INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

CAMPUS JABOATÃO DOS GUARARAPES

PÓS-GRADUAÇÃO EM GESTÃO E QUALIDADE EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

MARCUS DIEGO DE OLIVEIRA CASTELO BRANCO

IMPLEMENTAÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSOS APLICADO A AMBIENTES BASEADOS EM GNU/LINUX.

JABOATÃO DOS GUARARAPES

2021

MARCUS DIEGO DE OLIVEIRA CASTELO BRANCO

IMPLEMENTAÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSOS APLICADO A AMBIENTES BASEADOS EM GNU/LINUX.

Trabalho de conclusão de curso apresentada ao programa de Pós-Graduação em Gestão e Qualidade em Tecnologia da Informação e Comunicação do Instituto Federal de Ciência e Tecnologia de Pernambuco, como requisito para obtenção do título de pós-graduado em Gestão e Qualidade em Tecnologia da Informação e Comunicação.

Orientador: Prof. Me. Diego dos Passos Silva

JABOATÃO DOS GUARARAPES
2021

FICHA CATALOGRÁFICA

C349i Castelo Branco, Marcus Diego de Oliveira.

Implementação de gerenciamento de identidade e acessos aplicado a ambientes baseados em GNU/LINUX / Marcus Diego de Oliveira Castelo Branco; Orientador Prof. Me. Diego dos Passos Silva - Jaboatão dos Guararapes, 2021.

61f.; il.

Trabalho de Conclusão de Curso (Especialização em Gestão e Qualidade em Tecnologia da Informação e Comunicação) – IFPE - Campus Jaboatão dos Guararapes.

. Inclui Referências.

1. Tecnologia da Informação e Comunicação 2. Sistema operacional. 3. Software livre 4. Gerenciamento de ambientes de rede. I. Jesus, Nivson Santos de. II. IFPE. III. Título.

CDD 004.21

Catalogação na fonte elaborada pelo Bibliotecário Thiago Leite Amaro da Silva - CRB4/ 2.021

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PERNAMBUCO

Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco
Campus Jaboatão dos Guararapes
Divisão de Pesquisa e Extensão e Pós-graduação

ATA DE REALIZAÇÃO DE BANCA

No dia **24** de **março** de **2021** as **20h** na sala **on-line** do IFPE Campus Jaboatão dos Guararapes, compareceram a banca de defesa do Trabalho de Conclusão de Curso da Especialização *lato sensu* em **Gestão e Qualidade em Tecnologia da Informação e Comunicação,** do(a) aluno(a) **Marcus Diego de Oliveira Castelo Branco** que defendeu o trabalho intitulado **Implementação de Gerenciamento de Identidade e Acessos Aplicado a Ambientes Baseados em GNU/LINUX**, os(as) professores(as) que compõem a banca descrita abaixo, e concederam a nota 7,0 sendo o(a) aluno(a) considerado(a) APROVADO de acordo com a composição das notas estabelecida pela banca avaliadora.

COMPOSIÇÃO DA BANCA		
	NOTA	**ASSINATURA**
Prof. Diego dos Passos Silva (presidente da banca)	7,0	Documento assinado digitalmente gov.br Diego dos Passos Silva Data: 25/03/2021 15:07:48-0300
Prof. Luciano de Souza Cabral (1 avaliador)	7,5	Documento assinado digitalmente gov.br Luciano de Souza Cabral Data: 26/03/2021 09:15:09-0300 CPF: 032.667.094-70
Prof. Viviane Cristina Oliveira Aureliano (2 avaliador)	6,5	Documento assinado digitalmente gov.br Viviane Cristina Oliveira Aureliano Data: 06/04/2021 20:46:44-0300 CPF: 007.703.324-80
NOTA FINAL	7,0	

Documento assinado digitalmente
gov.br Marcus Diego de Oliveira Castelo Branco
Data: 07/04/2021 14:57:58-0300
CPF: 051.945.274-70

Marcus Diego de Oliveira Castelo Branco

Documento assinado digitalmente
gov.br Nilson Candido de Oliveira Jr
Data: 29/03/2021 11:46:39-0300
CPF: 031.073.834-22

Nilson Cândido de Oliveira Júnior
Coordenador do Curso de Pós-Graduação em Gestão e Qualidade em TIC
SIAPE: 1829625

Aos colegas de curso que foram fontes de incentivo e motivação para a conclusão deste trabalho de pesquisa!

AGRADECIMENTOS

Agradeço a todos os professores do IFPE Instituto Federal de Pernambuco campus Jaboatão dos Guararapes, pela excelência da qualidade técnica de cada um. Sou grato à minha família pelo apoio que sempre me deram durante toda a minha vida. A minha mãe Maria de Fátima, que sempre me apoiou nas pricipais dificuldaes da vida. Agradeço a minha esposa Viviane, que estive ao meu lado nesta jornada acadêmica. Deixo um agradecimento especial ao meu orientador Prof. Me. Diego dos Passos Silva pelo incentivo e dedicação do seu escasso tempo ao meu projeto de pesquisa. A todos que direta ou indiretamente fizeram parte de minha formação, meus agradecimentos.

“A vitalidade é demonstrada não apenas pela persistência, mas pela capacidade de começar de novo.” (F. Scott Fitzgerald)

RESUMO

Administrar um grande parque de servidores Linux se torna um desafio complexo quando muitos usuários necessitam ter acesso aos servidores. Esta tarefa pode ser negligenciada por administradores devido ao grande esforço dedicado a criação e manutenção da credenciais de acesso individualmente utilizadas. Neste trabalho foi apresentada a análise da ferramenta FreeIPA, fundamentada em *frameworks* de apoio de segurança da informação. O FreeIPA é uma solução baseda em software livre, composta de vários sistemas integrados, que oferece um ecossistema para a gestão centralizada de identidade e acessos, destinadas a sistemas operacionais Linux. Diante dos desafios da implementação da ferramenta FreeIPA, foram avaliadas a aplicabilidade de controles relacionados ao processo de gestão de identidades. Como contribuição, o trabalho busca apresentar a análise da ferramenta FreeIPA como ferramenta de apoio no processo de gerência de identidades e acessos, de forma estruturada, com metodologia fundamentada em *frameworks* de apoio.

Palavras-chave: IAM. Identidades. Acessos. FreeIPA. Gestão. Centralizada.

ABSTRACT

Managing a large number of Linux servers becomes a complex challenge when many users need access to the servers. This task can be neglected by administrators due to the great effort dedicated to creating and maintaining the access credentials used individually. In this work, the analysis of the FreeIPA tool was presented, based on information security support frameworks. FreeIPA is a solution based on free software, composed of several integrated systems, which offers an ecosystem for centralized identity and access management, aimed at Linux operating systems. In view of the challenges of implementing the FreeIPA tool, the applicability of controls related to the identity management process was evaluated. As a contribution, the work seeks to present the analysis of the FreeIPA tool as a support tool in the identity and access management process, in a structured way, with methodology based on support frameworks.

Keywords*: IAM. Identities. Access. FreeIPA. Management. Centralized.*

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABAC	Atribute-Based Access Control
API	Application Programming Interface
CA	Certification Authority
CEA	Cybersecurity Enhancement Act
DAC	Discretionary Access Control)
DNS	Domain Name System
DTM	Decentralized Trust Management
FQDN	Fully Qualified Domain Name
HBAC	Host-Based Access Control
IAM	Identity and Access Management
IdM	Identity Management
IEC	International Electrotechnical Commission
IPA	Identity,Policy and Audit
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OWASP	Open Web Application Security Project
PAM	Pluggable Authentication Modules
PIN	Personal Identification Number
RBAC	Rule-Based Access Control
RHEL	Red Hat Enterprise Linux
SSSD	System Security Services Daemon

SUMÁRIO

1 INTRODUÇÃO

As organizações utilizam cada vez mais soluções informatizadas para oferecer serviços, desenvolver e comercializar produtos pela internet, sem ter que abrir lojas físicas, reduzindo assim seus custos. O sucesso desse mercado crescente está relacionado com a forma como a tecnologia tem suportado essas relações de interesse. No entanto, a credibilidade destas organizações são atacadas quando incidentes de segurança são detectados ou quando seus dados, ou dados de seus usuários são obtidos para fins escusos. Diversas iniciativas em segurança da informação são acionadas para contribuir na minimização de riscos. Neste trabalho será abordada a administração da gerência de acessos e identidade, área que muitas vezes é a porta de entrada para exploração de vulnerabilidades. Muitas vezes as ameaças podem estar dentro da própria organização e as oportunidades pode contribuir para a obtenção de vantagens. Algumas ameaças estão relacionadas a ausência ou falhas na gerência de acessos, tais como:

a) Falhas em segmentação de funções que permitem que colaboradores tenham acesso a informações confidenciais em determinados sistemas, bancos de dados, repositórios de relatórios, entre outros;
b) Falha nos processos de mudança de função, onde os colaboradores deveriam ter acessos atualizados, assim perderiam acessos e ganhariam outros, como mudanças de filiais, ou mudanças de funções dentro da organização;
c) Desligamentos, aposentadorias, investigações, falecimento de colaboradores: o colaborador deveria ter seus acessos bloqueados, senhas de credenciais as quais ele conhece deveriam se trocadas, entre outras ações.

Diante do exposto, será proposto um projeto de gerenciamento de acesso para minimização de vulnerabilidades e apoio a gestão de controle de acesso, concentrando o escopo do trabalho a gestão de acessos a ambientes de servidores Linux, elevando a maturidade desta competência dentro das organizações.

1.1 JUSTIFICATIVA

O acesso ao sistema operacional Linux é nativamente realizado de forma simplificada, utilizando mecanismo de autenticação básica (usuário e senha) previamente definidos durante o processo de instalação. Dependendo do nível de maturidade das organizações, os ambientes Linux possuem gestão de usuários independentes, onde o mesmo usuário é criado com a mesma senha em todos os servidores, desta forma acabam vulneráveis em caso de vazamento de senhas, tipo de ataque conhecido como *"credential stuffing"*.

Segundo o OWASP (OWASP, 2018):

> O preenchimento de credenciais (*credential stuffing*) é a injeção automática de pares de nome de usuário/senha violados, a fim de obter acesso fraudulento às contas de usuário. Este é um subconjunto da categoria de ataque de força bruta: um grande número de credenciais derramadas são inseridas automaticamente

> nos sites até serem correspondidas potencialmente a uma conta existente, que o invasor pode sequestrar para seus próprios propósitos.

O presente trabalho propõe o planejamento e a construção de um processo de gestão de acessos, baseado em boas práticas e adoção de ferramentas de controle para gerenciamento de identidades e acessos. Partindo da hipótese que o FreeIPA pode servir como ferramenta de apoio para a gestão de identidade e acessos para sistemas Linux.

1.2 OBJETIVO GERAL

Este trabalho tem por objetivo apresentar um projeto de implementação de gerência de identidades e acessos, destinada ao controle de acesso aos servidores Linux, com o intuito de oferecer maior capacidade de administração centralizada no controle de acessos destes servidores.

1.3 OBJETIVOS ESPECÍFICOS

a) Identificar e aplicar boas práticas de gestão de identidades e acessos, para implementação de controles, sejam promovidos por processos bem descritos, sejam promovidos com apoio de sistemas de informação.
b) Implementar a ferramenta FreeIPA em ambiente de produção e realizar análise da ferramenta como plataforma de apoio para a implementação da gestão centralizada de identidade e acessos para ambientes Linux.

1.4 ESTRUTURA DA MONOGRAFIA

Este trabalho foi estruturado para fornecer fundamentação sobre os seguintes conceitos:

Quadro 1 – Estrutura da monografia (Autor,2019).

Capítulos	**Descrição**
Capítulo 01	Definição dos objetivos e justificativa.
Capítulo 02	Fundamentação teórica: a) Conceitos fundamentais sobre controle de acesso. b) PAM-Linux, método padrão de controle de acesso nativo aos sistemas GNU/Linux. c) Método de acesso RBAC – Rule-based Access Control. d) Metodologia de gerência adotada baseada no *Framework Core- Framework for Improving Critical Infrastructure Cybersecurity* – NIST e) Controles adotados com base no "NIST SP 800-53 Rev. 4 A" para elaboração de gerência de identidades e acessos. f) FreeIPA e sua utilização na proposta.
Capítulo 03	Implementação da solução proposta: a) Definição do Problema. b) Implementação da gerência de acessos para ambientes de servidores Linux. c) Análise dos resultados.
Capítulo 04	Análise dos resultados.
Capítulo 05	Considerações finais.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo serão apresentados os conceitos fundamentais de apoio ao estudo realizado, oferecendo a fundamentação teórica de apoio utilizada neste trabalho.

2.1 CONCEITOS FUNDAMENTAIS SOBRE CONTROLE DE ACESSO

Para implementação de qualquer modelo básico de controle de acesso, é necessário compreender os elementos que possibilitam a avaliação de diferentes formas de controle automatizado de acesso. Segundo (Rhand Leal, 2017), as normas da família ISO/IEC 27000 (ISO/IEC 27000 et al., 2018) definem os seguintes conceitos fundamentais:

- **Identificação**: métodos para prover um sujeito (entidade que solicita acessos) com uma identidade reconhecível (por exemplo uma conta de usuário, passaporte, etc.).
- **Autenticação**: métodos para assegurar que um sujeito é quem ele diz ser (senha, token, impressão digital, etc).
- **Autorização**: métodos para controlar quais ações um sujeito pode realizar em um objeto (por exemplo, lista de permissões do sujeito e lista de permissões do objeto).

Quanto aos métodos de autenticação, os seguintes conceitos podem ser usados, separadamente ou em combinação para realização da autenticação:

- **"Algo que se sabe"**: senhas e PINs;
- **"Algo que se possui"**: smart cards, tokens, chaves, etc;
- **"Algo que se é"**: biometria, padrões de voz, retina, impressão digital, etc.

2.2 PAM-LINUX

Ciente dos conceitos de identificação, autenticação e autorização, para maior entendimento sobre o processo de autenticação utilizados em sistemas GNU/Linux, é necessário conhecer o PAM-Linux (*Pluggable Authentication Modules for Linux* – Módulos de Autenticação Plugáveis para Linux). O PAM-Linux ou simplesmente PAM, é um conjunto de bibliotecas compartilhadas que permitem ao administrador do sistema local, escolher como os aplicativos autenticam os usuários (MORGAN; KUKUK, 2018c). O objetivo do projeto PAM-Linux é separar o desenvolvimento de software de concessão de privilégios do desenvolvimento de esquemas de autenticação seguros e apropriados (MORGAN; KUKUK, 2018b). O PAM permite definir diferentes combinações de mecanismos de autenticação para o aplicativo. O PAM pode ser configurado para impedir que determinados programas autentiquem os usuários e para avisar quando determinados programas tentam fazer a autenticação. Para maior compreensão, o aplicativo "login" é um desses programas que faz uso de bibliotecas do PAM. O aplicativo "login" faz duas coisas, primeiro verifica se o usuário solicitante é quem ele afirma ser e, em seguida, fornece o serviço solicitado, neste caso o "login". Esse processo é realizado por um aplicativo que faz uso de bibliotecas de funções para solicitar autenticação de usuários. Essas bibliotecas

do PAM são configuradas localmente com um arquivo de sistema, /etc/pam.conf (ou uma série de arquivos de configuração localizados em /etc/pam.d/).

As figuras 1 e 2 apresentam a arquitetura de comunicação do PAM e seus respectivos módulos.

Figura 1 – Comunicação entre componentes do PAM (SRIVASTAVA, 2009).

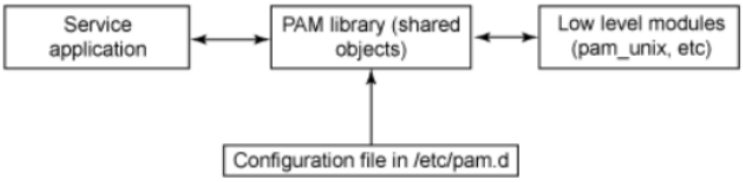
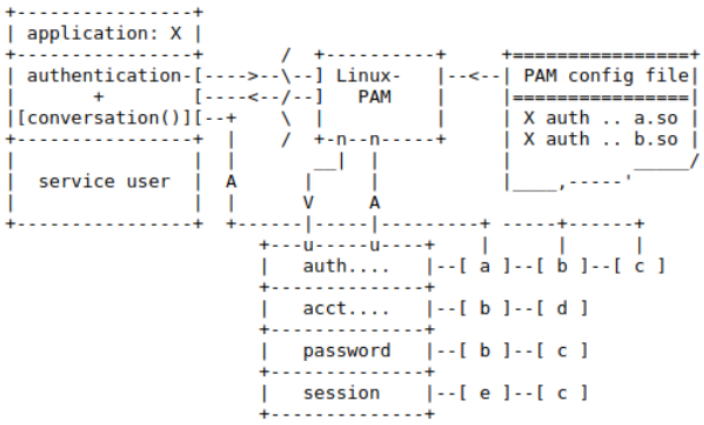


Figura 2 – Análise de módulos do PAM (MORGAN; KUKUK, 2018a).



Os módulos do PAM são classificados por tipo de módulo. Segundo (MORGAN; KUKUK, 2018a) qualquer módulo fornecido deve implementar pelo menos uma das quatro funções de tipo de módulo:

a) *account* (conta): Esse tipo de módulo executa o gerenciamento de contas com base em "não autenticação". Geralmente, é usado para restringir e/ou permitir o acesso a um serviço com base na hora do dia, nos recursos do sistema atualmente disponíveis (número máximo de usuários por exemplo) ou talvez na localização do usuário solicitante. Exemplo: logon 'root' apenas no console. Os módulos de account executam ações relacionadas ao acesso, à expiração de conta e de credencial, restrições/regras de senha, etc.

b) *Auth* (autenticação): Esse tipo de módulo fornece dois aspectos da autenticação do usuário. Em primeiro lugar, estabelece que o usuário é quem ele afirma ser, instruindo o aplicativo a solicitar uma senha ou outro meio de identificação ao usuário. Em segundo lugar, o módulo pode conceder associação ao grupo ou outros privilégios por meio de suas propriedades de concessão de credenciais. O módulo de autenticação é usado para autenticar usuários, configurar e cancelar credenciais.

c) *password* (senha): Esse tipo de módulo é necessário para atualizar o token de autenticação associado ao usuário. Normalmente, há um módulo para cada tipo de autenticação baseada em desafio-resposta. O módulo de gerenciamento de senha executa ações relacionadas à alteração e atualização de senha.

d) *session* (sessão): Esse tipo de módulo está associado a fazer coisas que precisam ser feitas para o usuário antes e/ou depois da prestação do serviço. Tais coisas incluem o registro de informações relativas à abertura e fechamento de algumas trocas de dados com um usuário, montagem de diretórios e etc. O módulo de gerenciamento de sessão é usado para inicializar e terminar sessões.

Regras para o mesmo tipo podem ser empilhadas (stacked). O PAM executa as regras empilhadas em ordem e retorna um único código no final do procedimento. As configurações dos módulos PAM obedecem a uma sintaxe, e o formato de cada regra é baseado em uma coleção de tokens separados por espaço, os três primeiros que não diferenciam maiúsculas de minúsculas, conforme apresentado no quadro 2:

Quadro 2 – Exemplo de configuração do arquivo *"/etc/pam.conf"* (Autor, 2021).

<serviço> <tipo> <controle> <caminho módulo> <argumentos módulo>

A sintaxe dos arquivos contidos no diretório "/etc/pam.d/" é idêntica ao arquivo "/etc/-pam.conf", exceto pela ausência de qualquer campo de "serviço" (primeiro campo). Nesse caso, o serviço deve ser o nome do próprio arquivo de configuração (escrito em letras maiúsculas) no diretório "/etc/pam.d/".

Um recurso importante do PAM é a possibilidade de empilhar várias regras, combinando os serviços de vários módulos PAM para uma determinada tarefa de autenticação.

O primeiro campo "serviço", geralmente é o nome familiar do aplicativo correspondente. Os aplicativos "login" e "su" são bons exemplos. O sinalizador de controle (*flag* de controle) informa o que fazer com o código de retorno de uma regra. Os possíveis sinalizadores de controle são:

a) ***required*** **(necessário)**: O resultado do módulo deve ser bem sucedido para que a autenticação continue. Mas o usuário não é informado, até que todos os testes de todos os módulos, que façam referência àquela interface estejam completos.

b) ***requisite*** **(requisito)**: No caso de um módulo retornar uma falha, o PAM encerrará a execução e retornará falha ao aplicativo ou à pilha PAM superior. O valor de retorno é aquele associado ao primeiro módulo *required* ou *requisite* que falhar. O resultado do módulo deve ser bem sucedido para que a autenticação continue. O usuário é informado imediatamente da falha de autenticação.

c) ***sufficient*** **(suficiente)**: Se esse módulo for bem-sucedido e nenhum módulo *required* anterior falhar, a estrutura do PAM retornará sucesso para o aplicativo ou para a pilha PAM superior, sem chamar nenhum módulo adicional. Se resultado do módulo falhar

o mesmo é ignorado. Em resumo, se o resultado de um módulo sinalizado como *sufficient* é de sucesso e nenhum módulo prévio sinalizado como *required* falhou, então nenhum outro resultado é necessário e o usuário é autenticado.

d) ***optional* (opcional)**: O sucesso ou falha deste módulo é importante apenas se for o único módulo na pilha associado a este serviço. O PAM ignorará o código de retorno desta regra.
e) ***include* (incluir)**: Para importar a configuração a partir de outros arquivos, inclui todas as linhas do arquivo para esse controle.
f) ***substack* (sub-pilha)**: Também inclui todas as linhas do tipo especificado do arquivo de configuração como argumento para esse controle. Difere de *"include"* porque uma *falha na substack* afetará apenas as regras definidas na própria *substack*. Uma *substack* é vista no arquivo de configuração como um único módulo com um único resultado.

2.3 RBAC

Algumas referências são encontradas para definir o Controle de Acesso com Base nas Funções (*Rule-Based Access Control* - RBAC). Segundo o *National Institute of Standards and Technology* (NIST) (NIST, 2014):

> O controle de acesso baseado em função (RBAC) é uma política de controle de acesso que restringe o acesso ao sistema da informação a usuários autorizados. As organizações podem criar funções específicas (*roles*) com base nas funções de trabalho e nas autorizações (ou seja, privilégios) para realizar as operações necessárias nos sistemas de informação organizacional associados às funções definidas pela organização. Quando os usuários são atribuídos às funções organizacionais, eles herdam as autorizações ou privilégios definidos para essas funções.

Segundo (ROUSE, 2012):

> O controle de acesso baseado em função (RBAC) é um método para restringir o acesso à rede com base nas funções de usuários individuais em uma empresa. O RBAC permite que os funcionários tenham direitos de acesso apenas às informações necessárias para realizar seus trabalhos e os impedem de acessar informações que não lhes pertencem.

Segundo (SANDHU; FERRAIOLO; KUHN, 2000), o RBAC fornece um nível valioso de abstração por promover a administração de segurança no nível da empresa/instituição e não somente no nível de identidade do usuário. O modelo NIST RBAC (FERRAIOLO et al., 2001) é pioneiro na direção da padronização de um modelo de RBAC. Contudo, é irrealista supor a existência de um único modelo definitivo para o RBAC.

O conceito básico de função (*role*) visa estabelecer permissões com base em funções, ou seja papéis funcionais da organização, logo em seguida atribuir usuários a uma ou mais funções. Com o RBAC, as decisões de acesso baseiam-se nas "funções" que os usuários individuais desempenham como parte de uma empresa. As funções podem representar as tarefas,

responsabilidades e qualificações associadas a uma empresa ou instituição. Como as funções dentro de uma empresa/instituição são relativamente persistentes com relação à rotatividade de usuários e reatribuição de tarefas, o RBAC fornece um mecanismo poderoso para reduzir a complexidade, o custo e o potencial de erro na atribuição de permissões de usuário na empresa (SANDHU; FERRAIOLO; KUHN, 2000). Como as funções dentro de uma empresa geralmente têm permissões sobrepostas, os modelos RBAC geralmente incluem recursos para estabelecer "hierarquias de funções", onde uma determinada função pode incluir todas as permissões de outra função. O RBAC também permite a especificação e a aplicação de uma variedade de "políticas de proteção" que podem ser adaptadas dependendo das necessidades da organização. As políticas aplicadas em um sistema específico são o resultado da configuração de vários componentes do RBAC. Muitos modelos de RBAC apoiam o estabelecimento de restrições de separação de tarefas entre funções. Isso fornece aos administradores recursos aprimorados para especificar e aplicar políticas corporativas em comparação com os padrões de controle de acesso existentes, como clássico Controle de Acesso Discricionário (*Discretionary Access Control* - DAC) e Controle de Acesso Mandatório (*Mandatory Access Control* - MAC). Devido à demanda por RBAC, os fornecedores incorporaram os recursos do RBAC em seus produtos de banco de dados, gerenciamento de sistemas incluindo sistemas operacionais. Esses esforços de desenvolvimento continuam sem qualquer acordo geral sobre o que realmente constitui os recursos do RBAC.

2.4 O FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

Nos Estados Unidos, a *Public Law 113 - 274 - Cybersecurity Enhancement Act of 2014* – CEA - lei de aprimoramento da segurança cibernética (EUA, 2014), foi concebida, para fortalecer a resiliência da infraestrutura, atualizando o papel do Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology* – NIST), com intuito de facilitar e apoiar o desenvolvimento de *frameworks* de risco de segurança cibernética.

Por meio do CEA, o NIST deve identificar medidas de segurança da informação e controles que podem ser adotados voluntariamente pelos proprietários e operadores de infraestrutura crítica, para ajudá-los a identificar, avaliar e gerenciar os riscos cibernéticos. Para dar conta das necessidades de segurança cibernética particulares das organizações, há uma grande variedade de maneiras de usar o *framework*. A decisão sobre como aplicá-lo é de responsabilidade da organização que o implementa (NIST, 2018). Segundo o NIST, o *Framework for Improving Critical Infrastructure Cybersecurity*, é composto de três partes: o núcleo do *framework* (*framework core*), por camadas de implementação (*Framework Implementation Tiers*), e o *framework* baseado em perfis (*Framework Profiles*). Cada componente *Framework* reforça a conexão entre objetivos do negócio/missão e atividades de segurança cibernética (NIST, 2018).

- ***Framework Core:*** Conjunto de atividades de segurança cibernética, resultados dese-

jados, e referências aplicáveis que são comuns em todos os setores de infraestrutura crítica. Composto por cinco funções simultâneas e contínuas: identificar, proteger, detectar, responder e recuperar.

- ***Implementation Tiers (Tiers):*** Fornece contexto sobre como uma organização vê o risco de segurança cibernética e os processos em vigor para gerenciar esse risco. As camadas descrevem o grau em que as práticas de gerenciamento de risco de segurança cibernética exibem as características definidas no *framework* (por exemplo, ciente de risco e ameaça, repetível e adaptável). As camadas caracterizam as práticas de uma organização em um intervalo, desde Parcial (Camada 1) até a Adaptável (Camada 4). Durante o processo de seleção de camada, uma organização deve considerar suas práticas atuais de gerenciamento de risco, ambiente de ameaças, requisitos legais e regulamentares, objetivos de negócio / missão e restrições organizacionais.
- ***Framework Profile ("Profile/Perfil"):*** Representa os resultados com base em necessidades de negócios que uma organização tenha selecionado a partir das categorias e subcategorias do *framework core*. O perfil pode ser caracterizado como o alinhamento das normas, diretrizes e práticas para o *framework core* em um cenário de implementação particular. Para desenvolver um perfil, uma organização pode rever todas as categorias e subcategorias e, com base em objetivos de negócios, missão e uma avaliação do risco, determinar quais são as mais importantes; pode adicionar categorias e subcategorias, conforme necessário para enfrentar os riscos da organização.

O *framework* não foi construído para ser uma regra, ele é prescritivo, porém ele fornece uma sugestão de passos para a construção de novo programa de segurança cibernética ou melhorar um programa já existente. Conforme mostra o quadro 3 serão utilizadas algumas das etapas sugeridas para construção do plano de implementação de gerência de acesso e ajuste das práticas de segurança cibernética atuais, a fim de alcançar o perfil de destino.

Quadro 3 – Recomendações do *framework core* - NIST (NIST, 2018).

Fase	**Descrição**
Passo 1: Priorizar e escopo	A organização identifica seus objetivos de negócios/missão e prioridades organizacionais de alto nível.
Passo 2: Orientação	A organização identifica sistemas relacionados e ativos, requisitos regulatórios e abordagem de risco global.
Passo 3: Criar um perfil atual.	A organização desenvolve um perfil atual, indicando quais resultados de categoria, subcategoria *framework core* estão sendo alcançados atualmente.
Passo 4: Realizar uma avaliação de riscos.	A organização analisa o ambiente operacional, a fim de discernir a probabilidade de um evento de segurança cibernética e o impacto que o evento poderia ter sobre a organização.
Passo 5: Criar um perfil de destino.	O perfil de destino deve refletir adequadamente critérios dentro do nível alvo de Implementação.
Passo 6: Determinar, analisar, priorizar lacunas.	Criar um plano de ação prioritário para reduzir as lacunas (refletindo missão, condutores, custos-benefícios, e os riscos) - para alcançar os resultados no perfil de destino. A organização deve determinar os recursos, incluindo o financiamento e força de trabalho, necessário para reduzir as lacunas.
Passo 7: Implementar plano de ação.	Ajustar práticas de segurança cibernética atuais, a fim de alcançar o perfil de destino. O framework identifica algumas referências informativas sobre as categorias e subcategorias. As organizações devem determinar quais padrões, normas e práticas podem ser usadas, incluindo aqueles que são específicos para cada setor do mercado.

O *framework* identifica algumas referências informativas sobre as categorias e subcategorias. As organizações devem determinar quais padrões, normas e práticas podem ser usadas, incluindo aqueles que são específicos para cada setor do mercado.

Para a construção dos passos 5, 6 e 7 do plano de implementação de gerência de acesso, apresentadas no quadro 4, é necessário conhecer as funções, categorias e subcategorias propostas pelo *framework core*.

Quadro 4 – Funções e categorias propostas no *framework core* (NIST, 2018).

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Ainda dentro de cada categoria existem subcategorias, que são subáreas do conhecimento que possuem recomendações de práticas e controles sugeridos por vários *frameworks* do mercado, servindo de apoio para a implementação do perfil de destino. Uma longa relação destas subcategorias com as recomendações de controles em forma de referências informativas podem ser encontrados no “apêndice A"do *framework core* (NIST, 2018). A gerência de identidade e acessos, está concentrada dentro da função *“protect”*, na categoria *“Identity Management and Access Control”*, cujo o identificador desta categoria é “PR.AC”. Atualmente conta com 7 subcategorias conforme o quadro 5.

Quadro 5 – Subcategorias da categoria: *Identity Management and Access Control* (NIST, 2018).

Identificador	**Descrição**
PR.AC-1	Identidades e credenciais são emitidas, obtidas, verificadas, revogadas e auditadas para dispositivos autorizados, usuários e processos.
PR.AC-2	O acesso físico a ativos é gerido e protegido.
PR.AC-3	O acesso remoto é gerenciado.
PR.AC-4	As permissões de acesso e autorizações são geridos, incorporando os princípios de privilégio mínimo e separação de funções.
PR.AC-5	A integridade da rede está protegido (por exemplo, a segregação de rede, a segmentação de rede).
PR.AC-6	As identidades são revisadas e vinculadas a credenciais e declaradas em interações.
PR.AC-7	Usuários, dispositivos e outros ativos são autenticados (por exemplo, fator único, multifator), proporcional ao risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais).

Como referências informativas, o *framework core* propõe controles de vários outros *frameworks* de mercado, conforme os quadros 6, 7 e 8. Dentre os *frameworks* referenciados existe o "NIST SP-800-53" - *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST, 2014), o qual foram observados os controles sugeridos para a implementação da IAM.

Quadro 6 – Subcategorias da catergoria PR.AC, *framework core* - parte 1 (NIST, 2018).

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Physical access to assets is managed and protected	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Remote access is managed	**CIS CSC** 12 **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1

Quadro 7 – Subcategorias da catergoria PR.AC, *framework core* - parte 2 (NIST, 2018).

Function	Category	Subcategory	Informative References
			NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	**CIS CSC** 9, 14, 15, 18 **COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9

Quadro 8 – Subcategorias da catergoria PR.AC, *framework core* - parte 3 (NIST, 2018).

Function	Category	Subcategory	Informative References
			ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

2.5 O FRAMEWORK NIST SP 800-53

Segundo o NIST, em sua 4ª revisão do NIST SP-800-53 (NIST, 2014):

> ...fornece um catálogo de controles de segurança e privacidade para os sistemas federais de informação e organizações e um processo para a seleção de controles para proteger as operações da organização (incluindo missão, funções, imagem e reputação), ativos da organização, os indivíduos, outras organizações, e a nação de um conjunto diversificado de ameaças, incluindo ataques cibernéticos, desastres naturais, falhas estruturais e erros humanos. Os controles são personalizáveis e implementado como parte de um processo para a organização que administra a segurança da informação e a privacidade (NIST, 2014).

Os controles são agrupados em famílias de controles dentro do *framework* SP-800-53. Cada família pode ser identificada pelo seu código "*ID*", formado por duas letras. O quadro 9 descreve as famílias de controles presentes no SP-800-53. Os controles por sua vez são identificados por números, de forma que podem ser referenciados pelo código da família seguido do número do controle dentro desta família, exemplo: AC-1, IA-2, AU-1.

Para a implementação de uma solução *Identity Management and Access Control*, o *framework core* recomenda vários *frameworks* de mercado. Para esse trabalho foi selecionado o *framework* NIST SP-800-53. O *framework core* já recomenda a avaliação de uma série de controles dentro das respectivas famílias do NIST SP-800-53.

Quadro 9 – Família de controles NIST SP-800-53 (NIST, 2014).

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Para a implementação de uma solução *Identity Management and Access Control*, o *framework core* recomenda a avaliação de uma série de controles dentro das respectivas famílias, conforme apresentado no quadro 10. Contudo, para a elaboração do "perfil de destino", alguns controles devem ser selecionados, para que seja possível a implementação gradual de perfis de segurança.

Quadro 10 – Subcategorias da categoria: *Identity Management and Access Control* (NIST, 2018).

Identificador	**Descrição**	**Controles**
PR.AC-1	Identidades e credenciais são emitidas, obtidas, verificadas, revogadas e auditadas para dispositivos autorizados, usuários e processos.	• AC-1, 2 • AI-1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
PR.AC-2	O acesso físico a ativos é gerido e protegido.	• PE-2, 3, 4, 5, 6, 8
PR.AC-3	O acesso remoto é gerenciado.	• AC-1, 17, 19, 20 • SC-15
PR.AC-4	As permissões de acesso e autorizações são geridos, incorporando os princípios de privilégio mínimo e separação de funções.	• AC-1, 2, 3, 5, 6, 14, 16, 24
PR.AC-5	A integridade da rede está protegido (por exemplo, a segregação de rede, a segmentação de rede).	• AC-4, 10 • SC-7
PR.AC-6	As identidades são revisadas e vinculadas a credenciais e declaradas em interações.	• AC-1, 2, 3, 16, 19, 24 • IA-2, 4, 5, 8 • PE-2 • PS-3
PR.AC-7	Usuários, dispositivos e outros ativos são autenticados (por exemplo, fator único, multifator), proporcional ao risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais).	• AC-7, 8, 9, 11, 12, 14 • IA-1, 2, 3, 4, 5, 8, 9, 10, 11

Os controles do *framework* NIST SP-800-53 são detalhados no "apêndice F - *Security Control Catalog*" deste framework, onde um catálogo de controles de segurança fornece uma série de salvaguardas e contramedidas para organizações e sistemas de informação.

Foram projetados 105 controles de segurança para facilitar a conformidade com as leis federais aplicáveis, ordens executivas, diretrizes, políticas, regulamentos, normas e diretrizes (NIST, 2014). Os controles de segurança no catálogo, com poucas exceções, foram projetados para serem neutros em termos de política e tecnologia, conforme pode ser observado na figura 3.

Figura 3 – Exemplo de controle proposto pelo NIST SP-800-53 (NIST, 2014).

FAMILY: ACCESS CONTROL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

   1. Access control policy [*Assignment: organization-defined frequency*]; and

   2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AC-1	**MOD** AC-1	**HIGH** AC-1

2.6 FREEIPA

O FreeIPA é uma solução integrada de identidade e autenticação para ambientes de rede Linux/UNIX (FREEIPA.ORG, 2021). Um servidor FreeIPA fornece informações centralizadas de autenticação, autorização e conta, armazenando dados sobre usuários, grupos, hosts e outros objetos necessários para gerenciar os aspectos de segurança de uma rede de computadores (FREEIPA.ORG, 2021). O FreeIPA é construído sobre componentes conhecidos de código aberto e protocolos padrões, com um foco na facilidade de gerenciamento e automação das tarefas de instalação e configuração. O FreeIPA é uma solução integrada de gerenciamento de informações de segurança que combina Linux, 389 Directory Server, MIT Kerberos, NTP, DNS e Dogtag (sistema de certificação). Consiste em uma interface da web e ferramentas de administração de linha de comando (FREEIPA.ORG, 2021).

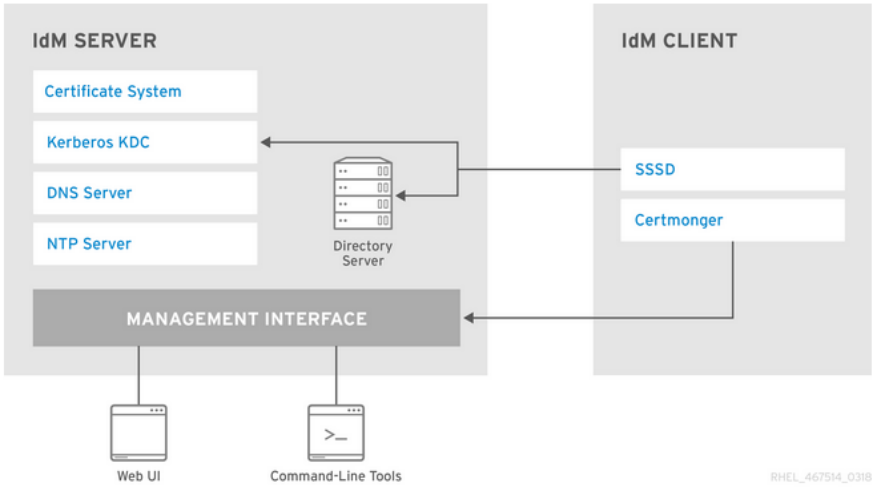
Desde a versão 6.4, o Red Hat Enterprise Linux - RHEL incluiu o conjunto de recursos de Gerenciamento de Identidade (*Identity Management - IdM*) para fornecer uma maneira clara e centralizada de gerenciar identidades de usuários, máquinas e serviços em grandes ambientes empresariais Linux/Unix. Além disso, o IdM oferece uma maneira de definir políticas de controle de acesso para gerir essas identidades. O IdM fornece acesso unificado para serviços de rede comuns definidos por padrões, incluindo PAM, LDAP, Kerberos, DNS, NTP e serviços de certificado, com base no trabalho realizado na comunidade de código-fonte aberto FreeIPA (projeto *upstream* do IdM) (NEWLANDS, 2014). Segundo a documentação do IdM (MUEHLFELD et al., 2019) que utiliza-se do FreeIPA para sua construção em modelo de comunidade e parceria com a Red Hat, apresentada na figura 4, os principais serviços oferecidos na solução do IdM/FreeIPA são:

- **Kerberos KDC**: Utiliza o protocolo Kerberos para oferecer suporte à conexão única. Com o Kerberos, o usuário precisa apenas apresentar o nome de usuário e a senha corretos uma vez. O usuário recebe um *ticket* que valida os acessos durante um intervalo de tempo determinado. Permite acesso aos serviços do IdM/FreeIPA sem solicitação de credenciais enquanto o *ticket* for válido.
- **Servidor de diretório LDAP**: Inclui uma instância interna do servidor de diretório LDAP, na qual armazena todas as informações do IdM/FreeIPA, como informações relacionadas ao Kerberos, contas de usuário, entradas de host, serviços, políticas, DNS e outros.
- **Autoridade de certificação (CA)**: Na maioria das implantações, uma autoridade de certificação integrada (CA) é instalada com o servidor IdM/FreeIPA. Também pode instalar o servidor sem a CA integrada, se criar e fornecer todos os certificados necessários independentemente.
- **Sistema de Nome de Domínio (DNS)**: Utiliza o DNS para descoberta dinâmica de serviços. O utilitário de instalação do cliente IdM/FreeIPA pode usar informações do DNS para configurar automaticamente a máquina cliente. Depois que o cliente é registrado no domínio do IdM/FreeIPA, ele usa o DNS para localizar servidores e

serviços do IdM/FreeIPA dentro do domínio.

- **Protocolo de tempo de rede (NTP)**: Muitos serviços exigem que servidores e clientes tenham o mesmo horário do sistema, dentro de uma certa variação. Por exemplo, os *tickets* Kerberos usam carimbos de data e hora (*timestamps*) para determinar sua validade e impedir ataques de reprodução. Se os horários entre o servidor e o cliente se desviarem do intervalo permitido, os *tickets* Kerberos serão invalidados.
- **O System Security Services Daemon (SSSD)**: é um aplicativo do lado do cliente para armazenar credenciais em cache. É recomendável usar o SSSD em máquinas clientes, pois simplifica a configuração do cliente necessária. O SSSD também fornece recursos adicionais, por exemplo:
  - Autenticação de cliente offline, garantida por armazenamento em cache de credenciais de armazenamento centralizado de identidade e autenticação local.
  - Consistência aprimorada do processo de autenticação, porque não é necessário manter uma conta central e uma conta de usuário local para autenticação offline.
  - Integração com outros serviços, como sudo.
  - Autorização de controle de acesso baseado em host (HBAC).
  - Com o SSSD, os administradores do IdM/FreeIPA podem definir todas as configurações de identidade centralizadas no servidor do IdM/FreeIPA. O armazenamento em cache permite que o sistema local continue as operações normais de autenticação se o servidor do IdM/FreeIPA ficar indisponível ou se o cliente ficar offline.
- **Certmonger**: O serviço do certmonger monitora e renova os certificados no cliente. Pode solicitar novos certificados para os serviços no sistema.

Figura 4 – Comunicação entre os serviços do IdM/FreeIPA (MUEHLFELD et al., 2019)



3 SOLUÇÃO PROPOSTA

Neste capítulo serão apresentadas maiores informações sobre o problema ao qual o projeto procura solucionar, bem como apresentar a implementação da solução escolhida para avaliação da gestão centralizada de identidades e acesso, o FreeIPA.

3.1 DESCRIÇÃO DO PROBLEMA

O mercado já possui soluções e metodologias bem consolidadas para a gestão de identidades e acessos, segmento conhecido como IAM (*Identity and Access Management* – Gerenciamento de identidades e acessos). Segundo o Gartner:

> O gerenciamento de identidades e acessos (IAM) é a disciplina que permite que as pessoas certas acessem os recursos certos nos momentos certos pelas razões certas (GARTNER, 2017) (GARTNER, 2017).

Segundo a Hitachi (HITACHI, 2017):

> O gerenciamento de identidades e acessos corporativo (IAM) é definido como um conjunto de processos e tecnologias para gerenciar de maneira eficaz e consistente números modestos de usuários e direitos em vários sistemas. Nesta definição, normalmente há menos de um milhão de usuários, mas os usuários normalmente têm acesso a vários sistemas e aplicativos. (HITACHI, 2017).

O IAM refere-se à nomeação e autenticação de entidades e à atribuição e atualização de seus direitos de autorização para os computadores e sistemas de rede de uma empresa. Amplamente reconhecido como uma tarefa de TI essencial e crescente, foi profundamente influenciado pelo desenvolvimento de modelos de gerenciamento de acesso, como Controle de Acesso Baseado em Função (*Role Based Access Control* - RBAC), Gerenciamento de Confiança Descentralizado (*Decentralized Trust Management* - DTM) e Controle de Acesso Baseado em Atributo (*Atribute-Based Access Control* - ABAC). Esses e outros modelos semelhantes aprimoraram a eficiência do gerenciamento e permitiram novos níveis de automação (GUNTER; LIEBOVITZ; MALIN, 2011).

Os riscos de acessos a ambientes críticos estão diretamente relacionados a capacidade de controlar os seu acessos. A Microsoft possui a solução Active Directory, uma implementação do diretório padrão da Internet e dos protocolos de nomenclatura, que usa um mecanismo de banco de dados para suporte transacional e suporta uma variedade de padrões de interface de programação de aplicativos (MICROSOFT DOCS, 2011). O Active Directory oferece centralização de atividades, o que simplifica a gestão de identidades e acessos destes ambientes. Entretanto, sistemas baseados em GNU/Linux muitas vezes são negligenciados e possuem gestão precária de controle de acesso. Geralmente utilizam a segurança nativa descentralizada oferecidas por padrão na distribuição. Por isso o *framework for Improving Critical Infrastructure Cybersecurity* - NIST e o *framework* NIST SP 800-53, foram adotados como guias de referência de boas práticas para a solução proposta.

3.2 IMPLEMENTAÇÃO DO IAM

O *framework for Improving Critical Infrastructure Cybersecurity* - NIST e o *framework* NIST SP 800-53, foram adotados como guias de referência de boas práticas. Amplamente adotados pelo mercado, foram utilizados como linha de base para a elaboração de um plano de gerenciamento de identidades e acessos. O principal objetivo deste trabalho é a implementação da gerência de identidades e acessos, tendo em vista que segundo o NIST:

> O *framework for Improving Critical Infrastructure Cybersecurity*, pode auxiliar com abordagens para identificação, autenticação, e autorização de indivíduos para acessar os ativos e sistemas organizacionais - sejam tomadas medidas para identificar e abordar as implicações de privacidade de gerenciamento de identidade e medidas de controle de acesso na medida em que elas envolvem coleta, divulgação ou uso de informações pessoais (NIST, 2018).

Com base nas informações obtidas, foi avaliada a aderência da ferramenta FreeIPA no processo de implementação da gerência de identidades e acessos (IAM), voltada para controle de ambientes de servidores GNU/Linux, substituindo assim o gerenciamento local realizado individualmente em cada servidor, quanto a liberação e concessão de acessos e privilégios.

Como estratégia, foram levantadas algumas necessidades importantes para o sucesso da implementação do IAM, e os *frameworks* do NIST foram fundamentais para identificação de pontos relevantes nesta implementação. Tomando como referência a possibilidade de escolha entre os três componentes do *Framework for Improving Critical Infrastructure Cybersecurity* para a produção deste trabalho, foi adotado o uso do *framework profile*.

Fazendo uso do *framework profile* no cenário proposto, a organização pode selecionar os controles relevantes para o perfil de destino, criando assim um perfil personalizado.

A construção de um plano de segurança cibernética para toda organização está fora do escopo deste trabalho, portanto apenas algumas das etapas sugeridas pelo *framework core* foram priorizadas para o desenho do plano simplificado, conforme descrito na quadro 11.

Quadro 11 – Plano de segurança simplificado segundo recomendação NIST (NIST, 2018).

Fase	**Descrição**
Passo 1: Priorizar e escopo.	A grande maiorias das organizações precisam proteger os seus dados. Medidas para esse controle são relevantes para a missão de qualquer organização na era da tecnologia da informação.
Passo 2: Orientação.	Os servidores hospedados no datacenter devem estar protegidos contra acesso de pessoas não autorizadas.
Passo 3: Criar um perfil atual.	No perfil atual, o ambiente possui apenas controle de acesso nativo oferecidos pelos sistemas GNU/Linux baseados em PAM, de forma descentralizada, sem nenhum processo, controle e gestão claramente definidos.
Passo 4: Realizar uma avaliação de riscos.	O ambiente possui colaboração de parceiros técnicos que possuem rotatividade de pessoal, fora do controle da organização contratante. A organização necessita de maiores controles de segurança na gestão de identidades e acessos.
Passo 5: Criar um perfil de destino.	O perfil de destino deve contemplar uma série de categorias e subcategorias que atendam aos requisitos de segurança, que contemplem a gerência de identidades e acessos (objetivo principal deste trabalho).
Passo 6: Determinar, analisar, priorizar lacunas.	A implementação de gerência de identidades e acessos é fundamental para a redução de uso não autorizado de ativos estratégicos, reduzindo todo impacto de exploração de acessos.
Passo 7: Implementar plano de ação.	Seleção de categorias e subcategorias que estão relacionadas a implementação de gerenciamento de identidades e acessos, bem como selecionar padrões de mercado, normas, práticas e controles sugeridos pelo *framework core*, de forma a se adequar ao perfil de destino desejado.

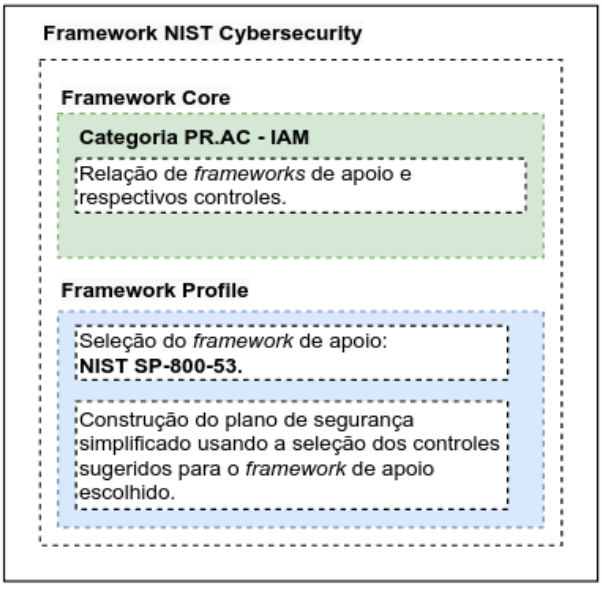
Para a construção dos passos 5, 6 e 7 do plano de segurança simplificado, que são os passos diretamente relacionados com a criação de perfil, priorização e implementação, foram necessários *frameworks* de apoio para oferecer os controles para implementação dos níveis de segurança desejados. Como referências informativas, o *framework core*, presente no *framework Improving Critical Infrastructure Cybersecurity*, propõe controles de vários outros *frameworks* de mercado como apoio, conforme as figuras 6, 7 e 8. Dentre os *frameworks* referenciados, o adotado foi o NIST SP-800-53 - *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST, 2014), o qual foram observados os controles sugeridos para a implementação da IAM. O NIST SP-800-53 reúne diversos controles, contudo, para a elaboração do perfil de destino, apenas alguns controles foram selecionados, para que seja possível a implementação gradual de perfis de segurança, dentro do objetivo de implementação do IAM conforme mostra o quadro 12.

Quadro 12 – Controles selecionados da subcategoria PR.AC-1 segundo recomendação do *framework core* (Autor, 2021).

Subcategoria	**Controles**
PR.AC-1: Identidades e credenciais são emitidas, obtidas, verificadas, revogadas e auditadas para dispositivos autorizados, usuários e processos.	• PR.AC-1/AC-1: *Access Control Policy and Procedures* • PR.AC-1/AC-2: *Account Management* • PR.AC-1/AI-1: *Identification and Authentication Policy and Procedures* • PR.AC-1/AI-2: *Identification and Authentication (Organizational Users)* • PR.AC-1/AI-3: *Device Identification and Authentication* • PR.AC-1/AI-4: *Identifier Management* • PR.AC-1/AI-5: *Authenticator Management* • PR.AC-1/AI-6: *Authenticator Feedback* • PR.AC-1/AI-7: *Cryptographic Module Authentication* • PR.AC-1/AI-8: *Identification and Authentication (Non-Organizational Users)* • PR.AC-1/AI-9: *Service Identification and Authentication* • PR.AC-1/AI-10: *Adaptive Identification and Authentication* • PR.AC-1/AI-11: *Re-authentication*

Portanto a figura 5 apresenta a relação entre o *Framework for Improving Critical Infrastructure Cybersecurity*, o *framework core*, o *framework profile* e o *framework* NIST SP 800-53.

Figura 5 – Relação entre os *frameworks* utilizados no trabalho (Autor, 2021).



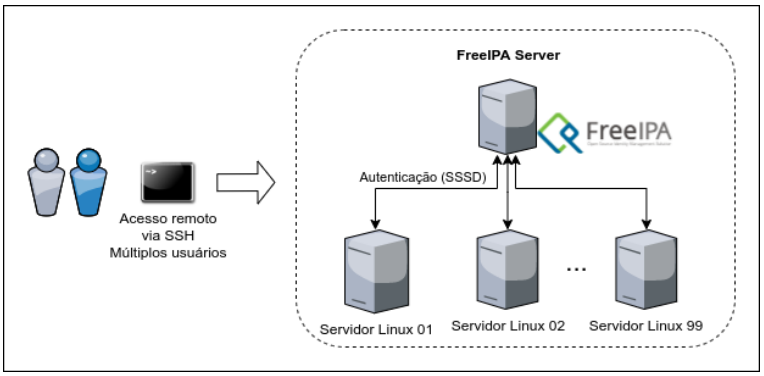
Dentro das categorias de controles ofertados para IAM pelo *framework* NIST SP-800-53, em suas subcategorias, ainda existem os aprimoramentos de controle, que são controles ainda mais refinados dentro de cada subcategoria. Como o objetivo é implementar a gestão centralizada de acesso aos servidores GNU/Linux, muitos controles não se aplicam ao contexto e por isso não foram implantados.

Outros controles são importantes, porém não são basilares. O principal critério para a aplicação da análise destinadas aos controles essenciais, é sua relação com os processos de identificação, autenticação e autorização necessários para a gestão de acessos aos servidores GNU/Linux. Portanto das principais categorias sugeridas pelo *framework* NIST SP-800-53, a categoria com maior relevância foi a PR.AC-1, onde serão visitadas as principais subcategorias para concentração da análise dedicada a estes controles.

3.2.1 Configuração do servidor FreeIPA

A figura 6 representa a arquitetura dos servidores no fornecimento de acesso remoto aos servidores Linux com a autenticação centralizada.

Figura 6 – Arquitetura dos servidores - acesso remoto utilizando o FreeIPA (Autor, 2021).



Para a implementação da solução de gerenciamento de identidades e acessos, como prova de conceito, serão utilizadas duas máquinas: servidor FreeIPA para autenticação centralizada e um cliente. Serão usados duas distribuições GNU/Linux diferentes de maior utilização em ambientes corporativos: CentOS e Ubuntu. As configurações utilizadas nestes servidores podem ser visualizadas no quadro 13.

Neste cenário, o servidor FreeIPA será implementado no CentOS. Antes de iniciar o processo de instalação, é necessário atualizar os pacotes da distribução utilizada conforme o comando abaixo:

```
# yum upgrade -y
```

A solução do FreeIPA utiliza o ntpd como serviço de sincronização de horários entre os servidores. Por isso é necessário que o chronyd seja desabilitado com os comandos abaixo:

```
# systemctl stop chronyd
# systemctl disable chronyd
```

Quadro 13 – Configurações dos servidores (Autor, 2021).

Servidor FreeIPA	**Cliente autenticação centralizada**
• Papel: Servidor freeipa • Servidor Linux: CentOS 7 • Servidor virtual: VirtualBox • Memória RAM: 2GB • Disco rígido: 10 GB • Nome do servidor: freeipa • Domínio: lab.net • Endereço IP: 192.168.15.100/24 • Gateway: 192.168.15.1/24 • Nameserver: 8.8.8.8	• Papel: Cliente • Servidor Linux: Ubuntu 20.04 LTS • Servidor virtual: VirtualBox • Memória RAM: 2GB • Disco rígido: 10 GB • Nome do servidor: cliente01 • Domínio: lab.net • Endereço IP: 192.168.15.101/24 • Gateway: 192.168.15.1/24 • Nameserver: 8.8.8.8

Para a instalação do FreeIPA foram utilizados os comandos:

```
# yum install ipa-server ipa-server-dns -y
```

Para o sucesso da configuração é necessário que o nome DNS da máquina seja resolvido para o endereço IP, do mesmo modo que o endereço IP seja resolvido reversamente para o mesmo nome de máquina, caso contrário podem surgir problemas com as gerações de certificados durante a configuração de novos clientes. Exemplo:

```
# hostnamectl set-hostname freeipa.lab.net
# hostname
```

Realizar o *logoff* do usuário e novo *login*. Reiniciar a máquina caso tenha problemas ao obter a sessão como novo nome do servidor.

Configurar a consulta de DNS nesta etapa é muito importante e deve ser realizada logo após a conclusão da instalação de todos os pacotes. Isso exige um endereço de DNS válido. Configurar para que as consultas de DNS sejam reliazadas para a própria máquina (127.0.0.1). Essa configuração será utilizada pois o FreeIPA irá implementar um serviço de DNS e deve consultar DNS localmente em si mesmo ao término da configuração.

```
# cat /etc/resolv.conf
# Generated by NetworkManager
search lab.net
nameserver 127.0.0.1
```

Configure o arquivo hosts para que o nome do seja resolvido localmente:

```
# vi /etc/hosts
192.168.15.100   freeipa.lab.net  freeipa
```

Verifique se a resolução de nomes está funcionando com o apoio do comando ping:

```
# ping -c1 freeipa.lab.net
```

A configuração do servidor FreeIPA pode ser realizada em "modo *prompt*"onde são questionados os valores para cada parâmetro, ou na opção direta, onde todos os parâmetros e argumentos são fornecidos na linha de comando, conforme descrito a seguir:

```
# ipa-server-install -a "redhat@1" --hostname=freeipa.lab.net -r LAB.NET \
  -p redhat@1 -n lab.net -U --setup-dns --forwarder=8.8.8.8
```

Com a conclusão da configuração do FreeIPA, será apresentada a seguinte informação:

```
Setup complete
Next steps:
        1. You must make sure these network ports are open:
                TCP Ports:
                  * 80, 443: HTTP/HTTPS
                  * 389, 636: LDAP/LDAPS
                  * 88, 464: kerberos
                  * 53: bind
                UDP Ports:
                  * 88, 464: kerberos
                  * 53: bind
                  * 123: ntp

        2. You can now obtain a kerberos ticket using the
           command: 'kinit admin'. This ticket will allow
           you to use the IPA tools (e.g., ipa user-add)
           and the web user interface.

Be sure to back up the CA certificates stored in /root/cacert.p12
These files are required to create replicas. The password for these
files is the Directory Manager password
```

Por fim, reiniciar o serviço de SSH:

```
# systemctl restart sshd
```

Se tudo ocorreu bem, será possível realizar a criação de um ticket kerberos utilizando as credenciais usada na instalação do FreeIPA com o comando kinit:

```
# kinit admin
Password for admin@LAB.NET: ********

# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@LAB.NET
Valid starting       Expires              Service principal
02/10/2021 21:39:08  02/11/2021 21:39:04  krbtgt/LAB.NET@LAB.NET
```

De posse de um *ticket* Kerberos ativo, gerado na etapa anterior, consulte a existência do usuário "admin"criado durante a configuração do FreeIPA:

```
# ipa user-find admin
```

```
--------------
1 user matched
--------------
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@LAB.NET
  UID: 1233600000
  GID: 1233600000
  Account disabled: False
----------------------------
Number of entries returned 1
----------------------------
```

Para testes rápidos, desabilitar o serviço firewalld conforme o comando a seguir:

```
# systemctl stop firewalld
# systemctl disable firewalld
```

Se todas as configurações ocorreram corretamente, será possível ativar o firewall e adicionar as liberações de portas conforme informado na notificação de conclusão da configuração do FreeIPA. Para que serviço FreeIPA esteja ativo na inicialização utilize o comando:

```
# systemctl enable ipa
```

Para consultar o status de todos os serviços do FreeIPA:

```
# ipactl status
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmin Service: RUNNING
named Service: RUNNING
httpd Service: RUNNING
ipa-custodia Service: RUNNING
ntpd Service: RUNNING
pki-tomcatd Service: RUNNING
ipa-otpd Service: RUNNING
ipa-dnskeysyncd Service: RUNNING
ipa: INFO: The ipactl command was successful
```

3.2.2 Ingressando um cliente no FreeIPA

Com o servidor FreeIPA implementado corretamente, o sistema está apto para receber novos clientes para a gerência centralizada de identidade e acessos gerenciados pelo FreeIPA.

As operações com FreeIPA precisam que exista a resolução de nomes. Caso não exista um serviço de DNS que resolva o nome do servidor na rede, pode ser utilizado o arquivo /etc/hosts para esta função, tanto para o servidor como para o cliente. Também é possível configurar o

FreeIPA para ser um servidor de DNS, sendo esta funcionalidade adotada durante a instalação do FreeIPA server. Observe as consultas de DNS realizadas para o servidor do FreeIPA:

```
dcastelob@cliente01:~$ nslookup freeipa.lab.net
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
*** Can't find freeipa.lab.net: No answer

dcastelob@cliente01:~$ nslookup freeipa.lab.net 192.168.15.100
Server:         192.168.15.100
Address:        192.168.15.100#53

Name:   freeipa.lab.net
Address: 192.168.15.100
```

Também configure o *nameserver* para realizar consultas no FreeIPA. As definições de rede no Ubuntu 20.04 são realizadas usando o serviço netplan e suas configurações foram realizadas no arquivo de configuração /etc/netplan/enp0s3.yaml:

```
# vi /etc/netplan/enp0s3.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses:
      - 192.168.15.101/24
      nameservers:
        addresses:
          - 192.168.15.100
      routes:
      - to: 0.0.0.0/0
        via: 192.168.15.1
        metric: 100

# netplan applay
```

Ao consultar novamente o nome FQDN, o seguinte resultado é apresentado:

```
dcastelob@cliente01:~$ nslookup freeipa.lab.net
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   freeipa.lab.net
Address: 192.168.15.100
```

Certifique-se também de que a definição de zona de horário (*timezone*) do servidor e do cliente estão igualmente configuradas. Diferenças mínimas de horário impedem o ingresso de novos clientes ao servidor FreeIPA:

```
# timedatectl set-timezone America/Recife

# timedatectl
               Local time: Thu 2021-02-11 11:52:27 -03
           Universal time: Thu 2021-02-11 14:52:27 UTC
                 RTC time: Thu 2021-02-11 14:52:28
                Time zone: America/Recife (-03, -0300)
System clock synchronized: yes
              NTP service: inactive
          RTC in local TZ: no

# date
Thu Feb 11 11:52:30 -03 2021
```

Ajuste o arquivo hosts para apresentar o nome FQDN:

```
# vi /etc/hosts
127.0.0.1 localhost
192.168.15.101 cliente01.lab.net        cliente01
```

Em seguida, testar a consulta do nome do servidor local:

```
# hostname -f
cliente01.lab.net
# hostname
cliente01
```

Por fim, instale os pacotes do cliente FreeIPA:

```
# apt-get install -y freeipa-client
```

Com os requisitos de rede atendidos, finalmente é possível ingressar o cliente01 no servidor FreeIPA. Esta operação pode ser realizada sem interação (silenciosamente). Observe as saídas apresentadas no comando, elas podem apontar alguns problemas que precisam ser solucionandos antes do ingresso no FreeIPA:

```
$ ipa-client-install -p admin -w "redhat@1" --domain=lab.net \
 --realm LAB.NET --server=freeipa.lab.net --mkhomedir \
 --unattended --force-join
```

Ao término da configuração é apresentada uma mensagem de sucesso:

```
Client configuration complete.
```

3.2.3 Acessando a interface de gerência do FreeIPA

Dentre todos os componentes de administração do FreeIPA, alguns são os mais importantes para este trabalho, são eles: a administração de *Users* (Usuários), *Hosts* (Máquinas), *Policy*

HABC (Politíca de HBAC) e a *Policy sudo* (Política de sudo).

a) *Users (Usuários)*: Administração de usuários que podem fazer uso da gerência de autenticação centralizada. Neste conjunto, entre outras configurações, chaves RSA podem ser definidas para configuração de SSH via chaves assimétricas.
b) *Hosts (Máquinas)*: Administração de máquinas que participam da gerência centralizada. Ao possuir o controle dos hosts, é possivel definir o controle de acesso a cada hosts usando as políticas de HBAC.
c) *Policy HABC (Política HBAC)*: *Host-Based Access Control* (HBAC) permite que sejam definidas políticas que controlam o acesso a hosts ou serviços com base nos acessos de usuários, grupos de usuários, grupos de hosts e (opcionalmente) o serviço que está sendo acessado.
d) *Policy sudo (Política de sudo)*: Destinado a gestão das configurações de sudo que podem atribuir acessos administrativos a determinados comandos de administração ou mesmo administração total com elevação de privilégios do usuário.

Para realizar o acesso ao endereço da console web do FreeIPA, não há uma entrada de DNS na rede local. Para contornar esta situação pode ser configurado o endereço IP do Freeipa no arquivo hosts ("/etc/hosts") da máquina local que vai utilizar o navegador para acessar a interface web de gerência do FreeIPA.

```
# vi /etc/hosts
192.168.15.100  freeipa.lab.net
```

O FreeIPA já possui um usuário "admin"cuja senha foi definida no momento do provisionamento do serviço. O acesso pode ser realizado usando essas credenciais pela console web de administração "https://freeipa.lab.net", conforme figura 7. Neste caso, já é possível visualizar todas as configurações disponíveis no FreeIPA, bem como visualizar os usuários existentes conforme a figura 8 e hosts presentes na solução conforme mostra a figura 9.

Figura 7 – Login da interface de gerência do FreeIPA (Autor, 2021).

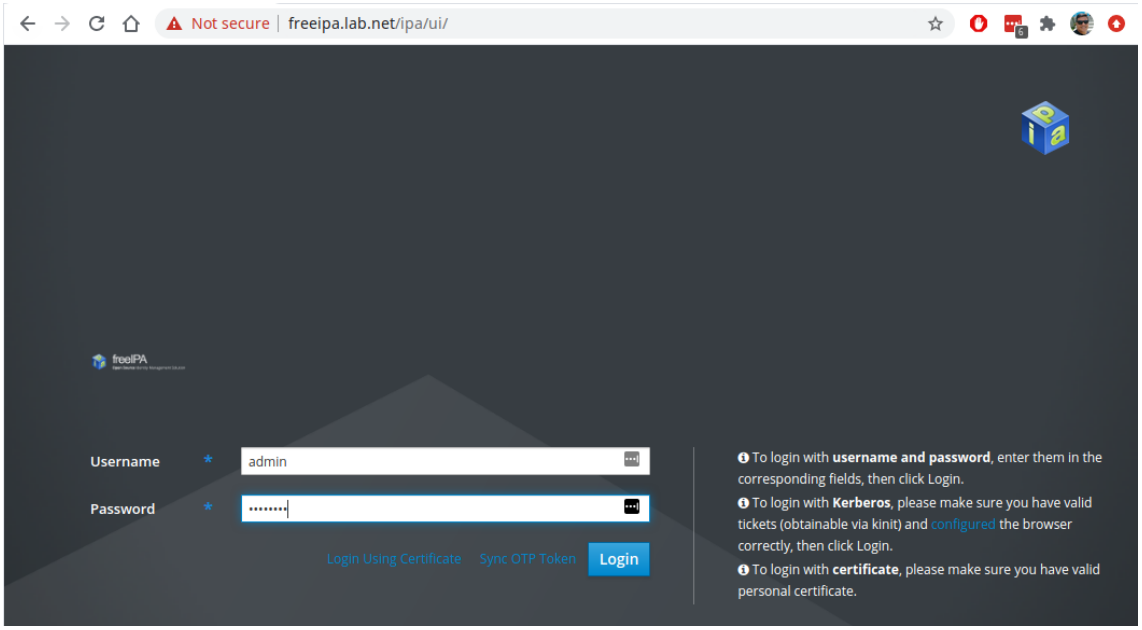


Figura 8 – Visualização de usuários do FreeIPA (Autor, 2021).

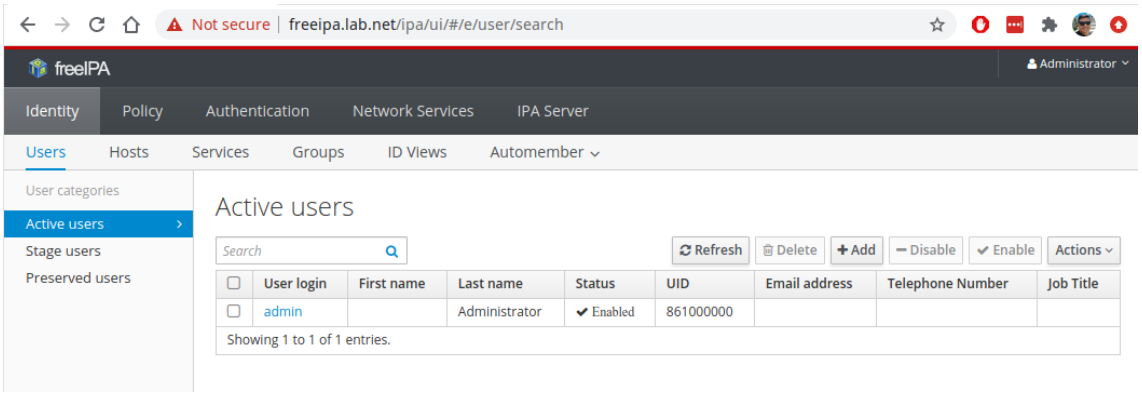
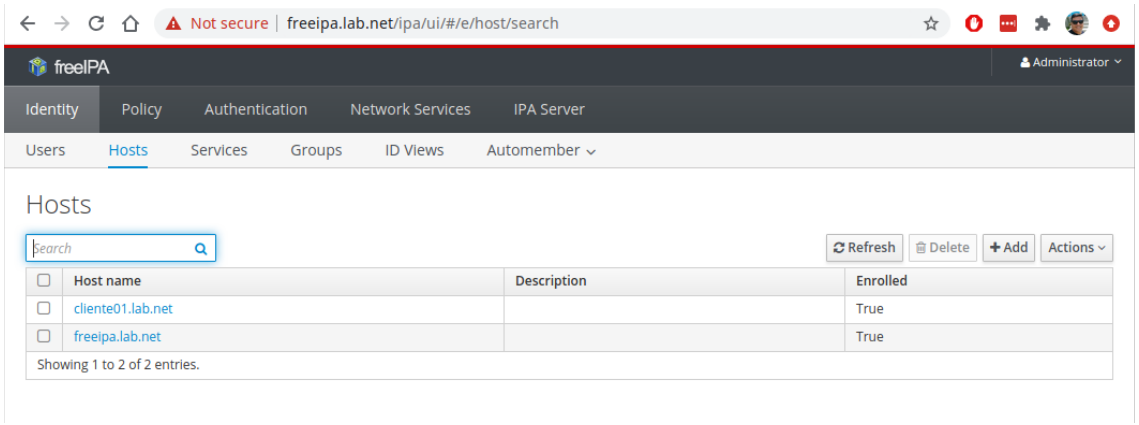


Figura 9 – Visualização de hosts do FreeIPA (Autor, 2021).



3.2.4 Configuração da gerência de usuários e acessos

Este é o alvo principal do trabalho onde serão implementados os mecanismos de gerência de usuários. Para isso, são necessárias algumas ações no FreeIPA:

a) Cadastrar usuário;
b) Gerar um par de chaves simétricas para o usuário;
c) Atualizar os dados do usuário para incluir a chave pública usada no acesso SSH;
d) Cadastrar host(s);
e) Criar grupo de hosts (para simplificar o acesso quando oportuno);
f) Cadastrar política HBAC autorizando que um usuário/grupo tenha acesso ao host ou grupo de host;

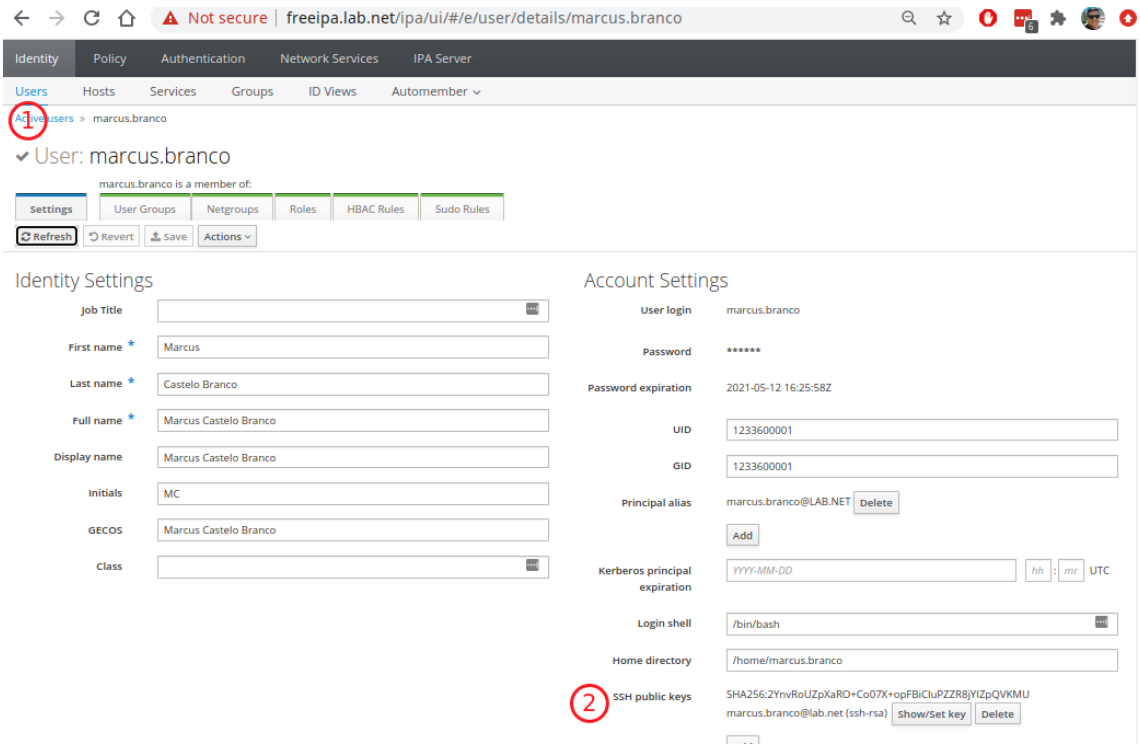
Foi realizado o acesso usando apenas as credenciais (login e senha) definidos no FreeIPA com sucesso. No entanto para aumentar a segurança no controle de acesso foi configurado o uso de chaves para conexão via SSH.

Criando uma chave RSA para uso na conexão SSH. A chave pública (*.pub) deve ser cadastrada no perfil do usuário conforme apresentado na figura 10.

```
$ ssh-keygen -t rsa -b 2048 -C marcus.branco@lab.net \
  -f .ssh/marcus.branco.freeipa

$ cat .ssh/marcus.branco.freeipa.pub
ssh-rsa AAAAB3NzaC1yc2EAA...
... zKDayUAABiN6YcSW2v/d+NV marcus.branco@lab.net
```

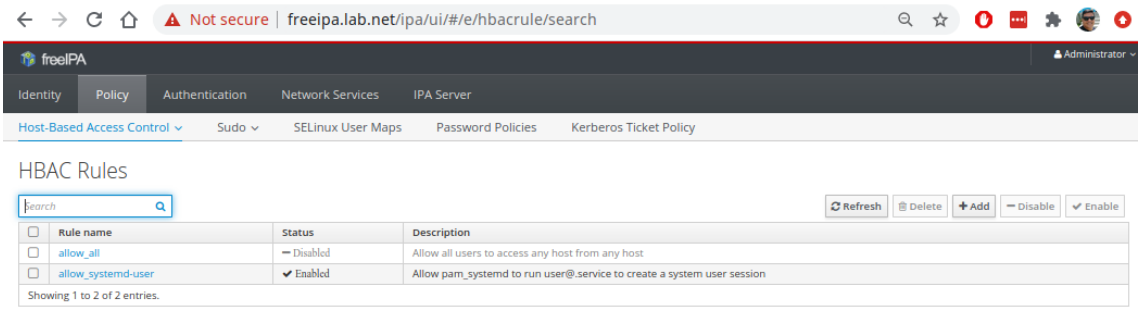
Figura 10 – Incluindo chave pública SSH para usuário no FreeIPA (Autor, 2021).



Até o presente momento, o usuário "marcus.branco"foi criado e pode fazer uso de sua chave SSH, mas seu acesso ainda não foi autorizado para os servidores. Por padrão o FreeIPA permite que todos os usuários criados tenham acesso aos servidores, devido a existência da *Policy HBAC allow_all* criada por padrão para evitar problemas logo no primeiro contato com

o serviço. Esse comportamento não é desejado e portanto será ajustado para um controle de acesso mais restritivo. Para isso é necessário desativar a política HBAC "*allow_all*"conforme apresentado na figura 11.

Figura 11 – Desativando a política HBAC allow-all no FreeIPA (Autor, 2021).



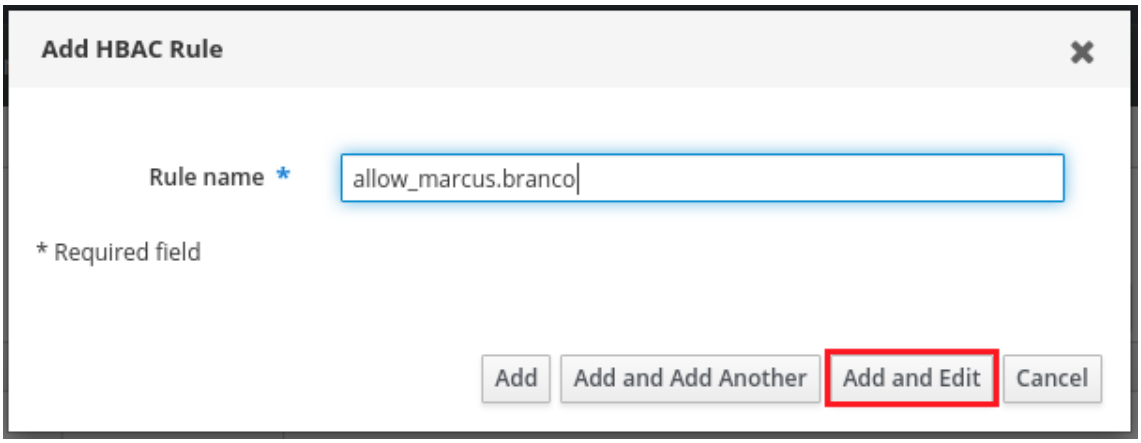
3.2.5 Configuração de políticas HBAC

Para realizar a liberação de acesso é utilizada uma "política de HBAC". Acesse a "*Policy*", em seguida "HBAC"e clique em "[*add*]". Com isso será aberto um formulário para criação de política. Utilize a opção "[*add and edit*]"que salva e encaminha para edição da política, conforme apresentado na figura 12.

Dentre as opções oferecidas estão as seguintes configurações:

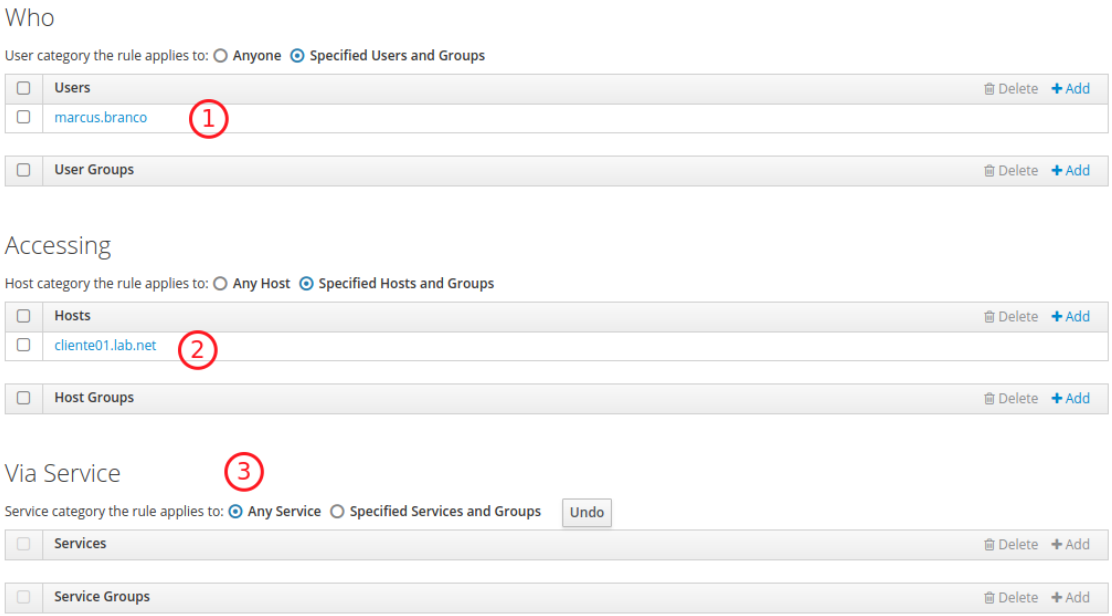
1. ***Who***: Quais usuários ou grupos serão incluídos nessa *HBAC policy*;
2. ***Accessing***: Quais servidores ou grupos de servidores serão disponibilizados para a *policy*;
3. ***Via Service***: Especifique o tipo de serviço de autenticação que pode ser usado. É recomendado todos os serviços mesmo que somente seja utilizado o SSHD.

Figura 12 – Criando política HBAC no FreeIPA (Autor, 2021).



Conforme descrito na figura 13, foi liberado o acesso do usuário marcus.branco ao host client01.lab.net utilizando quaisquer mecanismos de autenticação. Após a tentativa de acesso utilizando chaves RSA, a conexão SSH foi estabelecida com sucesso.

Figura 13 – Definindo acessos na política HBAC no FreeIPA (Autor, 2021).

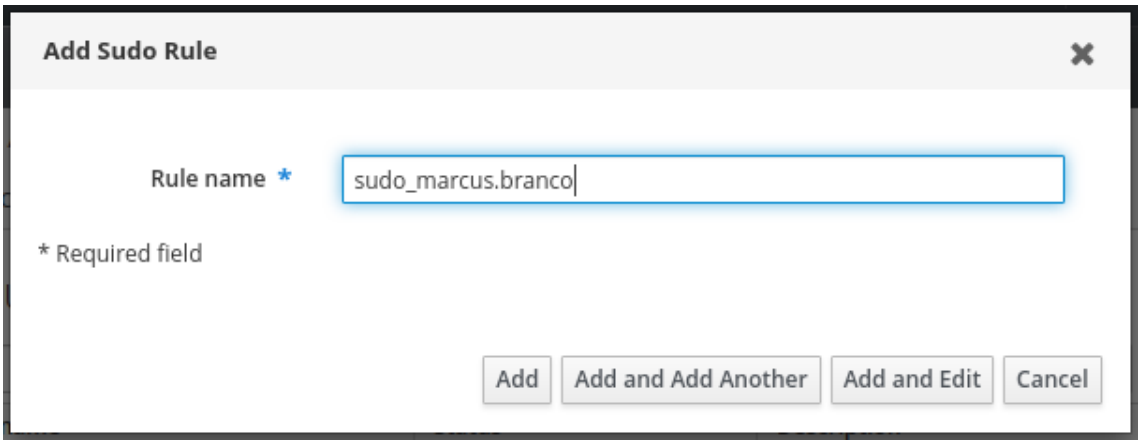


3.2.6 Configuração de políticas de sudo

Uma vez configurada a política de acesso do usuário através da política de HBAC, para autorizar a execução de comandos administrativos é necessário também a criação de uma "*policy* para os usuários sudo. Com o uso de políticas sudo é possivel elevar os privilégios dos usuários para execução de comandos administrativos, ou até mesmo a elevação total de privilégios, executando comandos como super-usuário.

De forma semelhante a criação da política HBAC, é necessário criar e editar a nova política para usuários sudo, conforme apresentado na figura 14.

Figura 14 – Definindo acessos na política sudo no FreeIPA (Autor, 2021).



Dentre as opções oferecidas na política para usuários sudo, existem as seguintes configurações:

1. ***Who***: Quais usuários ou grupos serão incluídos nesta *sudo policy*;
2. ***Options***: Permite definir opções suportadas pelo sudo. Uma delas é a possibilidade de não solicitar revalidação de senha: !authenticate;
3. ***Access this host***: Quais serviços serão liberados para acesso aos hosts ou grupos de hosts;
4. ***Run Commands***: Quais os comandos o (usuário) sudo poderá executar. Como recomendação inicial, adote a opção "*any commands*", que autoriza a execução de todos os comandos;
5. ***As Whom***: Essa função permite restringir possibilidade de execução de comandos como outros usuários. Como recomendação inicial utilizar "*anyone*" e "*any group*" respectivamente.

Foi configurada uma política que permite elevação de privilégios do usuário, sem redigitar a senha, permitindo acesso a todos os comandos como superusuário, conforme apresentado nas figuras 15 e 16.

Vale ressaltar que o FreeIPA não aplica as configurações imediatamente, existe uma latência entre a persistência da configuração e a efetiva aplicação da mesma.

3.2.7 Configurações extras do FreeIPA

Uma configuração não funcional importante, consiste em alterar o terminal de comandos padrão dos usuários cadastrados no FreeIPA. Por padrão é definido o uso do "/bin/sh". Para alterar o terminal padrão para o bash, acesse via console web: *IPA Server* » *Configuration*, localizar o *Default shell*, alterar para "/bin/bash", por fim, clicar em "[*save*]"no topo do formulário.

Caso algum usuário tenha sido criado antes dessa alteração, será necessário definir os interpretadores de comando (shell) corretos para cada um deles.

Figura 15 – Configurando opções adicionais na política sudo no FreeIPA (Autor, 2021).

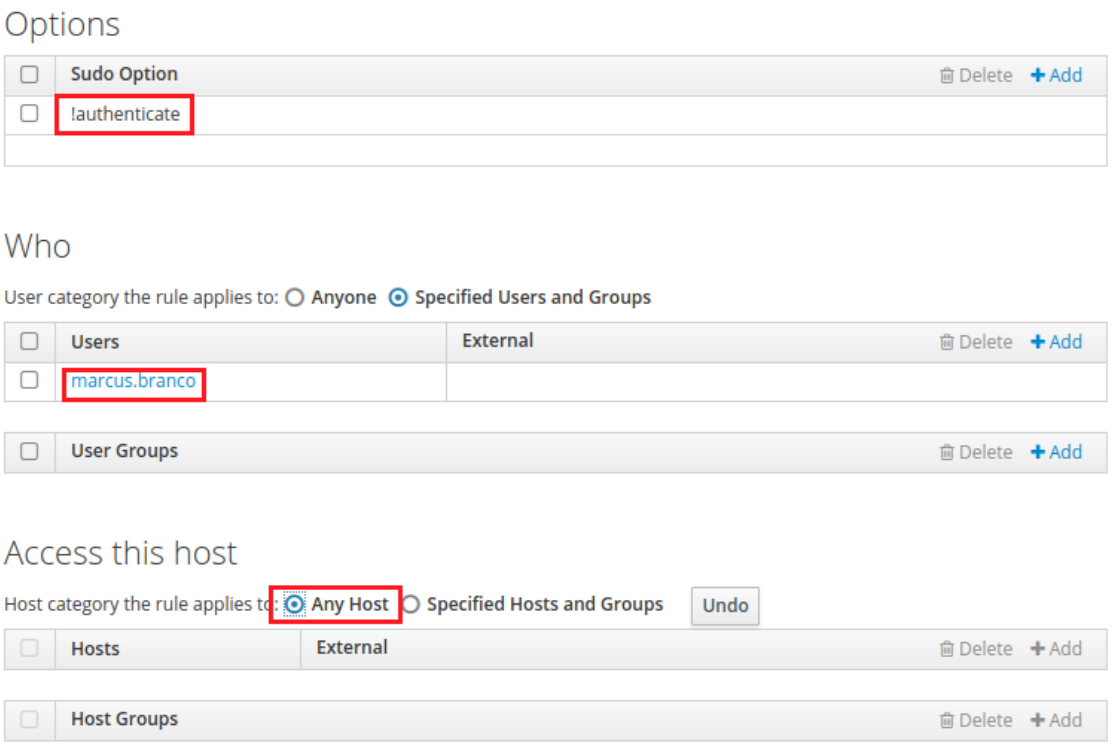
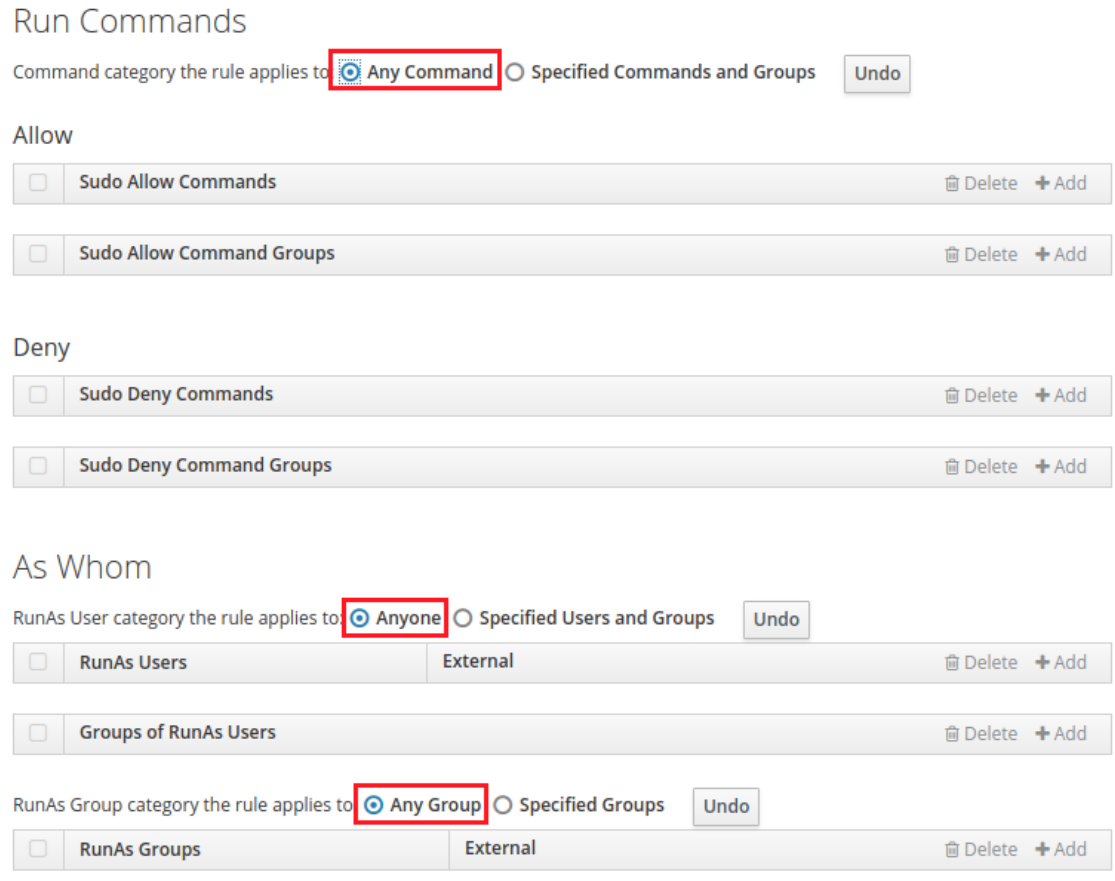


Figura 16 – Configurando comandos na política sudo no FreeIPA (Autor, 2021).



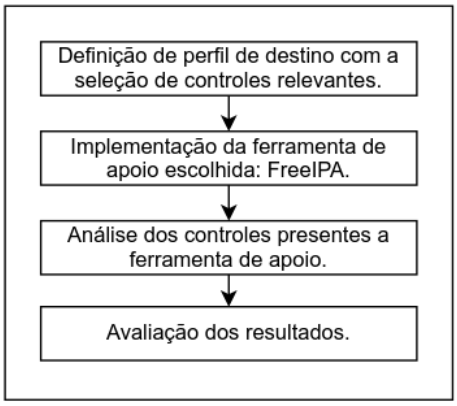
4 ANÁLISE DOS RESULTADOS

Neste capítulo serão apresentados os resultados decorrentes da análise realizada sobre os controles selecionados, aplicados durante a avalição da ferramenta analisada (FreeIPA), assim apresentando uma análise crítica sobre os resultados obtidos.

4.1 ANÁLISE DOS CONTROLES DO PERFIL DE DESTINO

De forma estruturada foi realizada a construção do perfil de destino, baseado nos controles selecionados a partir da categoria relacionada a gerência de identidades e acessos existentes no *framework core*, foi realizada a instalação e configuração da ferramenta FreeIPA e foi avaliada a aderência destes controles selecionados nesta ferramenta. Um resumo sobre as atividades pode ser compreendido na figura 17.

Figura 17 – Resumo das atividades para análise dos resultados (Autor, 2021).



Cada controle pode apresentar tópicos de aprimoramento, apontando elementos adicionais associados ao controle. Os quadros 14, 15, 16, e 17 apresentam um resumo dos principais controles e a percepção de sua implementação no FreeIPA.

No intuito de reduzir a análise, quando um controle e seus aprimoramentos não são aderentes ao escopo deste estudo, estes foram suprimidos dos quadros. Como resultado da avaliação dos controles, foram criados as seguintes classificações para cada controle:

a) *Implementado*: Quando a funcionalidade existe nativamente na ferramenta e seu uso foi avaliado;
b) *Funcionalidade existente mas não implementada*: Quando a funcionalidade foi identificada na ferramenta, porém não foi possível implementar o uso;
c) *Não implementado nativamente*: Quando a funcionalidade não existe nativamente, porém é possível (usando recursos da própria ferramenta) realizar as operações com apoio de scripts externos;
d) *Não existente*: Quando a funcionalidade não foi identificada nativamente na ferramenta;

e) *Fora do escopo do cenário*: Quando a funcionalidade não é aderente ao objetivo desejado.

Quadro 14 – Controles sugeridos pelo NIST verificados no FreeIPA - parte 1 (Autor, 2021).

Descrição	**Controles**	**Observações**
PR.AC-1/AC-1: *Access Control Policy and Procedures*	*Access Control Policy and Procedures*	Não existente. Relacionado a política de segurança.
PR.AC-1/AC-2: *Account Management*	(1) *Automated system account management*	Não existente.
	(2) *Removal of temporary / emergency accounts*	Não implementado nativamente.
	(3) *Disable inactive accounts*	Não implementado nativamente.
	(4) *Automated audit actions*	Implementado.
	(5) *Inactivity logout*	Não existente.
	(6) *Dynamic privilege management*	Não existente.
	(7) *Role - based schemes*	Implementado.
	(8) *Dynamic account creation*	Não existente.
	(9) *Restrictions on use of shared / group accounts*	Não existente.
	(10) *Shared / group account credential termination*	Não existente.
	(11) *Usage conditions*	Não existente.
	(12) *Account monitoring / atypical usage*	Não existente.
	(13) *Disable accounts for high - risk individua*	Não existente.

Quadro 15 – Controles sugeridos pelo NIST verificados no FreeIPA - parte 2 (Autor, 2021).

Descrição	**Controles**	**Observações**
PR.AC-1/AI-1: *Identification and Authentication Policy and Procedures*	AI-1: *Identification and Authentication Policy and Procedures*	Não existente. Relacionado a política de segurança.
PR.AC-1/AI-2: *Identification and Authentication (Organizational Users)*	(1) *Network access to privileged accounts*	Implementado.
	(2) *Network access to non - privileged accounts*	Implementado.
	(3) *Local access to privileged accounts*	Implementado.
	(4) *Local access to non - privileged accounts*	Implementado.
	(5) *Group authentication*	Não existente.
	(6) *Network access to privileged accounts - separate device*	Funcionalidade existente mas não implementada.
	(7) *Network access to non - privileged accounts - separate device*	Não implementado nativamente.
	(8) *Network access to privileged accounts - replay resistant*	Implementado.
	(9) *Network access to non - privileged accounts - replay resistant*	Implementado.
	(10) *Single sign - on*	Implementado.
	(11) *Remote access - separate device*	Funcionalidade existente mas não implementada.
	(12) *Acceptance of piv credentials*	Não existente.
	(13) *Out - of - band authentication*	Não existente.
PR.AC-1/AI-3: *Device Identification and Authentication*	(1) *Cryptographic bidirectional authentication*	Não existente.
	(2) *Cryptographic bidirectional network authentication*	Não existente.
	(3) *Dynamic address allocation*	Não existente.
	(4) *Device attestation*	Implementado.

Quadro 16 – Controles sugeridos pelo NIST verificados no FreeIPA - parte 3 (Autor, 2021).

Descrição	**Controles**	**Observações**
PR.AC-1/AI-4: *Identifier Management*	(1) *Prohibit account identifiers as public identifiers*	Não existente. Relacionado a política de segurança.
	(2) *Supervisor authorization*	Implementado.
	(3) *Multiple forms of certification*	Funcionalidade existente mas não implementada.
	(4) *Identify user status*	Implementado.
	(5) *Dynamic management*	Não existente.
	(6) *Cross - organization management*	Não existente.
	(7) *In - person registration*	Não existente.
PR.AC-1/AI-5: *Authenticator Management*	(1) *Password - based authentication*	Implementado.
	(2) *Pki - based authentication*	Implementado.
	(3) *In - person or trusted third - party registration*	Não existente.
	(4) *Automated support for password strength determination*	Implementado.
	(5) *Change authenticators prior to delivery*	Implementado.
	(6) *Protection of authenticators*	Fora do escopo do cenário.
	(7) *No embedded unencrypted static authenticators*	Não existente.
	(8) *Multiple information system accounts*	Implementado.
	(9) *Cross - organization credential management*	Fora do escopo do cenário.
	(10) *Dynamic credential association*	Fora do escopo do cenário.
	(11) *Hardware token - based authentication*	Funcionalidade existente mas não implementada.
	(12) *Biometric - based authentication*	Fora do escopo do cenário.
	(13) *Expiration of cached authenticators*	Implementado.
	(14) *Managing content of pki trust stores*	Implementado.
	(15) *Ficam - approved products and services*	Fora do escopo do cenário.

Quadro 17 – Controles sugeridos pelo NIST verificados no FreeIPA - parte 4 (Autor, 2021).

Descrição	**Controles**	**Observações**
PR.AC-1/AI-6: *Authenticator Feedback*	*Authenticator Feedback*	Implementado.
PR.AC-1/AI-7: *Cryptographic Module Authentication*	*Cryptographic Module Authentication*	Implementado.
PR.AC-1/AI-10: *Adaptive Identification and Authentication*	*Adaptive Identification and Authentication*	Não existente.
PR.AC-1/AI-11: *Re-authentication*	*Re-authentication*	Implementado.

O resumo de controles agrupados pela classificação pode ser observado na tabela 1, onde é possível visualizar o quantitativo e o respectivo percentual de cada classificação.

Tabela 1 – Resumo de controles por classificação (Autor, 2021)

Classificação	**Quantidade**	**Percentual**
Não implementado nativamente.	03	05%
Funcionalidade existente mas não implementada.	04	07%
Fora do escopo do cenário.	05	09%
Implementado.	22	38%
Não existente.	24	41%
Total	**58**	**100%**

Com base nas classificações estabelecidas, levando em consideração que os controles classificados como "*Implementado*", "*Funcionalidade existente mas não implementada*"e "*Não implementado nativamente*", foram qualificados como "aderentes", são promissores apesar não terem sido efetivamente avaliados em sua totalidade. Os demais controles classificados como"*Não existente*"e "*Fora do escopo do cenário*"foram qualificados como "não aderentes". Portanto, conforme apresentado na tabela 2, podemos avaliar que houve abrangência de 50% de cobertura dos controles identificados na solução utilizando o FreeIPA.

Tabela 2 – Resumo de controles por classificação de aderência (Autor, 2021).

Classificação de aderência	Quantidade	Percentual
Aderente.	29	50%
Não aderente.	29	50%
Total	**58**	**100%**

Avaliando mais abertamente as categorias de controles qualificados como aderentes é possível visualizar o quantitativo destes controles por categoria, apresentados na tabela 3.

Tabela 3 – Resumo de controles aderentes por categoria(Autor, 2021).

Classificação	Categoria de controles	Total categoria	Quantidade
Implementado	PR.AC-1/AC-2: Account Management	13	02
	PR.AC-1/AI-2: Identification and Authentication (Organizational Users)	13	07
	PR.AC-1/AI-3: Device Identification and Authentication	04	01
	PR.AC-1/AI-4: Identifier Management	07	02
	PR.AC-1/AI-5: Authenticator Management	15	07
	PR.AC-1/AI-6: Authenticator Feedback	01	01
	PR.AC-1/AI-7: Cryptographic Module Authentication	01	01
	PR.AC-1/AI-11: Re-authentication	01	01
Funcionalidade existente mas não implementada.	PR.AC-1/AI-2: Identification and Authentication (Organizational Users)	13	02
	PR.AC-1/AI-4: Identifier Management	07	01
	PR.AC-1/AI-5: Authenticator Management	15	01
Não implementado nativamente.	PR.AC-1/AC-2: Account Management	13	02
	PR.AC-1/AI-2: Identification and Authentication (Organizational Users)	13	01
		Total	**29**

Agrupando todos os resultados aderentes, é possível visualizar o percentual de controles cobertos por categoria, conforme apresentado na tabela 4.

Tabela 4 – Resumo de controles aderentes por categoria (Autor, 2021).

Categoria	**Total categoria**	**Quantidade**	**Percentual**
PR.AC-1/AC-2: Account Management	13	04	33,77%
PR.AC-1/AI-2: Identification and Authentication (Organizational Users)	13	10	76,92%
PR.AC-1/AI-3: Device Identification and Authentication	04	01	25%
PR.AC-1/AI-4: Identifier Management	07	04	42,86%
PR.AC-1/AI-5: Authenticator Management	15	08	53,33%
PR.AC-1/AI-6: Authenticator Feedback	01	01	100%
PR.AC-1/AI-7: Cryptographic Module Authentication	01	01	100%
PR.AC-1/AI-11: Re-authentication	01	01	100%

4.2 AVALIAÇÃO DOS RESULTADOS

Com base nos resultados obtidos pela análise dos controles do perfil de destino, é possível verificar na tabela 1, que o FreeIPA não contempla todos os controles recomendados, no entanto, Dos 58 controles selecionados, 22 controles estavam "implementados"no FreeIPA (38%), 04 a funcionalidade existiam mas não foram implementados (07%) e 03 não implementava nativamente (05%). Quando considerado que estas classificações são qualificáveis como "aderentes", o FreeIPA cobre 50% dos controles selecionados (tabela 2).

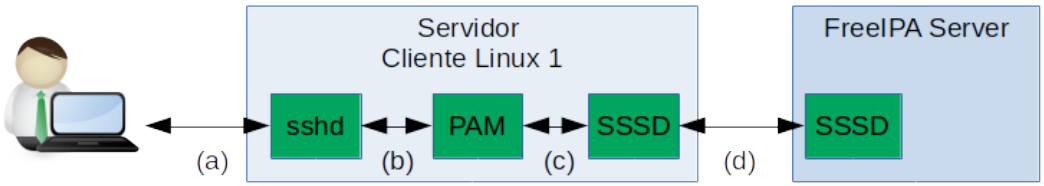
As categorias consideradas como mais relevantes podem ser descritas pelo *framework* NIST SP 800-53 (NIST, 2014):

- **PR.AC-1/AI-2: *Identification and Authentication (Organizational Users)*:** O sistema de informação identifica e autentica exclusivamente os usuários organizacionais (ou processos que atuam em nome dos usuários organizacionais). As organizações empregam senhas, tokens ou biometria para autenticar as identidades dos usuários ou, no caso, autenticação multifator, ou alguma combinação delas.
- **PR.AC-1/AI-5: *Authenticator Management***: Os sistemas de informação suportam o gerenciamento de autenticador individual por configurações definidas pela organização e restrições para várias características do autenticador, incluindo, por exemplo, comprimento mínimo de senha, composição de senha, janela de tempo de validação para tokens únicos sincronizados de tempo e número de rejeições permitidas durante o estágio de verificação de autenticação biométrica. Ações específicas que podem ser tomadas para proteger autenticadores incluem, por exemplo, manter a posse de autenticadores individuais, não emprestar ou compartilhar autenticadores individuais com outros e relatar autenticadores perdidos, roubados ou comprometidos imediatamente.

Avaliando o grupo de controles mais relevantes, a abrangência de controles das categorias *PR.AC-1/AI-2: Identification and Authentication (Organizational Users)* (10/13, 76,92%) e *PR.AC-1/AI-5: Authenticator Management* (08/15, 53,33%), 18 controles atendidos das categorias mais relevantes representam aproximadamente 31% dos controles (18/58). Mesmo selecionando apenas os controles classificados como "implementados"nas duas categorias citadas, seriam 14/58 aproximadamente 24%.

Como foi apresentado, o FreeIPA é um conjunto de aplicações que geram um ecossistema que possibilita concentrar diversas tarefas de controle, como pode ser visualizado na figura 18.

Figura 18 – Fluxo de autenticação simplificado: acesso em servidor cliente (Autor, 2021).



Grande parte dos controles são implementados por mecanismos locais em servidores GNU/Linux. Com a implementação do FreeIPA a gerência desses controles de forma centralizada facilita a administração das identidades e autorizações de acesso.

De forma simplificada o processo de autenticação utilizando o FreeIPA acontece com os seguintes passos:

a) O usuário faz acesso via SSH ao servidor cliente, membro da gestão centralizada do FreeIPA;
b) O mecaninsmo de autenticação do SSH faz uso do PAM local do servidor;
c) O serviço PAM local foi configurado para fazer uso do SSSD, componente instalado e configurado no momento em que o servidor é adicionado na gestão centralizada do FreeIPA utilizando o cliente FreeIPA;
d) O serviço SSSD local se comunica com o serviço SSSD do FreeIPA. No FreeIPA, várias regras e políticas são avaliadas para identificar se o usuário pode se autenticar com as credenciais fornecidas.

De forma independente, os mecanismos de identificação e autenticação local de sistemas GNU/Linux oferecidos pelos mecanismos de login gerenciados pelo PAM, já ofereciam grandes pontos de controle. O principal desafio era controlar todo o acesso de forma distribuída em cada servidor, desde a definição de política de senhas, até a criação de usuários e atribuição de chaves de acesso. Muitos controles são implementados pelo PAM, outros são atendidos por métodos de acesso remoto via SSH (*Secure Shell*), onde são utilizadas chaves criptográficas.

O FreeIPA tem o papel de oferecer um catálogo centralizado, orquestrando os mecanismos de autenticação local, orientando os servidores a avaliar a aprovação de acesso mediante ao conjunto de políticas de acesso, baseadas em configurações de acessos a máquinas (*HBAC Rules*). Além do mecanismo de autenticação, o FreeIPA também permite implementação de políticas de sudo. O "sudo"possibilita a alteração de privilégios de usuários, o que permite a gestão de privilégios, controlados por máquinas, grupos de máquinas ou para todas as máquinas gerenciadas.

Muitos controles interessantes não são implementados nativamente. Porém fazendo uso de API ou linha de comando do próprio serviço do FreeIPA, podem ser automatizados via scritps e agendamentos.

O conjunto de ferramentas do FreeIPA atua com objetivo de trabalhar de forma integrada e estas ferramentas atendem a vários controles. Muitos destes controles não se aplicam a gestão de acesso servidores GNU/Linux, outros são interessantes (apesar de não implementados).

Conforme mostrado, o FreeIPA não implementa todos os controles sugeridos pelo *framework* NIST SP 800-53. Contudo, a avaliação técnica do FreeIPA realizada neste trabalho tornou possível validar o objetivo geral da solução proposta: apresentar um projeto de implementação de gerência de identidades e acessos, destinada ao controle de acesso aos servidores Linux, com o intuito de oferecer maior capacidade de administração centralizada.

5 CONSIDERAÇÕES FINAIS

Quando iniciou-se o trabalho de pesquisa, existia a necessidade de encontrar alternativas de gestão de identidade e acessos, que auxiliassem os administradores de infraestrutura a implementar uma gestão centralizada de acessos em servidores Linux.

Contextualizando o cenário, geralmente o acesso ao sistema operacional GNU/Linux é realizado nativamente de forma simplificada e independente, utilizando mecanismo de autenticação básica e local, baseado em usuário e senha, muitas vezes definidos durante o processo de instalação. Em algumas organizações administradores de sistemas criam a mesma conta de usuário em vários servidores, o que abre algumas possibilidades de problemas com o vazamento de credenciais, principalmente se esta conta possuir privilégios administrativos.

Outro problema comum está relacionado a ambientes onde um dado usuário pode possuir várias credenciais diferentes (usuario e senha) para garantir o acesso a diferentes servidores, sendo uma atividade complexa o gerenciamento destas credenciais de acesso por servidor.

O maior desafio acontece quando é necessário realizar manutenções nas credenciais de acesso nestes servidores, seja por rotatividade de colaboradores, que exige o bloqueio e/ou criação de novas credenciais, seja por políticas de utilização de senhas mais seguras, entre outros. Administrar um grande quantitativo de acessos e oferecer garantias de acesso legítimo em um grande parque de hosts pode ser um desafio complexo.

Para atender esta necessidade, como objetivo geral foi realizada um estudo conceitual sobre a implementação do IAM (*Identity and Access Management* – Gerenciamento de identidades e acessos). O NIST ofereceu dois importantes *frameworks* de apoio: *frameworks NIST Framework for Improving Critical Infrastructure Cybersecurity* e SP 800-53. Como principal objetivo específico, foi realizada análise da ferramenta FreeIPA como plataforma de apoio para implementação desta gerência de identidade e acessos.

Com o apoio e direcionamento dos *frameworks* NIST destinados a segurança da informação, foram elencados os controles mais relevantes e desejados para soluções de gestão de acesso e identidade. Uma implementação prática da ferramenta FreeIPA foi realizada, com o objetivo de avaliação sobre quais dos controles sugeridos pelos *frameworks* poderiam ser atendidos e sua eficácia.

O FreeIPA apresenta um conceito de gestão baseada em HBAC. Permite de forma simples, porém eficiente, criar políticas de acessos, sejam políticas específicas e granulares, ou políticas de acessos amplas, baseadas em agrupamentos de recursos. A ferramenta também apresenta gestão via interface web, o que não exige instalação de cliente de administração local; e gestão em modo texto, o que possibilita automações na gestão de identidade e acessos.

Para esse estudo foram levantados os principais controles desejados para um nível de maturidade inicial, que oferecesse o mínimo necessário de gestão de acesso centralizado; que reduzisse o esforço em tarefas de gestão e aumentassem a segurança na gestão de acessos, seguindo as orientações do *framework profile*, presente no *framework for Improving Critical*

Infrastructure Cybersecurity.

Foram contabilizados e classificados os controles selcionados para o perfil de destino possibilitando a análise de resultados. Foi apresentado como o FreeIPA se comportou quando avaliado sobre a ótica estruturada, fundamentada nos *frameworks NIST*.

Dos 58 controles selecionados, 22 controles estavam "implementados"no FreeIPA (38%), 04 a funcionalidade existia mas não foi implementada (07%) e 03 não implementava nativamente (05%). Estes controles foram considerados como "aderentes"e representam 50% dos controles. Avaliando o grupo de controles mais relevantes, a abrangência de controles das categorias *PR.AC-1/AI-2: Identification and Authentication (Organizational Users)* (10/13; 76,92%) e *PR.AC-1/AI-5: Authenticator Management* (08/15; 53,33%), 18 controles atendidos das categorias mais relevantes representam aproximadamente 31% dos controles (18/58). Mesmo selecionando apenas os controles classificados como "implementados"nas duas categorias citadas, seriam 14/58 aproximadamente 24%, cobrindo mais do que 20% dos principais controles selecionados. Seguido príncípio de Paretto (BALLOU, 2006), conhecido como 80/20, neste cenário, 20% dos controles mais relevantes atenderiam a 80% das necessidades principais, o que torna o FreeIPA uma ferramenta promissora por cobrir grande parte dos controles mais relevantes para atividades cotidianas para a gestão de identidades e acessos em ambientes Linux.

Portanto o FreeIPA se comportou como uma solução bem estruturada, de fácil administração e aderente aos principais controles selecionados. Não cabendo a esta ferramenta, única e exclusivamente a solução de todos os pontos de gestão e controle de acessos, mas o resultado foi promissor e bastante satisfatório, o que confirma a hipótese inicial sobre o estudo do FreeIPA como ferramenta de apoio na gestão de identidade e acessos para sistemas Linux.

Como contribuição, a pesquisa desenvolveu o pensamento estruturado para avaliação de uma ferramenta, com base em um conjunto de controles, boas práticas e recomendações, que são amplamente reconhecidas pelo mercado e academia. Assim construiu uma mecanismo mais eficiente de avaliação de soluções dedicadas a dispositivos de gestão e controle.

Como objetivos relacionados a trabalhos futuros, alguns controles ainda não implementados podem ser explorados, alguns presentes no FreeIPA, outros fornecidos por outras ferramentas de apoio, ou desenho de processos organizacionais. Dentre esses controles presentes no FreeIPA, um em especial será alvo de projetos futuros: A implementação de segundo fator de autenticação com gestão centralizada. Devido a limitação de tempo, não foi possível ampliar a pesquisa em busca de ferramentas adicionais, que fossem complementares ao FreeIPA e que implementassem os controles adicionais relacionados a gestão de identidade e acessos propostos pelo NIST, ficando este estudo de ferramentas complementares ao FreeIPA, mais um objetivo para trabalhos futuros.

REFERÊNCIAS

BALLOU, Ronald H. **Gerenciamento da cadeia de suprimentos/logística empresarial; tradução Raul Rubenich**. [S.l.]: Porto Alegre: Bookman, 2006.

FERRAIOLO, David F. et al. Proposed NIST Standard for Role-Based Access Control. **ACM Transactions on Information and System Security**, v. 4, n. 3, p. 224–274, 2001. ISSN 15577406.

FREEIPA.ORG. **About - FreeIPA**. 2021. Disponível em: <https://www.freeipa.org/page/About#What_is_FreeIPA.3F>.

GARTNER. **Identity Management - Access Management - Gartner Research**. 2017. Disponível em: <https://www.gartner.com/it-glossary/identity-and-access-management-iam/>.

HITACHI. **IAM Project Best Practices**. 2017. Disponível em: <https://hitachi-id.com/documents/best-practices-for-identity-management-projects.php?page=1>.

ISO/IEC 27000 et al. INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and. **ACM Workshop on Formal Methods in Security Engineering.Washington, DC, USA**, Gaithersburg, MD, v. 34, n. 19, p. 45–55, apr 2018. ISSN 17517362. Disponível em: <http://www.worldcat.org/title/service-operation/oclc/254028066&referer=brief_resultshttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdfhttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdfhttp://k504.khai.edu>.

MORGAN, Andrew G.; KUKUK, Thorsten. **A Linux-PAM page**. 2018. Disponível em: <http://www.linux-pam.org/>.

MORGAN, Andrew G.; KUKUK, Thorsten. **Chapter 1 Introduction**. 2018. Disponível em: <http://www.linux-pam.org/Linux-PAM-html/sag-introduction.html>.

MORGAN, Andrew G.; KUKUK, Thorsten. **Chapter 3. Overview**. 2018. Disponível em: <http://www.linux-pam.org/Linux-PAM-html/sag-overview.html>.

MUEHLFELD, Marc et al. **1.2. The Identity Management Domain Red Hat Enterprise Linux 7 | Red Hat Customer Portal**. 2019. 535 p. Disponível em: <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/linux_domain_identity_authentication_and_policy_guide/idm-domain>.

NEWLANDS, Ellen. **Who Goes There? Identity Management in Red Hat Enterprise Linux 7 Beta**. 2014. Disponível em: <https://www.redhat.com/en/blog/who-goes-there-identity-management-red-hat-enterprise-linux-7-beta>.

NIST. SP 800-53 Rev.4 - Security and Privacy Controls for Federal Information Systems and Organizations. **National Institute of Standards and Technology (NIST) - Special Publication**, Gaithersburg, MD, v. 800-53, p. 1–460, apr 2014. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

NIST. **Framework for Improving Critical Infrastucture**. Gaithersburg, MD: [s.n.], 2018. Disponível em: <http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdfhttps://doi.org/10.6028/NIST.CSWP.04162018>.

OWASP. **Credential stuffing - OWASP**. 2018. Disponível em: <https://www.owasp.org/index.php/Credential_stuffing>.

Rhand Leal. **Controle de acesso da ISO 27001: Uso de autenticação pode dois fatores**. 2017. Disponível em: <https://advisera.com/27001academy/pt-br/blog/2017/01/17/como-a-autenticacao-por-dois-fatores-apoia-a-conformidade-com-os-controles-de-acesso-da-iso-27001/>.

ROUSE, Margaret. **What is role-based access control (RBAC)?** 2012. Disponível em: <https://searchsecurity.techtarget.com/definition/role-based-access-control-RBAC>.

SANDHU, Ravi; FERRAIOLO, David; KUHN, Richard. NIST model for role-based access control: Towards a unified standard. **Proceedings of the ACM Workshop on Role-Based Access Control**, n. January, p. 47–63, 2000.

SRIVASTAVA, Vishal. **Entendendo e Configurando o PAM**. 2009. 8 p. Disponível em: <https://www.ibm.com/developerworks/br/library/l-pam/l-pam-pdf.pdf>.