

Creazione e gestione di gruppi sul Server

Michele Storelli

6 Giugno 2025

Obiettivo dell'Esercizio

L'obiettivo di questo esercizio è implementare la gestione dei gruppi utenti in Windows Server 2022, creando un ambiente tematico ispirato al "Signore degli Anelli" per familiarizzare con la creazione di gruppi, l'assegnazione di permessi specifici e la comprensione della loro importanza per la sicurezza e l'amministrazione del sistema. Questo report descrive i passaggi eseguiti per la rinominazione del server, l'installazione di un nuovo dominio Active Directory, la configurazione iniziale di unità organizzative (OU), gruppi di sicurezza e utenti, la gestione dei permessi su file e cartelle, la configurazione dei criteri di restrizione software per programmi specifici, e infine la verifica delle politiche implementate su un client aggiunto al dominio.

1 Rinominazione del Server a TerraDiMezzo

Il primo passo fondamentale per stabilire la nostra infrastruttura di dominio è stato assegnare al server un nome appropriato e significativo. Il server Windows Server 2022, inizialmente con un nome generato automaticamente, è stato rinominato in **TerraDiMezzo**.

Passaggi per rinominare il server:

1. Accesso al server Windows Server 2022 con un account avente permessi amministrativi.
2. Apertura del *Server Manager*.
3. Nel pannello di sinistra, selezione di **Server locale (Local Server)**.
4. Individuazione della sezione "Nome computer". Il nome predefinito del computer era "WIN-P5RNF8F6I72P".
5. Clic sulla voce del nome del computer per aprire la finestra "Proprietà del sistema".
6. Nella scheda **Nome computer (Computer Name)**, clic sul pulsante **Modifica (Change)**.
7. Nel campo "Nome computer", è stato digitato il nuovo nome: **TerraDiMezzo**.

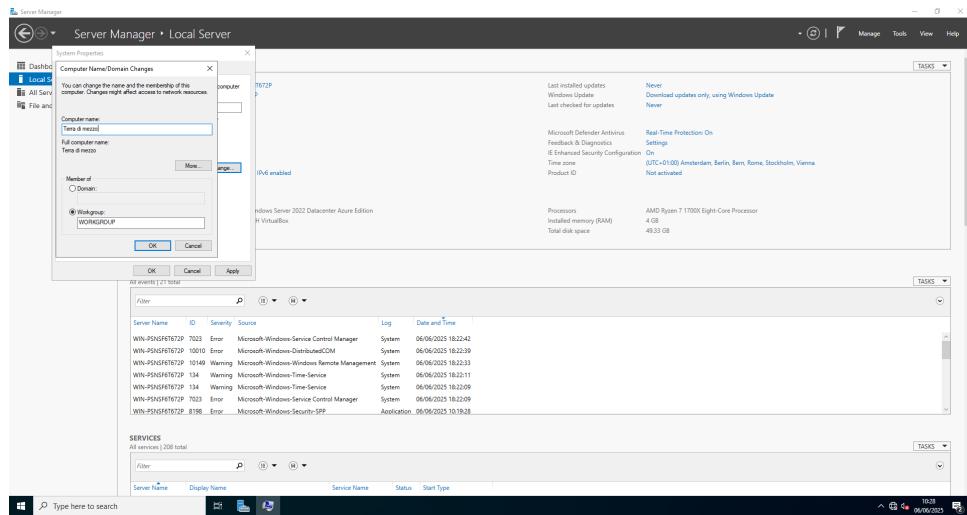


Figure 1: Interfaccia per la rinominazione del computer a TerraDiMezzo.

8. Conferma delle modifiche cliccando **OK** in tutte le finestre aperte. Il server ha richiesto un riavvio per applicare il nuovo nome, operazione eseguita cliccando **Riavvia ora (Restart Now)**.

Una volta riavviato, il server ha risposto correttamente al nome di **TerraDiMezzo**, confermando il successo dell'operazione.

2 Creazione della Foresta Fangorn.local e Installazione di Active Directory Domain Services (AD DS)

Ora che il server si chiama **TerraDiMezzo**, il passo successivo è stato stabilire il cuore del nostro ambiente di gestione utenti: la creazione della foresta **Fangorn.local** e l'installazione dei Servizi di Dominio Active Directory (AD DS).

Passaggi per l'installazione di AD DS:

1. Accesso al server **TerraDiMezzo** (Windows Server 2022) con un account che ha i permessi amministrativi.
2. Apertura del *Server Manager*.
3. Clic su **Aggiungi ruoli e funzionalità** (**Add Roles and Features**).
4. Scelta del tipo di installazione: **Installazione basata su ruoli o su funzionalità** (**Role-based or feature-based installation**).
5. Selezione di **TerraDiMezzo** come server di destinazione.
6. Nella lista dei ruoli server, selezione di **Servizi di dominio Active Directory** (**Active Directory Domain Services**). Quando richiesto di aggiungere le funzionalità necessarie per AD DS, si è cliccato su **Aggiungi funzionalità** (**Add Features**).

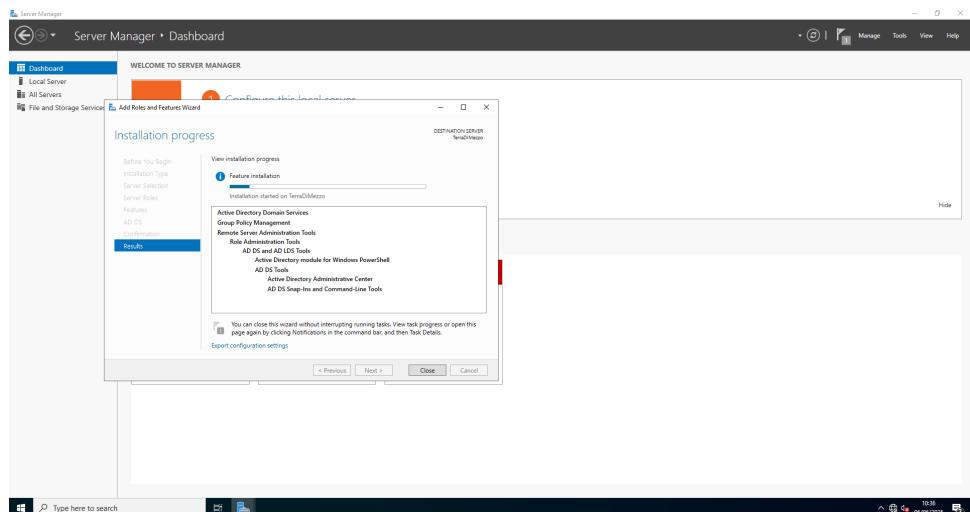


Figure 2: Installazione dei Servizi di dominio Active Directory (AD DS).

7. Dopo l'installazione delle funzionalità, è stato cliccato sul link **Promuovi questo server a controller di dominio** (**Promote this server to a domain controller**).
8. Configurazione della distribuzione:
 - È stata selezionata l'opzione **Aggiungi una nuova foresta** (**Add a new forest**).
 - Nel campo **Nome dominio radice** (**Root domain name**), è stato digitato **Fangorn.local**.
9. Configurazione delle opzioni del controller di dominio, inclusi il livello di funzionalità della foresta e del dominio, e l'impostazione di una password per la modalità ripristino servizi directory (DSRM).
10. Dopo aver rivisto il riepilogo delle selezioni e superato i controlli dei prerequisiti, si è avviata l'installazione.
11. Al termine dell'installazione, il server si è riavviato automaticamente, presentando la schermata di login del dominio **FANGORN\Administrator**.

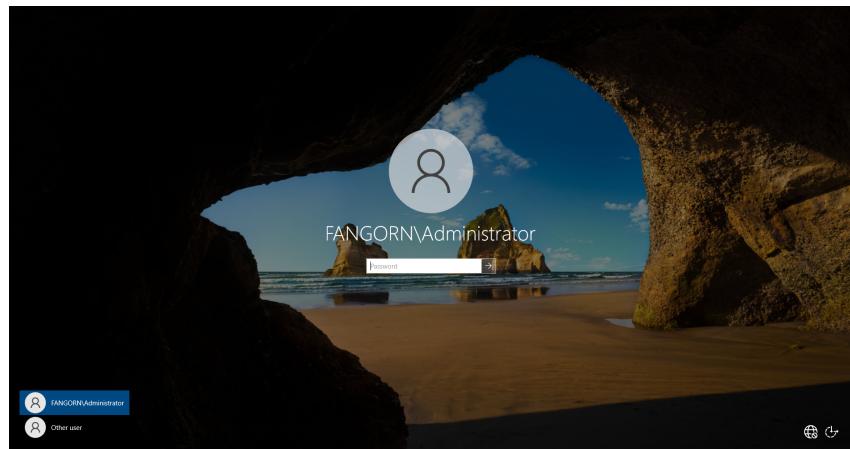


Figure 3: Schermata di login del dominio FANGORN dopo l'installazione di AD DS.

Il server **TerraDiMezzo** è ora configurato come Domain Controller per la foresta **Fangorn.local**, pronto per la gestione di utenti e gruppi.

3 Creazione di Unità Organizzative (OU), Gruppi e Utenti

Con la foresta **Fangorn.local** operativa, si è proceduto alla creazione delle Unità Organizzative (OU), seguite dalla creazione dei gruppi di sicurezza al loro interno e infine degli utenti, assegnando questi ultimi ai rispettivi gruppi, riflettendo la gerarchia e la divisione di responsabilità nella Terra di Mezzo.

Creazione delle Unità Organizzative (OU) e dei Gruppi di Sicurezza:

1. Apertura del *Server Manager* e selezione di **Utenti e computer di Active Directory (Active Directory Users and Computers)** dal menu **Strumenti (Tools)**.
2. Espansione del dominio **Fangorn.local** nel riquadro di navigazione sinistro.
3. Clic con il tasto destro sul dominio **Fangorn.local**, selezione di **Nuovo (New)** e poi **Unità Organizzativa (Organizational Unit)**.
4. Sono state create le seguenti OU:
 - **La_Compagnia_dell_Anello**
 - **Le_Forse_di_Mordor**
5. All'interno di ciascuna OU, sono stati creati i seguenti gruppi di sicurezza (ambito globale):
 - Nella OU **La_Compagnia_dell_Anello**: **Portatore_dell_Anello**

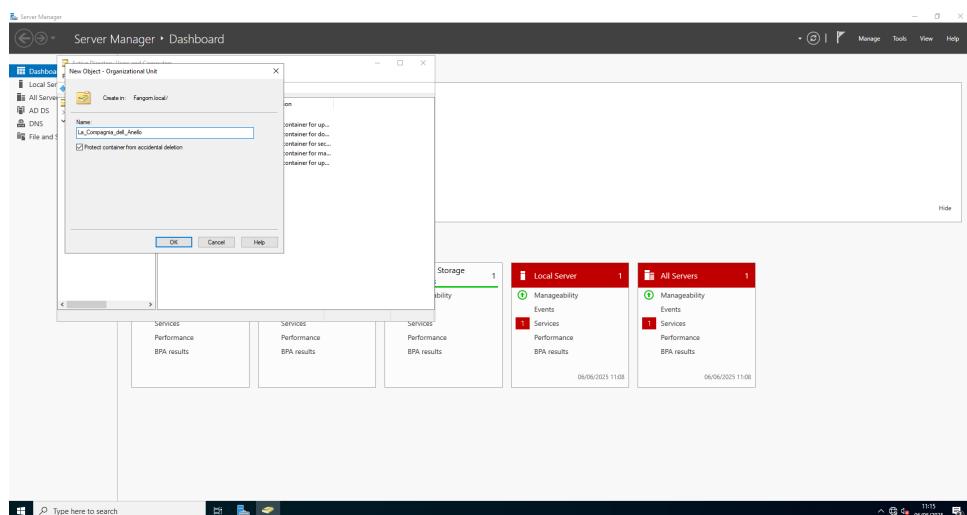


Figure 4: Creazione della OU **La_Compagnia_dell_Anello**.

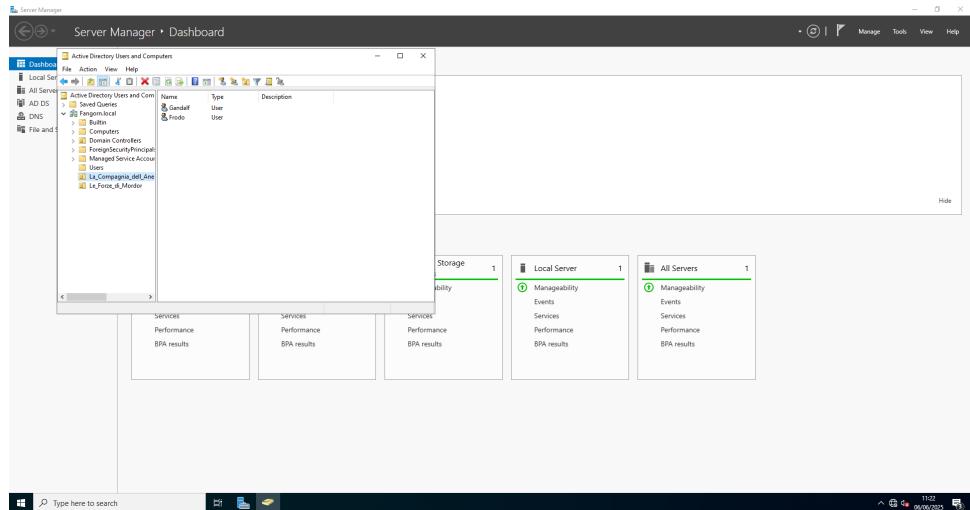


Figure 5: Gruppo di sicurezza Portatore_dell_Anello all'interno della OU La_Compagnia_dell_Anello.

- Nella OU Le_Force_di_Mordor: Cacciatori_dell_Anello

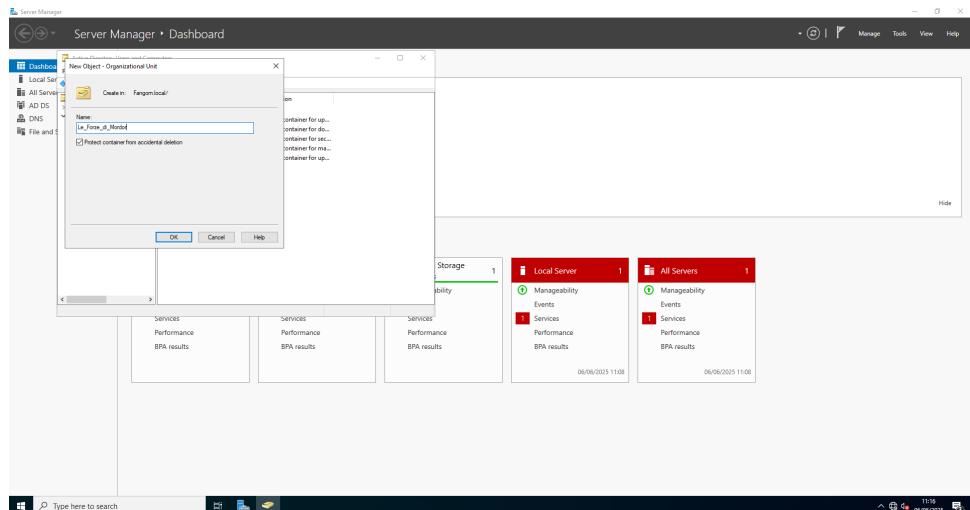


Figure 6: Creazione della OU Le_Force_di_Mordor.

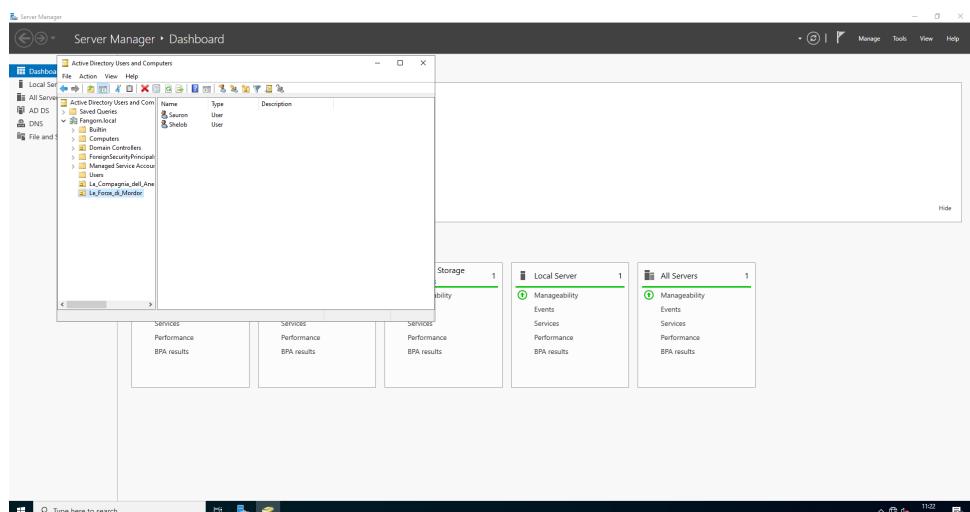


Figure 7: Gruppo di sicurezza Cacciatori_dell_Anello all'interno della OU Le_Force_di_Mordor.

Creazione e Aggiunta degli Utenti ai Gruppi:

1. In ADUC, all'interno delle rispettive OU, creazione degli utenti di prova:

- Nella OU **La_Compagnia_dell_Anello**: **Gandalf**, **Frodo**
- Nella OU **Le_Forse_di_Mordor**: **Sauron**, **Shelob**

Ogni utente è stato creato con un nome di accesso utente nel formato **utente@Fangorn.local** e una password.

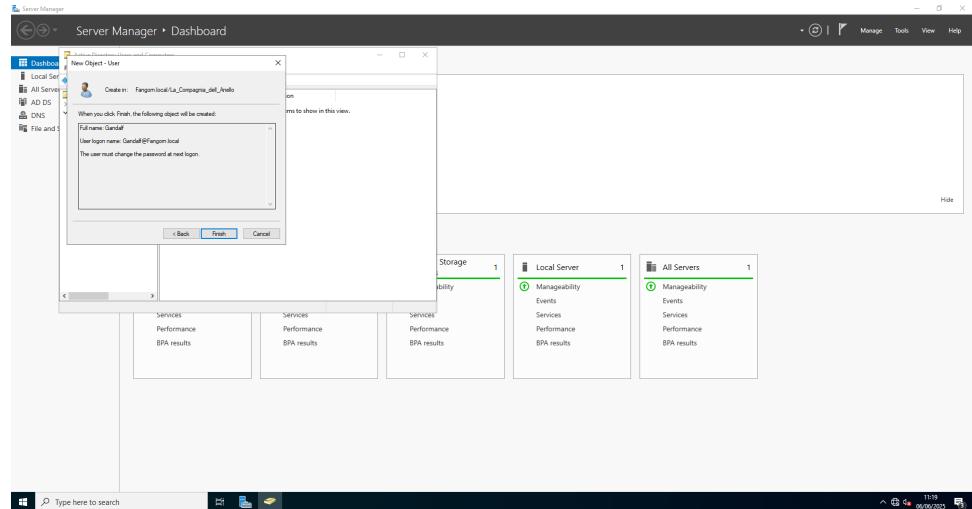


Figure 8: Creazione dell'utente Gandalf.

2. Aggiunta degli utenti ai rispettivi gruppi di sicurezza:

- Gli utenti **Gandalf** e **Frodo** sono stati aggiunti al gruppo **Portatore_dell_Anello**.

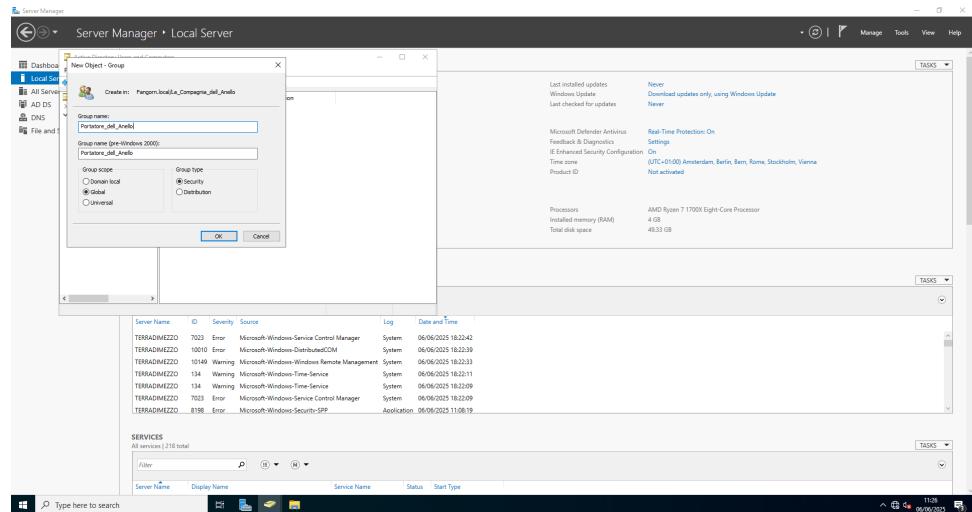


Figure 9: Proprietà del gruppo **Portatore_dell_Anello** che mostra l'aggiunta di utenti.

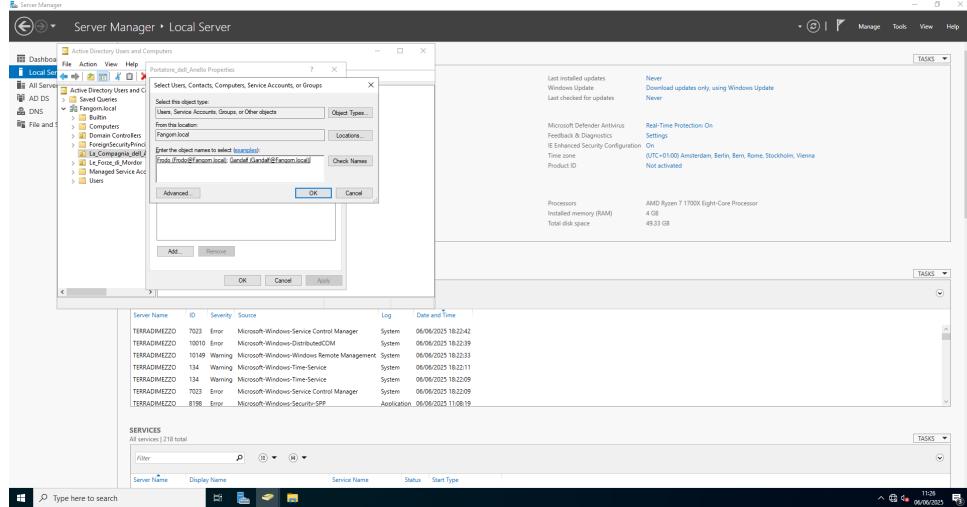


Figure 10: Aggiunta di Frodo e Gandalf al gruppo Portatore_dell_Anello.

- Gli utenti Sauron e Shelob sono stati aggiunti al gruppo Cacciatori_dell_Anello.

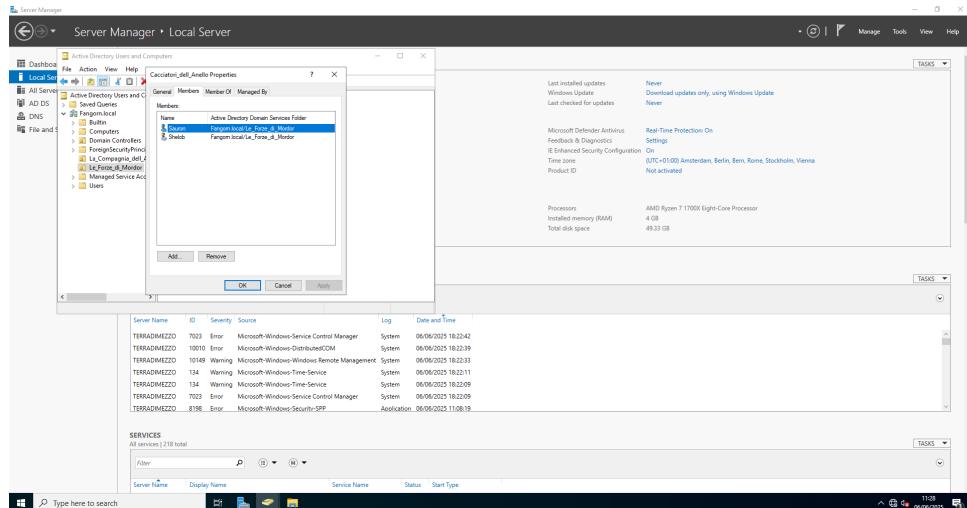


Figure 11: Membri del gruppo Cacciatori_dell_Anello (Sauron e Shelob).

Gli utenti sono ora correttamente assegnati ai rispettivi gruppi, stabilendo le basi per l'applicazione dei permessi.

4 Assegnazione dei Permessi su File e Cartelle

Per gestire l'accesso ai dati, sono state create due cartelle tematiche sul server e sono stati assegnati permessi specifici a ciascun gruppo.

Scenario:

- Creazione di una cartella C:\Unico_Anello, destinata a contenere informazioni cruciali per il gruppo Portatore_dell_Anello. Il gruppo Cacciatori_dell_Anello non avrà accesso a questa cartella.
- Creazione di una cartella C:\Covo_di_Shelob, destinata a ospitare i piani e le risorse del gruppo Cacciatori_dell_Anello. Il gruppo Portatore_dell_Anello non avrà accesso a questa cartella.

Passaggi per l'assegnazione dei permessi:

1. **Creazione delle Cartelle:** Le cartelle Unico_Anello e Covo_di_Shelob sono state create direttamente nella root del drive C:\ del server.

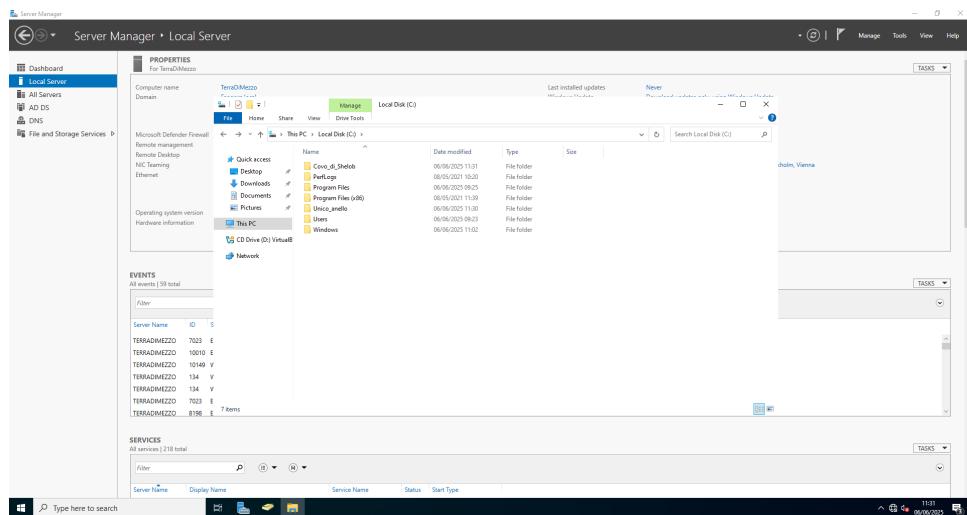


Figure 12: Cartelle create sul disco C: del server.

2. Configurazione Permessi per C:\Unico_Anello:

- Clic con il tasto destro sulla cartella Unico_Anello, selezione di **Proprietà (Properties)** e navigazione alla scheda **Sicurezza (Security)**.
- Clic su **Modifica (Edit)** e poi **Aggiungi (Add)**.
- È stato aggiunto il gruppo Portatore_dell_Anello.
- Sono stati assegnati i permessi di **Controllo completo (Full Control)** al gruppo Portatore_dell_Anello. Questo permette ai membri del gruppo di consultare, modificare e aggiungere informazioni vitali.
- Assicurarsi che il gruppo Cacciatori_dell_Anello non abbia permessi espliciti o ereditati che consentano l'accesso a questa cartella, oppure impostare un permesso di "Deny" se necessario per superare ereditarietà indesiderate.

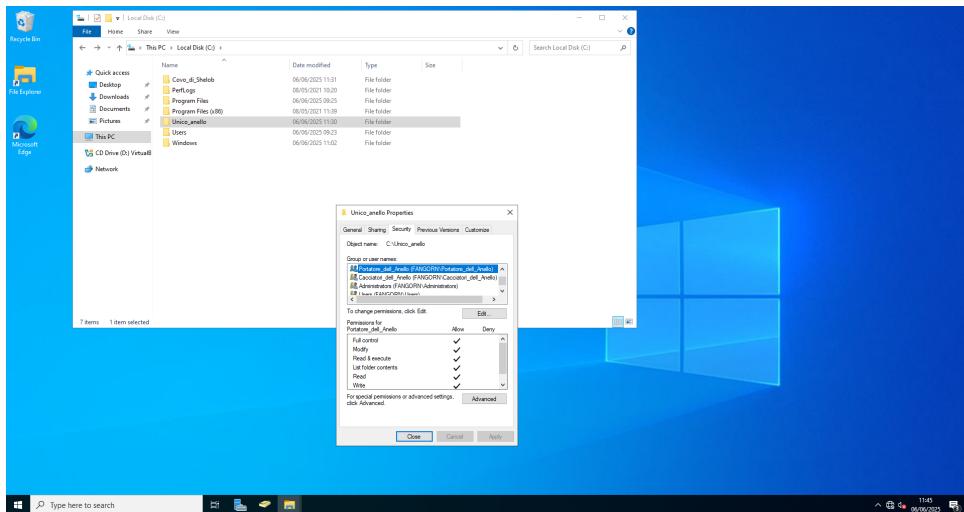


Figure 13: Permessi NTFS per il gruppo Portatore_dell_Anello sulla cartella Unico_Anello.

3. Configurazione Permessi per C:\Covo_di_Shelob:

- Operazione simile per la cartella Covo_di_Shelob.
- È stato aggiunto il gruppo Cacciatori_dell_Anello.
- È stato assegnato il permesso di **Controllo completo (Full Control)** al gruppo Cacciatori_dell_Anello. Questo garantisce a Sauron e ai suoi alleati il controllo totale sulle loro macchinazioni.
- Assicurarsi che il gruppo Portatore_dell_Anello **non** abbia permessi esplicativi o ereditati che consentano l'accesso a questa cartella.

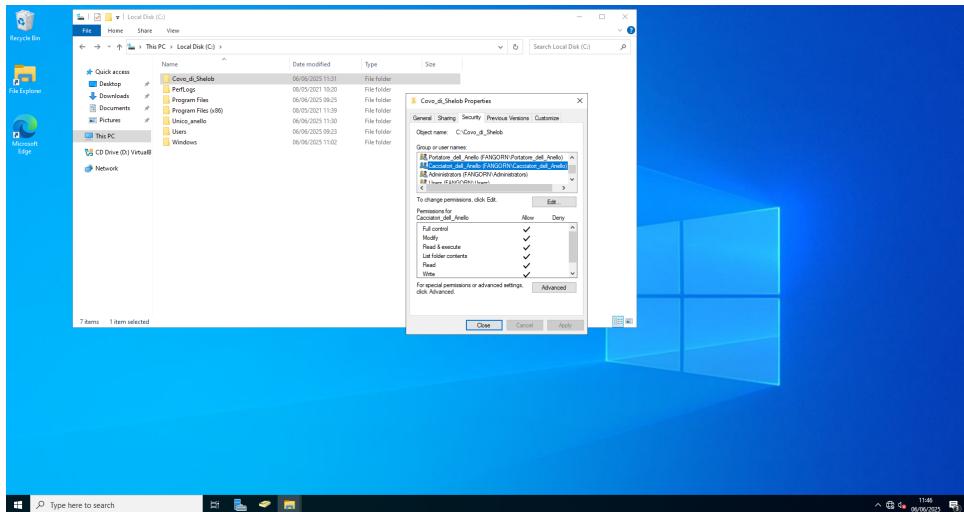


Figure 14: Permessi NTFS per il gruppo Cacciatori_dell_Anello sulla cartella Covo_di_Shelob.

Assegnazione di permessi per Accesso Remoto al server (RDP):

Per consentire al gruppo Portatore_dell_Anello di accedere al server **TerraDiMezzo** tramite Desktop Remoto:

1. Clic con il tasto destro su **Questo PC (This PC)** e selezione di **Proprietà (Properties)**.
2. Clic su **Impostazioni remote (Remote settings)** nel riquadro di sinistra.
3. Nella sezione "Desktop remoto", clic su **Seleziona utenti (Select Users)**.

4. È stato aggiunto il gruppo **Portatore_dell_Anello** agli utenti che possono accedere tramite Desktop Remoto.

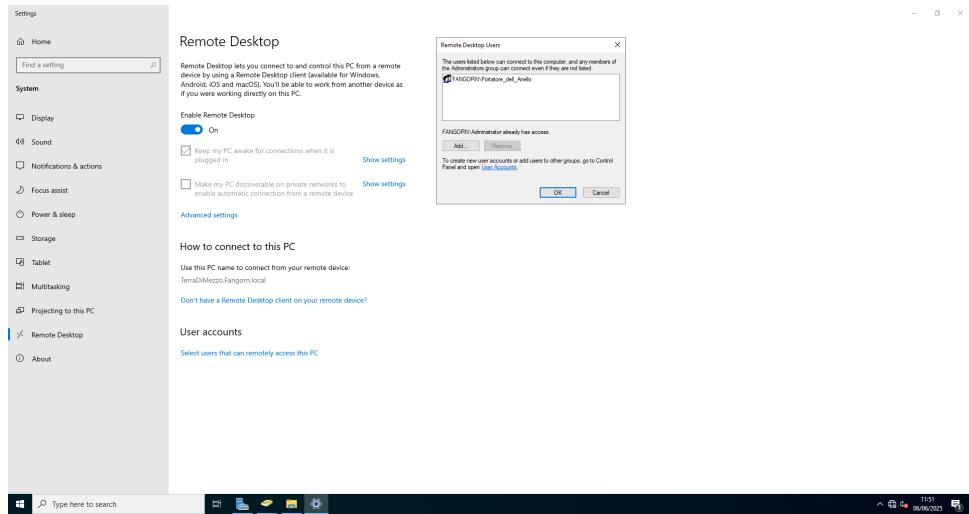


Figure 15: Configurazione degli utenti che possono accedere tramite Desktop Remoto.

Questo accesso remoto è cruciale per i membri del gruppo per coordinare le azioni e accedere alle risorse da lontano.

5 Gestione dei Permessi per Programmi Specifici (Criteri di Restrizione Software)

Per un controllo più granulare, sono stati configurati i Criteri di Restrizione Software (SRP) per limitare l'esecuzione di programmi a specifici gruppi.

Scenario:

- Solo il gruppo **Cacciatori_dell_Anello** può usare la **Calcolatrice (calc.exe)**. Il gruppo **Portatore_dell_Anello** non potrà usare la Calcolatrice.
- Solo il gruppo **Portatore_dell_Anello** può usare il **Blocco Note (notepad.exe)**. Il gruppo **Cacciatori_dell_Anello** non potrà usare il Blocco Note.

Passaggi per la configurazione dei Criteri di Restrizione Software (SRP):

1. Apertura di **Gestione Criteri di Gruppo (Group Policy Management)** dal *Server Manager*.
2. Creazione di due nuove GPO (Group Policy Object):
 - **Restrizioni_unico_anello**
 - **Restrizioni_terra_di_mezzo**
3. Collegamento delle GPO alle rispettive Unità Organizzative:
 - La GPO **Restrizioni_unico_anello** è stata collegata alla OU **La_Compagnia_dell_Anello**.
 - La GPO **Restrizioni_terra_di_mezzo** è stata collegata alla OU **Le_Forse_di_Mordor**.

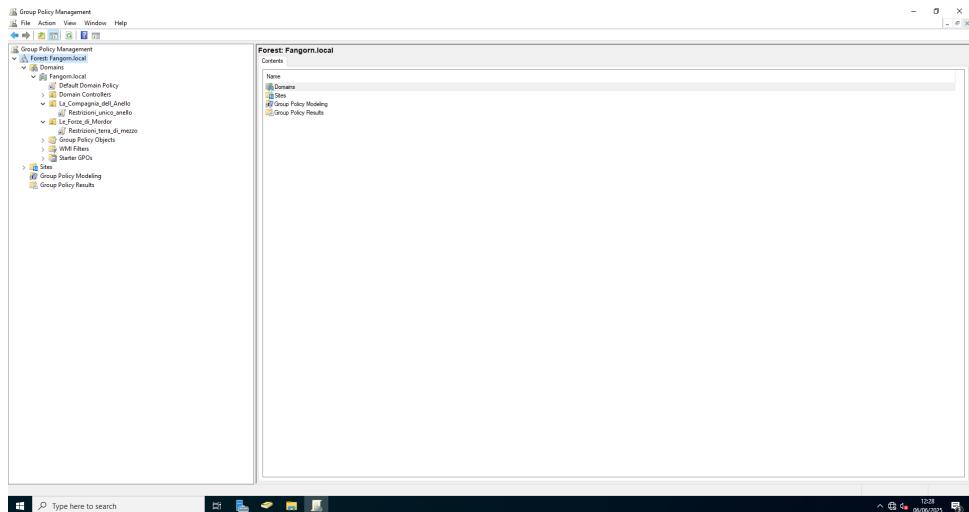


Figure 16: Esempio di GPO collegata al dominio Fangorn.local.

4. **Configurazione della GPO Restrizioni_unico_anello (per il gruppo Portatore dell'Anello):** Navigando in **Configurazione computer > Criteri > Impostazioni di Windows > Impostazioni di sicurezza > Criteri di restrizione software**, è stata impostata una **Regola Path** che impedisce l'esecuzione della Calcolatrice (calc.exe). Tutti gli altri programmi non esplicitamente bloccati da altre regole o consentiti, saranno eseguibili.

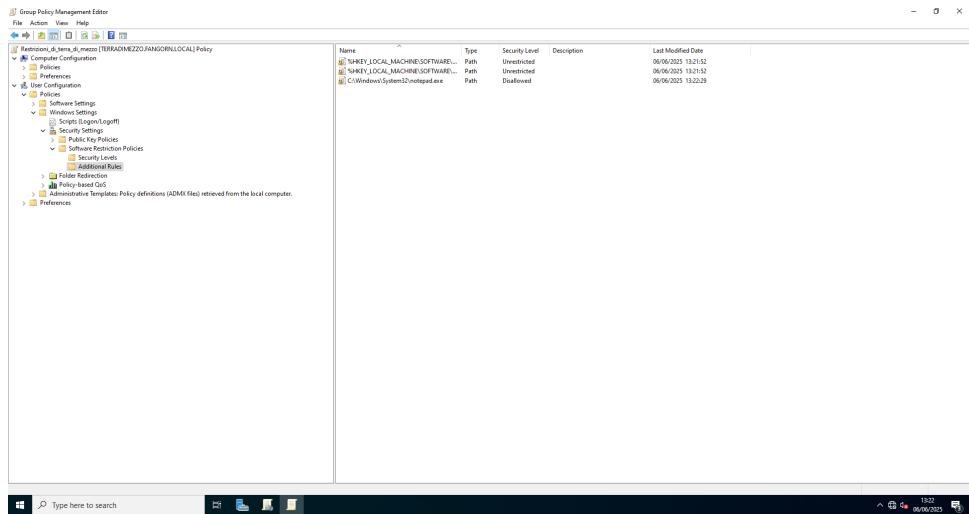


Figure 17: Regole SRP configurate per impedire l’uso della Calcolatrice (per il gruppo Portatore dell’Anello).

- 5. Configurazione della GPO Restrizioni_terra_di_mezzo (per il gruppo Cacciatori dell’Anello):**
 Similmente, in questa GPO, è stata impostata una **Regola Path** che impedisce l’esecuzione del Blocco Note (`notepad.exe`). Tutti gli altri programmi non esplicitamente bloccati da altre regole o consentiti, saranno eseguibili.

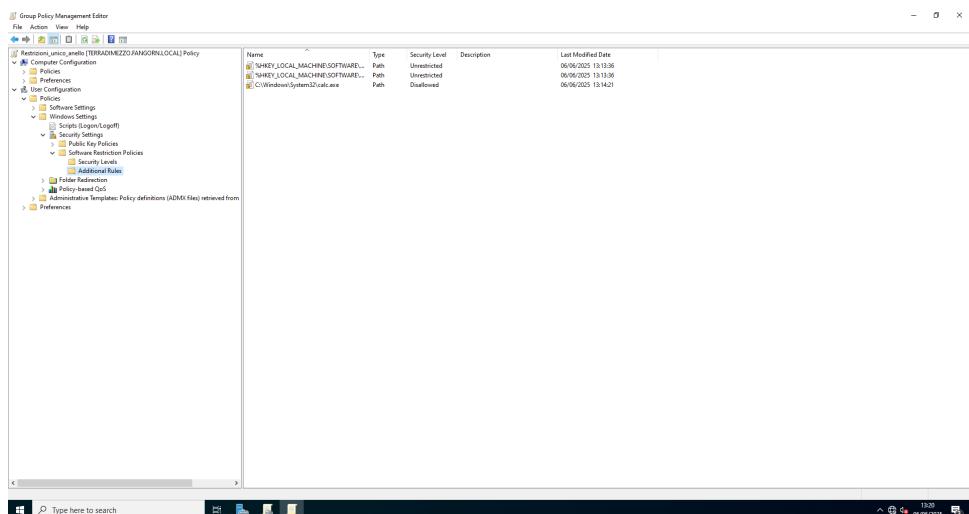


Figure 18: Regole SRP configurate per impedire l’uso del Blocco Note (per il gruppo Cacciatori dell’Anello).

Per l’applicazione immediata delle policy, è stato eseguito `gpupdate /force` sui computer client.

6 Unione di un Client al Dominio e Verifica dei Permessi

Per convalidare l'efficacia delle politiche implementate, un computer client con Windows 10 è stato aggiunto al dominio **Fangorn.local** e sono stati eseguiti test di accesso.

Passaggi per unire il client al dominio:

- Configurazione IP del Client:** L'indirizzo IP del client è stato impostato staticamente (es., 192.168.10.10), con il DNS primario puntato al server **TerraDiMezzo** (192.168.10.2).

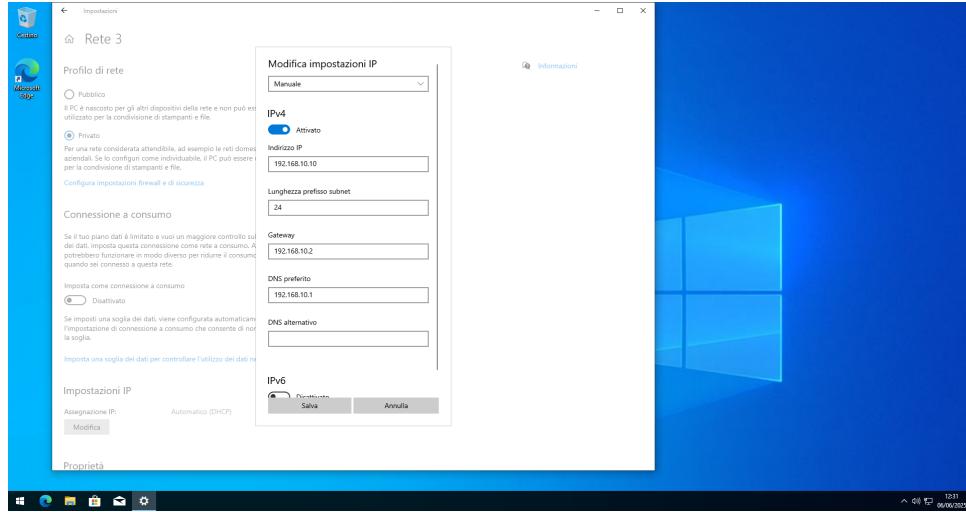


Figure 19: Configurazione IP del client Windows 10.

- Rinominazione e Unione al Dominio:** Il nome del computer client è stato modificato (es., in **Client1**) e unito al dominio **Fangorn.local**. Le credenziali di un account amministrativo del dominio sono state richieste e fornite.

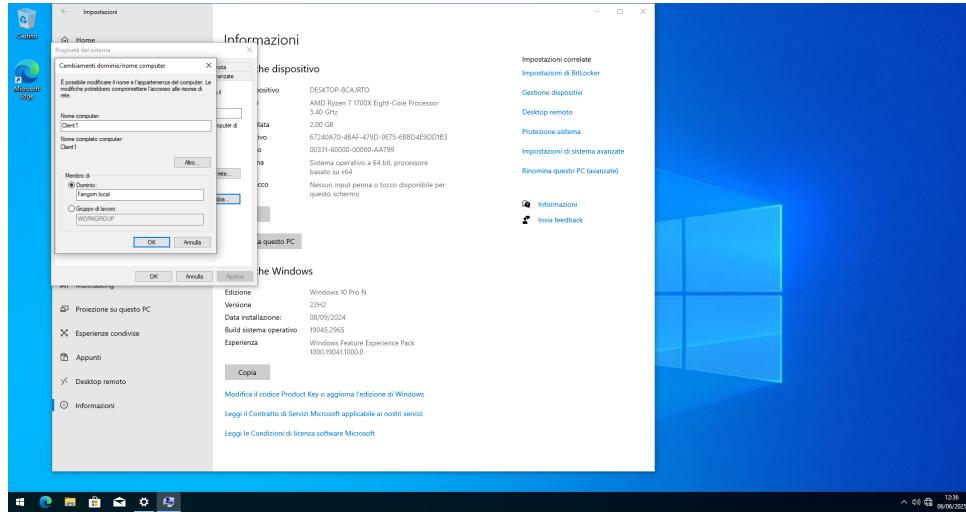


Figure 20: Interfaccia per unire il client al dominio **Fangorn.local**.

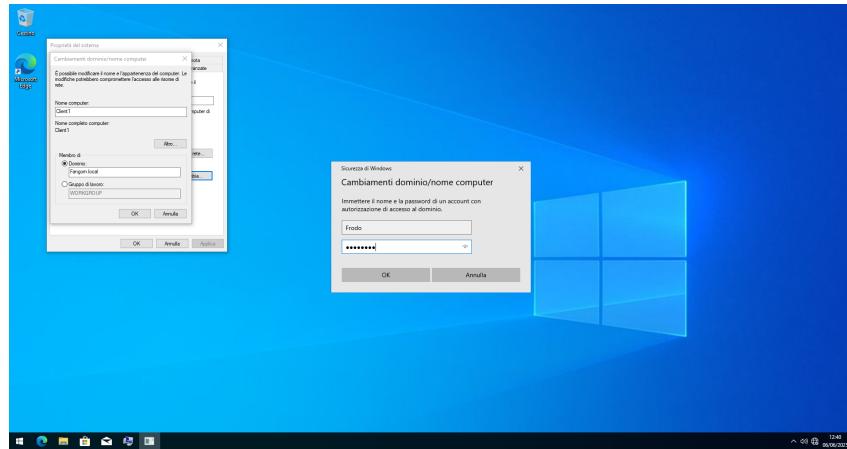


Figure 21: Richiesta delle credenziali di dominio per l'unione del client.

Il client è stato riavviato per completare l'unione al dominio.

Verifica dei permessi per l'utente Frodo (Membro del gruppo Portatore_dell_Anello):

1. Accesso sul client Windows 10 con l'account di dominio **Frodo**.
2. **Accesso a C:\Unico_Anello (Server)**: L'accesso alla cartella condivisa \\TerraDiMezzo\Unico_anello è stato consentito, permettendo a **Frodo** di visualizzare i contenuti e operare sui file.

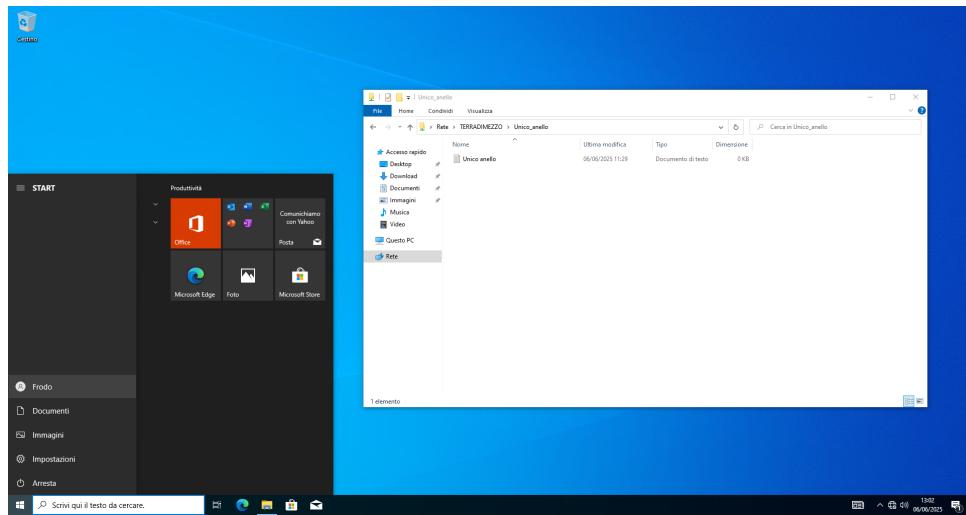


Figure 22: Accesso riuscito di Frodo alla cartella condivisa Unico_Anello.

3. **Accesso a C:\Covo_di_Shelob (Server)**: L'accesso alla cartella condivisa \\TerraDiMezzo\Covo_di_Shelob è stato negato, come previsto, confermando che il gruppo Portatore_dell_Anello non ha accesso a questa risorsa.

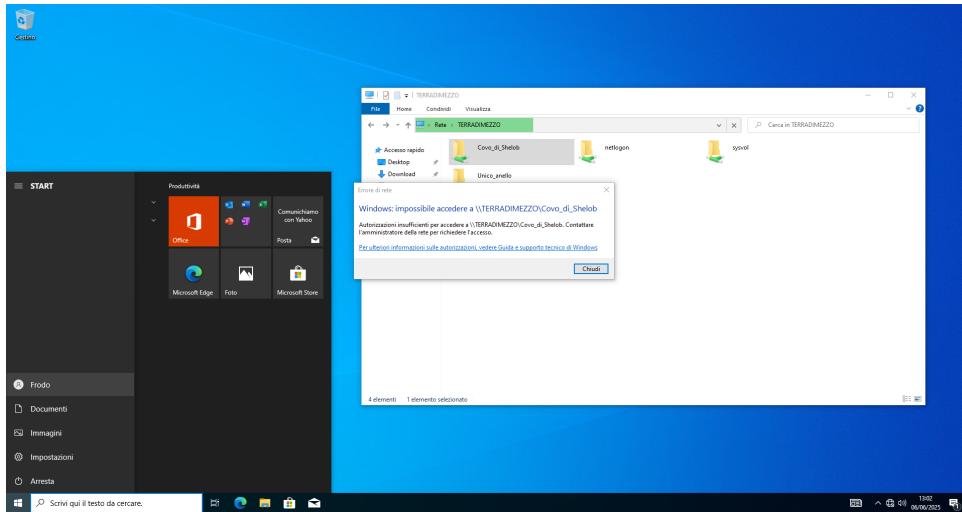


Figure 23: Accesso negato a Frodo per la cartella Covo_di_Shelob.

4. **Esecuzione del Blocco Note (notepad.exe) sul Client:** Il Blocco Note si è avviato correttamente.
5. **Esecuzione della Calcolatrice (calc.exe) sul Client:** L'esecuzione della Calcolatrice è stata bloccata dai Criteri di restrizione software, con un messaggio che indica che l'app è stata bloccata dall'amministratore di sistema.

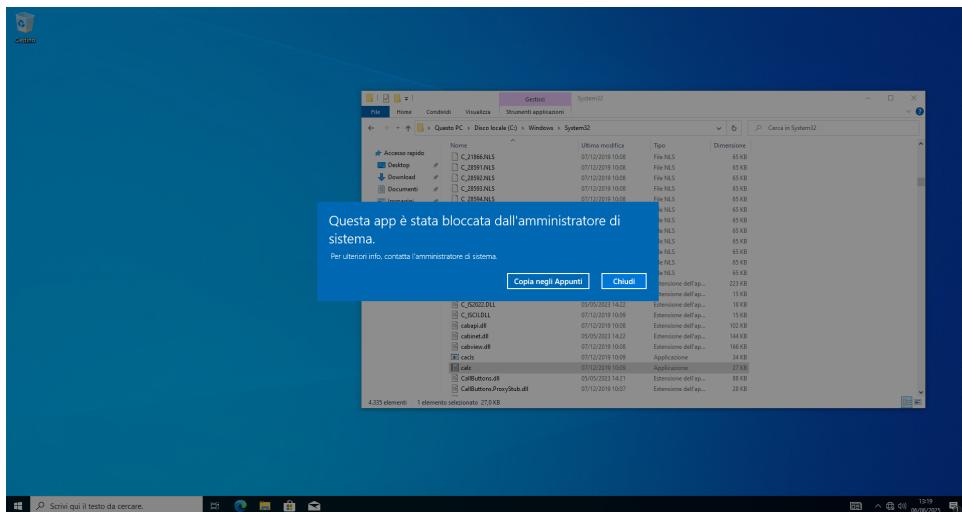


Figure 24: Blocco dell'esecuzione della Calcolatrice per Frodo.

Verifica dei permessi per l'utente Sauron (Membro del gruppo Cacciatori_dell_Anello):

1. Accesso sul client Windows 10 con l'account di dominio Sauron.

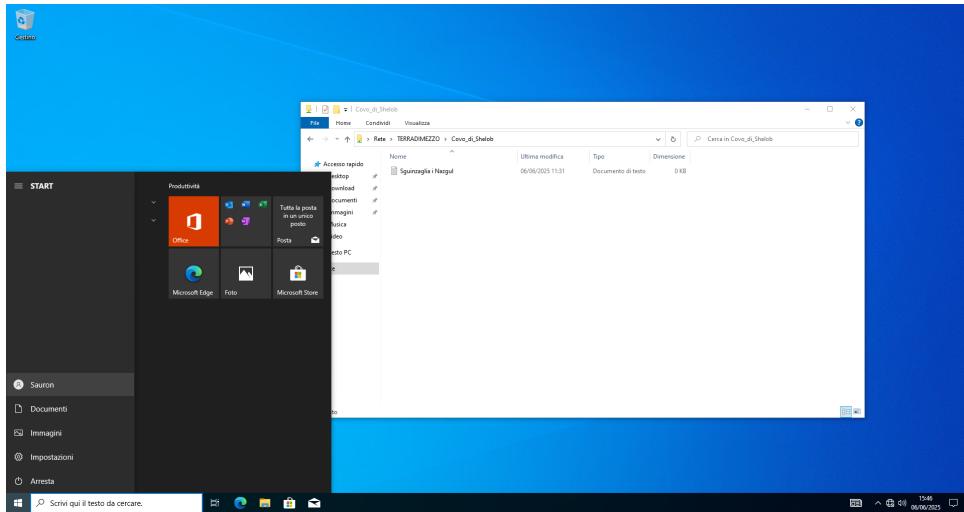


Figure 25: Desktop del client con l'utente Sauron loggato e accesso a Covo_di_Shelob.

2. **Accesso a C:\Covo_di_Shelob (Server):** L'accesso alla cartella condivisa \\TERRADIMEZZO\Covo_di_Shelob è stato consentito, permettendo a Sauron il pieno controllo.
3. **Accesso a C:\Unico_Anello (Server):** L'accesso alla cartella condivisa \\TERRADIMEZZO\Unico_Anello è stato negato, come previsto, confermando che il gruppo Cacciatori_dell_Anello non ha accesso a questa risorsa.

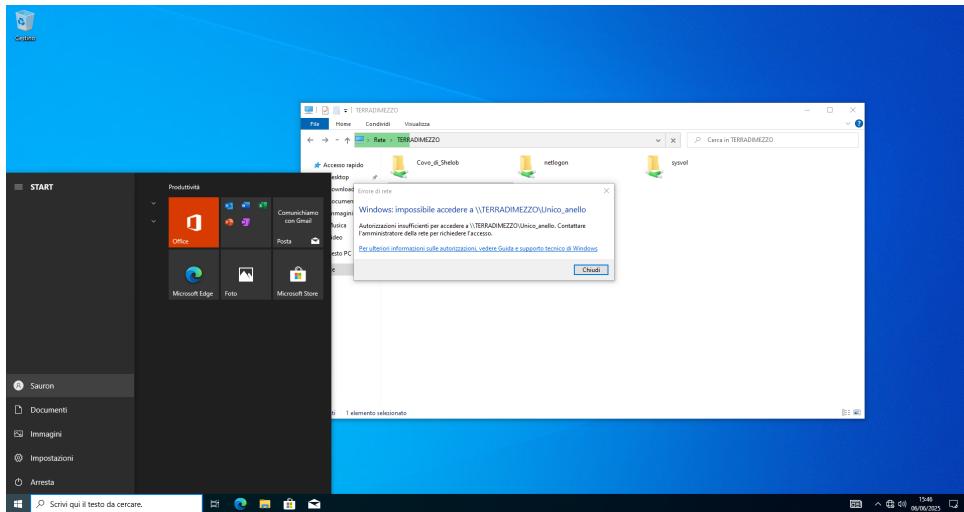


Figure 26: Accesso negato a Sauron per la cartella Unico_Anello.

4. **Esecuzione del Blocco Note (notepad.exe) sul Client:** L'esecuzione del Blocco Note è stata bloccata dai Criteri di restrizione software.
5. **Esecuzione della Calcolatrice (calc.exe) sul Client:** La Calcolatrice si è avviata correttamente.

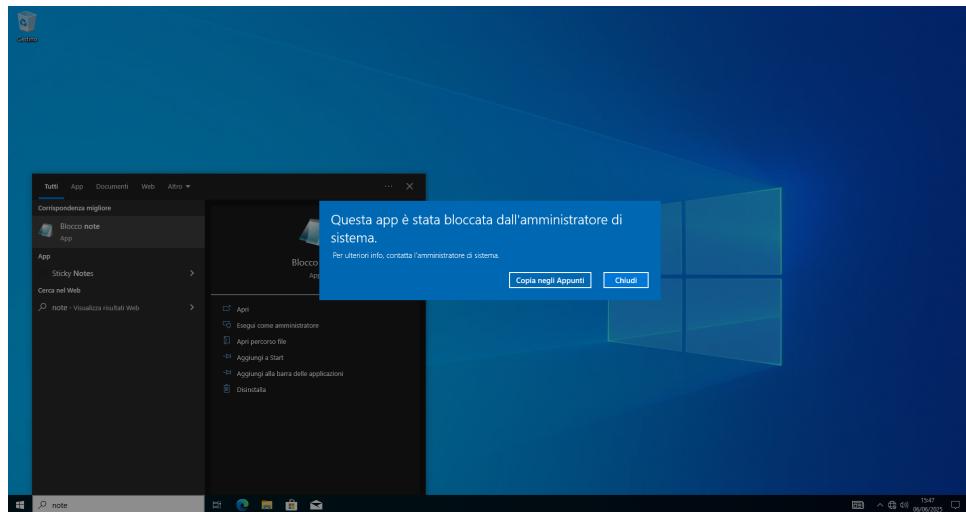


Figure 27: Blocco dell'esecuzione della Calcolatrice per Sauron.

7 Conclusioni

Questo esercizio ha dimostrato con successo l'implementazione e la gestione di un ambiente Active Directory su Windows Server 2022, caratterizzato da una struttura di unità organizzative, utenti e gruppi ispirata al "Signore degli Anelli". La configurazione ha incluso la rinominazione del server, l'installazione dei Servizi di Dominio Active Directory, la creazione di OU per `La_Compagnia_dell_Anello` e `Le_Forse_di_Mordor`, al cui interno sono stati creati i rispettivi gruppi di sicurezza (`Portatore_dell_Anello` e `Cacciatori_dell_Anello`) e gli utenti. È stata effettuata l'assegnazione granulare di permessi su file, cartelle e programmi tramite Criteri di Gruppo e Criteri di Restrizione Software.

Le verifiche condotte su un client unito al dominio hanno confermato che le politiche di sicurezza sono state applicate correttamente, garantendo che ciascun gruppo abbia accesso esclusivo alle risorse e agli strumenti necessari per le proprie attività. Questo controllo preciso è fondamentale per la sicurezza e l'efficienza di qualsiasi infrastruttura IT.