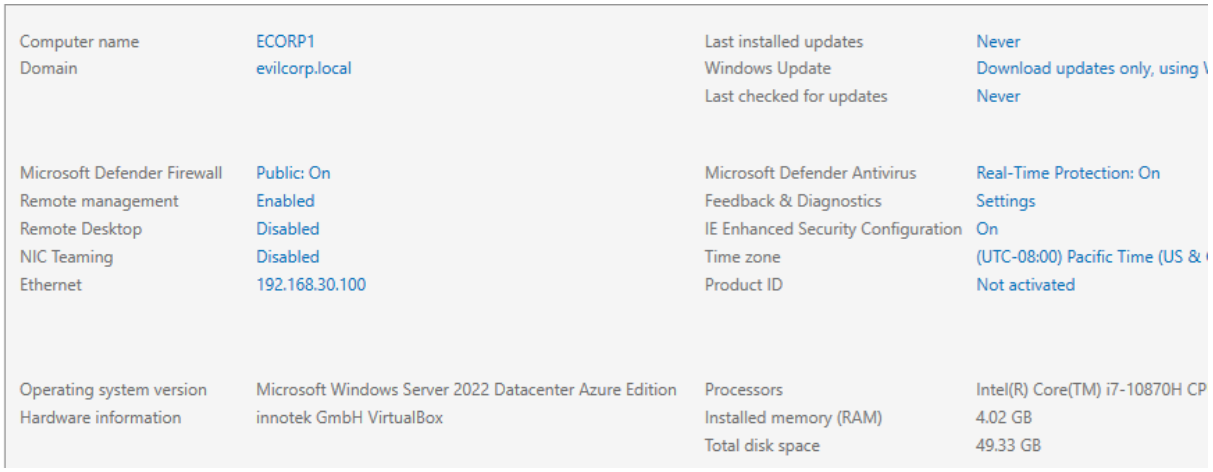
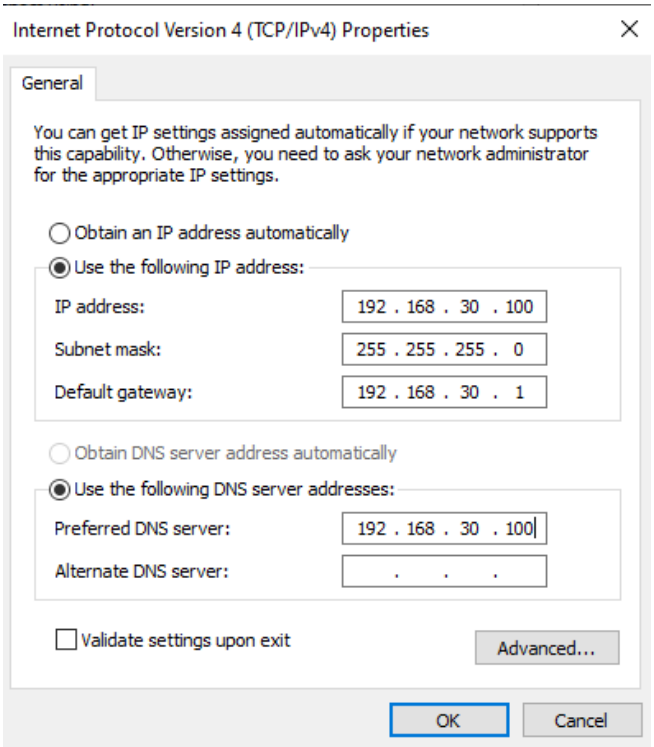
Creazione di gruppi in Windows Server 2022

L'esercizio di oggi consiste nella creazione di gruppi di utenti in Windows Server 2022.

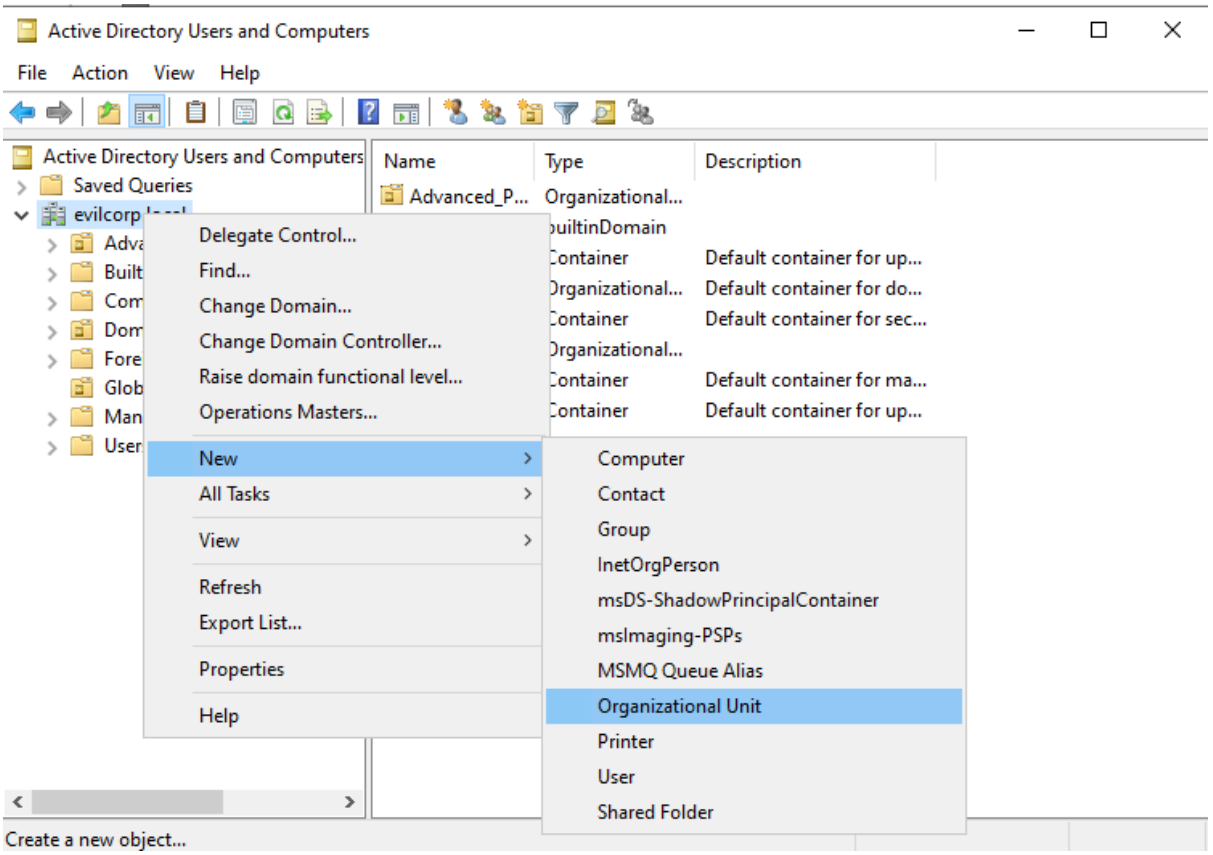
1. **Fase 1: Preparazione**
   Per prima cosa creiamo il server e mettiamo tutte le impostazioni necessarie.



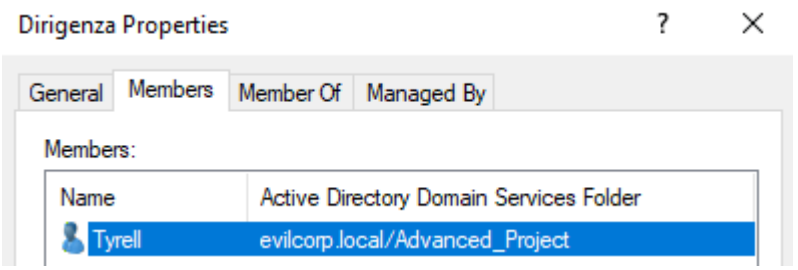
   Ho impostato il nome del computer con **ECORP1** e il dominio con **evilcorp.local** (stile Mr. Robot) e ho impostato l'indirizzo IP della macchina a 192.168.30.100.



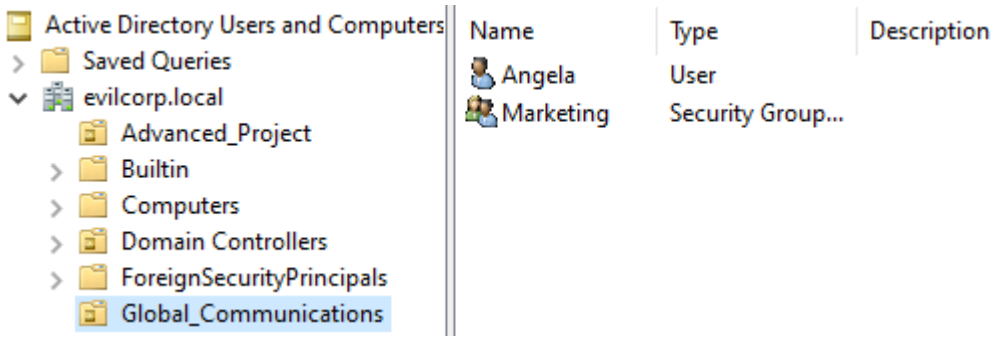
2. **Creazione dei gruppi**
   Successivamente sono passato alla creazione dei gruppi usando il tool **Active Directory Users and Computers**

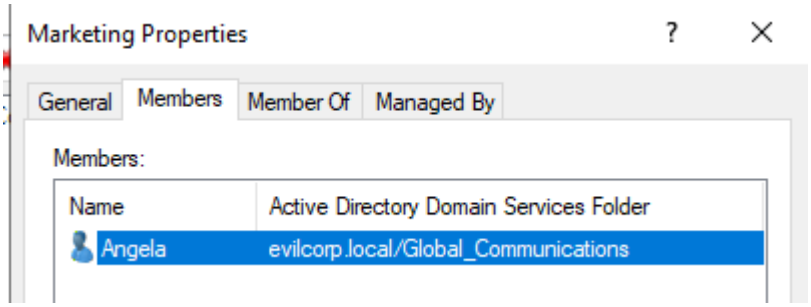


Seguendo l'immagine qui sopra, ho prima creato delle Organizational unit, che ho chiamato **Advanced_Project** per l'amministrazione, e **Global_Communications** per il marketing. All'interno di queste unità vanno creati i gruppi ai quali andranno poi aggiunti i vari permessi.
All'interno di Advanced_Project ho aggiunto il gruppo **Dirigenza** e successivamente ho aggiunto al gruppo l'utente Tyrell.

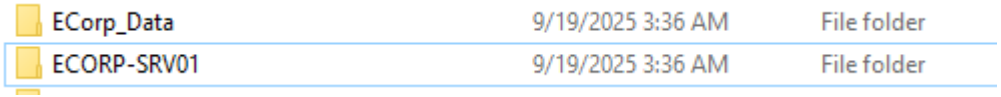


All’interno dell’unità Global_Communications ho creato il gruppo **Marketing** e ho aggiunto a quest’ultimo l’utente Angela.





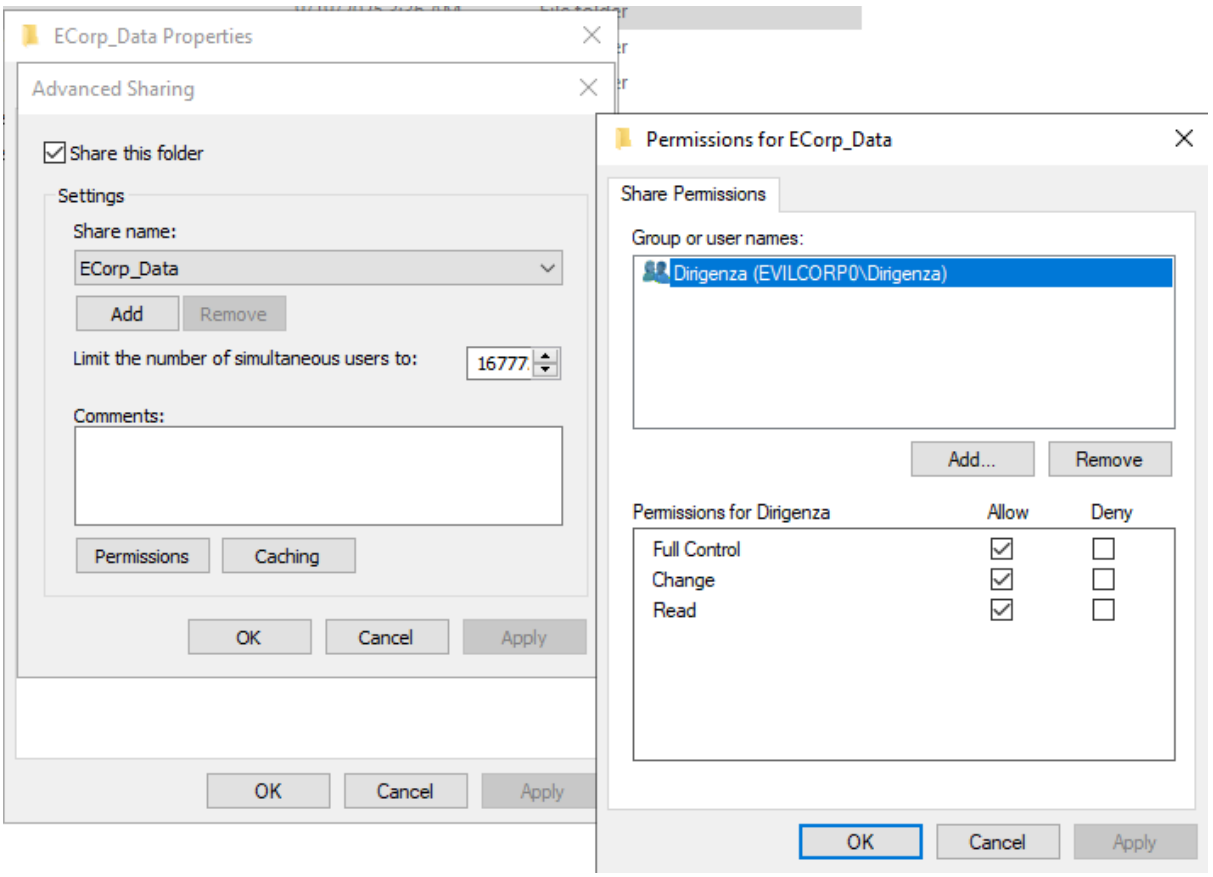
3. **Creazione File e Assegnazione permessi**
   In seguito ho creato due cartelle nel file system del Windows Server, in modo da poter stabilire i permessi dei gruppi



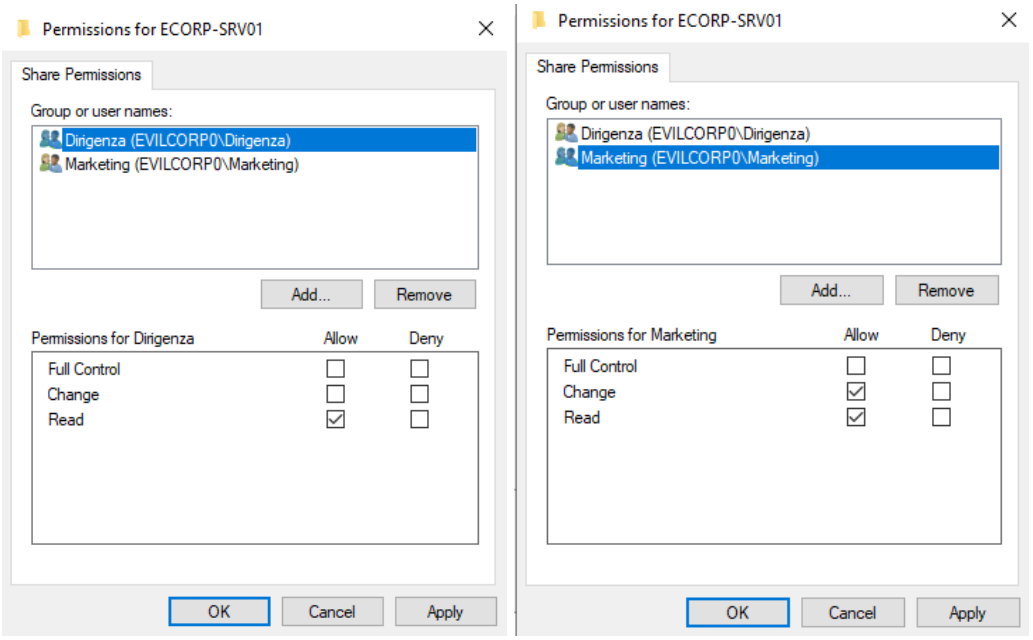
ECorp_Data è la cartella su cui il gruppo Dirigenza avrà il pieno controllo. Per impostare ciò dobbiamo entrare nelle proprietà della cartella

Una volta entrati nelle proprietà della cartella seguiamo questi passaggi:

1. Selezioniamo **Sharing**
2. Da sharing selezioniamo **Advanced Sharing**
3. In Advance Sharing selezioniamo **Permissions**
4. Rimuoviamo il gruppo Everyone e aggiungiamo il gruppo che ci interessa, in questo caso Dirigenza
5. Andiamo a impostare il **Full Control**

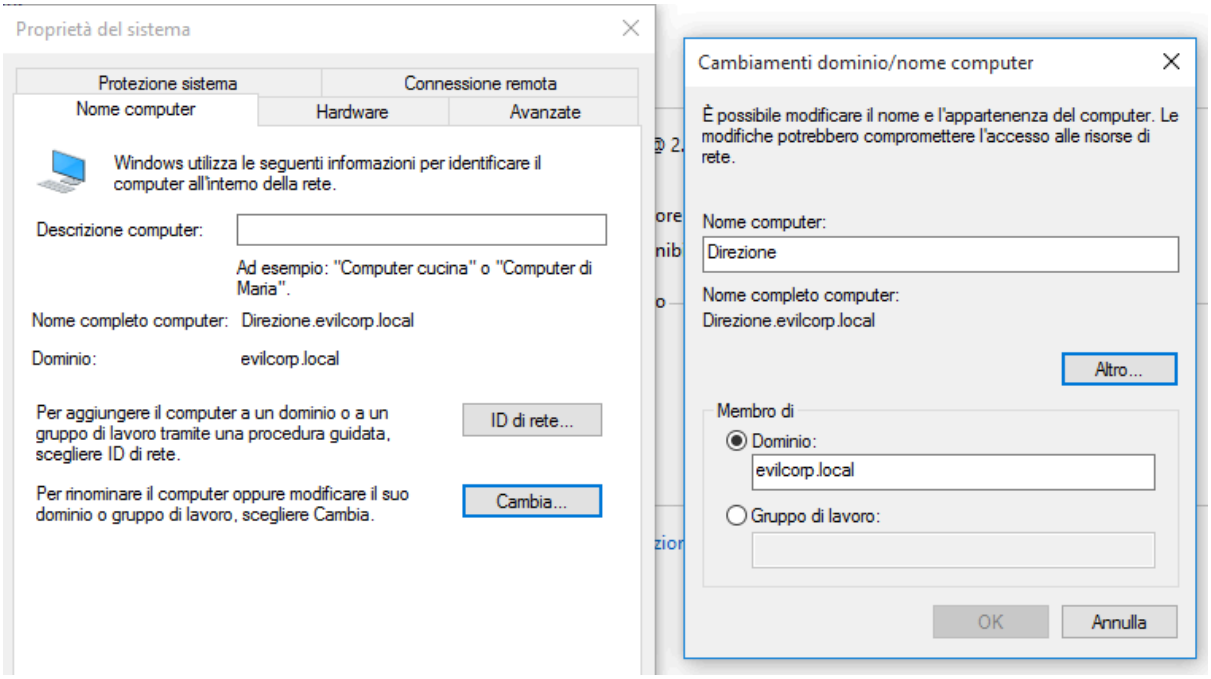


Seguendo questi passaggi abbiamo dato il pieno controllo della cartella ECorp_Data alla Dirigenza.
Seguiamo gli stessi passaggi per la cartella ECORP-SRV01 impostando come permessi solamente quello di lettura e scrittura, e aggiungendo il permesso di sola lettura al gruppo dirigenza.

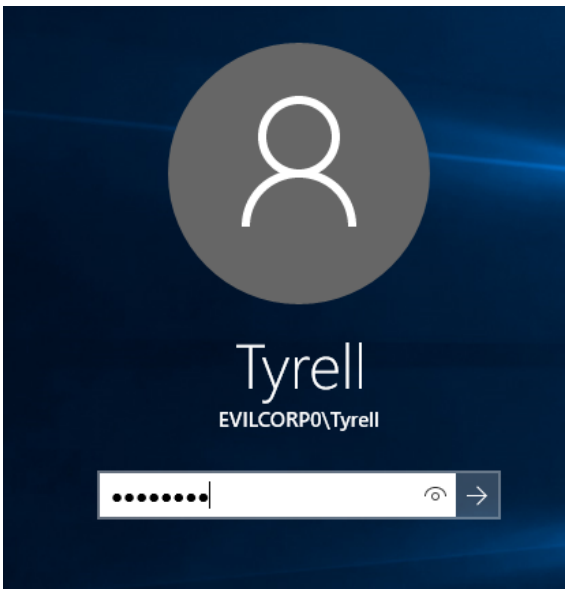


Ho configurato le autorizzazioni in modo che la cartella "ECorp_Data" sia accessibile esclusivamente ai membri del gruppo Dirigenza. Per la cartella "ECORP-SRV01", i membri del gruppo Marketing possono creare e modificare file al suo interno, ma non possono alterare le proprietà della cartella stessa. Il gruppo Dirigenza, invece, ha solo permessi di lettura per la cartella Marketing.
L'accesso in sola lettura permette alla dirigenza di rimanere aggiornata sulle strategie, le campagne e i risultati del marketing senza interferire con il flusso di lavoro del team dedicato.

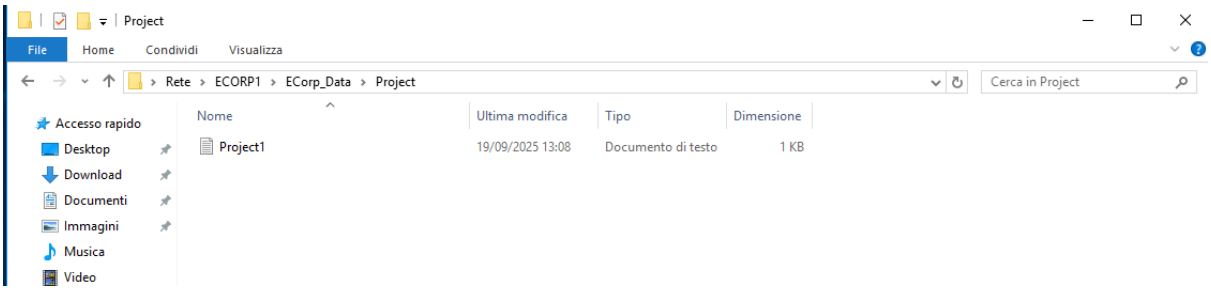
4. **Verifica**
   Per verificare il funzionamento dei permessi che ho impostato, mi sposto su una macchina Windows 10 pro, che ho configurato in modo che sia collegata al Windows Server,ho quindi cambiato il nome del computer e ho aggiunto il dominio evilcorp.local, in modo che sia collegato, ho impostato l'indirizzo IP a 192.168.30.120 e come DNS ho impostato l'IP del Windows Server 192.168.30.100.



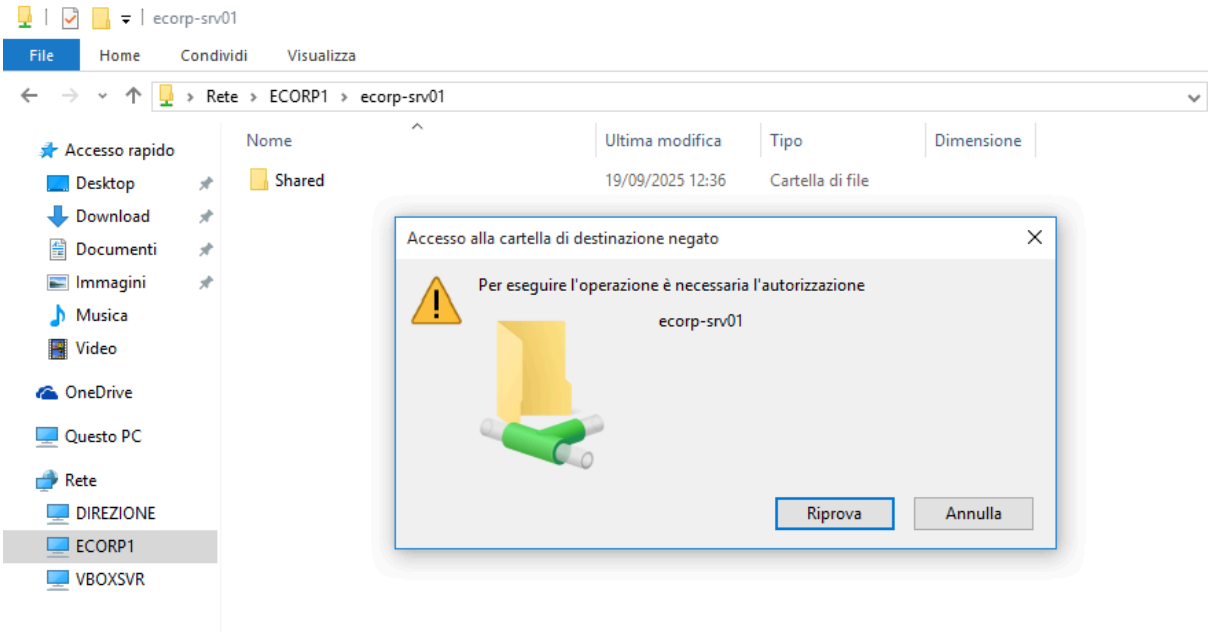
In seguito ho effettuato l'accesso con l'account Tyrell



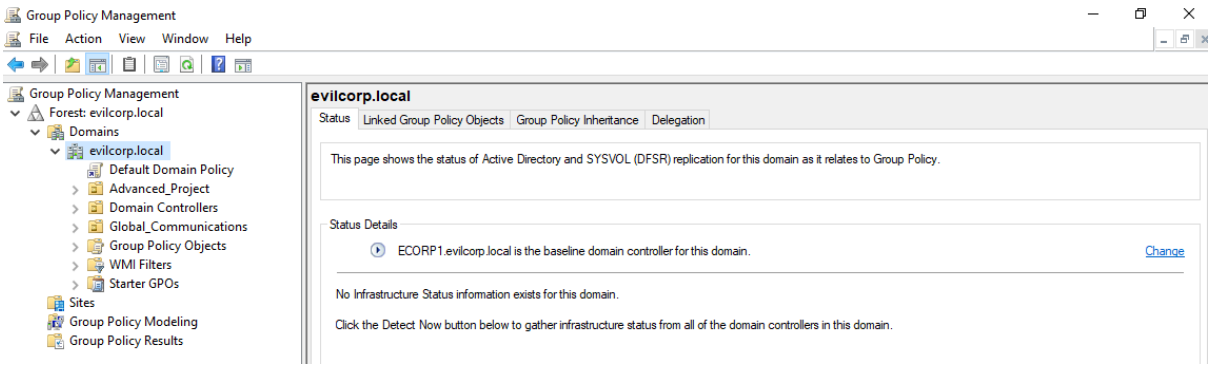
Una volta eseguito l'accesso, sono entrato nel file explorer, ho digitato il percorso della cartella ECorp_Data e posso modificare, aggiungere e rimuovere file.



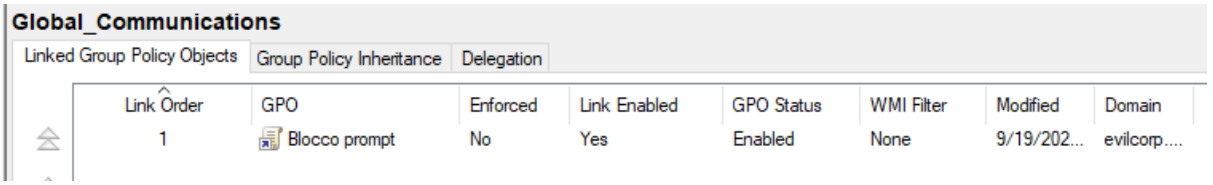
Se invece mi metto nella cartella ECORP-SRV01 posso solamente vedere i file all'interno e non potrò modificare o aggiungere nulla



5. **Utilizzo GPO per bloccare il prompt dei comandi**
   Un'altra cosa che è necessario aggiungere è impossibilitare gli utenti del gruppo marketing nel poter utilizzare il prompt dei comandi. Per fare ciò seleziono da Tools il **Group Policy Management.**

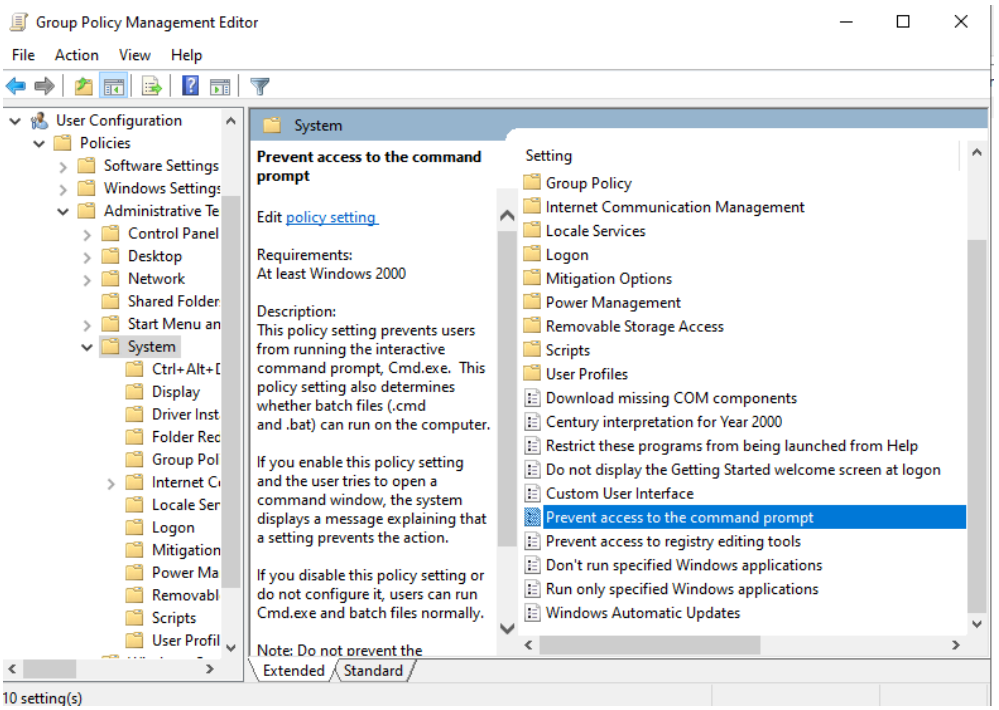


Con il tasto destro clicco su Global_Communications e seleziono "**Create a GPO in this domain, and Link it here...**" e le assegno il nome Blocco Prompt:

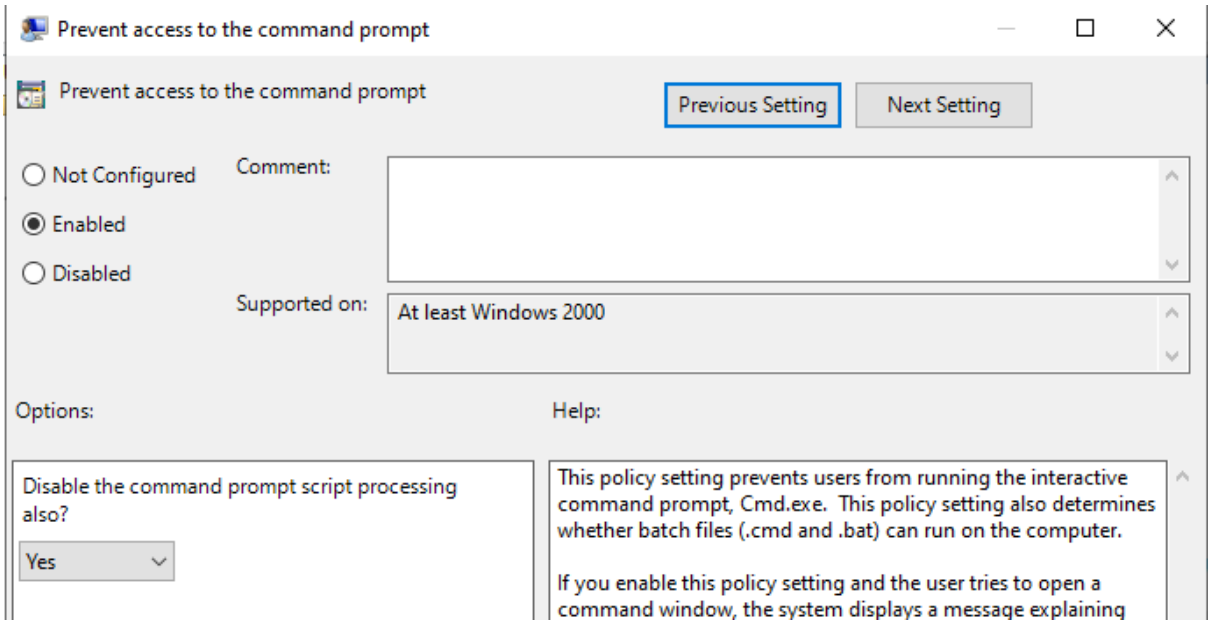


Ora clicchiamo con il tasto destro sulla policy appena creata e selezioniamo **edit,** si aprirà l'editor.
Successivamente navighiamo nel seguente percorso.

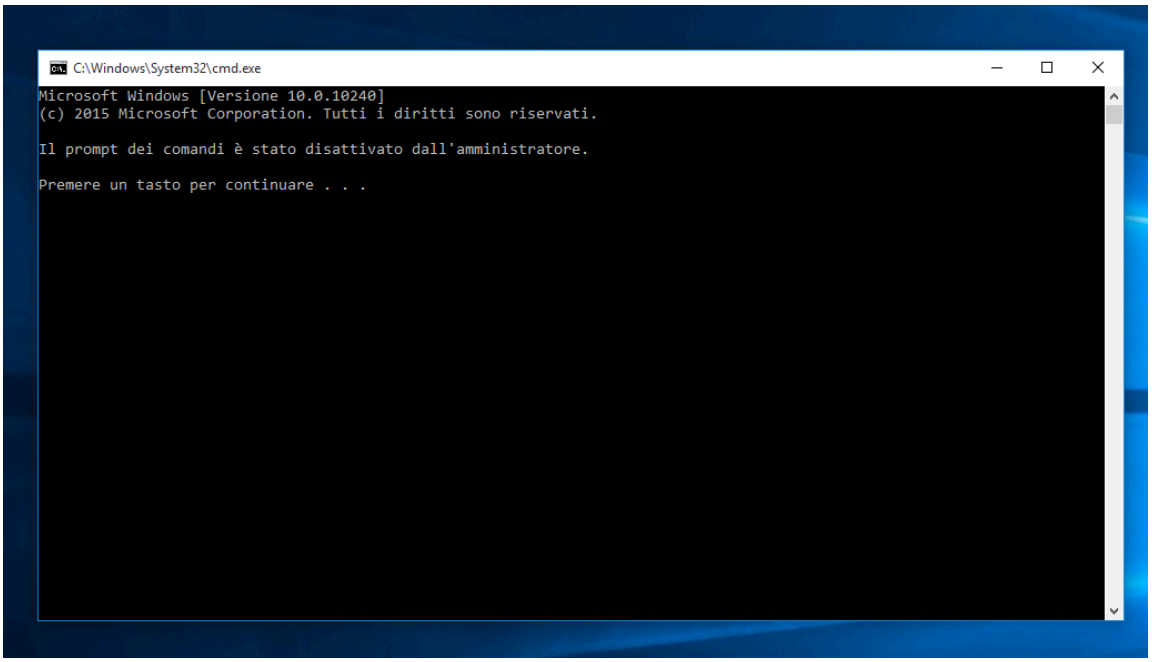
`User Configuration > Policies > Administrative Templates > System`



Una volta trovata la policy giusta la selezioniamo cliccando due volte e la abilitiamo.

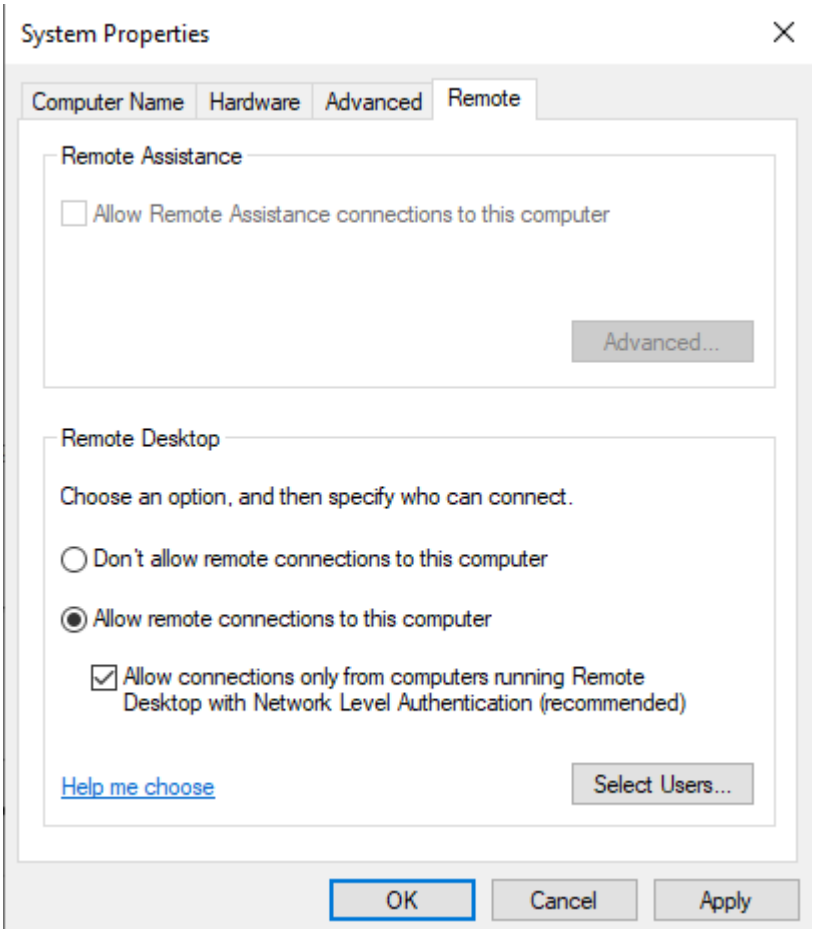


- **Verifica**

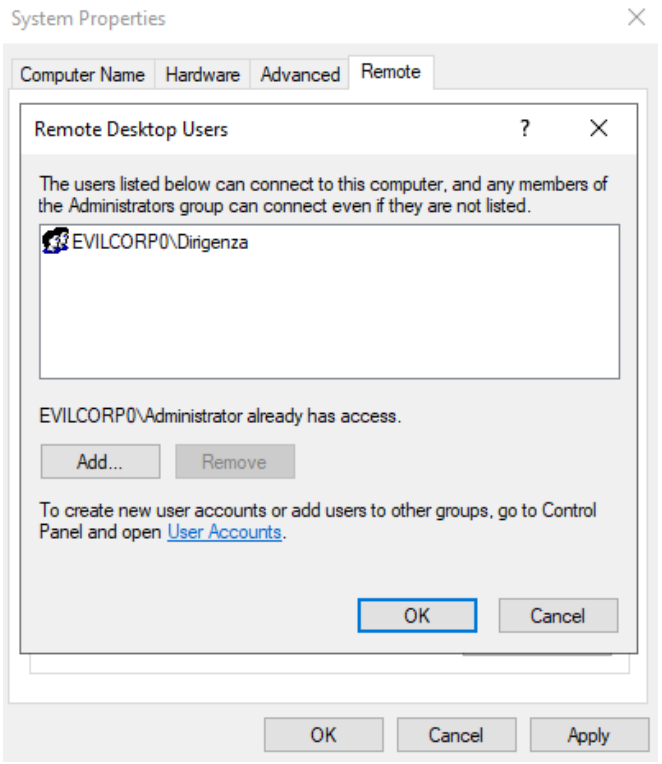


Il prompt è stato correttamente disabilitato.

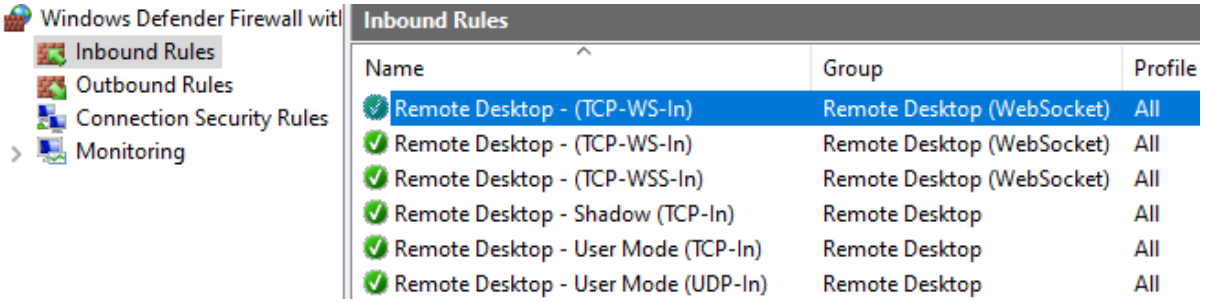
6. **Abilitazione accesso remoto**
   Ora passiamo all'abilitazione dell'accesso remoto al server che ho impostato solamente per il gruppo Dirigenza.



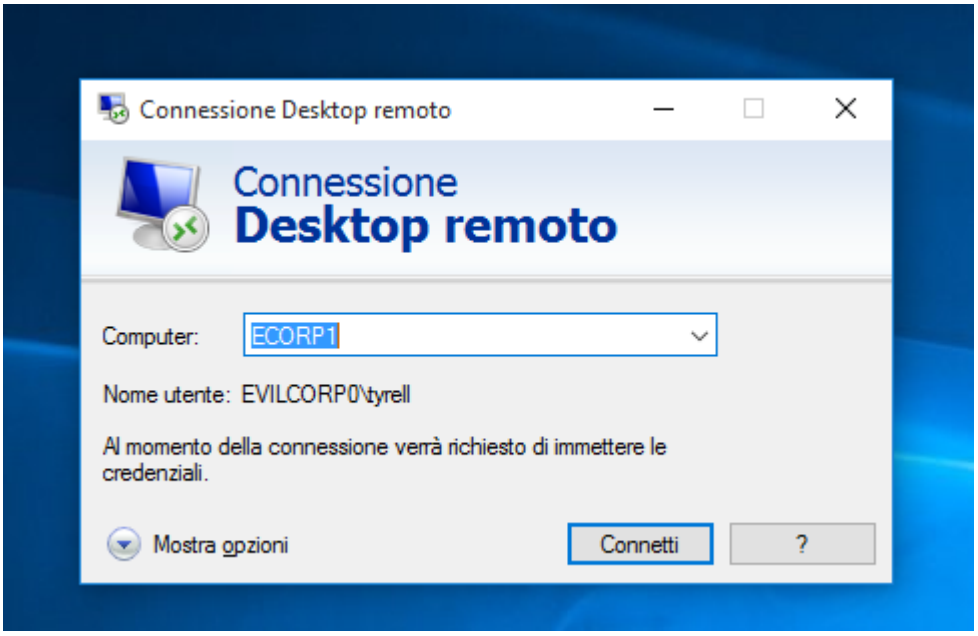
Selezioniamo **Allow remote connections to this computer** e successivamente selezioniamo **Select Users…** e aggiungiamo Dirigenza



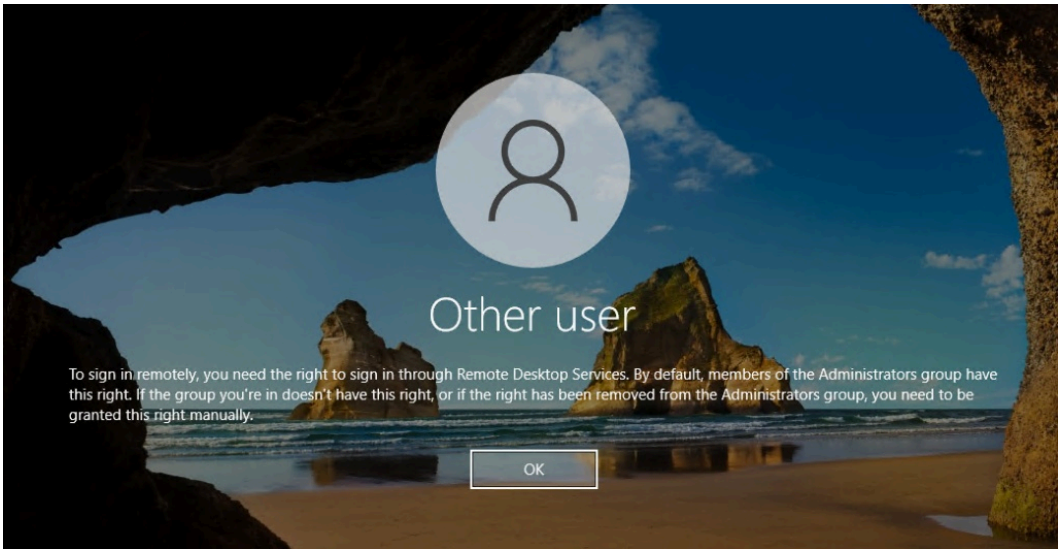
Una volta applicato controlliamo le regole firewall relative al Remote Desktop, e qualora fossero disabilitate le abilitiamo.



Ora provo ad utilizzare il Desktop Remote Access:

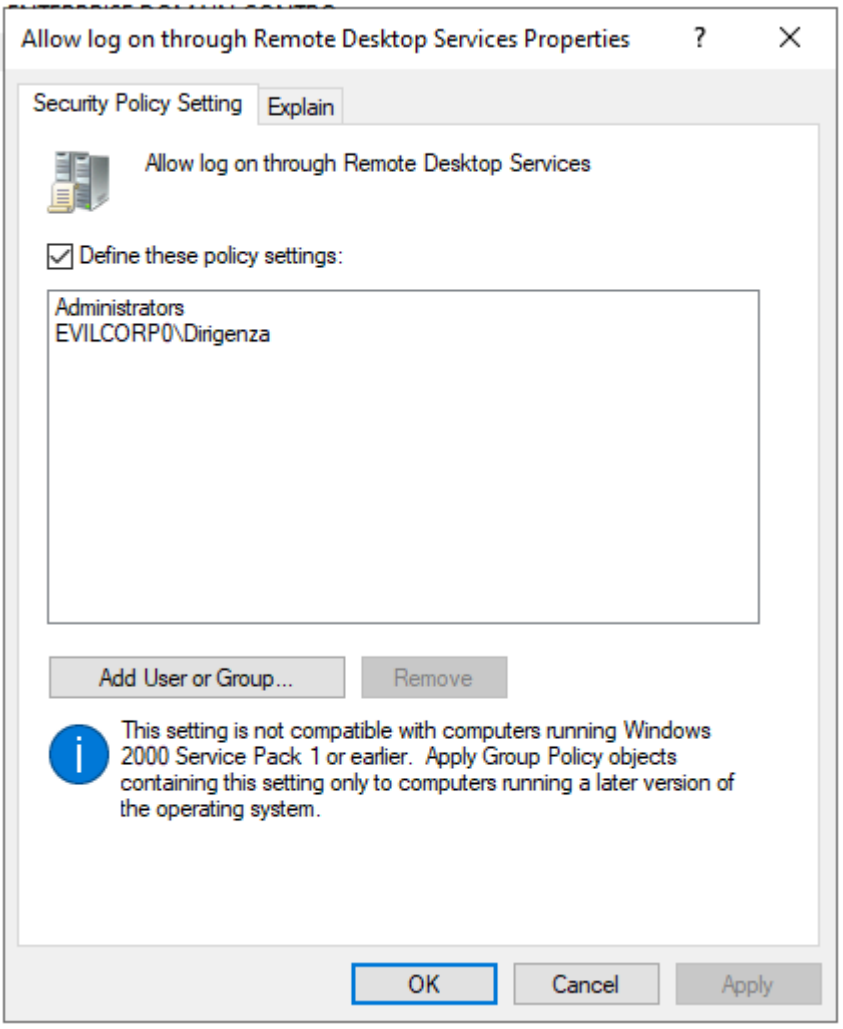


Mi connetto inserendo le credenziali, ma ottengo un errore:



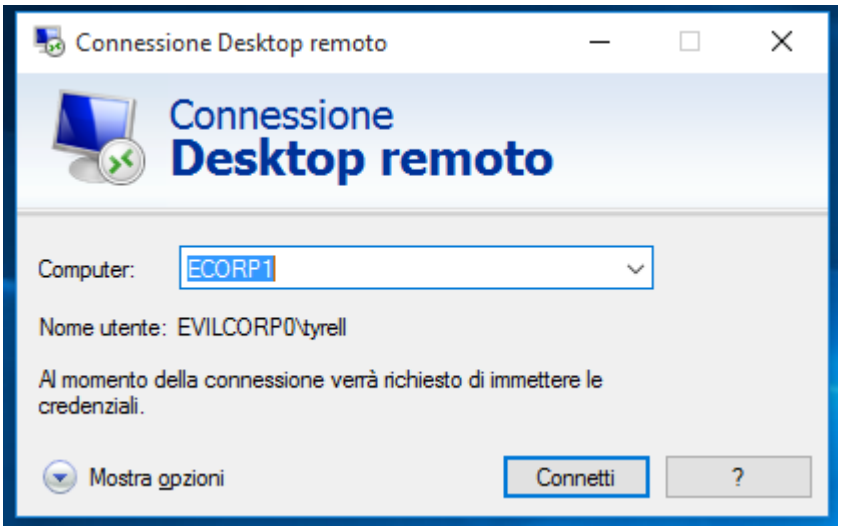
Per far fronte a questa problematica devo navigare più internamente, dando uno sguardo alle policy perché molto probabilmente stanno sovrascrivendo le impostazioni locali del server.

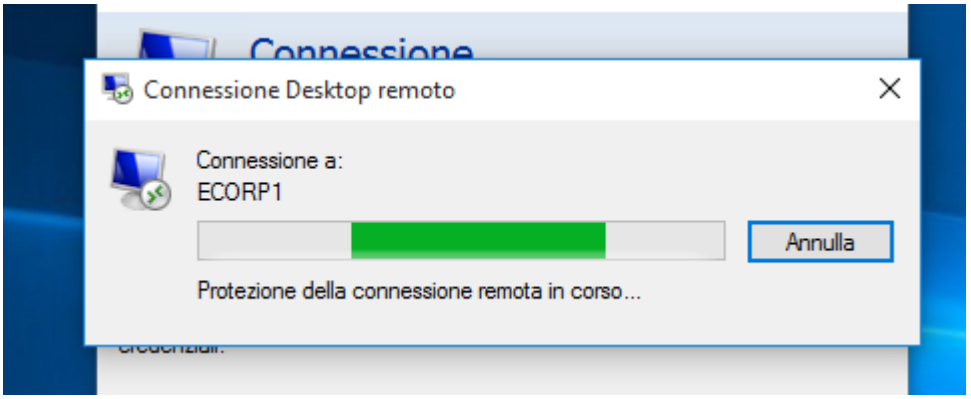
Apro il "**Group Policy Management**" e faccio l'edit di **Default Domain Controllers Policy**. Si apre l'editor e da qui seguiamo il percorso `Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment`. Ci ritroviamo davanti tutte le policy di base del server, cerchiamo la policy Allow log on through Remote Desktop Services e impostiamo il gruppo Dirigenza.

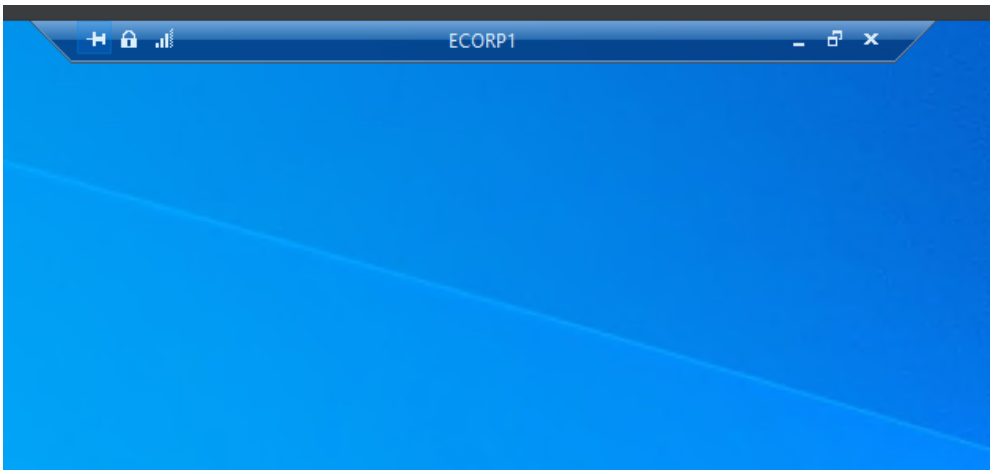


Ora l'accesso remoto dovrebbe essere operativo.

- **Verifica**







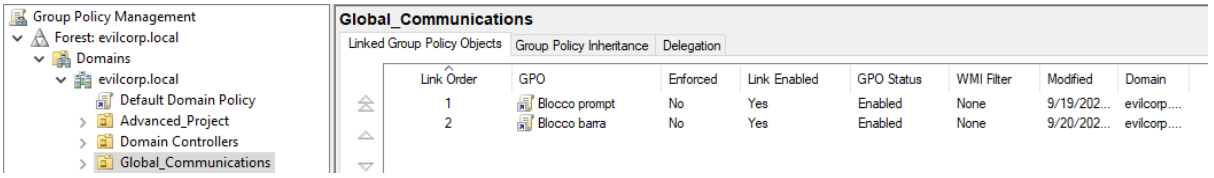
Abbiamo eseguito correttamente l'accesso tramite Remote Desktop.

7. **Modifiche alle impostazioni di sistema**
   Per ultima cosa aggiungo una policy al gruppo Marketing che vieti la possibilità di modificare la barra di windows.

- Da Server Manager, andiamo su "Tools" > "Group Policy Management".

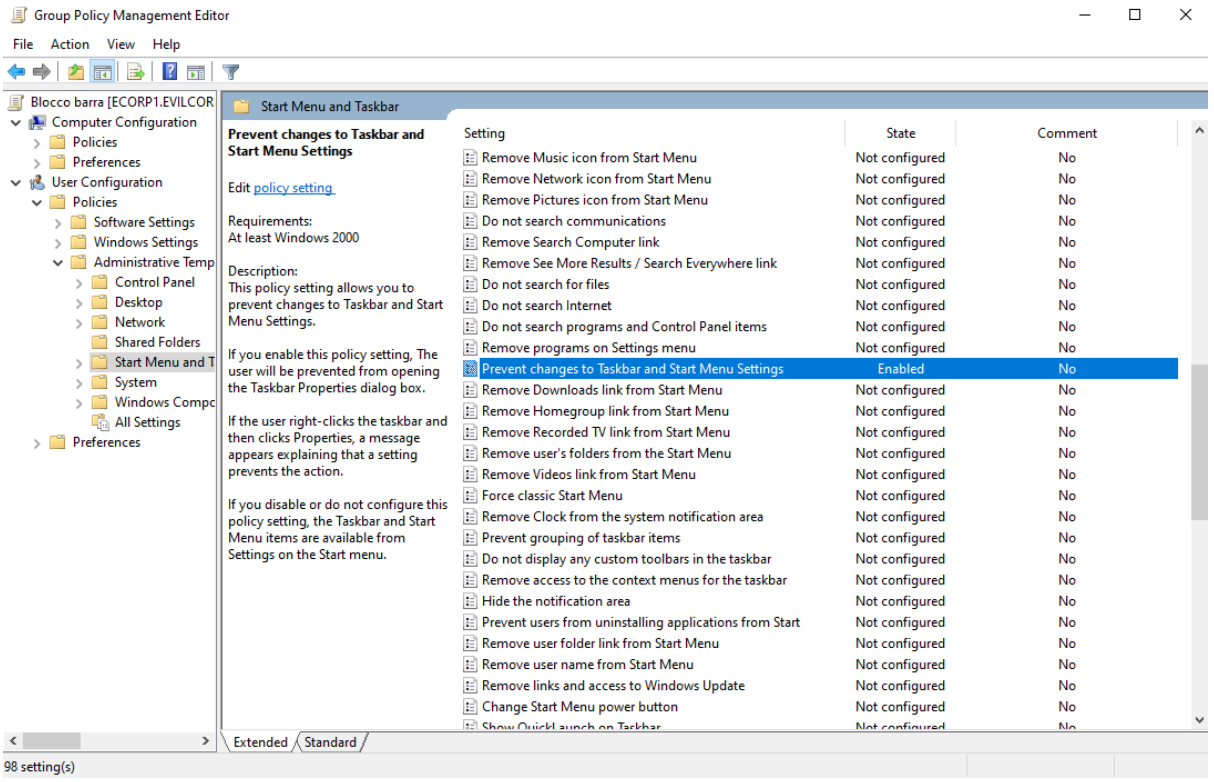
Crea e Collega una Nuova GPO

- Selezioniamo Global_Connections
- Facciamo clic con il tasto destro sull'OU e scegliamo "**Create a GPO in this domain, and Link it here...**". e la chiamiamo **Blocco barra**



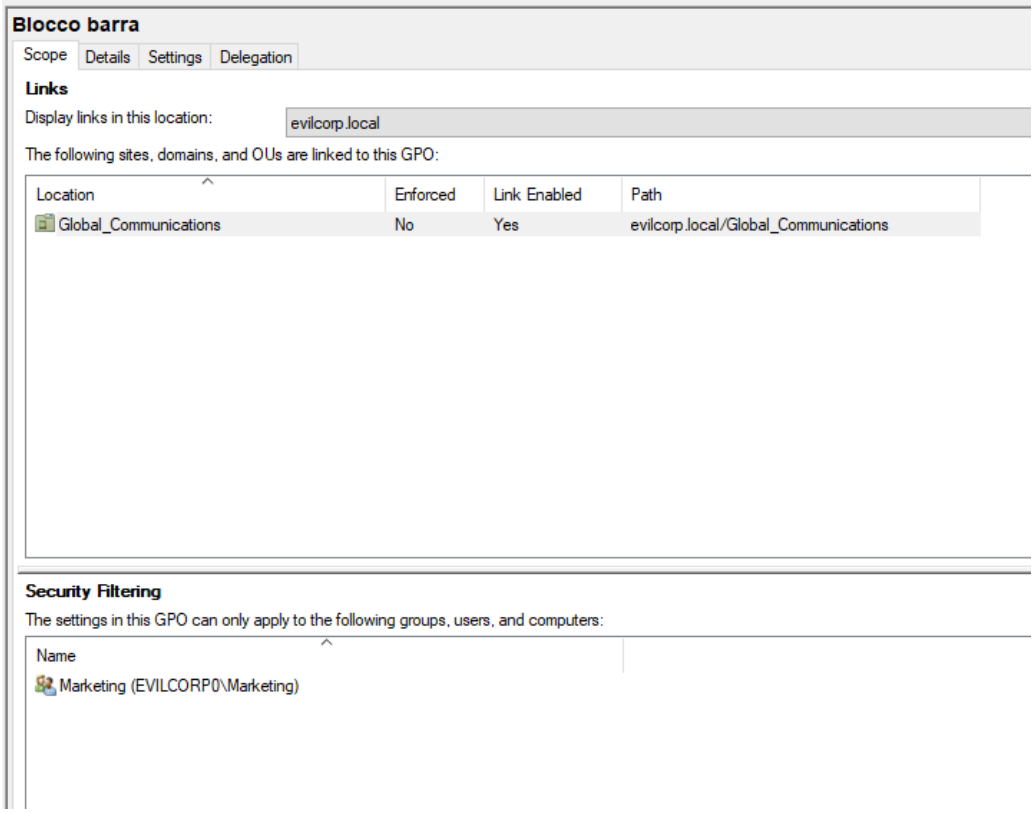
Adesso la dobbiamo modificare, facciamo quindi tasto destro su di essa e facciamo edit. Si apre il Group policy management editor e andiamo al seguente percorso:

`User Configuration > Policies > Administrative Templates > Start Menu and Taskbar`



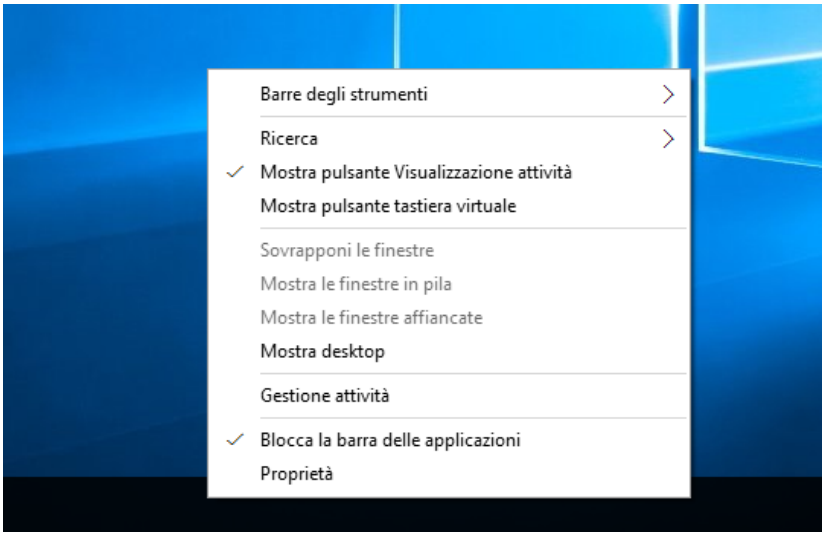
Selezioniamo **Prevent changes to Taskbar and Start Menu Settings** e la abilitiamo.

Successivamente da Gruop policy management impostiamo il gruppo a cui vogliamo che la policy venga abilitata.

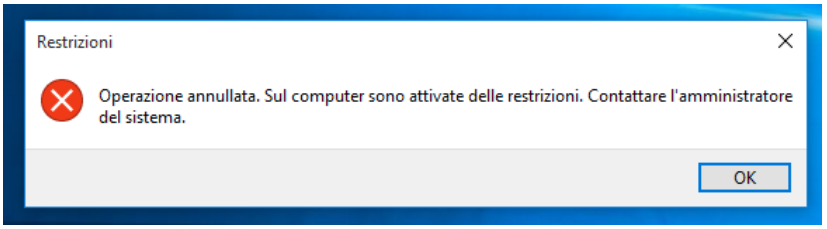


- **Verifica**

  Accediamo al computer di Angela, che si trova nel gruppo marketing e proviamo a fare una modifica alla barra di Windows.



  Selezionando proprietà avremmo un messaggio di errore



Conclusione

In sintesi, questa esercitazione ha illustrato la procedura dettagliata per la gestione degli accessi e delle risorse in un ambiente Windows Server 2022. Abbiamo coperto la creazione di gruppi di utenti, la configurazione delle unità organizzative (OU), l'assegnazione di utenti ai gruppi e, successivamente, l'impostazione e la verifica dei permessi di accesso alle cartelle. L'esercitazione ha anche mostrato come impedire l'uso di specifiche applicazioni a un gruppo e come abilitare l'accesso remoto alla macchina. È stato evidente come una gestione accurata dei permessi sia fondamentale per garantire la sicurezza e un controllo granulare sull'accesso alle risorse, aspetti cruciali in ogni contesto aziendale.