

APLICAÇÃO DO OPENLDAP NO GERENCIAMENTO DE USUÁRIOS EM REDES DE PEQUENO PORTE

Gabriel Barco Borges¹, Saulo Henrique da Mata²

Resumo: O OpenLDAP é um serviço de diretório de código aberto, que permite a autenticação e gerenciamento de usuários em uma rede, este software pode ser instalado junto a um servidor para gerenciar informações sobre usuários, grupos, permissões e outros recursos encontrados nele. O objetivo deste trabalho é instalar e configurar este sistema como uma alternativa ao Active Directory da Microsoft (que envolve maiores custos para instalação por conta de sua licença), e também administrar usuários e outros recursos que a ferramenta possibilita. Além disso busca-se por meio desse trabalho estudar a viabilidade desse software em uma rede de pequeno porte, analisando sua escalabilidade e flexibilidade. A metodologia empregada consistirá na instalação e configuração do OpenLDAP em uma máquina virtual Debian, hospedada em um ambiente Proxmox. O propósito é autenticar e gerenciar as contas de usuário dos membros do "PET Computação IFTM Campus Ituiutaba", proporcionando facilidade de uso e disponibilizando recursos das máquinas de forma eficiente por meio desta ferramenta.

Palavras-chave: OpenLDAP. Autenticação de Usuários. Serviços de diretório.

APPLICATION OF OPENLDAP IN USER MANAGEMENT FOR SMALL-SCALE NETWORKS

Abstract: OpenLDAP is an open-source directory service that enables user authentication and management in a network. This software can be installed alongside a server to handle information about users, groups, permissions, and other resources within it. The objective of this project is to install and configure this system as an alternative to Microsoft's Active Directory (which involves higher installation costs due to its license) and to administer users and other features provided by the tool. Additionally, this project aims to explore the feasibility of this software in a small-scale network, analyzing its scalability and flexibility. The employed methodology will involve the installation and configuration of OpenLDAP on a Debian virtual machine hosted in a Proxmox environment. The purpose is to authenticate and manage user accounts for members of the "PET Computação IFTM Campus Ituiutaba", providing user-friendly access and efficiently allocating machine resources through this tool.

Keywords: OpenLDAP. User authentication. Directory service.

¹Estudante de Ciência da Computação, IFTM, Campus Ituiutaba, gabriel.borges@estudante.iftm.edu.br

²Professor Orientador, IFTM, Campus Ituiutaba, saulodamata@iftm.edu.br

1 INTRODUÇÃO

Os serviços de diretório têm sido cada vez mais utilizados em todas as organizações do mundo, sejam faculdades, empresas, entre outras. Essa grande demanda se deve ao fato de que em qualquer uma dessas é praticamente essencial centralizar a autenticação de usuários, com o objetivo de reduzir custos e facilitar a administração (BERBELINI, 2017). Com esse aumento em sua necessidade, vários serviços como Active Directory (AD), OpenLDAP e Edirectory, vêm se destacando no mercado. Estas ferramentas não se limitam apenas à autenticação de usuários, como também podem servir como suporte para a realização de atividades tais como nomeação, localização, segurança, entre outras relacionadas a gerir a infraestrutura de recursos nas organizações (CRUZ et al., 2023).

Esses serviços surgiram, mediante à necessidade de se ter um único diretório que possibilitasse ao usuário acessar todos os recursos da empresa com apenas uma única senha, o que não era antes feito, assim, funcionários de uma empresa por exemplo, possuíam várias delas para acessarem diferentes setores.

Como a própria Microsoft define o seu próprio sistema, "o Active Directory é um serviço de diretório que armazena informações sobre objetos em rede e disponibiliza essas informações a usuários e administradores de rede"(MICROSOFT, 2023). Com a sua popularização, tornaram-se indispensáveis para qualquer organização. Logo, não demorou para que fossem criados serviços de código aberto, isto é, acessíveis a qualquer pessoa que queira examinar, modificar, aprimorar, distribuir ou usá-los para qualquer finalidade. Isso se refere ao caso do OpenLDAP, que, como outros destes serviços, é mantido pela própria comunidade de desenvolvedores que o utilizam.

"Comumente o AD é confundido como o concorrente do LDAP, o que não é o caso, porquê ele não é nada mais que um exemplo de um serviço de diretório que suporta LDAP"(BERTOLLI, 2016). O LDAP pode ser definido então, como o protocolo dos sistemas de diretório, ou seja, um meio para consultar os itens em qualquer um dos mesmos que o suportam.

2 SERVIÇOS

Os serviços de diretório desempenham um papel crucial na gestão de identidades e no controle de acesso em ambientes de rede. Estes serviços são projetados para armazenar, organizar e recuperar informações sobre usuários, grupos, recursos e outras entidades em uma rede. Eles

fornecem uma estrutura hierárquica que permite o acesso e a busca eficientes dos dados, seguindo o modelo de árvore, onde cada nó representa uma entrada ou objeto.

Atualmente, existem várias soluções de diretório disponíveis, cada uma com características e funcionalidades distintas. Nesta seção, será demonstrado o estado da arte atual desses serviços, com foco no Lightweight Directory Access Protocol (LDAP), que se baseia no padrão X.500, um protocolo pesado, que opera sobre a pilha completa de protocolos OSI e requer uma quantidade significativa de recursos computacionais.

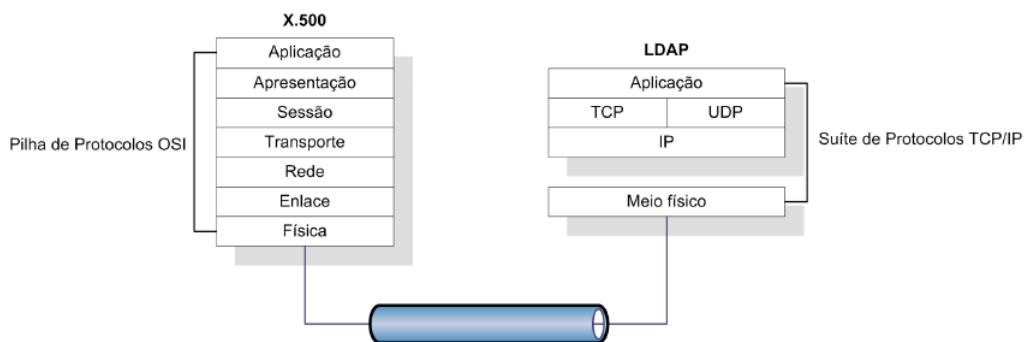


Figura 1: X.500 sobre OSI vs. LDAP sobre TCP/IP (MACHADO; JUNIOR, 2020).

Como ilustrado na Figura 1, o LDAP é projetado para operar sobre TCP/IP e fornece a maioria das funcionalidades do X.500 com um custo muito menor, pois não precisa rodar na pilha de sete camadas OSI (MACHADO; JUNIOR, 2020).

2.1 LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

Como foi citado anteriormente, o modelo de árvore de nós é usado para representar a estrutura hierárquica de um serviço de diretório LDAP. Nesse modelo, os nós são os elementos fundamentais que compõem o diretório e organizam as informações armazenadas nele.

O LDAP foi desenvolvido para ser servidor de diretório com propósito geral, ou seja, foi desenvolvido para que os administradores possam definir que tipo de informação vai ser armazenada pelo servidor, com clareza e cuidado (SILVA, 2021). Logo, seus nós podem representar diferentes tipos de objetos ou entidades, como usuários, grupos, computadores, organizações, unidades organizacionais, entre outros, dependendo da finalidade e do escopo do diretório.

A organização dos dados é feita em forma de uma árvore hierárquica. Cada nó possui um identificador único chamado de "Distinguished Name"(DN). Como exemplificado na figura 2, temos então os respectivos nós:

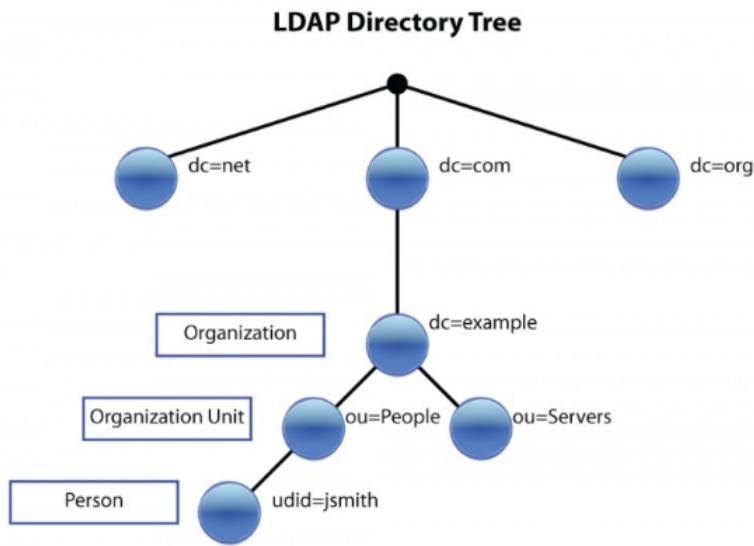


Figura 2: Exemplo da estrutura de um diretório LDAP

- Nó raiz (Root): Esse é o ponto de partida da árvore de diretório LDAP. É o nível mais alto da hierarquia e serve como base para toda a estrutura do diretório. Pode ser imaginado como a raiz de uma árvore, de onde se ramificam os demais nós. Pode ser representado por: *DN: dc=iftm,dc=edu,dc=br*.
- Organização (Organization): Representa uma entidade ou empresa dentro do diretório. Pode ser comparada a uma unidade dentro da própria organização ou à própria organização. Como por exemplo: "IFTM Campus Ituiutaba". É um nível abaixo do nó raiz. Pode ser representado por: *DN: o=iftmitba,dc=iftm,dc=edu,dc=br*.
- Unidades Organizacionais (Organizational Units): São subníveis dentro da organização. Elas ajudam a organizar os dados em grupos lógicos. Cada unidade organizacional pode corresponder a um departamento ou uma divisão específica dentro da unidade da organização. Por exemplo, "PET Computação IFTM Campus Ituiutaba", é uma unidade organizacional dentro da organização "IFTM Ituiutaba". Pode ser representado por: *DN: ou=petiftm,o=iftmitba,dc=iftm,dc=edu,dc=br*
- Pessoa (People): Também chamadas de "usuários", são as entidades individuais dentro do diretório. Representam pessoas ou contas associadas aos serviços da organização. Cada usuário possui um identificador exclusivo e informações adicionais, como nome, endereço de email, etc. Por exemplo, "Gabriel Barco" é um usuário dentro da unidade

organizacional "PET Computação IFTM Campus Ituiutaba". Pode ser representado por:
DN: uid=gabriel.barco,ou=petiftm,o=iftmitba,dc=iftm,dc=edu,dc=br

Vale ressaltar que caso a organização provedora do sistema não veja necessidade de separar a estrutura de sua organização em mais entidades, como foi mostrado, ou que a própria entidade seja a responsável pelo sistema, seguindo o exemplo acima, o nó "Organization" pode também ser representado por: *DN: o=iftm,dc=iftm,dc=com*.

O LDAP utiliza uma abordagem cliente-servidor, onde os clientes enviam solicitações ao servidor para buscar, adicionar, modificar ou remover informações no diretório. O protocolo é baseado em texto e utiliza o modelo de comunicação "pedido-resposta", no qual as solicitações são enviadas pelo cliente e então, o servidor retorna uma resposta contendo o resultado ou erro ao solicitante.

O protocolo LDAP é padronizado e assim como protocolos de rede, a estrutura de diretório e serviços providos por um servidor com ele estão todos disponíveis em RFCs (Requests for Comments). A versão mais atual é a v.3 (versão 3), um padrão desenvolvido em 1997 na RFC 2251. A especificação original foi atualizada em 2006, e RFCs de 4510 a 4519 fornecem especificações mais claras e coesivas para o LDAP (SILVA, 2021).

Outra característica importante deste protocolo, é o fato de ele não ser vinculado a um sistema operacional ou provedor de serviços específico. Permitindo que diferentes sistemas e aplicativos se comuniquem e acessem informações de diretório de maneira padronizada.

Essa natureza genérica do LDAP permite que ele seja utilizado em uma ampla variedade de casos de uso, desde autenticação e autorização de usuários até armazenamento de informações sobre recursos de rede, como endereços de email, números de telefone, informações de contato, entre outros (AMARAL, 2010).

Além disso, o LDAP é extensível, o que significa que novos atributos e esquemas de diretório podem ser definidos e adicionados de acordo com as necessidades específicas de uma organização. Isso oferece flexibilidade para adaptar o serviço de diretório às necessidades particulares de uma infraestrutura de TI.

Atualmente existem inúmeras soluções de diretório baseadas em LDAP disponíveis no mercado, dentre as mais populares entre elas, podemos citar: OpenLDAP, Microsoft Active Directory (AD), Novell eDirectory, Oracle Internet Directory e IBM Tivoli Directory Server. Cada uma delas possui recursos específicos e atende a diferentes necessidades de gerenciamento de diretório. A escolha da solução adequada dependerá dos requisitos e do ambiente de TI de cada

organização.

Na seção a seguir será explicado mais a fundo especificamente sobre o OpenLDAP, uma implementação de código aberto do LDAP que possui recursos e funcionalidades que o tornam mais eficiente e funcional para as mais diversas estruturas de rede (AUGUSTO, 2017).

2.2 OPENLDAP

O OpenLDAP é uma opção popular de solução de diretórios baseada em LDAP. Ele é especialmente desenvolvido para uso em plataformas Unix, mas também é distribuído para uso no Windows. Seu desenvolvimento ocorreu paralelamente ao desenvolvimento e padronização do protocolo LDAP. Atualmente, o OpenLDAP é mantido por uma comunidade de código livre, que conta com a participação de diversos desenvolvedores interessados em aprimorar o funcionamento do software (OLIVEIRA, 2010).

Dentre as principais características deste software podemos destacar (AMARAL, 2010):

- Suporte a IPv4 e IPv6
- Autenticação (Cryrus Sasl-Kerberos V, GSSAPI, Digest-MD5)
- Segurança no transporte – SSL e TLS
- Controle de acessos (ACLs)
- Escolha entre bancos de dados (GDBM ou DBD)
- Capacidade de atender a múltiplos bancos ao mesmo tempo
- Alto desempenho em múltiplas chamadas
- Replicação de base

Além disso, OpenLDAP oferece autenticação de usuários através de sua base de dados centralizada, o que facilita o controle e a correção de problemas em caso de erros nos logins dos usuários ou nas suas permissões (AUGUSTO, 2017).

O funcionamento dele envolve a comunicação entre um cliente LDAP e um servidor LDAP. O cliente emite solicitações para realizar operações de leitura, escrita, pesquisa e exclusão de dados no servidor. Essas solicitações são baseadas em comandos como, BIND (autenticação), ADD (adição de entrada), SEARCH (pesquisa), MODIFY (modificação) e DELETE (exclusão).

O pacote do OpenLDAP é composto por quatro componentes principais (SILVA, 2021):

- Servidores: Fornecem os serviços LDAP
- Clientes: Manipulam os dados LDAP
- Utilitários: Servidores LDAP de suporte
- Bibliotecas: Fornecem interfaces de programação para o LDAP

O funcionamento da comunicação desses componentes pode ser ilustrado conforme descrito na figura 3:

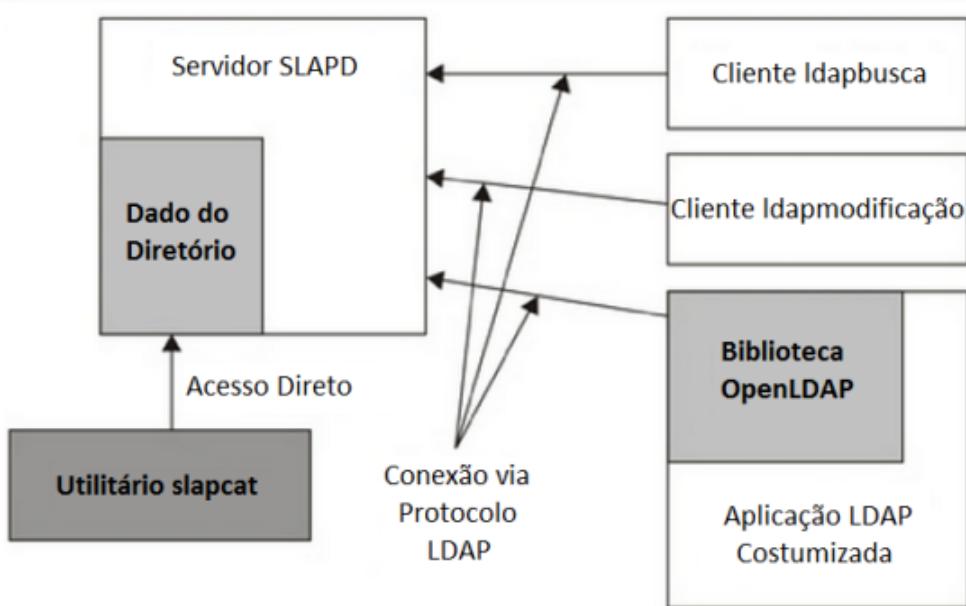


Figura 3: Exemplo da comunicação dos componentes do OpenLDAP (SILVA, 2021)

No OpenLDAP o servidor principal é chamado de SLAPD (Stand-Alone LDAP Daemon), que é responsável por receber solicitações LDAP dos clientes, processá-las e fornecer as respostas correspondentes. O SLAPD funciona como um serviço em segundo plano, executando continuamente e aguardando conexões de clientes LDAP. Quando uma solicitação é recebida, o SLAPD a analisa e a encaminha para o processamento adequado.

Este servidor tem como função armazenar dados no diretório local ou prover acesso a fontes de dados externas. Tipicamente, além de oferecer serviços de autenticação e busca de informações em diretórios, também oferece suporte nas operações de adição, exclusão e modificação de dados em diretórios. Não menos importante, esse servidor é o responsável por oferecer controle de acesso detalhado ao diretório (AMARAL, 2010).

Os clientes LDAP geralmente se conectam a um servidor SLAPD usando o protocolo LDAP por meio da rede, enviando solicitações para executar várias operações. Como esse protocolo

opera na pilha TCP/IP, o cliente normalmente inicia estabelecendo uma conexão com o servidor de diretório. Após estabelecer a conexão, o cliente se autentica e, em seguida, executa as operações desejadas, como pesquisas, adições, modificações, exclusões e outras.

Como ilustrado na Figura 3, ao contrário dos clientes, os utilitários não realizam operações usando o protocolo LDAP. Os dados são manipulados em camadas mais baixas e sem mediação pelo servidor, são usados na realidade para a manutenção do servidor (SILVA, 2021).

Por fim, as bibliotecas do OpenLDAP são componentes essenciais que fornecem funcionalidades para o desenvolvimento e a interação com o serviço de diretório. Elas são responsáveis por encapsular a complexidade do protocolo LDAP e fornecer uma interface de programação que facilita a criação de aplicativos que interagem com o servidor SLAPD.

Dentre as principais bibliotecas do OpenLDAP podemos destacar (AMARAL, 2010):

- JLDAP: biblioteca escrita em Java projetada para fornecer acesso a serviço de diretórios LDAP. Define duas interfaces síncronas e assíncronas para o LDAP de forma a atender uma ampla variedade de aplicações.
- JDBC LDAP: biblioteca escrita em Java que tem como função prover acesso a serviço de diretórios LDAP àqueles que preferem utilizar linguagem SQL19 e JDBC20.
- IdapC++: biblioteca escrita na linguagem C++ que tem como função prover acesso a serviços de diretórios LDAP a partir de programas escritos nessa linguagem.

No OpenLDAP existem também as listas de controles de acesso (ACLs), elas são mecanismos utilizados para controlar o acesso aos dados armazenados no diretório LDAP. Elas permitem definir políticas de segurança que determinam quais operações um determinado usuário ou grupo de usuários podem executar em relação aos registros e atributos do diretório.

As ACLs são configuradas por meio de regras definidas no arquivo de configuração do servidor SLAPD (slapd.conf ou slapd.d). Cada regra de ACL especifica uma combinação de filtros de entrada (entry) e atributos que devem ser correspondidos para que a regra seja aplicada.

Utilizando como exemplo a entrada uid=gabriel.barco, ou=petifm, o=iftmitba, dc=iftm, dc=edu, dc=br, ilustrada pela hierarquia da Figura 2, uma regra nas ACLs para controlar o acesso aos valores dessa entrada teria a seguinte sintaxe (OLIVEIRA, 2010):

```
access to dn.exact="uid=gabriel.barco,ou=petifm,o=iftmitba,dc=iftm,dc=edu,dc=br"
by dn.exact="uid=admin,ou=petifm,o=iftmitba,dc=iftm,dc=edu,dc=br" write
by self read
```

by * none

Essa configuração, portanto, fornece um controle de acesso granular para garantir que apenas o administrador e o próprio usuário tenham permissões específicas na entrada LDAP mencionada.

3 SERVIDOR

A conexão do OpenLDAP com outros servidores pode ser estabelecida para diversos propósitos, como autenticação centralizada, gerenciamento de usuários e controle de acesso. O OpenLDAP é uma solução de diretório LDAP genérica e flexível, o que permite sua integração com diferentes tipos de servidores.

No contexto específico deste projeto, o OpenLDAP será implementado em uma máquina virtual (VM) hospedada pelo Proxmox, que será configurada como um servidor LDAP dedicado.

Conectando-se a uma VM do Proxmox, como será explicado na seção a seguir, é possível integrar o processo de autenticação dos usuários. Isso permitirá que os mesmos utilizem suas credenciais do diretório LDAP para acessar o servidor.

3.1 PROXMOX

O Proxmox é uma plataforma de virtualização de servidores de código aberto baseada no kernel do Linux. Ele combina tecnologias de virtualização de contêineres (LXC), e máquinas virtuais (KVM), para fornecer uma solução completa de virtualização para data centers e ambientes empresariais.

Hoje, o Proxmox se destaca por proporcionar um ambiente intuitivo e objetivo tendo em mente a gestão de máquinas virtuais. Na prática, basta poucos cliques para acompanhar, personalizar e dar instruções aos dispositivos conectados (OLIVEIRA, 2022).

O Proxmox permite a criação, gerenciamento e monitoramento de máquinas virtuais e contêineres em um ambiente centralizado. Ele oferece recursos avançados, como alta disponibilidade, migração ao vivo, balanceamento de carga e armazenamento compartilhado, tornando-o adequado para ambientes de produção e missão crítica.

A arquitetura dele é baseada em um hipervisor que executa a virtualização, permitindo a alocação eficiente de recursos físicos, como CPU, memória e armazenamento, para as máquinas virtuais e contêineres. O Proxmox também fornece uma interface web intuitiva, conhecida

como Proxmox VE (Virtual Environment), que facilita a administração e o monitoramento das instâncias virtuais.

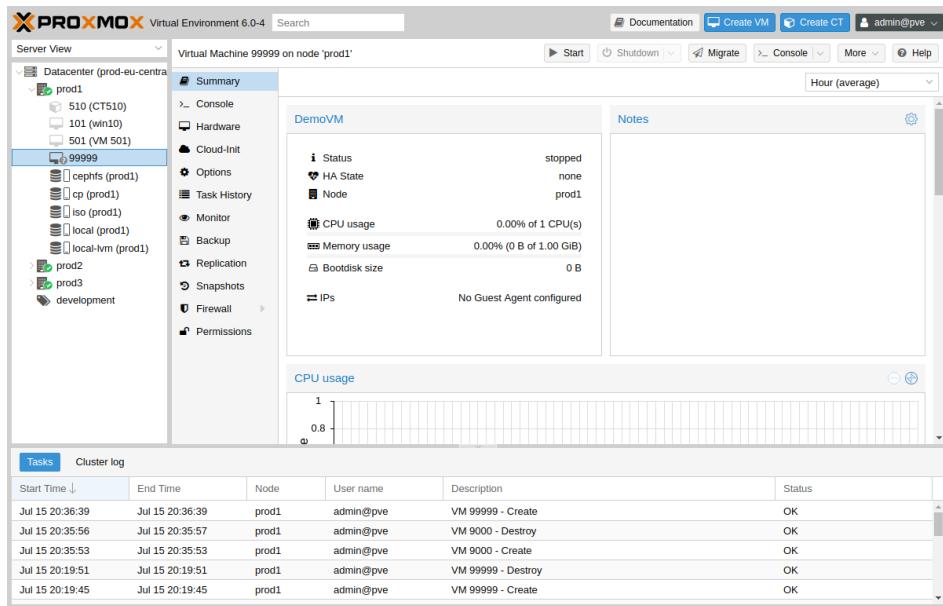


Figura 4: Exemplo da interface gráfica do Proxmox. Disponível em: <https://pve.proxmox.com/wiki/Graphical_User_Interface>

A plataforma Proxmox é escalável e flexível, permitindo que os administradores de sistema criem e gerenciem facilmente várias máquinas virtuais e contêineres em um único local. Além disso, o Proxmox suporta recursos avançados de rede, como VLANs e balanceamento de carga, para oferecer maior flexibilidade e desempenho.

A integração de uma VM hospedada pelo Proxmox com o OpenLDAP, oferece uma série de benefícios para o gerenciamento e a segurança do servidor. Alguns desses benefícios incluem:

- Centralização do gerenciamento de usuários: O OpenLDAP permite a criação de uma base de dados centralizada no servidor para o armazenamento de informações de autenticação de usuários.
- Autenticação única (Single Sign-On): Ao utilizar o OpenLDAP como um serviço de diretório, é possível implementar a autenticação única em todas as máquinas conectadas ao servidor.
- Aumento da segurança: O uso do OpenLDAP como serviço de diretório permite uma gestão mais eficaz das políticas de segurança do servidor.

4 MATERIAL E MÉTODOS

O desenvolvimento do projeto proposto, demandou a instalação e configuração de uma máquina virtual Debian, dentro de um servidor Proxmox. Para isso, foram seguidas as etapas recomendadas para garantir uma implementação adequada e funcional.

Para a instalação do Proxmox, foi realizado o uso de hardware compatível com seus requisitos mínimos (Proxmox Server Solutions GmbH, 2023). O hardware usado para sua implementação foi: um processador Intel Xeon E-2336 @ 2.90GHz, memória RAM de 16 GB e um disco rígido com 64 GB de espaço.

Após verificada a estabilidade da versão escolhida do Proxmox, foi realizado o procedimento de instalação padrão do Proxmox VE 7.4, que incluiu o download da imagem ISO, criação de uma mídia de instalação (DVD ou USB), inicialização do servidor a partir da mídia e execução do assistente de instalação. Foram fornecidas as informações necessárias, como configurações de rede adequadas, senhas de acesso e seleção do disco para uma instalação eficiente.

Com a instalação do servidor Proxmox bem sucedida, foi prosseguida a implementação da máquina virtual, que contém a versão 12.1.0 do Debian, instalada como CLI, possuindo 2GB de memória RAM e 32GB de armazenamento, como ilustrado na Figura 5 a seguir.

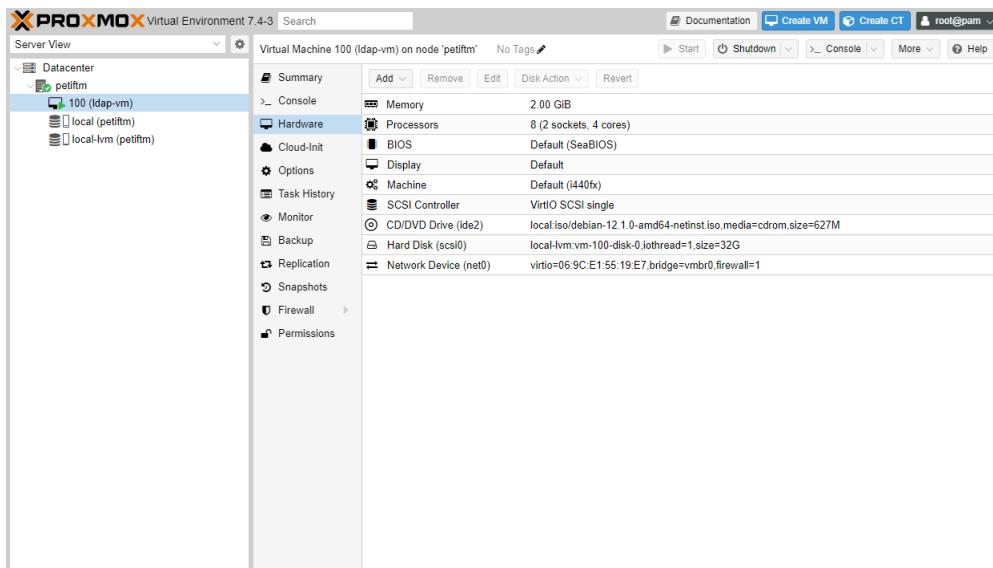


Figura 5: Configurações de hardware da máquina virtual Debian

Os requisitos de hardware da VM independem da instalação do OpenLDAP, pois ele é um serviço de diretório leve que pode ser executado em hardware modesto. No entanto, é importante notar que o desempenho do OpenLDAP pode ser afetado pelo hardware subjacente, portanto, quanto melhor for o desempenho esperado, maior deve ser a qualidade do hardware.

5 SERVIDOR OPENLDAP

Nesta seção, será descrito detalhadamente o processo de instalação dos pacotes e componentes necessários para configurar o ambiente virtual Debian, de forma que funcione como um servidor LDAP, que será usado para manter as informações nele inseridas.

Além disso serão demonstradas, as configurações necessárias para que o LAM (LDAP Account Manager), uma ferramenta de gerenciamento de contas LDAP, seja capaz de administrar as informações no diretório.

5.1 INSTALAÇÃO DOS PACOTES E COMPONENTES

Os pacotes e componentes que serão instalados são essenciais para o funcionamento do ambiente. A seguir, serão explicados cada um desses pacotes em detalhes, e seu papel na infraestrutura do projeto.

O primeiro passo é a instalação dos componentes, como descrito no código abaixo, que em conjunto formam a base para criar um ambiente web, que servirá de base para hospedar o LAM.

```
1 sudo apt install apache2 php php-cgi libapache2-mod-php php-mbstring php-common php-pear -y
```

Cada pacote instalado a partir desse comando, podem ser descritos abaixo como:

- apache2: O Apache é um servidor web que lida com solicitações de páginas da web e as envia aos navegadores dos clientes.
- php: PHP é uma linguagem de programação do lado do servidor que permite criar páginas web dinâmicas e interativas.
- php-cgi: O PHP-CGI é um interpretador que permite ao servidor web (como o Apache) processar scripts PHP.
- libapache2-mod-php: Este módulo do Apache integra o PHP ao servidor, permitindo a execução de scripts PHP.
- php-mbstring: A extensão mbstring ajuda a lidar com caracteres e texto multibyte em diferentes idiomas.
- php-common: O pacote php-common contém recursos e configurações compartilhadas necessárias para o PHP funcionar corretamente.

- **php-pear:** O PEAR é um sistema de gerenciamento de pacotes que fornece bibliotecas e extensões adicionais para expandir a funcionalidade do PHP.

Esses componentes trabalham em conjunto para criar um ambiente web flexível e poderoso. O Apache gerencia as solicitações e respostas HTTP, enquanto o PHP processa scripts e gera conteúdo dinâmico. As extensões e módulos adicionais, incluem funcionalidades extras para atender a diversas necessidades de desenvolvimento web.

Finalizado o processo de instalação do ambiente web, foi realizada a instalação dos pacotes essenciais relacionados ao LDAP.

```
1 sudo apt install slapd ldap-utils -y
```

Este comando desempenha um papel crucial na configuração do ambiente, instalando o servidor LDAP ("slapd") e um conjunto de ferramentas úteis para interagir com ele ("ldap-utils"). Como visto na figura 3 o SLAPD, é o principal Daemon responsável pelas funções do servidor.

A partir do comando abaixo é possível extrair dados de um servidor LDAP e exibi-los no formato LDIF (LDAP Data Interchange Format) no terminal. O LDIF é um formato de texto que representa as entradas e informações armazenadas em um diretório LDAP.

```
1 sudo slapcat
```

```
petiftm@debian-server:~$ sudo slapcat
dn: dc=iftm,dc=edu,dc=br
objectClass: top
objectClass: dcObject
objectClass: organization
o: iftm.edu.br
dc: iftm
structuralObjectClass: organization
entryUUID: 6d298ce4-d70b-103d-83e2-096fcc1c0d95
creatorsName: cn=admin,dc=iftm,dc=edu,dc=br
createTimestamp: 20230824204913Z
entryCSN: 20230824204913.0401482#000000#000#000000
modifiersName: cn=admin,dc=iftm,dc=edu,dc=br
modifyTimestamp: 20230824204913Z
```

Figura 6: Retorno do comando "sudo slapcat"

Após realizada a instalação do servidor LDAP, foi feita através do comando abaixo, a inserção do pacote do LAM no sistema, que como mencionado anteriormente, é uma ferramenta útil para administrar e simplificar o gerenciamento de contas por meio de uma interface web.

```
1 sudo apt install ldap-account-manager -y
```

Conforme instalado o pacote, o próximo passo foi a configuração do servidor Apache para trabalhar de forma adequada com o PHP-CGI, garantindo que os scripts PHP sejam processados

corretamente. Eles garantem que o servidor seja capaz de suportar corretamente o módulo do LAM.

```
1 sudo a2enconf php*-cgi  
2 sudo systemctl reload apache2  
3 sudo systemctl enable apache2
```

Os comandos acima também recarregam e garantem que o Apache seja inicializado automaticamente, sempre que o sistema for reiniciado, proporcionando alta disponibilidade à interface web do LAM. Além disso, a partir do comando abaixo, é possível verificar o status do serviço do servidor web Apache no sistema.

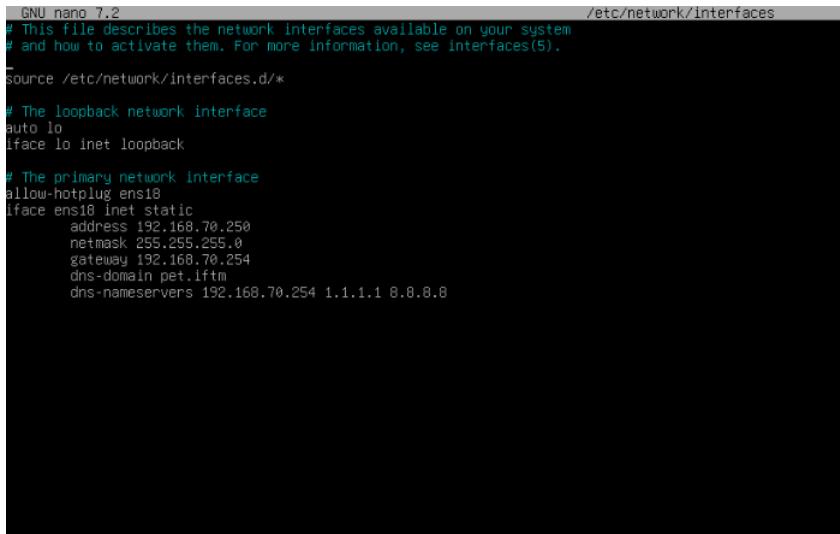
```
1 sudo systemctl status apache2
```

```
betifm@debian-server:~$ sudo systemctl status apache2  
● apache2.service - The Apache HTTP Server  
    Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)  
    Active: active (running) since Thu 2023-08-24 17:47:31 -03; 6min ago  
      Docs: https://httpd.apache.org/docs/2.4/  
        Main PID: 10743 (apache2)  
          Tasks: 6 (limit: 2305)  
            Memory: 29.4M  
              CPU: 199ms  
            CGroup: /system.slice/apache2.service  
                ├─10743 /usr/sbin/apache2 -k start  
                ├─13833 /usr/sbin/apache2 -k start  
                ├─13834 /usr/sbin/apache2 -k start  
                ├─13835 /usr/sbin/apache2 -k start  
                ├─13836 /usr/sbin/apache2 -k start  
                └─13837 /usr/sbin/apache2 -k start  
  
ago 24 17:47:31 debian-server systemd[1]: Starting apache2.service - The Apache HTTP Server...  
ago 24 17:47:31 debian-server systemd[1]: Started apache2.service - The Apache HTTP Server.  
ago 24 17:51:10 debian-server systemd[1]: Reloading apache2.service - The Apache HTTP Server...  
ago 24 17:51:10 debian-server systemd[1]: Reloaded apache2.service - The Apache HTTP Server.  
ago 24 17:52:43 debian-server systemd[1]: Reloading apache2.service - The Apache HTTP Server...  
ago 24 17:52:43 debian-server systemd[1]: Reloaded apache2.service - The Apache HTTP Server.
```

Figura 7: Retorno do comando "sudo systemctl status apache2"

Como configuração adicional, também foi atribuído à máquina virtual Debian um endereço IP estático, para que sempre seja possível acessar a interface web, pelo mesmo endereço em outras máquinas da mesma rede. Essa configuração pode ser feita a partir do comando para a modificação do arquivo abaixo.

```
1 nano /etc/network/interfaces
```



```

GNU nano 7.2                               /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
-
source /etc/network/interfaces.d/*
#
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens10
iface ens10 inet static
    address 192.168.70.250
    netmask 255.255.255.0
    gateway 192.168.70.254
    dns-domain pet.litm
    dns-nameservers 192.168.70.254 1.1.1.1 8.8.8.8

```

Figura 8: Arquivo "/etc/network/interfaces"

5.2 CONFIGURAÇÃO DO LDAP ACCOUNT MANAGER

Ao acessar a interface web do LAM, ilustrada na figura 9 abaixo, pelo endereço do servidor definido ("http://IP-Server/lam"), foram necessárias configuração dos perfis de servidor para o funcionamento do gerenciador, a partir da aba "LAM configuration".

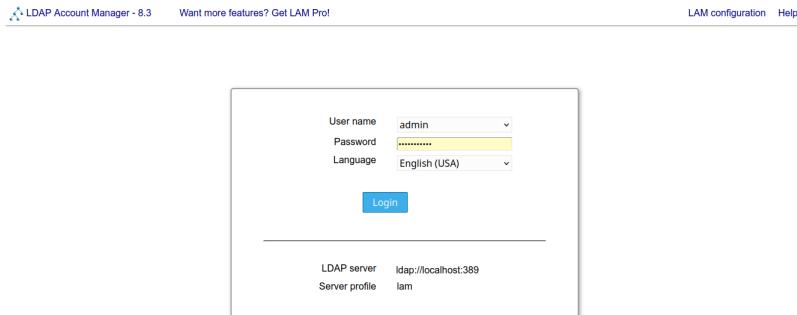


Figura 9: Tela inicial do LDAP Account Manager

As configurações realizadas na aba de "General Settings", incluem a alteração do "Tree Sufix" para o sufixo do domínio anteriormente estabelecido, a "List of Valid Users" para o sufixo da conta de admin criada, além da definição de uma nova senha para a conta padrão LAM utilizada.

Além dessas configurações, também foram alterados os sufixos dos tipos de conta existentes no servidor, para os sufixos correspondentes às configurações feitas. Alterações essas demons-

tradas abaixo nas figuras 10a e 10b.

(a) Configurações gerais do LAM

(b) Configurações de tipos de conta do LAM

Figura 10: Configuração dos perfis de servidor

Realizadas as configurações adequadas, o servidor ficou pronto para receber as informações de contas de usuários, ou grupos como ilustrado na figura 11. Após isso, foram criados os perfis de cada usuário a fim de validar seu devido funcionamento.

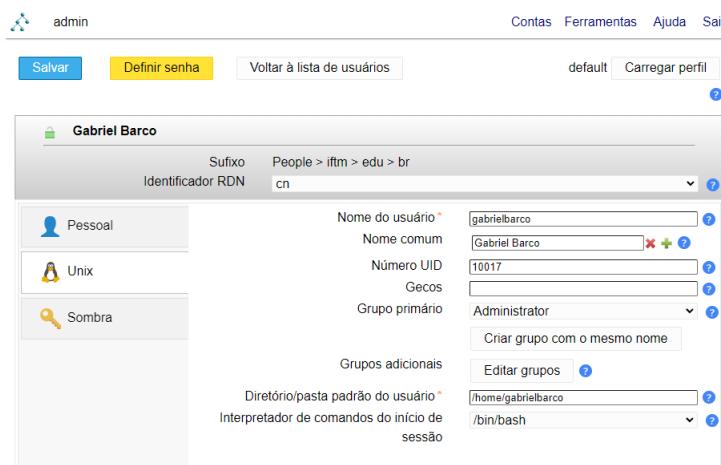


Figura 11: Tela de criação de usuário

Com a criação completa, os perfis também podem ser visualizados tanto na interface do LAM, quanto pela extração direta dos dados do servidor LDAP, com o uso do comando "slapcat", como demonstrado na figura 6.

6 CLIENTE OPENLDAP

Com o servidor finalizado, as contas e grupos de usuários já puderam ser criadas e armazenadas no diretório LDAP, com isso restou apenas as configurações adequadas em cada máquina,

para fazer com que estas fossem capazes de ler, tanto os usuários para fins de autenticação, quanto os grupos criados para definição de permissões.

Como as máquinas existentes no PET Computação IFTM Campus Ituiutaba, possuíam mais de um sistema operacional, foi necessário criar opções de configuração para sistemas Unix, e Windows.

Além disso é importante ressaltar, que como dito antes, o OpenLDAP foi criado para ser uma ferramenta exclusiva de ambientes Linux, por mais que ele possa ser adaptado para funcionar no Windows, ele ainda não é capaz de oferecer todas as suas funcionalidades a este sistema.

6.1 INSTALAÇÃO NO AMBIENTE UNIX

Para a configuração do cliente Unix, foi utilizado o Arch Linux, que é o sistema operacional utilizado nos computadores do PET. As configurações em sistemas Unix são muito semelhantes, porém em distribuições distintas pode ser que os passos utilizados podem ser diferentes dos aqui demonstrados.

6.1.1 INSTALAÇÃO E CONFIGURAÇÃO DO PACOTE OPENLDAP

Inicialmente foi necessário por meio do comando abaixo, instalar pacotes relacionados ao LDAP e facilitar a integração do sistema com servidores deste protocolo.

```
1 sudo pacman -S openldap libldap nss-pam-ldapd open-ldap-clients
```

Os propósitos de cada pacote mencionado no comando são:

- **openldap:** Este é o pacote principal que instala o servidor de diretórios OpenLDAP.
- **libldap:** Este pacote contém a biblioteca de cliente LDAP. Ele fornece APIs para aplicativos que desejam interagir com servidores LDAP.
- **nss-pam-ldapd:** Esse pacote fornece serviços de nomes e autenticação para integrar sistemas Linux com um servidor LDAP.
- **open-ldap-clients:** Este pacote instala utilitários de linha de comando para interagir com servidores LDAP, como o OpenLDAP.

Após os pacotes serem instalados, foi necessário configurar a forma como o cliente LDAP (no caso, o OpenLDAP) se conecta a um servidor LDAP. Isso pode ser feito por meio das alterações adequadas do arquivo seguinte.

```
1 /etc/openldap/ldap.conf
2 BASE          dc=example,dc=com
3 URI           ldap://localhost
```

Essas configurações são essenciais para definir o ponto base e o servidor LDAP ao qual o cliente se conectará. No entanto, essas configurações são específicas do ambiente e devem ser ajustadas para corresponder a configuração LDAP estabelecida.

6.1.2 CONFIGURAÇÕES DE AUTENTICAÇÃO LDAP

Na instalação dos pacotes, realizada na seção anterior, o pacote *nss-pam-ldapd* foi instalado para habilitar a integração com servidores LDAP.

Além disso, o arquivo */etc/nsswitch.conf*, que desempenha um papel central na configuração do NSS (Name Service Switch), um recurso do sistema que gerencia várias fontes de informações, foi editado. Este arquivo instrui o NSS sobre quais fontes de dados devem ser usadas para quais bancos de dados do sistema.

Foi necessário adicionar a diretiva 'ldap' aos bancos de dados apropriados. Portanto, o arquivo */etc/nsswitch.conf* foi configurado da seguinte maneira:

```
1 /etc/nsswitch.conf
2 passwd: files ldap
3 group: files ldap
4 shadow: files ldap
```

Essas configurações permitiram a integração bem-sucedida do sistema com fontes de dados LDAP, possibilitando ver os usuários cadastrados no servidor ao executar o comando **getent passwd** no cliente.

Na configuração do PAM (Pluggable Authentication Module), a primeira edição foi feita no arquivo */etc/pam.d/system-auth*. Este arquivo é incluído na maioria dos outros arquivos do diretório */etc/pam.d*, o que significa que as alterações feitas aqui se propagarão para várias partes do sistema. No entanto, é importante observar que atualizações no pacote PAM base podem afetar esse arquivo (ARCLINUX, 2023).

Foi adicionado o termo 'pam_ldap.so', marcado como 'sufficient' no topo de cada seção, exceto na sessão 'session', cuja alteração é opcional. As configurações realizadas definem as políticas de autenticação e controle de contas.

```

1   /etc/pam.d/system-auth
2
3   auth      sufficient pam_ldap.so
4
5   auth      required  pam_unix.so      try_first_pass nullok
6
7   auth      optional  pam_permit.so
8
9   auth      required  pam_env.so
10
11
12  account   sufficient pam_ldap.so
13
14  account   required  pam_unix.so
15
16  account   optional  pam_permit.so
17
18
19  password  sufficient pam_ldap.so
20
21  password  required  pam_unix.so      try_first_pass nullok sha512
22      shadow
23
24  password  optional  pam_permit.so
25
26
27  session   required  pam_limits.so
28
29  session   required  pam_unix.so
30
31  session   optional  pam_ldap.so
32
33  session   optional  pam_permit.so

```

Além disso, é importante mencionar a configuração do arquivo `/etc/pam.d/su`. Neste arquivo, o termo 'pam_ldap.so' é incluído como 'sufficient', permitindo que a autenticação do usuário seja verificada com sucesso no diretório LDAP. A adição de 'use_first_pass' na seção de autenticação do módulo 'pam_unix.so' indica que a senha deve ser passada para o módulo em vez de solicitar novamente ao usuário.

```

1   /etc/pam.d/su
2
3   auth      sufficient  pam_rootok.so
4
5   auth      sufficient pam_ldap.so
6
7   auth      required   pam_unix.so use_first_pass
8
9   account   sufficient pam_ldap.so
10
11  account   required   pam_unix.so
12
13  session   sufficient pam_ldap.so
14
15  session   required   pam_unix.so

```

Para permitir que os usuários editem suas senhas, o arquivo `/etc/pam.d/passwd` também foi configurado, com 'pam_ldap.so' incluído como 'sufficient'. Isso permite que as senhas sejam atualizadas no diretório LDAP quando os usuários as modificam.

```
1 /etc/pam.d/passwd
2 password      sufficient pam_ldap.so
3 password      required      pam_unix.so sha512 shadow nullok
```

Para fazer a criação de pastas pessoais ao login, foi adicionado o termo 'pam_mkhomedir.so' à seção 'session' do arquivo `/etc/pam.d/system-login`, colocado acima das diretivas 'sufficient'. Essa modificação é responsável por ativar a criação de pastas pessoais ao fazer login por meio de um tty, SSH, xdm, sddm, gdm, etc (ARCLINUX, 2023).

Além disso foi aplicada uma mudança semelhante ao arquivo do PAM, `/etc/pam.d/su-l`, para habilitar esse comportamento na sessão de 'su -login'.

```
1 /etc/pam.d/system-login
2 session optional pam_loginuid.so
3 session include system-auth
4 session optional pam_motd.so          motd=/etc/motd
5 session optional pam_mail.so         dir=/var/spool/mail
6           standard quiet
7 -session optional pam_systemd.so
8 session required  pam_env.so
9 session required  pam_mkhomedir.so skel=/etc/skel umask=0077
10
11 /etc/pam.d/su-l
12 session required pam_mkhomedir.so skel=/etc/skel umask=0077
13 session sufficient  pam_ldap.so
14 session required   pam_unix.so
```

Por fim, para permitir o uso do 'sudo', que concede privilégios administrativos temporários, por usuários do LDAP, foi modificada a configuração do PAM no arquivo `/etc/pam.d/sudo`, adicionando o termo 'pam_ldap.so' para indicar que a autenticação pelo LDAP é aceitável para os privilégios.

```
1 /etc/pam.d/sudo
```

```

2   auth      sufficient pam_ldap.so
3   auth      required      pam_unix.so  try_first_pass
4   auth      required      pam_nologin.so

```

Além da configuração do PAM, foi incluído no arquivo `/etc/openldap/ldap.conf`, o grupo existente no servidor LDAP, contendo os usuários destinados a possuírem privilégios, de acordo com as configurações recomendadas abaixo.

```

1   /etc/openldap/ldap.conf
2   sudoers_base ou=sudoers,dc=example,dc=org

```

6.2 INSTALAÇÃO NO AMBIENTE WINDOWS

Para a instalação do cliente no ambiente Windows, foi instalado o software 'pGina' na versão 3.1.8. O pGina é uma alternativa ao provedor de credenciais padrão do Windows, que é a parte do sistema responsável por gerenciar os logins. Usando plug-ins, o pGina possibilita a configuração de vários aspectos do processo de login, abrangendo desde a autenticação e autorização até o registro de eventos e a manipulação de terminais (PGINA, 2012b).

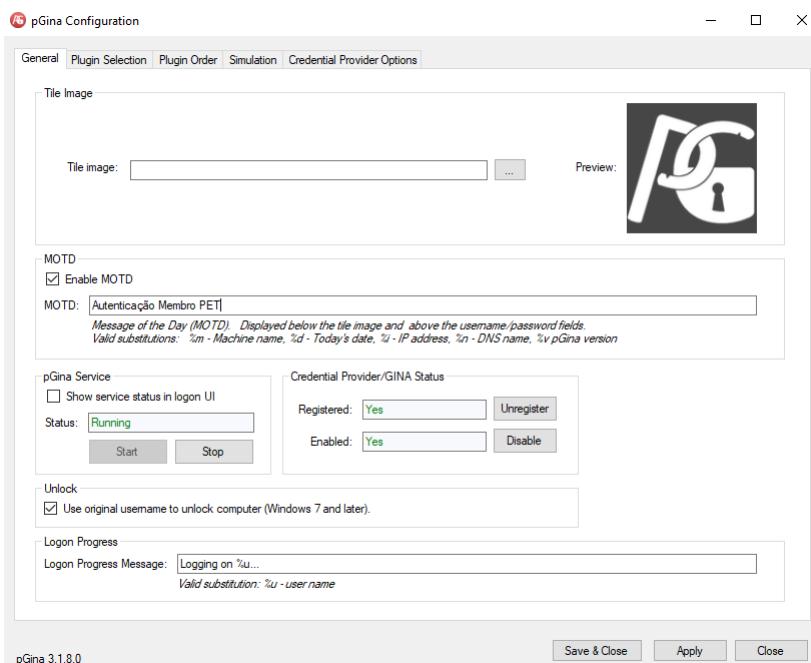


Figura 12: Software de configuração do pGina

O pGina administra o processo de login no Windows por meio da delegação de tarefas a um conjunto de plugins, que podem ser zero ou mais. Esses plugins têm a responsabilidade de

determinar se o usuário é realmente quem alega ser (autenticação), decidir se o usuário deve ter acesso (autorização) e executar outras ações relacionadas ao login.

Para a configuração, foram adicionadas as três etapas do plugin 'LDAP': a 'Autenticação', a 'Autorização' e o 'Gateway'. Também foi alterada a ordem de leitura dos plugins existentes, dando prioridade ao 'LDAP',

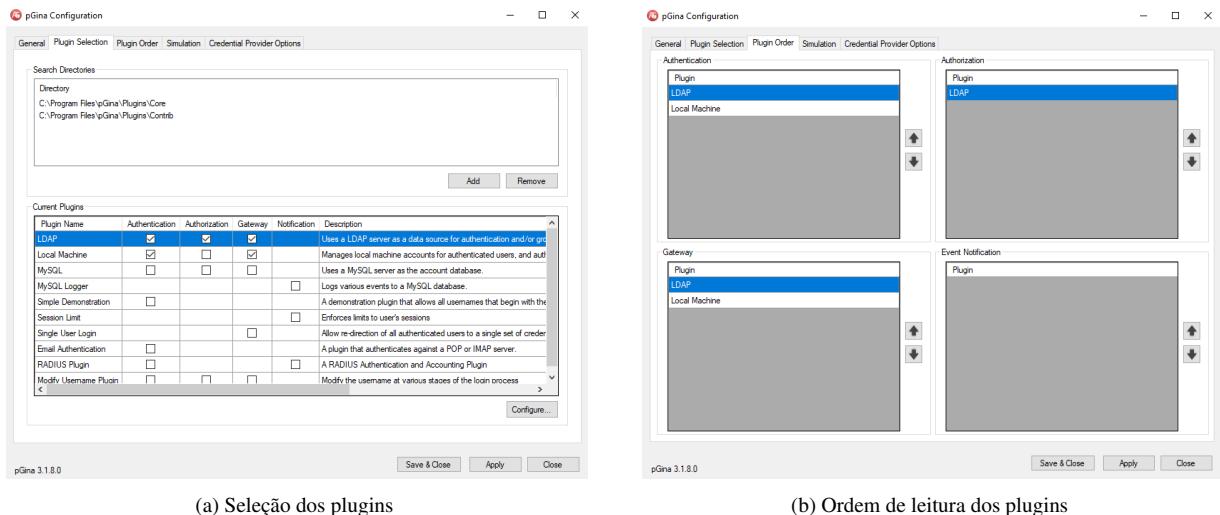


Figura 13: Configuração dos plugins do pGina

O plugin de autenticação LDAP fornece serviços de autenticação através de um servidor LDAP. Ele mapeia o nome de usuário para um Nome Distinto (DN) LDAP e tenta vincular-se ao servidor LDAP usando o DN. Se a ligação for bem-sucedida, ela fornecerá um resultado positivo ao serviço pGina (PGINA, 2012a).

Nas configurações do plugin, foram adicionados à seção do LDAP Server: o host, a porta, o DN 'admin', a senha, e o endereço para acessar os grupos, todos adequados ao servidor LDAP criado anteriormente, como será demonstrado na figura 14a.

Na seção de 'Autenticação', foi indicado ao plugin para procurar pela DN do usuário no momento da autenticação, procurando pelo 'uid' correspondente no servidor LDAP, caso exista.

Por fim na seção de 'Gateway', foi adicionada a regra que caso o usuário correspondente, seja pertencente do grupo 'Administrator', existente no servidor LDAP, ele será automaticamente movido ao grupo local 'Administradores' do Windows, que fornece ao usuário os privilégios de admin no sistema.

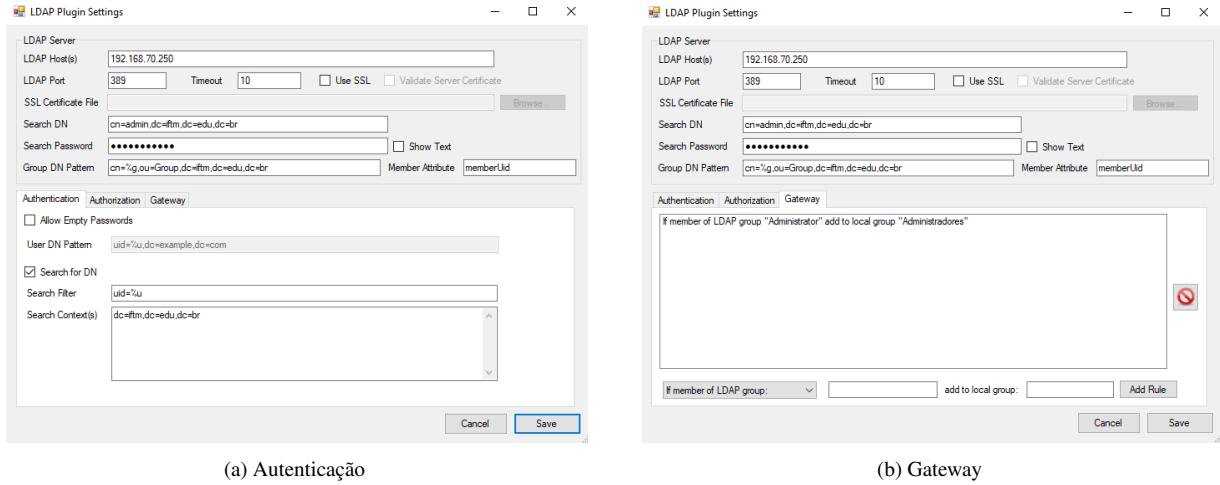


Figura 14: Configuração do plugin LDAP

7 RESULTADOS E DISCUSSÃO

Finalizadas as configurações, tanto no sistema Unix, como no Windows, foi realizada a reinicialização dos sistemas e, a partir disso, eles foram capazes de apresentar as opções de autenticação, de acordo com os usuários cadastrados anteriormente no servidor.



Figura 15: Telas de login dos sistemas

Ambos os sistemas foram capazes de autenticar os usuários, de acordo com as credenciais estabelecidas previamente, a medida que, qualquer alteração no servidor, é automaticamente percebida pelos clientes no momento da importação dos dados LDAP.

No momento em que o usuário se conecta em seu perfil pela primeira vez, o sistema acertadamente cria a pasta local respectiva à conta conectada, pasta essa, que apenas o próprio usuário logado e perfis administradores possuem acesso. Além disso o sistema verifica, de acordo com as regras preestabelecidas, o grupo em que o perfil está inserido, para definir suas permissões.

Como o OpenLDAP foi desenvolvido essencialmente para sistemas Unix, seu funciona-

mento no Windows se limita à autenticação via perfil fixo do pGina, diferentemente do Unix, onde todos os perfis cadastrados são exibidos ao usuário no momento do acesso.

Outra limitação existente no Windows, é a de que o sistema apenas realiza a importação do DN de cada usuário, portanto, os usuários são cadastrados no sistema com o nome correspondente ao seu 'username', além disso, essa restrição impossibilita a importação de outros recursos, que possam ser adicionados ao servidor.

7.1 TRABALHOS FUTUROS

Dadas as limitações do pGina, um próximo projeto interessante, seria o desenvolvimento de um sistema provedor de credenciais ainda mais completo para Windows, que seja capaz de importar todas as informações necessárias, tanto ao administrador da rede, quanto ao usuário conectado.

Outro possível trabalho, é a implementação do compartilhamento de recursos da mesma conta entre várias máquinas, esse método é viável graças ao método de autenticação centralizada adicionado aos sistemas clientes ao longo deste projeto.

8 CONCLUSÃO

Com base nos resultados obtidos anteriormente, pode-se afirmar que o OpenLDAP é uma solução viável e econômica para gerenciamento de usuários em redes de pequeno porte, capaz de oferecer recursos robustos para a gestão de grupos e permissões. Sua natureza de código aberto, não apenas reduz custos, mas também oferece uma comunidade ativa de desenvolvedores e usuários, proporcionando suporte contínuo e atualizações frequentes.

Além disso, a facilidade de instalação e configuração, conforme detalhado neste artigo, não apenas simplifica o processo para os administradores de rede, mas também reduz potenciais erros durante a implementação.

Assim, é possível concluir que o OpenLDAP não apenas atende, mas excede as expectativas para as finalidades adotadas neste projeto, consolidando-se como uma escolha sólida para organizações que buscam eficiência, economia e segurança em seus ambientes de rede.

REFERÊNCIAS

- AMARAL, B. da S. LDAP: Centralização e disponibilidade de informações. 2010. Disponível em: <http://professores.dcc.ufla.br/~terra/publications_files/students/2010_fumec_amaral.pdf>.
- ARCHLINUX. *LDAP authentication*. 2023. Disponível em: <https://wiki.archlinux.org/title/LDAP_authentication>. Acesso em: 30/10/2023.
- AUGUSTO, C. *OpenLDAP – O que é e para que serve?* 2017. Disponível em: <<http://ninandolinux.com.br/openldap-o-que-e-e-para-que-serve/>>. Acesso em: 30/05/2023.
- BERBELINI, G. Demonstrando Autenticação Centralizada com o OpenLDAP. *Faculdade de Tecnologia de Americana - Curso Superior de Tecnologia em Segurança da Informação*, 2017.
- BERTOLLI, E. *Entenda a diferença entre Active Directory e LDAP - Varonis*. 2016. <<https://www.varonis.com/pt-br/blog/entenda-a-diferenca-entre-active-directory-e-ldap>>. Acesso em: 24/05/2023.
- CRUZ, F. W. et al. Uma Ferramenta para a Administração de Serviços de Diretório Distribuídos Baseados no OpenLDAP. *Universidade Católica de Brasília - UCB*, 2023.
- MACHADO, E. S.; JUNIOR, F. d. S. M. Autenticação integrada baseada em serviço de diretório ldap. 2020. Disponível em: <<https://www.linux.ime.usp.br/~cef/mac499-06/monografias/erich/monografia.pdf>>.
- MICROSOFT. *Visão geral dos serviços de domínio Active Directory - Microsoft Learn*. 2023. Disponível em: <<https://learn.microsoft.com/pt-br/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>>. Acesso em: 09/05/2023.
- OLIVEIRA, L. M. de. Estudo sobre serviço de diretórios distribuídos para instituições acadêmicas. 2010. Disponível em: <<https://wiki.sj.ifsc.edu.br/images/6/64/Monografia-luiz-marcelo-2010-02.pdf>>.
- OLIVEIRA, P. Vantagens do proxmox: por que utilizar este software? 2022. Acesso em 30/05/2023. Disponível em: <<https://nova.escolalinux.com.br/blog/vantagens-do-proxmox-por-que-utilizar-este-software-1>>.
- PGINA. *Documentação do plug-in de autenticação LDAP*. 2012. Disponível em: <<http://pgina.org/docs/v3.0/ldap.html>>. Acesso em: 30/10/2023.
- PGINA. *Guia do usuário pGina*. 2012. Disponível em: <<http://pgina.org/docs/v3.0/user.html>>. Acesso em: 30/10/2023.
- Proxmox Server Solutions GmbH. *Proxmox VE - Requirements*. 2023. Disponível em: <<https://www.proxmox.com/en/proxmox-ve/requirements>>. Acesso em: 15/06/2023.
- SILVA, L. C. L. Um estudo sobre serviço de diretório e ferramentas de segurança da informação. 2021. Disponível em: <<https://repositorio.uniceub.br/jspui/bitstream/235/8153/1/51203326.pdf>>.