Zurigo 06.12.2024

Esercizio di oggi:

Creazione di Gruppi in Windows Server 2022

Obiettivo

Lo scopo di questo esercizio è di familiarizzare con la gestione dei gruppi di utenti in Windows Server 2022.

Imparerai a

-creare gruppi,

-assegnare loro permessi specifici,

-comprendere l'importanza della gestione dei gruppi per la sicurezza e l'amministrazione del sistema.

Today's exercise:

Creating Groups in Windows Server 2022

Objective

The purpose of this exercise is to familiarize you with managing user groups in Windows Server 2022.

You will learn to

-create groups,

- assign them specific permissions,

-understand the importance of group management for system security and administration.

As required by today's exercise we will create working groups with Windows Server 2022 in the Epicode.local Forest (this is the name of the forest domain).

1. Introduction Page1
2. Creating groups and users Page4
3. Creating a folder to share giving proper permissions Page6
4. Check that everything is working properly Page11
5. Conclusions Page14

1.Introduction

Windows Server 2022 and Active Directory: A Brief Overview

Windows Server 2022, the latest in Microsoft's server operating system line, offers a robust platform for managing network resources. One of its core components is **Active Directory**, a directory service that provides a centralized database for storing information about network objects, including users, computers, groups, and other resources.

Active Directory Groups: The Foundation of Permissions

Active Directory groups are collections of users, computers, or other security principals that share common attributes or require access to the same resources. These groups are the cornerstone of permissions management within an Active Directory environment.

By assigning permissions to groups rather than individual users, administrators can streamline the management of access control. When a user needs to be granted access to a specific resource, they are simply added to the appropriate group. This approach offers several advantages:

- **Efficiency:** Changes to permissions can be made quickly by modifying group membership, rather than updating individual user permissions.
- **Security:** By using groups, organizations can implement the principle of least privilege, ensuring that users only have the access they need to perform their job functions.
- **Scalability:** As an organization grows, groups can be easily created and managed to accommodate new users and resources.

The Role of Active Directory Groups in Security

Active Directory groups play a **critical role** in **enhancing security** within an organization. Here are some key ways they contribute to a secure environment:

- **Access Control:** By defining granular permissions for groups, administrators can control who has access to specific resources, such as files, folders, network shares, and applications.
- **Authentication:** Groups can be used to authenticate users for various services, including network login, remote access, and application access.

- **Auditing:** Active Directory provides detailed audit logs that track changes to group membership and permissions, making it easier to identify and investigate security incidents.
- **Delegation of Control:** Administrators can delegate control over specific resources to groups, allowing them to manage permissions without granting full administrative privileges.

Best Practices for Using Active Directory Groups

- **Create specific groups:** Develop a clear naming convention for groups and create groups based on roles, departments, or projects.
- **Limit group membership:** Avoid adding users to multiple groups unless it is absolutely necessary.
- **Regularly review group memberships:** Periodically review group memberships to ensure that users still require access to the resources associated with the group.
- **Utilize nested groups:** Create nested groups to simplify permissions management and reduce the number of groups required.
- **Implement strong password policies:** Enforce strong password policies to protect user accounts and prevent unauthorized access.
- **Regularly audit group membership:** Conduct regular audits of group membership to identify and address any security risks.

By effectively leveraging Active Directory groups, organizations can improve security, streamline administration, and enhance overall system management.

How is Active Directory organised? The Forest Structure

Understanding the Forest Structure in Active Directory

A forest in Active Directory is a logical grouping of one or more domains. It serves as a boundary for security, administration, and replication. A forest is the top-level container in the Active Directory hierarchy.

Why use a forest?

- Isolation: Multiple forests can be used to isolate different organizational units or business units. This provides enhanced security and allows for independent management.
- Scalability: Forests can be scaled independently, making it easier to manage large organizations.
- Organizational Structure: The forest structure can be aligned with the organizational structure of the company.

Key Components of a Forest

- Domain: A domain is a logical grouping of users, computers, and other objects. It's the basic unit of organization within a forest.
- Tree: A tree is a collection of one or more domains that share a common root domain.
- Forest: The top-level container that encompasses one or more trees.

Trust Relationships

To enable communication and resource sharing between domains in different forests, trust relationships can be established. These trust relationships determine how objects in one domain can access resources in another domain.

Types of Trust Relationships:

- Forest Trust: A trust relationship between two forests.
- Domain Trust: A trust relationship between two domains within the same forest or across different forests.

Important Considerations for Forest Design:

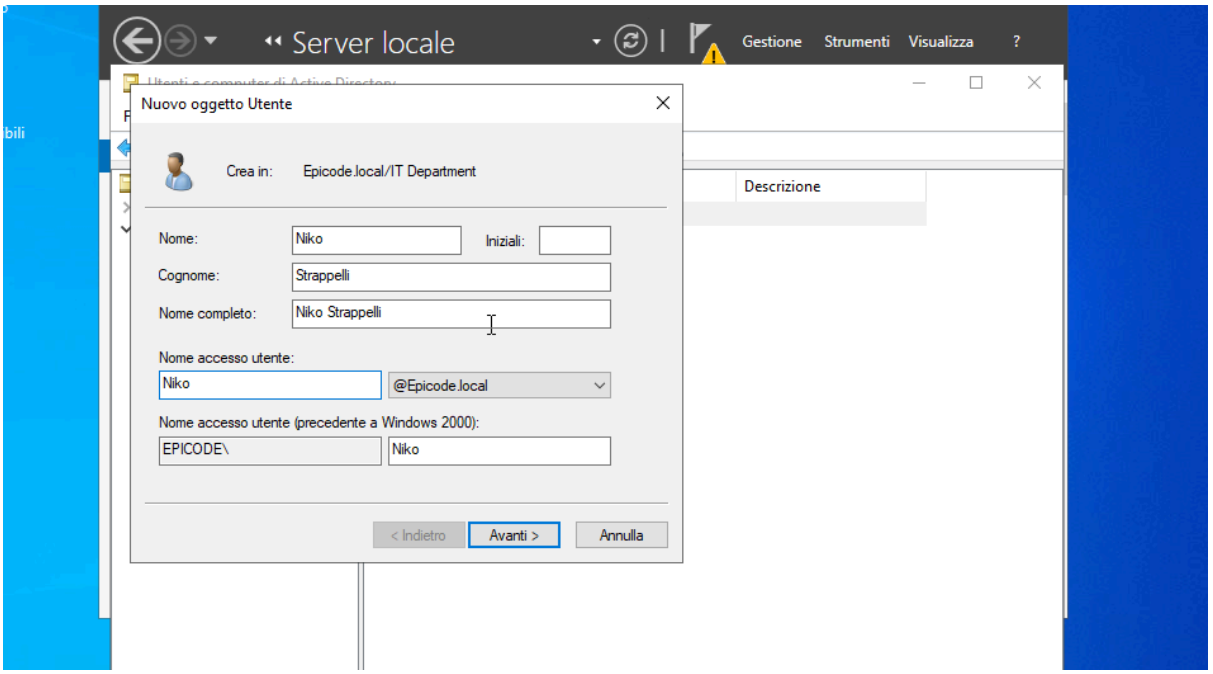
- **Security:** Consider the security implications of creating multiple forests. Each forest is a separate security boundary.
- **Management:** Managing multiple forests can be complex. Ensure you have adequate resources and expertise.
- **Cost:** Additional forests may require additional hardware and software licenses.
- **Performance:** The performance of your Active Directory environment can be impacted by the number of forests and domains.
- **Replication:** Configure replication between domain controllers in the forest to ensure data consistency.

In Conclusion

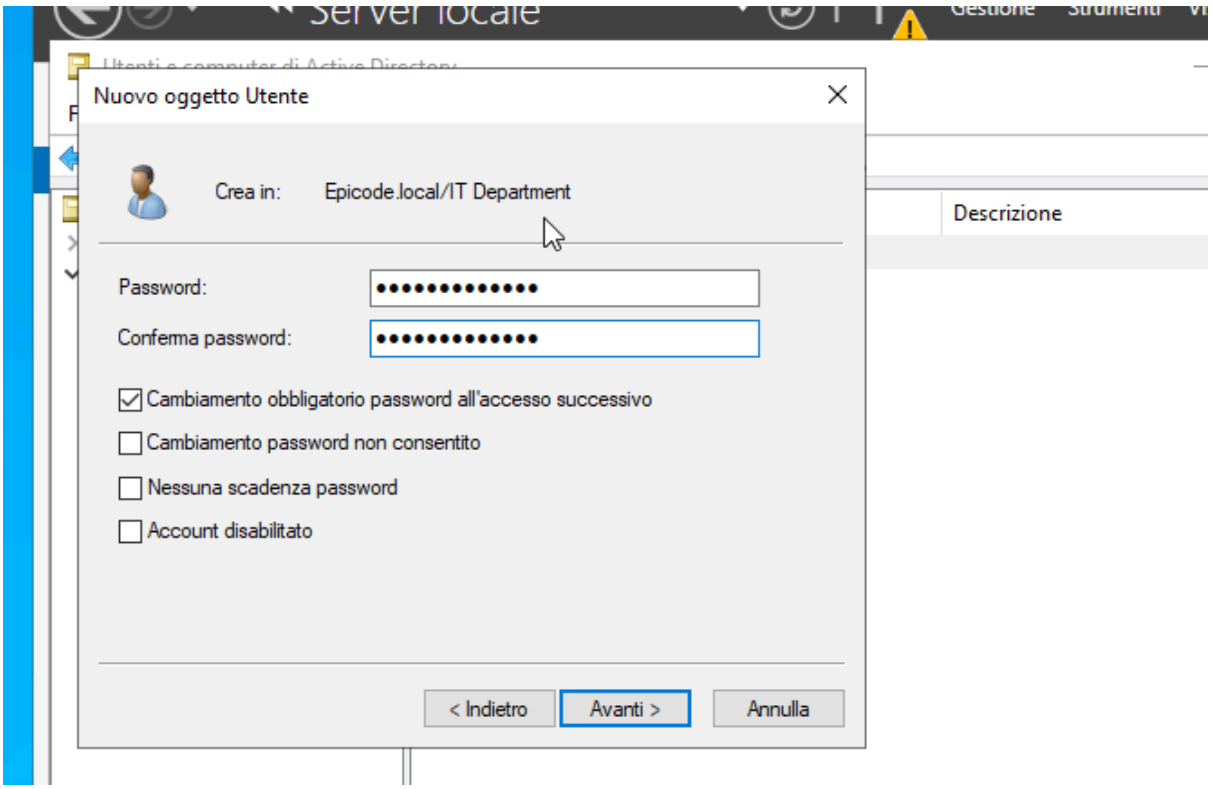
Understanding the forest structure is crucial for designing and managing a complex Active Directory environment. By carefully planning and configuring your forest, you can ensure optimal security, scalability, and performance for your organization.

2.Creating Groups and Users

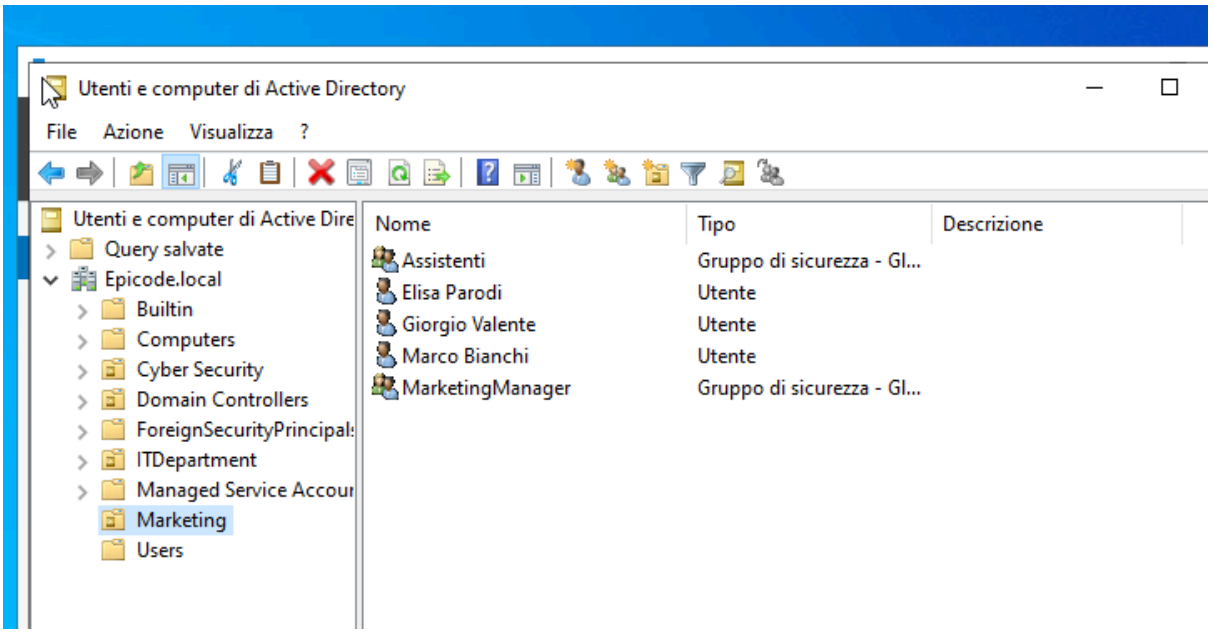
We start navigating into the Active Directory menù and we start to add a new user.



We need to setup a password for the new user; this one will be an easy one: that's the one the user we'll user for his/her first access and he/she needs to change as soon as the first access is done (we must be sure to select the change password option at the next login)



Of course for the exercise I've created more users and also I created few groups.



Let's have a deep view at the Marketing tree.
We have:

- Giorgio Valente — Marketing Manager — Part of MarketingManager group
- Elisa Parodi — Marketing assistant — Part of Assistenti group
- Marco Bianchi — Marketing assistant — Part of Assistenti group

3.Creating a folder to share giving proper permissions

I created a new folder on the Desktop shared with “Everyone” on the domain.

The "Everyone" option in various contexts, such as file permissions, group memberships, or application settings, serves a fundamental purpose: **to grant universal access**. It's a convenient way to make resources available to all users within a specific system or network.

Why the "Everyone" option is useful?

1. Simplifying Access:

- **Default permissions:** In many systems, "Everyone" is often assigned default permissions, such as read-only access to public files or folders. This simplifies file sharing and reduces the need for granular permissions for every user.
- **Public resources:** For resources that are intended for public consumption, such as shared documents or websites, granting "Everyone" access ensures broad availability.

2. Streamlining Administration:

- **Reducing overhead:** By using "Everyone" for general access, administrators can save time and effort in managing individual user permissions.
- **Consistency:** It provides a consistent level of access for all users, simplifying the management of permissions.

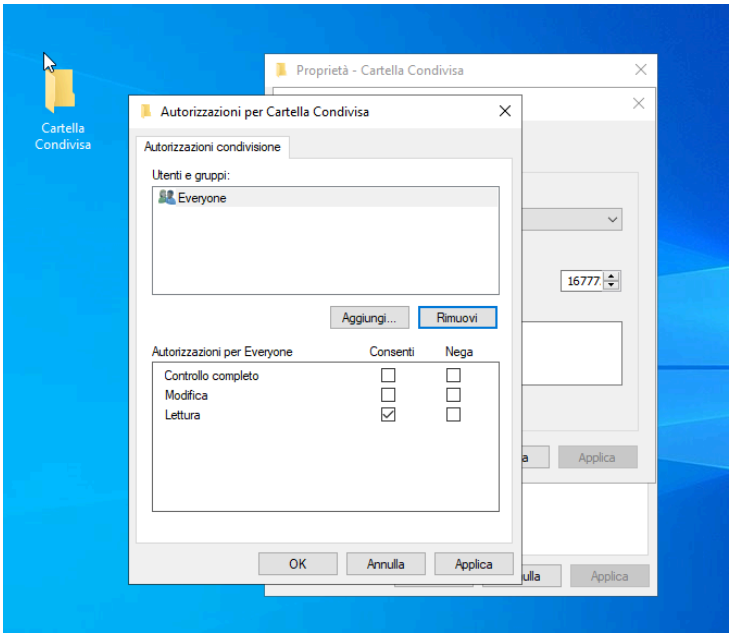
3. Flexibility:

- **Customizing permissions:** While "Everyone" provides a broad level of access, it can be combined with more specific permissions to fine-tune access control. For example, you might grant "Everyone" read-only access to a folder, but give specific users write permissions.

However, it's important to use the "Everyone" option judiciously:

- **Security risks:** Granting broad access to everyone can potentially compromise security. Be cautious when using "Everyone" and consider the potential risks.
- **Performance impact:** In large-scale systems, granting "Everyone" access to many resources can impact performance.
- **Clarity and organization:** Overusing "Everyone" can make it difficult to manage permissions and understand who has access to what.

In conclusion, the "Everyone" option is a valuable tool for simplifying access control, but it should be used thoughtfully and with an understanding of the potential security implications.

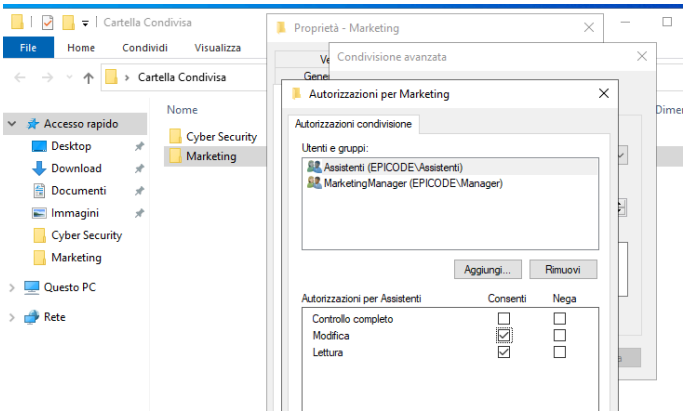


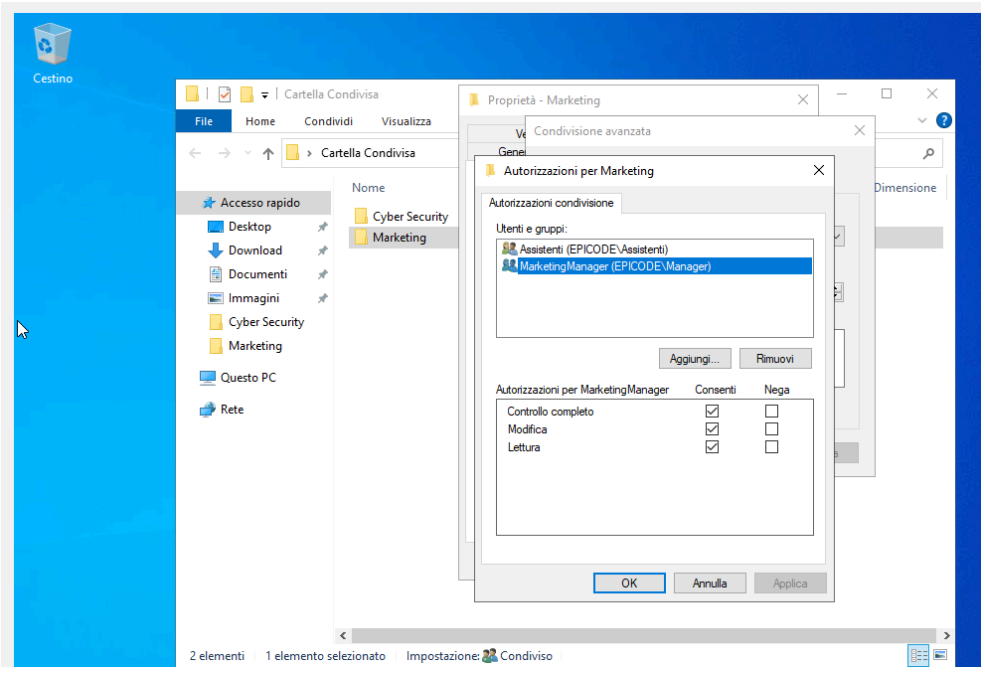
I will share this folder with “everyone” only in “read” options - every user can get access to it and I’ll setup more different sharing options later.

The sharing options in Active Directory are parental.

Inside the folder “Cartella Condivisa” I created two new folders named “Marketing” and “Cyber Security”.

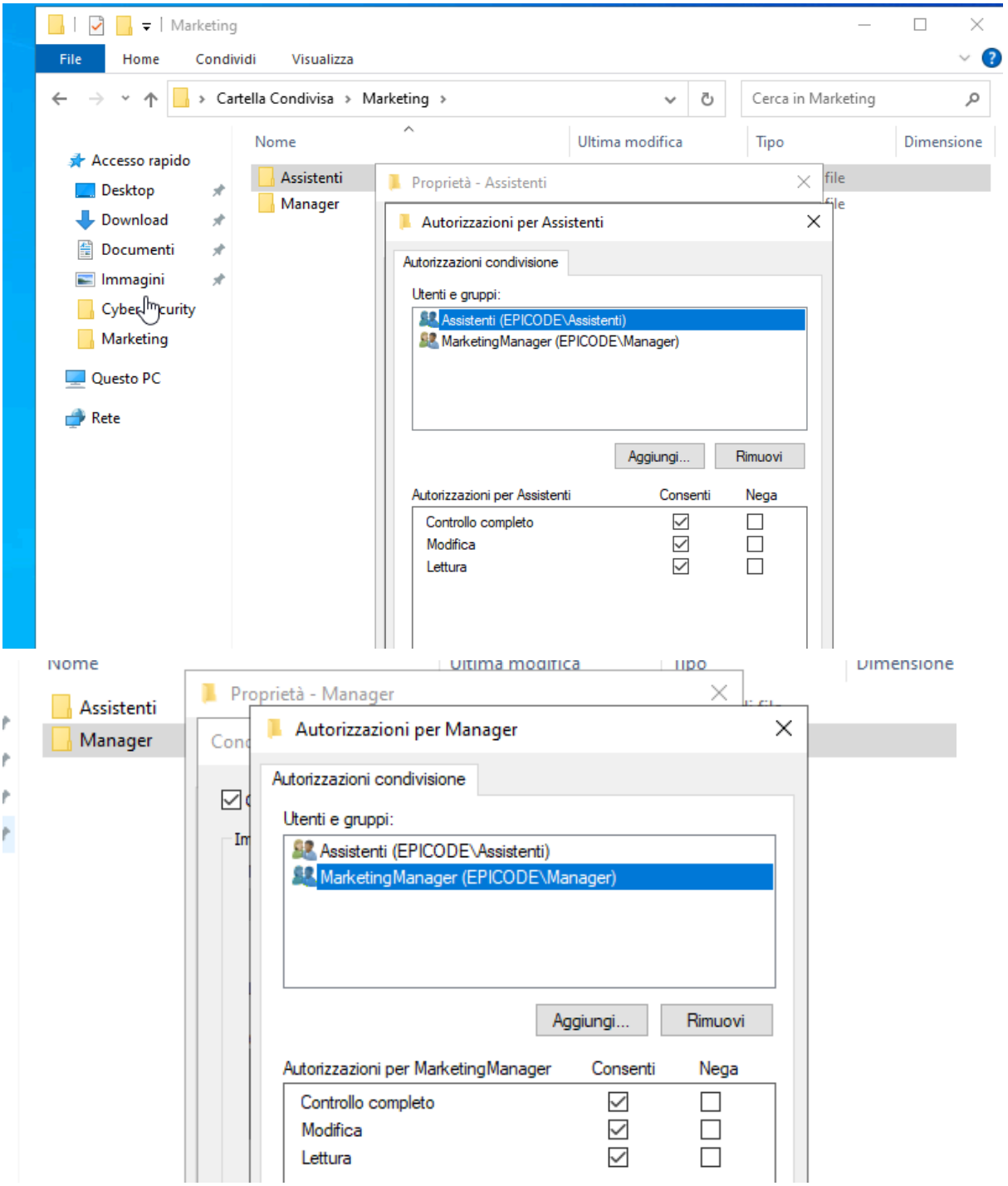
Let’s focus on the Marketing one.
When it comes about sharing options I gave to the MarketingManager group (of which Mr.Valente - marketing manager is part) full privileges or total control and I gave to the Assistenti group (of which Mrs.Parodi and Mr.Bianchi are part as they are assistent) only the read and modify option without giving them full access.

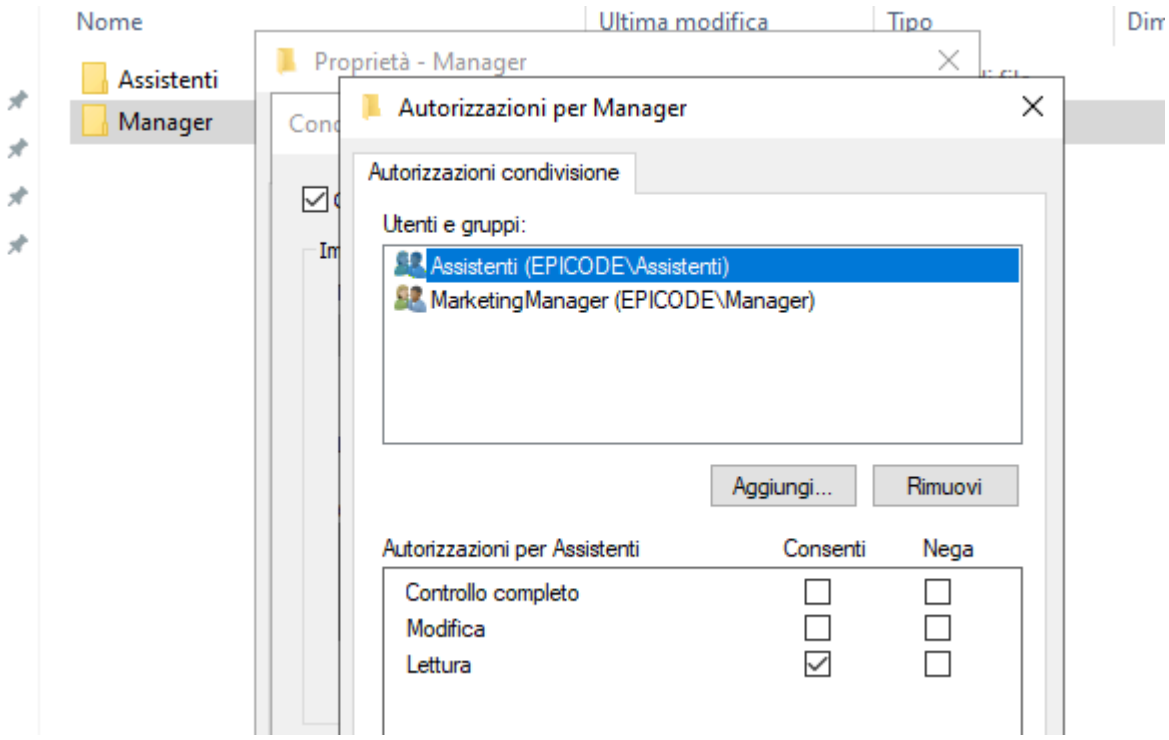




As we go deeper in this folder we’re gonna find two new folders:

- Assistenti (assistenti group has full control of it; of course also the marketingmanager group)
- Manager (in this case onlu the group marketing manager has fully access to the folder)


Marketing
File
Home
Condividi
Visualizza
Cartella Condivisa › Marketing ›
Cerca in Marketing
Accesso rapido
Desktop
Download
Documenti
Immagini
Cybersecurity
Marketing
Questo PC
Rete
Nome
Ultima modifica
Tipo
Dimensione
Assistenti
Manager
Proprietà - Assistenti
Autorizzazioni per Assistenti
Autorizzazioni condivisione
Utenti e gruppi:
Assistenti (EPICODE\Assistenti)
MarketingManager (EPICODE\Manager)
Aggiungi...
Rimuovi
Autorizzazioni per Assistenti
Consenti
Nega
Controllo completo
Modifica
Lettura
Proprietà - Manager
Autorizzazioni per Manager
Autorizzazioni condivisione
Utenti e gruppi:
Assistenti (EPICODE\Assistenti)
MarketingManager (EPICODE\Manager)
Aggiungi...
Rimuovi
Autorizzazioni per MarketingManager
Consenti
Nega
Controllo completo
Modifica
Lettura



I'm gonna explain a little bit better how everything is working in Active Directory.

Understanding File and Folder Permissions in Active Directory

File and folder permissions in Active Directory are crucial for controlling access to resources within a Windows domain. These permissions determine who can read, write, execute, or modify files and folders.

Key Permission Types:

- **Read:** Allows users to view the contents of a file or folder.
- **Write:** Allows users to modify the contents of a file or create new files and folders.
- **Execute:** Allows users to run executable files or access directories.
- **Full Control:** Grants complete control over a file or folder, including all of the above permissions.

Assigning Permissions:

- **Users and Groups:** Permissions can be assigned to individual users or groups of users.
- **Inheritance:** Permissions can be inherited from parent objects to child objects, creating a hierarchical structure.

- **Effective Permissions:** The effective permissions of a user are determined by combining the permissions granted directly to the user and the permissions inherited from groups to which the user belongs.

Best Practices for Assigning Permissions:

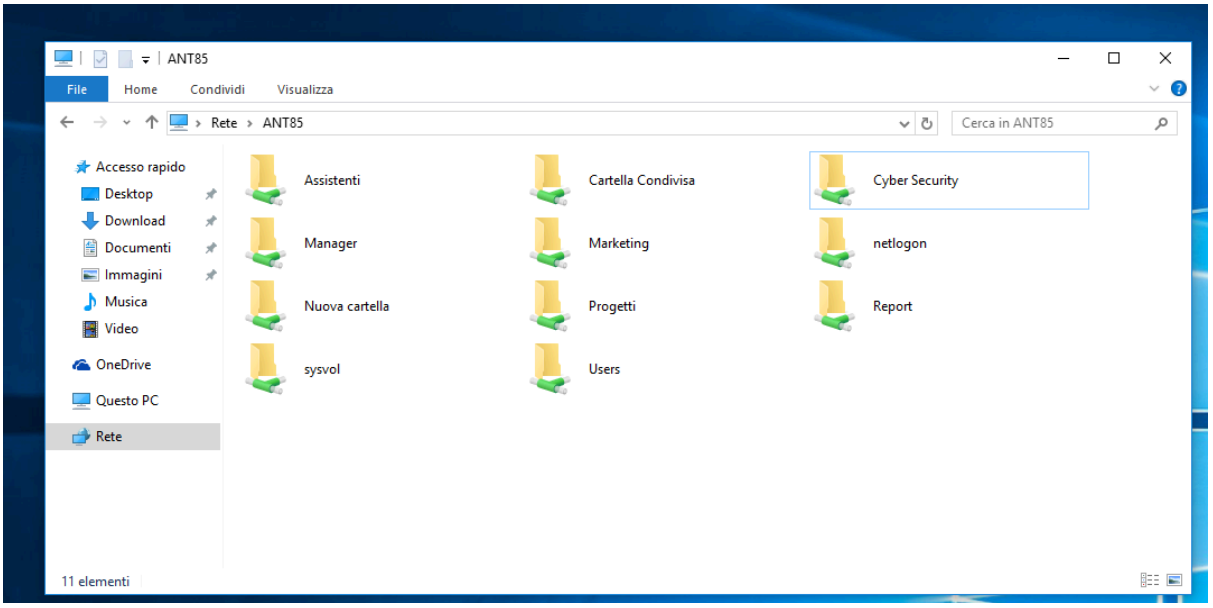
- **Principle of Least Privilege:** Grant users only the minimum permissions necessary to perform their tasks.
- **Regular Review:** Periodically review and update permissions to ensure they are still appropriate.
- **Use Groups:** Assign permissions to groups instead of individual users to simplify management.
- **Consider Security Risks:** Be mindful of the security implications of granting broad permissions.
- **Document Permissions:** Maintain clear documentation of permissions and their rationale.

By understanding and effectively managing file and folder permissions in Active Directory, you can protect sensitive data and ensure that users have the appropriate access to resources.

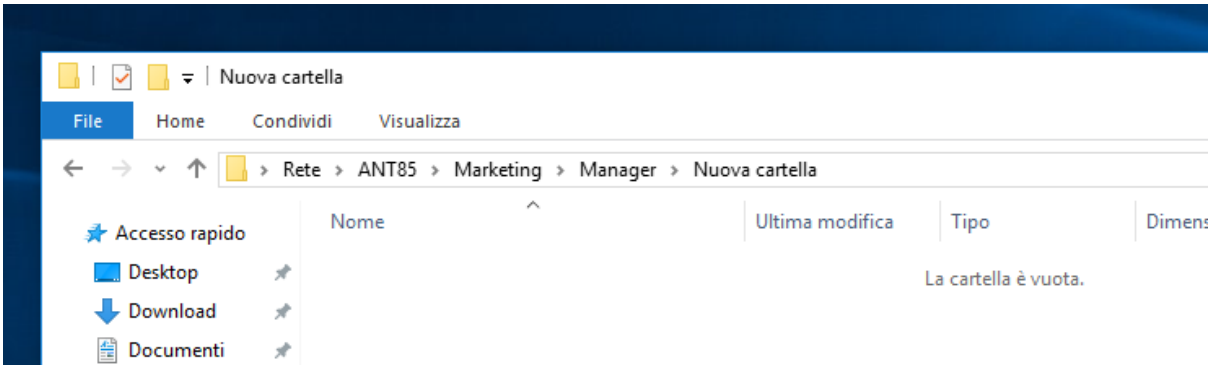
4.Check that everything is working properly

We access a remote computer connected to the domain server that we created on Windows Server 2022 (I called it Epicode.local) with the User Giorgio Valente - he's the Marketing Manager and he has fully access to the Marketing folder.

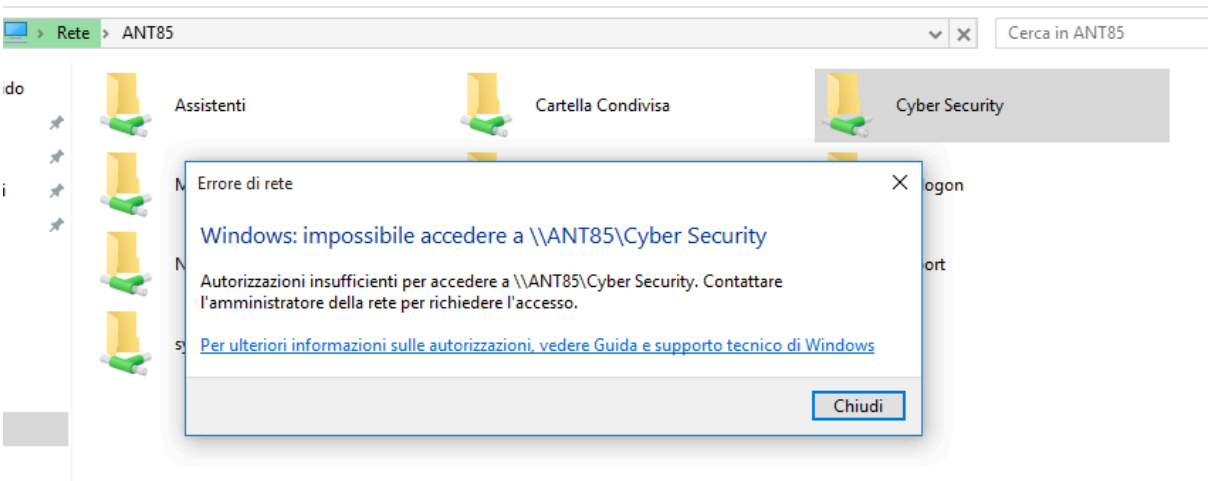
We run "\\ANT85.Epicode.local" on the Run dialog box and we can access to the domain and Giorgio gets this:



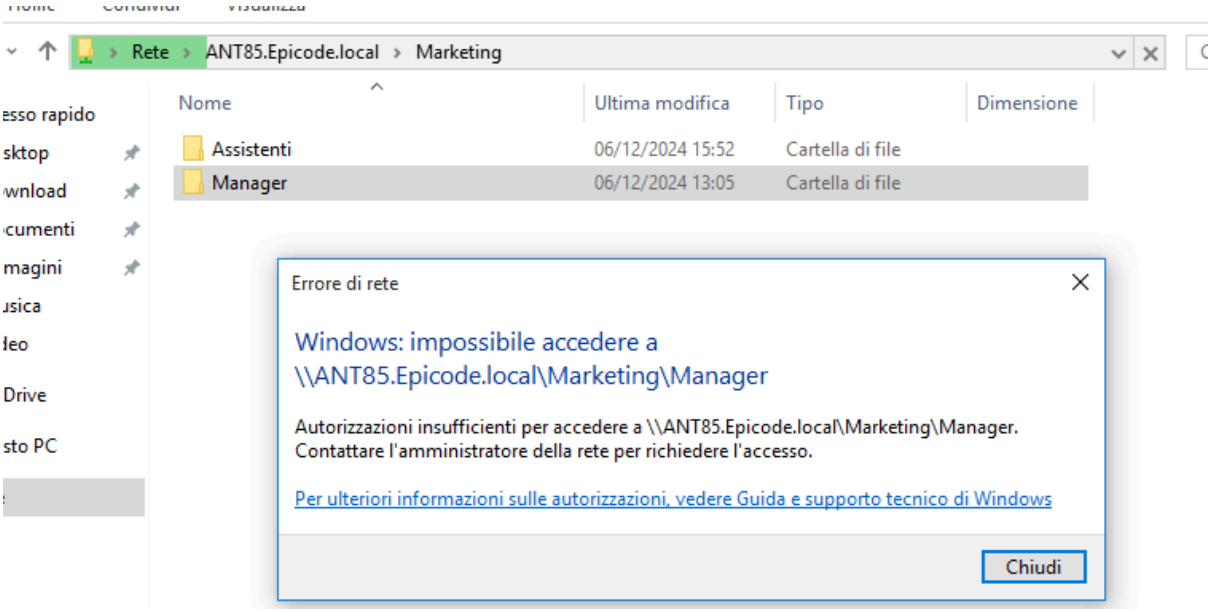
He can navigate through every folder in the Marketing main folder.



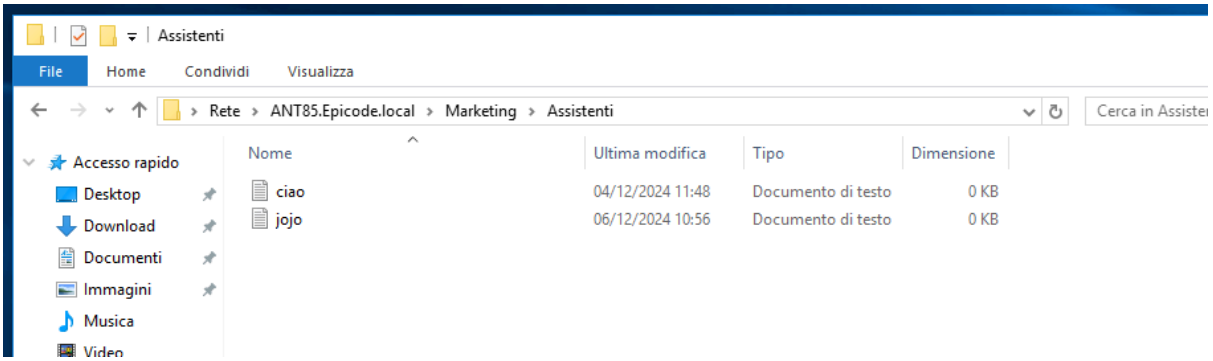
But he cannot get access to the folder Cyber Security because I didn't give him any access.



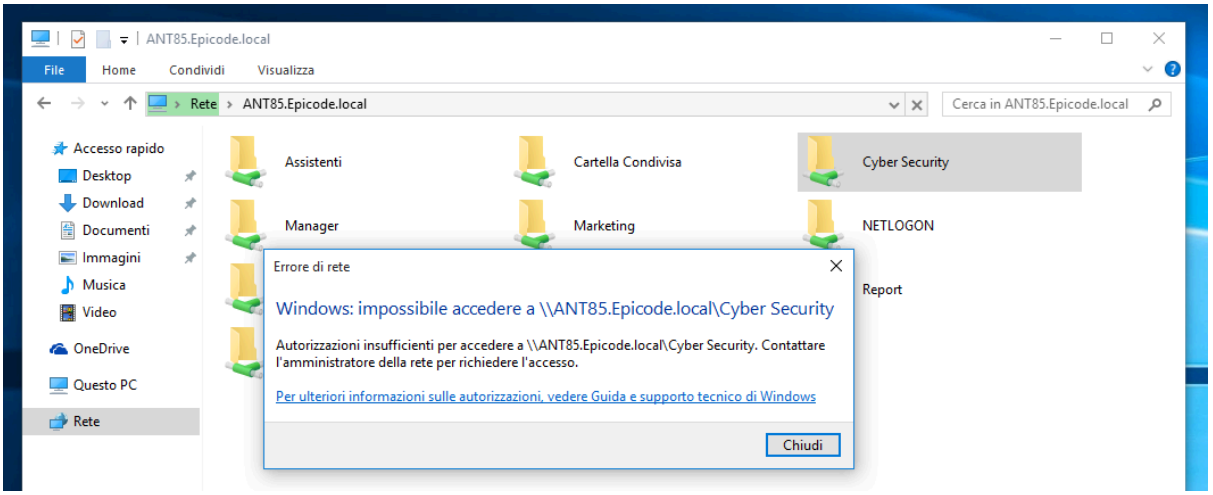
Now we get the access with the user Marco (just as a reminder - he's a marketing assistant). Technically he can access the Marketing folder but not the sub-folder Manager.



According to the picture everything is working as planned and just to have one more confirm he should be able to access the folder Assistenti.



And he’s in - it means that I was giving permissions in the right way.
Just as a final confirmation I was trying to navigate into the Cyber Security folder and he got no access (as it should be).



4.Conclusions

The Importance of User Management and Privileges in Windows Server 2022

In today's complex IT landscape, effective user management and privilege control are crucial to ensure the security and integrity of Windows Server 2022 environments. By implementing robust user management strategies, organizations can mitigate risks, enhance system security, and maintain operational efficiency.

Why User Management Matters

- **Security:**
  - **Limiting Access:** By assigning specific privileges to users, you can restrict access to sensitive resources, reducing the risk of unauthorized access and data breaches.
  - **Detecting Anomalies:** Monitoring user activity can help identify suspicious behavior and potential security threats.
- **Compliance:**
  - **Regulatory Requirements:** Many industries have strict compliance standards that require specific user management practices.
  - **Auditing:** Proper user management enables effective auditing and reporting, ensuring compliance with regulatory requirements.
- **Efficiency:**
  - **Streamlined Administration:** By managing users and groups efficiently, administrators can save time and reduce the risk of errors.
- **Disaster Recovery:**
  - User accounts and permissions are essential for restoring access to systems and data after a disaster.

Key Principles of User Management

- **Least Privilege Principle:** Grant users only the minimum privileges necessary to perform their tasks. This helps to minimize the potential impact of a security breach.
- **Role-Based Access Control (RBAC):** Assign permissions based on roles rather than individual users. This simplifies administration and reduces the risk of errors.
- **Regular Review and Auditing:** Regularly review user accounts and permissions to ensure they are still valid and necessary.
- **Strong Password Policies:** Enforce strong password policies to protect user accounts from unauthorized access.
- **Multi-Factor Authentication (MFA):** Implement MFA to add an extra layer of security.
- **User Account Control (UAC):** Use UAC to elevate privileges when necessary, reducing the risk of unauthorized actions.

By following these principles and leveraging the robust features of Windows Server 2022, organizations can establish a secure and efficient user management framework.

Understanding Role-Based Access Control (RBAC)

RBAC is a security model that assigns permissions to users based on their roles within the organization. In Active Directory, you can create groups and assign permissions to those groups. By adding users to specific groups, you can grant them the necessary permissions to perform their tasks.

Benefits of RBAC:

Improved Security:

By limiting user privileges to the minimum necessary, you can reduce the risk of unauthorized access and data breaches.

Simplified Administration:

Centralized management of user permissions through group policies.

Scalability:

Easily add or remove users from groups as needed.

Compliance:

Helps to meet compliance requirements by ensuring that only authorized users have access to sensitive information.

By understanding these roles and effectively implementing **RBAC**, you can create a secure and efficient Active Directory environment.

Thank you,

Antonio Bevilacqua