FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Marcelo Nascimento Silva de Souza Menezes

Paulo Sergio Meireles Junior

AUTENTICAÇÃO MULTIFATOR (MFA) PARA *ACTIVE DIRECTORY* (AD)

Americana, SP

2023

FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Marcelo Nascimento Silva de Souza Menezes

Paulo Sergio Meireles Junior

AUTENTICAÇÃO MULTIFATOR (MFA) PARA *ACTIVE DIRECTORY* (AD)

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Me. Maxwel Vitorino da Silva.

Área de concentração: Infraestrutura Física em Redes de Computadores.

Americana, SP

2023

FICHA CATALOGRÁFICA — Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

MENEZES, Marcelo Nascimento Silva de Souza
Junior Meireles, Paulo Sérgio

Autenticação multifator(mfa) para active directory(ad). / Marcelo Nascimento Silva de Souza Menezes, Paulo Sérgio Meireles Junior — Americana, 2023.

89f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi — Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Maxwel Vitorino Silva

1 . Computação em nuvens 2. Sistemas de informação 3. Sistemas operacionais. I. MENEZES, Marcelo Nascimento Silva de Souza, II. MEIRELES JUNIOR, Paulo Sérgio III. SILVA, Maxwel Vitorino IV. Centro Estadual de Educação Tecnológica Paula Souza — Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681518
681 518
681.3.066

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Marcelo Nascimento Silva de Souza Menezes
Paulo Sergio Meireles Junior

AUTENTICAÇÃO MULTIFATOR (MFA) PARA *ACTIVE DIRECTORY* (AD)

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Infraestrutura Física em Redes de Computadores.

Americana, 02 de dezembro de 2023.

Banca Examinadora:

Maxwel Vitorino da Silva (Presidente)
Mestre
Fatec Americana - Faculdade de Tecnologia de Americana Ministro Ralph Biasi

Wagner José da Silva (Membro)
Mestre
Fatec Americana - Faculdade de Tecnologia de Americana Ministro Ralph Biasi

Wellington Aires da Cruz Pereira (Membro)
Mestre
Fatec Americana - Faculdade de Tecnologia de Americana Ministro Ralph Biasi

AGRADECIMENTOS

A Deus, pela vida, pela saúde, pelas oportunidades, pelos aprendizados e sonhos concretizados!

Ao nosso orientador, Prof. Me. Maxwel Vitorino da Silva, pela paciência durante a orientação, pela disponibilidade e pela ajuda constante na realização deste trabalho de conclusão de curso de graduação. Seus apontamentos durante as aulas, contribuíram para esse processo. Nosso Obrigado!

Aos Professores, pela recepção, pela amizade e pelas experiências que contribuíram para realizarmos este sonho.

Aos (Às) amigos(as), que nos acompanharam durante essa graduação, pelo compartilhamento e pelo apoio nesta trajetória.

Aos (Às) funcionários(as), da FATEC – Americana pela recepção, atenção e acolhimento durante a graduação.

DEDICATÓRIA

Aos nossos pais, amigos (as) e familiares que de alguma forma contribuíram para nossa aprendizagem e não nos deixaram desistir!

RESUMO

Este trabalho aborda o tema Autenticação Multifator (MFA) para *Active Directory* (AD) na *Amazon* Web Services (AWS). A autenticação multifator é uma técnica de segurança que acrescenta camadas adicionais de proteção ao processo de autenticação, exigindo que os usuários forneçam várias formas de identificação antes de obter acesso a um sistema ou rede. O *Active Directory* é um serviço de diretório da *Microsoft* que gerencia o acesso a recursos de rede em um ambiente de rede Windows. Ao decorrer deste trabalho iremos explorar a importância da autenticação multifator como uma medida efetiva de segurança cibernética para proteger as empresas contra ameaças de segurança, também será discutido sobre a implementação do *Active Directory* utilizando a computação em nuvem com AWS. O objetivo principal do trabalho é demonstrar como a autenticação multifator pode ser implementada com sucesso no *Active Directory* para garantir a segurança dos recursos de rede da empresa. Também será abordado as diferentes versões do *Windows Server 2019*, a estrutura lógica do *Active Directory* e protocolos envolvidos no funcionamento da ferramenta.

Palavras-Chave: *Active Directory*; Protocolo LDAP; Autenticação Multifator; Computação em nuvem com AWS.

ABSTRACT

*This work explores the topic of Multi-factor authentication (MFA) for Active Directory (AD) on the Amazon Web Services (*AWS*) platform. Multi-factor authentication is a security technique that adds additional layers of protection to the authentication process, requiring users to provide multiple forms of identification before gaining access to a system or network. Active Directory is a Microsoft Directory Service that manages network resource access in a Windows network environment. Throughout this study, we delve into the significance of Multi-factor authentication as an effective cybersecurity measure to safeguard companies against security threats. We also discuss the implementation of Active Directory in a cloud computing environment using* AWS*. The main objective of this work is to demonstrate the successful implementation of Multi-factor authentication within Active Directory to ensure the security of a company's network resources. Additionally, this paper covers various versions of Windows Server 2019, the logical structure of Active Directory, and the protocols involved in its operation.*

Keywords: *Active Directory; LDAP Protocol; Multi-Factor Authentication;* AWS *Cloud Computing.*

LISTA DE FIGURAS

Sumário

1. INTRODUÇÃO

Com o objetivo de garantir a integridade da rede de computadores, a autenticação de usuários se tornou fundamental diante do crescente aumento da demanda por segurança de dados e informações. Nesse contexto, a autenticação multifator (MFA) tem ganhado importância como uma opção eficaz para garantir a segurança da autenticação de usuários, especialmente no *Active Directory* (AD) da *Microsoft*, um dos principais sistemas de gerenciamento de usuários e recursos de rede.

A tecnologia de computação em nuvem oferece uma infraestrutura de tecnologia da informação fundamentada em serviços que viabiliza o acesso remoto a recursos computacionais através da Internet. Dentro desse cenário, a questão da segurança de dados na computação em nuvem tem sido extensamente discutida e reconhecida como uma preocupação de extrema importância.

Este trabalho de conclusão de curso tem como objetivo apresentar uma solução de autenticação multifator para o AD, utilizando a plataforma *Windows Server 2019*. Para tanto, serão abordados conceitos relacionados ao *Windows Server 2019*, suas diferentes versões, funções do *Active Directory*, protocolo LDAP (*Lightweight Directory Access Protocol*) e computação na nuvem com AWS, utilizado para a comunicação com o serviço de diretório.

Também serão apresentados os diferentes aspectos do *Active Directory*, incluindo a estrutura lógica, criação de grupos de usuários, pastas compartilhadas e autenticação no AD.

Além disso, será discutido o uso do protocolo LDAP no *Active Directory*. Será descrito ainda o uso das *Group Policy Objects* (GPOs) do *Windows Server* 2019 para a implementação de políticas de segurança.

O trabalho está estruturado em onze capítulos. O primeiro capítulo estabelece a introdução, objetivos, justificativa e metodologia da pesquisa. O segundo capítulo apresenta o *Windows Server* 2019, suas diferentes versões e principais características.

O terceiro capítulo aprofunda os conceitos do *Windows Server* 2019, com foco nas funções do *Active Directory*. O quarto capítulo discorre sobre o protocolo LDAP, sua história, características e aplicações. O quinto capítulo é dedicado ao *Active Directory*, explorando sua estrutura lógica e autenticação de usuários, incluindo

tópicos como DNS, domínios, objetos, unidades organizacionais, árvore, floresta, relação de confiança, esquema e integração do DNS ao AD. O sexto capítulo descreve a utilização do protocolo LDAP no AD, incluindo seu suporte.

No sétimo capítulo, discute-se o uso das GPOs para a implementação de políticas de segurança. O oitavo capítulo, ponto central deste trabalho, aborda a autenticação multifator para o AD e suas vantagens. Os capítulos de nove a onze trazem novas perspectivas à pesquisa. O nono capítulo explora a computação em nuvem, com ênfase na AWS e o *Amazon Elastic Computer Cloud* (*Amazon* EC2) na Infraestrutura de Computação em Nuvem.

O décimo capítulo se concentra no desenvolvimento e criação de um ambiente de teste. Por fim, o décimo primeiro capítulo, a conclusão, sintetiza os principais resultados obtidos.

1.1 Objetivos

Os objetivos deste trabalho visam a compreensão e aplicação de conceitos relacionados ao *Windows Server 2019*, o *Active Directory*, a autenticação multifator e a integração com a plataforma *Amazon Web Services* (AWS) para reforçar a segurança da informação.

1.1.1 Objetivo Geral

O objetivo geral deste estudo consiste em realizar uma análise aprofundada do *Active Directory*, explorando o uso do *Windows Server 2019*, o protocolo LDAP, a plataforma AWS e a autenticação multifator.

1.1.2 Objetivos Específicos

Para atingir o objetivo geral, desdobramos os seguintes objetivos específicos:

- Descrever detalhadamente o funcionamento do *Active Directory* e sua estrutura;
- Implementar a autenticação multifator (MFA) de forma prática e demonstrando seus benefícios.

1.2 Justificativa

Este estudo tem como propósito destacar a importância da segurança da TI (Tecnologia da Informação) nas empresas, destacando como recursos como as GPOs, podem solucionar desafios cotidianos no ambiente de trabalho. Além disso, demonstraremos como a implementação da autenticação multifator (MFA) e a integração com a plataforma AWS contribuem para uma segurança mais robusta dos dados.

A AWS oferece um conjunto abrangente de serviços de segurança que auxiliam as empresas na proteção de seus recursos na nuvem (AWS, 2023). A autenticação multifator (MFA) é uma medida fundamental para proteger as contas de usuário contra possíveis ataques de hackers.

O uso do MFA em conjunto com o *Active Directory* contribui não apenas para a segurança das contas e dados sensíveis, mas também para o cumprimento de regulamentações de segurança e uma gestão mais eficiente das senhas dos usuários.

1.3 Metodologia da Pesquisa

Revisão da literatura com base em livros, artigos, sites, organizações e por isso, caracteriza-se como uma “pesquisa bibliográfica implica em um conjunto ordenado de procedimentos de busca por soluções, atento ao objeto de estudo, e que, por isso, não pode ser aleatório” (LIMA; MIOTO, 2007, p.38).

2. CONHECENDO O *WINDOWS SERVER 2019*

De acordo com o autor Bekim Dauti (2019) *Windows Server 2019* é uma versão do sistema operacional da *Microsoft* projetada especificamente para servidores e redes corporativas. Ele oferece diversas melhorias em relação às versões anteriores do *Windows Server*, incluindo recursos de segurança aprimorados, maior desempenho e escalabilidade, suporte para contêineres e recursos avançados de armazenamento e virtualização.

Algumas das principais características do *Windows Server 2019* incluem:

- **Recursos de segurança aprimorados:** como proteção de dados e criptografia de rede avançada.
- **Suporte para contêineres do *Docker* e do *Kubernetes*:** permitindo que os desenvolvedores criem e implantem aplicativos em contêineres com facilidade.
- **Melhorias no desempenho de armazenamento:** incluindo a capacidade de executar deduplicação de dados em volumes ReFS (sistema de Arquivos Resiliente) e o suporte para armazenamento persistente de memória (Pmem) para aplicativos de alta performance.
- **Novos recursos de virtualização:** incluindo a capacidade de usar o *Hyper-V*. (O *Hyper-V* Ele possibilita o espelhamento de máquinas virtuais entre *Hosts* de virtualização no *Windows Server 2019*. Você pode ter todo o seu ambiente de máquinas virtuais replicado em outro servidor (mesmo fora de sua rede) como uma forma de “site *backup*”.) para executar máquinas virtuais em nuvens públicas e privadas.
- **Suporte para *clusters* de *failover* estendidos:** permitindo que as empresas executem aplicativos críticos em *data centers* geograficamente distantes.

Sendo assim, segundo a *Microsoft* (2023) o *Windows Server 2019* é uma solução poderosa e flexível para empresas que desejam implantar e gerenciar uma infraestrutura de rede robusta e segura.

Conforme *Microsoft* (2023), *Windows Server 2019* é uma das versões mais recentes do sistema operacional de servidor da *Microsoft*, lançado em outubro de 2018. Ele é projetado para fornecer recursos avançados de gerenciamento de servidores e segurança para empresas de todos os tamanhos.

Algumas das principais características do *Windows Server 2019* incluem:

- **Segurança avançada:** o *Windows Server 2019* inclui várias camadas de segurança integradas para proteger seus dados e identidade. Ele também oferece suporte a criptografia TLS 1.3 e autenticação multifator.
- **Armazenamento aprimorado:** o sistema operacional inclui recursos de armazenamento aprimorados, como o suporte a armazenamento persistente de memória (NVDIMM-N) e a duplicação de dados.
- **Virtualização aprimorada:** o *Hyper-V* no *Windows Server 2019* oferece melhorias significativas na escalabilidade, desempenho e segurança da virtualização.
- **Gerenciamento simplificado:** o *Windows Admin Center* é uma nova ferramenta de gerenciamento baseada em navegador que simplifica o gerenciamento de servidores e serviços.
- **Melhorias em contêineres:** o *Windows Server 2019* inclui suporte a contêineres do Windows e Linux e oferece melhorias no desempenho e na compatibilidade.
- **Redes mais rápidas:** o *Windows Server 2019* inclui suporte a velocidades de rede de 40 e 100 GbE e oferece melhorias na eficiência do tráfego de rede.

2.1 Versões do *Windows Server 2019*

Conforme a *Microsoft* (2023) o *Windows Server 2019* apresenta diversas versões destinadas a atender as necessidades de empresas de diferentes portes e segmentos.

O ***Windows Server 2019 Standard*** é indicado para empresas de pequeno e médio porte e oferece recursos avançados de virtualização, segurança, gerenciamento de armazenamento, entre outros.

Já o ***Windows Server 2019 Datacenter*** é recomendado para empresas de grande porte e oferece recursos ainda mais avançados, como virtualização avançada, armazenamento definido por *software*, rede definida por *software* e segurança.

Para empresas de menor porte, com até 25 usuários e 50 dispositivos, a opção indicada é o ***Windows Server 2019 Essentials***, que oferece recursos essenciais de gerenciamento de servidor, *backup* e restauração de dados e segurança.

2.1.1 *Windows Server 2019 Essentials*

De acordo com a *Microsoft* (2023), o *Windows Server 2019 Essentials* representa um sistema operacional de servidor desenvolvido especialmente para empresas de pequeno porte que possuam até 25 usuários e 50 dispositivos. Este sistema oferece funcionalidades tais como compartilhamento de arquivos, acesso remoto, *backup* e restauração, além de integração com os serviços *Microsoft* 365 e *Azure*.

Principais recursos do *Windows Server 2019 Essentials*:

- **Fácil de usar:** o *Windows Server 2019 Essentials* possui um painel amigável que simplifica o gerenciamento do servidor para pequenas empresas.
- **Compartilhamento de arquivos:** o sistema operacional fornece um local central para armazenar e compartilhar arquivos dentro da organização.
- **Acesso remoto:** Os funcionários podem acessar a rede e os arquivos da empresa remotamente de qualquer dispositivo com conexão à internet.
- **Backup e restauração:** o *Windows Server 2019 Essentials* inclui um recurso integrado de *backup* e restauração, que permite às empresas protegerem seus dados e recuperá-los em caso de desastre.
- **Integração com os serviços do *Microsoft* 365 e do *Azure*:** o sistema operacional se integra aos serviços do *Microsoft* 365 e do *Azure*, permitindo que as empresas aproveitem as tecnologias e serviços de computação em nuvem.

No geral, o *Windows Server 2019 Essentials* oferece uma solução acessível e fácil de usar para pequenas empresas que buscam estabelecer uma infraestrutura de servidor confiável e segura.

2.1.2 *Windows Server 2019 Standard*

Conforme mencionado pelo autor Bekim Dauti em seu estudo de 2019, o *Windows Server 2019 Standard* é um sistema operacional voltado para servidores, desenvolvido pela *Microsoft* como parte da família de sistemas operacionais Windows NT (*New Technology*), destinado a usuários corporativos.

O referido sistema operacional foi concebido com o intuito de atender às demandas de organizações de grande porte, que necessitam de recursos avançados, tais como virtualização, rede, armazenamento e segurança.

Alguns dos principais recursos do *Windows Server 2019 Standard* incluem:

- **Segurança aprimorada:** o *Windows Server 2019 Standard* vem com recursos avançados de segurança, como o *Windows Defender Advanced Threat Protection (*ATP), que ajuda a proteger contra-ataques sofisticados.
- **Nuvem híbrida:** o *Windows Server 2019 Standard* oferece suporte a cenários de nuvem híbrida que permitem que as empresas integrem infraestrutura local com serviços de nuvem.
- **Serviço de migração de armazenamento:** esse recurso permite que as organizações migrem facilmente seus servidores existentes para um novo *hardware* ou infraestrutura de nuvem com o mínimo de tempo de inatividade.
- **Máquinas virtuais blindadas:** o *Windows Server 2019 Standard* oferece suporte a máquinas virtuais blindadas que fornecem segurança aprimorada para cargas de trabalho virtualizadas.
- ***Storage Spaces Direct*:** esse recurso permite que as organizações criem soluções de armazenamento altamente disponíveis e escaláveis usando servidores e discos padrão do setor.

No geral, o *Windows Server 2019 Standard* é um sistema operacional de servidor poderoso e confiável que fornece recursos avançados para empresas de todos os tamanhos.

2.1.3 *Windows Server 2019 Datacenter*

De acordo com a *Microsoft* (2023) *Windows Server 2019 Datacenter* é um sistema operacional de servidor desenvolvido pela *Microsoft* e projetado especificamente para atender às necessidades de data centers e outros ambientes empresariais de grande porte. Esta variante do *Windows Server 2019* é otimizada para virtualização e oferece suporte a cargas de trabalho mais robustas e alocação de memória superior em relação a outras versões do *Windows Server 2019*.

Alguns dos recursos do *Windows Server 2019 Datacenter* incluem:

- Suporte para até 64 soquetes e 2 *terabytes* de memória por servidor, permitindo máquinas virtuais maiores e taxas de consolidação mais altas.
- Recursos de rede definida por *software* (SDN), incluindo criptografia de rede virtual, otimização de desempenho de rede e filtragem de tráfego.
- *Storage Spaces Direct*, que permite a criação de soluções de armazenamento definido por *software* altamente disponíveis e escaláveis.
- Suporte para contêineres *Hyper-V*, que permitem a implantação de aplicativos em contêineres no *Windows Server*.
- Recursos de segurança aprimorados, incluindo *Shielded Virtual Machines*, que protegem as máquinas virtuais contra adulteração e acesso não autorizado.
- *Windows Defender Advanced Threat Protection*, que fornece detecção avançada de ameaças e recursos de resposta.

De acordo Theo Lins (2015) com Rede Definida por *Software* SDN (Rede definida por *Software*) é um modelo de arquitetura de rede que se utiliza de controladores baseados em *software* ou APIs para gerenciar e direcionar o tráfego na rede, bem como para estabelecer comunicação com a infraestrutura de *hardware* subjacente.

Tal abordagem difere das redes convencionais que se valem de dispositivos de *hardware* dedicados (tais como roteadores e *switches*) para a gestão do tráfego na rede. Uma SDN pode criar e administrar uma rede virtual ou mesmo gerir uma rede de *hardware* tradicional com a utilização de *software*.

Isso é diferente das redes tradicionais, que usam dispositivos de *hardware* dedicados (roteadores e *switches*) para controlar o tráfego de rede. Uma SDN pode criar e controlar uma rede virtual ou controlar uma rede de *hardware* tradicional com *software*.

3. CONCEITOS DO *WINDOWS SERVER 2019*

Segundo a *Microsoft* (2023) o *Windows Server 2019* representa o sistema operacional que facilita a conexão entre ambientes locais e os serviços do *Azure*, viabilizando a criação de cenários híbridos que otimizam os recursos já investidos. É possível reforçar a segurança e minimizar os riscos corporativos com a incorporação de diversas camadas de proteção diretamente no sistema operacional.

Aprimorando a infraestrutura do seu *Datacenter* para atingir níveis superiores de eficiência e capacidade de escalabilidade por meio da infraestrutura hiper convergente. O *Windows Server 2019* também oferece a possibilidade de desenvolver aplicativos nativos da nuvem e modernizar aplicativos convencionais, fazendo uso de contêineres e micros serviços.

Alguns conceitos importantes relacionados ao *Windows Server 2019* incluem:

- ***Active Directory*:** O *Active Directory* é um serviço de diretório que gerencia usuários, grupos e dispositivos em uma rede Windows. Ele permite a autenticação e autorização dos usuários e gerenciamento centralizado de recursos da rede.
- ***Hyper-V*:** O *Hyper-V* é a plataforma de virtualização da *Microsoft* que permite criar e gerenciar máquinas virtuais no *Windows Server 2019*.
- **Serviços de Área de Trabalho Remota:** Os Serviços de Área de Trabalho Remota permitem que os usuários acessem seus *desktops* e aplicativos remotamente através da rede.
- **Armazenamento definido por *software*:** O armazenamento definido por *software* é uma tecnologia de armazenamento que permite a criação de *pools* de armazenamento a partir de dispositivos de armazenamento físicos.
- **PowerShell:** O PowerShell é uma ferramenta de linha de comando que permite a automação de tarefas administrativas no *Windows Server 2019*.
- **Backup e Recuperação:** O *Windows Server 2019* inclui recursos de *backup* e recuperação para proteger dados críticos da empresa.

- ***Failover Clustering*:** O *Failover Clustering* é uma tecnologia de cluster que permite que vários servidores trabalhem juntos para fornecer alta disponibilidade e tolerância a falhas.

3.1 FUNÇÕES DO *ACTIVE DIRECTORY*

O *Active Directory* é um serviço de diretório que é amplamente utilizado em redes de computadores baseadas no sistema operacional *Windows Server*.

Algumas das funções do *Active Directory* são:

- **Gerenciamento de identidade e acesso:** o *Active Directory* fornece um local centralizado para gerenciar e controlar o acesso dos usuários, computadores e outros recursos da rede. Ele pode ser configurado para permitir ou negar o acesso a recursos específicos com base nas permissões atribuídas aos usuários ou grupos.
- **Autenticação:** o *Active Directory* é usado para autenticar usuários e computadores em uma rede. Ele permite que os usuários se autentiquem em vários serviços e aplicativos usando as mesmas credenciais.
- **Gerenciamento de políticas:** o *Active Directory* permite que os administradores de rede criem e gerenciem políticas de segurança para aplicar configurações consistentes em toda a rede. Isso inclui políticas de senha, diretivas de bloqueio de conta, políticas de segurança de rede e outras configurações.
- **Gerenciamento de recursos:** o *Active Directory* permite que os administradores gerenciem recursos em toda a rede, incluindo usuários, computadores, servidores, impressoras e outros dispositivos de rede.
- **Gerenciamento de serviços:** o *Active Directory* pode ser usado para gerenciar serviços e aplicativos na rede, incluindo serviços de diretório adicionais, como DNS e DHCP.

Em síntese, o *Active Directory* desempenha um papel primordial na administração e proteção de uma rede fundamentada em *Windows Server*. O referido sistema possibilita aos administradores a gestão de recursos de rede, o controle de acessos, autenticação e a aplicação de políticas de segurança em toda a rede.

4. PROTOCOLO DE ACESSO A DIRETÓRIO LEVE (LDAP)

De acordo com Allen e Puckett (2002), o LDAP trata-se de um protocolo de rede que foi desenvolvido para acessar e gerenciar informações armazenadas em serviços de diretórios, que são bancos de dados que armazenam informações hierárquicas, como dados de usuários, grupos e recursos em uma rede.

O LDAP pode ser utilizado em diversas aplicações de rede, como autenticação de usuários, gerenciamento de contas de usuários, acesso a recursos e serviços, entre outros. Ele é considerado um protocolo leve, porque utiliza uma quantidade relativamente pequena de recursos da rede, o que o torna eficiente e adequado para redes com grande quantidade de usuários e dispositivos.

Conforme Allen e Puckett (2002), o LDAP é um padrão aberto que pode ser utilizado em redes TCP/IP (*Transmission Control Protocol/Internet Protocol*) de diferentes tipos e possui produtos disponíveis para diversas plataformas. O protocolo organiza os recursos da rede de maneira hierárquica, como uma árvore de diretórios, na qual o diretório raiz é seguido pela rede da empresa, departamentos, dispositivos dos funcionário e recursos compartilhados por ele, como arquivos e impressoras.

4.1 Desenvolvimento do Protocolo

Nos anos 80, quando se pretendia desenvolver um serviço de mensagens baseado em *store-and-forward*, a série X.400, percebeu-se a necessidade de criar um protocolo capaz de organizar entradas em um serviço de nomes de forma hierárquica, suportando grandes quantidades de informação e possibilitando uma busca eficiente.

A Universidade de Michigan, com o apoio do Consortium do ISODE (*International Organization for Standardization Development Environment),* criou esse serviço em 1988, especificando a comunicação entre o cliente e o servidor do Diretório por meio do protocolo DAP *(Directory Access Protocol*), executado sobre a pilha de protocolos do modelo OSI (*Open Source Initiative*). O DAP é protocolo complexo que requer uma camada OSI completa e recursos computacionais significativos para funcionar.

A ITU (*International Telecommunications Union*) padronizou o X.500 como um Serviço de Diretório universal, com a finalidade de estabelecer conexões entre Serviços de Diretórios locais e formar um diretório global distribuído. Entretanto, a complexidade e alto custo do protocolo X.500 levou os pesquisadores da Universidade de Michigan a desenvolver um servidor mais simples, o LDAP (*Lightweight Directory Access Protocol*).

Em 1993, o LDAP foi introduzido como uma alternativa mais acessível ao protocolo DAP para acessar diretórios baseados no modelo X.500. O LDAP é executado diretamente sobre o TCP e oferece a maioria das funcionalidades do DAP, porém com um custo muito menor.

A primeira implementação do LDAP foi realizada pela Universidade de Michigan, e o grupo de pesquisadores responsáveis pelo desenvolvimento do protocolo disponibilizou o seu código-fonte na Internet e criou listas de discussão para divulgar e aprimorar o novo serviço. A evolução do LDAP foi acompanhada por pessoas de todo o mundo.

Em dezembro de 1997, o LDAP foi oficialmente reconhecido como um padrão da IETF (*Internet Engineering Task Force*). Posteriormente, a versão três do LDAP foi lançada como uma proposta padrão para Serviços de Diretório na Internet.

4.2 Características

O LDAP fornece a possibilidade de localizar facilmente informações e arquivos disponibilizados. Por exemplo, é possível pesquisar pelo sobrenome de um funcionário e encontrar dados como número de telefone, departamento de trabalho, projetos nos quais está envolvido e outras informações adicionadas ao sistema, bem como arquivos criados ou referenciados por ele. Cada funcionário deve ter uma conta de acesso no servidor LDAP para que possa adicionar informações sobre si mesmo e compartilhar arquivos.

O LDAP armazena informações de acordo com uma estrutura hierárquica em forma de árvore, onde as atualizações são realizadas com pouca frequência. O servidor LDAP é projetado para responder rapidamente a uma grande quantidade de consultas e oferece um alto nível de segurança.

O protocolo LDAP traz benefícios significativos, como a centralização da informação, redução da duplicação de dados e um único ponto de administração.

Além disso, ele utiliza um mecanismo de replicação hierárquico que permite que os privilégios sejam passados de pai para filho, com o nó pai tendo controle sobre o nó filho. Ele também fornece um mecanismo seguro para autenticação e troca de dados.

No momento atual, diversas aplicações oferecem suporte ao LDAP, incluindo a principal ferramenta do sistema operacional *Windows Server 2019*. O uso do LDAP tem crescido entre os administradores de redes, já que suas características e vantagens muitas vezes superam sua complexidade. Isso se reflete no fato de que cada vez mais sistemas operacionais e aplicações têm suporte para LDAP. No entanto, existem algumas limitações a serem consideradas com o uso do LDAP, tais como:

- A complexidade do protocolo, que pode requerer conhecimentos técnicos avançados para sua configuração e uso adequados;
- A necessidade de um servidor LDAP centralizado e confiável para garantir a integridade e segurança das informações armazenadas;
- A necessidade de um controle cuidadoso do acesso aos dados armazenados no LDAP, já que ele é uma ferramenta potencialmente sensível para armazenamento e compartilhamento de informações confidenciais.

4.3 Aplicações do LDAP

Para entendermos por que e como o LDAP se tornou uma ferramenta tão relevante na vida dos administradores de rede, é preciso compreender as dificuldades de gerenciar uma rede com uma base de dados descentralizada e como o protocolo LDAP pode ser útil para uma administração eficiente da rede.

Em outras palavras, o LDAP pode ser considerado tanto uma tecnologia quanto uma ferramenta. Por meio do LDAP é possível realizar a integração com outros serviços, complementando assim a infraestrutura de redes, fornecendo novos recursos e, especialmente, maior integração, diferentemente de outros protocolos e linguagens estabelecidos como exemplo: SNMP, HTTP, SMTP, IMAP ou SQL.

O LDAP é amplamente utilizado por empresas de todos os tamanhos em várias aplicações, como serviços de diretórios corporativos, gerenciamento de identidades e acesso, autenticação de usuários, gerenciamento de endereços de e-mail e muito mais. Algumas das empresas que utilizam o LDAP em suas aplicações incluem:

- *Microsoft (AD)*

- *IBM*
- *Oracle*
- *Google*
- *Red Hat*
- *Novell*
- *Sun Microsystems (agora parte da Oracle)*
- *Cisco*
- *Hewlett Packard Enterprise*
- *Amazon Web Services (AWS)*

Essas empresas utilizam o LDAP em diferentes contextos, desde serviços de diretórios corporativos até autenticação de usuários em aplicativos baseados na web.

Atualmente, a maioria dos administradores de rede prefere utilizar o LDAP em vez das bases de dados tradicionais, devido às suas vantagens e características já mencionadas, além do crescente número de aplicações que o suportam.

O LDAP é uma das tecnologias mais amplamente utilizadas na Internet, mas ainda é pouco compreendido pela maioria dos profissionais. Apesar de estar presente em todo lugar, muitos ainda desconhecem suas funcionalidades e benefícios.

Observe que, embora seja factível acessar o banco de dados à distância, o LDAP não é comumente empregado como protocolo na Internet, somente em Intranets, principalmente em organizações de grande porte, pois quanto mais numerosos são os usuários e documentos disponíveis, maior é a sua relevância.

Neste capítulo, foram apresentados os conceitos fundamentais do protocolo LDAP, sua trajetória, recursos, usos e exemplos de organizações que o empregam, tais como a *Microsoft* com o AD.

A seguir são apresentadas algumas das características do *Active Directory*, que é uma ferramenta que utiliza o protocolo LDAP para serviços de diretórios.

5. *ACTIVE DIRECTORY*

O Active Directory foi projetado para ser um serviço de diretório centralizado que permitisse aos administradores de rede gerenciarem de forma eficiente os recursos e usuários da rede em um ambiente Windows.

O *Active Directory* foi desenvolvido como uma solução para superar os problemas enfrentados pelos administradores de rede ao tentar gerenciar informações em vários servidores independentes. Antes do *Active Directory*, os administradores de rede precisavam gerenciar as informações de cada usuário e recurso em cada servidor separadamente, o que era demorado e propenso a erros.

Com a introdução do *Active Directory*, os administradores de rede puderam centralizar todas as informações em um único local, permitindo que eles gerenciassem facilmente usuários e recursos em toda a rede. O *Active Directory* também trouxe melhorias significativas na segurança e na capacidade de gerenciamento de diretivas de grupo.

Desde o seu lançamento, o *Active Directory* tem evoluído com o tempo e foi atualizado em cada nova versão do *Windows Server*. Hoje, o *Active Directory* é considerado um dos serviços de diretório mais poderosos disponíveis e é amplamente utilizado em organizações de todos os tamanhos.

O *Active Directory* possibilita que qualquer controlador de domínio seja o único ponto necessário para a administração de recursos publicados, que podem incluir periféricos, usuários, qualidade da conexão de rede para grupos de usuários e outros objetos.

O *Active Directory* oferece recursos aos administradores, permitindo que eles atribuam políticas em grandes empresas, instalem programas automaticamente e apliquem atualizações críticas em toda a organização. As redes do *Active Directory* podem variar de uma pequena instalação com alguns objetos a uma grande instalação com milhões de objetos.

De acordo com Param (2001), o *Active Directory* é um serviço de diretório do *Windows Server* que permite que as organizações mantenham informações centralizadas sobre os recursos e usuários da rede. Uma das características mais importantes do *Active Directory* é o uso do protocolo LDAP.

O *Active Directory* é um componente crítico da arquitetura de rede do *Windows Server*. Ele fornece um serviço de diretório que permite as organizações controlarem de forma centralizada as informações sobre os recursos dos usuários da rede e armazena informações de segurança da rede do Windows.

O *Windows Server* utiliza o *Active Directory* e um controlador de domínio em uma rede, permitindo o acesso a todos os objetos armazenados no *Active Directory* por meio do protocolo LDAP.

Responsável por armazenar informações sobre objetos na rede e permitir que administradores e usuários acessem essas informações de maneira fácil e organizada. O diretório, que é onde as informações são armazenadas, contém dados sobre os objetos do *Active Directory*, que normalmente incluem recursos compartilhados como servidores, arquivos, impressoras e contas de usuário e computador da rede.

A segurança é uma parte integrante do *Active Directory*, e é alcançada por meio da autenticação de *login* e do controle de acesso aos objetos no diretório. Com apenas um *login* na rede, os administradores podem gerenciar a organização e os dados do diretório em toda a rede, enquanto os usuários autorizados têm acesso a recursos em qualquer lugar da rede. A administração baseada em políticas facilita o gerenciamento mesmo em redes muito complexas.

De acordo com Oliver (2003), o *Active Directory* é indiscutivelmente a principal ferramenta dos servidores Windows, sendo agora uma ferramenta comum em muitas empresas em todo o mundo. Sua introdução no mercado teve um impacto significativo no centro da plataforma utilizada pelos usuários do Windows.

Atualmente, gerenciar uma rede Windows com uma base de dados descentralizada seria bastante desafiador e, com o *Active Directory*, a rede se torna mais segura e mais simples de ser administrada.

Existe uma forte conexão entre o *Active Directory* e o DNS, de forma que não é possível instalar o *Active Directory* sem ter o DNS. Na verdade, o *Active Directory* é construído sobre o DNS (*Domain Name System*).

5.1 DNS

DNS (*Domain Name System*) é um protocolo utilizado para traduzir nomes de domínio em endereços IP. No contexto do *Active Directory* (AD), o DNS é um

componente essencial, pois é utilizado como serviço localizador para resolver nomes de domínio, nomes de serviço do AD e nomes de sites em endereços IP.

No AD, o DNS é utilizado para nomear e localizar objetos dentro do diretório. Por exemplo, quando um cliente do AD precisa localizar um controlador de domínio, ele consulta o servidor DNS configurado para o domínio e solicita o registro SRV (*Service Location*) para o controlador de domínio.

Além disso, as zonas de DNS podem ser armazenadas no *Active Directory*. Isso significa que os arquivos da zona primária podem ser armazenados no AD para replicação em outros controladores de domínio. Isso simplifica a administração e melhora a confiabilidade do serviço DNS.

A estrutura hierárquica do DNS é semelhante à estrutura hierárquica do AD. Ambos usam uma estrutura baseada em árvore para organizar os objetos. Além disso, o nome do domínio DNS é o mesmo nome utilizado para o domínio do AD e ambos têm uma estrutura idêntica para a mesma organização. Por exemplo, *Microsoft*.com é um domínio DNS e um domínio do AD.

Quando uma nova árvore de domínio é criada em uma floresta existente, ou mesmo um nó filho da mesma árvore, uma relação de confiança da raiz da árvore é estabelecida por padrão. Em uma floresta, várias árvores de domínio podem pertencer à mesma floresta. Uma relação de confiança é criada automaticamente entre o domínio raiz da floresta e os domínios raiz de cada árvore.

Em resumo, o DNS é uma parte crítica da infraestrutura do *Active Directory*, pois é usado para localizar e nomear objetos dentro do diretório. O uso correto do DNS ajuda a garantir que o AD esteja funcionando corretamente e que os usuários tenham acesso aos recursos necessários.

A seguir, apresentaremos as camadas da estrutura lógica do *Active Directory*, ou seja, a forma como ele é visualizado pelos usuários e administradores do domínio.

5.2 Camadas de estrutura lógica do *Active Directory*

Quando os administradores e usuários utilizam as ferramentas de administração e pesquisa do AD, eles são apresentados aos elementos que constituem a estrutura do AD.

A localização do armazenamento das informações do *Active Directory* e a sincronização entre os DCs são determinadas pela sua estrutura física. No entanto, a

estrutura física pode diferir da estrutura lógica, que é composta por vários elementos, tais como Domínios, Árvore, Floresta, Relação de Confiança, Objeto do AD, Unidades Organizacionais e Esquemas. Cada um desses elementos será detalhado nas próximas seções.

5.2.1 Domínios

Os domínios no *Active Directory* são considerados unidades de replicação, os quais são responsáveis por gerenciar objetos, tais como usuários, grupos e computadores, definindo a fronteira administrativa. Cada domínio possui suas próprias diretivas de segurança e relações de confiança com outros domínios.

Qualquer alteração feita em um dos controladores de domínio é replicada para todos os outros controladores do domínio. Cada domínio é identificado por um sistema de nomes de domínios (DNS) e requer pelo menos um controlador de domínio. Se for necessário, o administrador pode criar vários domínios de forma fácil e rápida para atender às necessidades da rede.

De acordo com Santos e Câmara (2002), os domínios são uma divisão lógica no *Active Directory*, que tem como finalidade proporcionar segurança e replicação de diretórios. Os administradores de domínio têm a responsabilidade de criar, excluir e gerenciar todos os objetos que estão localizados no domínio designado. Eles também podem atribuir e redefinir senhas, além de delegar autoridade administrativa para outros usuários confiáveis em relação aos recursos da rede.

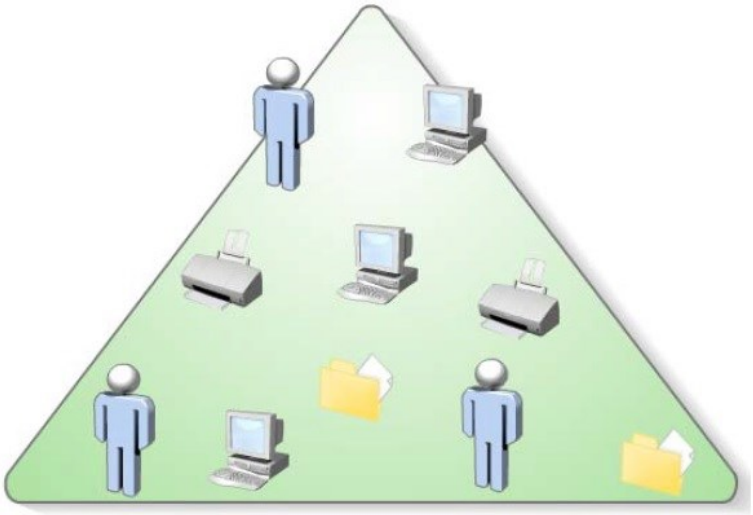
O administrador tem a opção de não criar domínios adicionais apenas para organizar as divisões e departamentos da empresa. Em vez disso, é possível utilizar unidades organizacionais dentro de um único domínio para essa finalidade. Ao criar um grupo, o gerenciamento de contas e recursos no domínio fica mais fácil.

O administrador pode então atribuir configurações de diretiva de grupo e incluir usuários, grupos e computadores. Isso simplifica significativamente a carga administrativa ao usar um único domínio. Além disso, o uso de políticas de grupo (GPO) por grupo permite que o administrador estabeleça como os recursos do domínio são acessados, configurados e utilizados. É importante observar que essas políticas são aplicadas somente no domínio e não entre diferentes domínios.

Através da Figura 1, é possível visualizar de forma evidente um domínio, que contém diversos objetos, tais como usuários, computadores, grupos, impressoras,

aplicativos, dentre outros. A seguir, será feita a descrição detalhada dos objetos presentes no AD.

Figura 1 - Domínio



Fonte: De autoria própria

5.2.2 Objetos do *Active Directory*

Cada entidade no *Active Directory* é representada por um objeto único, que pode ser um usuário, um computador, uma impressora, uma aplicação ou dados compartilhados. Além disso, um objeto pode funcionar como um recipiente para outros objetos. Por exemplo, um objeto Arquivo possui atributos como nome, localização e tamanho, enquanto um objeto Usuário do *Active Directory* deve conter atributos como nome, sobrenome e endereço de e-mail do usuário.

Segundo Posey (2006), ao criarmos objetos no *Active Directory*, podemos incluir informações relacionadas aos atributos de um objeto. Por exemplo, ao criar um objeto de usuário, é necessário incluir as informações básicas, como nome de usuário e senha, mas também é possível incluir outras informações, como endereço e número de telefone do usuário.

5.2.3 Unidades Organizacionais (UOs)

Em alguns casos, o domínio de uma organização pode ser muito grande e conceder acesso a todas as áreas possivelmente pode ser prejudicial. Por exemplo, se for necessário contratar pessoas para trabalhar em serviços específicos do *Active*

Directory, sem conceder acesso a todo o domínio, pode ser criado um usuário com privilégios específicos, como um administrador responsável pela folha de pagamento do grupo de contabilidade, conforme ilustrado na Figura 2.

Isso permite que o administrador do domínio conceda privilégios limitados a esse usuário, concedendo acesso total ou parcial à folha de pagamento. É possível criar administradores para grupos específicos, como o gerente do departamento jurídico, que terá controle total sobre o grupo jurídico, conforme mostrado na Figura 2. A ideia é subdividir o domínio em Unidades Organizacionais ou UOs.

Figura 2 - Unidade Organizacional

Fonte: De autoria própria

De acordo com (Anderson et al, 2001), a Unidade Organizacional (UO) é responsável por conceder controle sobre um conjunto de contas de usuários e/ou máquinas para um grupo específico de usuários. Essa funcionalidade permite, por exemplo, que um conjunto de pessoas em um determinado departamento possa redefinir senhas sem precisar torná-las administradoras com mais poderes do que o necessário.

Além disso, é possível restringir o grupo de pessoas que têm permissão para alterar as senhas. Essa abordagem ajuda a manter um controle mais granular sobre as permissões na rede, garantindo a segurança e a organização da estrutura.

De acordo com Shimonski (2005), ao instalar o *Active Directory* em uma organização, é fundamental levar em conta o sistema utilizado por ela e garantir que determinadas configurações importantes sejam implementadas. Uma dessas

configurações essenciais é o planejamento do ambiente local do usuário, por meio da criação de políticas que limitem seus acessos e concedam determinados privilégios.

5.2.4 Árvore

Conforme a Microsoft (2023) o *Active Directory*, uma árvore é um conjunto de um ou mais domínios interconectados em uma hierarquia lógica. É possível ter uma ou mais árvores no mesmo ambiente do *Active Directory*, dependendo da necessidade da organização.

Cada árvore tem um domínio raiz, que é o primeiro domínio criado na árvore e é considerado o ponto de entrada para a árvore. Cada domínio subsequente na árvore é filho do domínio pai e é conectado ao pai por um relacionamento de confiança transitiva.

As árvores no *Active Directory* permitem que organizações estruturem seus recursos de rede de maneira mais organizada e eficiente, permitindo melhor gerenciamento e controle de recursos. As árvores também podem ser utilizadas para impor políticas e restrições específicas em grupos de usuários e recursos da rede.

Algumas informações importantes sobre árvores no *Active Directory* incluem:

- As árvores podem ser criadas durante a instalação do *Active Directory* ou posteriormente por meio da criação de um novo domínio e sua associação a uma árvore existente.
- As árvores podem ter vários níveis de profundidade, permitindo uma estruturação flexível para diferentes necessidades organizacionais.
- As árvores são separadas logicamente umas das outras, o que significa que cada árvore pode ter suas próprias políticas de segurança, configurações e administração.
- Os nomes dos domínios em uma árvore devem ser exclusivos, mas podem ter subdomínios para ajudar a organizar a estrutura.
- As árvores também suportam a replicação de dados entre os domínios, permitindo que informações e recursos de rede sejam compartilhados entre diferentes partes da estrutura.

5.2.5 Floresta

Conforme destacado no contexto no *Active Directory* (2019), uma floresta é uma estrutura lógica que representa um conjunto de um ou mais domínios em uma única estrutura hierárquica, cada um com seu próprio conjunto de objetos e políticas.

Cada domínio dentro da floresta compartilha uma única árvore de nomes, o que significa que cada domínio pode ser referenciado usando um nome completo distinto, que inclui o nome do domínio e o nome da floresta.

A floresta do *Active Directory* também possui um controlador de domínio raiz, que é o primeiro controlador de domínio instalado na floresta. O controlador de domínio raiz é responsável por manter a segurança e a integridade da floresta e por replicar informações de diretório entre os domínios.

Além disso, as florestas permitem que os usuários acessem recursos em qualquer domínio dentro da floresta sem precisar autenticar novamente, desde que tenham as permissões adequadas. Isso é possível porque a floresta compartilha uma única hierarquia de segurança.

As florestas também permitem o estabelecimento de relações de confiança entre domínios e florestas. As relações de confiança permitem que os usuários autenticados em uma floresta acessem recursos em outra floresta sem precisar autenticar novamente.

Em resumo, uma floresta no *Active Directory* é uma estrutura lógica que fornece um meio de gerenciar e organizar um ou mais domínios em uma única hierarquia, permitindo o compartilhamento de informações de diretório e o acesso a recursos em toda a estrutura.

5.2.6 Relação de Confiança

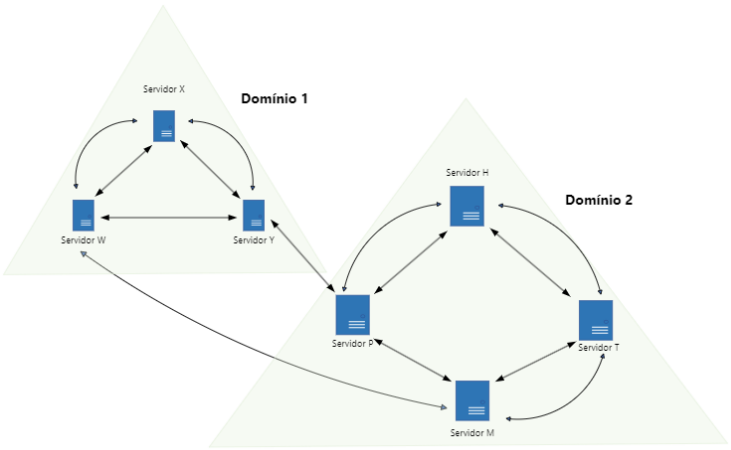
Quando uma nova árvore de domínio é criada dentro de uma floresta existente, ou mesmo um novo nó é adicionado à árvore existente, uma relação de confiança é automaticamente estabelecida com a raiz da árvore. O *Active Directory* consiste em uma estrutura hierárquica composta por um ou mais domínios, e várias árvores de domínio podem coexistir na mesma floresta.

Na floresta, uma relação de confiança é estabelecida automaticamente entre o domínio raiz da floresta e os domínios raiz de cada árvore.

De acordo com Santana (2000), ao usar domínios em uma rede, é possível refletir a estrutura de uma empresa. Quando vários domínios são utilizados, é estabelecido o conceito de relação de confiança, que permite aos usuários de ambos os domínios acessar recursos nesses domínios.

No *Windows Server 2019*, as relações de confiança podem ser bidirecionais e transitivas. Por exemplo, se o servidor X confia no servidor Y e Y confia no servidor W, o servidor X também confiará no servidor W. Além disso, a Figura 3 ilustra um exemplo de várias relações de confiança entre servidores.

Figura 3 - Relação de Confiança



Fonte: De autoria própria

5.2.7 Esquema do *Active Directory*

O conjunto de regras que definem quais tipos de objetos e informações podem ser armazenados no *Active Directory* é chamado de Esquema do *Active Directory*. As definições do Esquema são armazenadas como objetos no próprio diretório, permitindo que o *Active Directory* as gerencie com as mesmas operações utilizadas para gerenciar outros objetos no diretório. As definições do Esquema incluem dois tipos de objetos: atributos e classes, que também são conhecidos como objetos.

5.2.8 Integração do DNS ao *Active Directory*

De acordo com Posey (2005), tanto o *Active Directory* quanto o DNS têm a mesma estrutura hierárquica, embora sejam implementados de maneiras diferentes

para diferentes finalidades. O nome do DNS é o mesmo utilizado para o *Active Directory* e eles possuem a mesma estrutura para a organização. Isso significa que um domínio DNS, como *Microsoft*.com, é também um domínio *Active Directory*.

De acordo com o que foi mencionado anteriormente, as zonas do DNS podem ser armazenadas no *Active Directory*. Caso estejamos utilizando o serviço DNS do *Windows Server 2019*, os arquivos de zona principal podem ser armazenados no *Active Directory*, possibilitando a replicação em outros controladores de domínio.

O AD emprega o DNS como um serviço de localização, solucionando o domínio, o site e os nomes de serviço do AD para um endereço IP. Ao acessar o domínio do *Active Directory*, o usuário pode consultar o servidor DNS configurado para encontrar o endereço IP do serviço LDAP em execução em um controlador de domínio específico.

Durante o desenvolvimento do *Active Directory* pela *Microsoft*, uma das principais prioridades era garantir a compatibilidade com o DNS. O AD foi criado não apenas para ser completamente compatível com o DNS, mas também para garantir que os dois sistemas não pudessem funcionar separadamente. Se o DNS não estiver funcionando corretamente, o AD também não funcionará.

Foi realizada a configuração automática do endereço IP para evitar conflitos de IP na rede TCP/IP. Como cada computador na rede precisa ter um endereço IP exclusivo, o protocolo DHCP (*Dynamic Host Configuration Protocol*) é utilizado para alocar esses endereços de forma dinâmica. Além disso, é necessário interagir com um servidor DNS para garantir o correto funcionamento da rede.

De acordo com as informações apresentadas por Araujo (1997), configurar o endereço IP de um computador conectado a uma rede da Internet não é suficiente para garantir o seu funcionamento adequado. É necessário também configurar outros parâmetros de rede.

Para que a máquina possa ser configurada automaticamente, um cliente DHCP busca identificar um ou mais servidores DHCP que possam fornecer os parâmetros necessários.

5.3 Autenticação no AD

A autenticação é uma medida essencial para garantir a segurança da comunicação. É importante que os usuários comprovem suas identidades para as

pessoas com quem estão se comunicando e verifiquem a identidade de outras pessoas. No entanto, em uma rede, pode ser difícil comprovar a identidade das pessoas, já que elas não estão fisicamente presentes durante a comunicação. Isso pode permitir que um usuário mal-intencionado intercepte mensagens ou se faça passar por outra pessoa física ou jurídica.

O certificado digital é um meio confiável de autenticação que permite verificar a identidade de uma pessoa ou organização. Ele utiliza técnicas de criptografia para garantir a segurança da comunicação entre as partes, especialmente em situações em que não há contato físico entre elas. O uso dessas técnicas reduz significativamente o risco de interceptação, alteração ou falsificação de mensagens por pessoas mal-intencionadas. Além disso, a criptografia dificulta a falsificação de certificados, garantindo que as entidades envolvidas na comunicação são de fato quem dizem ser.

De acordo com Melber (2005), os administradores de rede buscam informações sobre quem está utilizando o sistema, em quais computadores e quais recursos estão sendo acessados, entre outras informações relevantes. No entanto, nem todos os usuários têm acesso à rede e aos seus recursos, apenas aqueles que estão autenticados no domínio têm permissão para entrar.

Quando o usuário insere suas credenciais de acesso, o *Active Directory* verifica se ele tem permissão para acessar o domínio solicitado. A autenticação de usuários torna a rede mais segura e impede o acesso de usuários não autorizados.

Serão apresentados adiante os benefícios decorrentes da utilização de grupos para gerenciar usuários, permitindo a definição de políticas de acesso a recursos para os grupos e não para usuários individuais. Isso simplifica o trabalho do administrador de rede, tornando a administração mais eficiente e organizada.

5.4 Criando grupos de usuários e definindo diretivas por grupos

De acordo com a Microsoft (2023), um grupo no *Active Directory* é uma unidade de gerenciamento que contém contas de usuários, computadores, contatos e outros grupos. Os usuários e computadores que são adicionados a um grupo específico são chamados de membros do grupo.

Os grupos podem ser categorizados por seu escopo e tipo. O escopo de um grupo determina a extensão em que o grupo é aplicado no domínio ou floresta do *Active Directory*.

As configurações de Diretiva de Grupo no *Active Directory* são utilizadas para gerenciar vários aspectos do ambiente de trabalho do usuário. Isso inclui a disponibilidade de programas para os usuários, programas que aparecem na área de trabalho do usuário e as opções disponíveis no menu Iniciar.

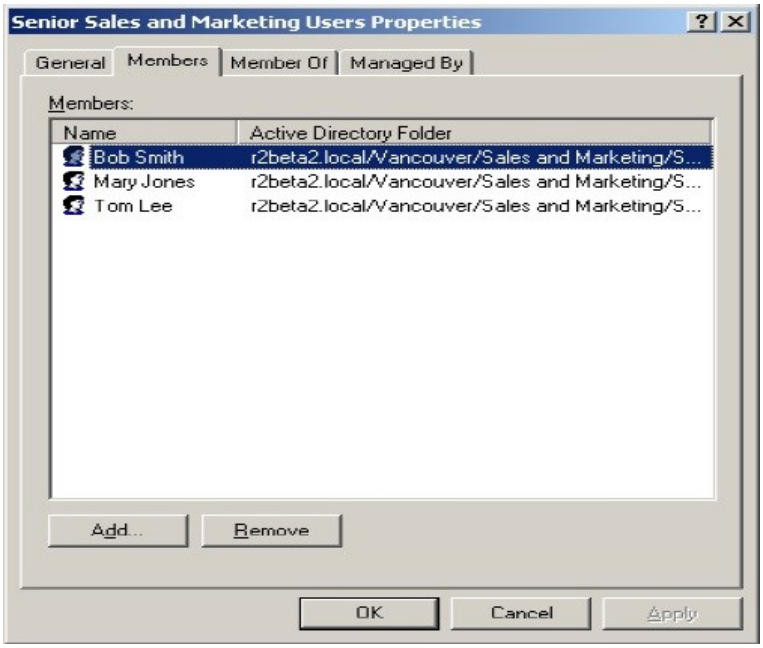
Essas configurações são definidas em um objeto de Diretiva de Grupo, que é associado a objetos específicos do *Active Directory*, como sites, domínios ou unidades organizacionais.

O uso de grupos no *Active Directory* pode facilitar a administração ao permitir a atribuição de um conjunto comum de permissões e direitos para várias contas simultaneamente, em vez de atribuir essas permissões e direitos individualmente para cada conta. Isso pode simplificar ainda mais a administração, permitindo a atribuição de permissões para um recurso compartilhado a um grupo, em vez de usuários individuais. Isso garante que todos os membros do grupo tenham o mesmo acesso ao recurso compartilhado.

De acordo com Tulloch (2005), o administrador do domínio adiciona um usuário em um ou mais grupos de acordo com as necessidades do seu perfil. Entretanto, esse usuário pode precisar de permissões especiais adicionais que não foram fornecidas pelo administrador.

Por exemplo, na Figura 4, apenas Bob Smith, Mary Jones e Tom Lee recebem a política em execução. Inicialmente, o grupo global Sênior Venda é criado usando Usuários e Computadores do *Active Directory* e somente esses três usuários são adicionados como membros. Esses usuários terão permissões especiais adicionais, incluindo controle total sobre o grupo.

Figura 4 - Grupos de Usuários e Diretivas



Fonte: Tulloch (2005)

De acordo com Tulloch (2005), um administrador pode conceder a um usuário permissões de grupo e pode dar a ele permissões especiais diretamente em sua conta, além de cadastrá-lo em vários outros grupos.

A Figura 5 ilustra o conceito de grupo de usuários, no qual o grupo Contabilidade tem acesso a um recurso compartilhado na rede. Todos os usuários que fazem parte do grupo Contabilidade também têm permissão para acessar o recurso compartilhado com os mesmos níveis de acesso do grupo, já que os usuários herdam as permissões do grupo.

Figura 5 - Grupos de Usuários

Fonte: De autoria própria

Podemos analisar algumas informações relevantes relacionadas aos grupos de usuários, tais como:

- Grupos são compostos por diversas contas de usuários.
- Os membros de um grupo possuem as mesmas permissões do grupo ao qual pertencem.
- Um usuário pode pertencer a vários grupos.
- Grupos podem ser incluídos em outros grupos.
- Contas de computador também podem fazer parte de grupos.

A Diretiva de Grupo não se aplica somente a usuários e computadores clientes, mas também a servidores membros, controladores de domínio e a qualquer computador dentro do escopo de gerenciamento que esteja contido no domínio.

Por padrão, a Diretiva de Grupo do *Active Directory* é aplicada no nível do domínio, ou seja, é aplicada ao domínio como um todo e afeta todos os usuários e computadores dentro dele. Isso ocorre no nível acima da raiz de Usuários e Computadores do *Active Directory*.

A Diretiva de Grupo do *Active Directory* inclui as configurações de diretiva para usuários e computadores. É possível aplicar diretivas para computadores específicos ou usuários específicos, dependendo da hierarquia de prioridade definida para cada departamento ou organização dentro da empresa. Se uma diretiva for aplicada em nível de computador e estiver no topo da hierarquia de diretivas para aquele domínio, então todos os usuários seguirão as políticas definidas para aquele computador, de acordo com as normas estabelecidas pelo administrador do domínio.

As diretivas por grupos tornam o gerenciamento da rede mais fácil para o administrador. Por exemplo, quando um novo funcionário é contratado, em vez de definir políticas específicas para esse usuário, é possível simplesmente avaliar quais acessos ele precisa ter e atribuí-lo a um ou mais grupos. Dessa forma, de acordo com a necessidade desse usuário, ou mesmo em caso de uma promoção, é possível conceder e revogar acessos apenas adicionando ou removendo o usuário dos grupos de diretivas correspondentes.

Segundo o autor Tulloch (2005), a política de grupo é extremamente importante e essencial para a criação de um projeto bem-sucedido no *Active Directory* com um planejamento de diretiva de grupos. Se os locais, domínios e OUs forem criados incorretamente, a política do grupo será difícil de ser utilizada e os problemas serão difíceis de serem identificados.

Portanto, a primeira etapa durante o planejamento é estabelecer regras para a política do grupo na rede, planejando como o próprio *Active Directory* o que será executado. Esse planejamento envolve decisões como: quantas florestas serão abertas (uma ou várias), quantas árvores de domínio, quantos domínios filhos, qual a estrutura de cada domínio, entre outras.

Cada uma dessas decisões deve ser tomada com algumas questões em mente: "Qual será o impacto das minhas decisões? Como a política do grupo será implementada na minha empresa?". Ao fazer essas perguntas, é possível gerenciar melhor as diretivas e grupos, evitando erros futuros e facilitando o gerenciamento pelo administrador da rede.

Os objetos do *Active Directory* que podem receber diretivas são apenas Computadores e Usuários. A aplicação da diretiva não é possível em grupos de segurança, pois para fins de desempenho, os grupos de segurança são utilizados para filtrar a diretiva por meio de uma entrada de Controle de Acesso (ACE) chamada "Aplicar Diretiva de Grupo". Essa entrada pode ser definida como "Permitir" ou "Negar", ou então, não ser configurada.

No que diz respeito às políticas de acesso, é importante determinar se um usuário tem permissão para acessar qualquer computador do domínio. Embora um usuário possa efetuar *login* em qualquer computador dentro do domínio, se um computador estiver utilizando uma política de autenticação de computador, apenas usuários locais poderão acessá-lo. No entanto, a política de autenticação de computador tem precedência sobre a política de usuário.

Na seção seguinte, será apresentado o processo de compartilhamento de pastas por meio de grupos, no qual somente os usuários registrados nesses grupos terão permissão de acesso às pastas compartilhadas por eles.

5.5 Pastas compartilhadas

As pastas compartilhadas no *Active Directory* são utilizadas para apresentar os recursos compartilhados disponíveis em um computador. Em alguns casos, uma conexão com uma impressora é tratada como uma conexão com um recurso compartilhado. Esses recursos compartilhados podem ser uma pasta compartilhada, uma impressora compartilhada ou um tipo de recurso que não seja reconhecido pelo sistema.

Um recurso compartilhado no *Active Directory* permite que usuários acessem aplicativos, informações ou dados pessoais. O administrador pode decidir conceder ou negar permissões para cada recurso compartilhado. Atribuir permissões a grupos é uma maneira eficiente de gerenciar recursos compartilhados, já que o administrador pode adicionar ou remover usuários de grupos sem precisar reatribuir permissões individualmente. Isso simplifica a administração e evita erros de atribuição de permissões.

Cada usuário do domínio tem direito a uma pasta privada para armazenar seus arquivos, que pode ter uma limitação de espaço. Além disso, o administrador pode criar uma ou várias pastas compartilhadas, que podem ser acessadas por todos os usuários do domínio com permissões definidas pelo administrador. Essas permissões podem variar desde somente leitura até controle total ou alteração dos arquivos, ou ainda serem restritas a apenas um grupo específico de usuários.

Neste capítulo, foi apresentado algumas ferramentas do *Windows Server 2019*, apresentamos também a integração do DNS ao domínio do *Active Directory*, no qual o DNS possui o mesmo nome do domínio. Também foram apresentadas as camadas de estrutura lógica do AD, que é a forma como o AD é apresentado aos usuários e administradores. A autenticação de usuários no domínio foi destacada como uma medida importante para aumentar a segurança da rede.

No próximo segmento, será apresentado o uso do protocolo LDAP no AD, juntamente com os serviços que ele fornece.

6. UTILIZAÇÃO DO PROTOCOLO LDAP NO *ACTIVE DIRECTORY*

Conforme a obra de (Weltman, R., & Dahbura 2000) o LDAP (Protocolo de Acesso a Diretórios Leves) foi projetado para simplificar o acesso a serviços de diretório, proporcionando uma solução direta e segura para consulta e gerenciamento de informações em um diretório.

LDAP sugere que ele foi criado como uma solução simples para acessar serviços de diretório, sem a complexidade de outros protocolos similares. Ele define as operações que podem ser realizadas para consultar e alterar informações em um diretório, bem como a maneira segura de acessar essas informações. O LDAP é capaz de localizar e listar objetos de diretório, além de permitir consultas e gerenciamento do *Active Directory*.

O acesso dos clientes do *Active Directory* à rede e aos recursos compartilhados é realizado por meio da comunicação com os computadores do domínio. Para essa comunicação, é utilizado o protocolo LDAP para acessar os controladores de domínio e catálogos globais. O LDAP permite a consulta e modificação de informações no diretório de forma segura, bem como a localização de objetos de diretório e a administração do *Active Directory*.

O protocolo LDAP estabelece as regras para que um cliente possa se conectar a um servidor de diretório, bem como para executar as operações e compartilhar informações contidas no diretório.

6.1 Suporte do LDAP ao *Active Directory*

Ao utilizar o LDAP, o *Active Directory* possibilita a integração com serviços de diretório de outros fornecedores, já que o LDAP é um padrão aberto da Internet. O suporte do *Active Directory* ao LDAP é oferecido por meio de um objeto de provedor LDAP que faz parte do recurso ADSI (*Active Directory Service Interfaces*).

Esse recurso oferece suporte a interfaces de programação de aplicativos em linguagem C para o LDAP. Dessa forma, outros aplicativos de serviços de diretório podem ser facilmente modificados para acessarem informações no *Active Directory* utilizando o ADSI e o LDAP.

7. GPO (*GROUP POLICE*)

Segundo o autor Jeremy Moskowitz (2008), GPO (*Group Policy Object*) é um recurso do *Active Directory*, um serviço de diretório da *Microsoft*, que permite que os administradores de rede gerenciem as configurações dos computadores e usuários em uma rede.

Conforme Tulloch (2005), GPO é um conjunto de configurações de política que são aplicadas a um grupo de computadores ou usuários dentro de um domínio do *Active Directory*. As políticas de grupo são usadas para controlar as configurações de segurança, *software*, configurações de rede e outras opções em computadores e usuários dentro de uma rede.

Os administradores podem usar o console de Gerenciamento de Política de Grupo (GPMC) para criar, editar, gerenciar e atribuir GPOs a usuários e computadores específicos na rede. As configurações de política de grupo podem ser aplicadas a todos os computadores em um domínio ou a um subconjunto específico de computadores ou usuários, dependendo das necessidades da organização.

Em resumo, os GPOs são uma ferramenta essencial para gerenciar e manter a segurança e o desempenho de uma rede de computadores, permitindo que os administradores de TI gerenciem as configurações de políticas de grupo em larga escala de maneira eficiente e centralizada.

7.1 GPO - DESABILITAR PAINEL DE CONTROLE

Para desabilitar o Painel de Controle em um ambiente Windows usando as Políticas de Grupo (GPO), siga as etapas abaixo:

1. Abra o Editor de Política de Grupo. Você pode acessá-lo digitando "gpedit.msc" na caixa de pesquisa do menu Iniciar ou no Executar.
2. Navegue até Configuração do Computador > Modelos Administrativos > Painel de Controle.
3. Selecione a opção "Proibir acesso ao Painel de Controle e às suas ferramentas".

4. Clique em "Ativado" e, em seguida, clique em "Aplicar" e "OK" para salvar as alterações.

Depois de fazer isso, o Painel de Controle será desabilitado em todos os computadores que estão na mesma unidade organizacional (OU) do *Active Directory* que tiverem essa GPO aplicada a eles. É importante lembrar que essa configuração pode afetar as contas de usuário que precisam acessar o Painel de Controle para realizar tarefas administrativas. Se isso for necessário, você pode criar uma GPO separada para permitir que usuários específicos acessem o Painel de Controle.

7.2 GPO - DESABILITAR PROPRIEDADE DE LAN (*ETHERNET*)

Para desabilitar a propriedade da LAN (*Ethernet*) em uma GPO, siga as etapas abaixo:

1. Abra o Editor de Política de Grupo. Você pode acessá-lo digitando "gpedit.msc" na caixa de pesquisa do menu Iniciar ou no Executar.
2. Navegue até Configuração do Computador > Modelos Administrativos > Rede > Adaptadores de Rede.
3. Selecione a opção "Proibir que os usuários habilitem ou desabilitem uma conexão de rede".
4. Clique em "Ativado" e, em seguida, clique em "Aplicar" e "OK" para salvar as alterações.

Depois de fazer isso, a propriedade da LAN (*Ethernet*) será desabilitada e os usuários não poderão habilitar ou desabilitar a conexão de rede. É importante lembrar que essa configuração pode afetar os usuários que precisam habilitar ou desabilitar a conexão de rede para conectar-se a outras redes ou solucionar problemas de conectividade. Se isso for necessário, você pode criar uma GPO separada para permitir que usuários específicos habilitem ou desabilitem a conexão de rede.

7.3 GPO – BLOQUEIO CD/DVD/USB

Para realizar o bloqueio do driver de CD/DVD/USB utilizando as políticas de GPO, siga as seguintes etapas:

1. Abra o Editor de Política de Grupo. Você pode acessá-lo digitando "gpedit.msc" na caixa de pesquisa do menu Iniciar ou no Executar.

2. Navegue até Configuração do Computador > Modelos Administrativos > Sistema > Acesso de armazenamento removível.
3. Selecione a opção "Remova a funcionalidade 'Unidade de CD-ROM'" e/ou "Remova a funcionalidade 'Unidade de disquete'" e/ou "Remova o acesso à unidade USB".
4. Clique em "Ativado" para cada uma das opções selecionadas e, em seguida, clique em "Aplicar" e "OK" para salvar as alterações.

Depois de fazer isso, o uso de CD/DVD/USB será bloqueado em todos os computadores que estão na mesma unidade organizacional (OU) do *Active Directory* que tiverem essa GPO aplicada a eles. É importante lembrar que essa configuração pode afetar as tarefas diárias dos usuários que precisam usar esses dispositivos para realizar suas atividades. Se isso for necessário, você pode criar uma GPO separada para permitir que usuários específicos usem esses dispositivos.

7.4 GPO – CONFIGURAÇÕES DO INTERNET EXPLORER

As configurações do Internet Explorer podem ser configuradas usando a GPO. Para fazer isso, siga as etapas abaixo:

1. Abra o Editor de Política de Grupo. Você pode acessá-lo digitando "gpedit.msc" na caixa de pesquisa do menu Iniciar ou no Executar.
2. Navegue até Configuração do Computador ou Configuração do Usuário > Modelos Administrativos > Componentes do Windows > Internet Explorer.
3. Selecione a política que você deseja configurar. Por exemplo, você pode querer bloquear a opção de alterar a página inicial ou permitir que os usuários salvem senhas no Internet Explorer.
4. Clique em "Ativado" para cada uma das opções selecionadas e, em seguida, clique em "Aplicar" e "OK" para salvar as alterações.

Depois de fazer isso, as configurações do Internet Explorer serão configuradas de acordo com a GPO definida. É importante lembrar que essas configurações podem afetar a experiência do usuário no Internet Explorer, portanto, certifique-se de que as políticas sejam configuradas corretamente e adequadamente testadas antes de implantá-las em um ambiente de produção.

7.5 GPO – PAPEL DE PAREDE PADRÃO

A configuração base da GPO não possui um papel de parede padrão no *Active Directory*. No entanto, é possível configurar um papel de parede utilizando uma diretiva de grupo (GPO).

A configuração do papel de parede pode ser encontrada nas opções de Configuração do Usuário no Editor de Diretiva de Grupo. Para definir um papel de parede padrão, é necessário criar uma diretiva de grupo, configurar as opções de papel de parede e aplicá-la aos usuários ou grupos de usuários apropriados.

O papel de parede padrão do GPO no *Active Directory*, portanto, é configurado pelo administrador de rede de acordo com as necessidades e requisitos da organização.

7.6 GPO – DESABILITAR COMMAND

Para desabilitar um comando (como um executável ou um *script*) em um GPO (*Group Policy Object*), você pode seguir estes passos:

1. Abra o Editor de Gerenciamento de Diretiva de Grupo (GPMC) em um controlador de domínio.
2. Selecione a GPO apropriada na árvore de diretivas de grupo. Clique com o botão direito do mouse na GPO e selecione "Editar".
3. Na janela do Editor de Diretiva de Grupo, navegue até Configuração do Computador > Diretivas > Modelos Administrativos > Sistema.
4. Encontre a política "Impedir acesso à linha de comando" e dê um duplo clique sobre ela.
5. Selecione "Ativado" e clique em "Aplicar" e "OK".
6. Reinicie o computador para que as alterações entrem em vigor.

Depois de seguir esses passos, o acesso à linha de comando será impedido em todos os computadores afetados pela GPO. Observe que, se você precisar permitir o acesso à linha de comando novamente, basta voltar a política "Impedir acesso à linha de comando" e selecionar "Desativado" ou "Não configurado".

7.7 GPO – DESABILITAR REGEDIT

Para desabilitar o Regedit (Editor do Registro do Windows) através de uma GPO (Política de Grupo), siga os seguintes passos:

1. Abra o Editor de Gerenciamento de Política de Grupo (gpedit.msc).
2. Navegue até "Configuração do Computador" -> "Modelos Administrativos" -> "Componentes do Windows" -> "Editor do Registro".
3. Clique duas vezes em "Impedir o acesso ao Editor do Registro".
4. Selecione a opção "Habilitado" e clique em "OK".
5. Reinicie o computador para que as alterações tenham efeito.

Caso você queira aplicar essa configuração em vários computadores em um domínio, você pode criar uma GPO no Controlador de Domínio e vinculá-la às Unidades Organizacionais (OU) apropriadas. Depois, você pode usar o Editor de Gerenciamento de Política de Grupo para configurar a política em questão como mencionado acima.

No próximo capítulo, adentraremos o fascinante mundo da Autenticação Multifator (MFA), conforme delineado na introdução deste trabalho. Essa técnica de segurança, exigindo a apresentação de múltiplos fatores para acessar recursos, desempenha um papel crucial na proteção da identidade e no fortalecimento das políticas de acesso.

8. AUTENTICAÇÃO MULTIFATOR

Conforme a *Microsoft* (2023), *Multi-factor authentication* (MFA) é uma técnica de segurança que requer a apresentação de dois ou mais fatores de autenticação para permitir o acesso a um recurso. A autenticação multifator (MFA) desempenha um papel fundamental em fortalecer a política de gerenciamento de identidade e acesso (IAM). Em vez de se limitar à solicitação de um simples nome de usuário e senha, a MFA requer a apresentação de um conjunto de fatores de verificação adicionais, aumentando assim a segurança e reduzindo a probabilidade de sucesso de ataques cibernéticos.

De acordo com Gunawardana, Kushantha (2023), a autenticação multifatorial envolve o uso de dois ou mais elementos para verificar a identidade de um usuário durante o processo de *login*. Trata-se de um procedimento que requer múltiplas etapas de autenticação para garantir a identidade do usuário ao acessar uma ferramenta ou aplicação. Portanto, a MFA é uma medida fundamental para a segurança, uma vez que os nomes de usuário e senhas são vulneráveis e frequentemente reutilizados para acessar diversas contas, aumentando o risco de ataques.

Algumas das práticas recomendadas para as empresas com o objetivo de proteger seus recursos digitais e garantir a segurança dos acessos. Isso inclui a criação de diferentes níveis de acesso, como administradores, gerentes e outros usuários com privilégios reduzidos, bem como a implementação de políticas de senha robustas, que exigem a inclusão de caracteres especiais, letras maiúsculas e minúsculas, e números. Além disso, é aconselhável usar várias credenciais de segurança, como exigir que as senhas sejam alteradas regularmente, geralmente a cada 90 dias.

8.1 Autenticação Multifator (MFA) para *Active Directory* (AD)

No contexto do *Active Directory* (AD), o MFA pode ser implementado de várias maneiras, mas geralmente envolve a integração com serviços de autenticação de terceiros que fornecem os fatores de autenticação adicionais.

Aqui estão os passos básicos para implementar o MFA para o *Active Directory*:

- **Selecionar uma solução de MFA:** Existem várias soluções de MFA disponíveis no mercado, algumas das quais podem ser integradas ao *Active Directory*. É importante escolher uma solução que atenda aos requisitos de segurança, facilidade de uso e compatibilidade com o AD.
- **Configurar a solução de MFA:** Após a seleção da solução de MFA, é necessário configurá-la corretamente. Isso geralmente envolve a instalação do *software* de MFA em um servidor dedicado, a configuração do MFA para se comunicar com o AD e a configuração dos usuários do AD para uso do MFA.
- **Configurar a Autenticação de dois fatores (2FA):** O próximo passo é configurar a autenticação de dois fatores (2FA) para o AD. Isso envolve a configuração da solução de MFA para exigir um segundo fator de autenticação para acesso ao AD, além do nome de usuário e senha padrão.
- **Testar a implementação:** É importante testar a implementação do MFA para garantir que tudo esteja funcionando corretamente. Isso inclui testar a autenticação com o segundo fator, testar o acesso aos recursos do AD e testar a capacidade de gerenciamento do MFA.
- **Gerenciar e monitorar o MFA:** O último passo é gerenciar e monitorar o MFA. Isso envolve a criação de políticas de segurança para o MFA, a monitoração do uso do MFA pelos usuários e a solução de problemas em caso de problemas de autenticação.

É importante notar que a implementação do MFA para o *Active Directory* pode ser um processo complexo e requer um conhecimento detalhado do AD e das soluções de MFA disponíveis. No entanto, o MFA é uma técnica de segurança essencial para proteger o AD contra ameaças cibernéticas.

8.2 Autenticação Multifator (MFA) para AWS

A autenticação multifator (MFA) é uma recomendação da *Amazon* para reforçar a segurança dos recursos da AWS. A MFA acrescenta uma camada adicional de proteção, uma vez que exige que os usuários forneçam uma autenticação exclusiva proveniente de um dispositivo MFA compatível da AWS, além de suas credenciais de *login* padrão, ao acessar os sites ou serviços da AWS. Isso contribui para um ambiente mais seguro e confiável.

8.3 Dispositivos virtuais MFA

A autenticação multifatorial (MFA) pode ser implementada por meio de um autenticador virtual que funciona em dispositivos como telefones, emulando um dispositivo físico. Esses aplicativos de autenticação virtual utilizam o algoritmo de senha de uso único com marcação temporal (TOTP) e oferecem suporte para vários *tokens* em um único dispositivo. Durante o processo de *login*, os usuários são solicitados a inserir um código válido no dispositivo em uma segunda página da web.

É fundamental ressaltar que cada dispositivo MFA virtual alocado a um usuário deve ser exclusivo, o que impede que um usuário utilize o dispositivo MFA de outra pessoa para autenticação. No entanto, é importante observar que, devido à possibilidade de execução em dispositivos móveis não seguros, a MFA virtual pode não fornecer o mesmo nível de segurança oferecido pelas chaves de segurança FIDO.

Portanto, é recomendável que a MFA virtual seja utilizada temporariamente enquanto se aguarda a aprovação da compra do *hardware* apropriado ou enquanto se espera pela entrega do mesmo. Para obter uma lista de aplicativos compatíveis que podem ser utilizados como dispositivos MFA virtuais, é aconselhável consultar a página de Autenticação Multifator da AWS.

A integração da autenticação multifatorial (MFA) é uma medida crucial para fortalecer a segurança em ambientes digitais, especialmente ao considerar a transição para a computação em nuvem. A MFA, que envolve a apresentação de dois ou mais fatores de autenticação, desempenha um papel fundamental na proteção contra ameaças cibernéticas, como destacado no contexto do Active Directory (AD). Ao implementar a MFA para o AD, seguindo as práticas recomendadas de Smith, as organizações podem criar uma camada adicional de segurança ao acessar recursos na nuvem, como os oferecidos pela Amazon Web Services (AWS). A AWS, líder global em serviços em nuvem, reconhece a importância da MFA como uma recomendação para reforçar a segurança dos recursos. Além disso, ao explorar serviços específicos, como o *Amazon Elastic Computer Cloud* (Amazon EC2), a segurança é aprimorada com recursos como autenticação por chaves de criptografia e grupos de segurança. Assim, a implementação consistente da MFA, combinada com as soluções avançadas da AWS, cria um ambiente mais seguro e confiável para operações em nuvem.

9. COMPUTAÇÃO EM NUVEM

A ideia de computação em nuvem tem raízes que remontam às décadas de 1960, quando visionários como Joseph Carl Robnert Licklide já imaginavam uma rede interconectada de computadores que permitiria o acesso a programas e dados de qualquer lugar. A visão de John McCarthy sobre recursos de computação sendo usados como serviços, baseados no princípio '*pay as you go*', estabeleceu os fundamentos da computação em nuvem que conhecemos hoje. No entanto, foi apenas em 1997, com a tese de Ramnath Chellappa, que o termo 'computação em nuvem' começou a ganhar definição e forma.

Segundo Lecheta (2014), a *Amazon*.com desempenhou um papel fundamental na evolução da computação em nuvem. Com o lançamento da *Amazon* Web Services (AWS), a empresa se tornou uma líder global no fornecimento de infraestrutura de TI e serviços em nuvem. A AWS oferece uma variedade de serviços, desde hospedagem de sites até soluções de banco de dados e armazenamento, todos seguindo o modelo '*pay as you go*'. Isso proporcionou às empresas e desenvolvedores a flexibilidade e escalabilidade necessárias para atender às demandas de um mercado em constante evolução.

Portanto, a história da computação em nuvem está intrinsecamente ligada à visão pioneira de cientistas como John McCarthy e Joseph Carl Licklide, que moldaram os princípios fundamentais da computação em nuvem. Atualmente, a *Amazon* AWS desempenha um papel significativo na liderança desse mercado, oferecendo soluções confiáveis e inovadoras que atendem às necessidades de empresas e profissionais em todo o mundo. Essa conexão traça a evolução da computação em nuvem, desde suas origens até a liderança atual da *Amazon* AWS no setor, criando uma transição suave e coesa entre os dois temas.

9.1 Computação em nuvem com a AWS

Conforme Lecheta (2014), a *Amazon* Web Services (AWS) é reconhecida em todo o mundo como a plataforma de computação em nuvem mais amplamente adotada, oferecendo uma extensa gama de mais de 200 serviços em *Datacenters* distribuídos globalmente. Empresas que vão desde *startups* de rápido crescimento até

grandes corporações e órgãos governamentais escolheram a AWS para otimizar custos, aumentar a agilidade e acelerar seus processos de inovação.

A diversidade de serviços oferecidos pela AWS é notavelmente abrangente, abrangendo desde infraestrutura básica, como computação, armazenamento e bancos de dados, até soluções inovadoras como aprendizado de máquina, inteligência artificial, data *lakes*, análise de dados e Internet das Coisas. A AWS fornece um ambiente que facilita a migração de aplicativos para a nuvem e permite a concretização de projetos que antes seriam difíceis de conceber.

Uma das distinções marcantes da AWS é a profundidade de recursos disponíveis em seus serviços. Por exemplo, a AWS oferece a mais ampla seleção de bancos de dados especializados para atender às necessidades de diferentes tipos de aplicativos, garantindo a escolha da ferramenta mais adequada com base em critérios de custo e desempenho.

Além disso, a AWS tem a maior e mais dinâmica comunidade de usuários, com milhões de clientes ativos e uma vasta rede de parceiros em todo o mundo. Essa colaboração se estende por diversos setores e tamanhos de organização, abrangendo desde *startups* até grandes empresas e órgãos governamentais. A Rede de Parceiros da AWS (APN) inclui milhares de integradores de sistemas especializados nos serviços da AWS, bem como dezenas de milhares de fornecedores independentes de *software* (ISVs) que adaptam suas soluções para integração com a plataforma da AWS.

A AWS foi meticulosamente projetada para oferecer um dos ambientes de computação em nuvem mais seguros e flexíveis disponíveis atualmente. Sua infraestrutura central foi concebida para atender aos rigorosos requisitos de segurança de instituições militares, instituições bancárias globais e outras organizações que lidam com informações altamente sensíveis. Isso é respaldado por um conjunto avançado de mais de 300 recursos e serviços essenciais de segurança, conformidade e governança, que atendem a 143 normas de segurança e certificações de conformidade.

A AWS está constantemente na vanguarda da inovação, permitindo que você adote as tecnologias mais recentes para testes e desenvolvimento mais rápidos. Com um histórico de constante evolução, a AWS introduziu tecnologias pioneiras, como o AWS Lambda em 2014, que possibilitou aos desenvolvedores executarem código sem a necessidade de provisionar ou gerenciar servidores. A AWS também oferece o

Amazon SageMaker, um serviço totalmente gerenciado de aprendizado de máquina que permite que desenvolvedores e cientistas de dados utilizem essa tecnologia, mesmo sem experiência anterior.

Com mais de 17 anos de experiência, a AWS acumulou um histórico notável em termos de confiabilidade, segurança e desempenho, tornando-se a escolha confiável para aplicações críticas. A AWS continua liderando a indústria com a mais extensa experiência operacional em uma escala sem precedentes, superando qualquer outro provedor de serviços em nuvem.

9.2 *Amazon Elastic Computer Cloud* (*Amazon* EC2) na Infraestrutura de Computação em Nuvem

A computação em nuvem desempenha um papel fundamental na atualidade, permitindo que organizações acessem e gerenciem recursos computacionais de forma escalável e eficiente. Um dos serviços emblemáticos da *Amazon* Web Services (AWS), o *Amazon Elastic Computer Cloud*, amplamente conhecido como *Amazon* EC2, oferece capacidade de computação escalável sob demanda, revolucionando a maneira como empresas desenvolvem e implementam aplicativos, ao mesmo tempo em que controlam custos e aprimoram a agilidade no processo.

O *Amazon* EC2 possibilita a criação de servidores virtuais, ou seja, instâncias, conforme necessário. Os usuários têm a capacidade de configurar a segurança e as redes associadas a essas instâncias, bem como gerenciar o armazenamento de dados. Essa flexibilidade permite o dimensionamento vertical, possibilitando a adição de capacidade para lidar com cargas de trabalho intensivas, como processamentos mensais ou picos de tráfego em um site. Quando a demanda diminui, a capacidade pode ser reduzida, otimizando recursos e custos.

A instância do EC2 é configurada dentro de uma zona de disponibilidade em uma região específica. Para garantir a segurança, um grupo de segurança age como um *firewall* virtual controlando o tráfego de entrada e saída. A autenticação ou acesso à instância é assegurada por chaves de criptografia, com a chave privada armazenada localmente e a chave pública na instância. Além disso, o armazenamento é suportado por um volume do *Amazon Elastic Block Store* (EBS), garantindo a persistência dos dados.

O *Amazon* EC2 oferece diversos recursos de alto nível:

- **Instâncias:** São servidores virtuais escaláveis, adaptados às necessidades do usuário.
- **Imagens de Máquina da *Amazon* (AMIs):** AMIs são modelos pré-configurados que incluem o sistema operacional e *software* adicional, simplificando a configuração de instâncias.
- **Tipos de instância:** Existem várias configurações de CPU, memória, armazenamento e redes disponíveis, oferecendo flexibilidade para atender a diferentes requisitos.
- **Pares de Chaves:** São utilizados para proteger as informações de *login* das instâncias. A AWS armazena a chave pública, enquanto o usuário mantém a chave privada em local seguro.
- **Volumes de Armazenamento de Instâncias:** Destinam-se a dados temporários que são excluídos quando uma instância é interrompida, hibernada ou encerrada.
- **Volumes do *Amazon* EBS:** Fornecem armazenamento persistente para dados, sendo essenciais para aplicativos que exigem alta disponibilidade.
- **Regiões, Zonas de Disponibilidade e *Outposts*:** A infraestrutura da AWS está distribuída em várias regiões e zonas de disponibilidade, permitindo aos usuários escolherem onde hospedar seus recursos.
- **Grupos de Segurança:** Funcionam como *firewall*s virtuais, controlando protocolos, portas e intervalos de IP que podem acessar as instâncias.
- **Endereços IP Elásticos:** São endereços IPv4 estáticos que facilitam a migração de instâncias e aplicações em ambientes dinâmicos.
- **Tags:** São metadados que podem ser atribuídos aos recursos do *Amazon* EC2, simplificando a organização e a gestão.

O *Amazon* EC2 proporciona às organizações a capacidade de otimizar seus recursos de forma escalável. Ao explorar esses recursos, as empresas podem aumentar sua flexibilidade, agilidade e eficiência operacional na era da computação em nuvem.

10. DESENVOLVIMENTO

No contexto do desenvolvimento deste projeto, uma série de etapas cruciais foram executadas para concretizar a implementação de um sistema de autenticação multifator (MFA) integrado ao *Active Directory* na AWS. Primeiramente, procedeu-se à criação do serviço de diretório na plataforma AWS, estabelecendo assim a base da infraestrutura de autenticação. Em sequência, uma instância EC2, utilizando o sistema operacional *Windows Server 2019*, foi configurada, na qual se procedeu à instalação dos pacotes necessários para a configuração do *Active Directory* (AD).

Um momento decisivo no processo envolveu a integração bem-sucedida do *Windows Server com* o serviço de diretório previamente criado na AWS, o que possibilitou a autenticação e gerenciamento remoto e seguro dos usuários. Adicionalmente, foi criada uma segunda instância EC2, agora com o sistema Debian 12, que foi configurada como servidor RADIUS (*Remote Authentication Dial-In User Service).* Para essa configuração, foram empregadas ferramentas como o *FreeRADIUS*, responsável pela autenticação MFA, bem como o UFW, responsável pelo gerenciamento do *firewall*, garantindo, assim, a segurança do ambiente. O Netcat-OpenBSD também desempenhou um papel crucial na integração e comunicação entre os diversos componentes do sistema. Todas essas ações culminaram na criação de um ambiente de autenticação multifator sólido, integrado ao *Active Directory*, solidificando as bases para a segurança e gestão de identidades no ecossistema da AWS.

10.1 Ambiente de Teste

O ambiente de teste concebido ao longo do desenvolvimento deste projeto representa uma implementação robusta de autenticação multifator (MFA) perfeitamente integrada ao *Active Directory*, no contexto da infraestrutura AWS. Inicialmente, estabeleceu-se o serviço de diretório na plataforma AWS como o alicerce fundamental da infraestrutura de autenticação. Posteriormente, uma instância EC2, operando com o sistema *Windows Server 2019*, foi configurada e equipada com os pacotes imprescindíveis para a efetiva implementação do *Active Directory* (AD).

Um ponto crítico nesse processo reside na bem-sucedida integração do *Windows Server com* o serviço de diretório hospedado na AWS, o que viabilizou a

autenticação e o gerenciamento seguros e remotos dos usuários. Além disso, uma segunda instância EC2 foi provisionada, agora com o sistema Debian 12, sendo configurada para operar como um servidor RADIUS (*Remote Authentication Dial-In User Service*).

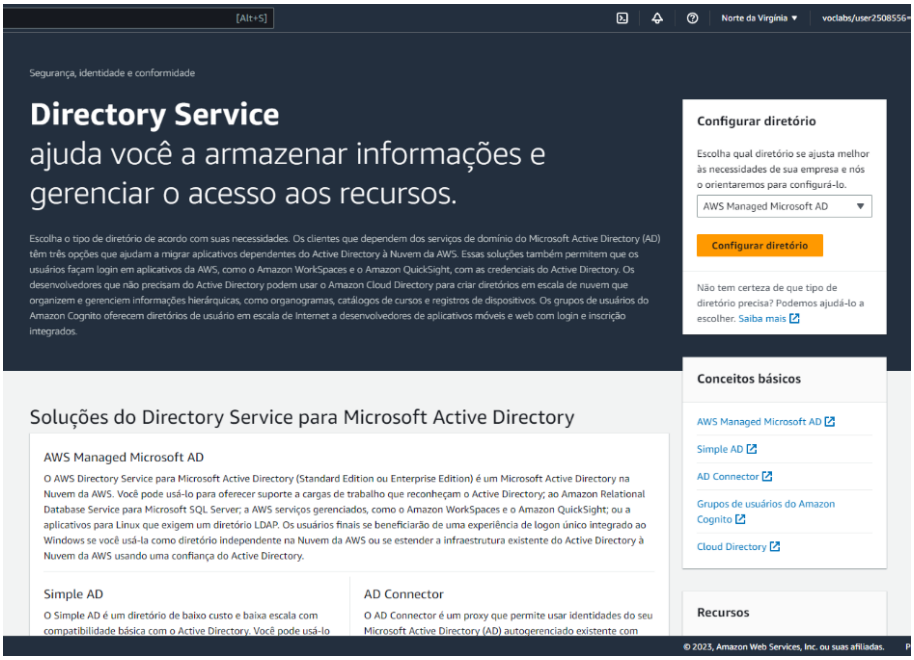
Para essa configuração, utilizaram-se ferramentas como o *FreeRADIUS*, que desempenhou o papel central na autenticação MFA, e o UFW, responsável pela eficaz administração do *firewall*, fortalecendo, assim, a segurança do ambiente.

O Netcat-OpenBSD também teve uma contribuição fundamental, simplificando a integração e a harmoniosa comunicação entre os componentes do sistema. Como resultado, esse ambiente de teste consolidou as bases para a autenticação multifator no contexto do *Active Directory*, representando um avanço significativo na busca pela segurança e administração de identidades no ecossistema AWS.

10.1.1 Criação do Serviço de Diretório na AWS

A Figura 6 exibe a interface destinada à criação do serviço de diretório. É possível acessar essa área por meio do console da AWS, pesquisando por "*Directory Service*". Avançou-se ao clicar sobre o botão "Configurar diretório".

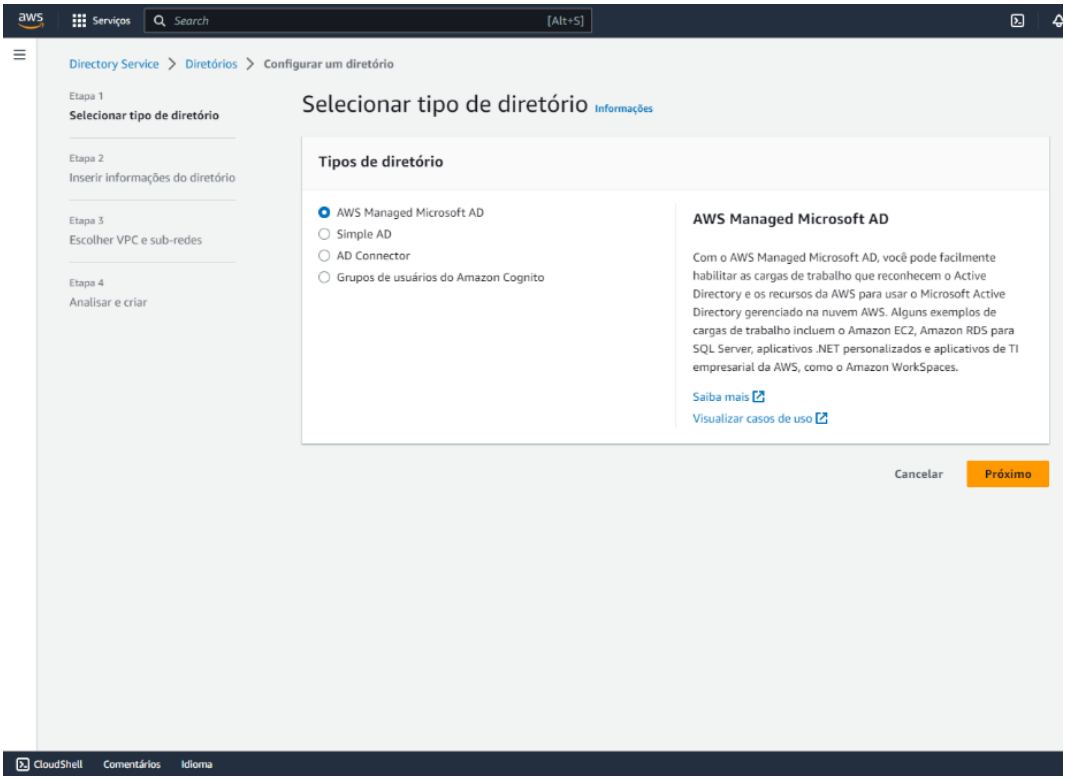
Figura 6 - Criação do Serviço de Diretório na AWS



Fonte: De autoria própria

A Figura 7 exibe os tipos de diretório, a saber: "*AWS Managed Microsoft AD",* "*Simple AD*", "AD Connector" e "Grupos de usuários do *Amazon* Cognito". Dentre essas opções, selecionou-se o diretório "*AWS Managed Microsoft AD*" devido à sua ampla gama de funcionalidades, que atendem às necessidades deste trabalho. Consequentemente, clicou-se sobre o botão "Próximo".

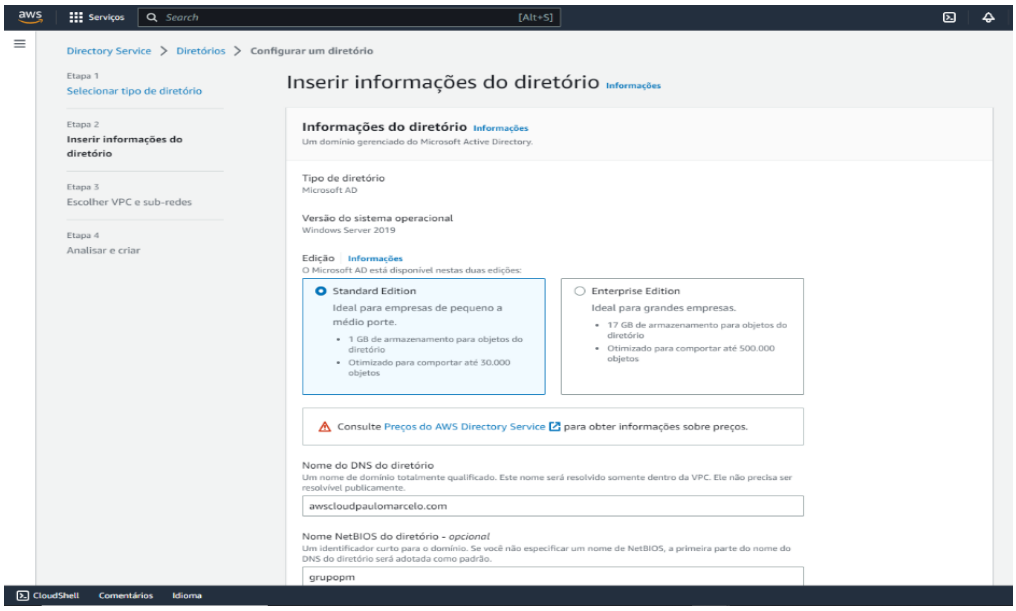
Figura 7 - Criação do Serviço de Diretório na AWS



Fonte: De autoria própria

A Figura 8 apresenta uma interface onde é possível escolher a edição do diretório, incluindo a versão "*Standard Edition*" (adequada para empresas de pequeno e médio porte) e a versão "Enterprise Edition" (indicada para grandes empresas), que se relacionam com a capacidade de armazenamento de informações. Considerando o ambiente de teste de pequeno porte, optou-se pela versão "*Standard Edition*".

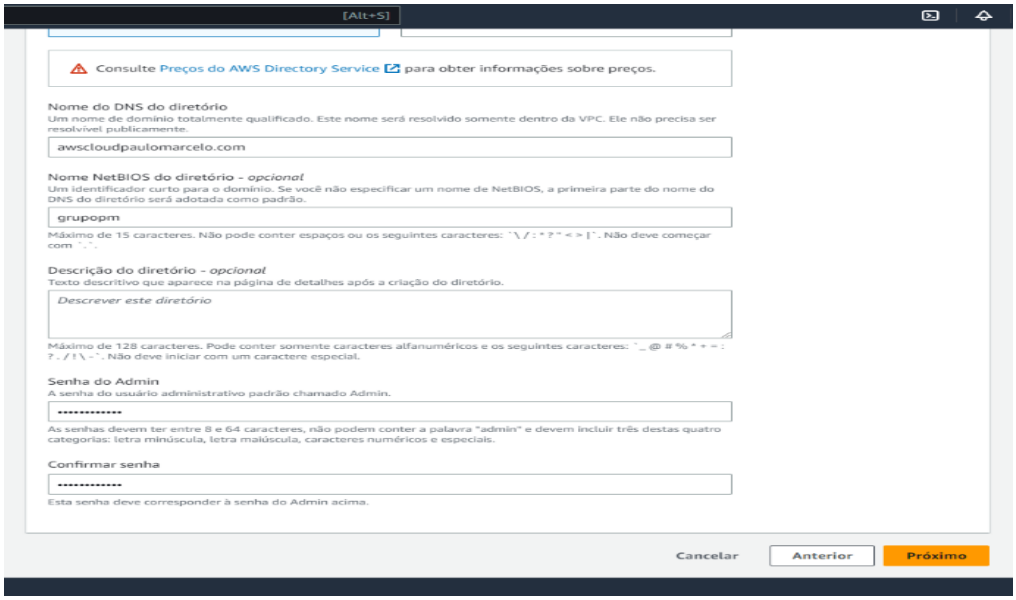
Figura 8 - Criação do Serviço de Diretório na AWS



Fonte: De autoria própria

A Figura 9 exibe a interface para o preenchimento dos campos relativos ao diretório. Preenchemos os campos "Nome do DNS do diretório", "Nome NetBIOS do diretório", "Senha do Admin" e "Confirmar senha" com as informações correspondentes: "AWScloudpaulomarcelo.com", "grupopm", "i4@0rOjUQA8#" e "i4@0rOjUQA8#". Após o devido preenchimento dos campos, avançou-se clicando sobre "Próximo".

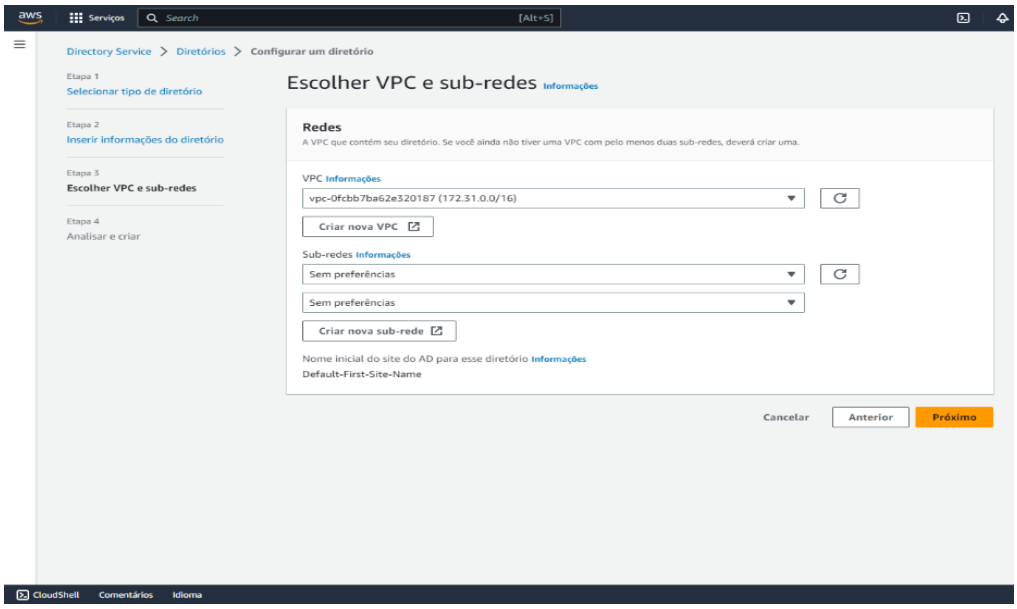
Figura 9 - Criação do Serviço de Diretório na AWS



Fonte: De autoria própria

A Figura 10 mostra a interface onde é possível selecionar a VPC e as sub-redes do diretório. Pode-se optar por uma VPC personalizada pelo cliente ou pela VPC padrão fornecida pela AWS. Para fins de teste, selecionamos a VPC padrão da AWS e mantivemos as opções referentes à escolha das sub-redes como "Sem preferência", permitindo que a AWS escolhesse as sub-redes mais apropriadas. Prosseguiu-se clicando sobre o botão "Próximo".

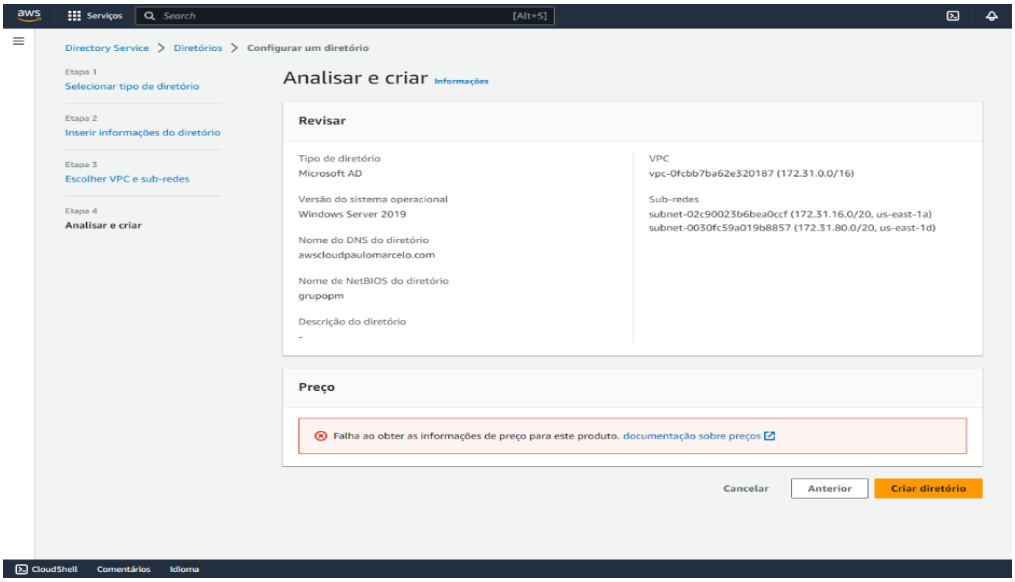
Figura 10 - Criação do Serviço de Diretório na AWS



Fonte: De autoria própria

A Figura 11 exibe a interface da AWS na qual é possível verificar todas as informações inseridas/selecionadas durante a criação do serviço de diretório. Essas informações abrangem o "Tipo de diretório", a "Versão do sistema operacional", o "Nome do DNS do diretório", o "Nome de NetBIOS do diretório", a "Descrição do diretório", a "VPC" e as "Sub-redes". Observou-se que todas as informações apresentadas estavam em conformidade com o que foi preenchido, o que permitiu continuar-se com a criação do serviço de diretório por meio do botão "Criar diretório".

Figura 11 - Criação do Serviço de Diretório na AWS

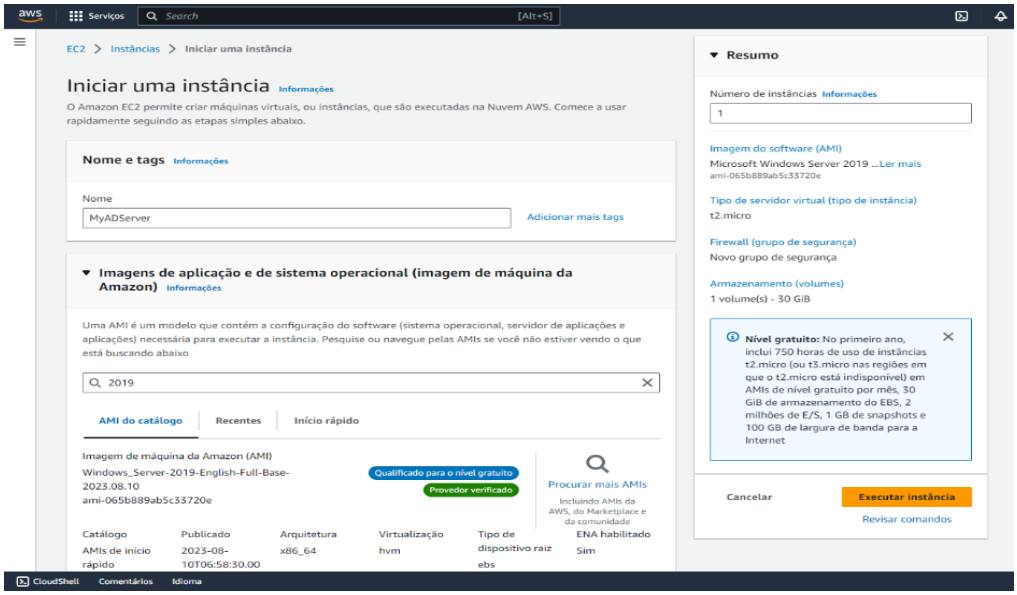


Fonte: De autoria própria

10.1.2 Criação do *Windows Server 2019* na AWS

A Figura 12 exibe a interface da plataforma AWS, na qual é possível criar uma instância. Essa interface pode ser acessada seguindo o caminho: EC2 > Instâncias > Iniciar uma instância. Além disso, na mesma imagem, é visível o campo "Nome e tags" que foi devidamente preenchido com o rótulo "*MyADServer*".

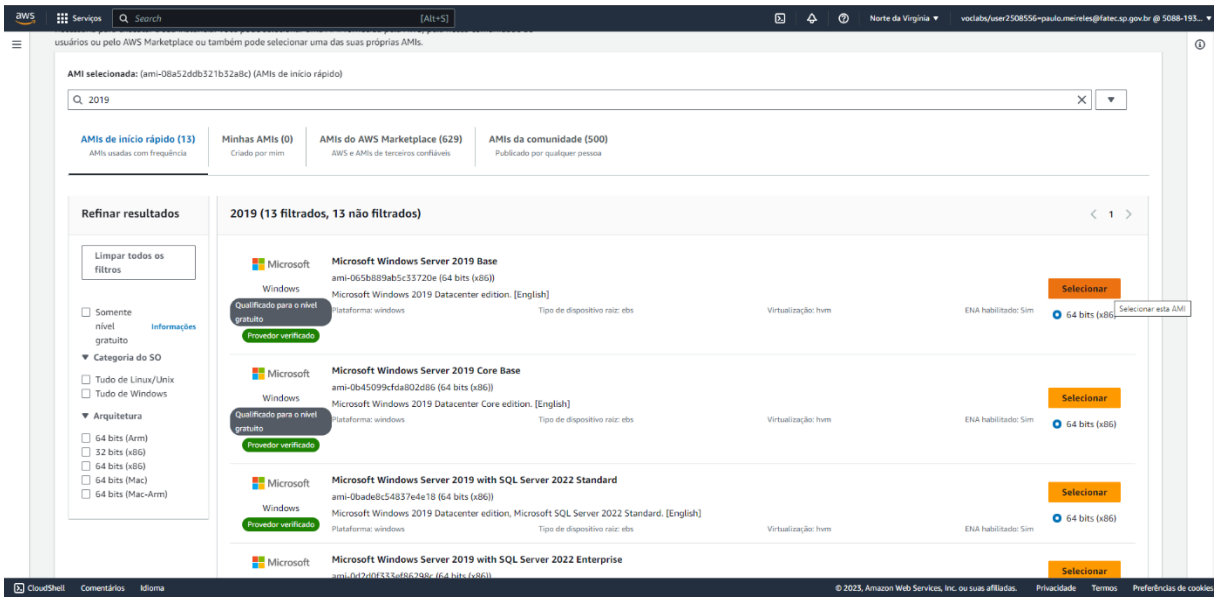
Figura 12 - Criação do *Windows Server* 2019 na AWS



Fonte: De autoria própria

A Figura 13 apresenta a interface da AWS na qual é possível selecionar o sistema operacional a ser instalado na instância EC2. Para este ambiente de teste, optou-se pelo sistema operacional "*Microsoft Windows Server 2019 Base*" com o propósito de configurá-lo para fornecer as funcionalidades do *Active Directory*.

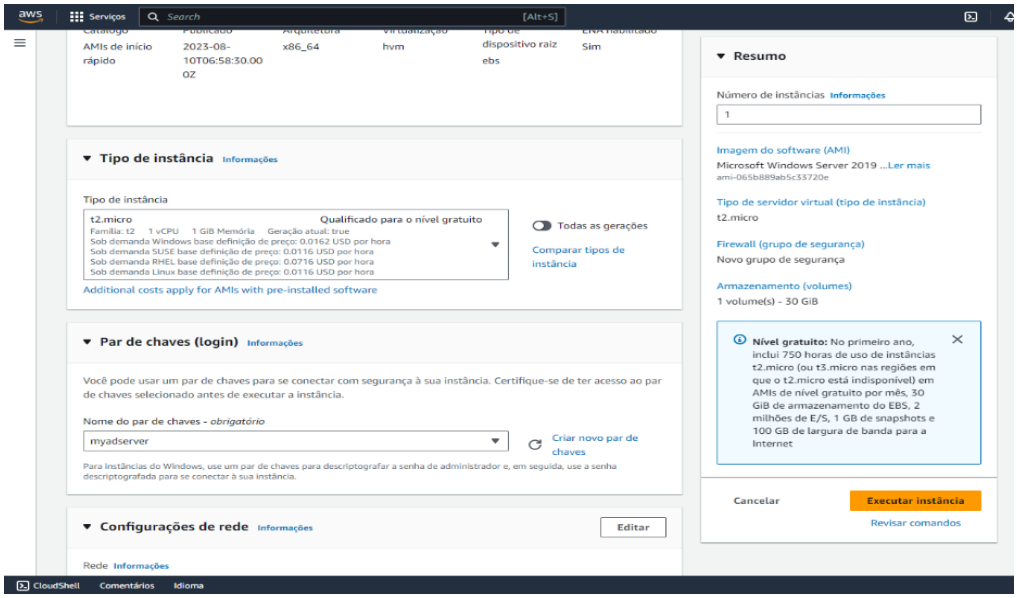
Figura 13 - Criação do *Windows Server* 2019 na AWS



Fonte: De autoria própria

Na Figura 14, é possível visualizar a interface da AWS que oferece a opção de selecionar um "Par de chaves (*login*)" já existente ou criar um. Neste contexto de teste, optou-se por utilizar um "Par de chaves" previamente existente.

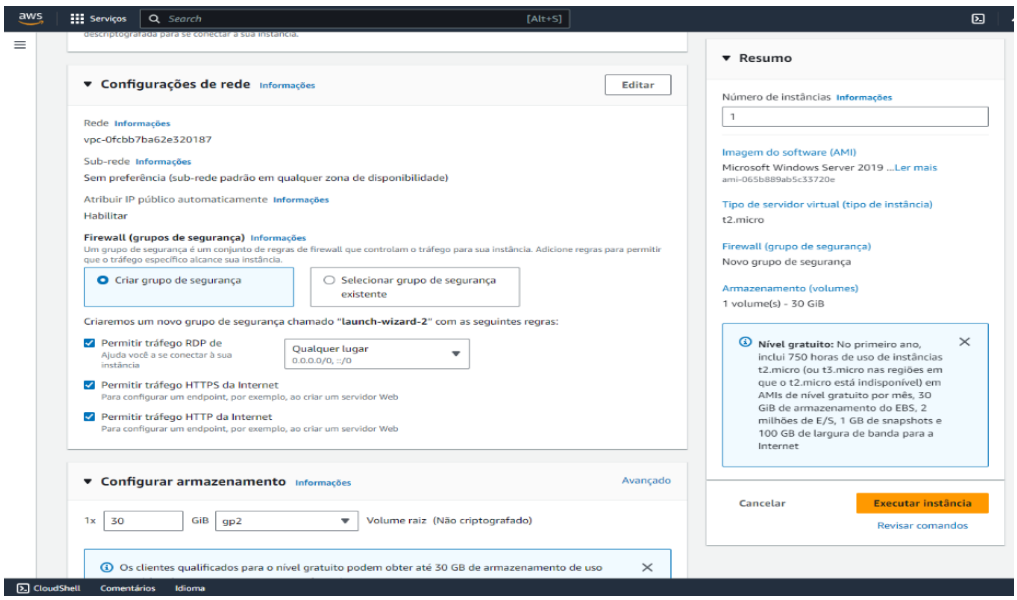
Figura 14 - Criação do *Windows Server* 2019 na AWS



Fonte: De autoria própria

A Figura 15 mostra a interface da AWS na qual é possível configurar as "configurações de rede" da EC2 que está sendo criada. Para este ambiente de teste, escolheu-se a opção de criar um grupo de segurança que permite o tráfego SSH de qualquer origem, além de possibilitar o tráfego HTTPS e HTTP da internet.

Figura 15 - Criação do *Windows Server* 2019 na AWS



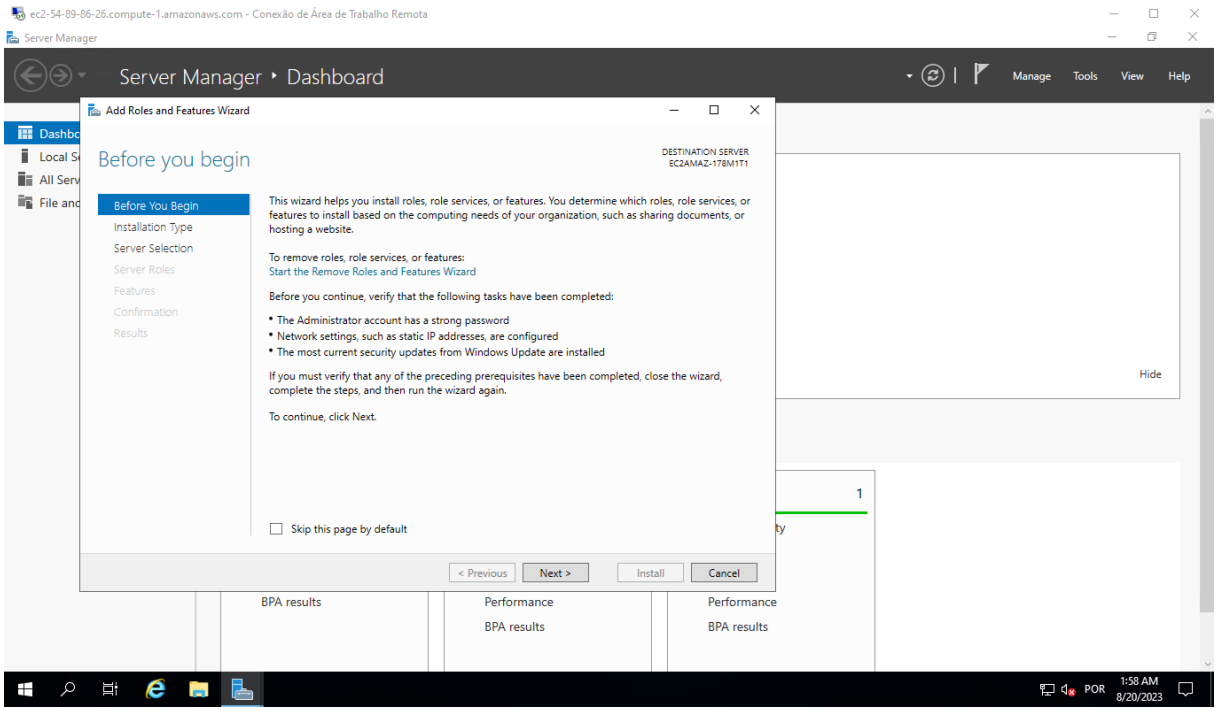
Fonte: De autoria própria

Após a realização das configurações mencionadas acima, procedeu-se ao clique em "Executar instância" para que a instância fosse efetivamente criada.

10.1.3 Adicionando funções e recursos ao *Windows Server*

A Figura 16 apresenta a interface do *Windows Server*, a qual possibilita ao utilizador adicionar funções e recursos ao sistema operacional. Essa interface pode ser acessada por meio do botão "Iniciar", seguindo a rota: Gerenciador de Servidores > Gerenciar > Adicionar Funções e Recursos. Procedeu-se a instalação clicando no botão "Avançar".

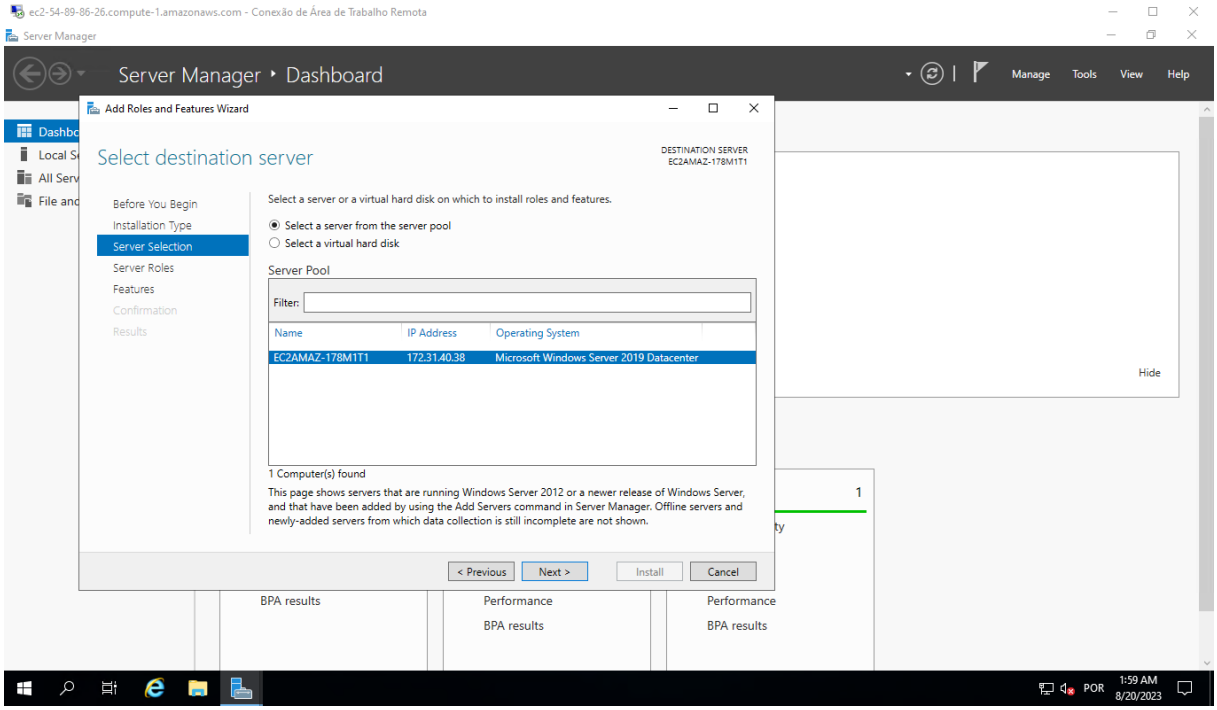
Figura 16 - Adicionando funções e recursos ao *Windows Server*



Fonte: De autoria própria

A Figura 17 exibe a tela subsequente na adição de funções e recursos, oferecendo ao utilizador duas opções: "Instalação baseada em função ou recurso" ou "Instalação de Serviços de Área de Trabalho Remota". Procedeu-se com a instalação selecionando a primeira opção e, em seguida, clicando em "Avançar".

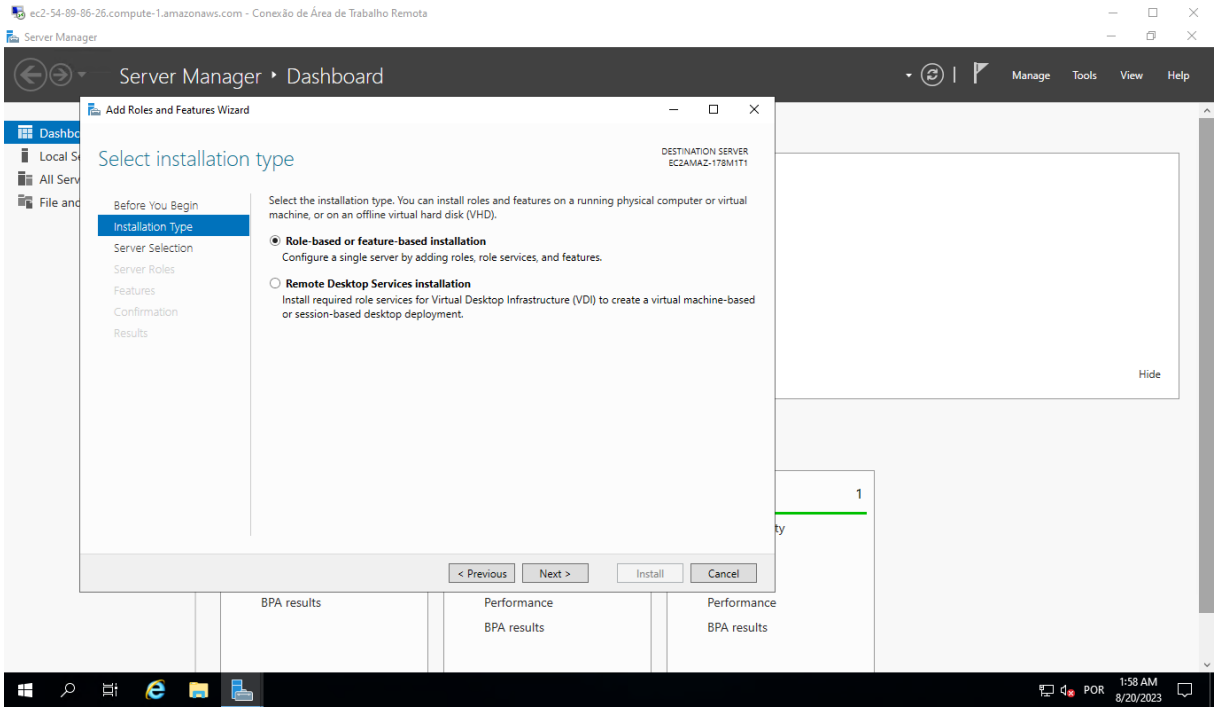
Figura 17 - Adicionando funções e recursos ao *Windows Server*



Fonte: De autoria própria

A Figura 18 apresenta a interface onde é possível selecionar um servidor ou disco virtual rígido no qual as funções e recursos serão instalados. Procedeu-se com a instalação selecionando a opção "Selecionar um servidor no pool de servidor" e clicando no botão "Avançar".

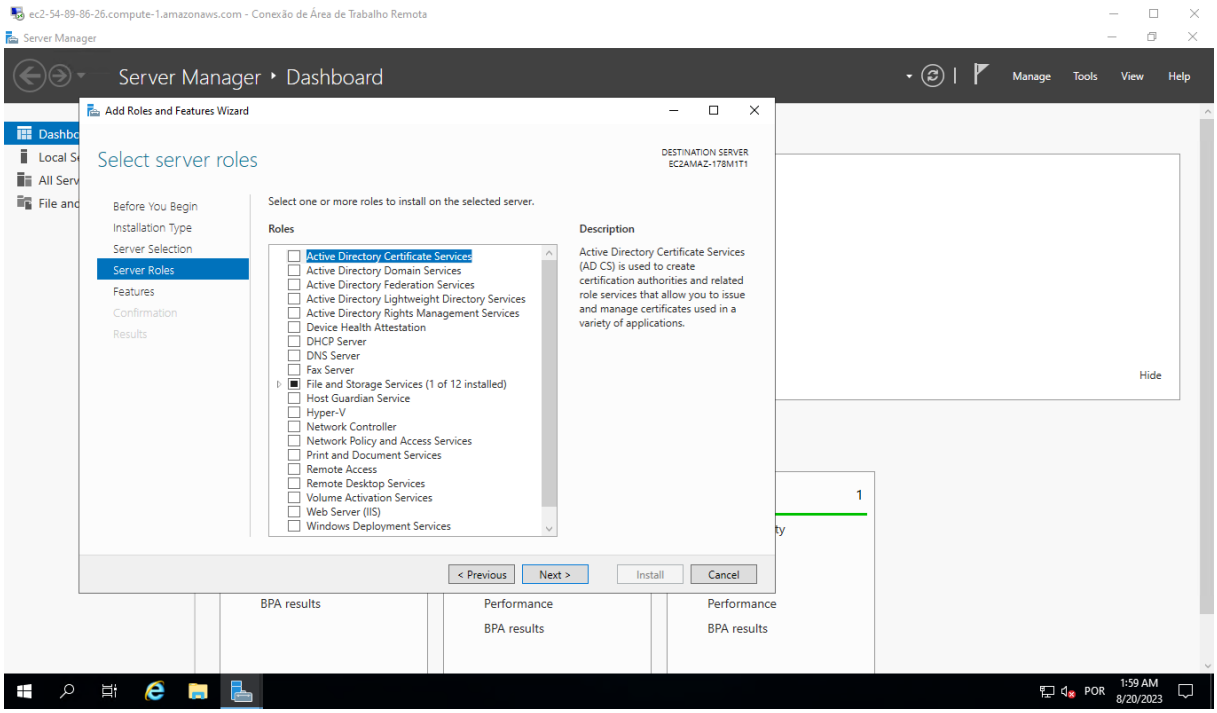
Figura 18 - Adicionando funções e recursos ao *Windows Server*



Fonte: De autoria própria

A Figura 19 exibe a interface onde é possível selecionar funções para o servidor. Neste ambiente de teste, não selecionou-se nenhuma função e procedeu-se com a instalação por meio do botão "Avançar".

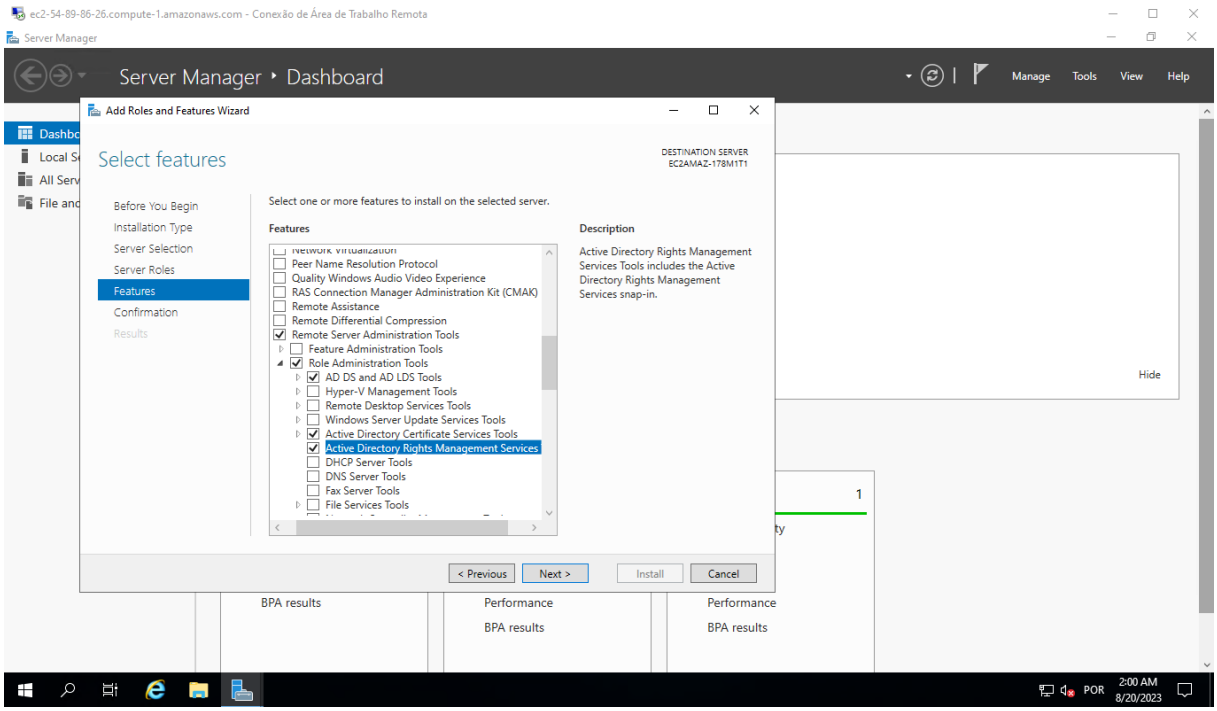
Figura 19 - Adicionando funções e recursos ao *Windows Server*



Fonte: De autoria própria

A Figura 20 apresenta a interface na qual é possível escolher os recursos a serem instalados. Neste ambiente de teste, selecionou-se os seguintes pacotes de recursos: "*Active Directory Rights Management Services Tools*", "*Active Directory Certificate Services Tools*" e "AD DS and AD LDS tools". Procedeu-se a instalação clicando em "Avançar".

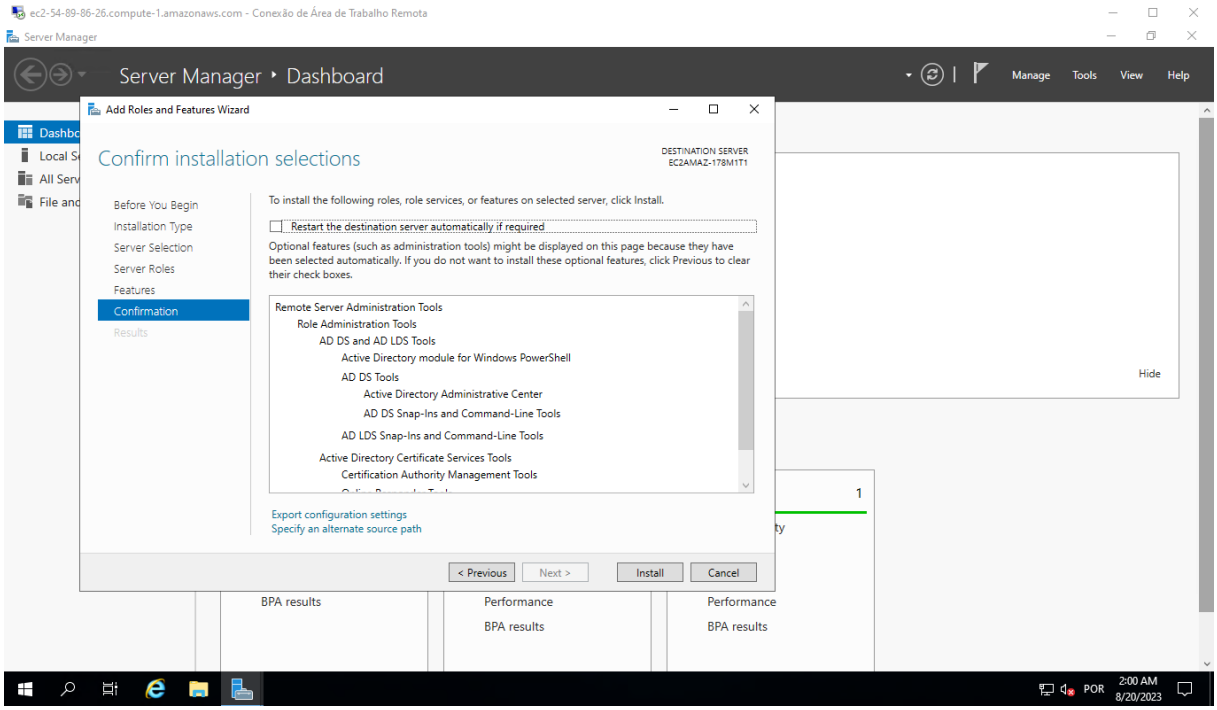
Figura 20 - Adicionando funções e recursos ao *Windows Server*



Fonte: De autoria própria

A Figura 21 exibe a interface que mostra as funções e recursos que serão instalados. Verificamos que os pacotes previamente selecionados estavam de acordo com o planejado, portanto, procedeu-se com a instalação por meio do botão "Instalar".

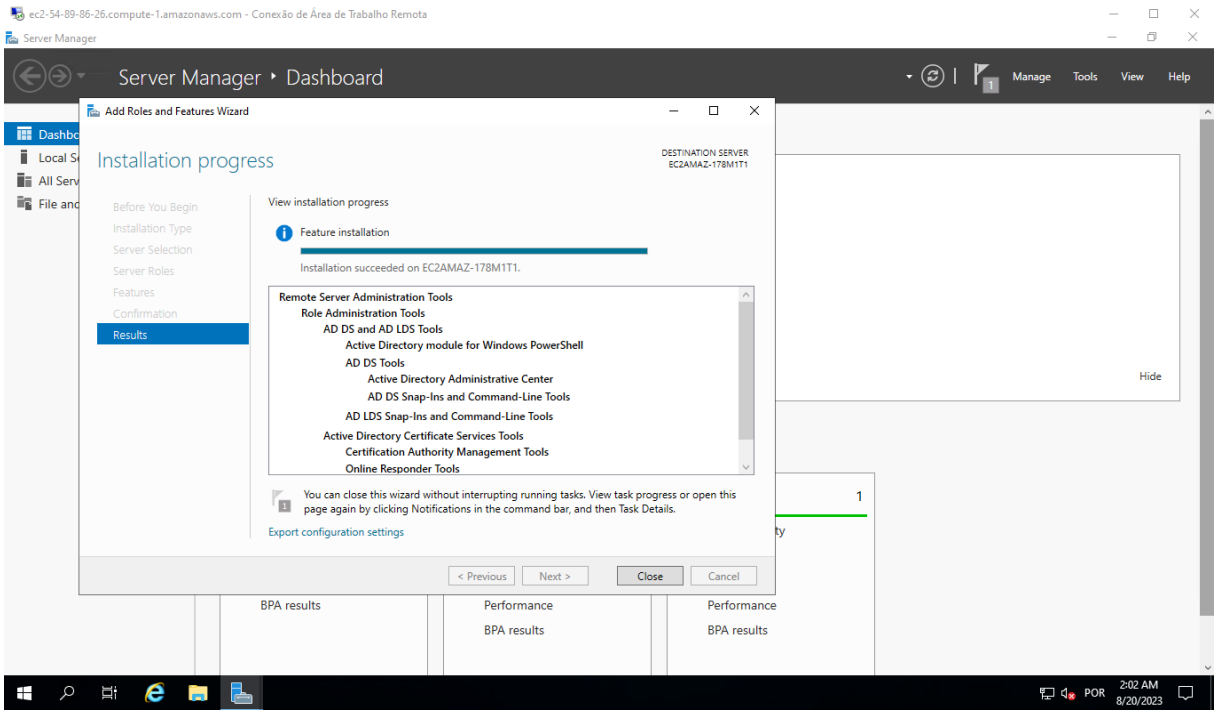
Figura 21 - Adicionando funções e recursos ao *Windows Server*



Fonte: De autoria própria

A Figura 22 apresenta a interface onde é possível verificar que a instalação dos recursos foi bem-sucedida.

Figura 22 - Adicionando funções e recursos ao *Windows Server*

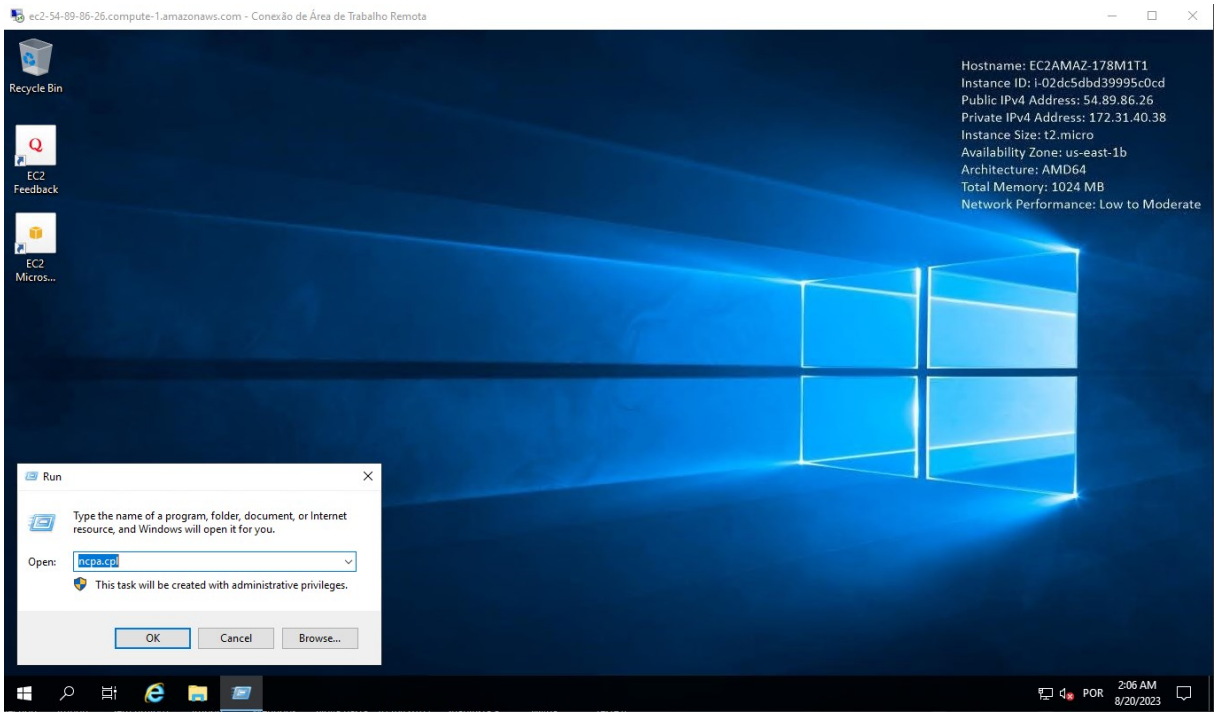


Fonte: De autoria própria

10.1.4 Join entre o Serviço de Diretório e o *Windows Server*

A Figura 23 ilustra a tela inicial do *Windows Server*, onde, por meio da barra de pesquisa, acessou-se a caixa de diálogo "Executar". Utilizou-se essa ferramenta para executar o comando "ncpa.cpl" com o objetivo de acessar as configurações de rede e adaptadores.

Figura 23 - Join entre o Serviço de Diretório e o *Windows Server*

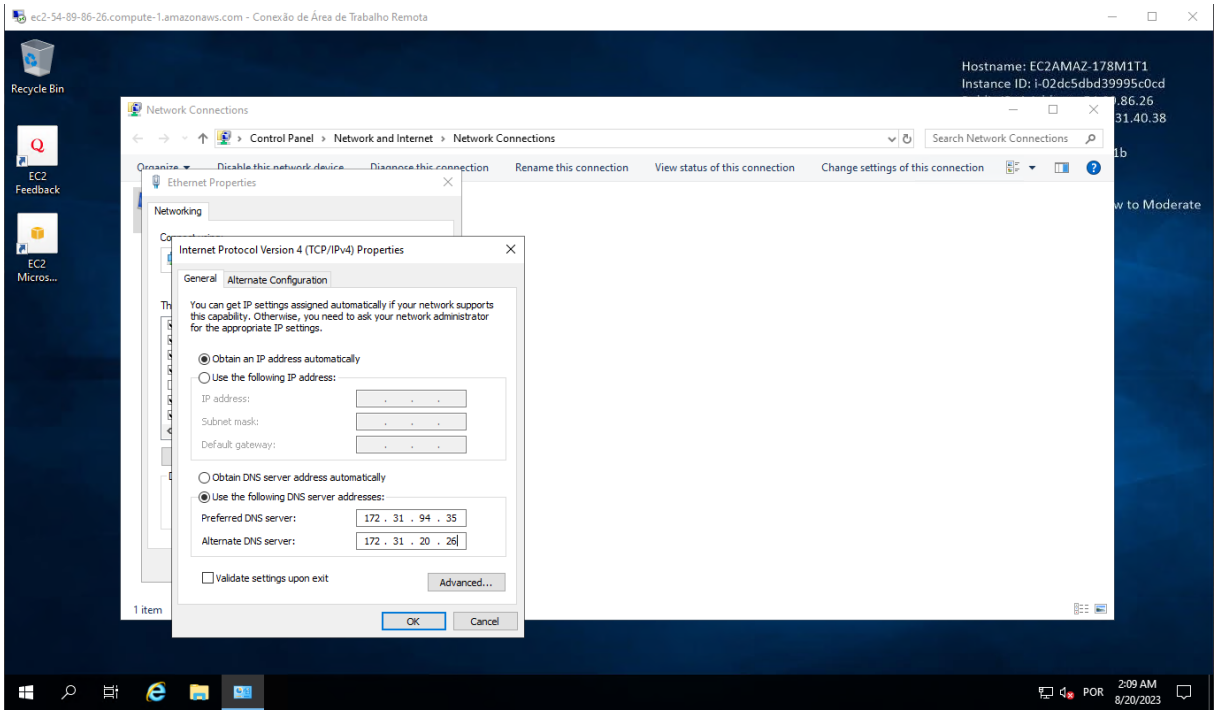


Fonte: De autoria própria

Na Figura 24, podemos observar a interface "Conexões de Rede". Através dela, selecionou-se o adaptador de rede "*Ethernet*". Com um clique do botão direito sobre esse adaptador, escolhemos a opção "Propriedades". Em seguida, selecionou-se o item "Protocolo IP Versão 4 (TCP/IPv4)" e clicou-se na opção "Propriedades".

Nesta última interface exibida, optamos por "Usar os seguintes endereços de servidor DNS" e preenchemos os campos com os respectivos endereços de DNS do serviço de AD. Após o preenchimento correto, clicou-se no botão "OK" para salvar as alterações realizadas.

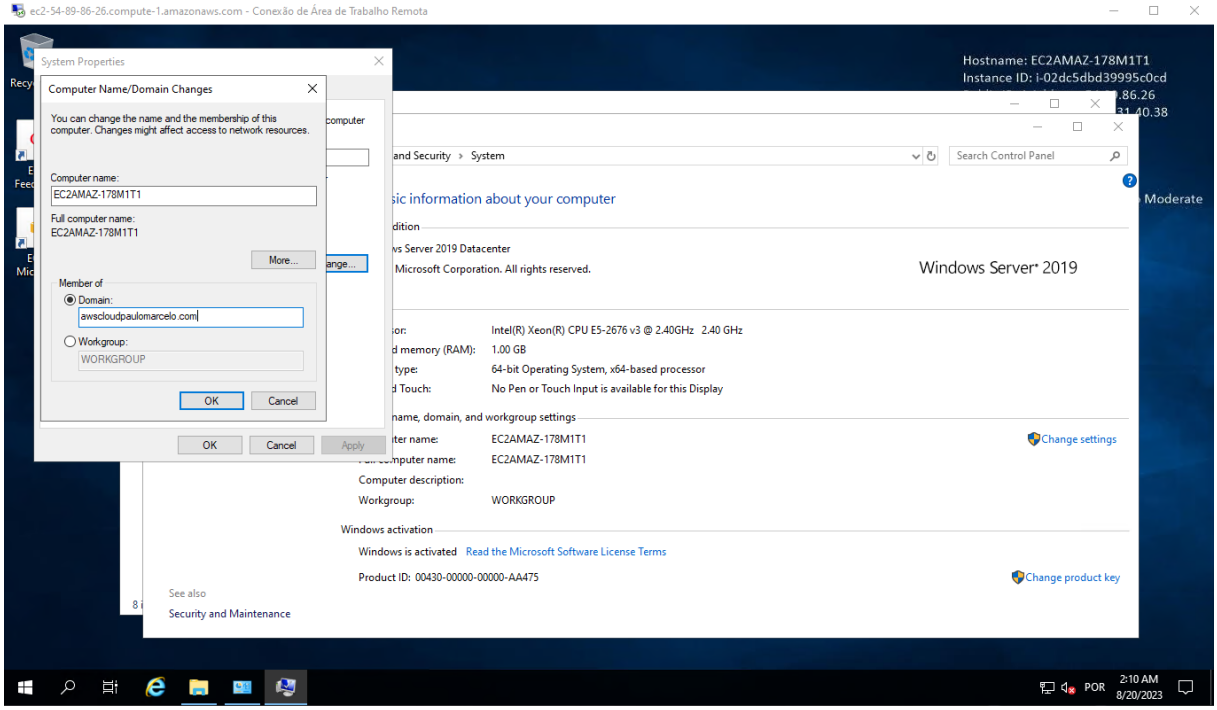
Figura 24 - Join entre o Serviço de Diretório e o *Windows Server*



Fonte: De autoria própria

A Figura 25 exibe a tela inicial do *Windows Server*. Por meio da barra de pesquisa, acessou-se a caixa de diálogo "Executar" e, utilizando o comando "*control.exe /name Microsoft.System*", clicou-se em "Configurações avançadas do sistema". Posteriormente, selecionamos "Nome do computador" e clicou-se em "Alterar". Preenchemos o campo "Domínio" com o domínio escolhido no momento da criação do serviço de diretório na AWS e, em seguida, clicou-se em "OK".

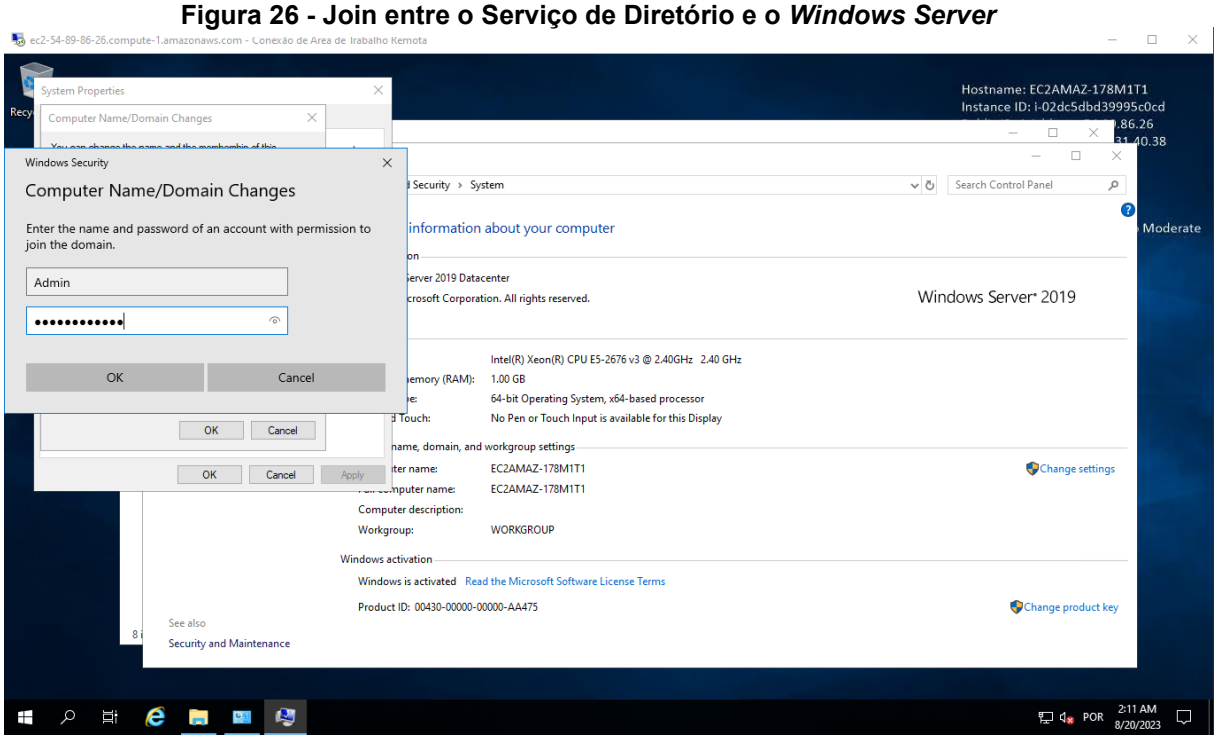
Figura 25 - Join entre o Serviço de Diretório e o *Windows Server*



Fonte: De autoria própria

A Figura 26 apresenta uma caixa de diálogo que permite o *login* utilizando as credenciais de usuário e senha escolhidas no momento da criação do serviço de diretório na AWS. Neste caso, utilizou-se o usuário "Admin" e a senha "i4@0rOjUQA8#", em seguida, clicou-se em "OK".

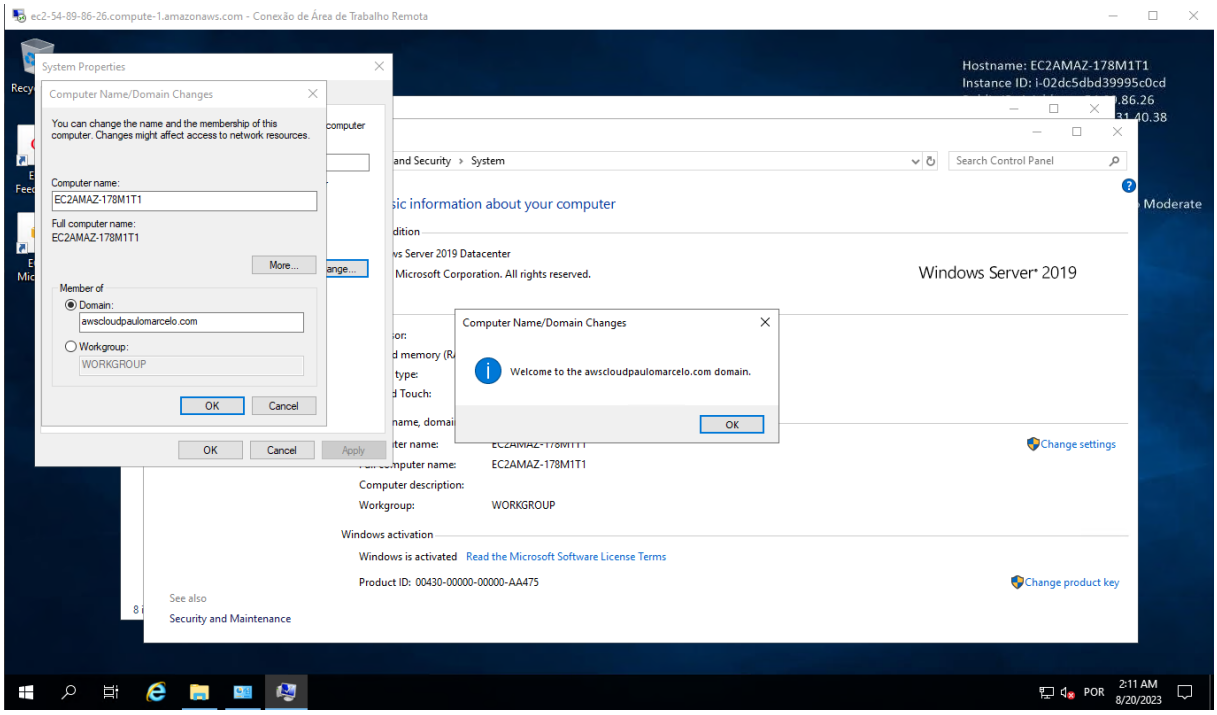
Figura 26 - Join entre o Serviço de Diretório e o *Windows Server*



Fonte: De autoria própria

Por fim, a Figura 27 exibe uma caixa de alerta informando que a alteração de domínio foi realizada com sucesso.

Figura 27 - Join entre o Serviço de Diretório e o *Windows Server*

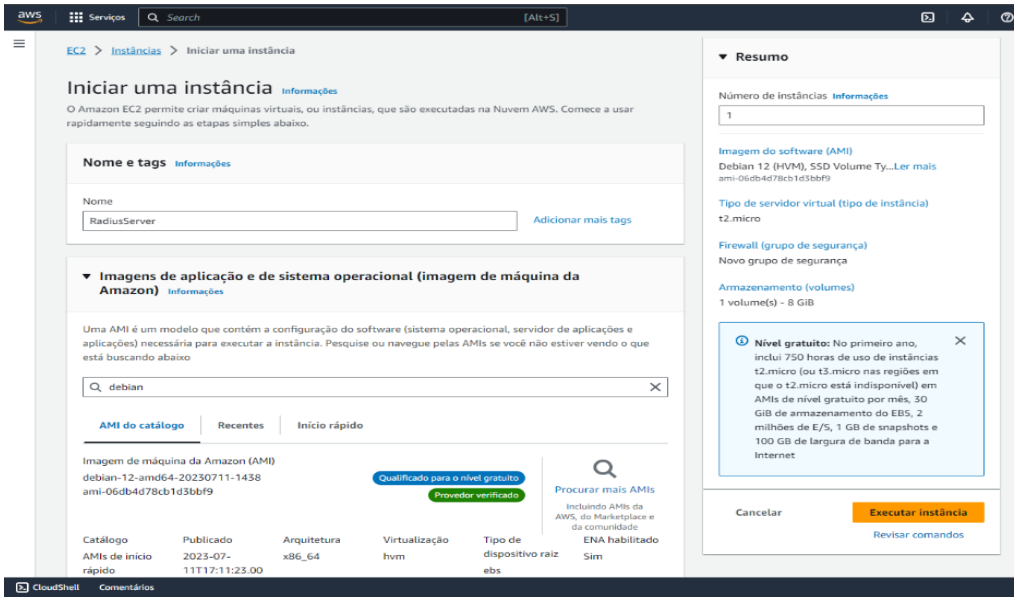


Fonte: De autoria própria

10.1.5 Criação do Servidor Radius na AWS

A Figura 28 apresenta a interface da plataforma AWS, na qual é possível criar uma instância. Essa interface pode ser acessada seguindo o caminho: EC2 > Instâncias > Iniciar uma instância. Além disso, na mesma imagem, é evidente o campo "Nome e tags" que foi devidamente preenchido com o rótulo "*RadiusServer*".

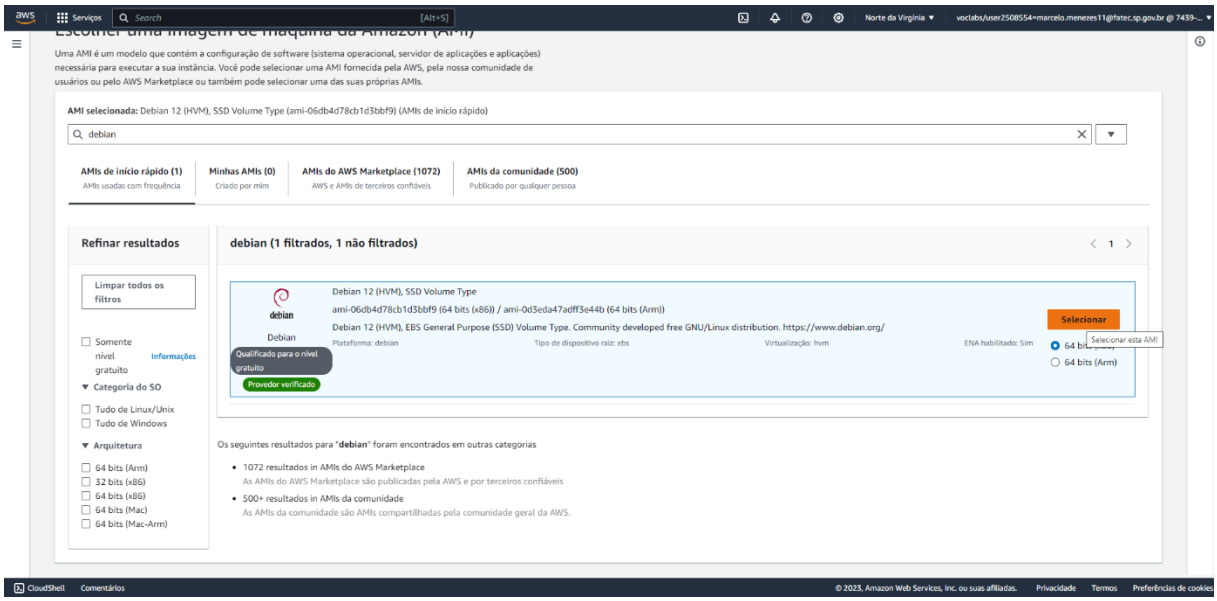
Figura 28 - Criação do Servidor Radius na AWS



Fonte: De autoria própria

Por sua vez, a Figura 29 exibe a interface da AWS na qual é possível selecionar o sistema operacional a ser instalado na instância EC2. Para este ambiente de teste, optou-se pelo sistema operacional "Debian 12", com o propósito de configurá-lo para fornecer as funcionalidades de um servidor RADIUS.

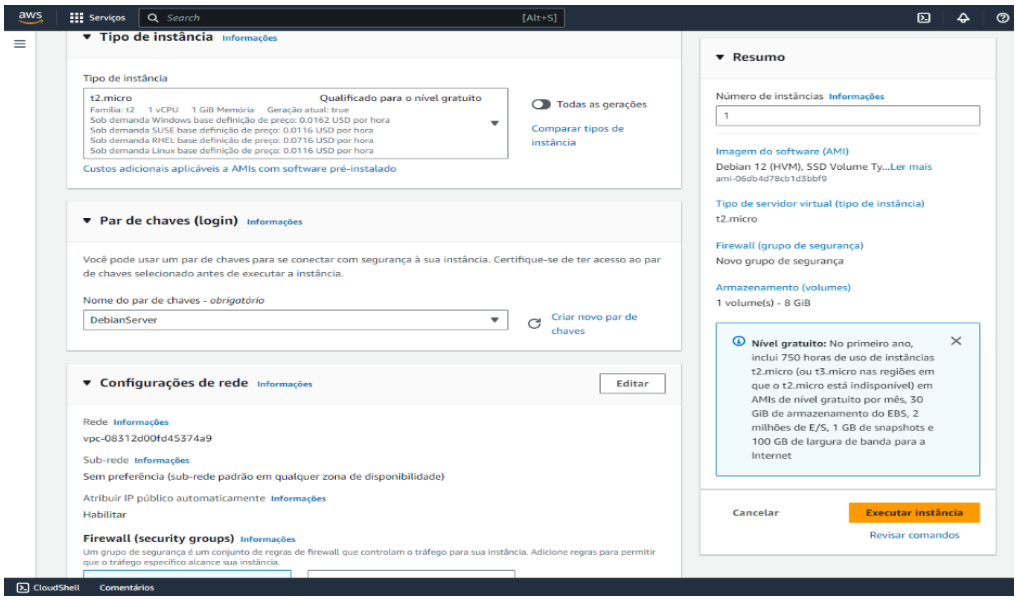
Figura 29 - Criação do Servidor Radius na AWS



Fonte: De autoria própria

Na Figura 30, é possível visualizar a interface da AWS que oferece a opção de selecionar um "Par de chaves (*login*)" já existente ou criar. Neste contexto de teste, optou-se por utilizar um "Par de chaves" previamente existente.

Figura 30 - Criação do Servidor Radius na AWS

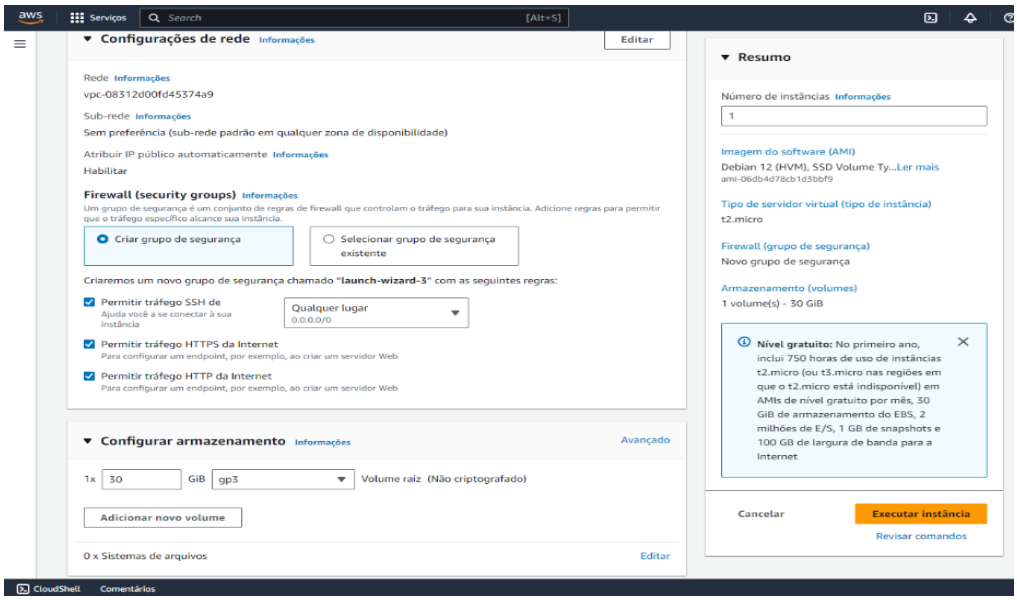


Fonte: De autoria própria

A Figura 31 apresenta a interface da AWS na qual é possível configurar as "configurações de rede" da EC2 que está sendo criada. Para este ambiente de teste,

escolheu-se a opção de criar um grupo de segurança que permite o tráfego SSH de qualquer origem, além de possibilitar o tráfego HTTPS e HTTP da internet.

Figura 31 - Criação do Servidor Radius na AWS



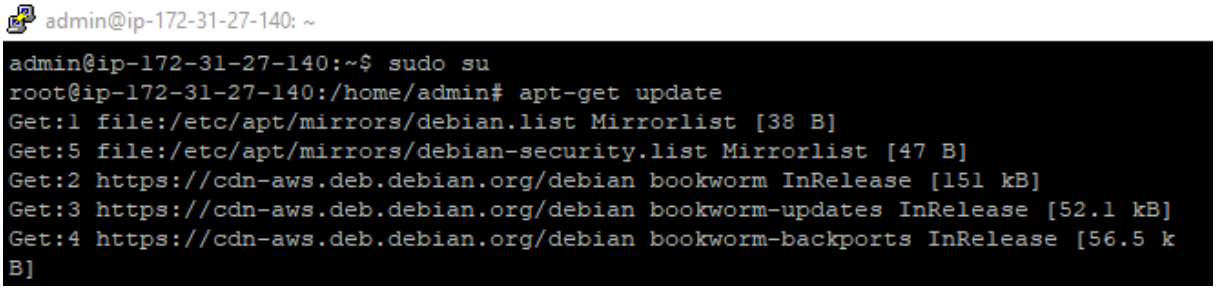
Fonte: De autoria própria

Após a realização das configurações mencionadas acima, procedeu-se ao clique em "Executar instância" para que a instância fosse efetivamente criada.

10.1.6 Configuração do Servidor Radius

A Figura 32 apresenta os passos iniciais da configuração do Servidor RADIUS no sistema Debian, iniciamos o processo de preparação do ambiente para a instalação e configuração do servidor RADIUS. Para isso, adotamos alguns passos essenciais.

Figura 32 - Configuração do Servidor Radius



Fonte: De autoria própria

Primeiramente, executou-se o comando sudo su para obter acesso privilegiado de superusuário, também conhecido como *root*. O uso de "sudo" (Superuser Do) permite que se execute comandos com privilégios de administrador, o que é necessário para a instalação de pacotes e configurações críticas do sistema. O comando "sudo su" permite ao utilizador entrar na sessão de superusuário, facilitando a execução de múltiplos comandos com privilégios elevados sem a necessidade de usar "sudo" repetidamente.

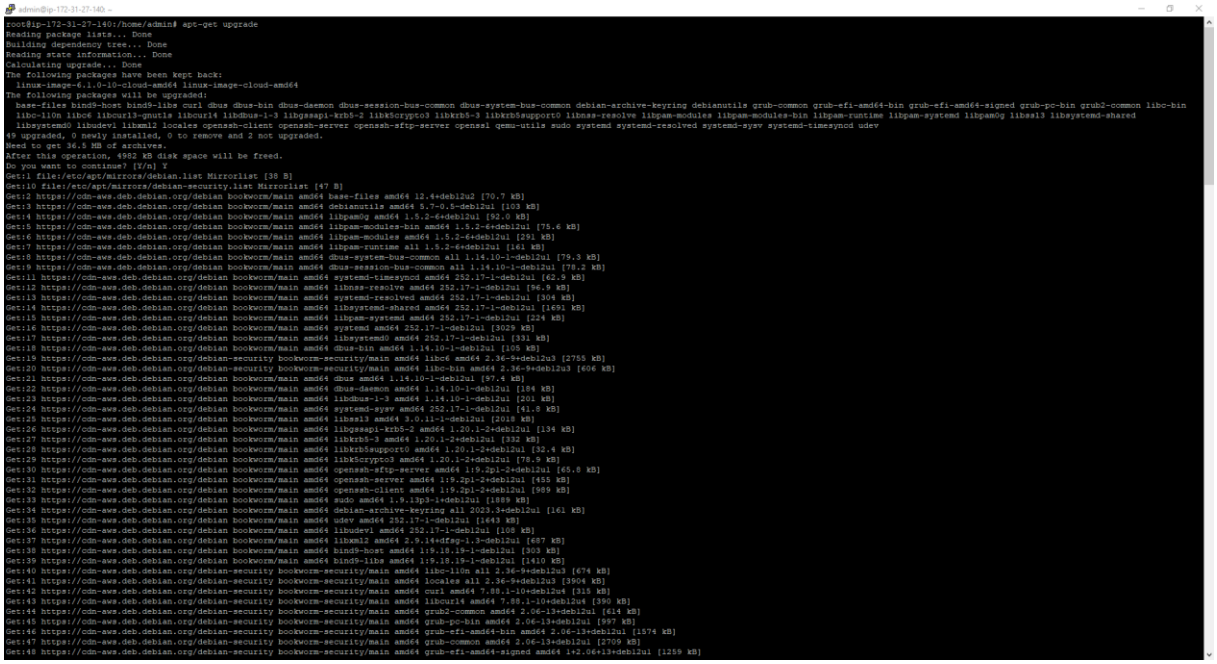
Em seguida, executou-se o comando *apt-get update*. Esse comando é utilizado para atualizar a lista de pacotes disponíveis no sistema. Quando o servidor RADIUS está sendo configurado, é fundamental garantir que o sistema tenha as informações de pacotes mais recentes para instalar as dependências necessárias e os componentes do servidor RADIUS.

O comando "*apt-get update*" verifica os repositórios de pacotes configurados no sistema e atualiza as informações sobre as versões disponíveis, as dependências e outras informações importantes que são necessárias para o gerenciamento e instalação de pacotes.

Esses passos iniciais são cruciais para garantir que o ambiente de teste esteja atualizado e preparado para receber as próximas etapas da configuração do servidor RADIUS no Debian.

Na Figura 33 da configuração do Servidor RADIUS no Debian, procedeu com a preparação do ambiente, executou-se o comando "*apt-get upgrade*". Esta etapa é crucial para garantir que o sistema esteja atualizado com as versões mais recentes dos pacotes já instalados.

Figura 33 - Configuração do Servidor Radius

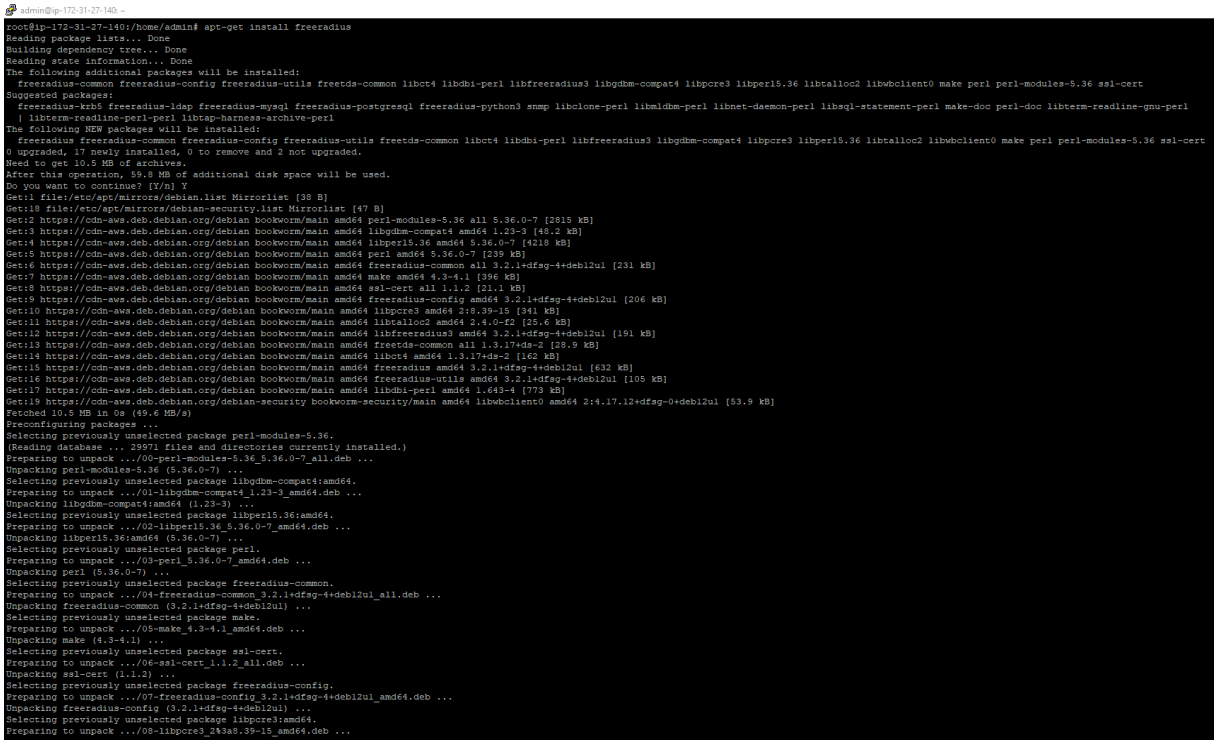


Fonte: De autoria própria

O comando "*apt-get upgrade*" é utilizado para atualizar todos os pacotes já instalados no sistema para suas versões mais recentes disponíveis nos repositórios configurados. A atualização de pacotes é uma prática importante para corrigir possíveis vulnerabilidades de segurança, melhorar o desempenho do sistema e garantir a compatibilidade entre os componentes do servidor RADIUS e outras dependências.

Na Figura 34 da configuração do Servidor RADIUS no Debian, executou-se o comando "*apt-get install FreeRADIUS".* Essa etapa é fundamental para a instalação do *FreeRADIUS*, o *software* que será responsável por gerenciar a autenticação e autorização de usuários na rede.

Figura 34 - Configuração do Servidor Radius



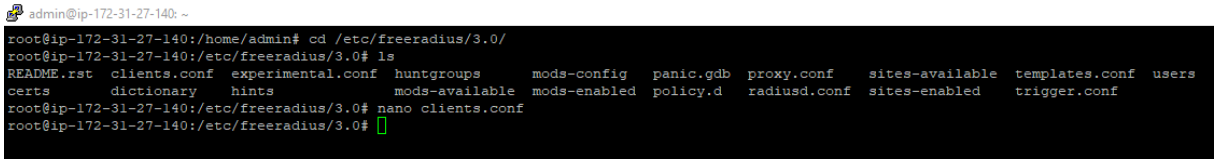
Fonte: De autoria própria

O comando "*apt-get install FreeRADIUS*" utiliza o sistema de gerenciamento de pacotes APT (*Advanced Package Tool*) para instalar o pacote *FreeRADIUS* e suas dependências. O *FreeRADIUS* é uma implementação de código aberto do protocolo RADIUS, amplamente utilizado em sistemas de autenticação e autorização em redes.

A instalação do *FreeRADIUS* é um passo crítico na criação de um servidor RADIUS funcional, pois fornece as ferramentas necessárias para a autenticação de usuários, permitindo-lhes acessar recursos da rede com base em políticas predefinidas.

Na Figura 35 da configuração do Servidor RADIUS no Debian, primeiramente, utilizou-se o comando "cd /etc/*FreeRADIUS*/3.0/", que tem o objetivo de navegar até o diretório onde as configurações do *FreeRADIUS* estão armazenadas. Este é um passo essencial para acessar e editar os arquivos de configuração que determinam o comportamento do servidor.

Figura 35 - Configuração do Servidor Radius

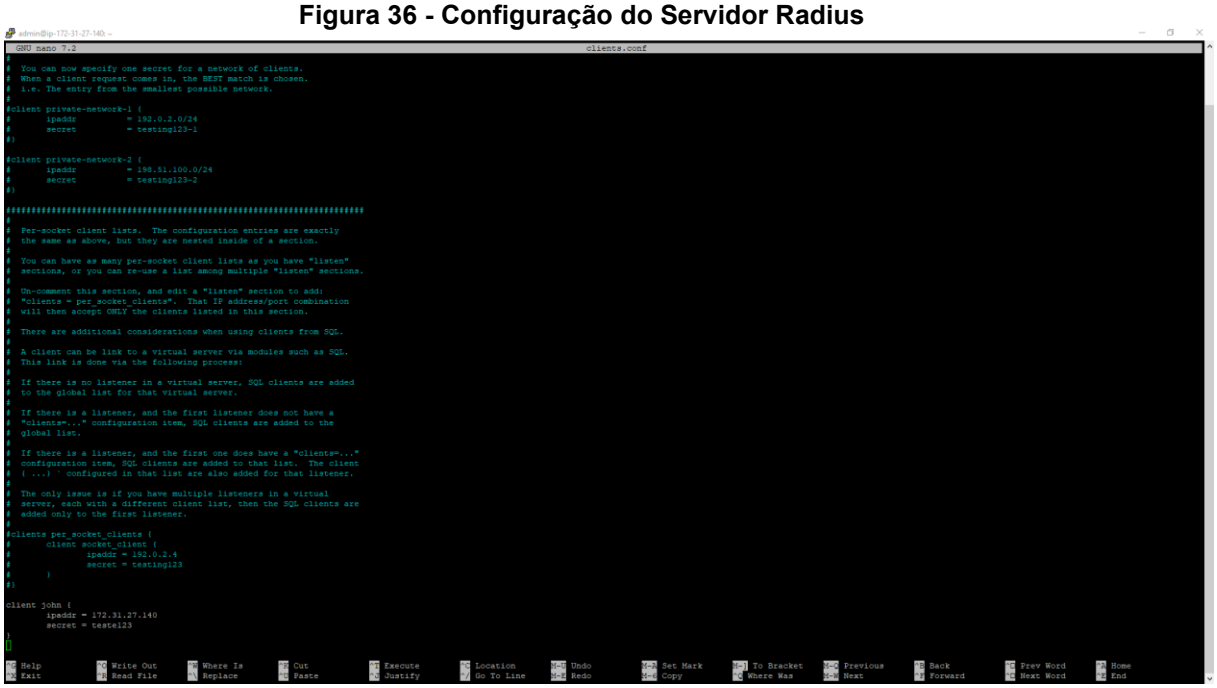


Fonte: De autoria própria

Em seguida, executou-se o comando "*nano clients.conf*". O editor de texto "nano" é uma ferramenta de linha de comando que permite a edição de arquivos de configuração de forma simples e direta. O arquivo "*clients.conf*" é especialmente importante, pois ele contém informações sobre os clientes autorizados a se conectar ao servidor RADIUS. Esses clientes podem incluir dispositivos de rede, pontos de acesso Wi-Fi e outros componentes que precisam da autenticação RADIUS para acessar recursos da rede.

Na Figura 36 da configuração do Servidor RADIUS no Debian, adicionou-se uma configuração de cliente ao arquivo "*clients.conf*". Essa etapa é crucial para definir quais clientes específicos terão acesso autorizado ao servidor RADIUS, bem como as informações de autenticação necessárias para essa autorização.

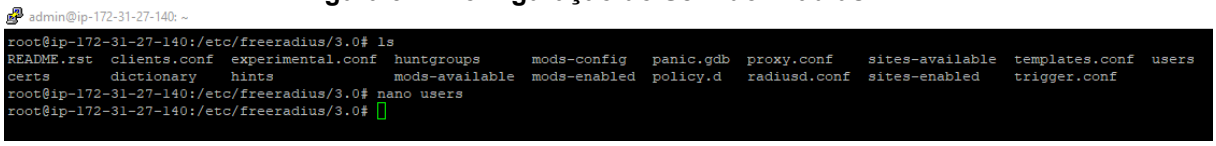
Figura 36 - Configuração do Servidor Radius



Fonte: De autoria própria

Na Figura 37 da configuração do Servidor RADIUS no Debian, executou-se uma série de comandos para listar os arquivos presentes no diretório "/etc/*FreeRADIUS*/3.0" e abrir o arquivo "*users*". Essa etapa é crucial para acessar e personalizar o arquivo "*users*", que contém informações sobre os usuários autorizados a autenticar-se na rede.

Figura 37 - Configuração do Servidor Radius

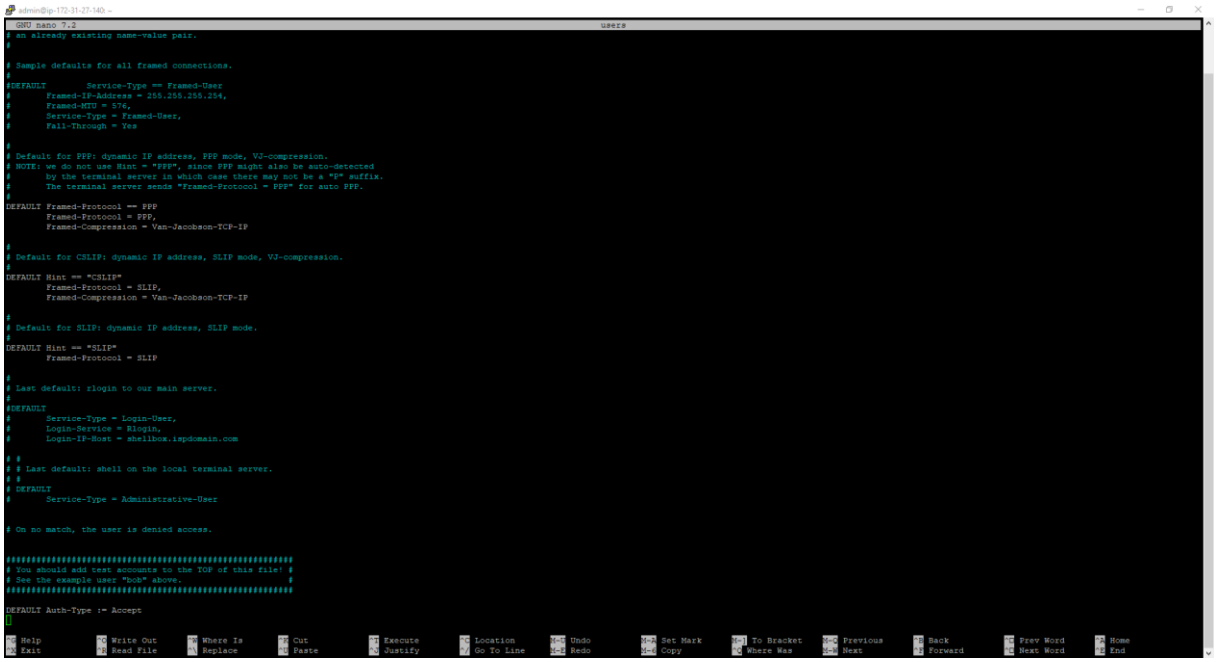


Fonte: De autoria própria

Primeiramente, utilizou-se o comando "ls" para listar os arquivos e diretórios no diretório "/etc/*FreeRADIUS*/3.0", permitindo a visualização dos arquivos de configuração relevantes para o servidor RADIUS. Em seguida, acessou-se o arquivo "*users*" com o editor de texto "nano". Esse arquivo é um componente fundamental da configuração do *FreeRADIUS*, pois contém informações sobre os usuários que têm permissão para autenticar-se no servidor RADIUS, permitindo a definição de credenciais, políticas de acesso e outras informações específicas para cada usuário ou grupo de usuários.

Na Figura 38 da configuração do Servidor RADIUS no Debian, realizou-se uma configuração importante no arquivo "*users*". Executou-se o comando "*DEFAULT Auth-Type := Accept*", que desempenha um papel fundamental na configuração do comportamento padrão do servidor RADIUS em relação à autenticação dos usuários.

Figura 38 - Configuração do Servidor Radius



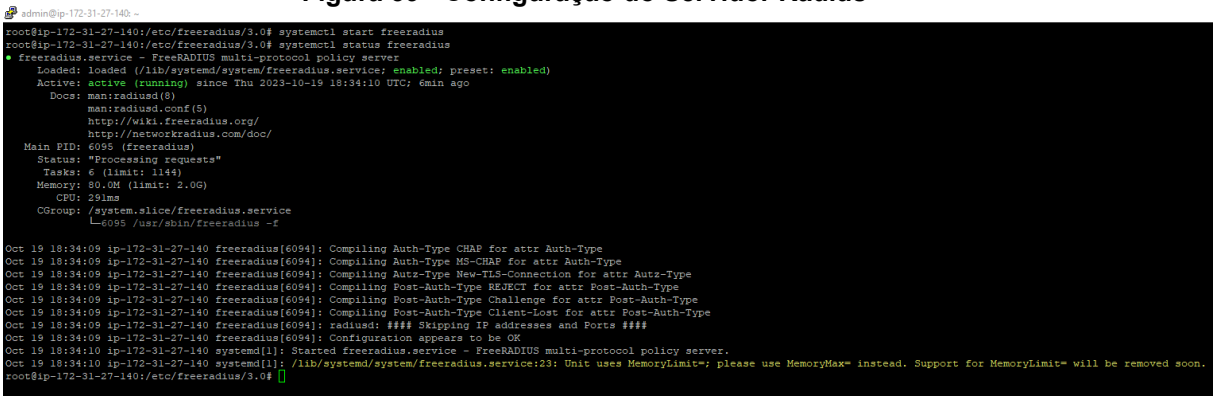
Fonte: De autoria própria

Este comando define a política de autenticação padrão para todos os usuários que não possuem configurações específicas definidas no arquivo "*users*". O

"*DEFAULT*" indica que essa configuração se aplica a todos os usuários que não tenham uma configuração de autenticação personalizada.

Na Figura 39 da configuração do Servidor RADIUS no sistema Debian, executou-se os comandos "*systemctl start FreeRADIUS"* e *"systemctl status FreeRADIUS*". A resposta desses comandos confirma que o serviço *FreeRADIUS* está ativo, em execução e configurado para ser iniciado automaticamente durante o processo de inicialização do sistema.

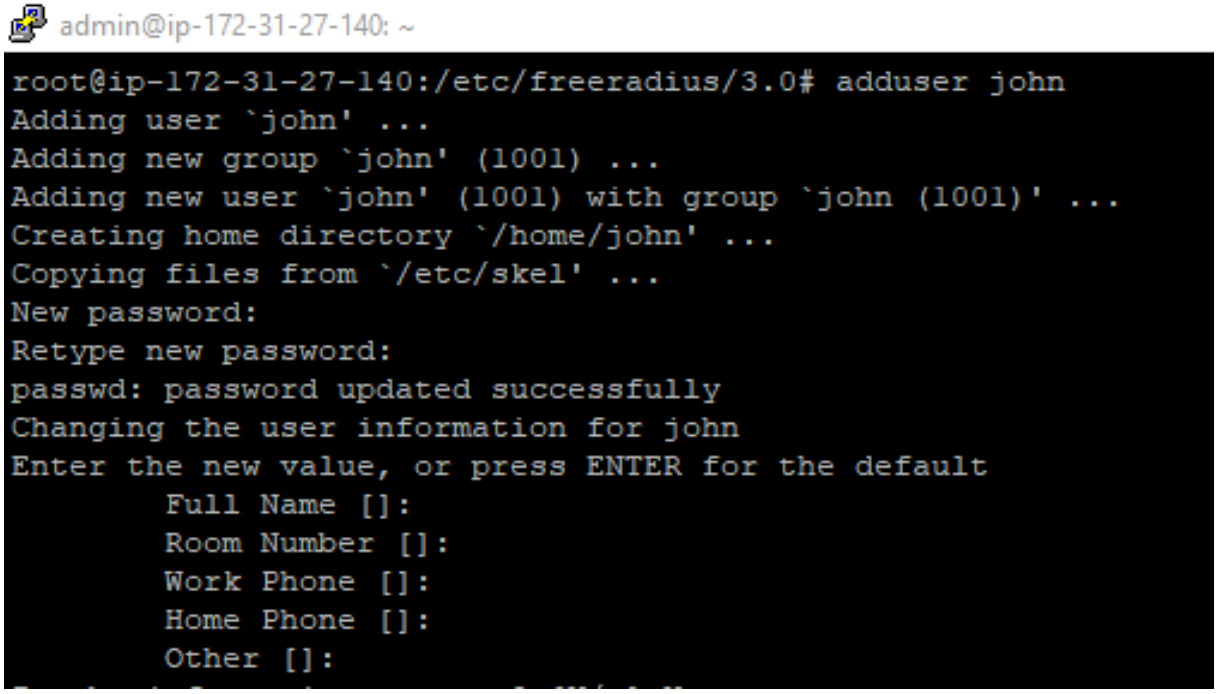
Figura 39 - Configuração do Servidor Radius



Fonte: De autoria própria

Na Figura 40 da configuração do Servidor RADIUS no Debian, executou-se o comando "adduser john" com o propósito de criar um usuário chamado "*john*" no sistema. Essa ação é realizada em preparação para futuros testes de autenticação no servidor RADIUS.

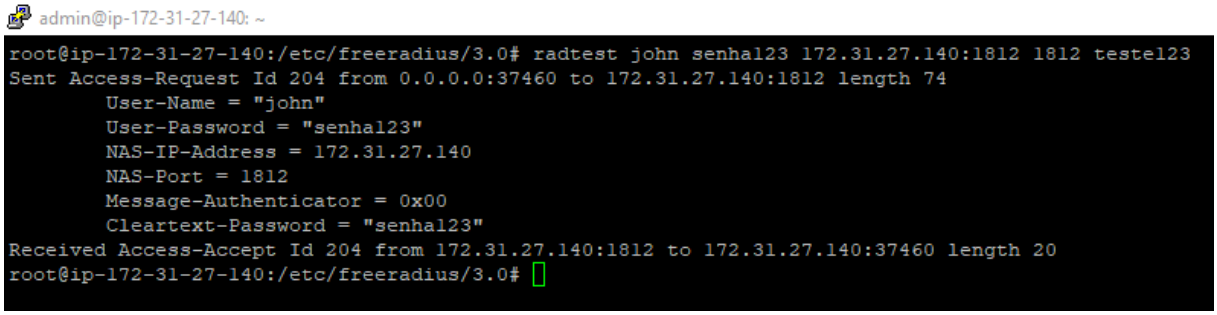
Figura 40 - Configuração do Servidor Radius



Fonte: De autoria própria

Na Figura 41 da configuração do Servidor RADIUS no Debian, executou-se o comando "radtest john senha123 172.31.27.140:1812 1812 teste123" com o objetivo de testar o processo de autenticação no servidor RADIUS.

Figura 41 - Configuração do Servidor Radius

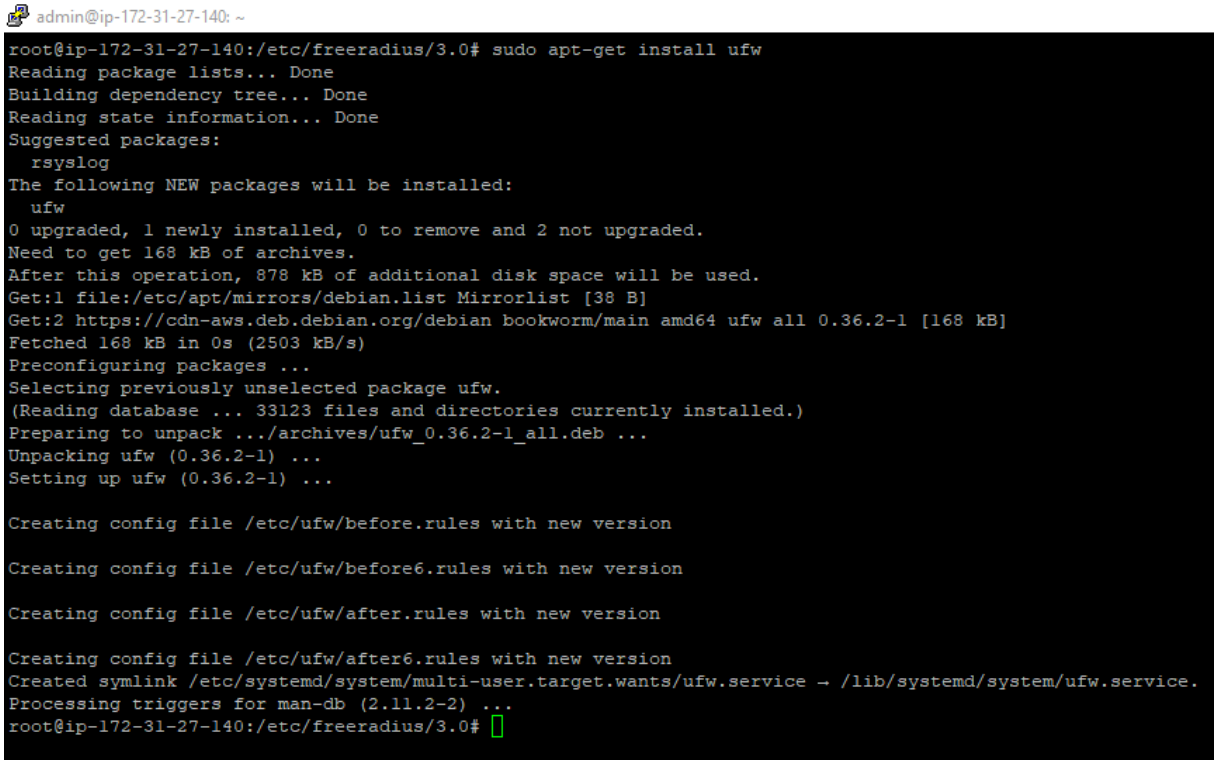


Fonte: De autoria própria

A resposta "*Received Access-Accept Id* 204 from 172.31.27.140:1812 *to* 172.31.27.140:37460 *length* 20" indica que o teste foi bem-sucedido.

Na Figura 42 da configuração do Servidor RADIUS no Debian, executou-se o comando "apt-get install ufw" com o objetivo de instalar o *Uncomplicated Firewall* (UFW) no sistema. O UFW é uma ferramenta que simplifica a configuração e a gestão de regras de *firewall* em sistemas Linux.

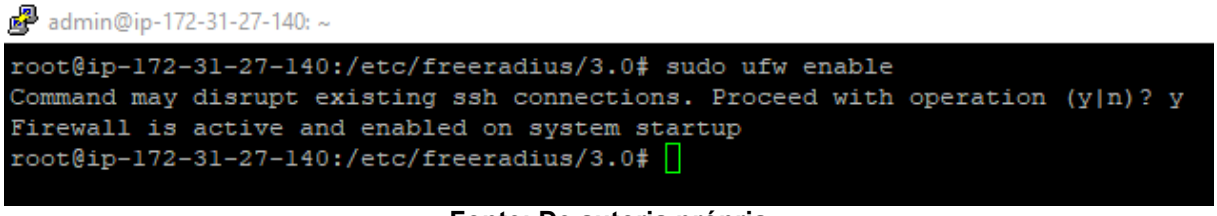
Figura 42 - Configuração do Servidor Radius



Fonte: De autoria própria

Na Figura 43 da configuração do Servidor RADIUS no Debian, executou-se o comando "*sudo ufw enable*" com o objetivo de ativar o *Uncomplicated Firewall* (UFW) no sistema. A ativação do UFW é um passo fundamental para tornar as regras de *firewall* efetivas e aplicá-las às configurações de segurança da rede.

Figura 43 - Configuração do Servidor Radius



Fonte: De autoria própria

Na Figura 44 da configuração do Servidor RADIUS no Debian, executou-se uma série de comandos relacionados ao *Uncomplicated Firewall* (UFW) para fortalecer a segurança do servidor e controlar o tráfego de rede de acordo com as políticas de segurança.

Figura 44 - Configuração do Servidor Radius

Fonte: De autoria própria

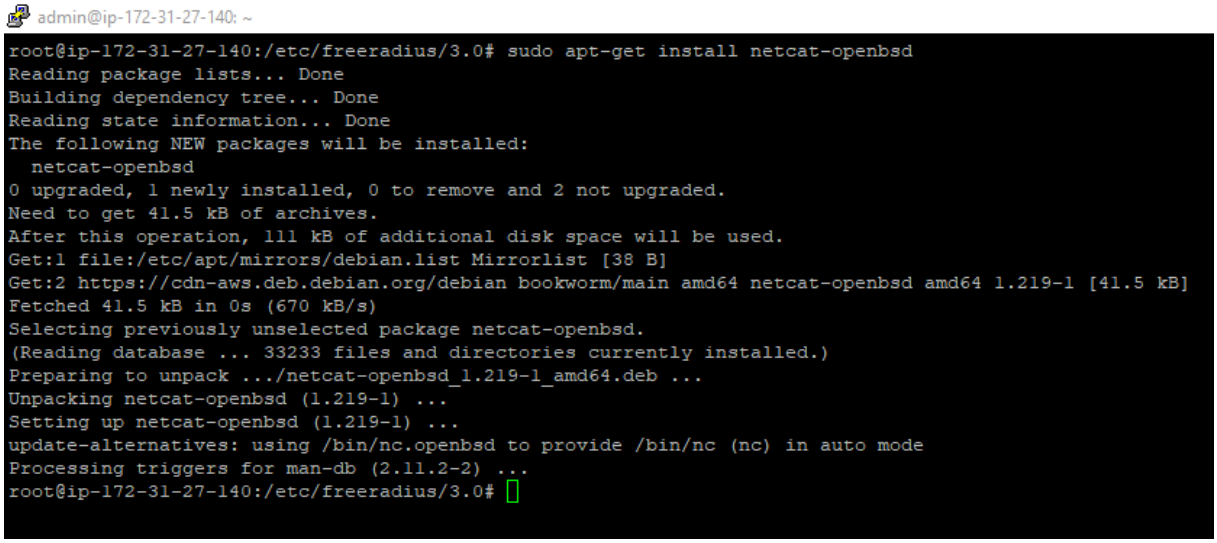
Os comandos realizados foram:

1. "*sudo ufw allow* 1812/*udp*": Este comando permite o tráfego UDP na porta 1812, que é a porta padrão para o protocolo RADIUS. Isso é essencial para permitir que as solicitações de autenticação RADIUS sejam recebidas pelo servidor.
2. "*sudo ufw allow 22/tcp*": Esse comando permite o tráfego TCP na porta 22, que é a porta padrão para o serviço SSH. Permitir o SSH é importante para que você possa administrar o servidor de forma segura e remota.
3. "*sudo ufw reload*": Este comando recarrega as regras do *firewall* após as alterações feitas com os comandos anteriores. Isso garante que as novas regras de *firewall* sejam aplicadas imediatamente.
4. "*sudo ufw status*": O comando "*sudo ufw status*" é usado para verificar o status atual do *Uncomplicated Firewall*. A mensagem de resposta indica que o UFW está ativo, e ele também lista as portas que estão liberadas, que neste caso são a porta 1812 (para o RADIUS) e a porta 22 (para o SSH).

Na figura 45 da configuração do Servidor RADIUS no Debian, executou-se o comando "*apt-get install netcat-openbsd*" para instalar o pacote *"netcat-openbsd*" no

sistema. O Netcat é uma ferramenta versátil que fornece funcionalidades relacionadas à rede, permitindo a criação de conexões de rede, transferência de dados e outras tarefas de rede.

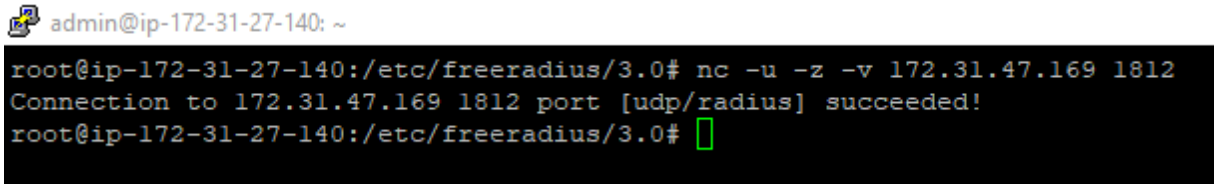
Figura 45 - Configuração do Servidor Radius



Fonte: De autoria própria

Na figura 46 da configuração do Servidor RADIUS no Debian, executou-se o comando "nc -u -z -v 172.31.47.169 1812" com o objetivo de verificar a conectividade com o servidor RADIUS em 172.31.47.169 na porta 1812, utilizando o protocolo UDP.

Figura 46 - Configuração do Servidor Radius



Fonte: De autoria própria

A mensagem de resposta "*Connection to 172.31.47.169 1812 port [udp/radius] succeeded*!" indica que a conexão foi bem-sucedida. Isso confirma que o servidor RADIUS em 172.31.47.169 está acessível e responde às solicitações na porta 1812, que é a porta padrão para o protocolo RADIUS.

11. CONSIDERAÇÕES FINAIS

Ao recapitular de maneira concisa os pontos essenciais abordados neste Trabalho de Conclusão de Curso (TCC) sobre a implementação de Autenticação Multifator (MFA) para o *Active Directory* (AD), é possível observar uma abordagem integral desde a introdução até a aplicação prática.

A estruturação cuidadosa do trabalho em onze capítulos proporcionou uma análise aprofundada do contexto, destacando aspectos fundamentais do *Windows Server 2019*, do *Active Directory*, do protocolo LDAP e das políticas de segurança por meio das *Group Policy Objects* (GPOs).

O oitavo capítulo, central na discussão, enfoca o desenvolvimento da autenticação multifator para o *Active Directory*, ressaltando a pertinência e atualidade do tema. A explanação das vantagens dessa abordagem sublinha a importância crucial da segurança na autenticação de usuários, apresentando soluções concretas para mitigar riscos.

A descrição detalhada do ambiente de teste no capítulo 10, oferece uma aplicação prática do conhecimento adquirido. A criação do serviço de diretório na AWS, do *Windows Server 2019*, do servidor Radius, e a configuração desses elementos evidenciam a viabilidade da implementação bem-sucedida da autenticação multifator em um ambiente real.

Ao enfatizar os resultados alcançados com as ferramentas utilizadas, destaca-se a eficácia da aplicação prática, evidenciando a integração bem-sucedida do MFA com o AD.

Diante do exposto, concluímos que os objetivos delineados no início foram alcançados de maneira satisfatória. A pesquisa não apenas abrangeu aspectos teóricos pertinentes, mas também ofereceu uma visão prática por meio do ambiente de teste na AWS.

Este estudo representa uma contribuição valiosa para a compreensão e aplicação eficaz da autenticação multifatorial no contexto do Active Directory. Ele consolida os conhecimentos teóricos e práticos adquiridos ao longo da pesquisa, fornecendo uma abordagem teórica e prática inédita em língua portuguesa até os dados de elaboração deste documento.

REFERÊNCIAS

ALLEN, Robbie; PUCKETT, Richard. **Managing Enterprise Active Directory Services.** 1. ed. New York: Pearson Education, 2002.

AMAZON WEB SERVICES. **Uso de autenticação multifator (MFA) na AWS.** Disponível em: https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/id_credentials_mfa.html#id_credentials_mfa-what-is-mfa. Acesso em: 10 nov. 2023

ANDERSON, Christa; MINASI, Mark; SMITH, Brian; TOOMBS, Doug. **A Bíblia do Windows 2000 Server.** 1. ed. São Paulo: Makron Books, 2001.

ARAUJO, Gorgonio. **DHCP: Por que Usar?.** Disponível em: https://memoria.rnp.br/newsgen/9705/n1-2.html. Acesso em: 10 maio 2023.

DAUTI, Bekim. **Windows Server 2019 Administration Fundamentals: A beginner's guide to managing and administering Windows Server environments.** 2. ed. Chicago: Packt Publishing, 2019.

GUNAWARDANA, Kushantha. **Aprenda a ficar Anônimo na Internet.** 1. ed. São Paulo: Novatec Editora Ltda., 2023.

LECHETA, Ricardo R. **AWS para Desenvolvedores.** 1. ed. São Paulo: Novatec Editora Ltda., 2014.

LIMA, M. E.; MIOTO, R. C. T. **Pesquisa bibliográfica: um estudo de sua estrutura.** Revista Katálysis, v. 10, n. 2, p. 37-45, 2007.

LINS, Theo. **Redes Definidas Por Software (Software Defined Networks) SDN.** Disponível em: https://www2.decom.ufop.br/imobilis/redes-definidas-por-software-software-defined-networks-sdn/. Acesso em: 20 maio 2023.

MARSHALL, Oliver. **Windows 2003 Active Directory: An overview.** Disponível em: https://techgenix.com/windows_2003_active_directory_overview/. Acesso em: 01 maio 2023.

MELBER, Derek. **Windows & Active Directory Auditing.** Disponível em: https://techgenix.com/windows-active-directory-auditing/. Acesso em: 14 maio 2023.

MICROSOFT. **Árvores de Domínio.** Disponível em: https://learn.microsoft.com/pt-br/windows/win32/ad/domain-trees. Acesso em: 01 nov. 2023.

MICROSOFT. **Autenticação multifator no Microsoft.** Disponível em: https://www.microsoft.com/pt-br/security/business/identity-access/microsoft-entra-mfa-multi-factor-authentication. Acesso em: 01 nov. 2023.

MICROSOFT. **Comparação das edições Standard e Datacenter do Windows Server 2019.** Disponível em: https://learn.microsoft.com/pt-br/windows-server/get-started/editions-comparison-windows-server-2019?tabs=full-comparison. Acesso em: 10 set. 2023.

MICROSOFT. **Grupos de segurança do Active Directory.** Disponível em: https://learn.microsoft.com/pt-br/windows-server/identity/ad-ds/manage/understand-security-groups. Acesso em: 03 nov. 2023.

MICROSOFT. **Introdução ao Windows Server.** Disponível em: https://learn.microsoft.com/pt-br/windows-server/get-started/get-started-with-windows-server. Acesso em: 15 set. 2023.

MICROSOFT. **Windows Server 2019 Essentials.** Disponível em: https://www.microsoft.com/pt-br/evalcenter/evaluate-windows-server-2019-essentials. Acesso em: 20 set. 2023.

MINASI, Mark. **Dominando o Windows Server 2003 - A Bíblia.** 1. ed. São Paulo: Makron Books, 2005.

MOSKOWITZ, Jeremy. **Group Policy: Fundamentals, Security, and Troubleshooting.** 1. ed. New York: Sybex, 2008.

PARAM, Kelvin. **Building a Bridge to the Active Directory.** Disponível em: https://www.perl.com/pub/2001/12/19/xmlrpc.html/. Acesso em: 01 maio 2023.

POSEY, Brien. **Introducing Windows Vista's Active Directory Search Tool.** Disponível em: https://techgenix.com/introducing-windows-vistas-active-directory-search-tool/. Acesso em: 05 maio 2023.

POSEY, Brien. **Making Your DNS Service Fault Tolerant.** Disponível em: https://techgenix.com/making-dns-service-fault-tolerant/. Acesso em: 05 maio 2023.

SANTANA, Fabiano de. **WINDOWS 2000 - AD – Active Directory.** Disponível em: https://www.juliobattisti.com.br/fabiano/artigos/activedirectory.asp. Acesso em: 01 maio 2023.

SANTOS, Anderson; CAMARA, Fábio. **Implantando o Active Directory.** 1. ed. Florianópolis: Visual Books, 2002.

SHIMONSKI, Robert J. **File System Planning for Active Directory 101.** Disponível em: https://techgenix.com/file-system-planning-active-directory/. Acesso em: 20 maio 2023.

TULLOCH, Mitch. **How to Implement Group Policy Security Filtering.** Disponível em: https://techgenix.com/group-policy-security-filtering/. Acesso em: 16 maio 2023.

WELTMAN, Rob; DAHBURA, Tony. **LDAP Programming with Java.** 1. ed. Austin: Addison-Wesley Professional, 2000.