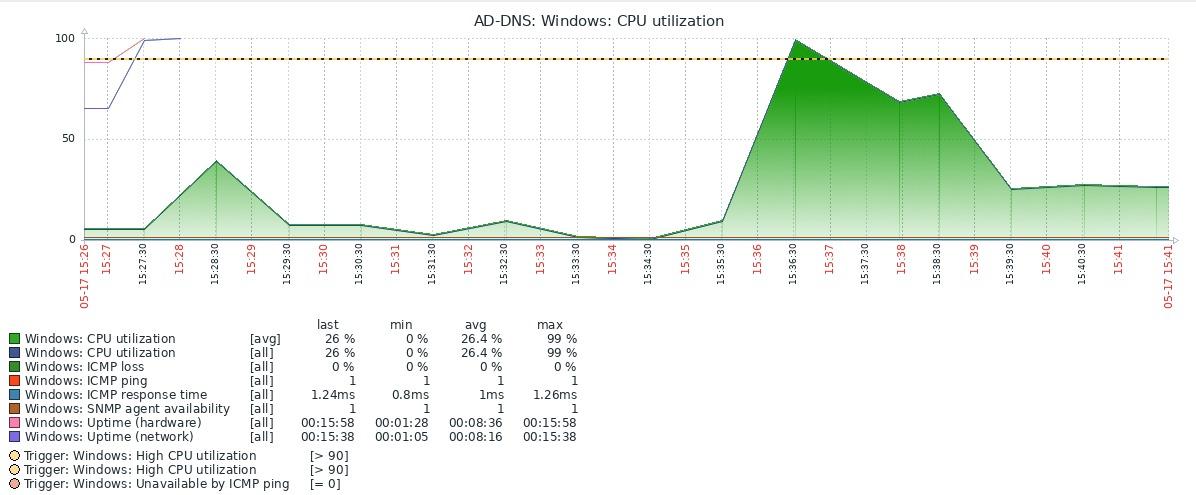
**Fonte: Zabbix**

**Figura 47: Espaço em disco utilizado**



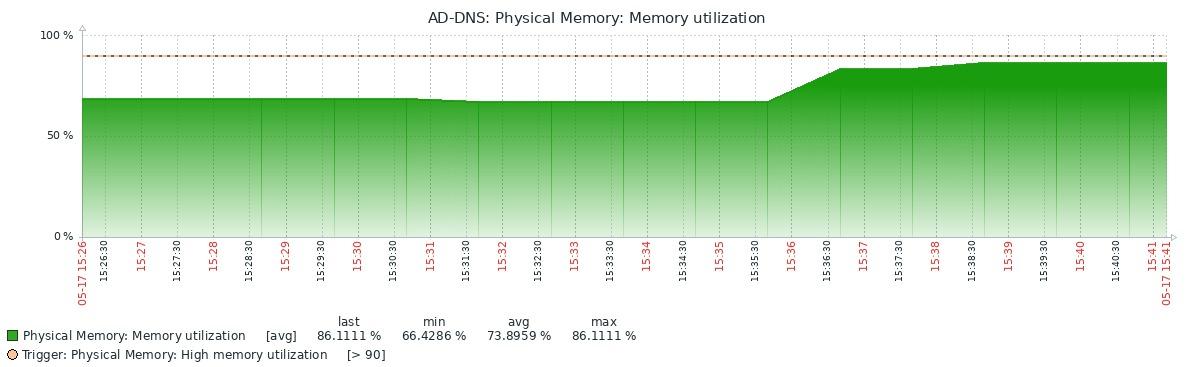
**Fonte: Zabbix**

**Figura 48: Utilização de CPU**

****

**Fonte: Zabbix**

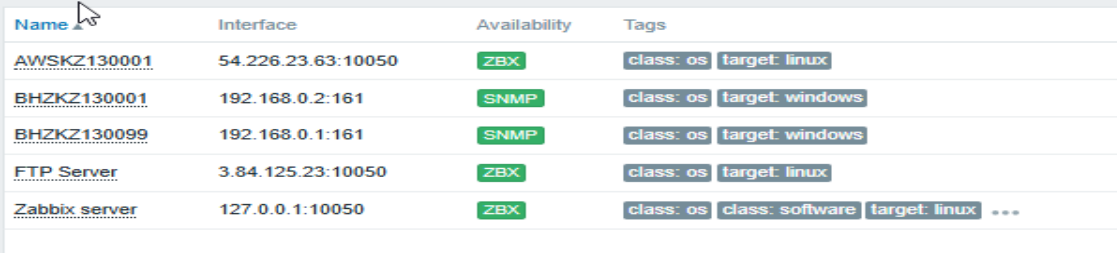
**Figura 49: Utilização de memória**

****

**Fonte: Zabbix**

**3.5 - Monitoramento do servidor de DHCP - On Premise**

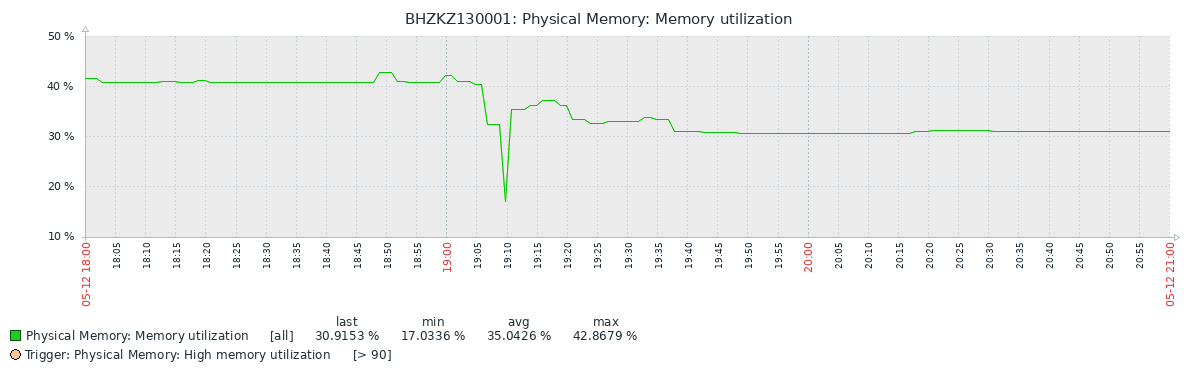
Assim como os servidores de AD e DNS, o servidor DHCP foi concebido em uma máquina cujo sistema operacional é o Windows Server 2022 Standard. Desta forma, a configuração deste ambiente para ser monitorado pelo Zabbix ocorreu de forma semelhante ao destes servidores. A figura abaixo demonstra a conexão efetiva nos servidores monitorados pelo Zabbix On Premise:

**Figura 50: Utilização de memória servidor DHCP**

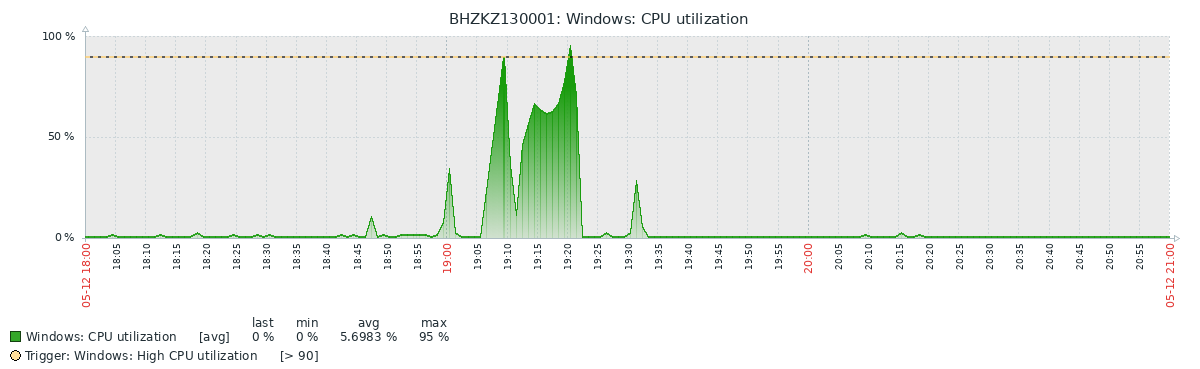
**Fonte: Elaboração própria/Zabbix**

Após a configuração e criação do host do DHCP no servidor Zabbix, foi possível extrair dados de monitoramento em tempo real daquele servidor. Foram realizados testes do monitoramento enviando arquivos para o servidor e análise de como estes envios seriam medidos pelo servidor Zabbix.

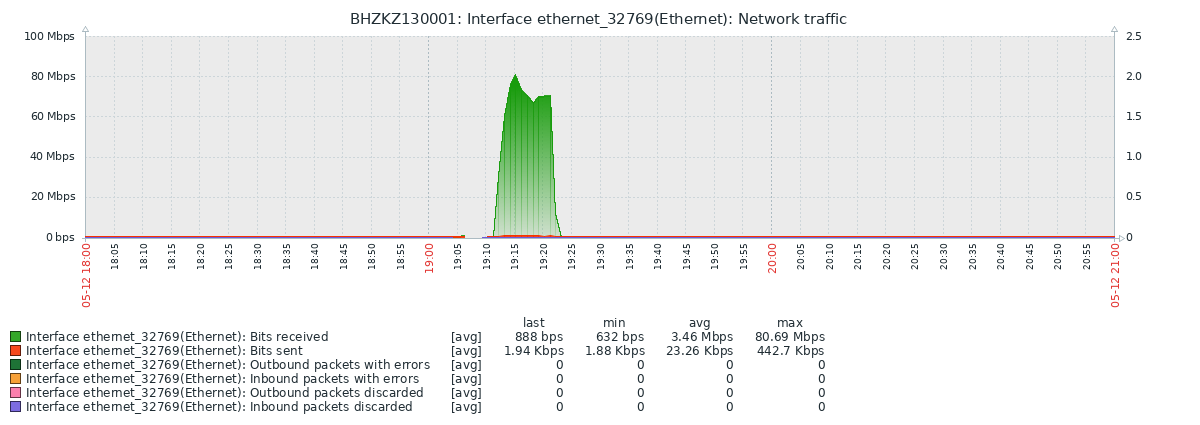
Importante destacar que para a interface dos servidores on premises com a rede mundial de computadores foi-se criado um servidor para funcionar como roteador - BHZKZ130099. Desta forma, toda conexão da internet dos demais servidores on premise passam por este servidor. As imagens abaixo demonstram alguns exemplos de gráficos produzidos pelo servidor de monitoramento:

**Figura 51: Utilização de memória servidor DHCP**

**Fonte: Elaboração própria/Zabbix**

**Figura 52: Utilização de CPU servidor DHCP**

**Fonte: Elaboração própria/Zabbix**

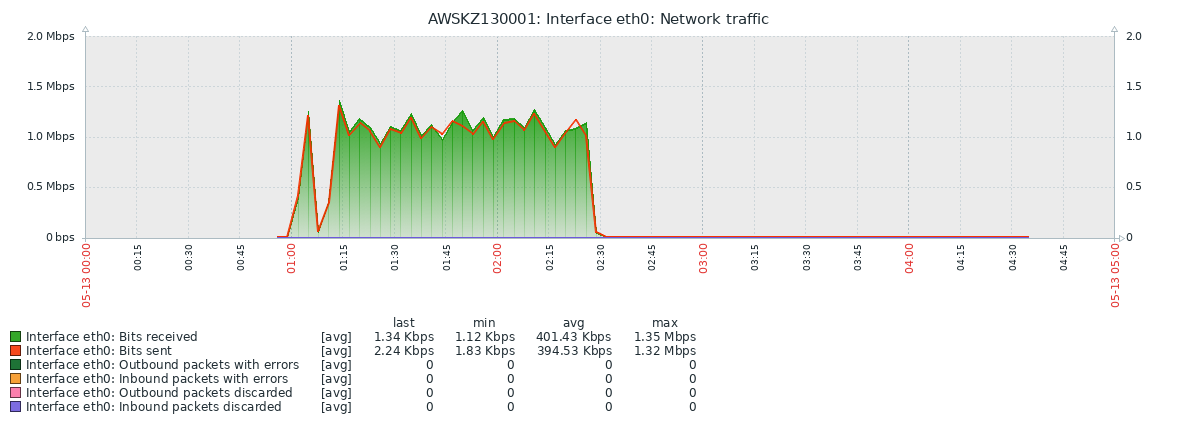
**Figura 53: Taxa de transferência de rede servidor DHCP**

**Fonte: Elaboração própria/Zabbix**

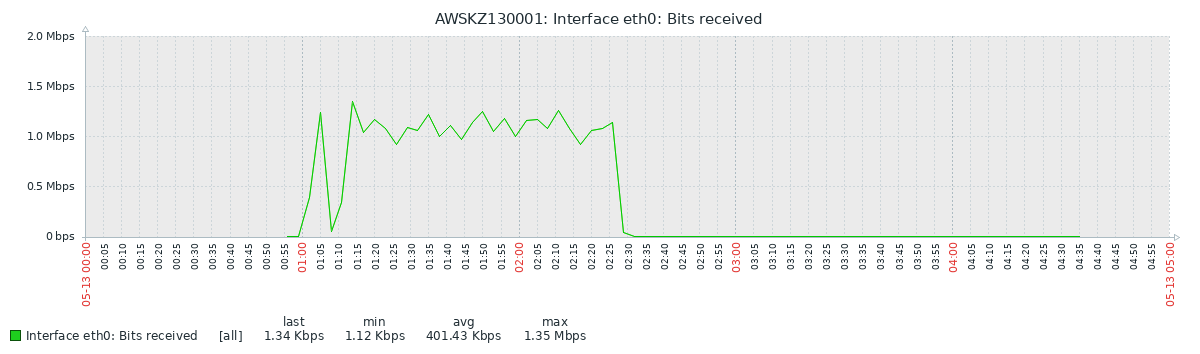
**3.5 - Monitoramento do servidor de Proxy- AWS**

Para o monitoramento do servidor Proxy (AWSKZ130001) na nuvem - AWS - foi instalado o Zabbix Agent neste equipamento. O sucesso da conexão entre o servidor Zabbix e o servidor Proxy na nuvem pode ser visto na Figura 50.

Após configurarmos uma máquina local para que esta utilize o servidor proxy, todo o tráfego de internet desta máquina local é encaminhado, obrigatoriamente, para o servidor proxy. Desta forma, podemos avaliar a efetividade do monitoramento via servidor Zabbix ao simularmos um alto consumo de internet na máquina local. Para o teste, foi realizada a reprodução contínua de vídeos no sítio eletrônico YouTube. Os resultados podemos verificar nas imagens abaixo:

**Figura 54: Taxa de transferência de rede servidor Proxy**

**Fonte: Elaboração própria/Zabbix**

**Figura 55: Taxa de transferência de bits servidor Proxy**

**Fonte: Elaboração própria/Zabbix**

Nestas imagens podemos ver que enquanto houve a execução do vídeo no YouTube a taxa de transferência de rede ficou alta, decrescendo após a finalização desta execução e mantendo-se estável com o baixo consumo da máquina. Desta forma, podemos verificar o êxito no monitoramento através do servidor Zabbix on premises para o servidor em nuvem.

**REFERÊNCIAS**