SPECIFICATION DOCUMENT

Emil Cheteg C00275877

Securing Active Directory (AD) with Open-Source Tools in a Proxmox and Hyper-V Virtual Environment

02/12/2024

Contents

Part 1: Specification

1. Executive Summary

The goal of this project is to create a secure and well-structured Active Directory (AD) infrastructure for a company. The setup will involve configuring a primary Domain Controller (DC) on a physical server using virtualization technologies to add and manage additional domain-joined devices. The project will also focus on. Creating an organisational structure within AD by defining Organisational Units (OU's) based on departments, locations and user roles, while ensuring appropriate user and group configurations like security groups, distribution groups. Etc. After establishing the domain and structure. The security posture of the environment will be assessed and strengthened through a series of audits and tests. Finally, disaster recovery procedures will be implemented using VM technology for backup and recovery.

2.Introduction

2.1 Background

Active Directory is a key tool for managing users, computers and network resources in many organisations. It handles who can access what and ensures smooth operations. However, Active Directory is a common target for cyber-attacks, so keeping it secure is very important. This project focuses on creating a secure and well organised Active Directory setup for a sample company. It will include physical and virtual devices, strong security measures and proper monitoring to protect against threat.

2.2 Problem Statement

Active Directory is often the main system for managing access to a company's network. However, poor setup and weak security can make it easy for attackers to exploit. Gain higher privileges, access sensitive data, or cause breaches. This project will focus on building a secure Active Directory system with clear organisation, proper user roles management and strong security measures. It will also include backup and recovery plans to keep the business running smoothly in case of issues.

2.3 Objectives

The objective of the project are as follows:

- Set up and configure a primary Domain Controller on physical device and additional virtual Domain Controller.
- Implement a logical structure within Active Directory, including Organisational Units for departments, locations, users, and computers.
- Establish and configure security groups and distribution groups for managing permissions effectively
- Integrate both physical and virtual devices into the AD domain, ensuring secure authentication and access.
- Assets the security of the AD environment using various tools and implement necessary hardening measures.
- Set up a disaster recovery solution to back up the AD database and configuration, ensuring that the system can recover quickly in case of failure.

2.4 Scope

This project focuses on setting up and securing an Active Directory infrastructure, particularly addressing the following key aspects.:

- Domain Controller Setup: The primary domain controller will be set up on the physical server with additional virtual domain controllers to ensure redundancy.
- Organizational Units (OUs): OUs will be configured to represent the company's departments, locations, and user roles.
- User and Group Management: Security groups, distribution groups, and user permissions will be configured according to organizational needs.
- Security Hardening: The Active Directory environment will be truly assessed for security vulnerabilities, and necessary steps will be taken to secure it.
- Backup and Disaster Recovery: Veeam Backup will be used to ensure regular backups of the Active Directory database, ensuring fast recovery in case of disaster.

Benefits of Virtualisation:

- Cost Savings: Virtualization reduces hardware cost because multiple virtual machines can run on one physical server.
- Scalability: It’s easy to add more virtual Domain Controllers as the organization grows, making it easier to scale the AD infrastructure.
- High Availability: Virtualization ensures that if one domain controller fails, another one can take over without much downtime., keeping the system available.
- Better Resource Management: Virtualization helps allocate resources efficiently. Virtual machines can use only the resources they need, optimising server usage.
- Easier Testing: Virtual machines can be isolated from the production environment, making it safer to test new configurations and security measures.
- Disaster Recovery: Virtualization helps with disaster recovery by allowing quick backup and restoring VM's easily in this case of a failure.

3. Literature Review

3.1 Key Features of Active Directory

Why is Active Directory Important?

Active Directory makes it easier to manage network resources by centralising control. This simplifies handling or multiple users and devices. Ensures the rules are applied consistently. And makes managing access more efficient. It also plays an important role in keeping an organisation IT system secure and reliable.

Real-World Example:

At our university, with thousands of students and faculty, Active Directory helps the IT team manage user accounts, provide access to systems like e-mail, management tools, and the library database, and apply security rules consistently across the campus network.

However, managing Active Directory can be tough, especially for organisations with limited budgets for expensive security tools. The growing complexity of IT systems and advanced cyber threats make keeping Active Directory secure even harder. This research focuses on tackling this challenge is by exploring free open-source tools to improve Active Directory security in virtual environments.

3.2 Questions:

Effectiveness of open-source tools:

Can open-source stores effectively identify and mitigate? Active Directory vulnerabilities?

Role of virtualization technologies:

What roles do virtualization technologies play in hatching the resilience of Active Directory environments?

Cost effective security solutions:

How can organisation achieve a cost-efficient balance between security and operational flexibility?

3.2 Security Best Practices for AD

Securing Active Directory is crucial for protecting sensitive data and controlling access to the network. Two and hey security, I will follow these key steps:

- Applying the least privilege principle to give users only the access they need, reducing risk of MIS use.
- Enforce strong password policies with complex passwords, Regular updates, an account lockout after failed attempts.
- Use Group Policy objects. To ensure all devices follow consistent security rules such as logging controls and software restrictions.
- Implement multifactor authentication for extra protection, especially for admin accounts by requiring a second verification step like a phone code.

3.3 Security Measures for AD

To keep the Active Directory environment secure, following these steps can be done:

Security audits: Regular cheques will be done on the Active Directory setup to find any weakness or mistakes. These cheques will focus on user permissions and security settings to make sure everything is correct and safe.

Preventing privilege escalation: It is important to stop users from gaining higher access than they should have. I will carefully manage user roles and permissions to prevent unauthorised access to sensitive data.

Vulnerability scanning: Regular scans will be performed to find any weakness in the system that hackers could exploit. These scans will find problems before they can be used by attackers.

Real time monitoring: Continuous monitoring will be set up to keep an eye on all Active Directory's activities. This includes tracking logins, access to sensitive files, and any usual action that might suggest someone is trying to break into the system.

3.4 Virtualisation Technologies

Virtualization will play an important role in this project. The primary domain controller can be set up on a physical server, and other Domain Controller and devices can be created as virtual machines. Virtualization helps make the system more flexible and reliable. If one virtual machine fails, another one can quickly take its place.

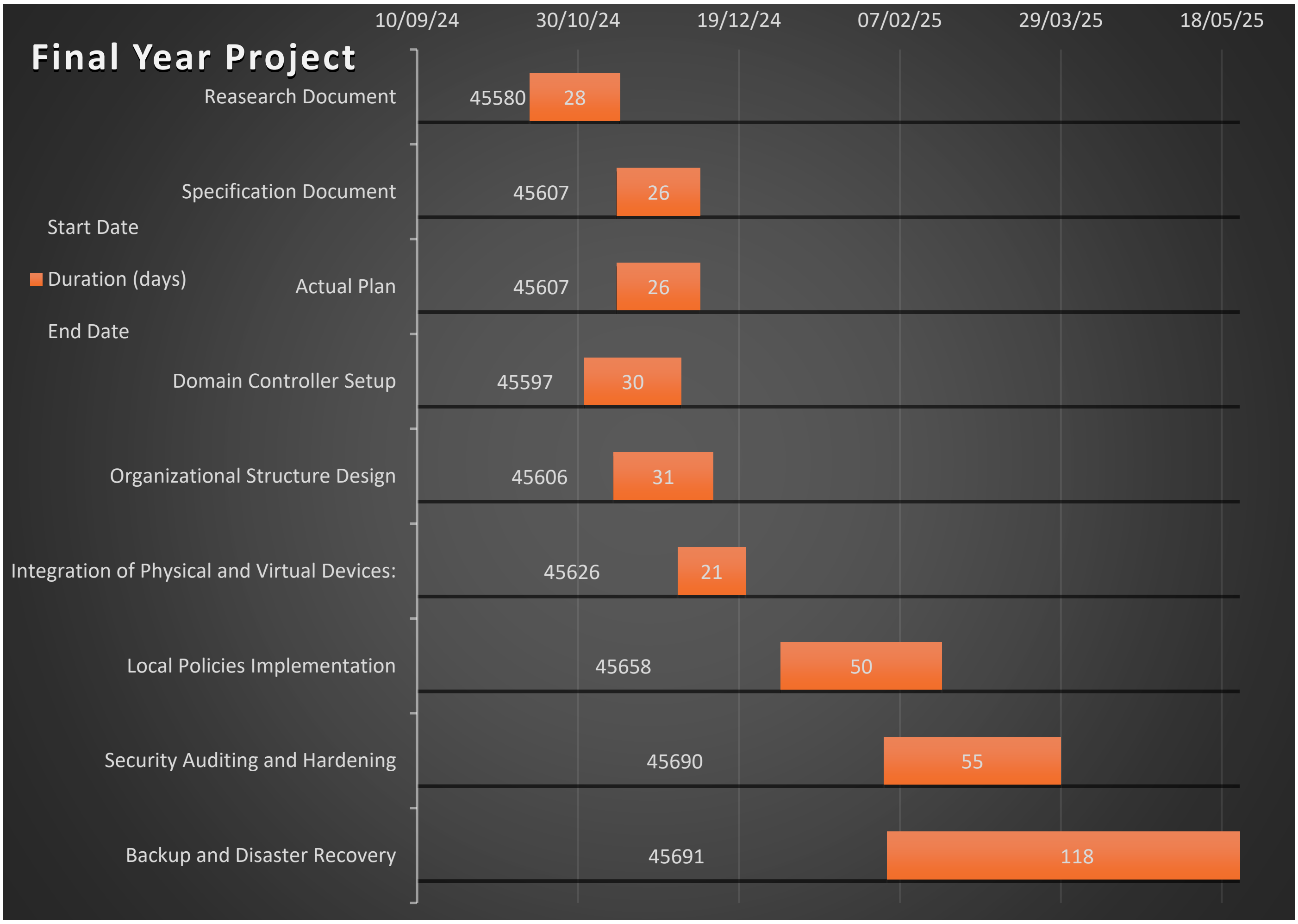
These machines will act as an additional domain controller or other network devices like computers or test servers. Even though these devices are virtual, they will still follow the same security rules and be part of the Active Directory network. The only difference is that they are sitting in a virtual environment or in a cloud.

The biggest benefit of virtualization is that it makes it easier to expand the system. If the company grows, more virtual devices can be added without needing more physical hardware. It also makes backup and recovery easier, because virtual machines can be quickly restored if something goes wrong.

Part 2: Implementation Plan

Project Timeline and Gantt Chart

The Gantt chart below shows the project timeline, highlighting the main tasks how they depend on each other for setting up a securing the Active Directory system. It shows the steps needed to complete the project from start to finish. The chart includes key stages like setting up the domain controller, designed organisational structure, securing the system, integrating devices, and setting up backup and recovery.



4. Methodology

4.1 Domain Controller Setup

First step in setting up the Active Directory environment is to install Windows Server on a physical machine and promote it to a domain controller. This server will play a crucial role in managing the Active Directory (AD) services, such as user authentication, managing access to network resources, and ensuring security across the network. As part of the setup, we will install the Active Directory Domain Services (AD DS) role., which allows the user to take on the responsibilities of managing the domain.

In addition to Active Directory Domain System (AD DS), The DNS (Domain Name System Service) will also be installed. DNS is critical for ensuring the devices on that Devices on the network can locate and communicate with the domain controller. It resolves domain name to IP addresses, making sure devices can find resources in their domain. Then we'll configure DNS to work with Active Directory to ensure smooth communication within the domain. Additionally, the DHCP (Dynamic Host Configuration Protocol) role will be set up on the domain controller as shown in Figure1.

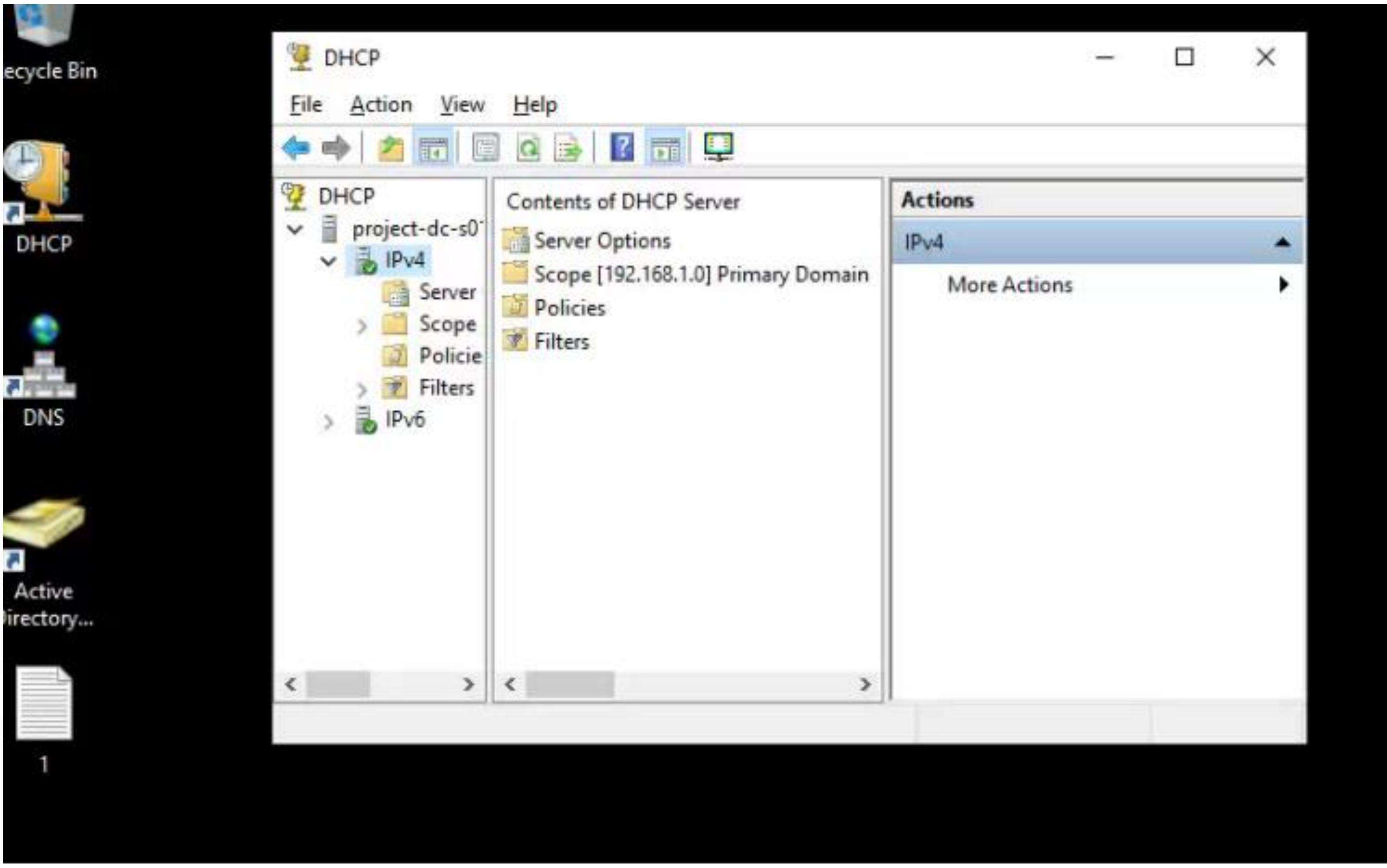


Figure1

DHCP will automatically assign IP addresses to devices joining the network, which simplifies network management and ensures that each device gets the correct network settings and the corresponding IP address followed by the subnet masks and DNS as shown in Figure2.

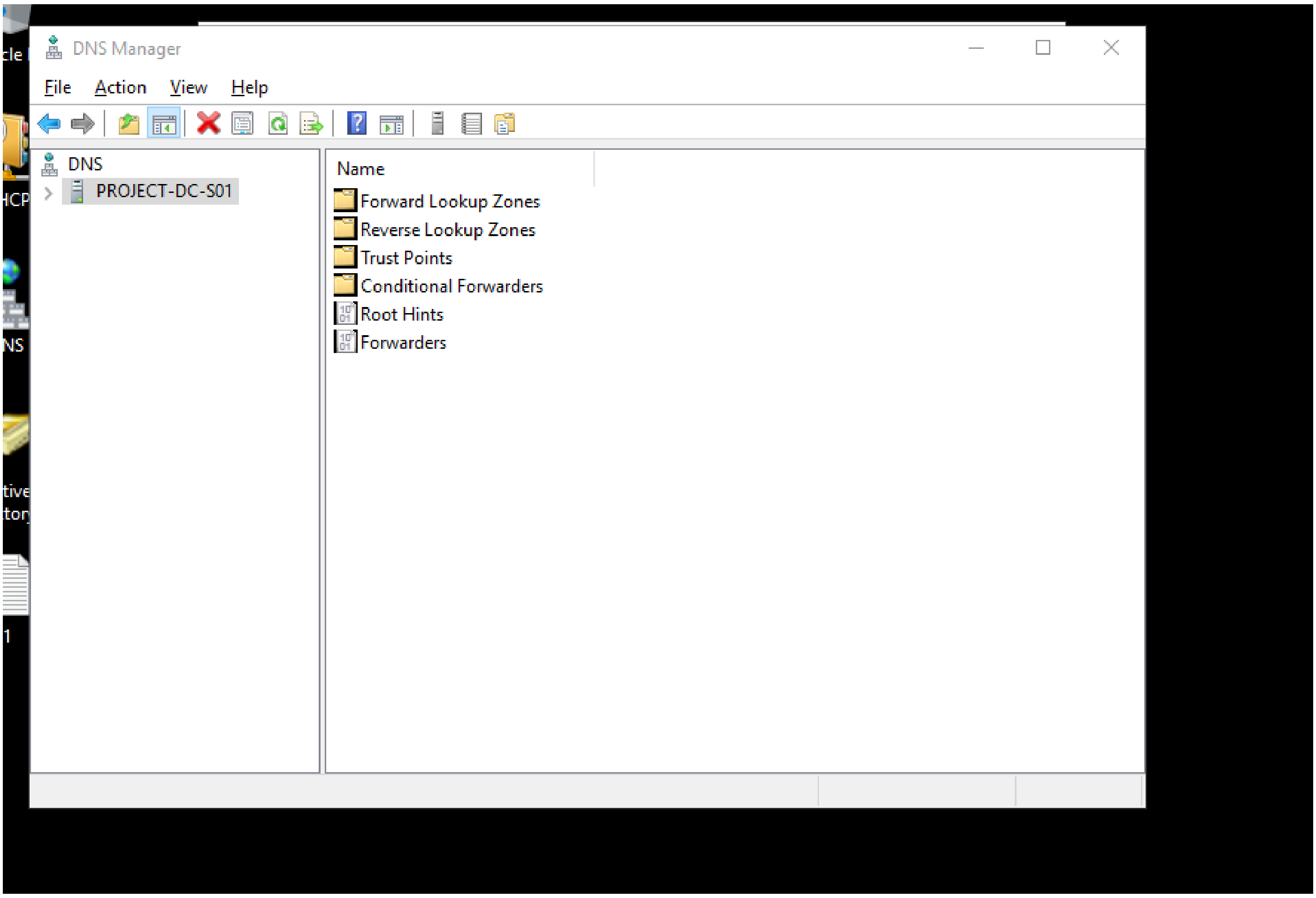


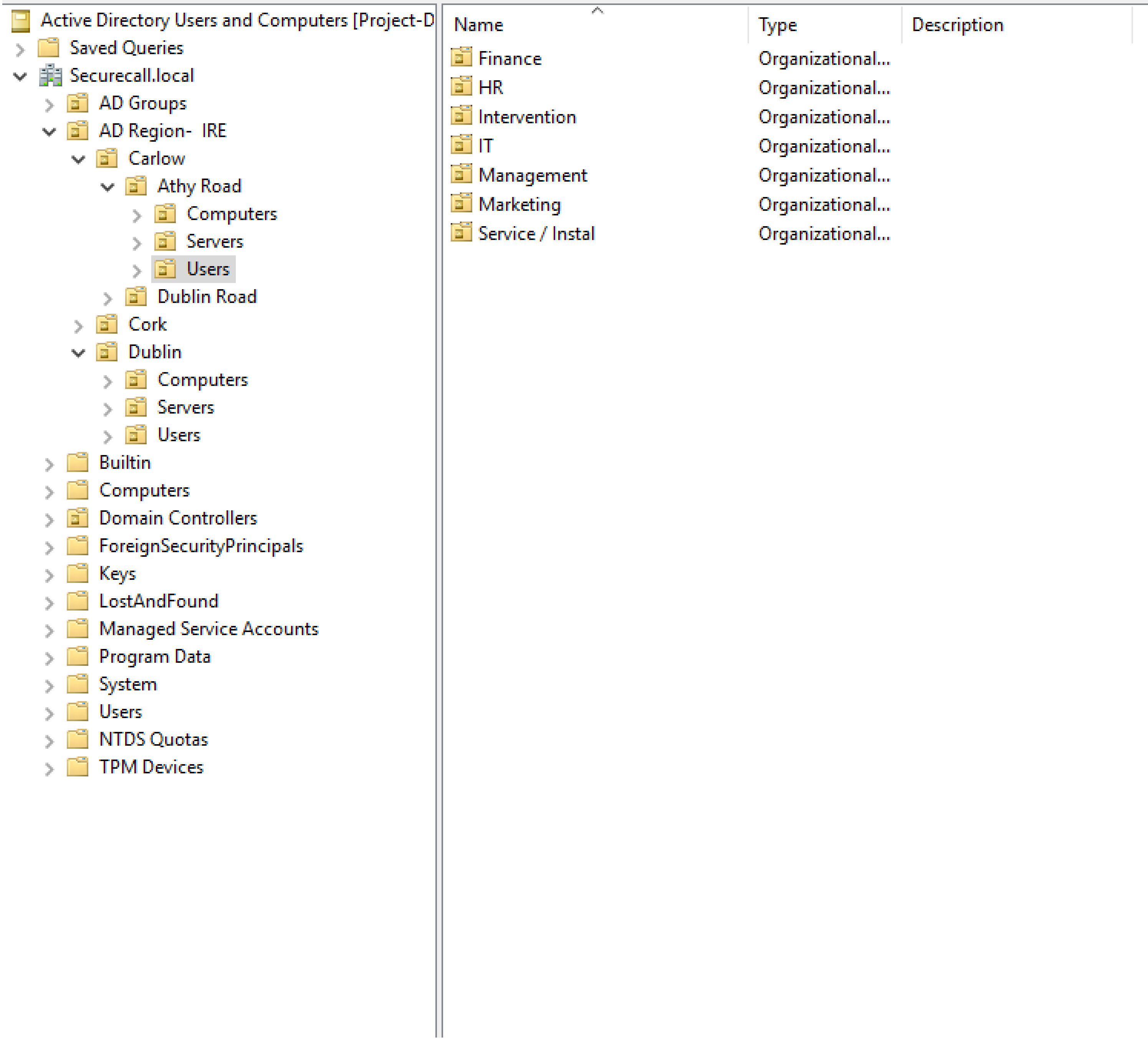
Figure2

Finally, during the setup process will create a new domain within a New Forest, which is the top-level structure in Active Directory that organises the entire network. This new domain will be the root of the Active Directory higher hierarchy. We will also ensure that time synchronisation is configured as all domain-joined devices need to have synchronised clocks for proper authentication. After the installation will verify the setup using diagnostic tools to ensure that the domain controller is functioning correctly an all roles like AD DS, DNS and DHCP are working as expected. This setup will serve as the foundation of our Active Directory environment.

4.2 Organisational Structure Design

Once the primary domain controller is operational, the next step will be to design the Active Directory structure. Organisational Units (Ous) will be created to reflect the company's department, location and user roles. This ensures that the Active Directory environment is organised in a way that aligns with the company's business structure. For example, separate Organisation Units will be created for IT, HR, Marketing and Finance. Departments, and each, Organisational units (OU's) will have its own set of users and computer objects as shown in Figure3 and Figure 4.

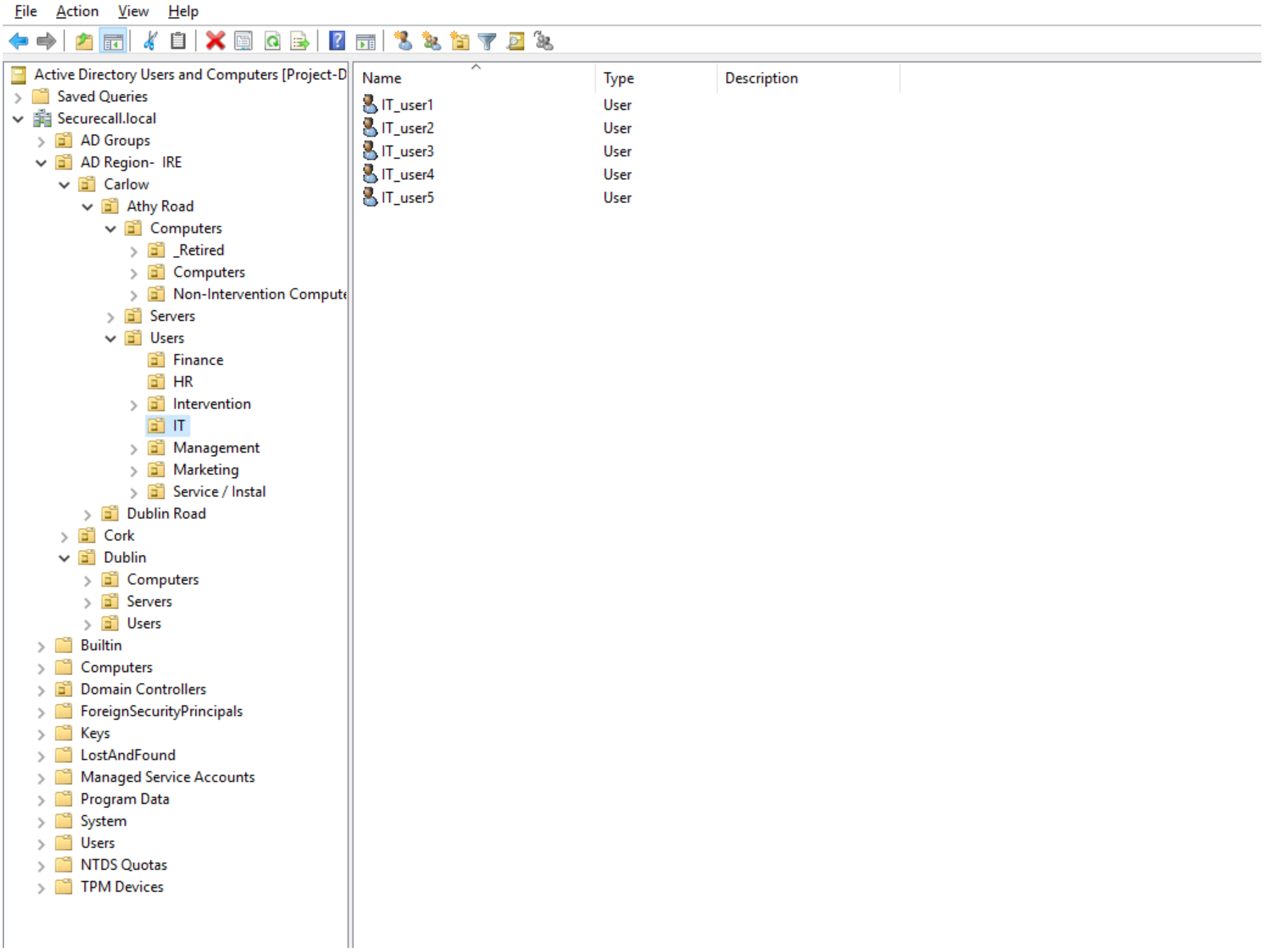
Figure



- Active Directory Users and Computers [Project-D
  - Saved Queries
  - Securecall.local
    - AD Groups
    - AD Region- IRE
      - Carlow
        - Athy Road
          - Computers
          - Servers
          - Users
        - Dublin Road
      - Cork
      - Dublin
        - Computers
        - Servers
        - Users
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Keys
    - LostAndFound
    - Managed Service Accounts
    - Program Data
    - System
    - Users
    - NTDS Quotas
    - TPM Devices

Name	Type	Description
Finance	Organizational...	
HR	Organizational...	
Intervention	Organizational...	
IT	Organizational...	
Management	Organizational...	
Marketing	Organizational...	
Service / Instal	Organizational...	

Figure3



```
Active Directory Users and Computers [Project-D
  Saved Queries
  Securecall.local
    AD Groups
    AD Region- IRE
      Carlow
        Athy Road
          Computers
            _Retired
            Computers
            Non-Intervention Compute
          Servers
          Users
            Finance
            HR
            Intervention
            IT
            Management
            Marketing
            Service / Instal
        Dublin Road
      Cork
      Dublin
        Computers
        Servers
        Users
    Builtin
    Computers
    Domain Controllers
    ForeignSecurityPrincipals
    Keys
    LostAndFound
    Managed Service Accounts
    Program Data
    System
    Users
    NTDS Quotas
    TPM Devices
```

Name	Type	Description
IT_user1	User	
IT_user2	User	
IT_user3	User	
IT_user4	User	
IT_user5	User	

Figure4

Additionally, security groups will be created to manage user permissions and access to resources. Distribution groups will be set up for e-mail communication with specific teams and departments. This approach ensured that users can be managed effectively according to their role within the organisation.

4.3 Integration of Physical and Virtual Devices

Physical devices such as PC's, laptops and servers will be integrated into the Active Directory domain by joining them to the domain using network configuration. Each device will be assigned an IP address from the predefined IP range created during the domain controller setup, ensuring they are within the same subnet as the domain controller. This is crucial for having the best communication between devices and the domain. To join the domain, each device will be configured to authenticate via Active Directory using the username and password that were created on the domain controller during setup. Once joined, the devices will be part of the Active Directory environment. Allowing them to authenticate and access domain resources securely.

In parallel, virtualization, devices running on platforms such as Proxmox and Hyper V will also be added to the domain in the same manner, ensuring they are within the same IP addresses range and subnet as the physical devices. These virtual devices will be set up with the same security policies and user credentials as the physical ones, ensuring a consistent and unified network environment. After joining the domain, all devices, whether physical or virtual, will receive the appropriate Group Policy object that defines security settings, user permissions, and access to network resources. This ensures that all devices in the network are securely configured and follow the same security standards, providing consistency and reducing administrative overhead.

4.4 Security Auditing and Hardening

Once the Active Directory environment is set up and running, the next step is to check how secure it is by using various tools to find any weakness or mistakes in the system setup. The goal is to strengthen the system and prevent any vulnerabilities that could be exploited by attackers.

First, PingCastle will perform a full security health check off the Active Directory setup. This tool will look for any misconfiguration or security issues within the Active Directory environment, like weak settings or incorrect permissions. It will also provide a report that highlights any problems, helping us to understand where the system is vulnerable. Based on this report, we can take immediate action to fix this weakness an improve security.

Next, we'll use Bloodhound to check for any potential risk where attackers could gain higher access or permissions than they should have. This tool looks at how users, group and permission are set up in Active Directory. It helps us see if any users have unnecessary or risky access to sensitive data or system, and it can also point out areas where privileges escalations might be possible (where a normal user could gain administrative access). By identifying these potential attacks paths, we can remove risky permissions and lock down access to prevent unauthorised users from gaining control.

Another important tool can will be used is Open VAS. This tool will scan the network, and all the devices connected to the Active Directory domain. It will search for known vulnerabilities such as outdated software, open ports or misconfiguration system that could be exploited by hackers. OpenVAS will give us a detailed report on those vulnerabilities, so we can patch or fix any weak spots before they become a problem.

Finally, Wazuh will be used to monitor the Active Directory environment in real-time. It will track all user activity, system logs and events happening in the domain. If someone tries to log in using incorrect credentials or if there is any unusual behaviour like multiple failed login attempts, Wasuh will send an alert to notify us. This allows us to quickly respond to potential security threats and investigate any suspicious activities before they escalate.

After gathering results from these tools, we'll take steps to improve the security of the Active Directory environments. This could include updating the password policies to make them stricter (such as requiring longer and more complex passwords), turning off unnecessary services that might be vulnerable, and ensuring that only authorised administrators have access to critical areas of the system. We'll also set up stronger permissions, implement multifactor authentication (MFA) where needed and make sure that only those who really need access to sensitive information or administrative privileges have it. These measures will keep help ensure that the Active Directory environment is more secure and less likely to be targeted by hackers or any other attackers.

4.5 Backup and Disaster Recovery

Finally, a backup strategy will be implemented using Veeam Backup and Replication to ensure regular backups of the Active Directory database and configuration settings. These backups will be stored in secure, redundant location to mitigate the risk of data loss in case of a failure. Regular disaster recovery tests will be conducted to ensure the integrity of the backup data and verify that the Active Directory environment can be restored quickly in case of a failure.

5. Expected Outcomes

Upon completion of the Project, the following outcomes are expected:

- A fully functional and secure Active Directory infrastructure with a clear organisational structure.
- Proper configuration of user and group permissions, including security and distribution groups.
- Integration of both physical and virtual devices into the Active Directory domain with consistent security policies.
- A very good Active Directory environment. With identify vulnerabilities mitigated.
- A reliable disaster recovery plan with regular backups and fast recovery capabilities.
- Clear and comprehensive documentation of all configuration’s security assessments and recovery procedures.