



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS  
Instituto de Ciências Exatas e de Informática

## Projeto de Infraestrutura de Rede: Universidade - Instituto Acadêmico de Excelência (IAE)\*

Antônio Rubens O. Junqueira<sup>1</sup>  
Arthur Neves da Silveira<sup>2</sup>  
Beatriz Pereira da Costa<sup>3</sup>  
Denis Alves da Silva Leite<sup>4</sup>  
Laís Lara Ferreira dos Santos<sup>5</sup>  
Sávio Sérgio Pereira da Silva<sup>6</sup>  
Fábio Leandro Rodrigues Cordeiro<sup>7</sup>

### Resumo

O projeto de infraestrutura de redes do Instituto Acadêmico de Excelência (IAE) foi planejado para criar um ambiente de TI estável e seguro, abrangendo o planejamento físico-lógico, a virtualização, os serviços em nuvem e o monitoramento, utilizando uma topologia em estrela para conectar seus quatro campi eficientemente. A preparação do ambiente incluiu a virtualização de servidores via VirtualBox e a implementação de serviços na nuvem AWS EC2. A gerência e monitoramento de ambientes de redes foram realizados com Zabbix, analisando métricas que confirmaram o desempenho da infraestrutura. Robustos mecanismos de segurança da informação foram implementados via Política de Segurança da Informação (PSI), uma Cartilha de Boas Práticas e análise de vulnerabilidades OWASP Top 10, abordando e mitigando os principais riscos. Em conclusão, a solução projetada é tecnicamente sólida, escalável e segura para as demandas atuais e futuras da IAE.

**Palavras-chave:** Infraestrutura de Redes; Virtualização; Serviços em Nuvem; Segurança da Informação; Monitoramento de Redes.

\*Artigo apresentado ao Instituto de Ciências Exatas e Informática da Pontifícia Universidade Católica de Minas Gerais, campus PUC Minas Virtual, como pré-requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

<sup>1</sup>Aluno(a) do Programa de Graduação em Sistemas de Informação – [antonio.junqueira@sga.pucminas.br](mailto:antonio.junqueira@sga.pucminas.br).

<sup>2</sup>Aluno(a) do Programa de Graduação em Sistemas de Informação – [asilveira@sga.pucminas.br](mailto:asilveira@sga.pucminas.br).

<sup>3</sup>Aluno(a) do Programa de Graduação em Sistemas de Informação – [beatriz.costa.1440855@sga.pucminas.br](mailto:beatriz.costa.1440855@sga.pucminas.br).

<sup>4</sup>Aluno(a) do Programa de Graduação em Sistemas de Informação – [dasleite@sga.pucminas.br](mailto:dasleite@sga.pucminas.br).

<sup>5</sup>Aluno(a) do Programa de Graduação em Sistemas de Informação – [laís.lara@sga.pucminas.br](mailto:laís.lara@sga.pucminas.br).

<sup>6</sup>Aluno(a) do Programa de Graduação em Sistemas de Informação – [savio.sergio@sga.pucminas.br](mailto:savio.sergio@sga.pucminas.br).

<sup>7</sup>Professor(a) do Programa de Graduação em Sistemas de Informação – [fabio@pucminas.br](mailto:fabio@pucminas.br).

## 1 ANÁLISE, PLANEJAMENTO E PROTOTIPAÇÃO DA SOLUÇÃO

O projeto de infraestrutura de redes da universidade Instituto Acadêmico de Excelência (IAE) tem como foco criar um ambiente de TI estável e seguro. A iniciativa contempla o planejamento físico e lógico da rede, a virtualização de servidores locais, a implantação de serviços na nuvem e o uso de ferramentas de monitoramento como o Zabbix. Também foram adotadas práticas de segurança da informação para garantir a integridade, disponibilidade e confidencialidade dos dados institucionais.

Este projeto tem como objetivo planejar e implementar uma infraestrutura de rede que permita conectividade segura e eficiente entre os diferentes campi da universidade. A iniciativa busca integrar os serviços acadêmicos e administrativos por meio de soluções tecnológicas avançadas, garantindo acesso otimizado à internet, gerenciamento de usuários e proteção dos dados institucionais.

### 1.1 Análise da Solução

Instituto Acadêmico de Excelência (IAE), fundado em 05 de março de 1995. Momento histórico em que um grupo de seis estudantes recém-mestrados realizou o sonho de fazer a diferença na educação superior do país, preparando líderes críticos e agentes de mudança no mundo. Para isso, criaram uma instituição que poderia inspirá-los a enfrentar os desafios além do meio acadêmico.

Com o objetivo de promover o acesso ao conhecimento e à educação na cidade de Belo Horizonte, capacitando indivíduos para que possam não apenas expandir suas habilidades, mas também compartilhar seu aprendizado com o mundo.

Após 30 anos da sua fundação, a IAE possui atualmente o total de 5.760 alunos, 185 professores e 156 outros funcionários, sendo todos distribuídos por quatro campi em Belo Horizonte e região metropolitana, conforme distribuição da Tabela 1.

**Tabela 1 – Relação de alunos, salas, professores e funcionários dos campi.**

Nome	Alunos	Salas	Professores	Funcionários
Campus 1	3600	105	105	80
Campus 2	1260	37	37	33
Campus 3	900	27	27	28
Campus 4	320	16	16	15

**Fonte:** Elaborado pelos autores

A IAE oferece cursos presenciais das áreas de Ciências Exatas, Ciências Humanas, Saúde, Engenharia e Tecnologia. A sede (Campus 1) contempla as áreas sociais, saúde e engenharias, o Campus 2 e 3 abrangem áreas sociais e humanas e o Campus 4 de extensão apenas as práticas de saúde. A distribuição completa entre os campi pode ser observada por meio do seguinte documento: [Diagrama dos Cursos do IAE](#).

## 1.2 Planejamento da Solução

### 1.2.1 *Missão, Visão e Valores da Universidade*

A IAE tem como missão promover o acesso ao conhecimento e à educação, capacitando indivíduos para que possam não apenas expandir suas habilidades, mas também compartilhar seu aprendizado com o mundo. Buscando criar um ambiente onde o saber é disseminado de forma a transformar o ser humano, tanto pessoal quanto profissionalmente, e oferecer cursos de graduação em diversas áreas do conhecimento.

Possui como visão ser reconhecida como uma instituição de referência em educação, inovação e inclusão, que prepara indivíduos para se tornarem líderes críticos e agentes de mudança no mundo. Tendo como objetivo promover o desenvolvimento pleno dos alunos e inspirá-los a enfrentar os desafios além do meio acadêmico, contribuindo, assim, para um futuro mais justo e sustentável.

Seus valores: Foco em Inovação, Ética, Pesquisa, Sustentabilidade, Compromisso com o ensino e com a comunidade, Diversidade e Inclusão.

### 1.2.2 *Estruturas dos Campi*

- Laboratórios Clínicos: Destinados ao atendimento ao público e às práticas supervisoriadas. Possui 1 computador destinado ao atendimento. Atende os cursos de Medicina, Fisioterapia, Nutrição, Odontologia, Psicologia, Educação Física, Enfermagem e Farmácia.
- Laboratórios de Informática: Focados no desenvolvimento de documentos e pesquisas. São equipados com computadores básicos, otimizados para o uso de Office e softwares de baixo custo de recursos.
- Laboratórios de Desenvolvimento: Destinados ao uso de softwares robustos, como engenharia e desenvolvimento de sistemas. Atendem os cursos de Engenharia, Sistemas de Informação e Ciências da Computação.
- Sala Interativa: Com espaço destinado à interação de alunos e professores. Conta com 2 computadores básicos e é utilizada para ensino dinâmico, como simulação, desenvolvimento de projetos em grupo e outras atividades práticas.
- Studio Audiovisual: Voltado para a produção de conteúdos multimídia. Possui 2 computadores específicos para a gravação, edição de vídeos, imagens e áudio, além de transmissões ao vivo.

- Laboratórios de Química: Usados para ensino de química, experiências e análises. Equipados com computadores básicos para apoiar a avaliação de resultados e a consulta de fontes.

### 1.3 Prototipação da Solução

#### 1.3.1 Mapeamento de Serviços

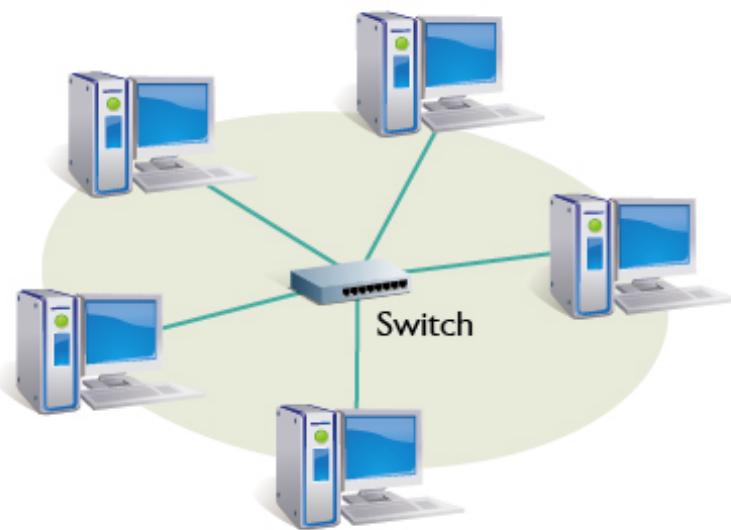
- Servidores Web e Banco de Dados: Utilizados pelos sistemas da universidade (biblioteca, matrícula, finanças, etc.). Armazenam e gerenciam dados específicos de cada serviço.
- DHCP (*Dynamic Host Configuration Protocol*): Atribui automaticamente endereços IP e configurações de rede a dispositivos, como computadores e smartphones.
- DNS (*Domain Name System*): Resolve nomes de domínios para endereços IP, facilitando o acesso a recursos internos e externos da universidade.
- LDAP (*Lightweight Directory Access Protocol*): Gerencia autenticação, organização e controle de usuários e grupos na rede institucional.
- Serviço de FTP (*File Transfer Protocol*): Usado para compartilhar e transferir materiais acadêmicos, backups e outras informações.
- Rede: Segregada entre redes acadêmicas, administrativas e de visitantes, compartilhando wi-fi para alunos e funcionários.
- NFS (*Network File System*): Compartilha diretórios e arquivos entre servidores e computadores, centralizando o armazenamento de conteúdos acadêmicos.
- Proxy e Cache (*Squid*): Filtra e controla o acesso à internet, bloqueando conteúdos inadequados e otimizando o tráfego.
- Firewall e Segurança: Protege a rede contra ataques, controla o tráfego e controla o acesso físico às instalações, como nas catracas.

#### 1.3.2 Topologia e Protótipo da Solução na Cisco Packet Tracer

A topologia escolhida para a implementação da rede do Instituto Acadêmico de Excelência foi a topologia em estrela. Essa abordagem consiste na ligação de todos os dispositivos da rede — como computadores, switches e roteadores — a um ponto central, que neste caso é o switch principal. Assim, cada dispositivo se conecta diretamente ao ponto central, formando uma estrutura que se assemelha a uma estrela.

A opção pelo modelo em estrela deu-se principalmente pelo seu alto grau de simplicidade, tanto na administração quanto na manutenção da rede. Em um ambiente como o de uma universidade, onde existem várias estações de trabalho compartilhando recursos, é preciso que o tráfego seja gerenciado de forma organizada e que problemas específicos — como a falha de um determinado ponto da rede — não interfiram na comunicação de toda a estrutura. Na topologia em estrela, se um computador apresentar problemas ou for removido da rede, ele não afeta o funcionamento das outras estações, sendo o ponto central o responsável pelo roteamento da comunicação. A Figura 1 apresenta o esquema da topologia implementada.

**Figura 1 – Representação da Topologia Estrela**



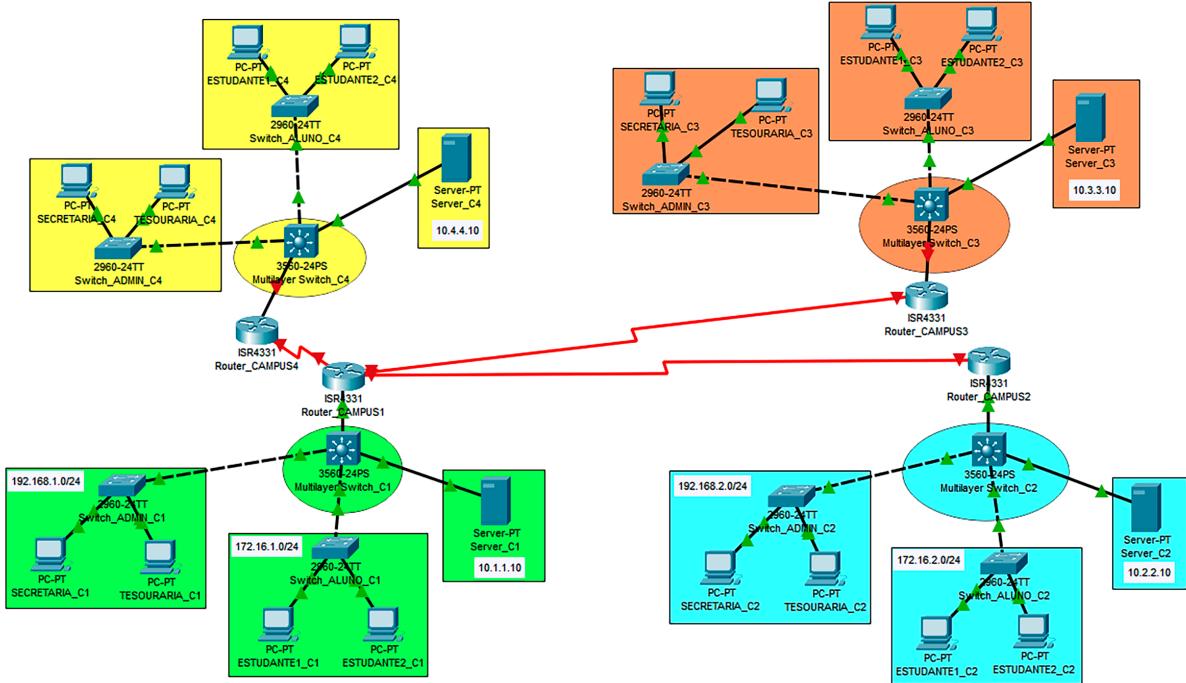
**Fonte:** (Digital, 2018)

Além disso, essa topologia proporciona escalabilidade, sendo relativamente simples acrescentar novos computadores ou dispositivos à rede, bastando conectá-los ao ponto central. Dessa forma, o modelo em estrela estendida revela-se conveniente para atender às necessidades de uma instituição de ensino, que apresenta crescimento gradual tanto de usuários quanto de recursos compartilhados.

Com base nessa abordagem, o protótipo da rede da IAE foi criado no Cisco Packet Tracer, a fim de simular o tráfego de dados, o compartilhamento de recursos e o comportamento da rede na presença de diferentes dispositivos. A Figura 2 mostra o protótipo em execução no software, evidenciando tanto o posicionamento de computadores, switches e roteador quanto o tráfego de pacotes entre eles.

### **1.3.3 Planilha de Equipamentos**

A planilha de equipamentos desempenha um papel fundamental no desenvolvimento do projeto de infraestrutura de redes da universidade. Por meio dela, é possível ter uma visão clara e organizada de todos os dispositivos necessários para atender às demandas de conectividade

**Figura 2 – Protótipo da Rede no Cisco Packet Tracer**

**Fonte:** Elaborado pelos autores

em cada um dos campi.

Com essa informação, o planejamento torna-se mais preciso, facilitando tanto o dimensionamento da rede quanto a alocação de recursos, a avaliação de custos e a futura manutenção da infraestrutura. Dessa forma, a planilha proporciona uma base consistente para a implementação da rede de forma eficiente e adequada às necessidades da instituição. Logo abaixo, a Tabela 2 é referente às salas de aula da sede da IAE. A planilha completa, com as informações de todos os quatro campi, pode ser acessada pelo [link](#).

#### 1.3.4 Planilha de Endereçamento de IPs

A planilha de endereçamento de IP apresenta a organização lógica da rede da universidade, detalhando, para cada campus e sala, o nome, o endereço IP, a máscara de sub-rede, o gateway e o range de IPs disponíveis. Essa organização é fundamental para garantir uma administração mais clara e eficiente da rede, facilitando tanto a manutenção quanto a escalabilidade da estrutura. A coluna de DHCP IP permanecerá vazia neste momento, sendo reservada para uma futura implementação de alocação dinâmica de endereços, se necessária. Logo abaixo, na Tabela 3 estão os endereços IPs referentes à sede do IAE e do Campus 2. A planilha completa, com as informações de todos os quatro campi, pode ser acessada pelo [link](#).

**Tabela 2 – Equipamentos das salas de aula do Campus 1.**

Planilha de Inventário de Equipamentos - Campus 1 / Sede					
Tipo Ativo	Modelo	Fabricante	Quantidade	Valor	Valor Total
Computador	OptiPlex Micro i3-12100T 8gb DDR5 256GB win 11 Pro	Dell	105	4.248,00	446.040,00
Monitor	Monitor Dell de 21.5"SE2222H	Dell	105	729,00	76.545,00
Projetor	Projetor Powerlite E20 Epson	Epson	105	3.599,10	377.905,50
Mesa Escritório	ESCRIVANINHA OFFICE PRESENCE BRANCO - DEMÓBILE Branca	Demóbile	105	239,90	25.189,50
Cadeira Escritório	Cadeira Ágata Gerente Gir Braço Regulável Courvim Preto	IdeaFlex	105	366,00	38.430,00
Cadeira Universitária	Cadeira Ágata Secretária Universitária Pé palito Tecido kit 5 un	IdeaFlex	420	931,50	391.230,00
Cabo de Rede	Cabo de Rede Cat6 MPT Azul, 1 Metro	MPT Cable	2100	3,89	8.169,00
Conector	Conector Rj45 Cat6 Soho Plus Furukawa Macho	Furukawa	105	3,97	416,85
Keystone	Conectores Rj45 Femea Keystone Furukawa Multilan Cat6	Furukawa	105	33,00	3.465,00
Placa Espelho	Espelho Modular 4x2 com 1 Saída Branco - 4306	Central Cabos	105	5,00	525,00
Patch Corde	Patch Cord Cat6 1.5m Furukawa	Furukawa	105	9,90	1.039,50
Ar condicionado	Ar Condicionado Split Hw Inverter Philco	Philco	105	2.231,55	234.312,75

**Fonte:** Elaborado pelos autores

### 1.3.5 Cálculo de Links

A planilha Cálculo de Links de Dados e de Internet apresenta o dimensionamento da largura de banda necessária para atender às demandas de comunicação da universidade em seus quatro campi, considerando o tráfego gerado pelos principais serviços e aplicações utilizadas, como Internet Banking, Videoconferência, Sistema Legado, Suporte Remoto, Web, E-mail e ERP. Ela proporciona uma visão clara e detalhada da capacidade de tráfego exigida, sendo uma ferramenta importante tanto para o planejamento da rede quanto para garantir um desempenho satisfatório e uma conectividade estável para todos os usuários. O cálculo realizado pode ser observado na Figura 3.

**Tabela 3 – Endereços IPs da sede da IAE e Campus 2.**

Planilha de IPs					
Nome	IP address	Subnet Mask	IP Gateway	IP Range	IP DHCP
Campus 1: Administrativo	192.168.1.0/24	255.255.255.0	192.168.1.1	192.168.1.1 - 192.168.1.254	192.168.1.10 - 192.168.1.254
Campus 1: Alunos	172.16.1.0/24	255.255.255.0	172.16.1.1	172.16.1.1 - 172.16.1.254	172.16.1.10 - 172.16.1.254
Campus 1: Servidores	10.1.1.0/24	255.255.255.0	10.1.1.1	10.1.1.10	
Campus 2: Administrativo	192.168.2.0/24	255.255.255.0	192.168.2.1	192.168.12.1 - 192.168.12.254	192.168.12.10 - 192.168.12.254
Campus 2: Alunos	172.16.2.0/24	255.255.255.0	172.16.2.1	172.16.12.1 - 172.16.12.254	172.16.12.10 - 172.16.12.254
Campus 2: Servidores	10.2.2.0/24	255.255.255.0	10.2.2.1	10.2.2.10	

Fonte: Elaborado pelos autores

**Figura 3 – Cálculo de Links de Dados e de Internet**

Cálculo de Links de dados e de Internet									
Necessidades Corporativas		Campus 01/Matriz = 232		Campus 02 = 77		Campus 03 = 64		Campus 04 = 19	
Aplicação	Requisitos (kbps)	Quantidade	Total (kbps)	Quantidade	Total (kbps)	Quantidade	Total (kbps)	Quantidade	Total (kbps)
Internet Banking	1200	4	4800	0	0	0	0	0	0
Videoconferência	1800	5	9000	1	1800	1	1800	1	1800
Sistema Legado	200	11	2200	6	1200	6	1200	2	400
Supporte Remoto	800	7	5600	5	4000	5	4000	1	800
Web	1600	3884	6214400	1330	2128000	955	1528000	338	540800
E-mail	400	3884	1553600	1330	532000	955	382000	338	135200
ERP	400	10	4000	6	2400	6	2400	1	400
		Total App	7793600	Total App	2669400	Total App	1919400	Total App	679400
		Total Internet	7776800	Total Internet	2662400	Total Internet	1912400	Total Internet	676400
		Link Internet		Link Matriz <--> C 02		Link Matriz <--> C 03		Link Matriz <--> C 04	
Redutor capacid.	1	13028000		2662400		1912400		676400	

Fonte: Elaborado pelos autores

## 2 PREPARAÇÃO DO AMBIENTE EM NUVEM E VIRTUALIZAÇÃO LOCAL

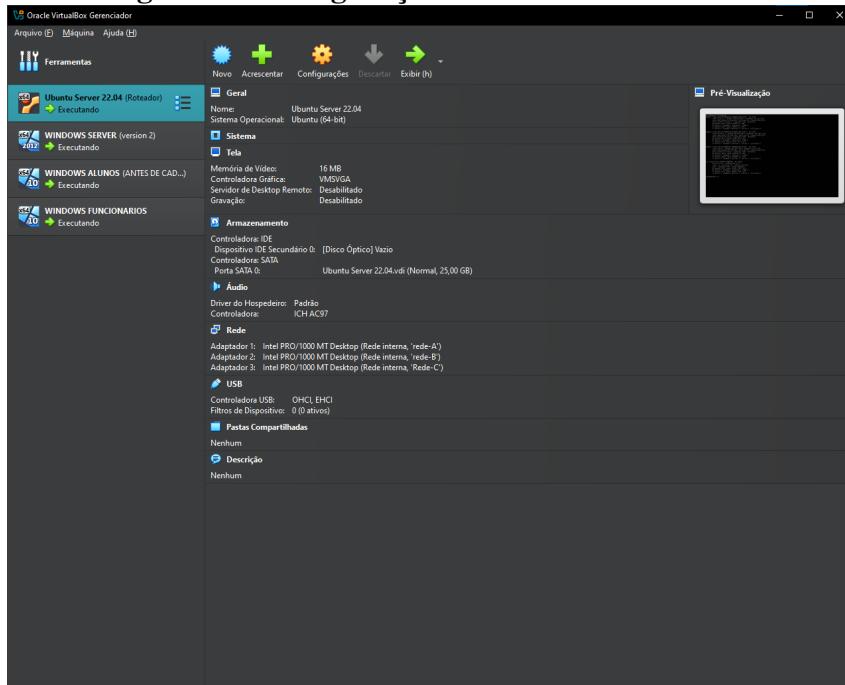
O VirtualBox foi utilizado para criar máquinas virtuais, segmentando a rede entre alunos, administradores e servidores. Cada MV foi configurada com IPs estáticos, garantindo conectividade e controle adequado de acesso. Já na nuvem, foram criadas instâncias EC2 para hospedar serviços críticos, otimizando disponibilidade e escalabilidade. A configuração incluiu regras de segurança e comunicação entre servidores locais e na nuvem. Para demonstrar que cada serviço instalado localmente e na nuvem estavam funcionando como o esperado, foi gravado um vídeo com testes de uso. Para acessá-lo, basta entrar no [Link](#).

## 2.1 Serviços em Máquinas Virtuais Locais pelo VirtualBox

### 2.1.1 Servidor DHCP

Tela demonstrativa da instalação e configuração do VirtualBox e da instalação de 4 máquinas virtuais, sendo o Ubuntu Server, Windows Server e dois Windows Pro de funcionário e de aluno. Na Figura 4 são observadas as configurações do Ubuntu Server utilizado, as 3 redes que foram criadas para os diferentes níveis de acesso: Rede A (Alunos): 172.16.0.0/24 - Destinada aos alunos e laboratórios; Rede B (Administrativo): 192.168.1.0/24 - Destinada aos funcionários e dispositivos administrativos; Rede C (Servidores): 10.0.0.0/24 - Rede dedicada para hospedar os servidores críticos da instituição. A Figura 5 mostra a configuração da Rede A, e a Figura 6 mostra a interface de Rede no Ubuntu ao utilizar o comando "ifconfig".

**Figura 4 – Configuração do VirtualBox e Redes**



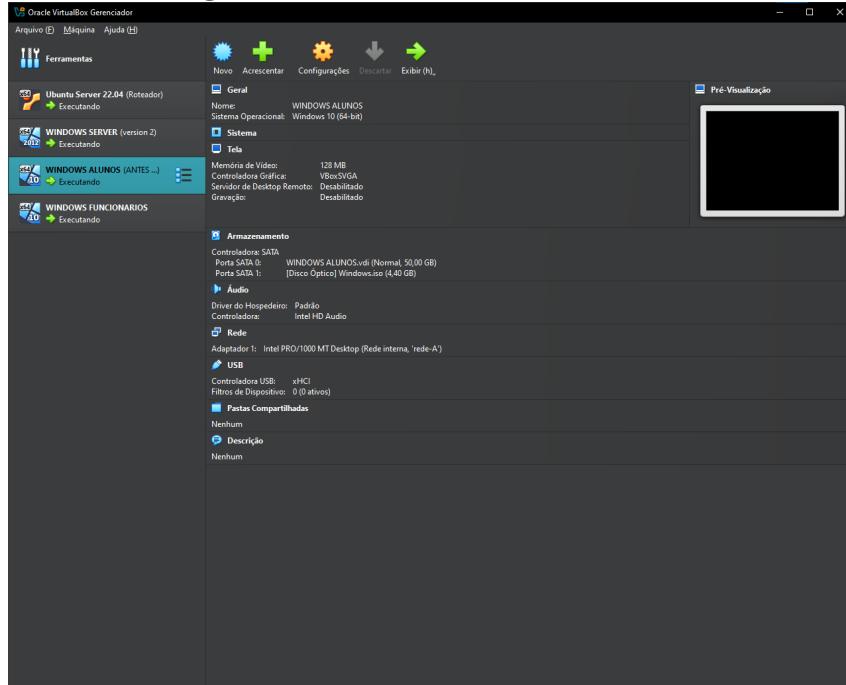
**Fonte:** Elaborado pelos autores

Cada máquina está em execução (Running) com as configurações de CPU, memória e disco de cada máquina. A Figura 6 mostra a configuração de rede, ou seja, as placas adaptadas para a comunicação entre as VMs.

A tela do comando ifconfig no Ubuntu, na Figura 6, mostra informações detalhadas sobre todas as interfaces de rede do sistema, incluindo: Nome da interface, Endereço IPv4, Máscara de sub-rede, Endereço IPv6, Endereço MAC, Status da Interface, Pacotes enviados e recebidos, e Informações de broadcast e multicast. Redes configuradas:

- enp0s3 - IP 172.16.0.1 (corresponde à rede dos alunos)
- enp0s8 - IP 192.168.1.1 (corresponde à rede administrativa)

**Figura 5 – Windows Aluno na Rede A**



Fonte: Elaborado pelos autores

**Figura 6 – Interfaces de Rede no Ubuntu (ifconfig)**

```
savio@server:~$ ifconfig
enp0s3: flags=163<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
      inet 172.16.0.1  brd 255.255.255.0  broadcast 172.16.0.255
        netmask 255.255.255.0  broadcast 172.16.0.255
          inet6 fe80::a00:2ff%fe10:65fa  brd fe80::ff:fe10:65fa  scopeid 0x20<link>
            ether 00:00:27:18:65:fa  txqueuelen 1000  (Ethernet)
              RX packets 106666 bytes 11000000 (10.6 MB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 6222  bytes 1266954 (1.2 MB)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
enp0s8: flags=163<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
      inet 192.168.0.1  brd 255.255.255.0  broadcast 192.168.0.255
        netmask 255.255.255.0  broadcast 192.168.0.255
          inet6 fe80::a00:27ff%fe14:cd18  brd fe80::ff:fe14:cd18  scopeid 0x20<link>
            ether 00:00:27:18:cd:18  txqueuelen 1000  (Ethernet)
              RX packets 2097  bytes 412288 (412.2 KB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 2307  bytes 377520 (377.5 KB)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
enp0s9: flags=4163<UP,BROADCAST,RUNNING,MULTICAST  mtu 1500
      inet 10.0.0.1  brd 255.255.255.0  broadcast 10.0.0.255
        netmask 255.255.255.0  broadcast 10.0.0.255
          inet6 fe80::a00:27ff%fe14:9843  brd fe80::ff:fe14:9843  scopeid 0x20<link>
            ether 00:00:27:18:98:43  txqueuelen 1000  (Ethernet)
              RX packets 29613  bytes 2981649 (2.9 MB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 24326  bytes 3533801 (3.0 MB)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING  mtu 65536
      inet 127.0.0.1  brd 127.255.255.255  broadcast 127.255.255.255
        netmask 255.0.0.0  broadcast 127.255.255.255
          loop  txqueuelen 1000  (Local Loopback)
            RX packets 9142  bytes 780769 (780.7 KB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 9142  bytes 780769 (780.7 KB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
savio@server:~$
```

Fonte: Elaborado pelos autores

- enp0s9 - IP 10.0.0.1 (corresponde à rede dos servidores)

A Figura 7 mostra a configuração do serviço DHCP através do arquivo /etc/dhcp/dhcpd.conf, para atribuição automática de IPs e informações de configuração de rede (Máscara, Gateway, DNS) para os dispositivos que se conectam a determinada rede.

Rede Administrativa 192.168.1.0: Foi determinado um range de endereços IP entre 192.168.1.51 e 192.168.1.100, com o roteador padrão sendo o próprio servidor no IP 192.168.1.1.

Rede dos Alunos 172.16.0.0: Foi determinado um range de endereços IP entre 172.16.0.100

**Figura 7 – Configuração DHCP (dhcpd.conf)**

```

Ubuntu Server 22.04 (Roteador) [Executando] - Oracle VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

GNU nano 7.2                               /etc/dhcp/dhcpd.conf

# set.
#host fantasia {
#    hardware ethernet 08:00:07:26:c0:e5;
#    fixed-address fantasia.example.com;
#}

# You can declare a class of clients and then do address allocation
# based on that. The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.
#class "foo" {
#    match if substring(option vendor-class-identifier, 0, 4) = "SUNW";
#}

#shared-network 224-29 {
#    subnet 10.17.224.0 netmask 255.255.255.0 {
#        option routers rtr-224.example.org;
#    }
#    subnet 10.0.29.0 netmask 255.255.255.0 {
#        option routers rtr-29.example.org;
#    }
#    pool {
#        allow members of "foo";
#        range 10.17.224.10 10.17.224.250;
#    }
#    pool {
#        deny members of "foo";
#        range 10.0.29.10 10.0.29.230;
#    }
#}

subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.109;
    option routers 192.168.1.1;
    option domain-name-servers 10.0.0.2;
    option domain-name "exemploadministrativo.org";
}

subnet 172.16.0.0 netmask 255.255.255.0 {
    range 172.16.0.100 172.16.0.150;
    option routers 172.16.0.1;
    option domain-name-servers 10.0.0.2;
    option domain-name "exemploaluno.org";
}

[ Soft wrapping of overlong lines enabled ]

```

Fonte: Elaborado pelos autores

**Figura 8 – IPs Estáticos e DNS (netplan)**

```

Ubuntu Server 22.04 (Roteador) [Executando] - Oracle VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

GNU nano 7.2                               /etc/netplan/00-installer-config.yaml

# This is the network config written by "subiquity"
network:
  version: 2
  ethernets:
    ens3:
      dhcp4: false
      addresses: [172.16.0.1/24]
      nameservers:
        addresses: [10.0.0.2]
    ens4:
      dhcp4: false
      addresses: [192.168.1.1/24]
      nameservers:
        addresses: [10.0.0.2]
    ens5:
      dhcp4: false
      addresses: [10.0.0.1/24]
      nameservers:
        addresses: [10.0.0.2]
  version: 2

[ Soft wrapping of overlong lines enabled ]

```

Fonte: Elaborado pelos autores

e 172.16.0.150, com o roteador padrão sendo o próprio servidor no IP 172.16.0.1.

Todas as interfaces utilizam máscara de sub-rede 255.255.255.0 (rede de Classe C). Ambas as redes tiveram o servidor DNS centralizado, definido como o 10.0.0.2, e atribuídas em diferentes domínios: exemploadministrativo.org e exemploaluno.org.

Para garantir que o servidor mantenha IPs fixos em todas as suas interfaces, foi configurado o arquivo de rede /etc/netplan/00-installer-config.yaml, como mostrado na Figura 8. Nesta configuração, o DHCP foi desativado para evitar a obtenção automática e todas as inter-

**Figura 9 – Habilitação de Roteamento (IP forwarding)**

```

Ubuntu Server 22.04 (Kali) [Executando] - Oracle VM VirtualBox
Arquivo Maquina Visualizar Entrada Dispositivos Ajuda

GNU nano 7.2          /etc/sysctl.conf

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Setting this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

#####
# additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofed traffic and Denial of Service attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.

#
# Do not accept ICMP redirects (prevent MITM attacks)
#net.ipv4.conf.all.accept_redirects = 0
#net.ipv4.conf.default.accept_redirects = 0
#
#_or_
# Accept ICMP redirects only for gateways listed in our default
# gateway list (enabled by default)
#net.ipv4.conf.all.secure_redirects = 1
#
# Do not send ICMP redirects (we are not a router)
#net.ipv4.conf.all.send_redirects = 0
#
# Log Martian Packets
#net.ipv4.conf.all.log_martians = 1

#####
# Router Discovery redirects
#disabled=1, 1=enable all, >1 bitmask of sync functions
# See https://www.kernel.org/doc/html/latest/admin-guide/syntax.html
# for what other values do
#kernel.synd=498

net.ipv4.ip_forward=1

```

**Fonte:** Elaborado pelos autores

faces definidas com IPs estáticos. Além dos IPs já mencionados, foi especificado também o DNS principal apontando o servidor 10.0.0.2, para que ele possa resolver nomes de domínio corretamente mesmo em ambientes internos.

Por fim, para possibilitar o roteamento de pacotes entre as três redes diferentes, foi necessário ativar o IP forwarding no servidor, mostrado na Figura 9. A alteração foi realizada no arquivo /etc/sysctl.conf, desconectando a linha que habilita o encaminhamento de pacotes IPv4 e permitindo que o servidor não apenas atribua IPs, mas também atue como um roteador entre as redes dos alunos, administrativa e dos servidores.

### 2.1.2 Servidor DNS

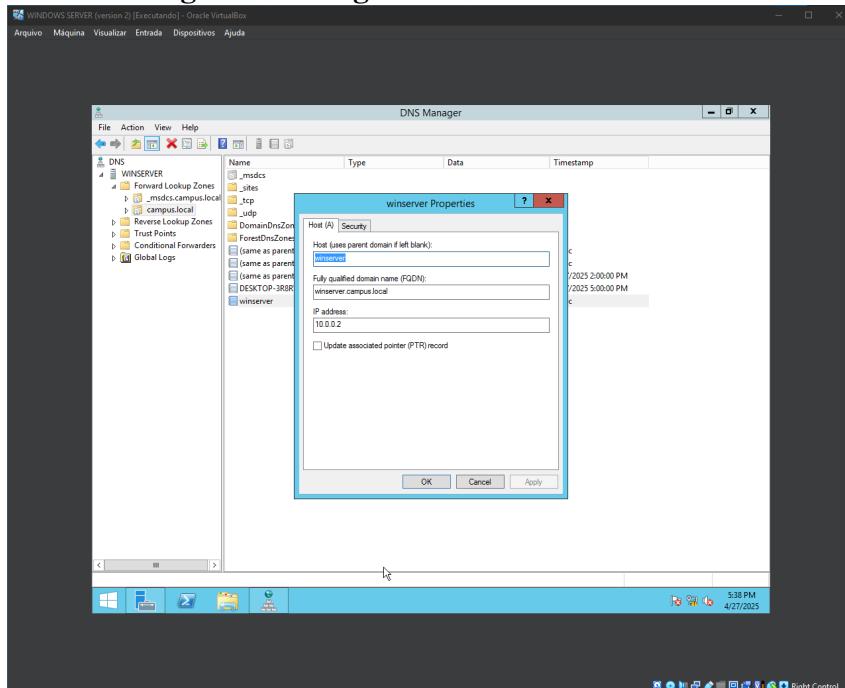
Configuração do DNS Windows Server, na Figura 10, demonstra a criação de um Registro A no Gerenciador DNS. O host chamado “winserver” está sendo criado, e o nome FQDN completo ficou winserver.campus.local. Além disso, o IP associado é o 10.0.0.2.

### 2.1.3 Servidor LDAP

O LDAP (Lightweight Directory Access Protocol) é um protocolo usado para acessar e gerenciar informações de diretórios. No contexto de servidores, ele é frequentemente usado para armazenar informações de usuários, grupos e autenticação.

A Figura 11 comprova que o serviço OpenLDAP (slapd) está ativo e executando corretamente na VM Ubuntu Server. Em seguida, foi feito o carregamento inicial da estrutura de

**Figura 10 – Registro A no DNS Windows**



Fonte: Elaborado pelos autores

**Figura 11 – Execução e Estrutura de OUs do LDAP**

```

Ubuntu server [Executando] - Oracle VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
just raised the bar for easy, resilient and secure k8s cluster deployment.
https://ubuntu.com/engage/secure-kubernetes-at-the-edge
Manutenção de Segurança Expandida para Applications não está ativa.
As atualizações podem ser aplicadas imediatamente.
Ativar ESM Apps para poder receber possíveis futuras atualizações de segurança.
Consulte https://ubuntu.com/esm ou execute: sudo pro status

antonio@antoniorubens:~$ sudo systemctl status slapd
[sudo] password for antonio:
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
  Loaded: loaded (/etc/init.d/slapd; generated)
  Started: started (/etc/init.d/slapd)
  Active: active (running) since Sun 2025-05-10 14:08:49 UTC; 19min ago
    Docs: man:systemd-sysv-generator(8)
   Process: 3774444 P /etc/init.d/slapd start (code=exited, status=0/SUCCESS)
   Tasks: 3 (limit: 2272)
  Memory: 6.4M (peak: 7.3M)
     CPU: 10ms
    CGroup: /system.slice/slapd.service
           └─393 /usr/sbin/slapd -h "ldap:/// ldap:///" -g openldap -u openldap -F /etc/ldap/slapd.d

mai 10 14:08:48 antoniorubens systemd[1]: Starting slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)...
mai 10 14:08:49 antoniorubens slapd[973]: * Starting OpenLDAP slapd
mai 10 14:08:49 antoniorubens [928]: $openLDAP: slapd 2.6.7+dfsg-1+deb11u8.5 (Dec 9 2024 02:56:18) $ 
mai 10 14:08:49 antoniorubens slapd[939]: slapd starting
mai 10 14:08:50 antoniorubens slapd[973]: ...done.
mai 10 14:08:49 antoniorubens systemd[1]: Started slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol).
antonio@antoniorubens:~$ sudo ldapadd -x -D cn=admin,dc=tiangua,dc=local -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=people,dc=tiangua,dc=local"
adding new entry "ou=groups,dc=tiangua,dc=local"
antonio@antoniorubens:~$ 

```

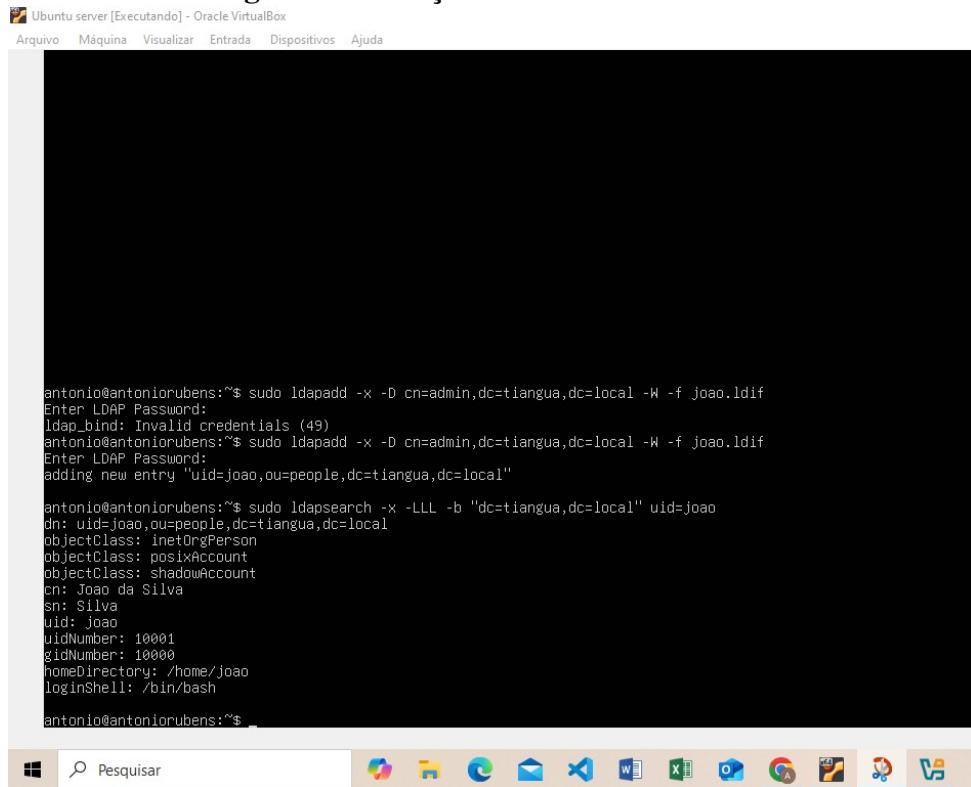
Fonte: Elaborado pelos autores

diretório com o comando `ldapadd`, usando o arquivo `base.ldif`, que criou duas unidades organizacionais: `people` (para usuários) e `groups` (para grupos), preparando o ambiente para armazenar contas e configurar permissões de forma estruturada.

Após a estrutura inicial do diretório ter sido criada, foi realizada a adição de um novo usuário, utilizando o comando "`ldapadd`" com o arquivo "`joao.ldif`", o usuário João da Silva foi adicionado com sucesso à unidade organizacional `people`, mostrado na Figura 12. Em seguida, foi utilizado o comando `ldapsearch` para consultar os dados do usuário "`joao`" no diretório e os atributos LDAP associados.

A Figura 13 mostra os resultados de consulta, exibindo os usuários e grupos cadastrados no diretório LDAP da estrutura `dc=tiangua,dc-local`. Sendo:

**Figura 12 – Adição e consulta de usuário**



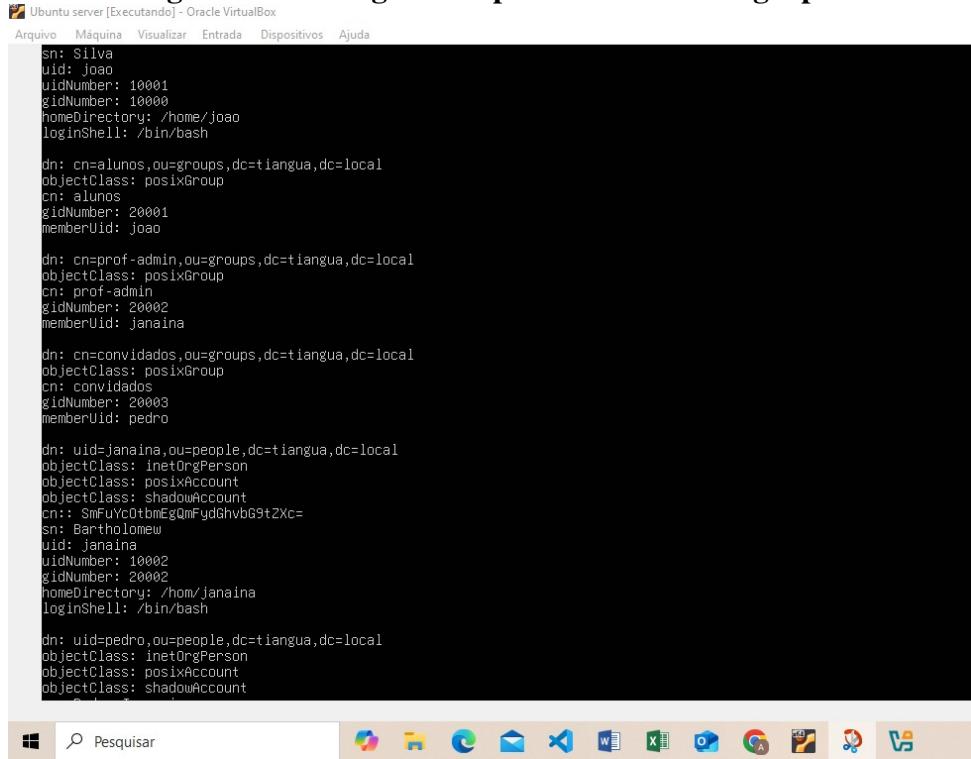
```
Ubuntu server [Executando] - Oracle VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

antonio@antoniorubens:~$ sudo ldapadd -x -D cn=admin,dc=tiangua,dc=local -W -f joao.ldif
Enter LDAP Password:
ldap_bind: Invalid credentials (49)
antonio@antoniorubens:~$ sudo ldapadd -x -D cn=admin,dc=tiangua,dc=local -W -f joao.ldif
Enter LDAP Password:
adding new entry "uid=joao,ou=people,dc=tiangua,dc=local"

antonio@antoniorubens:~$ sudo ldapsearch -x -LLL -b "dc=tiangua,dc=local" uid=joao
dn: uid=joao,ou=people,dc=tiangua,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Joao da Silva
sn: Silva
uid: joao
uidNumber: 10001
gidNumber: 10000
homeDirectory: /home/joao
loginShell: /bin/bash
antonio@antoniorubens:~$
```

Fonte: Elaborado pelos autores

**Figura 13 – Listagem completa de usuários e grupos**



```
Ubuntu server [Executando] - Oracle VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

sn: Silva
uid: joao
uidNumber: 10001
gidNumber: 10000
homeDirectory: /home/joao
loginShell: /bin/bash

dn: cn=alunos,ou=groups,dc=tiangua,dc=local
objectClass: posixGroup
cn: alunos
gidNumber: 20001
memberUid: joao

dn: cn=prof-admin,ou=groups,dc=tiangua,dc=local
objectClass: posixGroup
cn: prof-admin
gidNumber: 20002
memberUid: janaina

dn: cn=convidados,ou=groups,dc=tiangua,dc=local
objectClass: posixGroup
cn: convidados
gidNumber: 20003
memberUid: pedro

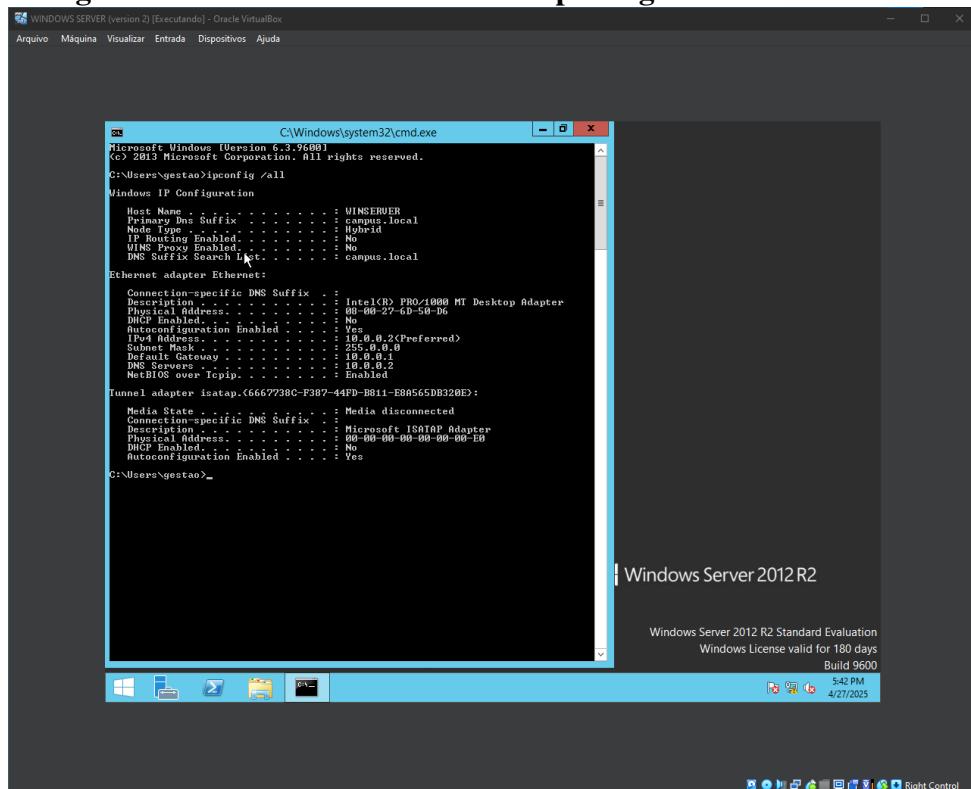
dn: uid=janaina,ou=people,dc=tiangua,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Bartholomeu
sn: Bartholomeu
uid: janaina
uidNumber: 10002
gidNumber: 20002
homeDirectory: /hom/janaina
loginShell: /bin/bash

dn: uid=pedro,ou=people,dc=tiangua,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
```

Fonte: Elaborado pelos autores

- OU people: usuários (João da Silva, Janaina Bartholomeu, Pedro)
- OU groups: grupos (alunos, prof-admin, convidados)

A listagem evidencia que os usuários foram alocados corretamente aos seus respecti-

**Figura 14 – Resultado do comando "ipconfig" no Windows Server**

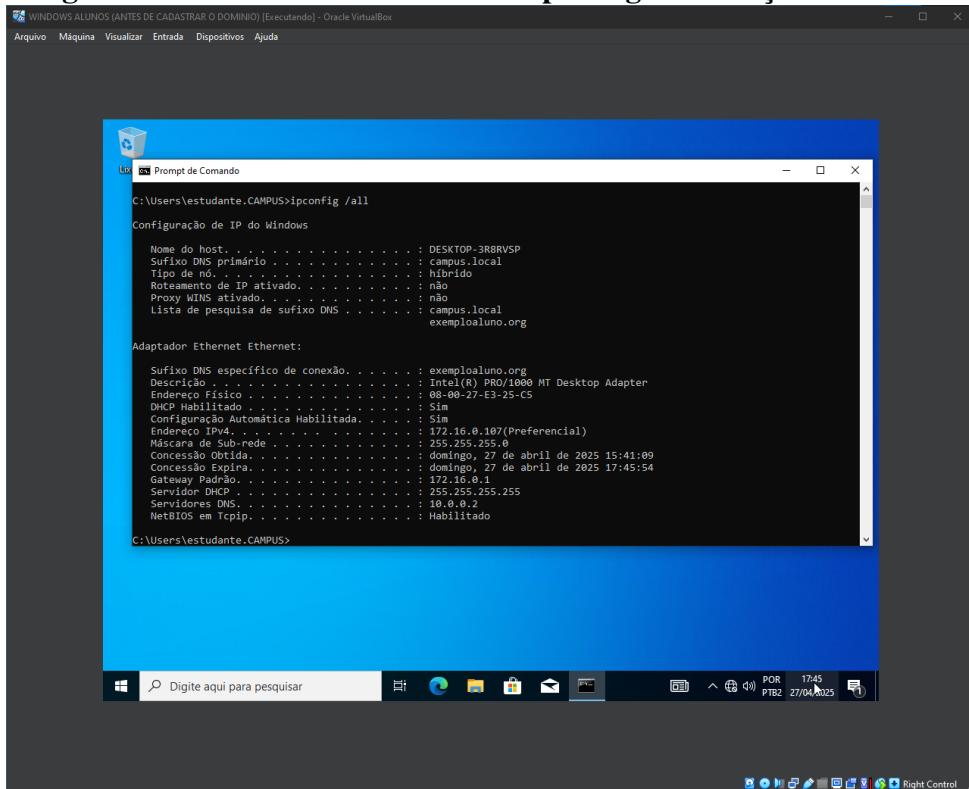
**Fonte:** Elaborado pelos autores

vos grupos via atributo memberUid, e os objetos foram atribuídos corretamente com as classes posixGroup e posixAccount, permitindo o controle de permissões no ambiente Linux. Na Figura 14 é apresentada a execução do comando ipconfig /all no Windows Server, validando a configuração de rede do ambiente:

- Host Name: WIN4H3I1R4IT, confirmando o nome do servidor.
- Primary DNS Suffix: campus.local, indicando que o servidor faz parte do domínio Active Directory criado anteriormente.
- Node Type: Hybrid, que é uma configuração comum para redes corporativas, pois permite a resolução de nomes tanto via métodos de broadcast quanto utilizando servidores WINS.
- IP Routing Enabled: No, indicando que o servidor não está roteando pacotes entre redes, o que é adequado para este cenário de domínio interno.

É importante observar que os adaptadores de rede estão configurados com o IP 10.0.0.2, o mesmo definido anteriormente durante a criação da zona DNS. Além disso, o servidor DNS configurado também é 10.0.0.2, apontando para o próprio servidor, conforme recomendado para controladores de domínio. Na Figura 15, é apresentada a execução do comando ipconfig /all em uma estação cliente da OU ALUNOS, confirmando a integração com o domínio:

- Nome do computador (Host Name): DESKTOP-3RR9V5P.

**Figura 15 – Resultado do comando "ipconfig" na Estação ALUNOS**

**Fonte:** Elaborado pelos autores

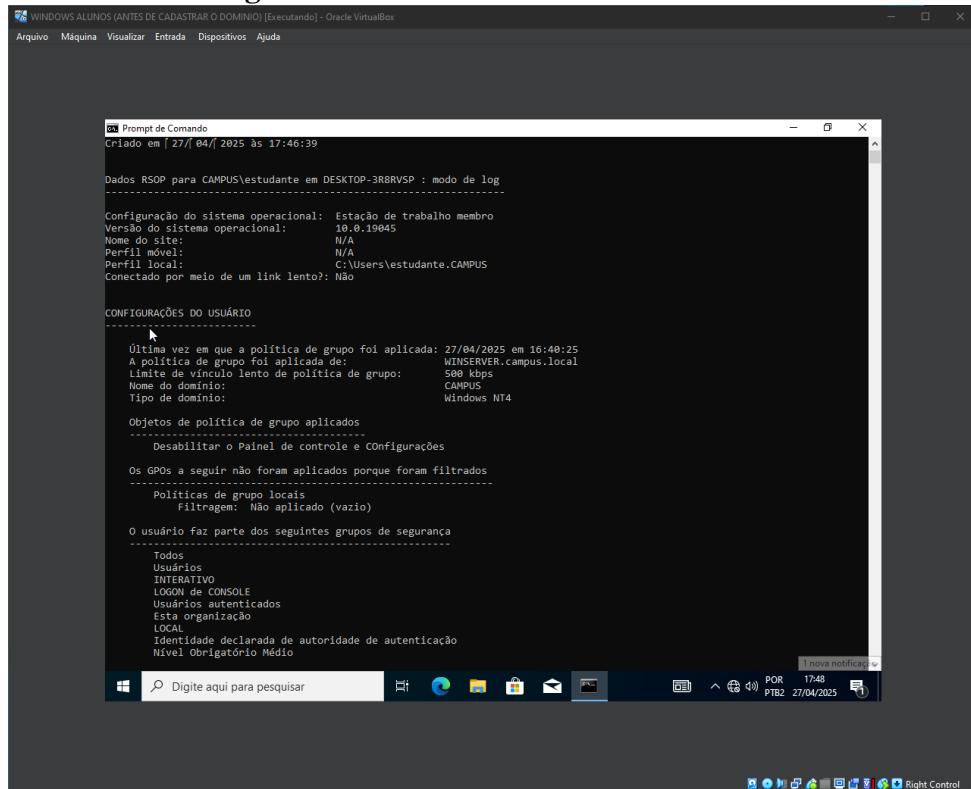
- Domínio DNS Primário: campus.local, indicando que a estação foi unida corretamente ao domínio Active Directory.
- Servidor DNS: 10.0.0.2, que corresponde ao Windows Server configurado para atuar como servidor DNS do domínio.
- Endereço IP: 10.0.0.67, atribuído dentro da faixa da rede 10.0.0.x.
- Nome da conexão: relacionado a exerciolucino.org, possivelmente uma configuração padrão ou nome de laboratório da máquina virtual.

Com isso, é possível concluir que a estação cliente foi integrada corretamente ao domínio campus.local, está resolvendo nomes corretamente através do servidor DNS configurado e a comunicação com o controlador de domínio está estabelecida e funcional, permitindo a aplicação das políticas de grupo (GPOs) atribuídas à OU ALUNOS.

A Figura 16 mostra o resultado de um comando RSOP para o usuário estudante no computador DESKTOP-3R8RVSP. Esse comando verifica quais políticas de grupo (GPOs) foram aplicadas. O usuário está em um computador com Windows 10, é membro do domínio CAMPUS e usa um perfil local. A política foi aplicada em 27/04/2025 pelo servidor “WIN-SERVER.campus.local”, sem problemas de conexão lenta.

A GPO aplicada foi “Desabilitar o Painel de controle e configurações”, ou seja, o estudante não pode acessar nem alterar as configurações do sistema. Nenhuma política local foi aplicada, reforçando que tudo vem do domínio. O usuário também pertence a grupos básicos

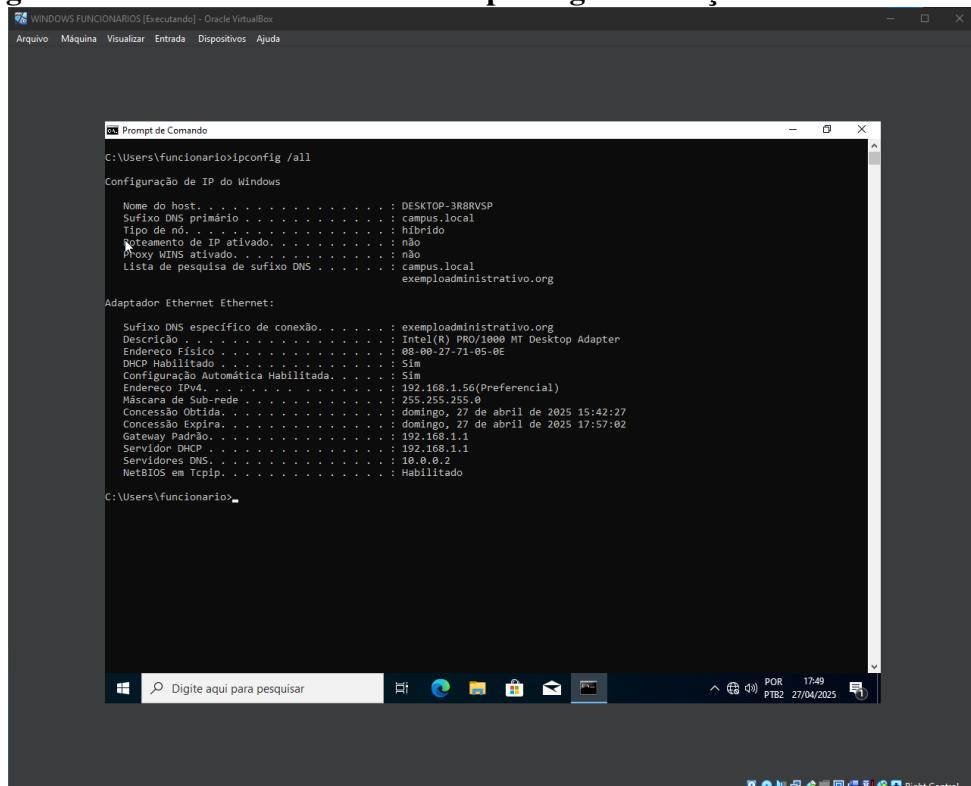
**Figura 16 – RSOP no Usuário Estudante**



**Fonte:** Elaborado pelos autores

de segurança, como Usuários, INTERATIVO e Usuários autenticados, o que é padrão em redes corporativas.

**Figura 17 – Resultado do comando "ipconfig" na Estação FUNCIONÁRIOS**



**Fonte:** Elaborado pelos autores

A Figura 17 mostra a execução do comando ipconfig /all em uma estação cliente da OU

FUNCIONÁRIOS, operada por um usuário funcionário:

- Nome do computador (Host Name): DESKTOP-3R8RVSP.
- Domínio DNS Primário: campus.local, indicando que a estação está corretamente unida ao domínio Active Directory.
- Tipo de Nó de Rede (Node Type): Hybrid, permitindo a resolução de nomes tanto por DNS quanto por WINS (mesmo que o proxy WINS esteja desativado).
- Lista de Sufixos DNS: inclui campus.local e exemploadministrativo.org, permitindo que o computador resolva nomes internos em ambos os domínios.
- DHCP: habilitado, com o IP atribuído automaticamente.
  - Endereço IPv4: 192.168.1.56, com máscara de sub-rede 255.255.255.0.
  - Gateway Padrão: 192.168.1.1, indicando o roteador local da rede.
  - Servidor DHCP: 192.168.1.1, provavelmente o próprio roteador.
  - Servidor DNS: configurado como 10.0.0.2, o servidor DNS do domínio campus.local.
- NetBIOS sobre TCP/IP: habilitado, permitindo comunicação em redes locais utilizando o protocolo NetBIOS.

**Figura 18 – RSOP no Usuário Funcionário**

The screenshot shows the Windows RSOP (Resultados de Execução de Política) tool running in a Command Prompt window titled 'Prompt de Comando'. The output displays various system configurations and security group policy details for the user 'funcionario' on the computer 'DESKTOP-3R8RVSP'. Key sections include:

- Configuração do sistema operacional:** Estação de trabalho membro, Versão do sistema operacional: 10.0.19045.
- CONFIGURAÇÕES DO USUÁRIO:** CN=funcionario, OU=USUARIOS, OU=FUNCIONARIOS, OU=CAMPUS-01, DC=campus, DC=local.
- Políticas de grupo:** A política de grupo foi aplicada de: SERVER.campus.local, Ultima vez que a política de grupo foi aplicada: 27/04/2025 em 16:44:15.
- Segurança:** O usuário faz parte dos seguintes grupos de segurança: Domain Users, Todos, Usuários, INTERATIVO, LOGON de CONSOLE, Usuários autenticados, Esta organização, LOCAL, Nível Obrigatório Médio.

**Fonte: Elaborado pelos autores**

A estação cliente FUNCIONÁRIOS está corretamente integrada ao domínio, recebendo a configuração de IP via DHCP da rede local e está utilizando o servidor DNS do domínio para

resolver nomes, garantindo o funcionamento adequado de serviços como login no domínio e aplicação de políticas de grupo.

A Figura 18 apresenta a utilização da ferramenta RSOP (Resultant Set of Policy) para análise das Políticas de Grupo aplicadas ao usuário CAMPUS\funcionario no computador DESKTOP-3R8RVSP.

O Sistema Operacional identificado como "Estação de trabalho membro" está com o Windows 10 na versão 10.0.19045, o usuário está utilizando um perfil local localizado em C:\Users\funcionario e a estação não está conectada via link lento, o que significa que a aplicação de GPOs ocorre normalmente, sem restrições de banda.

As Políticas de Grupo destinadas ao usuário FUNCIONÁRIO foram efetivamente processadas e aplicadas, garantindo a correta execução das restrições e configurações definidas para a OU FUNCIONÁRIOS.

## 2.2 Serviços em Máquinas Virtuais na Nuvem pela AWS

### 2.2.1 Servidor WEB

Foram criadas duas instâncias (máquinas virtuais) do tipo EC2 utilizando o serviço de computação em nuvem da AWS (Amazon Web Services), conforme mostrado na Figura 19. Essas instâncias serviram como base para a configuração do ambiente, permitindo a execução de aplicações e serviços em servidores virtualizados com controle total sobre o sistema operacional e os recursos computacionais.

As informações gerais como os IPs público e privado da primeira instância EC2, chamada "Srv Ubuntu 1", e os grupos de segurança configurados nela podem ser observados nas Figuras 20 e 21, respectivamente. Além disso, as informações e grupos de segurança da segunda instância, chamada "Srv Ubuntu 2", são mostrados nas Figuras 22 e 23.

**Figura 19 – Criação de duas instâncias (máquinas virtuais) EC2 no serviço de nuvem AWS**

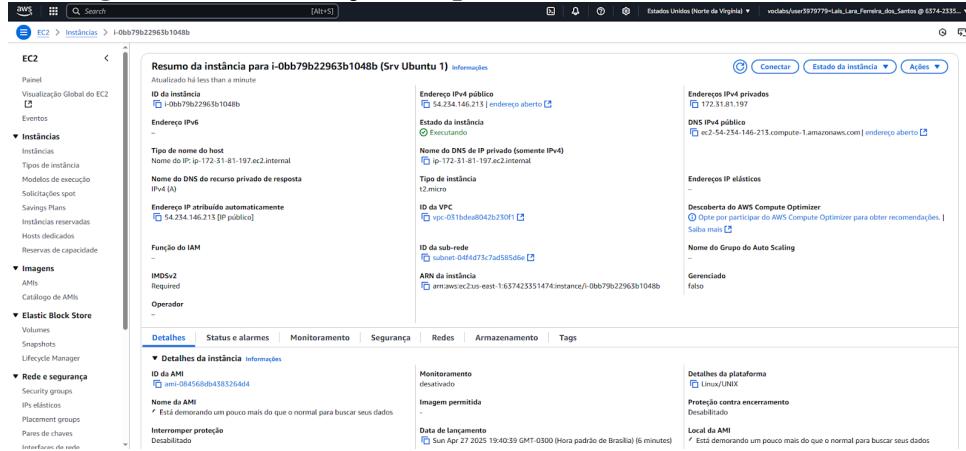
The screenshot shows the AWS Management Console interface for the EC2 service. The left sidebar has 'Instâncias' selected under 'Instâncias'. The main pane displays a table of instances with the following data:

Name	ID da instância	Estado da instância	Tipo de instância	Verificação de star	Status do alarme	Zona de disponibilidade	DNS IPv4 público	Endereço IP...	IP elástico
Srv Ubuntu 1	i-0bb790c2963b1048b	Executando	t2.micro	2/2 verificações a	Exibir alarmes +	us-east-1a	ec2-54-234-146-213.co...	54.234.146.213	-
Srv Ubuntu 2	i-00ea2f548798b6ccc	Executando	t2.micro	2/2 verificações a	Exibir alarmes +	us-east-1b	ec2-54-202-115-171.co...	54.202.115.171	-

**Fonte: Elaborado pelos autores**

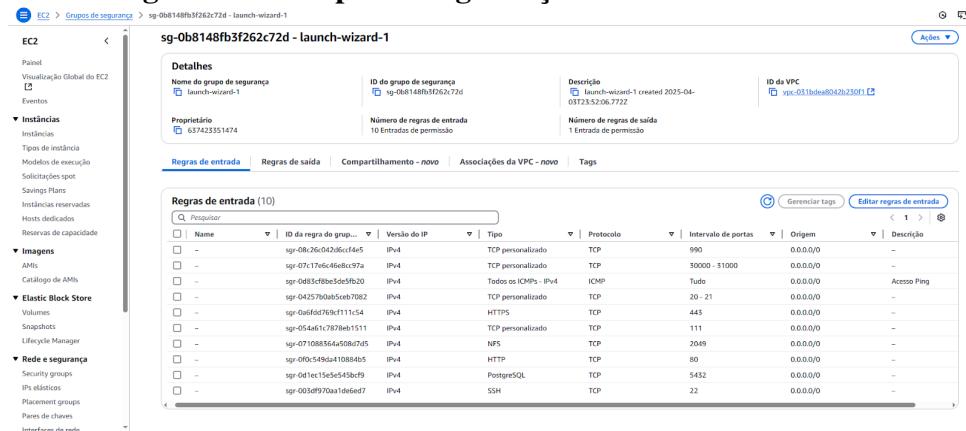
A instalação do servidor web Apache2 foi realizada em um ambiente Linux, com o objetivo de configurar e disponibilizar um servidor para hospedagem de páginas web. Inicialmente,

**Figura 20 – Informações da primeira instância (Srv Ubuntu 1)**



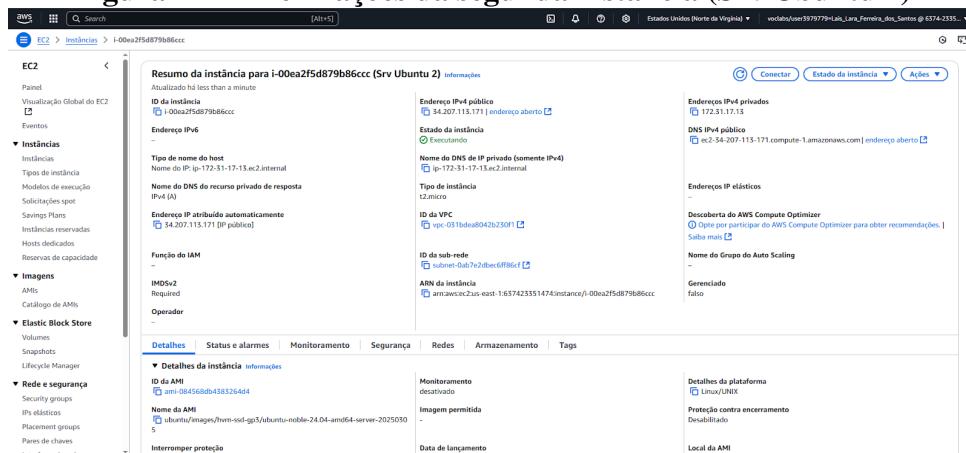
Fonte: Elaborado pelos autores

**Figura 21 – Grupos de segurança do Servidor Ubuntu 1**



Fonte: Elaborado pelos autores

**Figura 22 – Informações da segunda instância (Srv Ubuntu 2)**



Fonte: Elaborado pelos autores

procedeu-se à atualização dos pacotes do sistema utilizando o comando **sudo apt update**. Em seguida, o servidor Apache foi instalado por meio do comando **sudo apt install apache2 -y**.

Após a instalação, foi verificado o status do serviço Apache utilizando o comando **sudo systemctl status apache2**. Esse comando retornou a informação de que o serviço estava ativo (active) e em execução (running), como mostra a Figura 24. Além disso, foi realizada a conexão da instância Srv Ubuntu 1, criada na AWS, com a máquina local por meio do protocolo SSH, o

**Figura 23 – Grupos de segurança do Servidor Ubuntu 2**

The screenshot shows the AWS EC2 Security Groups interface. A specific security group named 'sg-031b94e065f392419 - launch-wizard-2' is selected. The 'Regras de entrada' tab is active, showing two inbound rules:

ID da regra de grupo	Versão do IP	Tipo	Protocolo	Intervalo de portas	Origem	Descrição
sgr-00759b6665568812b	IPv4	SSH	TCP	22	0.0.0.0/0	Acesso Ping
sgr-0882cb1c758d8475	IPv4	Todos os ICMPs - IPv4	ICMP	Tudo	0.0.0.0/0	Acesso Ping

Fonte: Elaborado pelos autores

**Figura 24 – Resultado do comando de status do Apache**

```
ubuntu@ip-172-31-81-197:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Sun 2025-04-27 22:40:58 UTC; 16min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 844 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 900 (apache2)
   Tasks: 55 (limit: 1129)
    Memory: 7.9M (peak: 8.1M)
      CPU: 92ms
     CGroup: /system.slice/apache2.service
             └─900 /usr/sbin/apache2 -k start
                 ├─901 /usr/sbin/apache2 -k start
                 ├─902 /usr/sbin/apache2 -k start
                 └─903 /usr/sbin/apache2 -k start

Apr 27 22:40:57 ip-172-31-81-197 systemd[1]: Starting apache2.service - The Apache HTTP>
Apr 27 22:40:58 ip-172-31-81-197 apachectl[885]: AH00558: apache2: Could not reliably d>
Apr 27 22:40:58 ip-172-31-81-197 systemd[1]: Started apache2.service - The Apache HTTP>
[lines 1-17 (END)]
```

Fonte: Elaborado pelos autores

**Figura 25 – Comando para conexão da instância via ssh.**

```
PS C:\Users\JR\ssh> ssh -i "lais.pem" ubuntu@ec2-54-234-146-213.compute-1.amazonaws.com
```

Fonte: Elaborado pelos autores

comando utilizado para realizar essa ação é mostrado na Figura 25.

Por fim, foi realizado um teste de funcionamento acessando o endereço IP público da máquina no navegador, por meio do link <http://<IP-DA-MÁQUINA>>. Ao fazer isso, foi exibida a página padrão do Apache com a mensagem "*It works!*", confirmando que o servidor estava operando corretamente, conforme a Figura 26.

**Figura 26 – Página web do servidor funcionando**



**Fonte:** Elaborado pelos autores

## 2.2.2 Serviço de DNS

O serviço de DNS foi instalado e, posteriormente, foi verificado se estava ativo utilizando os seguintes comandos:

- Atualização dos pacotes: **sudo apt update**
- Instalação do BIND9: **sudo apt install bind9 -y**
- Verificação do status: **sudo systemctl status bind9** (retornou “active (running)”, como mostrado na Figura ).

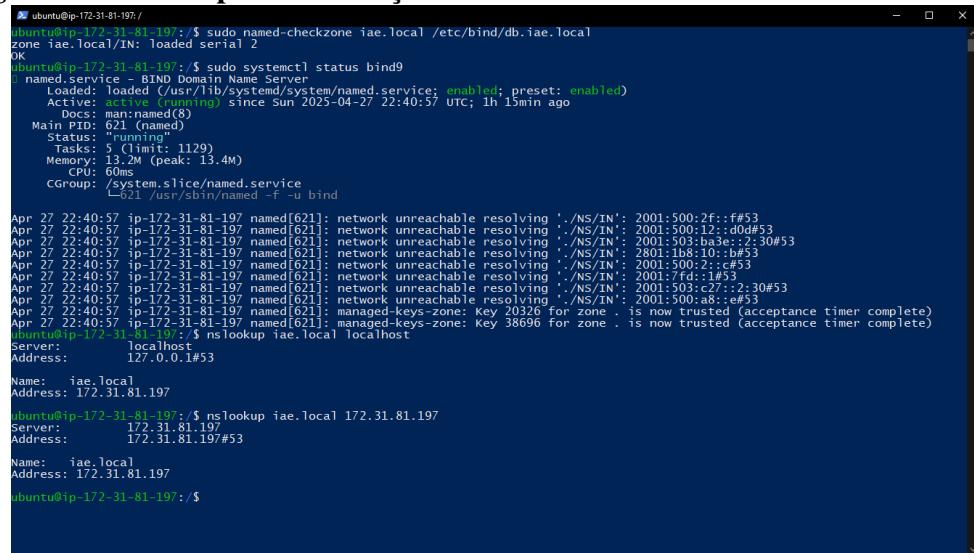
Após a instalação e verificação de funcionamento, foram editados os arquivos principais de configuração, realizando a criação de uma zona personalizada e um arquivo de zona:

- **/etc/bind/named.conf.local** → onde foram adicionadas as zonas.
- **/etc/bind/db.iae.local** → onde foi criado o arquivo da zona direta.

Para a criação de uma zona personalizada, foi adicionada a seguinte configuração no arquivo **named.conf.local**: **zone "iae.local" { type master;file "/etc/bind/db.iae.local";}**. Enquanto para a **criação do arquivo da zona**, foi copiado um arquivo modelo e editado, usando os seguintes comandos:

- Copiar o arquivo modelo: **sudo cp /etc/bind/db.local /etc/bind/db.iae.local**
- Editar o arquivo copiado: **sudo nano /etc/bind/db.iae.local**

Foram adicionados os registros do tipo A, NS, etc., apontando o domínio para o IP do servidor. Após a configuração dos arquivos, foram realizados testes para verificar que não havia erros na configuração e que o DNS estava funcionando corretamente. Primeiro, foi verificado

**Figura 27 – Testes para verificação do funcionamento correto do servidor DNS**


```

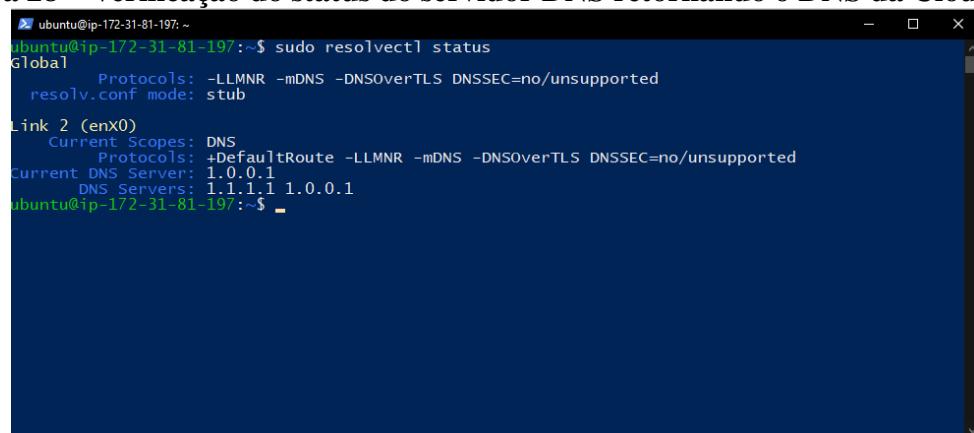
ubuntu@ip-172-31-81-197:~$ sudo named-checkzone iae.local /etc/bind/db.iae.local
Zone 'iae.local' loaded serial 2
OK
ubuntu@ip-172-31-81-197:~$ sudo systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: Loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-04-27 22:40:57 UTC; 1h 15min ago
       Docs: man:named(8)
     Main PID: 621 (named)
        Status: "running"
      Tasks: 5 (limit: 1129)
     Memory: 13.2M (peak: 13.4M)
        CPU: 60ms
      CGroup: /system.slice/named.service
             └─ 621 /usr/sbin/named -f -u bind

Apr 27 22:40:57 ip-172-31-81-197 named[621]: network unreachable resolving '.NS/IN': 2001:500:2f::f#53
Apr 27 22:40:57 ip-172-31-81-197 named[621]: network unreachable resolving '.NS/IN': 2001:503:c27::2:30#53
Apr 27 22:40:57 ip-172-31-81-197 named[621]: network unreachable resolving '.NS/IN': 2001:503:b7c::10#53
Apr 27 22:40:57 ip-172-31-81-197 named[621]: network unreachable resolving '.NS/IN': 2801:1b8:10::b#53
Apr 27 22:40:57 ip-172-31-81-197 named[621]: network unreachable resolving '.NS/IN': 2001:500:2::c#53
Apr 27 22:40:57 ip-172-31-81-197 named[621]: network unreachable resolving '.NS/IN': 2001:7fd::1#53
Apr 27 22:40:57 ip-172-31-81-197 named[621]: network unreachable resolving '.NS/IN': 2001:503:c27::2:30#53
Apr 27 22:40:57 ip-172-31-81-197 named[621]: managed-keys-zone: Key 20320 for zone . is now trusted (acceptance timer complete)
Apr 27 22:40:57 ip-172-31-81-197 named[621]: managed-keys-zone: Key 38696 for zone . is now trusted (acceptance timer complete)
Server: localhost
Address: 127.0.0.1#53
Name: iae.local
Address: 172.31.81.197
ubuntu@ip-172-31-81-197:~$ nslookup iae.local localhost
Server: 172.31.81.197#53
Address: 172.31.81.197
Name: iae.local
Address: 172.31.81.197
ubuntu@ip-172-31-81-197:~$ nslookup iae.local 172.31.81.197
Server: 172.31.81.197#53
Address: 172.31.81.197
Name: iae.local
Address: 172.31.81.197
ubuntu@ip-172-31-81-197:~$ 
```

Fonte: Elaborado pelos autores

se o arquivo da zona criada (`/etc/bind/db.iae.local`) estava com as configurações corretas por meio do comando “**`sudo named-checkzone iae.local /etc/bind/db.iae.local`**”. Após a resposta positiva, foi verificado se o servidor bind9 estava ativo e funcionando na máquina virtual. Por fim, para verificar se o servidor DNS estava funcionando corretamente, foi utilizado o comando `nslookup` de duas formas diferentes, sendo elas “**`nslookup iae.local localhost`**” e “**`nslookup iae.local 172.31.81.197`**”, retornando as informações corretas como era esperado. Todos os testes mencionados podem ser observados na Figura 27.

Além disso, também foi configurado o modo cliente do DNS de modo que a busca não fosse mais para o domínio local (EC2 da AWS) mas sim para o servidor DNS público da Cloudflare. O status dessa alteração pode ser observado na Figura 28.

**Figura 28 – Verificação do status do servidor DNS retornando o DNS da Cloudflare.**


```

ubuntu@ip-172-31-81-197:~$ sudo resolvectl status
Global
  Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: stub

Link 2 (enx0)
  Current Scopes: DNS
    Protocols: +DefaultRoute -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  Current DNS Server: 1.0.0.1
    DNS Servers: 1.1.1.1 1.0.0.1
ubuntu@ip-172-31-81-197:~$ 
```

Fonte: Elaborado pelos autores

## 2.2.3 Serviço de Banco de Dados (PostgreSQL)

### 2.2.3.1 Configuração e criação de primeiros usuários e banco de dados

Primeiramente, foi realizada a instalação e a configuração do PostgreSQL. Assim, a instalação foi feita utilizando o comando "sudo apt install postgresql -y", e em seguida, foi verificado se o serviço estava funcionando corretamente com o comando "sudo systemctl status postgresql", e ele estava ativo e em execução, conforme a Figura 29.

**Figura 29 – Testes do PostgreSQL no terminal**

```

ubuntu@ip-172-31-81-197:~$ sudo systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/usr/lib/systemd/system/postgresql.service; enabled; preset: enabled)
   Active: active (exited) since Sun 2025-04-27 22:41:00 UTC; 2h 11min ago
     Process: 1017 ExecStart=/bin/true (code-exited, status=0/SUCCESS)
    Main PID: 1017 (code-exited, status=0/SUCCESS)
       CPU: 1ms

Apr 27 22:41:00 ip-172-31-81-197 systemd[1]: Starting PostgreSQL RDBMS...
Apr 27 22:41:00 ip-172-31-81-197 systemd[1]: Started PostgreSQL RDBMS.
ubuntu@ip-172-31-81-197:~$ sudo -i -u postgres
postgres@ip-172-31-81-197:~$ psql sede_iae
psql (16.8 (Ubuntu 16.8-0ubuntu0.24.04.1))
Type "help" for help.

sede_iae=# \l
                                         List of databases
   Name   | Owner  | Encoding | Locale Provider | Collate | Ctype | ICU Locale | ICU Rules | Access privileges
-----+-----+-----+-----+-----+-----+-----+-----+-----+
campus2_iae | postgres | UTF8 | libc | C.UTF-8 | C.UTF-8 |
campus3_iae | postgres | UTF8 | libc | C.UTF-8 | C.UTF-8 |
extensao_iae | postgres | UTF8 | libc | C.UTF-8 | C.UTF-8 |
postgres | postgres | UTF8 | libc | C.UTF-8 | C.UTF-8 |
sede_iae | postgres | UTF8 | libc | C.UTF-8 | C.UTF-8 |
template0 | postgres | UTF8 | libc | C.UTF-8 | C.UTF-8 |
template1 | postgres | UTF8 | libc | C.UTF-8 | C.UTF-8 |
(7 rows)

sede_iae=# \dt
Did not find any relations.
sede_iae=# CREATE TABLE alunos (
sede_iae(# id SERIAL PRIMARY KEY,
sede_iae(# nome VARCHAR(100) NOT NULL,
sede_iae(# curso VARCHAR(100) NOT NULL,
sede_iae(# contato VARCHAR(50),
sede_iae(# email VARCHAR(100) NOT NULL
sede_iae(# );
CREATE TABLE
sede_iae=# \t
                                         List of relations
 Schema | Name  | Type  | Owner
-----+-----+-----+-----+
 public | alunos | table | postgres
(1 row)

sede_iae=# \q
postgres@ip-172-31-81-197:~$ psql -U postgres -c "\du"
                                         List of roles
 Role name | Attributes
-----+-----+
 postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS
 usuario   | 
```

**Fonte:** Elaborado pelos autores

Durante a instalação, o PostgreSQL cria, por padrão, o superusuário chamado "**postgres**". Para acessar o PostgreSQL como o superusuário padrão, foi utilizado o comando "sudo -u postgres psql". Com o PostgreSQL acessado como superusuário, foi criado um novo banco de dados chamado "sede\_iae" com o seguinte comando SQL:

```
CREATE DATABASE sede_iae;
```

Após a criação do banco de dados, criou-se o usuário chamado "usuario" para ser o superusuário que terá permissões completas sobre o banco "sede\_iae". Para isso, foi utilizado o seguinte comando SQL:

```
CREATE USER usuario WITH ENCRYPTED PASSWORD 'senhabd@123' ;
```

Após criar o usuário, foi concedida a ele as permissões de superusuário para que ele pudesse gerenciar o banco de dados sede\_iae. Isso é feito com o seguinte comando SQL:

```
GRANT ALL PRIVILEGES ON DATABASE sede\_\_iae TO usuario;
```

Após o banco de dados ter sido criado e o usuário "usuario" recebido as permissões necessárias, foi utilizado o usuário "usuario" para conectar-se ao banco "sede\_iae", executando o seguinte comando: `psql -U usuario -d sede_iae`.

Por fim, ao se conectar ao banco de dados "sede\_iae" com o usuário "usuario", foi realizado um teste criando uma tabela chamada "aluno" para verificar se as permissões estavam funcionando corretamente. O comando utilizado para criar a tabela foi:

```
CREATE TABLE alunos (
    id SERIAL PRIMARY KEY,
    nome VARCHAR(100) NOT NULL,
    curso VARCHAR(100) NOT NULL,
    contato VARCHAR(50),
    email VARCHAR(100) NOT NULL,
);
```

Na Figura 29 são mostrados os comandos feitos no terminal da instância ubuntu para verificar se o PostgreSQL estava devidamente configurado e funcionando na máquina virtual. Os testes de funcionamento foram feitos por meio da verificação do status, entrada no modo de edição de banco de dados (sede\_iae), teste de listagem dos bancos de dados já existentes, criação da tabela “alunos” e verificação dos usuários registrados.

### 2.2.3.2 Conexão ao pgAdmin

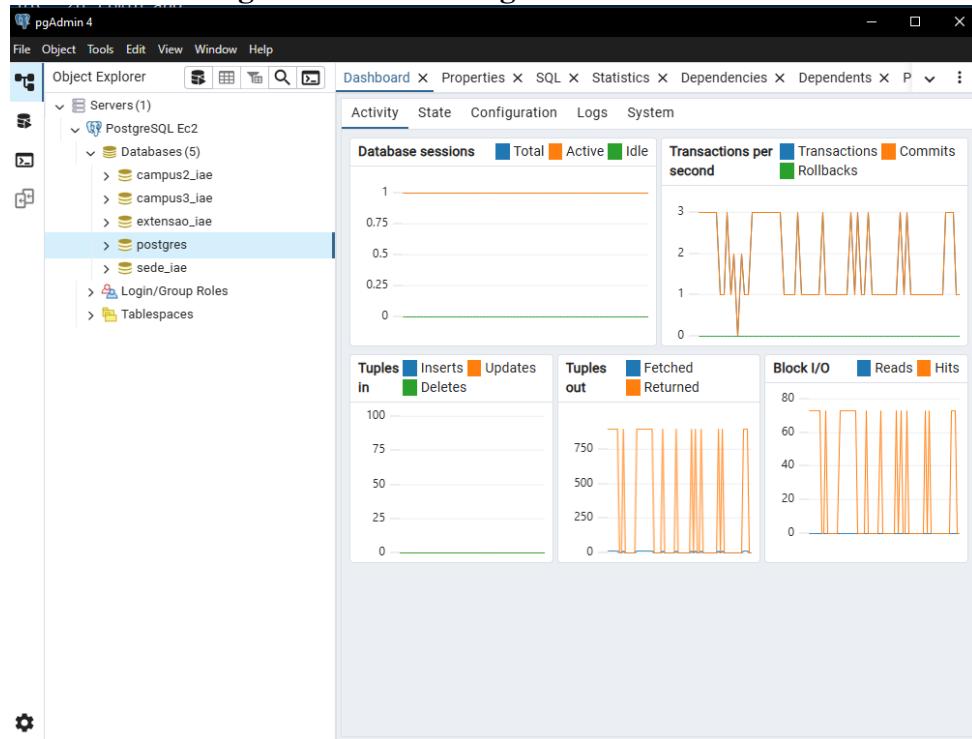
- **Host:** O IP do servidor onde o PostgreSQL está instalado, sendo o IP público da instância EC2 criada anteriormente;
- **Nome do banco de dados:** sede\_iae;
- **Usuário:** usuario;
- **Senha:** senhabd@123 (senha definida para o usuário usuario durante a criação).

Após registrar essas informações no pgAdmin pela primeira vez, já é possível ter acesso aos bancos de dados criados pelo terminal enquanto a instância estiver ativa na AWS. Este teste de sincronização pode ser observado na Figura 30.

Além do mais, caso haja necessidade de acessar o PostgreSQL remotamente, é necessário editar o arquivo de configuração para permitir conexões externas. O caminho do arquivo de configuração pg\_hba.conf geralmente é: `/etc/postgresql/16/main/pg_hba.conf`.

Após realizar as alterações de configuração, foi necessário reiniciar o PostgreSQL para aplicar as mudanças. Isso é feito com o seguinte comando: `sudo systemctl restart postgresql`.

**Figura 30 – Tela do PgAdmin funcionando**



Fonte: Elaborado pelos autores

## 2.2.4 Serviço de FTP com vsftpd

### 2.2.4.1 Instalação e configuração do vsftpd

Primeiramente, foram feitas a instalação e a configuração do vsftpd. Para a instalação do vsftpd, foi utilizado o comando **"sudo apt install vsftpd"** e a configuração foi feita editando o arquivo de configuração usando **"sudo nano /etc/vsftpd.conf"** e alterando as principais opções:

- listen=YES
- local\_enable=YES
- write\_enable=YES
- userlist\_enable=YES
- userlist\_deny=NO

Em seguida, os usuários FTP de alunos, de professores e do administrativo foram criados (Usuários e Senhas no final do arquivo), usando os seguintes comandos nesta ordem:

- sudo useradd -m (user)
- sudo passwd ftpuser (senha)
- sudo mkdir -p /etc/vsftpd/

- echo ftpuser | sudo tee /etc/vsftpd/user\_list

Além de criar um repositório para cada usuário, a propriedade e as permissões também foram alteradas. Portanto, ao final, cada usuário era proprietário de sua pasta e conseguia acessar apenas ela, sendo impedido de entrar e realizar ações em qualquer outra. Por exemplo, usuários 'professor' eram proprietários da pasta 'professor' e só conseguiam acessar, editar, adicionar ou excluir arquivos nesta única pasta. Estas permissões são mostradas na Figura 31.

Depois de configurar no terminal da instância, foi necessário liberar a porta no firewall da AWS para que o FTP funcionasse corretamente, ou seja, no Security Group da instância, adicionando a seguinte regra:

- **Tipo:** FTP
- **Protocolo:** TCP
- **Porta:** 21
- **Origem:** 0.0.0.0/0

Após concluir a configuração, foram realizados testes para verificar se o serviço estava funcionando corretamente. Primeiro, verifica-se o status do firewall e das portas que estão conectadas. Em seguida, é feita a verificação de criação e propriedade dos repositórios criados, sendo um para cada usuário registrado (admin\_ie, aluno e professor). Esses usuários são proprietários de suas pastas, podendo criar, editar e excluir arquivos, mas não conseguem acessar as pastas dos outros usuários. Em seguida, é feito o teste de entrada no FTP do usuário professor, sendo bem-sucedido. Todos esses testes são mostrados na Figura 31.

**Figura 31 – Testes do serviço de FTP pelo terminal Ubuntu**

```

ubuntu@ip-172-31-81-197:~$ sudo ufw status
Status: active
To                         Action      From
--                         --          --
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
5432                      ALLOW       Anywhere
111                       ALLOW       Anywhere
2049                      ALLOW       Anywhere
30000:31000/tcp           ALLOW       Anywhere
20,21,990/tcp              ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
443/tcp (v6)               ALLOW       Anywhere (v6)
5432 (v6)                 ALLOW       Anywhere (v6)
111 (v6)                  ALLOW       Anywhere (v6)
2049 (v6)                 ALLOW       Anywhere (v6)
30000:31000/tcp (v6)       ALLOW       Anywhere (v6)
20,21,990/tcp (v6)         ALLOW       Anywhere (v6)

ubuntu@ip-172-31-81-197:~$ cd /home
ubuntu@ip-172-31-81-197:~/home$ ls
admin_ie  aluno  professor  ubuntu
ubuntu@ip-172-31-81-197:~/home$ ls -l
total 16
drwx----- 3 admin_ie admin_ie 4096 Apr 27 19:15 admin_ie
drwx----- 3 aluno    aluno    4096 Apr  5 20:22 aluno
drwx----- 3 professor professor 4096 Apr 26 17:21 professor
drwxr-x--- 4 ubuntu   ubuntu   4096 Apr 21 00:21 ubuntu
ubuntu@ip-172-31-81-197:~/home$ ftp professor@localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> -

```

**Fonte: Elaborado pelos autores**

### 2.2.4.2 Utilização do FTP via Filezilla

Para o cliente conseguir usar o serviço de FTP de forma visual, foi escolhido o software Filezilla para esta função. Para ter acesso às informações no Filezilla, é necessário conectar-se a um usuário já criado anteriormente, inserindo os campos:

- **Host:** IP da instância;
- **Usuário:** Coluna "Usuário"do Quadro 1;
- **Senha:** Coluna "Senha"do Quadro 1;
- **Porta:** 21.

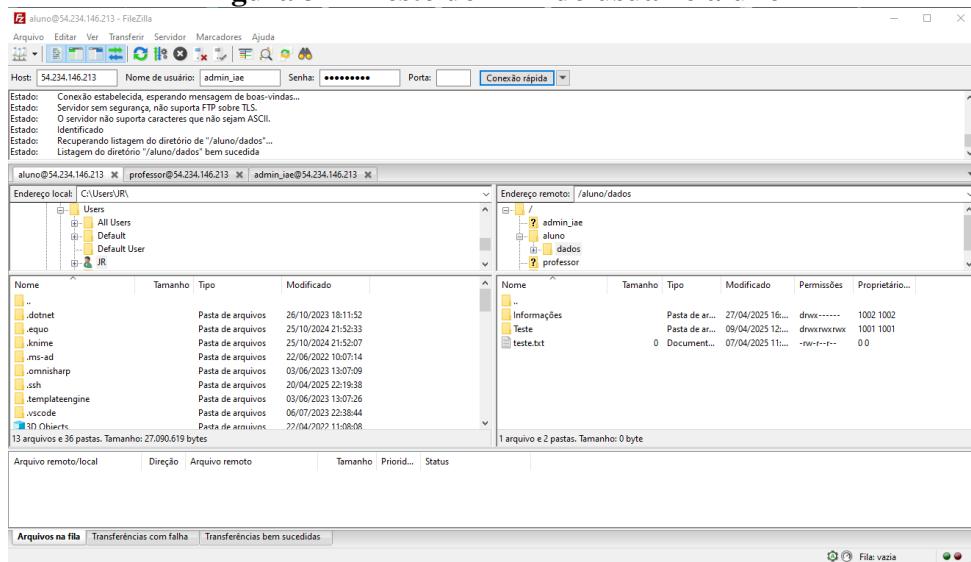
**Quadro 1 – Login de acesso dos usuários no servidor FTP**

Usuário	Senha
admin_ie	Admin@123
professor	Prof@123
aluno	Aluno@123

**Fonte:** Elaborado pelos autores

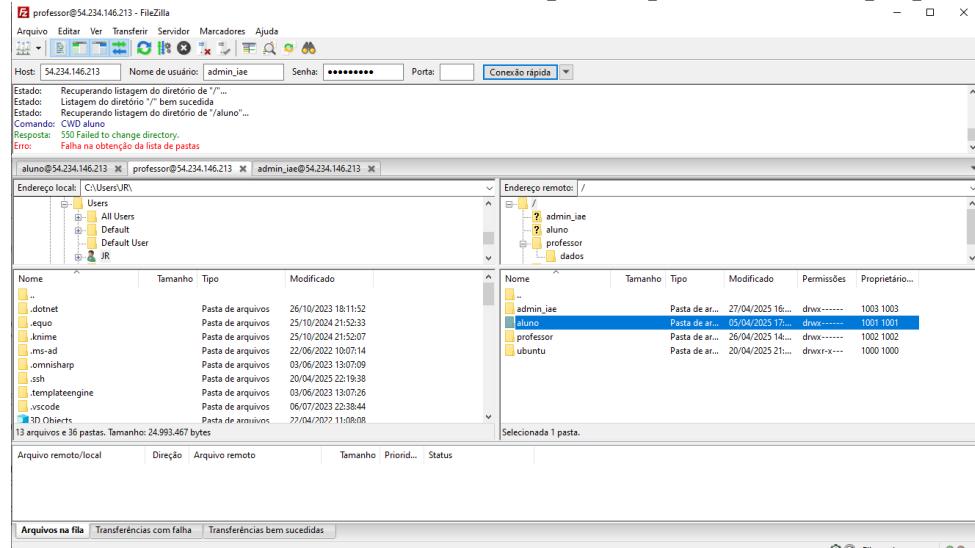
Para realizar o teste do FTP no modo cliente utilizando o Filezilla, o host de entrada foi o IP Público da máquina “Srv Ubuntu 1”, sendo ele no momento do teste: 54.234.146.213. Bem como, o login e o acesso de todos os usuários foram verificados. A Figura 32 mostra o teste feito no usuário “aluno”.

**Figura 32 – Teste do FTP do usuário aluno**



**Fonte:** Elaborado pelos autores

Além disso, foi realizada a verificação dos acessos de cada usuário, garantindo que só conseguiram acessar as pastas nas quais são proprietários. No exemplo da Figura 33, o usuário “professor” tenta entrar na pasta “aluno”, porém é mostrada uma mensagem de erro e ele não consegue efetuar a entrada.

**Figura 33 – Teste de acesso dos usuários em pastas que eles não são proprietários**

Fonte: Elaborado pelos autores

## 2.2.5 Serviço NFS Servidor e Cliente

### 2.2.5.1 Configuração do Serviço de NFS no Servidor

Primeiramente, foi feita a conexão à instância EC2 'Srv Ubuntu 1' ao servidor NFS usando SSH. No servidor NFS, os pacotes necessários para o compartilhamento de arquivos foram instalados com o comando 'sudo apt install nfs-kernel-server'.

Em seguida, foi criado um diretório no servidor onde os arquivos seriam compartilhados, usando o comando 'sudo mkdir /mnt/shared\_dir'. As permissões necessárias foram configuradas para garantir que o diretório fosse acessível pelo cliente NFS:

- sudo chown nobody:nogroup /mnt/shared\_dir
- sudo chmod 777 /mnt/shared\_dir

O próximo passo foi configurar o compartilhamento NFS. Portanto, o arquivo de configuração do NFS foi editado para permitir o compartilhamento do diretório com o cliente. No arquivo '/etc(exports', foi adicionada a seguinte linha para permitir o compartilhamento com a máquina cliente: /mnt/shared\_dir <IP-do-cliente> (rw, sync, no\_subtree\_check).

Após a configuração, as mudanças foram aplicadas e o serviço NFS foi reiniciado para que as alterações entrassem em vigor. Por fim, foi necessário verificar se o compartilhamento estava funcionando para garantir que o NFS estava ativo e o status do serviço foi verificado com o comando: sudo systemctl status nfs-kernel-server.

### 2.2.5.2 Instalação do serviço de NFS no Cliente

Agora, a conexão foi feita à instância EC2 cliente 'Srv Ubuntu 2' (máquina que vai acessar o compartilhamento) via SSH. Para permitir que o cliente monte o compartilhamento, o pacote NFS foi instalado com o seguinte comando: 'sudo apt install nfs-common'. Em

seguida, foi criado um diretório no cliente onde o compartilhamento NFS seria montado: 'sudo mkdir /mnt/nfs\_teste'.

O compartilhamento NFS foi acessado com o comando mount, montando o diretório compartilhado do servidor NFS: 'sudo mount <IP-do-servidor>:/mnt/shared\_dir /mnt/nfs\_teste'.

O <IP-do-servidor> foi substituído pelo IP da máquina servidor (Srv Ubuntu 1) e para verificar se o compartilhamento foi montado corretamente, foi utilizado o comando 'df -h'.

Para testar o compartilhamento via NFS entre servidor e cliente, primeiramente, as duas instâncias criadas foram conectadas via SSH, cada uma em um terminal da máquina host. A instância ip-172-31-81-197 (servidor NFS) compartilha '/srv/shared\_dir'. O cliente ip-172-31-17-13 monta este diretório em '/mnt/nfs\_teste' e acessa os mesmos arquivos, confirmando o funcionamento do compartilhamento em rede. No momento do teste, foi criado o arquivo 'teste3.txt' que foi listado em ambos os terminais, como pode ser observado na Figura 34.

**Figura 34 – Teste de compartilhamento de arquivos entre servidor e cliente no serviço de NFS**

The screenshot shows two terminal windows. The left window is on the server (Ubuntu 1) with IP 172.31.81.197, showing the command 'ls' in the directory /srv/shared\_dir, which lists 'teste.txt', 'teste2.txt', and 'teste3.txt'. The right window is on the client (Ubuntu 2) with IP 172.31.17.13, showing the command 'df -h' output, which includes a line for '/mnt/nfs\_teste' mounted at '/dev/xvda10' with 6.8G used and 50% usage. Both terminals show the same list of files ('teste.txt', 'teste2.txt', 'teste3.txt') in their respective shared directories.

**Fonte:** Elaborado pelos autores

### 2.2.6 Servidor Proxy

Para configurar o servidor proxy, foi instalado o Squid em uma instância EC2, por meio do comando 'sudo apt-get install squid'.

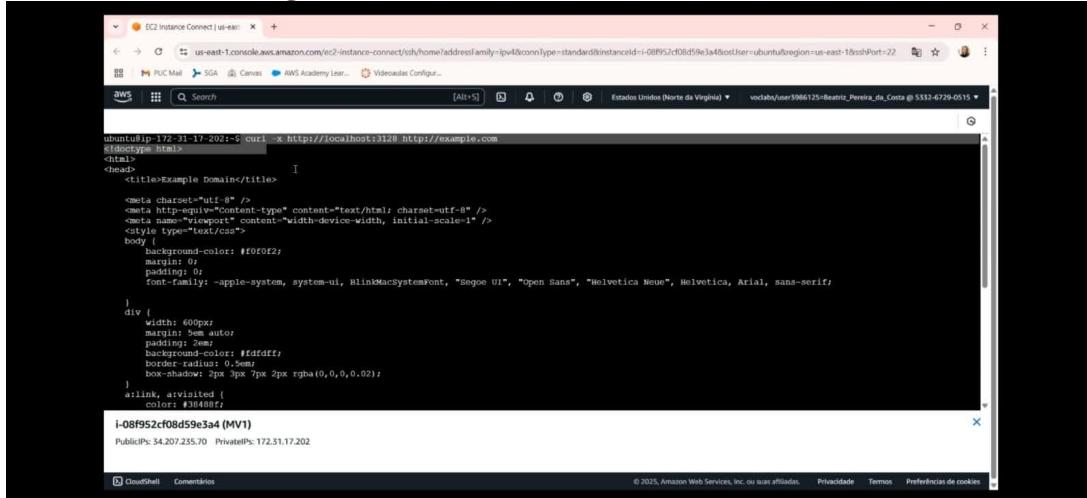
Após a instalação, o arquivo de configuração do Squid (**/etc/squid/squid.conf**) foi editado para permitir o tráfego de entrada na porta 3128, que é a porta padrão do proxy. Além disso, a configuração foi ajustada para permitir acesso apenas de IPs específicos, garantindo a segurança do servidor. Também foi necessária a abertura de portas necessárias no Security Group da AWS para permitir acesso HTTP/HTTPS (porta 3128).

Em seguida, foi feita a configuração do proxy no cliente. Para realizá-la, primeiro são feitas as configurações do IP do servidor proxy e a porta, bem como a verificação de que a configuração estava funcionando (ex: usando curl ou navegadores). No Ubuntu, o arquivo **/etc/environment** foi editado para incluir as configurações do proxy:

- Servidor: http\_proxy="http://<IP\_PUBLICO>:3128"
- Cliente: https\_proxy="http://<IP\_PUBLICO>:3128"

Em seguida, foi feito um teste utilizando o comando '**curl**' para verificar se a configuração estava funcionando corretamente, conforme a Figura 35. O comando retornou um status 200 OK, indicando que a requisição foi bem-sucedida.

**Figura 35 – Teste usando o comando “curl”**

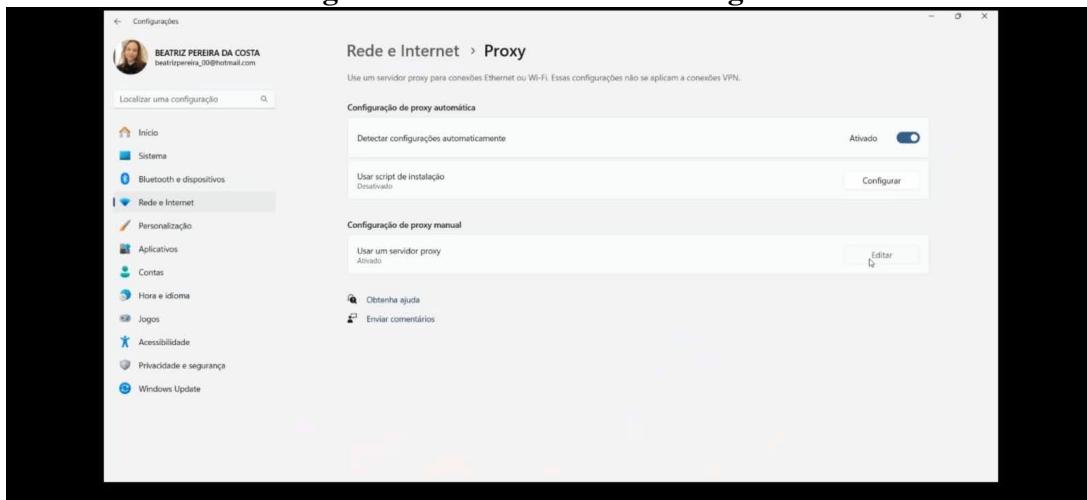


```
ubuntu@ip-172-31-17-202:~$ curl -x http://localhost:3128 http://example.com
<!DOCTYPE html>
<html>
<head>
    <title>example domain</title>
    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
        body {
            background-color: #f0f0f2;
            margin: 0;
            padding: 0;
            font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;
        }
        div {
            width: 60px;
            margin: 5em auto;
            padding: 2em;
            background-color: #fff;
            border-radius: 0.5em;
            box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
        }
        a {
            text-decoration: none;
            color: #304ffe;
        }
    </style>
    i-08f952cf08d59e3a4 (MV1)
    Public IPs: 34.207.235.70 Private IPs: 172.31.17.202
</head>
<body>
<div>
<a href="http://example.com">example.com</a>
</div>
</body>
</html>
```

**Fonte: Elaborado pelos autores**

Além disso, para garantir que o proxy estava funcionando, foram realizados testes com o comando **curl**, que fez requisições HTTP ao site '[www.google.com](http://www.google.com)', como mostra a Figura 35. O servidor proxy respondeu corretamente, registrando a requisição no log do Squid. Também foi feito o teste utilizando o navegador para garantir que o acesso à internet estava sendo feito através do proxy, mostrado na Figura 36.

**Figura 36 – Teste usando o navegador**



**Fonte: Elaborado pelos autores**

### **2.2.7 Serviço de Cache**

O Squid foi instalado com o comando 'sudo apt install squid', garantindo que a versão mais recente fosse instalada na máquina. Após a instalação, o arquivo de configuração principal do Squid, localizado em **/etc/squid/squid.conf**, foi editado para definir os parâmetros necessários para o cache. Neste arquivo, foi configurado o diretório onde o Squid armazena o cache, que é a pasta **/var/spool/squid**. Para isso, foi adicionada a seguinte linha ao arquivo **squid.conf**: 'cache\_dir ufs /var/spool/squid 1000 16 256'.

Além disso, foram definidos os limites de tamanho de objetos que o Squid pode armazenar, com as seguintes configurações:

- `maximum_object_size` 50 MB
  - `minimum_object_size` 0 KB

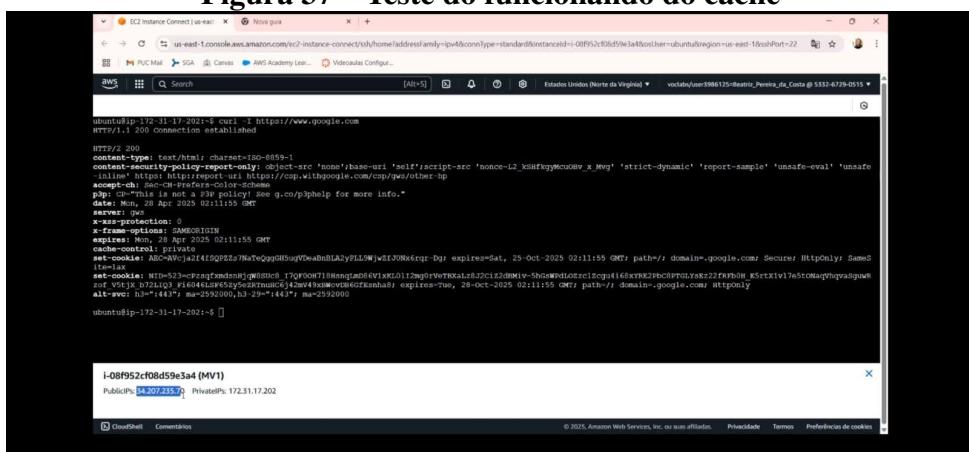
Essas configurações definem o tamanho máximo e mínimo dos objetos armazenados no cache. No caso, objetos de até 50MB são armazenados, e o menor objeto possível é de 0 KB.

Além disso, para melhorar a performance de acesso aos objetos mais frequentemente usados, foi configurada também a memória do cache, com a seguinte linha: 'cache\_mem 256 MB'. O parâmetro **cache\_mem** define a quantidade de memória RAM que o Squid pode usar para armazenar objetos em cache. Foi configurado para 256MB, o que acelera o acesso a conteúdos frequentemente solicitados.

Após editar o arquivo de configuração, foi executado o comando `'sudo squid -z'` para inicializar o sistema de cache. Esse comando prepara os diretórios de armazenamento do cache e cria a estrutura de dados necessária.

Por fim, para verificar se o cache estava funcionando, foi utilizado o comando **curl** com a opção **-x** para direcionar as requisições através do proxy Squid. O exemplo foi '**curl -x http://localhost:3128 http://example.com**', como mostrado na Figura 37.

**Figura 37 – Teste do funcionando do cache**



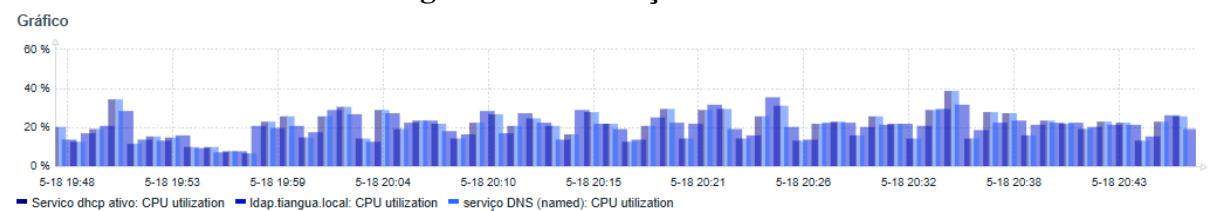
Fonte: Elaborado pelos autores

### 3 GERÊNCIA E MONITORAÇÃO DE AMBIENTES DE REDES

#### 3.1 Monitoramento do Ambiente Local

No gráfico da Figura 38 é possível observar as atividades alternantes dos serviços e o monitoramento das CPUs no qual os serviços estão sendo monitorados em conjunto.

**Figura 38 – Utilização das CPUs**



Fonte: Elaborado pelos autores

##### 3.1.1 Monitoramento Servidor DHCP

Os gráficos representados nas Figuras 39, 40, 41, 42 referem-se à máquina virtual Ubuntu Server que hospeda o serviço DHCP, responsável por atribuir automaticamente configurações de rede aos clientes. As figuras citadas (CPU, Memória, Rede e Disco) mostram o comportamento do sistema entre 10:26 e 20:10 do dia 18/06.

No gráfico da Figura 39, a utilização média da CPU foi de 14,90%, com pico máximo de 46,45% ao final do período — valor dentro dos limites normais e sem disparo de alertas. Já no gráfico da Figura 40, o uso de memória RAM variou de 26,63% a 36,71%, com média de 35%, sem indícios de vazamentos ou sobrecarga. O tráfego de rede na interface enp0s3, mostrado na Figura 41, teve média de 9,69 Kbps recebidos e 85,97 Kbps enviados, com quedas momentâneas por volta das 11:35 e 16:18 — possivelmente por reinicializações ou encerramento de atividades. Na Figura 42, a utilização do disco (sda) apresentou picos de até 50% entre 11:55 e 12:20, mas com fila de I/O baixa (média de 0,055), indicando operação estável.

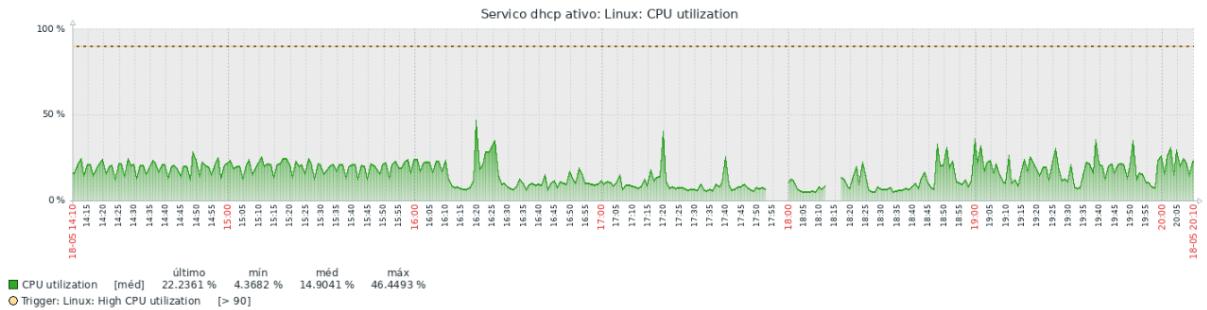
Em resumo, o serviço DHCP está operando de forma estável, eficiente e dentro dos parâmetros esperados, sem indícios de falhas ou gargalos nos recursos do sistema.

##### 3.1.2 Monitoramento Servidor DNS

Os gráficos representados nas Figuras 43, 44, 45, 46 são referentes à máquina virtual Ubuntu Server que hospeda o serviço DNS, responsável pela resolução de nomes na rede. O processo principal monitorado indiretamente através do consumo de CPU é o bind9.

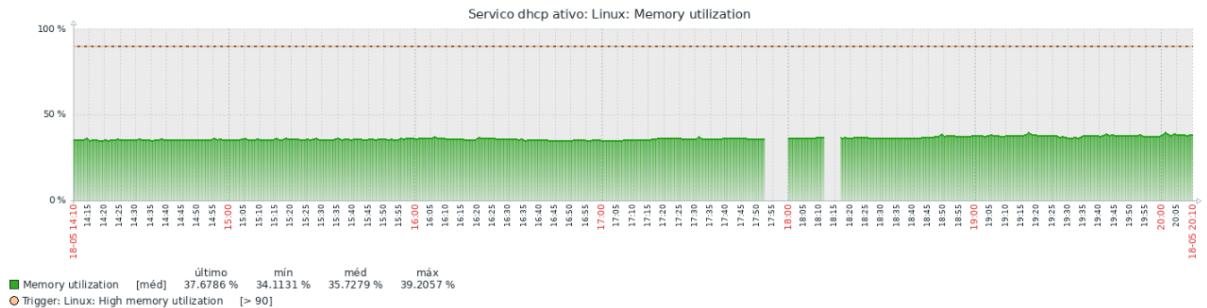
No período analisado, mostrado no gráfico da Figura 43, o consumo médio de CPU

**Figura 39 – Serviço DHCP gráficos da CPU**



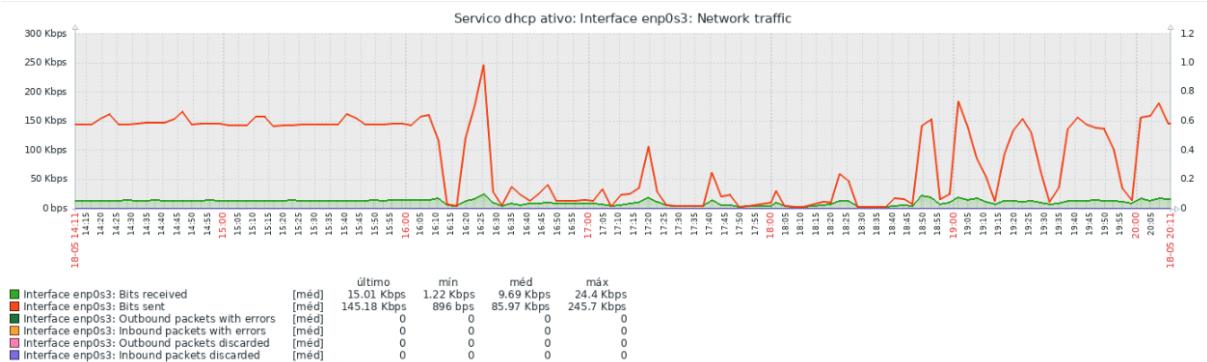
Fonte: Elaborado pelos autores

**Figura 40 – Serviço DHCP gráficos de Memória**



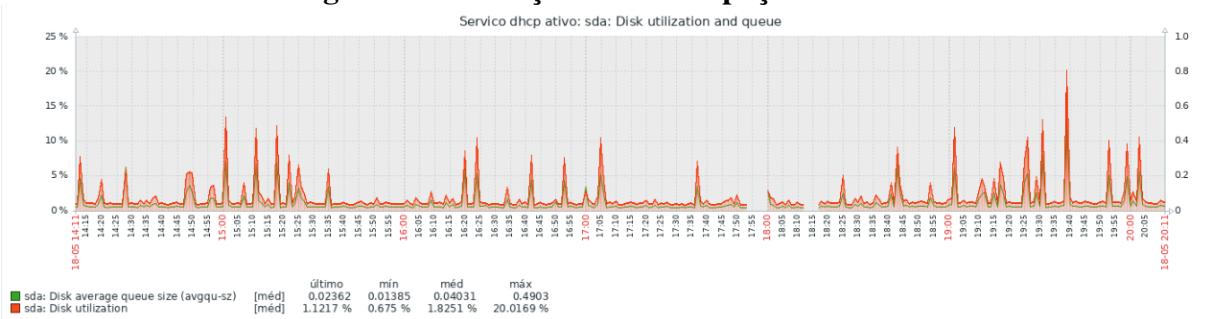
Fonte: Elaborado pelos autores

**Figura 41 – Serviço DHCP Tráfego de rede**



Fonte: Elaborado pelos autores

**Figura 42 – Serviço DHCP Ocupação de disco**



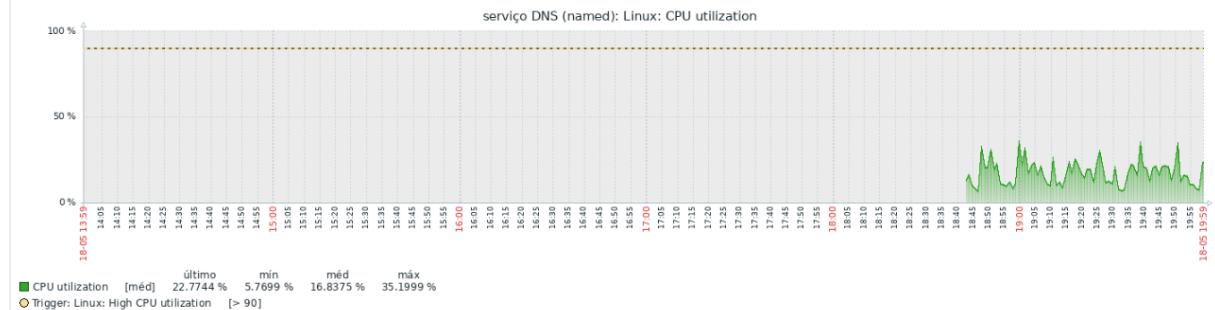
Fonte: Elaborado pelos autores

foi de 16%, o valor máximo registrado foi de 35%, e o valor mínimo observado foi de 7,6%. Observa-se que o consumo de CPU da VM DNS manteve-se, em média, em torno de 18%.

Houve picos de utilização que atingiram aproximadamente 40% em momentos específicos, coincidindo com os horários de maior volume de consultas DNS na rede. Os valores de consumo ficaram em torno de 10%, como mostrado na Figura 45.

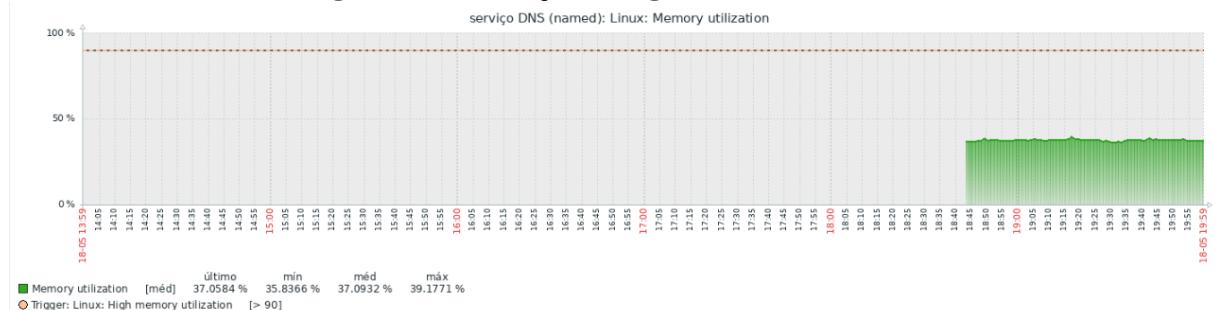
O monitoramento da interface enp0s3 associada ao serviço DNS (named) mostra atividade crescente a partir das 18:50, indicando consultas e respostas DNS válidas. O tráfego atinge picos de 171 Kbps, com ausência total de erros ou perdas, confirmando o funcionamento estável do serviço.

**Figura 43 – Serviço DNS gráficos da CPU**



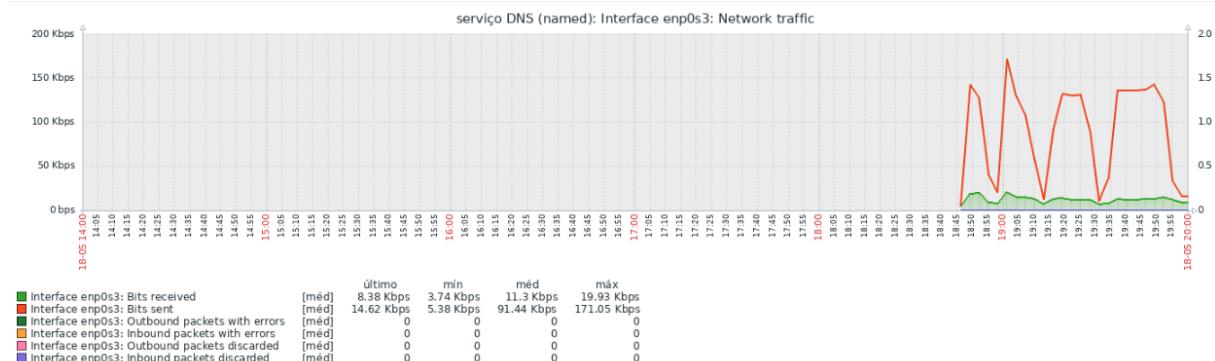
Fonte: Elaborado pelos autores

**Figura 44 – Serviço DNS gráficos de Memória**

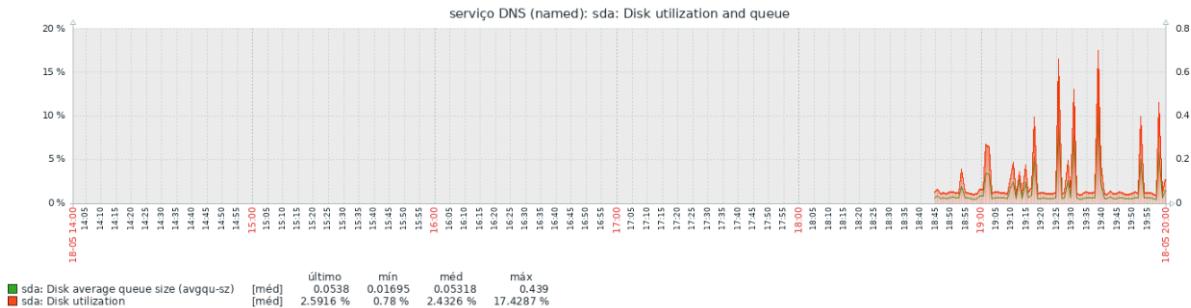


Fonte: Elaborado pelos autores

**Figura 45 – Serviço DNS Tráfego de rede**



Fonte: Elaborado pelos autores

**Figura 46 – Serviço DNS Ocupação de disco**

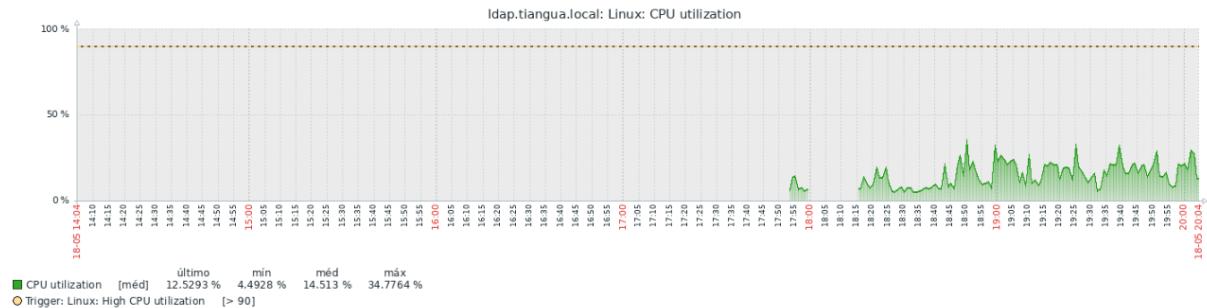
**Fonte:** Elaborado pelos autores

### 3.1.3 Monitoramento Servidor LDAP

Os gráficos representados nas Figuras 47, 48, 49, 50 referem-se à máquina virtual Ubuntu Server dedicada a hospedar o serviço LDAP (Lightweight Directory Access Protocol), que provê autenticação centralizada e informações de diretório. O processo principal associado é o slapd.

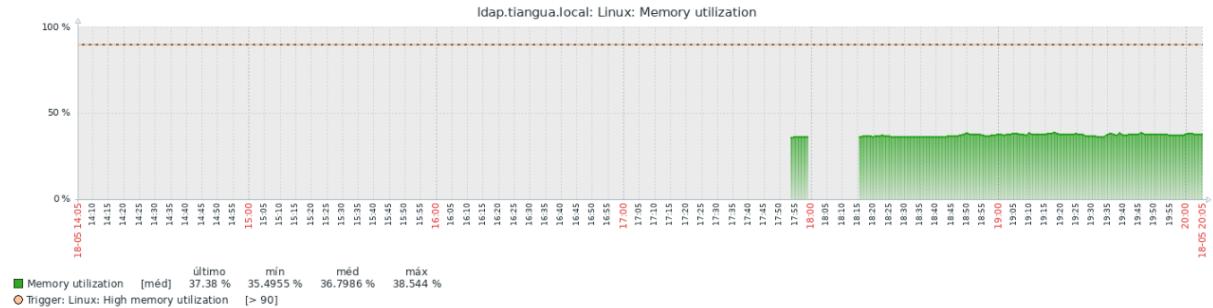
No período de monitoramento, mostrado na Figura 48, o consumo médio de memória foi de aproximadamente 36%. O valor máximo registrado foi de 38% e o mínimo de 35%. Durante as últimas horas, o consumo de memória pela VM LDAP mostrou-se relativamente estável. Observa-se um patamar de uso constante em torno de 36% da memória total alocada para a VM. Não houve picos abruptos ou vales significativos, nem uma tendência clara de aumento ou diminuição gradual, indicando que o serviço slapd e o sistema operacional mantiveram um footprint de memória consistente após a inicialização e o carregamento de seus caches.

O monitoramento da utilização de CPU do host ldap.tiangua.local mostra um aumento gradual de atividade após as 18:00, com média de 16,2% e pico de 35,4%, que pode ser observado na Figura 47. O sistema opera dentro de limites seguros, sem ultrapassar o limite crítico de 90% configurado na trigger de alerta.

**Figura 47 – Serviço LDAP gráficos da CPU**

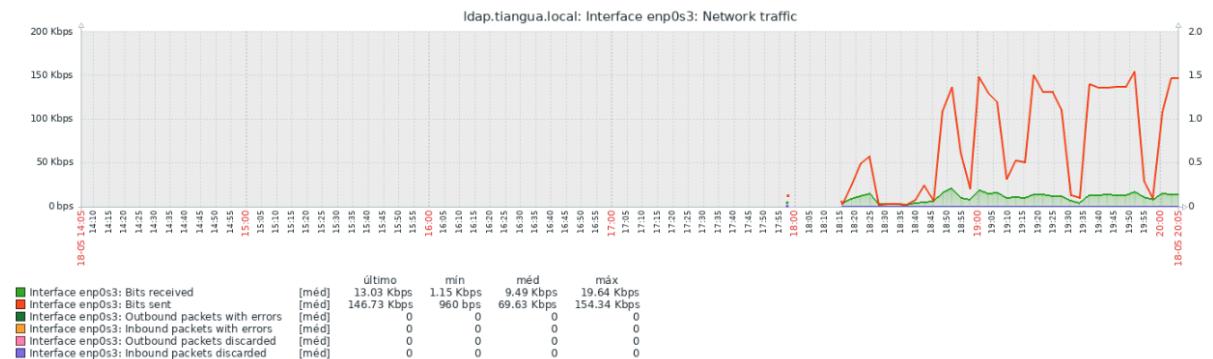
**Fonte:** Elaborado pelos autores

**Figura 48 – Serviço LDAP gráficos de Memória**



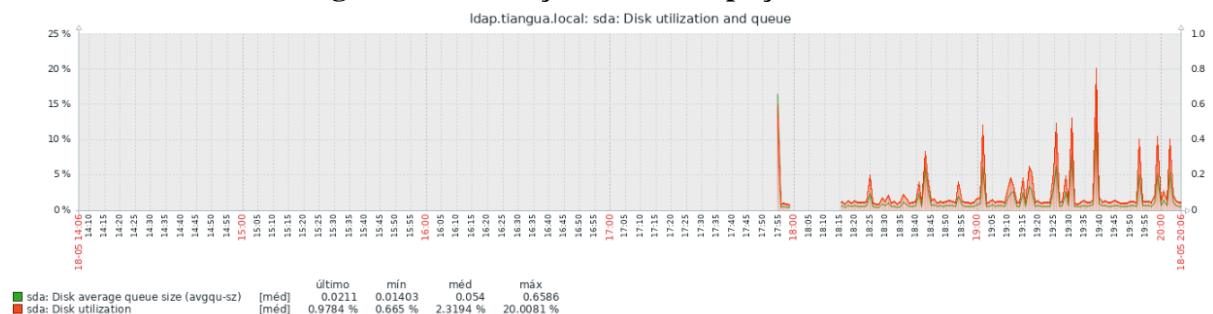
Fonte: Elaborado pelos autores

**Figura 49 – Serviço LDAP Tráfego de rede**



Fonte: Elaborado pelos autores

**Figura 50 – Serviço LDAP Ocupação de disco**



Fonte: Elaborado pelos autores

### 3.2 Monitoramento do Ambiente na Nuvem

Realizou-se o monitoramento da instância EC2 executando Linux Ubuntu na AWS instalada e configurada na etapa anterior, utilizando a ferramenta Zabbix. Para fazer esse monitoramento, uma nova instância EC2 foi criada na AWS, sendo responsável por essa função e tendo as seguintes configurações:

- **IP Privado:** 172.31.20.110
- **Sistema Operacional:** Ubuntu Server 24.04
- **Intervalo de portas:** 10050 - 10051/TCP

- **Login Zabbix:**

- **Usuário:** Admin
- **Senha:** IAE@2025

A máquina virtual monitorada é a instância “Srv Ubuntu 1” que possui as seguintes configurações:

- **IP Privado:** 172.31.81.197
- **Sistema Operacional:** Ubuntu Server 24.04
- **Nome do servidor no Zabbix:** Servidor Geral AWS
- **Monitoramento via:** Zabbix Agent2 (porta 10050)
- **Templates aplicados:** Linux by Zabbix agent active, AWS EC2 by HTTP e PostgreSQL by Zabbix agent 2 active.

O objetivo da análise é avaliar o desempenho e a saúde do sistema ao longo de um intervalo de tempo, com base em diversos indicadores como utilização de CPU, memória, disco e rede. Para a realização dos testes, o servidor web foi utilizado simultaneamente por vários usuários navegando pelo sistema e consumindo os vídeos presentes nele.

### **3.2.1 Utilização do CPU**

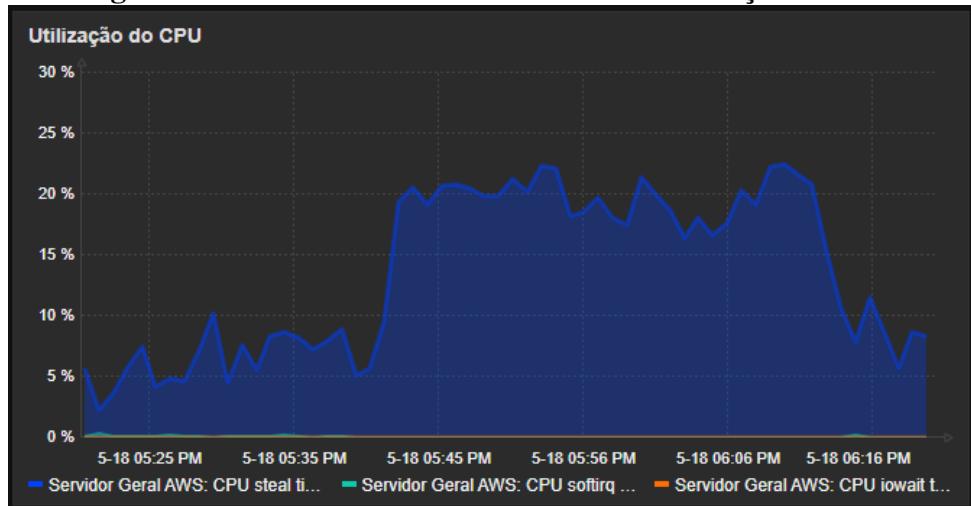
O gráfico "Utilização do CPU", representado na Figura 51, mostra uma variação entre aproximadamente 3% e 20%, com um pico de utilização mais constante nos minutos finais do intervalo observado. Este comportamento pode indicar o início de uma carga de trabalho mais intensa, sugerindo a necessidade de atenção contínua para identificar processos consumidores de CPU.

O gráfico "Tempo de utilização no sistema e usuário", na Figura 52, mostra que a maior parte do tempo de CPU foi consumida em modo sistema, com picos de uso em torno de 0,5%, enquanto o tempo em modo de usuário foi levemente inferior. No intervalo em que ambos foram em torno de 0,1%, no período entre 17:43 e 18:12, o servidor web estava com pouca movimentação de usuários, enquanto nos intervalos de picos havia muitos acessos simultâneos.

### **3.2.2 Carregamento do Sistema Linux**

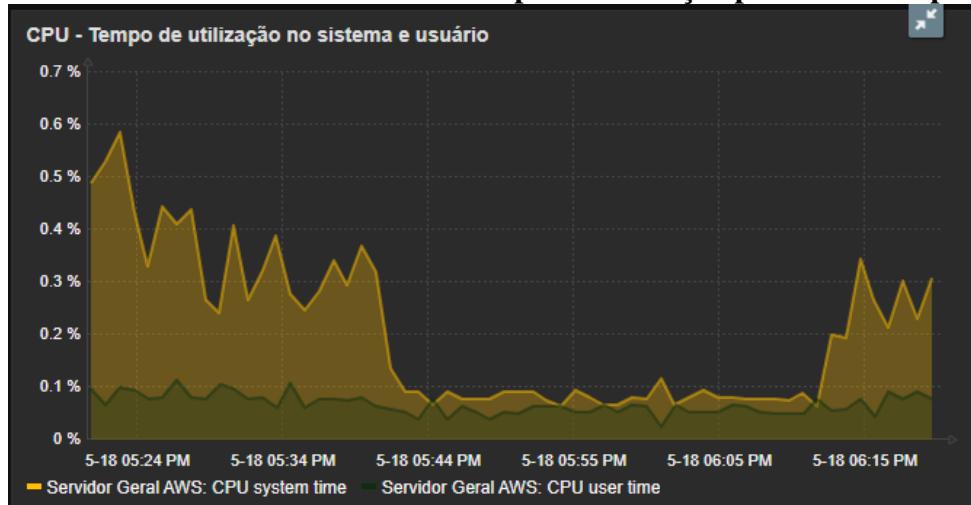
A carga média do sistema ("Load average"), mostrada na Figura 53, apresentou valores baixos, abaixo de 0,3, indicando que a instância não está sobrecarregada. Mesmo nos picos, os valores permaneceram em níveis aceitáveis, o que demonstra um bom dimensionamento dos recursos computacionais em relação à carga processada.

**Figura 51 – Gráfico de monitoramento da utilização do CPU**



Fonte: Elaborado pelos autores

**Figura 52 – Gráfico de monitoramento do tempo de utilização pelo sistema e pelo usuário**



Fonte: Elaborado pelos autores

**Figura 53 – Gráfico de monitoramento do carregamento do sistema Linux**



Fonte: Elaborado pelos autores

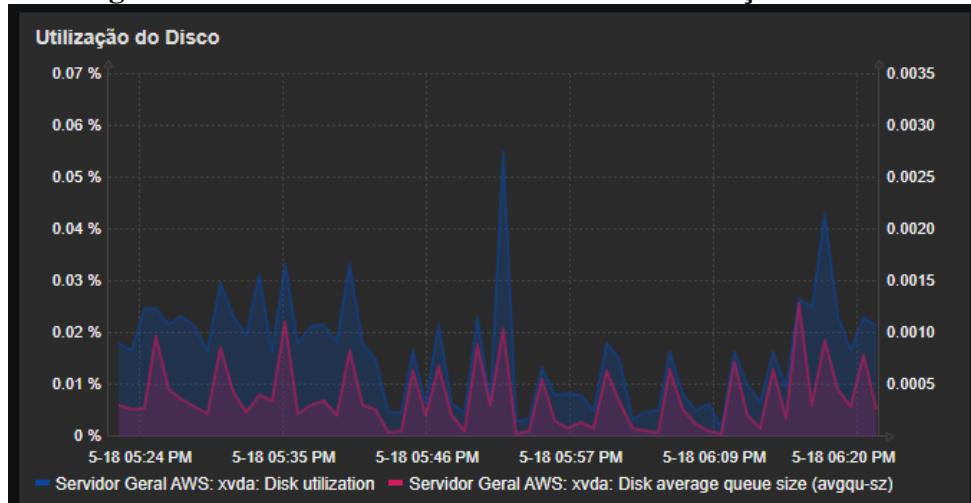
### 3.2.3 Utilização de Disco

A "Utilização do Disco", mostrada na Figura 54, manteve-se em níveis baixos, com a maioria dos valores abaixo de 0,05%. Houve poucos picos, sem constância, o que sugere um uso esporádico e sem gargalos visíveis. Apenas quando a instância foi ativada, houve um pico de utilização de 2,7%, mas que provavelmente ocorreu por ter sido iniciada.

O "Tempo médio de espera do disco", Figura 55, e as "Taxas de leitura/gravação de

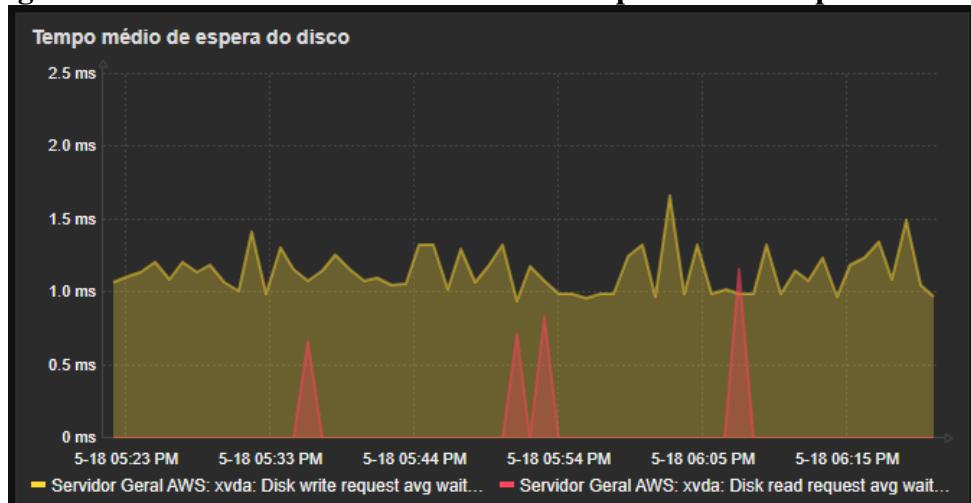
disco", Figura 56, também permaneceram dentro de margens aceitáveis, sem indícios de lentidão no subsistema de armazenamento. Isso é essencial para garantir um bom desempenho em operações de leitura e escrita de dados. O tempo médio de espera variou entre 1 ms a 1,5 ms, enquanto as taxas se mantiveram abaixo de 1 r/s, tendo apenas um pico inicial quando a instância foi iniciada.

**Figura 54 – Gráfico de monitoramento da utilização do disco**



Fonte: Elaborado pelos autores

**Figura 55 – Gráfico de monitoramento do tempo médio de espera do disco**

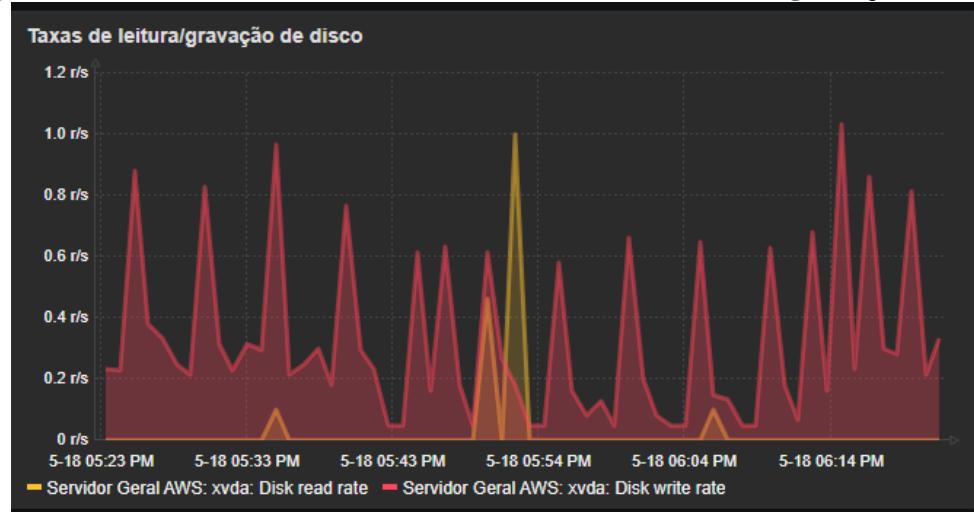


Fonte: Elaborado pelos autores

### 3.2.4 Uso da memória

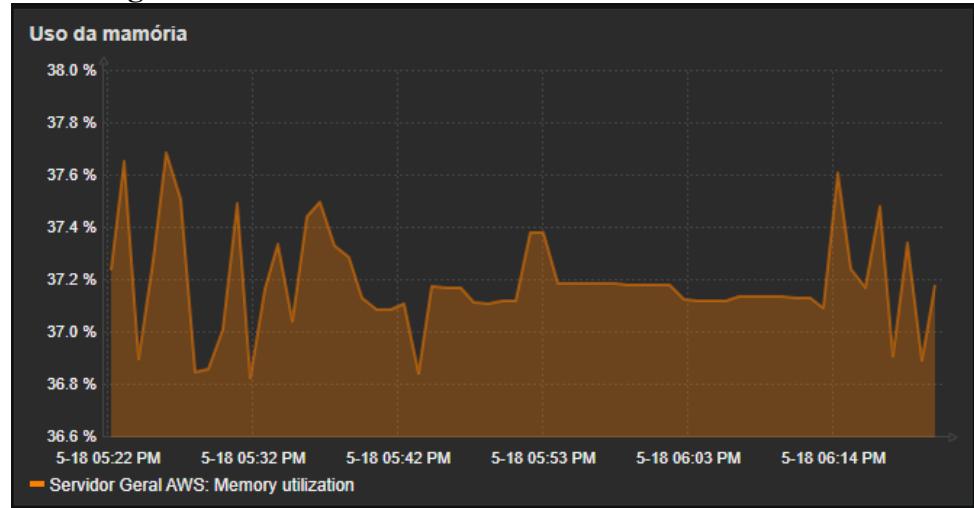
O uso de memória variou entre 36,8% e 37,7%, como mostrado na Figura 57, indicando que ainda há uma boa margem de memória livre. Não foram identificados picos ou quedas abruptas, o que sugere estabilidade no consumo e ausência de vazamentos de memória por parte dos serviços em execução.

**Figura 56 – Gráfico de monitoramento das taxas de leitura e gravação do disco**



Fonte: Elaborado pelos autores

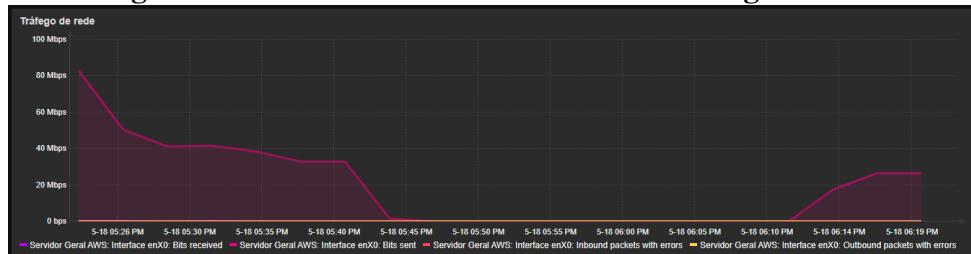
**Figura 57 – Gráfico de monitoramento do uso da memória**



Fonte: Elaborado pelos autores

### 3.2.5 Tráfego de Rede

O tráfego de rede, conforme a Figura 58, mostra variação entre 20 Mbps e 80 Mbps, com um pico notável próximo dos 80 Mbps durante o intervalo monitorado. O volume de pacotes enviados e recebidos também acompanharam esse padrão. Esse comportamento é esperado em servidores ativos em rede, mas deve ser monitorado em períodos de maior carga para garantir que não haja saturação de banda. Nos períodos de maiores valores de Mbps o servidor web recebe mais acessos, enquanto que durante às 17:44 e 18:06 não havia movimentação, o que explica os baixos valores.

**Figura 58 – Gráfico de monitoramento do tráfego de rede**

**Fonte:** Elaborado pelos autores

### 3.2.6 Conclusão do monitoramento no ambiente da nuvem

Os dados obtidos por meio do Zabbix indicam que a instância EC2 “Srv Ubuntu 1” monitorada apresentou bom desempenho e estabilidade operacional. Além disso, não foram detectadas falhas ou sobrecargas significativas nos recursos analisados (CPU, memória, disco e rede). Logo, todos os serviços monitorados operam dentro dos parâmetros aceitáveis, validando a configuração atual do ambiente como adequada. O dashboard criado no sistema ‘Zabbix’ é mostrado na Figura 59, no qual todos os gráficos mencionados anteriormente estão juntos, permitindo uma visualização em conjunto.

Para dar continuidade à operação, é de suma importância manter o monitoramento ativo e realizar análises periódicas, principalmente em momentos de pico de utilização, visando antecipar possíveis gargalos ou falhas, tendo em vista que, na análise, tais momentos foram os que trouxeram os maiores números.

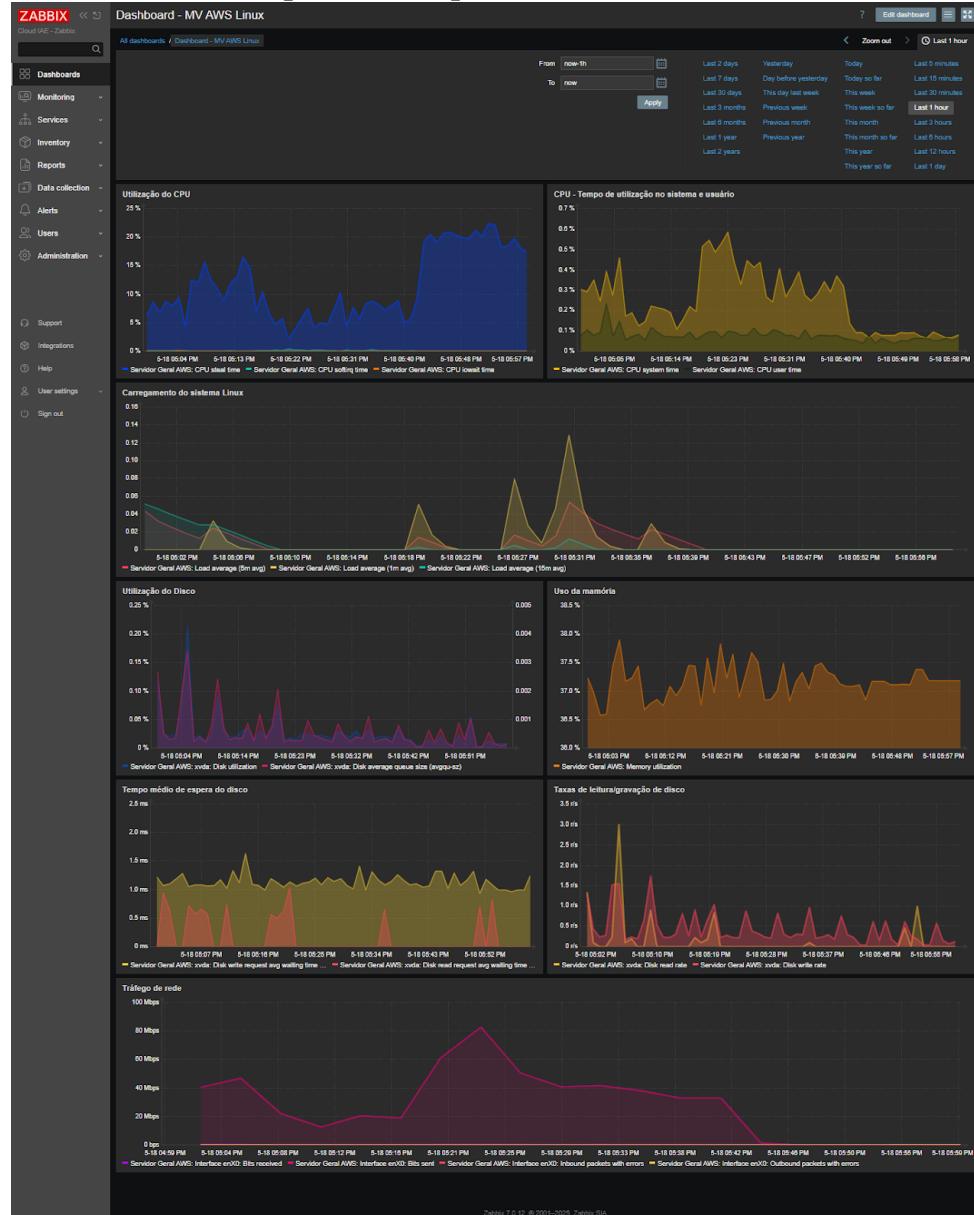
## 4 MECANISMOS DE SEGURANÇA DA INFORMAÇÃO

### 4.1 Política de Segurança da Informação (PSI)

A Política de Segurança da Informação (PSI) é um componente essencial para a proteção dos ativos digitais em qualquer instituição, especialmente em ambientes acadêmicos que lidam com grande volume de dados sensíveis, como informações de alunos, servidores e pesquisas. No Brasil, o (Brasil, 2018) institui a Política Nacional de Segurança da Informação no âmbito da administração pública federal, reforçando a importância de garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação. Internacionalmente, a norma ISO/IEC 27001 serve como referência para a gestão da segurança da informação, definindo diretrizes para proteger dados contra ameaças, assegurar a continuidade das operações e promover a confiança nos sistemas utilizados.

No contexto de uma universidade, a PSI tem como principal objetivo minimizar os riscos de incidentes relacionados à segurança da informação, estabelecendo diretrizes claras para o uso adequado dos recursos de TI. Uma política bem estruturada contribui para o alinhamento dos colaboradores com as normas institucionais, promove a conformidade com a Lei Geral de

**Figura 59 – Dashboard completo da máquina virtual Linux Ubuntu da AWS no Zabbix**



**Fonte:** Elaborado pelos autores

Proteção de Dados (LGPD) e fortalece a governança digital da instituição. Além disso, favorece a transparéncia, a eficiência operacional e a experiência de toda a comunidade acadêmica ao assegurar que os dados estejam protegidos e disponíveis quando necessário. A Política de Segurança da Informação do Instituto Acadêmico de Excelência pode ser consultada por meio do link disponibilizado abaixo.

*Link: [Política de Segurança da Informação da IAE](#).*

## 4.2 Cartilha de Boas Práticas de Acesso Seguro

A Cartilha de Boas Práticas de Acesso Seguro é um complemento fundamental à Política de Segurança da Informação, pois visa orientar toda a comunidade acadêmica — alunos,

professores, técnicos e demais colaboradores — sobre comportamentos seguros no uso dos recursos de tecnologia da informação e comunicação. Em um ambiente universitário, onde o acesso à rede e a sistemas digitais é constante e diversificado, adotar práticas conscientes no manuseio dos recursos digitais e utilização de computadores e conexões é essencial para prevenir acessos não autorizados, vazamentos de dados e outros incidentes que possam comprometer a integridade das informações institucionais.

Além de promover a conscientização e a responsabilidade individual, a cartilha contribui para a criação de uma cultura organizacional voltada à segurança da informação. Quando todos os usuários estão alinhados às boas práticas, os riscos de incidentes são significativamente reduzidos. Dessa forma, a cartilha atua não apenas como um material educativo, mas como uma ferramenta estratégica de prevenção, reforçando o compromisso da instituição com a proteção de seus dados e com a continuidade segura de suas atividades acadêmicas e administrativas.

A [Cartilha de Acesso Seguro da IAE](#) completa pode ser observada nas Figuras 60 e 61.

**Figura 60 – Frente da Cartilha de Acesso Seguro da IAE**



Fonte: Elaborado pelos autores

### 4.3 Análise de Vulnerabilidade

Os 3 principais riscos de segurança, entre os dez listados pela (Foundation, 2025), identificados com relevância e relacionados com nossos serviços WEB para nossa instituição de ensino e que devem ser explorados para prevenção de acidentes e consequências maiores devido ao mal gerenciamento das redes, dos sistemas e das informações contidas nos mesmos.

**Figura 61 – Verso da Cartilha de Acesso Seguro da IAE**

### O QUE É PROIBIDO?

*Atenção aos comportamentos que comprometem a segurança:*

- Compartilhar seu login ou senha com qualquer pessoa.
- Instalar programas sem a autorização da equipe de TI.
- Salvar arquivos da faculdade em pendrives ou dispositivos pessoais.
- Usar os computadores da IAE para fins pessoais ou ilegais.
- Divulgar informações da instituição em redes sociais ou outros canais sem permissão formal.

### CONSCIENTIZAÇÃO E TREINAMENTO

A IAE oferece treinamentos e campanhas periódicas para te ajudar a:

- Identificar e evitar golpes.
- Criar senhas super seguras.
- Cuidar melhor dos seus dados e dos dados da faculdade.
- Não perca! Sua participação é muito importante para a segurança de todos!

### A SEGURANÇA É UMA JORNADA CONTÍNUA.

As ameaças evoluem constantemente, e por isso, na IAE, buscamos melhorar nossas práticas de segurança, mantendo vigilância constante e adaptando nossas defesas.

Isso significa que estamos sempre atentos para:

Incluir novas ameaças      Atender exigências legais      Atualizar medidas de proteção

*Sua colaboração é essencial para manter um ambiente digital seguro para todos.*

### SEGURANÇA FÍSICA E EQUIPAMENTOS

- Use nossos equipamentos (notebooks, computadores de laboratório, projetores) com responsabilidade e cuidado. Eles são ferramentas importantes para suas atividades!
- Nunca retire equipamentos da instituição sem ter uma autorização formal.
- Em caso de perda, roubo ou qualquer dano, avise a equipe de TI imediatamente. Sua rapidez é fundamental!

### IDENTIFICOU ALGO SUSPEITO?

Sua ajuda é essencial! Se você notar algo suspeito, avise imediatamente a equipe de segurança:

- Acessos ou movimentações não autorizadas em sua conta ou sistemas.
- Perda ou vazamento de dados (seus ou da IAE).
- Vírus, malware ou qualquer comportamento estranho no seu computador ou na rede.

Como nos avisar?

Envie um e-mail para: [ti@iae.edu.br](mailto:ti@iae.edu.br)

Ou entre em contato com o Suporte de TI.

**Fonte: Elaborado pelos autores**

#### **4.3.1 A01:2017 - Injection (Injeção de comandos)**

Sistemas como o sistema de biblioteca, gestão acadêmica, financeiro e de alta gestão acessam bancos de dados com frequência e aceitam entrada de dados dos usuários, como login, consulta de notas, etc. Portanto, são vulneráveis a SQL Injection, LDAP Injection, entre outras. Os serviços impactados são: servidor Web e Banco de Dados, LDAP e Serviço DNS (em casos de injeção maliciosa via campos configuráveis).

##### **4.3.1.1 Exemplos de problemas com Injection**

Nos sistemas de biblioteca, ou outros sistemas que envolvem cadastros e transações, a manipulação indevida de campos por meio de formulários ou URLs pode comprometer a integridade dos dados. Isso pode resultar em ações não autorizadas, como registros incorretos ou uso indevido de informações, causando transtornos aos usuários e à administração do sistema.

No módulo financeiro, podem ocorrer impactos como o acesso, modificação ou exclusão indevida de dados relacionados a cobranças, boletos, notas fiscais e registros de pagamento. Também há o risco de manipulação de informações bancárias de alunos ou da instituição, além da possibilidade de alteração no status de dívidas, o que pode permitir, por exemplo, o cancelamento de cobranças sem a devida autorização.

Em sistemas acadêmicos, falhas na validação de dados e na autenticação podem expor informações acadêmicas e financeiras, permitir alterações indevidas no sistema e facilitar o acesso não autorizado a contas de alunos e funcionários, comprometendo a segurança e a

integridade das operações.

#### **4.3.1.2 Consequências Diretas de Injection**

- Vazamento de dados sensíveis: Através de uma injeção SQL, um invasor pode acessar informações como dados pessoais de alunos, notas, documentos acadêmicos, senhas, informações bancárias ou relatórios internos comprometendo a confidencialidade e possível violação de LGPD (Lei Geral de Proteção de Dados).
- Alteração ou destruição de dados no banco: Um atacante pode usar comandos como delete ou update via injeção para modificar ou apagar registros do banco de dados impactando na perda de registros acadêmicos, boletins, históricos, controle de biblioteca e dados financeiros, comprometendo o funcionamento da instituição.
- Escalada de privilégios: Através de manipulação de comandos, um usuário comum pode se autenticar como administrador, ganhando acesso total ao sistema e o controle completo da aplicação, podendo alterar regras, usuários, senhas e permissões.
- Execução de comandos no servidor: Em casos mais graves (como Command Injection), o invasor pode executar comandos no sistema operacional, instalar malwares ou abrir backdoors comprometendo a totalidade do servidor e da rede interna.
- Comprometimento de sistemas interligados: Uma injeção bem-sucedida no sistema acadêmico pode permitir movimentações que afetam o LDAP, banco de dados financeiro ou até o ambiente de e-mails, podendo gerar a expansão do ataque para múltiplos sistemas da universidade.

#### **4.3.1.3 Ações recomendadas**

- Para evitar injeções (como SQL ou LDAP), é essencial validar o tipo e o formato dos dados, impedir letras em campos numéricos e limitar o tamanho dos textos. Caracteres especiais devem ser higienizados com funções de escape. A validação deve ocorrer no servidor, mesmo que também exista no cliente, pois o navegador pode ser manipulado.
- Use consultas parametrizadas (prepared statements) no lugar de SQL por concatenação. Prefira ORMs como Hibernate, Sequelize, Eloquent ou SQLAlchemy, que aplicam essas práticas automaticamente. Se não usar ORM, utilize bind parameters.

#### **4.3.2 A02:2017 - Broken Authentication (Autenticação Quebrada)**

O sistema usa LDAP para autenticação, o que é ótimo, mas exige configuração correta e segurança nos canais. Se a autenticação for mal implementada, pode permitir login indevido ou sessão hijacking. Os sistemas mais impactados são LDAP, servidor Web (sistemas acadêmicos), FTP (acesso por credencial) e Firewall (se houver login para o painel).

#### **4.3.2.1 Exemplos de problemas com Broken Authentication**

O Sistema de Gestão Acadêmica (SGA) centraliza funções como matrícula, histórico escolar, boletins e dados financeiros. Caso haja falhas de segurança, invasores podem acessar contas de usuários e alterar registros acadêmicos.

O Portal Administrativo e Financeiro é utilizado por setores internos da instituição e contém informações sensíveis, como boletos, contratos e movimentações financeiras. A falta de proteção adequada pode expor esses dados a acessos não autorizados.

O Serviço de Autenticação Central, como LDAP ou Active Directory, controla o login único dos sistemas integrados. Se mal configurado ou exposto, pode permitir que invasores obtenham credenciais ou alterem permissões de acesso.

#### **4.3.2.2 Consequências Diretas de Broken Authentication**

- Acesso indevido a dados pessoais e acadêmicos: Um atacante pode se passar por outro aluno ou funcionário, acessando boletins, CPF, e histórico escolar.
- Privilégios indevidos (elevação de privilégios): Usuários comuns podem explorar falhas para obter permissões administrativas, conseguindo alterar dados da instituição, grades curriculares ou senhas de outros usuários.
- Comprometimento de múltiplos sistemas integrados: Se o sistema usa autenticação centralizada (LDAP), o comprometimento de uma conta pode permitir acesso a diversos serviços da universidade: biblioteca, Wi-Fi, sistemas acadêmicos, e-mail institucional etc.

#### **4.3.2.3 Ações recomendadas**

- Verificar uso de protocolos seguros (HTTPS/LDAPS), garantindo que o tráfego de autenticação esteja protegido por criptografia. Ação: Certificar-se de que todos os logins, APIs e acessos ao LDAP ocorrem via HTTPS ou LDAPS, evitando o envio de credenciais em texto claro.
- Revisar política de senhas, garantindo que as senhas dos usuários tenham complexidade e força suficientes. Ações: Avaliar se há exigência de mínimo de caracteres, uso de letras maiúsculas e minúsculas, números e símbolos, expiração periódica e bloqueio após tentativas incorretas.
- Analisar persistência e controle de sessões para prevenir sequestro de sessão ou uso prolongado de sessões sem supervisão. Ação: Verificar se há expiração automática de sessão por inatividade, tokens de sessão são regenerados após login e os cookies de sessão estão com flags Secure e HttpOnly ativadas.
- Garantir armazenamento seguro das credenciais, protegendo as senhas contra vazamentos e ataques internos e avaliando se estão sendo armazenadas com algoritmos de hash

seguros como bcrypt, scrypt, Argon2 (e nunca em texto puro ou com hash fraco como MD5/SHA1).

- Verificar proteção contra força bruta e automação impedindo ataques de login automatizado. Ação: Validar se há limitação de tentativas de login (bloqueio temporário ou CAPTCHA), registro de tentativas falhas em log e alertas para tentativas suspeitas.
- Revisar permissões de acesso e privilégios, evitando que usuários comuns tenham acesso a funções administrativas. Ação: Auditar perfis de usuários, verificando se cada função possui apenas os privilégios estritamente necessários (princípio do menor privilégio).

#### **4.3.3 A06:2017 - Security Misconfiguration (Configuração Incorreta de Segurança)**

Ambientes que utilizam vários serviços, como DNS, DHCP, LDAP, FTP, Web, Banco de Dados, Proxy, Firewall e NFS, apresentam maior risco de erros de configuração e falhas de integração. Quanto mais sistemas ativos, maior a chance de configurações padrão inseguras não serem corrigidas.

Muitos softwares são instalados com senhas fracas, usuários padrão e serviços desnecessários ativados. Se não forem revisados, deixam o sistema vulnerável a ataques. A exposição de serviços e diretórios sem necessidade — como painéis de administração ou backups públicos — também aumenta o risco de vazamentos e acessos indevidos.

A falta de atualizações e patches de segurança permite que falhas conhecidas permanecem exploráveis. Softwares antigos sem suporte ainda usados por compatibilidade agravam o problema. Além disso, permissões excessivas, como scripts com acesso de escrita desnecessário ou serviços rodando como root, ampliam a superfície de ataque. Sem auditorias periódicas, esses problemas persistem sem detecção. Abaixo estão os impactos por serviço:

- Web e Banco de Dados: Senhas fracas, diretórios abertos e painéis expostos podem causar vazamento de dados e manipulação indevida.
- LDAP: Sem LDAPS e com permissões incorretas, pode haver roubo de credenciais e comprometimento do login centralizado.
- FTP: Acesso anônimo e sem criptografia pode expor arquivos sensíveis.
- Firewall/Proxy: Regras amplas e ausência de logs permitem invasões e dificultam o controle da rede.
- DNS/DHCP: Sem restrições, podem ocorrer ataques como DNS spoofing e uso indevido da rede.
- NFS: Permissões amplas e sem autenticação podem permitir acesso indevido a arquivos e estações.

#### **4.3.3.1 Exemplos de Problemas com Diretas de Security Misconfiguration**

A exposição do painel administrativo do sistema, acessível publicamente via caminhos como /admin e sem restrições adicionais, representa um risco significativo. Atacantes podem explorá-lo tentando senhas padrão ou falhas conhecidas. O uso de credenciais fracas ou padrão em serviços como banco de dados, FTP ou LDAP facilita ataques automatizados. Combinado com senhas previsíveis, isso pode permitir o controle completo desses serviços.

A presença de portas desnecessárias abertas na rede pública, como Telnet, FTP ou MySQL, amplia a superfície de ataque. Esses serviços, muitas vezes desatualizados, ficam vulneráveis a varreduras e explorações. Além disso, mensagens de erro detalhadas exibidas ao usuário, como falhas de SQL, revelam informações internas da aplicação. Esse tipo de exposição pode ser explorado por atacantes para compreender e comprometer o sistema.

Permissões excessivas em arquivos e diretórios podem expor dados sensíveis, especialmente quando pastas como /backup ou /logs estão acessíveis via navegador ou rede. Isso permite o download indevido de arquivos com senhas, configurações ou até mesmo cópias de banco de dados. Ademais, a ausência de protocolos seguros, como HTTPS ou LDAPS, representa um risco significativo durante o login ou autenticação. Transmissões feitas em HTTP simples podem ser interceptadas por terceiros, especialmente em redes públicas, comprometendo credenciais de acesso.

Configurações inadequadas em serviços como NFS, como o uso da opção no\_root\_squash sem restrição de IP, permitem que usuários remotos atuem como root. Isso facilita o acesso ou a modificação de arquivos de outros usuários ou da própria instituição.

#### **4.3.3.2 Consequências Diretas de Security Misconfiguration**

- Exposição de dados e arquivos sensíveis em diretórios de backup, logs ou arquivos de configuração deixados acessíveis na web ou em compartilhamentos abertos (FTP/NFS) podem trazer o vazamento de senhas, dados pessoais de alunos e funcionários, informações financeiras ou chaves de acesso a sistemas.
- Acesso não autorizado a sistemas administrativos, painéis de administração sem restrição de IP, autenticação fraca ou com credenciais padrão (ex: admin:admin) permitem a um invasor poder assumir controle de sistemas como gestão acadêmica, biblioteca, financeiro ou rede.
- Execução de serviços desnecessários ou vulneráveis como Telnet, FTP ou banco de dados escutando em interfaces públicas sem necessidade aumentam a superfície de ataque e risco de exploração de falhas conhecidas.
- Uso de versões desatualizadas de software do PHP, Apache, MySQL, OpenLDAP, etc são vulneráveis e se conhecidas podem ser exploradas para comprometer os serviços.
- Permissões excessivas em arquivos ou usuários, Scripts com permissão de escrita para qualquer usuário (chmod 777) ou serviços rodando como root desnecessariamente po-

dem causar falhas de segurança pode levar ao controle total do sistema ou à modificação maliciosa de arquivos.

- Ausência de criptografia na comunicação de sistemas que realizam autenticação ou troca de dados em HTTP ou LDAP sem TLS tem impacto nas credenciais ou dados sensíveis podem ser interceptados em redes locais ou Wi-Fi da instituição.

#### **4.3.3.3 Ações recomendadas**

- Verificar configurações inseguras, todos os serviços (web, banco de dados, FTP, LDAP, DNS, NFS, Squid, etc.) devem ser revisados para remover senhas padrão, serviços desnecessários e permissões excessivas. Desative o que não for usado e limite o acesso a IPs autorizados.
- Usar protocolos seguros, serviços críticos devem usar HTTPS (para web) e LDAPS (para LDAP). Substitua FTP por SFTP ou FTPS. Isso protege dados e senhas contra interceptação.
- Controlar acesso remoto, uide as portas abertas e limite acessos com firewall e segmentação de rede. Interfaces administrativas (como /admin ou phpMyAdmin) devem ser protegidas com IP autorizado e autenticação em dois fatores.
- Manter sistemas atualizados, atualizar regularmente o sistema operacional e os softwares para corrigir falhas de segurança. Adote uma rotina de manutenção contínua.
- Corrigir permissões em arquivos e pastas, evite permissões como 777 ou leitura pública em arquivos sensíveis (logs, backups, configs). Verifique compartilhamentos via NFS e FTP.

## 5 CONCLUSÃO

O desenvolvimento deste projeto de infraestrutura de rede para o Instituto Acadêmico de Excelência (IAE) permitiu a aplicação prática de conceitos fundamentais de arquitetura de redes, serviços de diretório, virtualização e segurança da informação em um ambiente corporativo acadêmico. A estrutura proposta foi implementada com base em uma topologia em estrela, segmentação de rede por domínios funcionais (alunos, administrativos e professores) e uso de VLANs lógicas em ambientes virtualizados locais via VirtualBox e em nuvem via AWS EC2.

Os serviços críticos — como DHCP, DNS, LDAP, FTP, NFS, Web e Banco de Dados — foram devidamente configurados e integrados, com testes de conectividade, autenticação e resoluções internas validados com sucesso. O monitoramento ativo por meio do Zabbix permitiu a coleta e análise de métricas de desempenho e disponibilidade, possibilitando a identificação de gargalos e a validação da estabilidade dos serviços implantados.

Adicionalmente, foram estabelecidas políticas formais de segurança da informação com base na ISO/IEC 27001, reforçadas por boas práticas operacionais e pela análise de vulnerabilidades alinhadas à OWASP Top 10. Tais medidas garantem não apenas a integridade e disponibilidade dos serviços, mas também a conformidade com normativas legais, como a LGPD.

Conclui-se que a solução projetada é tecnicamente sólida, escalável e segura, capaz de atender às demandas atuais da instituição e preparada para adaptações futuras. O projeto demonstrou, de forma integrada, a importância do planejamento estruturado, da configuração correta de serviços e da gestão contínua do ambiente de rede para garantir a eficiência operacional em contextos acadêmicos complexos.

## REFERÊNCIAS

**BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018.** 2018. *Diário Oficial da União*, Brasília, DF. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2018/Decreto/D9637.htm](https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm)>. Acesso em: 8 jun. 2025.

**DIGITAL, I. M. Aula 03 - Componentes de uma rede - parte 2.** 2018. Disponível em: <<https://materialpublic.imd.ufrn.br/curso/disciplina/4/19/3/4>>. Acesso em: 19 jun. 2025.

**FOUNDATION, O. OWASP Top Ten 2025.** 2025. Disponível em: <<https://owasp.org/www-project-top-ten/>>. Acesso em: 7 jun. 2025.