IMPLEMENTAÇÃO DE SISTEMA DE AUTENTICAÇÃO CENTRALIZADA COM LDAP PARA INTEGRAÇÃO DE SERVIÇOS DE REDE E GERENCIAMENTO DE PROCESSOS
UMA ABORDAGEM PARA OTIMIZAÇÃO DO CONTROLE DE ACESSO E SEGURANÇA EM AMBIENTES CORPORATIVOS, INTEGRANDO PROXY, OWNCLOUD E KANBOARD COM LDAP

SEGUNDO-SARGENTO – LUÍS EDUARDO RECZKOWSKI
SEGUNDO-SARGENTO – ELIEZER LIMA DA SILVA
TERCEIRO-SARGENTO – LUAN MACEDO DE OLIVEIRA
TERCEIRO-SARGENTO – BEATRIZ GERMANO RODRIGUES

RESUMO

A autenticação centralizada é fundamental para a gestão eficiente de usuários e a aplicação consistente de políticas de segurança em ambientes com múltiplos serviços de rede. Em infraestruturas de Tecnologia da Informação compostas por sistemas interdependentes, a criação manual de contas para cada serviço gera sobrecarga administrativa e dificulta o controle padronizado de acessos. Este artigo aborda essa limitação por meio da implementação de uma infraestrutura unificada de autenticação baseada no protocolo Lightweight Directory Access Protocol (LDAP). O objetivo foi implantar um diretório centralizado para autenticação em diversos serviços, eliminando redundâncias e aumentando a eficiência operacional e a segurança. As questões centrais envolveram a onfiguração do LDAP como ponto único de autenticação e a adoção de mecanismos que garantissem a integridade e a confidencialidade das redenciais trafegadas. A metodologia compreendeu a instalação e configuração de um servidor OpenLDAP om estrutura hierárquica, a habilitação de omunicação segura via StartTLS e a integração progressiva de serviços como Squid (proxy), Kanboard (gestão de processos) e OwnCloud (compartilhamento de arquivos), todos autenticando diretamente na base LDAP. Também foi implementado um firewall com nftables, visando proteger a infraestrutura e restringir acessos não autorizados. Os resultados demonstraram que a autenticação centralizada simplifica a administração de usuários, unifica o controle de acesso e amplia a rastreabilidade das ações. A solução adotada mostrou-se eficaz, segura e escalável, representando um modelo replicável para consolidar autenticação em ambientes heterogêneos, com impacto direto na redução do esforço administrativo e na elevação da segurança da rede.

Palavras-chave: *LDAP, Autenticação Centralizada, StartTLS, Proxy.*

1 INTRODUÇÃO

O LDAP foi concebido para fornecer um diretório digital, funcionando como uma agenda online estruturada hierarquicamente, semelhante a um sistema de arquivos. Ele permite organizar dados em forma de árvore e oferece recursos avançados, como buscas com filtros complexos, representação de entidades por meio de atributos e controle restrito de acesso. Essas funcionalidades tornam o LDAP uma solução robusta para serviços de diretório.

1.1 DESAFIOS EM AMBIENTES DE TI DISTRIBUÍDOS

A gestão de identidades e permissões em ambientes de Tecnologia da Informação

vem se tornando cada vez mais complexa, pois múltiplos sistemas críticos demandam autenticações independentes. Criar e manter contas manuais em cada aplicação gera retrabalho e potencializa inconsistências nas regras de acesso

Nesse contexto, o Lightweight Directory Access Protocol (LDAP) destaca-se como ferramenta capaz de organizar dados de usuários em estrutura hierárquica e servir de diretório único para autenticação. Ao concentrar credenciais em um único repositório, o LDAP simplifica a administração e suporta a integração de diferentes serviços, garantindo maior confiabilidade nos processos de acesso.

1.2 VANTAGENS DA ADOÇÃO DO LDAP EM AMBIENTES CORPORATIVOS

A ausência de autenticação centralizada expõe as organizações a riscos de segurança—como acessos não autorizados, duplicidade de contas e controle fragmentado—além de sobrecarregar a equipe de TI com tarefas de provisionamento e desprovisionamento de usuários. A implementação de uma solução baseada em OpenLDAP não apenas mitiga essas vulnerabilidades, mas também viabiliza a aplicação uniforme de políticas de segurança, facilita conformidade com normas e reduz custos operacionais.

Esta pesquisa oferece um modelo escalável capaz de consolidar o controle de acesso a serviços como Squid, OwnCloud e Kanboard.

1.3 DEFINIÇÃO DO PROBLEMA: IMPACTOS DA AUTENTICAÇÃO CENTRALIZADA

Gerenciar identidades e acessos em ambientes com múltiplos sistemas representa um desafio recorrente em infraestruturas de TI. O uso de credenciais distintas por serviço dificulta o controle de acessos, eleva os custos operacionais e pode comprometer a segurança.

Diante disso, esta pesquisa propõe analisar como a adoção do OpenLDAP como núcleo de autenticação centralizada pode aprimorar a segurança e otimizar a gestão de acessos, além de identificar os impactos dessa implementação em uma infraestrutura integrada.

1.4 OBJETIVOS DA PESQUISA

O objetivo geral é desenvolver e implantar um sistema de autenticação centralizada em LDAP para unificar o controle de acesso e o gerenciamento de usuários em serviços de rede (Proxy, servidor de arquivos e gestão de processos), reforçando a eficiência operacional e a segurança. Para isso, estabelecem-se os seguintes objetivos específicos:

a) Configurar e validar OpenLDAP: instalar e estruturar usuários/grupos, habilitar StartTLS e ACLs, e ativar logs/auditoria.

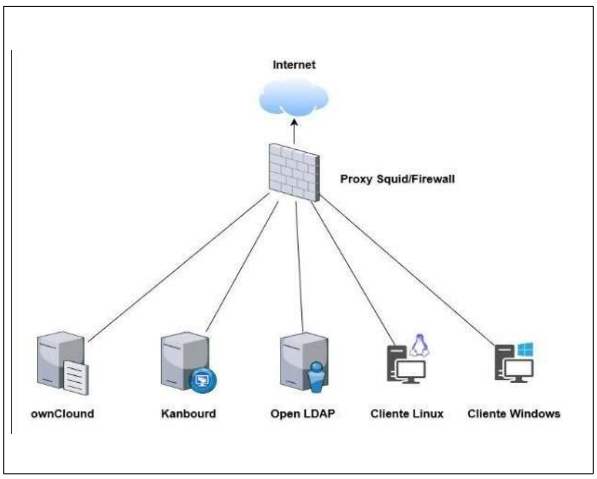
b) Integrar o Squid ao LDAP: implementar autenticação, definir ACLs por grupos e gerar relatórios de acesso.

c) Integrar o OwnCloud: configurar autenticação única, quotas e permissões via LDAP e avaliar eficácia pelos logs.

d) Integrar o Kanboard: habilitar login único, definir fluxos e permissões baseados em LDAP e monitorar logs de atividade.

e) Segurança e avaliação: aplicar firewall com nftables para serviços LDAP e integrados; mensurar impacto na eficiência e segurança antes e depois; documentar redução de retrabalho, consistência de políticas e fortalecimento da auditoria.

FIGURA 1: Infraestrutura



Fonte: os autores

1.5 VISÃO GERAL: METODOLOGIA, RESULTADOS E PERSPECTIVAS

A estrutura deste trabalho está organizada da seguinte forma: inicialmente, são apresentados os fundamentos teóricos sobre LDAP e autenticação centralizada.

Em seguida, descreve-se a metodologia adotada para a implementação da solução. Na sequência, são analisados os resultados obtidos, com foco na eficiência e segurança dos acessos.

Por fim, são expostas as conclusões e sugestões para futuras aplicações.

2 DESENVOLVIMENTO

A crescente complexidade na gestão de identidades e acessos em ambientes corporativos tem impulsionado a adoção de soluções de autenticação centralizada. O protocolo Lightweight Directory Access Protocol (LDAP) destaca-se como ferramenta eficaz para consolidar informações de usuários e grupos, proporcionando autenticação unificada em diversos serviços de rede.

SARI; HIDAYAT (2006) demonstraram a eficácia do LDAP na centralização de autenticação em um sistema de informações de recursos humanos, evidenciando ganhos em segurança e simplificação administrativa. Em ambiente educacional, WU; HUANG; YU (2014) desenvolveram um sistema de autenticação unificada baseado em LDAP para campus digital, eliminando múltiplos logins e fortalecendo a estrutura de diretório, o que reforça a adoção de diretórios hierárquicos em instituições que demandam gestão de usuários distribuída.

Embora os benefícios do LDAP sejam amplamente reconhecidos, OBIMBO; FERRIMAN (2011) salientam que a configuração adequada é fundamental para evitar falhas e assegurar desempenho estável. Seguindo essa linha, CHEN; PUNCHHI; TRIPUNITARA (2022) discutem a usabilidade das Listas de Controle de Acesso (ACLs) no OpenLDAP, demonstrando que um planejamento criterioso da estrutura de esquemas e políticas reduz a ocorrência de erros de autorização e amplia a escalabilidade da solução.

Identifica-se, entretanto, lacuna na literatura no que tange à integração simultânea de múltiplos serviços — proxy, servidor de arquivos e sistema de gestão de processos — em um único diretório LDAP. Este estudo propõe preencher esse espaço, adotando práticas consolidadas de configuração segura de OpenLDAP, conforme orientações de OBIMBO; FERRIMAN (2011) e CHEN; PUNCHHI; TRIPUNITARA (2022), de modo a garantir alta disponibilidade, aderência a políticas de segurança e facilidade de manutenção.

2.1 DIAGNÓSTICO INICIAL E ORGANIZAÇÃO DO AMBIENTE VIRTUALIZADO

O projeto teve início com a observação da infraestrutura existente na Seção de Informática da Escola de Comunicações, destacando a ausência de um sistema de autenticação centralizada para os serviços em uso.

Com base nessa constatação, identificou-se a necessidade de um ambiente

de testes que refletisse a futura solução de produção. Por essa razão, adotou-se o Proxmox VE, plataforma de código aberto que combina virtualização completa (KVM) e containers (LXC), permitindo criar um laboratório representativo da arquitetura final.

Essa escolha viabilizou a simulação das integrações desejadas e fundamenta a expansão do modelo para atender, de forma replicável, as infraestruturas de outras organizações militares do Exército Brasileiro.

Estrutura Proposta:

a) Servidor LDAP Primário (OpenLDAP): Armazena e gerencia as credenciais, grupos e políticas de autenticação de forma centralizada. Sua configuração contempla criptografia (StartTLS), ACLs refinadas e logging para auditoria.

b) Servidor LDAP de replicação (OpenLDAP): Replica periodicamente a base do LDAP Master, mantendo-se sincronizado por meio de replicação automática. Atua como servidor de contigência para autenticação em caso de falha do servidor principal.

c) Servidor Proxy (Squid): Realiza o controle de acesso à internet com autenticação via LDAP, aplicando regras restritivas de firewall para forçar o uso do proxy e gerar relatórios com o SARG.

d) Servidor de Arquivos (OwnCloud): Integra-se ao LDAP para autenticação e gerenciamento centralizado de cotas e permissões de usuários, promovendo segurança e organização no armazenamento de dados.

e) Servidor de Gestão de Tarefas (Kanboard): Permite login unificado via LDAP, viabilizando o controle de acessos e a colaboração por meio da metodologia Kanban.

f) Cliente Debian 12: Utiliza o SSSD para autenticação persistente no LDAP, permitindo login offline, aplicação de políticas e cache seguro de credenciais.

g) Cliente Windows 10: Integra-se ao LDAP com pGina, possibilitando autenticação unificada e compatível com ambientes mistos.

A infraestrutura implementada proporciona:

a) Centralização da autenticação: facilita o gerenciamento de usuários e grupos, garantindo consistência e segurança.

b) Alta disponibilidade: com redundância e failover automático, assegura continuidade dos serviços mesmo em caso de falha do servidor principal.

c) Eficiência operacional: a administração centralizada por meio do Proxmox simplifica o gerenciamento e manutenção do ambiente.

d) Segurança reforçada: implementação de proxy autenticado, firewall e políticas de acesso unificadas protegem contra acessos não autorizados

e) Escalabilidade: estrutura modular permite replicação para outras unidades do Exército Brasileiro, facilitando a expansão conforme ecessário

2.2.1 INSTALAÇÃO E CONFIGURAÇÃO DO OPENLDAP

FIGURA 2: Software OpenLDAP

Fonte: https://www.linkedin.com/pulse/openldap-comprehensive-overview-louis-byun-dyqqc

Foi instalado o OpenLDAP 2.5.13 em uma VM (Virtual Machine) com Debian 12, visando centralizar a autenticação na rede 10.0.0.0/24. A instalação, realizada via apt, incluiu os pacotes slapd e ldap-utils. No debconf, definiram-se o domínio lab.escom, o

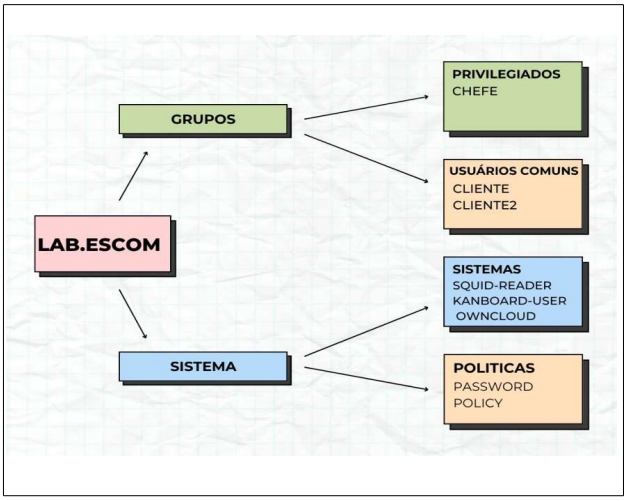
Base DN dc=lab,dc=escom, o administrador cn=admin e o backend MDB (PATIL, 2020; HERTZOG, 2018)

O DIT (Directory Information Tree) foi estruturado de forma modular, com unidades organizacionais para usuários, grupos, perfis privilegiados e serviços, viabilizando controle granular de permissões. As entradas foram gerenciadas principalmente pelo LDAP Account Manager (LAM). A política de senhas, aplicada via ldapadd, utilizou o schema ppolicy, com criptografia do tipo SSHA.

Para compatibilidade com sistemas Unix/Linux, foram carregados os schemas posixAccount, inetOrgPerson e shadowAccount via autenticação EXTERNAL. Inseriram-se contas de serviço, usuários comuns e perfis administrativos. A consistência do DIT foi validada com ldapsearch.

Consolidada a estrutura, o LAM passou a ser a interface padrão de gerenciamento, garantindo uma solução segura, modular e de fácil administração para o controle de identidades.

FIGURA 3: Ilustração da Base de Dados



Fonte: os autores

2.2.2 IMPLEMENTAÇÃO DO SERVIDOR LDAP DE REPLICAÇÃO

Após a configuração do servidor OpenLDAP primário, adotou-se o modelo "servidor principal e secundário" (mestre e seguidor), centralizando em um único ponto todas as alterações na base e evitando inconsistências entre múltiplas fontes.

No servidor principal, ativou-se o módulo e a sobreposição syncprov via arquivo LDIF (Lightweight Directory Interchange Format), permitindo que o servidor secundário receba cópias periódicas atualizadas da base dc=lab,dc=escom Reaproveitou-se a conta de serviço squid-reader, com permissões apenas de leitura, assegurando integridade dos dados sem permitir gravações diretas no nó seguidor.

No servidor secundário, instalaram-se os pacotes slapd e ldap-utils em uma máquina com Debian 12. Configurou-se a diretiva syncrepl para conexão ao principal em ldap://10.0.0.4, com StartTLS, empregando o mesmo certificado (ldap.crt) do servidor principal. O StartTLS, como mecanismo de segurança, permite que a conexão seja iniciada em texto claro e posteriormente convertida para TLS, sendo exigido no LDAP que nenhuma consulta ocorra antes do estabelecimento do canal seguro (MONTEIRO, 2021).

Importou-se o módulo ppolicy, essencial à replicação: qualquer divergência de módulos entre os servidores causa falhas. Após reiniciar o serviço, validou-se com ldapsearch -ZZ que as entradas do servidor seguidor eram idênticas às do principal, comprovando o espelhamento.

Assim, o modelo mestre-seguidor adotado garante que apenas o servidor principal realize gravações, enquanto o secundário atua como ponto de consulta de contingência, minimizando inconsistências, mantendo alta disponibilidade e facilitando a manutenção da infraestrutura de autenticação.

2.2.3 INTEGRAÇÃO COM O SERVIDOR PROXY (SQUID)

FIGURA 4: Software Proxy Squid

Fonte: https://www.squid-cache.org/Artwork/Sticker.png

Após a implantação do OpenLDAP, o Squid foi configurado como proxy autenticado usando basic_ldap_auth -Z para conexão segura e alta disponibilidade com dois servidores LDAP (10.0.0.4 e 10.0.0.5). A conta de serviço squid-reader busca usuários em ou=grupos,dc=lab,dc=escom via filtro uid=%s.

Para permissões, ext_ldap_group_acl valida grupos diretamente. ACLs ligam usuários aos grupos “privilegiados” e “usuarios”: o primeiro tem navegação irrestrita; o segundo sofre bloqueios por domínios e palavras-chave a partir de arquivos de blacklist. A ordem dessas ACLs torna o arquivo modular, de modo que basta ajustar a posição de cada regra (ou incluir novos arquivos de blacklist) para alterar as permissões aplicadas a cada grupo

A configuração inclui SSL Bump para interceptar e inspecionar tráfego HTTPS, usando certificados dinâmicos gerados por sslcrtd. Regras para o método CONNECT e portas seguras (por exemplo, 443) restringem acessos não autorizados, ampliando a visibilidade sobre o conteúdo e fortalecendo a segurança da rede.

Ajustes de cache e logs aumentaram desempenho e rastreabilidade, enquanto o acesso livre a repositórios APT simplificou atualizações. O resultado é um ambiente seguro, centralizado, com inspeção de tráfego HTTPS, gestão administrativa otimizada e maior proteção da infraestrutura de rede.

2.2.4 INTEGRAÇÃO COM O SERVIDOR DE ARQUIVOS (OWNCLOUD)

FIGURA 5: Software ownCloud

Fonte: https://www.sim-networks.com/en/kb/owncloud-installatio

Após implantar o OpenLDAP, instalou-se o **ownCloud 10.15.2-1+12.2_all.deb** em Debian 12. Como o ownCloud exige **PHP 7.4**, opção não oferecida pelos repositórios oficiais do Debian 12, recorreu-se ao repositório **deb.sury.org** de Ondřej Surý, amplamente reconhecido na comunidade Debian manter diversos arquivos de pacotes pessoais (Personal Package Archives ou PPAs) Instalaram-se também o **Apache 2.4** e o **MariaDB 10.3**.

No MariaDB, criou-se o banco de dados ‘owncloud’ e o usuário ‘owncloud user’ com privilégios restritos, fortalecendo a segurança. O pacote do ownCloud foi extraído em /var/www/html/owncloud, e o diretório de dados foi posicionado em /var/oc_data/ (fora da raiz web), com permissões adequadas e proprietário www-data, seguindo práticas de endurecimento recomendadas.

Configurou-se um **VirtualHost SSL** para forçar criptografia em todas as conexões HTTP, atendendo às diretrizes de segurança do ownCloud.

Em seguida, habilitou-se o aplicativo de integração LDAP no ownCloud e definiram-se:

- **Servidor primário**: 10.0.0.4:389 (StartTLS ativado);
- **Servidor de replicação / contingência**: 10.0.0.5:389;
  Foram informados o DN de leitura e o filtro ((objectclass=inetOrgPerson)

(objectclass=posixAccount)) para importar usuários e grupos. O teste “Testar Base DN” confirmou a conectividade.

A partir dessa configuração, todo o controle de autenticação e as permissões de acesso a arquivos e pastas no OwnCloud passaram a ser gerenciados pelo OpenLDAP, assegurando um ambiente unificado, resiliente e seguro.

2.2.5 INTEGRAÇÃO COM O SISTEMA DE GESTÃO DE PROJETOS (KANBOARD)

FIGURA 6: Software Kanboard

Fonte: https://en.wikipedia.org/wiki/Kanboard

O Kanboard foi instalado em um servidor Debian 12 com Apache, PostgreSQL e PHP configurados com os módulos necessários. A instalação ocorreu via wget, com extração do pacote e alocação em /var/www/html/kanboard, e ajustes de permissões para garantir seu funcionamento.

O VirtualHost do Apache foi configurado para conexões criptografadas, atendendo aos requisitos de segurança. A base de dados foi criada no PostgreSQL com usuário exclusivo e permissões restritas, conforme boas práticas.

A autenticação foi integrada ao OpenLDAP, utilizando grupos e usuários organizados em unidades específicas, o que permitiu o uso imediato do sistema sem necessidade de gerenciar credenciais localmente.

No entanto, o Kanboard não suporta múltiplos servidores LDAP nativamente — limitação contornada com uma solução abordada em seção específica.

O sistema de logs foi configurado para registrar eventos essenciais, mantendo o desempenho e a segurança do ambiente de produção.

2.2.6 AUTENTICAÇÃO CENTRALIZADA, SEGURA E COM PERSISTÊNCIA EM CLIENTES LINUX

FIGURA 7: Sistema Operacional Debian 12

Fonte: https://www.notebookcheck.info/O-Debian-12-5-traz-uma-serie-de-atualizacoes-de-seguranca-e-correcoes-de-bugs-para-a-popular-distribuicao-Linux.803446.0.html

Implementou-se no cliente Debian 12 uma configuração de autenticação centralizada por meio do daemon SSSD (System Security Services Daemon), que autentica por meio do servidor OpenLDAP utilizando o protocolo StartTLS para comunicação segura. O SSSD permitiu o uso de cache persistente de credenciais, assegurando a continuidade do acesso dos usuários mesmo em casos de indisponibilidade temporária do servidor LDAP.

A configuração integrou-se diretamente à estrutura LDAP existente, contemplando usuários e grupos previamente definidos, o que agilizou significativamente a implantação do sistema e facilitou o gerenciamento unificado de identidades. A autenticação passou a contar com suporte a criação automática dos diretórios home dos usuários, garantindo ambiente operacional consistente sem necessidade de intervenções manuais.

Adotou-se a utilização do certificado TLS para criptografia da comunicação, reforçando a segurança do canal entre cliente e servidor.

Essa abordagem centralizada e segura otimiza a administração de autenticações no ambiente Debian, reduzindo a complexidade operacional e aumentando a robustez da infraestrutura de TI. A persistência do cache e o uso de StartTLS contribuem para maior disponibilidade e confiabilidade dos serviços, fundamentais em ambientes corporativos críticos.

2.2.7 AUTENTICAÇÃO CENTRALIZADA, SEGURA E COM PERSISTÊNCIA EM CLIENTES WINDOWS

FIGURA 8: Sistema Operacional Windows 10

Fonte: https://tecnoblog.net/noticias/windows-10-for-workstations/

Para estender a autenticação centralizada a sistemas operacionais mistos, foi adotado o pGina nos clientes Windows 10. Essa ferramenta de código aberto substitui o mecanismo nativo do Windows, permitindo autenticação via servidores LDAP, entre outros backends.

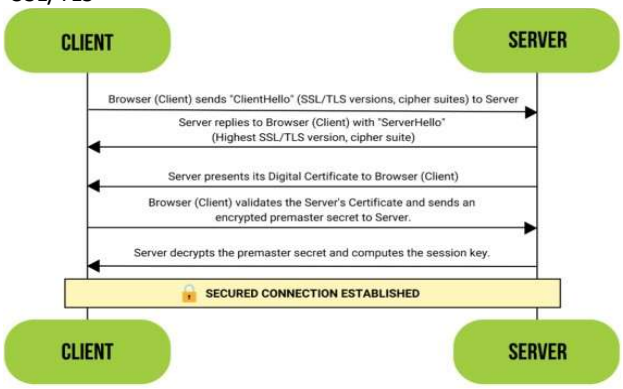
Configurado com o protocolo StartTLS, o pGina assegura comunicação segura entre os clientes Windows e o servidor OpenLDAP. Também permite a criação automática do perfil local após autenticação bem-sucedida, padronizando o gerenciamento de usuários e mantendo o acesso mesmo se o servidor LDAP estiver indisponível.

A implementação promoveu integração homogênea entre Linux e Windows, mantendo a centralização da autenticação, além de simplificar a administração e ampliar a segurança e a escalabilidade da infraestrutura.

2.3 CONSIDERAÇÕES SOBRE SEGURANÇA

Durante o desenvolvimento da infraestrutura, adotaram-se práticas estratégicas focadas na segurança da informação, visando proteger dados sensíveis e garantir integridade e disponibilidade dos serviços. A comunicação entre serviços críticos, como o diretório LDAP, ocorre exclusivamente por canais cifrados via STARTTLS, que, por operar sobre a porta padrão do LDAP, oferece maior flexibilidade e compatibilidade em ambientes complexos, em comparação ao LDAPS tradicional.

FIGURA 9: Diagrama de uma conexão encriptada por SSL/TLS



Fonte: https://www.ssl.com/article/ssl-tls-handshake-ensuring-secure-online-interactions/

Políticas restritivas no OpenLDAP limitam o acesso à base de dados a usuários técnicos autorizados, enquanto certificados digitais válidos asseguram a autenticidade das conexões. O controle de acesso é reforçado pelo firewall nftables, cuja política padrão bloqueia todo tráfego, liberando apenas conexões internas essenciais (proxy HTTP/HTTPS, LDAP e SSH).

O sistema foi endurecido por parâmetros kernel aplicados via sysctl,

incluindo a desabilitação de redirecionamentos ICMP e source routing (net.ipv4.conf.all.accept_redirects=0 e net.ipv4.conf.all.accept_source_route=0), ativação de filtragem anti-spoofing (net.ipv4.conf.all.rp_filter=1), registro de pacotes suspeitos (net.ipv4.conf.all.log_martians=1), proteção contra ataques DDoS (net.ipv4.icmp_echo_ignore_broadcasts=1) e uso de cookies TCP SYN (net.ipv4.tcp_syncookies=1). Essas medidas elevam a robustez da rede contra exploração e negação de serviço.

Permissões rigorosas garantem operação de serviços com privilégios mínimos: chaves privadas acessíveis somente ao usuário root (exemplo: arquivo de chave privada do OpenLDAP com permissão 600) e diretórios de aplicação sob propriedade restrita (como /etc/squid com proprietário proxy:proxy), atendendo ao princípio do menor privilégio.

Foi implementada rotina automatizada de backup da base LDAP, com armazenamento seguro, verificação de integridade e versionamento. Monitoramento e auditoria contínuos via syslog garantem rastreabilidade e rápida resposta a incidentes

Por fim, a utilização do PHP 7.4 no OwnCloud, embora potencialmente vulnerável por estar fora do suporte oficial, tem seu risco mitigado pela restrição de acesso à rede interna controlada pelo firewall, garantindo a segurança

Assim, a infraestrutura desenvolvida assegura uma solução robusta, baseada em boas práticas consolidadas de segurança em redes Linux, com múltiplas camadas de defesa e gestão eficaz dos riscos.

2.4 DESAFIOS ENFRENTADOS

Durante a implantação da infraestrutura, optou-se pelas versões mais recentes e estáveis dos sistemas operacionais e serviços, visando garantir segurança, suporte e compatibilidade. Inicialmente, considerou-se o uso do Wekan para gerenciamento de processos. No entanto, sua dependência do MongoDB impôs desafios significativos.

2.4.1 INVIABILIDADE DO MONGODB NO DEBIAN 12

O MongoDB foi removido dos repositórios oficiais do Debian após adotar a Server Side Public License (SSPL), considerada não livre pelas Diretrizes de Software Livre do Debian (DFSG) e não reconhecida pela Ope Source Initiative. Além disso, as versões recentes do MongoDB requerem bibliotecas obsoletas, como a libssl1.1, ausente no Debia 12. Embora seja possível contornar essa limitação, isso exigiria manutenção manual e introduziria riscos de segurança por operar fora do ciclo oficial de atualizações

Considerou-se ainda o uso de repositórios do Debian 11 para obter o MongoDB e suas dependências. Contudo, essa prática — conhecida como *FrankenDebian* — é desaconselhada pela comunidade, pois pode causar conflitos de dependências, instabilidade e dificuldades de manutenção (DEBIAN, 2025).

2.4.2 ADOÇÃO DO KANBOARD COMO ALTERNATIVA VIÁVEL

Diante dessas limitações, optou-se por substituir o Wekan pelo Kanboard, ferramenta open-source baseada no modelo Kanban, compatível com o Debian 12 e que utiliza o PostgreSQL como banco de dados — solução robusta, amplamente suportada e alinhada às melhores práticas de produção. Além disso, o Kanboard permite integração com autenticação centralizada via LDAP, atendendo

ao objetivo de unificação do controle de acesso.

2.4.3 IMPLEMENTAÇÃO DE REDUNDÂNCIA NO LDAP PARA O KANBOARD

Embora o Kanboard não ofereça suporte nativo a failover LDAP, foi desenvolvido um script em shell (kanboard_ldap_monitor.sh) para monitorar dois servidores LDAP distintos e ajustar dinamicamente o arquivo de configuração conforme a disponibilidade dos serviços. Essa abordagem se mostrou eficaz em ambientes de teste e produção, assegurando a operação contínua do Kanboard mesmo diante de falhas temporárias no servidor LDAP primário. Além disso, evita reinicializações do servidor Apache, minimizando impactos no desempenho e na disponibilidade da aplicação. A lógica simples do script facilita a manutenção e pode ser adaptada a outros sistemas com estrutura de autenticação semelhante.

2.4.4 SUBSTITUIÇÃO DO SAMBA 4 POR OWNCLOUD PARA COMPARTILHAMENTO DE ARQUIVOS

Inicialmente, planejou-se utilizar o Samba 4 integrado ao OpenLDAP para o compartilhamento de arquivos. No entanto, essa abordagem foi revista devido à obsolescência dessa integração nas versões recentes do Samba.á que o uso do OpenLDAP como backend é classificado como funcionalidade legada, com suporte descontinuado e incompatibilidades com padrões modernos de replicação e autenticação (UBUNTU, 2025).

Atualmente, o Samba utiliza seu servidor LDAP interno baseado no modelo Active Directory, o que torna a configuração com OpenLDAP mais complexa e pouco recomendada. A equipe Samba descontinuou o suporte ao OpenLDAP como backend para o Samba AD DC devido à complexidade técnica envolvida, especialmente na adaptação dos componentes necessários para replicação, controle de acesso e esquema, que não são compatíveis com servidores LDAP tradicionais. Assim, o uso do OpenLDAP nessa função é considerado legado e com suporte descontinuado (SAMBA, 2025).

Diante dessas limitações, optou-se pelo OwnCloud como solução de compartilhamento de arquivos. Essa plataforma de código aberto permite hospedar serviços de armazenamento com controle total dos dados, oferecendo recursos como criptografia de ponta a ponta, autenticação em dois fatores e políticas de conformidade. Também conta com controle detalhado de permissões, auditoria e compatibilidade com LDAP, facilitando a gestão de usuários e atendendo aos requisitos de segurança da infraestrutura.

2.4.5 CORREÇÃO NA FERRAMENTA DE MONITORAMENTO DE LOGS DO PROXYSQUID (LIGHTSQUID)

Durante a implementação do LightSquid para análise dos logs do proxy Squid, foi detectado um problema causado pela fixação do ano no script lightparser.pl, o que impossibilitava o processamento correto dos dados para anos posteriores. Para resolver essa limitação, aplicou-se uma correção no ano do script. Essa alteração corrigiu os erros relacionados à data, garantindo o funcionamento adequado do sistema e a precisão dos relatórios gerados (FINISKY, 2021).

FIGURA 10: Relatório gerado pelo Lightsquid

Fonte: os autores

2.5 MÉTODOS DE PESQUISA

A metodologia adotada neste projeto é de natureza **exploratória-aplicada**, com um enfoque predominantemente **qualitativo**, alinhada ao objetivo de investigar possibilidades práticas de integração entre serviços de rede em um ambiente simulado, inspirado na infraestrutura da Seção de Informática da Escola de Comunicações. A abordagem exploratória permitiu investigar tecnologias já existentes e seu potencial de adaptação e uso conjunto, enquanto o caráter aplicado direcionou o trabalho para a construção de uma solução funcional e testável, capaz de ser replicada ou adaptada a contextos similares.

A proposta consistiu em **desenvolver, configurar e validar** um ambiente de rede virtualizado, utilizando a plataforma **Proxmox VE**, que permitiu a criação e gerenciamento eficiente de múltiplas máquinas virtuais Dentro desse ambiente, foram implantados servidores baseados no sistema operacional **Debian**, sobre os quais foram instalados e integrados os principais serviços de rede: autenticação centralizada via **OpenLDAP**, controle de acesso à internet com o **Squid (Proxy)**, compartilhamento e sincronização de arquivos com o **OwnCloud**, e gerenciamento de tarefas por meio do **Kanboard**, uma aplicação leve baseada no método Kanba

A estrutura lógica e funcional do sistema foi cuidadosamente desenhada para simular com fidelidade o ambiente real da Seção de Informática. Um conjunto de máquinas clientes foi configurado para representar usuários finais, com perfis distintos e permissões específicas, que acessariam os serviços de forma integrada. O comportamento do sistema foi analisado por meio da coleta de **dados empíricos**, extraídos de **arquivos de log**, **testes de autenticação** e **monitoramento de desempenho**, permitindo avaliar a eficiência da integração, a estabilidade dos serviços e o comportamento dos usuários em diferentes cenários de uso.

Para a implementação e posterior avaliação do ambiente proposto, foram utilizadas as seguintes **ferramentas e tecnologias**:

a) Proxmox VE: plataforma de virtualização de código aberto que permitiu a criação de um ambiente isolado, seguro e modular, facilitando a gestão de recursos e a simulação de um cenário realista;

b) OpenLDAP: utilizado como serviço central de diretório, responsável por armazenar e gerenciar as credenciais e informações dos usuários, permitindo a autenticação unificada em todos os serviços conectados;

c) Squid Proxy: configurado para atuar no controle, filtragem e monitoramento do tráfego de internet, com regras definidas a partir dos grupos e permissões cadastrados no LDAP.

d) OwnCloud: ferramenta de nuvem privada adotada para possibilitar o armazenamento, compartilhamento e sincronização de arquivos, com base em perfis de acesso definidos no diretório central.

e) Kanboard: aplicação para organização de tarefas baseada em Kanban, integrada ao sistema para permitir a criação de fluxos de trabalho colaborativos e a visualização de atividades por grupo ou usuário.

f) Shell Script: utilizado para automatizar rotinas administrativas, como criação de usuários, sincronização de permissões, backup de dados e reinicialização de serviços, aumentando a eficiência operacional.

g) Comandos específicos: ferramentas como ldapsearch, getent, wbinfo, pdbedit e net foram empregadas para realizar testes de conectividade, verificação de autenticação,

consulta a diretórios e diagnóstico de integração entre os serviços.

2.6 APRESENTAÇÃO E ANÁLISE DE DADOS

A apresentação dos dados foi realizada com base em uma série de testes práticos de autenticação entre os diversos serviços integrados no ambiente de rede. O principal objetivo desses testes foi verificar, de forma empírica, se a comunicação entre os sistemas estava ocorrendo de maneira eficaz, confiável e, principalmente, segura. Para isso, foram simulados cenários de uso real, contemplando diferentes perfis de usuários e permissões, a fim de validar o comportamento do sistema em condições semelhantes às do dia a dia

A seguir, estão descritos os principais resultados observados durante os testes:

a) Proxy Squid: A integração com o serviço de diretório via LDAP mostrou-se eficaz no controle de acesso à internet. A autenticação permitiu aplicar políticas de navegação conforme os grupos definidos no diretório, garantindo que cada usuário acessasse a rede conforme seu perfil, ampliando o controle da TI sobre o tráfego.

b) Servidor OwnCloud: Os testes mostraram que usuários LDAP conseguiram logar e acessar pastas conforme suas permissões, comprovando o funcionamento correto da integração. A autenticação centralizada garantiu consistência nas permissões e facilitou uma administração mais segura e eficiente do ambiente.

c) Kanboard: O login único (SSO) via LDAP funcionou conforme esperado, permitindo o acesso sem criação de múltiplas credenciais. Isso facilitou o uso e reduziu riscos de segurança ligados a senhas fracas ou repetidas.

Além das validações funcionais, analisaram-se logs de autenticação, gráficos de tempo de resposta e registros de erro, oferecendo uma visão geral do desempenho. Os indicadores apontaram melhora significativa na organização do ambiente de TI, incluindo: redução de contas duplicadas, eliminando inconsistências e facilitando o gerenciamento de identidades; maior controle de acesso, com auditorias mais precisas e políticas de segurança mais eficazes; e, reforço na segurança interna, com autenticação centralizada e controle de acesso padronizado.

Em resumo, os testes confirmaram que a integração com autenticação centralizada via LDAP trouxe ganhos significativos em segurança, gestão e eficiência, consolidando uma infraestrutura mais robusta e alinhada às boas práticas de TI.

2.7 DISCUSSÃO DOS RESULTADOS

A implementação do sistema de autenticação centralizada mostrou-se eficiente e escalável, atendendo às demandas de ambientes com múltiplos serviços integrados. Os testes confirmaram sua capacidade de lidar de forma segura e coesa com diferentes tipos de autenticação, unificando a gestão de credenciais.

A integração entre os diversos serviços foi bem-sucedida, a equipe de implantação, precisou realizar ajustes manuais e refinar as políticas de controle de acesso para garantir a consistência e a conformidade entre os sistemas.

A principal contribuição deste estudo está na aplicação prática de um ambiente unificado de autenticação em um contexto militar, ainda pouco explorado em termos de modernização de TI com foco em integração e segurança. Ao comprovar a viabilidade técnica e os benefícios desse modelo em uma instituição de ensino técnico-militar, o projeto se torna uma referência para futuras iniciativas. A metodologia adotada, desde o planejamento até a validação com testes funcionais e análise de desempenho, pode ser

replicada em outras unidades com desafios similares.

O estudo também identificou limitações, como a curva de aprendizado no uso do OpenLDAP por equipes menos experientes e a carência de documentação técnica completa, essencial para garantir a continuidade do sistema em caso de mudanças na equipe.

Em resumo, o projeto mostrou ser possível implementar um ambiente de autenticação centralizada robusto, eficiente e seguro em instituições com exigências específicas, contribuindo para o avanço da gestão de identidade e acesso.

3 CONCLUSÃO

A implantação de um sistema centralizado de autenticação e controle baseado em LDAP (Lightweight Directory Access Protocol) promove melhorias significativas na eficiência operacional e na segurança em ambientes corporativos e educacionais. A integração do LDAP com serviços essenciais, como proxy, compartilhamento de arquivos e sistemas de gerenciamento de processos, potencializa o controle, a escalabilidade e a gestão unificada de acessos.

Por meio da centralização das credenciais em uma base única, o LDAP simplifica o gerenciamento das permissões, elimina a necessidade de múltiplas autenticações e reduz a carga administrativa da equipe de TI.

A definição granular de permissões para usuários e grupos, conforme suas funções, fortalece a segurança do acesso a diretórios e recursos compartilhados, garantindo conformidade com políticas internas de proteção da informação. Além disso, a arquitetura LDAP se destaca pela escalabilidade, atendendo desde pequenas redes até grandes infraestruturas, reduzindo a complexidade da manutenção.

Dessa forma, a adoção desse modelo configura uma estratégia eficaz para organizações que buscam otimizar a administração, aprimorar a segurança da informação e consolidar um ambiente tecnológico robusto e coeso.

3.1 RESULTADOS

O estudo demonstrou que a adoção de uma infraestrutura baseada em LDAP, aliada à integração com soluções como proxy, compartilhamento de arquivos e gestão de tarefas, resulta em avanços significativos na administração de redes corporativas e institucionais. A estrutura proposta, composta por servidores especializados e clientes Linux e Windows integrados, evidenciou os seguintes ganhos operacionais e de segurança:

a) Centralização robusta da autenticação e autorização, com armazenamento unificado de contas, grupos e políticas de acesso, possibilitando maior controle sobre permissões e eliminação da redundância de credenciais;

b) Controle refinado de acesso à internet, por meio da integração do Squid com o LDAP, com aplicação de políticas de navegação personalizadas, autenticação obrigatória e monitoramento por meio do Lightsquid;

c) Organização e segurança no compartilhamento de arquivos, com controle de cotas e permissões vinculado à hierarquia de usuários e grupos do LDAP, conforme implementado no OwnCloud;

d) Rastreabilidade e controle nos processos corporativos, com autenticação centralizada em ferramentas como o Kanboard, o que permite associar atividades diretamente aos usuários e facilitar auditorias;

e) Alta disponibilidade e escalabilidade da autenticação, asseguradas por meio da replicação automática do servidor LDAP primário para o secundário, garantindo

contingência e continuidade dos serviços mesmo diante de falhas;

f) Segurança aprimorada, com uso de StartTLS, regras de firewall restritivas, autenticação obrigatória.

Em síntese, a integração de serviços a uma base LDAP unificada demonstrou ser uma abordagem técnica viável, segura e escalável, com elevado potencial de padronização e automação, com possibilidade de reprodução em Organizações Militares do Exército Brasileiro

3.2 IMPLICAÇÕES PRÁTICAS E TEÓRICAS

Os resultados mostram que usar o LDAP como base para controle de acesso centralizado é viável e alinhado com os princípios de segurança e eficiência. A integração com serviços como proxy, compartilhamento de arquivos e gestão de tarefas comprovou a simplificação do gerenciamento de usuários e permissões, reduzindo credenciais redundantes e o esforço da equipe técnica.

Do ponto de vista teórico, o estudo se apoia em conceitos já consolidados, como sistemas distribuídos, autenticação unificada e administração centralizada de identidade. Esses fundamentos podem ser úteis em pesquisas sobre automação de redes, controle de privilégios e conformidade com políticas internas de segurança.

Embora a proposta apresentada dependa de ajustes conforme o ambiente, ela pode servir como referência inicial para projetos em instituições que buscam mais controle e organização no acesso a serviços de rede. Também pode ser aproveitada em contextos educacionais e em iniciativas de capacitação técnica voltadas à gestão de infraestrutura de TI.

3.3 LIMITAÇÕES E CONSIDERAÇÕES

Algumas limitações inerentes ao escopo e ao ambiente de testes adotado neste estudo merecem atenção ao avaliar a validade e a aplicabilidade dos resultados. A prova de conceito foi implementada em um laboratório virtualizado com um número restrito de usuários e dados controlados, o que impede a reprodução completa da complexidade e da escala de uma rede corporativa de grande porte, como as que se encontram no contexto do Exército Brasileiro

Além disso, não foram coletadas métricas de desempenho de forma detalhada, pois o hardware disponível para o laboratório não suportava confortavelmente as máquinas virtuais necessárias para o estudo, quanto mais testes de estresse que exigiriam maior capacidade de processamento e memória. Por essa razão, a avaliação sobre escalabilidade, latência de autenticação e consumo de recursos permaneceu qualitativa e dependerá de medições objetivas em ambientes com infraestrutura mais robusta

Outro ponto relevante refere-se às variáveis ligadas à operação e à manutenção contínua do sistema. Fatores como rotatividade de pessoal, prazos de atualização da documentação e procedimentos internos não foram examinados em profundidade durante a pesquisa. Embora tenham sido adotadas boas práticas de estruturação e auditoria, o impacto de mudanças organizacionais no suporte diário e na administração do diretório LDAP só poderá ser plenamente compreendido em um cenário institucional real, com equipes operando de forma contínua.

Essas limitações não invalidam os resultados apresentados, mas indicam a necessidade de expandir o estudo para ambientes reais, com maior número de usuários, coleta sistemática de métricas de desempenho e acompanhamento efetivo das rotinas de manutenção. Investigações posteriores em infraestrutura mais capaz contribuirão para verificar a robustez da proposta e ajustar eventuais lacunas

observadas em contextos de maior complexidade.

3.4 RECOMENDAÇÕES E DIREÇÕES FUTURAS

Com base nos resultados obtidos, recomenda-se que, antes da adoção do LDAP, sejam identificados os serviços a serem integrados, bem como definidas as políticas de grupos e permissões conforme as necessidades da organização. A compatibilidade entre os sistemas existentes e a estrutura proposta deve ser validada previamente. A capacitação técnica da equipe responsável — especialmente quanto à administração do diretório, protocolos de autenticação e integração com serviços como proxy, compartilhamento de arquivos e sistemas garantir a segurança e a eficiência do processo.

É recomendável manter a documentação atualizada da estrutura do diretório, regras de acesso e fluxos de autenticação, além disso, o uso de um ambiente de testes (sandbox) ajuda a identificar incompatibilidades e reduzir riscos na migração para produção.

Como direções futuras, sugere-se investigar a viabilidade técnica de adaptar o LDAP para que este possa se alimentar automaticamente de bases corporativas já existentes no Exército Brasileiro, como o **SiCaPEx — Sistema de Cadastramento do Pessoal do Exército**. Tal integração permitiria automatizar a criação e o gerenciamento de contas e permissões com base nos dados atualizados de pessoal, reduzindo o retrabalho administrativo e aumentando a coerência entre os sistemas.

Outra linha de pesquisa relevante é a integração do LDAP com sistemas amplamente utilizados no ambiente militar, como o **SPED — Sistema de Protocolo Eletrônico de Documentos**, avaliando sua aplicação como repositório unificado de autenticação para sistemas contábeis e fiscais sob gestão militar. Também se recomenda estudar a aplicação conjunta do LDAP com soluções de autenticação federada (como SAML e OpenID Connect), bem como com infraestruturas híbridas ou em nuvem (por exemplo, Azure AD e AWS Directory Service).

Por fim, o desenvolvimento ou adoção de ferramentas que automatizem tarefas administrativas — como a criação de usuários, atribuição de grupos e geração de relatórios — pode contribuir para tornar a gestão mais eficiente e reduzir falhas operacionais Estudos comparativos com outras soluções de diretórios (como FreeIPA, Active Directory e OpenDJ) em contextos similares podem fornecer subsídios para decisões mais bem fundamentadas sobre adoção e manutenção de sistemas de controle de acesso. de gerenciamento de tarefas — é um passo essencial para garantir a segurança e a eficiência do processo

É recomendável implementar medidas como criptografia de dados em trânsito (por exemplo, com StartTLS), registro de logs para auditoria, e documentação atualizada da estrutura do diretório, regras de acesso e fluxos de autenticação. A utilização de um ambiente de testes (sandbox) pode ajudar a identificar incompatibilidades e reduzir riscos na migração para produção.

Como direções futuras, sugere-se investigar a viabilidade técnica de adaptar o LDAP para que este possa se alimentar automaticamente de bases corporativas já existentes no Exército Brasileiro, como o **SiCaPEx — Sistema de Cadastramento do Pessoal do Exército**. Tal integração permitiria automatizar a criação e o gerenciamento de contas e permissões com base nos dados atualizados de pessoal, reduzindo o retrabalho administrativo e aumentando a coerência entre os sistemas.

Outra linha de pesquisa relevante é a integração do LDAP com sistemas amplamente utilizados no ambiente militar, como o **SPED — Sistema de Protocolo Eletrônico de Documentos**, avaliando sua

aplicação como repositório unificado de autenticação para sistemas contábeis e fiscais sob gestão militar. Também se recomenda estudar a aplicação conjunta do LDAP com soluções de autenticação federada (como SAML e OpenID Connect), bem como com infraestruturas híbridas ou em nuvem (por exemplo, Azure AD e AWS Directory Service).

Por fim, o desenvolvimento ou adoção de ferramentas que automatizem tarefas administrativas — como a criação de usuários, atribuição de grupos e geração de relatórios — pode contribuir para tornar a gestão mais eficiente e reduzir falhas operacionais Estudos comparativos com outras soluções de diretórios (como FreeIPA, Active Directory e OpenDJ) em contextos similares podem fornecer subsídios para decisões mais bem fundamentadas sobre adoção e manutenção de sistemas de controle de acesso

ABSTRACT

Centralized authentication is essential for efficient user management and consistent enforcement of security policies in environments with multiple network services. In IT infrastructures composed of interdependent systems, manually creating accounts for each service leads to administrative overhead and hinders standardized access control. This article addresses this limitation through the implementation of a unified authentication infrastructure based on the Lightweight Directory Access Protocol (LDAP). The objective was to deploy a centralized directory for authentication across various services, eliminating redundancies and enhancing operational efficiency and security. The core issues involved configuring LDAP as a single point of authentication and adopting mechanisms to ensure the integrity and confidentiality of transmitted credentials. he methodology included the installation and onfiguration of an OpenLDAP server with a hierarchical structure, the enabling of secure ommunication via StartTLS, and the progressive integration of services such as Squid (proxy), Kanboard (process management), and OwnCloud (file sharing), all authenticating directly against the LDAP directory. A firewall was also implemented using nftables to protect the infrastructure and restrict unauthorized access. The results showed that centralized authentication simplifies user administration, unifies access control, and enhances the traceability of actions. The adopted solution proved to be effective, secure, and scalable, representing a replicable model for consolidating authentication in heterogeneous environments, with a direct impact on reducing administrative effort and increasing network security.

Keywords: LDAP, Centralized Authentication, StartTLS, Proxy.

REFERÊNCIAS

SARI, R. F.; HIDAYAT, S. Integrating Web Server Applications With LDAP Authentication: Case Study on Human Resources Information System of UI. In: **INTERNATIONAL SYMPOSIUM ON COMMUNICATIONS AND INFORMATION TECHNOLOGIES**, 6., 2006, Bangkok. Anais... Bangkok: IEEE, 2006. p. 307–312 Disponível em: https://doi.org/10.1109/ISCIT.2006.340053. Acesso em: 17 maio 2025

WU, Z.; HUANG, W.; YU, L. Design and Implementation of Unified Identity Authentication System Based on LDAP in Digital Campus. **Advanced Materials Research**, v. 912–914, p. 1213–1217, 2014. Disponível em: https://doi.org/10.4028/www.scientific.net/AMR.912-914.1213. Acesso em: 19 maio 2025

OBIMBO, C.; FERRIMAN, B. Vulnerabilities of LDAP As An Authentication Service. **Journal of Information Security**, v. 2, p. 151–157, 2011. Disponível em: https://doi.org/10.4236/jis.2011.24015. Acesso em: 7 maio 2025.

CHEN, Y.; PUNCHHI, R.; TRIPUNITARA, M. The poor usability of OpenLDAP Access Control Lists. **IET Information Security**, v. 17, 2022. Disponível em: https://doi.org/10.1049/ise2.12079. Acesso em: 20 maio 2025.

GESTENBERGER, Guilherme Santoro, **Passo a Passo para Elaboração de artigos científicos e TCC**. Disponível em: https://www.udemy.com/course/passo-a-passo-para-elaboracao-de-artigos-cientificos-e-tcc. Acesso em: 5 abril 2025.

PATIL, Jitendra. **How to Install OpenLDAP Server and Configure the OpenLDAP Client**. Disponível em: https://blog.clairvoyantsoft.com/installation-of-openldap-server-and-configure-the-openldap-client-8be45698f8c8. Acesso em: 3 abril 2025.

HERTZOG, Ed. **How-To OpenLDAP Server Installation, in 15 Minutes or Less.** Disponível em:

https://medium.com/@PhillyWebGuy/how-to-openldap-server-installation-in-15-minutes-or-less-99df3ba14fb7. Acesso em: 3 abril 2025.

FINISKY. **LightSquid Hardcode Year Fix**. Disponível em: https://finisky.github.io/2021/01/03/lightsquidhardcodeyear.en/. Acesso em: 12 maio 2025

MONTEIRO, Steven. **An internet-wide analysis of TLS configurations of public LDAP servers. 2021.** University of Twente, Enschede. Disponível em: http://essay.utwente.nl/87004/1/Monteiro_BA_EEMCS.pdf. Acesso em: 25 abril 2025

DEBIAN. **DontBreakDebian. Debian Wiki**, 15 abr. 2025. Disponível em: https://wiki.debian.org/DontBreakDebia Acesso em: 21 maio 2025

UBUNTU. **Samba OpenLDAP backend legacy. Ubuntu Server Guide. [S.l.], 2024.** Disponível em: https://documentation.ubuntu.com/server/how-to/samba/openldap-backend-legacy/. Acesso em: 4 maio 2025.

SAMBA. **Frequently Asked Questions. SambaWiki [S.l.], 2025.** Disponível em: https://wiki.samba.org/index.php/FAQ. Acesso em: 13 maio 2025.

APÊNDICE

APÊNDICE A – Procedimento Operacional Padrão (POP) - Autenticação Centralizada