PROGETTO S10L5

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.

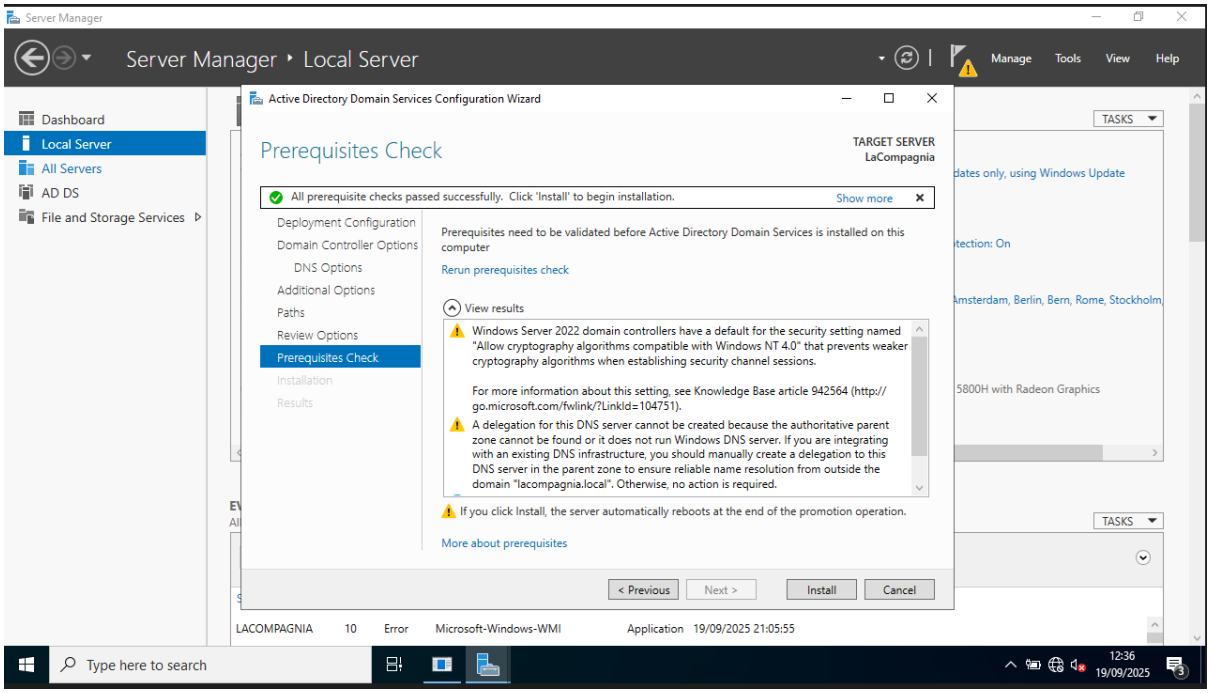
Istruzioni

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. 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.

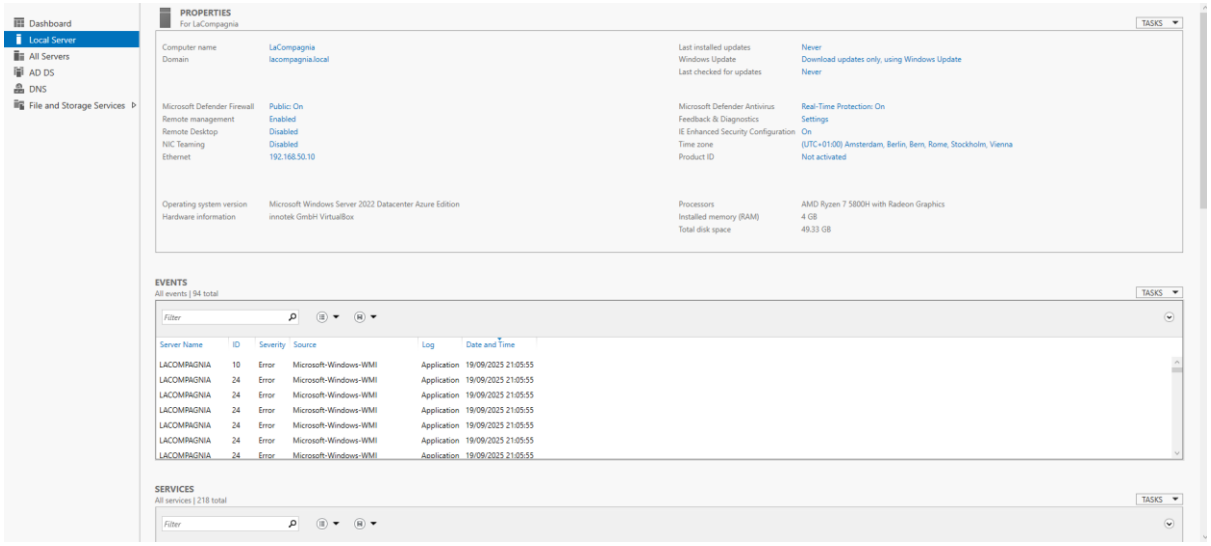
- Eventuali problemi riscontrati e come li hai risolti.

Configurazione e Creazione di dominio su Windows Server 2022

Ho avviato la configurazione di **Active Directory Domain Services** tramite Server Manager su Windows Server 2022.



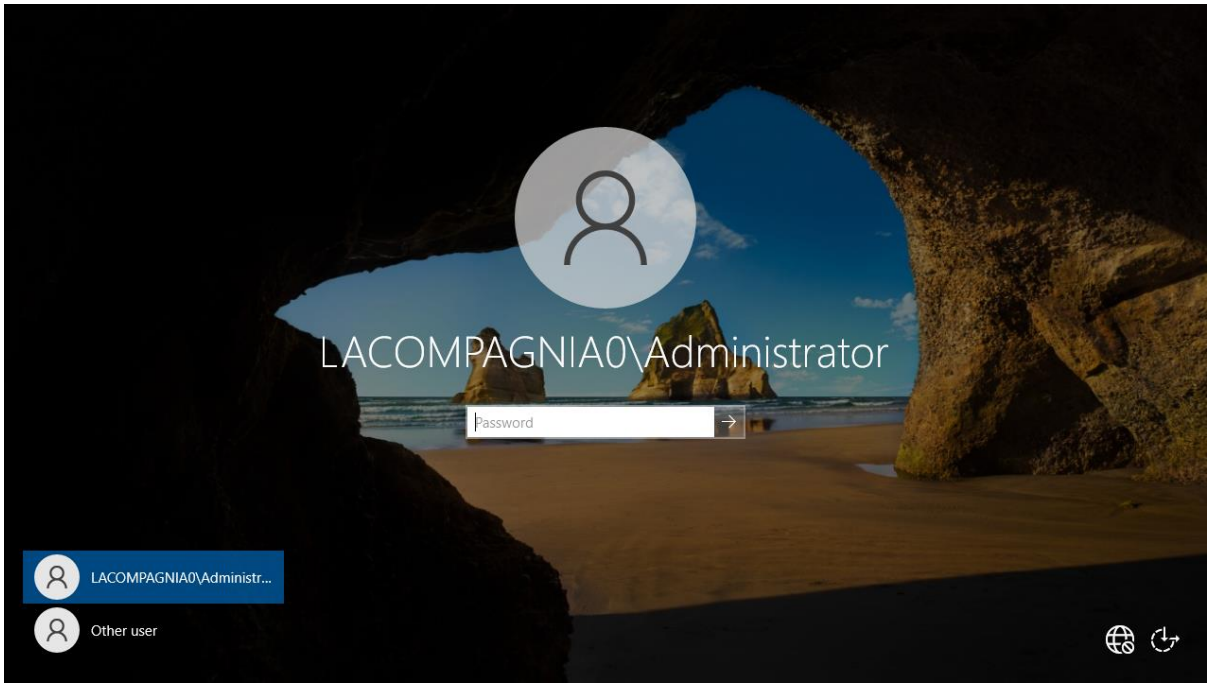
Dopo aver cliccato su **Install**, il server è stato promosso correttamente come controller di dominio per **lacompagnia.local**.



Accesso post-promozione – Dominio lacompagnia.local

Dopo il **riavvio obbligatorio** seguito alla promozione del server a domain controller, mi sono ritrovato davanti alla schermata di accesso di Windows Server 2022, questa volta sotto il dominio appena creato: **lacompagnia.local**.

L'utente visualizzato è **LACOMPAGNIA0\Administrator**, conferma che il server è ora correttamente integrato nel dominio. Da qui posso accedere con le credenziali dell'amministratore di dominio e iniziare la gestione centralizzata degli account, delle policy e dei servizi.

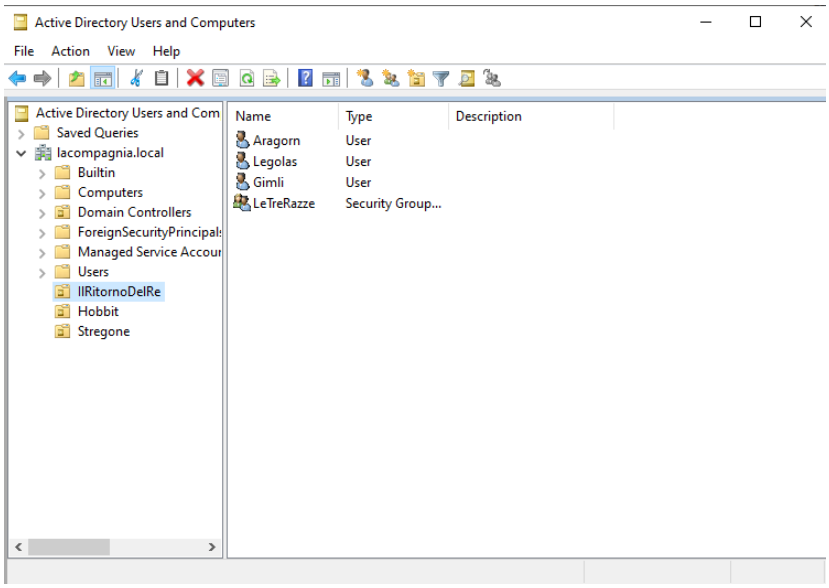


Creazione di organizzazioni, utenti e gruppi:

Nel contesto della configurazione del dominio **lacompagnia.local** su Windows Server 2022, ho progettato una struttura organizzativa tematica per la gestione centralizzata di utenti e gruppi. L'obiettivo è garantire **ordine, chiarezza e coerenza funzionale**, sfruttando al tempo stesso una logica narrativa ispirata al mondo fantasy per rendere la documentazione più coinvolgente e memorabile. Le configurazioni sono:

- **IlRitornoDelRe**
  All'interno del dominio **lacompagnia.local**, ho creato una nuova **Organizational Unit (OU)** chiamata **IlRitornoDelRe.** All'interno dell'**OU** ho creato un G**ruppo chiamato LeTreRazze**, che raccoglie tre utenti distinti:
  - **Aragorn**
  - **Legolas**
  - **Gimli**

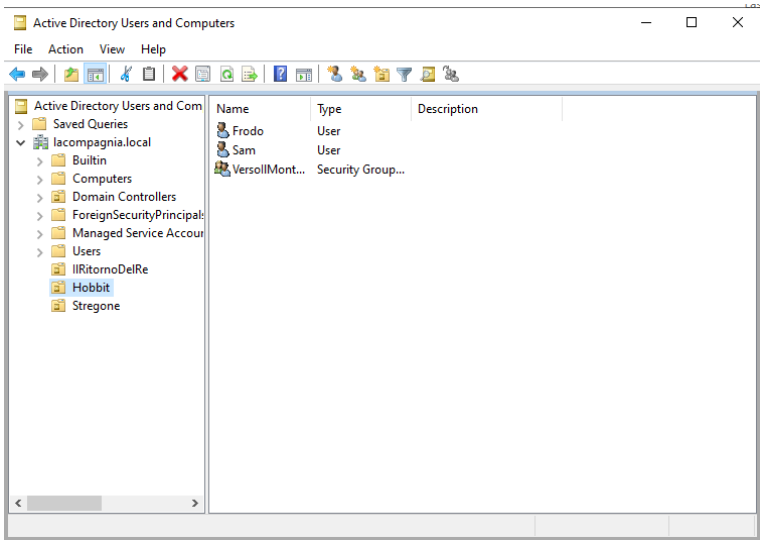
  Questa struttura mi permette di applicare policy e permessi in modo centralizzato



- **Hobbit**

  All'interno del dominio **lacompagnia.local**, ho creato una nuova **Organizational Unit (OU)** chiamata **Hobbit**. All'interno dell'OU ho creato un **Gruppo** chiamato **VersoIlMonteFato,** che raccoglie due utenti distinti:

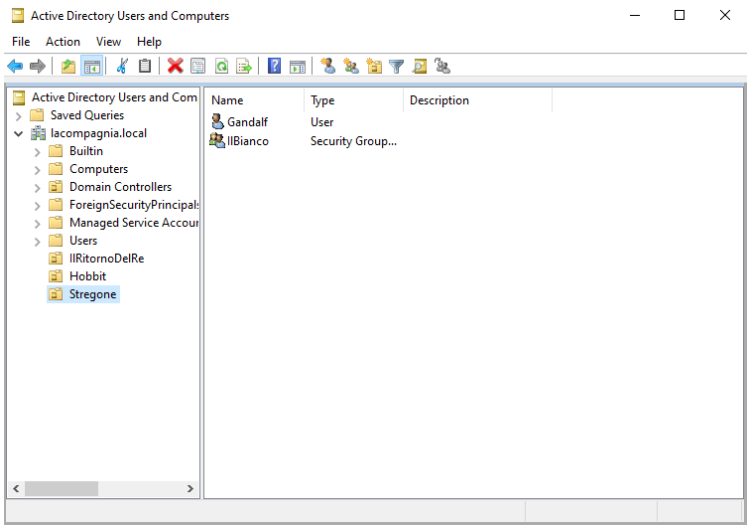
  - **Frodo**
  - **Sam**



- **Stregone**

  Nel dominio **lacompagnia.local**, ho creato l'**Organizational Unit (OU)** chiamata **Stregone.** All'interno dell'OU ho creato un **Gruppo** chiamato **IlBianco,** che raccoglie 1 utente:

  - **Gandalf**



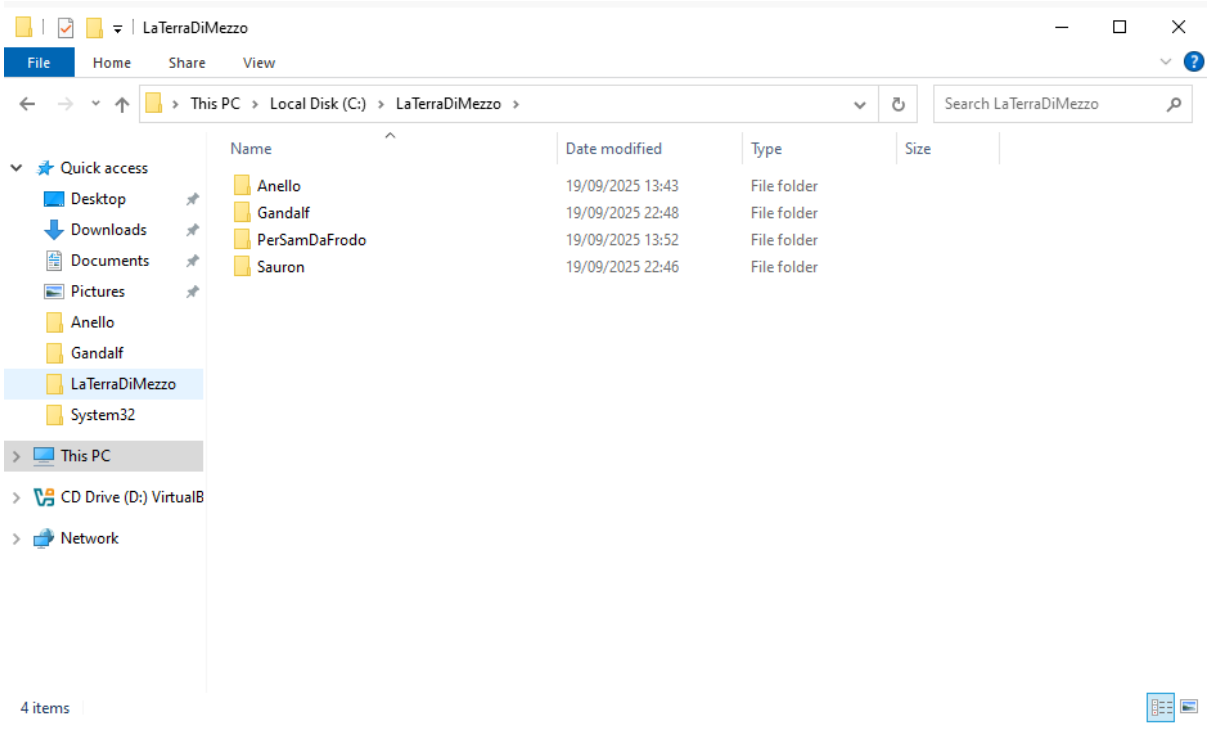
Creazione delle Cartelle

All'interno del computer che funge da **server nel dominio lacompagnia.local**, ho creato la cartella principale denominata **LaTerraDiMezzo**, che fungerà da contenitore per le risorse condivise.

Al suo interno ho predisposto le seguenti sottocartelle, ciascuna destinata a specifici gruppi o utenti, e che verranno configurate con **condivisione e permessi dedicati**:

- **Anello**
- **Gandalf**
- **PerSamDaFrodo**
- **Sauron**

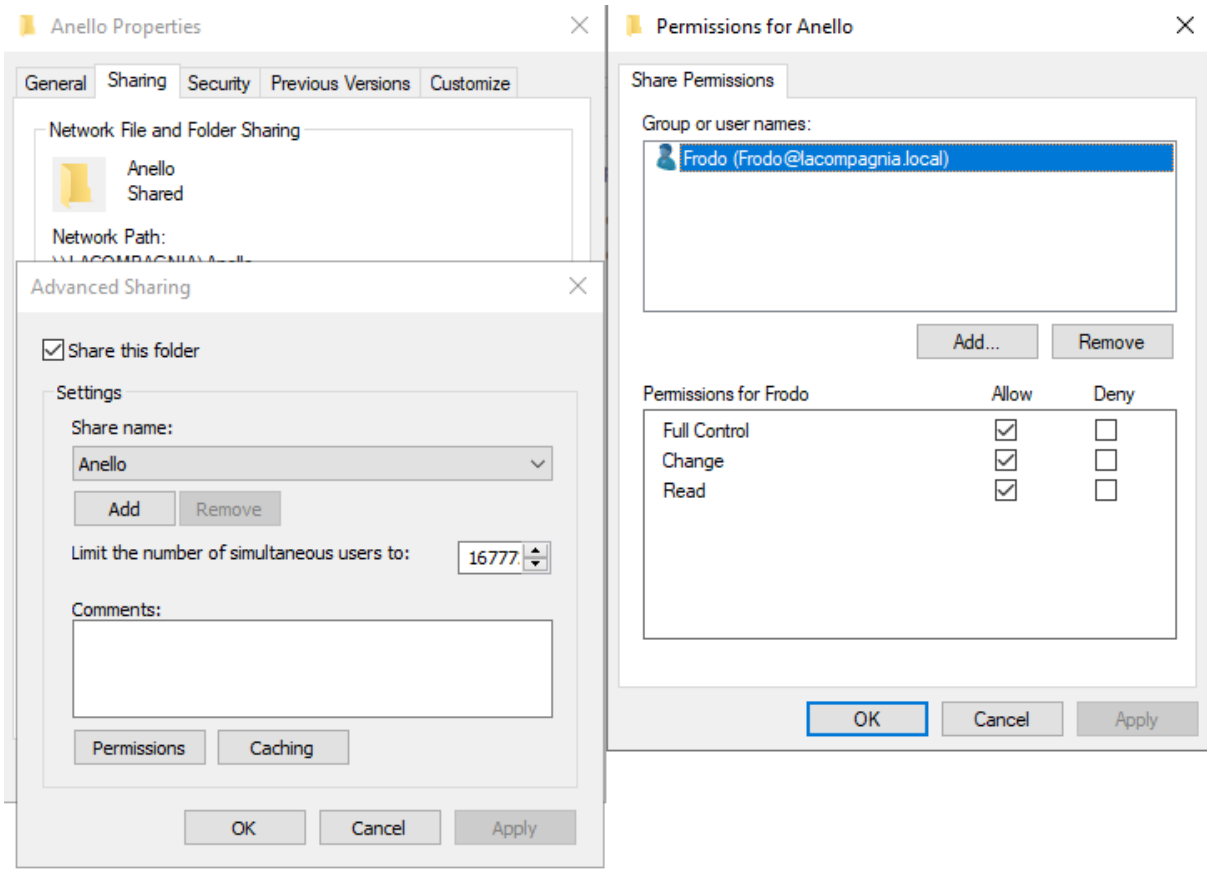
Questa struttura mi permetterà di applicare **policy di accesso**, assegnando permessi NTFS e di condivisione in base ai ruoli definiti nell'Active Directory.



Gestione Permessi Cartelle

Anello

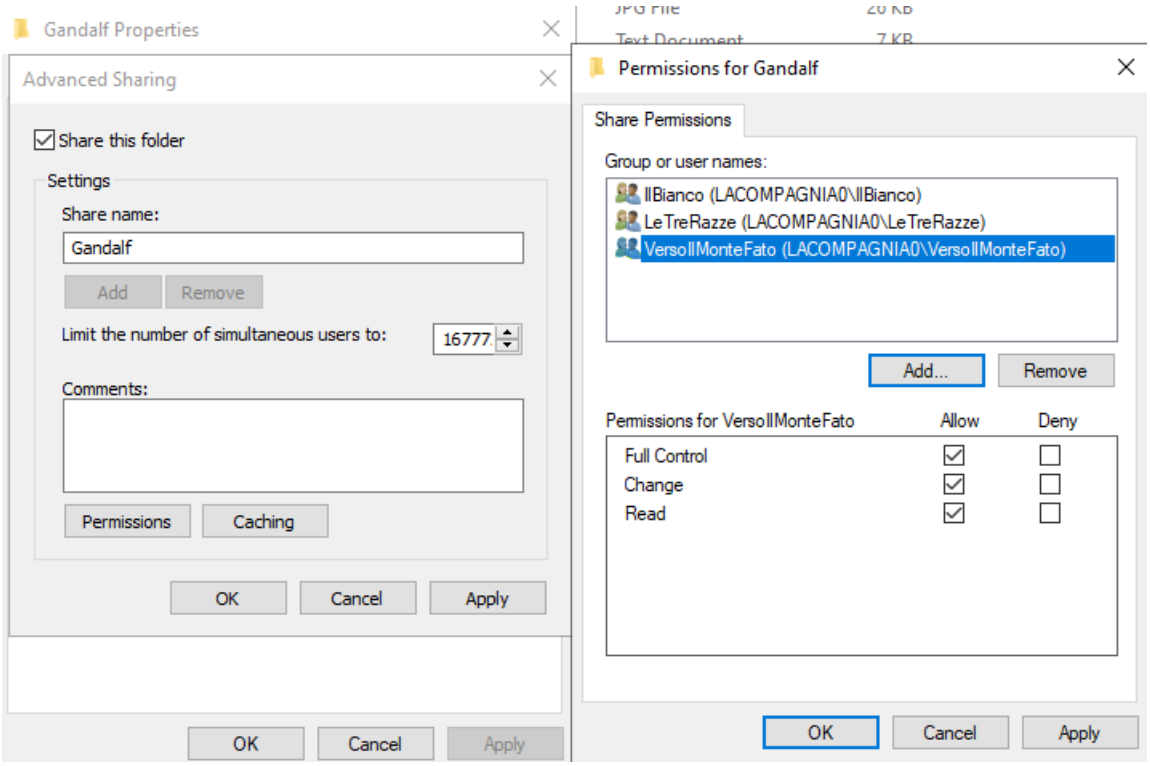
Per la cartella **Anello** viene dato il **Full Control** solamente all'utente **Frodo**



Gandalf

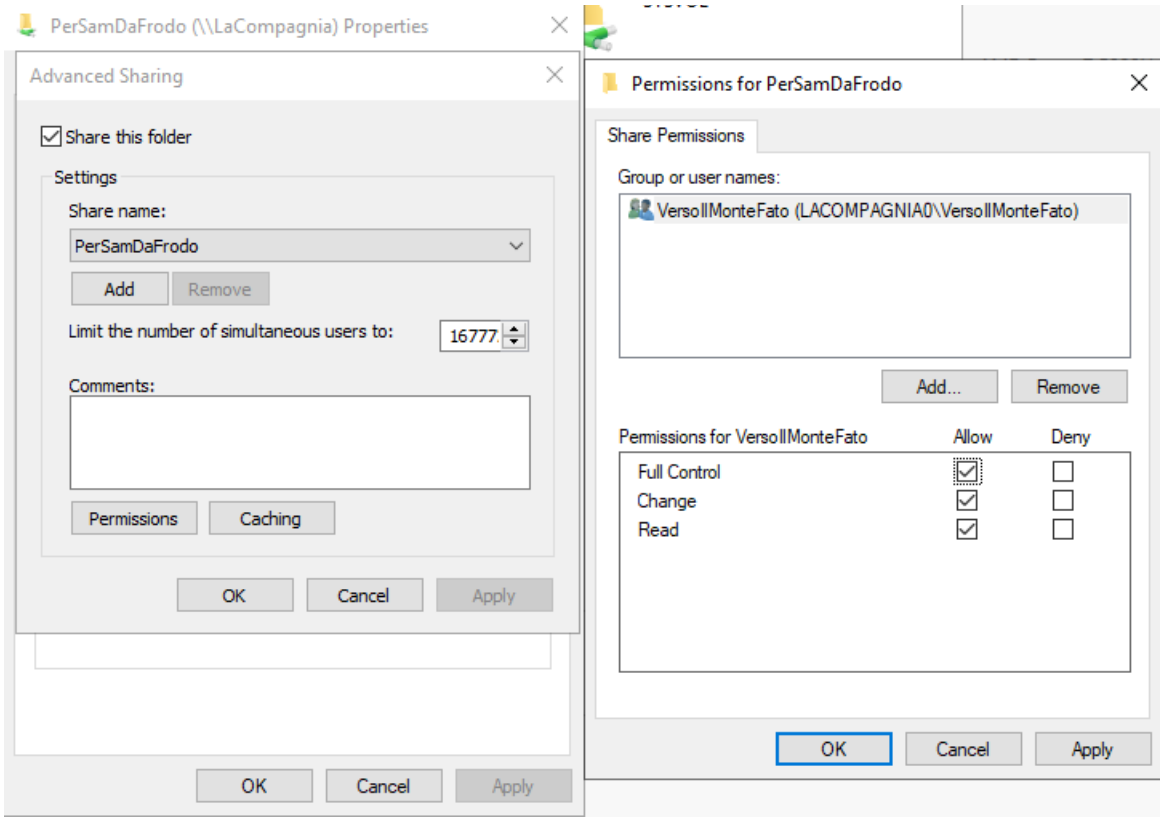
Per la cartella **Gandalf** viene dato il **Full Control** ai gruppi:

- **IlBianco**(Gandalf)
- **LeTreRazze**(Aragorn,Legolas e Gimli)
- **VersoIlMonteFato**(Frodo e Sam)



PerSamDaFrodo

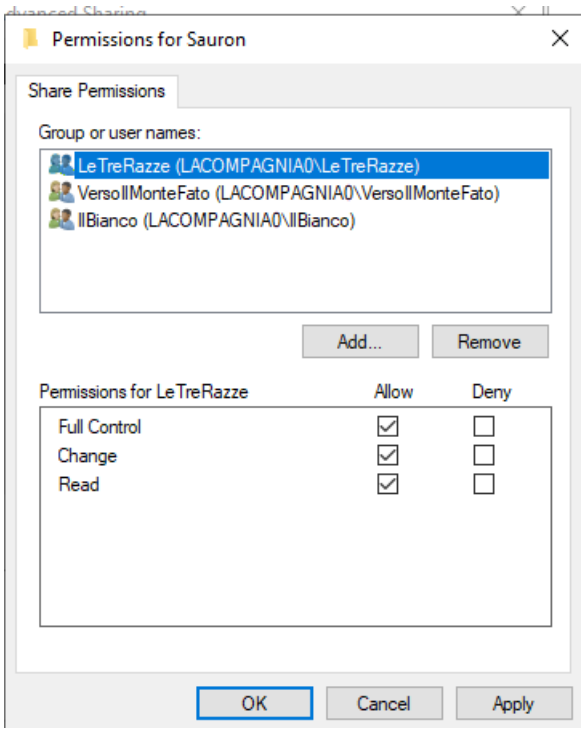
Per la Cartella **PerSamDaFrodo** viene dato il **Full Control** al gruppo **VersoIlMonteFato** (Frodo e Sam)



Sauron

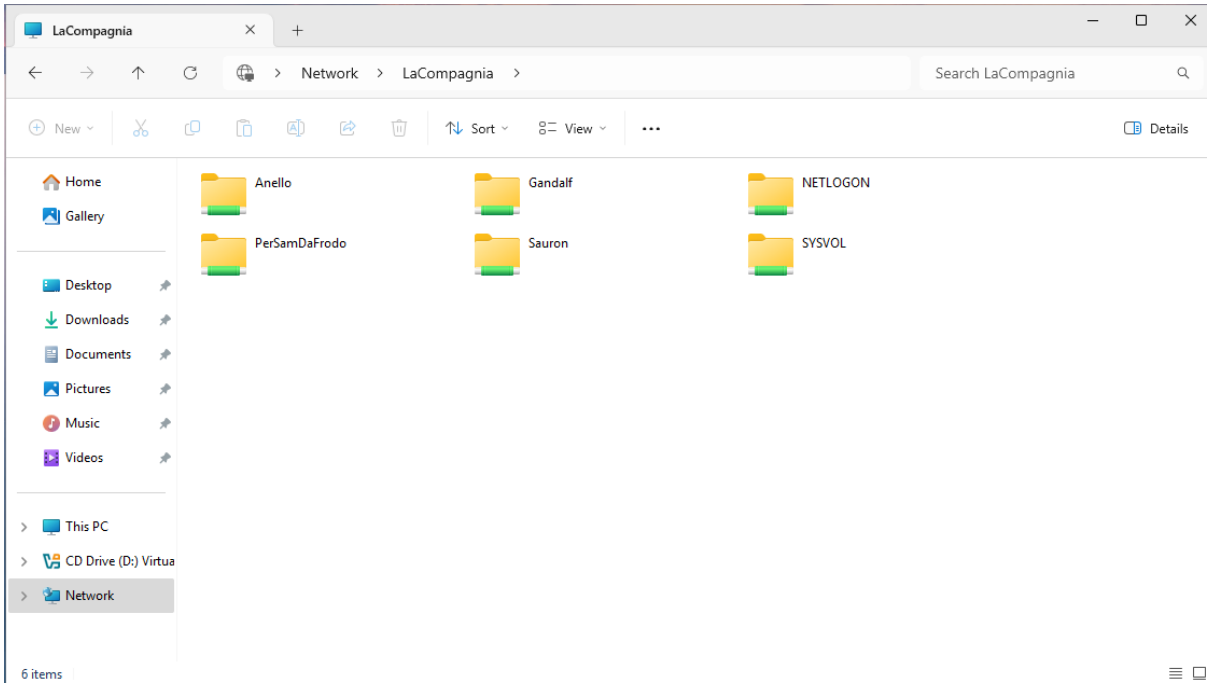
Per la cartella **Sauron** viene dato il **Full Control** ai gruppi:

- **IlBianco**(Gandalf)
- **LeTreRazze**(Aragorn,Legolas e Gimli)
- **VersoIlMonteFato**(Frodo e Sam)

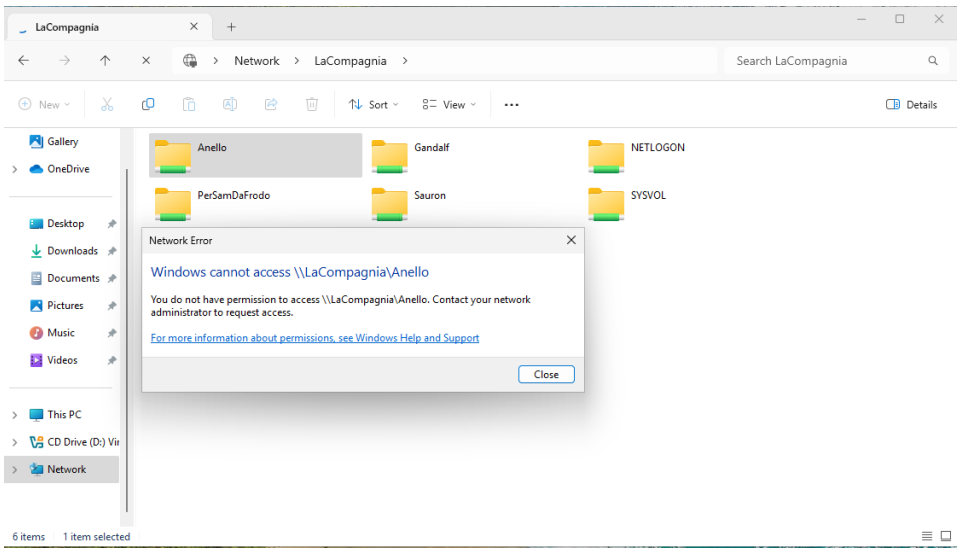


Verifica permessi cartelle

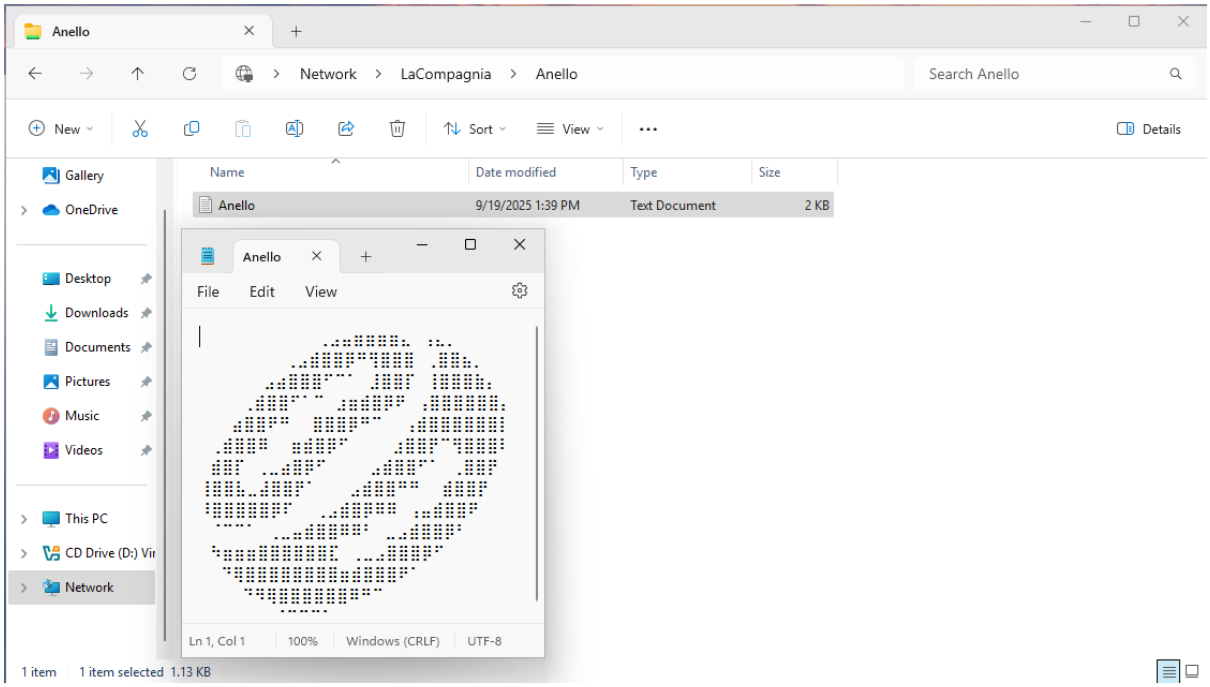
Accedendo al server tramite la sezione **Network** e digitando il percorso `\\LaCompagnia`, utilizzando l'utente **Gandalf** appartenente al dominio **lacompagnia.local**, vengono visualizzate correttamente le cartelle condivise precedentemente configurate all'interno della directory principale **LaTerraDiMezzo**.



Ad esempio, l'utente **Gandalf** non ha accesso alla cartella **Anello**, poiché i permessi di **Full Control** sono stati assegnati esclusivamente all'utente **Frodo**. Questa configurazione garantisce che solo Frodo possa visualizzare, modificare o gestire i contenuti della cartella, mantenendo un livello di riservatezza coerente con il ruolo assegnato all'interno del dominio **lacompagnia.local**.



Accedendo al server con l'utente **Frodo**, quest'ultimo dispone dei permessi necessari per accedere alla cartella **Anello** all'interno della directory condivisa **LaTerraDiMezzo**. Oltre alla visualizzazione della cartella, Frodo può anche aprire e gestire il file **Anello.txt**, grazie ai privilegi di **Full Control** assegnati esclusivamente al suo account.

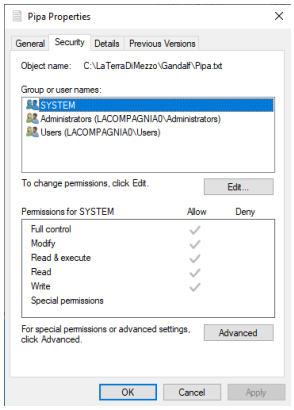


Un altro esempio significativo riguarda la cartella **Gandalf**, situata all'interno della directory condivisa **LaTerraDiMezzo**. Al suo interno sono presenti due file:

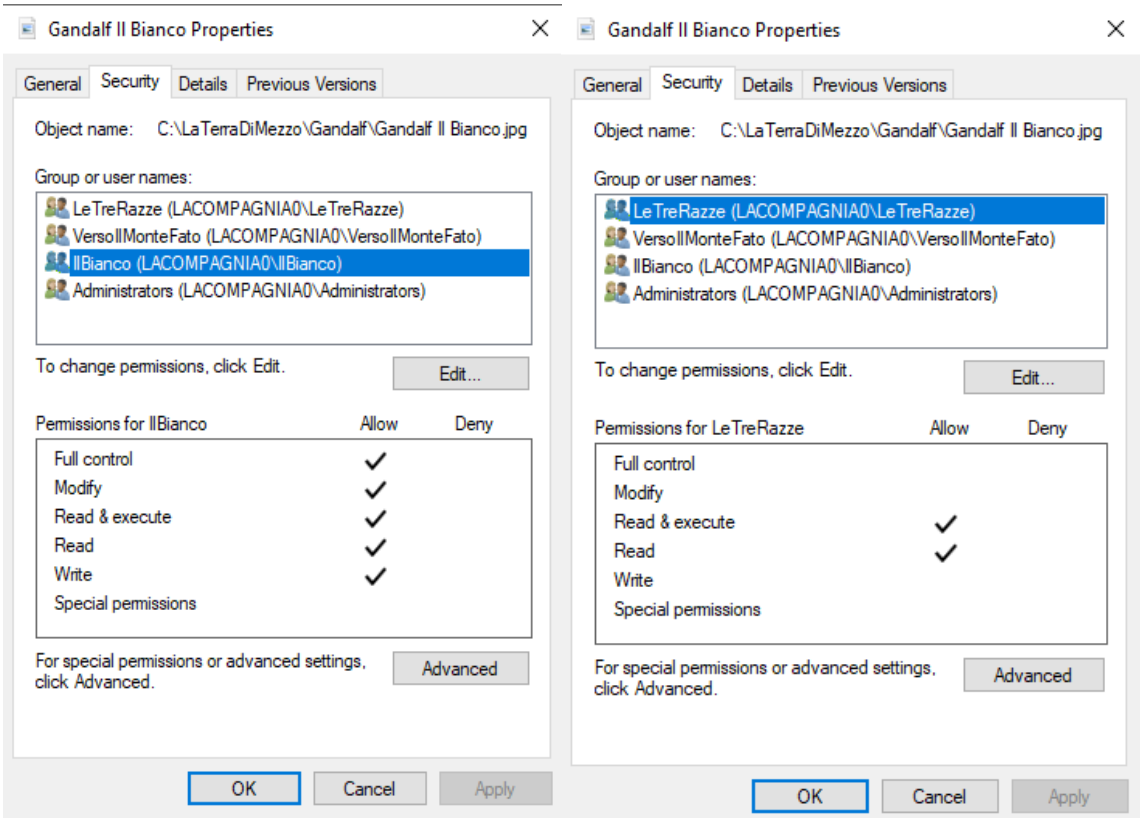
- **GandalfIlBianco.jpg**
- **Pipa.txt**

I permessi assegnati ai file sono differenziati:

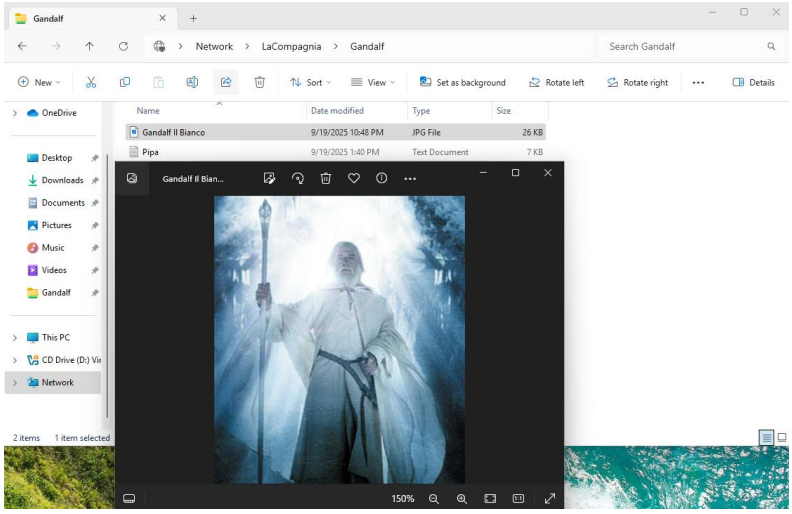
- Per **Pipa.txt**, è stato concesso il **Full Control** a tutti e tre i gruppi definiti nel dominio: **IlBianco**, **LeTreRazze** e **VersoIlMont...**. Questo consente una gestione condivisa del file tra le diverse "fazioni" dell'infrastruttura.



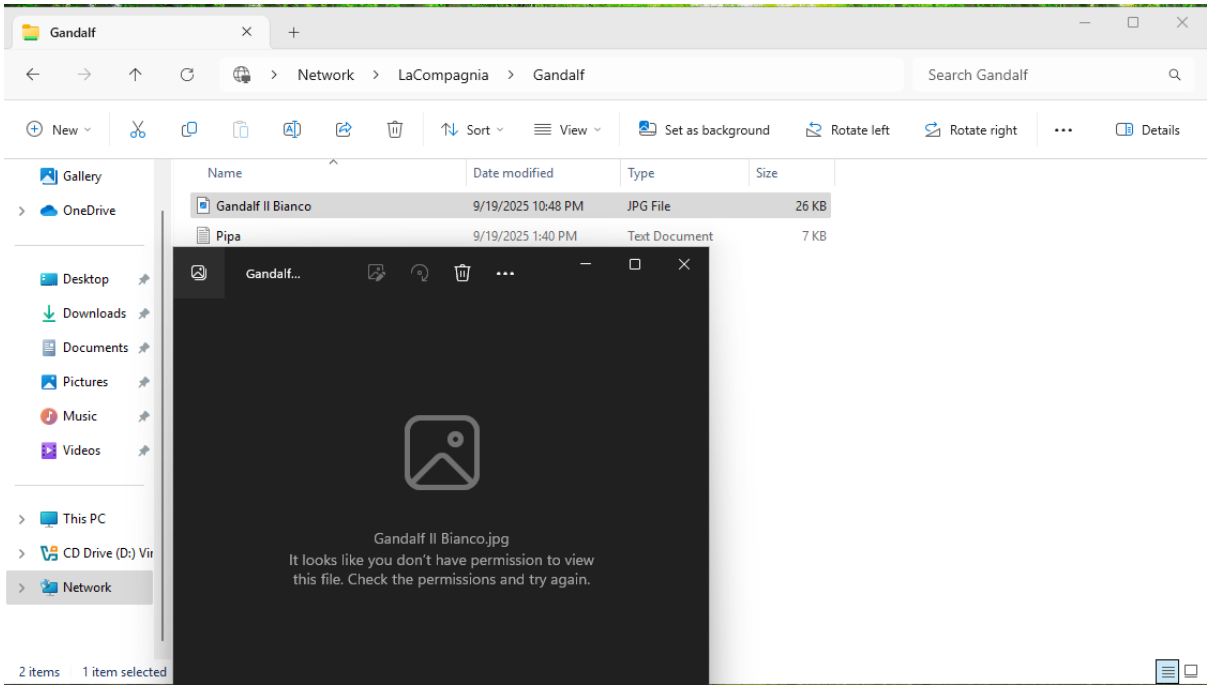
- Per **GandalfIlBianco.jpg**, invece, il **Full Control** è riservato esclusivamente ai gruppi **IlBianco** e **LeTreRazze(in questo caso solamente la lettura e esecuzione)**, escludendo **VersoIlMont…** dall'accesso. Questa scelta riflette una logica di accesso più restrittiva, coerente con il ruolo e la riservatezza del contenuto.



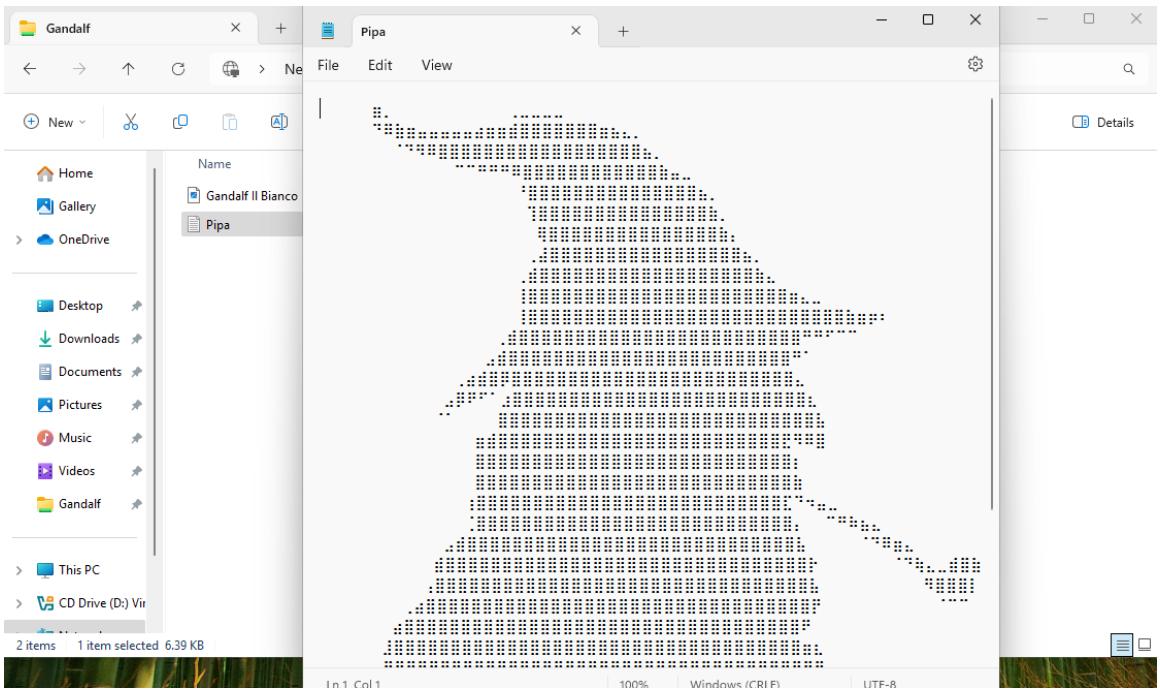
Come previsto dalla configurazione dei permessi, accedendo con l'utente **Aragorn** è possibile **visualizzare il file GandalfIlBianco.jpg** all'interno della cartella **Gandalf**. Questo è reso possibile dal fatto che Aragorn appartiene al gruppo **LeTreRazze**, uno dei due gruppi autorizzati su quel file.



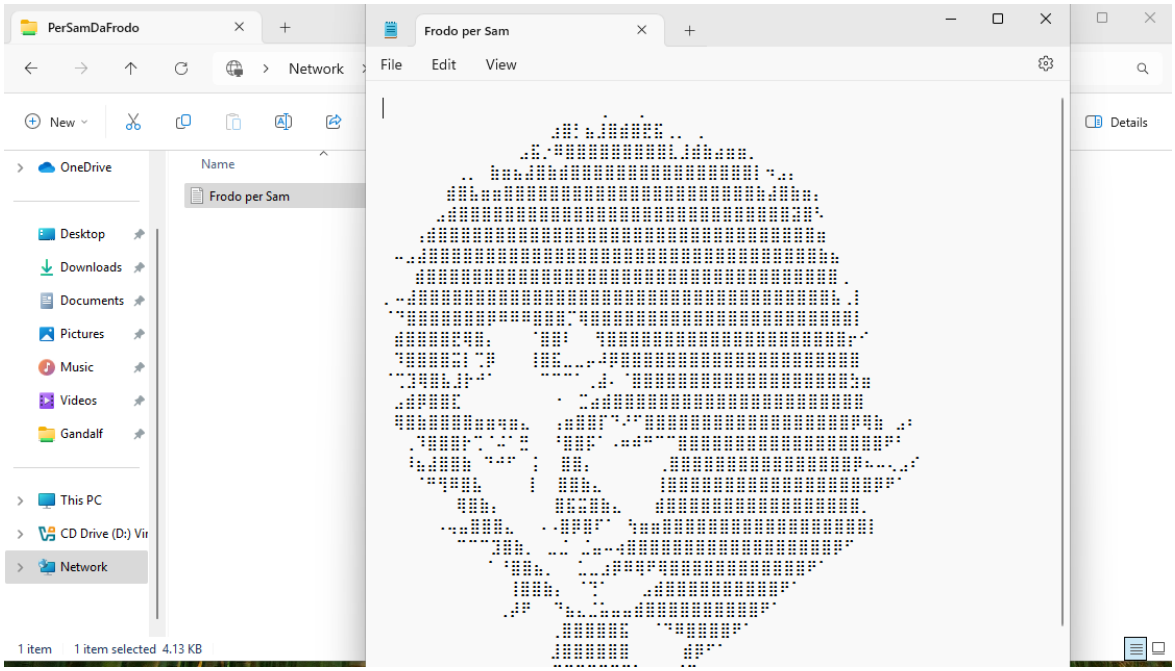
Accedendo con l'utente **Frodo**, non sarà possibile visualizzare né aprire il file **GandalfIlBianco.jpg** all'interno della cartella **Gandalf**, poiché il suo account non appartiene a nessuno dei gruppi autorizzati (**IlBianco** e **LeTreRazze**) che dispongono dei permessi su quel file.



Sia l'utente **Frodo** che l'utente **Aragorn** possono entrambi accedere al file **Pipa.txt** all'interno della cartella **Gandalf**, grazie ai permessi di **Full Control** assegnati ai rispettivi gruppi di appartenenza: **VersoIlMont...** per Frodo e **LeTreRazze** per Aragorn.



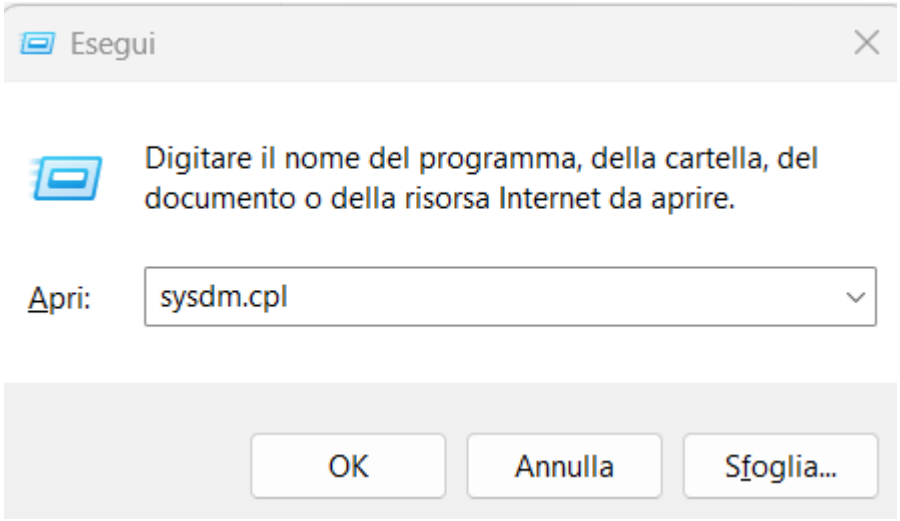
Come ultimo test, ho utilizzato la cartella **PerSamDaFrodo**, situata all'interno della directory condivisa **LaTerraDiMezzo**, affinché sia **visibile e accessibile esclusivamente** dal gruppo **VersoIlMonteFato**, composto dagli utenti **Frodo** e **Sam**.



Configurazione accesso remoto al server

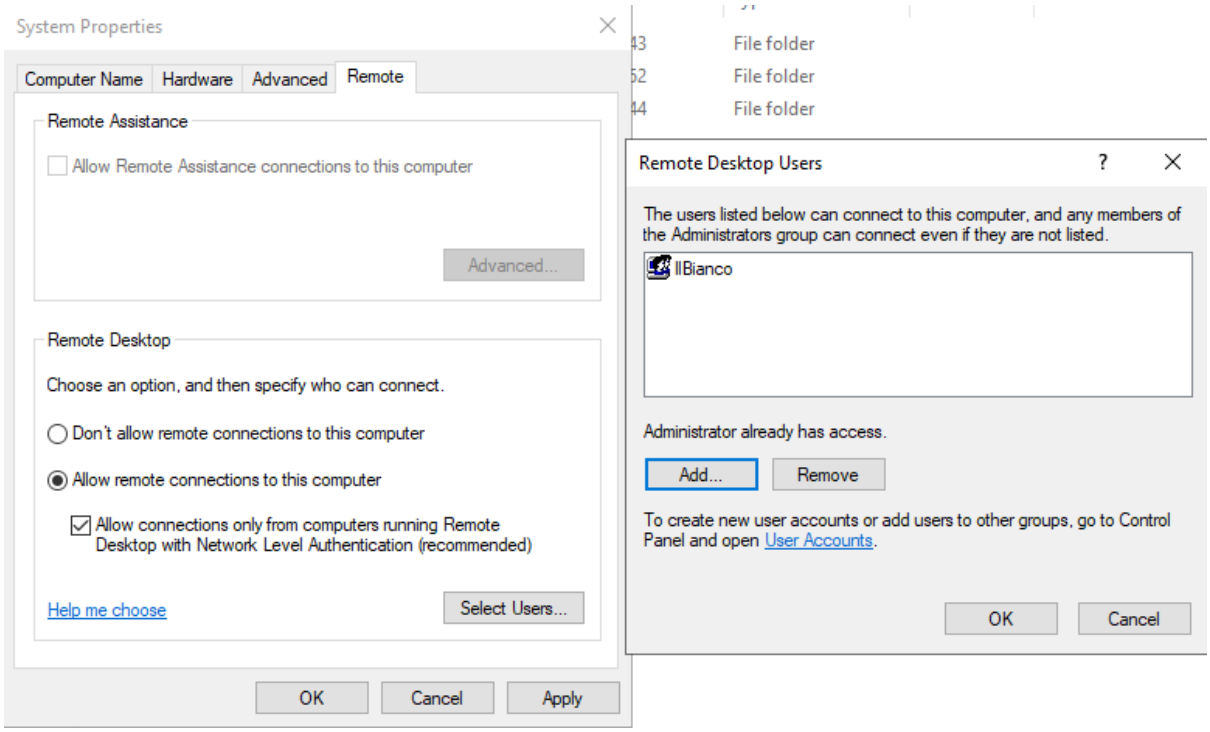
Per aprire la finestra delle **Proprietà del sistema** in modo rapido, è sufficiente premere la combinazione **Windows + R** per avviare la finestra **Esegui**, quindi digitare il comando:

- sysdm.cpl



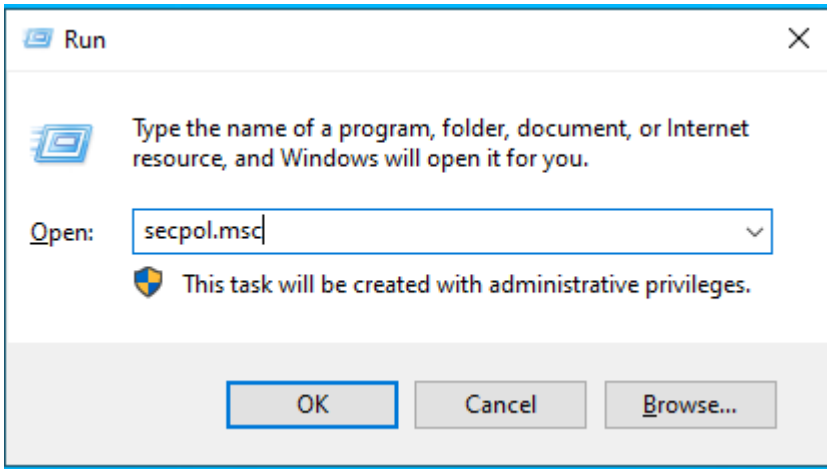
Successivamente, procediamo con l'**abilitazione del controllo remoto** sul server. Dopo aver attivato l'opzione corrispondente nelle **Proprietà del sistema**, accediamo alla sezione dedicata alla **selezione degli utenti autorizzati**.

In questo caso, aggiungiamo il **gruppo IlBianco** all'elenco degli utenti abilitati al controllo remoto, garantendo così all'utente Gandalf di potersi connettere al server tramite **Remote Desktop**.

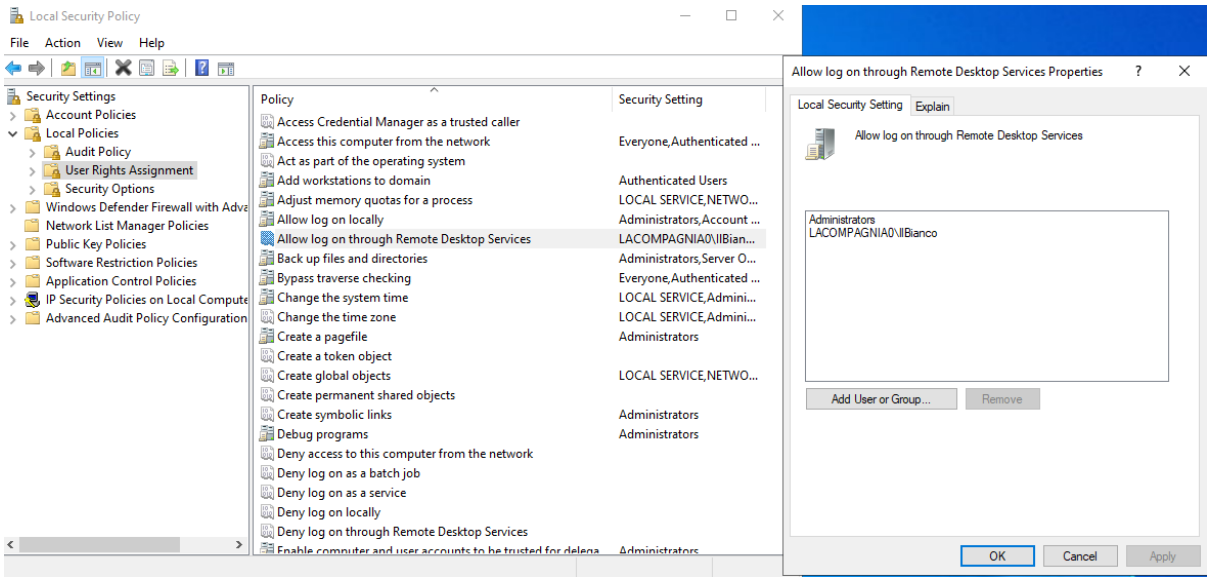


Continuiamo con l'abilitazione dei permessi da remoto aprendo il "Local Security Policy" sempre dall'esegui con Windows+R col seguente comando:

- secpol.msc

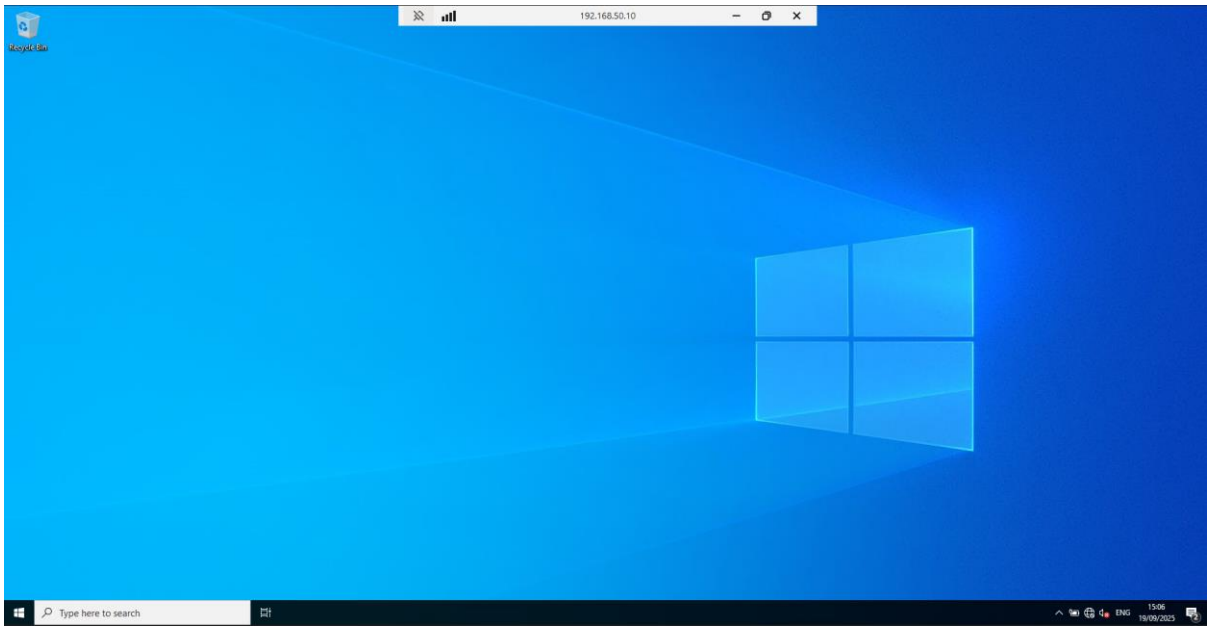


Dal secpol aggiungiamo il nostro utente per la connessione remota, nel nostro caso do i permessi solo all'utente **Gandalf** che fa parte del gruppo **IlBianco.**

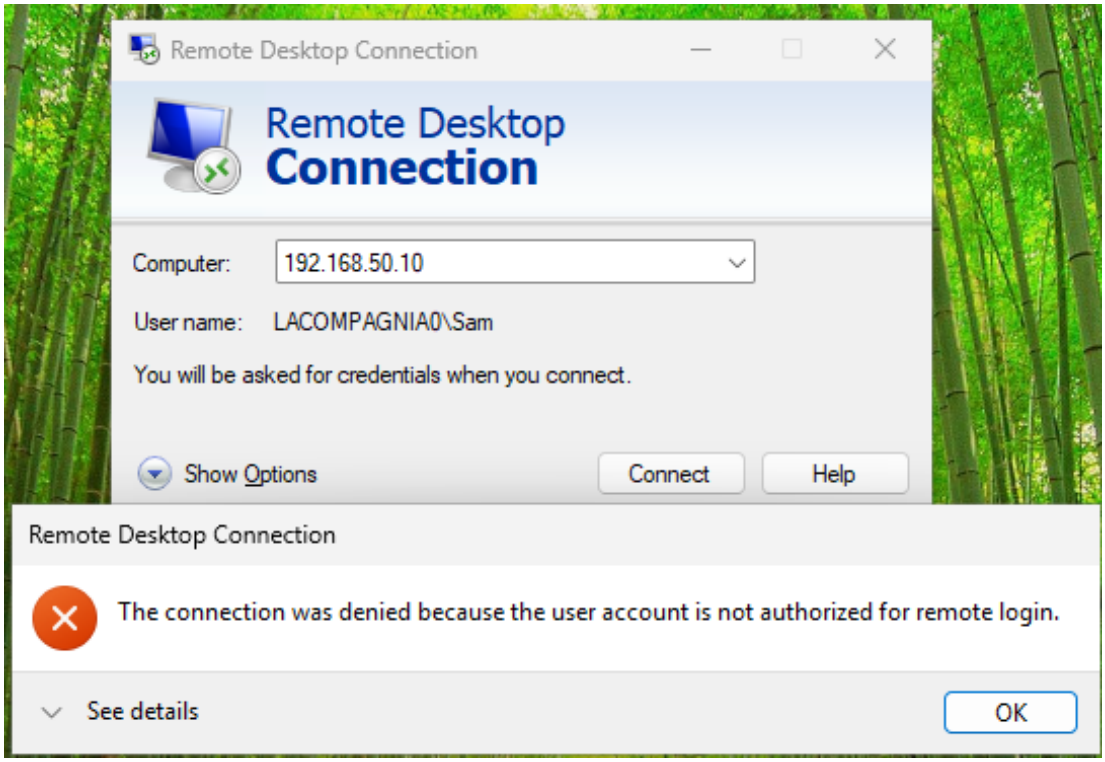


Verifica permessi accesso remoto al server

Tramite l'applicazione "Remote Desktop Controller" riusciamo a verificare anche la connessione da Remote con l'unico utente a cui sono stati dati i permessi, usiamo quindi **Gandalf** e l'esito è positivo facendoci connettere alla macchina server



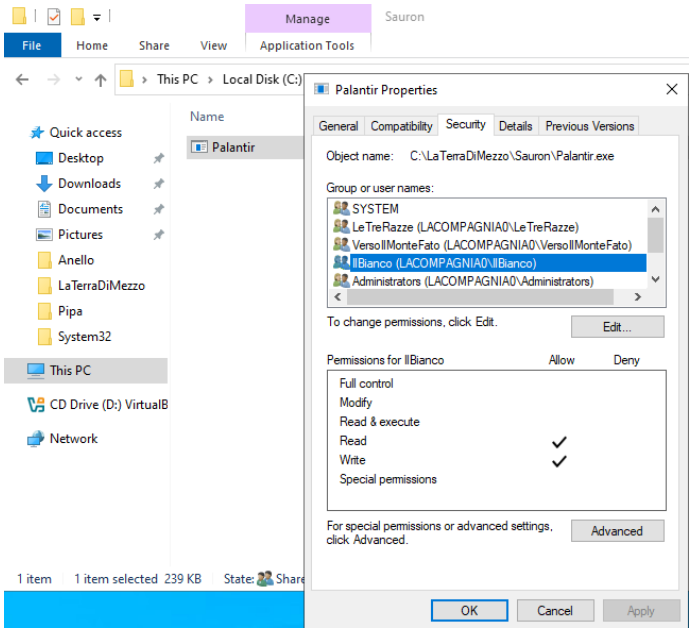
Proviamo successivamente con un utente che non ha i permessi in questo Sam



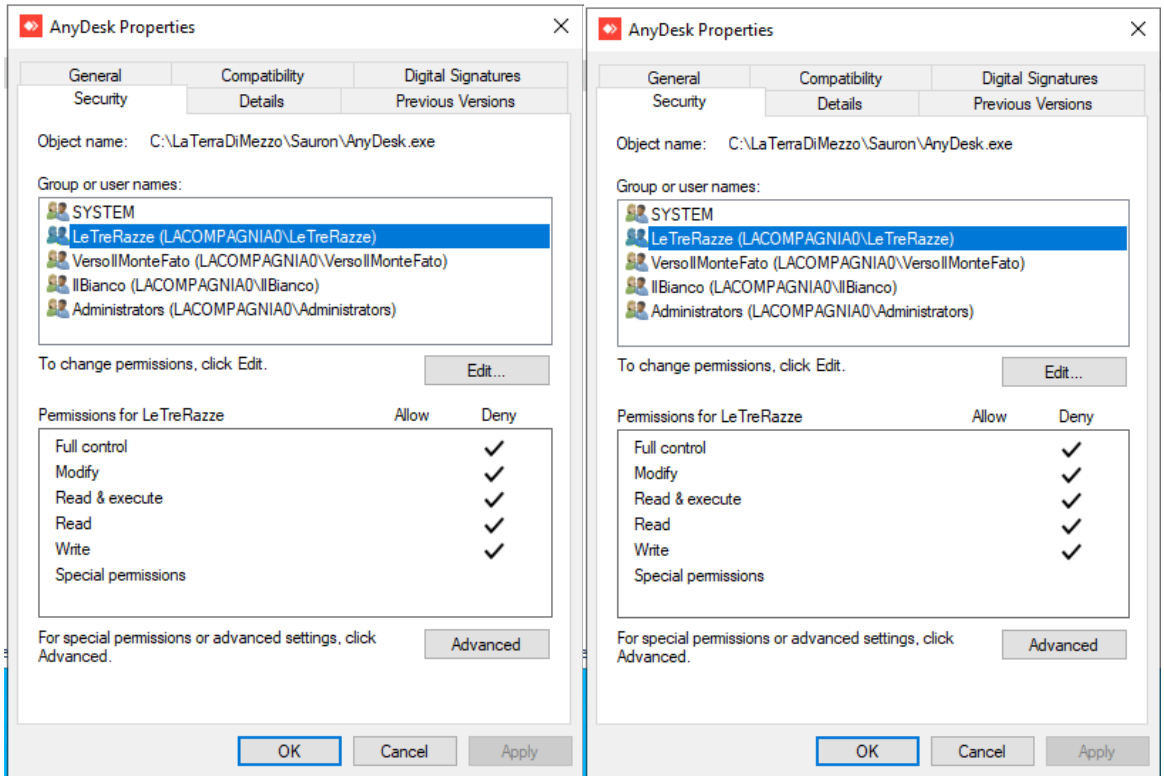
Gestione permessi per file eseguibili

All'interno della cartella **Sauron**, situata nella directory condivisa **LaTerraDiMezzo**, sono presenti due file eseguibili:

- **palantir.exe** – File creato manualmente, configurato per essere **eseguibile da tutti gli utenti**, indipendentemente dal gruppo di appartenenza.

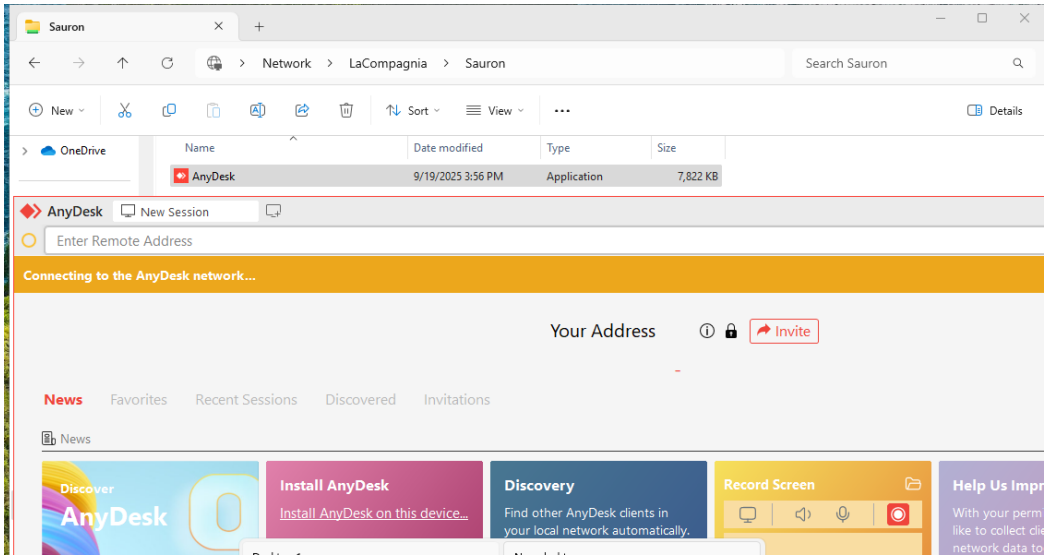


- **anydesk.exe** – File con accesso **limitato esclusivamente all'utente Gandalf**, grazie a una configurazione mirata dei permessi NTFS.

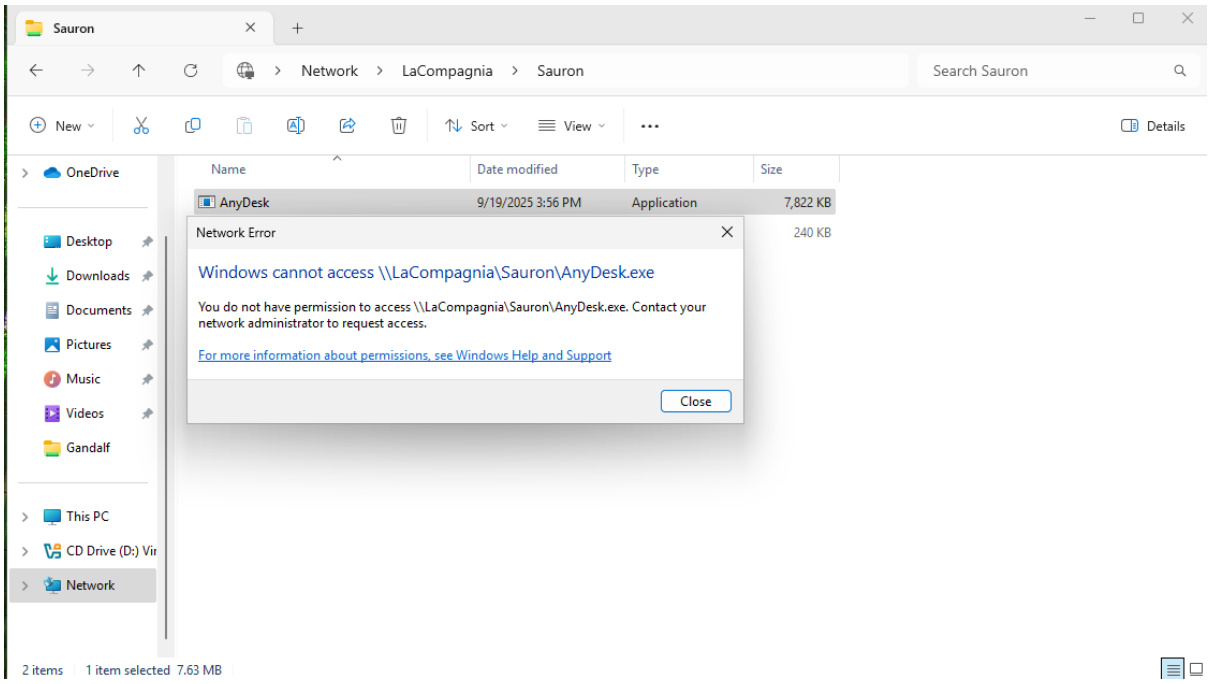


Verifica permessi eseguibili

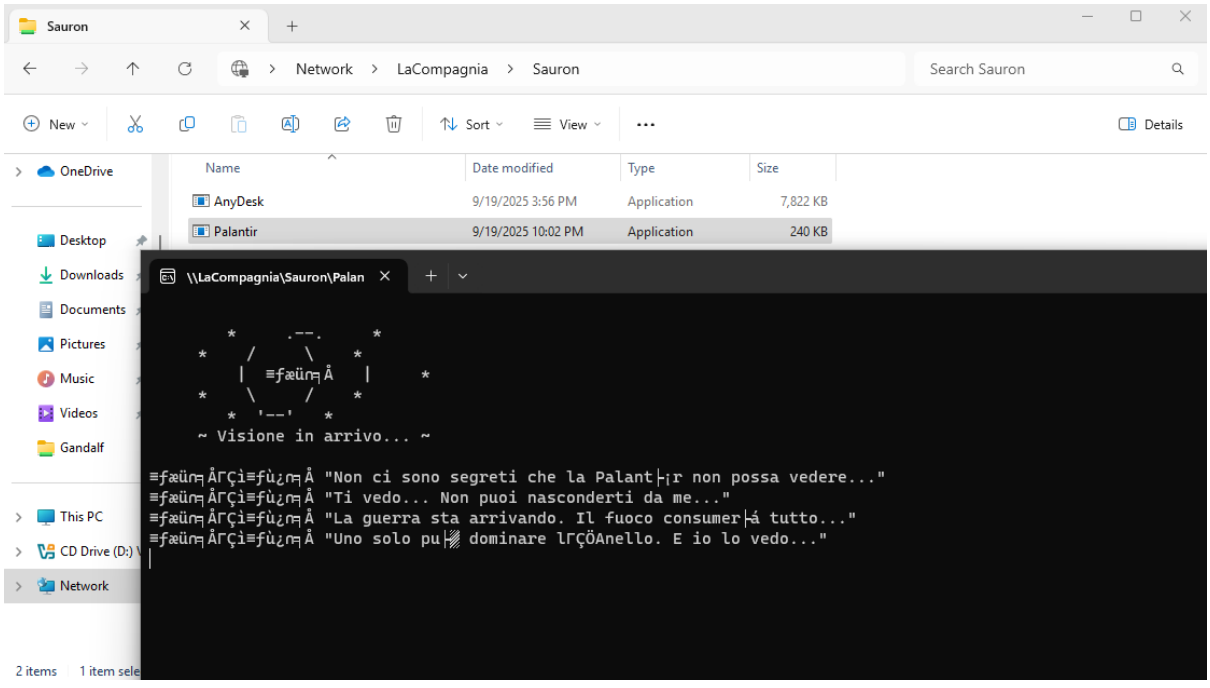
Dopo aver effettuato il login dalla macchina client provo ad aprire dalla cartella **Sauron** il file.exe di **anydesk** con l'utente **Gandalf** e questo infatti può aprirlo senza problemi



Successivamente provo ad avviarlo con l'utente **Sam** che, come da permessi, non può aprire il file.exe

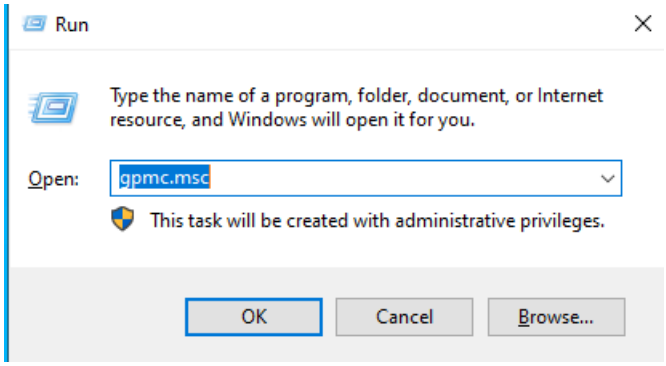


Mentre, come da permessi, potrà aprire il file **palantir.exe**

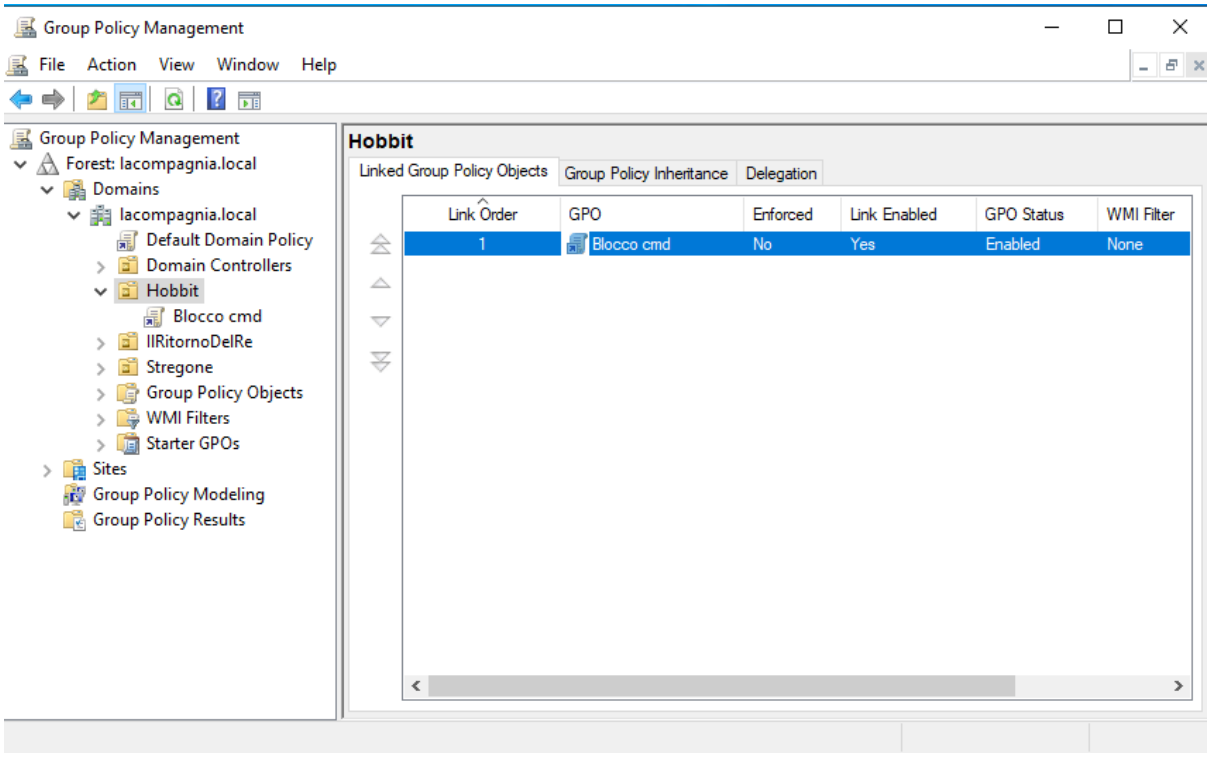


Creazione permessi di autorizzazioni di sistema

Iniziamo con l'apertura del Group Policy Management con Windows+R e il comando seguente

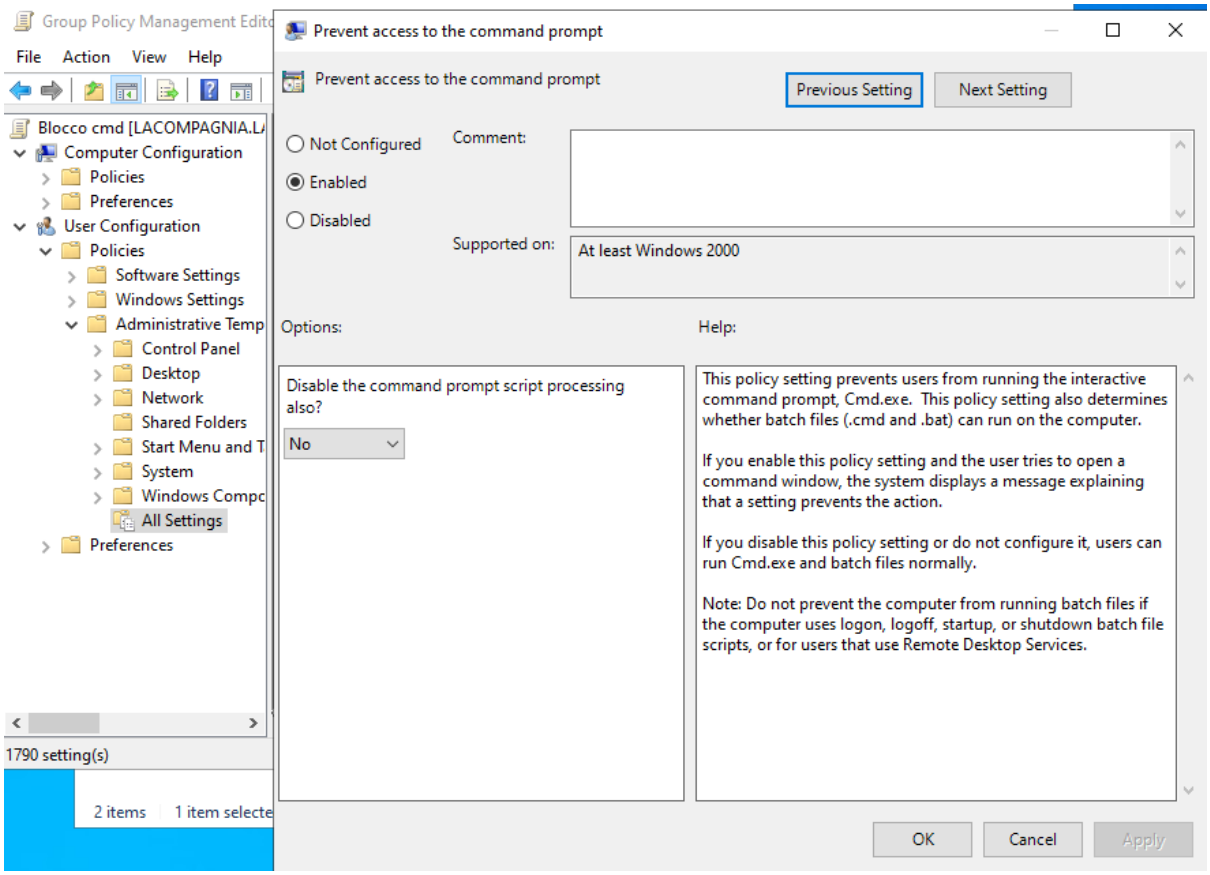


Arrivo al percorso dove sono presenti le **OU** per cui voglio settare la nuova GPO (Group Policy Object), nel nostro caso si tratta delle OU **Hobbit, IlRitornoDelRe,** vediamo il percorso seguito nello screen seguente. Creo inoltre il nuovo **GPO** dal nome "Blocco cmd"



Abbiamo editato il nuovo **GPO** e dopo aver seguito il percorso nella foto seguente troviamo la locazione dell'opzione **Prevent access to the command prompt.**

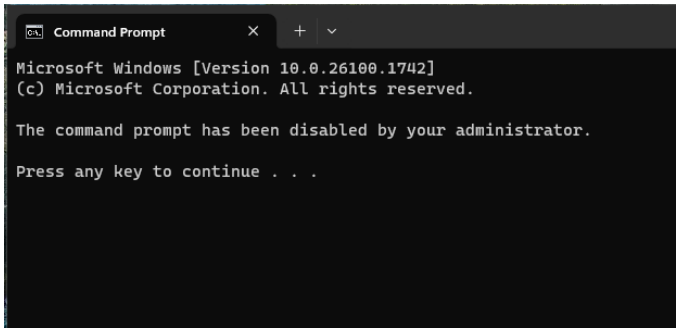
Abbiamo aperto i settings e l'abbiamo configurato come "enabled" che in questo caso disabiliterà il command prompt per l'utente selezionato.



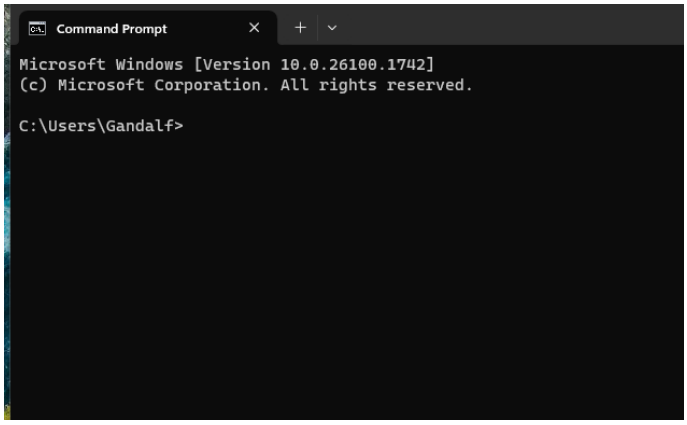
Verifica permessi di autorizzazioni di sistema

Effettuiamo un test di accesso con l'utente **Legolas**, appartenente all'Organizational Unit **IlRitornoDelRe**, sulla quale è stata precedentemente applicata la **Group Policy "Blocca cmd"**.

Come previsto, al tentativo di eseguire il prompt dei comandi (**cmd.exe**), il sistema ne impedisce l'esecuzione, confermando che la **GPO è correttamente applicata** e attiva per l'utente in questione.



Effettuando l'accesso con l'utente **Gandalf**, che **non è soggetto alla GPO "Blocca cmd"**, l'esecuzione del **cmd.exe** avviene regolarmente, come da comportamento predefinito del sistema.



Conclusioni

L’esercizio ha dimostrato con efficacia la capacità di progettare, configurare e documentare un’infrastruttura Active Directory tematica, mantenendo al tempo stesso rigore tecnico e coerenza funzionale.

Obiettivi raggiunti:

- Creazione di **Organizational Units** ispirate al mondo fantasy, con utenti e gruppi coerenti con la narrazione.
- Configurazione di **cartelle condivise** con permessi NTFS e di condivisione granulari, assegnati in base ai ruoli definiti.
- Verifica dell’accesso alle risorse da parte di utenti appartenenti a gruppi autorizzati e non autorizzati.
- Implementazione e test di **Group Policy Objects (GPO)** mirate, come il blocco del prompt dei comandi.
- Gestione differenziata dei **file eseguibili**, con restrizioni di esecuzione basate su utenti e gruppi.

L’intera struttura riflette una **logica di sicurezza ben definita**, dove ogni risorsa è protetta da regole chiare e verificabili. L’approccio narrativo ha reso la documentazione più coinvolgente, facilitando la comprensione e la memorizzazione dei concetti.

Questo esercizio rappresenta un ottimo esempio di come sia possibile **unire creatività e competenza sistemistica**, trasformando un ambiente tecnico in un regno digitale ordinato, sicuro e narrativamente coerente.