PROJECT FINAL REPORT

EMIL CHETEG C00275877

SECURING ACTIVE DIRECTORY (AD) WITH OPEN-SOURCE TOOLS

IN A PHYSYCAL AND HYPER-V VIRTUAL ENVIRONMENT

27/04/2025

Contents

Introduction

This report describes the setup and configuration of a network using Windows server 2019. The goal of this project was to create a secure and efficient system for managing users, devices, and resources in a business environment. The process involved installing and configuring a Domain Controller, setting up Active Directory, and applying security measures to protect the network. Additionally, tools like NinjaOne , Wazuh, PingCastle , BloodHound , PRTG Map , Kerbrute and NMAP For integrated to improve system management, security monitoring, remote access and pen testing.

In this document, I will explain the steps taken to complete the project, the tools used, and how the system was tested for performance and security. The report also includes a review of the project success and challenges, as well as lessons learned through the process. (2019, 2024)

Setup

The initial setup of the domain infrastructure involved installing and configuring a Windows Server 2019 machine as a domain controller. Additionally, other physical servers were configured to host virtual machines (VMs) using Hyper-V, enabling the simulation of a scalable and secure business environment. Hyper V replica was setup for replication of the second Domain Controller. An Ubuntu server was setup to serve as a device where Open-source tools are installed and configured. Below is a comprehensive overview of what has been completed.

Windows Server 2019 Installation

The process began with the preparation of a bootable USB drive containing the Windows Server 2019 installation files. I downloaded the ISO file from Microsoft official website and used it to Rufus to create a bootable USB. This step included selecting the USB drive in Rufus, specifying the downloaded ISO, and ensuring the appropriate partition scheme (GPT) West chosen for UEFI systems.

With the USB drive ready I Install Windows Server 2019 on the physical PC. This required configuring the BIOS to prioritise booting from the USB. Once the installation with is launched I follow these steps:

1. Selected the "Desktop Experience" installation option to include a graphical interface.
2. Partitioned the hard drive for the operating system.
3. Configured regional and language settings.
4. Completed the installation by creating an administrator account and setting a secure password.

Configuring the Domain Controller

After Installing Windows Server 2019, I proceeded to configure the machine as a domain controller. This involved installing the necessary role and setting up the DHCP, DNS and Active Directory Domain Services

(AD DS).

Role Installation

Using the server manager, I launched the “Add roles and Features” wizard. In this wizard, I selected the following roles:

- Active Directory Domain Services (AD DS): Essential for domain management and authentication.
- DNS Server: Required for name resolution within the network.
- DHCP Server: To dynamically allocate IP addresses to devices.

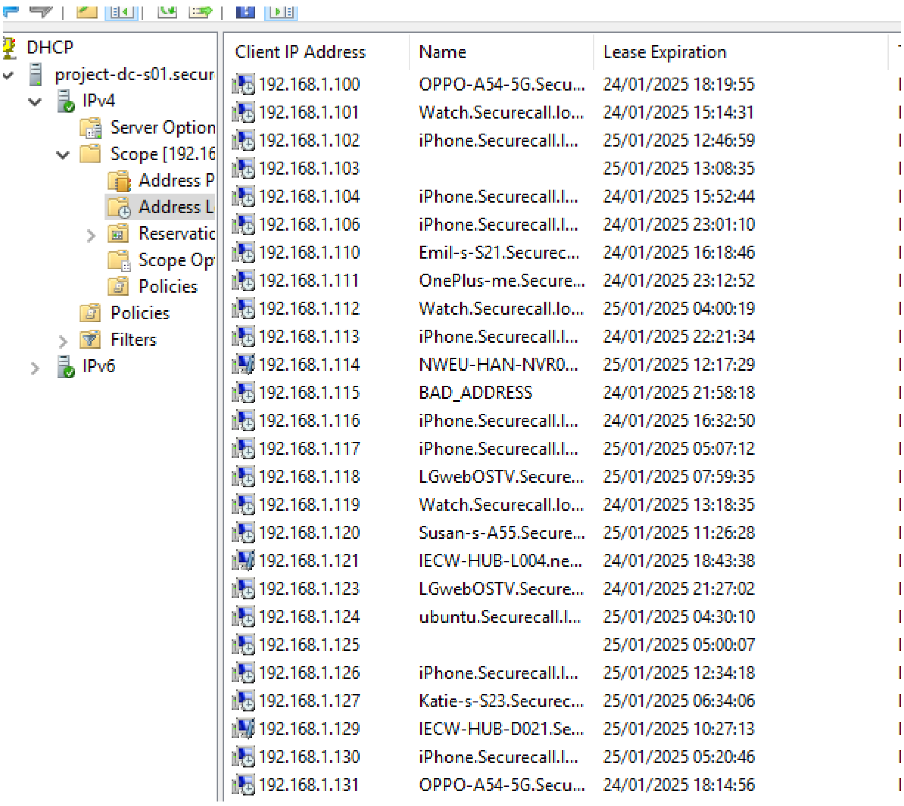
Additional features, such as Group Policy Management, were enabled to facilitate centralised policy control.

DHCP Configuration

The DHCP server was configured with customized IP addresses range to manage network resources and efficiently. The following address allocation were implemented (As shown in Figure 1):

- **192.168.1.1–1.99**: Reserved and excluded from the DHCP scope.
- **192.168.1.100–1.149**: Assigned for key infrastructure devices, including the domain controller.
- **192.168.1.150–1.200**: Allocated for the guest network's router DHCP.
- **192.168.1.201–1.254**: Excluded from DHCP scope to allow for manual assignments if needed.

The DCP options were configured to direct devices to use the domain controllers IP address : 192.168.1.30 for DNS resolution and to set the gateway address for external traffic



Client IP Address	Name	Lease Expiration
192.168.1.100	OPPO-A54-5G.Secu...	24/01/2025 18:19:55
192.168.1.101	Watch.Securecall.lo...	24/01/2025 15:14:31
192.168.1.102	iPhone.Securecall.l...	25/01/2025 12:46:59
192.168.1.103		25/01/2025 13:08:35
192.168.1.104	iPhone.Securecall.l...	24/01/2025 15:52:44
192.168.1.106	iPhone.Securecall.l...	24/01/2025 23:01:10
192.168.1.110	Emil-s-S21.Securec...	24/01/2025 16:18:46
192.168.1.111	OnePlus-me.Secure...	24/01/2025 23:12:52
192.168.1.112	Watch.Securecall.lo...	25/01/2025 04:00:19
192.168.1.113	iPhone.Securecall.l...	24/01/2025 22:21:34
192.168.1.114	NWEU-HAN-NVR0...	25/01/2025 12:17:29
192.168.1.115	BAD_ADDRESS	24/01/2025 21:58:18
192.168.1.116	iPhone.Securecall.l...	24/01/2025 16:32:50
192.168.1.117	iPhone.Securecall.l...	25/01/2025 05:07:12
192.168.1.118	LGwebOSTV.Secure...	25/01/2025 07:59:35
192.168.1.119	Watch.Securecall.lo...	24/01/2025 13:18:35
192.168.1.120	Susan-s-A55.Secure...	25/01/2025 11:26:28
192.168.1.121	IECW-HUB-L004.ne...	24/01/2025 18:43:38
192.168.1.123	LGwebOSTV.Secure...	24/01/2025 21:27:02
192.168.1.124	ubuntu.Securecall.l...	25/01/2025 04:30:10
192.168.1.125		25/01/2025 05:00:07
192.168.1.126	iPhone.Securecall.l...	25/01/2025 12:34:18
192.168.1.127	Katie-s-S23.Securec...	25/01/2025 06:34:06
192.168.1.129	IECW-HUB-D021.Se...	25/01/2025 10:27:13
192.168.1.130	iPhone.Securecall.l...	25/01/2025 05:20:46
192.168.1.131	OPPO-A54-5G.Secu...	24/01/2025 18:14:56

Figure1

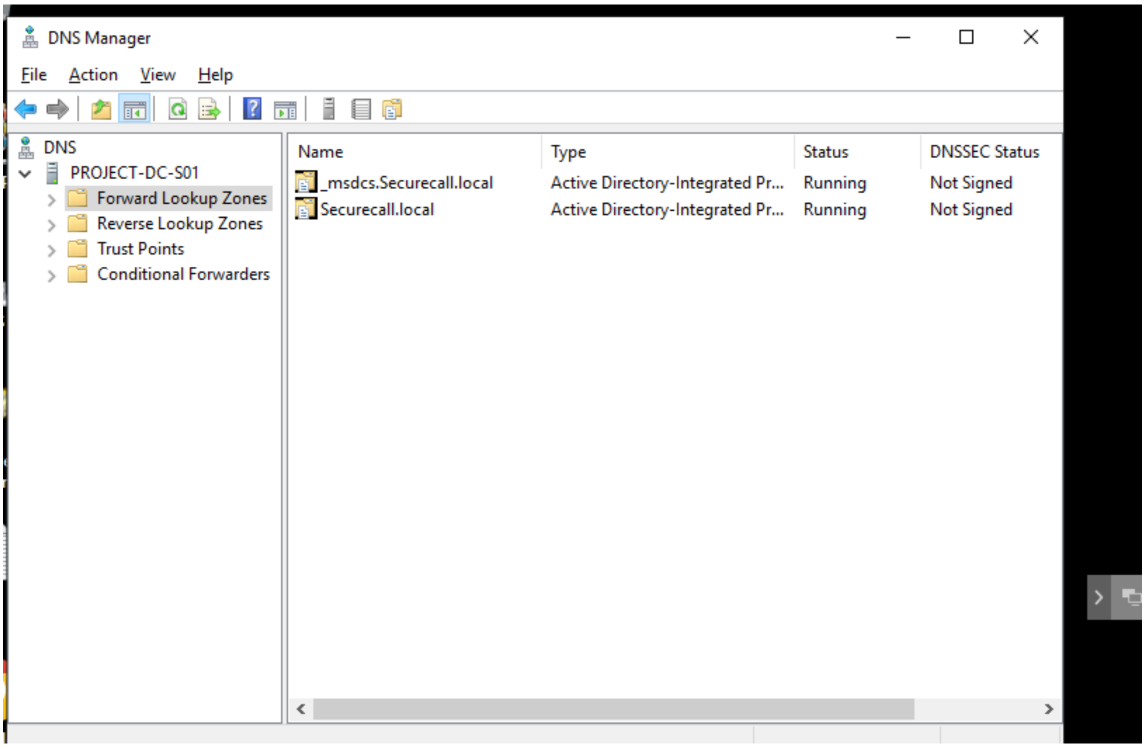
DNS Configuration

The DNS server was set up to manage name resolution for all the devices within the domain. A forward look up zone was created for the domain "Securecall.local," allowing devices to resolve host names to IP addresses. A reverse lookup zone was also configured to enable IP to host name resolution, ensuring seamless communication and network diagnostics (As shown in Figure 2).

Promoting to Domain Controller

The Server was promoted to a Domain Controller by completing the following steps:

1. Running the Active Directory domain services configuration wizard
2. Creating a New Forest with a root domain “Securecall.local”
3. Configuring Replication options and verifying the integration of DHCP and DNS with Active Directory



DNS
- PROJECT-DC-S01
  - Forward Lookup Zones
  - Reverse Lookup Zones
  - Trust Points
  - Conditional Forwarders

Name	Type	Status	DNSSEC Status
_msdcs.Securecall.local	Active Directory-Integrated Pr...	Running	Not Signed
Securecall.local	Active Directory-Integrated Pr...	Running	Not Signed

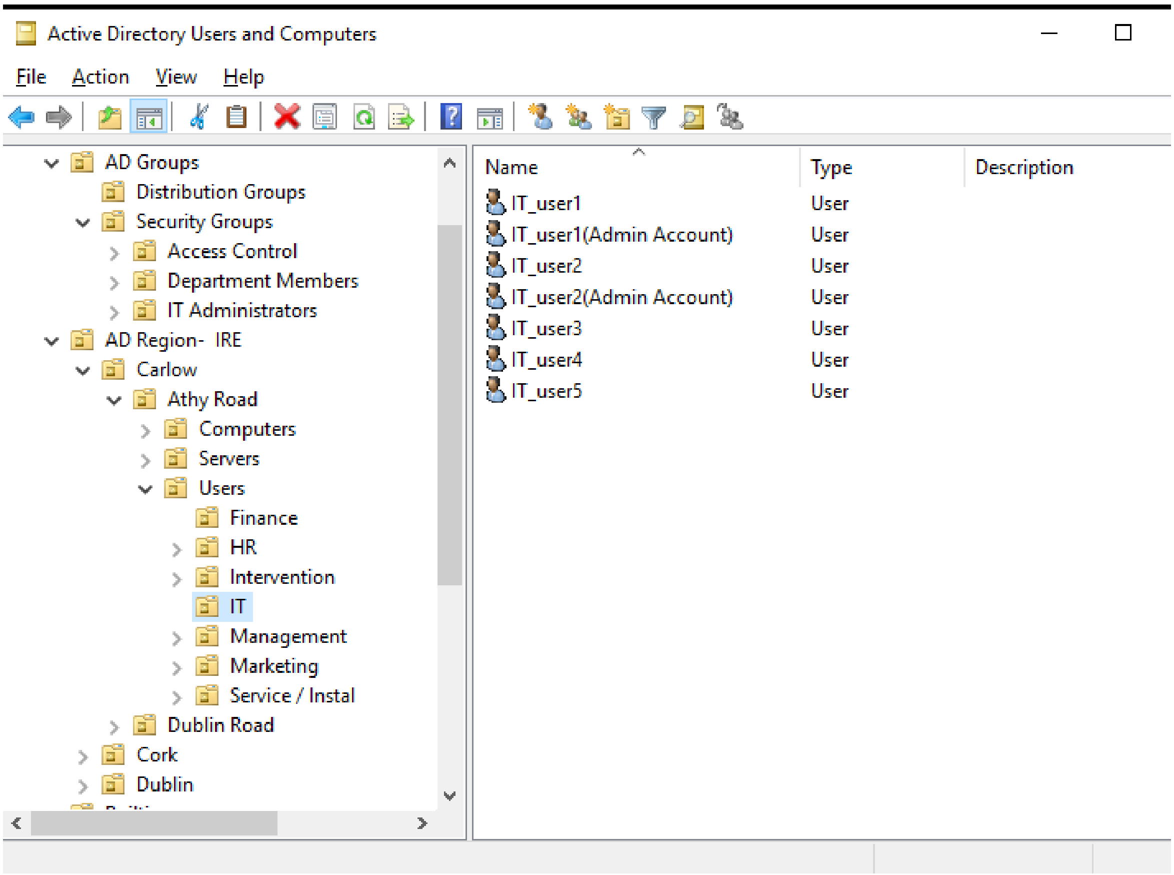
Figure 2

Active Directory Structure

To organize the domain and simplify management, I structured Active Directory by creating specific Organizational Units (OUs). These Ous included (Example on Figure 3):

- Admins: Containing accounts with administrative privileges for managing the domain.
- Guest Users: Containing accounts with restricted access for temporary users.
- Regions: Each region has its own OU, such as:
  - Carlow
  - Dublin
- Departments: Each region’s OU is further divided into departmental OUs, including:
  - Finance
  - HR

- Intervention
- IT
- Management
- Marketing
- Service/Instal

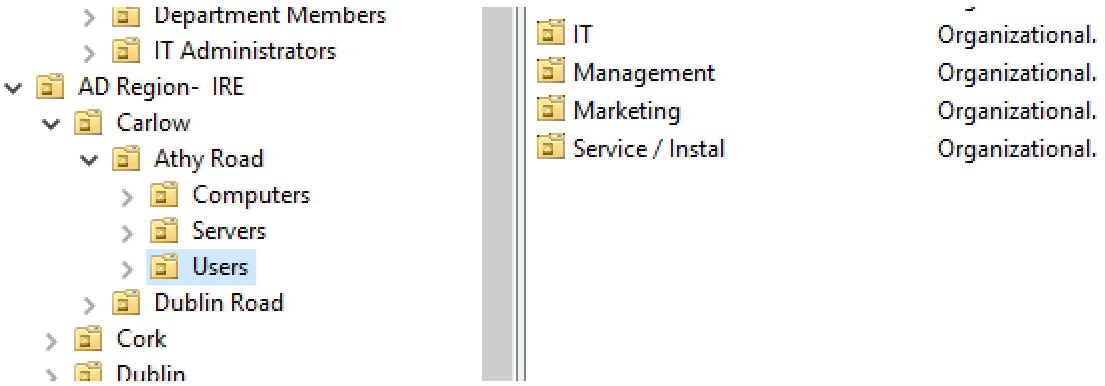


Name	Type	Description
IT_user1	User	
IT_user1(Admin Account)	User	
IT_user2	User	
IT_user2(Admin Account)	User	
IT_user3	User	
IT_user4	User	
IT_user5	User	

Figure 3

- Subdivisions: Within each department, OUs are further divided into (As shown in Figure 4):

- Servers
- PCs
- Users



```
  > Department Members
  > IT Administrators
v AD Region-  IRE
  v Carlow
    v Athy Road
      > Computers
      > Servers
      > Users
    > Dublin Road
  > Cork
  > Dublin
```

IT	Organizational.
Management	Organizational.
Marketing	Organizational.
Service / Instal	Organizational.

Figure 4

Security Groups were created to manage permissions effectively and align with this structure. These groups included:

- Department Members: For access control based on department roles.
- IT Admins: For administrative access across the domain.
- Distribution Groups: Established at both the department and regional levels to make communication easier.

Test user accounts were added to ensure the functionality of group policies, access controls, and communication workflows.

Importance of Structured Security Groups

Why Structured Security Groups Matters:

Better Security:

- Role-Based Access: Assigning permissions based on job roles ensures that people only access what they need, reducing the risk of unauthorized access.
- Least Privilege: Users get the minimum access required for their tasks, which helps protect sensitive information.

Easy Management:

- Central Control: Managing permissions from one place makes it simpler to apply and enforce security rules.
- Scalability: As the company grows, new users can be quickly added to the right groups without manual setup for each person.

Simplified Auditing and Compliance:

- Audit Trails: Clear records of who has access to what make it easier to review and ensure compliance with laws and policies.

Compliance: Consistent application of access controls helps meet industry standards and regulations.

Improved Communication:

- Distribution Groups: These groups help share information quickly and accurately within departments and regions.
- Collaboration: Grouping users by roles and departments makes it easier for team members to work together and share resources.

Testing and Validation:

- Test User Accounts: Using test accounts helps check that security settings work correctly before full deployment.

Virtualization with Hyper-V

A few other physical servers were configured to host virtual machines using the Hyper-V role. This was accomplished by installing the Hyper-V role via Server Manager and then enabling the Virtual Machine management and Hyper-V Platform Features (AnthonyBartolo, 2023).

Virtual Machine Configuration

Several VM's were created, including Windows 2019 and Ubuntu-based VM. The Ubuntu server was configured to maintain security by running Wazuh and PingCastle for data collection. Network adapters were set to use the domain controller's IP address (192.168.1.30) as their default gateway, while router's IP address (192.168.1.254) was designed for external traffic routing. The VM square then joined to the domain by verifying communication with that domain controller, allowing them to operate as domain members. This setup enabled centralised authentication and management through Active Directory

File Sharing and Device Integration

File Sharing

To centralise resources, shared folders were created on the domain controller with permissions based on job roles and access needs. Each department has its own folder, accessible only to its members, and some folders are accessible based on user roles, like admin folders for IT admins. Project folders are accessible only to team members involved in those projects. This setup ensures user can only access the files they need, improving security and preventing unauthorised access. Overall, this organisation of file sharing and device integration improve security, management, and teamwork.

Identified Risks and Gaps

The current setup provides a foundational infrastructure but has several areas requiring improvement.

Here are some gaps:

- Single point of failure: the domain relies on a single domain controller, making it vulnerable to downtime if the server fails.
- No endpoint protection: devices lack tools for detecting and responding to end point attacks.
- No backup solution: there is no mechanism for recovering data or configuration in case of failure.
- Unhardened Systems: security best practises have not been implemented, increasing the risk of compromise.
- Lack of monitoring: There is no centralised monitoring or alerting system

Security implemented

Remote Management with NinjaOne

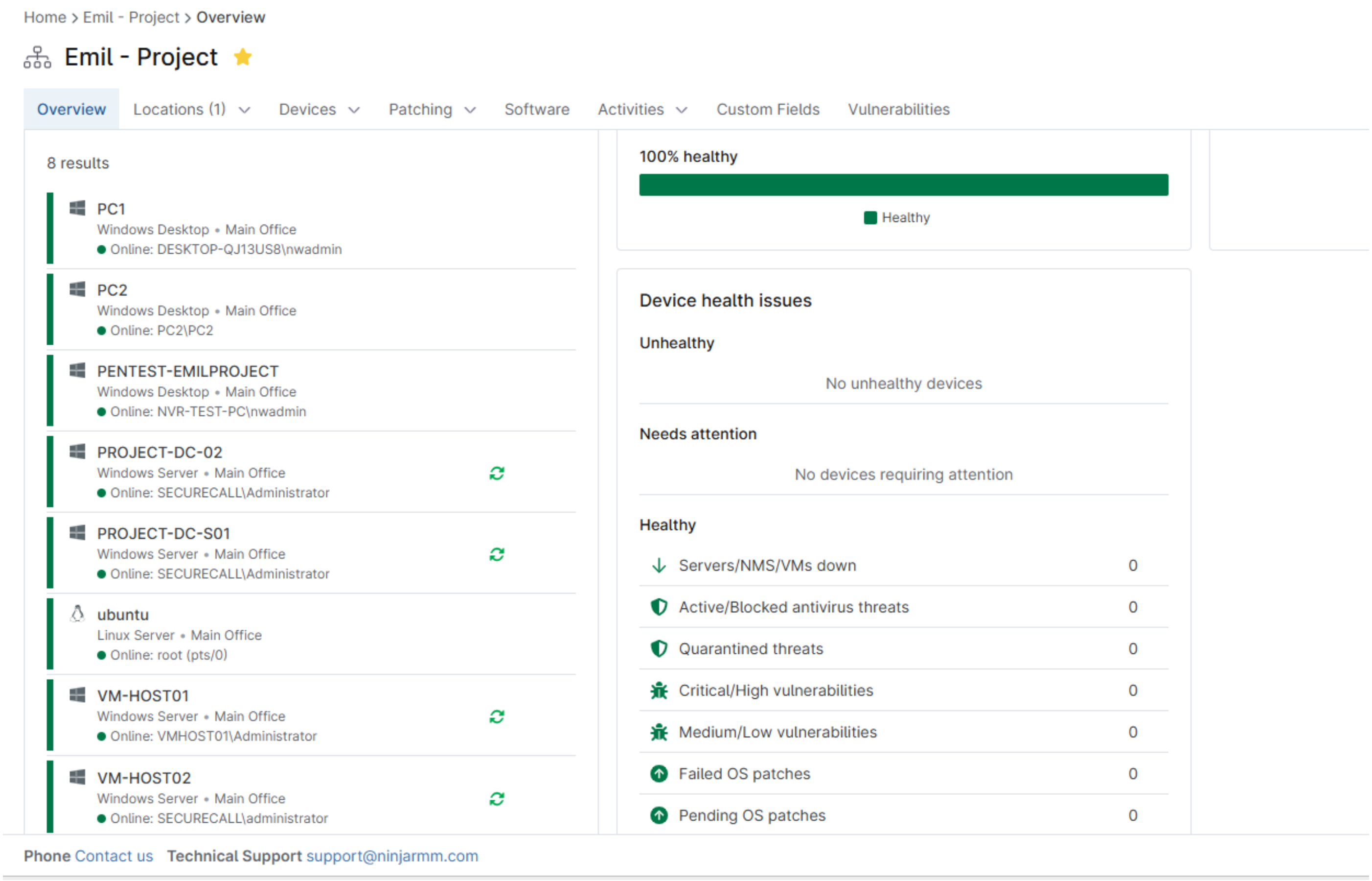
I choose NinjaOne because it is a tool that helps me manage and monitoring devices in real time. It lets me check the health and performance of systems so I can see things like their status, hardware, software, and security. With NinjaOne I can remotely access devices, fix issues, install software, and make sure everything stays up to date with automatic patch management. It also tracks assets, sends alerts, and generate reports. The platform works with other tools, making it easy to manage IT tasks all in one place. The cloud-based dashboard is simple to use, and I can handle everything from one spot without much hassle.

Installing ninja one on server was a relatively straightforward process, as it provides a cloud based remote monitoring and management platform for IT operations. I began by downloading the NinjaOne agent for servers from their official website and follow the installation instructions provided. Agent was easily installed using terminal commands, and I configure it as a service on the server NinjaOne. Agents were diploid to each device to allow me to collect data and connect remotely.

Key Capabilities and features of ninja 1 include:

Remote Access and Management:

All devices are organized within a dedicated folder labelled "Emil Project" (as shown in Figure5)



Home > Emil - Project > Overview

Emil - Project ★

Overview | Locations (1) | Devices | Patching | Software | Activities | Custom Fields | Vulnerabilities

8 results

PC1
Windows Desktop • Main Office
● Online: DESKTOP-QJ13US8\nwadmin

PC2
Windows Desktop • Main Office
● Online: PC2\PC2

PENTEST-EMILPROJECT
Windows Desktop • Main Office
● Online: NVR-TEST-PC\nwadmin

PROJECT-DC-02
Windows Server • Main Office
● Online: SECURECALL\Administrator

PROJECT-DC-S01
Windows Server • Main Office
● Online: SECURECALL\Administrator

ubuntu
Linux Server • Main Office
● Online: root (pts/0)

VM-HOST01
Windows Server • Main Office
● Online: VMHOST01\Administrator

VM-HOST02
Windows Server • Main Office
● Online: SECURECALL\administrator

100% healthy

🟩 Healthy

Device health issues

Unhealthy

No unhealthy devices

Needs attention

No devices requiring attention

Healthy

Servers/NMS/VMs down	0
Active/Blocked antivirus threats	0
Quarantined threats	0
Critical/High vulnerabilities	0
Medium/Low vulnerabilities	0
Failed OS patches	0
Pending OS patches	0

Phone Contact us **Technical Support** support@ninjarmm.com

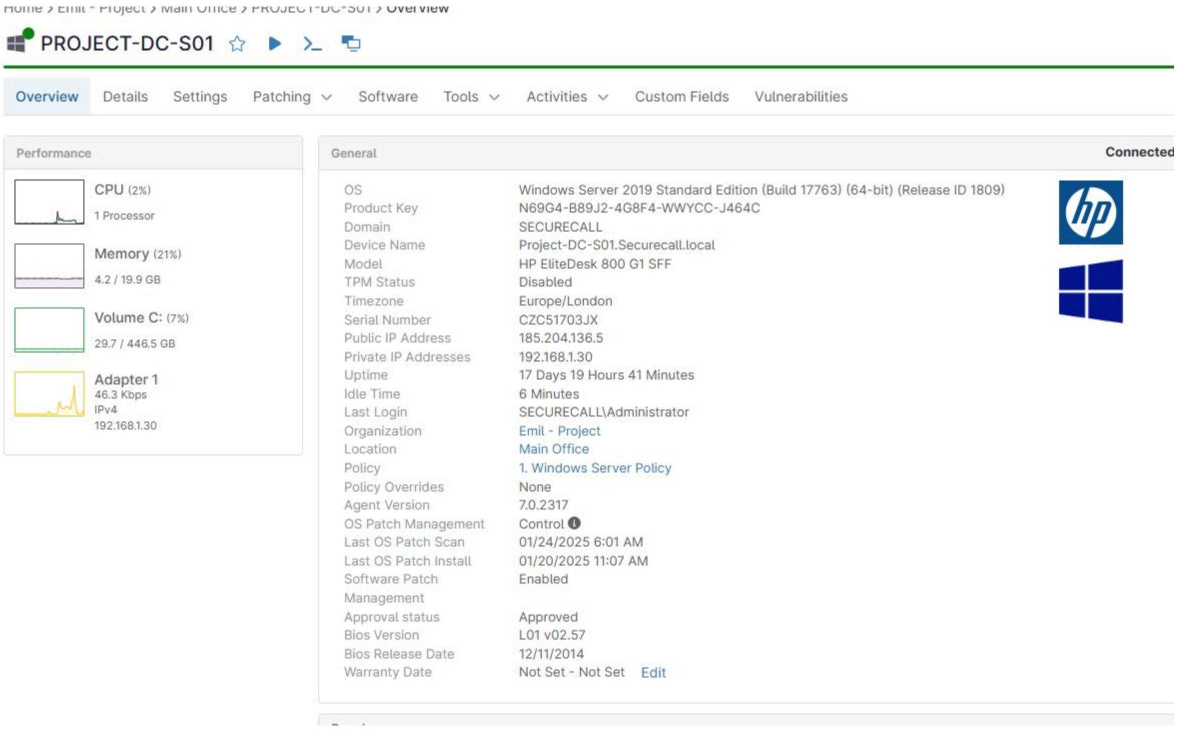
Figure5

Data Collection and Monitoring:

NinjaOne provides detailed insights to (as shown in Figure6):

- Hardware Usage: Real-time data on CPU, memory, volume and network adapters

- Software Information: Driver details, installed application, and vulnerabilities.



Home > Emil - Project > Main Office > PROJECT-DC-S01 > Overview

PROJECT-DC-S01

Overview | Details | Settings | Patching | Software | Tools | Activities | Custom Fields | Vulnerabilities

Performance

CPU (2%)
1 Processor

Memory (21%)
4.2 / 19.9 GB

Volume C: (7%)
29.7 / 446.5 GB

Adapter 1
46.3 Kbps
IPv4
192.168.1.30

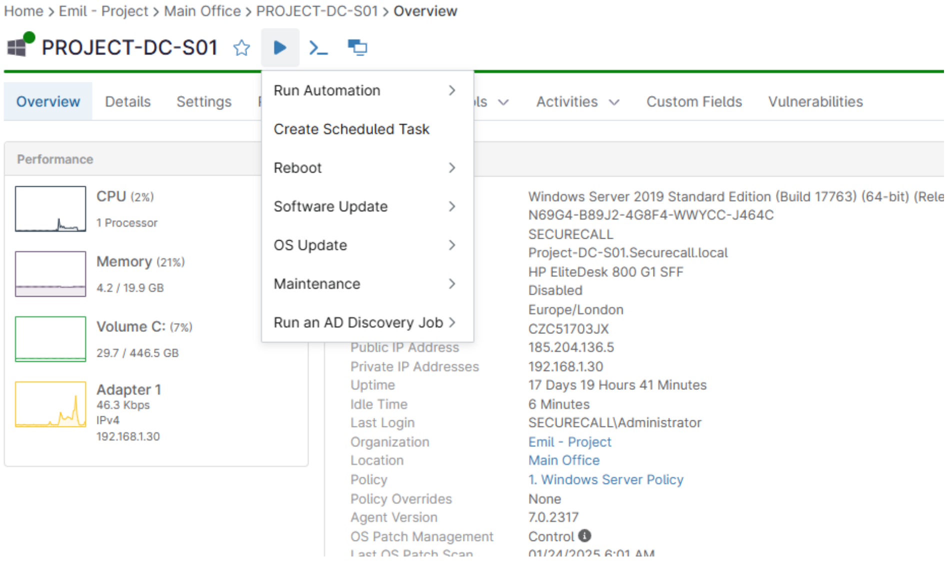
General | Connected

OS	Windows Server 2019 Standard Edition (Build 17763) (64-bit) (Release ID 1809)
Product Key	N69G4-B89J2-4G8F4-WWYCC-J464C
Domain	SECURECALL
Device Name	Project-DC-S01.Securecall.local
Model	HP EliteDesk 800 G1 SFF
TPM Status	Disabled
Timezone	Europe/London
Serial Number	CZC51703JX
Public IP Address	185.204.136.5
Private IP Addresses	192.168.1.30
Uptime	17 Days 19 Hours 41 Minutes
Idle Time	6 Minutes
Last Login	SECURECALL\Administrator
Organization	Emil - Project
Location	Main Office
Policy	1. Windows Server Policy
Policy Overrides	None
Agent Version	7.0.2317
OS Patch Management	Control
Last OS Patch Scan	01/24/2025 6:01 AM
Last OS Patch Install	01/20/2025 11:07 AM
Software Patch Management	Enabled
Approval status	Approved
Bios Version	L01 v02.57
Bios Release Date	12/11/2014
Warranty Date	Not Set - Not Set Edit

Figure 6

Patching and Software Deployment:

- Silent Installation and updates for software across all devices
- Custom script execution to automate tasks or enforce configurations (as shown in Figure7)



Home > Emil - Project > Main Office > PROJECT-DC-S01 > Overview

PROJECT-DC-S01

Overview | Details | Settings | ... | Activities | Custom Fields | Vulnerabilities

Performance

CPU (2%)
1 Processor

Memory (21%)
4.2 / 19.9 GB

Volume C: (7%)
29.7 / 446.5 GB

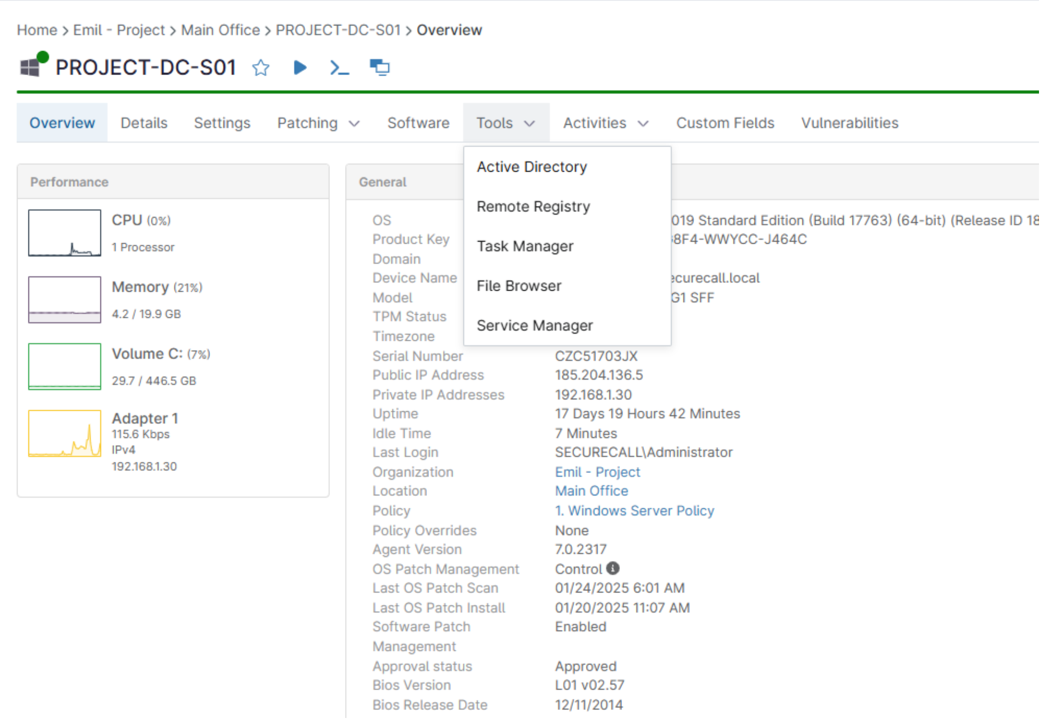
Adapter 1
46.3 Kbps
IPv4
192.168.1.30

	Windows Server 2019 Standard Edition (Build 17763) (64-bit) (Rele
	N69G4-B89J2-4G8F4-WWYCC-J464C
	SECURECALL
	Project-DC-S01.Securecall.local
	HP EliteDesk 800 G1 SFF
	Disabled
	Europe/London
	CZC51703JX
Public IP Address	185.204.136.5
Private IP Addresses	192.168.1.30
Uptime	17 Days 19 Hours 41 Minutes
Idle Time	6 Minutes
Last Login	SECURECALL\Administrator
Organization	Emil - Project
Location	Main Office
Policy	1. Windows Server Policy
Policy Overrides	None
Agent Version	7.0.2317
OS Patch Management	Control
Last OS Patch Scan	01/24/2025 6:01 AM

Figure7

Advanced Troubleshooting Tools:

- Access to remote registry, task manager, file browser, and system diagnostics for quick issue resolution (as shown in Figure8):



CPU (0%)
1 Processor

Memory (21%)
4.2 / 19.9 GB

Volume C: (7%)
29.7 / 446.5 GB

Adapter 1
115.6 Kbps
IPv4
192.168.1.30

OS	019 Standard Edition (Build 17763) (64-bit) (Release ID 18
Product Key	8F4-WWYCC-J464C
Domain	
Device Name	ecurecall.local
Model	G1 SFF
TPM Status	
Timezone	
Serial Number	CZC51703JX
Public IP Address	185.204.136.5
Private IP Addresses	192.168.1.30
Uptime	17 Days 19 Hours 42 Minutes
Idle Time	7 Minutes
Last Login	SECURECALL\Administrator
Organization	Emil - Project
Location	Main Office
Policy	1. Windows Server Policy
Policy Overrides	None
Agent Version	7.0.2317
OS Patch Management	Control
Last OS Patch Scan	01/24/2025 6:01 AM
Last OS Patch Install	01/20/2025 11:07 AM
Software Patch Management	Enabled
Approval status	Approved
Bios Version	L01 v02.57
Bios Release Date	12/11/2014

Figure 8

Vulnerability Management:

Identifies potential risks, ensuring devices remain secure and compliant.

By integrating NinjaOne into the domain setup, the organisation infrastructure is more visible, it improved system management, and streamlined workflows, ensuring devices across the network remain secure and operational (Rodriguez, 2024).

Wazuh Server Deployment

A dedicated Ubuntu 22.04 server was configured to host a Wazuh server, which provides centralized security monitoring and log collection (Wazuh, 2024)

Installation Process

- Installed Ubuntu 22.04 on a physical PC and configured it with a static IP for stable communication.
- Deployed the Wazuh server using its official repository and setup scripts, ensuring dependencies like Elasticsearch and Kibana were installed for data storage and visualization

Wazuh Integration

To install Wazuh on Ununtu Server, I followed the steps outlined in the official Wazuh documentation. I started by adding the Wazuh repository to my system and installing the necessary dependencies using the command line. Once I installed the Wazuh manager, hi configured to run as a service. However, as Wazuh is an open-source tool, it is available for free, but its setup can be a bit tricky. One of the difficulties I encounter was that while Wazuh works only on Ubuntu Server, and Ubuntu Server installation does not come with a GUI interface. Then I had to install and configure a web-based user interface, which would allow me to connect and manage Wazuh via a browser. Once everything was set up, I was able to monitor security events and configure the server through the browser interface.

Then Wazuh agents were deployed on the domain controller and other PC's and VM's (as shown in Figure 14)

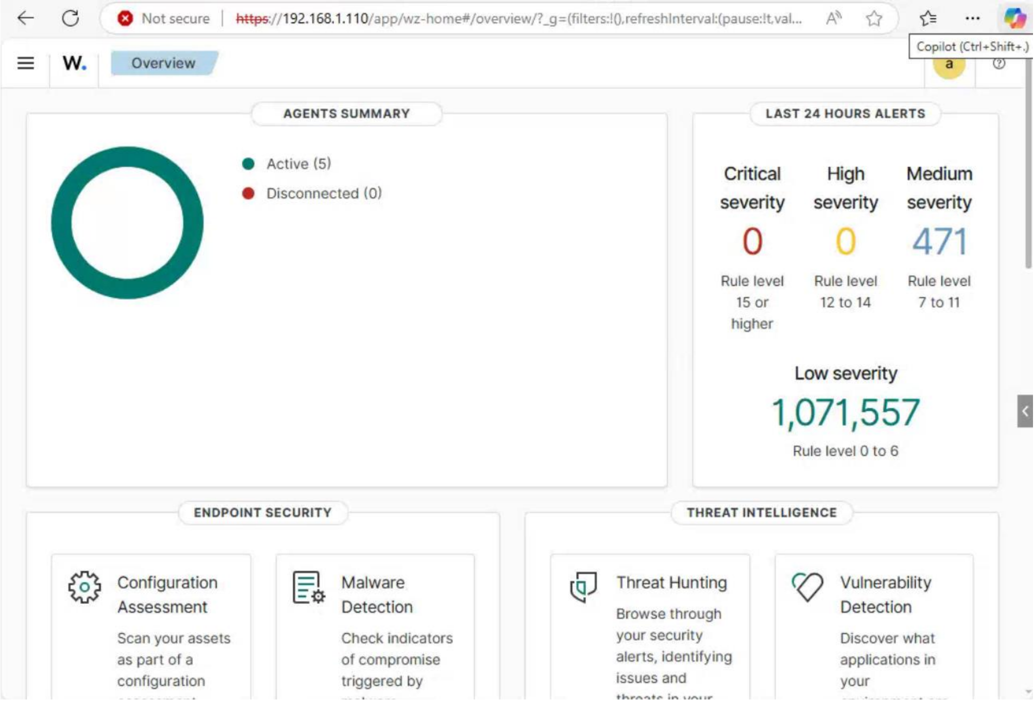
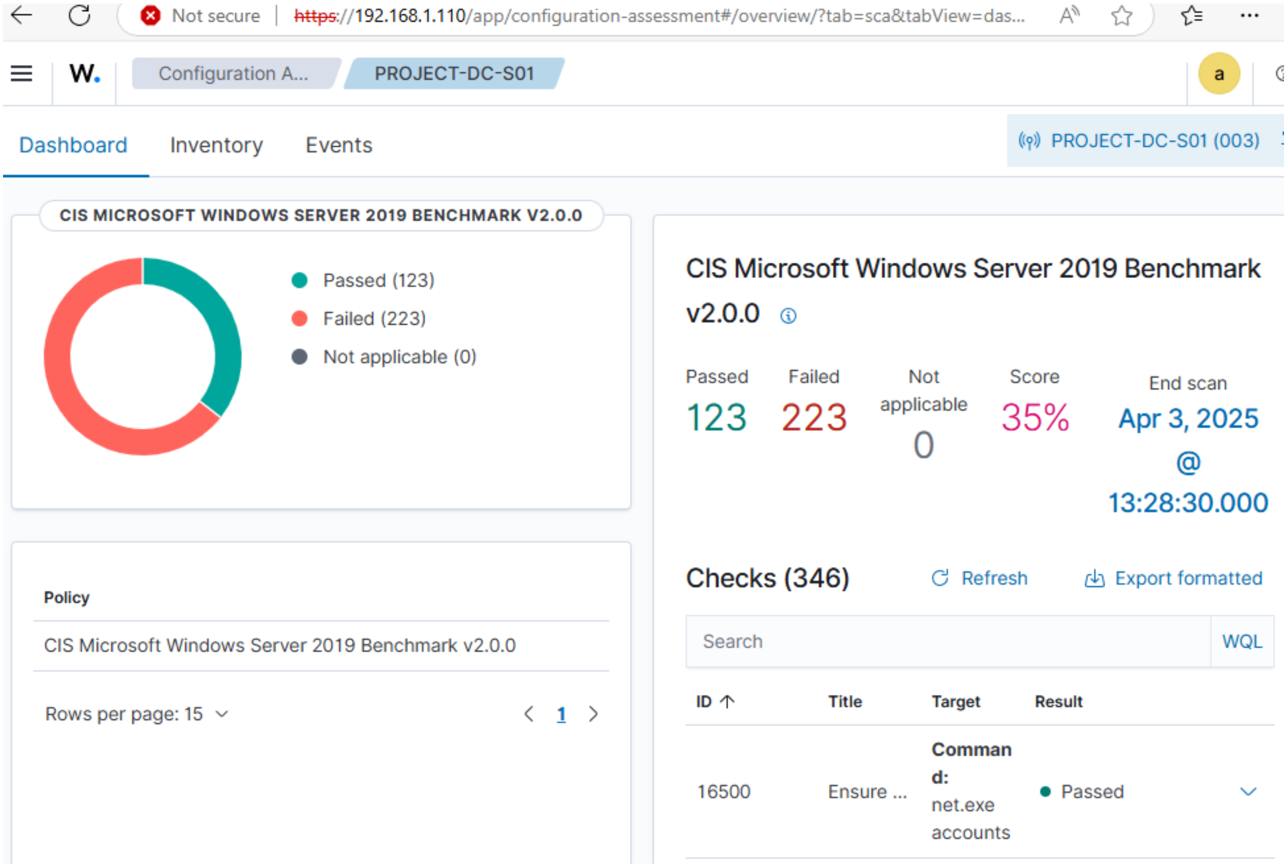


Figure 14

The agents enabled data collection for the following functionalities:

Configuration Assessment:

Identifies misconfiguration using CIS benchmarks:



CIS Microsoft Windows Server 2019 Benchmark v2.0.0

Passed	Failed	Not applicable	Score	End scan
123	223	0	35%	Apr 3, 2025 @ 13:28:30.000

Policy
CIS Microsoft Windows Server 2019 Benchmark v2.0.0

Checks (346)

ID ↑	Title	Target	Result
16500	Ensure ...	**Command:** net.exe accounts	● Passed

Figure 15

Threat Hunting:

Collects data for suspicious activities

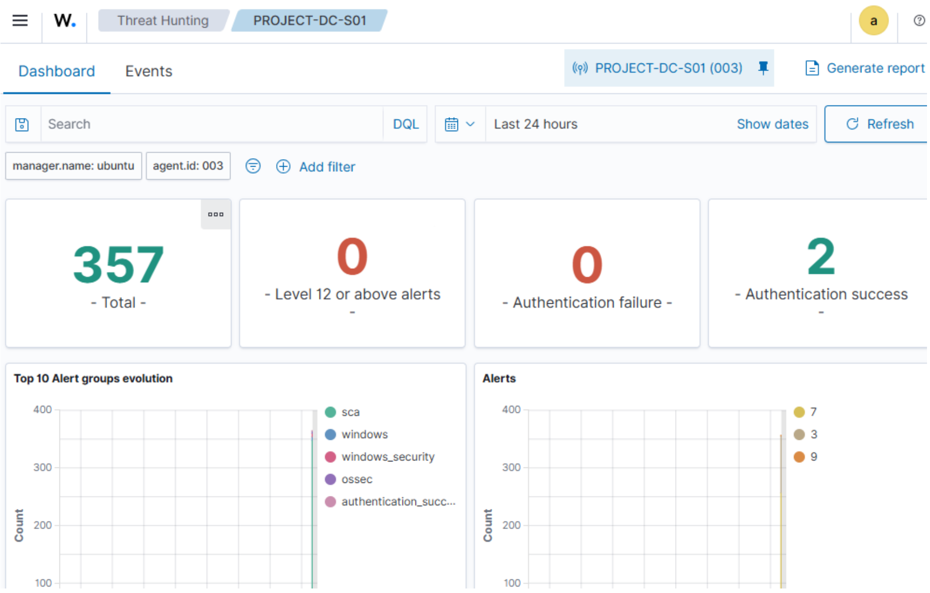


Figure 16

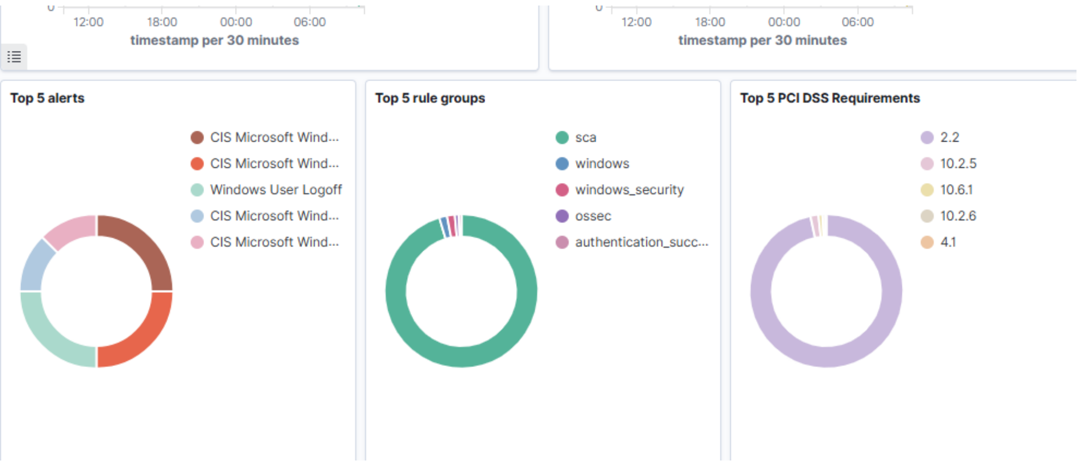
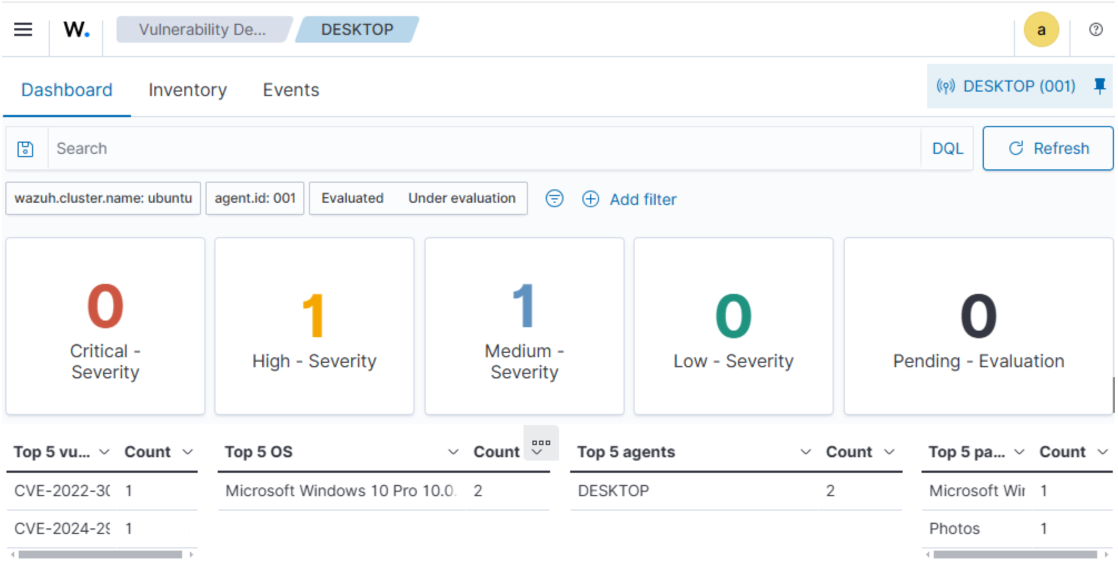


Figure 17

Vulnerability Assessment:

Identifies software and system vulnerabilities for remediation:



wazuh.cluster.name: ubuntu | agent.id: 001 | Evaluated | Under evaluation

0	1	1	0	0
Critical - Severity	High - Severity	Medium - Severity	Low - Severity	Pending - Evaluation

Top 5 vu...	Count
CVE-2022-3(	1
CVE-2024-2§	1

Top 5 OS	Count
Microsoft Windows 10 Pro 10.0.	2

Top 5 agents	Count
DESKTOP	2

Top 5 pa...	Count
Microsoft Wir	1
Photos	1

Figure18

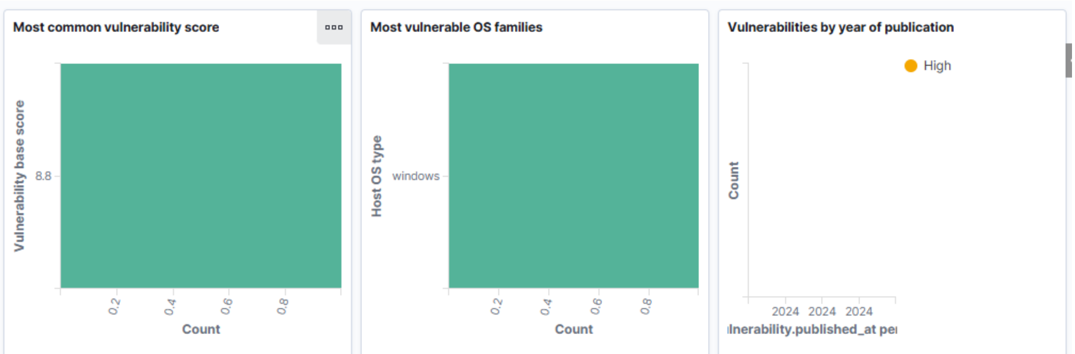


Figure 19

File Integrity Monitoring (FIM):

Tracks changes to critical system files to detect unauthorized modifications:

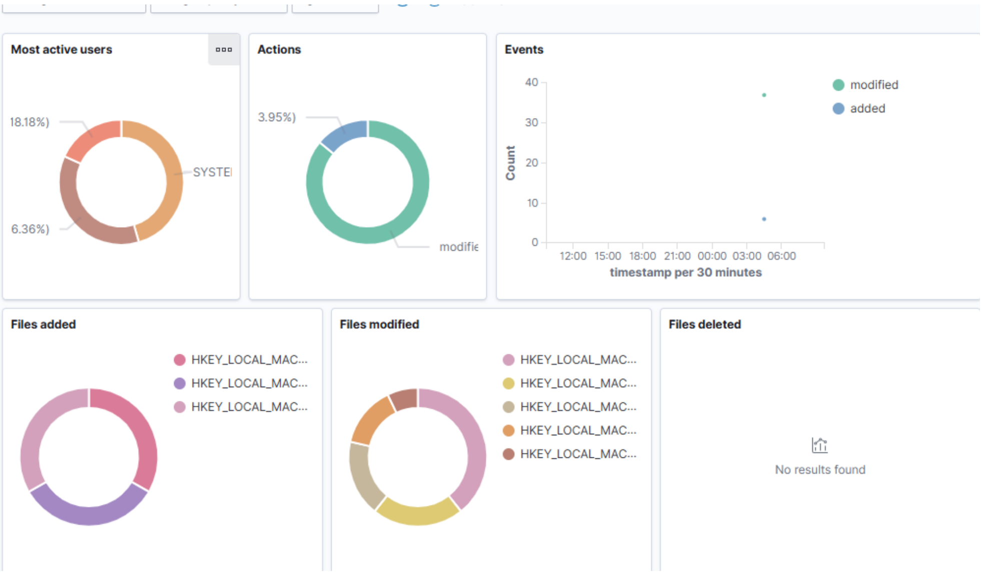


Figure 20

MITRE ATT&CK Framework:

Detects threats and MITRE techniques for a structured approach to threat mitigation:

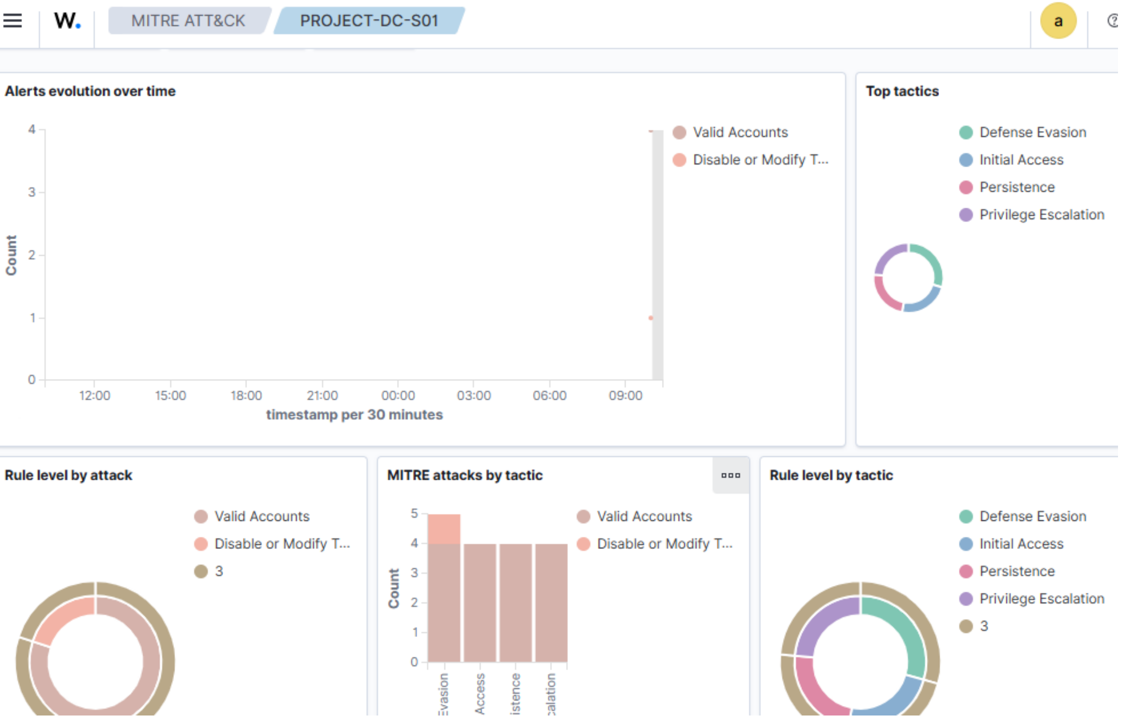
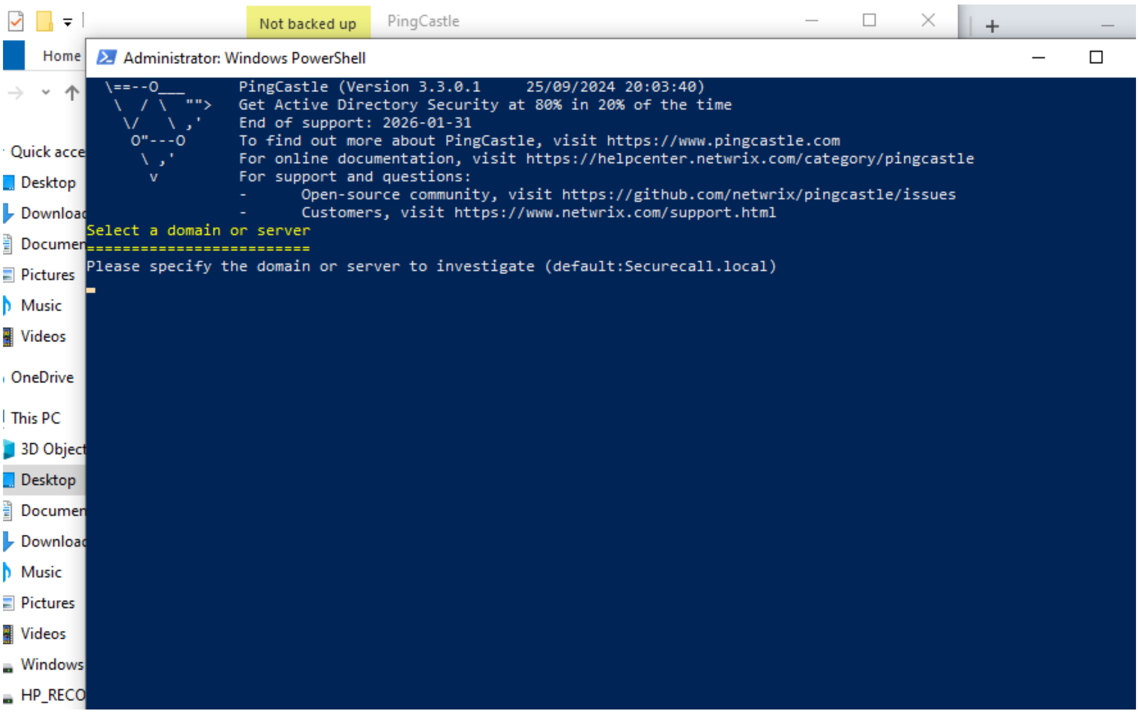


Figure 21

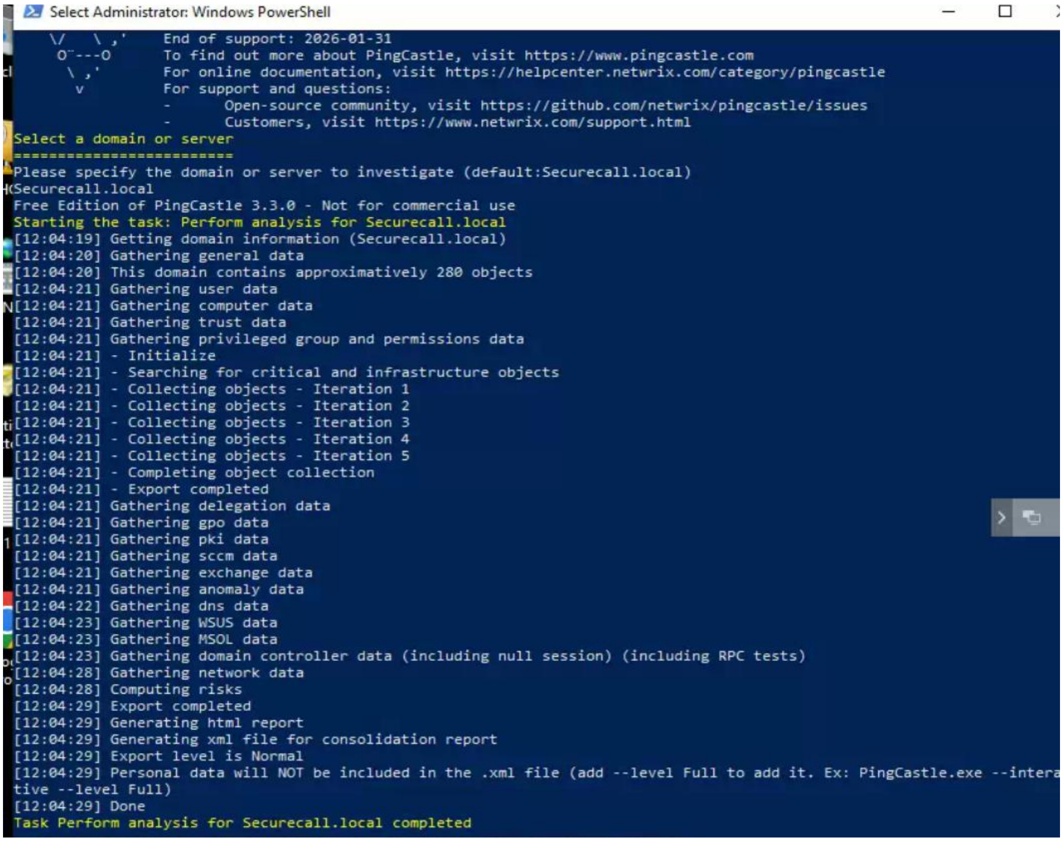
Ping Castle Integration

I installed PingCastle on the main server and I ran a script for investigating the main Domain Controller for checking the security of the Active Directory environment. (as shown on Figures 22 and 23):



```
 \==--O___      PingCastle (Version 3.3.0.1     25/09/2024 20:03:40)
  \  / \  "">   Get Active Directory Security at 80% in 20% of the time
   \/   \ ,'    End of support: 2026-01-31
    O"---O      To find out more about PingCastle, visit https://www.pingcastle.com
     \ ,'       For online documentation, visit https://helpcenter.netwrix.com/category/pingcastle
      v         For support and questions:
                -       Open-source community, visit https://github.com/netwrix/pingcastle/issues
                -       Customers, visit https://www.netwrix.com/support.html
Select a domain or server
=========================
Please specify the domain or server to investigate (default:Securecall.local)
```

Figure 22

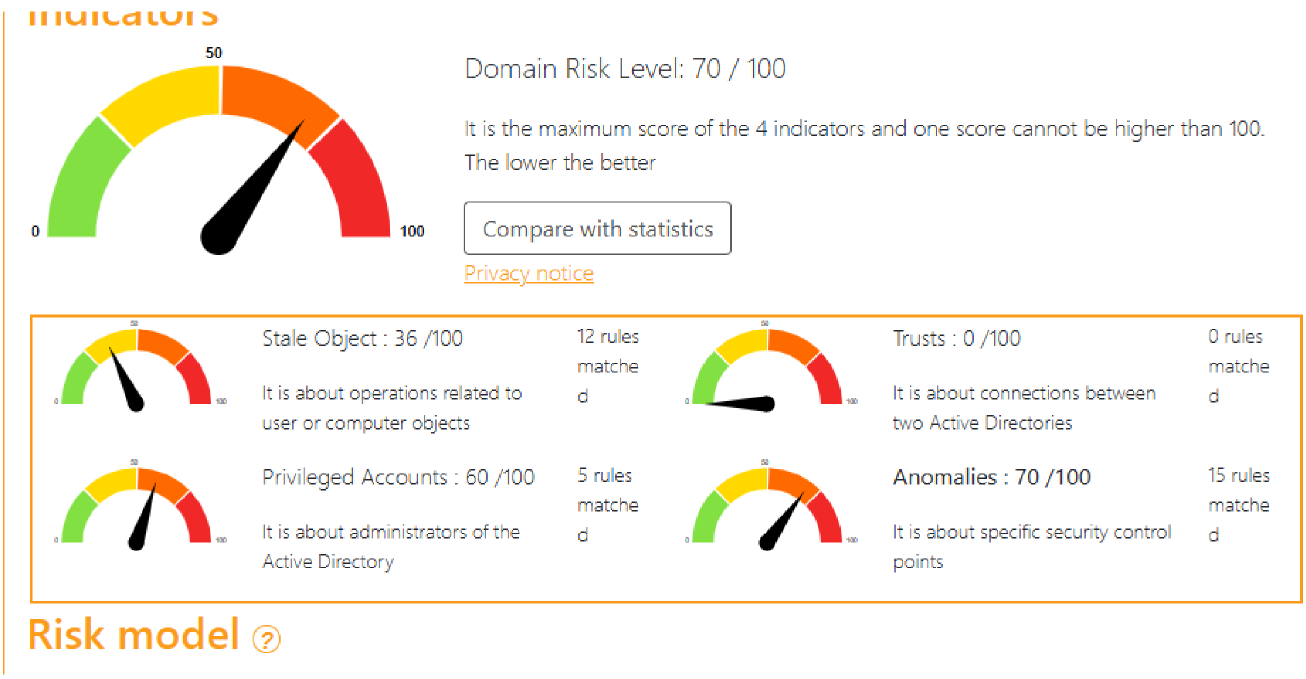


```
   \/   \ ,'    End of support: 2026-01-31
    O"---O      To find out more about PingCastle, visit https://www.pingcastle.com
     \ ,'       For online documentation, visit https://helpcenter.netwrix.com/category/pingcastle
      v         For support and questions:
                -       Open-source community, visit https://github.com/netwrix/pingcastle/issues
                -       Customers, visit https://www.netwrix.com/support.html
Select a domain or server
=========================
Please specify the domain or server to investigate (default:Securecall.local)
Securecall.local
Free Edition of PingCastle 3.3.0 - Not for commercial use
Starting the task: Perform analysis for Securecall.local
[12:04:19] Getting domain information (Securecall.local)
[12:04:20] Gathering general data
[12:04:20] This domain contains approximatively 280 objects
[12:04:21] Gathering user data
[12:04:21] Gathering computer data
[12:04:21] Gathering trust data
[12:04:21] Gathering privileged group and permissions data
[12:04:21] - Initialize
[12:04:21] - Searching for critical and infrastructure objects
[12:04:21] - Collecting objects - Iteration 1
[12:04:21] - Collecting objects - Iteration 2
[12:04:21] - Collecting objects - Iteration 3
[12:04:21] - Collecting objects - Iteration 4
[12:04:21] - Collecting objects - Iteration 5
[12:04:21] - Completing object collection
[12:04:21] - Export completed
[12:04:21] Gathering delegation data
[12:04:21] Gathering gpo data
[12:04:21] Gathering pki data
[12:04:21] Gathering sccm data
[12:04:21] Gathering exchange data
[12:04:21] Gathering anomaly data
[12:04:22] Gathering dns data
[12:04:23] Gathering WSUS data
[12:04:23] Gathering MSOL data
[12:04:23] Gathering domain controller data (including null session) (including RPC tests)
[12:04:28] Gathering network data
[12:04:28] Computing risks
[12:04:29] Export completed
[12:04:29] Generating html report
[12:04:29] Generating xml file for consolidation report
[12:04:29] Export level is Normal
[12:04:29] Personal data will NOT be included in the .xml file (add --level Full to add it. Ex: PingCastle.exe --intera
tive --level Full)
[12:04:29] Done
Task Perform analysis for Securecall.local completed
```

Figure 23

Once the scan was complete, I opened the generated HTML report to review the findings.

The analysis provided a detailed breakdown of potentials vulnerabilities and security issues within the environment like weak passwords policies, outdated configurations , and areas lacking proper security controls (as shown in Figures 24 and 25):



Domain Risk Level: 70 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Compare with statistics

Privacy notice

Stale Object : 36 /100 — It is about operations related to user or computer objects — 12 rules matched

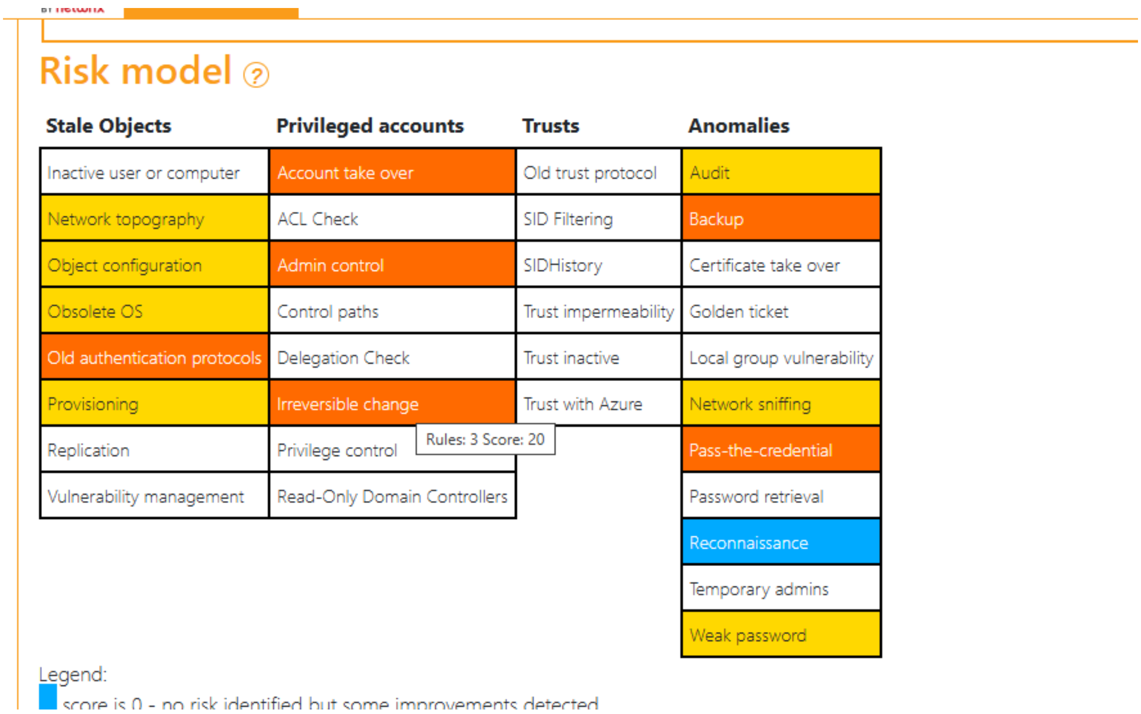
Trusts : 0 /100 — It is about connections between two Active Directories — 0 rules matched

Privileged Accounts : 60 /100 — It is about administrators of the Active Directory — 5 rules matched

Anomalies : 70 /100 — It is about specific security control points — 15 rules matched

Risk model ?

Figure 24



Risk model ?

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

Rules: 3 Score: 20

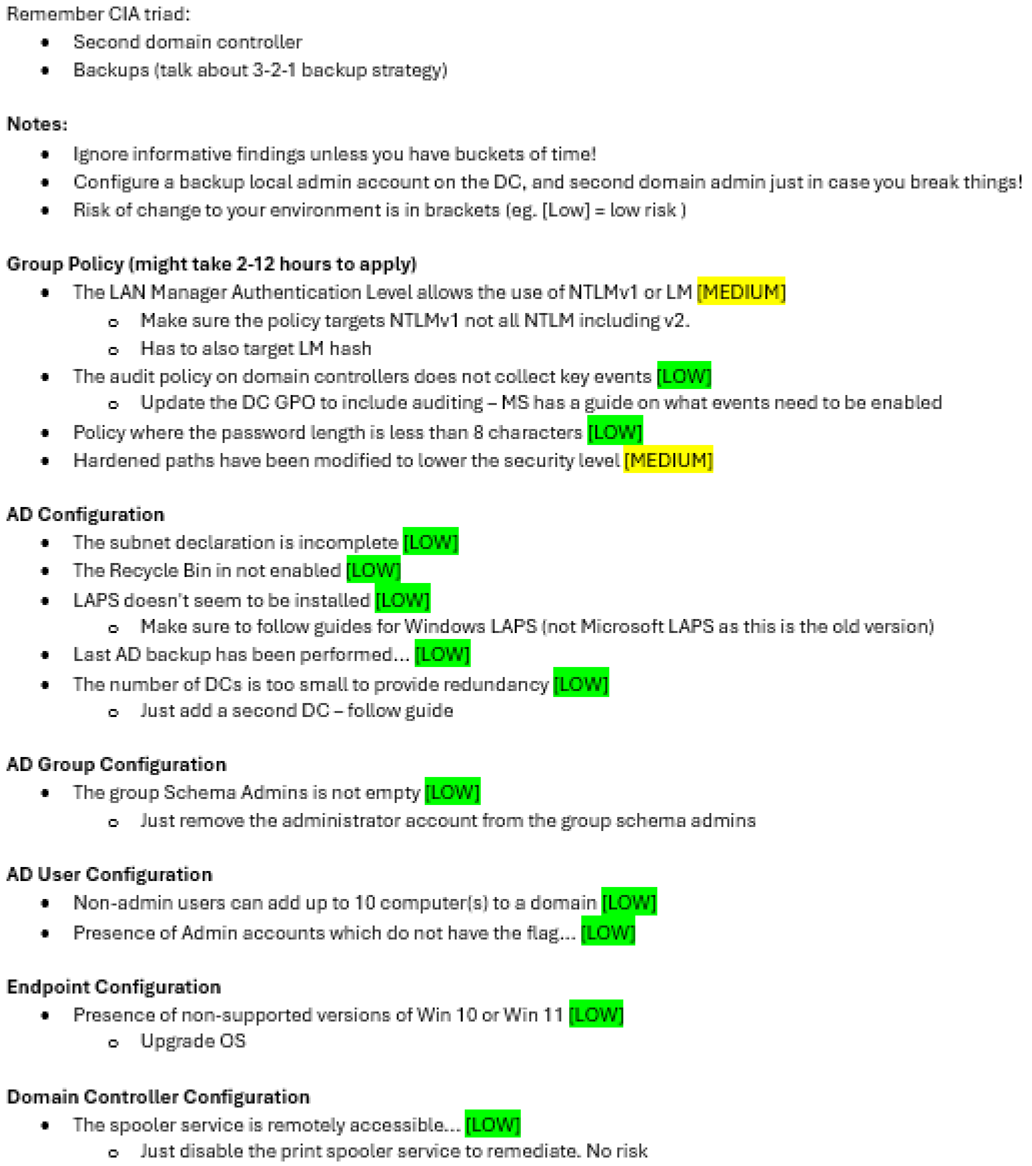
Legend:

🟦 score is 0 - no risk identified but some improvements detected

Figure 25

After going through the results, I identified several issues that needed to be addressed to improve the overall security. These issues require immediate attention, including improving password policies and updating certain configuration to ensure the rain with more secure and align with the best practises

I made a plan of action how I can do to start remediation and below can be seen the steps:



Remember CIA triad:

- Second domain controller
- Backups (talk about 3-2-1 backup strategy)

Notes:

- Ignore informative findings unless you have buckets of time!
- Configure a backup local admin account on the DC, and second domain admin just in case you break things!
- Risk of change to your environment is in brackets (eg. [Low] = low risk)

Group Policy (might take 2-12 hours to apply)

- The LAN Manager Authentication Level allows the use of NTLMv1 or LM [MEDIUM]
  - Make sure the policy targets NTLMv1 not all NTLM including v2.
  - Has to also target LM hash
- The audit policy on domain controllers does not collect key events [LOW]
  - Update the DC GPO to include auditing – MS has a guide on what events need to be enabled
- Policy where the password length is less than 8 characters [LOW]
- Hardened paths have been modified to lower the security level [MEDIUM]

AD Configuration

- The subnet declaration is incomplete [LOW]
- The Recycle Bin in not enabled [LOW]
- LAPS doesn't seem to be installed [LOW]
  - Make sure to follow guides for Windows LAPS (not Microsoft LAPS as this is the old version)
- Last AD backup has been performed… [LOW]
- The number of DCs is too small to provide redundancy [LOW]
  - Just add a second DC – follow guide

AD Group Configuration

- The group Schema Admins is not empty [LOW]
  - Just remove the administrator account from the group schema admins

AD User Configuration

- Non-admin users can add up to 10 computer(s) to a domain [LOW]
- Presence of Admin accounts which do not have the flag… [LOW]

Endpoint Configuration

- Presence of non-supported versions of Win 10 or Win 11 [LOW]
  - Upgrade OS

Domain Controller Configuration

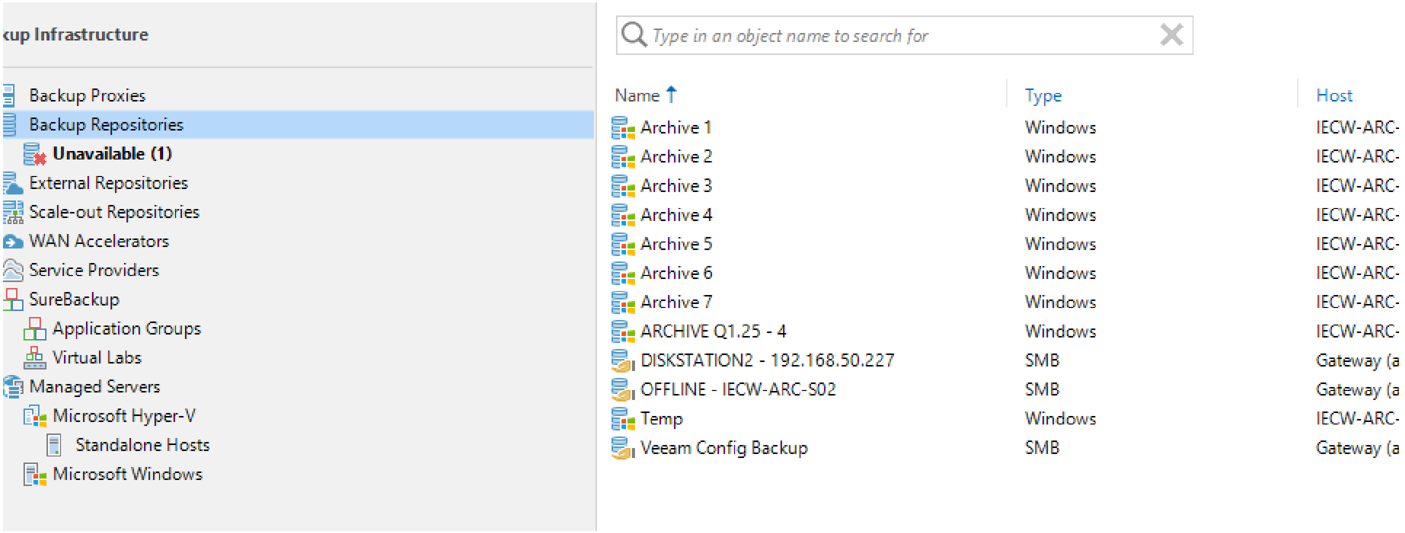
- The spooler service is remotely accessible… [LOW]
  - Just disable the print spooler service to remediate. No risk

Figure 26

Implemented Best Practices

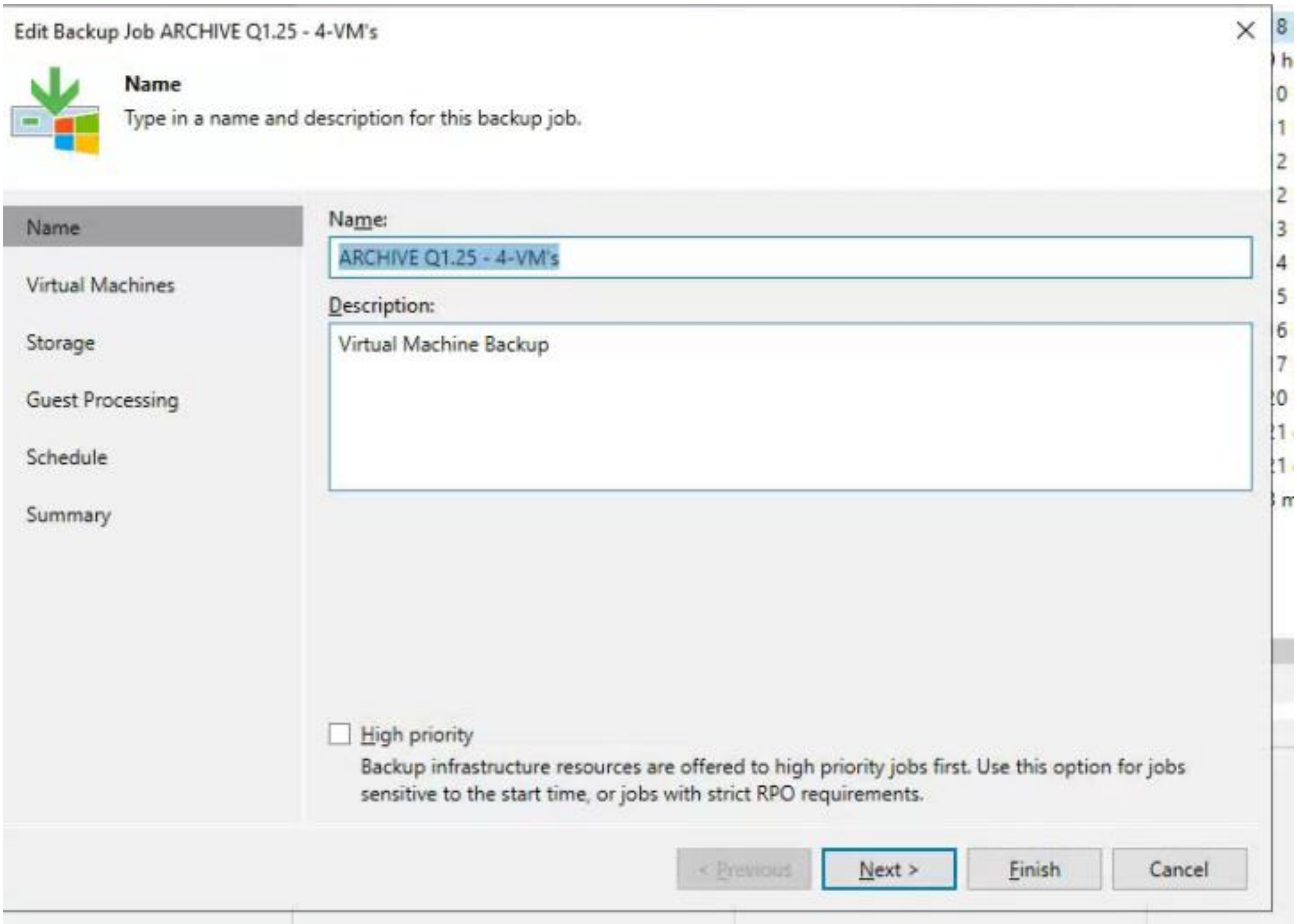
Backup Images on an external Hard Drive:

I used Veeam to do the backup internal and on external drives. The internal backups were set for running the backups daily and for external backups I choose to do them on external hard drives every month. To do this I had to create repositories and then do the backups and save them to drives that was called ARCHIVE (as shown in Figure 9,10,11, and 12) These external drives were stored in a vault just in case of a disaster (12, 2024).



Name ↑	Type	Host
Archive 1	Windows	IECW-ARC-
Archive 2	Windows	IECW-ARC-
Archive 3	Windows	IECW-ARC-
Archive 4	Windows	IECW-ARC-
Archive 5	Windows	IECW-ARC-
Archive 6	Windows	IECW-ARC-
Archive 7	Windows	IECW-ARC-
ARCHIVE Q1.25 - 4	Windows	IECW-ARC-
DISKSTATION2 - 192.168.50.227	SMB	Gateway (a
OFFLINE - IECW-ARC-S02	SMB	Gateway (a
Temp	Windows	IECW-ARC-
Veeam Config Backup	SMB	Gateway (a

Figure 9



Edit Backup Job ARCHIVE Q1.25 - 4-VM's

Name

Type in a name and description for this backup job.

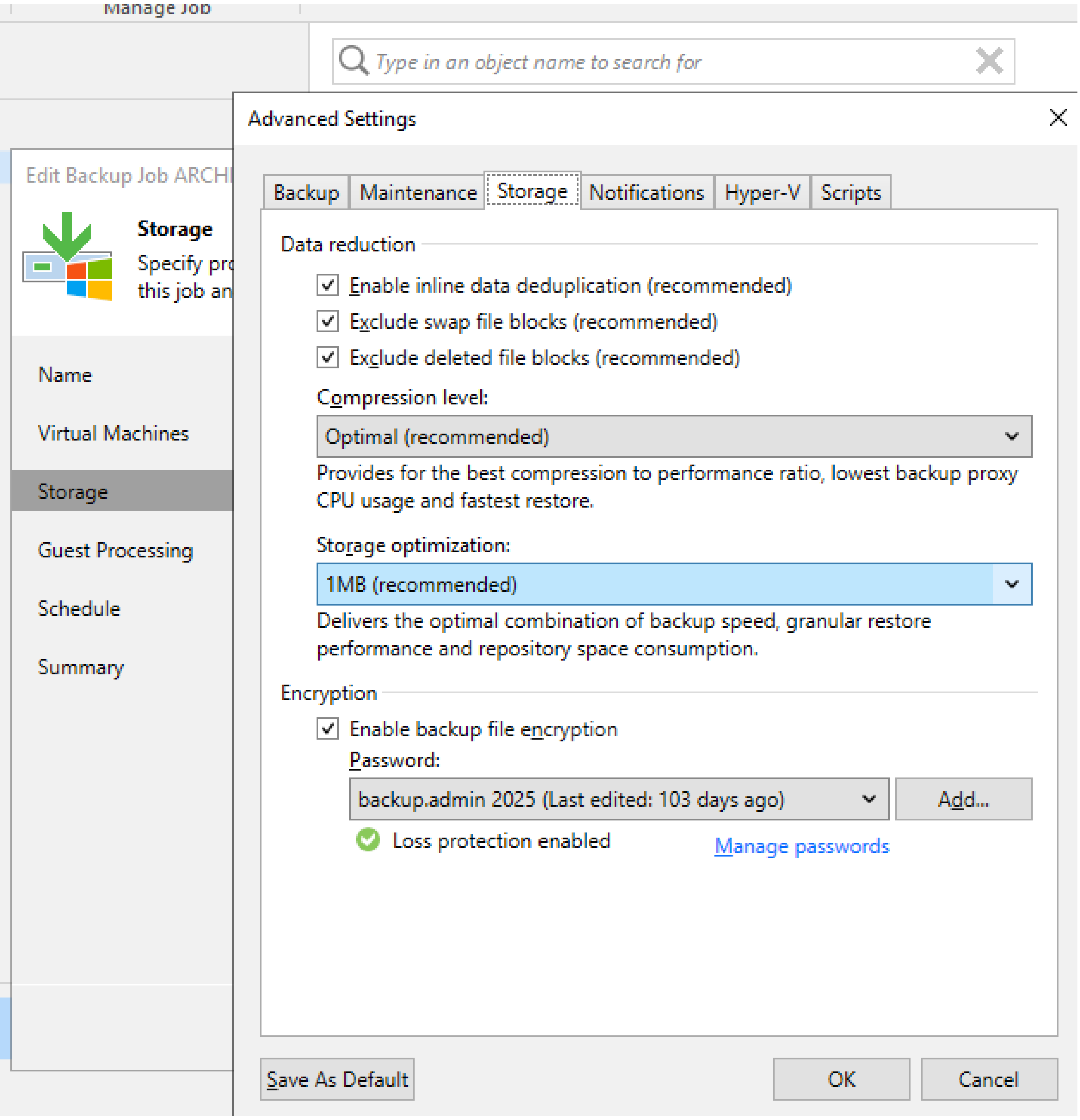
Name: ARCHIVE Q1.25 - 4-VM's

Description: Virtual Machine Backup

□ High priority

Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

Figure 10



Data reduction

☑ Enable inline data deduplication (recommended)

☑ Exclude swap file blocks (recommended)

☑ Exclude deleted file blocks (recommended)

Compression level: Optimal (recommended)

Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.

Storage optimization: 1MB (recommended)

Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.

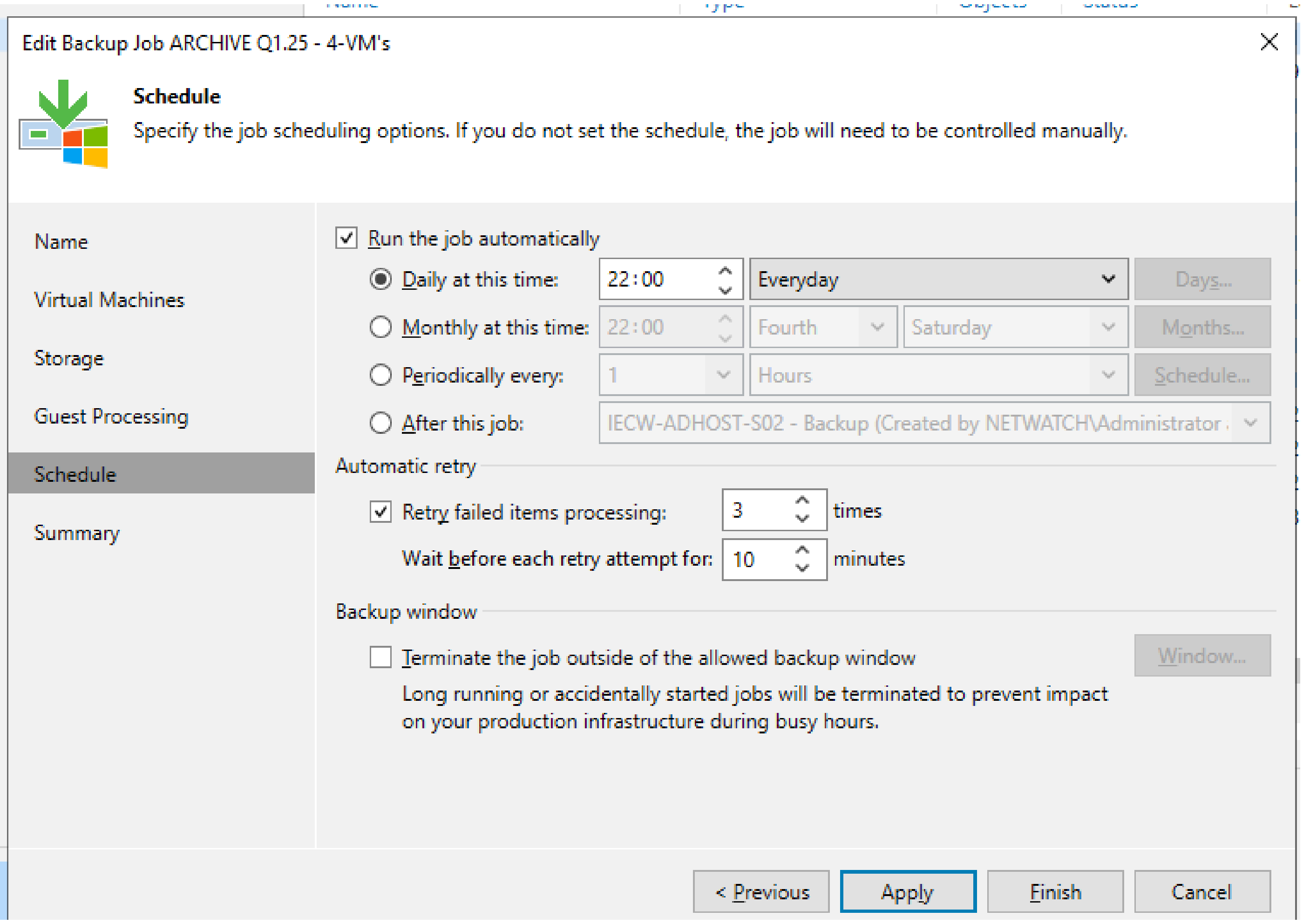
Encryption

☑ Enable backup file encryption

Password: backup.admin 2025 (Last edited: 103 days ago)

✓ Loss protection enabled

Figure 11



Edit Backup Job ARCHIVE Q1.25 - 4-VM's

Schedule

Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

● Daily at this time: 22 : 00 Everyday

○ Monthly at this time: 22 : 00 Fourth Saturday

○ Periodically every: 1 Hours

○ After this job: IECW-ADHOST-S02 - Backup (Created by NETWATCH\Administrator .

Automatic retry

☑ Retry failed items processing: 3 times

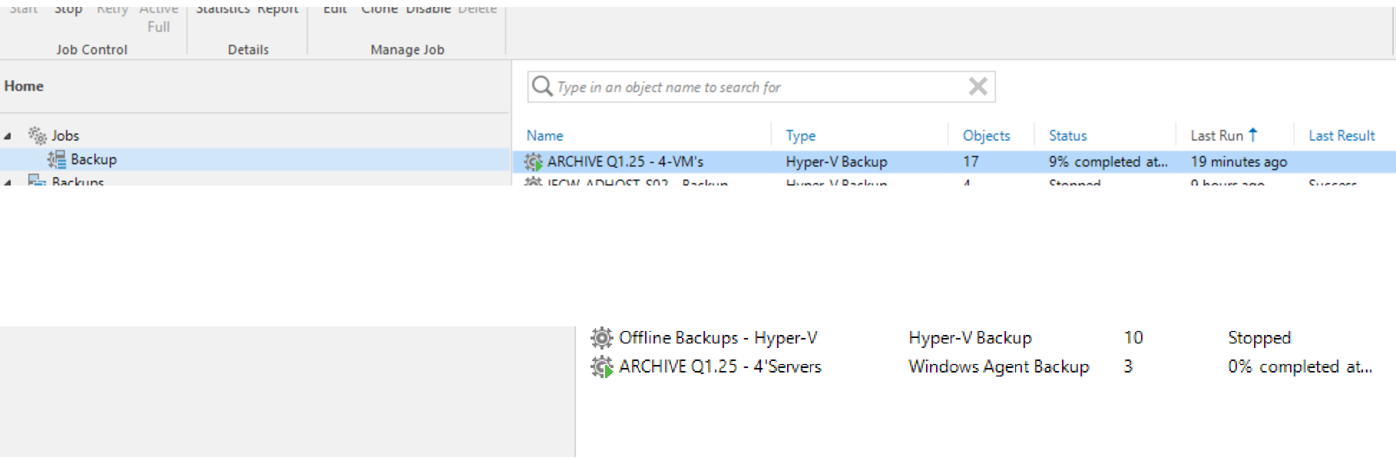
Wait before each retry attempt for: 10 minutes

Backup window

□ Terminate the job outside of the allowed backup window

Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

Figure 12



Name	Type	Objects	Status	Last Run	Last Result
ARCHIVE Q1.25 - 4-VM's	Hyper-V Backup	17	9% completed at...	19 minutes ago	
IECW-ADHOST-S02 - Backup	Hyper-V Backup	4	Stopped	9 hours ago	Success
Offline Backups - Hyper-V	Hyper-V Backup	10	Stopped		
ARCHIVE Q1.25 - 4'Servers	Windows Agent Backup	3	0% completed at...		

Figure 13

Hardening Systems:

Applied configurations based on recommendations from PingCastle, Wazuh and NinjaOne . This included improving group policies, securing passwords, and restricting administrative privileges.

Asset Management:

Achieved centralized tracking of assets through Wazuh for improved oversight.

Comparison Table: Before and After

I made a table to compare the system how it looks without any security implementation and how it would look like after implementing best practicing for monitoring and detecting risks and gaps, and what tools will help me doing this:

Feature	Before	Risk	After
EDR (Endpoint Detection)	None	Devices unprotected	Wazuh
Configuration Assessment	None	Misconfigurations undetected	Wazuh
Vulnerability Assessments	None	Vulnerabilities unresolved	Wazuh
SIEM	None	Lack of centralized monitoring	Wazuh
File Integrity Monitoring	None	Unauthorized file changes undetected	Wazuh
Threat Hunting	None	Inability to proactively detect threats	Wazuh
Log Collection	None	No centralized log storage	Wazuh
Hardening Best Practices	None	Devices not hardened so risk of compromise	Configurations using recommendations from Pingcastle, Bloodhound, Wazuh

Feature	Before	Risk	After
Asset Management	None	Limited visibility into devices	Wazuh
DC Replication	Single DC	Single point of failure	Planned for next phase
Backups	No backups	No restore opportunities	Backup plans underway

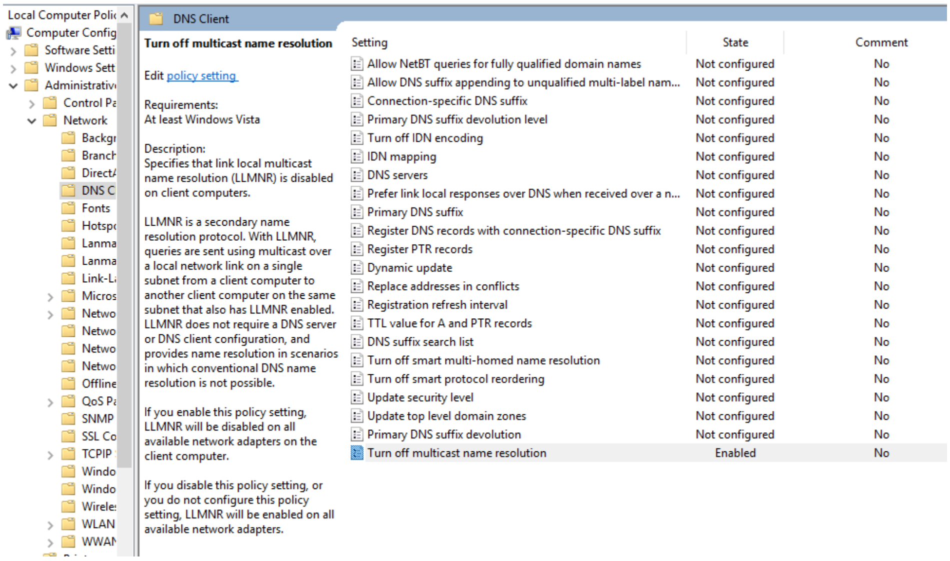
Improvements:

GPO Settup :

Disable LLMNR

Why disable LLMNR?

To protect if a Man-in-the-middle attacker gets between the client and the file server. If the attacker receives the LLMNR response, then the Windows service disclose the user’s credential hash to an untrusted third party. A smart attacker can relay on that hash to the file server and the network never think anything is wrong. In most cases LLMNR protocol is no longer need because DNS has taken over (Bradley, 2019).



Turn off multicast name resolution

Edit policy setting

Requirements:
At least Windows Vista

Description:
Specifies that link local multicast name resolution (LLMNR) is disabled on client computers.

LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in scenarios in which conventional DNS name resolution is not possible.

If you enable this policy setting, LLMNR will be disabled on all available network adapters on the client computer.

If you disable this policy setting, or you do not configure this policy setting, LLMNR will be enabled on all available network adapters.

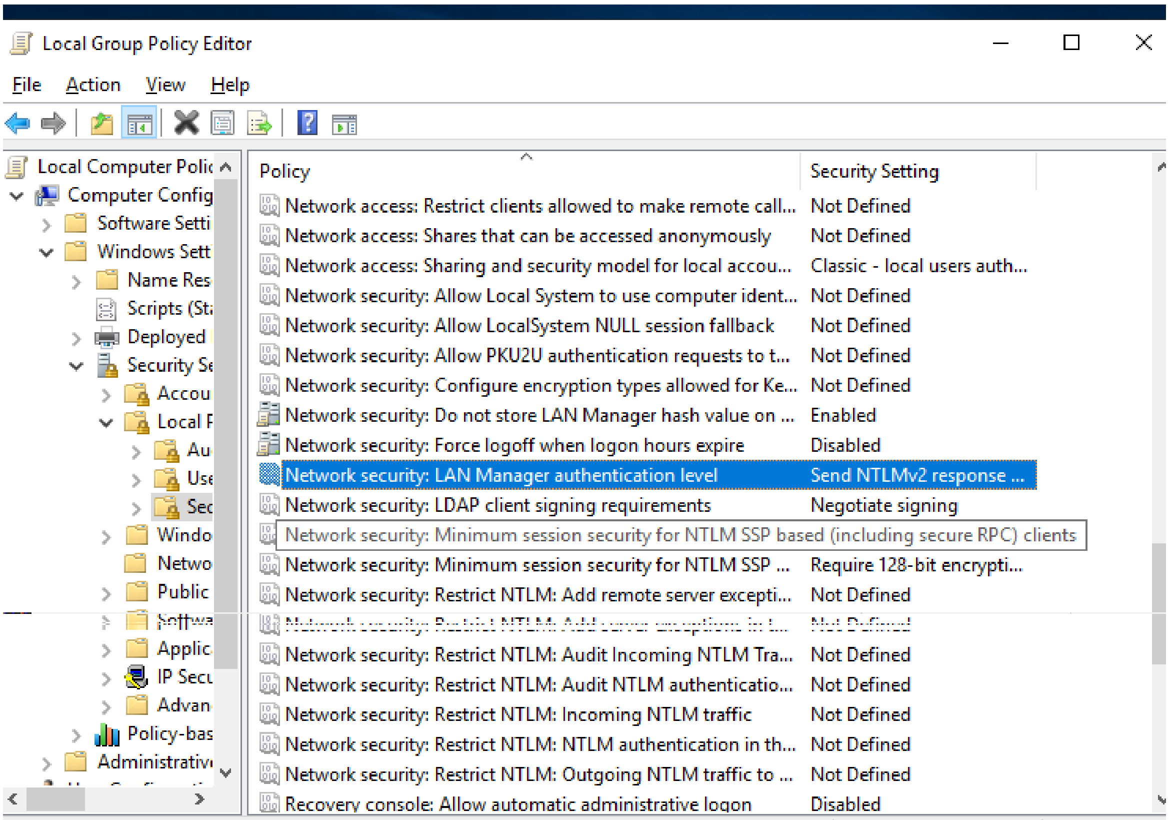
Setting	State	Comment
Allow NetBT queries for fully qualified domain names	Not configured	No
Allow DNS suffix appending to unqualified multi-label nam...	Not configured	No
Connection-specific DNS suffix	Not configured	No
Primary DNS suffix devolution level	Not configured	No
Turn off IDN encoding	Not configured	No
IDN mapping	Not configured	No
DNS servers	Not configured	No
Prefer link local responses over DNS when received over a n...	Not configured	No
Primary DNS suffix	Not configured	No
Register DNS records with connection-specific DNS suffix	Not configured	No
Register PTR records	Not configured	No
Dynamic update	Not configured	No
Replace addresses in conflicts	Not configured	No
Registration refresh interval	Not configured	No
TTL value for A and PTR records	Not configured	No
DNS suffix search list	Not configured	No
Turn off smart multi-homed name resolution	Not configured	No
Turn off smart protocol reordering	Not configured	No
Update security level	Not configured	No
Update top level domain zones	Not configured	No
Primary DNS suffix devolution	Not configured	No
Turn off multicast name resolution	Enabled	No

Figure 27

Disable NTLMv1

Why Disable NTLMv1?

NTLMV1 hashes can be intercepted and used for authentication relay attacks or even dictionary attacks, granting attackers unauthorized access to sensitive systems. New NTLM vulnerabilities have been disclosed over the last few years (Segal, 2025).



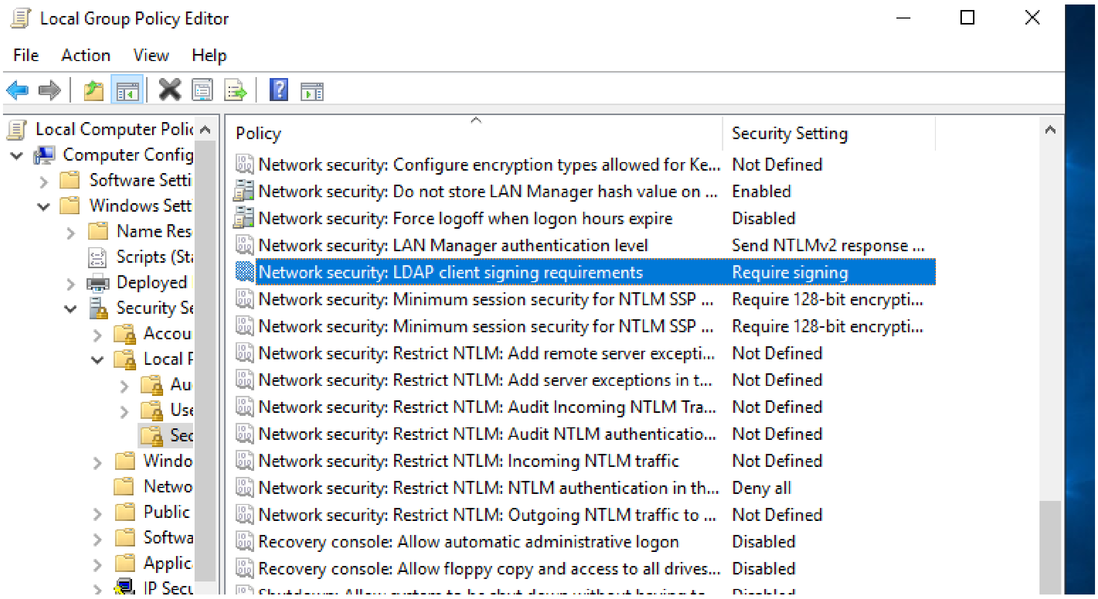
Policy	Security Setting
Network access: Restrict clients allowed to make remote call...	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accou...	Classic - local users auth...
Network security: Allow Local System to use computer ident...	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to t...	Not Defined
Network security: Configure encryption types allowed for Ke...	Not Defined
Network security: Do not store LAN Manager hash value on ...	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Send NTLMv2 response ...
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server excepti...	Not Defined
Network security: Restrict NTLM: Add server exceptions in t...	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Tra...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in th...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to ...	Not Defined
Recovery console: Allow automatic administrative logon	Disabled

Figure 29

Enforce LDAP Signing

Why?

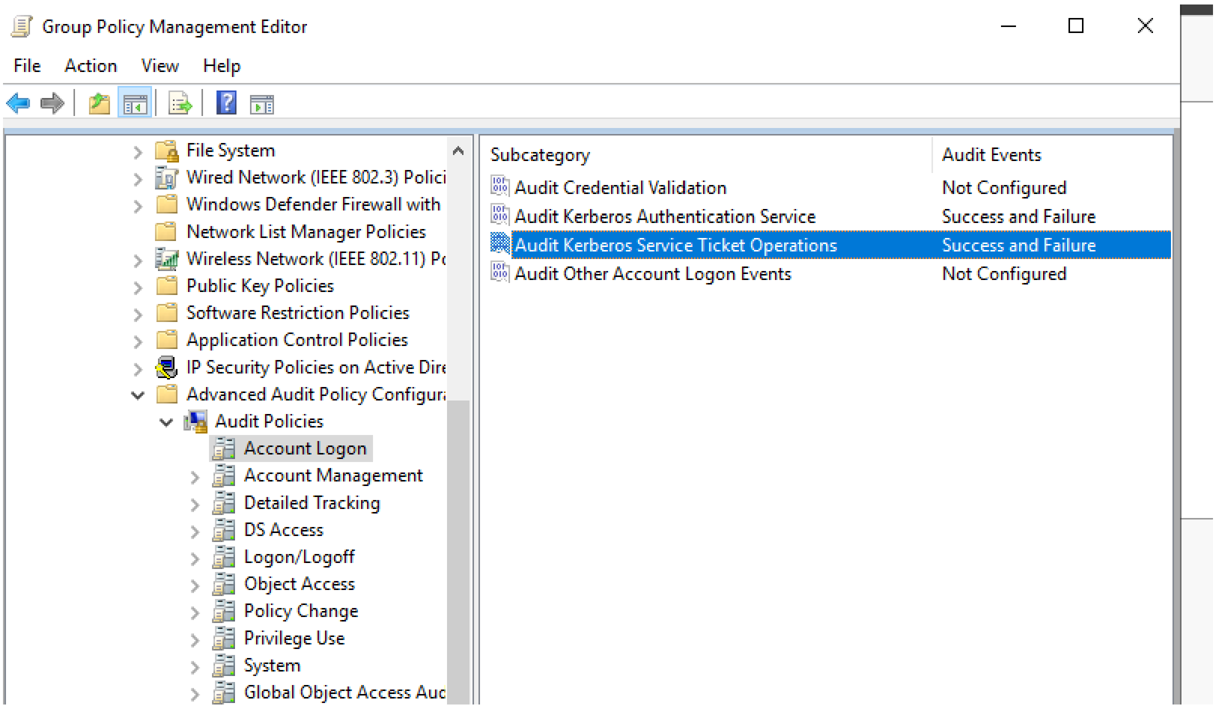
LDAP signing ensures that LDAP communication between clients and servers is secure, preventing Man-in-the-middle attacks. Enabling this will prevent against this kind of attacks (Server, 2025)



Policy	Security Setting
Network security: Configure encryption types allowed for Ke...	Not Defined
Network security: Do not store LAN Manager hash value on ...	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Send NTLMv2 response ...
Network security: LDAP client signing requirements	Require signing
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server excepti...	Not Defined
Network security: Restrict NTLM: Add server exceptions in t...	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Tra...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in th...	Deny all
Network security: Restrict NTLM: Outgoing NTLM traffic to ...	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives...	Disabled
Shutdown: Allow system to be shut down without having to ...	Disabled

Figure 30

Enable Kerberos Auditing via Group Policy


Group Policy Management Editor
File
Action
View
Help
File System
Wired Network (IEEE 802.3) Polici
Windows Defender Firewall with
Network List Manager Policies
Wireless Network (IEEE 802.11) Po
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Dire
Advanced Audit Policy Configura
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auc

Subcategory	Audit Events
Audit Credential Validation	Not Configured
Audit Kerberos Authentication Service	Success and Failure
Audit Kerberos Service Ticket Operations	Success and Failure
Audit Other Account Logon Events	Not Configured

Figure 31

System Audit Policy Configuration

I set Up Audit Policy to log both successful and failed security events across key areas. This includes system events, logon/logoff activity, file and registry access, privileged actions, process tracking, policy changes, and account management. It also covers Active Directory changes and account logon events like Kerberos. I verified the setup using the **auditpol /get /category:*** command to ensure everything is correctly configured.

Password Policy Configuration

I configured the Password Policy to enhance password security and enforce stronger password protection.

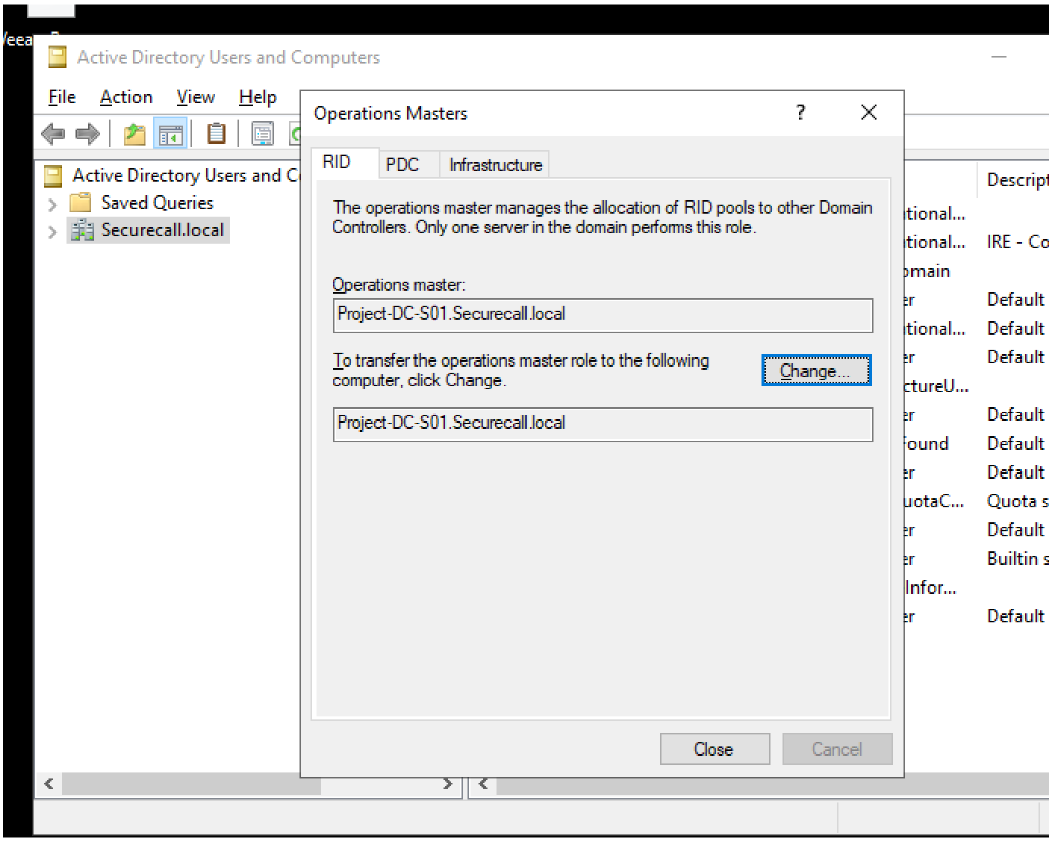
The settings were modified as follows:

I updated the password and account lockout settings to improve security. The minimum password length was increased from 7 to 11 characters to make passwords stronger. The maximum password age remains at 42 days, meaning users change their password every 42 days. The minimum age is still 1 day, so users can change their password right after setting a new one. To prevent password reuse, the system remembers the last 24 passwords. The account lockout threshold is set to “Never” so accounts won’t lock after failed login attempts. However, if a lockout does happen, the account will stay locked for 30 minutes. The system also tracks failed login attempts for 30 minutes before resetting the counter.

Steps to Add a Secondary Domain Controller:

I have setup two domain controllers in different regions, with the first domain controller located in Carlow, which serves as the primary controller with DNS, DHCP, and Active Directory setup. The second domain controller is in Dublin, acting as backup in case of issues like a power outage in Carlow. Although my project is based in Carlow, and I can’t physically manage both locations. I can demonstrate that this setup works. In a real-life scenario, to make this functional, a VPN tunnel would need to be established between both sites. This would allow the Dublin domain controller to take over the operation masters role if necessary, ensuring continuity of services even if the Carlow site experiences downtime. This setup offers a practical solution for improving reliability and availability in distributed environments.

Here I have the Carlow main domain controller running as master:



The operations master manages the allocation of RID pools to other Domain Controllers. Only one server in the domain performs this role.

Operations master:

Project-DC-S01.Securecall.local

To transfer the operations master role to the following computer, click Change.

Project-DC-S01.Securecall.local

Figure 32

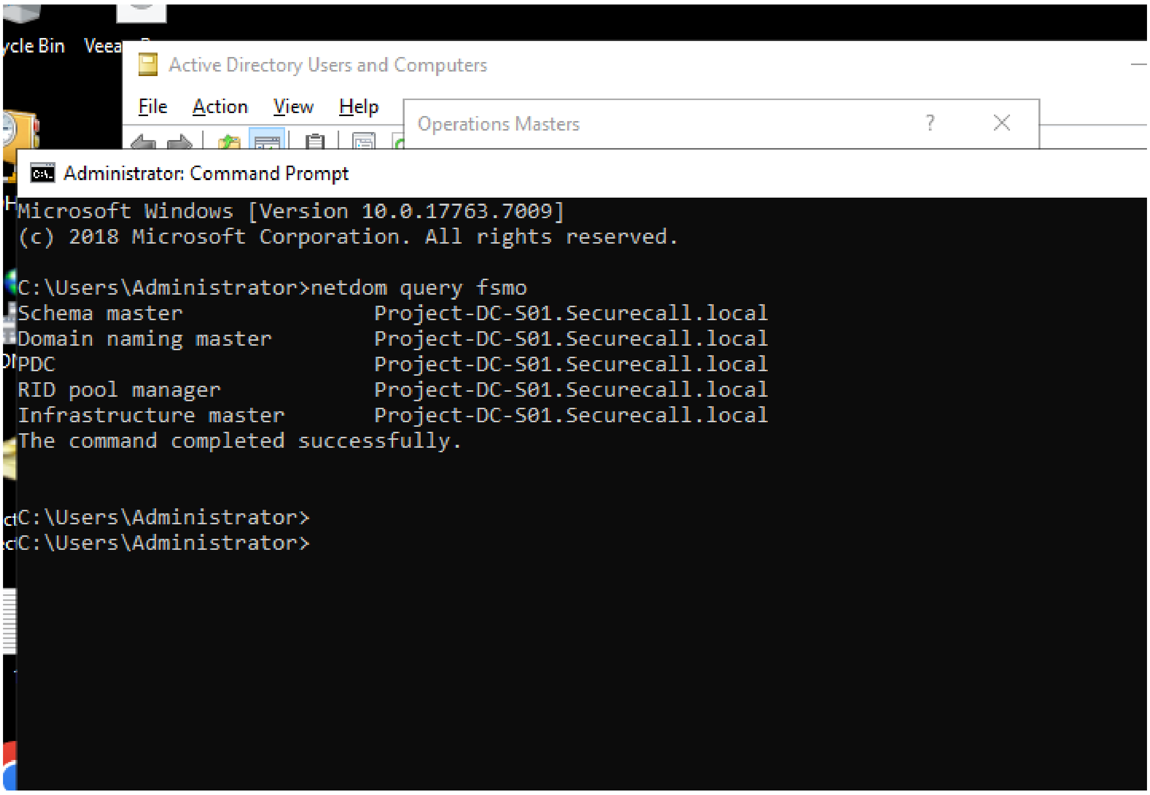
By running **netdom query fsmo** command we can see the details:

This will return the domain controllers that hold the FSMO roles. It will list the following roles:

- Schema Master
- Domain Naming Master
- PDC Emulator

- RID Master

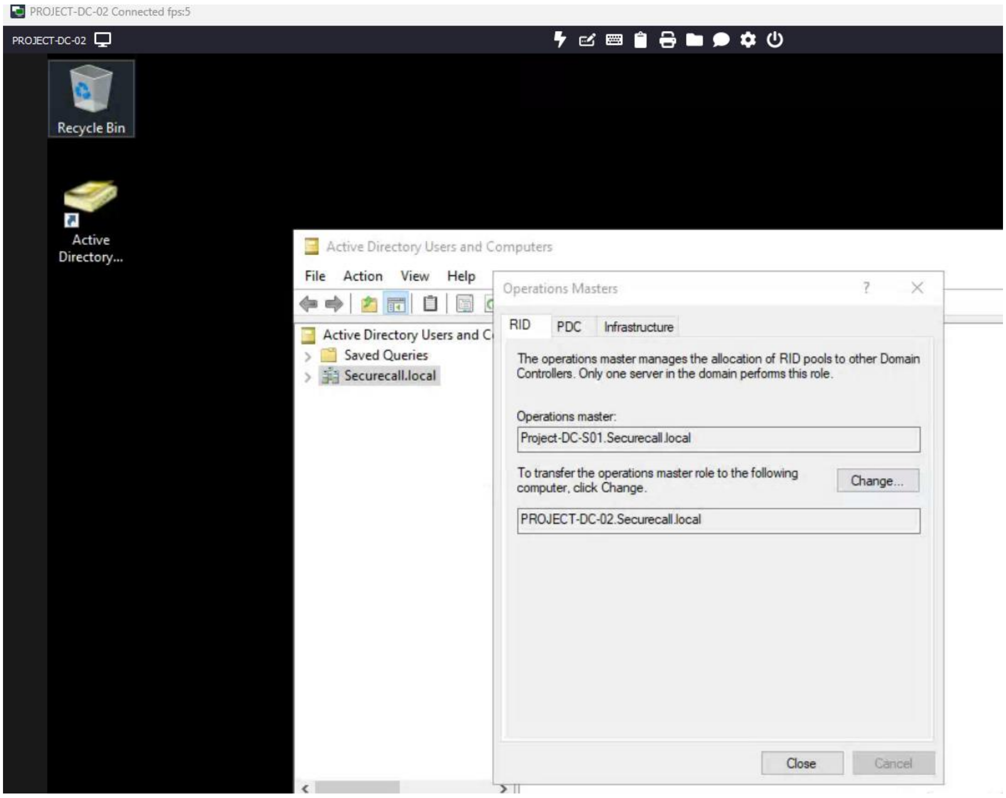
- Infrastructure Master


cle Bin
Veea
Active Directory Users and Computers
File
Action
View
Help
Operations Masters
Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.7009]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netdom query fsmo
Schema master               Project-DC-S01.Securecall.local
Domain naming master        Project-DC-S01.Securecall.local
PDC                         Project-DC-S01.Securecall.local
RID pool manager            Project-DC-S01.Securecall.local
Infrastructure master       Project-DC-S01.Securecall.local
The command completed successfully.


C:\Users\Administrator>
C:\Users\Administrator>
```

Figure 33

In this situation the master's is Carlow Domain Controller. Then we connect to the second domain, and we switch the master's to second domain controller. By pressing Change will change the masters operation and (shown in Figure bellow)



The operations master manages the allocation of RID pools to other Domain Controllers. Only one server in the domain performs this role.

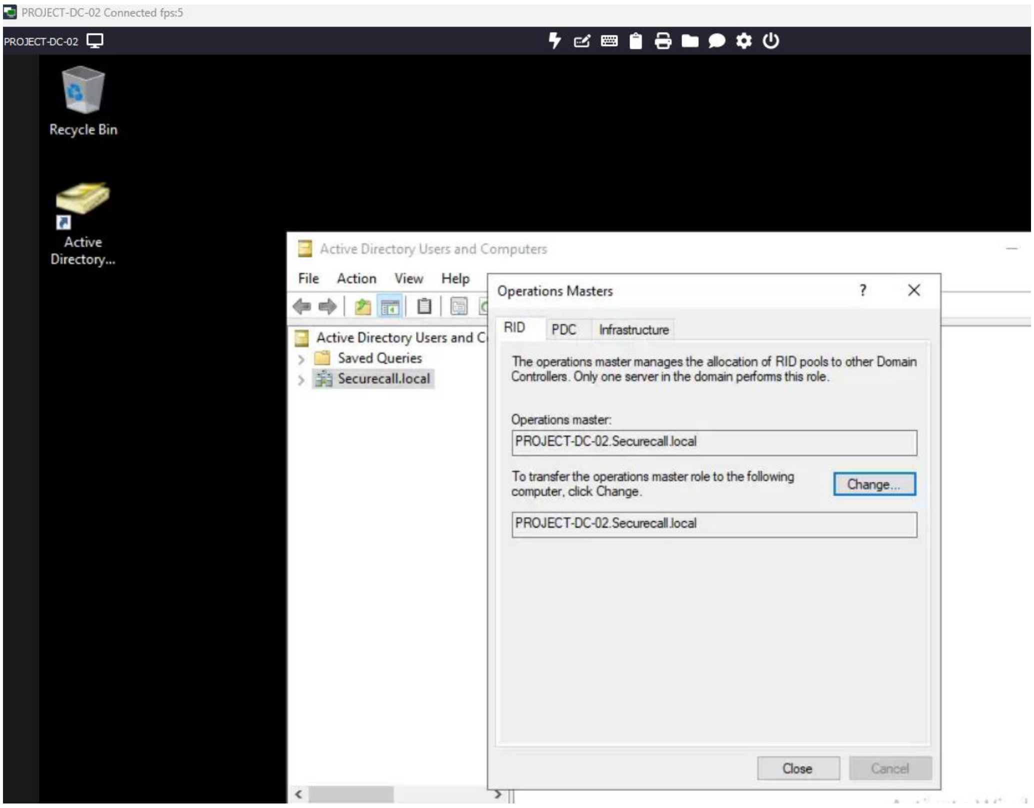
Operations master:

Project-DC-S01.Securecall.local

To transfer the operations master role to the following computer, click Change. Change...

PROJECT-DC-02.Securecall.local

And then the Second Domain controller takes control by being the masters:



The operations master manages the allocation of RID pools to other Domain Controllers. Only one server in the domain performs this role.

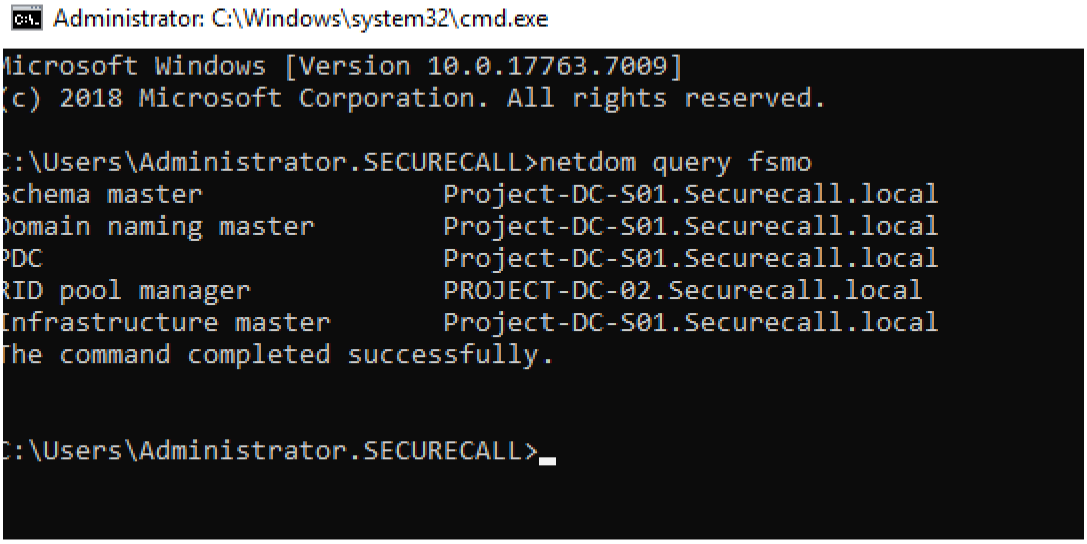
Operations master:

PROJECT-DC-02.Securecall.local

To transfer the operations master role to the following computer, click Change.

PROJECT-DC-02.Securecall.local

But it will only be master's on RID pool manager which will allow the functionality for the moment:



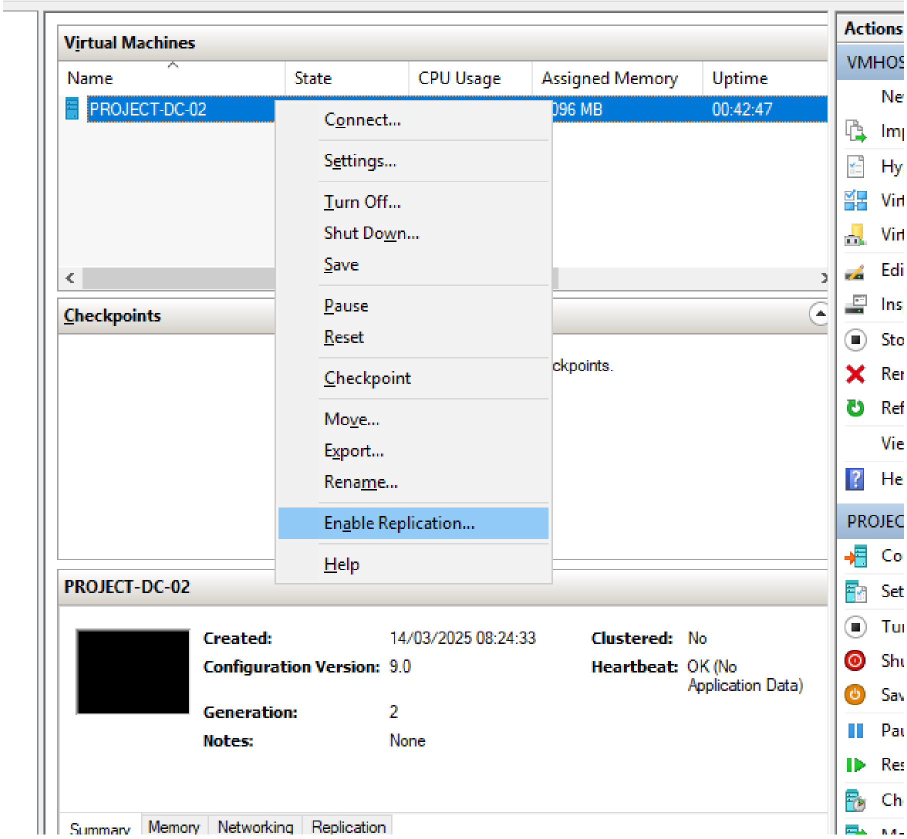
```
Microsoft Windows [Version 10.0.17763.7009]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.SECURECALL>netdom query fsmo
Schema master               Project-DC-S01.Securecall.local
Domain naming master        Project-DC-S01.Securecall.local
PDC                         Project-DC-S01.Securecall.local
RID pool manager            PROJECT-DC-02.Securecall.local
Infrastructure master       Project-DC-S01.Securecall.local
The command completed successfully.


C:\Users\Administrator.SECURECALL>_
```

Creating VM replication for Domain Controller:

The replica is specifically set up for the Dublin domain controller to replicate the Active Directory, DNS, and other critical services from the primary domain controller in Carlow. This setup ensures that the Dublin domain controller has an up-to-date copy of all necessary information, providing redundancy and backup in case of failure. However, the replication is configured only for the Dublin domain controller, meaning it can replicate data from Carlow but is not automatically taking over roles or services unless manually promoted. If the Carlow domain controller experiences an issue, the Dublin domain controller can serve as a backup for some services, but for full failover, additional steps, such as transferring FSMO roles (roles, 2025), would need to be carried out

Hyper-V Replica is an integral part of the Hyper-V role. It contributes to your disaster recovery strategy by replicating a virtual machine (VM) from one Hyper-V host server to another to keep your workloads available. Hyper-V Replica creates a copy of a live VM to a replica offline VM (Replica, 2025). Note the following:

As I have the Domain Controller on a VM I had to Enable Replication from this VM Server to the server I need to do the replication VM-HOST02 in my case



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime
PROJECT-DC-02			096 MB	00:42:47

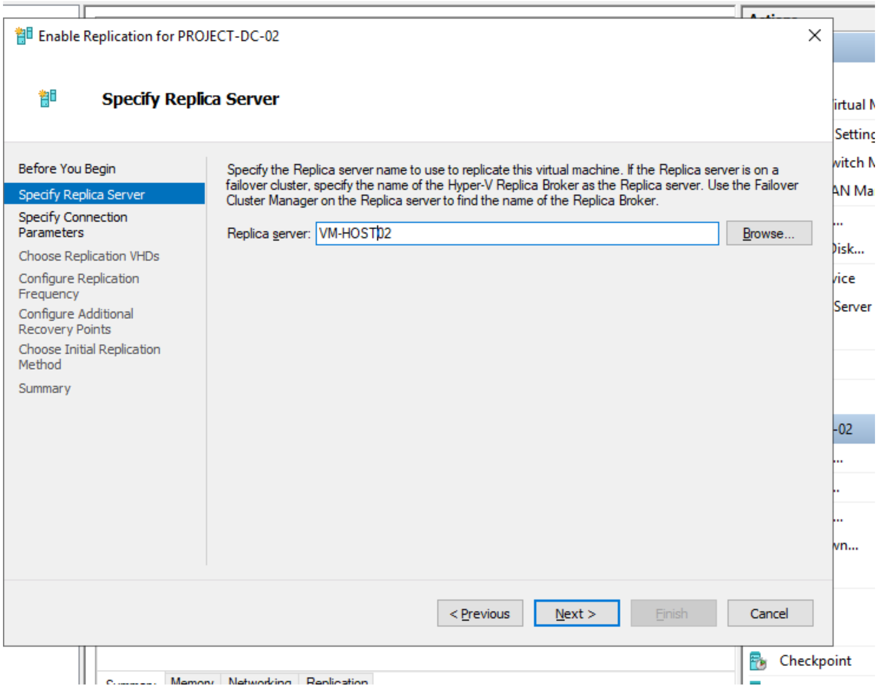
Checkpoints

ckpoints.

PROJECT-DC-02

Created: 14/03/2025 08:24:33
Configuration Version: 9.0
Generation: 2
Notes: None
Clustered: No
Heartbeat: OK (No Application Data)

Figure 35



Enable Replication for PROJECT-DC-02

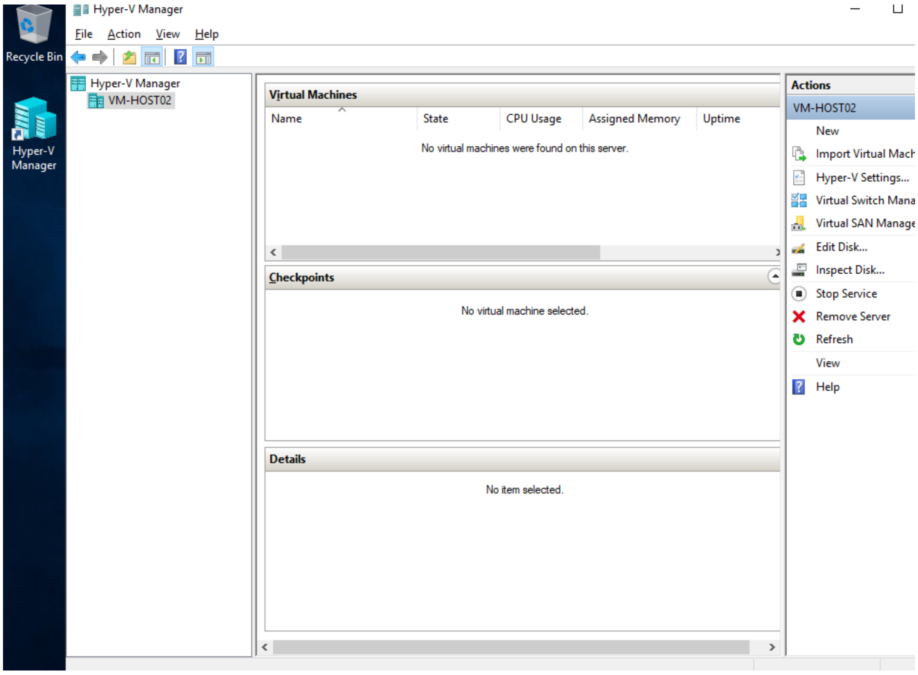
Specify Replica Server

Specify the Replica server name to use to replicate this virtual machine. If the Replica server is on a failover cluster, specify the name of the Hyper-V Replica Broker as the Replica server. Use the Failover Cluster Manager on the Replica server to find the name of the Replica Broker.

Replica server: VM-HOST02

Before You Begin
Specify Replica Server
Specify Connection Parameters
Choose Replication VHDs
Configure Replication Frequency
Configure Additional Recovery Points
Choose Initial Replication Method
Summary
Browse...
< Previous
Next >
Finish
Cancel
Checkpoint

Figure 36



Hyper-V Manager

Virtual Machines

No virtual machines were found on this server.

Checkpoints

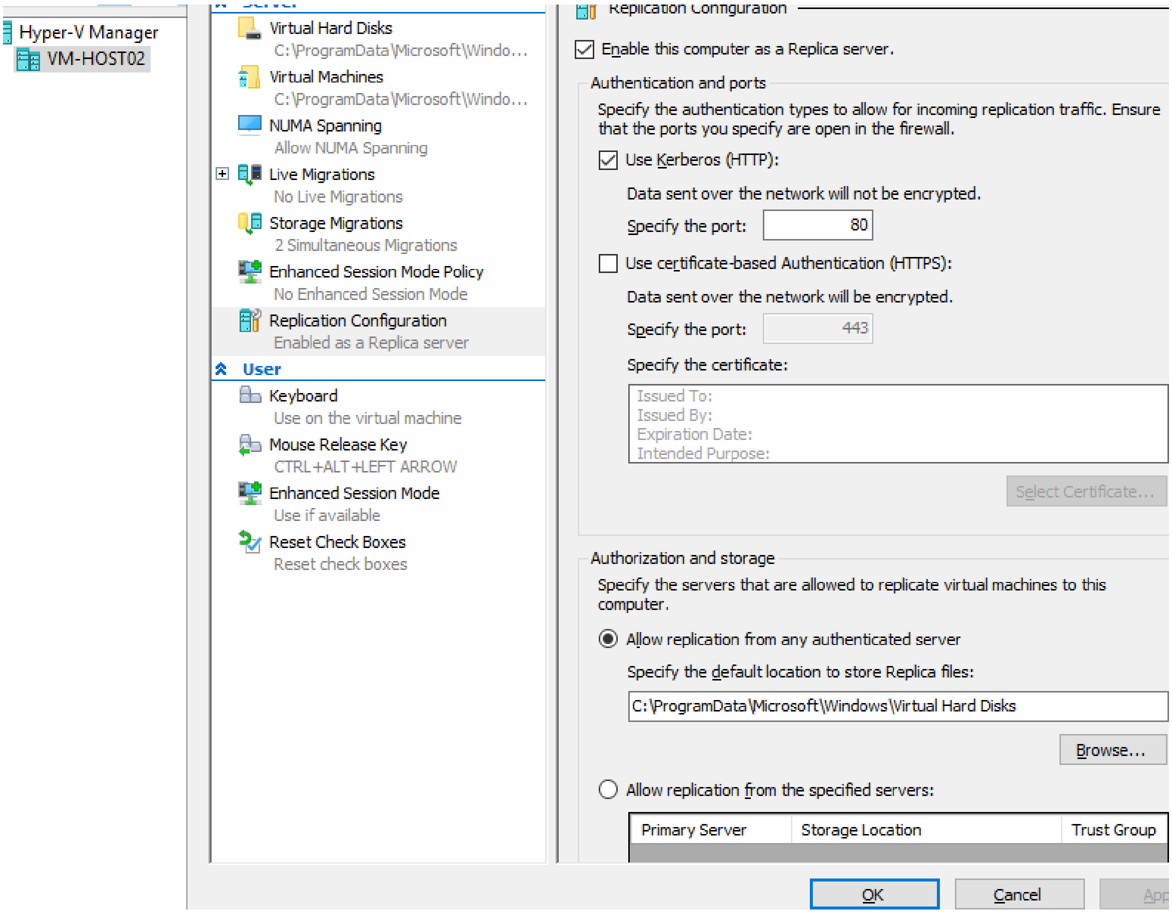
No virtual machine selected.

Details

No item selected.

Figure 37

Then I had to enable replication on the other server and Allow To connect through port 80 for creating Replication:



Hyper-V Manager
VM-HOST02

Virtual Hard Disks
C:\ProgramData\Microsoft\Windo...

Virtual Machines
C:\ProgramData\Microsoft\Windo...

NUMA Spanning
Allow NUMA Spanning

Live Migrations
No Live Migrations

Storage Migrations
2 Simultaneous Migrations

Enhanced Session Mode Policy
No Enhanced Session Mode

Replication Configuration
Enabled as a Replica server

User

Keyboard
Use on the virtual machine

Mouse Release Key
CTRL+ALT+LEFT ARROW

Enhanced Session Mode
Use if available

Reset Check Boxes
Reset check boxes

Replication Configuration

☑ Enable this computer as a Replica server.

Authentication and ports

Specify the authentication types to allow for incoming replication traffic. Ensure that the ports you specify are open in the firewall.

☑ Use Kerberos (HTTP):

Data sent over the network will not be encrypted.

Specify the port: 80

☐ Use certificate-based Authentication (HTTPS):

Data sent over the network will be encrypted.

Specify the port: 443

Specify the certificate:

Issued To:
Issued By:
Expiration Date:
Intended Purpose:

Authorization and storage

Specify the servers that are allowed to replicate virtual machines to this computer.

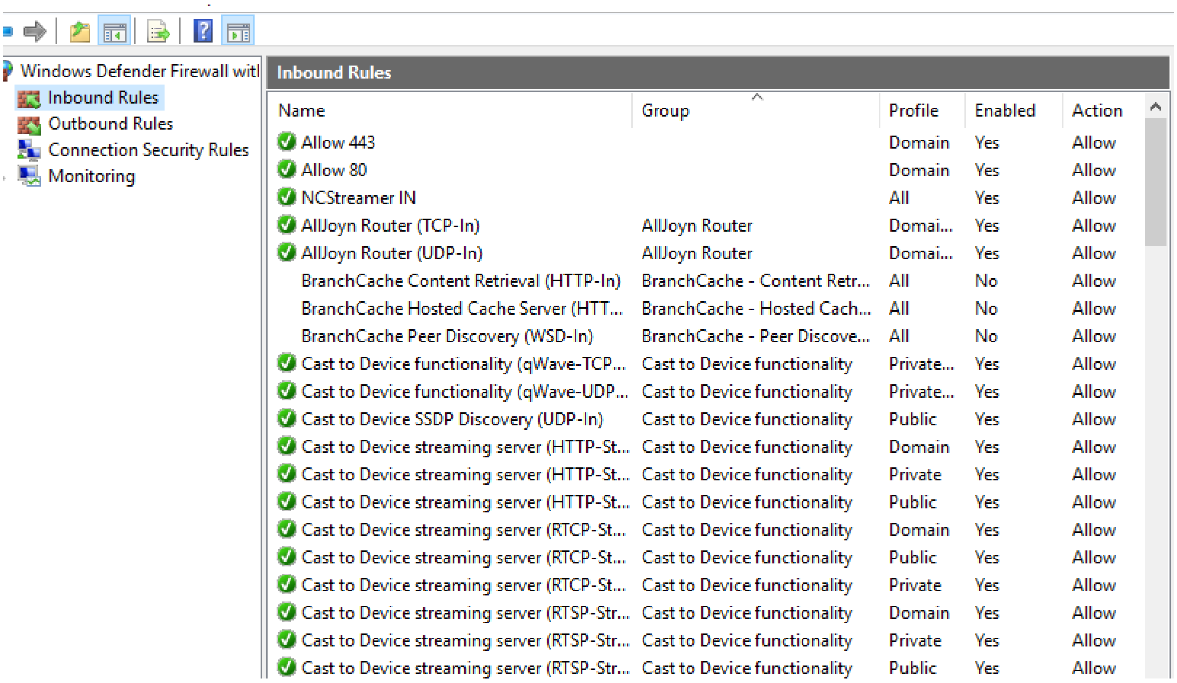
● Allow replication from any authenticated server

Specify the default location to store Replica files:

C:\ProgramData\Microsoft\Windows\Virtual Hard Disks

○ Allow replication from the specified servers:

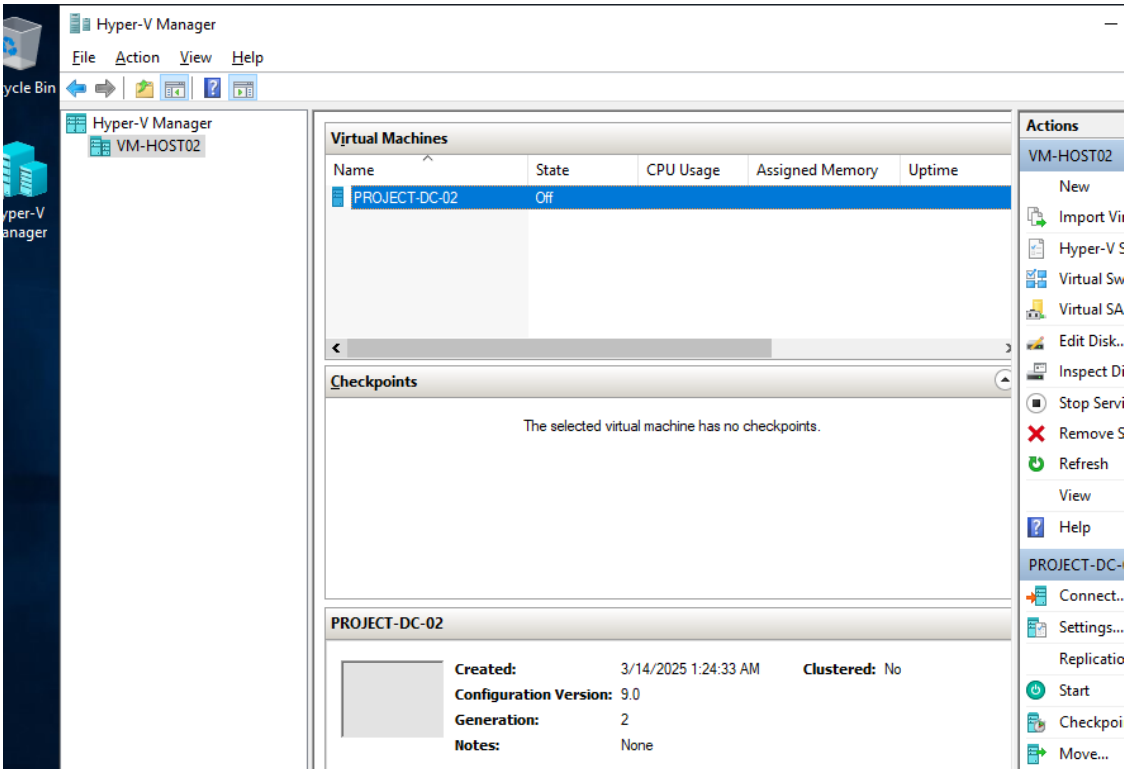
Primary Server	Storage Location	Trust Group



Inbound Rules

Name	Group	Profile	Enabled	Action
✓ Allow 443		Domain	Yes	Allow
✓ Allow 80		Domain	Yes	Allow
✓ NCStreamer IN		All	Yes	Allow
✓ AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow
✓ AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
✓ Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow
✓ Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow
✓ Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow
✓ Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes	Allow
✓ Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes	Allow
✓ Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes	Allow
✓ Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Domain	Yes	Allow
✓ Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Public	Yes	Allow
✓ Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Private	Yes	Allow
✓ Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Domain	Yes	Allow
✓ Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Private	Yes	Allow
✓ Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Public	Yes	Allow

Here I have the Domain Controller successfully replicate and turned OFF as the other one running on the other Server:



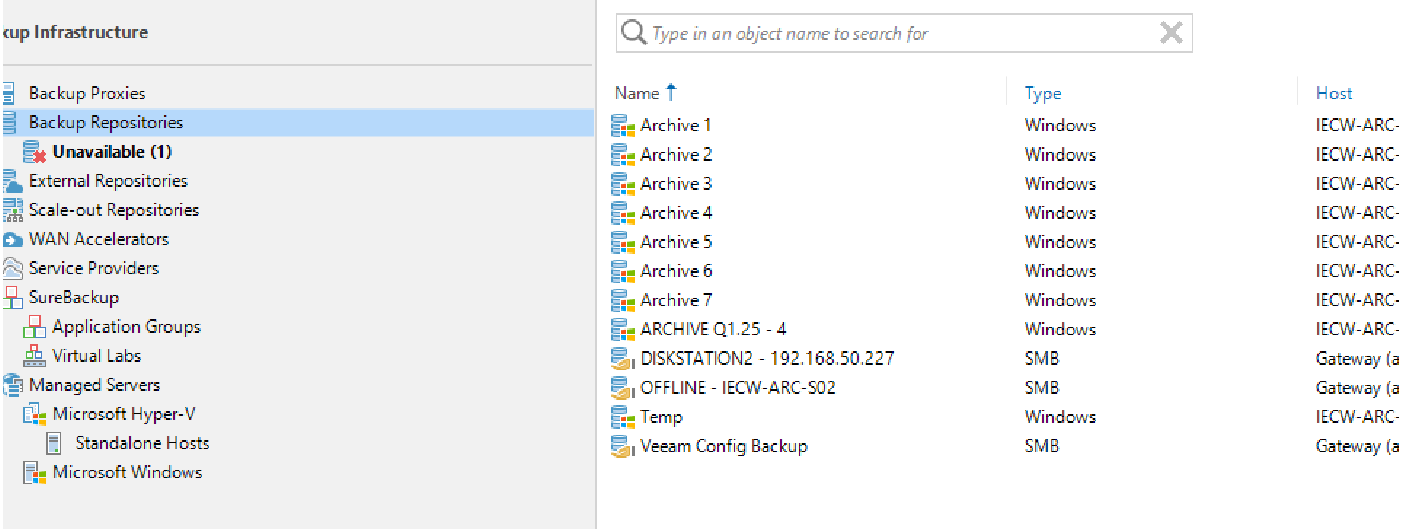
Name	State	CPU Usage	Assigned Memory	Uptime
PROJECT-DC-02	Off			

The selected virtual machine has no checkpoints.

PROJECT-DC-02

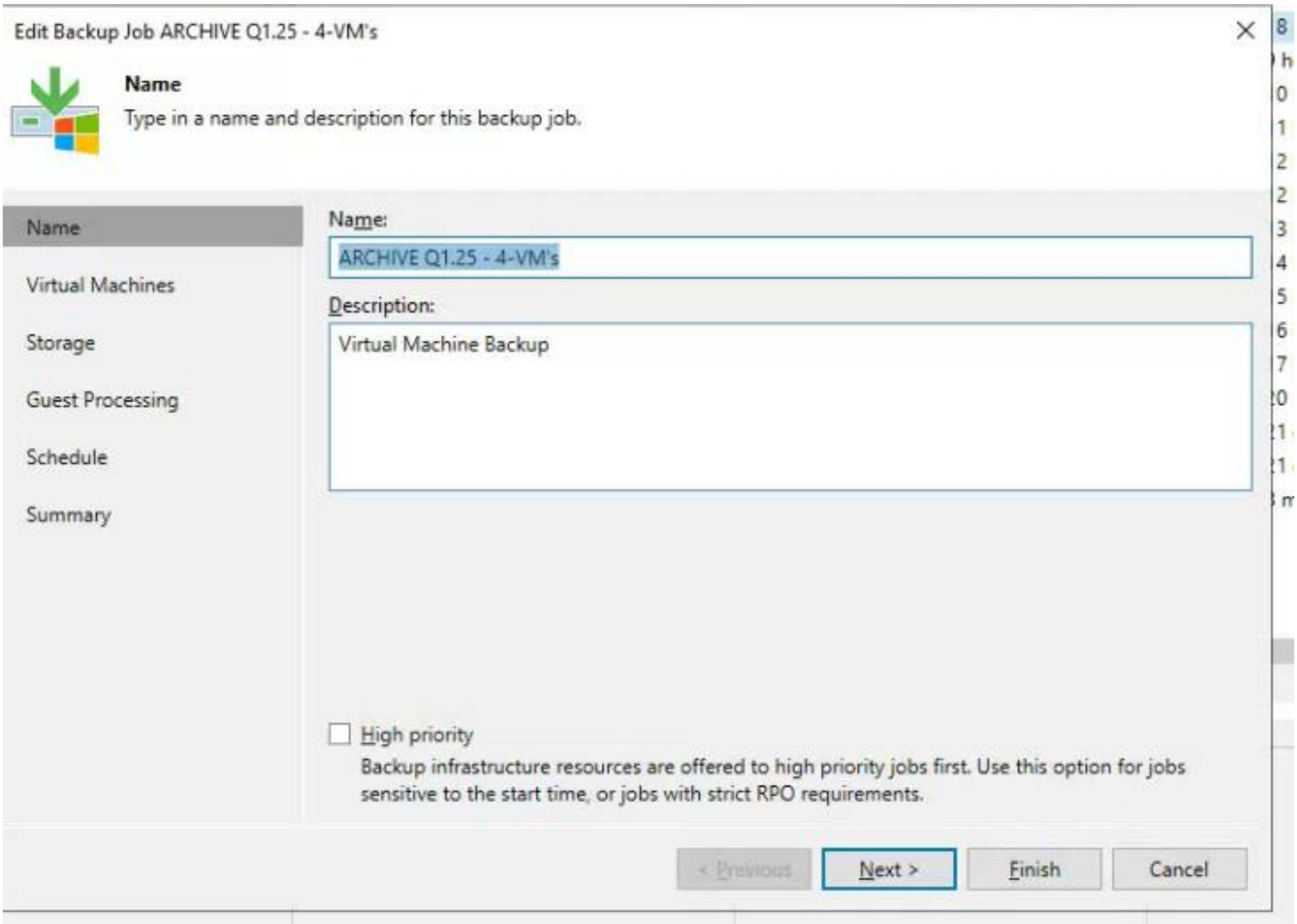
Created: 3/14/2025 1:24:33 AM **Clustered:** No
Configuration Version: 9.0
Generation: 2
Notes: None

Backup Images on an external Hard Drive:



Name ↑	Type	Host
Archive 1	Windows	IECW-ARC-
Archive 2	Windows	IECW-ARC-
Archive 3	Windows	IECW-ARC-
Archive 4	Windows	IECW-ARC-
Archive 5	Windows	IECW-ARC-
Archive 6	Windows	IECW-ARC-
Archive 7	Windows	IECW-ARC-
ARCHIVE Q1.25 - 4	Windows	IECW-ARC-
DISKSTATION2 - 192.168.50.227	SMB	Gateway (a
OFFLINE - IECW-ARC-S02	SMB	Gateway (a
Temp	Windows	IECW-ARC-
Veeam Config Backup	SMB	Gateway (a

Figure 38



Edit Backup Job ARCHIVE Q1.25 - 4-VM's

Name

Type in a name and description for this backup job.

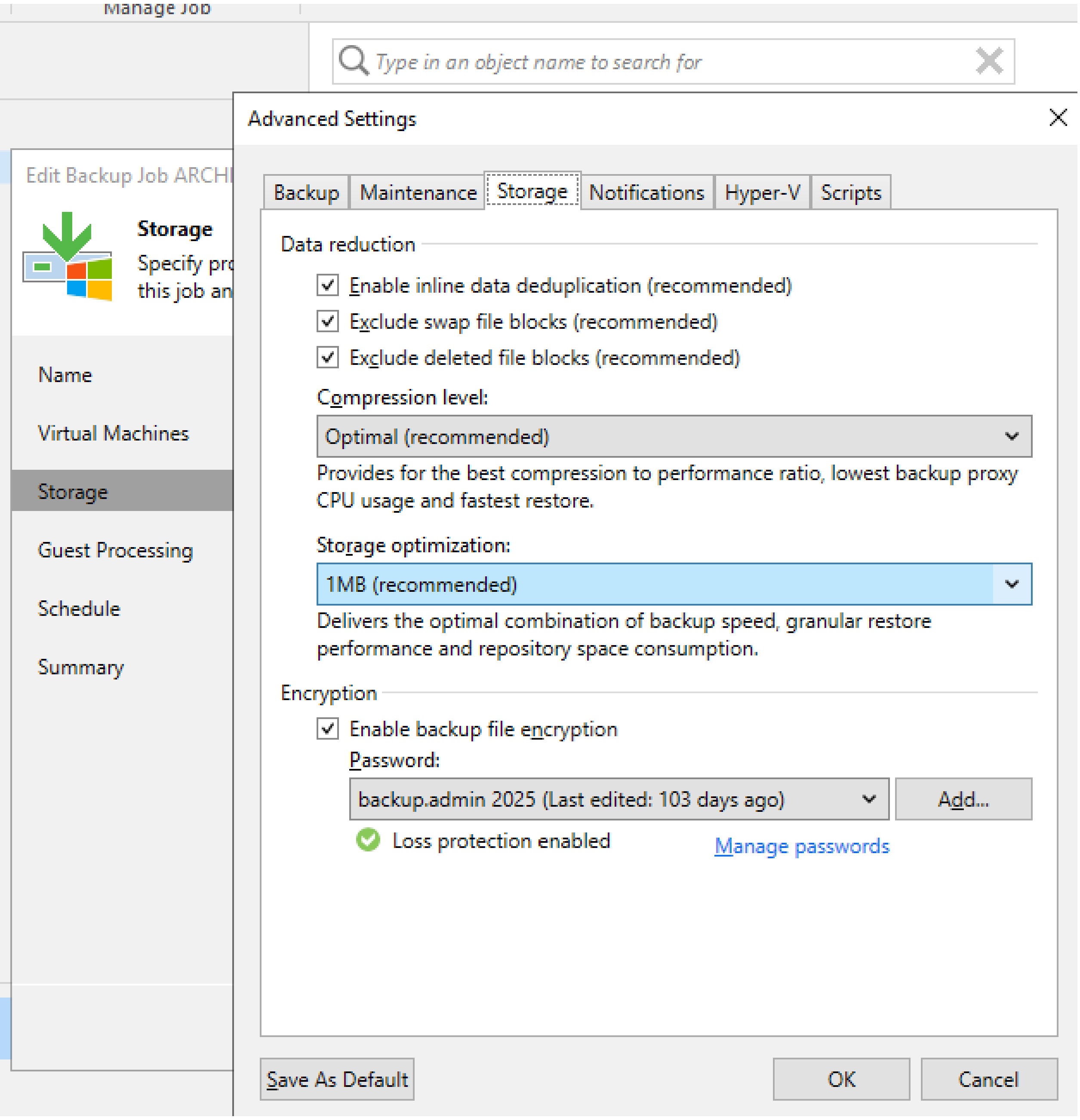
Name: ARCHIVE Q1.25 - 4-VM's

Description: Virtual Machine Backup

□ High priority

Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

Figure 39



Advanced Settings

Data reduction

☑ Enable inline data deduplication (recommended)

☑ Exclude swap file blocks (recommended)

☑ Exclude deleted file blocks (recommended)

Compression level: Optimal (recommended)

Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.

Storage optimization: 1MB (recommended)

Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.

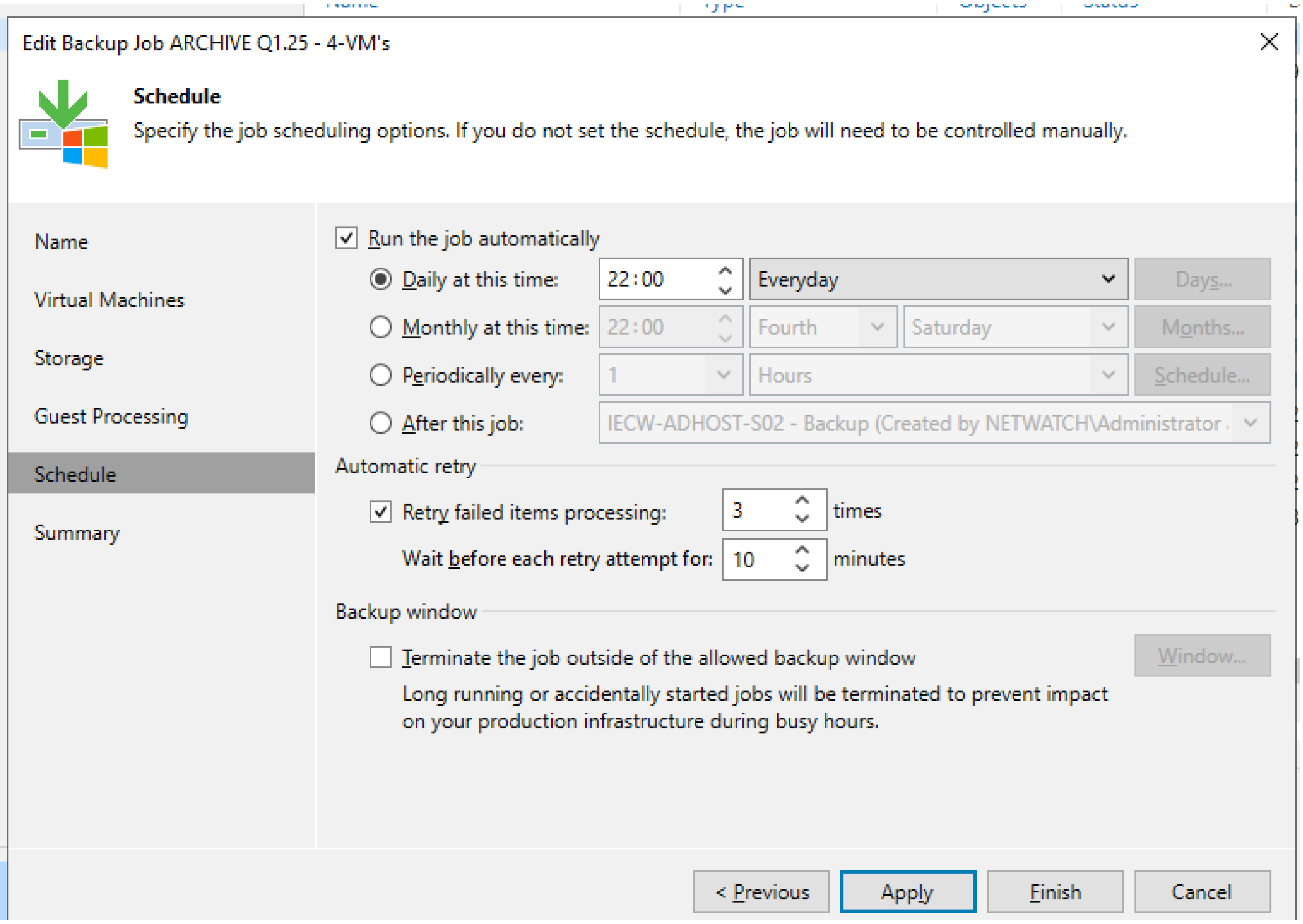
Encryption

☑ Enable backup file encryption

Password: backup.admin 2025 (Last edited: 103 days ago)

✓ Loss protection enabled

Figure 40



Edit Backup Job ARCHIVE Q1.25 - 4-VM's

Schedule

Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

- ● Daily at this time: 22 : 00 — Everyday — Days...
- ○ Monthly at this time: 22 : 00 — Fourth — Saturday — Months...
- ○ Periodically every: 1 — Hours — Schedule...
- ○ After this job: IECW-ADHOST-S02 - Backup (Created by NETWATCH\Administrator

Automatic retry

☑ Retry failed items processing: 3 times

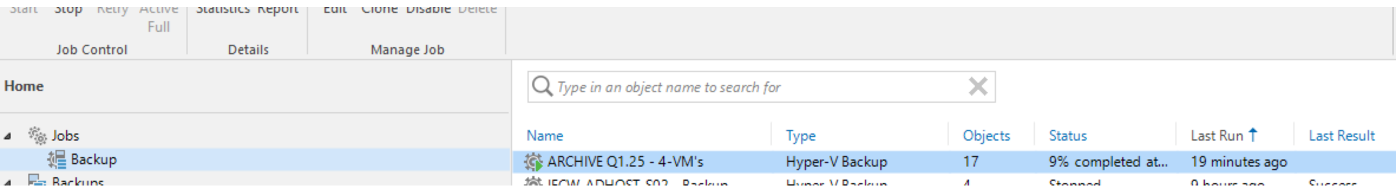
Wait before each retry attempt for: 10 minutes

Backup window

□ Terminate the job outside of the allowed backup window — Window...

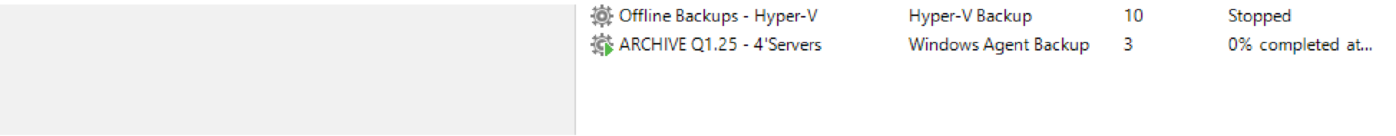
Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

Figure 41



Start Stop Retry Active Full
Job Control
Statistics Report
Details
Edit Clone Disable Delete
Manage Job
Home
Jobs
Backup
Backups
Type in an object name to search for

Name	Type	Objects	Status	Last Run	Last Result
ARCHIVE Q1.25 - 4-VM's	Hyper-V Backup	17	9% completed at...	19 minutes ago	
IECW-ADHOST-S02 - Backup	Hyper-V Backup	4	Stopped	9 hours ago	Success



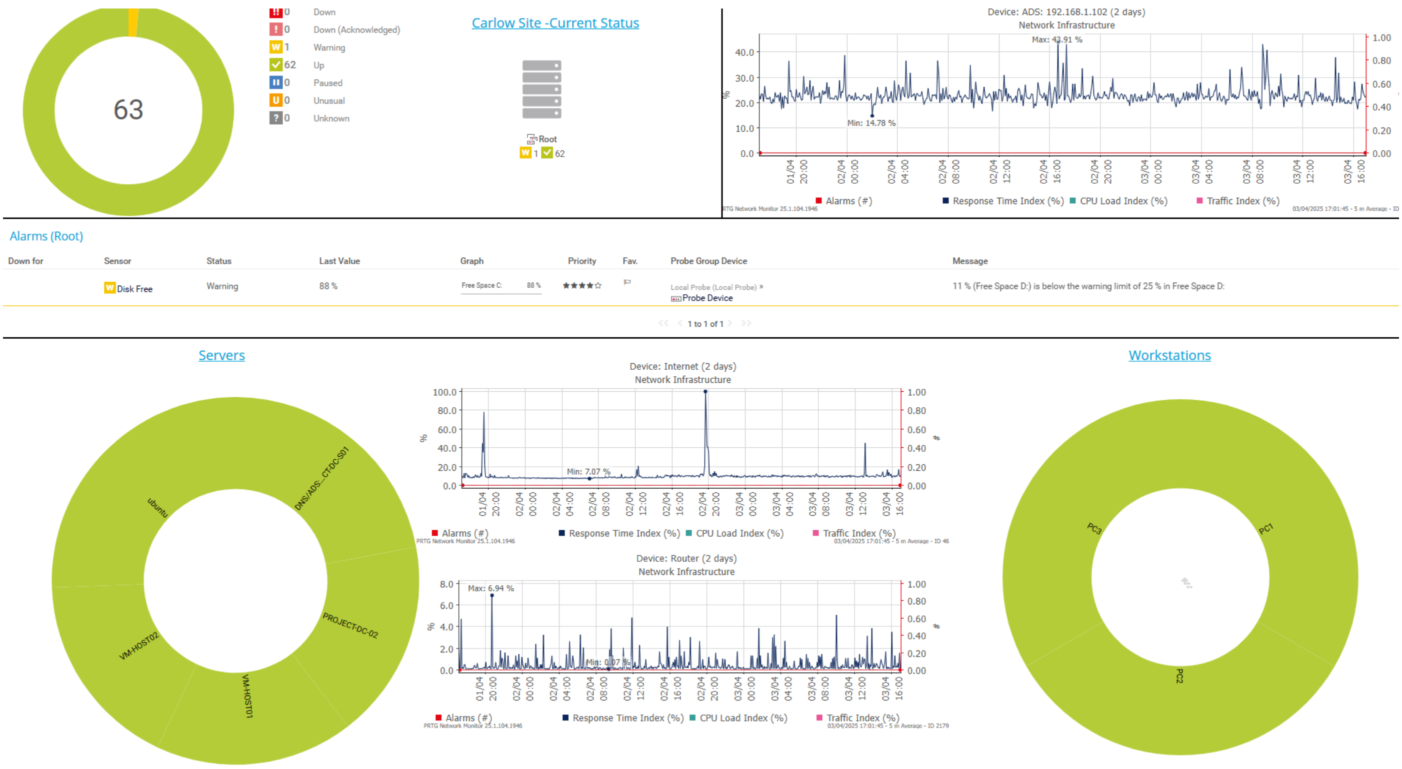
Offline Backups - Hyper-V	Hyper-V Backup	10	Stopped
ARCHIVE Q1.25 - 4'Servers	Windows Agent Backup	3	0% completed at...

PRTG Map

I added a PRTG Map to one of the PC's and configured it to monitor various devices across the network. This included both domain controllers, all servers, printers, static PC's, and network graphs. The PRTG system works by pinging these devices and using other monitoring functions to track their status and performance in real time. This setup allows me to keep and eye on the health and availability of all crucial devices, ensuring that any potential issues are quickly identified. With PRTG's monitoring, I can easily visualize network traffic, device uptime, and other key metrics, making it easier to manage and maintain the network infrastructure.

Map Designer in PRTG is a tool that lets you create custom network maps to visually monitor your devices (Designer, 2024). It allows you to arrange devices, servers, and networks graphs. with color-coded alerts to show device status – yellow warnings and red for offline devices. This helps you quickly see the health of your network and easily spot issues:

PRTG Map Monitoring live devices and traffic (as shown on Figure 42:



Alarms (Root)

Down for	Sensor	Status	Last Value	Graph	Priority	Fav.	Probe Group Device	Message
	W Disk Free	Warning	88 %	Free Space C: 88 %	★★★★☆		Local Probe (Local Probe) » Probe Device	11 % (Free Space D:) is below the warning limit of 25 % in Free Space D:

1 to 1 of 1

Figure 42

PEN TESTING:

Bloodhound:

Used to analyse Active Directory and identify potential attack paths, assisting in securing the domain against lateral movement threats (BloodHound, 2023).

I installed Bloodhound and Neo4j Desktop to analyse my Active Directory environment. This was setup on a PC that is not join to the domain and it is used for checking Active directory weak Paths as Pen Testing. First, I set up Neo4j Desktop, which acts as the database for storing and visualizing data. Then, I connected Bloodhound to Neo4j by entering the connection details (as shown in Figures 43 and 44)

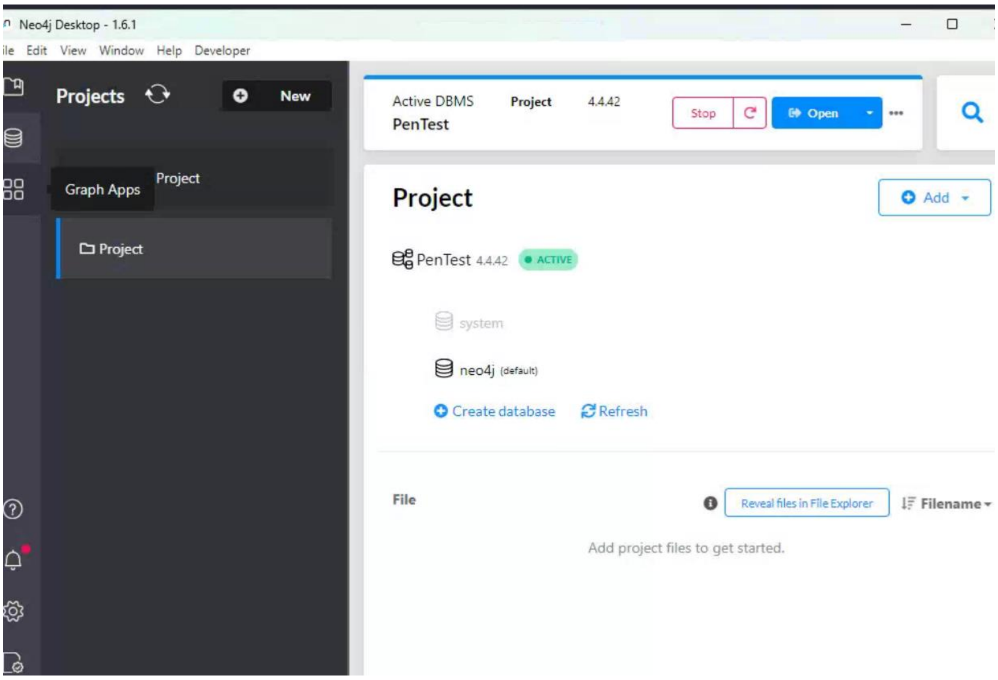
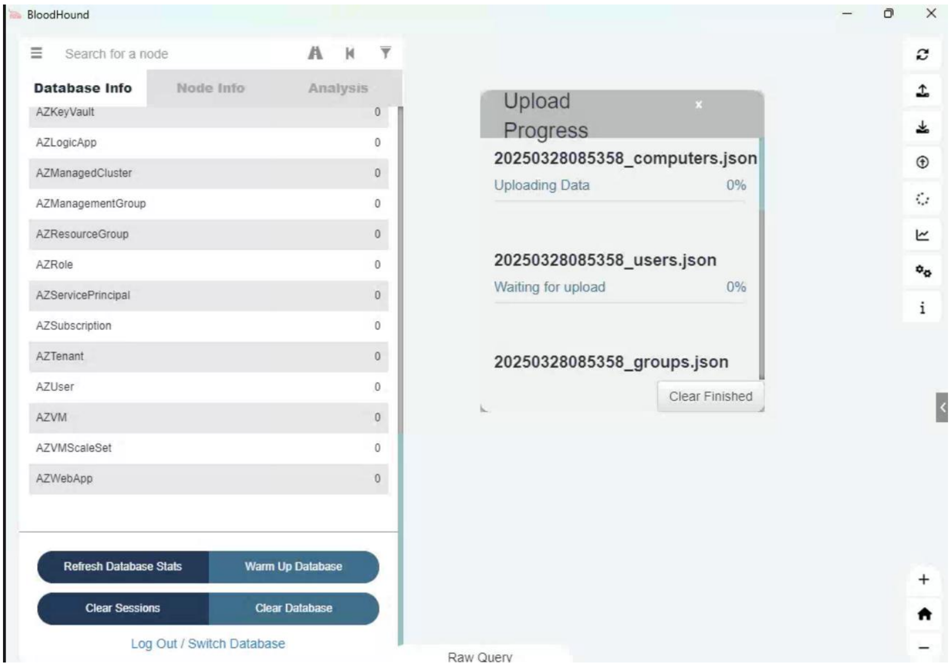


Figure 43



AZKeyVault	0
AZLogicApp	0
AZManagedCluster	0
AZManagementGroup	0
AZResourceGroup	0
AZRole	0
AZServicePrincipal	0
AZSubscription	0
AZTenant	0
AZUser	0
AZVM	0
AZVMScaleSet	0
AZWebApp	0

Upload Progress

20250328085358_computers.json
Uploading Data 0%

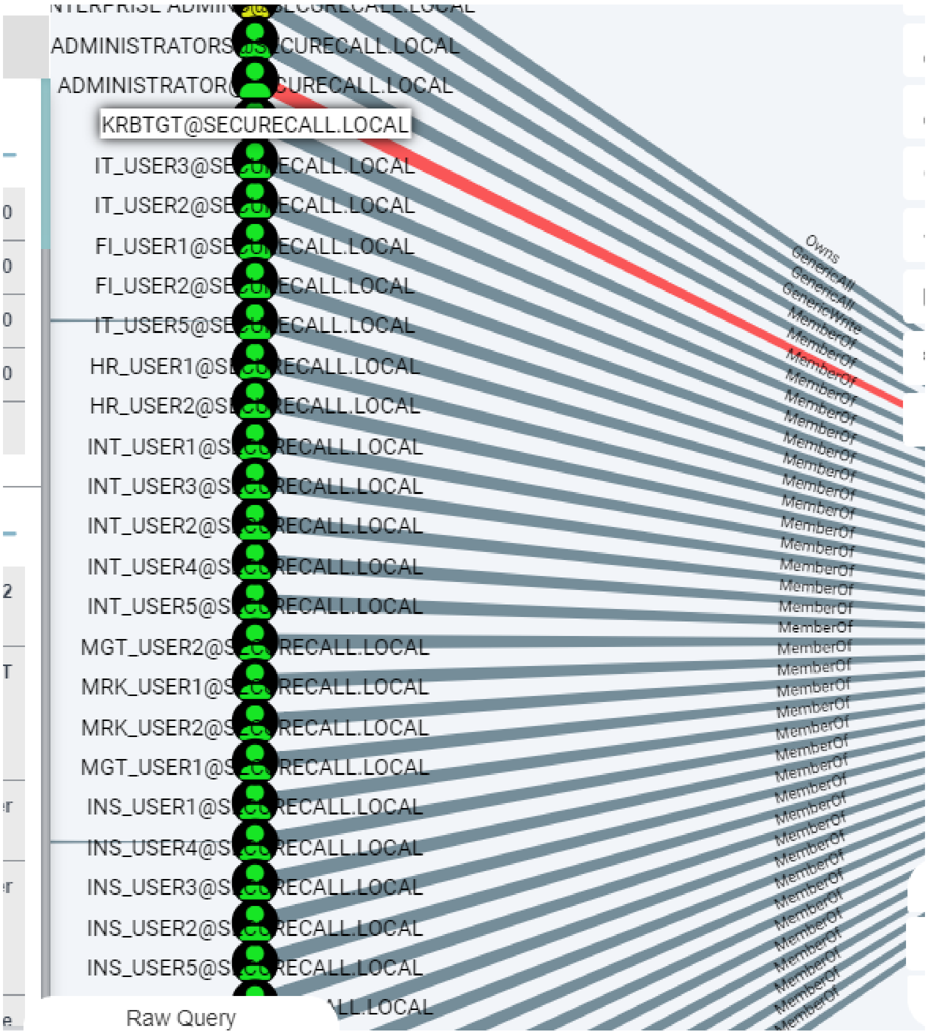
20250328085358_users.json
Waiting for upload 0%

20250328085358_groups.json

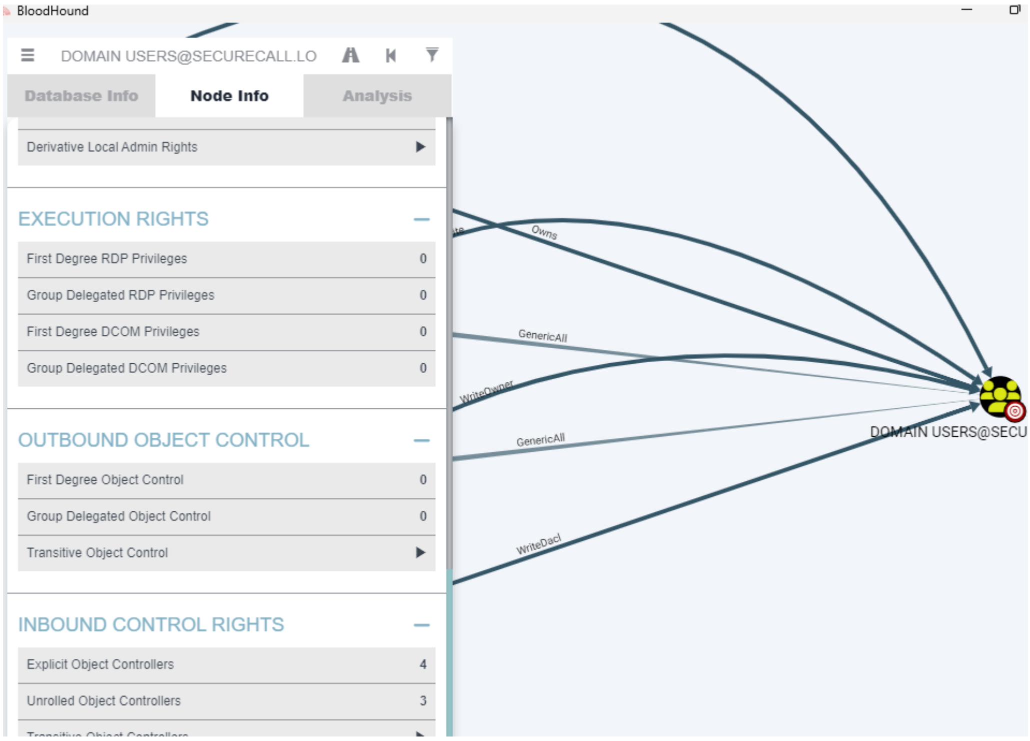
Figure 44

After all this, I ran the Sharp Hound tool using the command **SharpHound.exe -c All** to collect information about users, administrators, groups, and permissions in th Active Directory. One Sharp Hound finished, I imported the generated .Json files into Bloodhound Interface Graph. Bloodhound then displayed a graph showring the relationships and possible attack paths in the AD network. This allowed me to analyse potential risks and identify areas that needed attention.

Nothing major was found and no paths that represent risk were found eighter. I made some screenshots with the users and the connections they have directly to the domain (as shown bellow)


NTERPRISE ADMIN@SECURECALL.LOCAL
ADMINISTRATORS@SECURECALL.LOCAL
ADMINISTRATOR@SECURECALL.LOCAL
KRBTGT@SECURECALL.LOCAL
IT_USER3@SECURECALL.LOCAL
IT_USER2@SECURECALL.LOCAL
FI_USER1@SECURECALL.LOCAL
FI_USER2@SECURECALL.LOCAL
IT_USER5@SECURECALL.LOCAL
HR_USER1@SECURECALL.LOCAL
HR_USER2@SECURECALL.LOCAL
INT_USER1@SECURECALL.LOCAL
INT_USER3@SECURECALL.LOCAL
INT_USER2@SECURECALL.LOCAL
INT_USER4@SECURECALL.LOCAL
INT_USER5@SECURECALL.LOCAL
MGT_USER2@SECURECALL.LOCAL
MRK_USER1@SECURECALL.LOCAL
MRK_USER2@SECURECALL.LOCAL
MGT_USER1@SECURECALL.LOCAL
INS_USER1@SECURECALL.LOCAL
INS_USER4@SECURECALL.LOCAL
INS_USER3@SECURECALL.LOCAL
INS_USER2@SECURECALL.LOCAL
INS_USER5@SECURECALL.LOCAL
LL.LOCAL
Raw Query
Owns
GenericAll
GenericAll
GenericWrite
MemberOf

Few examples of Administrator rights and users' rights bellow:



Derivative Local Admin Rights ▶

EXECUTION RIGHTS

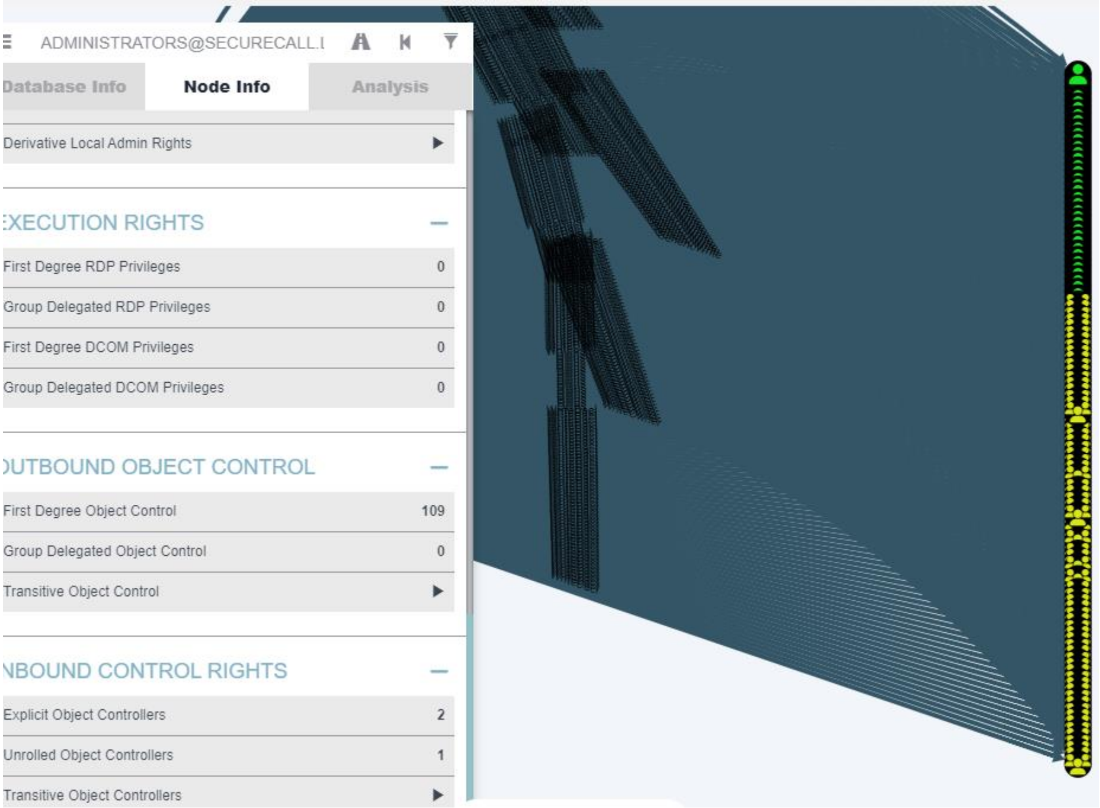
First Degree RDP Privileges	0
Group Delegated RDP Privileges	0
First Degree DCOM Privileges	0
Group Delegated DCOM Privileges	0

OUTBOUND OBJECT CONTROL

First Degree Object Control	0
Group Delegated Object Control	0
Transitive Object Control	▶

INBOUND CONTROL RIGHTS

Explicit Object Controllers	4
Unrolled Object Controllers	3
Transitive Object Controllers	▶



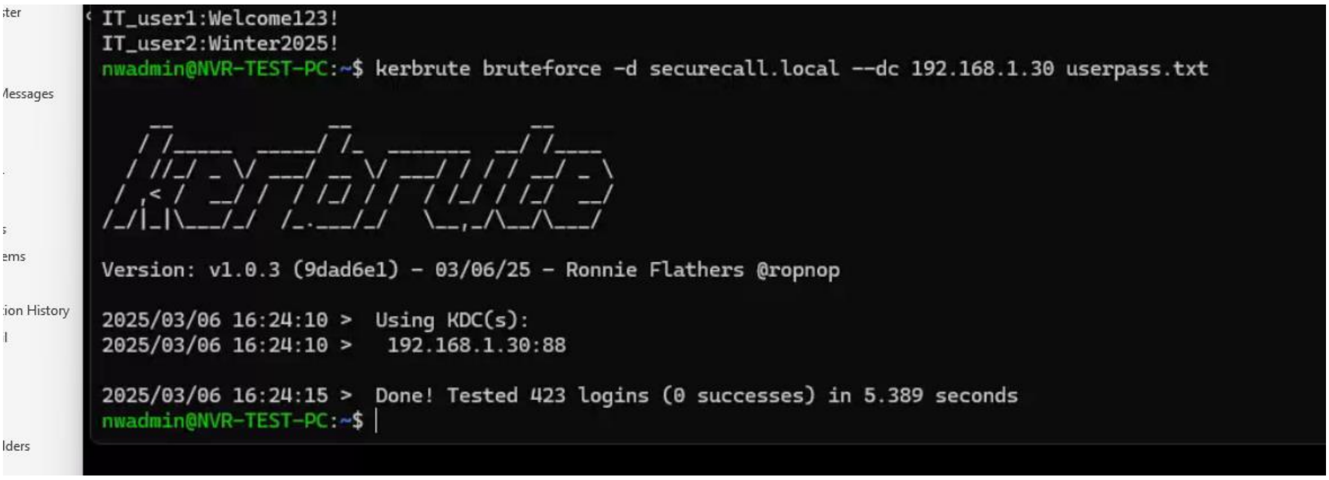
Derivative Local Admin Rights	▶
:XECUTION RIGHTS	—
First Degree RDP Privileges	0
Group Delegated RDP Privileges	0
First Degree DCOM Privileges	0
Group Delegated DCOM Privileges	0
)UTBOUND OBJECT CONTROL	—
First Degree Object Control	109
Group Delegated Object Control	0
Transitive Object Control	▶
\IBOUND CONTROL RIGHTS	—
Explicit Object Controllers	2
Unrolled Object Controllers	1
Transitive Object Controllers	▶

Kerbrute:

I tested a list of strong passwords using brute force method on Kerbrute(as shown in Figure 46). With this I tried many of possible combinations to break into the system. However, none of the attempts were successful.

This result shows that the passwords were strong enough to prevent the brute force attack from succeeding. It also highlights how important it is to use complex and unique passwords, as they are much harder to crack using brute force method.

Although I didn't succeed in breaking the passwords, this test was a good demonstration of how effective strong passwords can be in protecting accounts and systems.

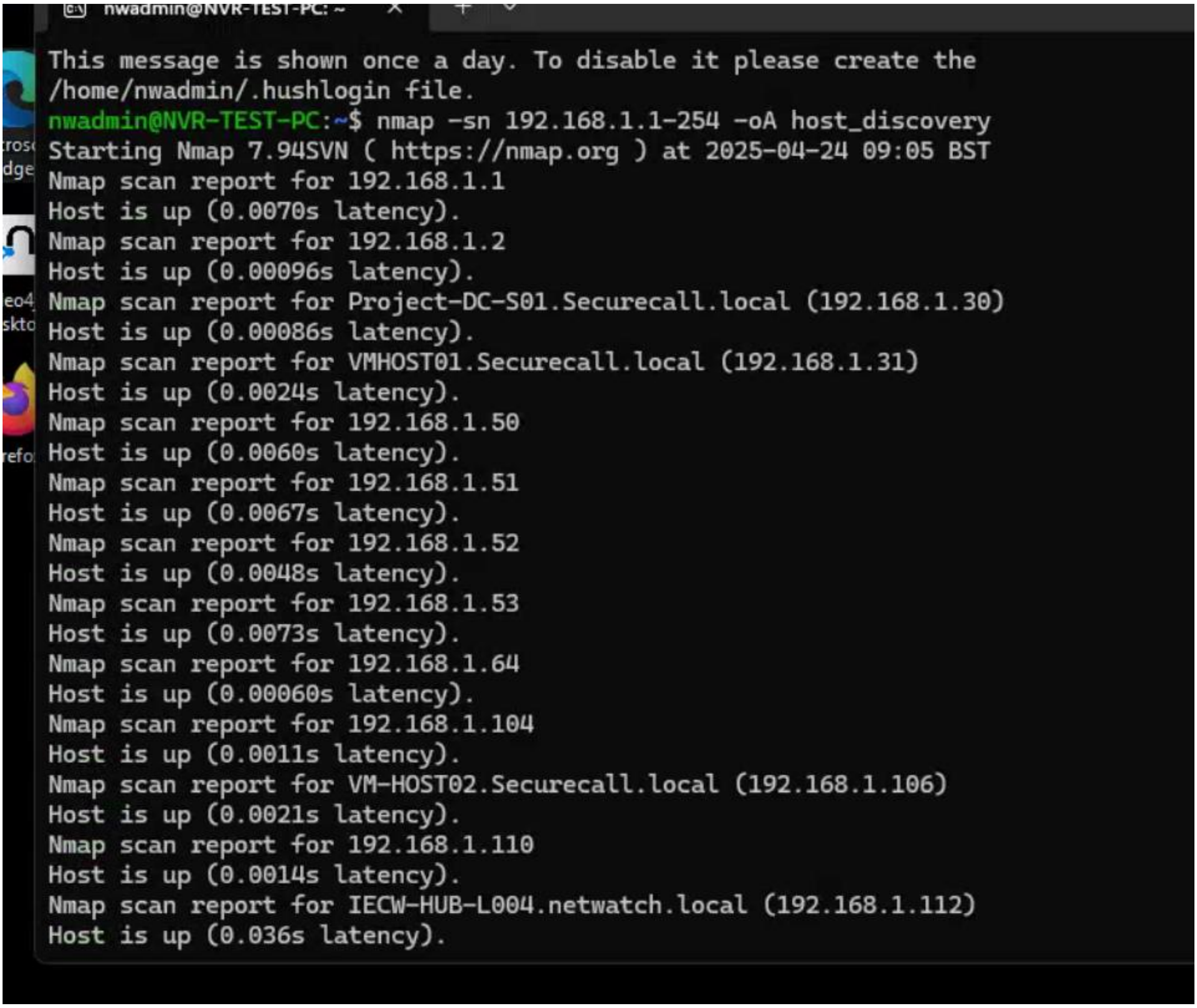


```
IT_user1:Welcome123!
IT_user2:Winter2025!
nwadmin@NVR-TEST-PC:~$ kerbrute bruteforce -d securecall.local --dc 192.168.1.30 userpass.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 03/06/25 - Ronnie Flathers @ropnop

2025/03/06 16:24:10 >  Using KDC(s):
2025/03/06 16:24:10 >   192.168.1.30:88

2025/03/06 16:24:15 >  Done! Tested 423 logins (0 successes) in 5.389 seconds
nwadmin@NVR-TEST-PC:~$ |
```

Figure 46

NMAP

I perform Host Discovery



```
This message is shown once a day. To disable it please create the
/home/nwadmin/.hushlogin file.
nwadmin@NVR-TEST-PC:~$ nmap -sn 192.168.1.1-254 -oA host_discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-24 09:05 BST
Nmap scan report for 192.168.1.1
Host is up (0.0070s latency).
Nmap scan report for 192.168.1.2
Host is up (0.00096s latency).
Nmap scan report for Project-DC-S01.Securecall.local (192.168.1.30)
Host is up (0.00086s latency).
Nmap scan report for VMHOST01.Securecall.local (192.168.1.31)
Host is up (0.0024s latency).
Nmap scan report for 192.168.1.50
Host is up (0.0060s latency).
Nmap scan report for 192.168.1.51
Host is up (0.0067s latency).
Nmap scan report for 192.168.1.52
Host is up (0.0048s latency).
Nmap scan report for 192.168.1.53
Host is up (0.0073s latency).
Nmap scan report for 192.168.1.64
Host is up (0.00060s latency).
Nmap scan report for 192.168.1.104
Host is up (0.0011s latency).
Nmap scan report for VM-HOST02.Securecall.local (192.168.1.106)
Host is up (0.0021s latency).
Nmap scan report for 192.168.1.110
Host is up (0.0014s latency).
Nmap scan report for IECW-HUB-L004.netwatch.local (192.168.1.112)
Host is up (0.036s latency).
```

Results:

I identified 24 active hosts on the Network. Key findings include several domain controllers and VM hosts, along with various unknown devices. Some hosts were identified as workstations joined to the domain, while others appeared to be third-party systems as the network is a guest network. Additionally, there were devices likely functioning as routers or switches. The scan utilized SYN scan, service version detection, OS detection, and skipped host multiple formats for detailed analysis. Nothing unprotected was found .

Scan for Open Ports & Services:

-sS: SYN scan

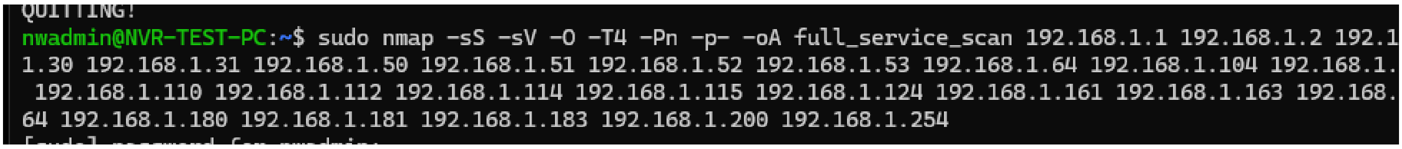
-sV: Service version detection

-O: OS detection

-Pn: Skip host discovery (since we know they’re up)

-p-: All ports (1–65535)

-oA: Save output in all formats (XML, grepable, normal)



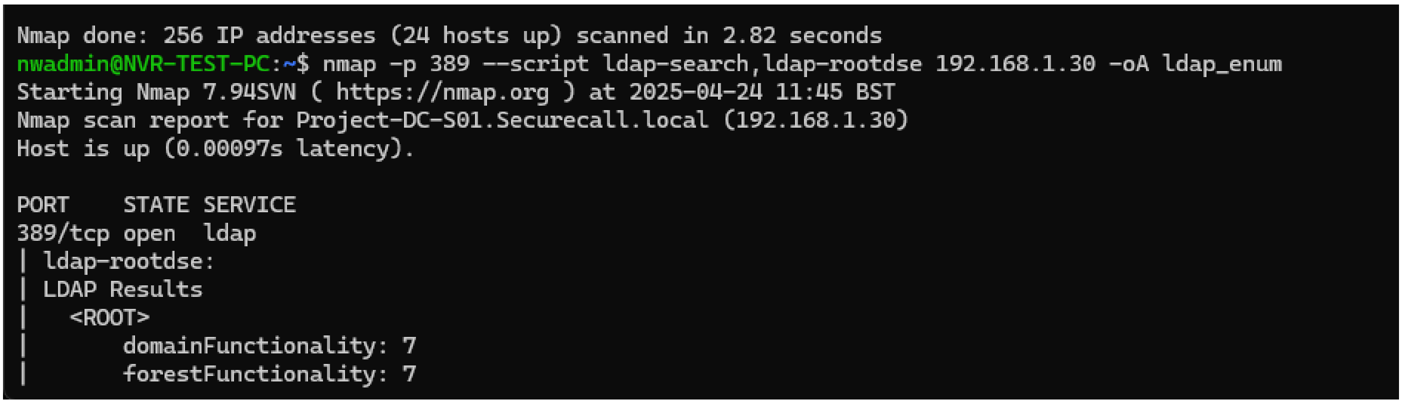
```
QUITTING!
nwadmin@NVR-TEST-PC:~$ sudo nmap -sS -sV -O -T4 -Pn -p- -oA full_service_scan 192.168.1.1 192.168.1.2 192.1
1.30 192.168.1.31 192.168.1.50 192.168.1.51 192.168.1.52 192.168.1.53 192.168.1.64 192.168.1.104 192.168.1.
 192.168.1.110 192.168.1.112 192.168.1.114 192.168.1.115 192.168.1.124 192.168.1.161 192.168.1.163 192.168.
64 192.168.1.180 192.168.1.181 192.168.1.183 192.168.1.200 192.168.1.254
[sudo] password for nwadmin:
```

Results:

The scan found multiple Windowws Server 2019 systems, Linux machines, and smart devices like LG TV’s where PRTG MAP is displayed. Key findings included exposed services such as Microsoft RPC, OpenSSh, and web applications on Node.js and lighted. Some services were running on non-standard ports (e.g. 8888,1520,2197), but they are not vulnerable. This is normally caused because Devices still running on Windows 10 as was the only devices I can use and they cant be upgraded to Windows 11.

Network scan for Open Ports and Services:

I performed a network scan on the domain controller (Project-DC-S01) within the domain I created, Securecall.local. The sacn targeted port 389, wich is used for LDAP services, to verify the configuration and functionality of the domain controller and Active Directory services :



```
Nmap done: 256 IP addresses (24 hosts up) scanned in 2.82 seconds
nwadmin@NVR-TEST-PC:~$ nmap -p 389 --script ldap-search,ldap-rootdse 192.168.1.30 -oA ldap_enum
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-24 11:45 BST
Nmap scan report for Project-DC-S01.Securecall.local (192.168.1.30)
Host is up (0.00097s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
```

Findings

The Nmap scan revealed the following key details:

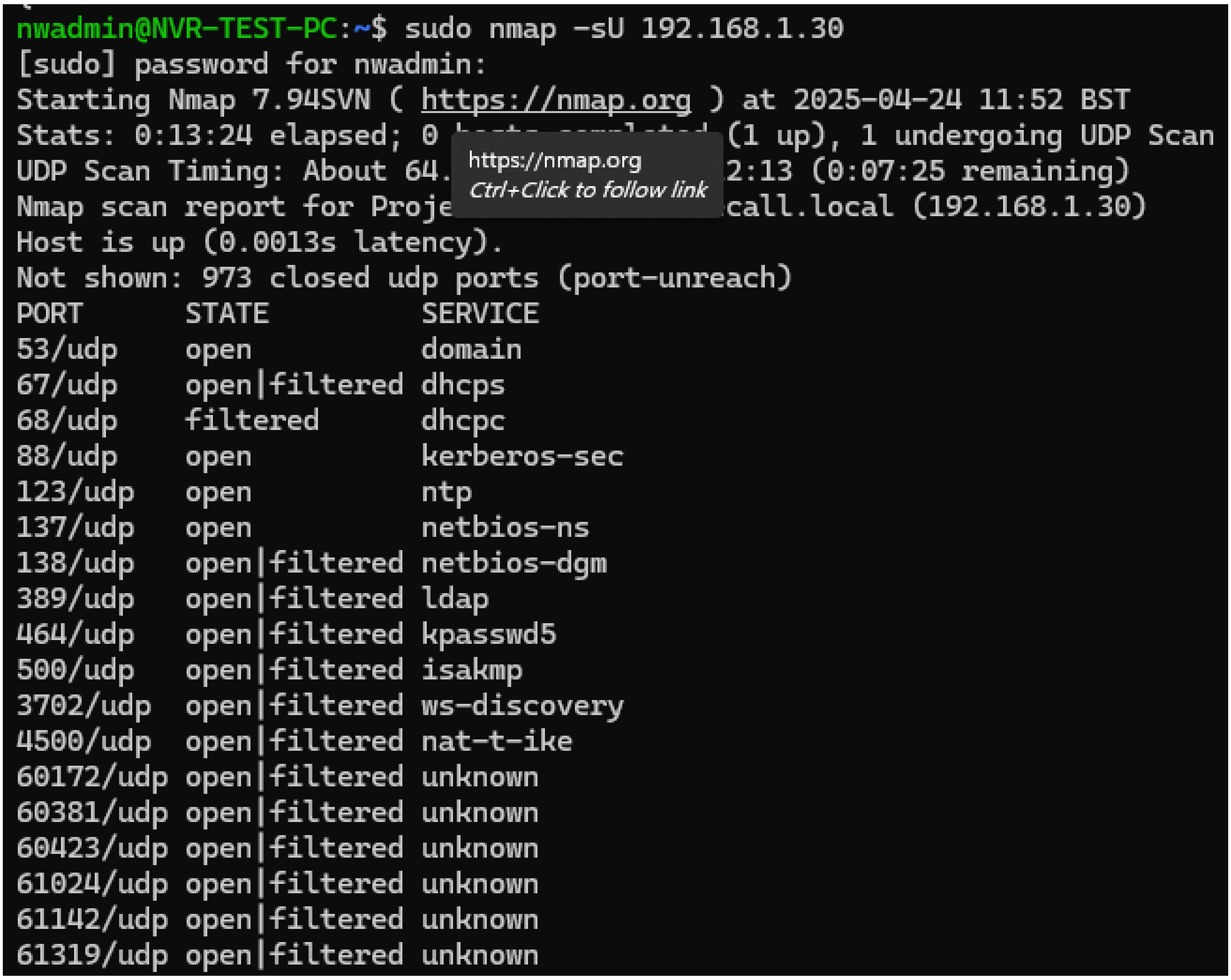
- Port 389: Open and running the LDAP service.
- Domain Functionality: Level 7
- Forest Functionality: Level 7
- Domain Controller Functionality: Level 7
- Root Domain Naming Context: DC=Securecall,DC=local
- LDAP Service Name: Securecall.local:project-dc-s01$@SECURECALL.LOCAL
- Global Catalog Ready: TRUE
- Supported SASL Mechanisms: GSSAPI, GSS-SPNEGO, EXTERNAL, DIGEST-MD5
- Supported LDAP Versions: 2, 3
- DNS Host Name: Project-DC-S01.Securecall.local
- Default Naming Context: DC=Securecall,DC=local

Results

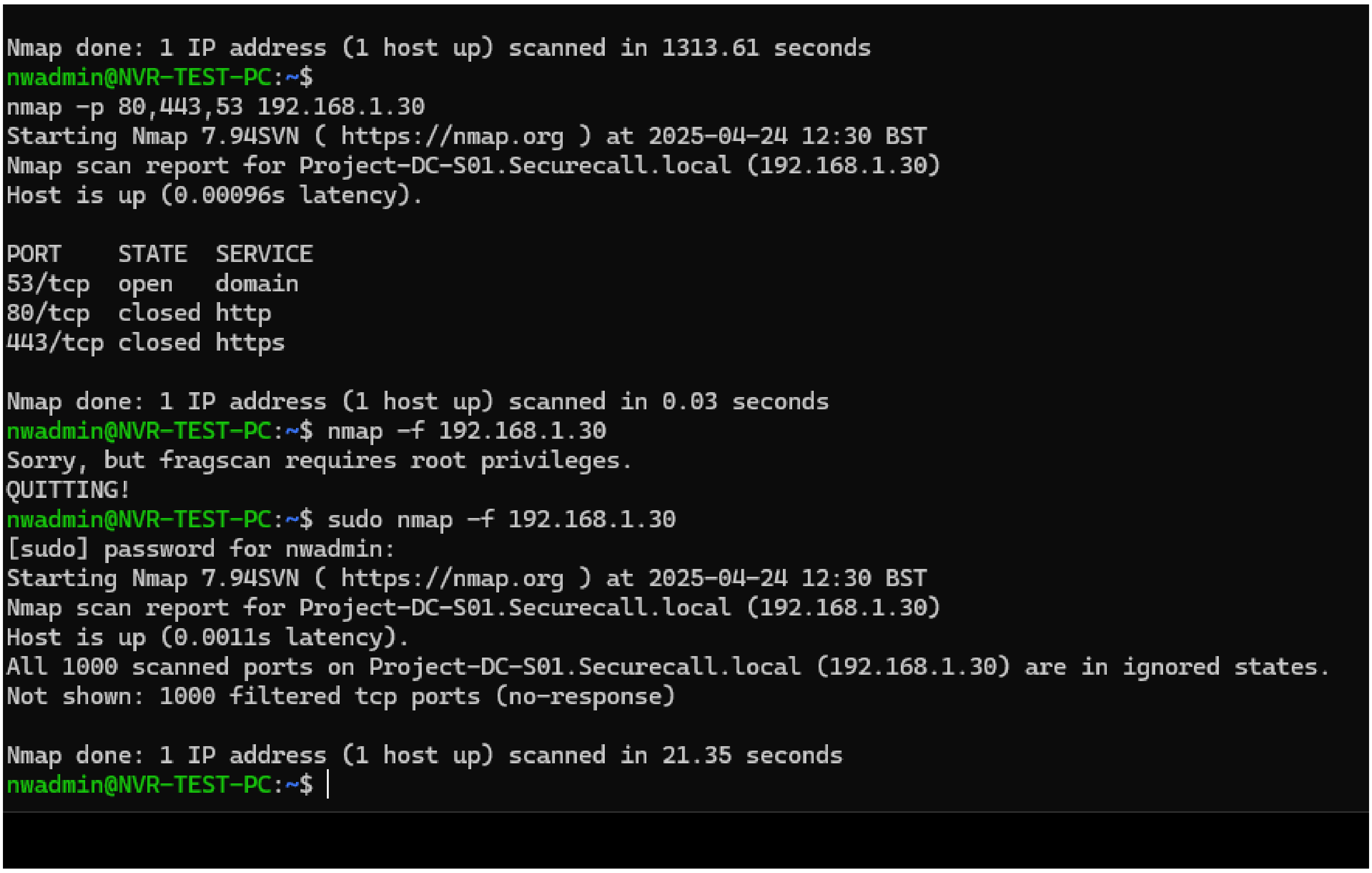
The scan results confirm that the domain controller is properly configured and functioning as expected. The advanced domain, forest, and domain controller functionality levels indicate that the setup supports a wide range of features and capabilities. The presence of multiple supported SASL mechanisms ensures secure authentication, and the support for LDAP version 2 and 3 guarantees compatibilities with various LDAP clients. The successful integration and configuration of both Domain Controller and Active Directory services provide a robust and secure communication within the network.

Network scan for Firewall and IDS Evasion, Specific Services and UDP Ports:

Some other network scans were done using NMAP on the same Domain Controller. These scans targeted various ports and services to verify the configuration and functionality of the domain controller and Active Directory services.



```
nwadmin@NVR-TEST-PC:~$ sudo nmap -sU 192.168.1.30
[sudo] password for nwadmin:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-24 11:52 BST
Stats: 0:13:24 elapsed; 0                (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 64.               2:13 (0:07:25 remaining)
Nmap scan report for Proje               call.local (192.168.1.30)
Host is up (0.0013s latency).
Not shown: 973 closed udp ports (port-unreach)
PORT      STATE         SERVICE
53/udp    open          domain
67/udp    open|filtered dhcps
68/udp    filtered      dhcpc
88/udp    open          kerberos-sec
123/udp   open          ntp
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
389/udp   open|filtered ldap
464/udp   open|filtered kpasswd5
500/udp   open|filtered isakmp
3702/udp  open|filtered ws-discovery
4500/udp  open|filtered nat-t-ike
60172/udp open|filtered unknown
60381/udp open|filtered unknown
60423/udp open|filtered unknown
61024/udp open|filtered unknown
61142/udp open|filtered unknown
61319/udp open|filtered unknown
```



```
Nmap done: 1 IP address (1 host up) scanned in 1313.61 seconds
nwadmin@NVR-TEST-PC:~$
nmap -p 80,443,53 192.168.1.30
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-24 12:30 BST
Nmap scan report for Project-DC-S01.Securecall.local (192.168.1.30)
Host is up (0.00096s latency).

PORT    STATE  SERVICE
53/tcp  open   domain
80/tcp  closed http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
nwadmin@NVR-TEST-PC:~$ nmap -f 192.168.1.30
Sorry, but fragscan requires root privileges.
QUITTING!
nwadmin@NVR-TEST-PC:~$ sudo nmap -f 192.168.1.30
[sudo] password for nwadmin:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-24 12:30 BST
Nmap scan report for Project-DC-S01.Securecall.local (192.168.1.30)
Host is up (0.0011s latency).
All 1000 scanned ports on Project-DC-S01.Securecall.local (192.168.1.30) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.35 seconds
nwadmin@NVR-TEST-PC:~$
```

Findings

UDP Scan The UDP scan revealed several open and filtered ports:

- 53/udp: Open (domain)
- 67/udp: Open|filtered (dhcps)
- 68/udp: Filtered (dhcpc)
- 88/udp: Open (kerberos-sec)
- 123/udp: Open (ntp)
- 137/udp: Open (netbios-ns)
- 138/udp: Open|filtered (netbios-dgm)
- 389/udp: Open|filtered (ldap)
- 464/udp: Open|filtered (kpasswd5)
- 500/udp: Open|filtered (isakmp)
- 3702/udp: Open|filtered (ws-discovery)

4500/udp: Open|filtered (nat-t-ike)

Several high-numbered ports: Open|filtered (unknown)

TCP Scan for Specific Services The scan for specific services (HTTP, HTTPS, and DNS) showed:

53/tcp: Open (domain)

80/tcp: Closed (http)

443/tcp: Closed (https)

Fragmentation Scan The fragmentation scan, which attempts to evade firewalls and intrusion detection systems, revealed that all 1000 scanned TCP ports were filtered with no response.

Result

The scan results confirm that the domain controller is properly configured and functioning as expected. Critical services like DNS, Kerberos, and NTP are active, and firewall rules are effectively protecting the system. Overall, the domain controller and Active Directory services provide a secure and robust communication framework within the network.

Description of Conformance to Specification and Design

The project was completed to the original plan, and the following tasks were successfully carried out:

- **Windows 2019 Installation:**

  Windows Servers 2019 was installed with the Desktop Experience option so that it has graphical interface, making it easier to manage.

- **Domain Controller Setup:**
  The Server was set up as a domain controller, and the correct roles – Active Directory Domain Services, DHCP, and DNS – were added, just as planned.

- **Network Configuration:**
  DHCP and DNS were set up properly, including IP address ranges and making sure the server handled DNS requests, following the design

- **Active Directory Structure**:
  The Active Directory was organized with Organizational Units (OUs) for users, departments, regions, and subdivisions. This helps with easier management and better security, matching the project design.

- **Group Policy Setup:**
  Security settings were applied as planned like disabling LLMNR and NTLMv1, requiring LDAP signing, and enabling Kerberos auditing. These settings make the system more secure and fallow best practices.

- **Password and security rules:**
  Password rules were put in place to require longer passwords and to lock accounts after several failed login attempts. This improves security and protects against unauthorised access.

- **Monitoring Setup and remediation:**

Monitoring Tools like Wazuh, PingCastle , PRTG, and NinjaOne were installed and configured. These tools help keep an eye on server's health and security in real time.

- **Penetration testing:**
  Security testing was done using Kerbrute, Bloodhound, and NMAP. The results were positive, showing that the system is well-secured with no major problems found.

- **Disaster Recovery Plan:**
  A disaster recovery plan was also created and implemented. This ensures that in case of a major problem or a failure, the system can be quickly restored with minimal downtime.

Minor Adjustments:

- Virtualization Setup: While virtualisation was part of the design, the initial number of VMs was adjusted during setup, only Hyper-V being use. Proxmox was not installed as originally planned due to some issues during installation. Using only Hyper-V compatibility and optical performance was ensured.
- Bloodhound was meant to be used for monitoring, but it ends up being use for Pen Testing instead

Improvements and Future Plans:

- **Secondary Domain Controller:**
  A second Domain Controller has been set up to ensure that if the main domain controller fails, the other one can quickly take over with the minimal downtime.

- **Hyper-V Replica Setup**
  Second Domain controller was set up as for replication using Hyper-V replica settings, making sure real-time copies of the server are available for fast recovery.

- **External Archive Backup**
  External Archive backups are done monthly to protect critical data and server configurations, improving disaster recovery and data protection.

- **Full Failover Capability**
  Full failover setup, including transferring FSMO roles, is planned. This allows the secondary domain controller to automatically take over if the primary domain controller fails, without minimal intervention.

Description of Learning

Technical Learning:

In this project, I learned a variety of technical skills related to server and network management. I installed and set up servers as domain controllers or Hyper-V to manage the network and user accounts. I worked with organ organising users and devices, creating groups to control access to resources. I gain experience in configuring network services like IP addresses assignment and device communication. I set up virtual machines on a separate server and learn how to manage them for testing different operating systems. I also learn how to implement strong password and security policies to engage network security. To monitor the networks health, I use tools to track devices, server status, and network traffic in real time, helping to quickly detect any issues. I learned how to setup replication between servers to ensure smooth recovery in case of a failure. I also learn how to use scripts in both windows PowerShell and LINUX server. Please help me automate tasks, manage configuration, and streamline system administration. Additionally, I practise penetration testing to identify potential vulnerabilities and security risk in the network, ensuring they were addressed before they could be exploited.

Personal Learning:

Beside the technical skills, I also learned a lot personally.:

- Problem-Solving: during this project, I run into some problems, like making sure the network settings work properly and getting virtual machines and physical machines connected to the domain. Setting up the open-source tools as free agent servers was challenging as well involving allot of configuration. Solving these issues helped me get better at troubleshooting.

- Time Management: I had to organise my time well to make sure I completed each part of the project on time. This helped me learn how to manage tasks and stay focused on what needed to be done next.

- Attention to detail: I realise how important it is to be careful and pay attention to small details, especially when setting up security groups, IP addresses, and network settings.

- Being flexible: some parts of the project didn't go as planned, and I had to adapt and make changes along the way. I learn how to be flexible and adjust my approach when needed.

Review of the Project

What Went Right?

The project went well in nearly all the areas. The installation of the servers was smooth, and the domain controllers was set up as planned, with a user-friendly interface that made management easier. The Active Directory system was organised effectively, which will simplify network management. Security improvements were made by disabling outdated protocols, enforcing stronger password etc. Monitoring tools were integrated, providing real time tracking of the networks health and helping to detect issues early for proactive management. The second domain controller was set up, with additional off a hyper V replica as well, an external backup along with replication were configured to ensure disaster recovery. Additionally, penetration testing was implemented which helped identify potential for their abilities before they could be exploited.

What Went Wrong?

- VPN Setup Not Done: VPN between the two regions was not able to be done for the school project because and access to the gas network and work where I created my environment. However, in real life scenario, I would establish a secure VPN connection between the domain controllers in a different location (e.g., Carlow and Dublin) To enable them to communicate securely.
- Small Configuration Changes: There were some unexpected adjustments needed, such as updating the DHCP range for devices. Since the network I set up was on the Guest network in a workplace where devices like phones TV's and other non-essential devices need to connect, I couldn't use the entire subnet for the DHCP range on my domain controller. I wanted to ensure this device didn't receive IP addresses from the DHCP server I created, so I had to configure it accordingly. Well, this cause some extra work, it was necessary to ensure the network remained secure and properly segmented.

What’s Still Left to Do?

Complete Failover Setup: The VPN connection needs to be established to ensure secure communication between domain controllers in different locations. This will help complete the failover system

More Penetration testing: While I did conduct some penetration testing, I wasn't able to complete a full test on the network and Active Directory as it wasn't originally planned. I had to do additional research before performing these tests and spend a lot of time on installing the proper apps for doing this Pen Testing, so there was limited time to fully analyse all potential abilities and security risks. I plan to conduct more through testing in the future.

If I Started Again, What Would I Do Differently?

If I were to do this project again, I would focus on redundancy first by ensuring the failover system, including the VPN connection an FSMO role transfer is fully operational. This is crucial for making sure the network can handle failures from the start. I would also spend more time planning configurations in detail, especially for IP addresses and DHCP, to avoid needing adjustments later. I will test each step more before moving on the next, as it would help catch any issues early and save time in the long run.

Advice for Others Doing a Similar Project:

Plan Carefully: make sure you understand the requirements of each part of the project and how everything connects before you start.

Test as You Go: Don't rush through the project. Test each part to ensure it works properly before moving on.

Make Security a Priority: Set up security measures early on, especially for user management and access control.

Keep Track of Everything: write down what you do and any problems you solve. This will help in the future if you need to make changes or fix things

Were My Technology Choices Good?

Using Windows server 2019 was the right choice for this project because it provided all the tools needed to set up and manage the network. Hyper V worked well for running virtual machines, allowing me to test different configurations and set up the system flexibly. Ping castle helped check the security of Active Directory by finding potential problems with group policies and access control, which could be risky if not fixed. The Linux server played an important role in supporting open-source tools and running various services. Wazuh was perfect for monitoring, helping to detect trend in vulnerabilities across the network. Ninja One made managing the network and devices remotely much easier, especially for maintenance and troubleshooting. PRTG was excellent from returning the networks help giving real time tracking and alerts for any problems. Finally, Bloodhound, NMAP and Ker brute. were useful for penetration testing, helping me find and fix security risk in the network

Conclusion

This project was a great learning experience where I got to set up and secure a network. I was able to create a stable and safe environment by installing the server, setting up user management, and applying important security settings.

I also learn how to monitor the network and check the weaknesses to make sure everything runs smoothly. Virtualization help me test different setup without affecting the main system, which made the process more flexible.

This project helped me understand the importance of planning, security, and a backup strategy to keep a network running safely. If I did it again, I would focus even more on making sure everything is set up for that long term, like ensuring the system can recover easily if something goes wrong.

Overall, the project was successful and helped me learn valuable skills and managing and securing networks

References

12, V. B. (2024, November 19). *veeam.com*. Retrieved from veeam.com: https://helpcenter.veeam.com/docs/backup/vsphere/backup_repository.html?ver=120

2019, S. (2024, january). *Microsoft*. Retrieved from Windows Server 2029: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019

AnthonyBartolo. (2023, february 22). *techcommunity.microsoft.com/*. Retrieved from techcommunity.microsoft.com/:

https://techcommunity.microsoft.com/blog/educatordeveloperblog/step-by-step-enabling-hyper-v-for-use-on-windows-11/3745905

BloodHound. (2023, january 01). *redcanary.com*. Retrieved from redcanary.com: https://redcanary.com/threat-detection-report/threats/bloodhound/#:~:text=BloodHound%20is%20an%20open%20source%20tool%20that%20can%20be%20used,testing%20activity%20and%20adversary%20use.

Bradley, S. (2019, October 30). *www.csoonline.com*. Retrieved from www.csoonline.com: https://www.csoonline.com/article/568015/how-to-disable-llmnr-in-windows-server.html

Designer, P. M. (2024, March 04). *paessler.com*. Retrieved from paessler.com: https://www.paessler.com/manuals/prtg/map_designer

Replica, S. u.-V. (2025, Januray 16). *learn.microsoft.com*. Retrieved from learn.microsoft.com: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/manage/set-up-hyper-v-replica

Rodriguez, A. (2024, October 15). *ninjaone.com*. Retrieved from ninjaone.com: https://www.ninjaone.com/docs/endpoint-management/hardware-inventory/creating-and-configuring-organizations/

roles, H. t. (2025, January 15). *learn.microsoft.com*. Retrieved from learn.microsoft.com: https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/view-transfer-fsmo-roles

Segal, D. (2025, January 16). *www.silverfort.com*. Retrieved from www.silverfort.com: https://www.silverfort.com/blog/ntlmv1-bypass-in-active-directory-technical-deep-dive/#:~:text=NTLMv1%20hashes%20can%20be%20intercepted,%2C%20including%20a%20zero%2Dday.

Server, H. t. (2025, January 15). *learn.microsoft.com*. Retrieved from learn.microsoft.com: https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/enable-ldap-signing-in-windows-server

Wazuh. (2024, January 01). *Wazuh.com*. Retrieved from Wazuh.com: https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/index.html