

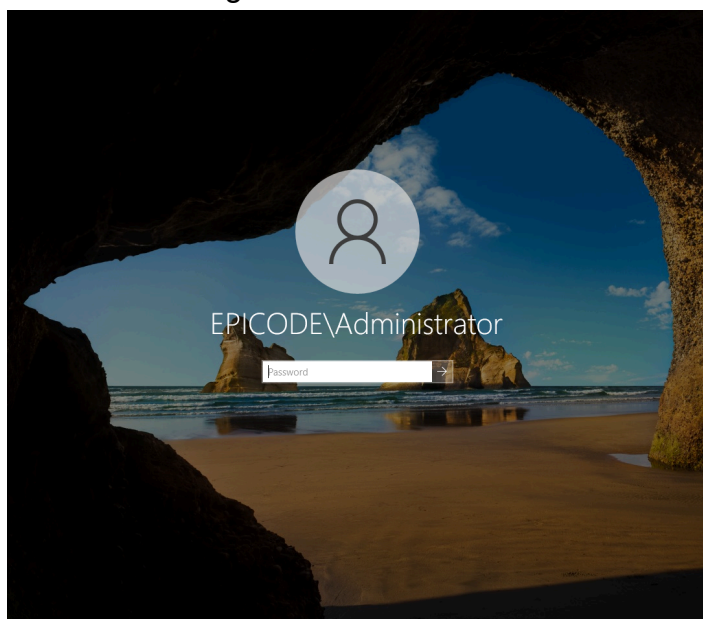
Obiettivo

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.

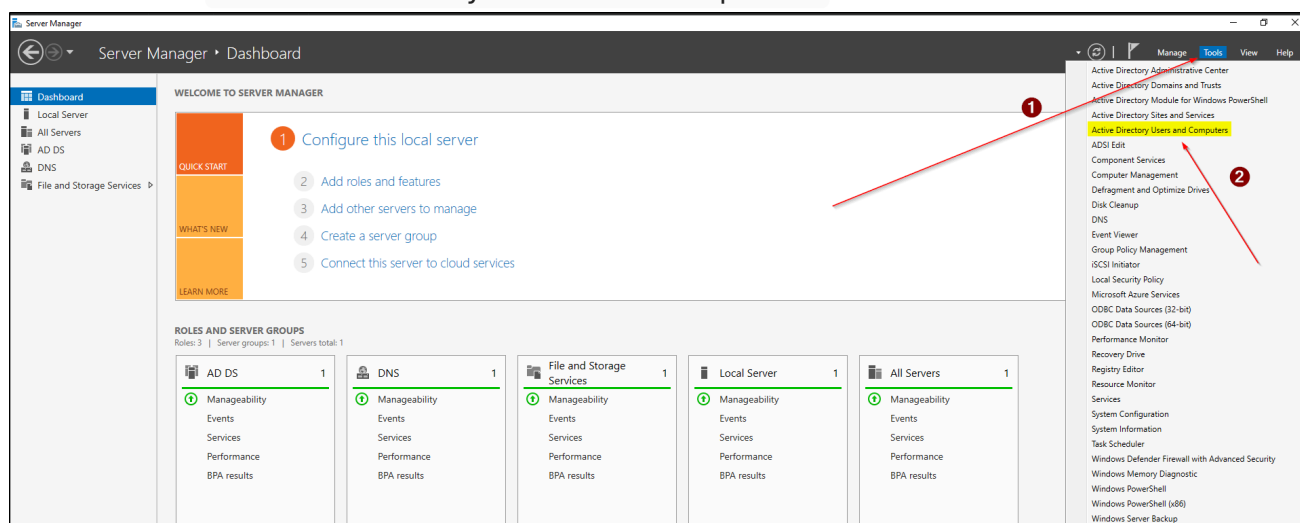
Configurazione : Istruzioni per Domain Controller

1. Il consiglio di Elrond

Effettuiamo il login al Windows Server come Administrator

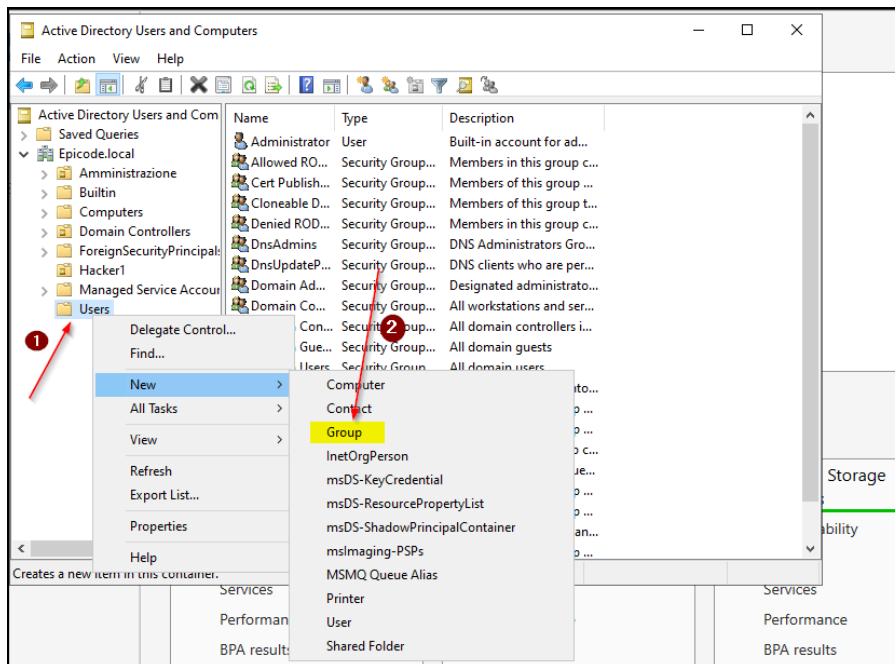


Dalla dashboard di Windows Server Manager andiamo su tools e successivamente selezioniamo Active Directory Users and Computers

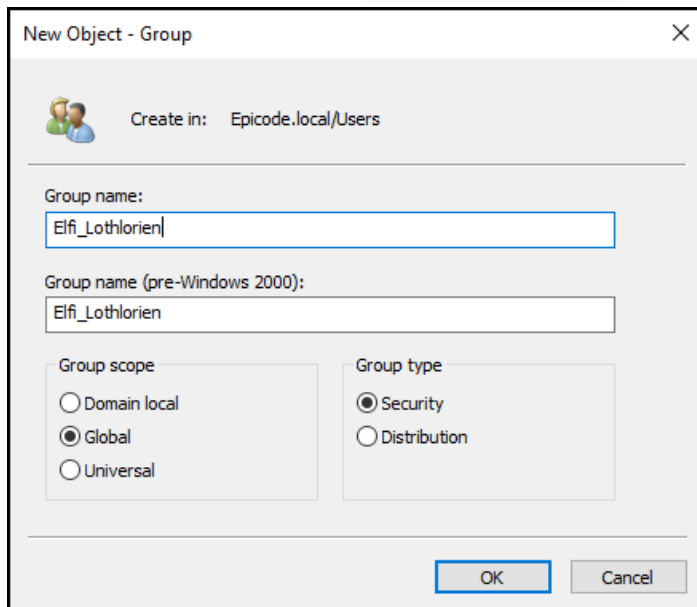


2. Le compagnie (Creazione Gruppi)

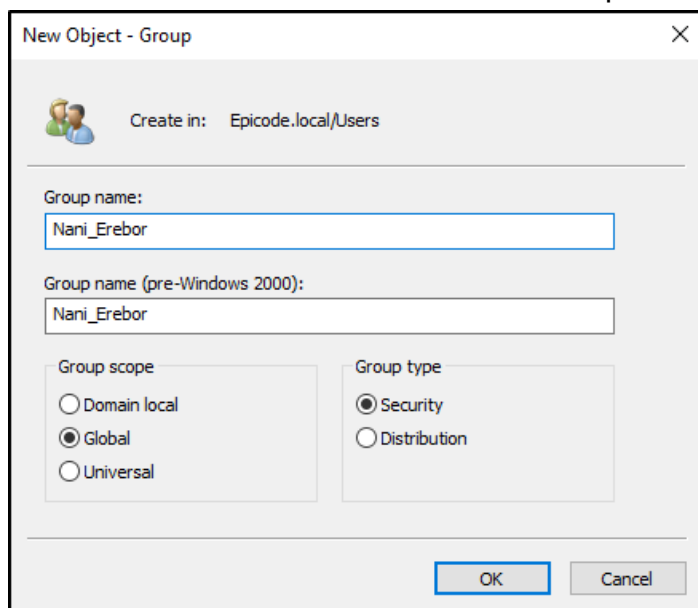
Dal pannello che verrà visualizzato espandiamo il dominio locale `Epicode.local` e andiamo a creare un nuovo gruppo all'interno di `Users`.



Creiamo il primo gruppo `Elfi_Lothlorien` lasciando invariate le altre impostazioni

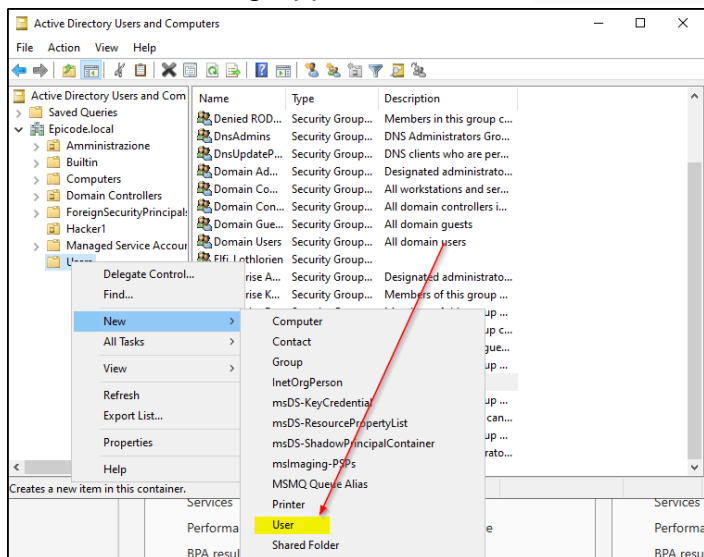


- Eseguiamo gli step precedenti per andare a creare un altro gruppo `Nani_Erebor` continuando a lasciare invariate le altre impostazioni



Gli Eroi (Creazione Utenti)

- Andiamo a creare ora gli utenti , seguiamo gli step precedenti ma invece di andare a creare un nuovo gruppo andiamo su New --> Users



- Creiamo il nostro primo eroe Legolas impostando First name e User login name

A screenshot of the 'New Object - User' dialog box. The 'Create in' field is set to 'Epicode.local/Users'. The 'First name' field contains 'Legolas'. The 'Initials' field is empty. The 'Last name' field is empty. The 'Full name' field contains 'Legolas'. The 'User login name' field contains 'legolas' and the domain dropdown is set to '@Epicode.local'. The 'User login name (pre-Windows 2000)' field contains 'EPICODE\'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

- Impostiamo una password e , soltanto a scopo di test , togliamo la spunta a User must change password at next login

New Object - User

Create in: Epicode.local/Users

Password: [dots]

Confirm password: [dots]

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

- Eseguiamo le operazioni precedenti per andare a creare il secondo utente Gimli

New Object - User

Create in: Epicode.local/Users

First name: Gimli Initials: [empty]

Last name: [empty]

Full name: Gimli

User logon name: gimli @Epicode.local

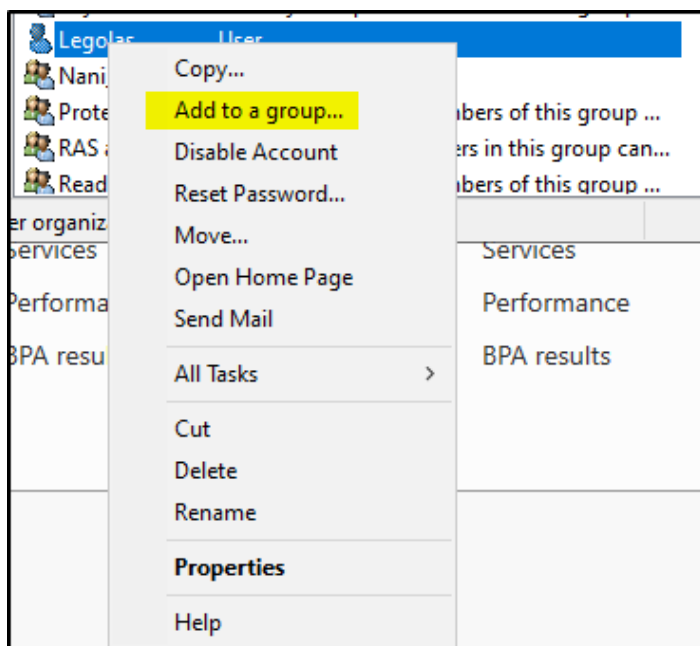
User logon name (pre-Windows 2000): EPICODE\ gimli

< Back Next > Cancel

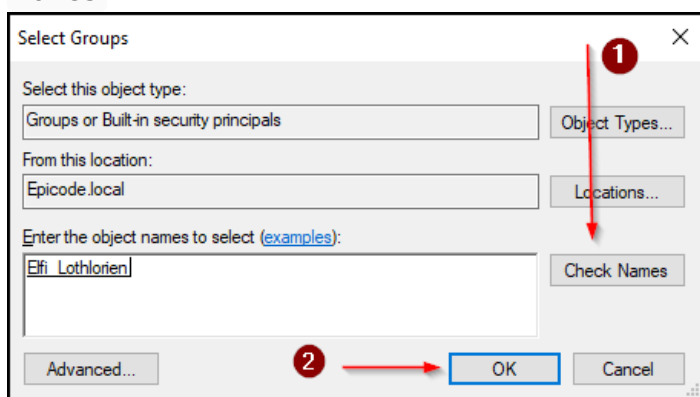
- Adesso che abbiamo i nostri due eroi possiamo passare alla fase di assegnazione

	Gimli	User
	Group Polic...	Security Group... Members in this group c...
	Guest	User Built-in account for gue...
	Key Admins	Security Group... Members of this group ...
	Legolas	User

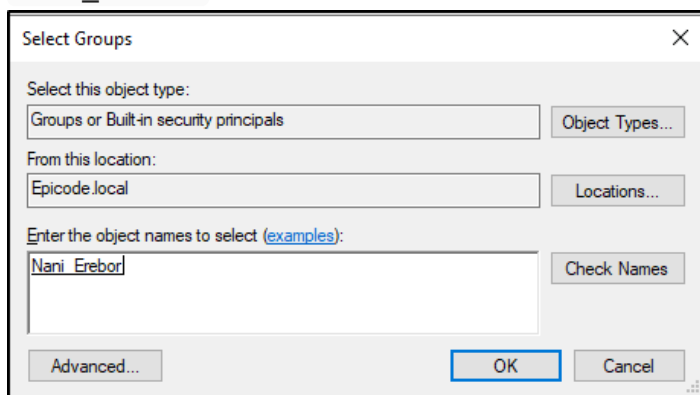
- Una volta individuati i due eroi all'interno dell'elenco , prendiamo ad esempio Legolas
tasto destro --> Add to group



Nella box che si apre scriviamo il nome del gruppo `Elfi` ed effettuiamo un `Check Names`

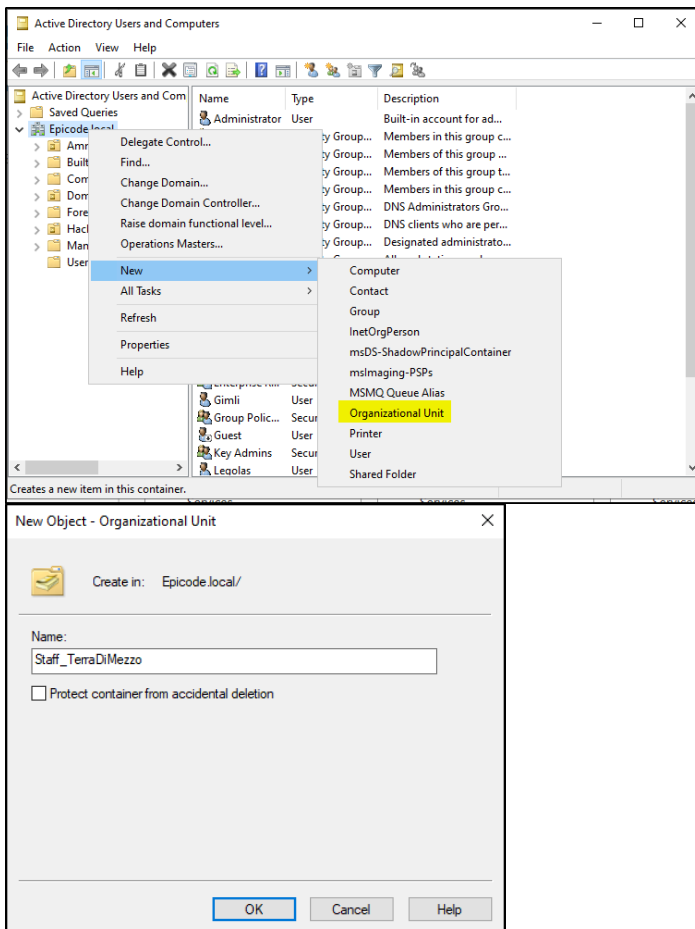


Effettuiamo le stesse operazioni per `Gimli` andando ad inserirlo nel gruppo `Nani_Erebor`

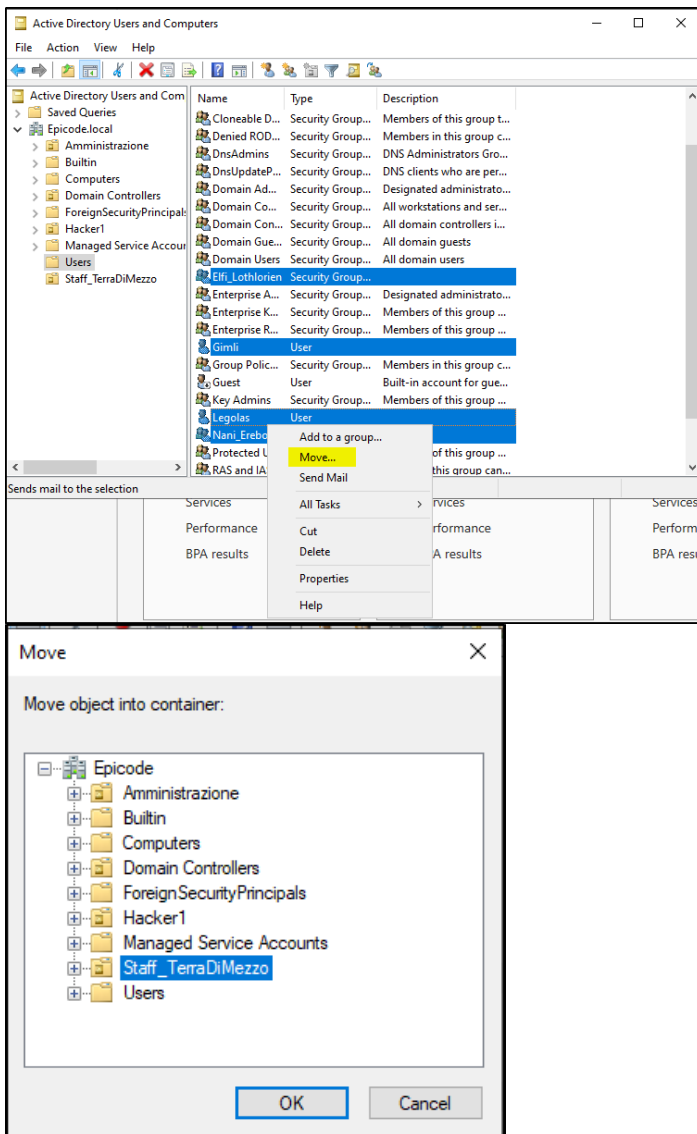


Creazione OU (TerraDiMezzo)

Dalla schermata di `Active Directory Users and Computers`, tasto destro sul nome del dominio(`epicode.local`) e scegliamo `New --> Organizational Unit` (Ci servirà successivamente per creare degli `Shortcut`) chiamandola `Staff_TerraDiMezzo` e togliendo la spunta da `Protect container from accidental deletion` (per ora ci semplifica la vita se dobbiamo cancellarla).



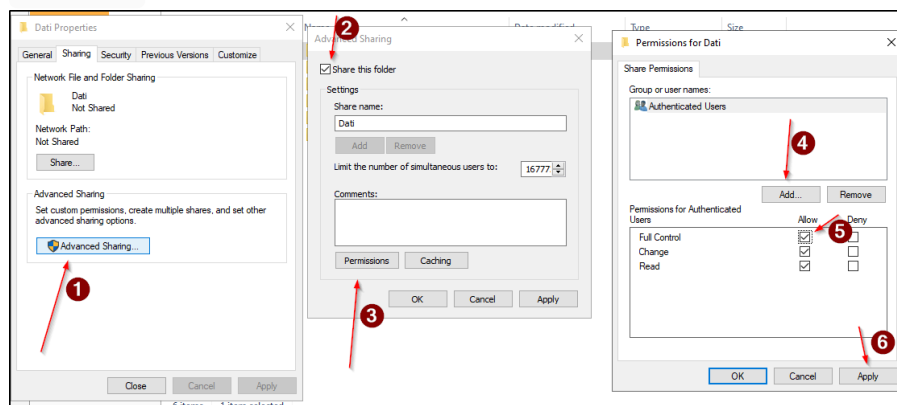
Ora non ci resta altro che selezionare Utenti e Gruppi e inserirli nella OU appena creata tramite il comando Move e la selezione *di Staff_TerraDiMezzo*



3. I confini del Regno (Assegnazione permessi)

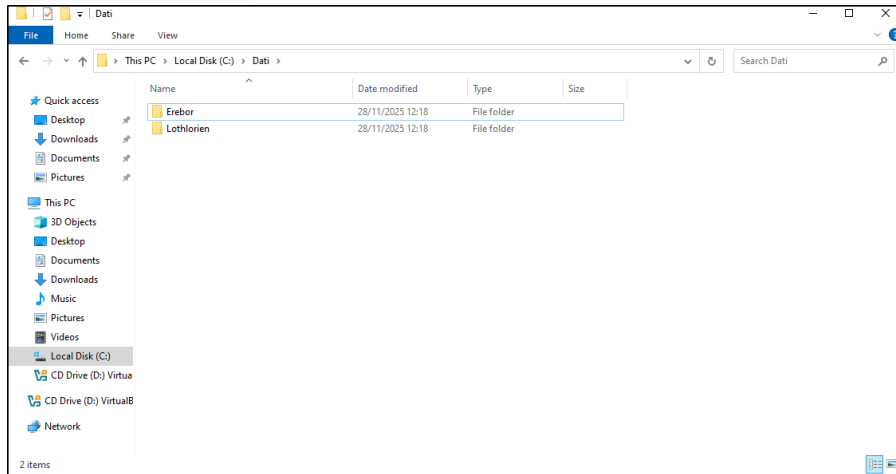
1. Creiamo una cartella dati all'interno del Disco C :

- andiamo sulle properties della cartella, nella scheda di sharing e successivamente su Advanced Settings
- Mettiamo la spunta su Share Folder
- Clicchiamo su Permissions , che di default presenta Everyone , selezioniamolo e rimuoviamolo poichè costituisce una bad practice.
- Andiamo su Add e inseriamo Authenticated Users e spuntiamo la casella Full Control



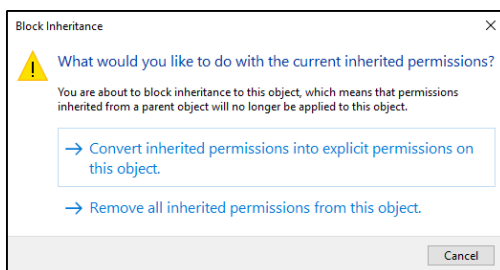
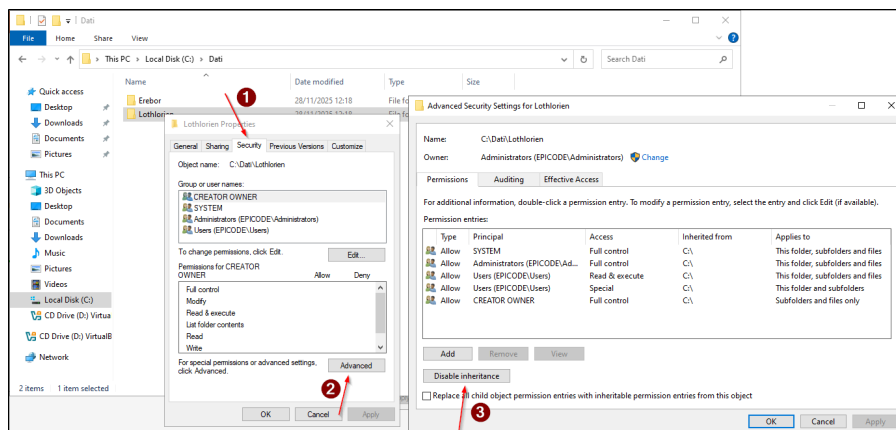
- *Perché "Full Control"?* Stiamo dicendo al "buttafuori" di far passare chiunque sia autenticato nel dominio, fidandoci che poi le "guardie interne" (NTFS) faranno il loro lavoro bloccando legolas da Erebor e gimli da Lothlorien.

2. Andiamo a creare 2 cartelle all'interno del nostro disco C:\Dati\Lothlorien e C:\Dati\Erebor

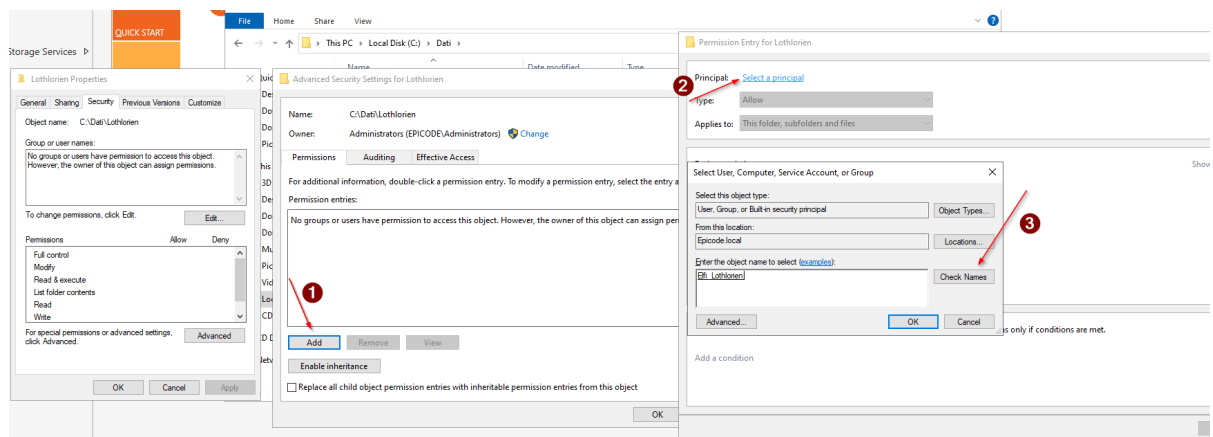


3. Procediamo alla configurazione dei permessi di C:\Dati\Lothlorien

- Click destro sulla cartella --> Properties --> Security --> Advanced e clicchiamo su Disable Inheritance --> Remove all inherited permissions from this object in modo da andare a rimuovere tutti i permessi pre-impostati nella creazione delle cartelle.

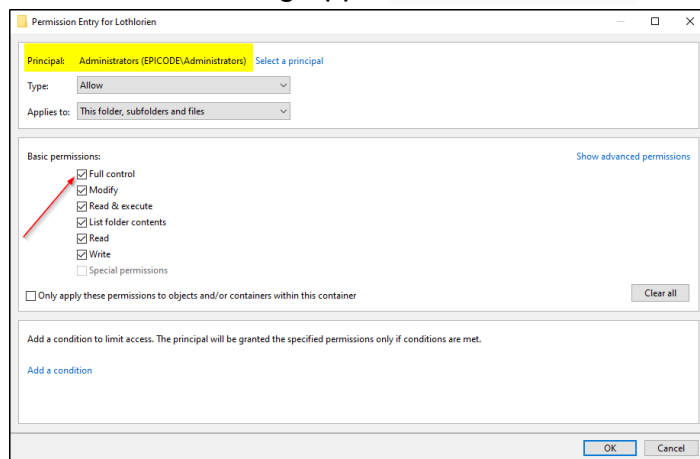


- Andiamo su Add --> Select a Principal --> Come prima inseriamo il nome del gruppo e poi effettuiamo un Check Names dopo aver inserito Elfi

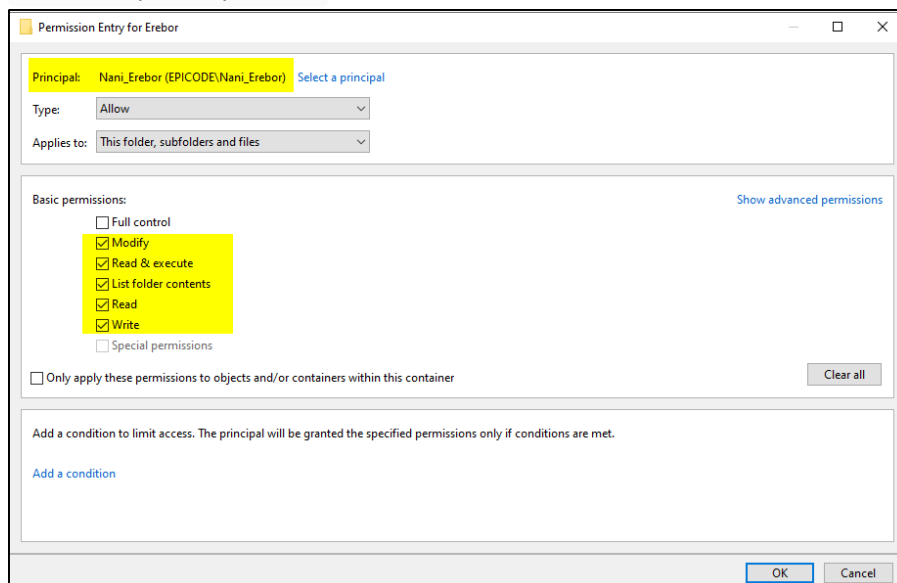


Diamo i permessi di Read & Execute , List Folder contents , Read e salviamo le impostazioni.

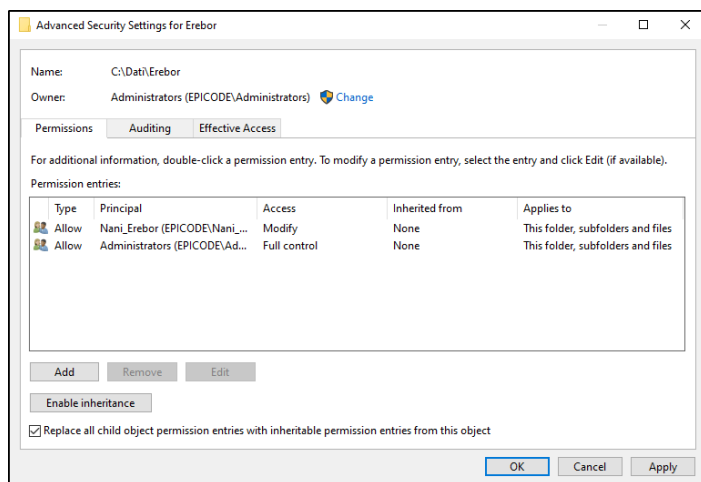
Inseriamo inoltre il gruppo Administrators con Full Control.



4. Effettuiamo, allo stesso modo , le configurazioni per C:\Dati\Erebor questa volta però inseriamo Nani_Erebor e assegniamo i permessi di Modify, Read & Execute, Read, Write



- Anche qui inseriamo Administrators con Full Control ottenendo la seguente configurazione finale per i permessi.

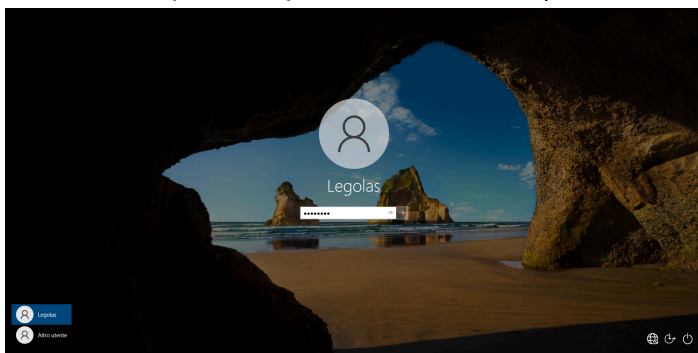


Il test di Frodo (Verifica dei permessi)

Permessi NTFS

I permessi NTFS che abbiamo impostato prima su `Lothlorien` e `Erebor` sono ancora validi e sono la nostra vera linea di difesa.

- `C:\Dati\Lothlorien` -> `Elfi_Lothlorien` (Read), Domain Admins (Full).
 - `C:\Dati\Erebor` -> `Nani_Erebor` (Modify), Domain Admins (Full).
1. Effettuiamo l'accesso ora al nostro client con `Legolas` (con la password che abbiamo impostato precedentemente)



2. Dopo l'inizializzazione dell'account andiamo su `Esplora File` e successivamente su `Rete`
3. Nella barra degli indirizzi digitiamo il percorso **UNC** (Universal Naming Convention) del nostro server e della condivisione `\\EPICODESERVER\Dati` per andare a visualizzare le nostre due cartelle.

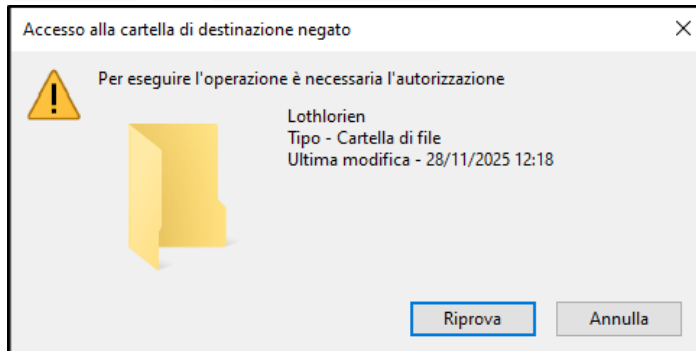


4. **Test per Legolas :**

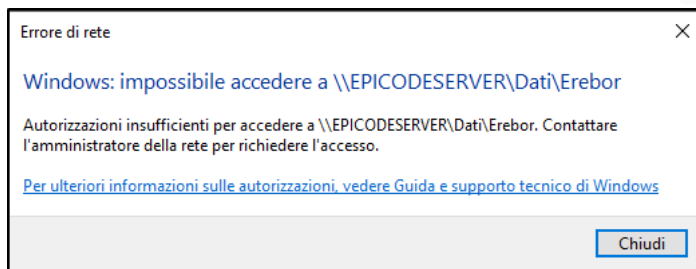
- Proviamo ad effettuare l'accesso a Lothlorien con SUCCESSO



- Provando invece a creare un file di testo all'interno della cartella otteniamo un FALLITO per Access Denied

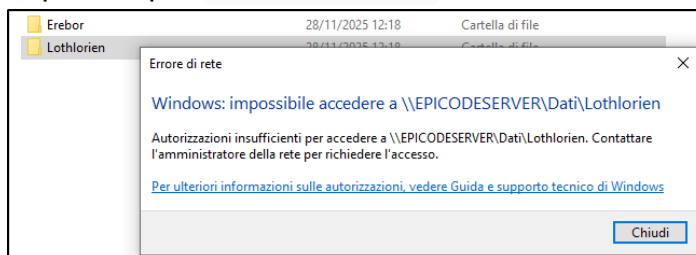


- Provando a entrare in Erebor otteniamo un altro FALLITO con Access Denied

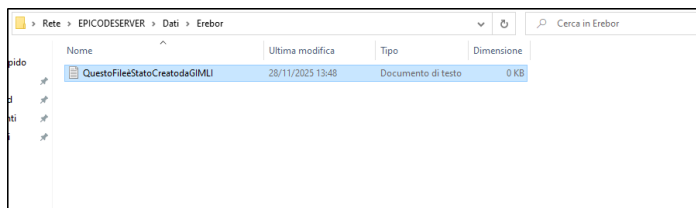


5. Test per Gimli

- Andiamo ad effettuare il login con Gimli e torniamo nel path \\EPICODESERVER\\Dati
- Proviamo ad effettuare l'accesso alla cartella Lothlorien con un fallimento aspettato per Access Denied



- Proviamo ora ad entrare e creare un file in Erebor con SUCCESSO

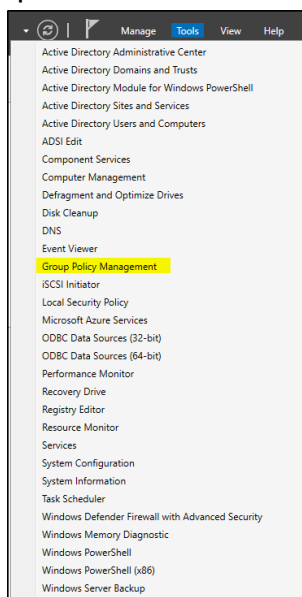


Il Decreto Reale (Group Policy Managment)

Il Group Policy Management serve a creare e gestire cartelle in modo centralizzato e automatico per gli utenti** in un ambiente di rete, utilizzando le *Group Policy Preferences (GPP)*. Invece di creare manualmente le cartelle su ogni computer, è possibile usare la console GPMC per:

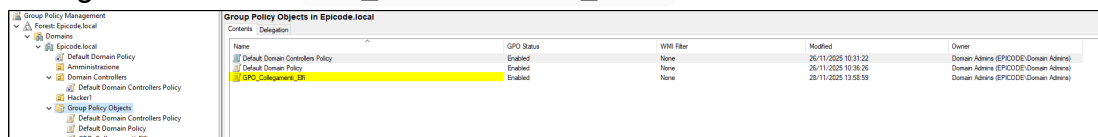
- **Creare cartelle:** Definire la creazione di una cartella specifica (es. "Documenti Condivisi") su tutti i computer client o per determinati utenti.
- **Configurare percorsi:** Stabilire percorsi di rete per le cartelle o rimappare le unità disco, rendendo più facile l'accesso alle risorse condivise.
- **Reindirizzare cartelle utente:** Spostare cartelle come "Documenti" su una posizione di rete centralizzata, semplificando il backup e l'accesso ai file da qualsiasi postazione.
- **Garantire coerenza:** Assicurare che tutti gli utenti abbiano le stesse cartelle con le configurazioni corrette, migliorando la produttività e riducendo gli errori.
- **Automatizzare le attività:** Eseguire l'operazione di creazione o reindirizzamento delle cartelle in automatico, senza bisogno di interventi manuali su ogni singolo PC

1. Andiamo sulla schermata del nostro server e torniamo nella sezione Tools andando questa volta su **Group Policy Management**



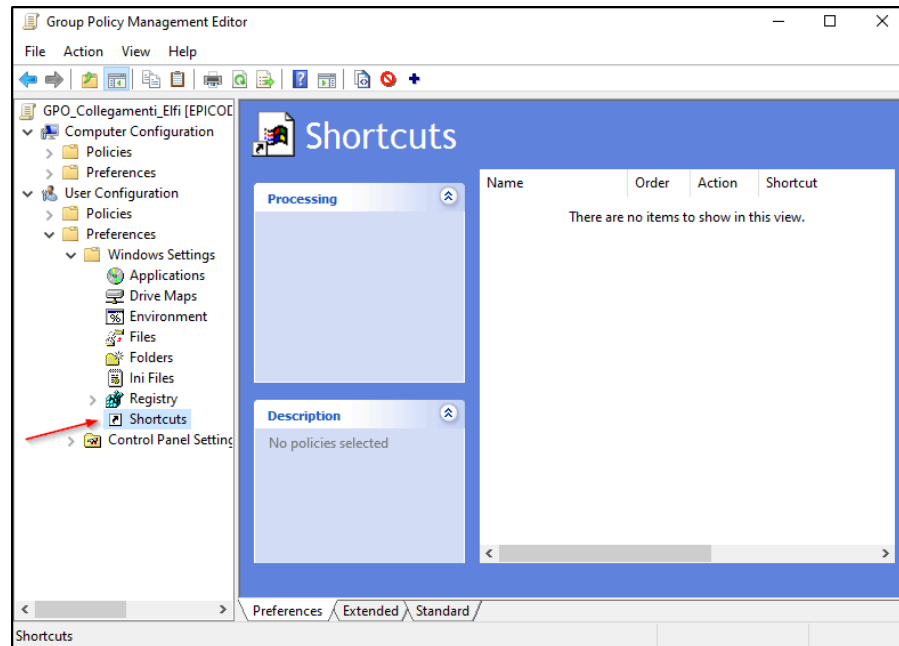
2. Andiamo ora a creare il decreto (**La pergamena**)

- Dal container **Group Policy Objects** , tasto destro e selezioniamo New , assegniamo il nome **GPO_Collegamenti_Elfi** e confermiamo.

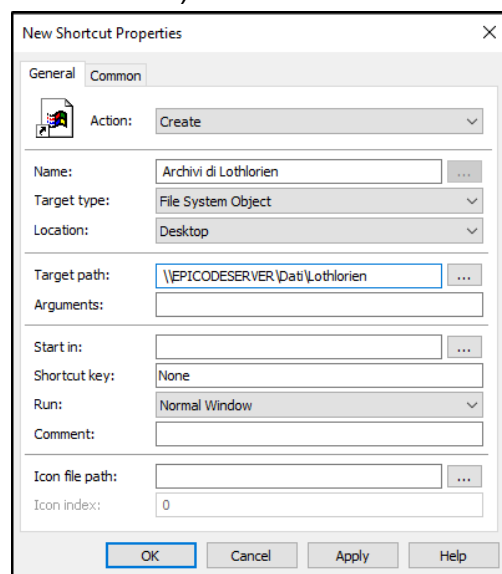


- Modifichiamo il nostro Object appena creato per fare in modo che sia assegnato a **Legolas** come da evidenza andiamo su **Shortcuts** e ne creiamo uno nuovo per il

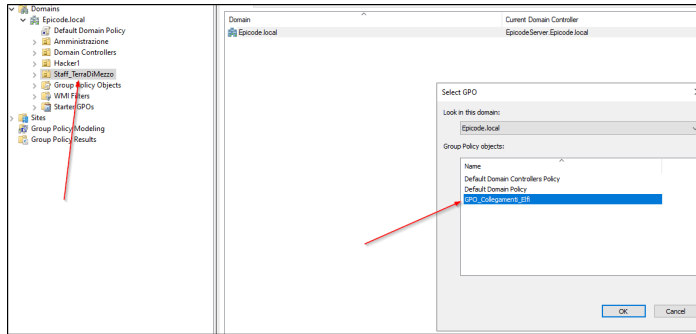
nostro utente.



- Impostiamo lo shortcut così :
 - **Action:** Create (Crea)
 - **Name:** Archivi di Lothlórien (Questo è il testo che Legolas vedrà sul desktop).
 - **Target type:** File System Object
 - **Location:** Desktop
 - **Target path:** \\EPICODESERVER\Dati\Lothlorien (Questo è il percorso di rete UNC).

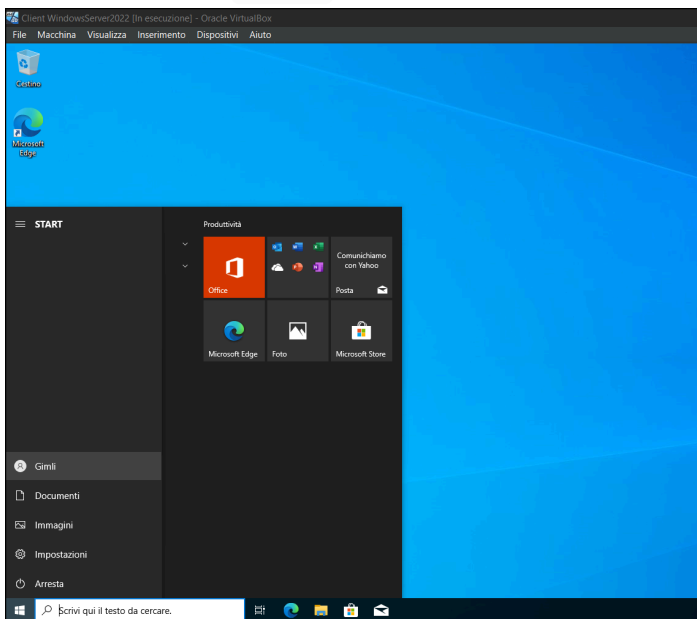


- Non ci resta ora che assegnare la GPO all'OU esistente

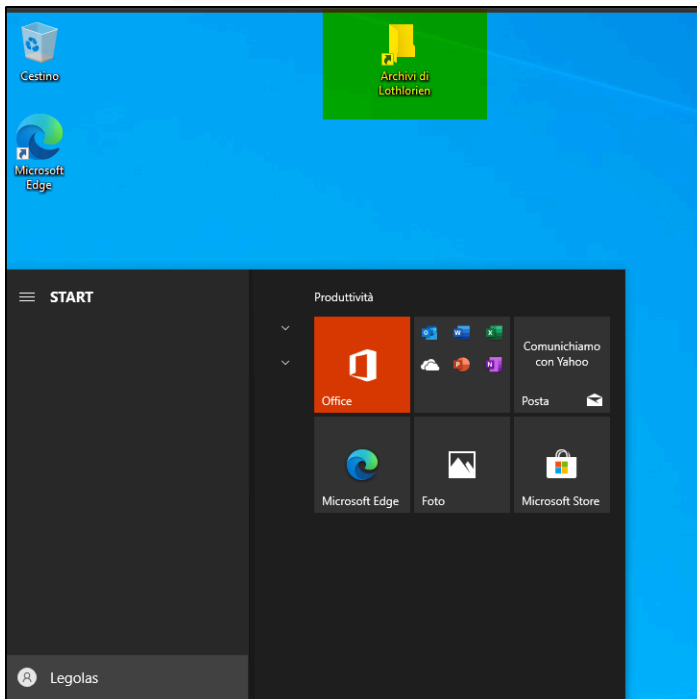


Il *Security Filtering* che abbiamo impostato (quello che dice "solo per Elfi_Lothlorien") funzionerà ancora perfettamente. La policy si applicherà a tutta l'OU, ma il filtro la attiverà solo per i membri del gruppo Elfi.

Andiamo ora a controllare se la nostra GPO è impostata correttamente. Effettuiamo l'accesso come Gimli e notiamo subito come non sia presente alcuno shortcut



Mentre per Legolas vediamo subito lo shortcut appena creato come da evidenza.



Conclusione

Questo esercizio ha unito i tre pilastri della gestione Windows: **Identità** (Active Directory), **Sicurezza** (permessi NTFS) e **Automazione** (Group Policy). Abbiamo applicato il Principio del Minimo Privilegio (PoLP) in modo granulare e abbiamo visto come, centralizzando la gestione, si possa orchestrare l'intero ambiente di un utente. Siamo passati dal "lavoro manuale" a una gestione strategica: ora 100 nuovi elfi possono essere resi operativi con lo stesso sforzo di uno solo.