

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

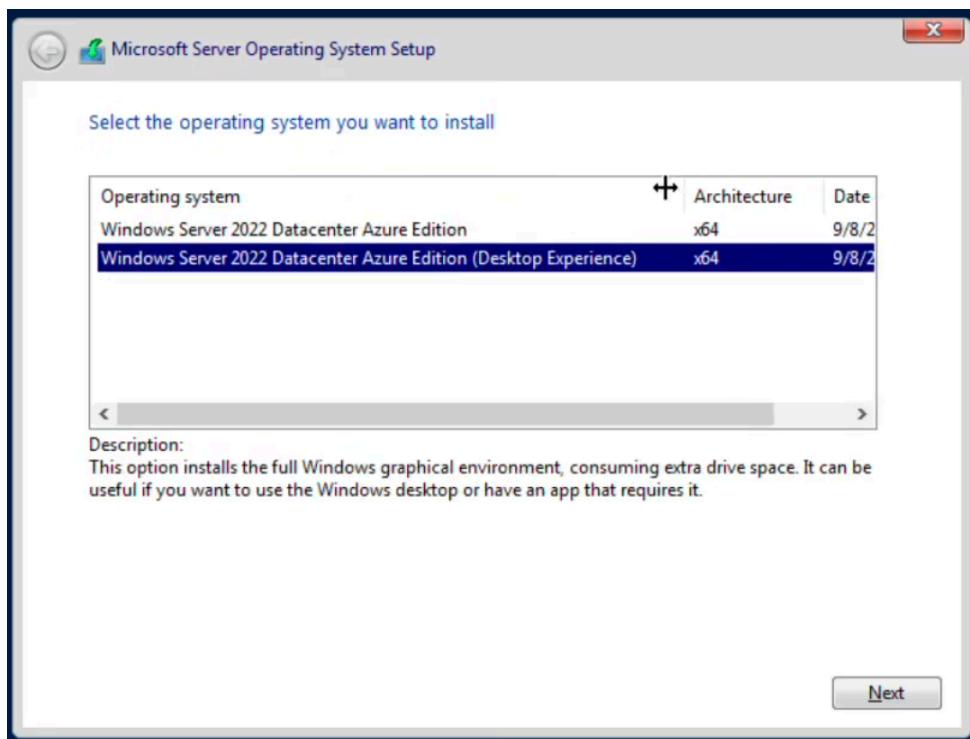
persone. Questo garantisce scalabilità: se un dipendente cambia ruolo, basta spostarlo di gruppo senza dover riconfigurare decine di cartelle.

- **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

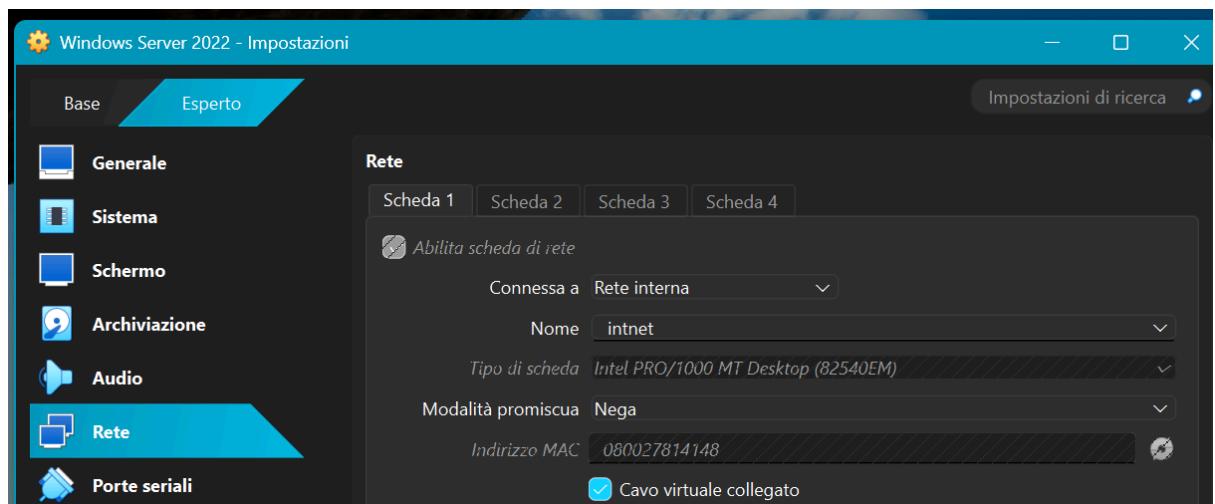
Preparazione del Server

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.

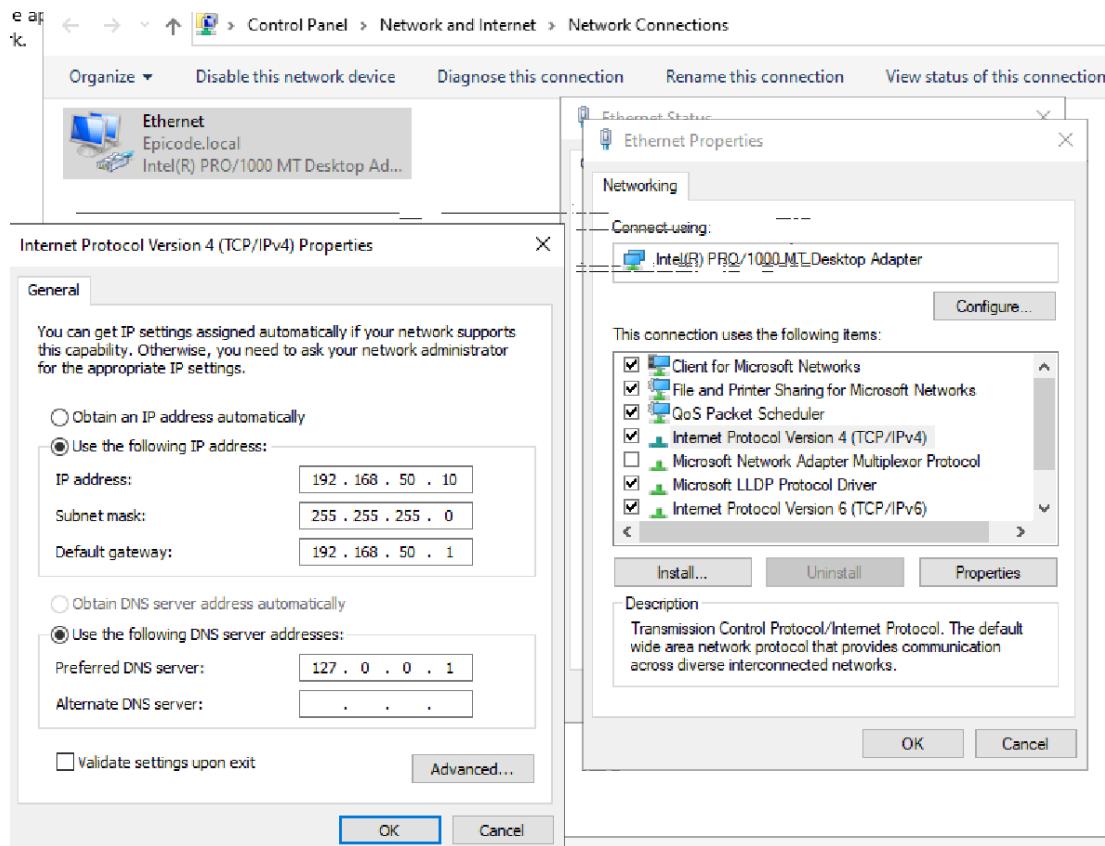


Dopo l'installazione, ho eseguito passaggi critici per la stabilità:

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.

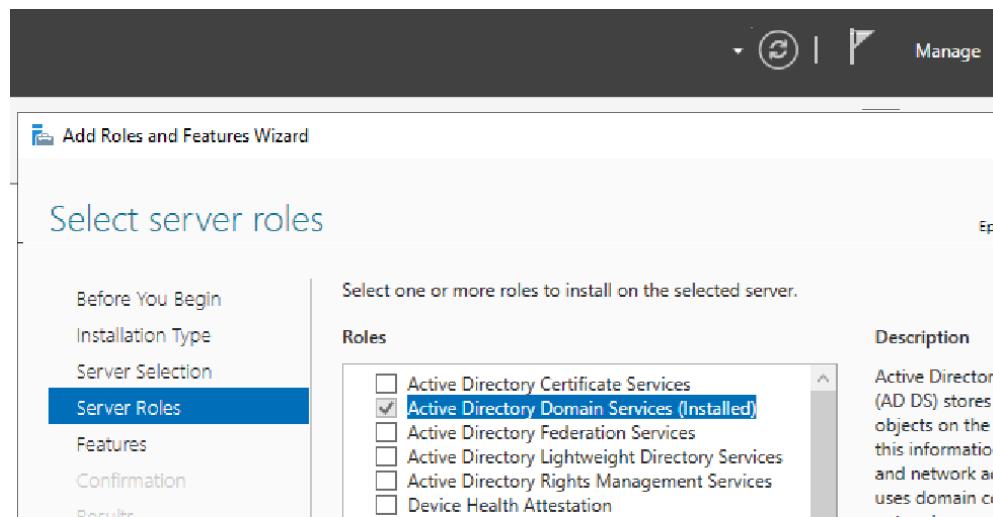


Ho assegnato un **IP Statico** al server (**192.168.1.106**) e, punto cruciale, ho impostato il **DNS Server** su **127.0.0.1** (localhost). Questo perché il server, una volta diventato Domain Controller, deve interrogare se stesso per risolvere i nomi della rete.

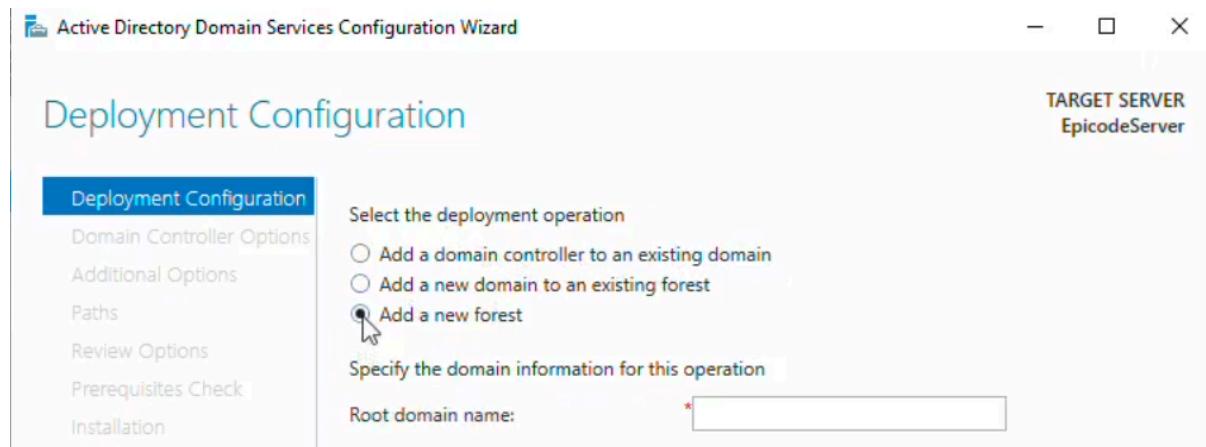


Promozione a Domain Controller

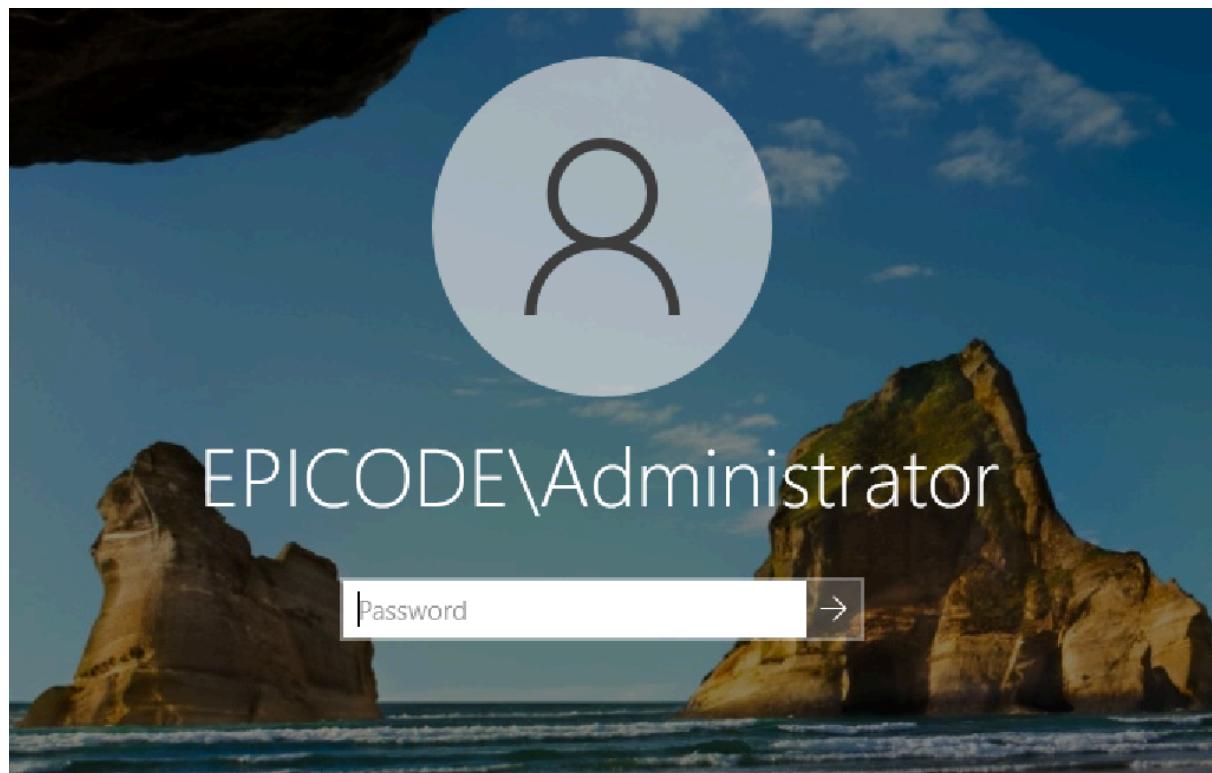
Tramite il **Server Manager**, ho aggiunto il ruolo **Active Directory Domain Services**.



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



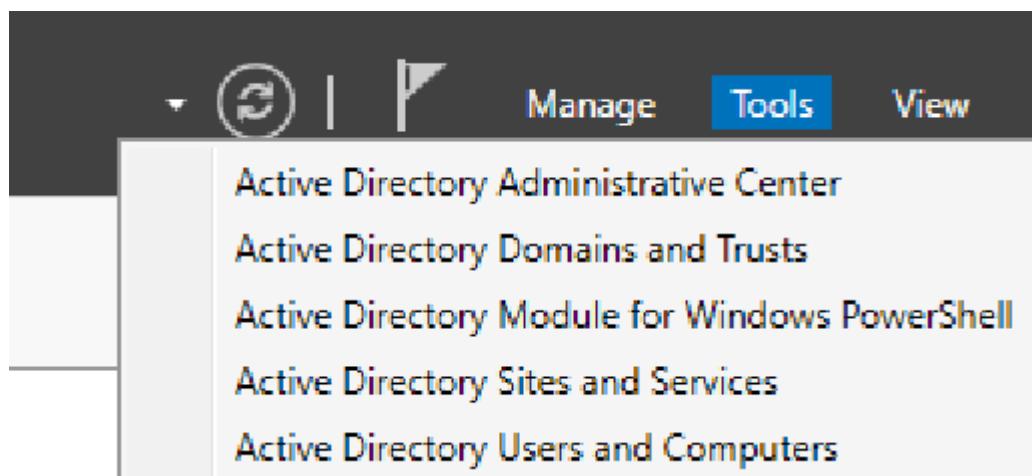
Gestione Identità e Accessi (IAM)

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... tional... 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

Creates a new item in this container.

Computer
Contact
Group
InetOrgPerson
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
User
Shared Folder

This screenshot shows the 'Active Directory Users and Computers' management console. A context menu is open over the 'Builtin' object in the 'Eicode.local' domain. The menu includes options like 'Delegate Control...', 'Find...', 'Change Domain...', etc., followed by a separator line and 'New'. A secondary dropdown menu under 'New' lists various object types: Computer, Contact, Group, InetOrgPerson, msDS-ShadowPrincipalContainer, msImaging-PSPs, MSMQ Queue Alias, Organizational Unit, Printer, User, and Shared Folder. The 'User' option is highlighted.

File Action View Help

Active Directory Users and Com
Saved Queries
Eicode.local

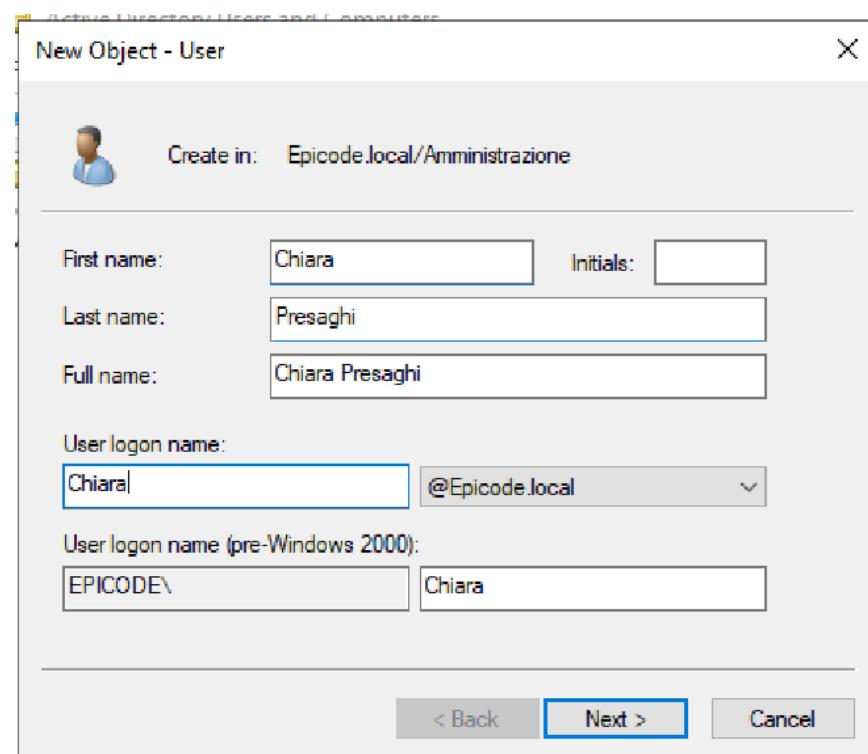
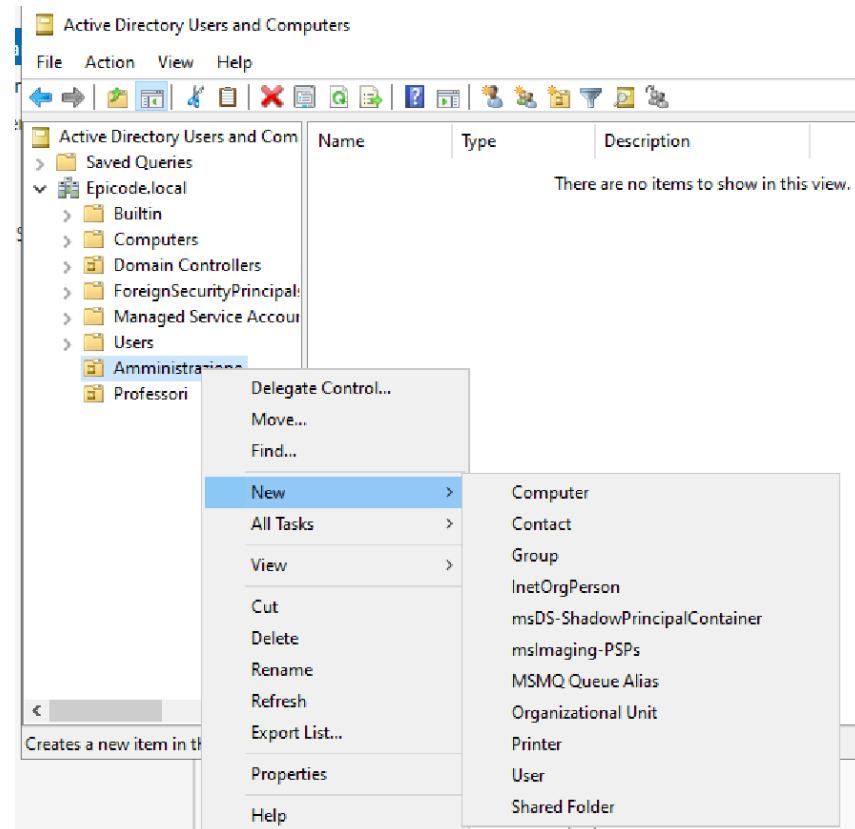
- > Builtin
- > Computers
- > Domain Controllers
- > ForeignSecurityPrincipal
- > Managed Service Account
- > Users
- > Amministrazione
- > Professori

Name

This screenshot shows the 'Active Directory Users and Computers' interface with a tree view of objects. The 'Eicode.local' domain is expanded, revealing its sub-objects: 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Managed Service Account', 'Users', 'Amministrazione', and 'Professori'. The 'Name' column is visible on the right side of the interface.

Creazione Utenti e Risoluzione Problemi

Ho popolato le OU con degli utenti poco fintizi:



Active Directory Users and Computers

File Action View Help

Back Forward Find Filter New Search

Active Directory Users and Com > Saved Queries Epicode.local Amministrazione

Name	Type
Chiara Presa...	User
Laura Tromb...	User

- In Amministrazione: Chiara e Laura.

First name:	Paolo	Initials:	<input type="text"/>
Last name:	<input type="text"/> Rampino		
Full name:	<input type="text"/> Paolo Rampino		
User logon name:	<input type="text"/> Akirad	@Epicode.local	<input type="button"/>
User logon name (pre-Windows 2000):	<input type="text"/> EPICODE\	<input type="text"/> Akirad	<input type="button"/>

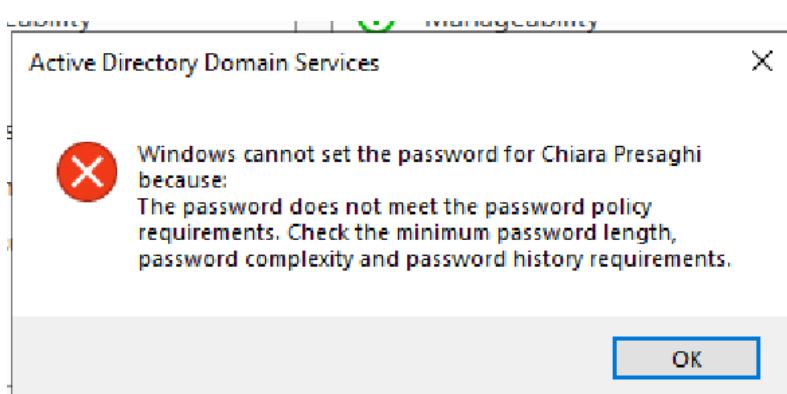
< Back Next > Cancel

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, a tree view displays the domain structure under 'Eicode.local'. The 'Professori' folder is highlighted with a gray selection bar. On the right, a list view shows the users in the 'Professori' group, with two entries: 'Henry Kapid...' and 'Paolo Rampi...', both listed as 'User' type accounts.

Name	Type
Henry Kapid...	User
Paolo Rampi...	User

- 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.

Paolo Rampino Properties

Member Of	Dial-in	Environ...
Remote control	Remote Desktop Servi...	
General	Address	Account
		Profile

User logon name:
Akirad @Epicode

User logon name (pre-Windows 2000):
EPICODE\ Akirad

[Logon Hours...](#) [Log On To...](#)

[Unlock account](#)

Account options:

<input checked="" type="checkbox"/> User must change password at next logon
<input type="checkbox"/> User cannot change password
<input type="checkbox"/> Password never expires
<input type="checkbox"/> Store password using reversible encryption

Gestione dei Gruppi

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

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

The screenshot shows a Windows-style dialog box titled "Amministrazione Properties". At the top left is a table with columns "Name", "Type", and "Description". It lists three entries: "Amministraz..." (Security Group), "Chiara Presa..." (User), and "Laura Tromb..." (User). Below the table is the main dialog area with the title "Select Users, Contacts, Computers, Service Accounts, or Groups".
The "Select this object type:" dropdown is set to "Users, Service Accounts, Groups, or Other objects".
The "From this location:" dropdown contains "Epicode.local".
The "Enter the object names to select (examples):" text input field contains "Chiara Presaghi (Chiara@Epicode.local); Laura Trombetta (Laura@Epicode.local)".
At the bottom right of the dialog are "OK" and "Cancel" buttons, with "OK" being highlighted by a blue border.

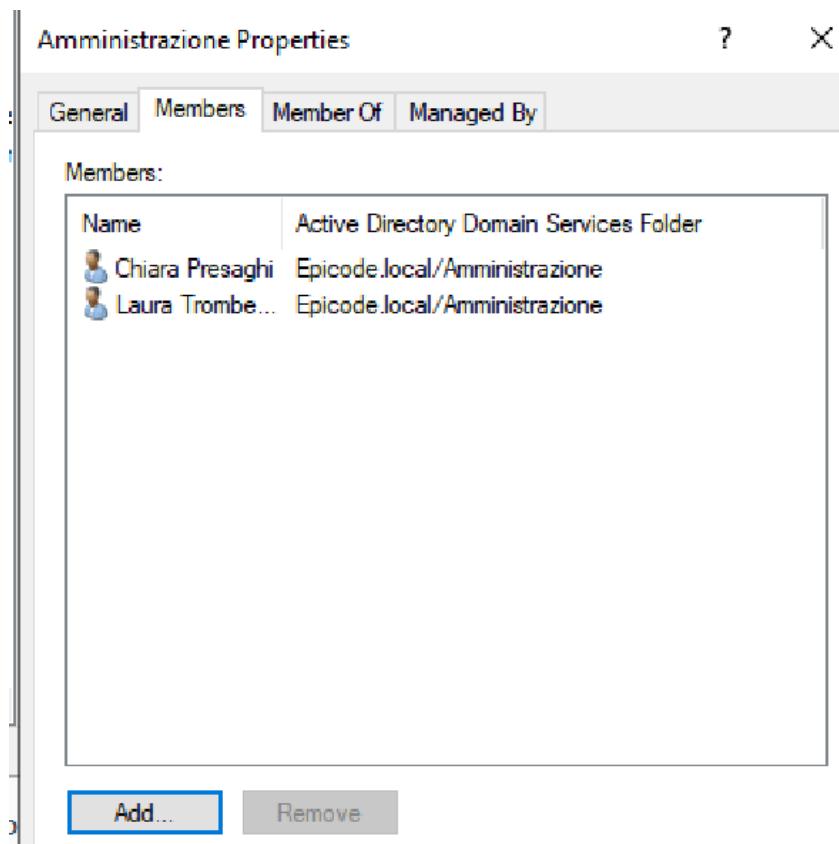
Amministrazione Properties

General Members Member Of Managed By

Members:

Name	Active Directory Domain Services Folder
Chiara Presaghi	Epicode.local/Amministrazione
Laura Trombe...	Epicode.local/Amministrazione

Add... Remove



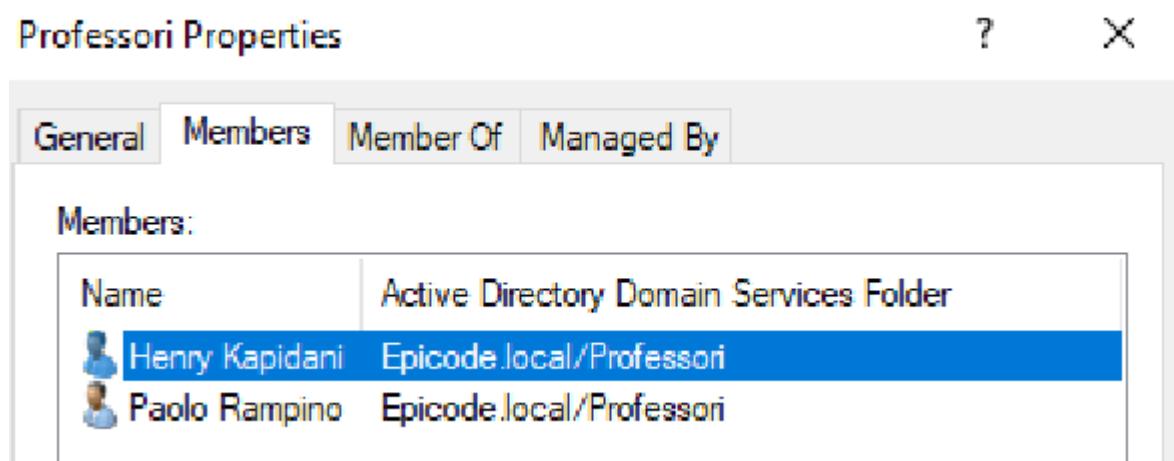
- Gruppo **Professori** (Membri: Paolo, Henry).

Professori Properties

General Members Member Of Managed By

Members:

Name	Active Directory Domain Services Folder
Henry Kapidani	Epicode.local/Professori
Paolo Rampino	Epicode.local/Professori



Sicurezza dei Dati (File Server)

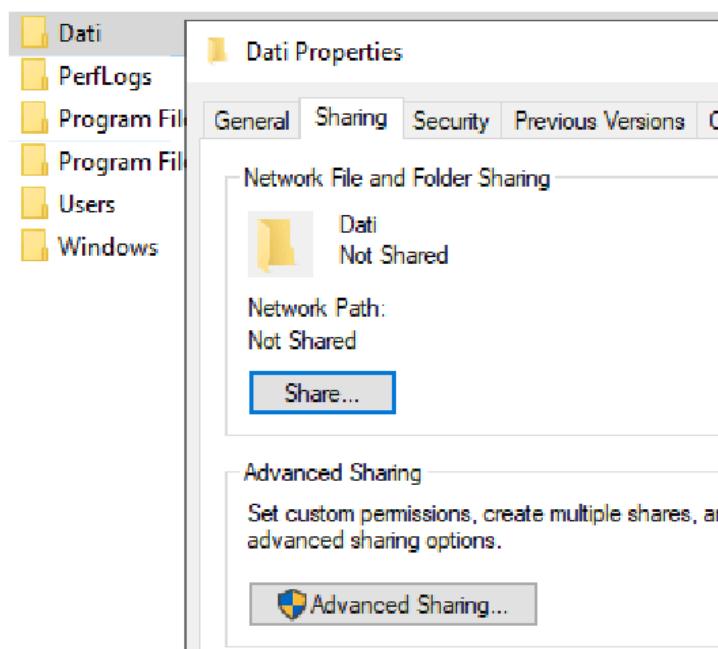
Ho creato una struttura di cartelle in C:\Dati per simulare un file server aziendale:

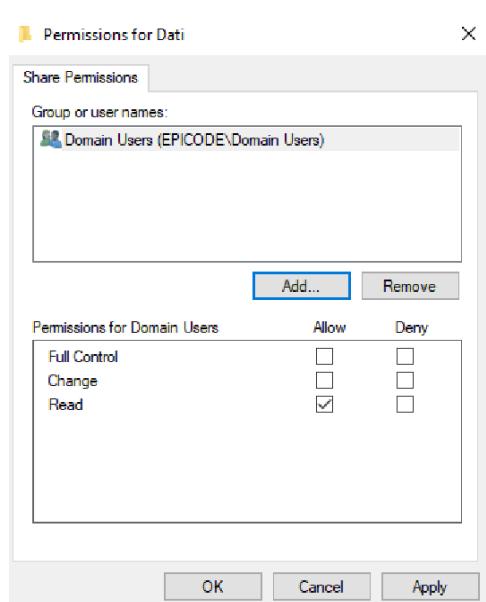
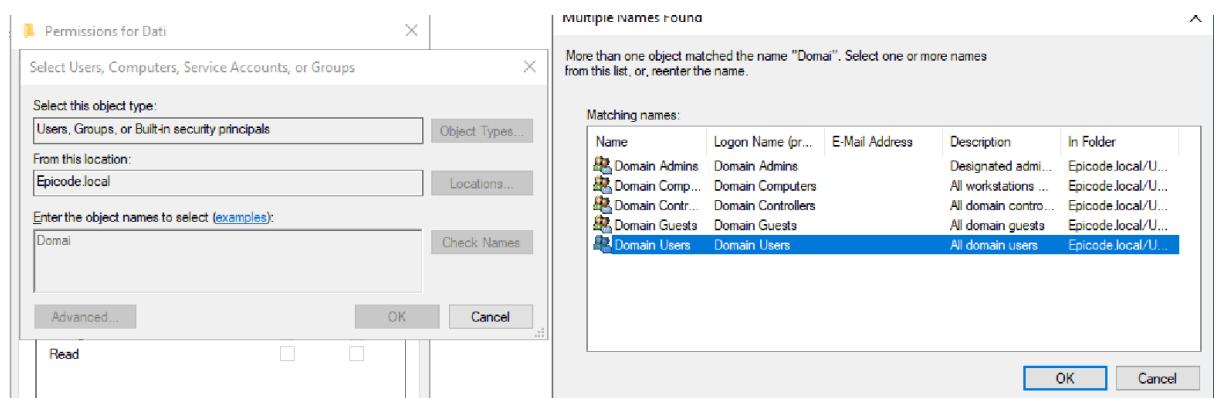
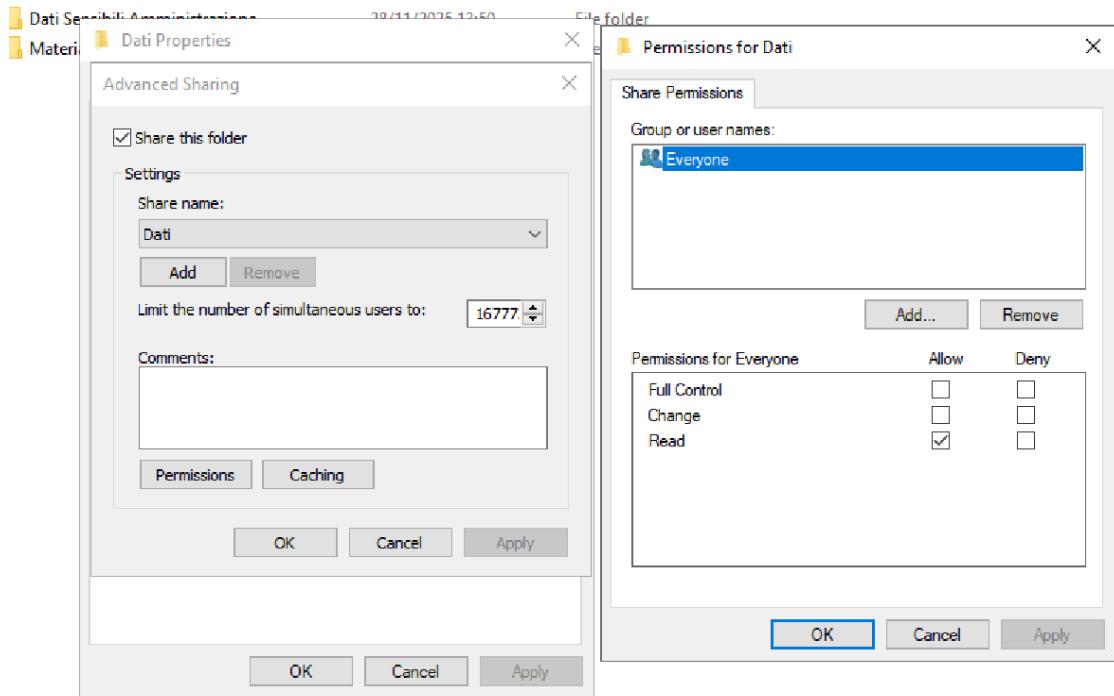
1. Dati Sensibili Amministrazione
2. Materiale Professori

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.



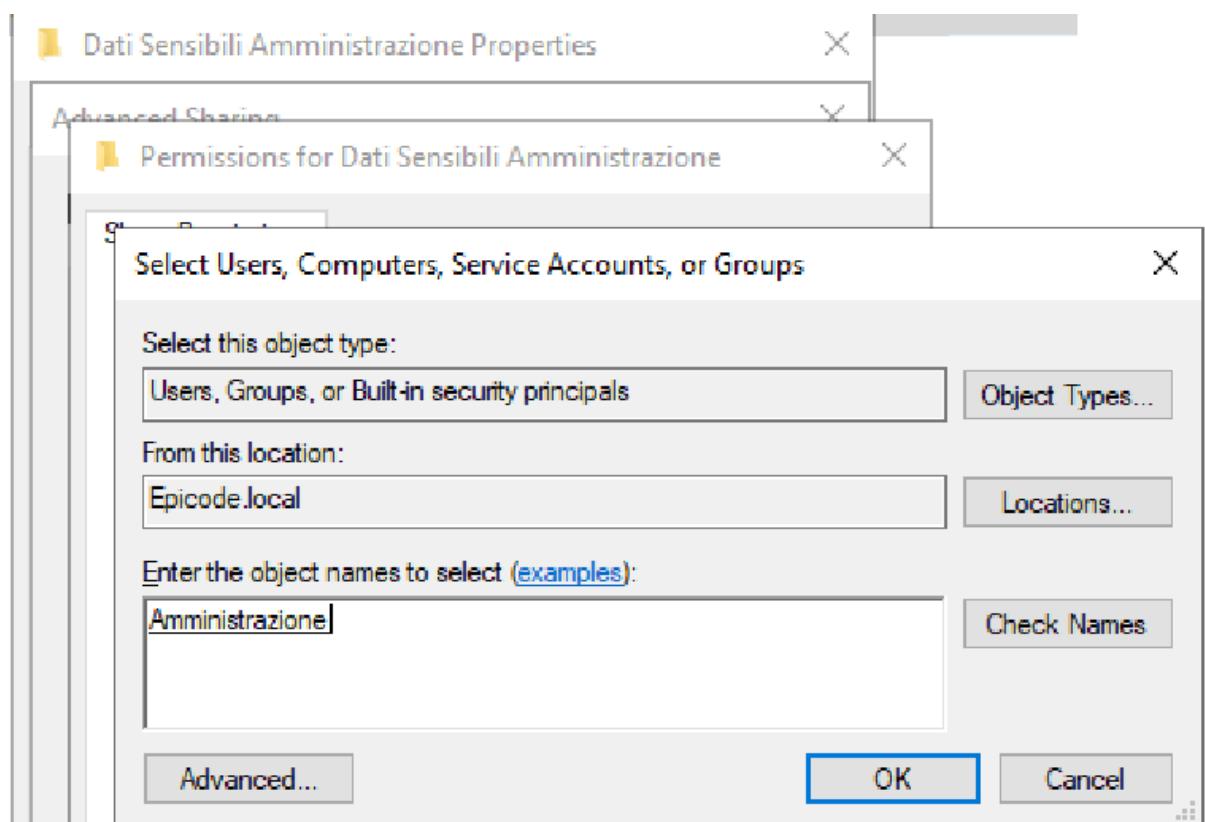


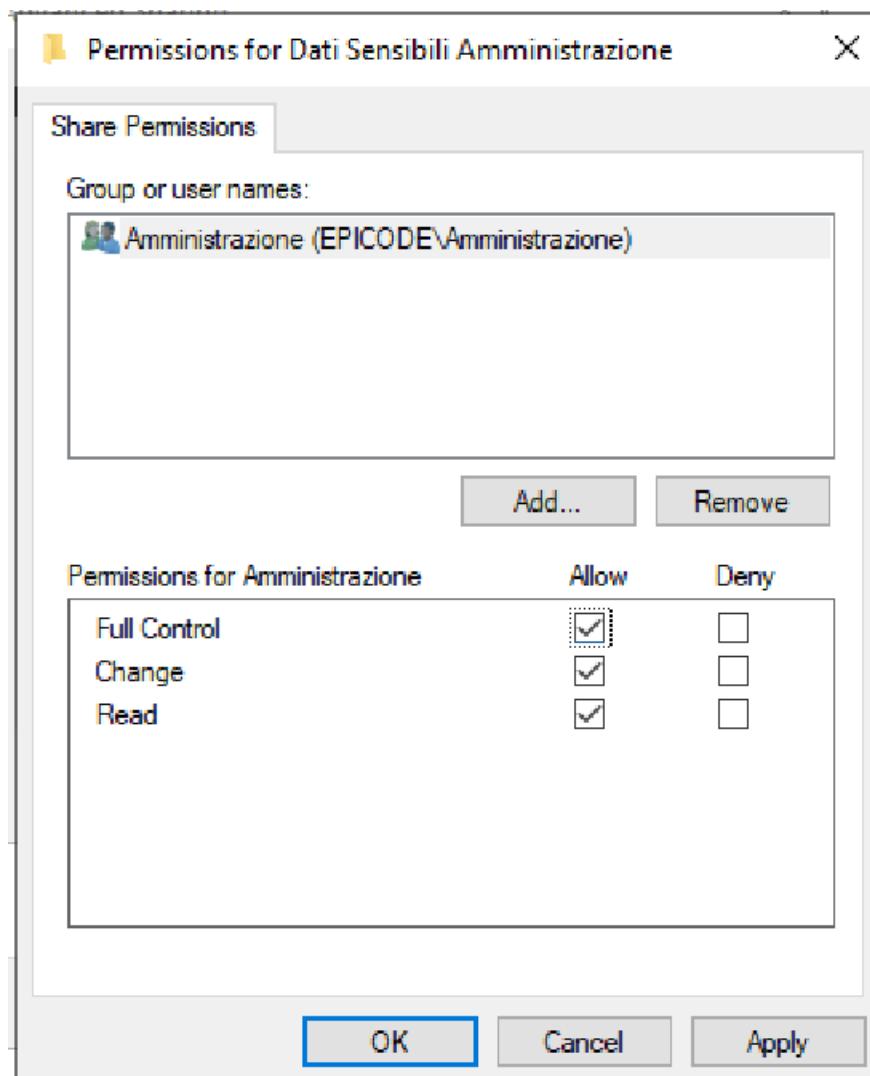
2. **Sicurezza (NTFS)**: Ho disabilitato l'ereditarietà sulle sottocartelle per definire permessi granulari.

Applicazione delle Restrizioni (Deny)

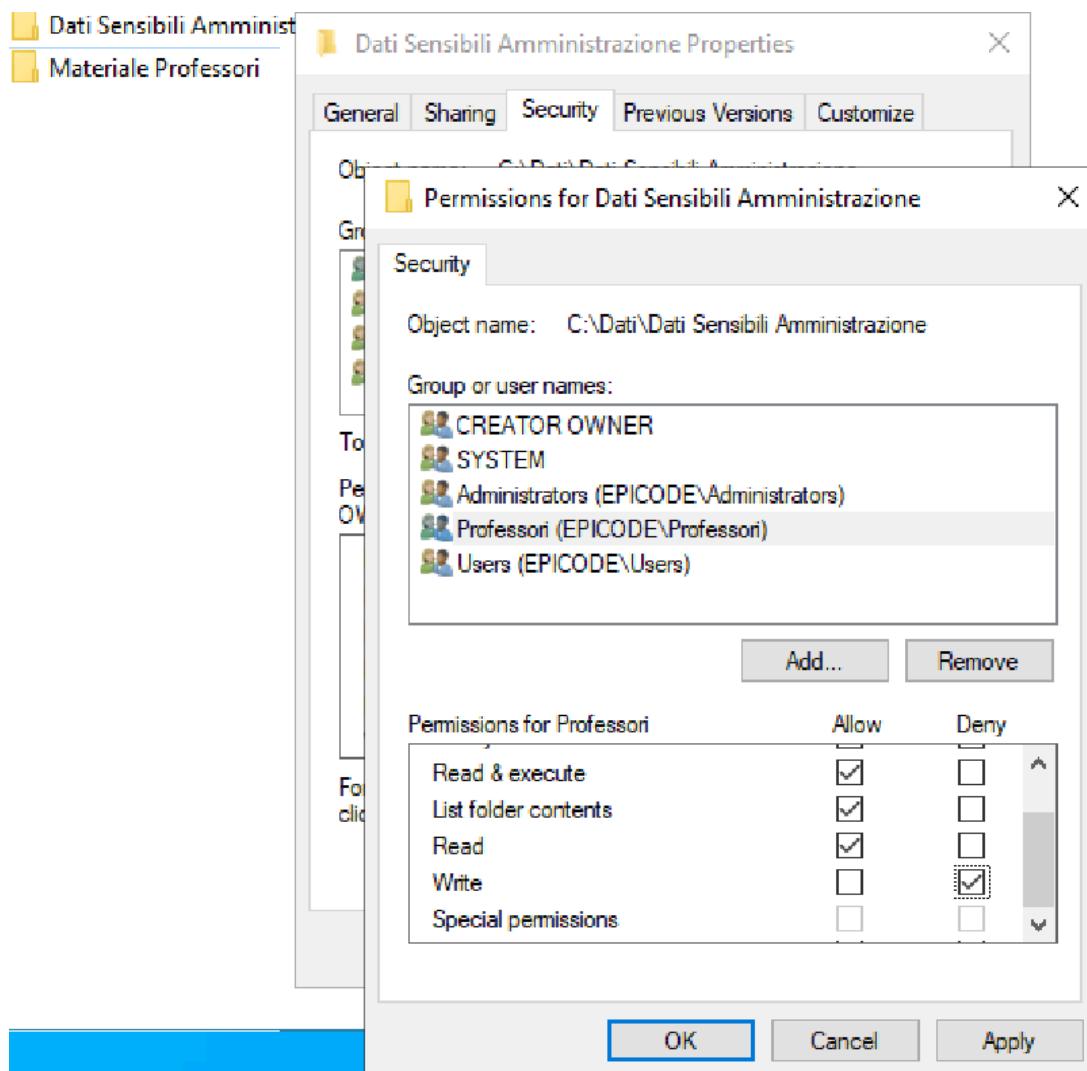
Ho configurato le Access Control Lists (ACL) con regole esplicite di blocco:

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

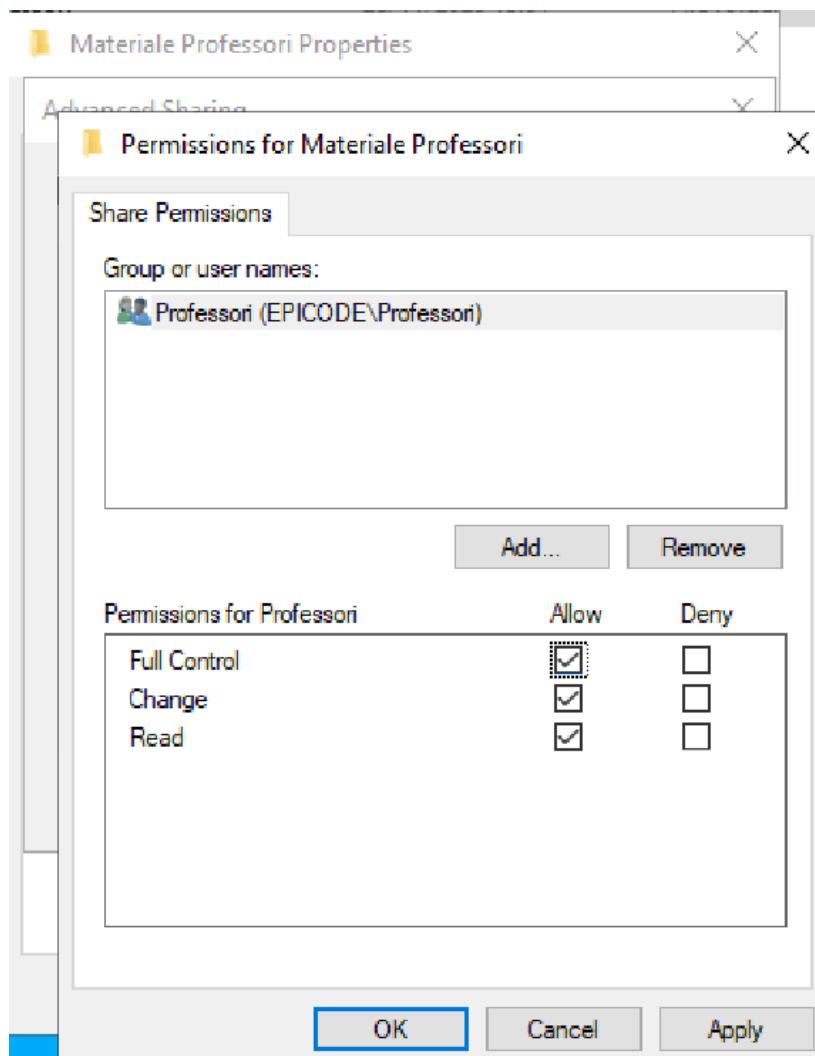




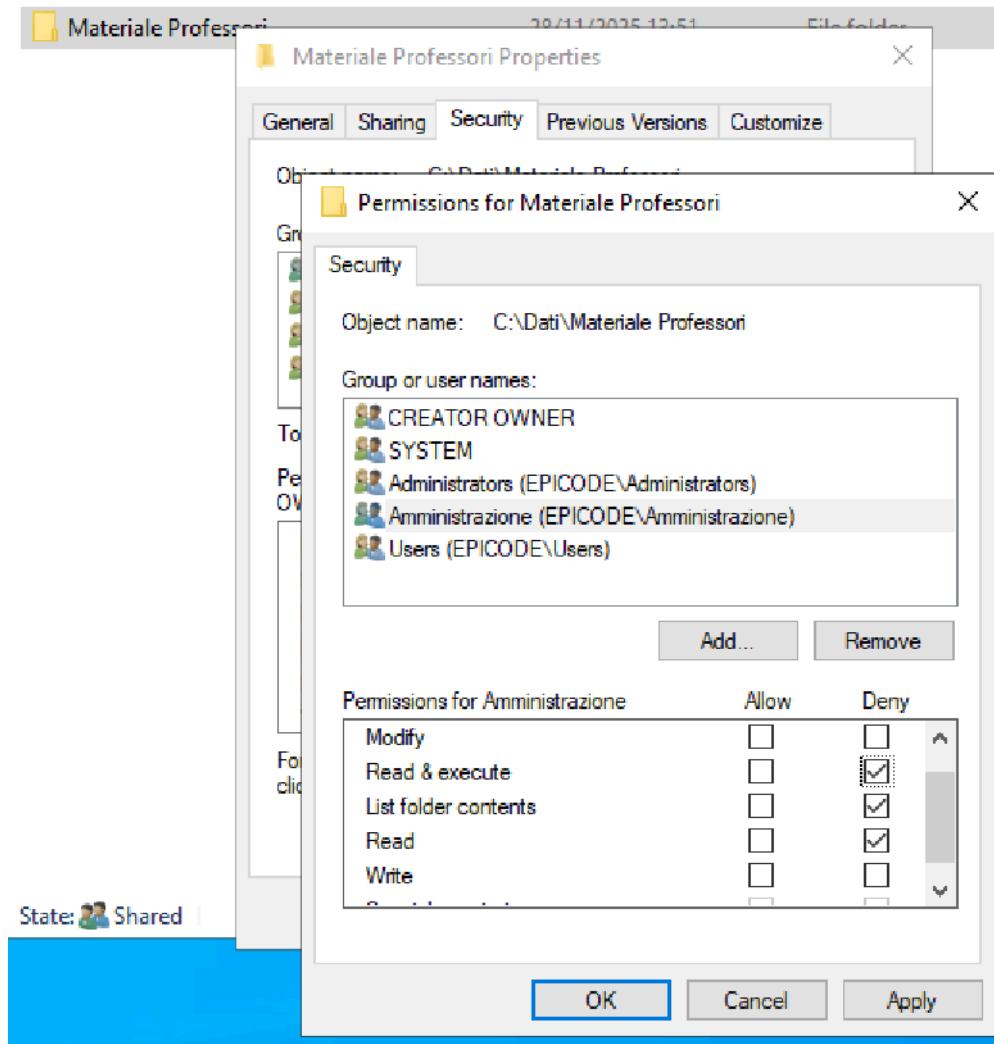
ma ho inserito una regola di **NEGA (Deny)** alla scrittura per il gruppo *Professori*.



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*.

The screenshot shows the Group Policy Management console. On the left, the navigation pane displays the forest 'Epicode.local' and its domains, with 'Epicode.local' and 'Default Domain' selected. The main pane is titled 'Professori' and shows a table of linked group policy objects. One row is selected, showing 'Policy Restrittive Utenti' at link order 1, enforced, with 'Link Enabled' set to 'Yes' and 'GPO Status' as 'Enabled'.

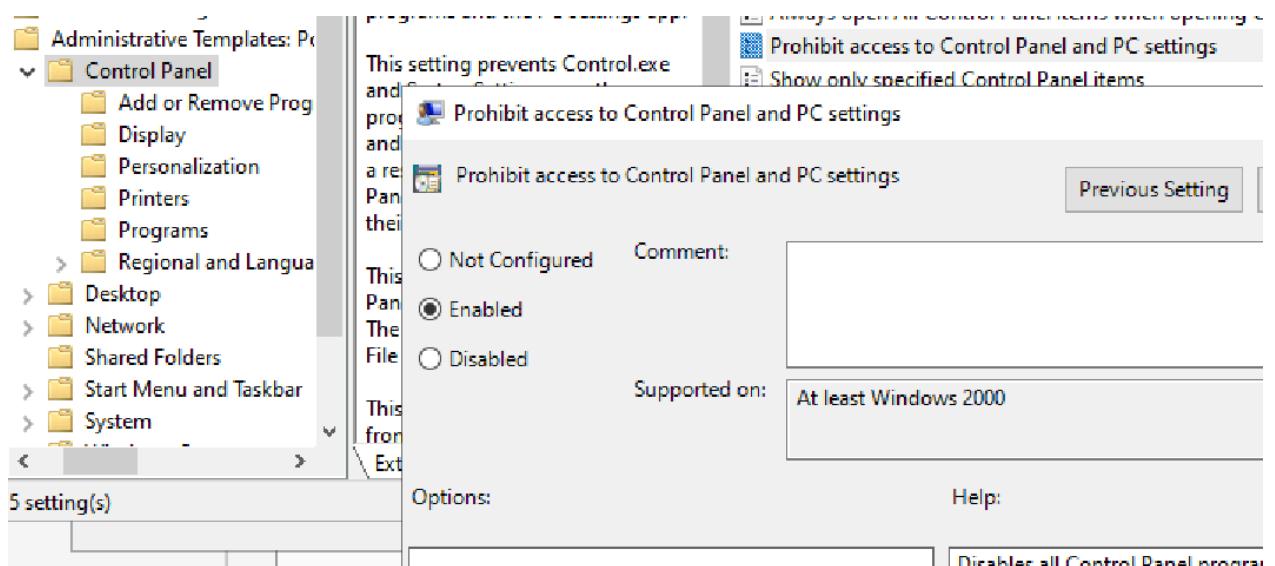
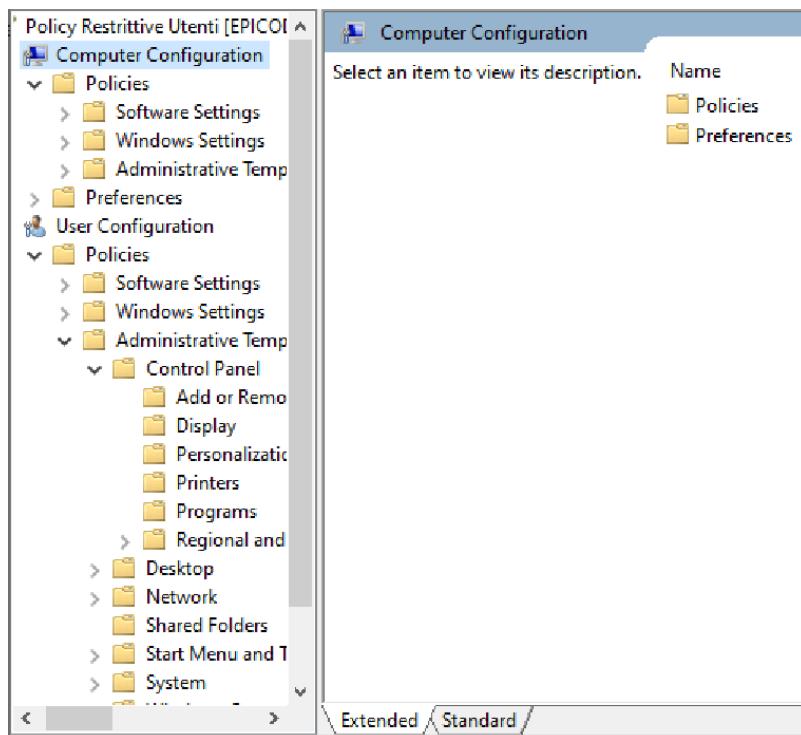
Ho configurato tre restrizioni principali:

- 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.

This screenshot shows the 'User Rights Assignment' dialog for the 'Allow log on through Remote Desktop Services' policy. The left pane shows the policy structure under 'Computer Configuration / Policies / Local Policies / User Rights Assignment'. The right pane lists various user rights, with 'Allow log on through Remote Desktop Services' highlighted. The 'Policy Setting' column shows 'Not Defined' for all items except the highlighted one, which has a blue background.

This screenshot shows the 'Properties' dialog for the 'Allow log on through Remote Desktop Services' policy. The left pane shows the policy structure under 'Computer Configuration / Policies / Local Policies / User Rights Assignment'. The right pane displays the 'User Rights Assignment' tab, which lists 'Administrators' and 'Amministrazione' as defined users. A note at the bottom states: 'This setting is not compatible with computers running Windows 2000 Service Pack 1 or earlier. Apply Group Policy objects containing this setting only to computers running a later version of the operating system.' Buttons for OK, Cancel, and Apply are at the bottom.

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.

The screenshot shows the 'User Configuration' section of the Group Policy Management console. The 'Policies' node is expanded, revealing 'Software Settings', 'Windows Settings', 'Administrative Templates', and 'System'. Under 'System', several policy settings are listed:

- Ctrl+Alt+Del Options
- Display
- Driver Installation
- Folder Redirection
- Group Policy
- Internet Communication Management
- Locale Services
- Logon
- Mitigation Options
- Power Management
- Removable Storage Access
- Scripts
- User Profiles
- Download missing COM components
- Century interpretation for Year 2000
- Restrict these programs from being launched from Help
- Do not display the Getting Started welcome screen at logon
- Custom User Interface
- Prevent access to the command prompt

The screenshot shows the details for the 'System' policy setting. It describes how this setting prevents Windows from running specified programs. If enabled, users cannot run programs added to the list of disallowed applications. If disabled, users can run any programs. This policy setting only affects programs started by the File Explorer.

Prevents Windows from running the programs you specify in this policy setting.

If you enable this policy setting, users cannot run programs that you add to the list of disallowed applications.

If you disable this policy setting or do not configure it, users can run any programs.

This policy setting only prevents users from running programs that are started by the File Explorer.

Setting

- Removable Storage Access
- Scripts
- User Profiles
- Download missing COM components
- Century interpretation for Year 2000
- Restrict these programs from being launched from Help
- Do not display the Getting Started welcome screen at logon
- Custom User Interface
- Prevent access to the command prompt
- Prevent access to registry editing tools
- Don't run specified Windows applications**
- Run only specified Windows applications

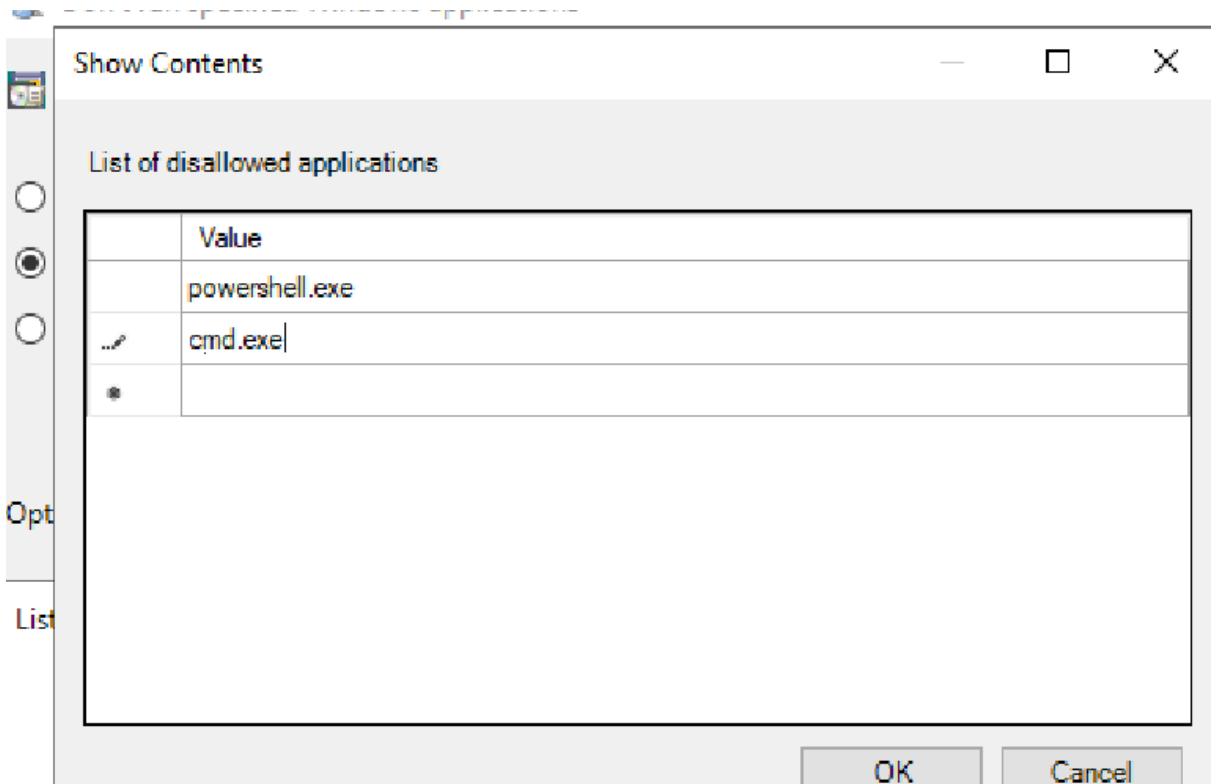
The screenshot shows the configuration page for the 'Don't run specified Windows applications' policy. It includes a title, a comment field, and configuration options:

Don't run specified Windows applications

Comment:

Not Configured Enabled Disabled

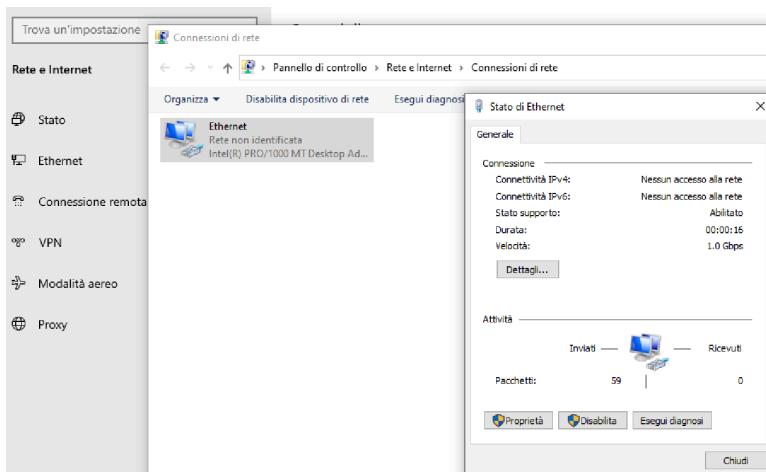
Supported on: [Add](#) [Import](#) [Export](#)

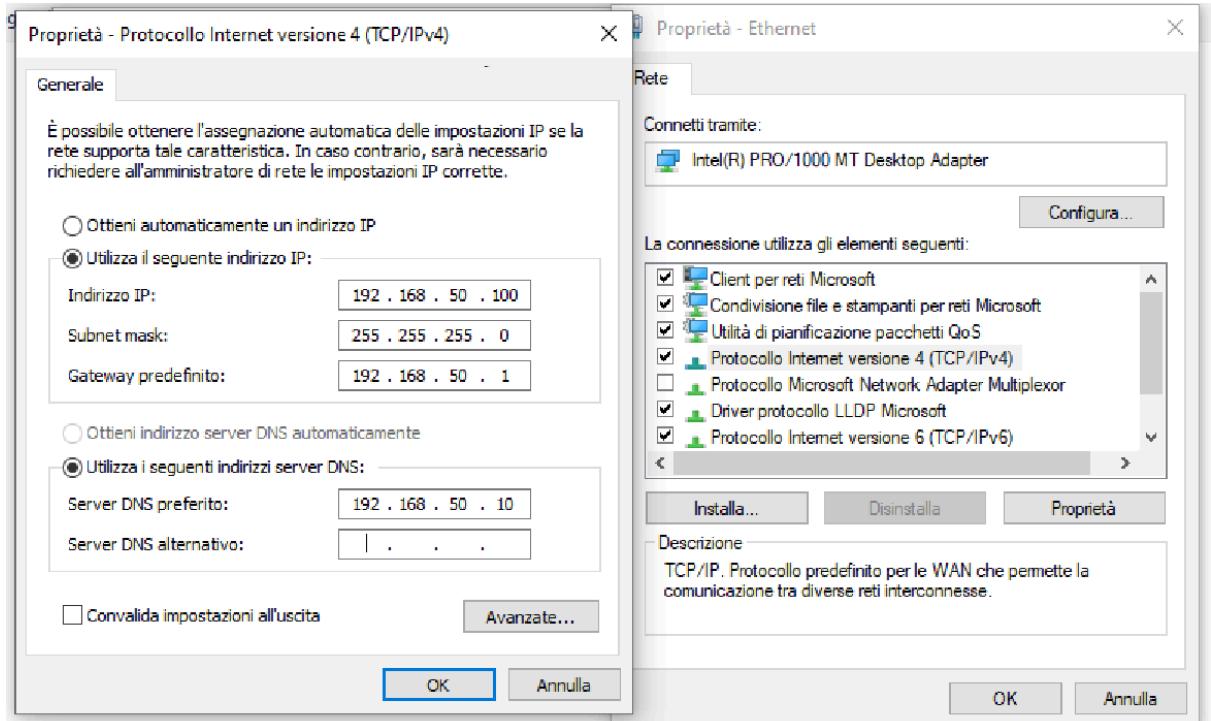


Verifica Finale (II Test)

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.

Home

Trova un'impostazione

- Sistema
- Assistente notifiche
- Alimentazione e sospensione
- Batteria
- Archiviazione
- Tablet
- Multitasking
- Proiezione su questo PC
- Esperienze condivise
- Appunti
- Desktop remoto
- Informazioni

Informazioni

Edizione: Windows 10 Pro N
Versione: 22H2
Data installazione: 08/09/2024
Build sistema operativo: 19045.2965
Esperienza: Windows Feature Experience Pack 1000.19041.1000.0

Copia

Modifica il codice Product Key o aggiorna l'edizione di Windows

Leggi il Contratto di Servizi Microsoft
Leggi le Condizioni di licenza software

Impostazioni correlate

Impostazioni di BitLocker
Gestione dispositivi
Desktop remoto
Protezione sistema
Impostazioni di sistema avanzate
Rinomina questo PC (avanzate)

Informazioni
Invia feedback

Proprietà del sistema

Protezione sistema		Connessione remota
Nome computer	Hardware	Avanzate
Windows utilizza le seguenti informazioni per identificare il computer all'interno della rete.		
Descrizione computer:		
Ad esempio: "Computer cucina" o "Computer di Maria".		
Nome completo computer: DESKTOP-8CAJIRTO		
Gruppo di lavoro: WORKGROUP		
Per aggiungere il computer a un dominio o a un gruppo di lavoro tramite una procedura guidata, scegliere ID di rete.		
ID di rete... Cambia...		
Per rinominare il computer oppure modificare il suo dominio o gruppo di lavoro, scegliere Cambia.		
Cambia...		

Cambiamenti dominio/nome computer

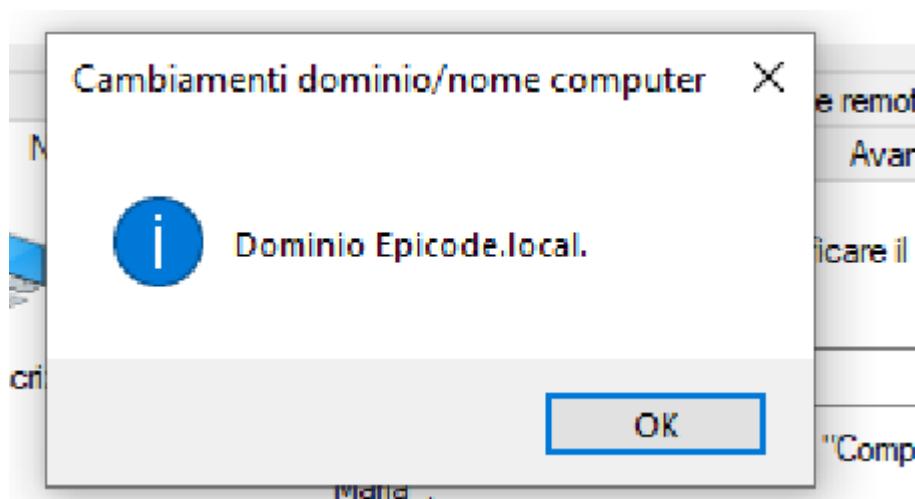
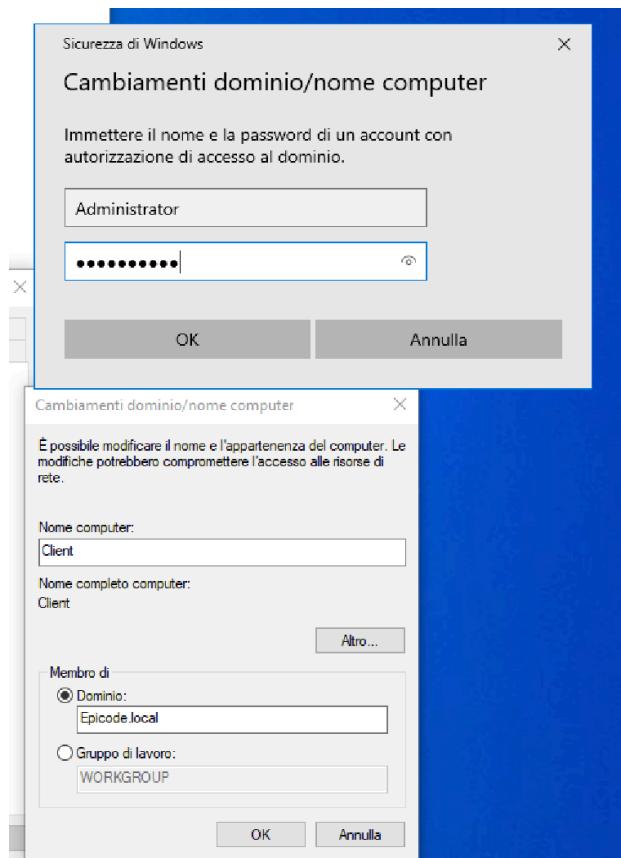
È possibile modificare il nome e l'appartenenza del computer. Le modifiche potrebbero compromettere l'accesso alle risorse di rete.

Nome computer: Client
Nome completo computer: Client

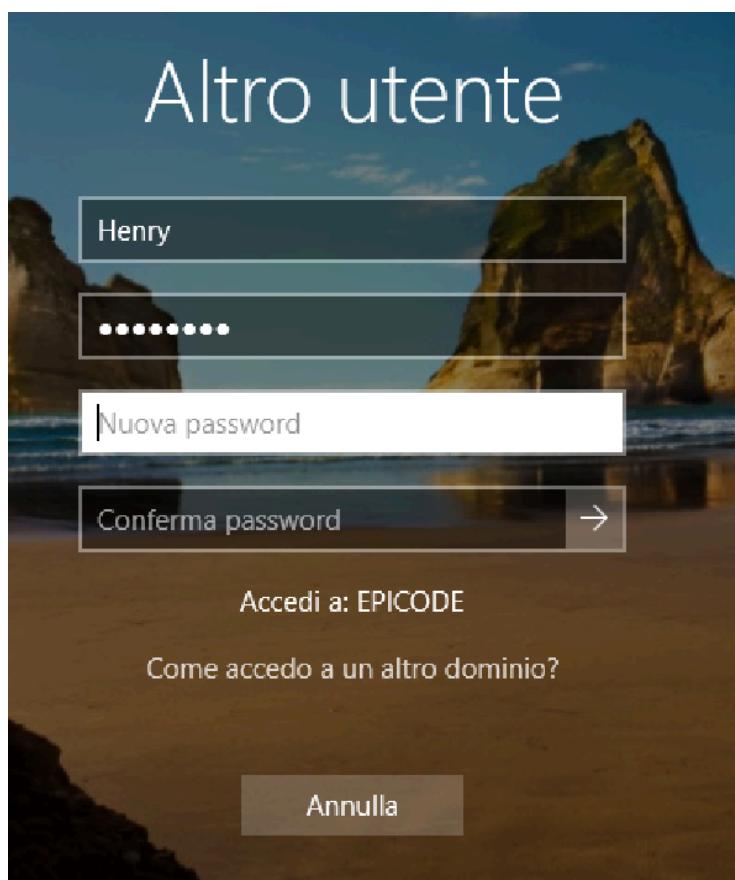
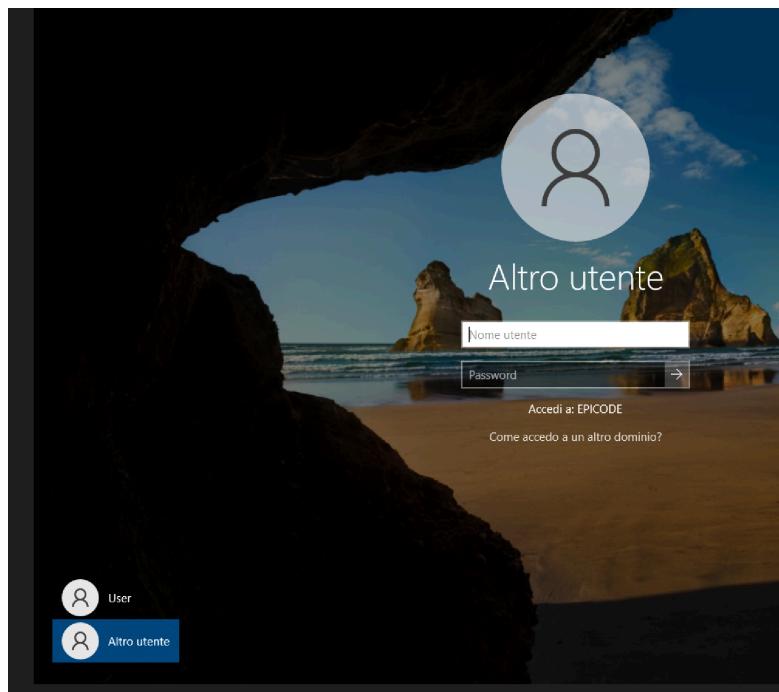
Membro di:

- Dominio: Epicode.local
- Gruppo di lavoro: WORKGROUP

OK Annulla Apply

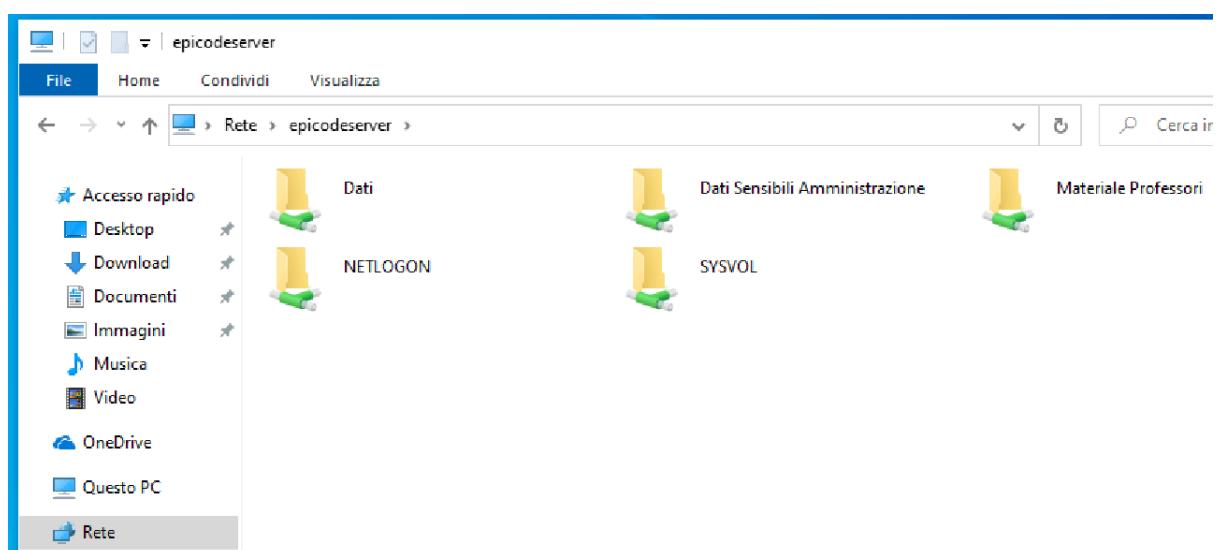
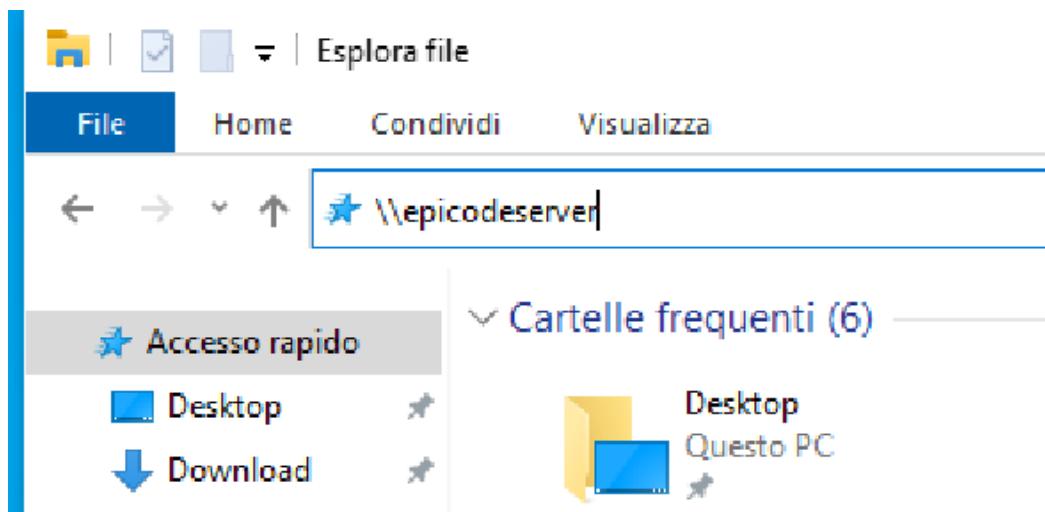


3. Ho effettuato l'accesso con l'utente **Henry** (simulando un membro del gruppo Professori) così da dimostrare che dovevo cambiare la password temporanea per effettuare il nuovo accesso, dato che solo l'utente **Paolo** (aka Akirad) non la doveva cambiare .



Risultati dei Test:

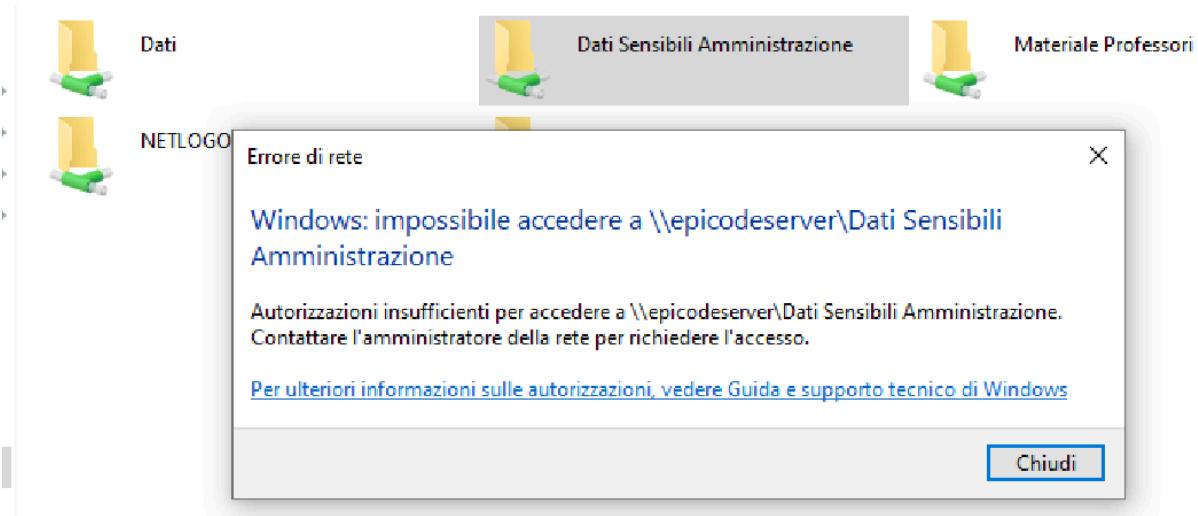
- Tentativo di accesso a \\EpicodeServer\\Dati\\Materiale



Professori: RIUSCITO

Nome	Ultima modifica	Tipo	Dimensione
Dati Sensibili Amministrazione	28/11/2025 13:50	Cartella di file	
Materiale Professori	28/11/2025 13:51	Cartella di file	

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



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

Conclusioni 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.