

Report Tecnico: Amministrazione e Gestione dei Gruppi in Windows Server 2025

Candidato: Bejte Gerald

Ambiente di Analisi: UTM Virtualization su macOS (Apple Silicon)

Sistema Operativo Target: Windows Server 2025

Data: 13 Febbraio 2026

Introduzione e Obiettivi

Il presente documento illustra le procedure di configurazione, gestione e auditing dei gruppi di utenti all'interno di un ambiente **Windows Server 2025**, virtualizzato tramite l'hypervisor **UTM** su architettura ARM.

L'obiettivo centrale dell'esercitazione è l'implementazione del principio del **"Least Privilege"** (**Minimo Privilegio**) attraverso una segmentazione logica degli utenti. In un'ottica di Cyber Risk e Management, la gestione oculata dei gruppi non è solo una necessità amministrativa, ma una contromisura critica per ridurre la superficie di attacco e prevenire movimenti laterali non autorizzati all'interno dell'infrastruttura di rete.

1. Configurazione della Rete e Indirizzamento IP

In questa prima fase, l'obiettivo è stato isolare l'ambiente di lavoro e stabilire una base di connettività solida per i servizi di dominio.

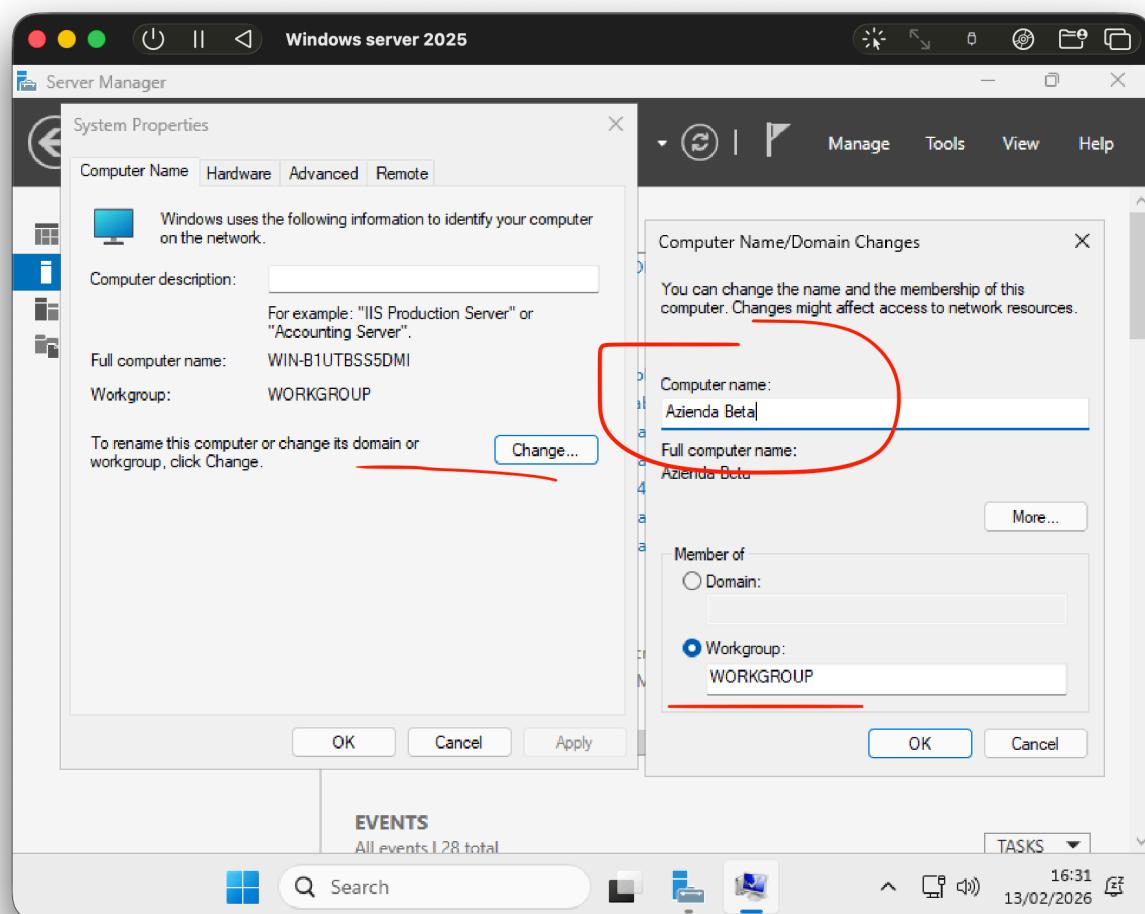
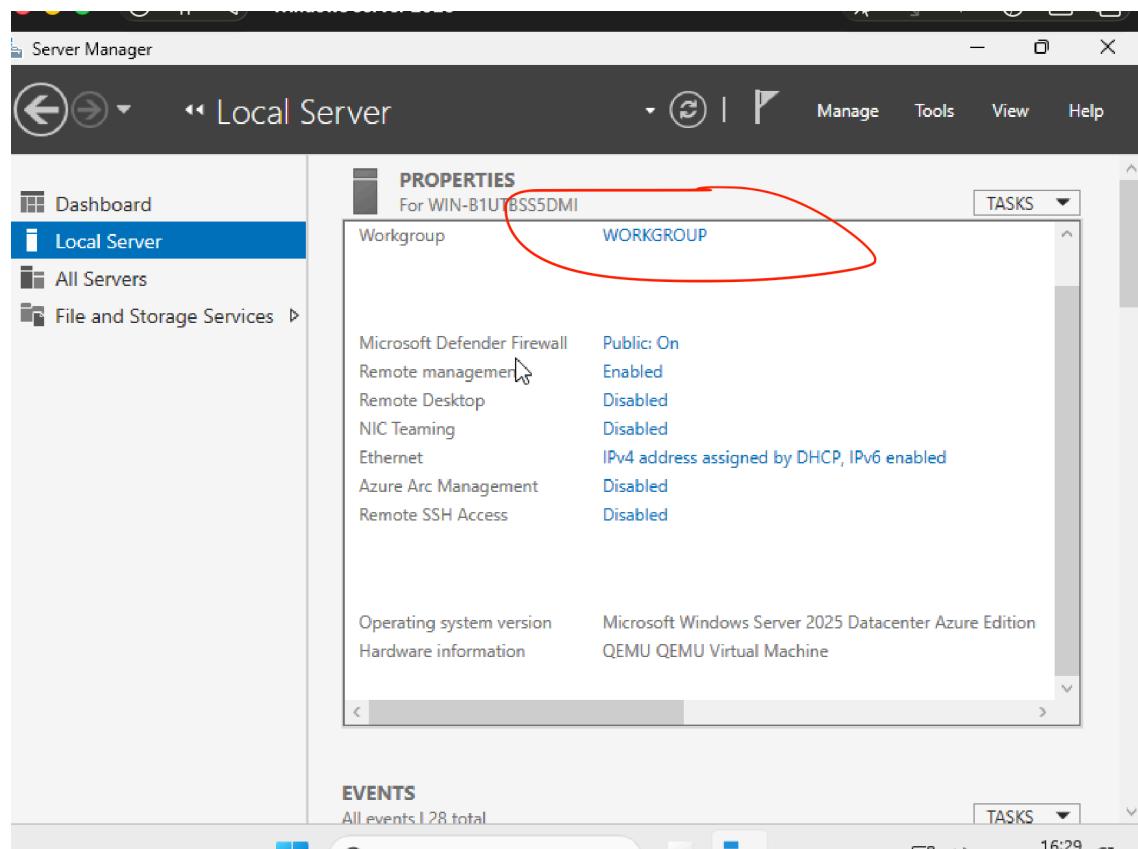
- Modalità Scheda di Rete:** La scheda di rete virtuale all'interno dell'ambiente UTM è stata impostata in modalità **Rete Interna**. Questa configurazione è essenziale per isolare il traffico del laboratorio dalla rete fisica del Mac M1, garantendo che le comunicazioni avvengano esclusivamente tra il server e i client autorizzati.
- Configurazione IP Statico:** È stato abbandonato l'indirizzamento dinamico in favore di una configurazione **IP Statica**. Un server che ospita servizi critici come Active Directory deve possedere un indirizzo immutabile affinché i client possano rintracciarlo correttamente.
- Verifica tramite Riga di Comando:** Utilizzando il comando `ipconfig` nel **Prompt dei comandi (CMD)**, è stato analizzato l'indirizzo inizialmente assegnato per definire i parametri statici finali.
- Parametri di Rete Applicati:**
 - Indirizzo IPv4:** 192.168.20.60

- **Subnet Mask:** 255.255.255.0
 - **Gateway Predefinito:** 192.168.20.1
 - **Configurazione DNS:** Nel campo del server DNS è stato inserito l'indirizzo **192.168.20.60** (l'IP del server stesso).
 - **Analisi Tecnica:** Impostare il server come DNS primario di se stesso è un passaggio obbligatorio. In questo modo, il sistema diventa l'autorità per la risoluzione dei nomi del dominio interno, permettendo la corretta registrazione e ricerca dei record SRV necessari per il funzionamento dei servizi di directory.
-

2. Personalizzazione e Configurazione del Sistema

In questa fase è stata eseguita la personalizzazione dei parametri identificativi e temporali del server per allinearli ai requisiti dell'organizzazione.

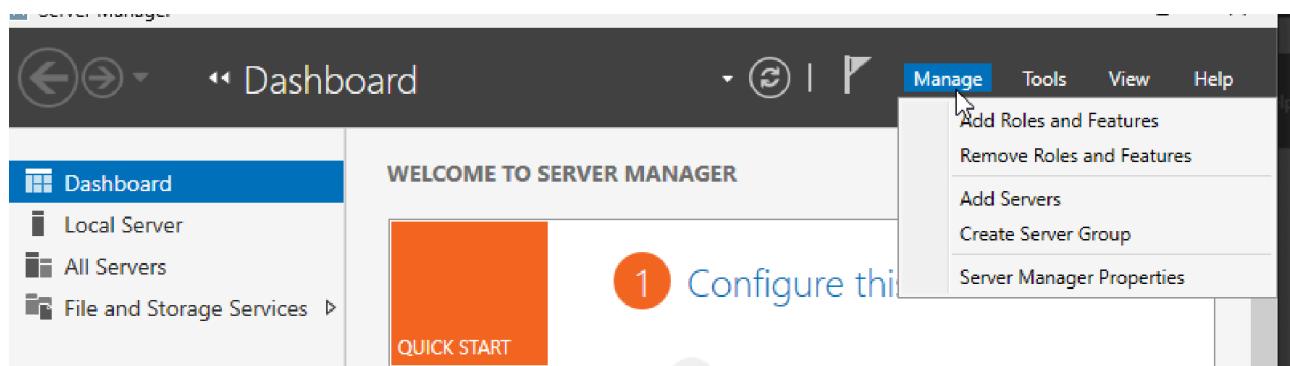
- **Ridenominazione del Server:** È stata aperta la finestra delle proprietà di sistema per modificare l'identificativo del computer. Il nome del server è stato cambiato da quello generico predefinito a **Azienda Beta**.
- **Analisi Tecnica del Naming:** La scelta di un nome significativo come **Azienda Beta** è fondamentale in un'ottica di cybersecurity e amministrazione. Un nome host standardizzato facilita l'identificazione univoca della risorsa all'interno dei log di audit, nelle scansioni di rete e nella gestione delle zone DNS, riducendo il rischio di confusione durante l'analisi degli incidenti.
- **Configurazione Temporale:** Si è proceduto alla modifica delle impostazioni di **Data e Ora** del sistema.
- **Importanza della Sincronizzazione Temporale:** La corretta impostazione dell'ora non è solo un parametro organizzativo, ma un requisito tecnico critico per il protocollo di autenticazione **Kerberos** utilizzato da Active Directory. Una discrepanza temporale (skew) superiore a 5 minuti tra il server e i client impedirebbe l'accesso alle risorse e la validazione dei ticket di sicurezza, rendendo instabile l'intero dominio.
- **Finalizzazione:** Dopo l'applicazione del nuovo nome host, il sistema ha richiesto un **riavvio forzato** per rendere effettive le modifiche e aggiornare i relativi record di rete.



3. Installazione di Active Directory Domain Services (AD DS)

In questa fase è stato implementato il servizio di directory fondamentale per la gestione centralizzata dell'intera rete aziendale.

- **Definizione e Finalità:** Active Directory (AD) è un servizio di directory sviluppato da Microsoft progettato per gestire e organizzare le risorse di rete, come utenti, computer e gruppi, fornendo autenticazione e autorizzazione centralizzate.
- **Obiettivi di Sicurezza e Amministrazione:**
 - **Gestione Centralizzata:** Facilita l'amministrazione delle risorse di rete da un unico punto di controllo.
 - **Hardening e Sicurezza:** Migliora la protezione delle risorse aziendali grazie a un sistema di autenticazione centralizzato.
 - **Group Policy (GPO):** Permette di applicare criteri di sicurezza e configurazioni specifiche in modo granulare a gruppi di utenti e computer.
 - **Interoperabilità:** È essenziale per l'integrazione con altri servizi Microsoft come Exchange e SharePoint.
- **Procedura Tecnica di Installazione:**
 - Accesso al menù **Manage** all'interno del Server Manager e selezione di **Add Roles and Features**.
 - Selezione del ruolo **Active Directory Domain Services** dall'elenco dei ruoli del server.
 - Inclusione delle funzionalità necessarie tramite il comando **Add Features**.
 - Avanzamento nelle schermate di configurazione mantenendo i parametri di default come previsto dalla traccia.
 - Esecuzione dell'**Installazione** e monitoraggio dell'avanzamento fino al completamento della procedura.
 - Chiusura della procedura guidata tramite il tasto **Close**.



Add Roles and Features Wizard

Before you begin

DESTINATION SERVER
AziendaBeta

Before You Begin

- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

Skip this page by default

< Previous **Next >** Install Cancel

Select destination server

DESTINATION SERVER
AziendaBeta

Before You Begin

- Installation Type
- Server Selection**
- Server Roles
- Features
- Confirmation
- Results

Select a server or a virtual hard disk on which to install roles and features.

Select a server from the server pool
 Select a virtual hard disk

Server Pool

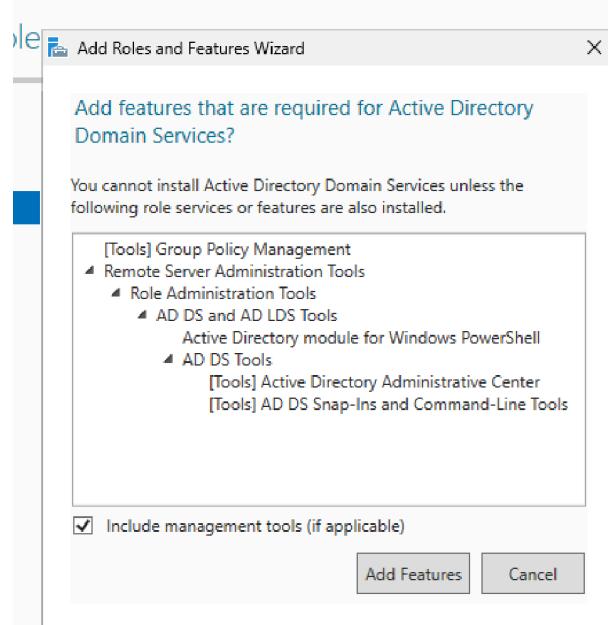
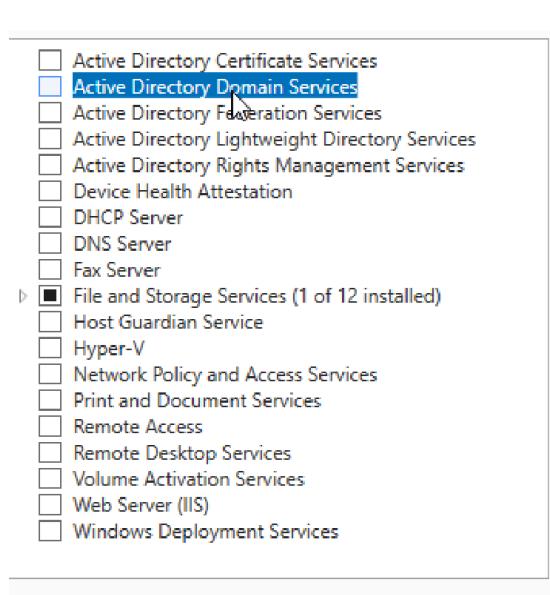
Name	IP Address	Operating System
AziendaBeta	192.168.64.25	Microsoft Windows Server 2025 Datacenter Azure Edition

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous **Next >** Install Cancel

SELECT SERVER ROLES:



Confirm installation selections

DESTINATION SERVER
AziendaBeta

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

To install the following roles, role services, or features on selected server, click **Install**.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click **Previous** to clear their check boxes.

Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

Export configuration settings
Specify an alternate source path

< Previous Next > **Install** Cancel

Quando è giunta al termine facciamo clic su Close.

4. Configurazione della Foresta e Promozione a Domain Controller

Dopo l'installazione dei ruoli, è necessario definire la struttura logica del network creando una nuova Foresta e promuovendo il server a Domain Controller.

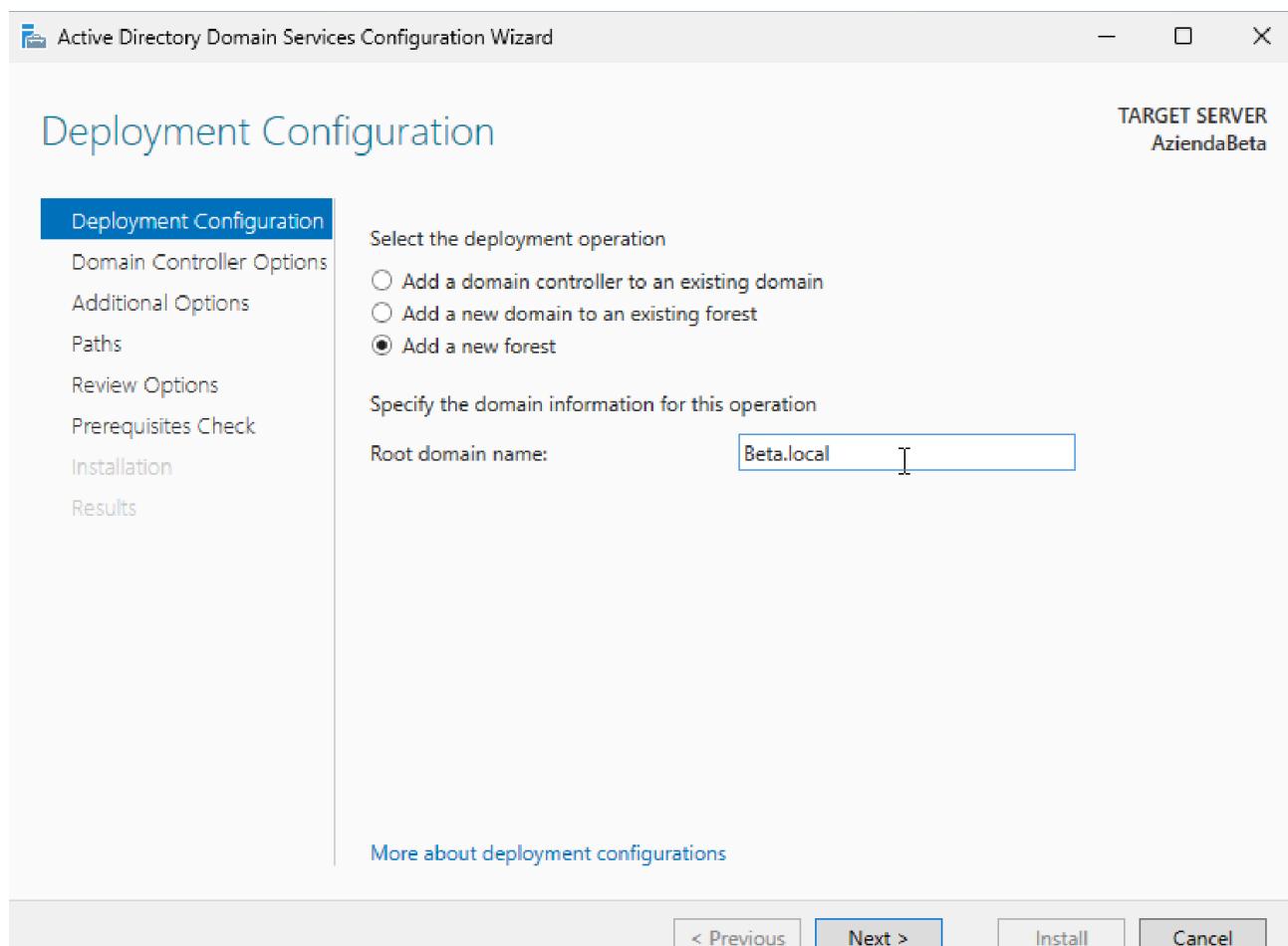
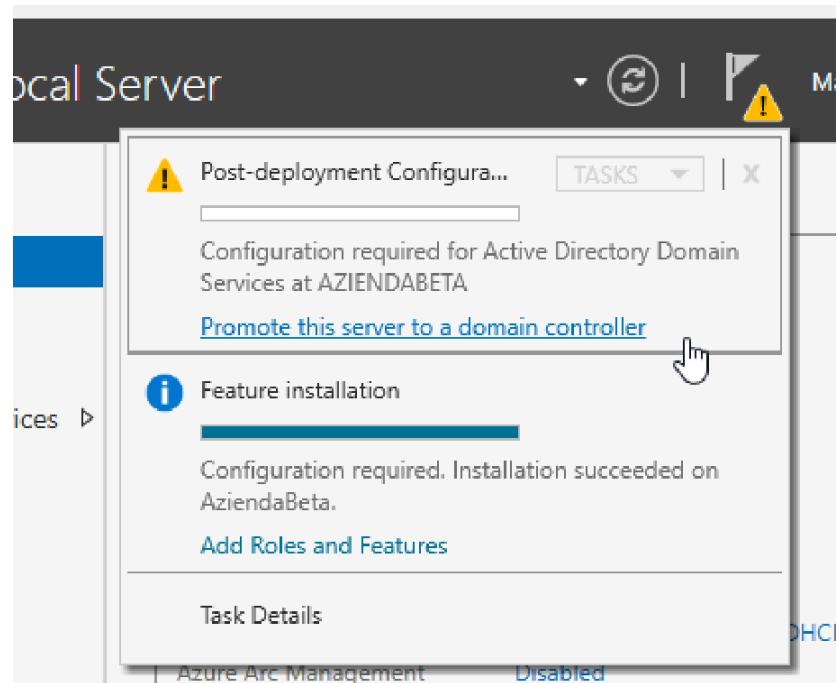
- **Concetti Chiave di Architettura:**

- **Cos'è una Foresta:** Rappresenta il contenitore di livello più alto in Active Directory. È un insieme di uno o più domini che condividono una struttura logica, uno schema comune e un catalogo globale.
- **Cos'è un Dominio:** È l'unità logica fondamentale che gestisce utenti e risorse, identificata da un nome DNS univoco. Svolge funzioni critiche di autenticazione, applicazione delle policy di sicurezza e replicazione dei dati tra i controller.

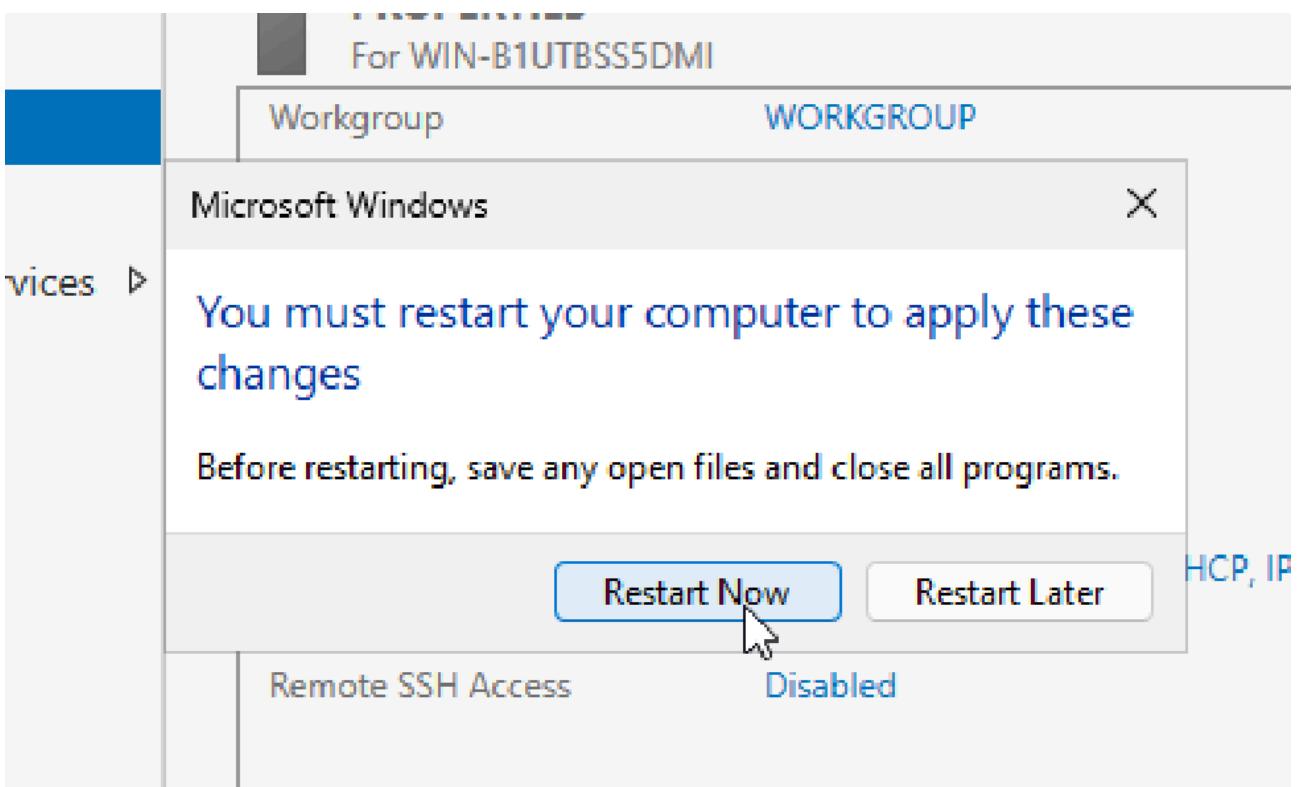
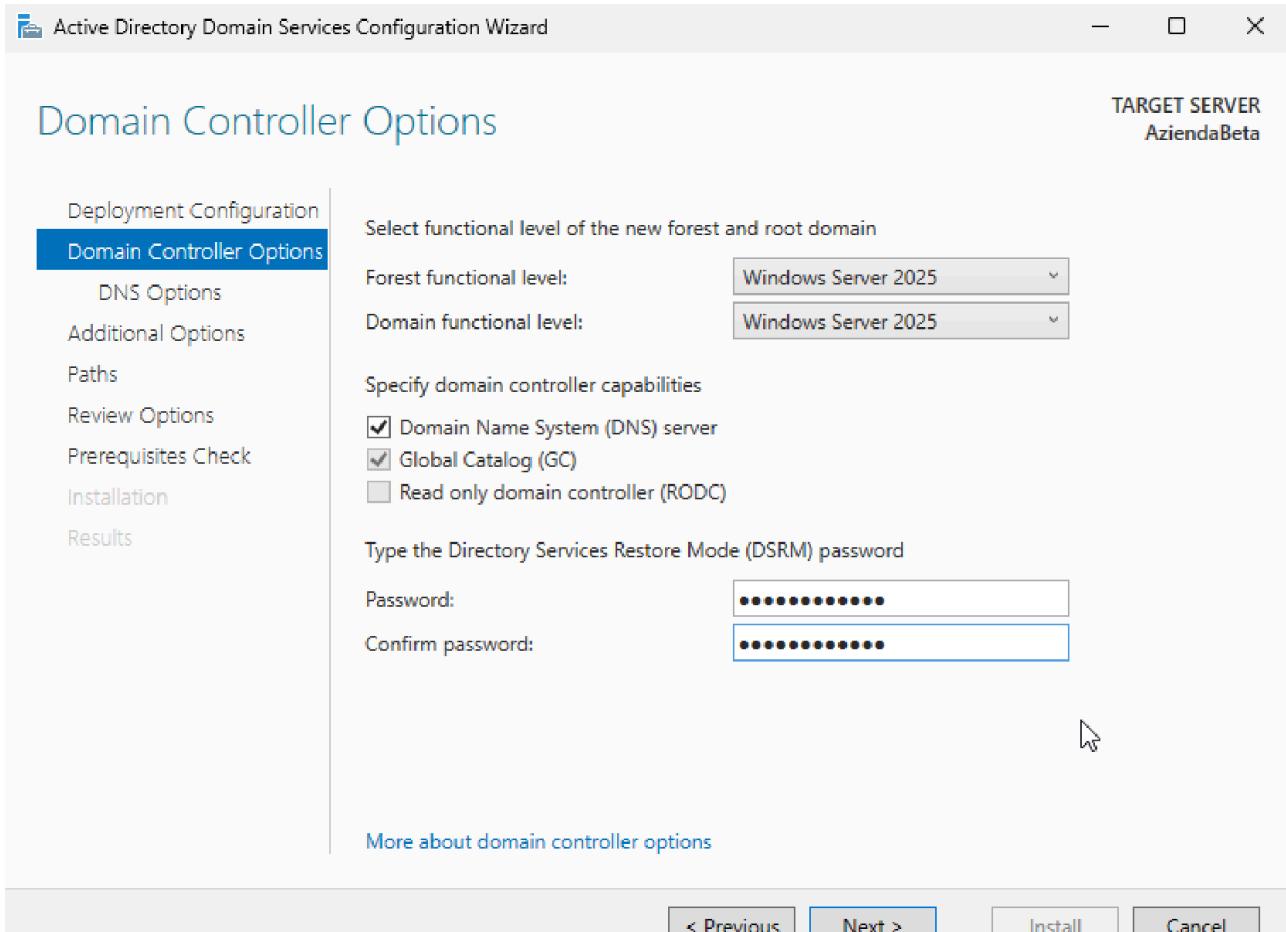
- **Procedura Tecnica di Promozione:**

- **Inizializzazione:** È stata selezionata la notifica contrassegnata dal **triangolo giallo** nel Server Manager, cliccando sulla voce blu "**Promote this server to a domain controller**".
- **Configurazione del Deployment:** È stata selezionata l'opzione "**Add a new forest**", inserendo il nome del dominio radice (es. **Beta.local**).
- **Sicurezza (DSRM):** È stata impostata una password specifica per il *Directory Services Restore Mode* (DSRM). Questa password, mantenuta distinta da quella dell'account Administrator, è vitale per il ripristino dei servizi in caso di corruzione del database di Active Directory.
- **Configurazione di Default:** I parametri relativi alle opzioni DNS e ai percorsi dei database (NTDS e SYSVOL) sono stati mantenuti ai valori di **default** per garantire la compatibilità standard.
- **Installazione e Finalizzazione:** Dopo la verifica dei prerequisiti, è stato cliccato il tasto **Install**. Al termine del processo, il sistema ha eseguito un **riavvio automatico** per configurare i database di sicurezza e inizializzare il dominio.

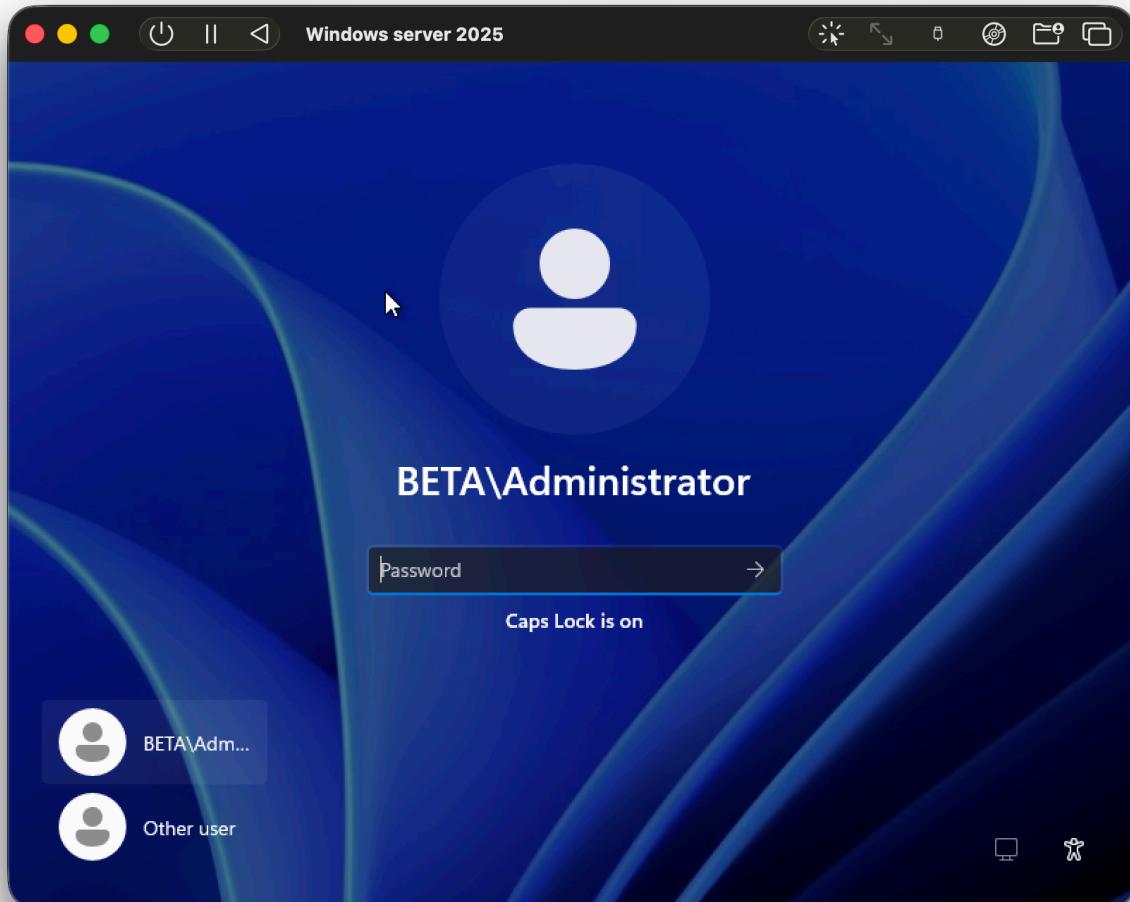
Passiamo al Punto 5? Adesso che il controller è attivo, possiamo documentare la creazione della **Organizational Unit (OU)** e dei **Gruppi** (Reparto It e Amministrazione), concludendo con la verifica dei permessi che hai effettuato. Ti do una mano con i passaggi per creare la OU?



È stata selezionata l'opzione "Add a new forest", inserendo il nome del dominio radice : Beta.local



Se tutto è andato bene dovremmo vedere questa schermata e due user



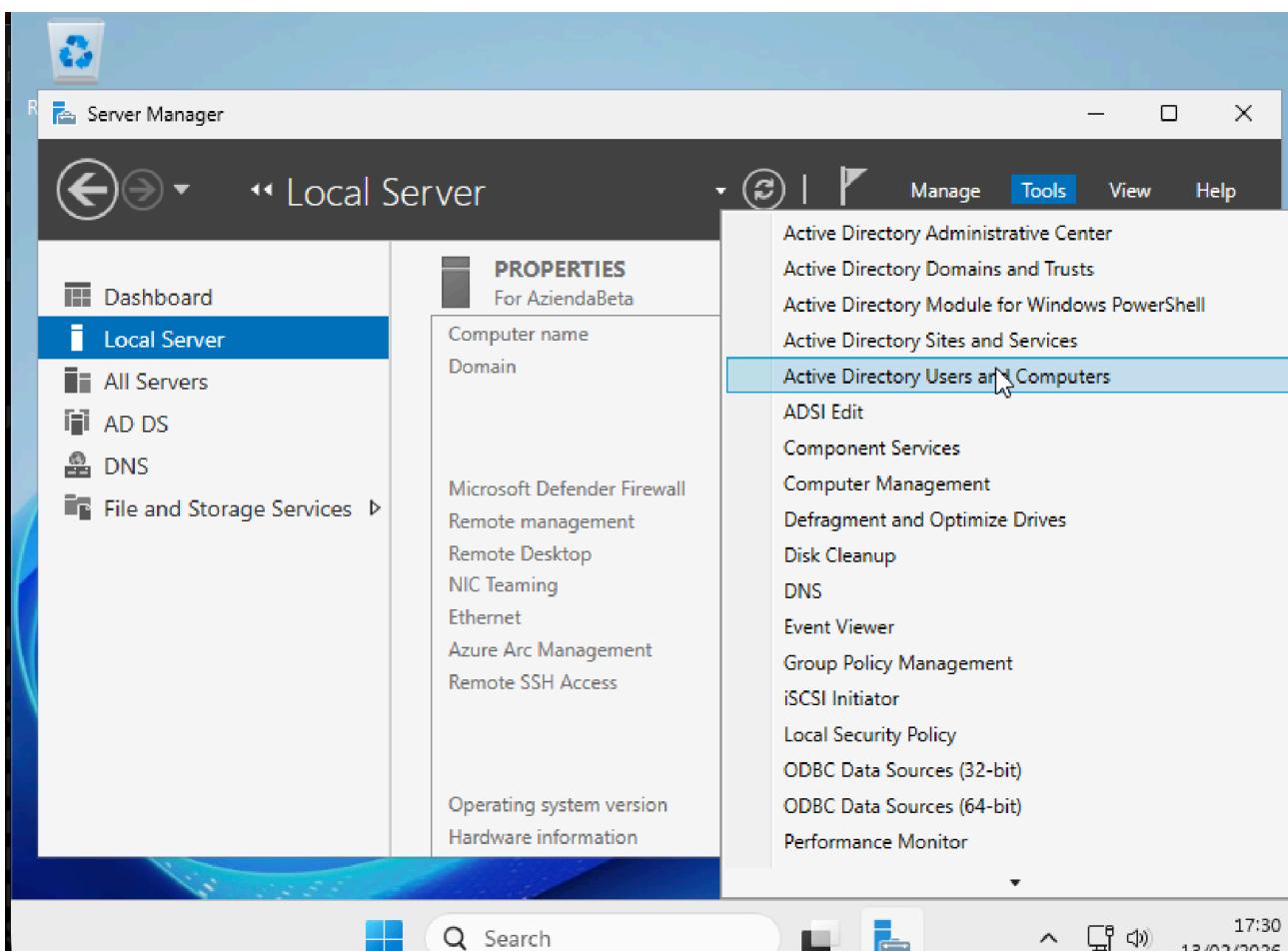
5. Gestione Logica: Unità Organizzative, Gruppi e Policy

In questa fase è stata definita la struttura gerarchica del dominio Beta.local per implementare una gestione granulare degli accessi e delle policy di sicurezza, organizzando le risorse in base alla struttura societaria.

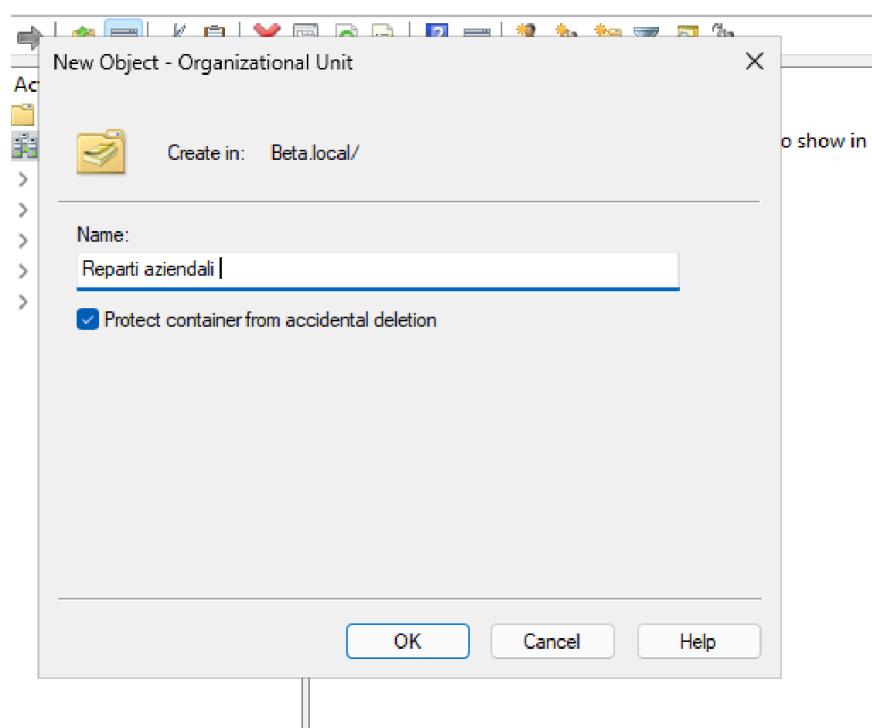
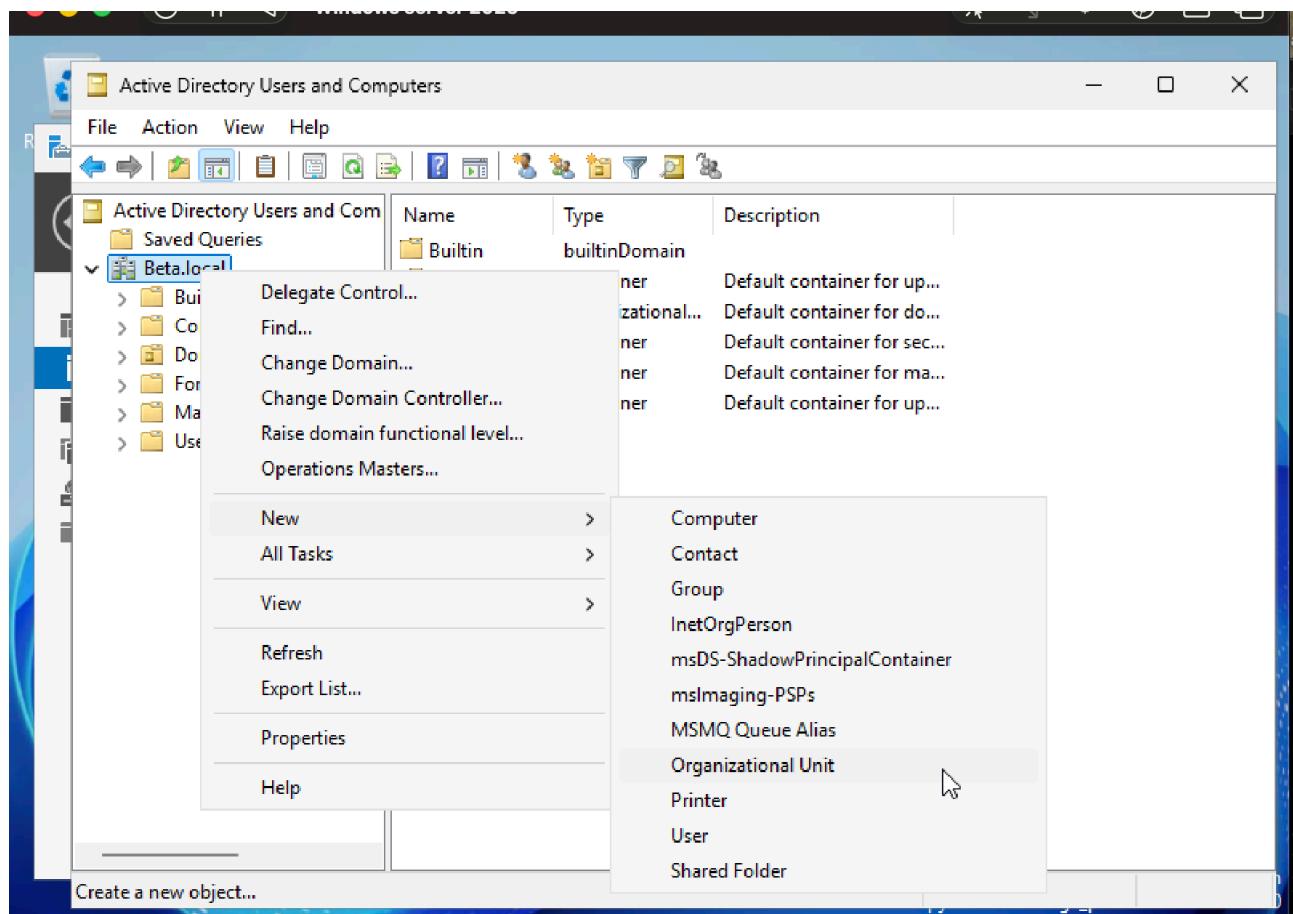
- **Importanza della Strutturazione Logica:**

- **Gruppi di Sicurezza:** Fondamentali per il controllo degli accessi, permettono di definire chi può interagire con specifiche risorse aziendali, migliorando l'efficienza e la consistenza delle autorizzazioni.
- **Group Policy (GPO):** Strumenti di centralizzazione che assicurano la standardizzazione delle configurazioni e l'automazione dei compiti di sicurezza in tutta l'organizzazione.

- **Unità Organizzative (OU):** Contenitori logici creati all'interno del dominio per raggruppare utenti e gruppi. La creazione di una OU "padre" permette di applicare policy comuni a più sottoreparti contemporaneamente.
- **Procedura Tecnica Eseguita:**
 - **Accesso agli Strumenti:** È stata aperta la console **Active Directory Users and Computers** dal menù **Tools** del Server Manager.
 - **Creazione dell'Unità Organizzativa Radice:** Partendo dal dominio **Beta.local**, è stata creata l'OU principale denominata **Reparti Aziendali**. Questa funge da contenitore primario per l'intera organizzazione.
 - **Creazione delle Sotto-Unità (Sub-OUs):** All'interno di "Reparti Aziendali", sono state create due unità organizzative specifiche per la segregazione dei dipartimenti:
 - **Amministrazione:** Destinata alla gestione del personale e delle risorse amministrative.
 - **Reparto It:** Destinata alla gestione dei tecnici e delle risorse infrastrutturali.
 - **Configurazione dei Gruppi:** All'interno di ciascuna sotto-OU, sono stati definiti i relativi gruppi di sicurezza. Questa struttura nidificata permette una gestione centralizzata e sicura, assicurando che le policy aziendali siano applicate correttamente a ogni livello della foresta gestita da **BetaServer**.

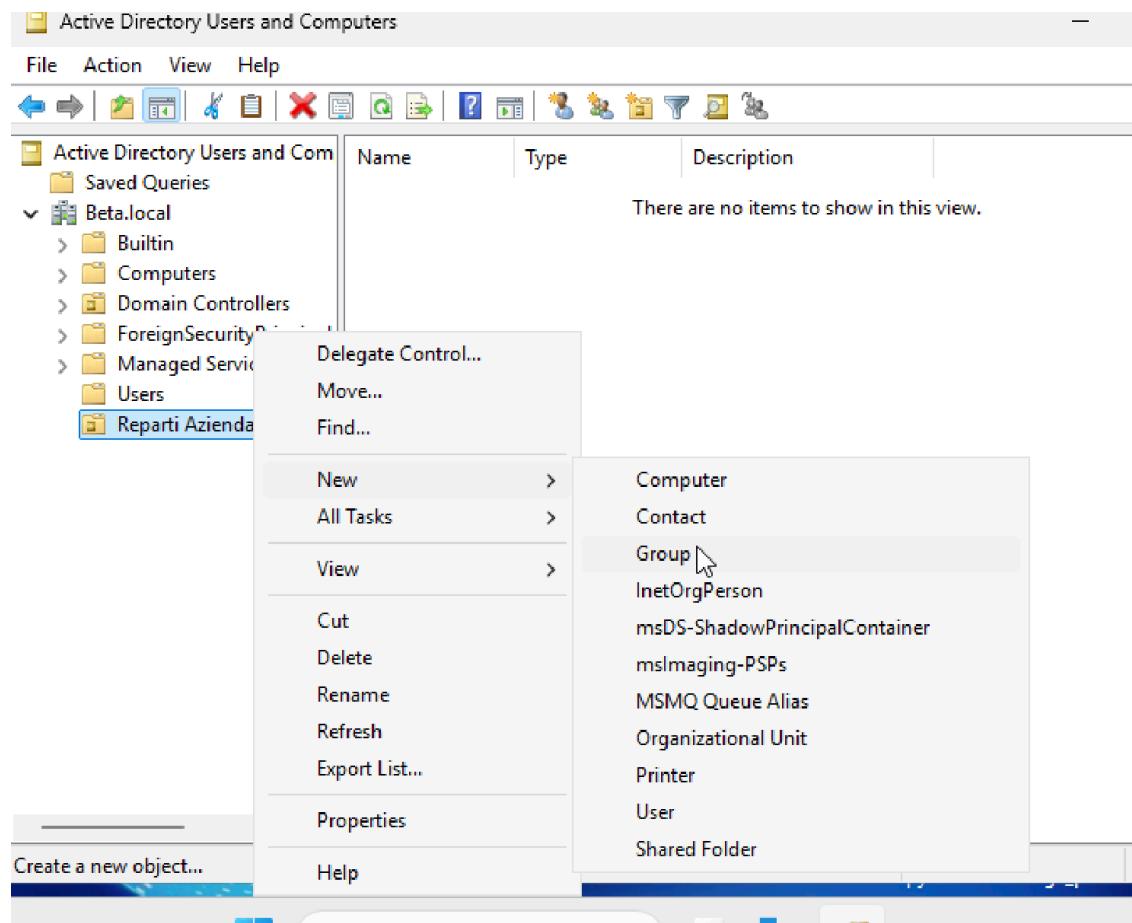


Clic destro sul dominio -> New -> **Organizational Unit**.

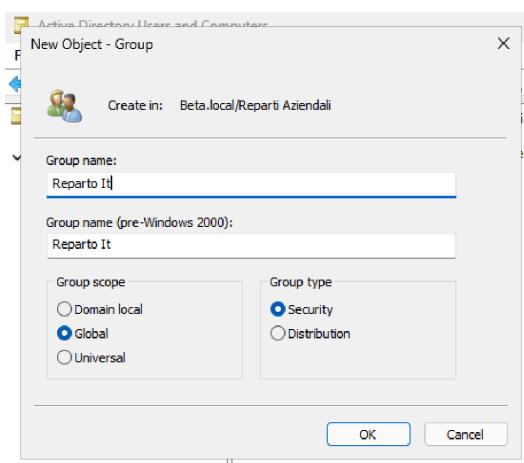


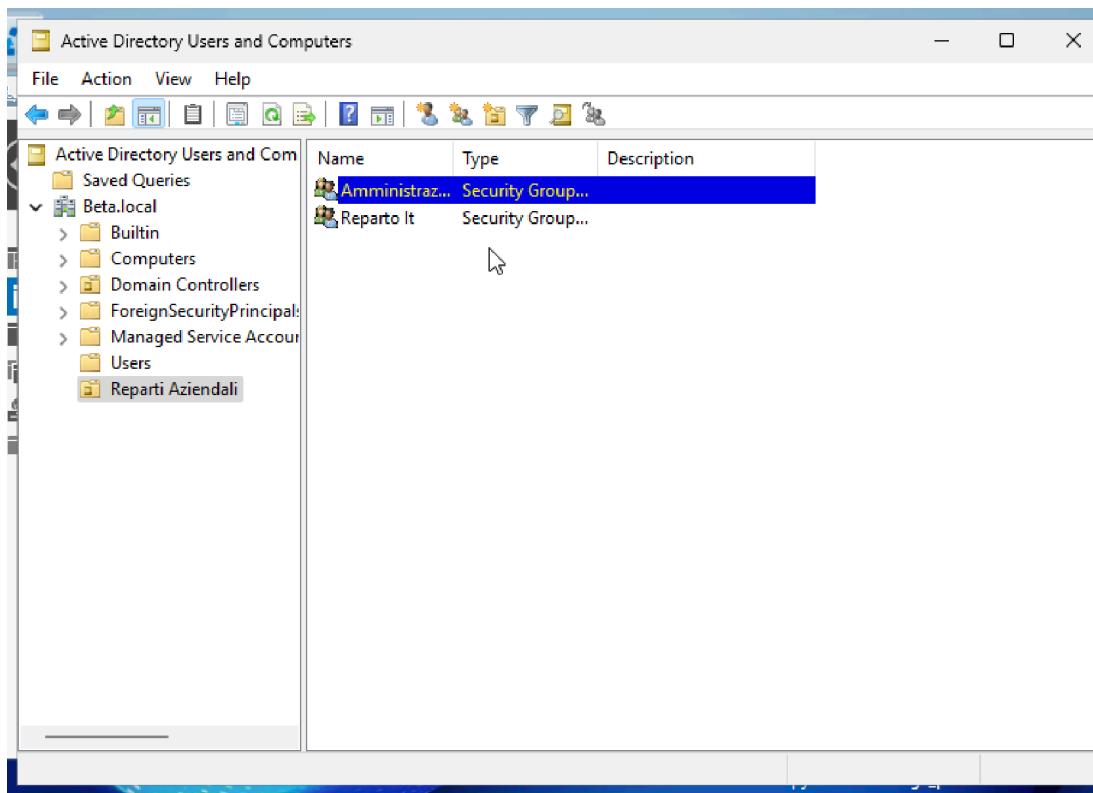
Andremo a creare il gruppo all'interno dell'Unità Organizzativa Amministrazione, e Reparto IT.

Su **Reparti Aziendali** Clic destro sul dominio -> **New -> New Group.**



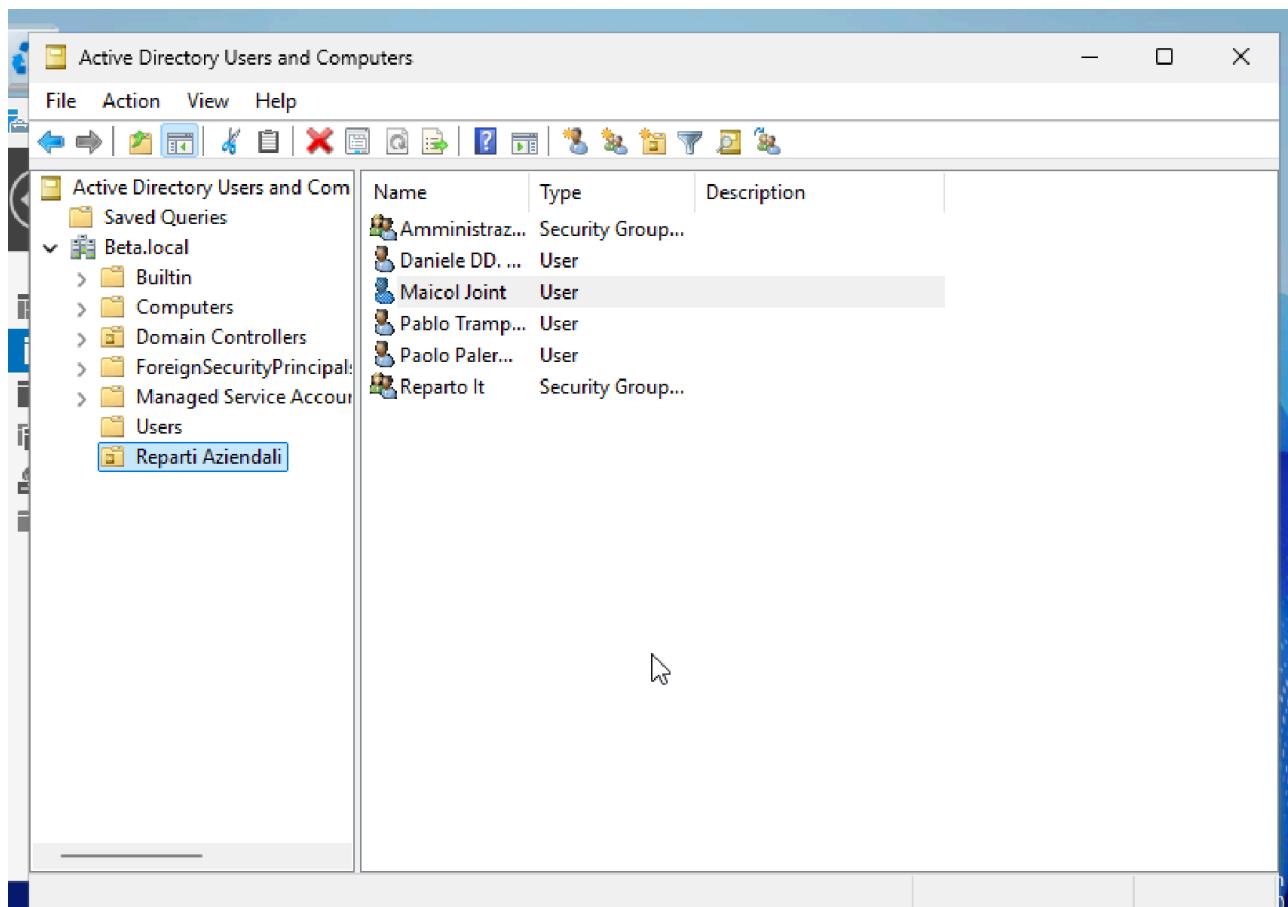
Creeremo Reparto It , e amministrazione , successivamente creeremo gli Users



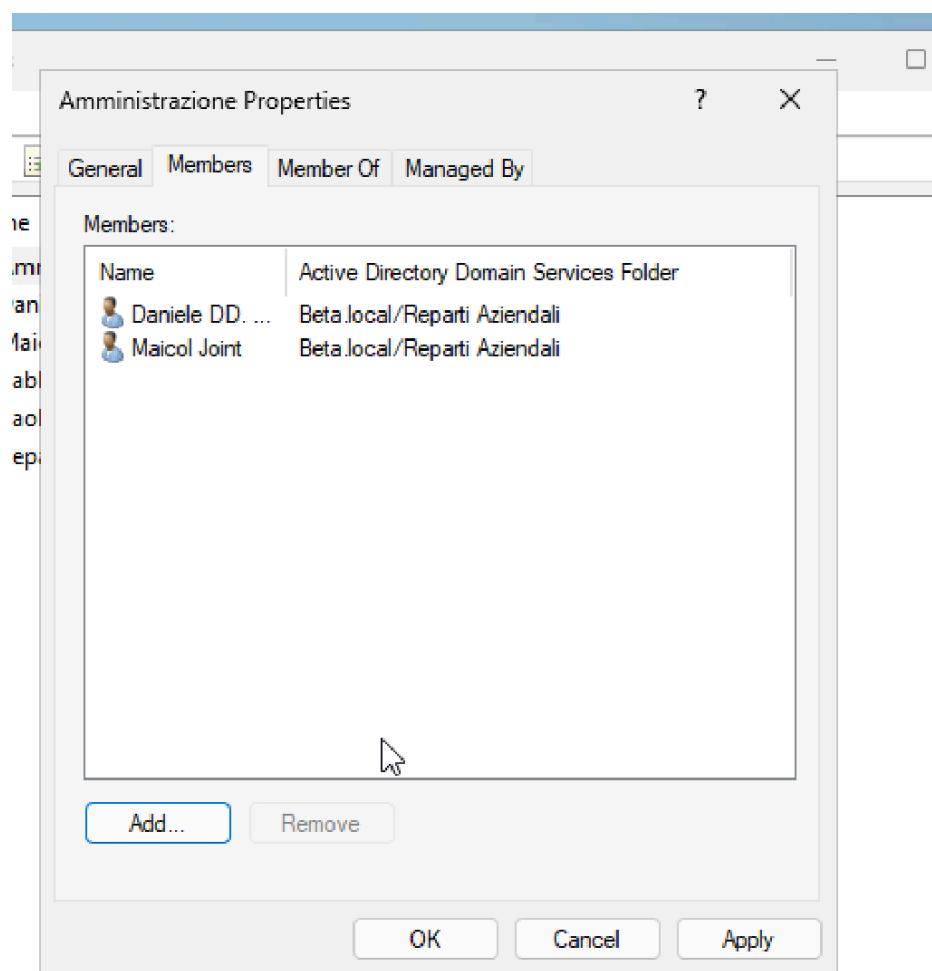
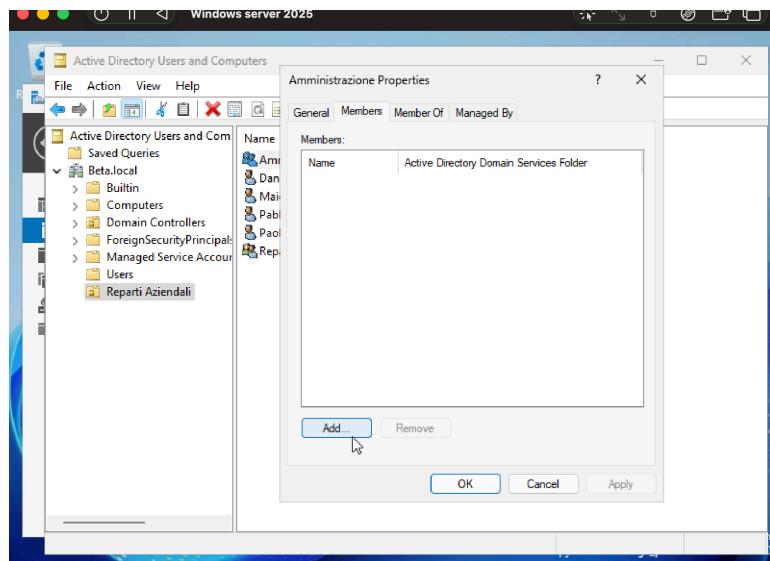


Su **Reparti Aziendali** Clic destro sul dominio -> **New -> New Group**.

Attribuiremo una password a ogni Users. Gli Users dovranno cambiare la password al primo accesso. L'amministratore del server in generale, non dovrebbe conoscere la password degli Users



Aggiungiamo i membri al gruppo ,



6. Configurazione delle Risorse Dati e Preparazione alle Group Policy

Una volta definita la struttura degli utenti e dei gruppi all'interno delle rispettive Unità Organizzative, il passaggio successivo consiste nella creazione delle risorse fisiche che saranno oggetto delle politiche di accesso.

- **Finalità Operativa:**

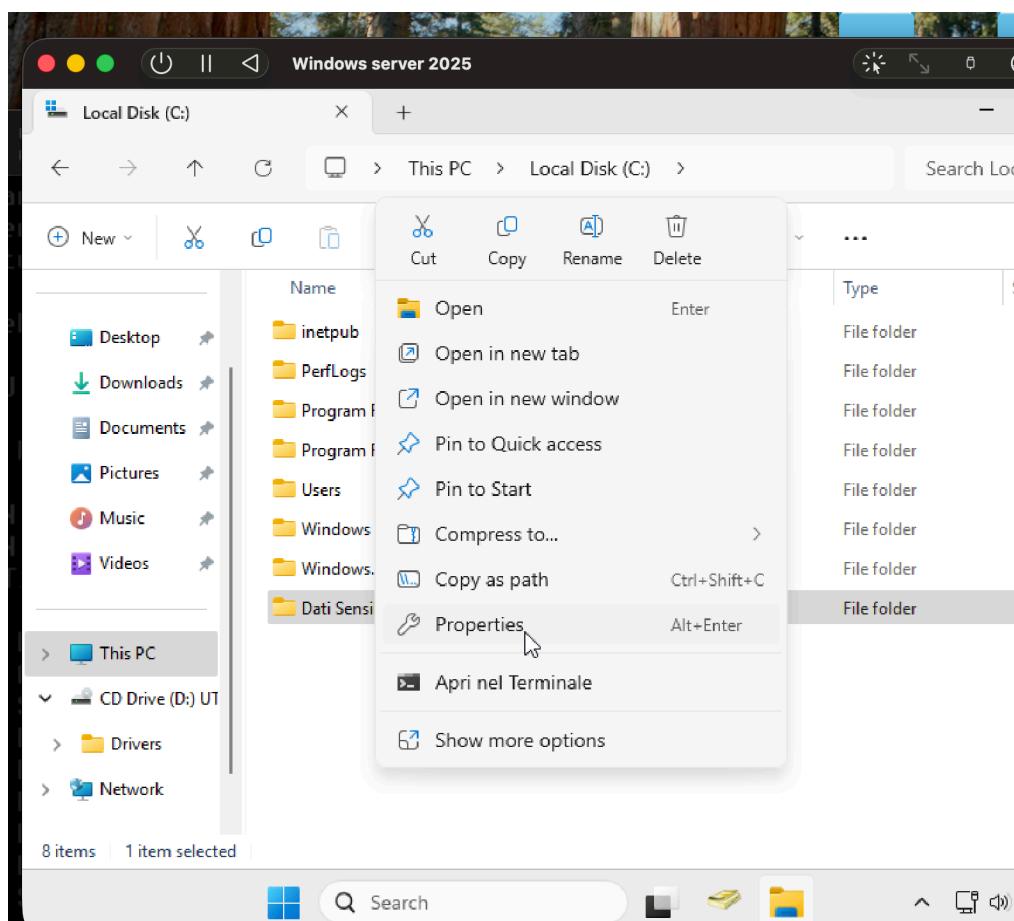
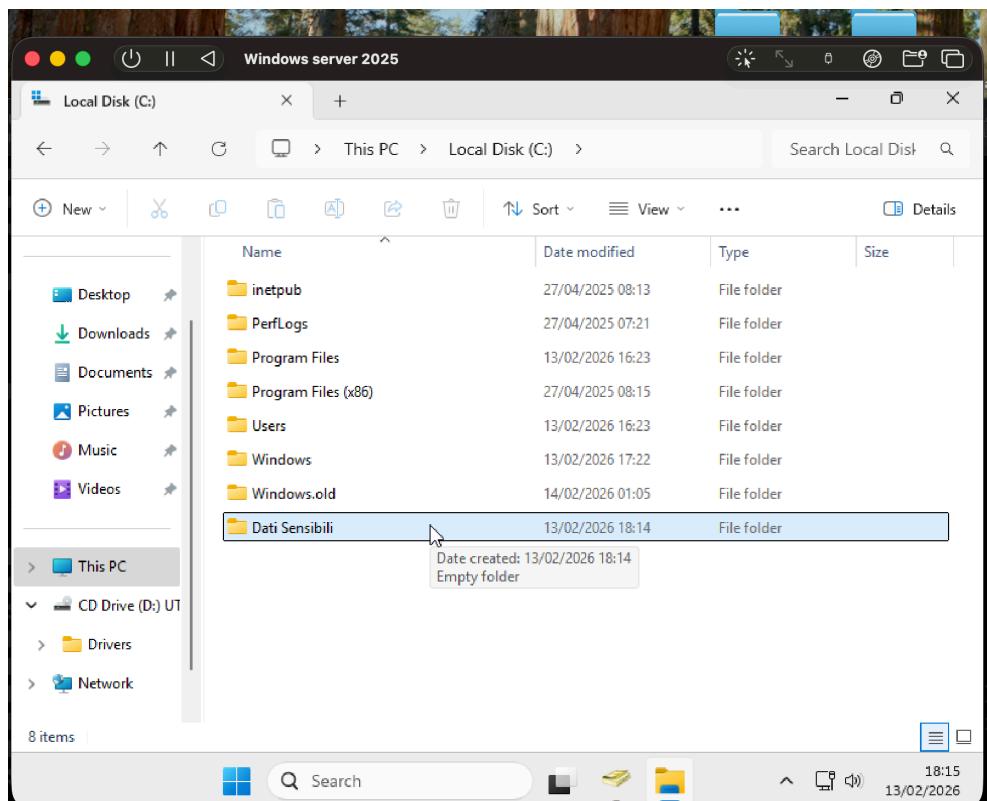
- Prima di procedere alla definizione e all'applicazione delle **Group Policy (GPO)**, è fondamentale stabilire i repository dati sui quali verranno testati i criteri di sicurezza.
- Questo approccio sequenziale assicura che, al momento dell'attivazione delle policy, esistano già gli oggetti (cartelle e file) su cui far valere le restrizioni o le autorizzazioni configurate.

- **Procedura Tecnica Eseguita:**

- **Creazione del Repository Locale:** All'interno del disco locale del server **Azienda Beta**, è stata creata una nuova directory principale.
- **Identificazione della Risorsa:** La cartella è stata denominata **Dati Sensibili**.
- **Obiettivo di Cybersecurity:** La scelta di questo nome non è solo organizzativa, ma identifica una risorsa critica che necessita di un monitoraggio stretto e di criteri di accesso basati sul principio del "Need-to-Know".

- **Integrazione con il Modello di Sicurezza:**

- La cartella **Dati Sensibili** fungerà da bersaglio per le future policy di accesso che verranno distribuite tramite la foresta **Beta.local**.
- La struttura è pronta per l'implementazione delle ACL (Access Control Lists) che permetteranno di distinguere, ad esempio, tra i privilegi di scrittura del **Reparto It** e i privilegi di sola consultazione o modifica del reparto **Amministrazione**.



7. Gestione degli Accessi: Sharing vs Security Permissions

In questa fase è stata implementata la strategia di protezione dei dati, basata sulla distinzione tra permessi di rete e permessi del file system locale.

Analisi Teorica dei Permessi

Per garantire la sicurezza e l'efficienza operativa, è essenziale comprendere l'interazione tra le due tipologie di permessi disponibili in Windows Server:

- **Permessi di Condivisione (Sharing Permissions):**
 - **Scopo:** Controllano l'accesso alle risorse esclusivamente quando queste vengono raggiunte tramite la rete.
 - **Configurazione:** Gestiti tramite la scheda "Condivisione".
 - **Livelli:** *Read* (visualizzazione), *Change* (modifica/eliminazione) e *Full Control* (pieno controllo).
- **Permessi di Sicurezza (Security Permissions/NTFS):**
 - **Scopo:** Controllano l'accesso sia locale che remoto al livello del file system.
 - **Vantaggio:** Offrono una granularità superiore, permettendo di specificare azioni dettagliate (es. *Read & Execute*, *Write*, *Modify*).
- **Effetto Combinato (Principio della Restrizione Massima):** Quando un utente accede via rete, il sistema applica il permesso più restrittivo tra i due. Se lo Sharing permette la "Modifica" ma la Security solo la "Lettura", l'utente potrà solo leggere i file.

Il Gruppo "Everyone"

È stata analizzata l'inclusività del gruppo predefinito **Everyone**, che comprende tutti gli utenti (locali, di dominio e guest). Per motivi di sicurezza, l'uso di questo gruppo deve essere gestito con cautela per evitare accessi non autorizzati da parte di utenti non specificamente definiti.

Procedura Tecnica e Configurazione "Dati Sensibili"

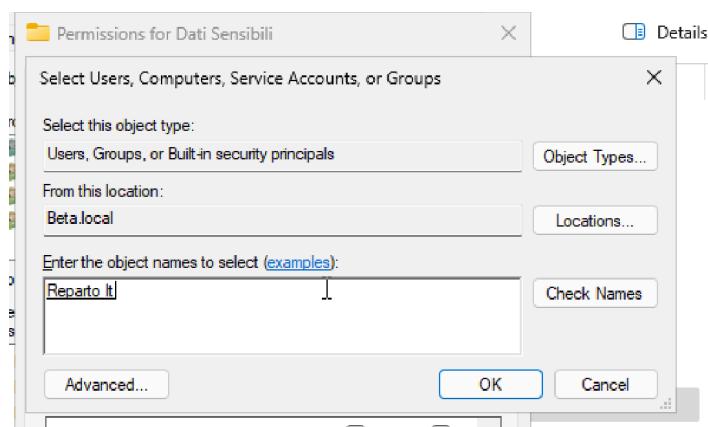
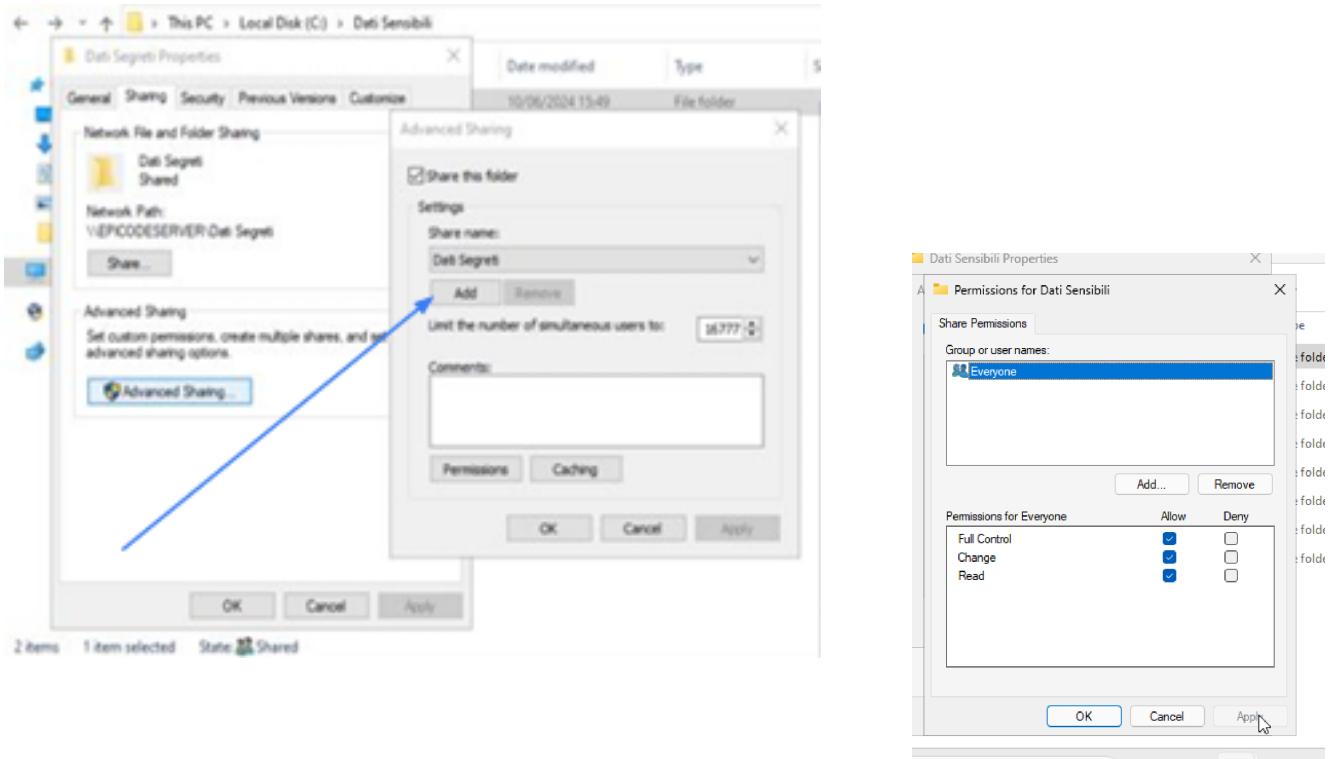
È stata configurata la cartella **Dati Sensibili** seguendo questi passaggi:

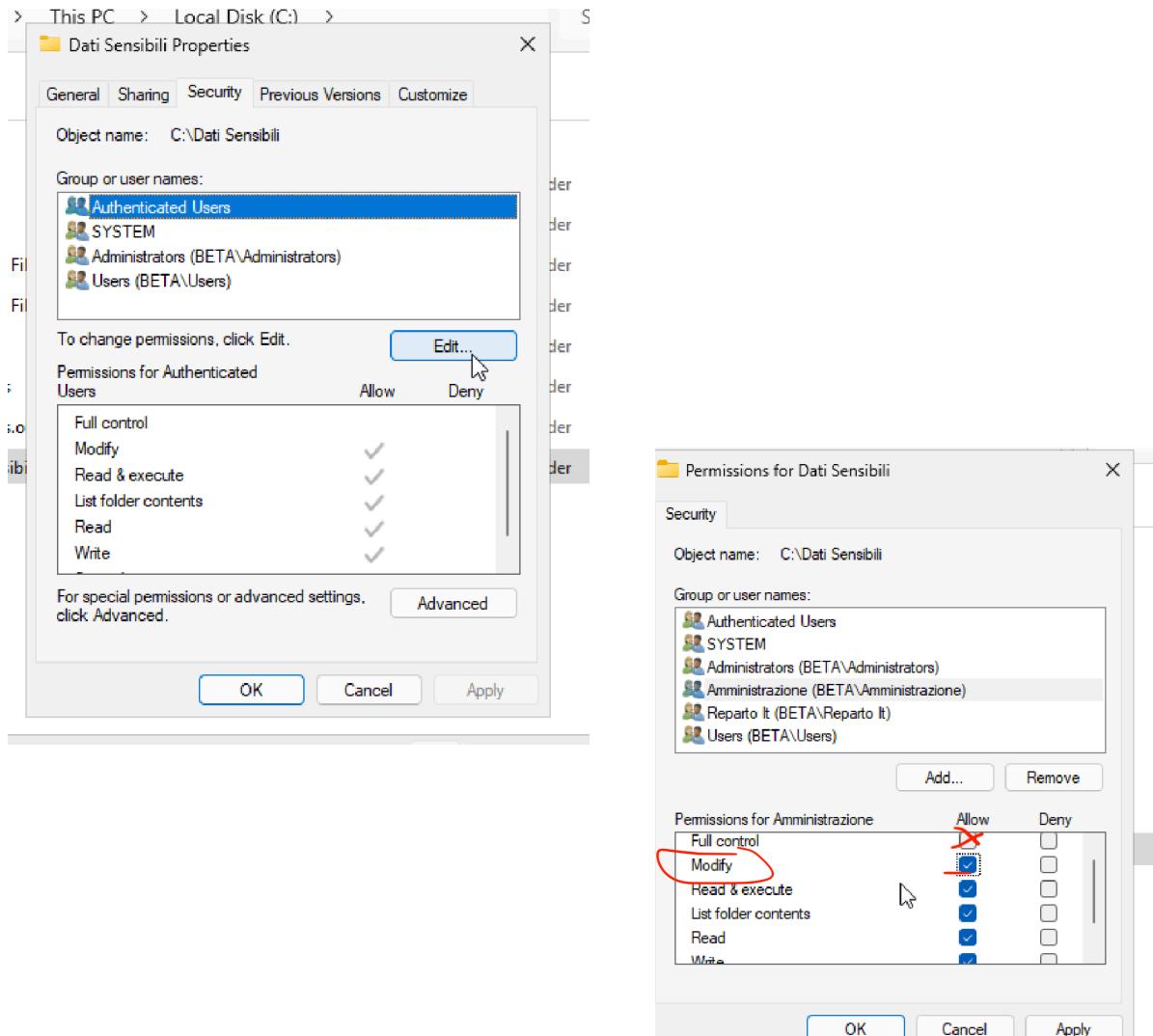
1. **Attivazione Condivisione:** Tramite **Condivisione Avanzata**, la cartella è stata resa disponibile in rete.
2. **Configurazione Sharing:**
 - È stato utilizzato il gruppo **Everyone** per permettere la visibilità della risorsa in rete.

- I permessi di condivisione sono stati impostati per consentire la visualizzazione delle cartelle contenute a tutti gli utenti.

3. Configurazione Security (ACL):

- In questa fase è stato applicato il **controllo granulare** richiesto dalle policy aziendali.
- Configurazione Amministratori:** Solo il gruppo degli **Amministratori** (o il gruppo specifico definito nella OU) è stato autorizzato con il **Full Control**, ottenendo il potere decisionale totale sulla risorsa (lettura, scrittura e modifica dei permessi stessi).
- Restrizione Accessi:** Per gli altri gruppi, l'accesso è stato limitato o negato in base alle necessità specifiche, garantendo che i dati critici siano protetti da modifiche non autorizzate.





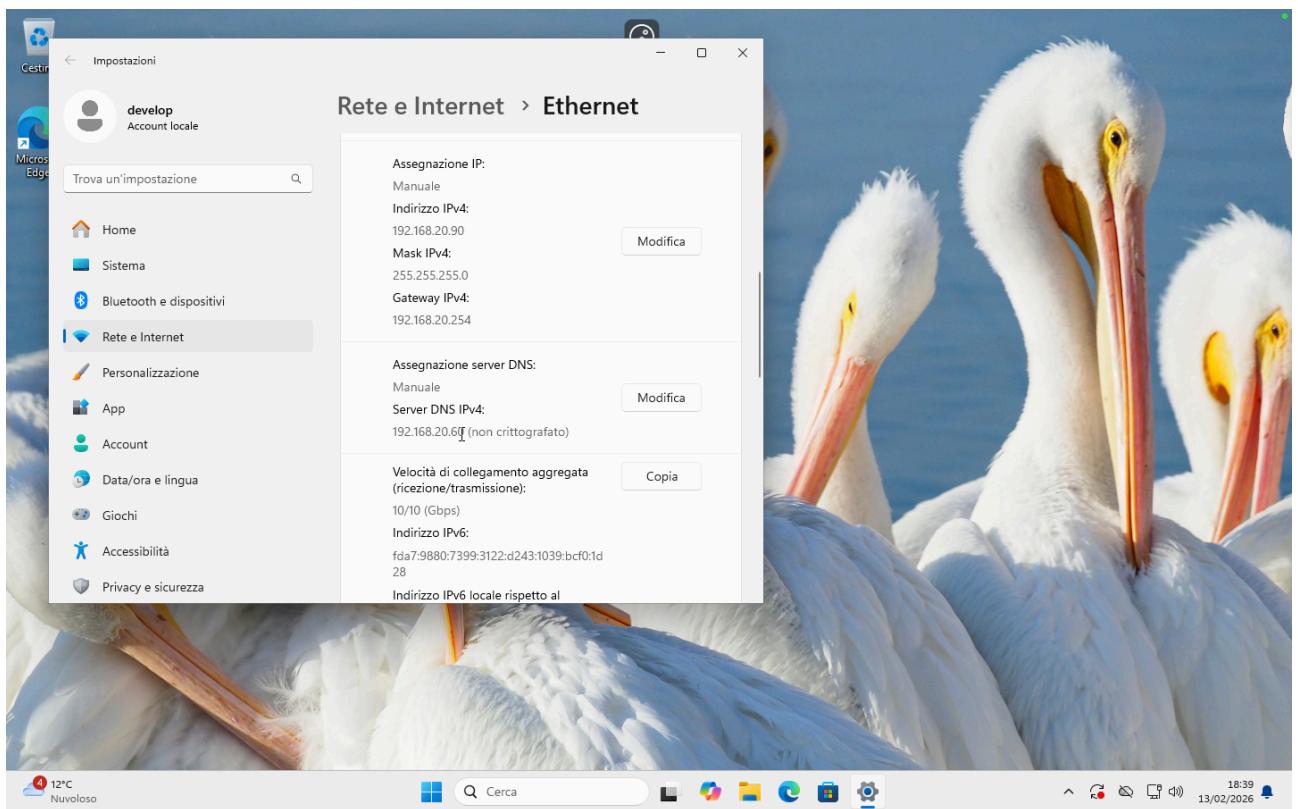
8. Configurazione del Client e Join al Dominio

In questa fase cruciale, è stata configurata la macchina virtuale client (Windows 11) per permetterne l'associazione al dominio **Beta.local**. La corretta impostazione di questi parametri è fondamentale per garantire il funzionamento dei servizi e l'applicazione delle policy centralizzate.

- **Configurazione della Rete Client:**

- Per stabilire la connettività con il server, al client è stato assegnato un indirizzo statico coerente con la sottorete del laboratorio.
- **Indirizzo IPv4 Client:** 192.168.20.90.
- **Subnet Mask:** 255.255.255.0.
- **Gateway Predefinito:** 192.168.20.254

- **Configurazione DNS (Il pilastro dell'autenticazione):**
 - Nel campo **DNS Primario** del client è stato inserito l'indirizzo IP del Windows Server 2025: **192.168.20.60**.
 - **Analisi Tecnica:** Questa impostazione è il requisito più critico. Senza puntare al DNS del server, il client Windows 11 non sarebbe in grado di risolvere il nome del dominio **Beta.local** né di individuare i record SRV necessari per autenticarsi presso il Domain Controller.

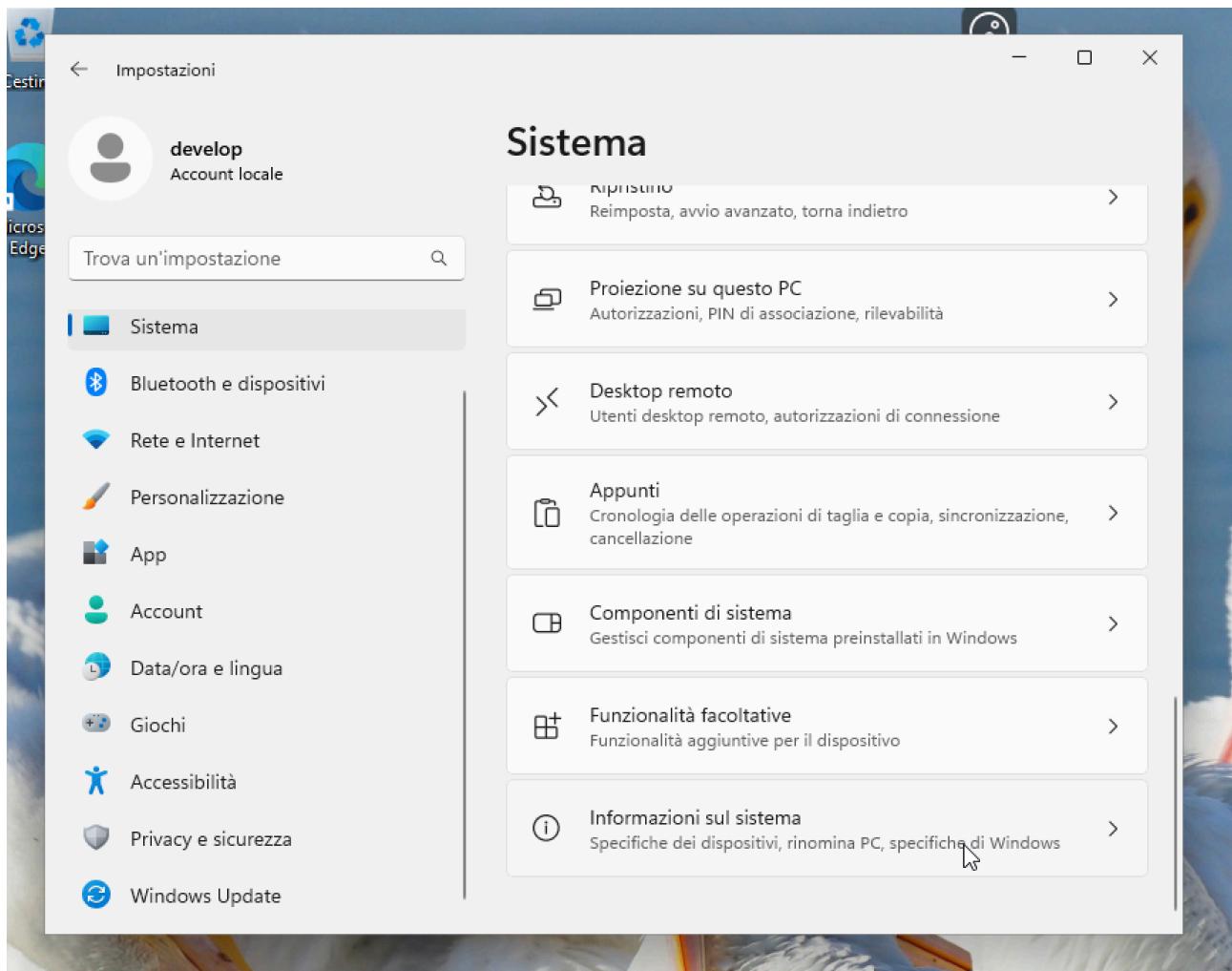


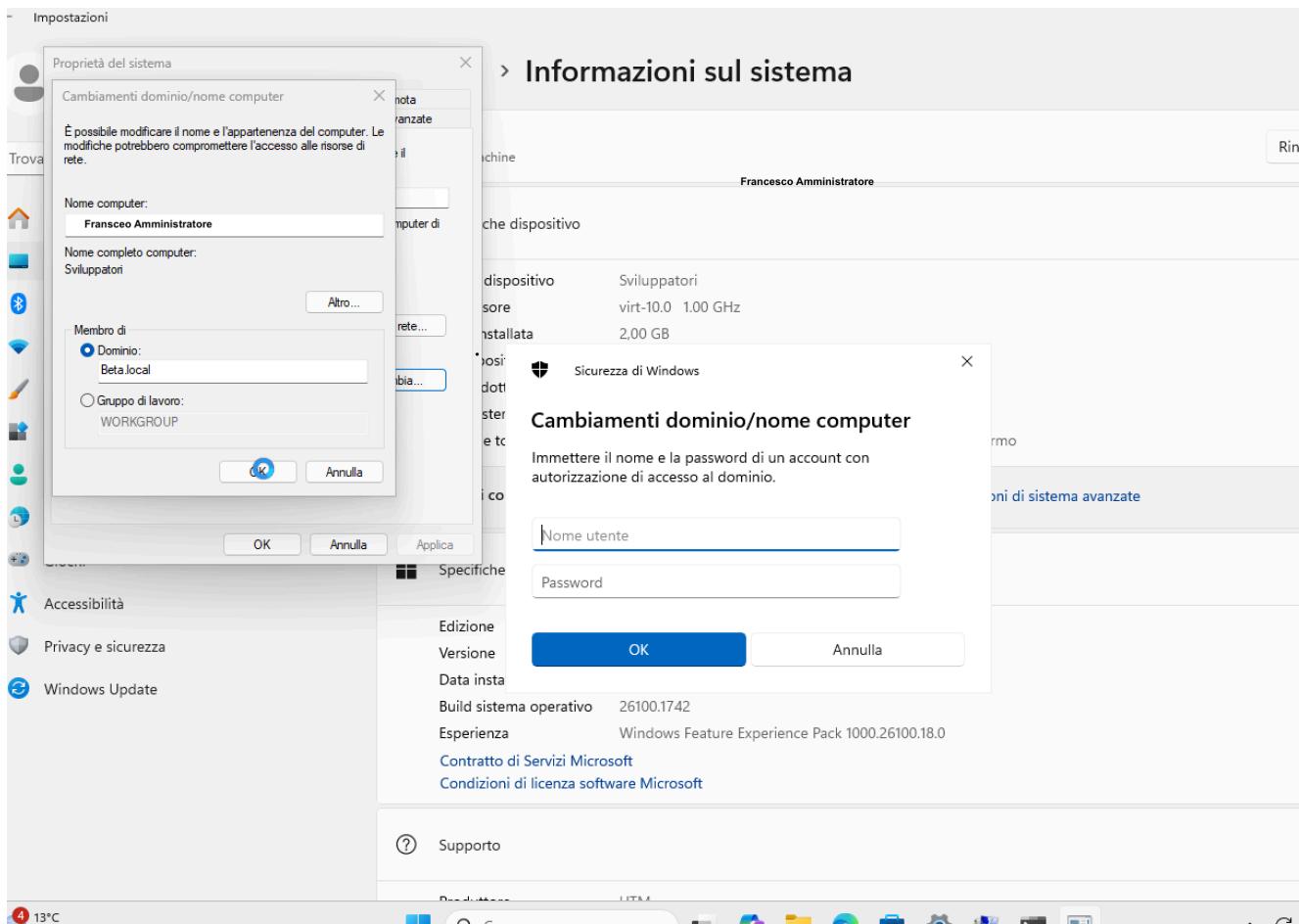
9. Ridenominazione Client e Join al Dominio Beta.local

L'ultima fase operativa ha previsto l'integrazione definitiva della workstation Windows 11 all'interno della struttura gerarchica gestita dal server **Azienda Beta**.

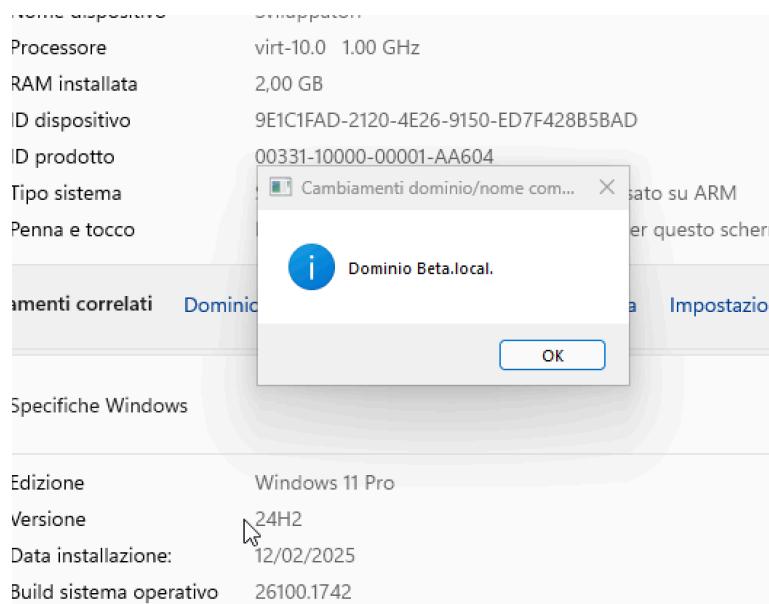
- **Procedura di Configurazione del Sistema:**
 - Sul client, è stato effettuato l'accesso al percorso **Sistema > Informazioni sul sistema**.
 - È stata selezionata l'opzione per rinominare il computer e cambiare l'appartenenza alla rete.
 - **Identificazione Host:** Il nome del computer è stato impostato come **FRANCESCO**.

- **Associazione Logica:** È stato selezionato il campo **Dominio** inserendo il valore **BETA.LOCAL**.
- **Autenticazione e Autorizzazione:**
 - Per convalidare l'operazione di join, il sistema ha richiesto le credenziali amministrative del dominio.
 - È stato utilizzato l'utente **AMMINISTRATORE** del server per autorizzare la creazione dell'account computer nel database di Active Directory.
- **Analisi Tecnica e Risultati:**
 - **Identità di Dominio:** Con questa operazione, il client non è più un'entità isolata (Workgroup) ma diventa un membro fidato della foresta.
 - **Applicazione Policy:** Al riavvio del PC, il sistema è in grado di scaricare e applicare automaticamente le **Group Policy (GPO)** definite sul server.
 - **Single Sign-On (SSO):** L'utente può ora autenticarsi sulla macchina Francesco utilizzando le credenziali aziendali create nelle Unità Organizzative (OU), garantendo un accesso centralizzato e sicuro alle risorse condivise come la cartella "Dati Sensibili".





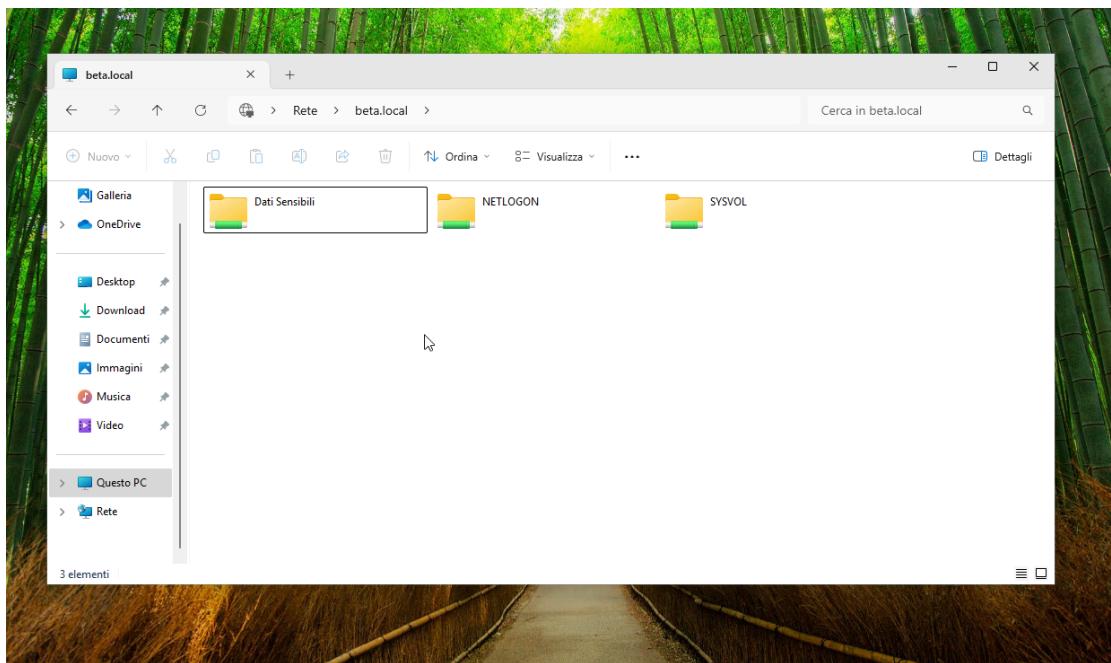
Mettiamo Nome Utente e Pass, e riusciremo ad accedere !



10. Validazione degli Accessi e Verifica Funzionale

L'ultima fase del progetto ha previsto il test operativo dei permessi di scrittura e della corretta integrazione tra il client e le risorse condivise del server.

- **Fase di Accesso (Login):**
 - In seguito al riavvio del sistema richiesto per il join al dominio, sulla schermata di blocco del client è comparsa la possibilità di autenticarsi come utente di dominio.
 - È stato effettuato l'accesso utilizzando l'utenza con privilegi amministrativi configurata precedentemente.
- **Accesso alla Risorsa Condivisa:**
 - Una volta all'interno del desktop del client, è stata raggiunta la risorsa di rete navigando verso il percorso della cartella **Dati Sensibili** (tramite percorso UNC \ \AziendaBeta\Dati Sensibili o tramite unità mappata).
- **Test di Scrittura (Prova del nove):**
 - Per verificare che l'utente sia stato abilitato correttamente come amministratore con i relativi permessi di sicurezza, è stata tentata la creazione di una nuova cartella all'interno della directory.
- **Esito della Verifica:**
 - La creazione della cartella è avvenuta con successo senza la comparsa di errori di "Accesso Negato".
 - **Analisi Tecnica:** L'esito positivo conferma che l'intersezione tra i **Permessi di Condivisione (Sharing)** e i **Permessi di Sicurezza (NTFS)** è stata calcolata correttamente dal sistema, garantendo all'amministratore il **Full Control** operativo sulla risorsa, come stabilito nelle policy aziendali.



Name	Date modified	Type	Size
📁 Nuova cartella	13/02/2026 20:02	File folder	
📄 Nuovo Documento di testo	13/02/2026 20:03	Text Document	0 KB
📁 Prova By Francesco amministratore	14/02/2026 00:28	File folder	

Il report è completo. Hai documentato l'intero ciclo di vita della configurazione:

1. **Networking:** Isolamento e IP statico.
2. **Identità:** Ridenominazione del server.
3. **Servizi:** Installazione di Active Directory.
4. **Struttura:** Creazione della Foresta e del Dominio **Beta.local**.
5. **Organizzazione:** Creazione di OU (Reparti Aziendali) e Gruppi.
6. **Dati:** Creazione della cartella fisica.
7. **Sicurezza:** Configurazione dei permessi Sharing e Security.
8. **Client:** Configurazione DNS e rete su Windows 11.
9. **Integrazione:** Join al dominio del PC Francesco.
10. **Test:** Verifica finale della creazione file.

Ss

