*Anais do Congresso Brasileiro de Iniciação Científica*
(https://periodicos.unisanta.br/COB)

ISSN 2317-1316

# Gerenciamento de Identidade Centralizado em Laboratórios Linux Acadêmicos Usando FreeIPA

# Centralized Identity Management in Academic Linux Laboratories Using FreeIPA

Enzo Benedetto Proença, Elieder Damasceno Sousa, Bruno da Silva Rodrigues, Fabio Kawaoka Takase

Universidade Presbiteriana Mackenzie, Faculdade de Computação e Informática, Curso de Ciência da Computação
E-mail para contato: enzo.proenca@mackenzista.com.br

*RESUMO – Este trabalho implementa uma arquitetura de código aberto para laboratórios acadêmicos de Linux, integrando o gerenciamento de identidades do FreeIPA à implantação do Debian baseada em PXE. LDAP e Kerberos oferecem suporte à autenticação centralizada de usuários e às políticas de acesso, enquanto DHCP, TFTP e o preseed automatizam a instalação e o ingresso das estações de trabalho no domínio. A abordagem oferece um ambiente de desenvolvimento simples de implantar e personalizável, além de reduzir a dependência de soluções proprietárias. No entanto, a consolidação dos serviços em um único host cria um ponto único de falha e aumenta a exposição a riscos de segurança, sendo necessária uma avaliação adicional em escala.*

**Palavras-chave:** Compliance; FreeIPA; Código Aberto; PXE; Autossoberania.

*ABSTRACT – This work implements an open-source architecture for academic Linux laboratories, integrating FreeIPA identity management with PXE-based Debian deployment. LDAP and Kerberos support centralized user authentication and access policies, while DHCP, TFTP, and preseed automate workstation installation and enrollment. The approach offers a straightforward, customizable development environment and reduces reliance on proprietary solutions. However, consolidating services on one host creates a single point of failure and increases security exposure, requiring further evaluation at scale.*

**Keywords:** Compliance; FreeIPA; Open-Source; PXE; Self-Sovereignty.

## 1 INTRODUCTION

Informatics laboratory management in academic environments requires a balance between user flexibility and effective control over the underlying infrastructure (Krumm, 2023).

ISSN 2317-1316

In this context where access management, governance and security are essential, Windows composes most endpoints, representing a share 66.14% of operating systems (OS) in the market, while Linux defines 2.94% of the share (Stat Counter Global Stats Desktop, 2025).

Nevertheless, approximately 40% of software developers use in their workstations Linux distributions (Stack Overflow, 2022). Therefore, there is an underlying need to provide Linux with a set of resources that enable the secure and efficient deployment and use of the operating system on professional endpoints, comparable to those provided by Microsoft for Windows OS.

Laboratories used by Computer Science students often require specific tools and software to support practical learning and skill development. Courses such as Operating Systems, Computer Networks, and Parallel Computing frequently require Linux-based environments, where students may need access to system-level resources and administrative capabilities (Davoli, 2004). In addition, students need a dedicated and persistent workspace where they can develop, test, and store their coursework and projects, even if access to system resources must be restricted.

Providing students with the flexibility required for hands-on learning while maintaining centralized identity and access management and ensuring infrastructure security across multiple Linux environments represents a significant management challenge. To address this challenge, combining Free Identity, Policy and Audit (FreeIPA) with Preboot eXecution Environment (PXE) provides a strategic and scalable Open-Source approach that integrates centralized identity and access management with automated infrastructure provisioning. Furthermore, FreeIPA can help mitigate the security risks and operational overhead associated with decentralized identity management. In parallel, PXE-based provisioning enables each workstation to be deployed through a consistent and standardized process for each type of environment, supporting a controlled and reproducible development environment for the academic community.

Within this context, this work proposes an open-source architecture that integrates FreeIPA and PXE to provide centralized identity management (IdM), automated operating system deployment, and workstation enrollment in academic Linux laboratories and discusses the expected benefits and challenges associated with its adoption. The proposed solution aims

ISSN 2317-1316

to reduce administrative overhead, improve infrastructure standardization, and enhance security through centralized authentication and authorization mechanisms.

This work is organized as follows. In section 2, materials and methods are presented. In section 3 results are presented and discussed, and in section 4 this work is concluded.

## 2 MATERIALS AND METHODS

This work adopts an experimental approach. A literature review was conducted to identify articles and documents related to centralized identity management, user directory, access policy and Linux to understand the concepts and technologies related to this study.

Based on this review, an open-source solution was deployed in the Software Production Environment Studies Laboratory (MackLEAPS) at Mackenzie Presbyterian University (UPM) as part of the Campus Living Lab Project.

### 2.1 Free Identity, Policy and Audit (FreeIPA)

FreeIPA is an open-source Identity and Access Management (IAM) platform designed to provide centralized administration of Linux environments through the integration of authentication, authorization, directory, and certificate management services (FreeIPA, 2023). By utilizing technologies such as the 389 Directory Server for Lightweight Directory Access Protocol (LDAP) services, MIT Kerberos for network authentication, and the Dogtag Certificate System for managing X.509 profile-based certificates (Boeyen, 2008), FreeIPA enables centralized administration of users and client hosts through command-line interfaces, web-based user interfaces, or application programming interfaces (APIs) (FreeIPA, 2023). It is capable of defining authentication and authorization policies for critical services, including DNS, SUDO, and SELinux, and implementing Single Sign-On (SSO).

### 2.2 Lightweight Directory Access Protocol (LDAP) and Kerberos

The LDAP is an application-layer protocol for accessing and maintaining distributed directory information services over IP networks. Standardized as an IETF Proposed Standard (Sermersheim, 2006), LDAP defines a common data model and set of operations for the

ISSN 2317-1316

centralized management of identity-related information, including user accounts, client hosts, and security policies.

Through its hierarchical directory structure, LDAP supports authentication and authorization mechanisms required for access control in distributed systems, enabling consistent policy enforcement and scalable identity management across heterogeneous environments (Sermersheim, 2006).

However, storing identity data is insufficient without a corresponding mechanism to verify that identity claims are genuine; this is the role fulfilled by Kerberos, the network authentication protocol, formally defined in Version 5 by (Neumann, 2005), that provides cryptographic verification of the identities of principals, such as users and network servers, operating over open and potentially insecure networks.

As a trusted third-party authentication service, Kerberos employs shared secret-key cryptography to establish identity without requiring trust in the host operating system or the physical security of the network. The protocol architecture centers on the Key Distribution Center (KDC), which comprises the Authentication Server (AS) and the Ticket-Granting Server (TGS) and maintains a database of principals and their associated secret keys.

In a typical exchange, a client requests credentials from the KDC and receives a ticket along with a temporary session key, which the client subsequently uses to authenticate itself to specific application servers. Through the use of authenticators and timestamps to mitigate replay attacks, the protocol supports mutual authentication and Single Sign-On (SSO) and is employed as an authentication mechanism in identity management systems such as FreeIPA.

Finally, LDAP and Kerberos can provide the directory and authentication services that constitute the core identity management functionality of FreeIPA.

### 2.3 Preboot eXecution Environment (PXE)

After identity and certificate management have been established, a further consideration is how client machines are initially deployed and enrolled within the network, a process addressed by the Preboot eXecution Environment (PXE) which is a standardized framework that enables a computer's firmware to perform specific networking operations prior to operating system initialization (PXESpec, 2013). It achieves this by extending established network

ISSN 2317-1316

protocols: an enhanced implementation of DHCP, conventionally used for network address assignment, is employed to locate and identify a boot server, while the Trivial File Transfer Protocol (TFTP), or its multicast variant for simultaneous transmission to multiple clients, delivers a compact program known as the Network Bootstrap Program (NBP) (PXESpec, 2013).

To ensure interoperability across diverse hardware configurations, PXE incorporates the Universal Network Device Interface (UNDI), which provides the NBP with a consistent means of network access independent of the specific network adapter installed.

The standardized procedure operates as follows: the client system broadcasts a request identifying itself as PXE-enabled, selects a server from the responses received, and subsequently downloads and executes the NBP.

This mechanism supports remote operating system deployment, execution of diagnostic utilities for system recovery, and diskless network operation. Collectively, these capabilities establish a predictable, hardware-independent environment for early-stage network processes.

# 3 RESULTS AND DISCUSSION

## 3.1 Results

The implemented architecture is described in the diagram presented in Figure 1. The existing network topology is extended by integrating a FreeIPA identity management instance directly onto the PXEServer node, alongside the existing DHCP, TFTP, and WEBServer components.

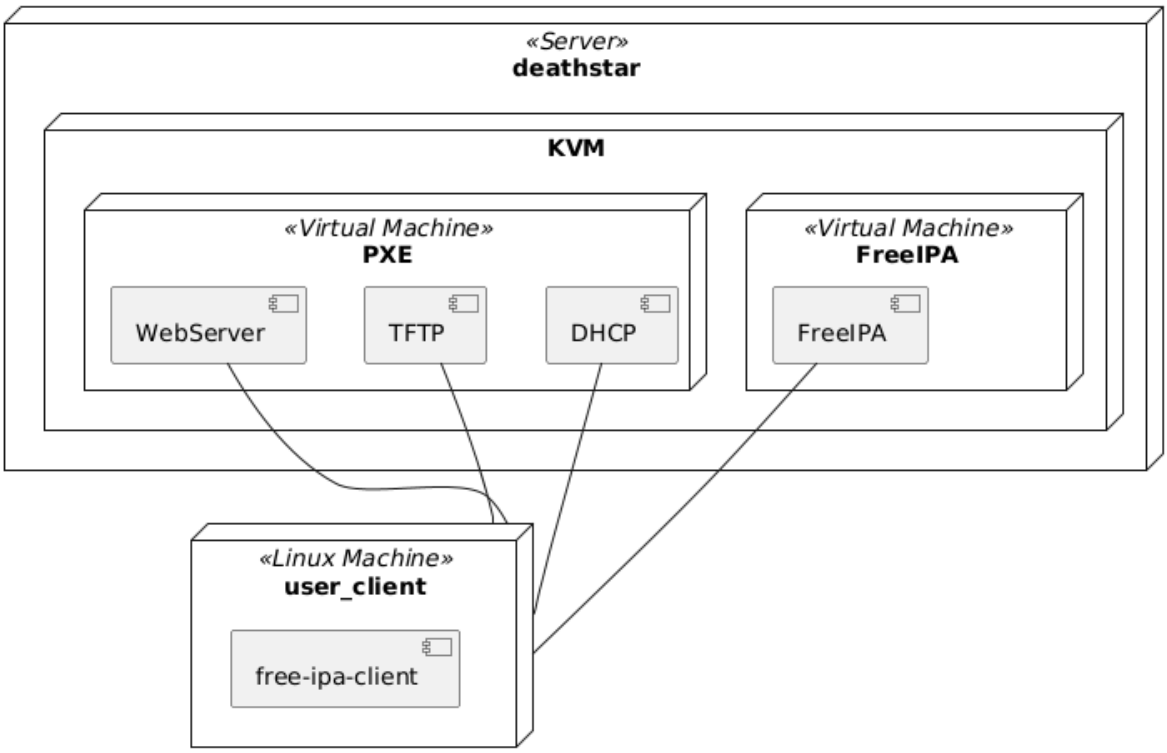
This co-location is architecturally justified by the tight coupling between network bootstrapping and identity provisioning in a diskless or thin-provisioning environment: as client1 and client2 initiate a PXE boot sequence through the hub, the DHCP service assigns network parameters and directs the client to the TFTP service for bootloader and kernel retrieval, after which the WEBServer can serve kickstart/preseed configuration files.

Embedding FreeIPA on the same host allows these provisioning files to reference IPA enrollment parameters (realm, domain, and one-time enrollment tokens) during provisioning-

ISSN 2317-1316

file generation, enabling each client to be automatically joined to the Kerberos realm and LDAP directory immediately upon first boot, without requiring a separate, manually invoked *ipa-client-install* step.

*Figure 1: Deployment Diagram*




With respect to component interaction, the architecture introduces a logical service layer within PXEServer: FreeIPA's LDAP/Kerberos endpoints operate concurrently with DHCP and TFTP, all bound to the same physical or virtual interface exposed to the hub segment.

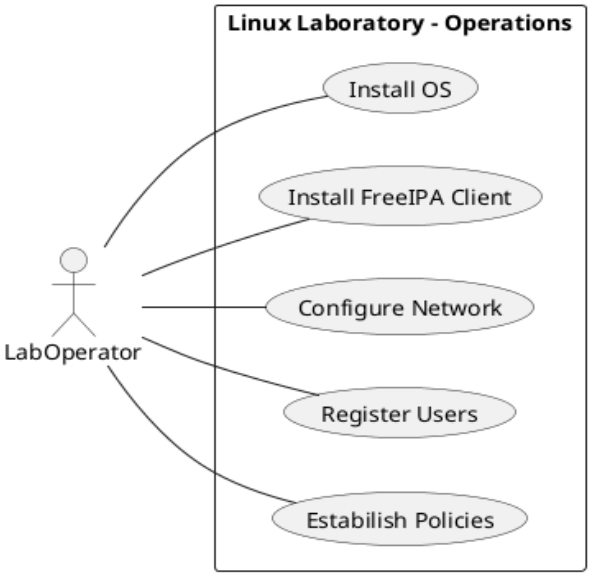
The WEBServer component is repurposed to host the FreeIPA-generated kickstart files, which embed the *ipa-client-install* invocation with pre-shared enrollment credentials or a random password (OTP) issued by the IPA CA. This design consolidates the conventionally distinct network-bootstrap, configuration-delivery, and identity tiers into a single administrative domain, reducing inter-host authentication overhead and latency during the provisioning window.

ISSN 2317-1316

In Figure 2, the main advantage of this solution is highlighted, where a single actor (in this case the laboratory operator) can configure what would otherwise be a multi-role workflow through a singular interface.

PXE eliminates the burden of configuring each singular machine within the 'Install OS', 'Configure network' and 'Install FreeIPA client', while FreeIPA allows for registering new users and setting up policies for them. Once enrolled, each client inherits centralized Kerberos authentication, LDAP-based user records, and HBAC/SUDO policies.

*Figure 2: Use cases diagram.*




## 3.2 Implementation

The FreeIPA installation followed the official documentation (FreeIPA, 2023), where the tool's dedicated DNS server is configured for use alongside the Kerberos domain. The host machine running FreeIPA requires a static FQDN hostname, forming the domain into which all users are integrated. After installation, the setup proceeded to the configuration of users, their groups, and permissions.

As part of the PXE server deployment, DHCP and TFTP servers were installed to automatically configure the network settings for users joining the domain. In addition to

ISSN 2317-1316

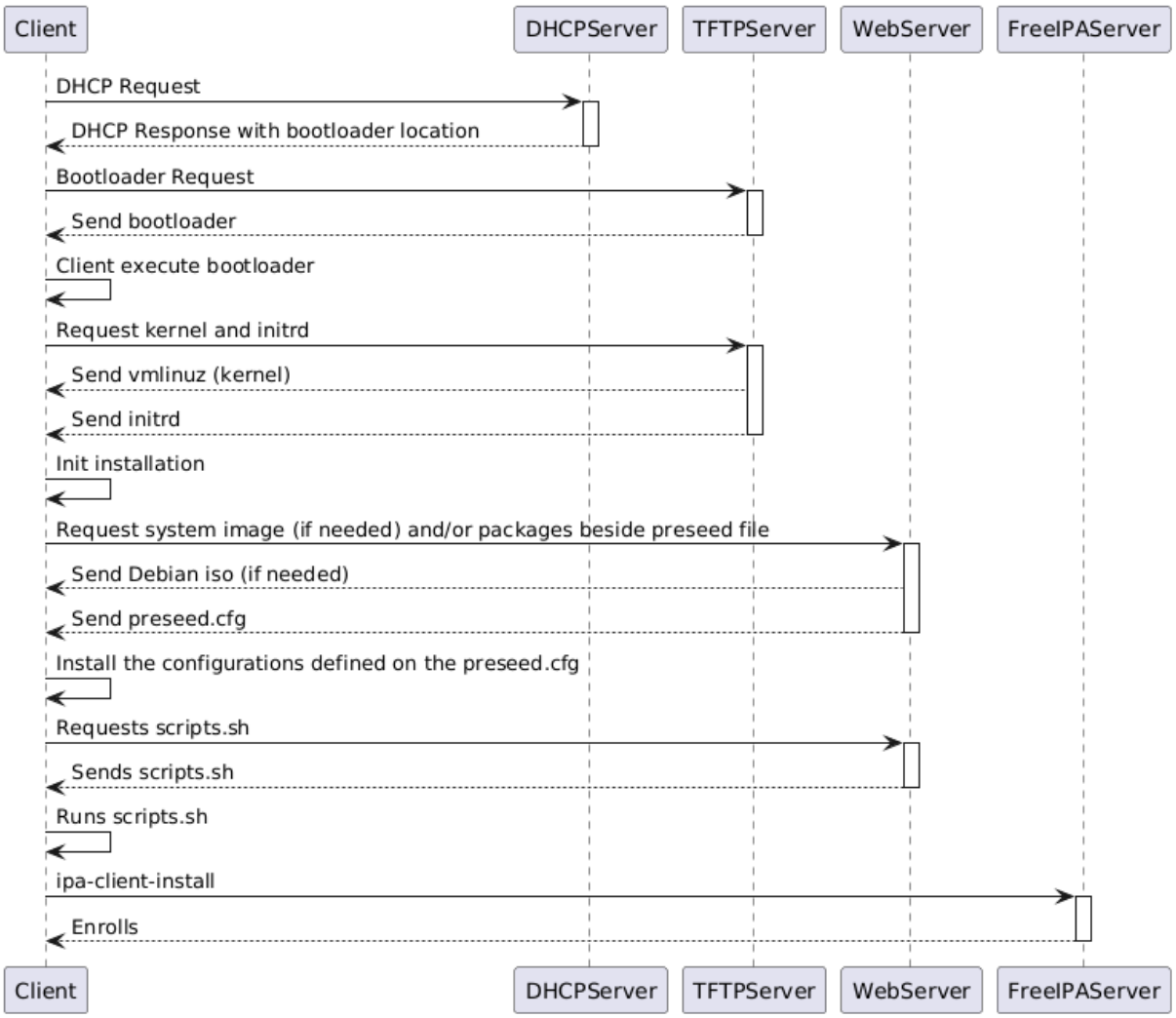
assigning an IP address to the client machine, the DHCP server also sends the path to the Debian system bootloader.

After the kernel has been initially loaded, the client then requests the full disk image from the TFTP server. The installation is carried out automatically using a preseed script, which applies customized settings for a software development laboratory environment.

The preseed file is essential at this stage, as it enables the provisioning of dozens of machines simultaneously without human intervention.

The communication between client and PXEServer will occur following the diagram proposed in Figure 3. This way the configuration will only need to happen on the first boot sequence and outside of the user's view.

*Figure 3: Sequence Diagram*



ISSN 2317-1316

### 3.3 Discussion

İş (İş, 2025) investigates and discusses cybersecurity challenges in academic institutions, with particular emphasis on vulnerabilities associated with Microsoft's Identity Management (IdM) services, especially Active Directory (AD), whose is now called Microsoft Entra ID. The study reports that incorporating network-connected devices into the AD structure resulted in a 60% decrease in endpoint-related security breaches. However, it also revealed significant security weaknesses, including excessive administrative privileges granted to 75% of non-administrative users. In addition, Active Directory is a proprietary solution that requires the Microsoft Windows Server ecosystem, which may represent a limitation for predominantly Linux-based academic environments.

Yeh (Yeh, 2002) elaborates on the usage of LDAP for a CA system and its advantages. This study's conclusion on LDAP's usage simplifies X.500's model and reduces overhead in communication by running TCP directly while also retaining scalability.

In the MackLEAPS deployment, access management and access levels proved to be simple and centralized since users, groups and sudo rules are defined once in FreeIPA and inherited by every enrolled workstation, with no per-machine configuration. This is consistent with centralized control that LDAP and Kerberos are expected to provide (Sermershein, 2006) and worked as intended in MackLEAPS laboratory.

The main advantage is that creating a standardized workstation for software laboratories is simplified, and reinstallation wipes previous data from the device, ensuring a predictable, reproducible environment, while user identities and policies remain preserved in the central directory.

One of the main difficulties during deployment was the development of a working preseed and a helper Bash script with *ipa-client-install* command. Preseed commands (e.g. *late_command*) run inside the installer environment, where the target system is only mounted under */target* and is not yet running (services, network configuration and hostname are not active). Since *ipa-client-install* requires a running system, it cannot be executed during installation. Instead, the script is placed on the target system, and enrollment only starts after both a cold boot and a first manual login using a root account, when the system is fully mounted

ISSN 2317-1316

and initialized. This also makes the process hard to test, as every change to the preseed or scripts requires a full Debian installation to be validated.

## 4 CONCLUSION

The management of Linux laboratories using FreeIPA as IAM proved itself suitable given its ease of deployment and ability to provide a pre-made environment for development with security. The benefits include self-sovereignty for organizations by decoupling from closed or paid solutions. Beyond that, it offers the flexibility to create custom-made environments for specific situations required by students. However, the consolidation introduces a single point of failure and an expanded attack surface, since directory, certificate authority, and DNS services all reside behind one exposed interface. A current limitation is the absence of Secure Boot, meaning that boot components are not cryptographically verified. Therefore, it should be considered in the next steps to strengthen the integrity of the provisioning process. We also should conduct the integration of FreeIPA with Microsoft Entra (formerly Azure AD). This would allow environments that already use Microsoft identity services to keep its granular control over Linux laboratory access, avoiding the problem highlighted by İş (2025).

## 5 DECLARATION ON THE USAGE OF AI

During the preparation of this work, the tool duck.ai was used to assist in translating sections of the text. The generated content was reviewed, edited, and validated by the authors, who assume full responsibility for the final text.

## 6 REFERENCES

N. Krumm, “Organizational and technical security considerations for laboratory cloud computing,” The Journal of Applied Laboratory Medicine, vol. 8, no. 1, pp. 180–193, 01 2023. [Online]. Available: https://doi.org/10.1093/jalm/jfac11.

Statcounter Global Stats, “Desktop Operating System Market Share Worldwide,” Oct. 2025. [Online]. Available: https://gs.statcounter.com/os-market-share/desktop/worldwide/

ISSN 2317-1316

Stack Overflow, "Developer Survey 2022," 2022. [Online]. Available: https://survey.stackoverflow.co/2022/#section-most-popular-technologies-operating-system

R. Davoli, "Teaching operating systems administration with user mode linux," in Proceedings of the 9th Annual SIGCSE Conference on Innovation and Technology in Computer Science Education, ser. ITiCSE '04. New York, NY, USA: Association for Computing Machinery, 2004, p. 112–116. [Online]. Available: https://doi.org/10.1145/1007996.1008027

Documentation — FreeIPA documentation. [Online]. Available: https://www.freeipa.org/page/Documentation.html

S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, and D. Cooper, "Internet x.509 public key infrastructure certificate and certificate revocation list (CRL) profile," Internet Engineering Task Force, Request for Comments RFC 5280, 2008, num Pages: 151. [Online]. Available: https://datatracker.ietf.org/doc/rfc5280.

J. Sermersheim, "Lightweight directory access protocol (LDAP): The protocol," Internet Engineering Task Force, Request for Comments RFC 4511, 2006, num Pages: 68. [Online]. Available: https://datatracker.ietf.org/doc/rfc4511

C. Neuman, S. Hartman, K. Raeburn, and T. Yu, "The kerberos network authentication service (v5)," Internet Engineering Task Force, Request for Comments RFC 4120, num Pages: 138. [Online]. Available: https://datatracker.ietf.org/doc/rfc4120.

Wayback machine. [Online]. Available: https://web.archive.org/web/20131102003141/http://download.intel.com/design/archives/wfm/downloads/pxespec.pdf

H. ˙Is¸, "A novel approach to enhancing active directory security in academic institutions," Balkan Journal of Electrical and Computer Engineering, vol. 12, no. 4, pp. 394–402, 2025. [Online]. Available: https://doi.org/10.17694/bajece.1567393

Y.-S. Yeh, W.-S. Lai, and C.-J. Cheng, "Applying lightweight directory access protocol service on session certification authority," vol. 38, no. 5, pp. 675–692. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128601002821