Unità 3 S10-L5

Data: 28 Novembre 2025

Alessandro Pietro Salerno

Report di Laboratorio: Configurazione e Sicurezza di Windows Server 2022

Oggetto: Esercitazione pratica su Active Directory, Gestione Permessi (ACL) e Group Policy (GPO).

Introduzione

In questa esercitazione ho affrontato la configurazione completa di un ambiente aziendale simulato basato su **Windows Server 2022**. L'obiettivo era passare da una macchina virtuale "nuda" a un'infrastruttura IT governata, sicura e centralizzata.

Per comprendere appieno le operazioni svolte, è necessario richiamare alcuni concetti teorici fondamentali che ho applicato:

- **Active Directory Domain Services (AD DS):** È il cuore pulsante della rete. Funge da database centralizzato che contiene e gestisce tutte le risorse (utenti, computer, stampanti). Senza AD, ogni computer sarebbe un'isola ingestibile.
- **Foresta e Dominio:** La Foresta è il contenitore logico più alto in AD, che racchiude uno o più Domini. Il Dominio è un confine di sicurezza amministrativa. Nel mio caso, ho creato una nuova foresta con un singolo dominio radice.
- **RBAC (Role-Based Access Control):** È il principio di assegnare i permessi ai *ruoli* (gruppi) e non alle singole

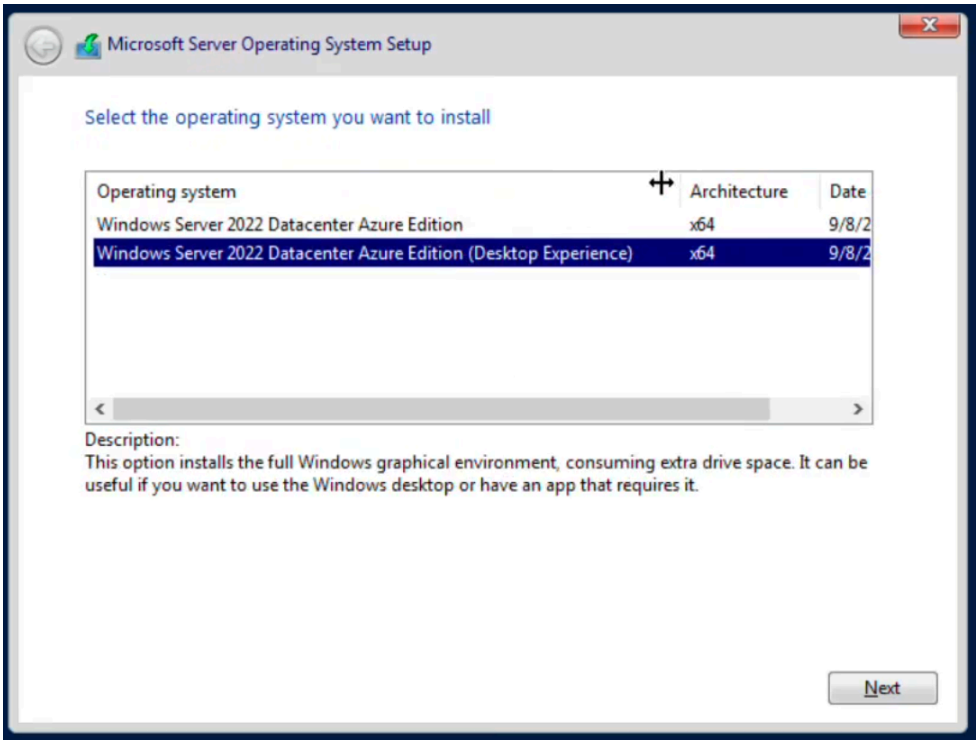
persone. Questo garantisce scalabilità: se un dipendente cambia ruolo, basta spostarlo di gruppo senza dover riconfigurare decine di cartelle.

- **Principio del Privilegio Minimo:** Regola fondamentale della sicurezza: un utente deve avere **solo** i permessi strettamente necessari per svolgere il suo lavoro, e niente di più.

Configurazione dell'Infrastruttura

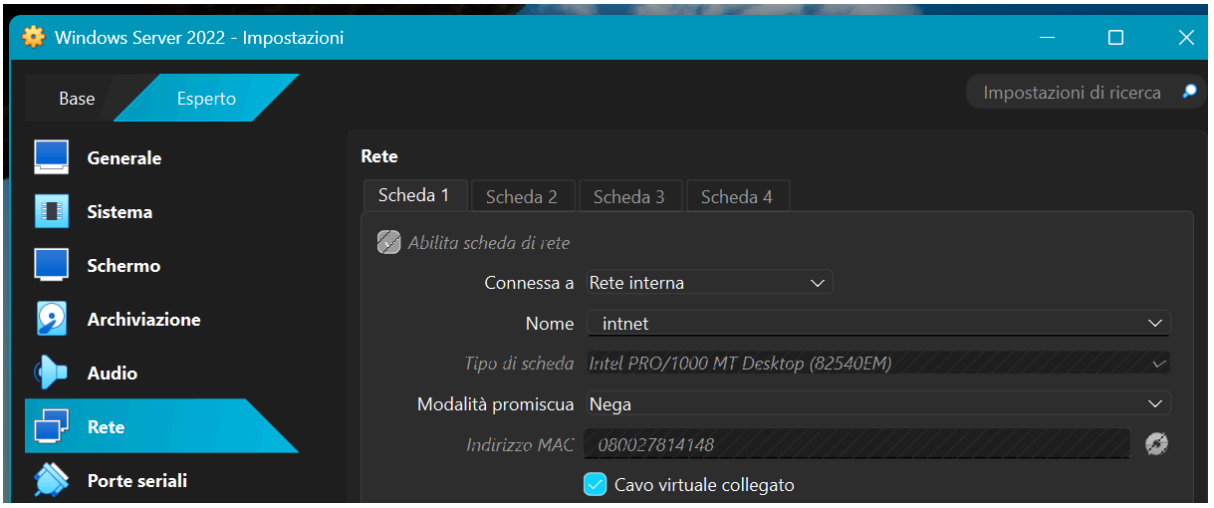
Preparazione del Server

Ho iniziato importando l'immagine ISO di Windows Server 2022 su VirtualBox. Durante l'installazione, ho scelto la versione con **Desktop Experience** per avere l'interfaccia grafica, essenziale per un apprendimento visivo.

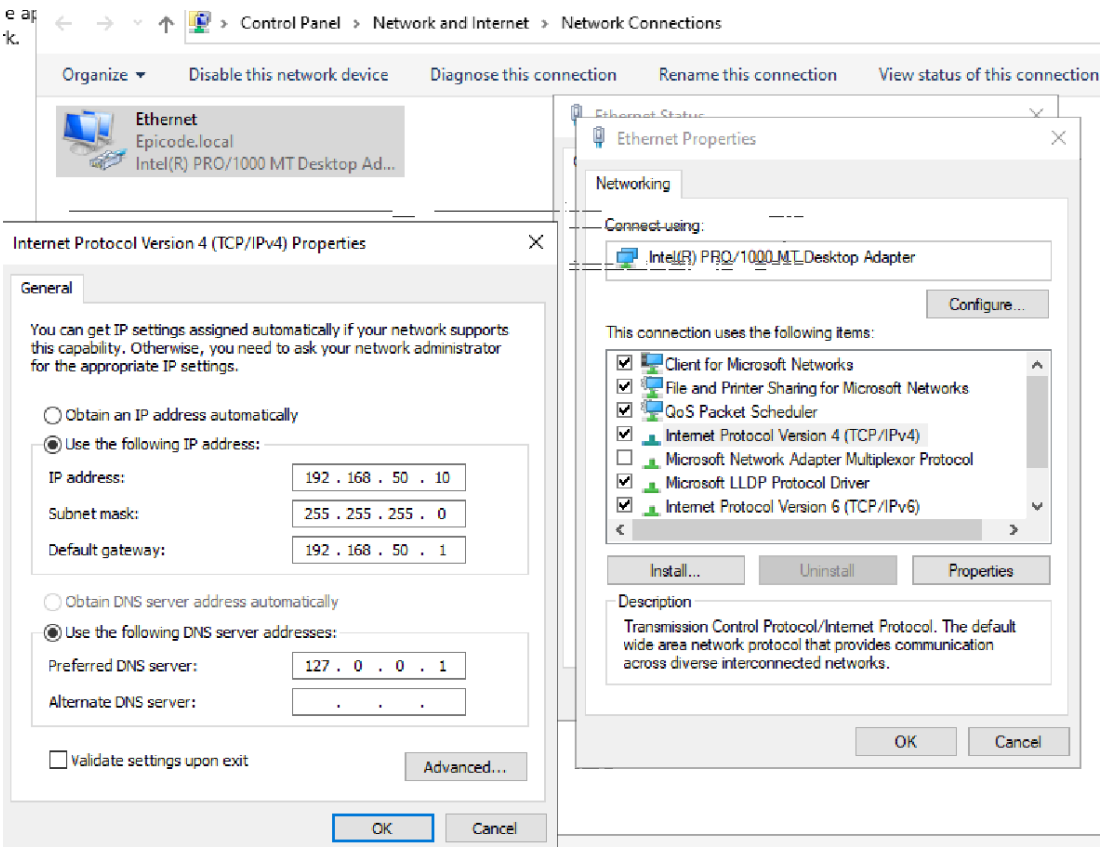


Dopo l'installazione, ho eseguito passaggi critici per la stabilità:

1. **Installazione Guest Additions:** Per garantire fluidità, risoluzione dello schermo corretta e integrazione mouse/tastiera con il mio PC ospite.
2. **Configurazione di Rete:** Ho impostato la scheda di rete su "Rete Interna" per isolare il laboratorio.

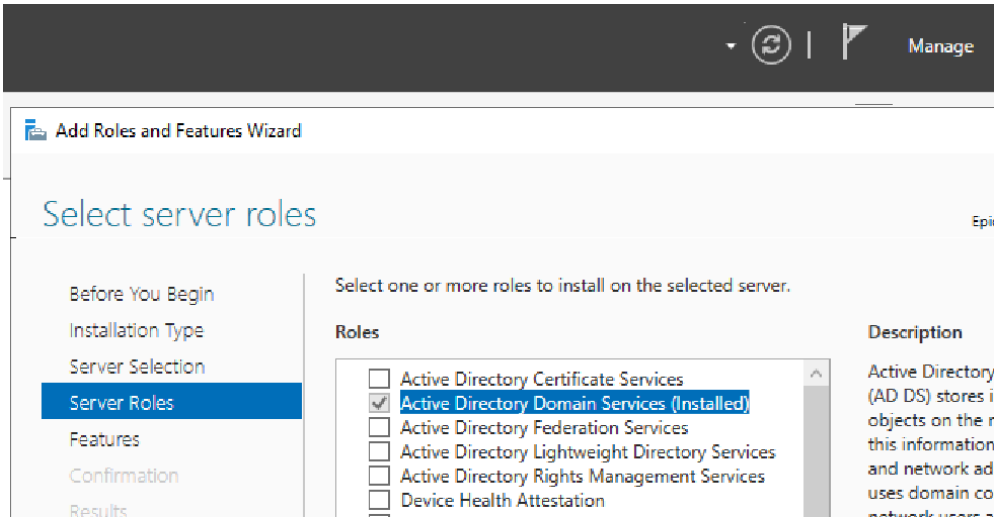


Ho assegnato un **IP Statico** al server (192.168.1.106) e, punto cruciale, ho impostato il **DNS Server** su 127.0.0.1 (localhost). Questo perché il server, una volta diventato Domain Controller, deve interrogare se stesso per risolvere i nomi della rete.

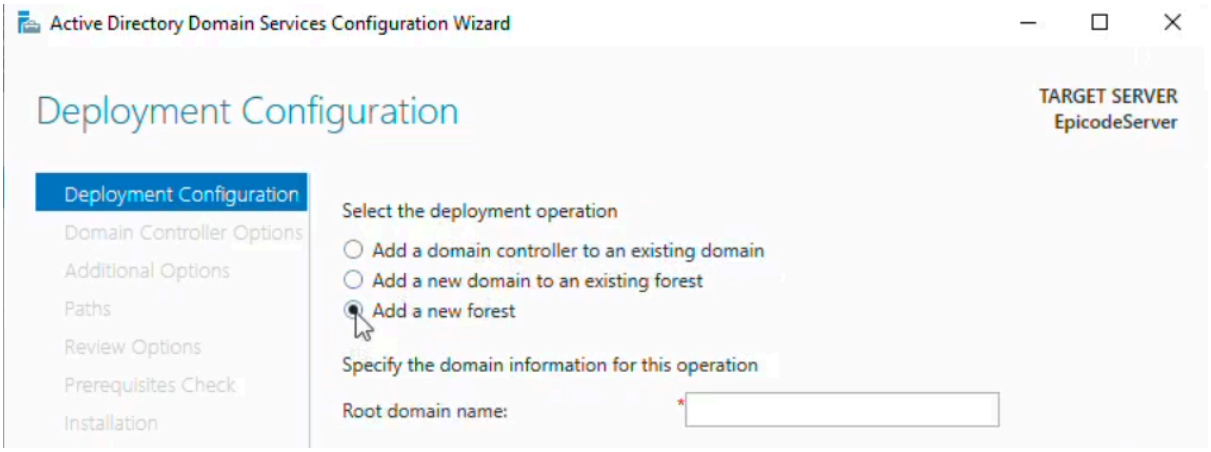


Promozione a Domain Controller

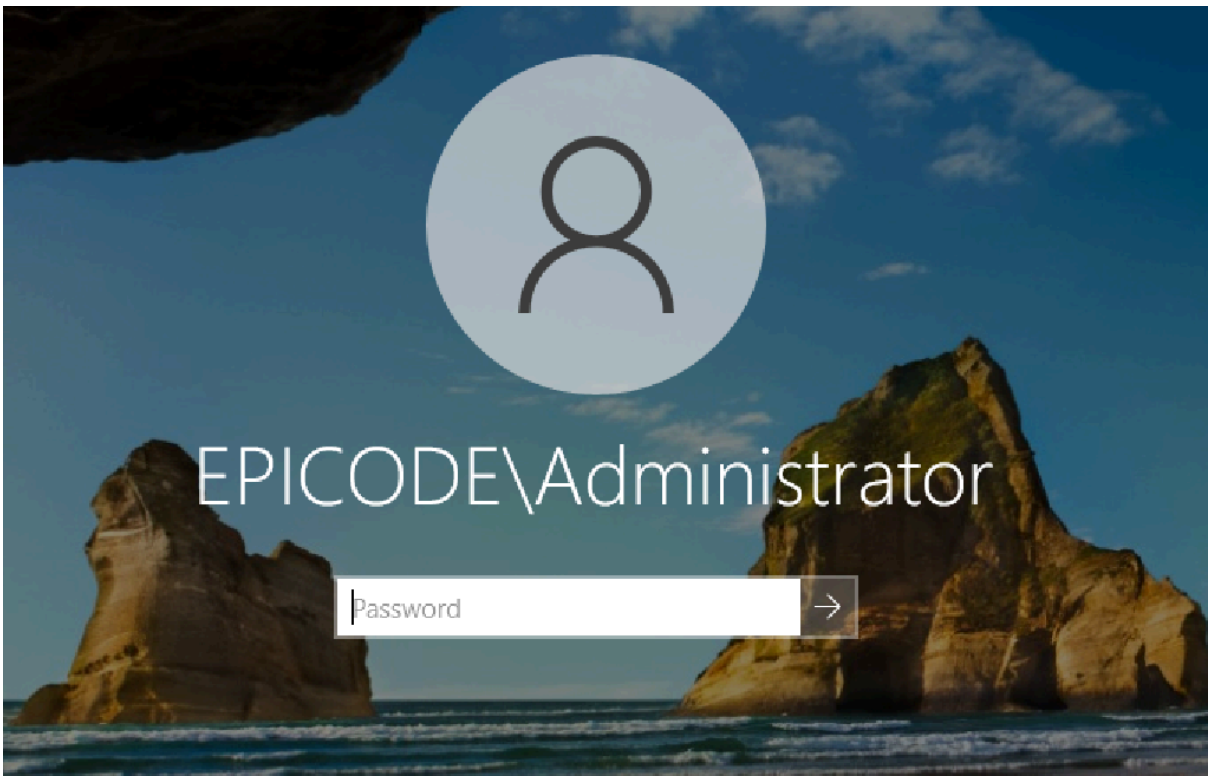
Tramite il *Server Manager*, ho aggiunto il ruolo **Active Directory Domain Services**.



Successivamente, ho promosso il server a Domain Controller creando una nuova foresta denominata **Epicode.local**.



Ho impostato una password sicura per la modalità di ripristino (DSRM) e completato la configurazione. Al riavvio, il login è cambiato in EPICODE\Administrator, confermando che il server ora gestisce un dominio.



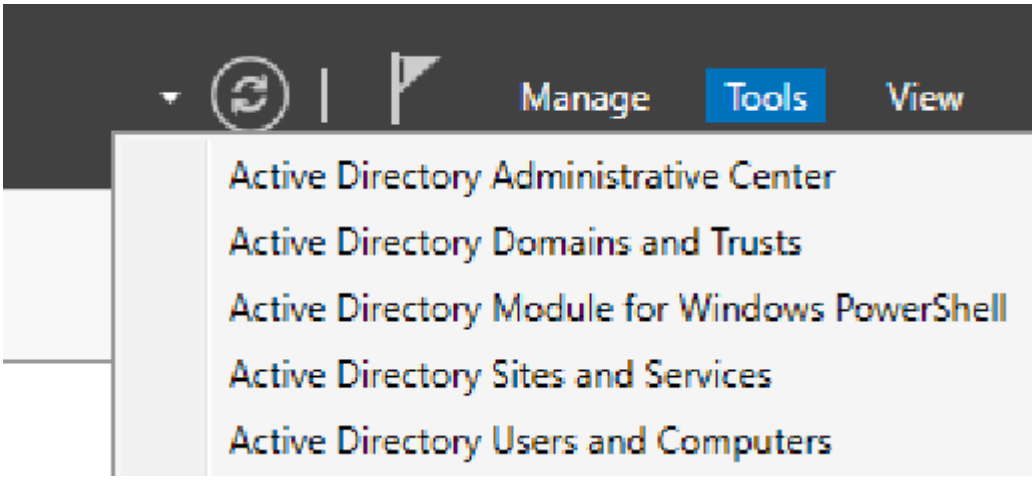
Gestione Identità e Accessi (IAM)

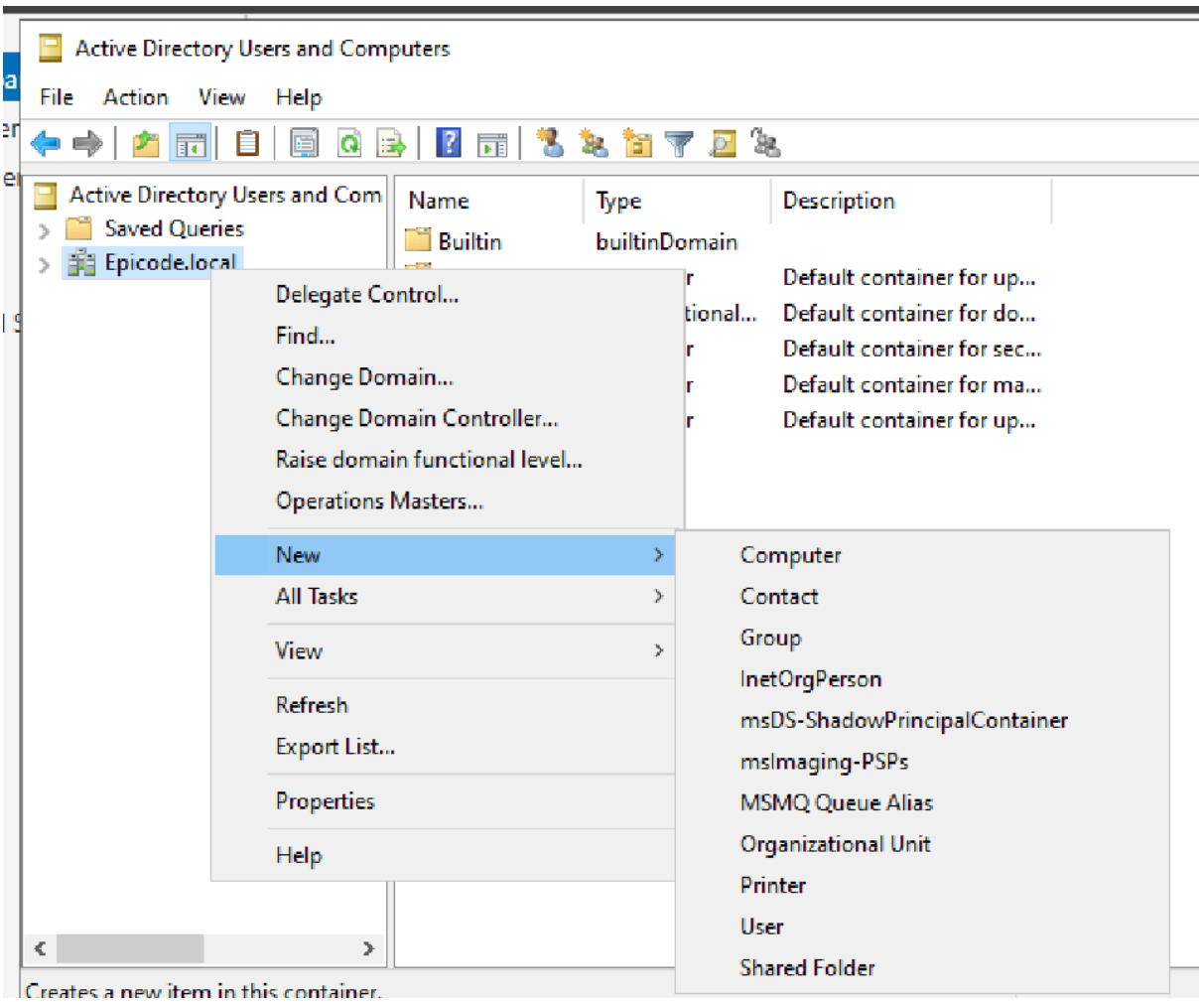
Non volendo un dominio disordinato, ho strutturato le risorse gerarchicamente.

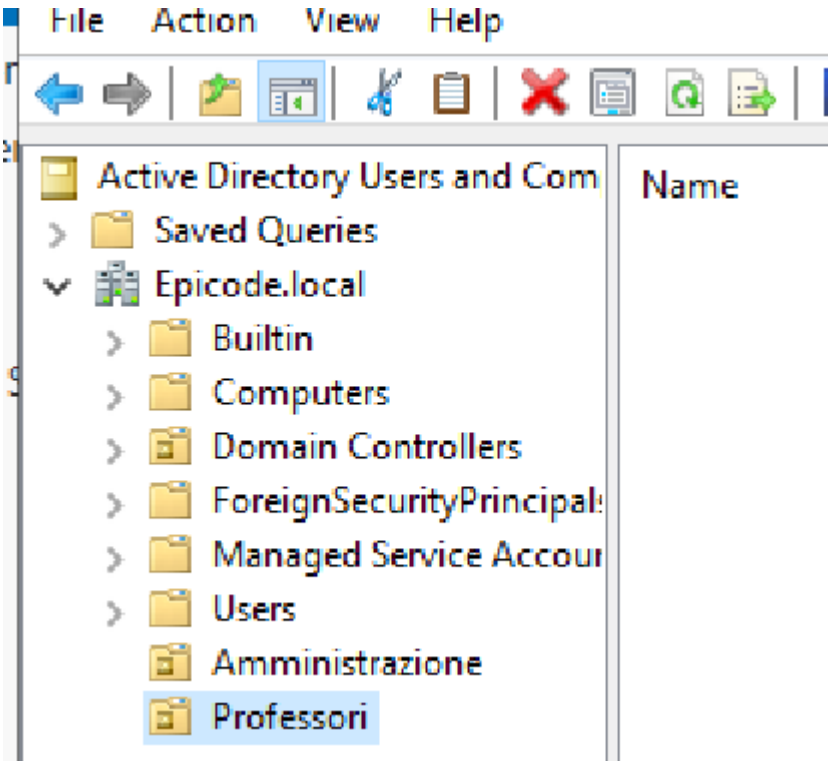
Creazione delle Unità Organizzative (OU)

Ho aperto lo strumento *Active Directory Users and Computers* e ho creato due contenitori logici (OU) per separare i dipartimenti:

- **Amministrazione**
- **Professori**

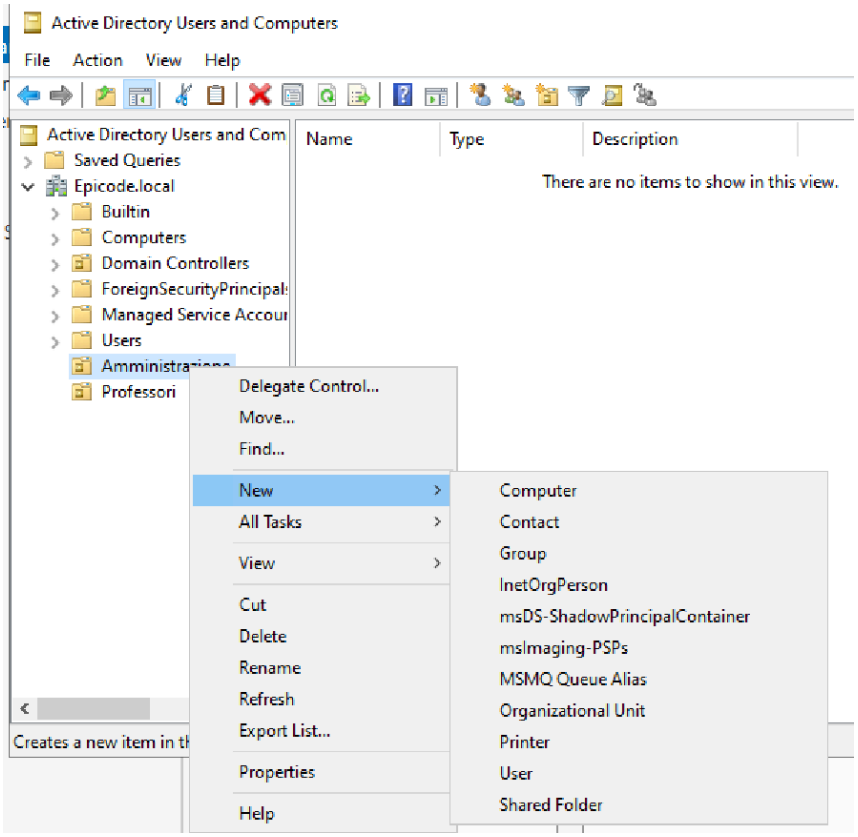


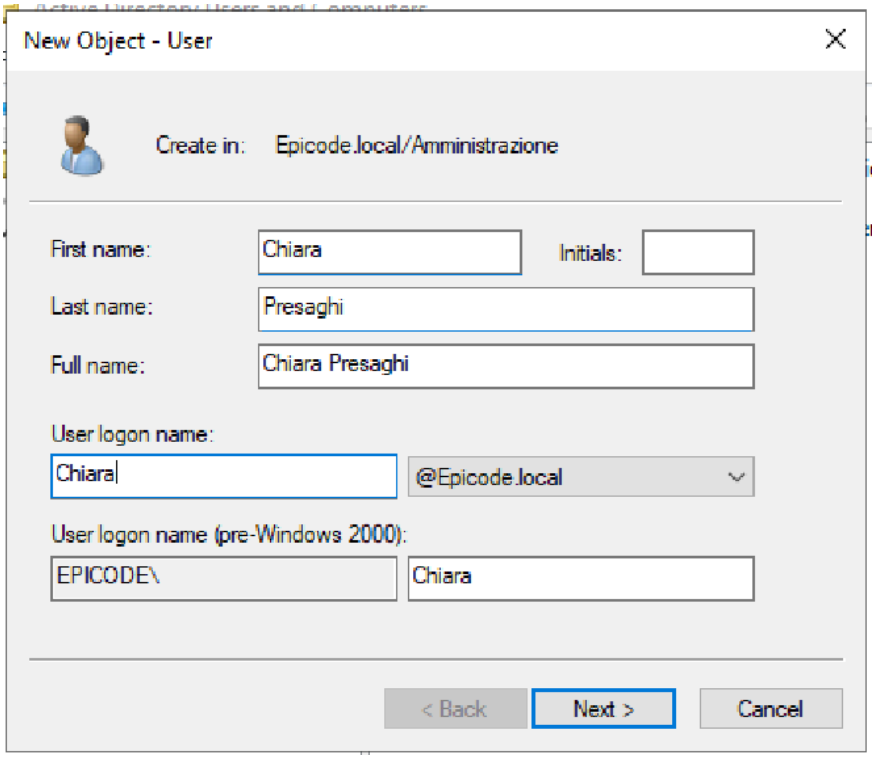

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
Epicode.local
Name
Type
Description
Builtin
builtinDomain
Default container for up...
Default container for do...
Default container for sec...
Default container for ma...
Default container for up...
Delegate Control...
Find...
Change Domain...
Change Domain Controller...
Raise domain functional level...
Operations Masters...
New
All Tasks
View
Refresh
Export List...
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-ShadowPrincipalContainer
mslmaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
User
Shared Folder
Creates a new item in this container.

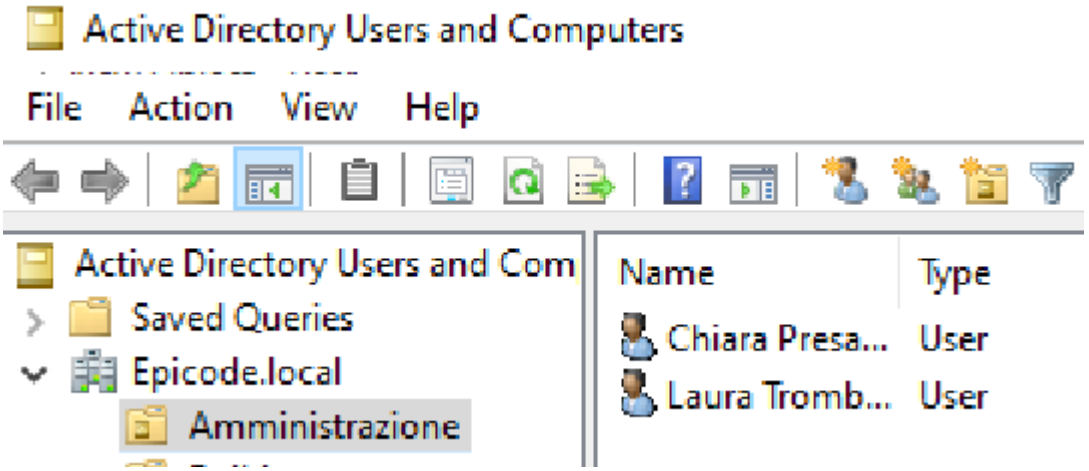

File
Action
View
Help
Active Directory Users and Com
Saved Queries
Epicode.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accou
Users
Amministrazione
Professori
Name

Creazione Utenti e Risoluzione Problemi

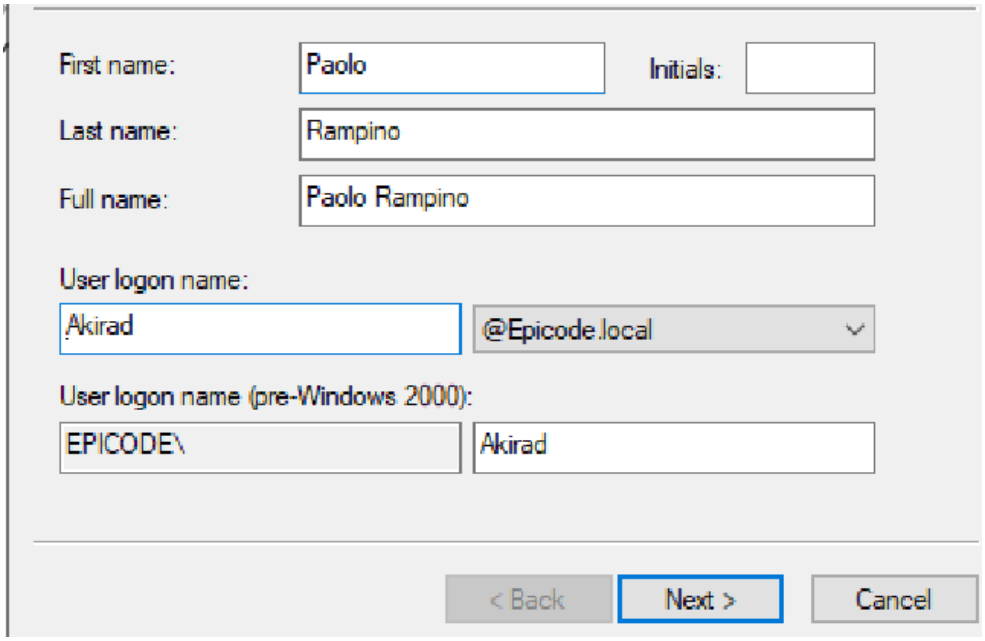
Ho popolato le OU con degli utenti poco fittizi:

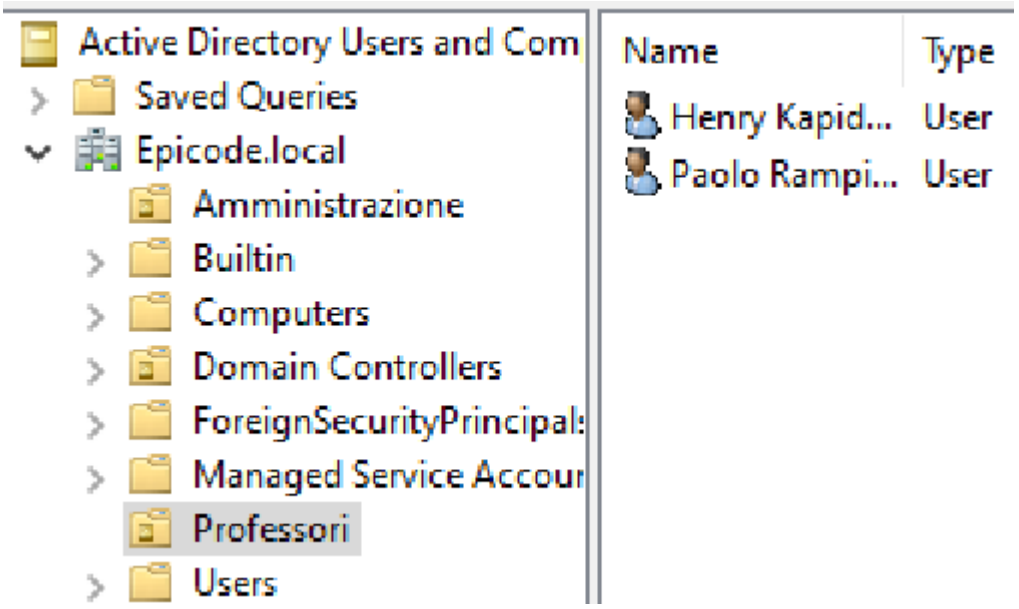






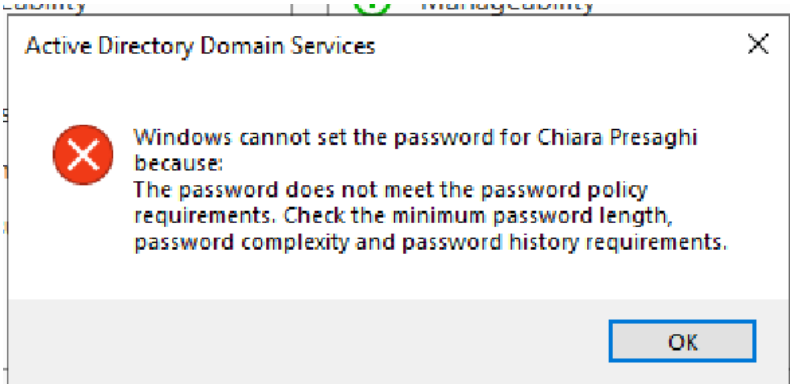
- In *Amministrazione*: **Chiara** e **Laura**.



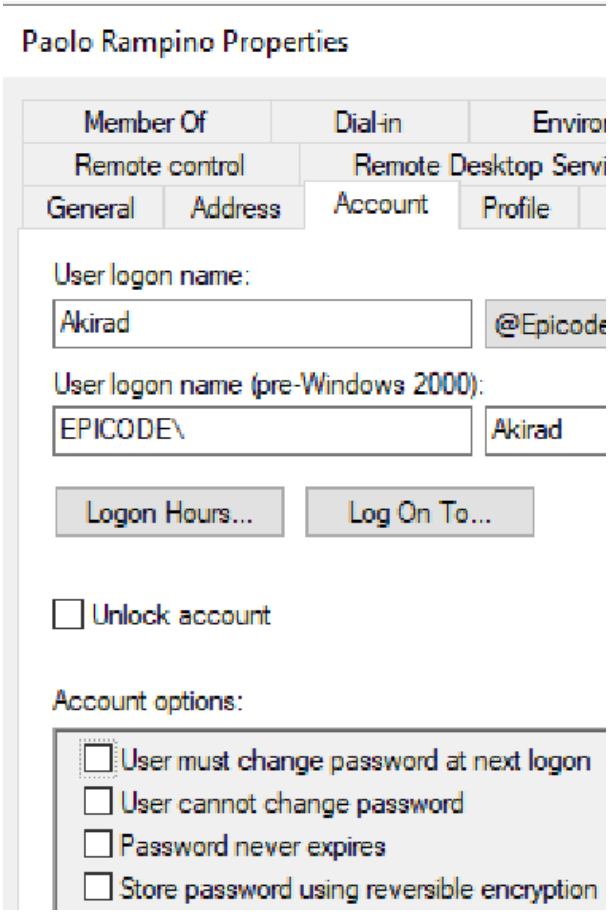


- In *Professori*: **Paolo (aka Akirad)** ed **Henry**.

🔴 **Problema affrontato:** Durante la creazione dell'utente Chiara, ho ricevuto un errore di sicurezza relativo alla password.



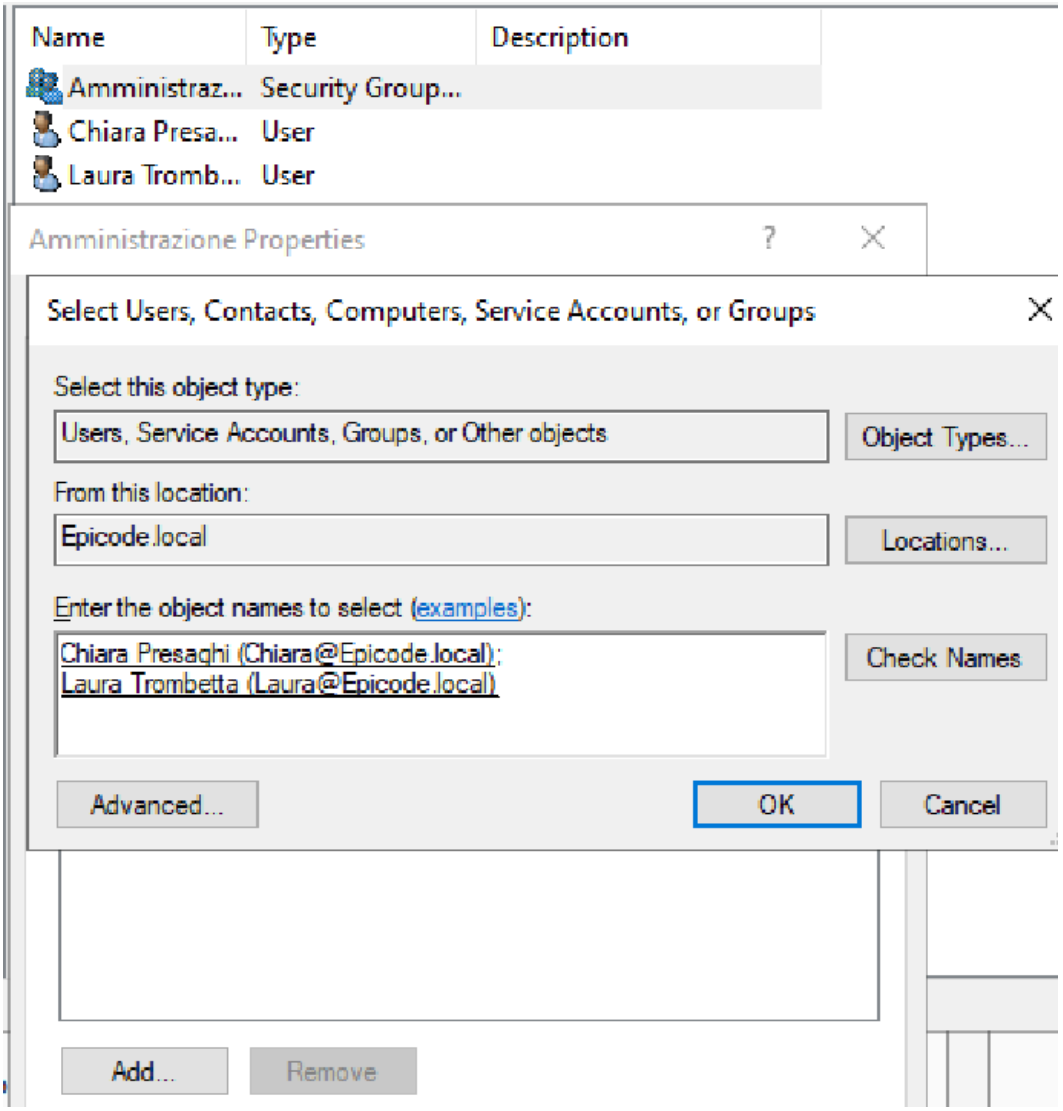
✅**Soluzione:** Ho compreso che la *Default Domain Policy* impone requisiti di complessità (lunghezza minima, uso di maiuscole/numeri/simboli) che io già rispettavo, il problema che ho scoperto in seguito una ricerca è stato quello di usare parole che facessero riferimento al nome utente… . Ho risolto utilizzando una password che non contenesse questi riferimenti e mantenendo la spunta su *"User must change password at next logon"* per obbligare l'utente a cambiarla al primo accesso. Solo L' utente prof Rampino non è stato impostato con questa configurazione, quindi non deve cambiare la password.

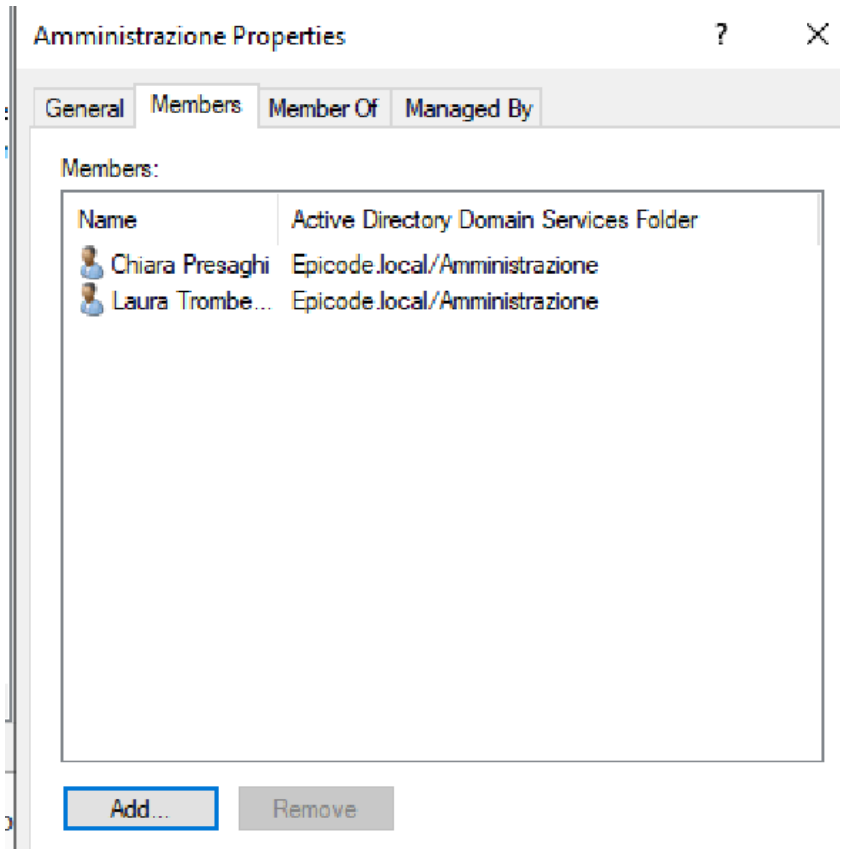


Gestione dei Gruppi

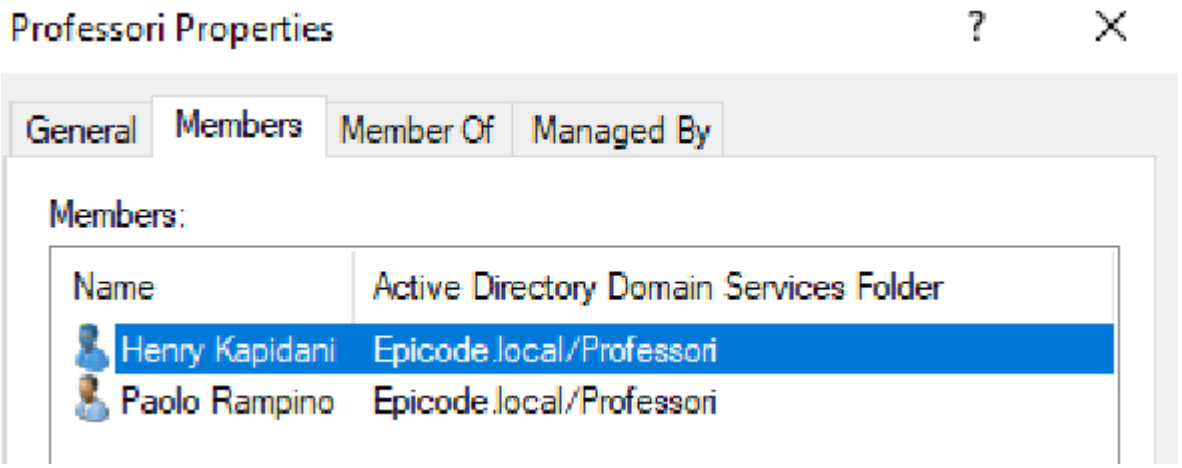
Applicando il principio RBAC, ho creato due gruppi di sicurezza globali:

- Gruppo **Amministrazione** (Membri: Chiara, Laura).





- Gruppo **Professori** (Membri: Paolo, Henry).



Sicurezza dei Dati (File Server)

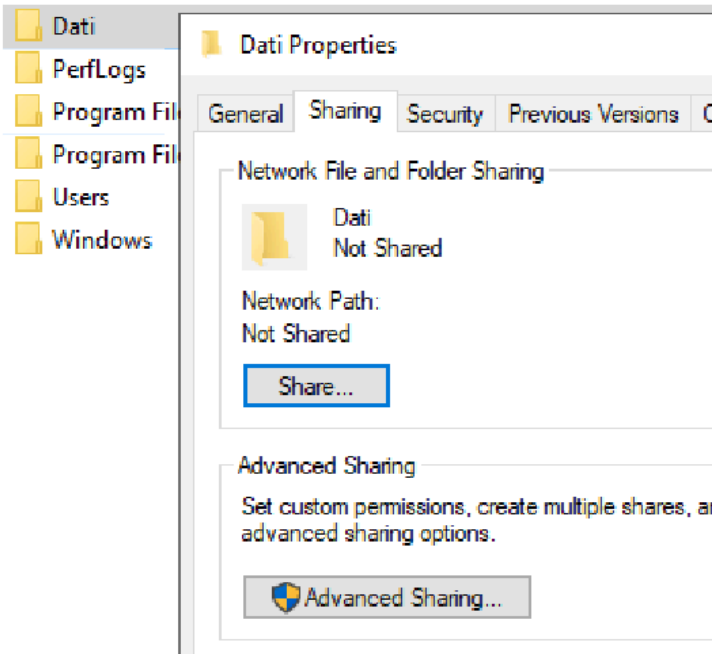
Ho creato una struttura di cartelle in C:\Dati per simulare un file server aziendale:

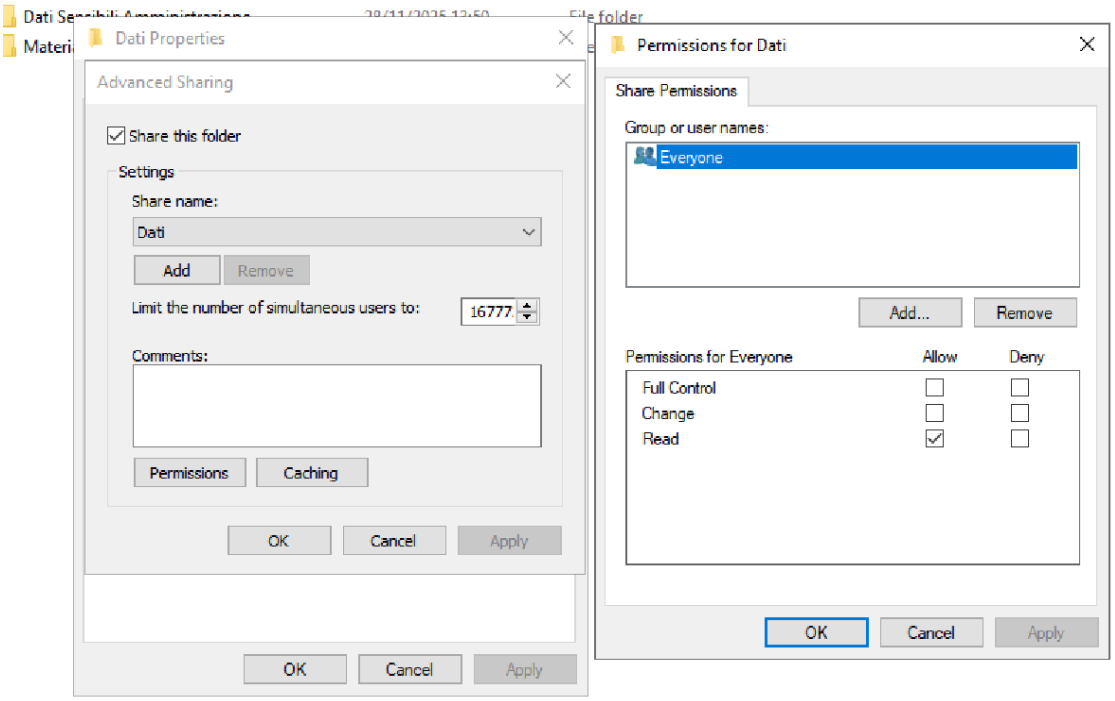
1. **Dati Sensibili Amministrazione**
2. **Materiale Professori**

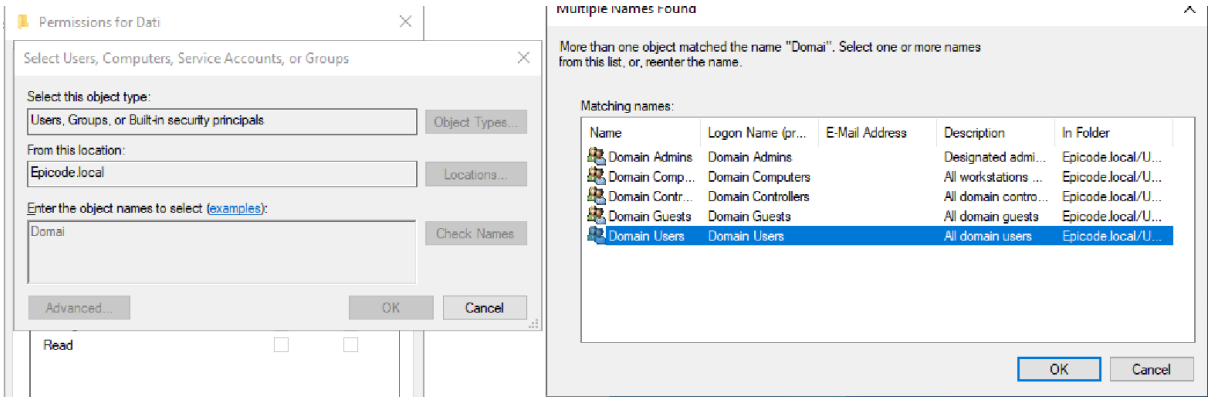
Strategia dei Permessi (Sharing vs Security)

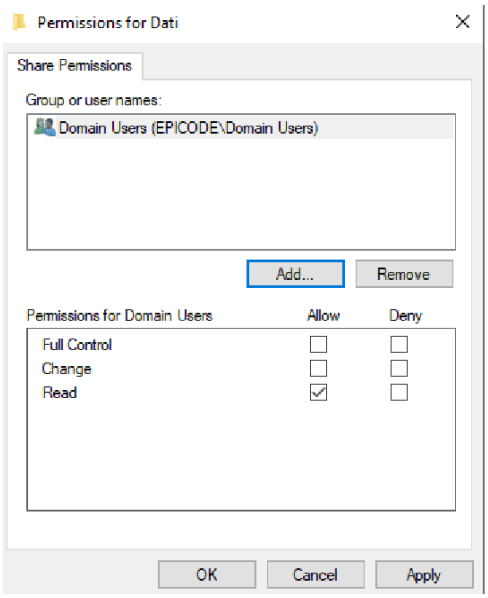
Ho adottato una strategia ibrida "Imbuto Largo, Filtro Stretto":

1. **Condivisione (Sharing):** Ho condiviso la cartella padre Dati, rimuovendo il gruppo Everyone (troppo insicuro) e aggiungendo il gruppo *Domain Users* con permessi di Lettura.




Dati Properties
Advanced Sharing
Share this folder
Settings
Share name:
Dati
Add
Remove
Limit the number of simultaneous users to:
16777
Comments:
Permissions
Caching
OK
Cancel
Apply
Permissions for Dati
Share Permissions
Group or user names:
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply


Permissions for Dati
Select Users, Computers, Service Accounts, or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
Epicode.local
Locations...
Enter the object names to select (examples):
Domai
Check Names
Advanced...
OK
Cancel
Read
Multiple Names Found
More than one object matched the name "Domai". Select one or more names from this list, or, reenter the name.
Matching names:
Name
Logon Name (pr...
E-Mail Address
Description
In Folder
Domain Admins
Domain Admins
Designated admi...
Epicode.local/U...
Domain Comp...
Domain Computers
All workstations ...
Epicode.local/U...
Domain Contr...
Domain Controllers
All domain contro...
Epicode.local/U...
Domain Guests
Domain Guests
All domain guests
Epicode.local/U...
Domain Users
Domain Users
All domain users
Epicode.local/U...
OK
Cancel

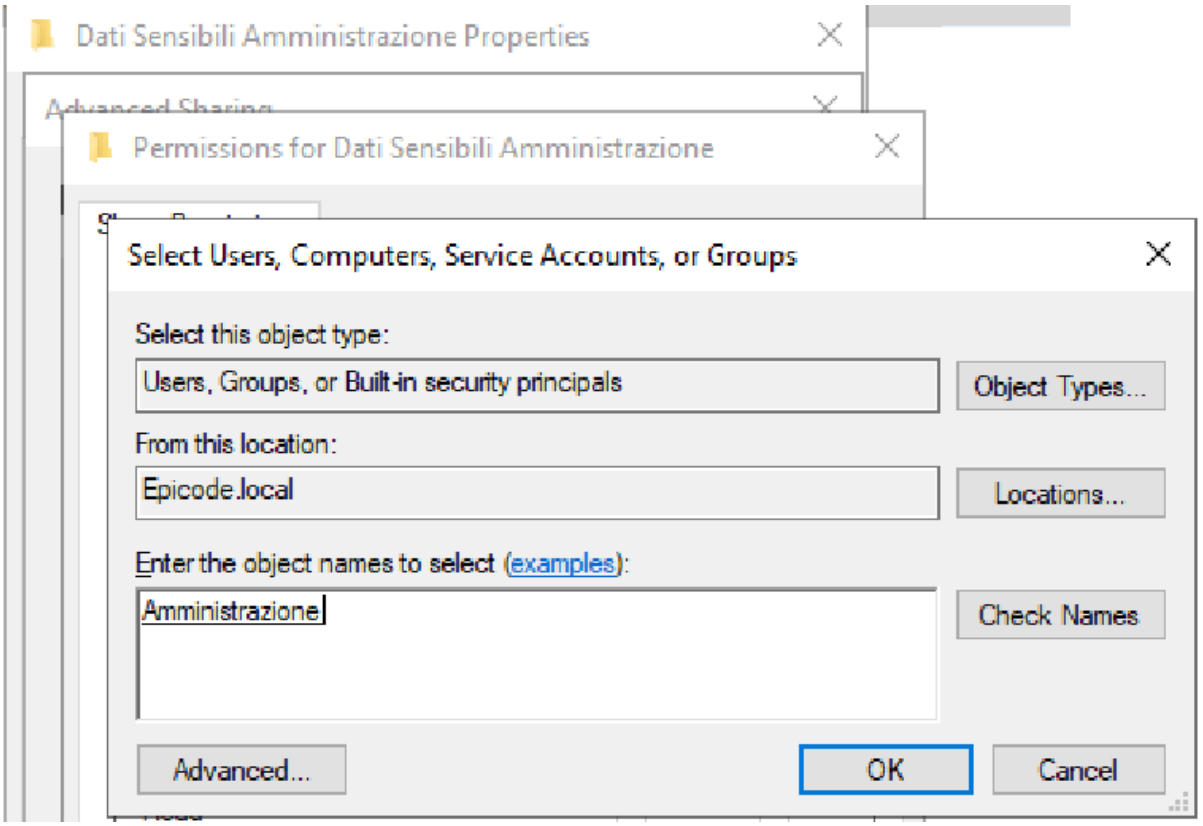

Permissions for Dati
Share Permissions
Group or user names:
Domain Users (EPICODE\Domain Users)
Add...
Remove
Permissions for Domain Users
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply

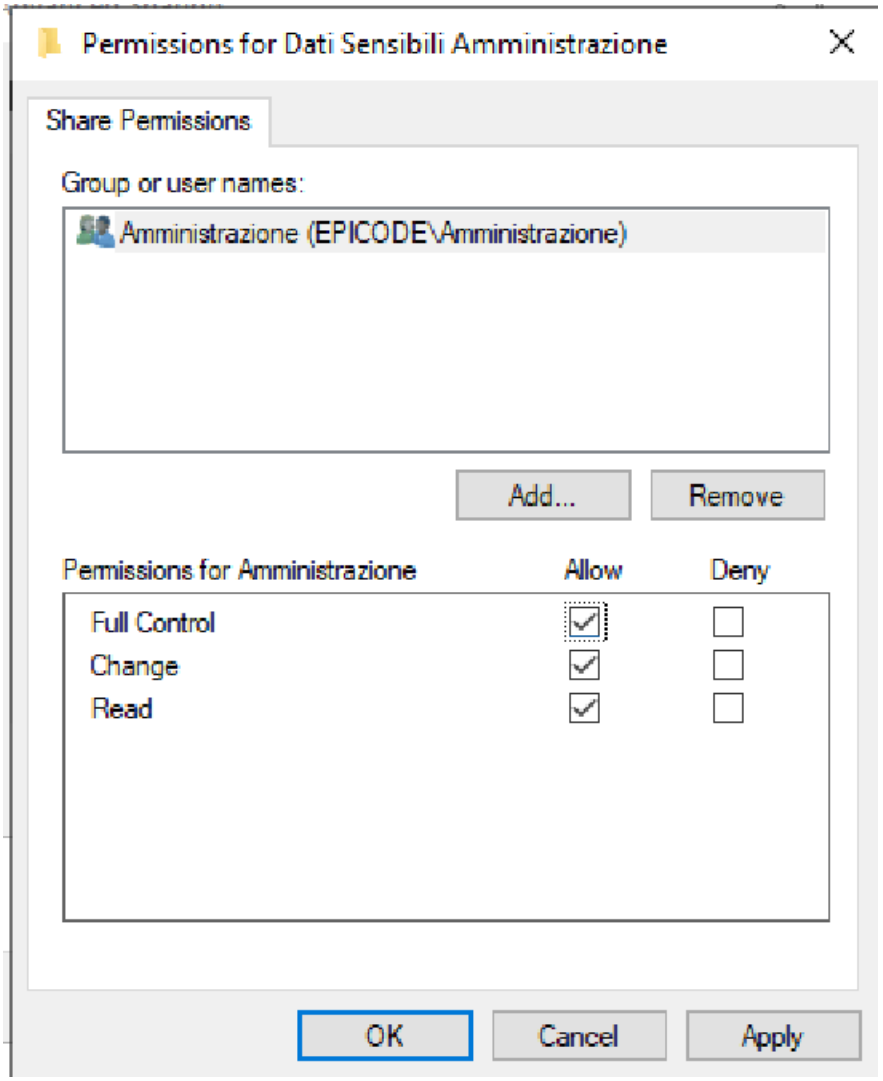
2. **Sicurezza (NTFS):** Ho disabilitato l'ereditarietà sulle sottocartelle per definire permessi granulari.

Applicazione delle Restrizioni (Deny)

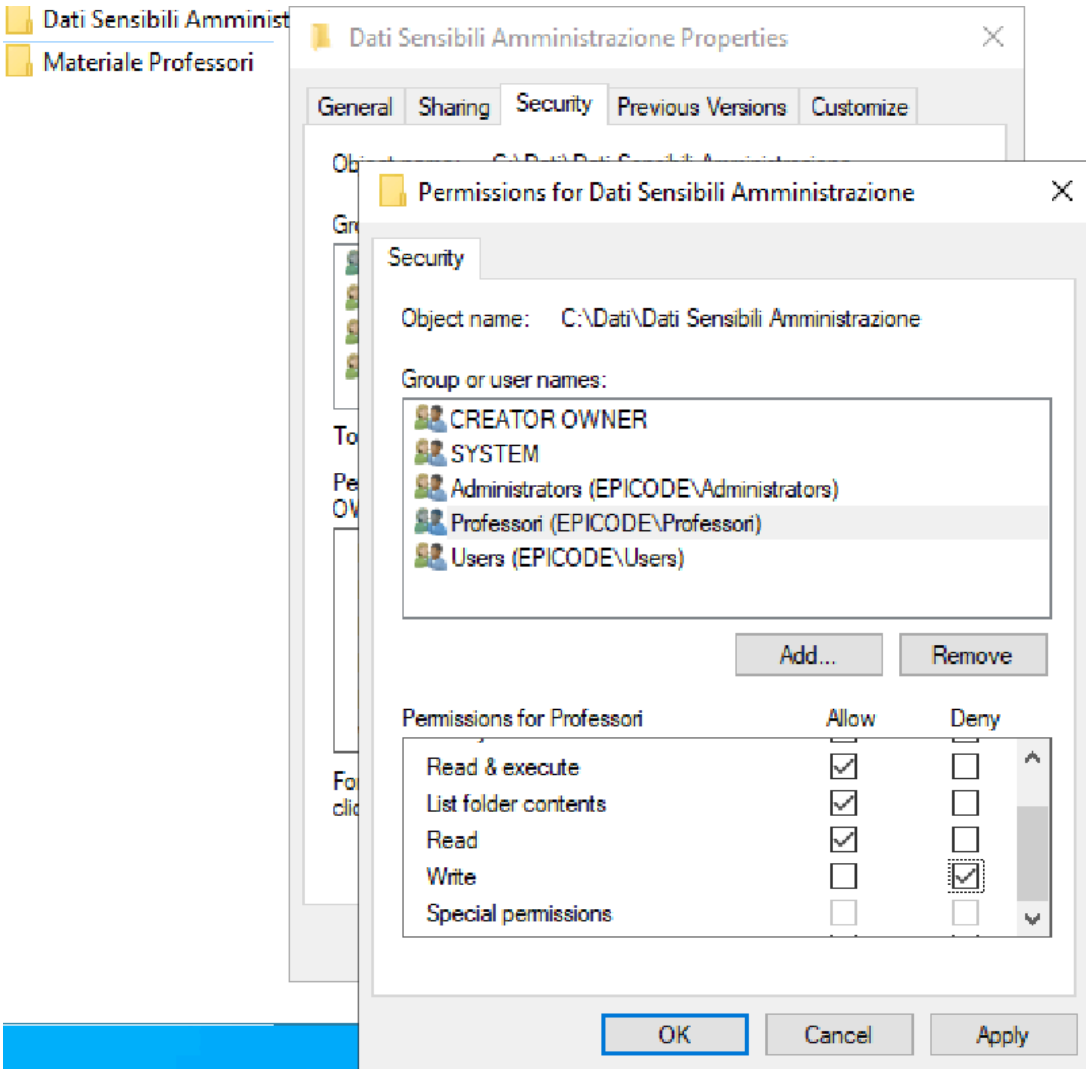
Ho configurato le Access Control Lists (ACL) con regole esplicite di blocco:

- **Su "Dati Sensibili Amministrazione":** Ho concesso l'accesso completo al gruppo *Amministrazione*,

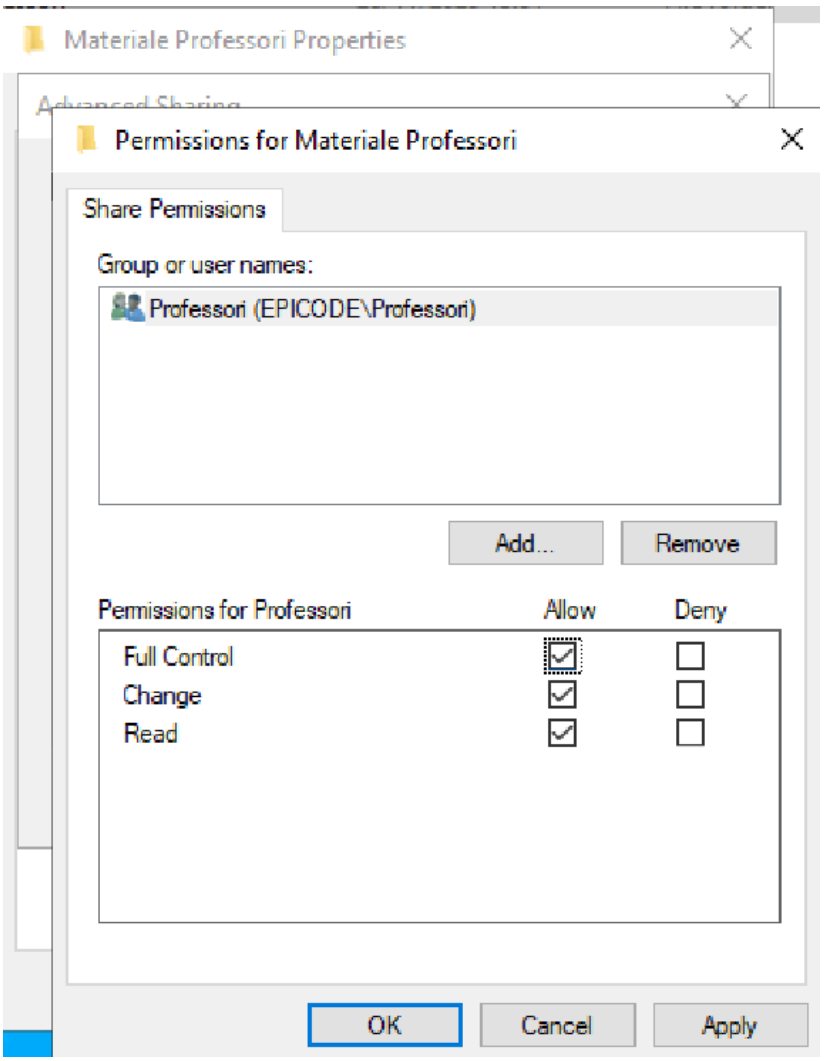




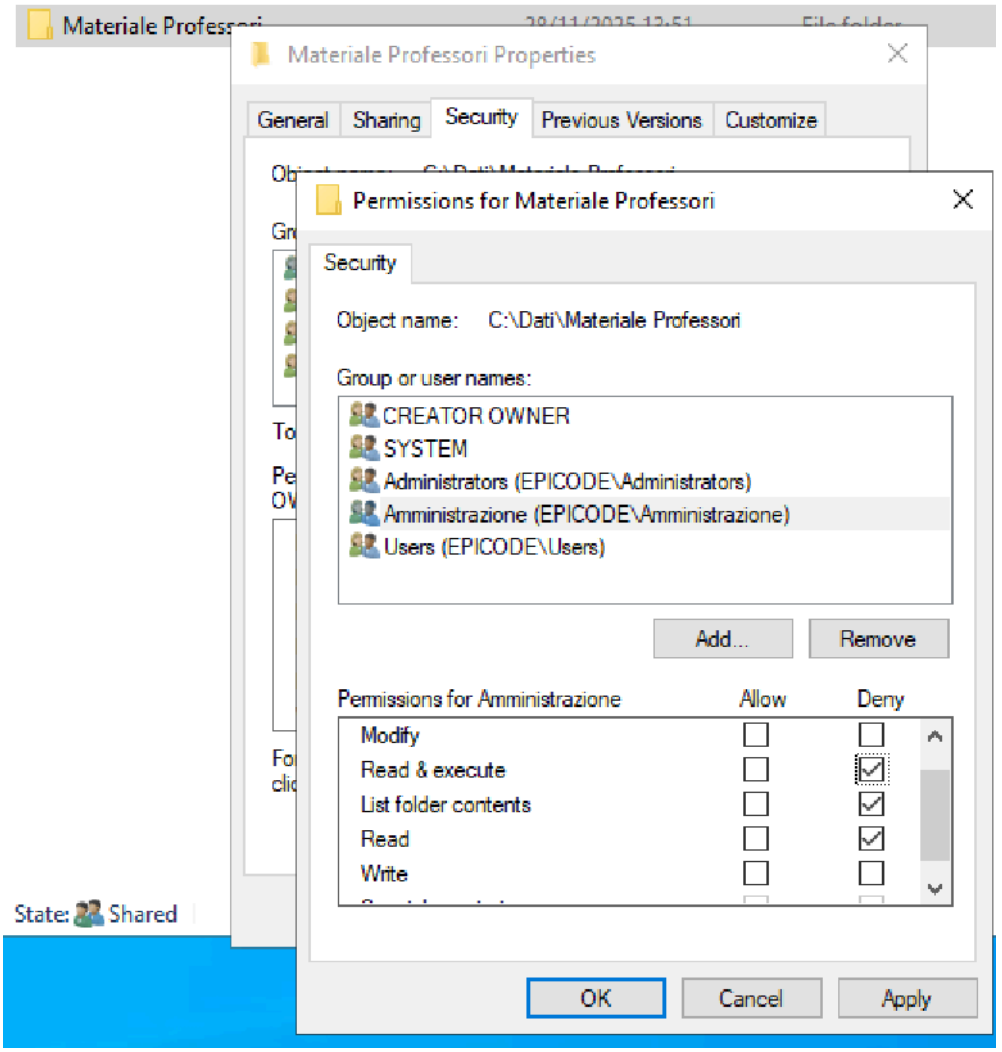
ma ho inserito una regola di **NEGA (Deny)** alla scrittura per il gruppo *Professori*.



Su "Materiale Professori": Ho concesso l'accesso al gruppo *Professori*,

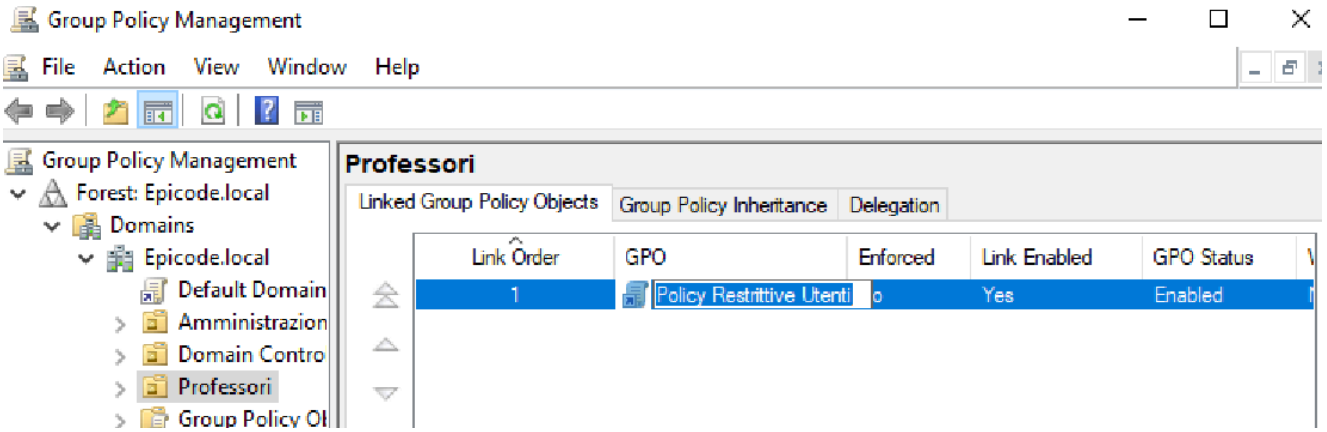


ma ho inserito una regola di **NEGA (Deny)** alla lettura per il gruppo *Amministrazione*.



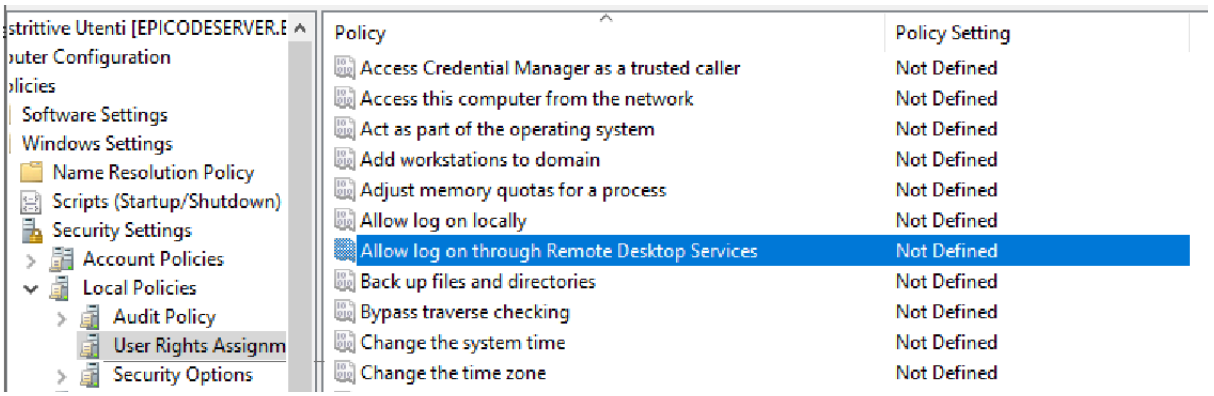
Sicurezza del Sistema (Group Policy - GPO)

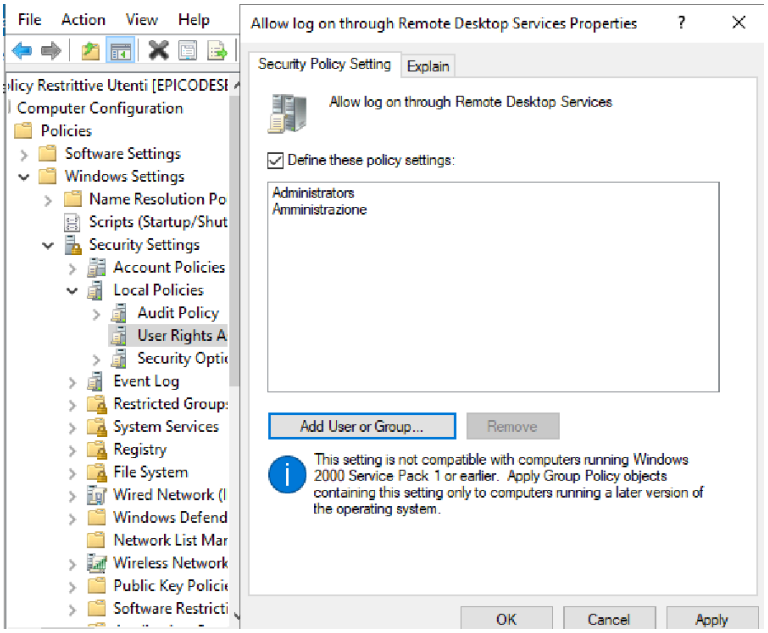
Oltre ai dati, ho messo in sicurezza il comportamento del sistema creando una GPO chiamata **"Policy Restrittive Utenti"**, collegata all'OU *Professori*.



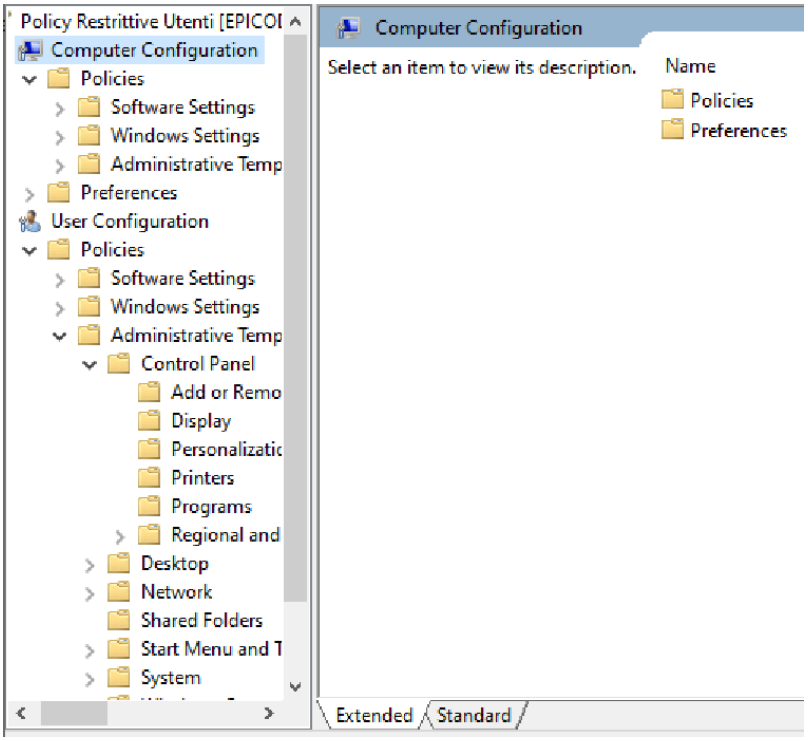
Ho configurato tre restrizioni principali:

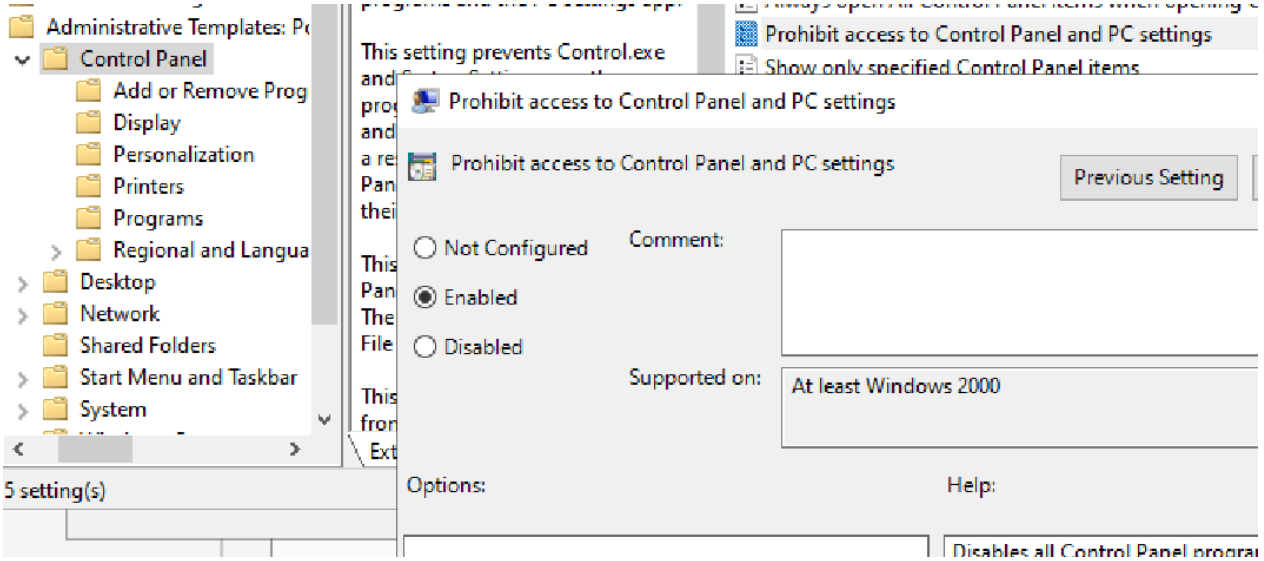
1. **Accesso Remoto (RDP):** Ho modificato i diritti utente locali per permettere l'RDP *solo* agli Administrators e al gruppo Amministrazione, tagliando fuori i Professori.





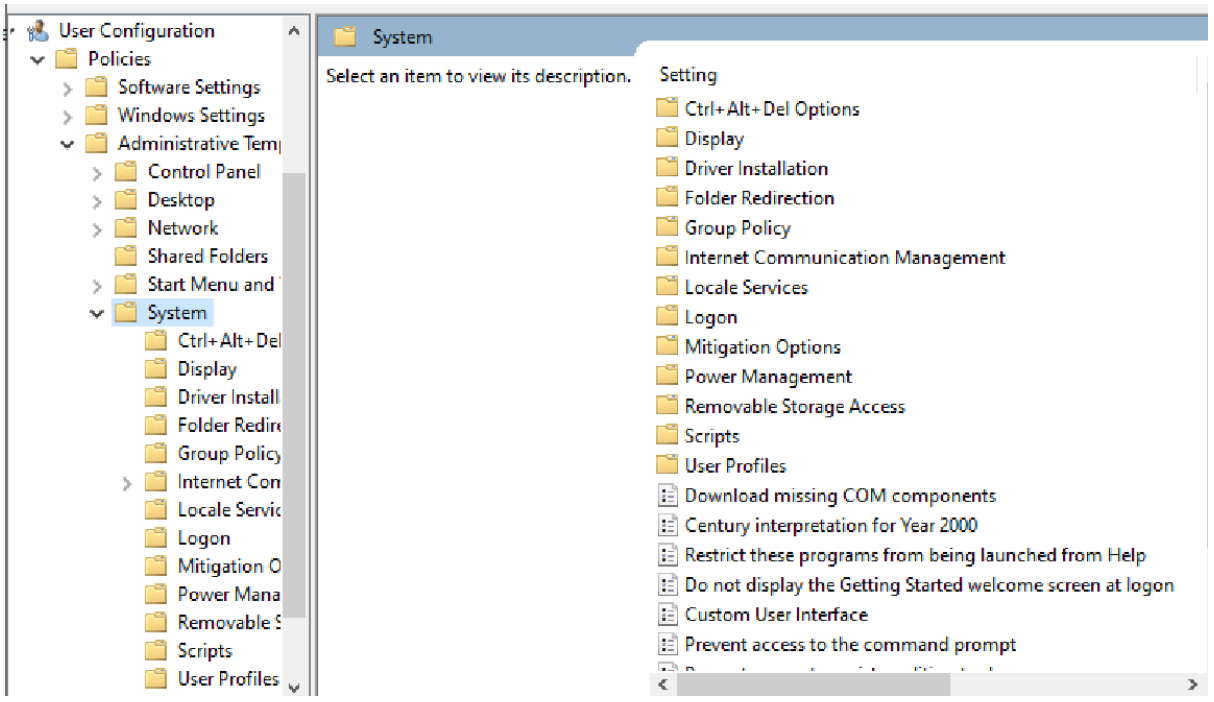
2. **Blocco Pannello di Controllo:** Ho abilitato la policy *"Prohibit access to Control Panel"*, impedendo agli utenti di modificare le impostazioni della macchina.

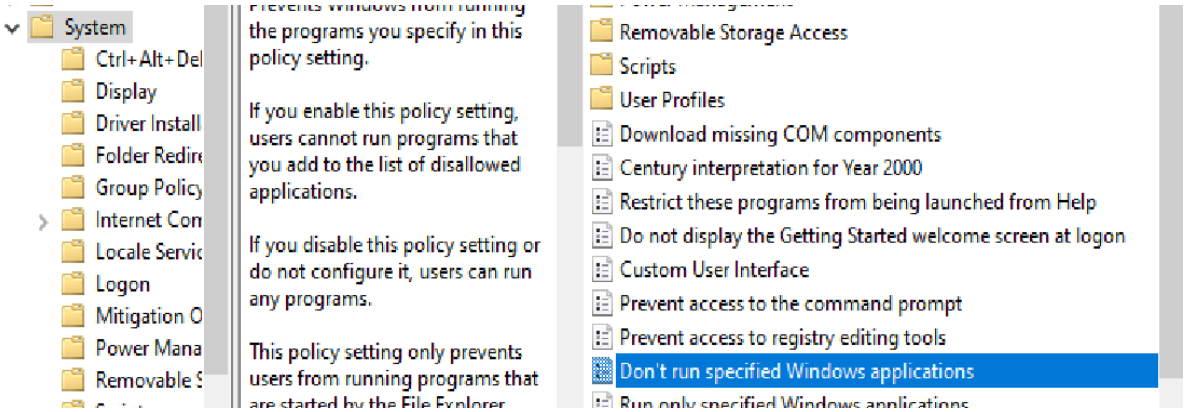


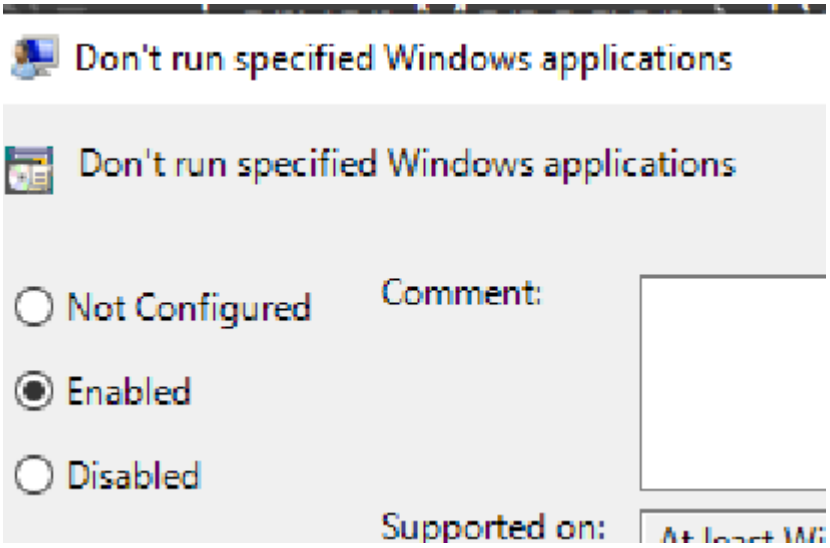


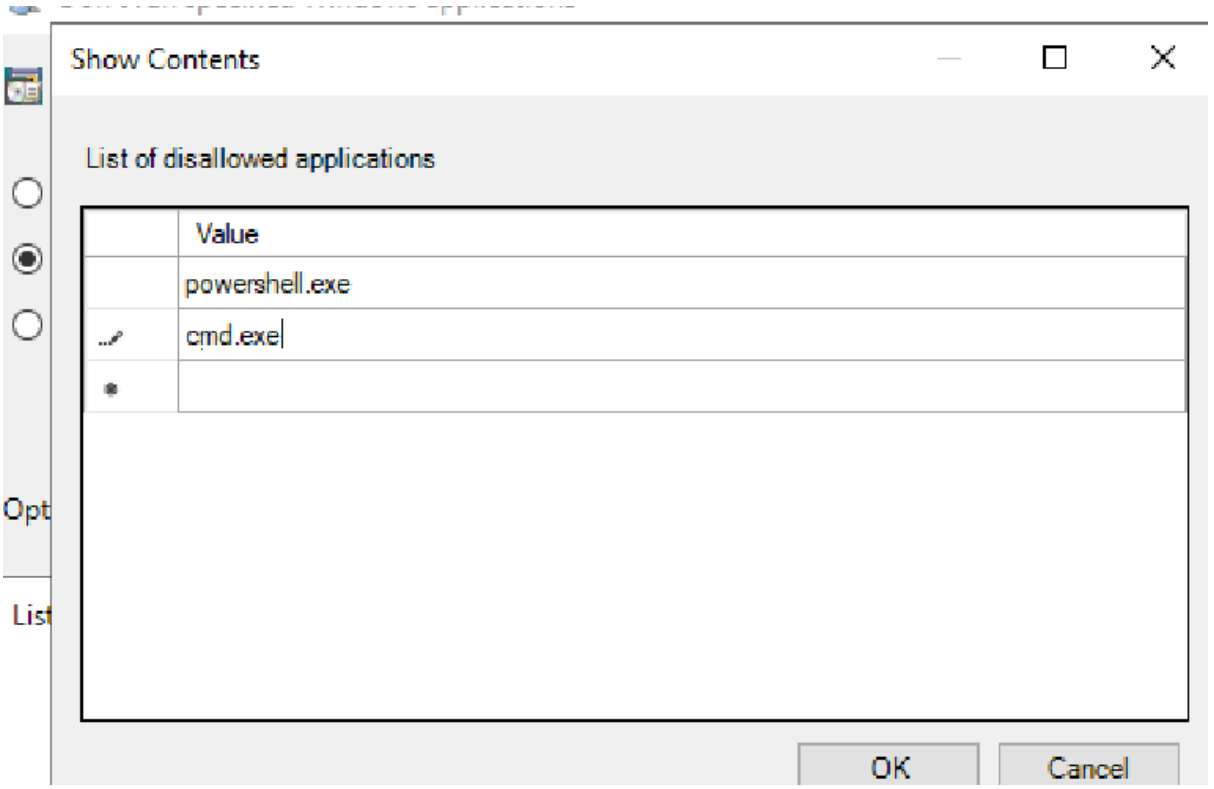
3. **Blocco Software:** Ho attivato una blacklist per impedire l'esecuzione di powershell.exe e cmd.exe, mitigando il rischio

di esecuzione di script malevoli.





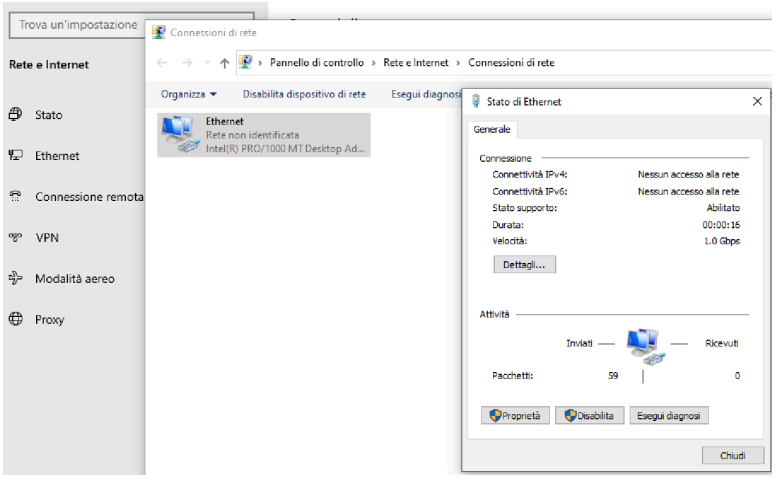


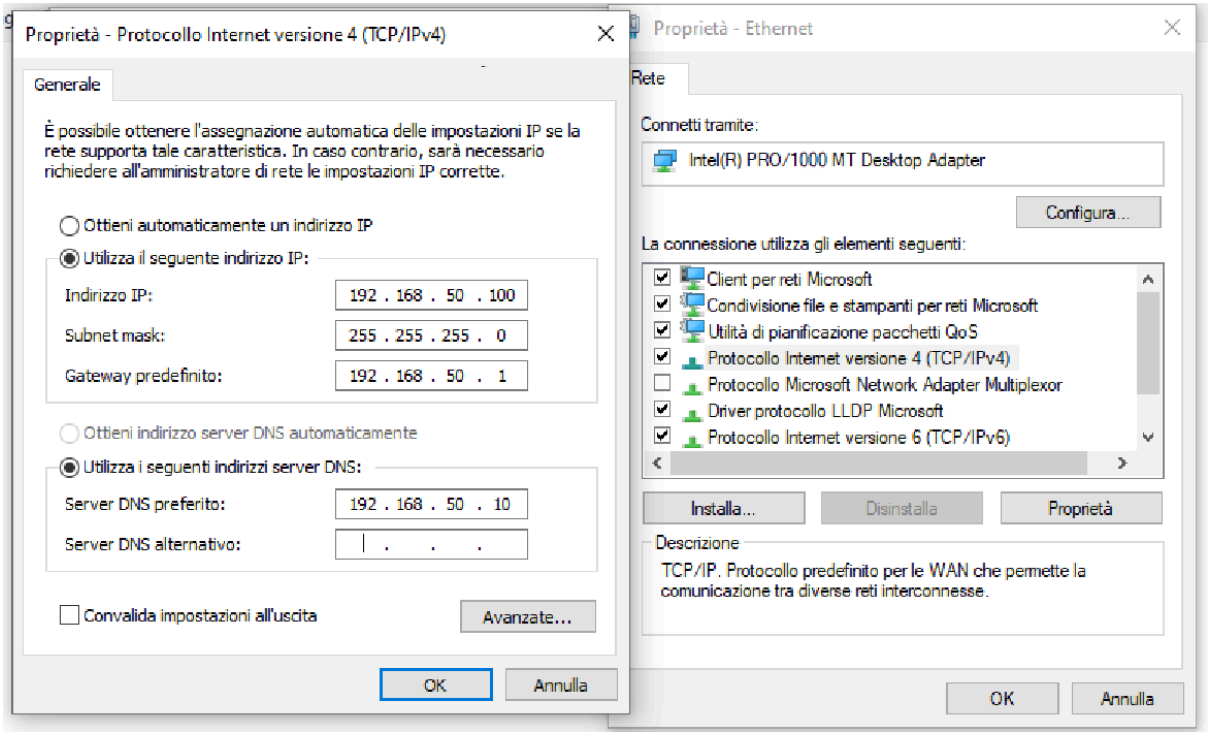


Verifica Finale (Il Test)

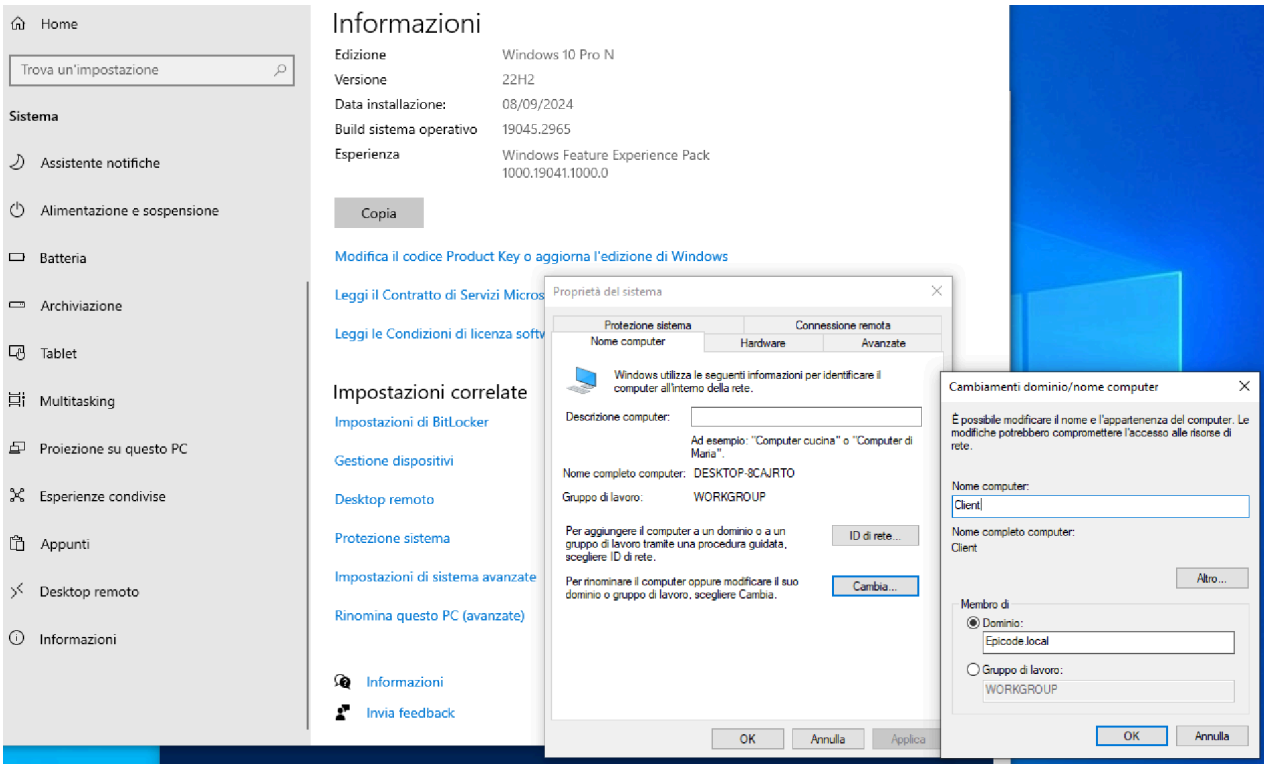
Per validare il tutto, ho configurato una macchina client **Windows 10 Pro**:

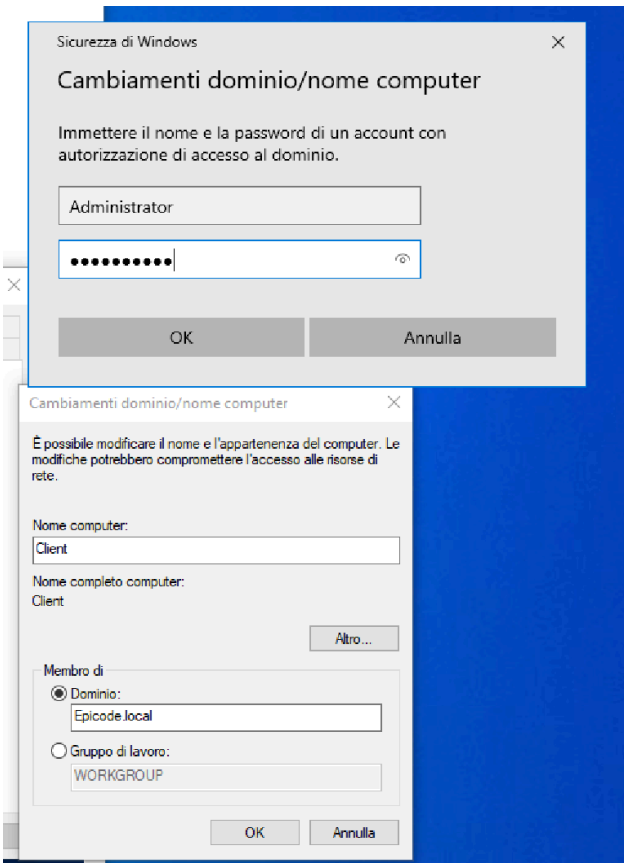
1. Ho impostato il DNS del client con l'IP del Server.

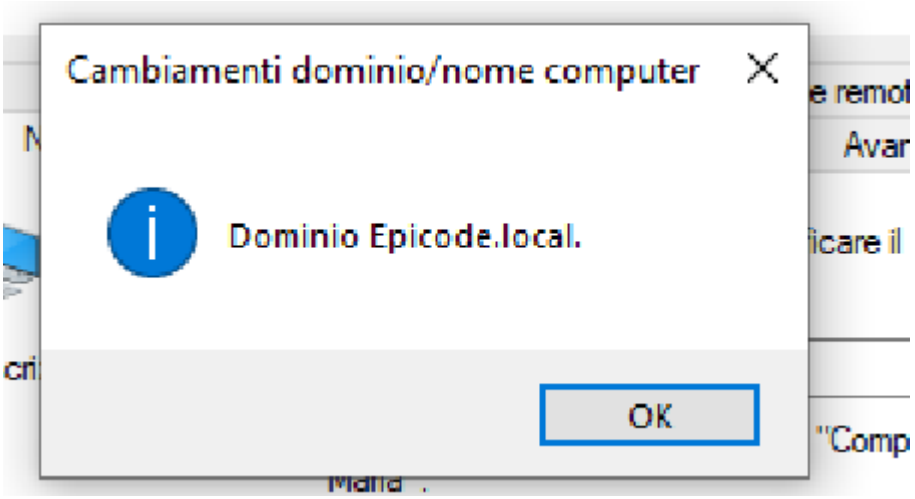




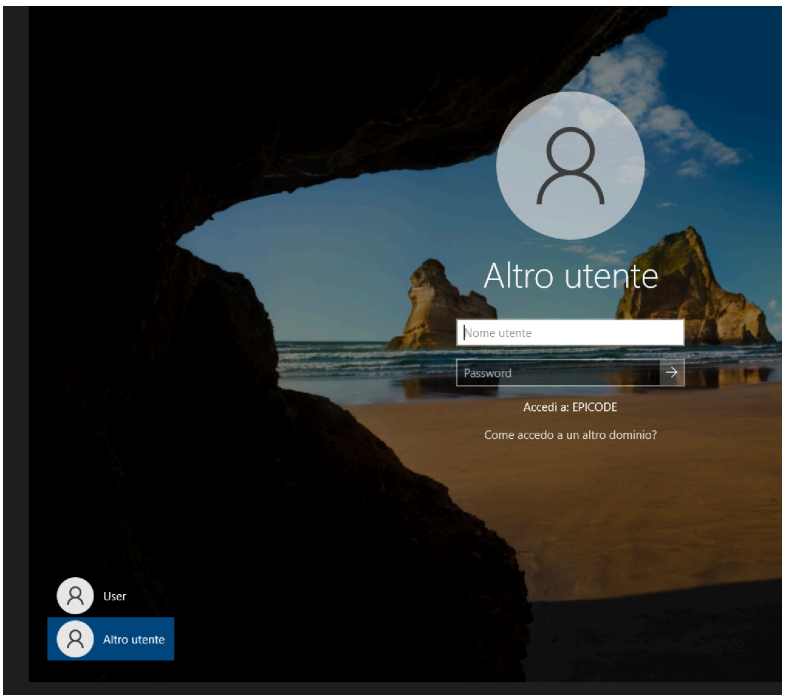
2. Ho unito il client al dominio Epicode.local.





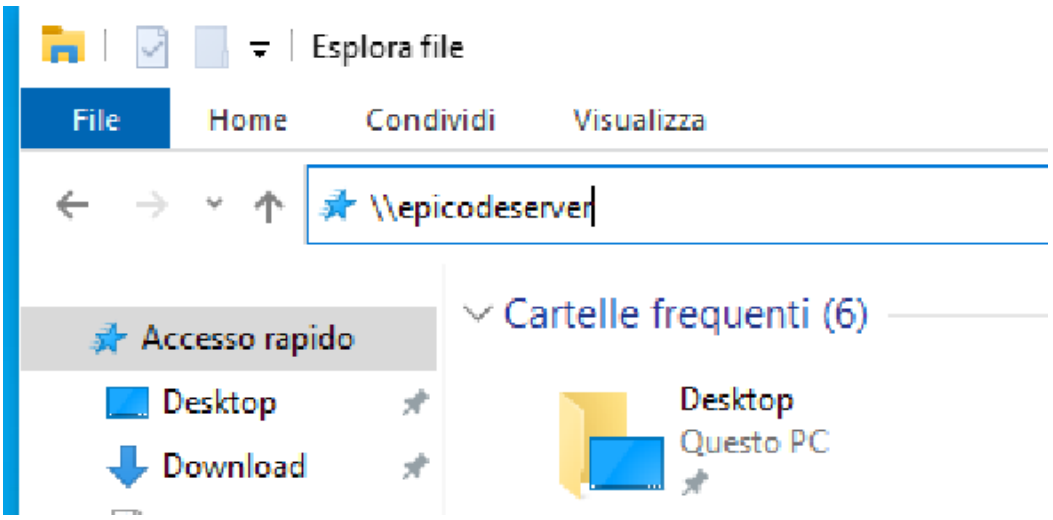


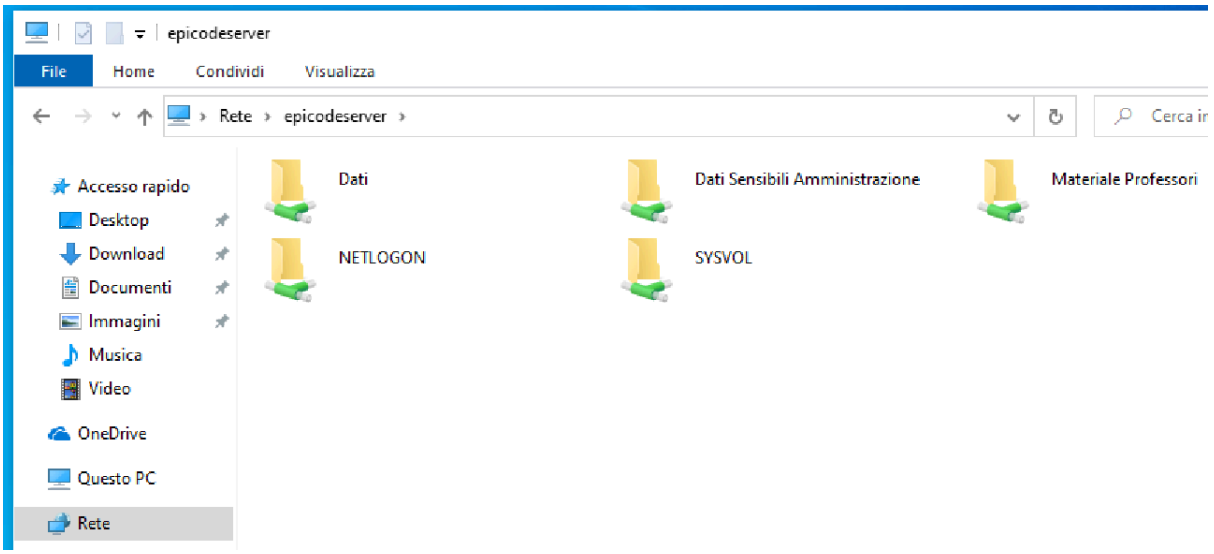
3. Ho effettuato l'accesso con l'utente **Henry** (simulando un membro del gruppo Professori)così da dimostrare che dovevo cambiare la password temporanea per effettuare il nuovo accesso, dato che solo l' utente **Paolo** (aka Akirad) non la doveva cambiare .



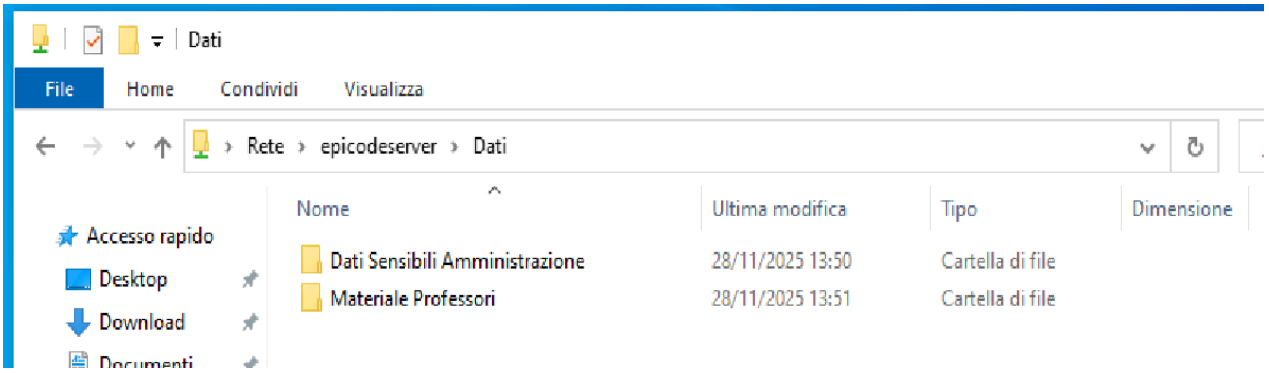
Risultati dei Test:

- Tentativo di accesso a \\EpicodeServer\Dati\Materiale

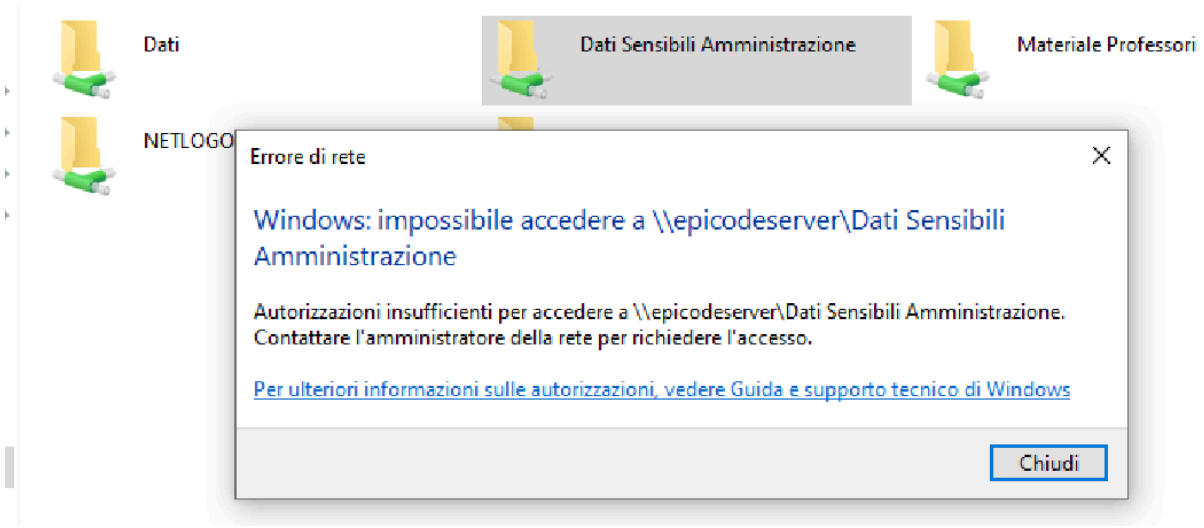




Professori: **RIUSCITO** ✅.



- Tentativo di accesso a \\EpicodeServer\Dati\Dati Sensibili Amministrazione: **FALLITO (Accesso Negato)** ❌.



- Tentativo di aprire il Pannello di Controllo: **BLOCCATO DAL SISTEMA** ✅.

Conclusione e Riflessioni

Questa esperienza pratica mi ha permesso di toccare con mano la complessità e la potenza di un'infrastruttura Windows Server. Ho imparato che:

1. **L'ordine è sicurezza:** Una struttura AD ben organizzata in OU semplifica enormemente l'applicazione delle policy.
2. **I permessi "Deny" sono potenti:** L'uso esplicito del "Nega" è un'arma a doppio taglio che va usata con cautela, ma garantisce blocchi certi (poiché il "Nega" vince sempre sul "Consenti").
3. **La difesa è a strati:** Non basta proteggere i file (NTFS), bisogna proteggere anche il sistema operativo (GPO) e l'accesso alla rete (Sharing).

In conclusione, ho trasformato un server base in un ambiente controllato, dove ogni utente può fare esattamente ciò che deve fare, e nulla di più.