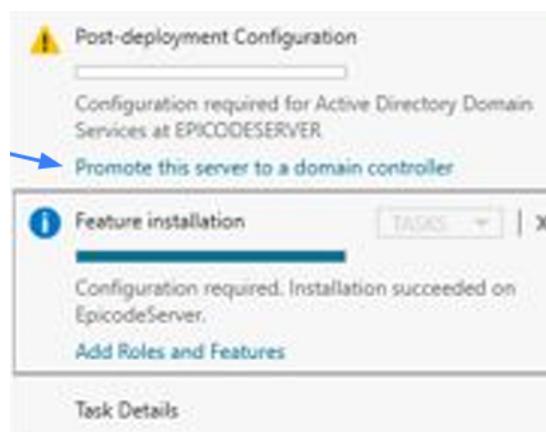


Step0.Creazione Foresta

Per la creazione della foresta iniziamo andando su manage



Si aprirà una finestra, ora andiamo su promote to a Domain server controller



Inseriamo Add new forest e diamo il nome al dominio, in questo caso Epicode.local, ed inseriamo la password e facciamo installa

The screenshot shows the "Add a new forest" configuration wizard. It includes the following fields:

- Select the deployment operation:**
 - Add a domain controller to an existing domain
 - Add a new domain to an existing forest
 - Add a new forest
- Specify the domain information for this operation:**

Root domain name:
- Select functional level of the new forest and root domain:**

Forest functional level:

Domain functional level:
- Specify domain controller capabilities:**

Domain Name System (DNS) server

Global Catalog (GC)

Read only domain controller (RODC)
- Type the Directory Services Restore Mode (DSRM) password:**

Password:

Confirm password:

Una volta riavviato possiamo vedere che il nome nel user ha una aggiunta ovvero il nome del dominio.

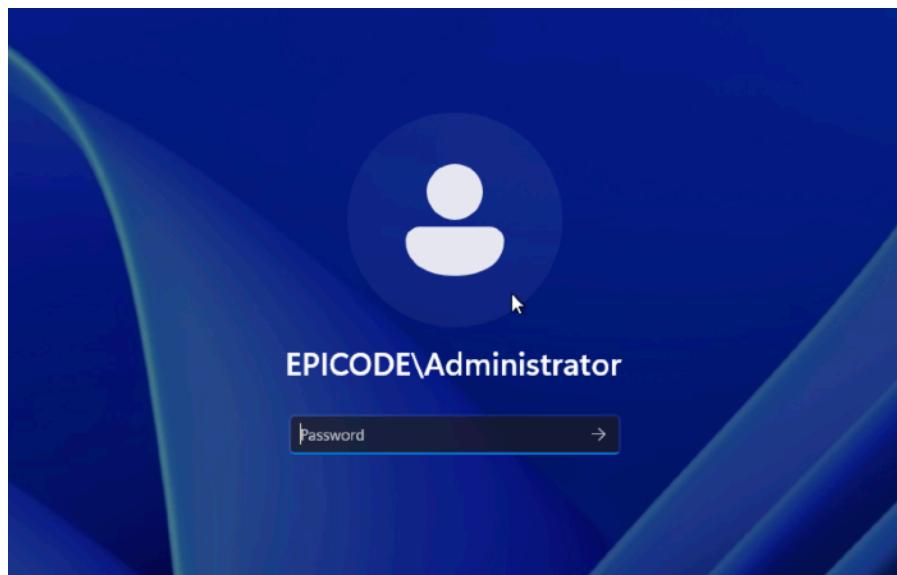


Esercizio di oggi: Creazione di Gruppi in Windows Server 2022

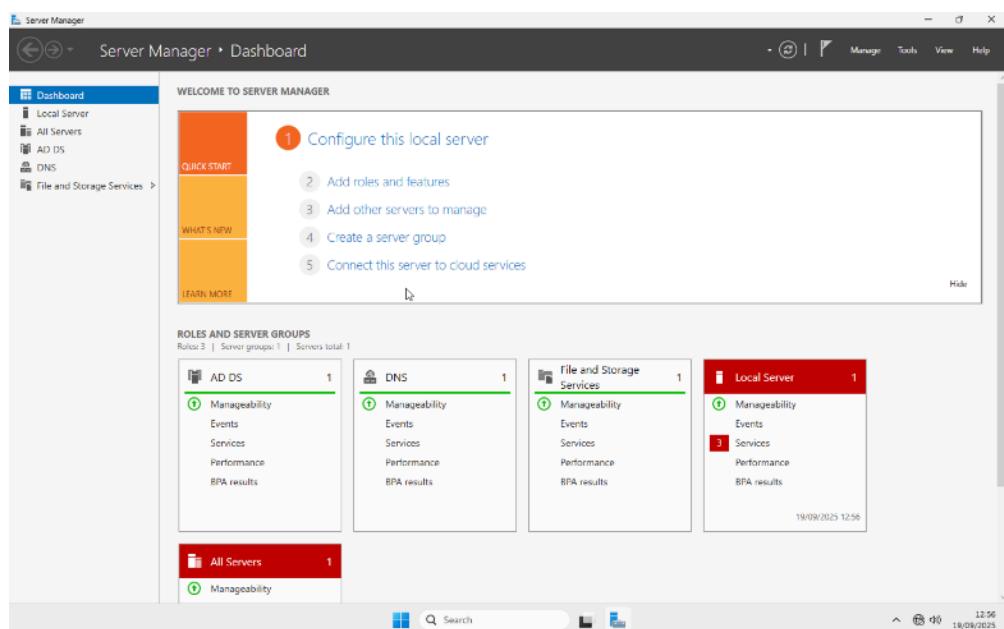
Obiettivo: Lo scopo di questo esercizio è di familiarizzare con la gestione dei gruppi di utenti in Windows Server 2022. Imparerai a creare gruppi, assegnare loro permessi specifici e comprendere l'importanza della gestione dei gruppi per la sicurezza e l'amministrazione del sistema.

Step1. Creazione e gestione utenti

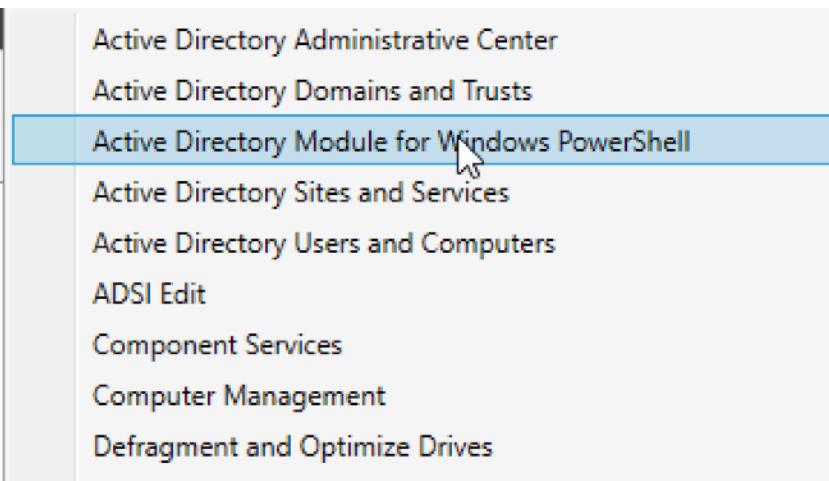
Facciamo l'accesso al windows server precedentemente



Una volta che si è avviata la macchina apparirà questa schermata



Andiamo in alto a destra tools e andiamo su add Directory Users and Computers



A questo punto abbiamo già creato in precedenza il dominio “epicode.local” ora creiamo i vari gruppi di lavoro

The screenshot shows the 'Active Directory Users and Computers' console. The left navigation pane shows the 'epicode.local' domain structure, including 'Amministrazione', 'BuiltIn', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Hacker1', 'Managed Service Account', and 'Users'. The right pane displays a table of objects:

Name	Type	Description
Condor	User	
Eliot	User	
Robot	Security Group...	

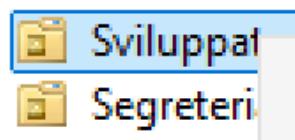
Col tasto destro su “epicode.local” facciamo new e Organizational unit

The screenshot shows the 'Active Directory Users and Computers' console with a context menu open over the 'epicode.local' domain node. The menu options include:

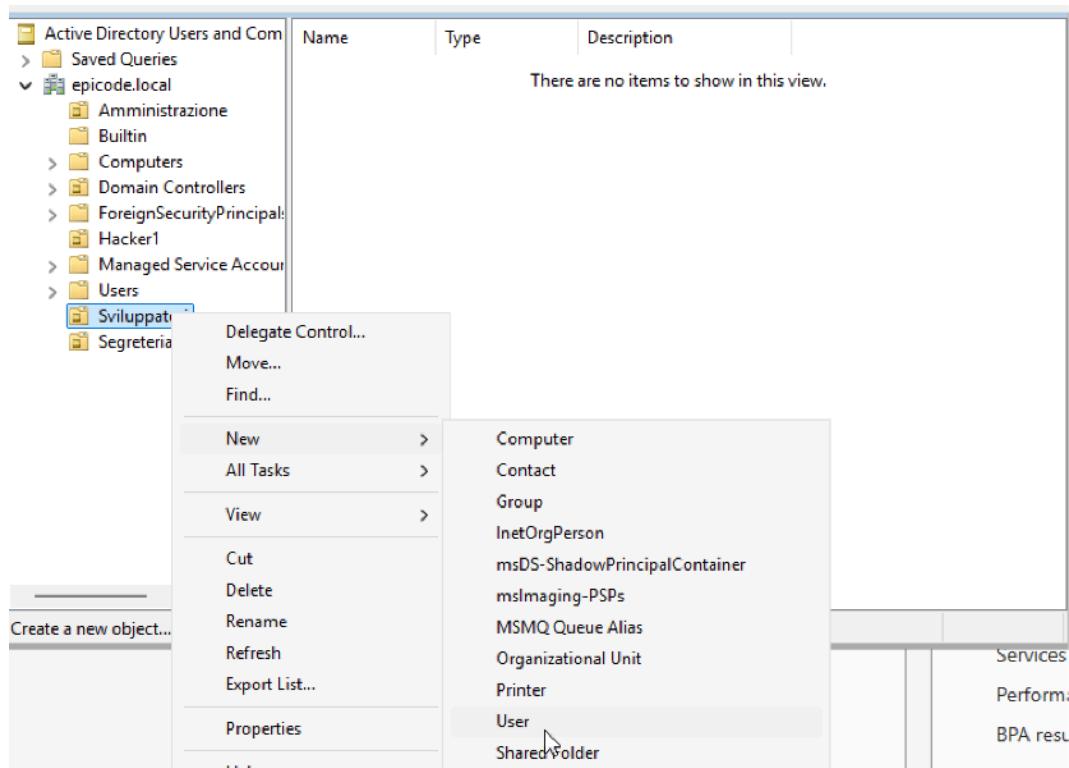
- Delegate Control...
- Find...
- Change Domain...
- Change Domain Controller...
- Raise domain functional level...
- Operations Masters...
- New > Computer
- All Tasks > Contact
- View > Group
- Refresh > InetOrgPerson
- Export List... > msDS-ShadowPrincipalContainer
- Properties > msImaging-PSPs
- Help > MSMQ Queue Alias
- Organizational Unit > Organization Unit
- Printer
- User
- Shared Folder

The 'Organizational Unit' option is highlighted with a mouse cursor.

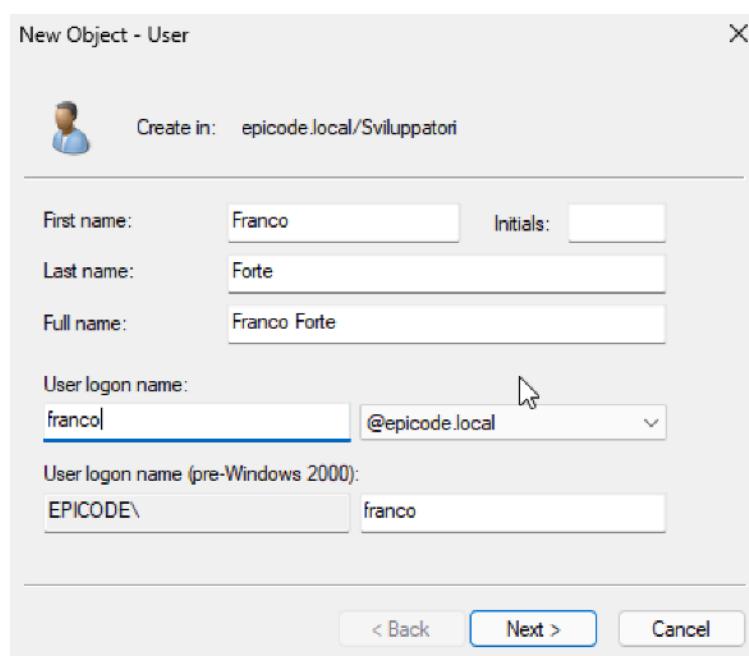
E creiamo due sezioni “Sviluppatori” e “Segreteria”



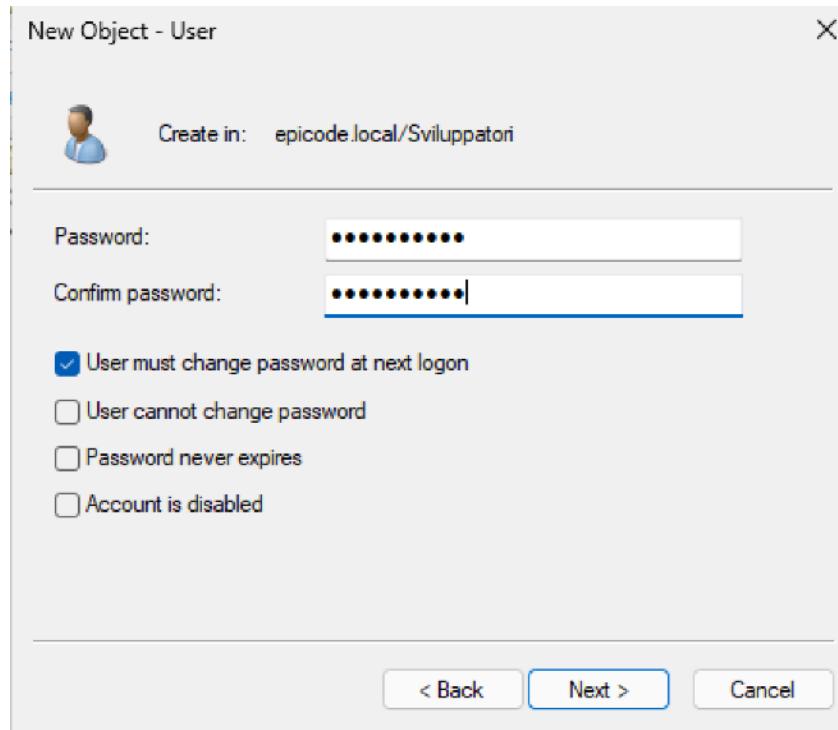
Ora nelle due sezioni aggiungiamo dei utenti, andiamo su sviluppatori-tasto destro-new-user



Aggiungiamo il primo User della sezione Sviluppatori ovvero Franco Forte con login user franco



Ci chiederà di inserire una password con varie opzioni, selezioni la prima e faccio next



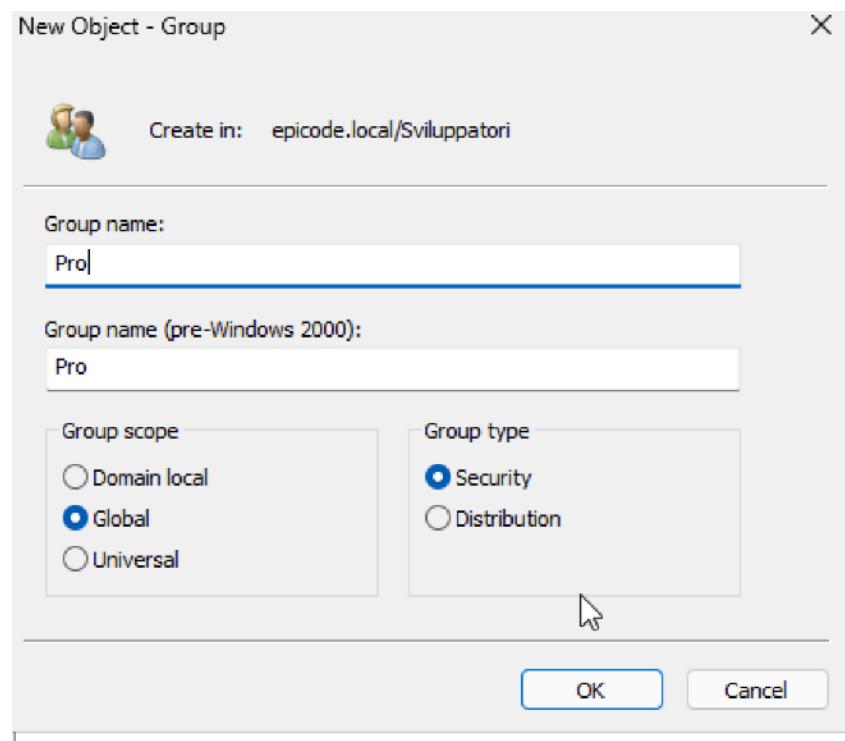
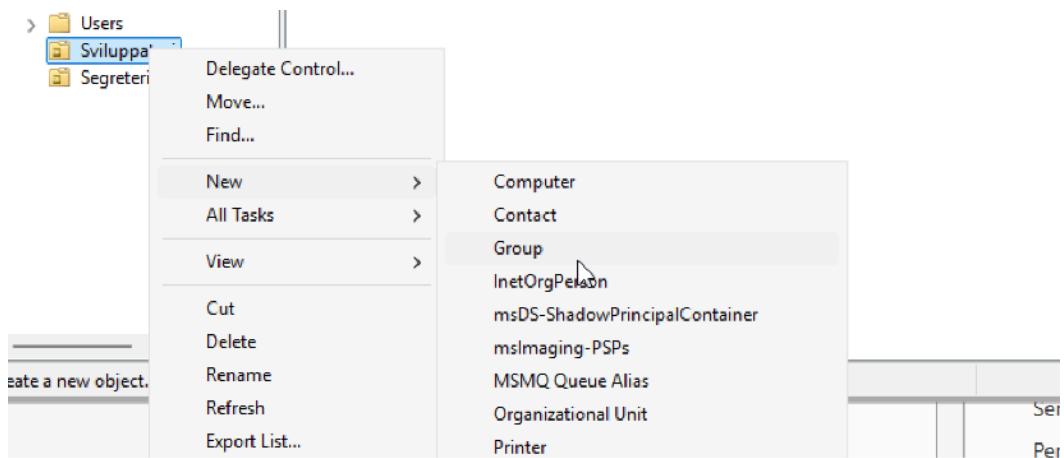
Spiegazione delle opzioni

- **User must change password at next logon:** Selezionando questa casella, l'utente sarà obbligato a **cambiare la password** che gli è stata assegnata la prima volta che si collega al sistema. Questa è una misura di sicurezza comune per garantire che solo l'utente conosca la propria password e che non si utilizzi una password predefinita nota all'amministratore.
 - **User cannot change password:** Spuntando questa opzione, l'utente non avrà l'autorizzazione di **modificare la propria password**. Questa impostazione viene usata spesso per account di servizio o account amministrativi condivisi, dove si vuole che la password rimanga fissa e gestita solo dagli amministratori di sistema.
 - **Password never expires:** Scegliendo questa opzione, la password dell'utente non sarà soggetta alle **politiche di scadenza** del sistema. Normalmente, le password devono essere cambiate periodicamente (ad esempio ogni 90 giorni) per motivi di sicurezza. Selezionare questa casella annulla questa regola per l'utente specifico. È utile per account di servizio che eseguono processi automatici e non necessitano di un cambio password regolare.
 - **Account is disabled:** Questa opzione **disabilita l'account**, impedendo all'utente di accedere al sistema. È utile per gli account di nuovi dipendenti prima del loro primo giorno di lavoro o per gli account di dipendenti che hanno lasciato l'azienda, in modo da bloccare l'accesso immediatamente.
-

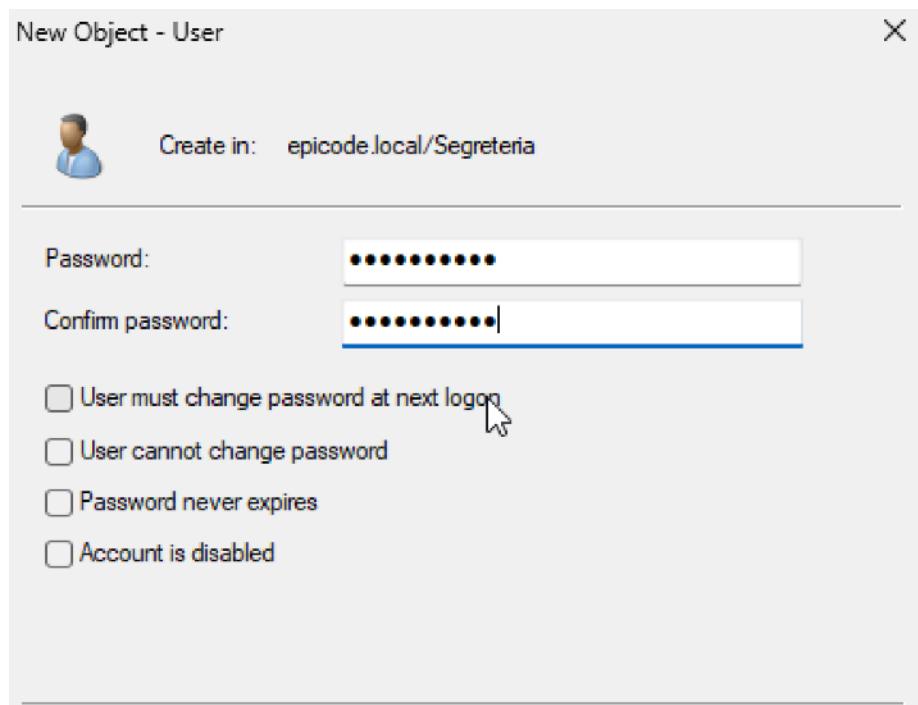
Aggiungiamo anche un secondo utente, sempre nella sezione sviluppatori, ovvero Giovanni Storti

Name	Type	Description
Franco Forte	User	
Giovanni Sto...	User	

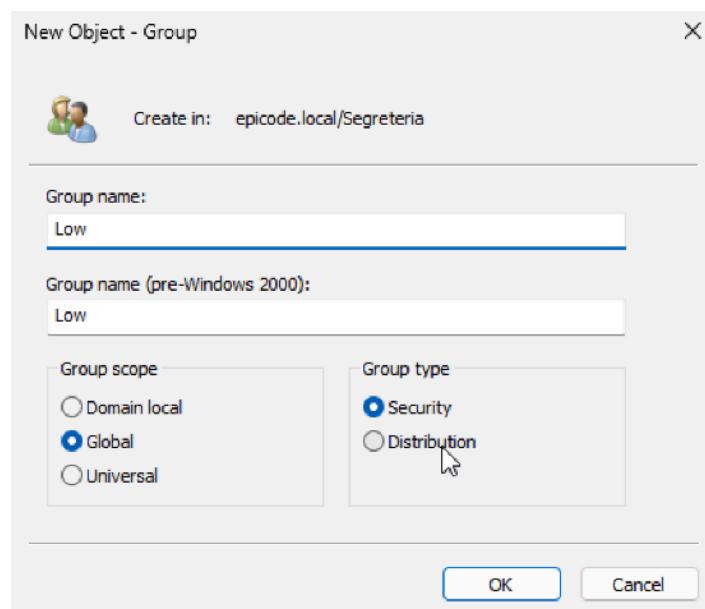
Ora creo il gruppo dentro Sviluppatori e lo chiamo Pro



Ora faccio lo stesso procedimento su Segreteria inserendo 2 user con più privilegi ed un terzo (Beta) senza che mi servirà dopo per accedere alla rete, tra le opzioni faccio in modo che non abbia opzioni attivate per quanto riguarda la password.



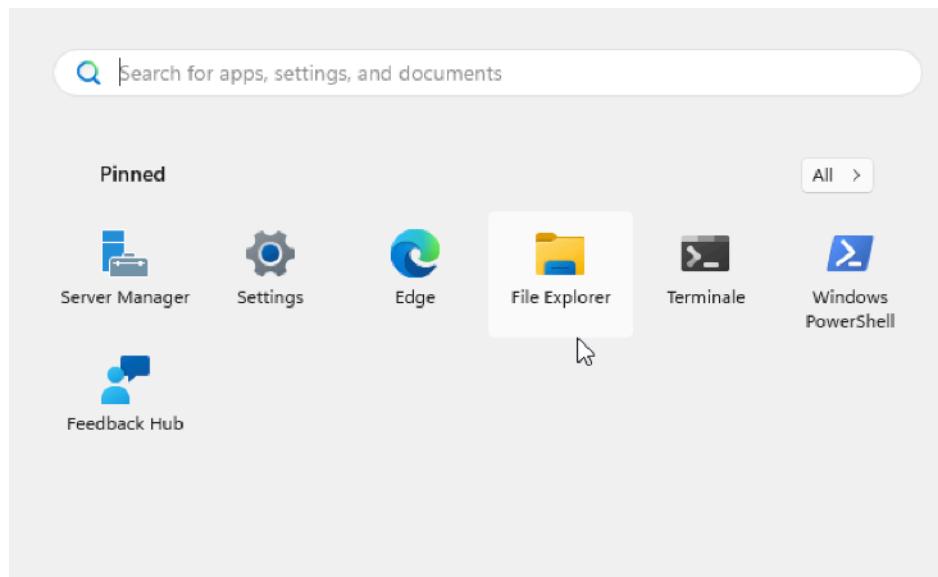
Creo anche in questa sezione un gruppo (LOW) che mi servirà dopo per dare i privilegi.



Name	Type	Description
Aldo Baglio	User	
beta	User	
Giacomo Po...	User	
Low	Security Group...	

Step2.Creazione dei file con privilegi

Apro file Explorer



Vado su “Questo pc” ed creo un file con il nome “Azienda”

Azienda	19/09/2025 13:14	File folder
---------	------------------	-------------

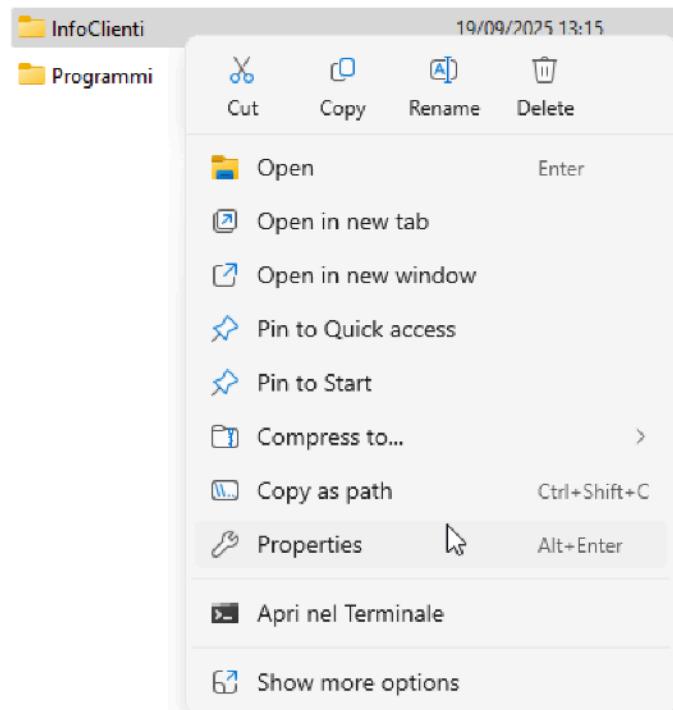
Sentro di essa creo altre due cartelle ed inserisco dei file di testo come esempio.

Programmi	19/09/2025 13:14	File folder
InfoClienti	19/09/2025 13:15	File folder

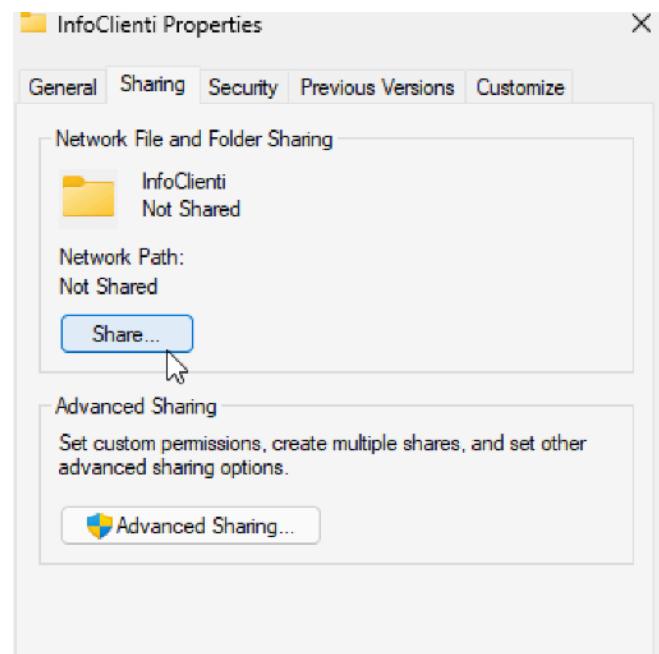
File:

Esempio	19/09/2025 13:15	Text Document	0 KB
Dati clienti	19/09/2025 13:15	Text Document	0 KB

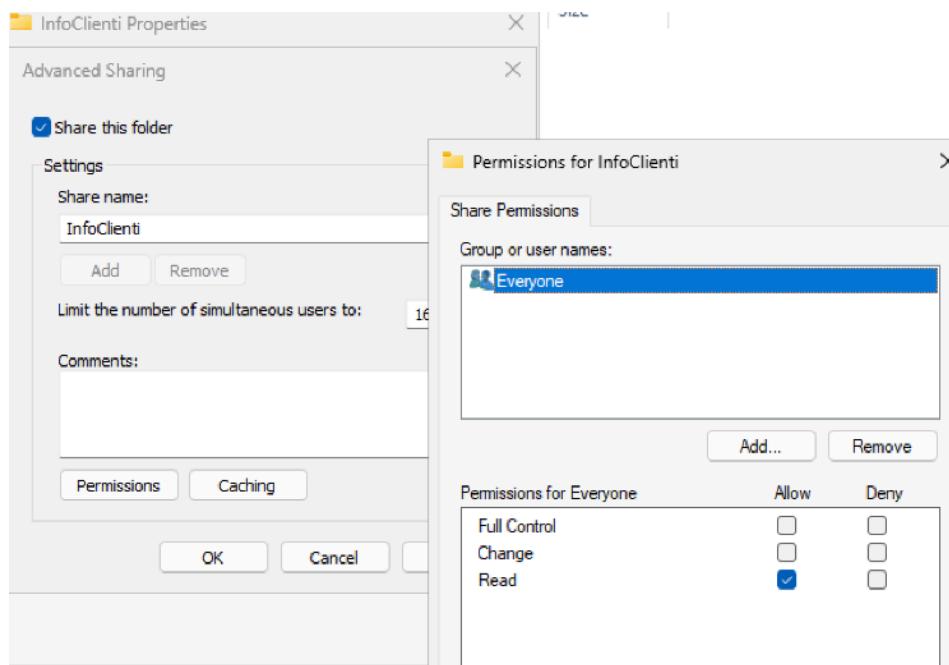
Ora voglio dare l'accesso alla cartella InfoClienti solo agli utenti che fanno parte del gruppo LOW ovvero Aldo e Giacomo. Quindi sulla cartella faccio tasto dentro e poi proprietà



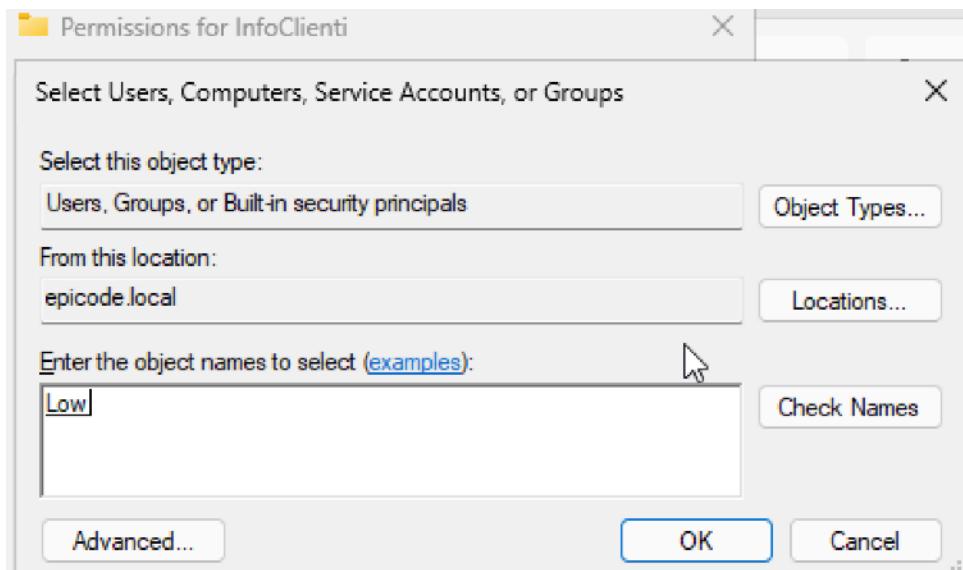
Dopo di che vado su sharing e advanced sharing



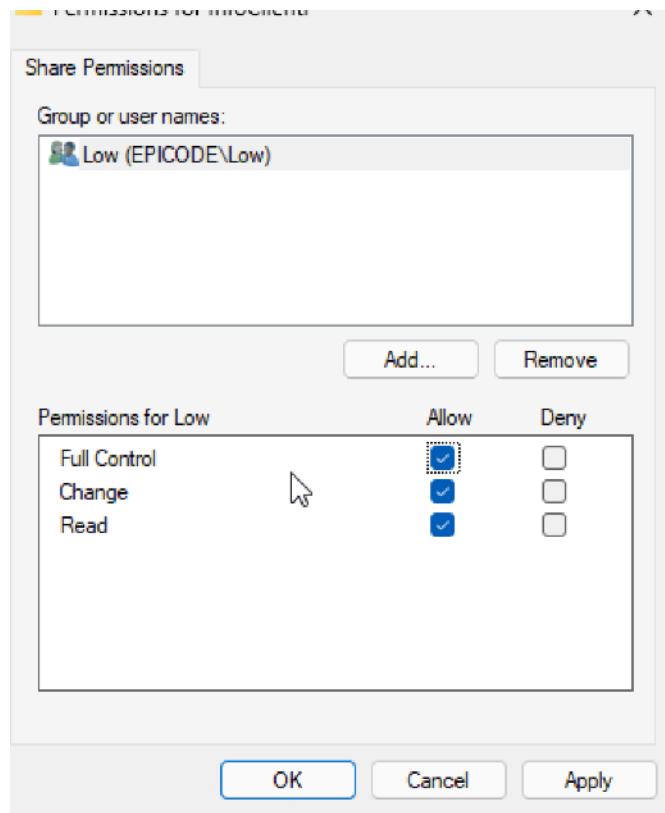
Ora posso vedere che per ora ed accessibile ad tutti quindi faccio delete e poi add



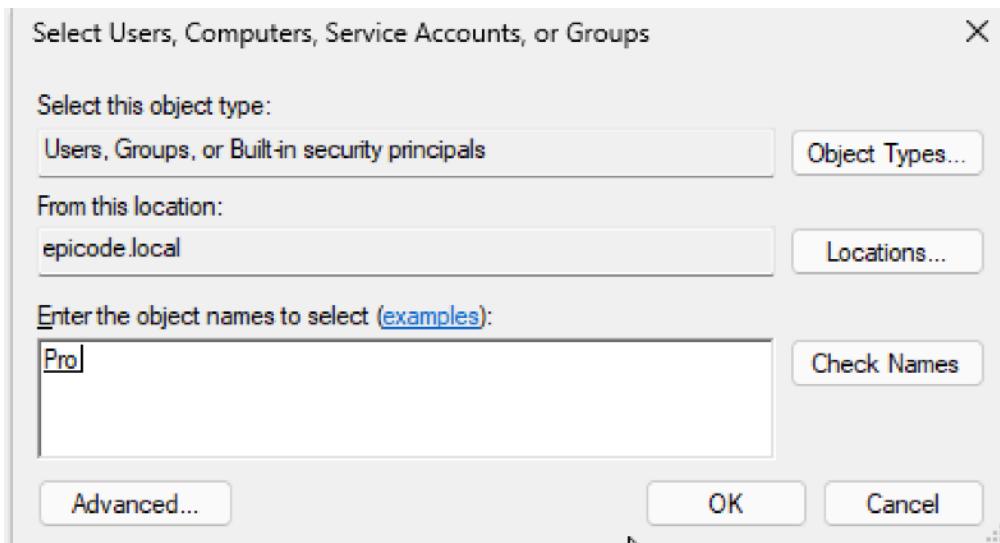
Aggiungo il nome del gruppo Low e per sicurezza faccio check names per verificare che il nome inserito sia giusto



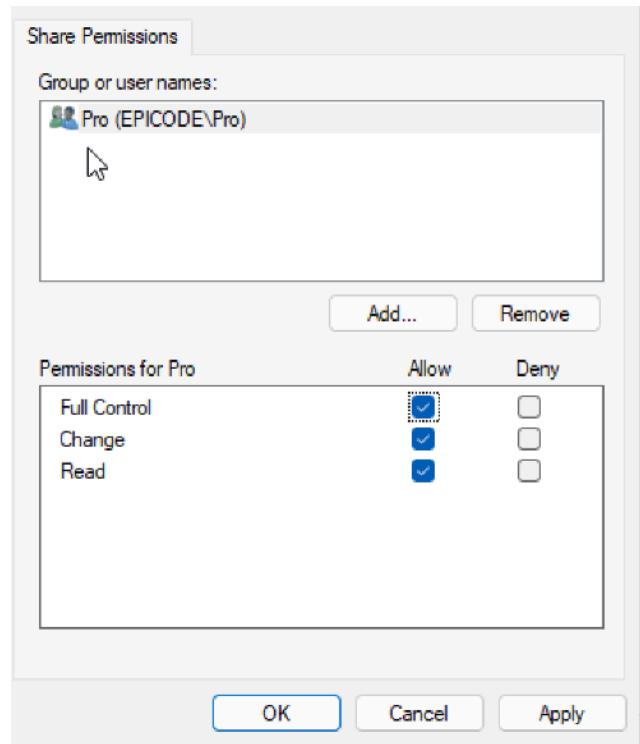
Dopo di che do pieno controllo ai membri Low



Faccio la stessa cosa per l'altra cartella “Programmi” con i permessi solo ai utenti nel gruppo Pro

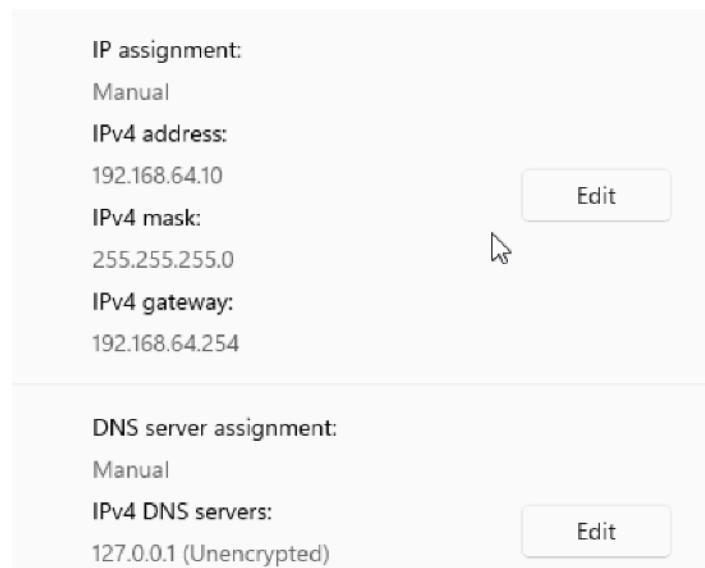


Anche in questo caso do permessi completi ai membri nei Pro



Step3. Collegamento tra il windows server e windows 10

Come prima cosa configuro la rete delle due macchine e controllo che comunichino

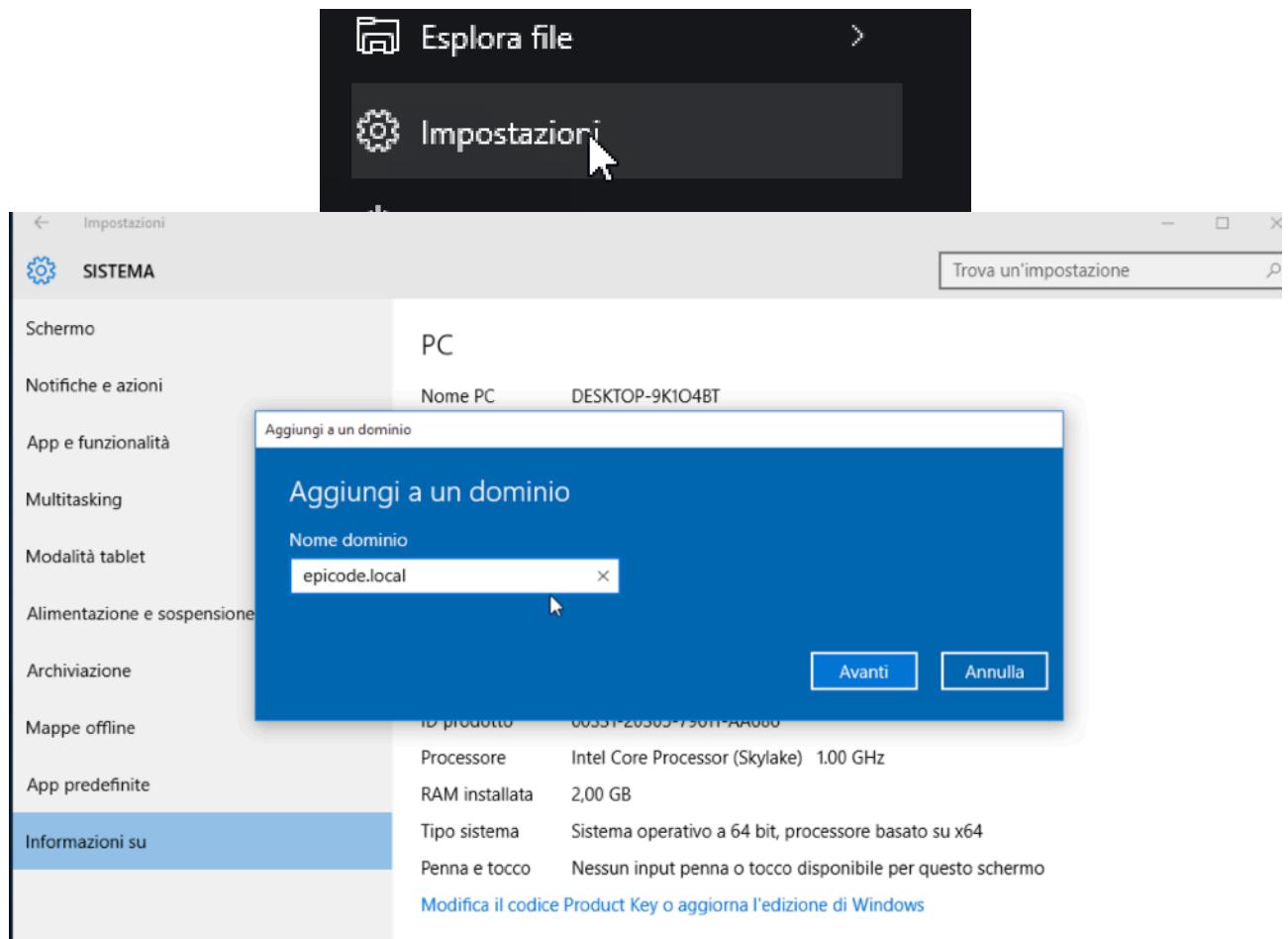


```
C:\Users\user>ping 192.168.64.10

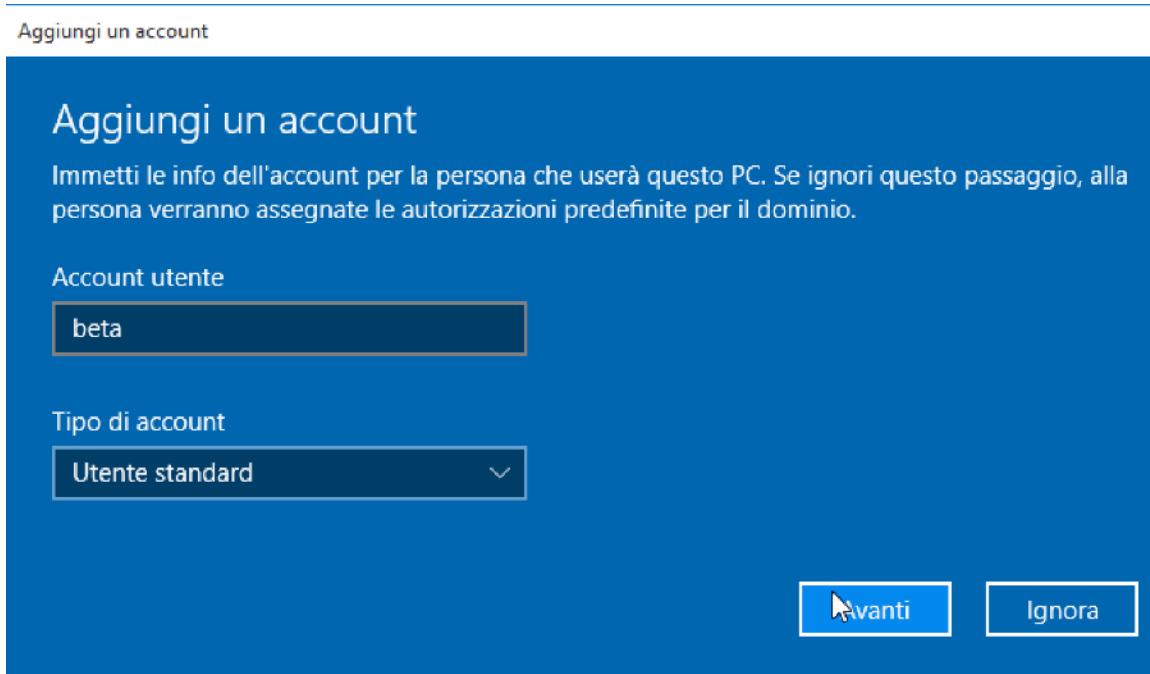
Esecuzione di Ping 192.168.64.10 con 32 byte di dati:
Risposta da 192.168.64.10: byte=32 durata=11ms TTL=128
Risposta da 192.168.64.10: byte=32 durata=2ms TTL=128
Risposta da 192.168.64.10: byte=32 durata=5ms TTL=128
Risposta da 192.168.64.10: byte=32 durata=1ms TTL=128

Statistiche Ping per 192.168.64.10:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 1ms, Massimo = 11ms, Medio = 4ms
```

Fatti tutti i collegamenti vado su impostazioni-informazioni su- ed aggiungi ad un dominio ed inserisco il dominio creato precedentemente

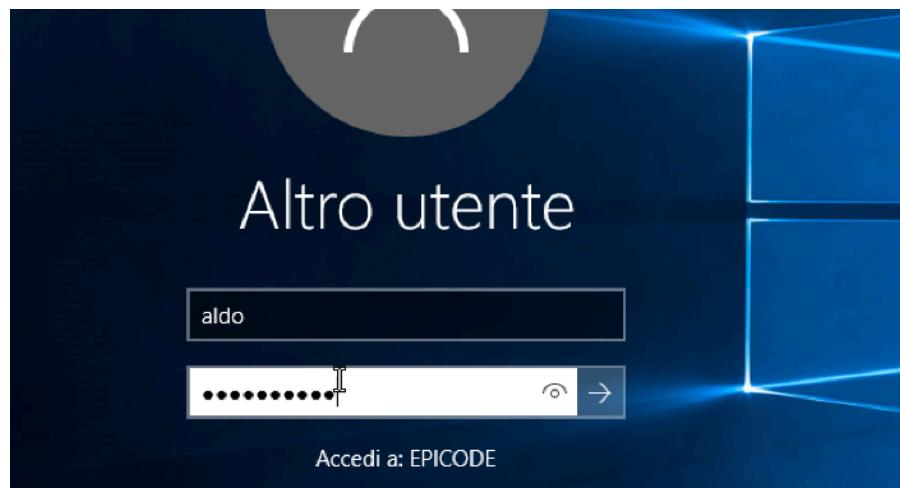


Una volta fatto mi chiederà di accedere ad un account ed userò l account senza privilegi
creato prima ovvero BETA

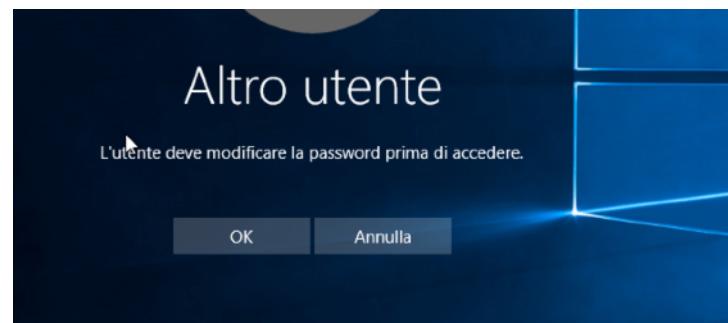


Step4. Controllo accessi e permessi

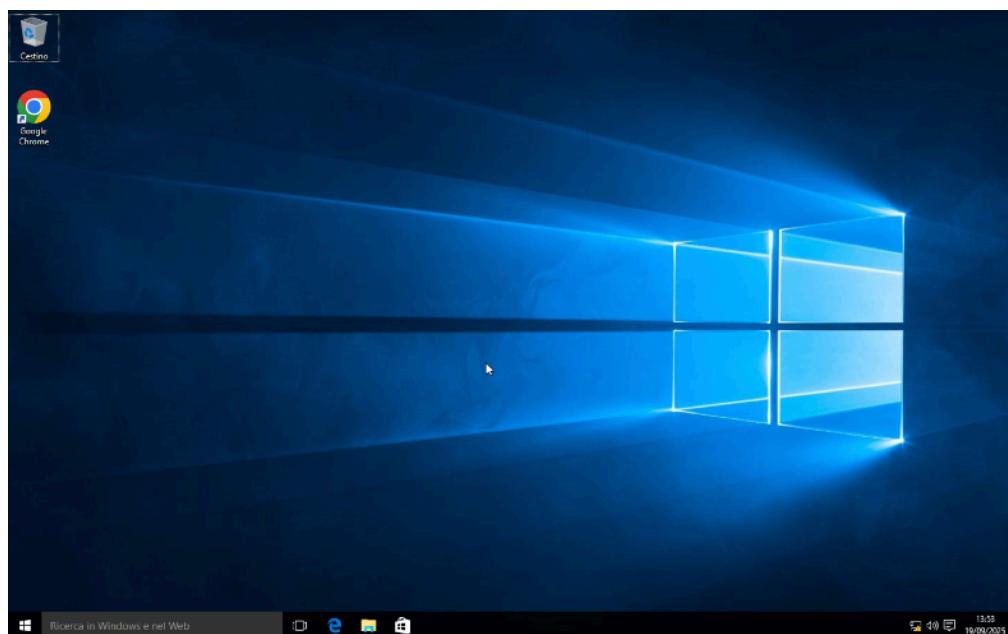
Riavvio la macchina windows 10 ed provo ad accedere ad uno dei utenti creati



Una volta inserita la password mi chiederà di cambiarla



Una volta dentro controllo i permessi che ha questo utente sui file creati, vado su file ed inserendo \\epicodeserver faccio l'accesso alla rete condivisa

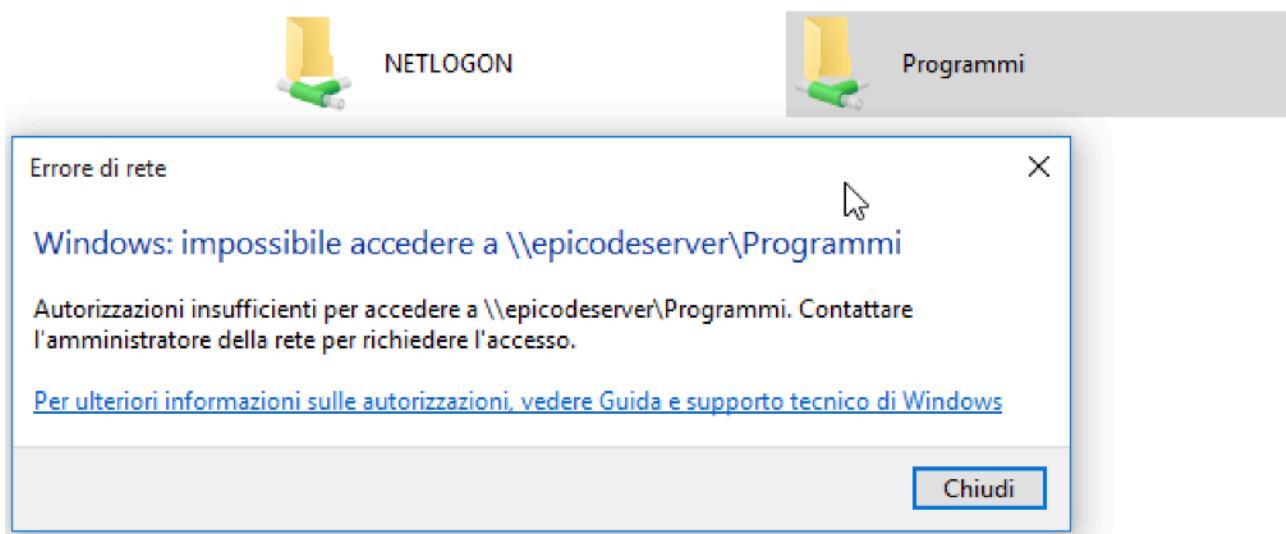


File > Rete > epicodeserver >

Accedo alle cartelle e provo ad entrare ed modificare i file nella cartella in cui l'utente Aldo ha l'accesso ovvero InfoClienti

A screenshot of a Windows File Explorer window. The left pane shows a tree view with 'Rete' expanded, showing 'epicodeserver' and 'InfoClienti'. The right pane displays the contents of the 'InfoClienti' folder, which includes subfolders 'Azienda', 'Dati Segreti', 'Dati Top', 'NETLOGON', and 'Programmi'. A file named 'Dati clienti' is selected, showing its details: 19/09/2025 13:15, Documento di testo, 0 KB. Below the file list, a 'Blocco note' window is open with the title 'Dati clienti - Blocco note'. The window contains the text 'prova modifica'. At the bottom of the window, the file 'Dati clienti' is listed again with the same details. The status bar at the bottom of the window shows '19/09/2025 15:02'.

Come si può vedere dagli screenshot ha piano controllo di modificare ed aggiungere file.
Ora provo ad entrare nella cartella dove il permesso non gli è stato concesso



Come si può vedere l'accesso gli viene negato.

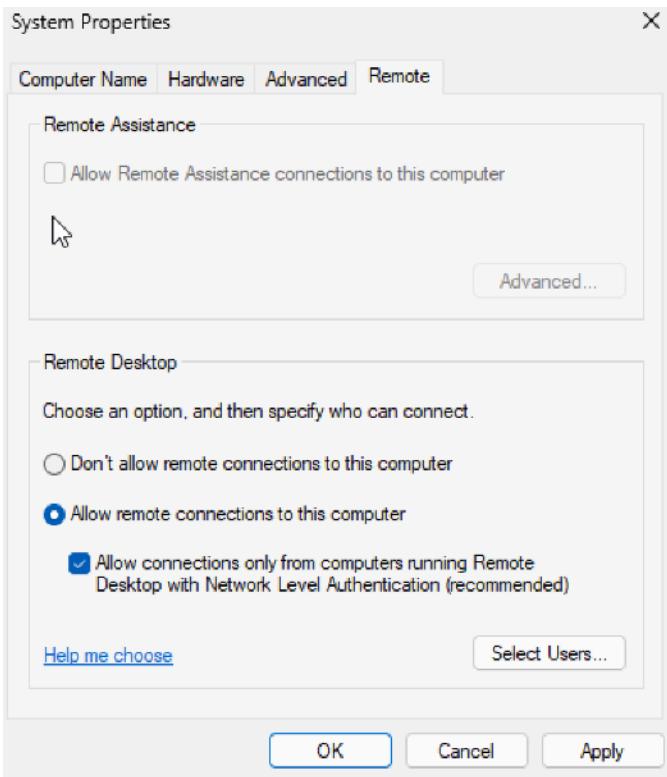
Step5. Connessione da remoto

Andando sulla schermata principale si può vedere che il remote Desktop è disattivato quindi per riuscire ad avere una connessione da remoto dobbiamo attivarlo.

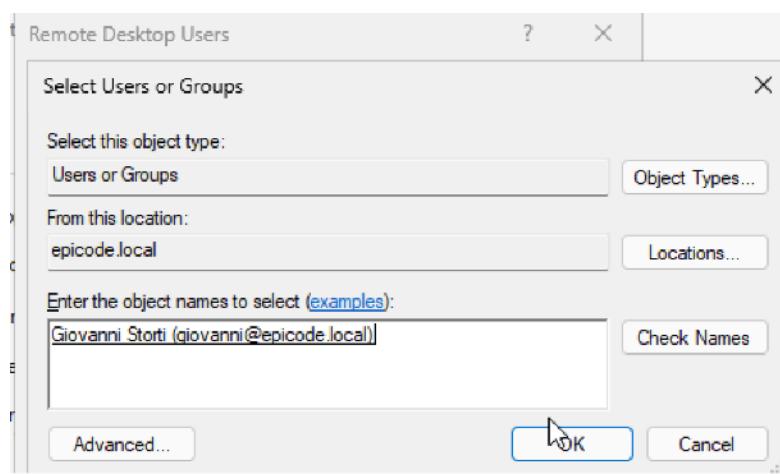
The screenshot shows the Azure portal's 'Properties' page for a server named 'EpicodeServer'. The 'Local Server' tab is active. In the 'Remote Desktop' section, the status is set to 'Enabled'. Other details include:

Setting	Value
Computer name	EpicodeServer
Domain	epicode.local
Microsoft Defender Firewall	Public: On
Remote management	Enabled
Remote Desktop	Enabled
NIC Teaming	Disabled
Ethernet	192.168.64.10, IPv6 enabled
Azure Arc Management	Disabled
Remote SSH Access	Disabled
Operating system version	Microsoft Windows Server 2025 Datacenter Azure Edition
Hardware information	QEMU QEMU Virtual Machine
Last installed updates	Windows Update
Last checked for updates	Never Download updates only, using Windows Update Today at 12:01
Microsoft Defender Antivirus	Real-Time Protection: On
Feedback & Diagnostics	Settings
IE Enhanced Security Configuration	On
Time zone	(UTC +01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Product ID	Not activated
Processors	virt-9.1
Installed memory (RAM)	3.99 GB

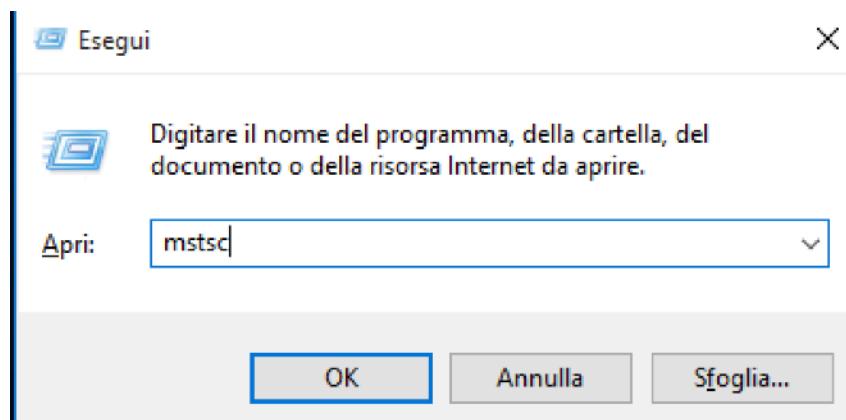
Cliccandoci possiamo attivare questa funzione ed darle il permesso ad utente o gruppi



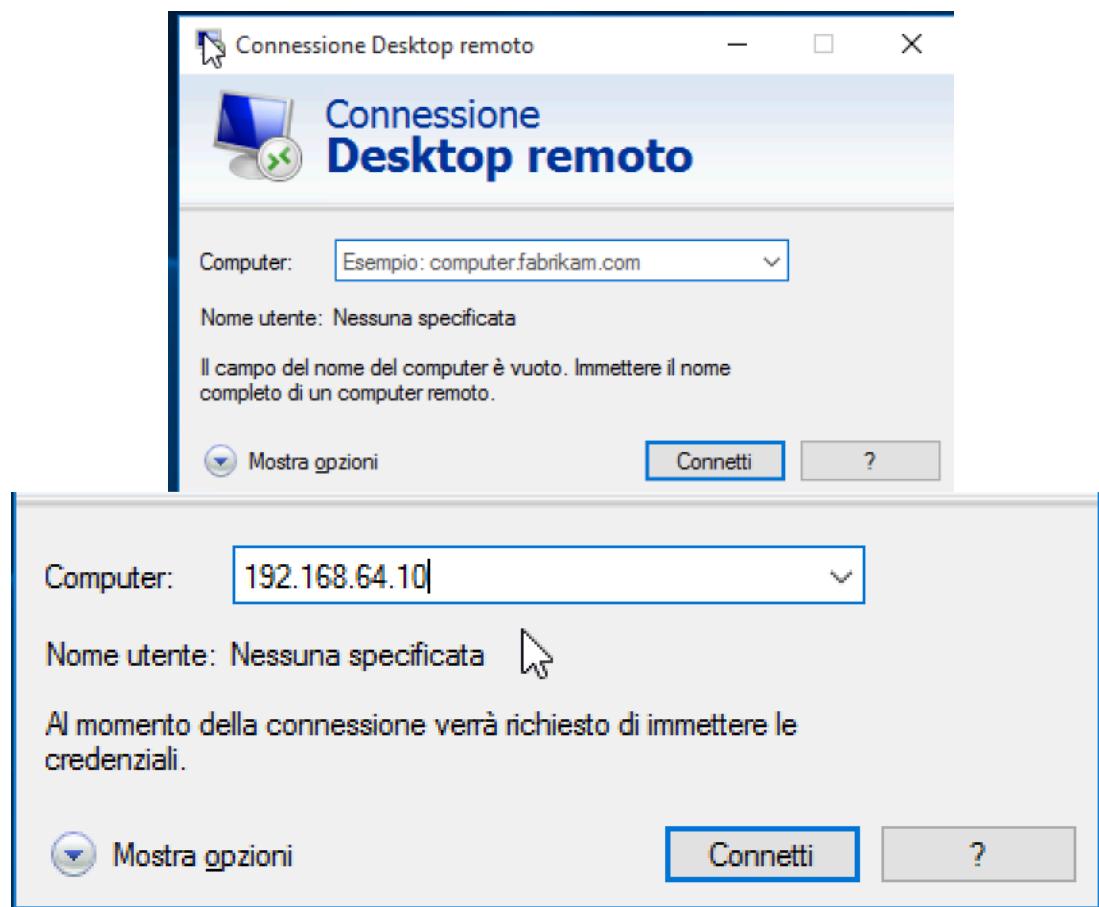
Do il permesso all'utente Giovanni Storti



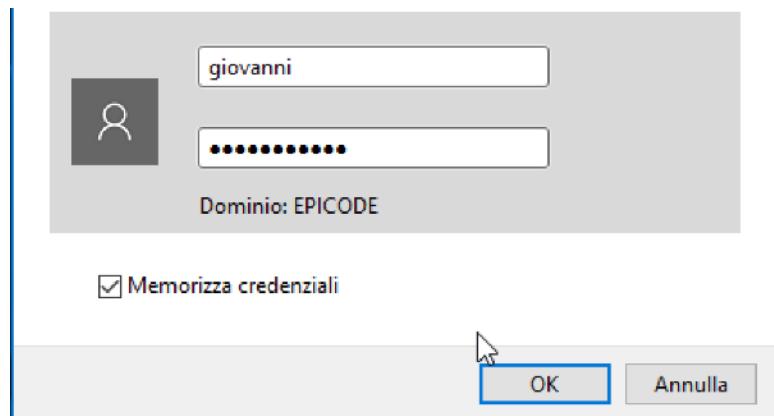
A questo punto vado sul mio windows 10, apro “esegui” ed inserisco “mstsc” per aprire l'app per accedere da remoto al server



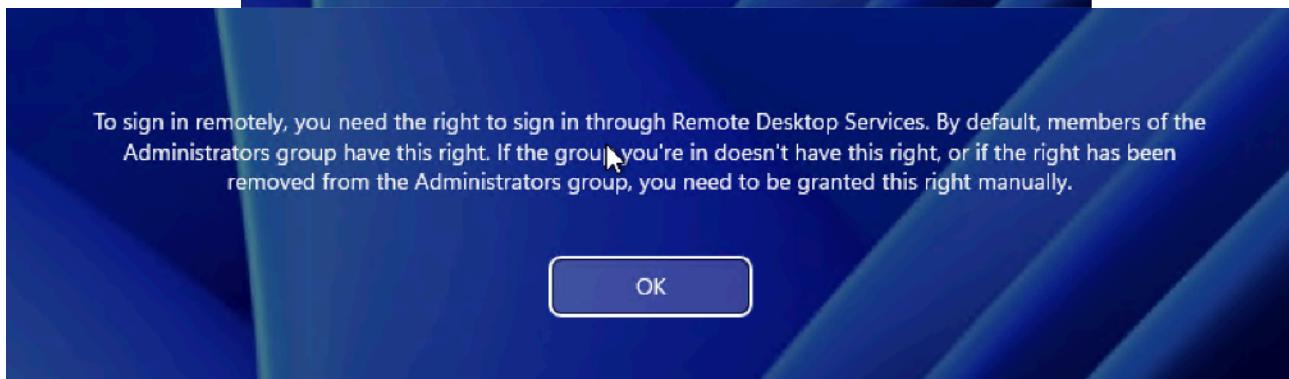
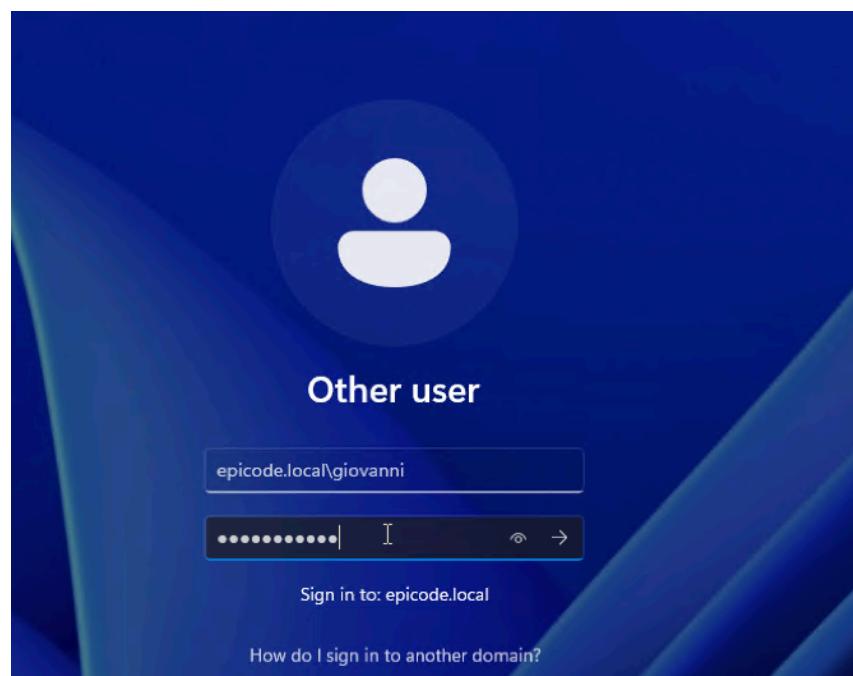
Una volta aperta l'applicazione inserisco l'ip del server



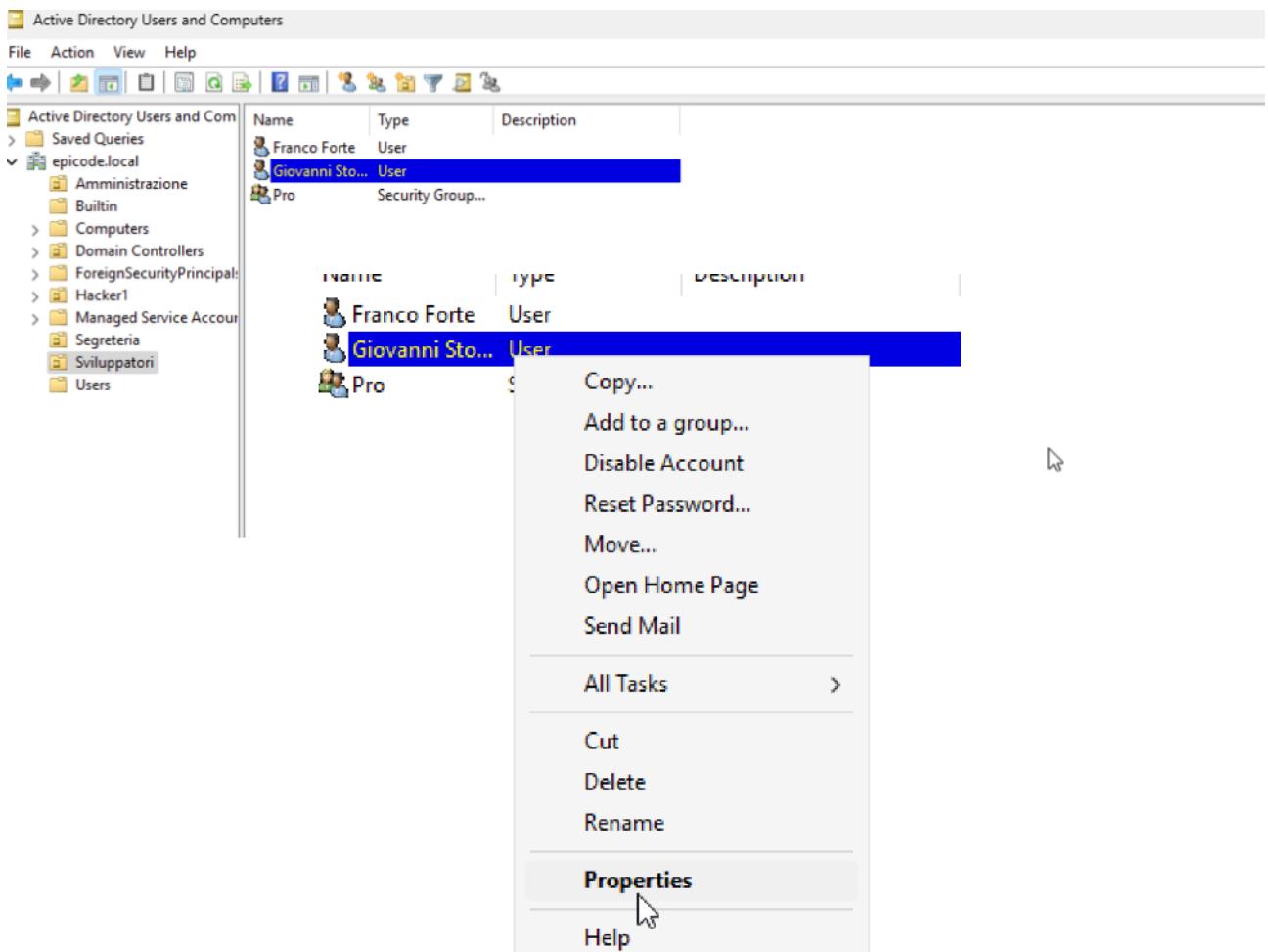
Inserisco i dati del utente a cui ho dato il permesso precedentemente



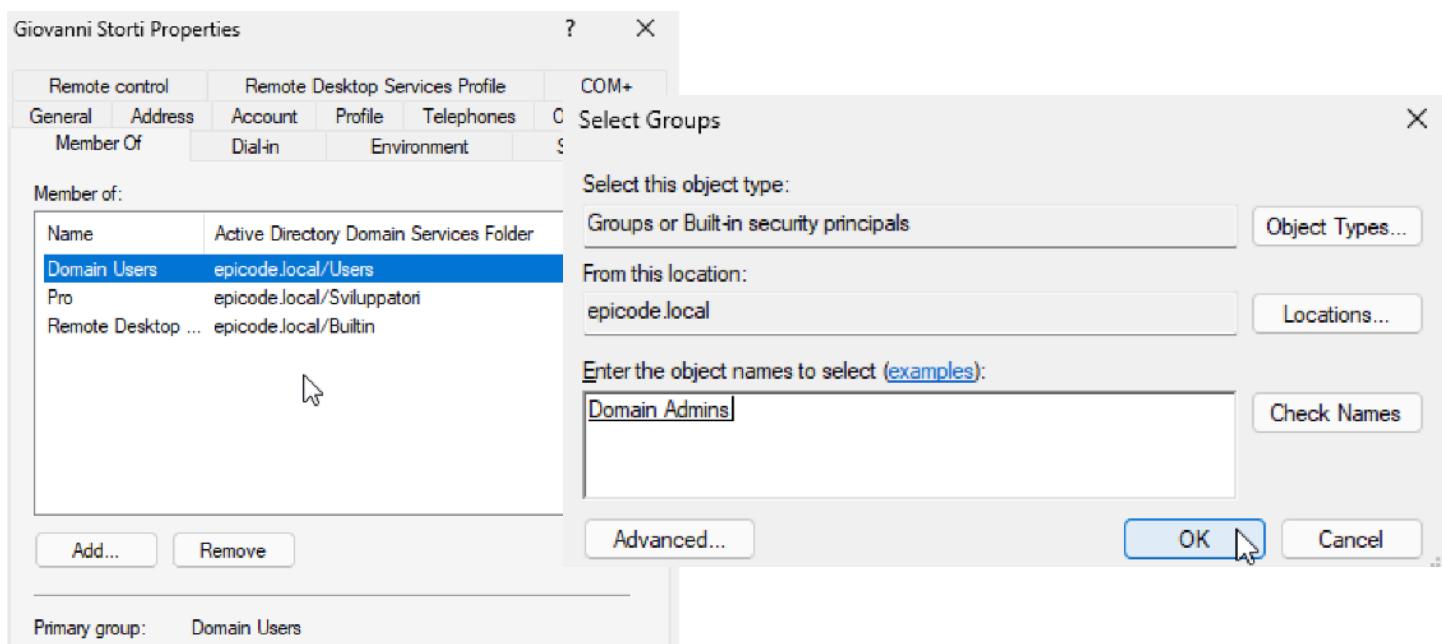
Mi appare la schermata di login quindi inserisco di nuovo i dati d'accesso.



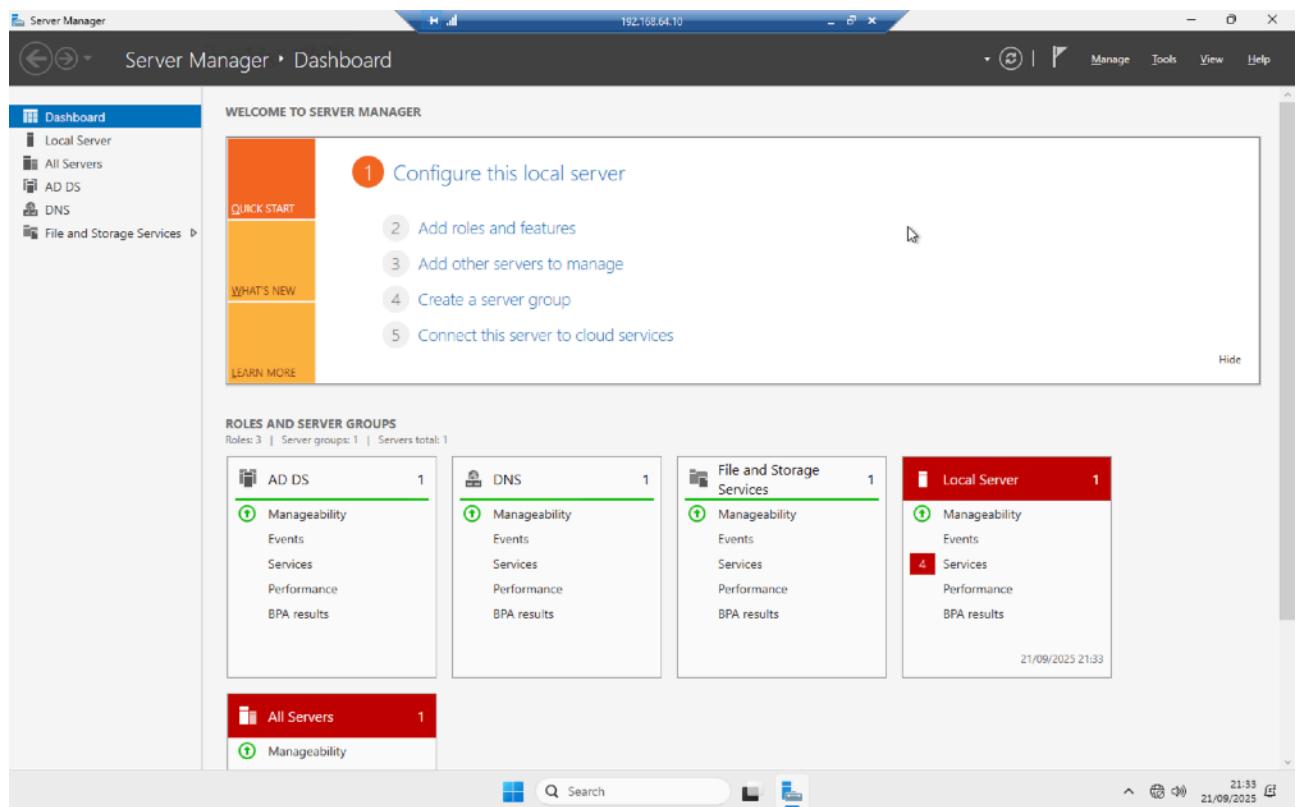
Come si può vedere dal ultimo screenshot mi dice che il permesso può essere dato solo agli amministratori quindi ho dovuto rendere Giovanni uno di essi, per fare ciò sono andato su utenti poi sul utente che mi interessava e poi proprietà.



Dopo di che sono andato su member of e ho fatto ad per aggiungere così il Domain Admin



Fatto il tutto sono di nuovo andato sul windows 10 ed ho rifatto il procedimento di prima per accedere al server da remoto e come si può vedere dal prossimo screen ho pieno accesso ed controllo al server.



Conclusioni del Report

Questo progetto ha permesso di mettere in pratica le competenze di base per l'amministrazione di un ambiente Windows Server. Le fasi di lavoro hanno riguardato la creazione e la configurazione di un dominio, la gestione degli utenti e l'impostazione dei permessi di accesso, includendo anche la risoluzione di un problema comune legato alla connettività remota.

Punti chiave del progetto:

- **Gestione Utenti e Gruppi:** La creazione degli utenti "Franco Fortax" e "Giovanni Storti" e la loro assegnazione a gruppi specifici all'interno delle Unità Organizzative "Sviluppatori" e "Segreteria" dimostra la corretta applicazione delle procedure di base di Active Directory.
- **Politiche di Sicurezza delle Password:** L'impostazione di opzioni come `User must change password at next logon` e `Password never expires` evidenzia la comprensione delle politiche di sicurezza necessarie per mantenere l'integrità del sistema.
- **Configurazione dell'Accesso Remoto:** Il tentativo di accesso tramite Connessione Desktop remoto e l'errore riscontrato hanno permesso di approfondire la gestione dei diritti di accesso, scoprendo che la semplice appartenenza a un gruppo non è sempre sufficiente, ma che le politiche di gruppo (Group Policy) possono influenzare le autorizzazioni. La risoluzione del problema ha richiesto un'analisi più dettagliata delle impostazioni di sicurezza a livello di dominio.