Babeș-Bolyai University

FSEGA

Department: Business Informatic Systems

Virtual Network Project

Infrastructură de rețea Windows + Ubuntu Server

Varvara Dorin-Robert

Horătău Darius Cristian

Ghețe Maria

Table of Contents

Introduction:.....3
Arhitecture Description: 4
Service Configuration .....**Error! Bookmark not defined.**
Problems We Faced .....**Error! Bookmark not defined.**
Conclusions 15

Introduction:

This project aimed to configure a virtual infrastructure consisting of three machines Windows Server, Windows 10 Pro, and Ubuntu Server.

- Windows Server was configured as a Domain Controller (Active Directory).
- Ubuntu Server provided network services such as Apache, Nginx, Mail Server, Samba, and SFTP, among others.

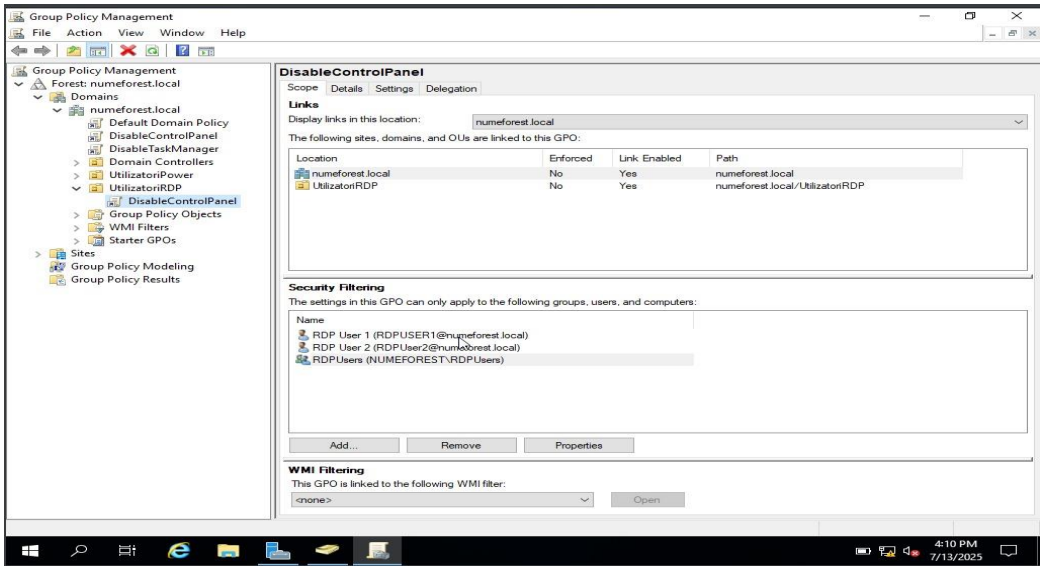
The project involved configuring essential services, testing connectivity, and ensuring network security through policies and firewall rules, successfully creating and analyzing a realistic network environment using only free software resources.

Arhitecture Description:

The first virtual machine in the infrastructure was configured as a Windows client, using the Windows 10 Pro operating system (or Windows 11 Pro, depending on the chosen configuration).

The role of this workstation was to simulate an end user in a company network, connected to the resources provided by the Windows and Linux servers in the infrastructure. To be able to access the resources offered by the Windows Server (VM2), this workstation was added to the previously created Active Directory domain, named numeforest.local.

After integration into the domain, users could benefit from the policies and restrictions imposed through GPO, as well as controlled access to shared folders and web services.



The workstation was equipped with a series of essential applications for administration and testing: PuTTY was used to access the command line of the Ubuntu server (VM3) through SSH connections. WinSCP allowed file transfers between the Windows client and the

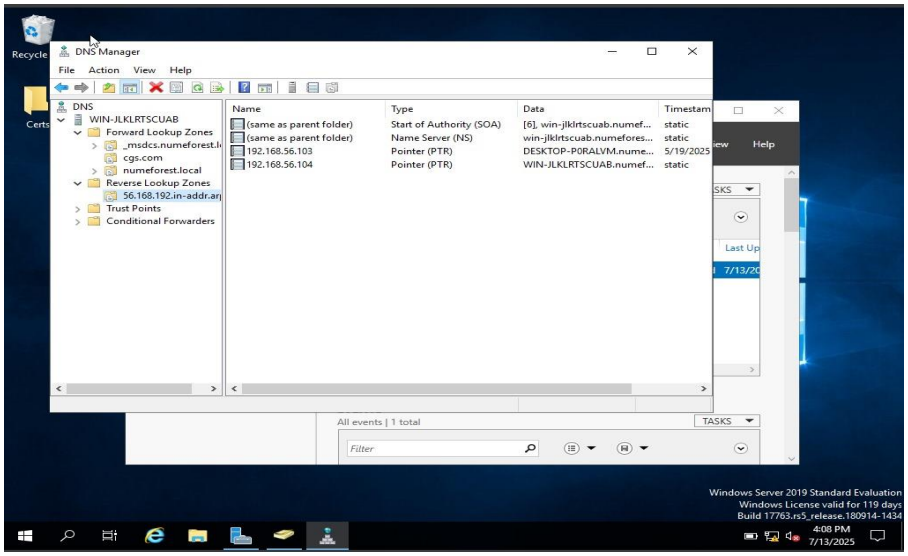
Ubuntu server via the SFTP protocol, demonstrating that the secure file transfer service was active and functional. Mozilla Thunderbird was configured as an email client to test sending and receiving messages within the infrastructure, using the mail server installed on Ubuntu.

A web browser (such as Microsoft Edge or Mozilla Firefox) was used to test connectivity to the websites hosted both on the Windows server (through IIS) and on Ubuntu (through Apache/Nginx), accessed via domains such as site4.numeforest.local,sj.ro,orcgs1.com.
In addition, the RDP (Remote Desktop Protocol) service was enabled on this workstation, allowing connection to the Windows server (VM2) for remote administration. Through this functionality, control and configuration tests were carried out directly from the server's graphical interface, without requiring physical interaction. This machine served as the central testing point, validating all the services configured on the other two machines and demonstrating the coherent operation of the network.

The second virtual machine in the infrastructure was configured with the role of the main server, using the Windows Server 2019 (or 2022) operating system. It played an essential role in network administration, providing authentication, name resolution, dynamic IP allocation, file sharing, and web application services.
The first step was promoting the machine to the role of Domain Controller by installing the Active Directory Domain Services and creating the numeforest.local domain. This established a centralized database of users and groups. Two main groups, PowerUsers and

RemoteDesktopUsers, were defined, and users were created and assigned accordingly. The Windows client (VM1) was then added to the domain to benefit from centralized authentication and group policies.

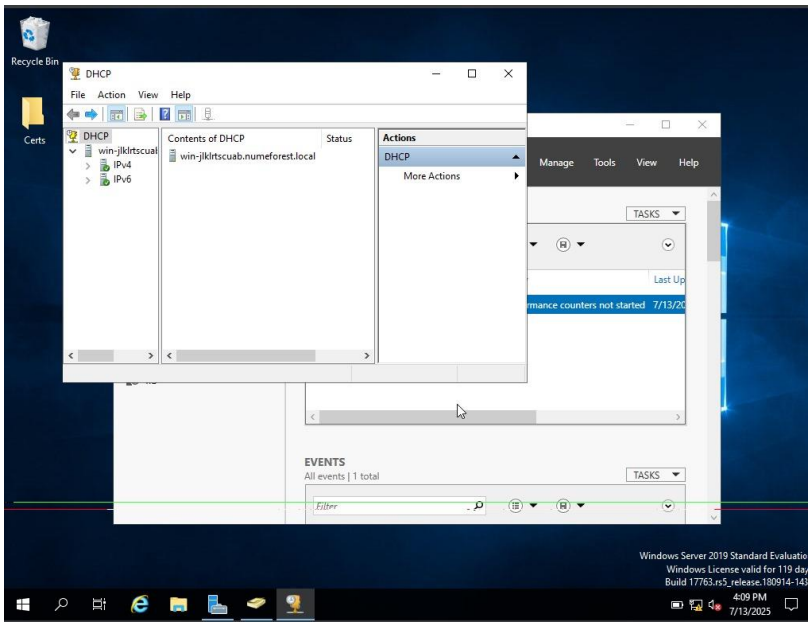
In parallel, the DNS service was installed, and two forward lookup zones (numeforest.local and sj.ro) and one reverse lookup zone were configured for mapping IP addresses to hostnames. These were used for name resolution within the network and to enable proper connectivity testing through hostnames.



Windows Server was also configured as a File Server by sharing two directories: one with Read-Only permissions, intended for standard users, and another with full access (Read/Write) for privileged users. These resources were tested from the Windows client, confirming the correct application of permissions based on group membership.

The DHCP service was also configured, allowing the automatic allocation of IP addresses to devices in the network. A dynamic scope was defined with an IP address range (e.g.,

192.168.1.100–192.168.1.200) to meet the infrastructure's requirements. Optionally, IP reservations can be made for servers or fixed workstations.



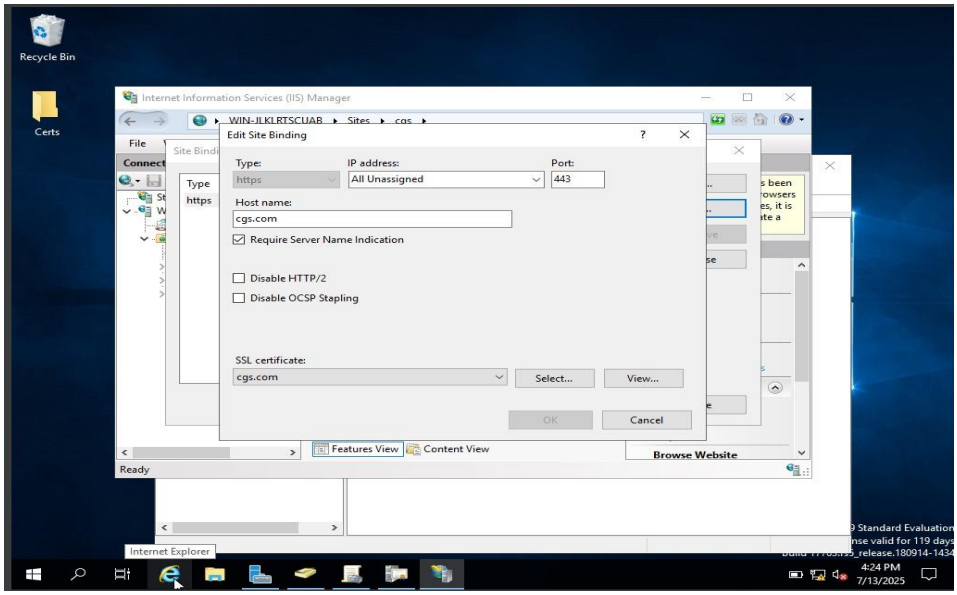
For hosting web applications, Internet Information Services (IIS) was installed, and three websites were created:

site4.numeforest.local

site5.numeforest.local

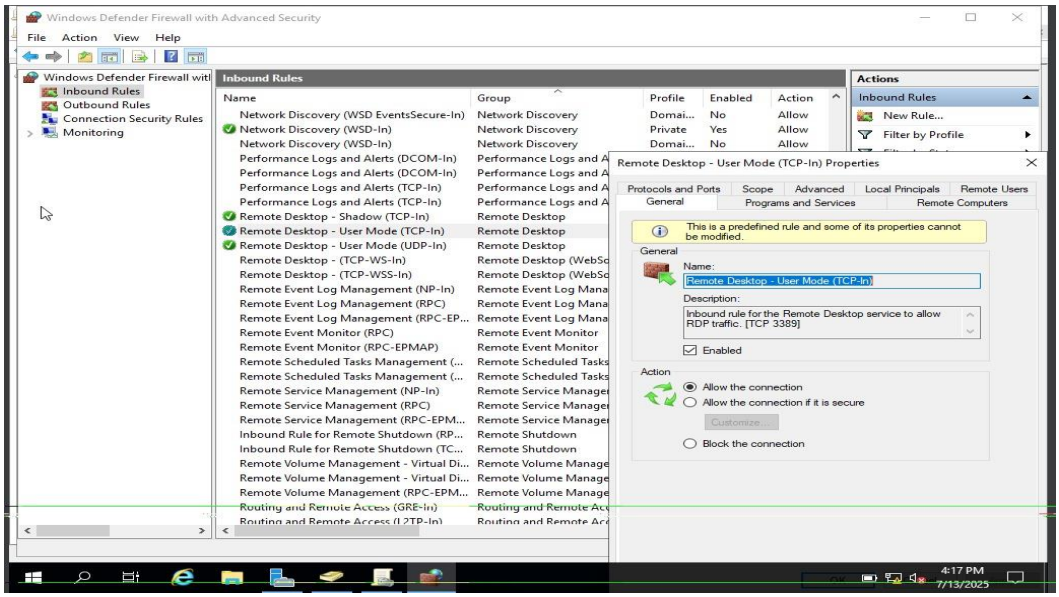
cgs.com.

Each site was configured to run on port 443 (HTTPS), using self-signed SSL certificates. The bindings were configured individually, and the websites were successfully tested from the browser on VM1.



Through the Group Policy Management Console (GPMC), group policies were defined to enforce restrictions on domain users, such as disabling access to the Control Panel and Task Manager. The policies were applied to the corresponding Organizational Units (OUs), and it was verified that they propagated correctly to the client workstation.

Finally, to secure the services, three rules were created in Windows Defender Firewall: one to allow RDP access, one for File and Printer Sharing, and one for HTTPS traffic (port 443), required for accessing the websites hosted by IIS. The tests performed confirmed that the rules worked properly and allowed access only for the configured services.



This virtual machine was the essential component of the Windows infrastructure, centralizing authentication, DNS, DHCP, GPO, and file-sharing services in a realistic and scalable manner.

The third virtual machine in the infrastructure was configured with the Ubuntu Server operating system, in a version without a graphical interface, accessible exclusively via SSH.

The role of this server was to complement the infrastructure with essential Linux-based services, providing web hosting, mail, file sharing, and secure file transfer functionalities. One of the main functionalities implemented on this server was web hosting. Apache or Nginx web servers were used, configured to host three distinct domains: site6.numeforest.local, sj.ro, and cgs1.com. Each of these domains was configured to operate over HTTPS, using self-signed SSL certificates. The VirtualHost configurations were done manually in dedicated files, and their functionality was tested both locally and from the Windows client's browser. The server was also equipped with a mail service, implemented using Postfix (for sending) and Dovecot (for receiving). This setup

allowed sending and receiving messages between local users defined on the system. Proper operation was confirmed both via the command-line interface (mail/mutt) and through the Mozilla Thunderbird client installed on VM1. For accessing messages through a graphical web interface, the RainLoop (or SquirrelMail) application was installed, enabling user authentication and communication directly from a browser within the local network. Additionally, the server provided file-sharing services through Samba. Two shared directories were created: one with read-only access and another with full read/write permissions, each configured to reflect real-world file-sharing scenarios among users.

Access to these directories was performed from Windows systems, confirming interoperability between Linux and Windows. For secure file transfer, the SFTP service was also enabled and configured, accessed from the Windows client using the WinSCP application. This allowed file access and transfer without relying on protocols.

At the security level, the UFW firewall was configured on the Ubuntu server, along with additional iptables rules. Only essential ports (such as 22 for SSH, 443 for HTTPS, and 143/25 for mail) were left open, while all other traffic was blocked. This contributed significantly to the security of available services.
Four local users were created on the server and were used for testing services such as mail, SFTP, and Samba. Each user had individual passwords and controlled access permissions.
This machine successfully simulated a real Linux server integrated into a mixed network, providing critical infrastructure services and

complementing the role of the Windows server to create a fully functional hybrid network.

Service Configuration

This section describes how the most important services in the project were configured, grouped by the three virtual machines. Each configuration is accompanied by relevant screenshots included in the final document to support the practical implementation.
On the Windows Server machine, the Active Directory Domain Services were installed and configured, with the server being promoted to Domain Controller and administrator of the domain numeforest.local. After configuration, four users and two security groups — PowerUsers and RemoteDesktopUsers — were created. Each user was added to one of these groups, and the Windows 10/11 workstation was joined to the domain to benefit from centralized authentication.
The same server also hosted the DNS service, with two forward lookup zones created for the domains numeforest.local and sj.ro, along with a reverse lookup zone. A and PTR records were manually added for each server, client, and configured site within the infrastructure, ensuring proper name resolution.
The DHCP service was enabled to automatically allocate IP addresses in the network. A dynamic IP range between 192.168.1.100 and 192.168.1.200 was defined, and the workstations in the network received valid addresses without manual intervention. Active leases in the DHCP console confirmed the correct operation of the service.
Windows Server was also configured as a file server by creating two shared directories. One of them was configured with read-only

permissions, while the other provided read/write access for privileged users. Permissions were configured both at the NTFS file system level and at the sharing level, and access was successfully tested from the Windows client.

For web hosting, IIS (Internet Information Services) was installed and configured, where three sites were created: site4.numeforest.local, site5.numeforest.local, and cgs.com. Each site was set to operate on port 443 with a self-signed SSL certificate. The websites were successfully accessed from the client workstation's browser.

Using the Group Policy Management Console, group policies were created to impose user restrictions. Access to the Control Panel and Task Manager was disabled to demonstrate the functionality of domain-level security policies. These policies were properly propagated and were visible after logging into the client workstation.

For traffic control, manual rules were defined in Windows Firewall to allow RDP (Remote Desktop) traffic, File and Printer Sharing, and HTTPS connections. Access to websites, shared folders, and remote connections was thus allowed in a controlled and secure manner.

On the Ubuntu server, both Apache and Nginx were installed, and within them, three distinct websites were created: site6.numeforest.local, sj.ro, and cgs1.com. Each site was configured in its own VirtualHost file and manually activated, protected by an SSL certificate. The sites were accessed through a browser from the Windows client workstation, confirming proper HTTPS functionality.

On the same Ubuntu server, a mail server was configured using Postfix for sending and Dovecot for receiving emails. Local users were created, and messages were tested both from the command line and through the Thunderbird application installed on Windows. In addition, the RainLoop application was installed as a webmail interface, allowing inbox access through a browser in an intuitive graphical environment.

For file sharing between Linux and Windows, Samba was used. Two shared directories were configured — one with read-only access and the other with full access. The configuration was made in the smb.conf file, and access was achieved from Windows Explorer using authentication with local Ubuntu users.

The Ubuntu server also provided secure file transfer capabilities via SFTP. Users could use the WinSCP application on the Windows workstation to upload and download files from their accounts through an encrypted connection.

The UFW firewall was activated on Ubuntu, allowing only the essential ports for the configured services to function: 22 for SSH, 443 for HTTPS, and 143/25 for mail services. Additionally, extra rules were defined in iptables for finer traffic control.

Finally, the functionality of the entire network was tested through ping between machines, DNS verification using nslookup, HTTPS testing for all six websites, email sending and receiving, as well as access to shared folders and the SFTP service.

Problems We Faced

1. The group policies (GPO) were not being properly applied on the client workstation
   After defining the group policies on the Windows server (through the Group Policy Management Console), we noticed that the configured restrictions such as disabling access to the Control Panel and Task Manager were not being reflected on the client workstation, even though it was already part of the domain. The main cause was that the domain users were not yet placed in an Organizational Unit (OU) to which the GPO policy was actually applied. After moving the user accounts into a dedicated OU and linking the GPO policy to that OU, we forced a policy refresh on the client using the command gpupdate /force. Upon the next login, the restrictions were successfully applied.

2. Configuring the Thunderbird email client was challenging
   Another difficulty arose during the configuration of the Mozilla Thunderbird application on the client workstation to connect to the mail server configured on Ubuntu. Initially, the client could not connect, returning errors related to authentication or the inability to detect the correct settings.

The issue was caused by two factors: first, the Dovecot server was not configured to accept plaintext authentication for local (non-SSL) connections; and second, Thunderbird was automatically attempting encrypted connections using invalid certificates, which triggered warnings.

The solution was to manually configure the account in Thunderbird, selecting the IMAP protocol on port 143 for receiving and SMTP on port 25 for sending, and explicitly accepting the unsigned certificate. After these adjustments, the client successfully connected to the server and was able to send and receive emails from local users.

Conclusions

Completing this project represented a valuable opportunity to apply, in a practical setting, the theoretical concepts learned during the Operating Systems course. The project involved collaboration among three members, each actively contributing to the configuration and testing of the services distributed across the three virtual machines: Windows client, Windows server, and Ubuntu server.

Teamwork was essential for dividing responsibilities, cross-verifying configurations, and efficiently solving issues encountered along the way.
Through joint effort, we successfully configured a functional and realistic network infrastructure that included essential services such as Active Directory, DNS, DHCP, GPO, File Sharing, Web Hosting, Mail Server, Samba, and SFTP. The integration of Windows and Linux components into a coherent network provided a clear understanding of how a complete

enterprise network is built and managed.

The challenges encountered during the process were addressed collaboratively, with each member contributing ideas and solutions, leading to more effective and applied learning. In the end, the project not only strengthened our technical knowledge but also developed essential teamwork, communication, and coordination skills.