

TRACCIA ESERCIZIO W10L5

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.

Istruzioni

1. **Preparazione:**
 - Accedi al tuo ambiente Windows Server 2022.
 - Assicurati di avere i permessi amministrativi necessari per creare e gestire gruppi.
2. **Creazione dei Gruppi:**
 - Crea due gruppi distinti. Puoi scegliere i nomi che preferisci per questi gruppi, ma assicurati che i nomi siano significativi per riflettere la loro funzione o ruolo all'interno dell'organizzazione (ad esempio, "Amministratori", "UtentiStandard", "MarketingTeam", "Sviluppatori", ecc.).

< > 3 5 ↺ ↻

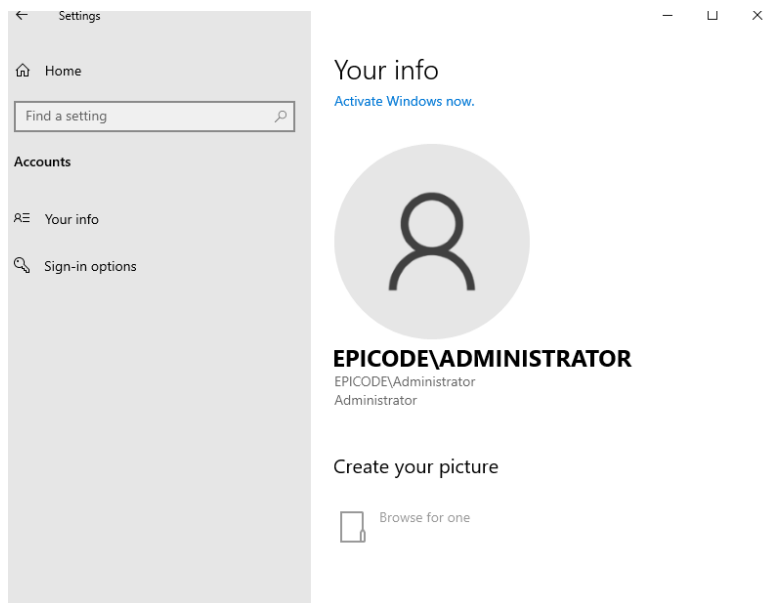
Esercizio di oggi: Creazione di Gruppi in Windows Server 2022

3. **Assegnazione dei Permessi:**
 - Per ogni gruppo, assegna permessi specifici. Puoi scegliere quali permessi concedere, ma assicurati di considerare i seguenti aspetti:
 - Accesso ai file e alle cartelle.
 - Esecuzione di programmi specifici.
 - Modifiche alle impostazioni di sistema.
 - Accesso remoto al server.
 - Documenta i permessi assegnati a ciascun gruppo, spiegando perché hai scelto tali permessi.
4. **Verifica:**
 - Una volta creati i gruppi e assegnati i permessi, verifica che le impostazioni siano corrette. Puoi farlo:
 - Creando utenti di prova e aggiungendoli ai gruppi.
 - Verificando che gli utenti abbiano i permessi assegnati in base al gruppo a cui appartengono.
5. **Documentazione:**
 - Scrivi un breve report che includa:
 - I nomi dei gruppi creati.
 - I permessi assegnati a ciascun gruppo.
 - I passaggi seguiti per creare e configurare i gruppi.
 - Eventuali problemi riscontrati e come li hai risolti.

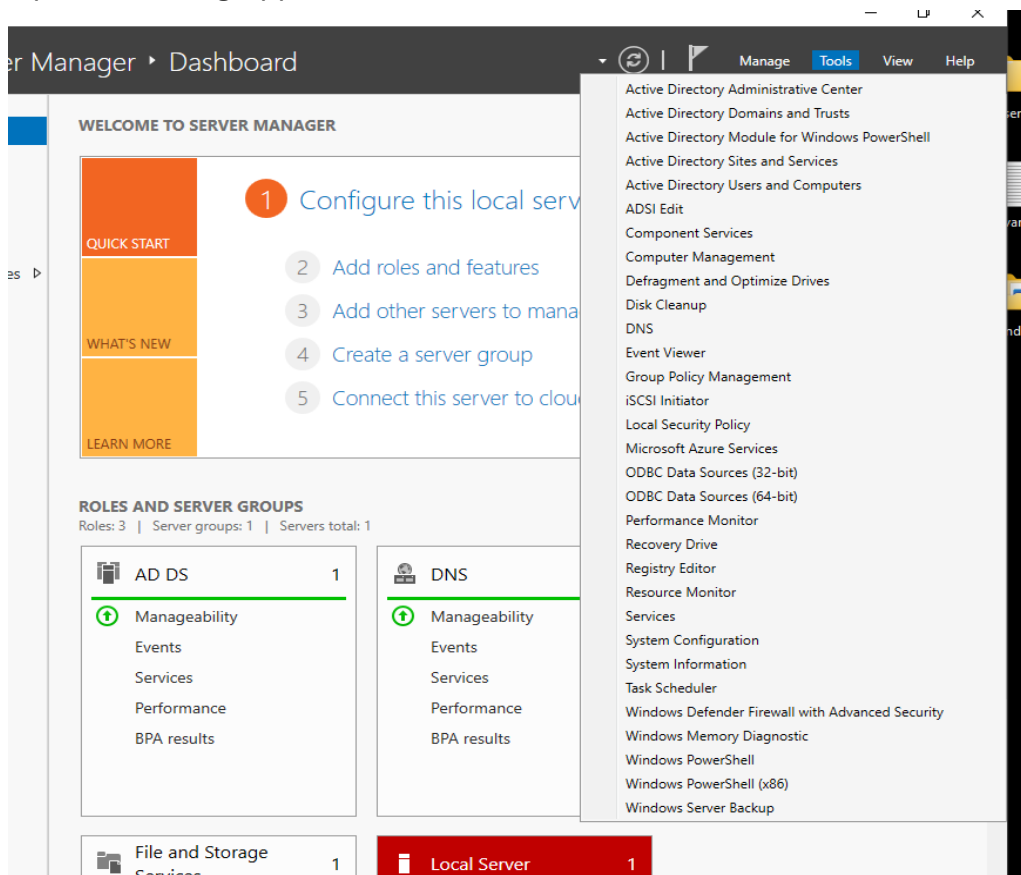
4

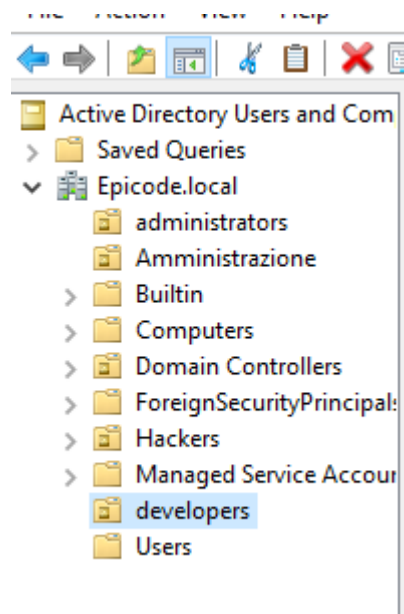
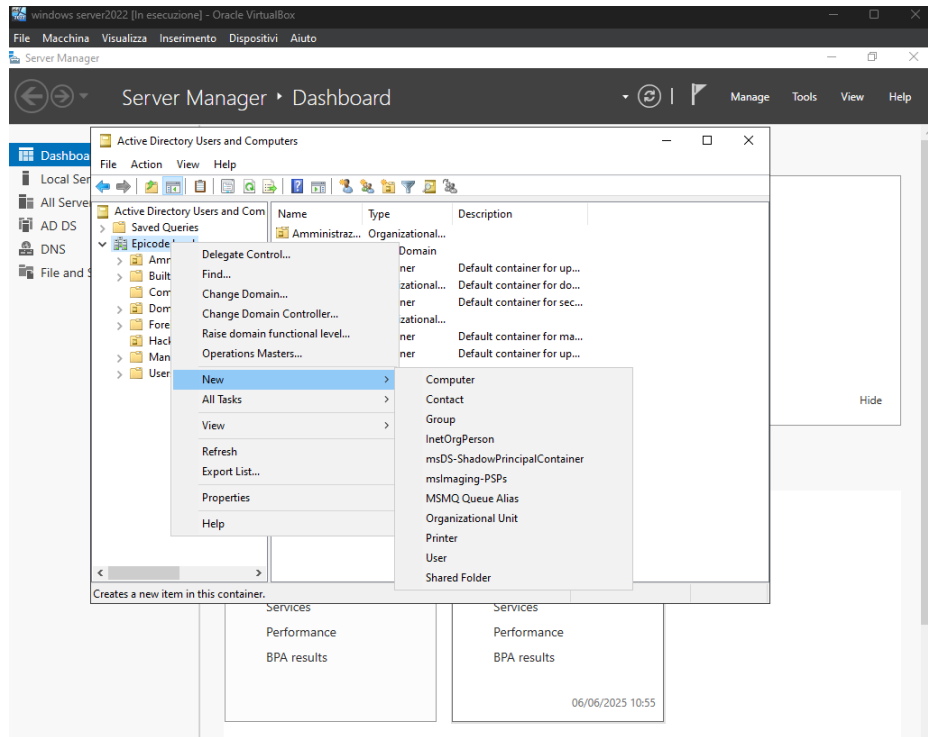
Creo due cartelle (ammin e develop) nella cartella di rete Dati W10L5 in cui possono entrare da pc Client user1 e user2 appartenente a gruppo amministratori e user 3, user4 appartenenti a gruppo sviluppatori. Per non confondere con altre impostazioni abbiamo anche definito due unità organizzative(administrators e developers).

1. **Preparazione:** Accediamo all'ambiente Windows Server 2022. Siamo già sicuri dei nostri permessi amministrativi ma per verificare che siamo amministratori...

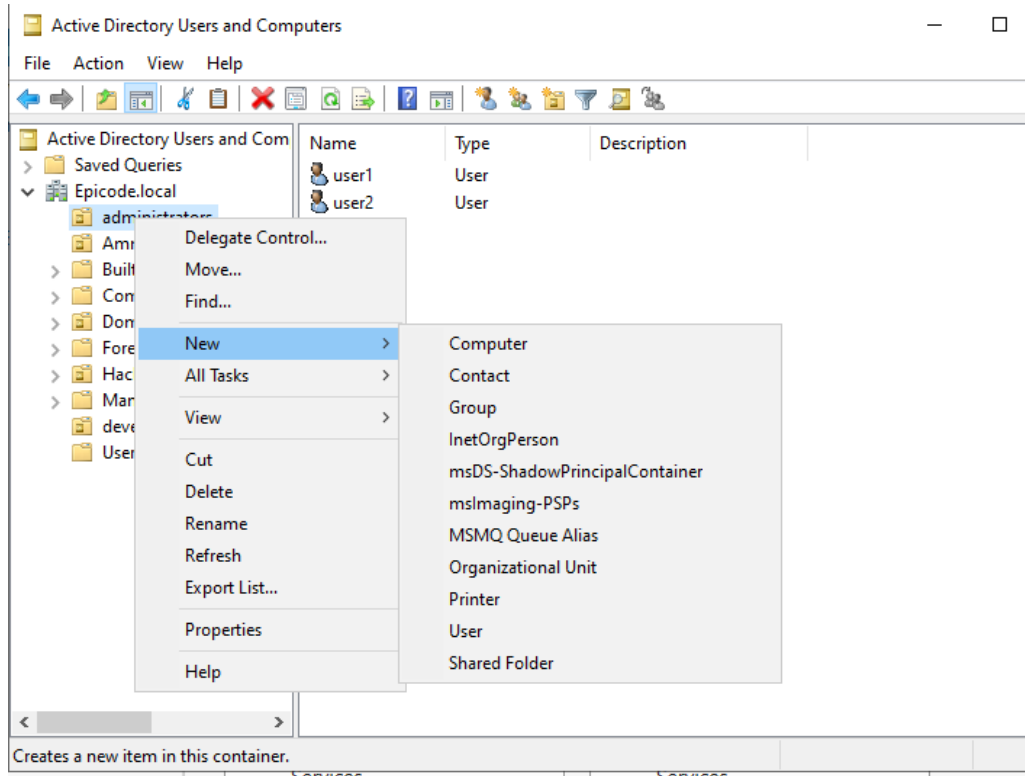


2. Creazione dei Gruppi: accedendo ad Active directory users and computers tramite Tools creiamo le unita organizzative a partire dalla nostra foresta/dominio preesistente Epicode.local
E poi due i due gruppi distinti

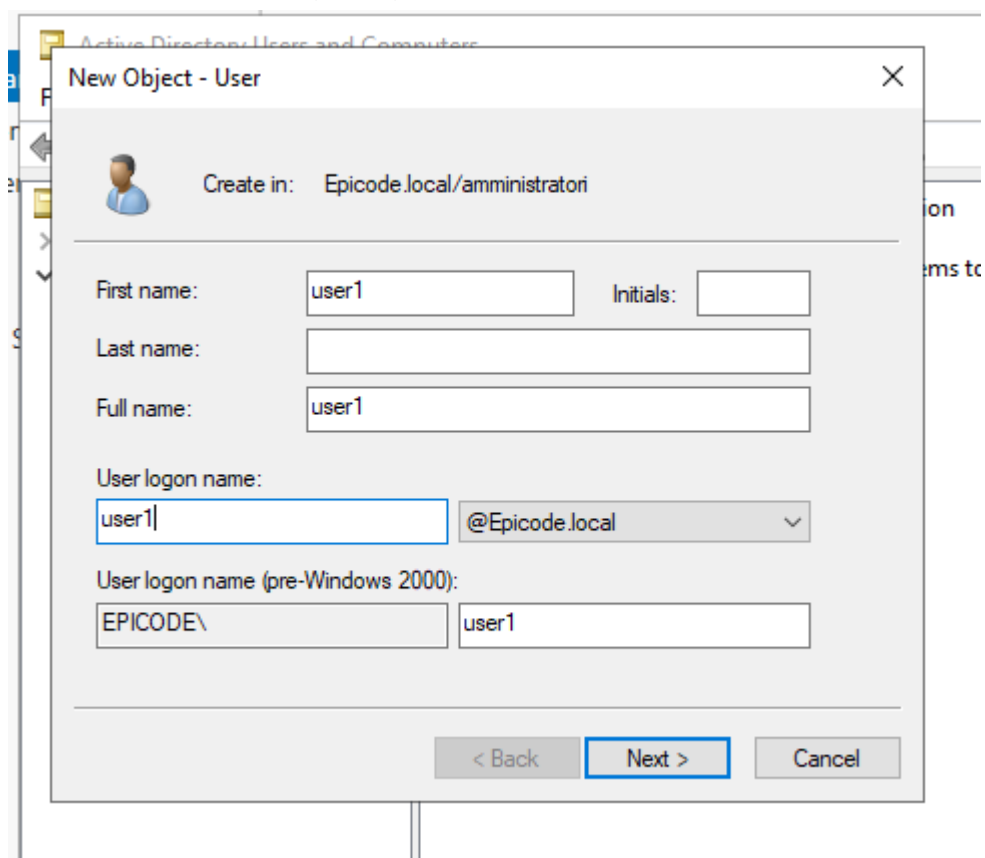




Create le nostre OU administrators e developers, andiamo a creare all'interno gli utenti e i rispettivi gruppi

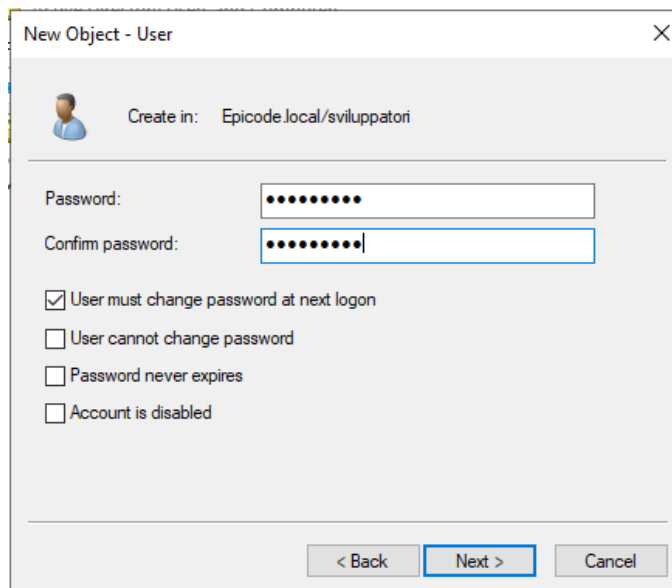


Taso dx su relativa OU, new , user



In administrators abbiamo gli utenti user1 e user2 mentre in developers abbiamo user3 e user4.

Ci verra' richiesta di impostare la password che faremo in modo che sia reimpostata al primo accesso per correttezza e sicurezza. Solo l'utente deve essere in possesso della password, nemmeno l'amministratore del server dovrebbe conoscerla.



New Object - User

Create in: Epicode.local/sviluppatori

Password:

Confirm password:

☒ User must change password at next logon

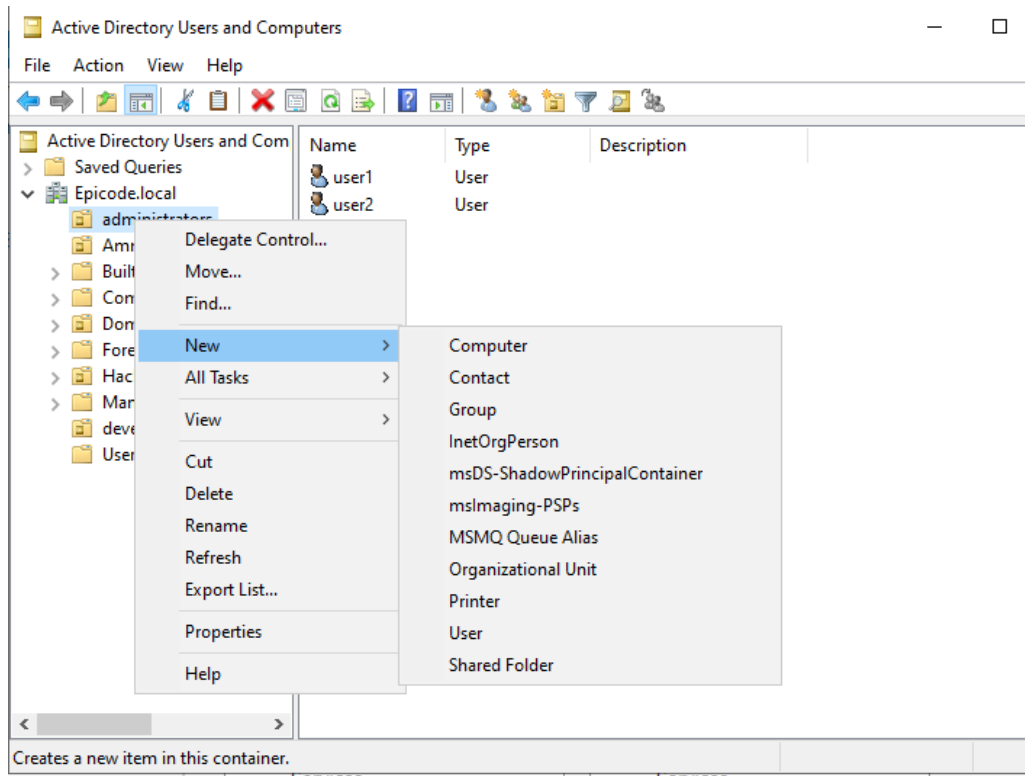
☐ User cannot change password

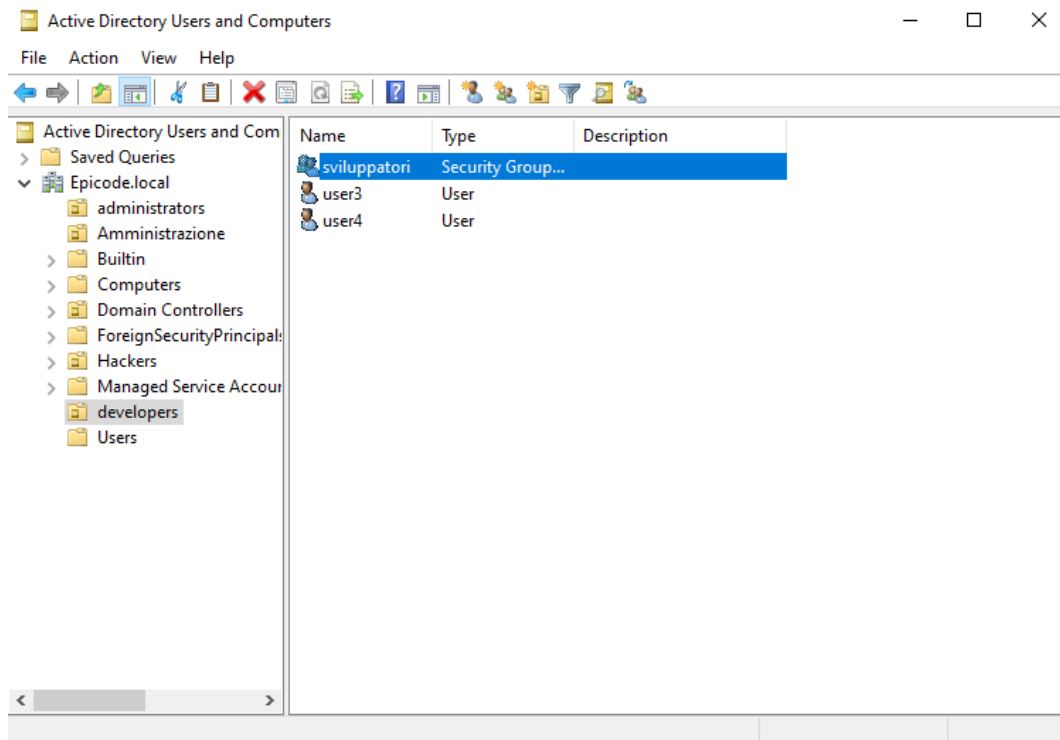
☐ Password never expires

☐ Account is disabled

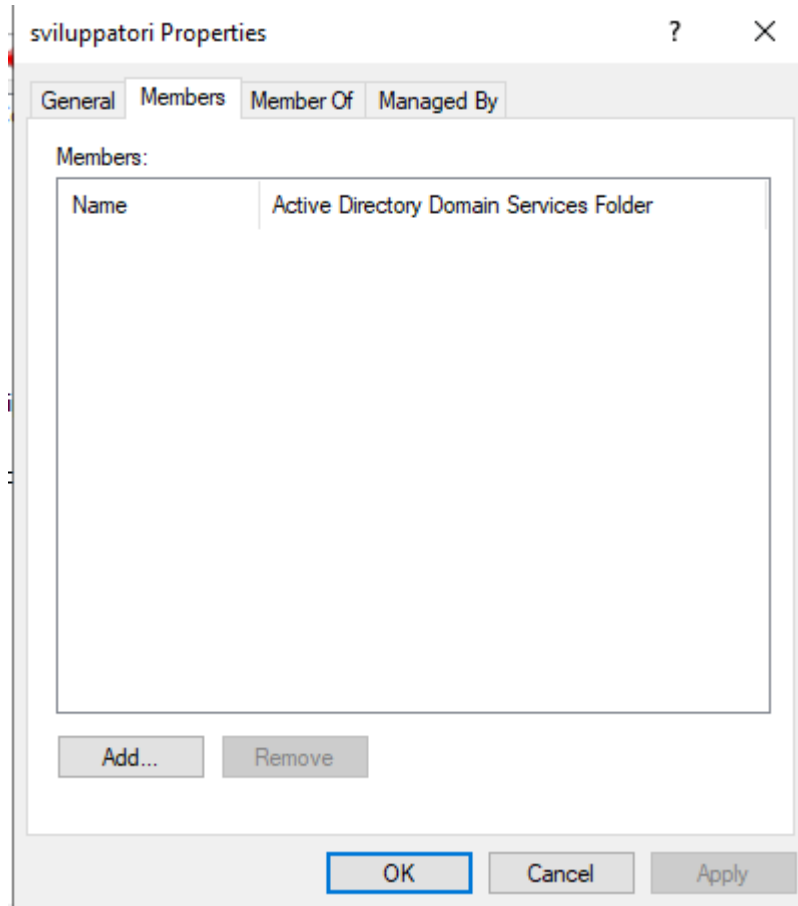
< Back Next > Cancel

Allo stesso modo aggiungiamo il gruppo scegliendolo dalla tendina

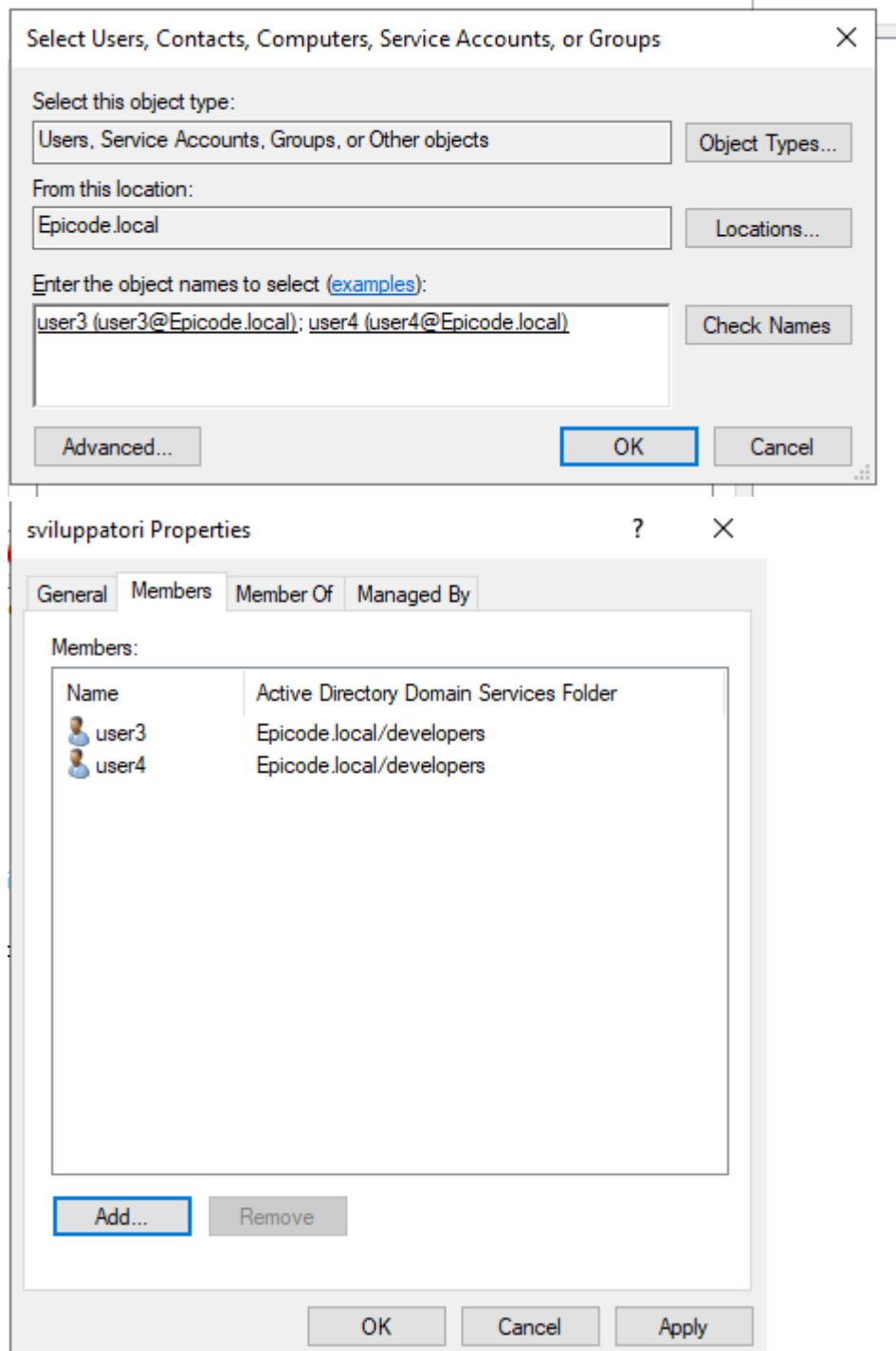




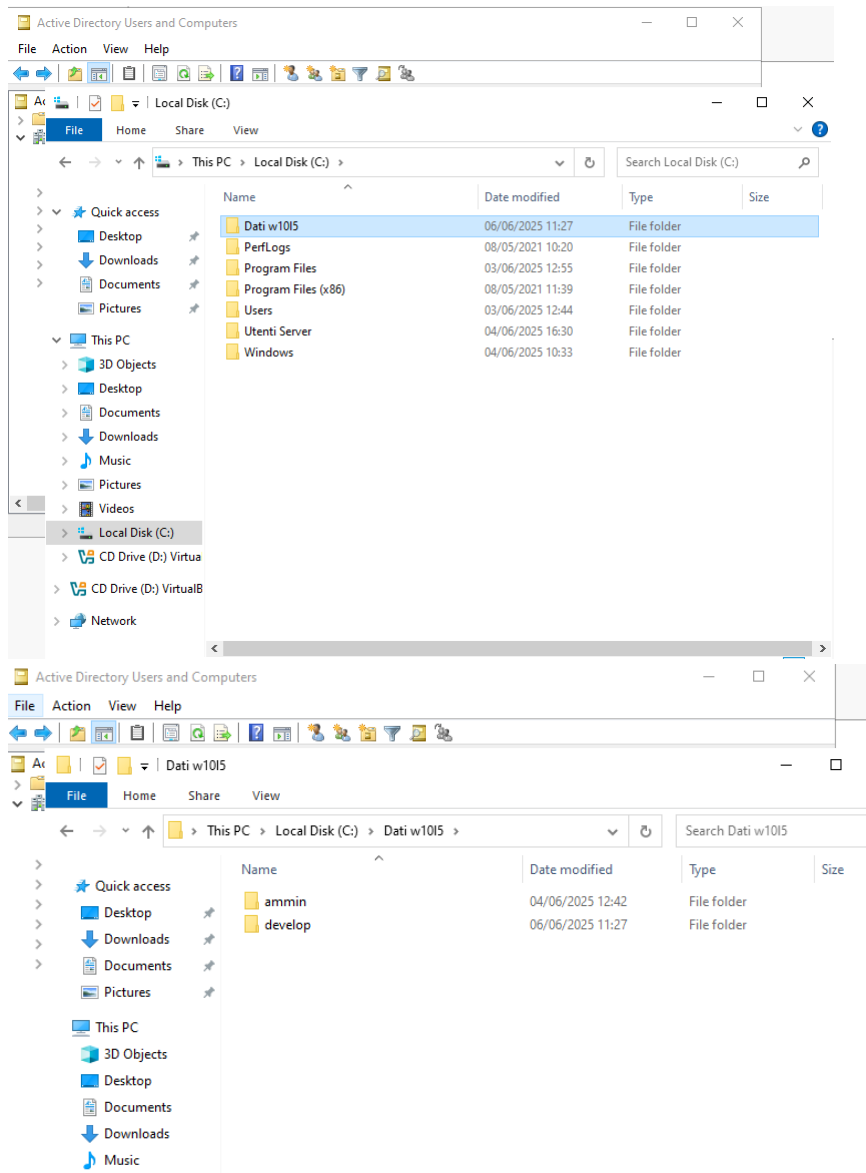
Selezionando il gruppo possiamo attribuirgli i membri



Allo stesso modo creiamo l'altro gruppo di sviluppatori a cui possono accedere user3 e user4 il tutto collocato in unità organizzativa developers.



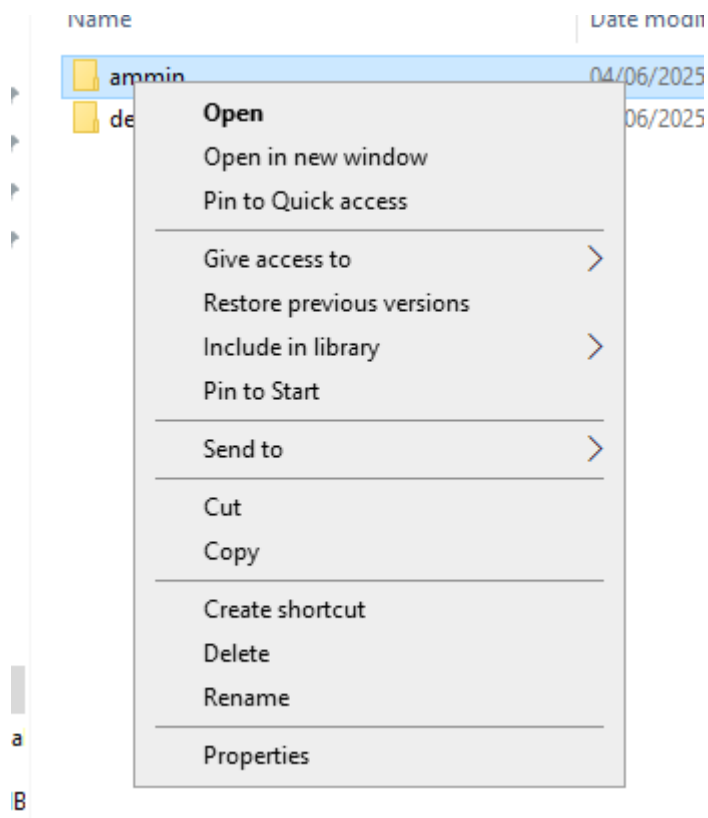
Creiamo la cartella Group Policy Dati W10L5 con all'interno le altre cartelle annidate e file relativi.



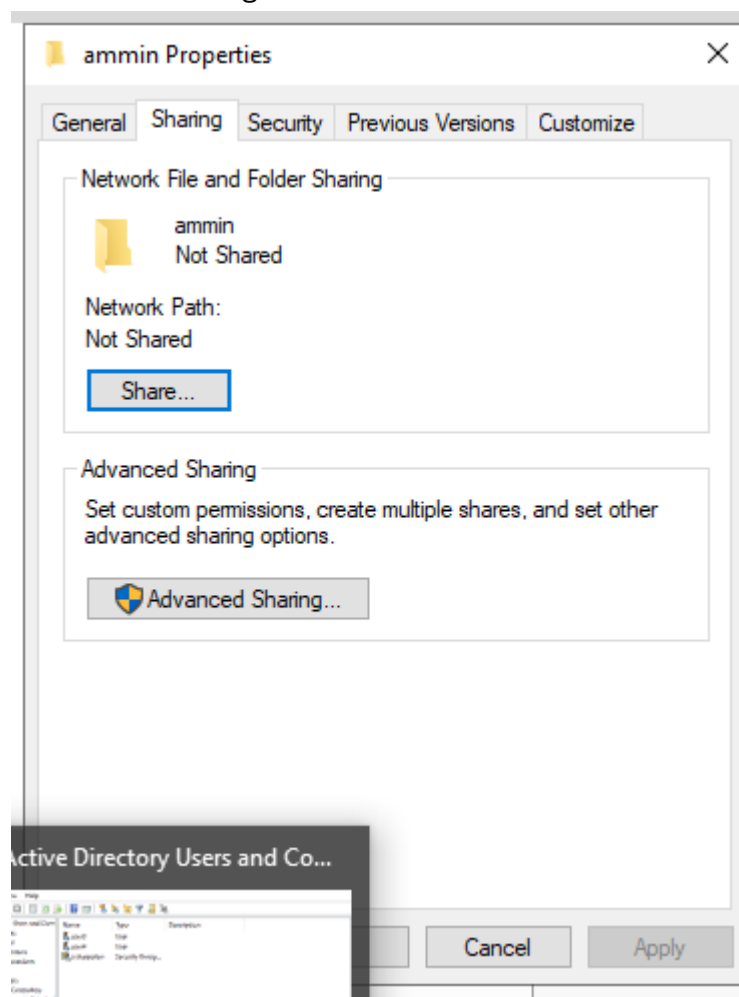
3. Assegnazione dei Permessi:

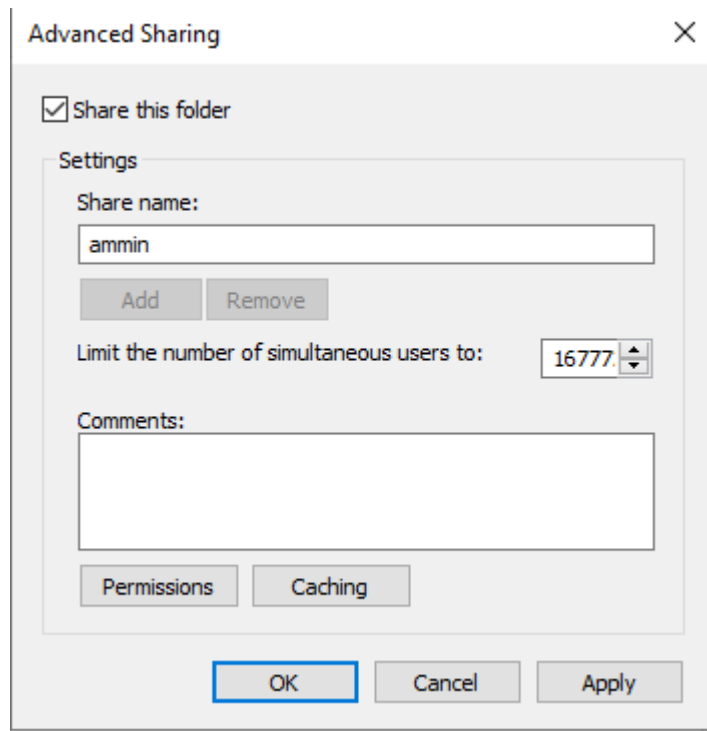
Tasto dx sulla cartella a cui dare i permessi e Properties

Accesso alla Cartella , Rimozione di "Everyone" ,Aggiunta del Gruppo relativo, Applicazione delle modifiche.

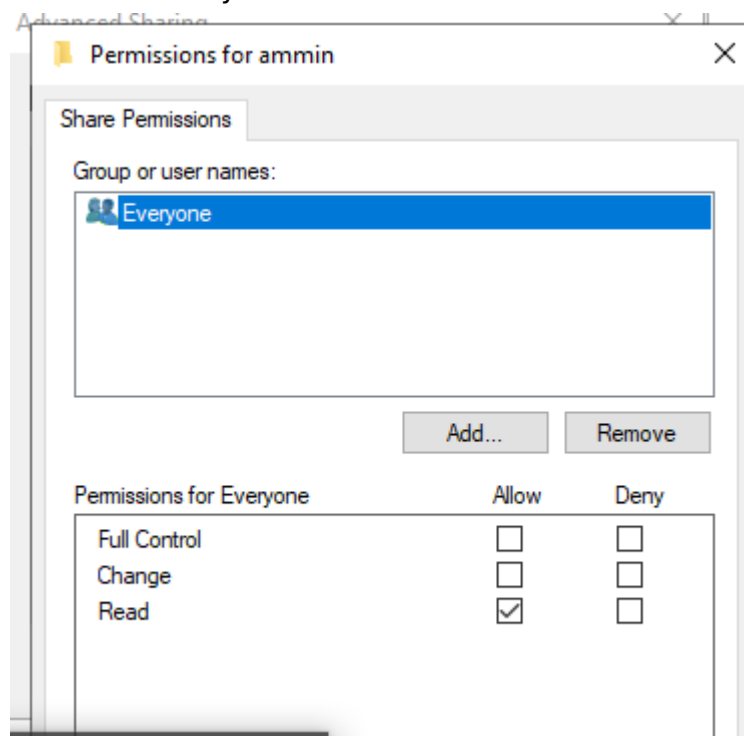


Advanced sharing

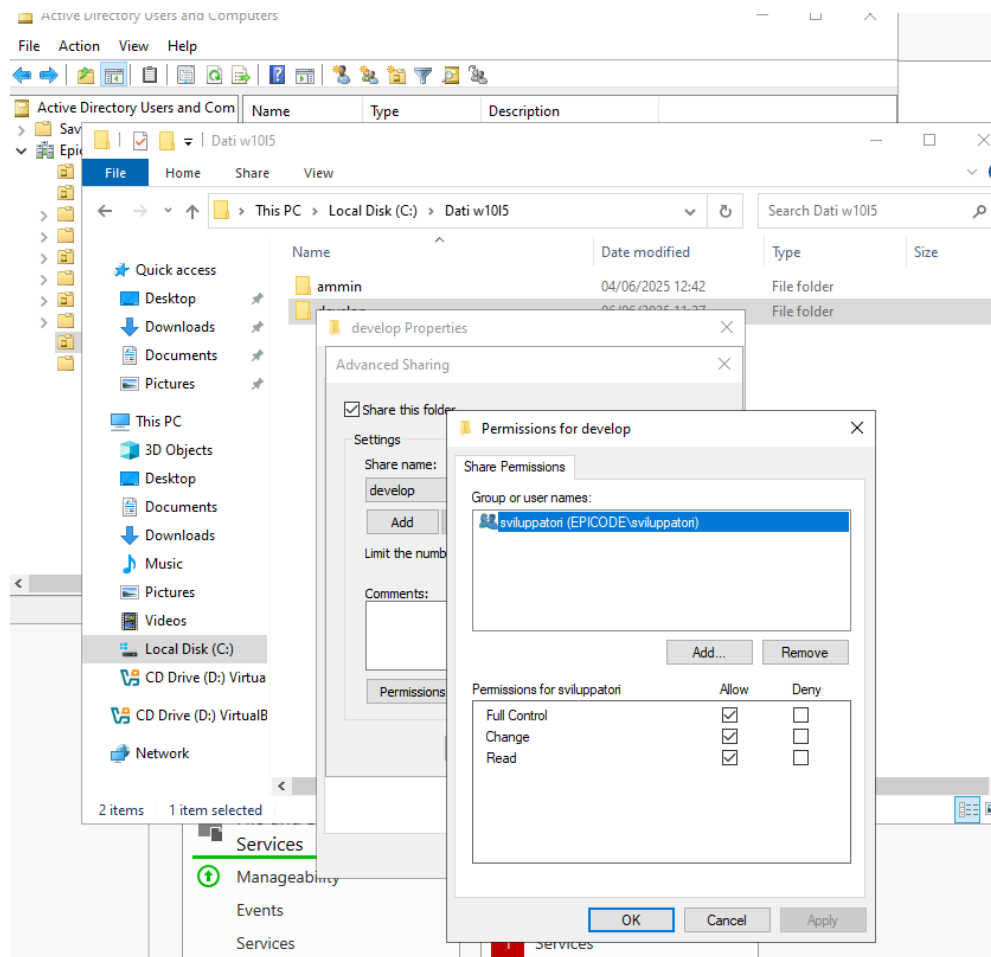




Rimozione everyone



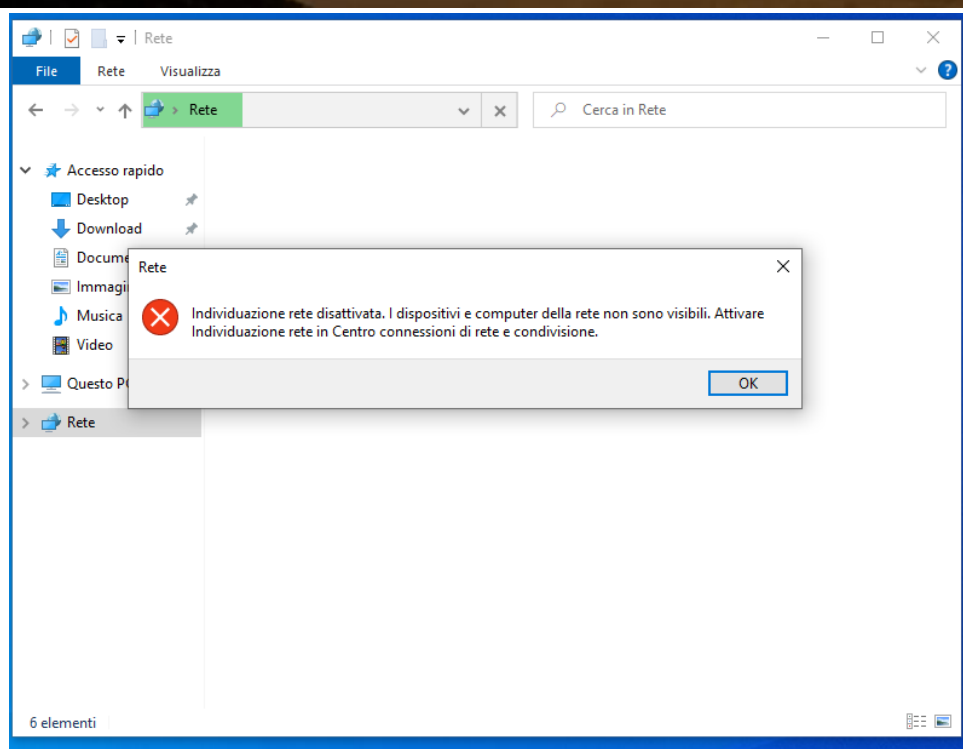
Aggiungiamo con add il gruppo o gli utenti

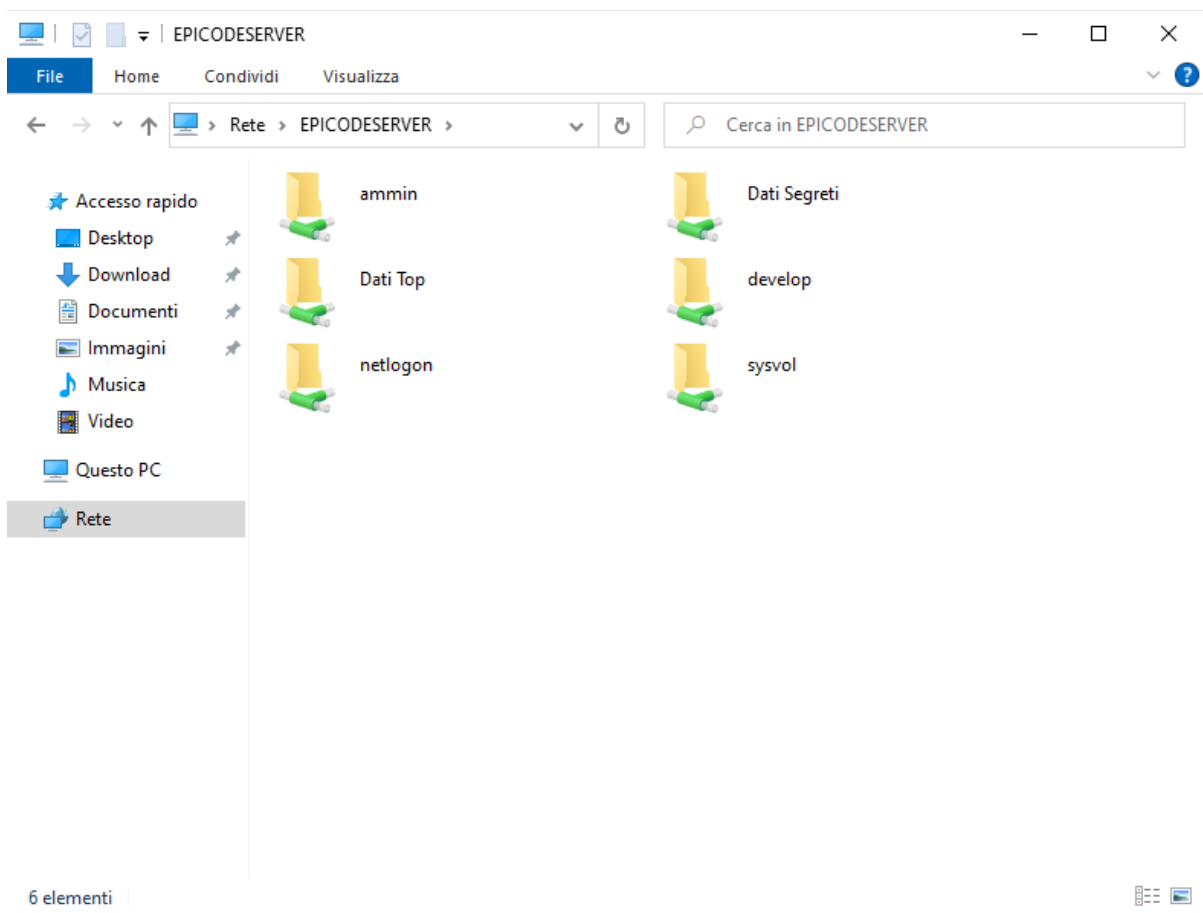
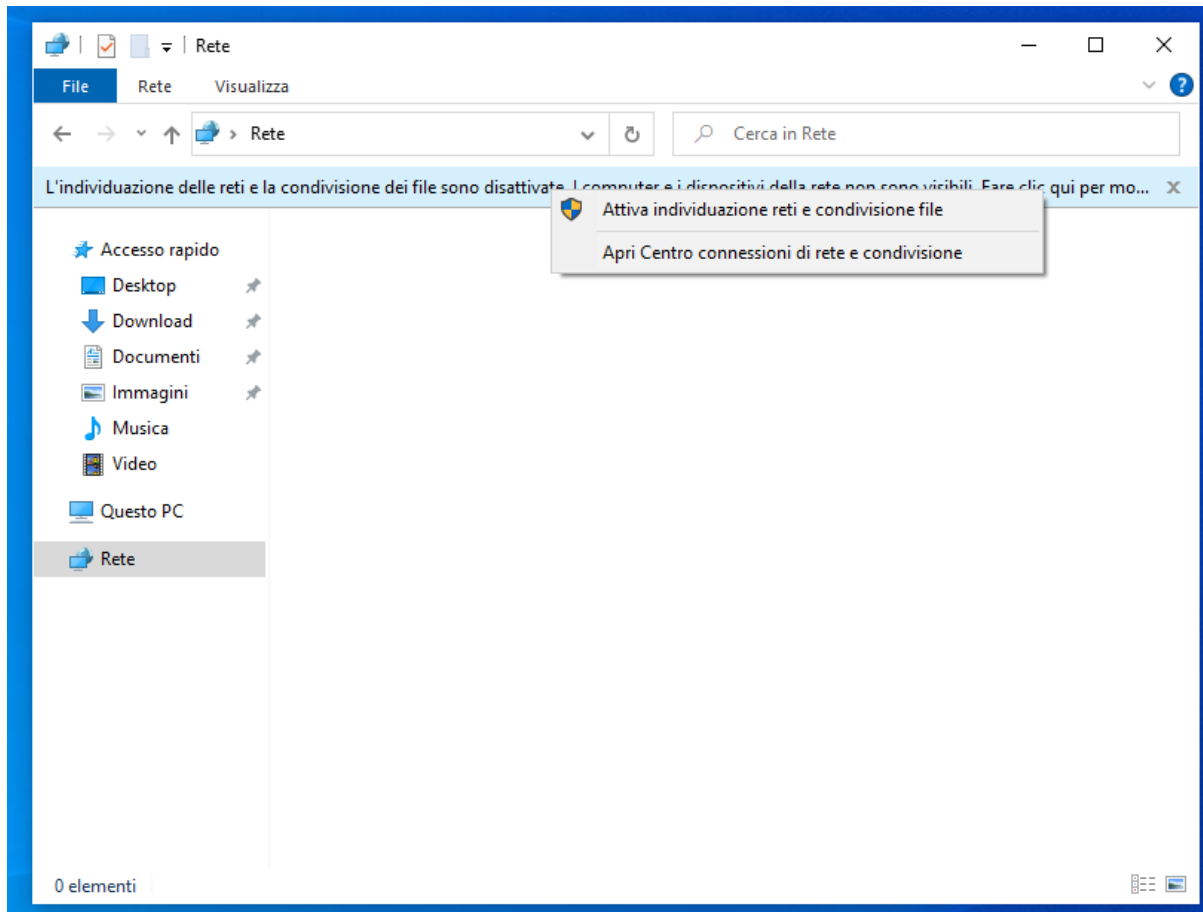


4. Verifica:

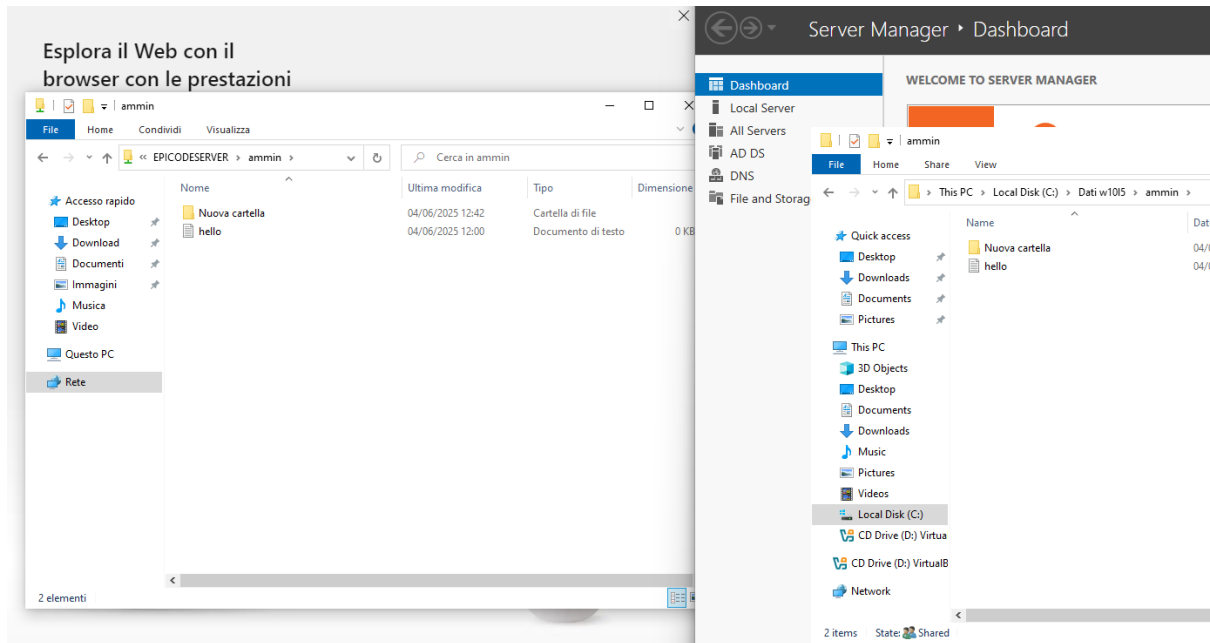
Una volta creati i gruppi e assegnati i permessi, verifichiamo che le impostazioni siano corrette. Facciamo direttamente un accesso al pc client con i relativi utenti dei due vari gruppi , per vedere se i permessi impostati soddisfano i requisiti. Ricapitolando volevamo che il gruppo sviluppatori avesse accesso alla cartella develop mentre il gruppo amministratori deve avere l'accesso alla cartella ammin. I gruppi ovviamente non possono entrare in altre cartelle.

Qui accediamo con l' user1 che appartiene al gruppo amministratori
E quindi ci aspettiamo che posso accedere solo alla cartella di rete server ammin

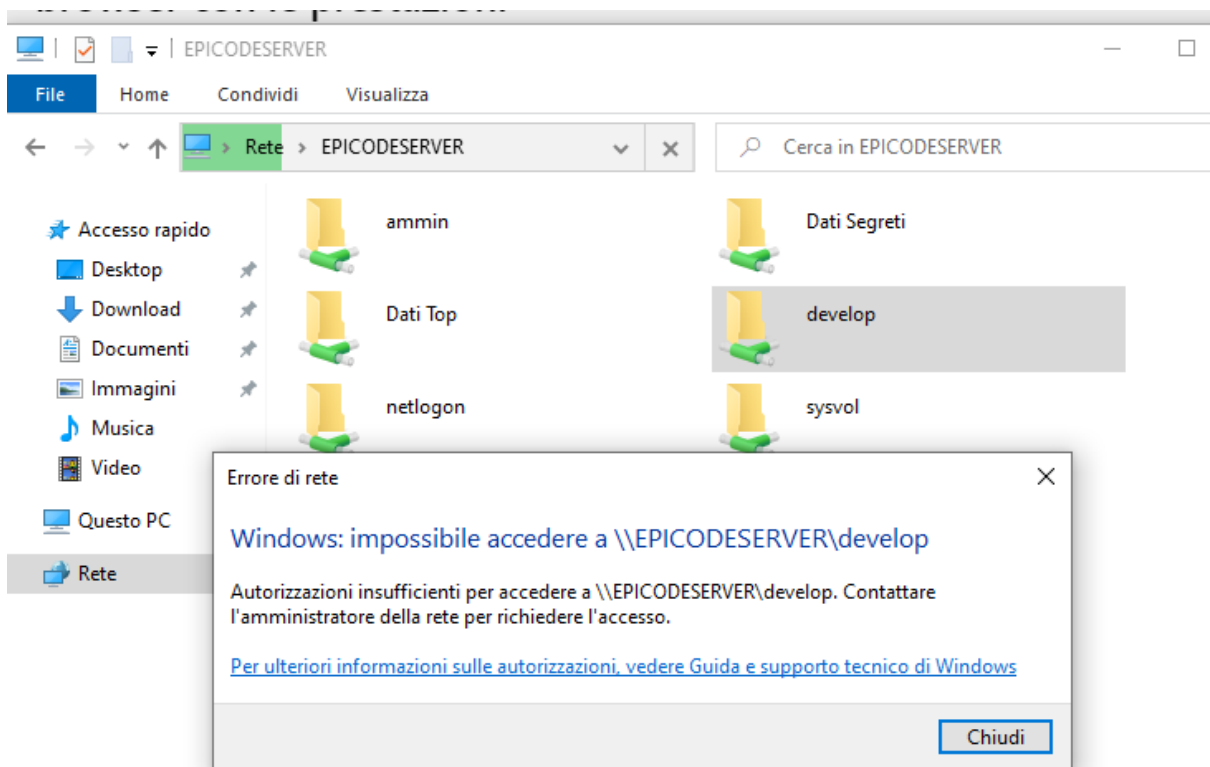




Effettivamente accede

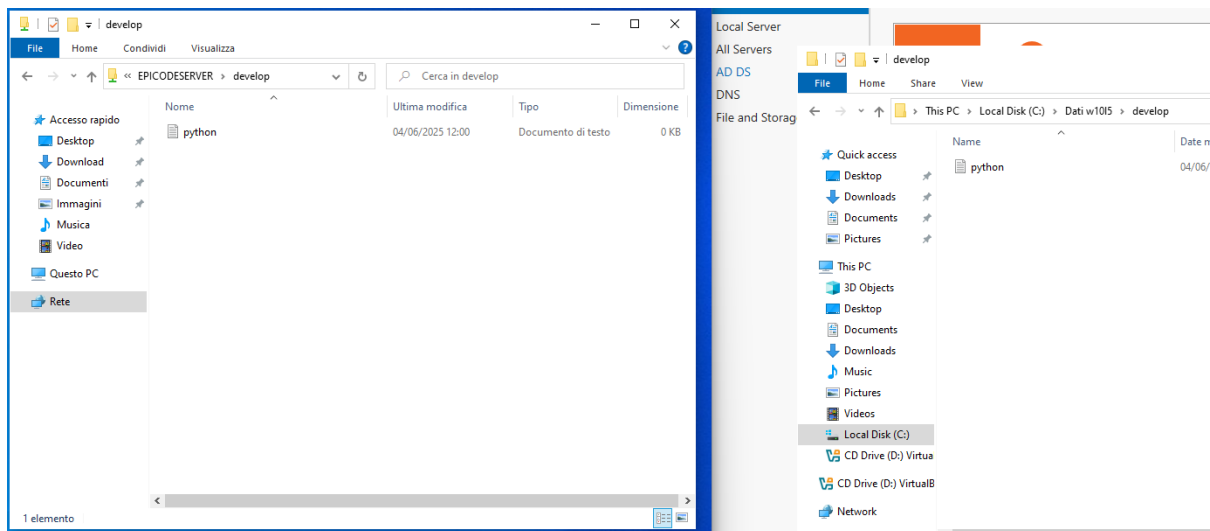


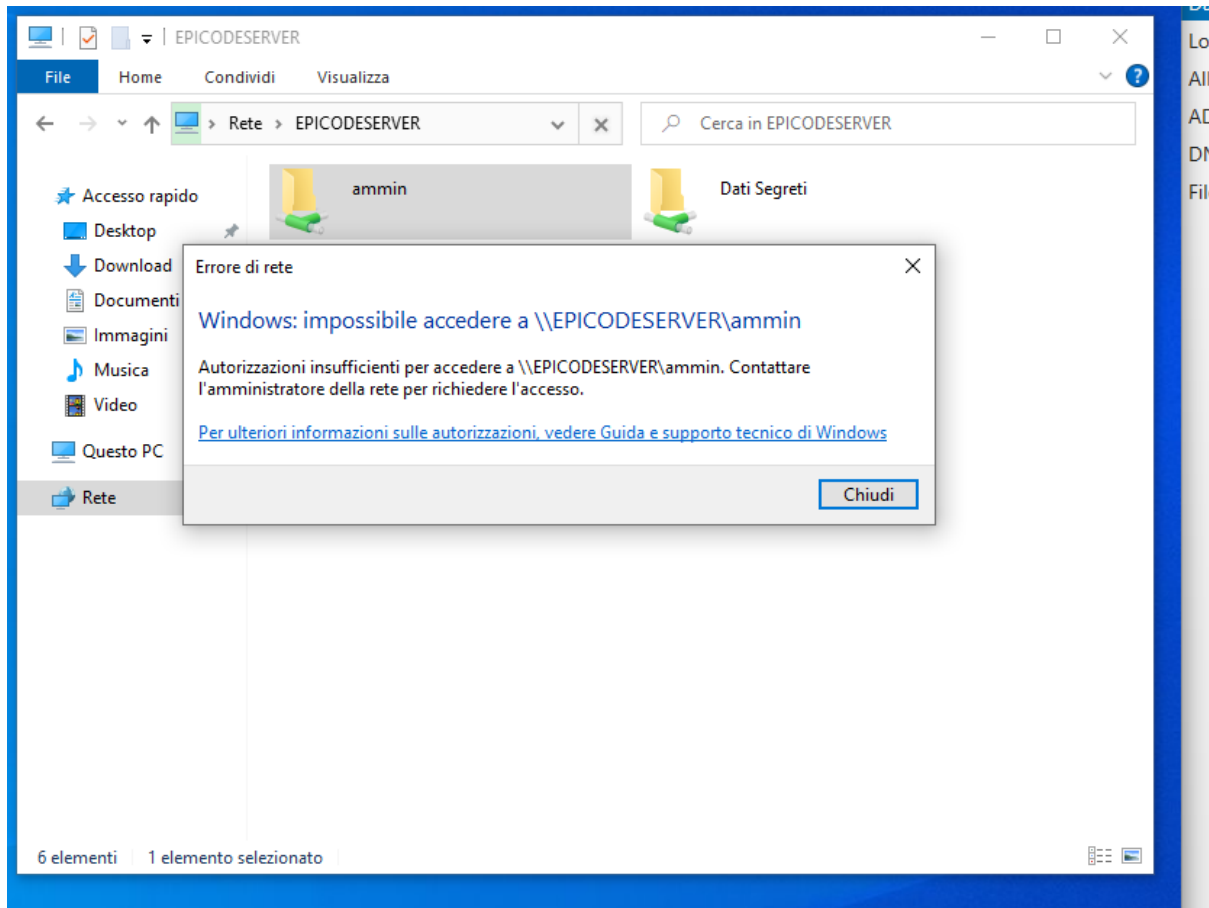
Ma vediamo se riesce ad accedere anche ad altre cartelle.



Giustamente compare errore

Rifacciamo l'accesso con altro utente user3 appartenente al gruppo sviluppatori.





Come prima accede solo alle cartelle a cui gli avevamo dato i permessi

Perché si danno i permessi alle cartelle di rete?

1. Sicurezza

- a. Evita che utenti non autorizzati possano leggere, copiare o modificare file sensibili.
- b. Si possono proteggere dati riservati (esempio: dati finanziari visibili solo al gruppo *Amministrazione*).

2. Controllo degli accessi

- a. Decidere quali gruppi o utenti possono:
 - i. vedere la cartella
 - ii. leggere i file
 - iii. creare nuovi file
 - iv. modificare o cancellare file

3. Facilitare la collaborazione

- a. Permettere solo a chi deve lavorare su determinati file di avere accesso completo, mentre altri possono solo leggere.
- b. Es.: il gruppo *Sviluppatori* può scrivere nella cartella *Progetti*, mentre il gruppo *Marketing* può solo leggerla.

4. Prevenire errori o incidenti

- a. Limitare la possibilità che un utente per sbaglio cancelli o modifichi file importanti.
- b. Dare i permessi minimi necessari per ogni ruolo.

Esempi pratici di permessi comuni

Gruppo/Utenza	Permesso sulla cartella di rete
Amministratori	Controllo completo
Ufficio HR	Lettura + scrittura
Tutti gli utenti	Sola lettura
Utenti esterni	Nessun accesso

Tipi di permessi principali

- **Lettura (Read)** → Può vedere e aprire i file.
- **Scrittura (Write)** → Può creare nuovi file o modificarli.
- **Modifica (Modify)** → Può cambiare o cancellare file.
- **Controllo completo (Full control)** → Può fare tutto, anche cambiare i permessi.

In pratica, dare i permessi alle cartelle di rete permette di garantire che **ogni utente abbia accesso solo ai dati che gli servono** e niente di più fondamentale in ogni rete aziendale o in un ambiente multiutente.