

Windows Server

1. Introduzione

L'obiettivo di questo esercizio è familiarizzare con la gestione dei gruppi di utenti in Windows Server 2022, creando gruppi, assegnando permessi specifici e verificando l'applicazione corretta delle autorizzazioni. Una gestione efficace dei gruppi consente di migliorare la sicurezza e l'amministrazione del sistema, riducendo il rischio di accessi non autorizzati e semplificando la gestione dei permessi.

2. Creazione e Configurazione dei Gruppi

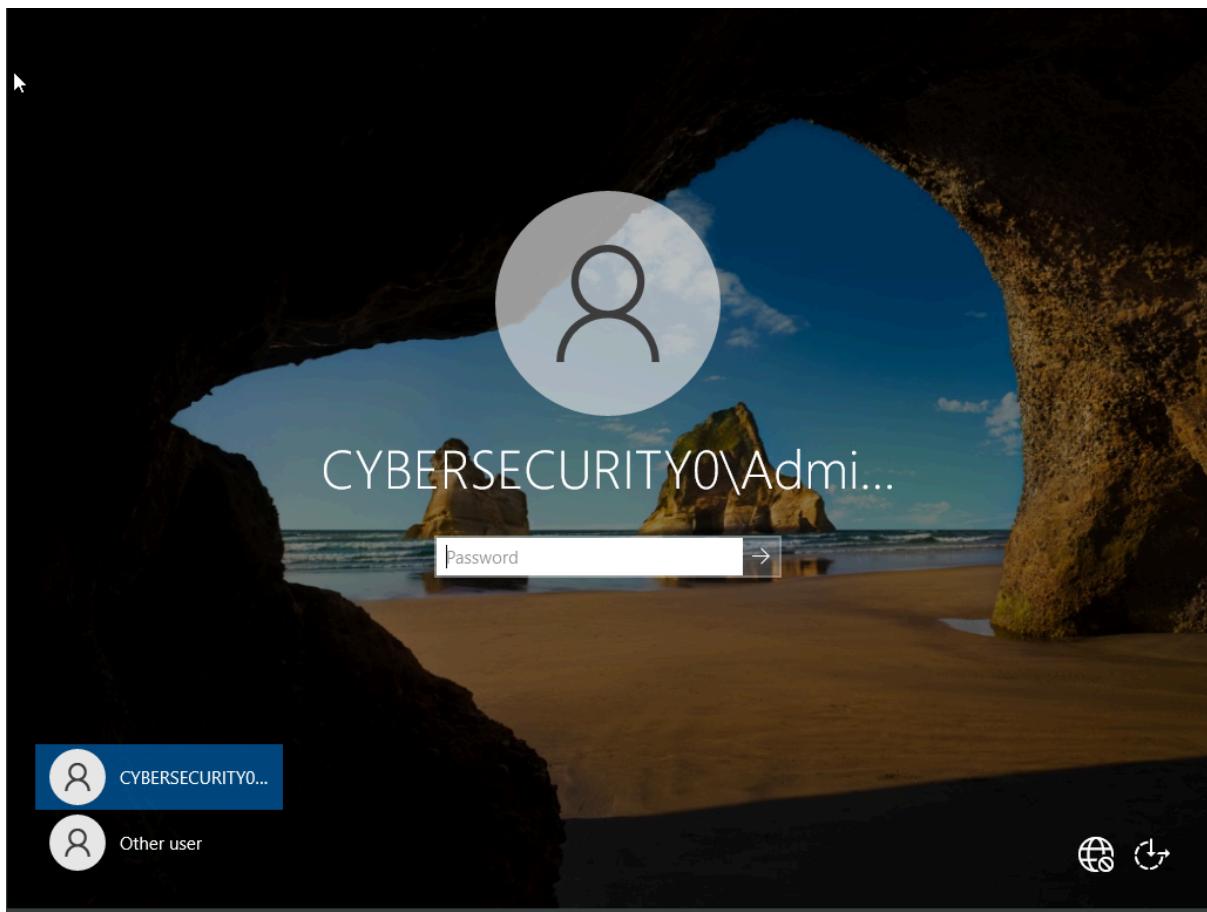
Sono stati creati i seguenti gruppi di utenti:

Falchidellanotte: Responsabili della gestione dell'infrastruttura IT. (Utenti: Simeone e Matteo)

HackerdiClasseB: Utenti con permessi limitati per l'utilizzo delle risorse aziendali. (Utenti: Sergio e Giuseppe)

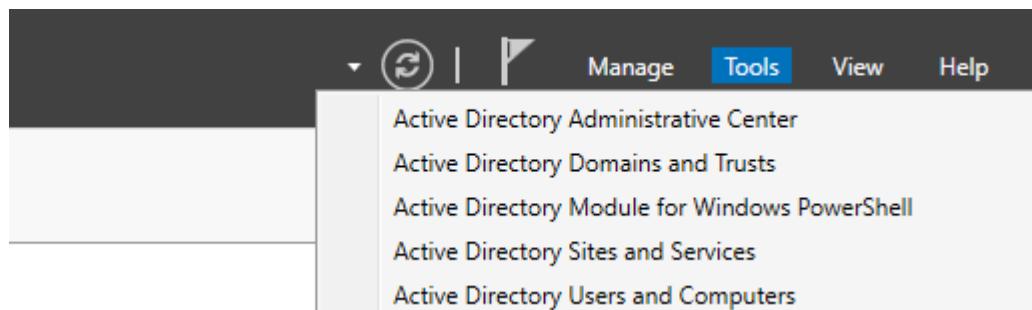
Passaggi seguiti:

Accedere a Windows Server 2022 con un account amministratore.



Aprire Server Manager.

Accedere a Tools > Active Directory Users and Computers.



Creare due nuove Unità Organizzative (OU): FalconLock e AntiHacker.

Creare gli utenti corrispondenti nelle rispettive OU:

FalconLock: Simeone e Matteo.

AntiHacker: Sergio e Giuseppe.

Creare due nuovi gruppi all'interno delle rispettive OU cliccando con il tasto destro sulla cartella New > Group.

Assegnare un nome significativo ai gruppi e aggiungere i membri corrispondenti:

Falchidellanotte → **FalconLock** (Simeone e Matteo).

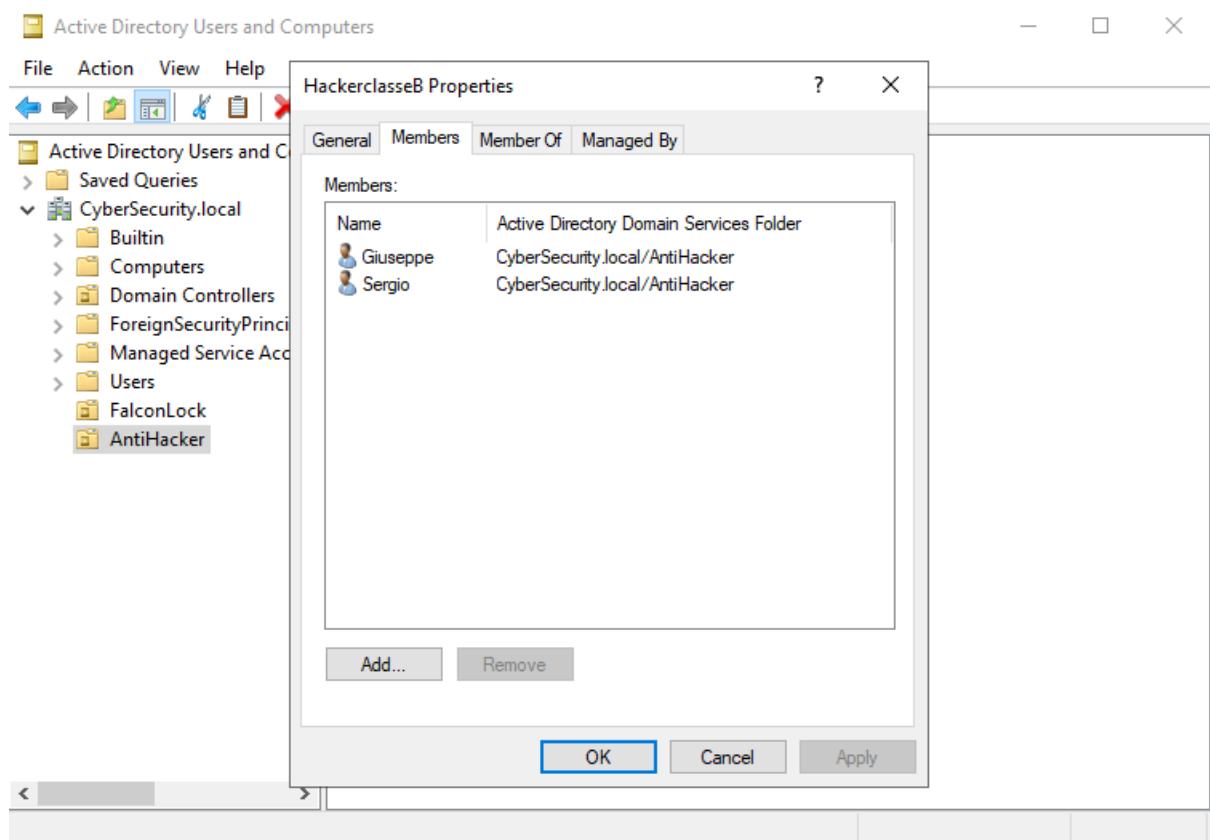
Hackerdi classeB → **AntiHacker** (Sergio e Giuseppe).

Confermare la creazione cliccando su "Crea".

The screenshot shows the Windows Active Directory Users and Computers (ADUC) management console. The title bar reads "Active Directory Users and Computers". The menu bar includes "File", "Action", "View", and "Help". Below the menu is a toolbar with various icons for navigation and management. The left pane displays a tree view of the Active Directory structure under "CyberSecurity.local", including "Builtin", "Computers", "Domain Controllers", "ForeignSecurityPrincipal!", "Managed Service Account", and "Users" folder. Within the "Users" folder, two groups are listed: "FalconLock" and "AntiHacker". The right pane is a table with columns "Name", "Type", and "Description". It shows one entry for the "FalconLock" group, which is a "Security Group..." type entry. Below the table, there is a message box with the text "Object created successfully." and a "Close" button.

Name	Type	Description
Falchidellan...	Security Group...	
Matteo	User	
Simeone	User	

Object created successfully.
Close



3. Assegnazione dei Permessi

Creazione delle Cartelle e Configurazione dei Permessi

Sono state create due cartelle con permessi differenziati:

Dati Super Segreti (accesso ristretto agli amministratori IT).

Dati Pubblici (accesso in sola lettura per utenti standard).

Permessi Assegnati:

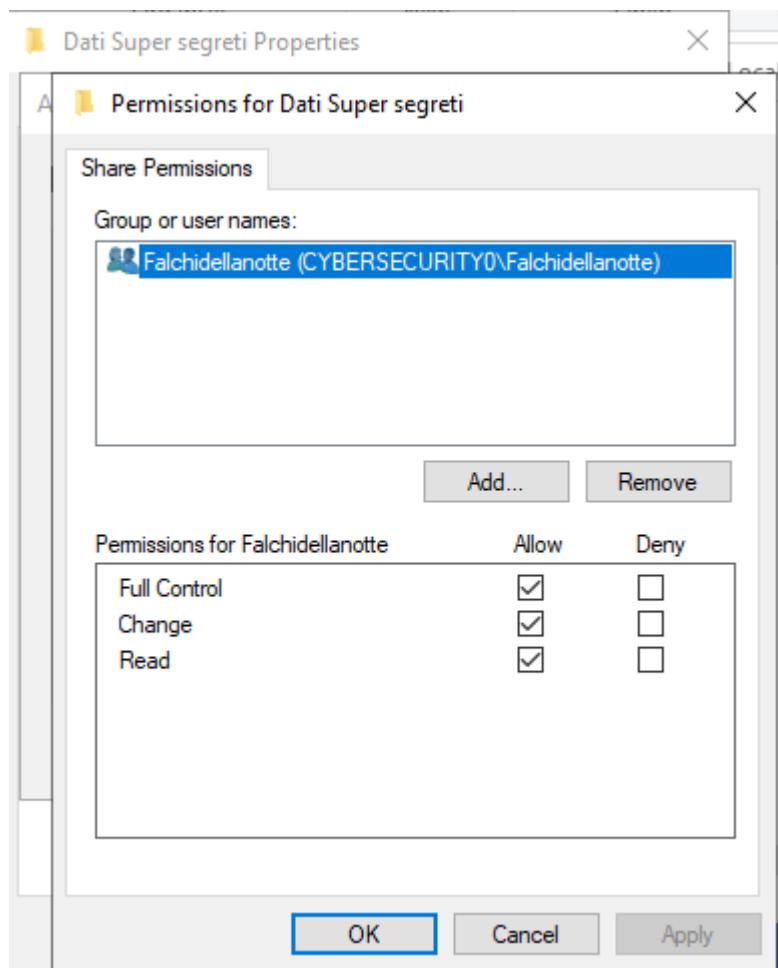
Falchidellanotte:

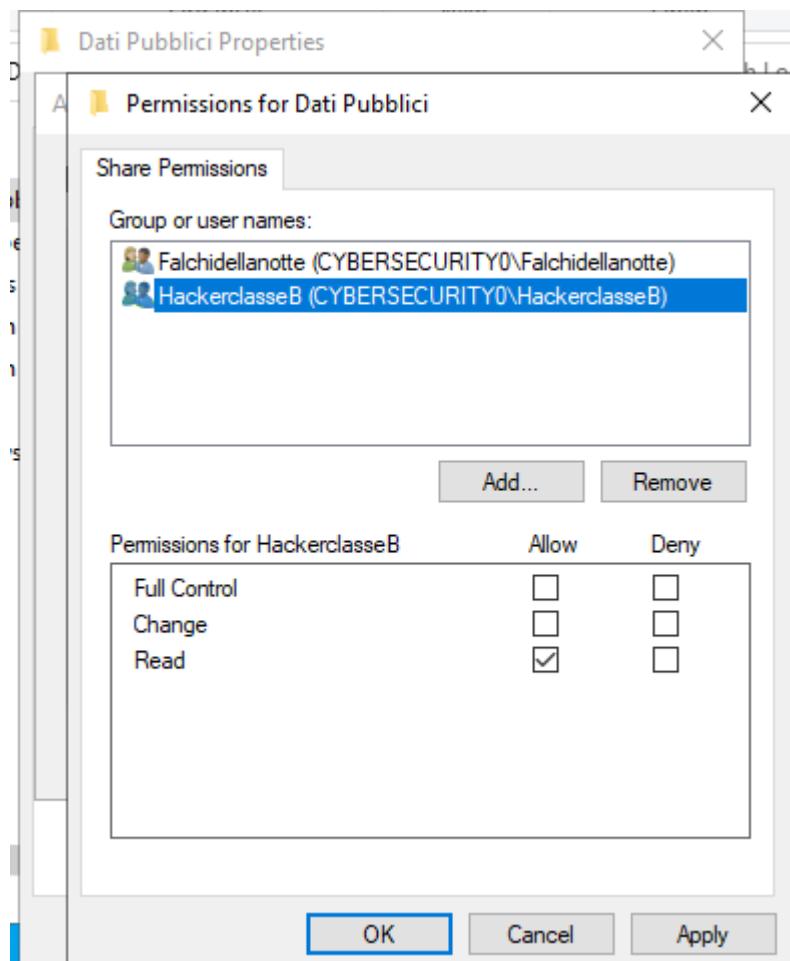
Accesso completo a entrambe le cartelle.

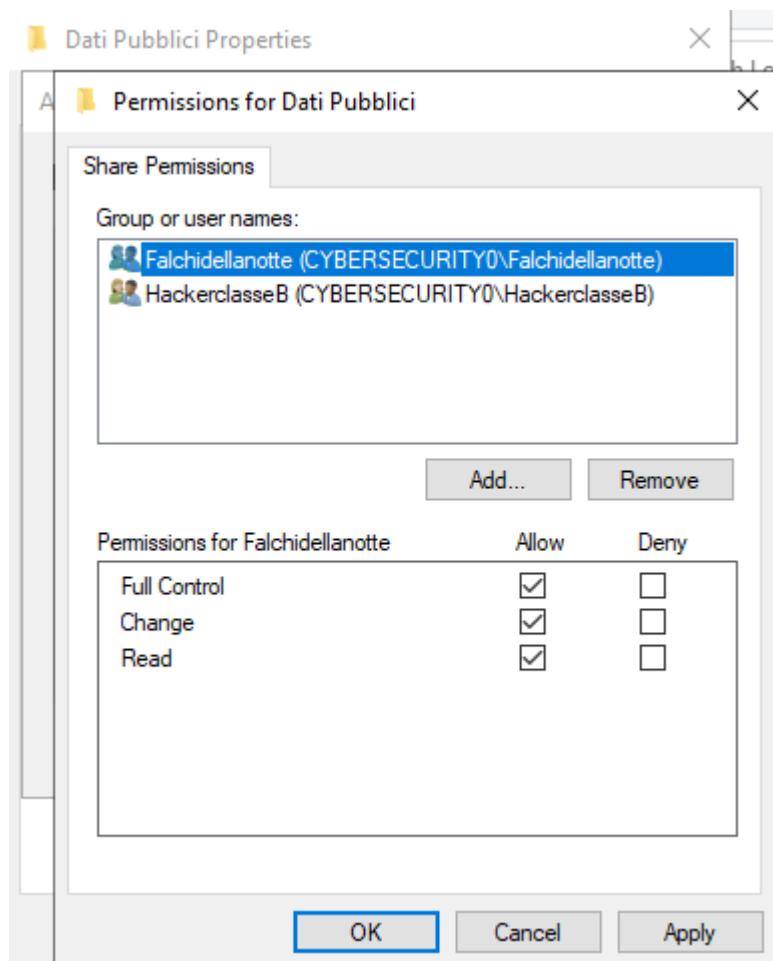
Hackerdi classeB:

Accesso in sola lettura alla cartella Dati Pubblici.

Accesso negato alla cartella Dati Super Segreti.







4.Creazione di un Collegamento Rapido sul Desktop

Per migliorare l'accesso alle risorse aziendali, è stato creato un collegamento rapido sul desktop per facilitare l'accesso a una cartella specifica.

Passaggi seguiti:

Aperto Windows Administrative Tools.

Navigato in Forest > Domains > CyberSecurity.local > Default Domain Policy.

Entrati nella policy con il tasto destro Edit.

Navigato in User Configuration > Preferences > Windows Settings > Shortcuts.

Creata un nuovo collegamento con le seguenti impostazioni:

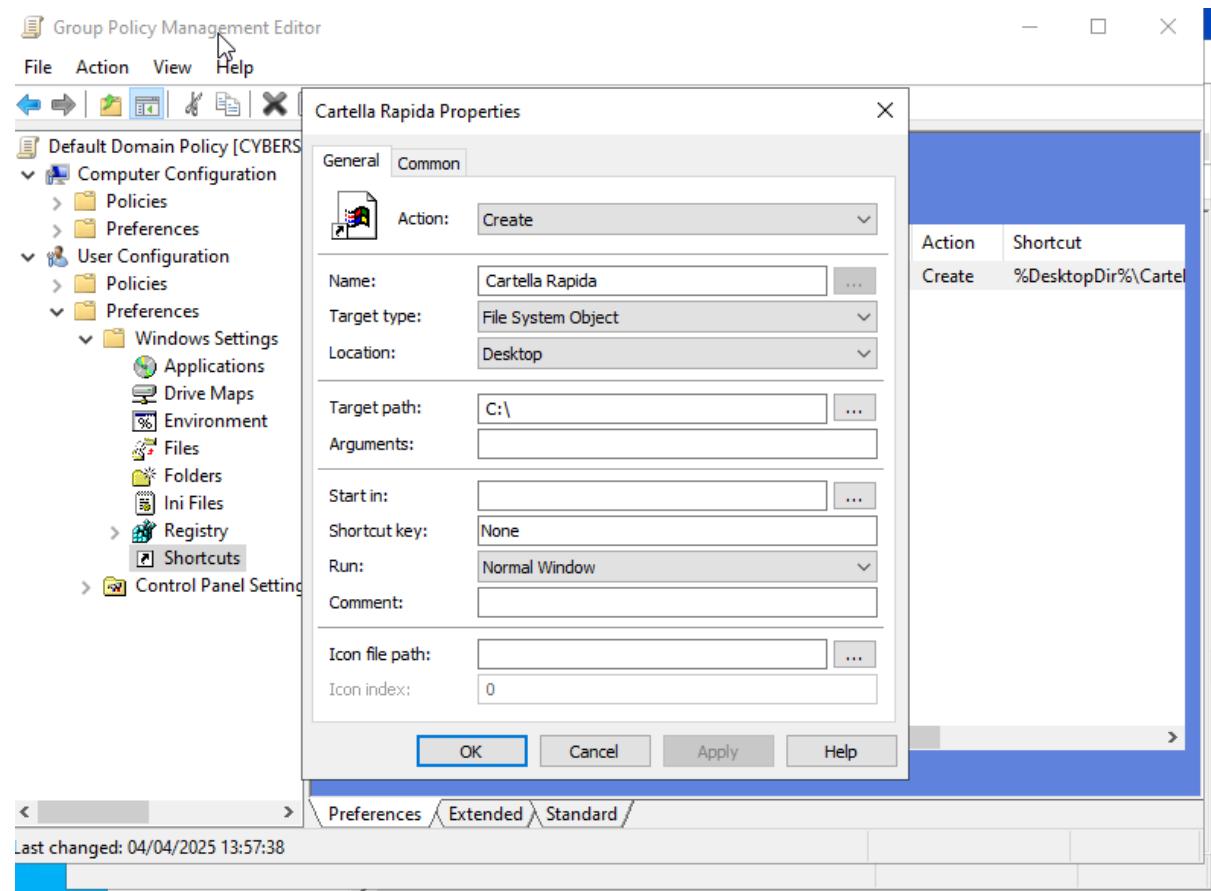
Nome: Cartella Rapida.

Percorso di destinazione: C:\

Posizione: Desktop.

Azione: Create.

Salvato e applicato la policy.



5. Verifica

Per garantire la corretta applicazione delle impostazioni, sono stati eseguiti i seguenti test:

Verifica permessi utenti: Effettuato l'accesso con gli utenti di prova per controllare le restrizioni applicate.

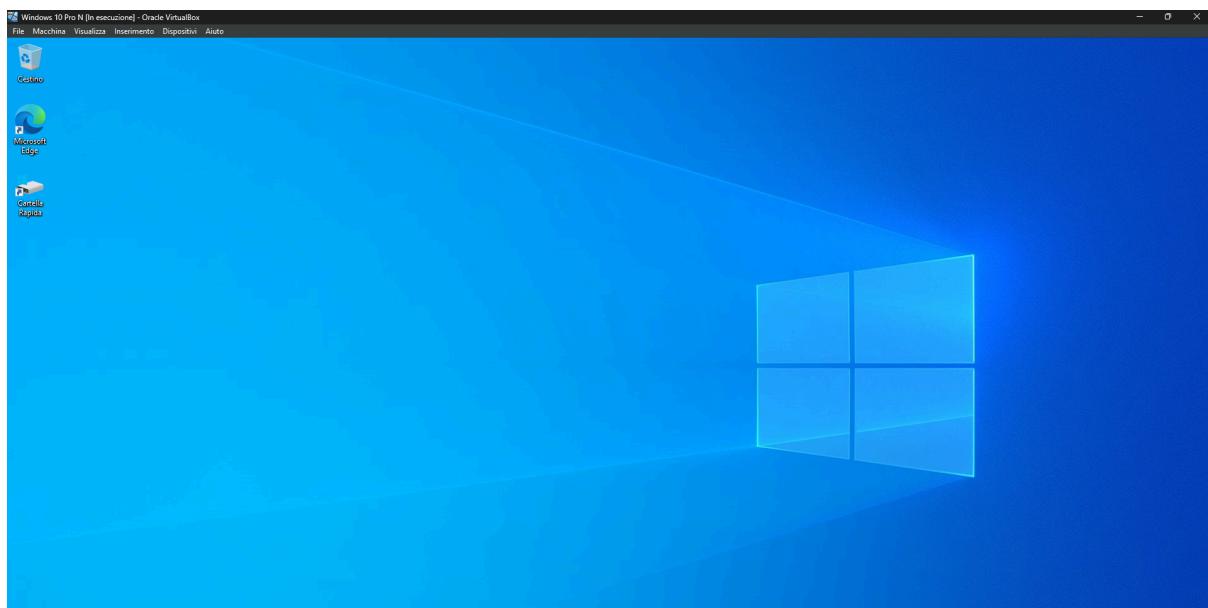
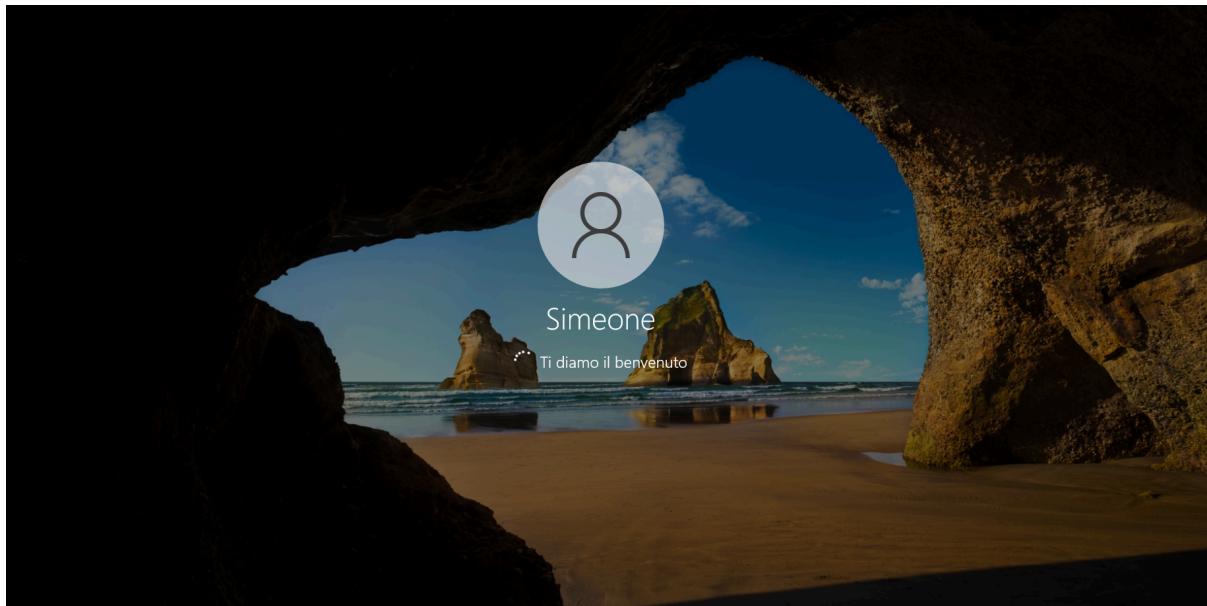
Test di accesso alle cartelle:

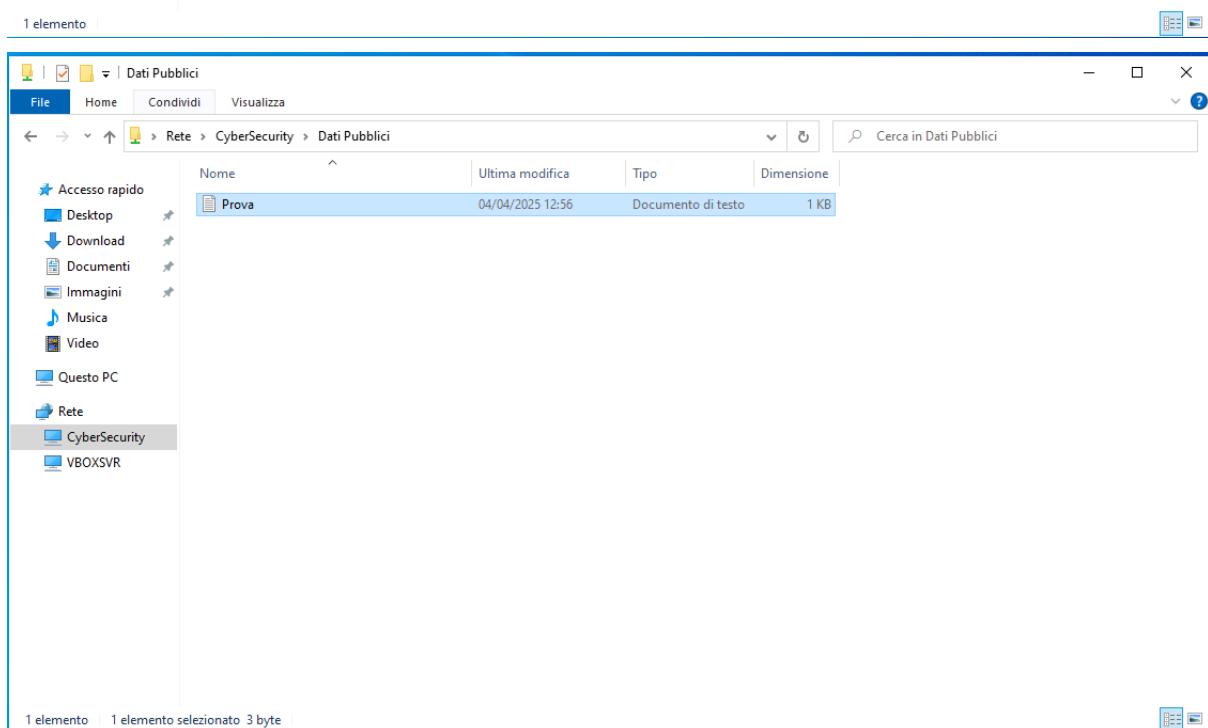
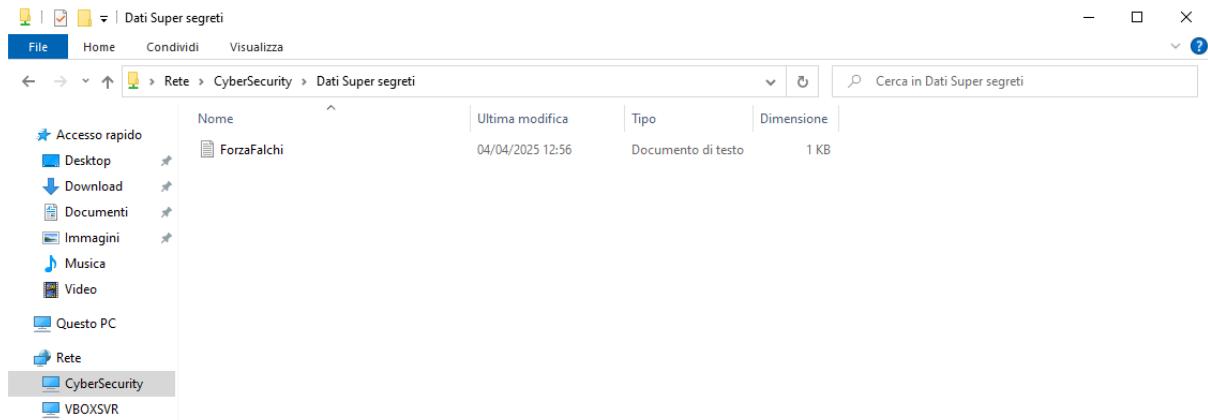
Utenti di **Falchidellanotte**: Accesso completo confermato.

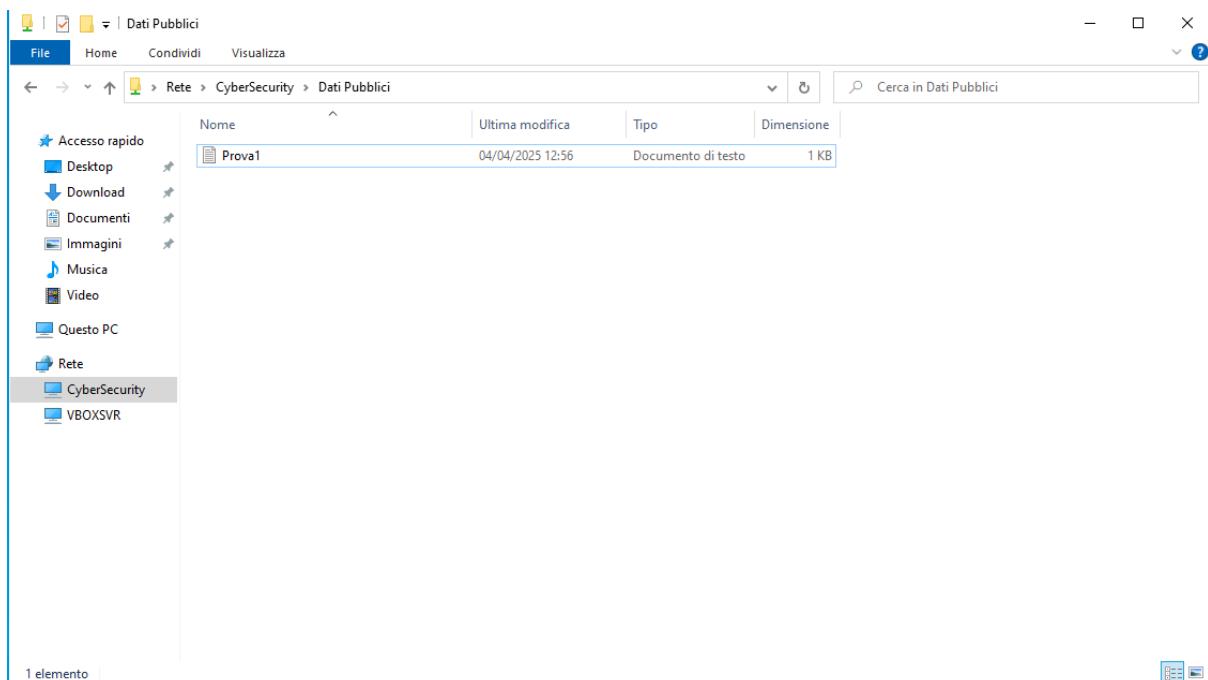
Utenti di **HackerdiClasseB**: Impossibilità di accedere ai Dati Super Segreti e accesso in sola lettura a Dati Pubblici.

Verifica del collegamento sul desktop: Testato con utenti standard e amministratori per garantire la corretta applicazione della policy.

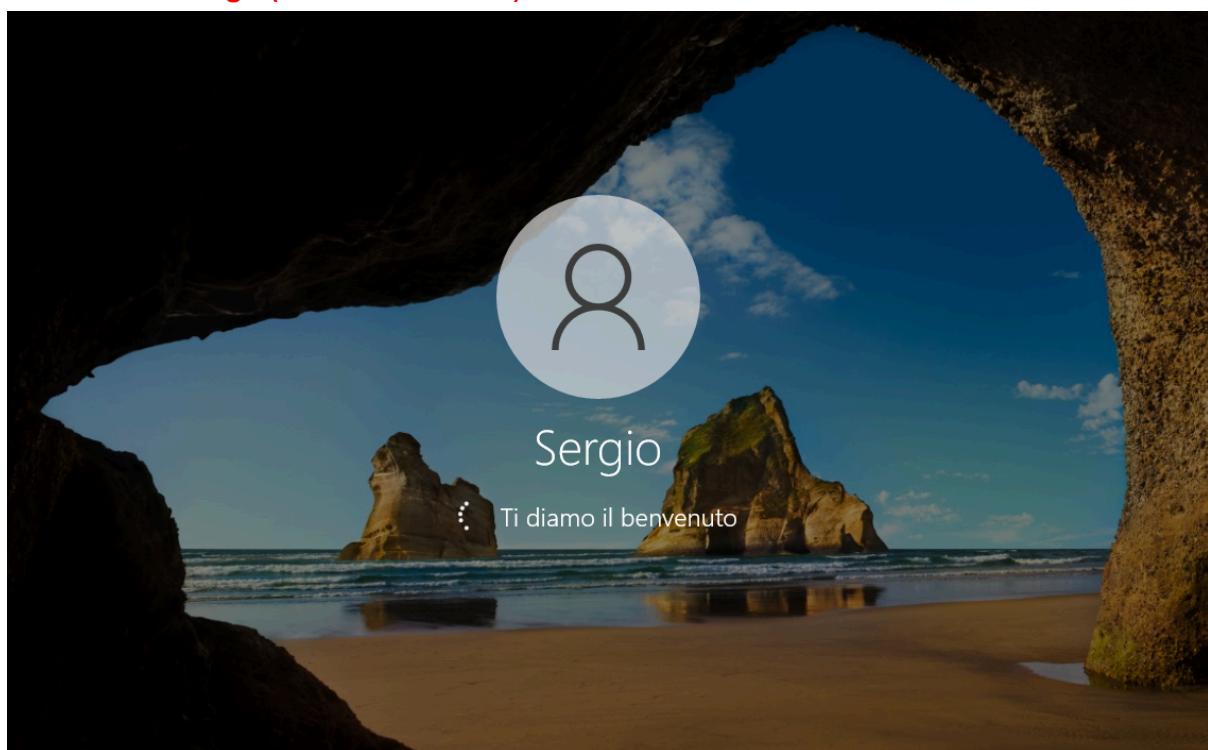
Accesso con **Simeone(Falchidellanotte)**:

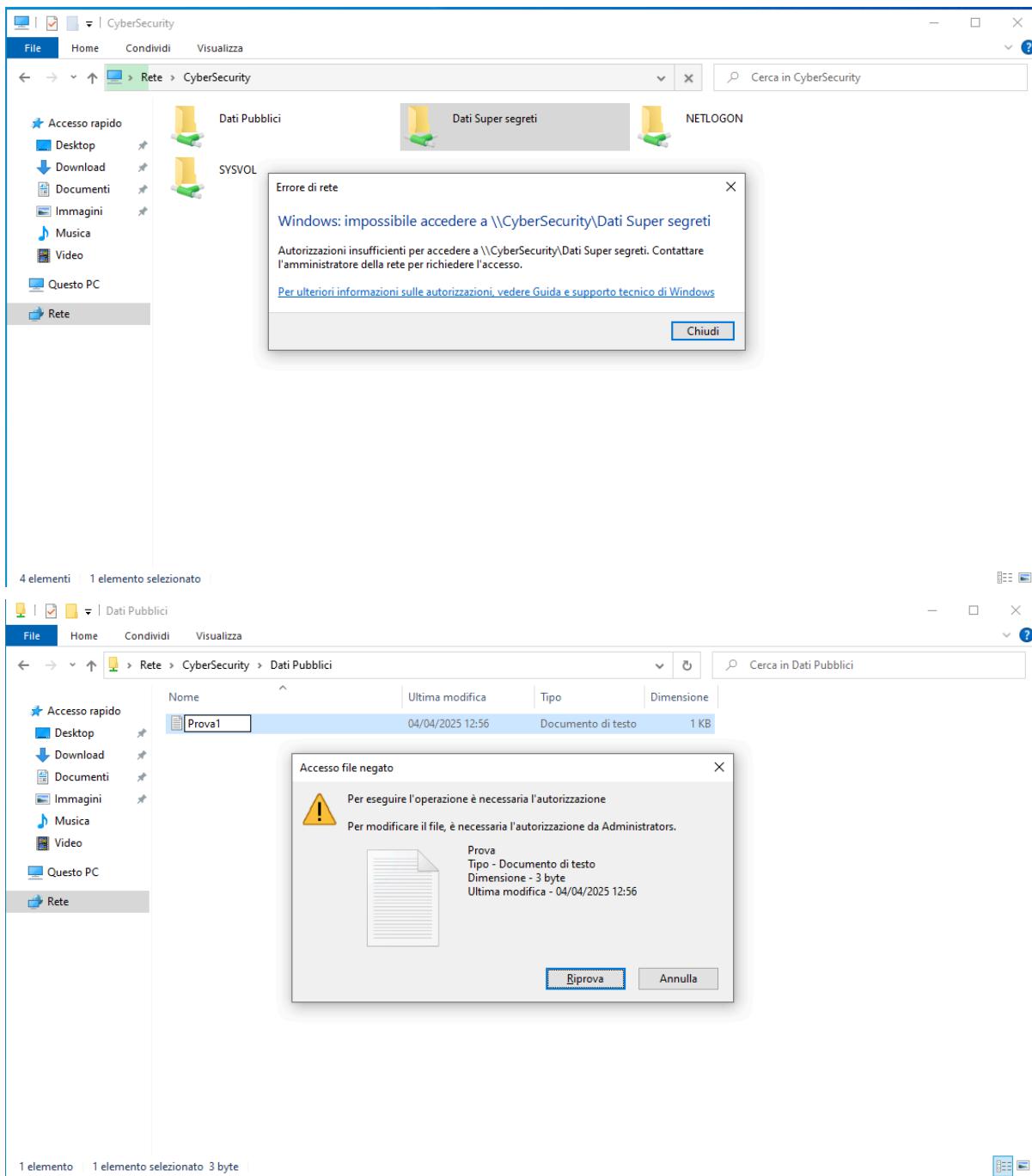






Accesso con **Sergio(HackerdiclasseB)**:





6. Conclusion

Questo esercizio ha permesso di comprendere l'importanza della gestione dei gruppi in Windows Server 2022, fornendo un controllo efficace degli accessi e migliorando la sicurezza complessiva. Inoltre, la creazione di un collegamento rapido evidenzia come le Group Policy Preferences possano essere utilizzate per semplificare la gestione e l'accessibilità delle risorse aziendali.

7. Configurazione della Connessione Remota

Per consentire l'accesso remoto al server, è stata attivata la funzione Remote Desktop.

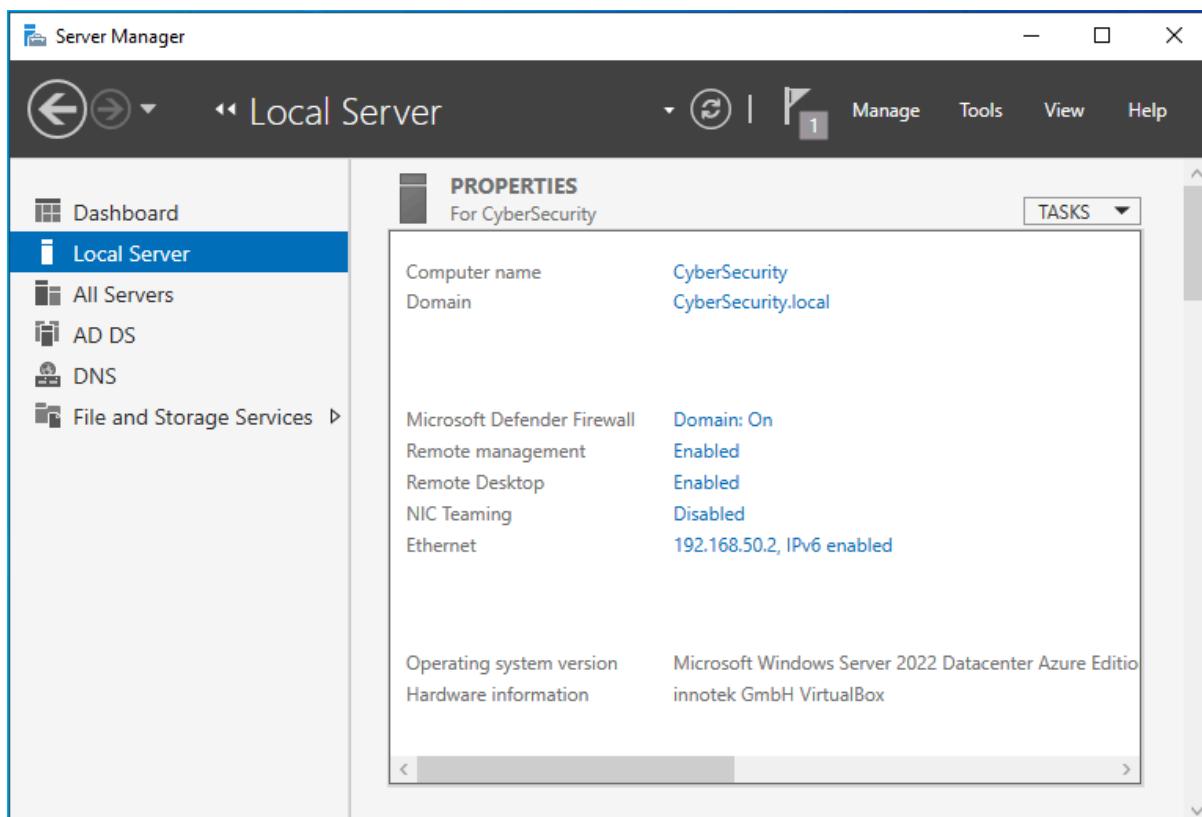
Passaggi seguiti:

Aperto Server Manager.

Selezionato Local Server dal menu laterale.

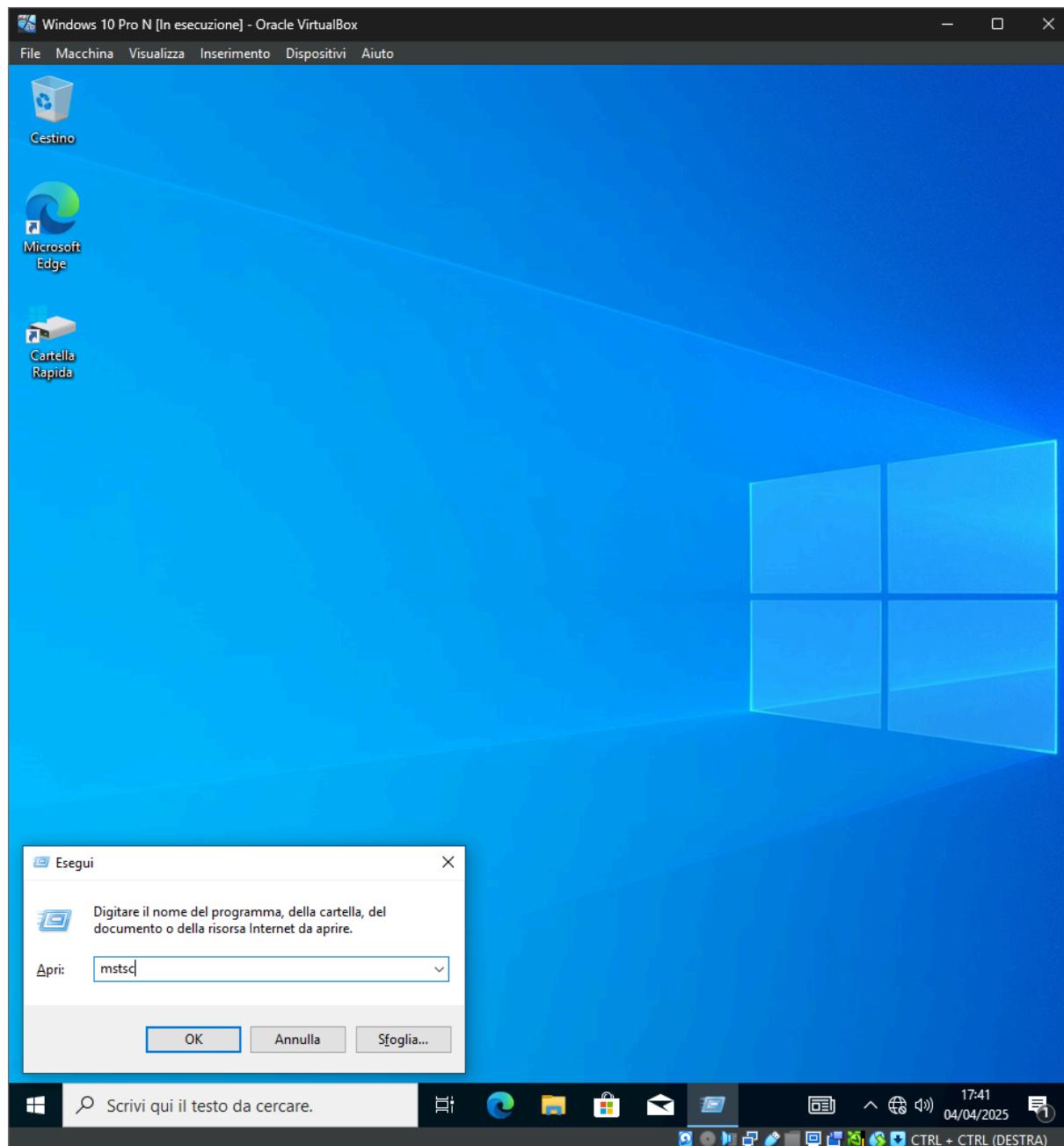
Cliccato su Remote Desktop e modificato lo stato su Enabled.

Abilitata l'opzione "Allow remote connections to this computer" nelle impostazioni avanzate.

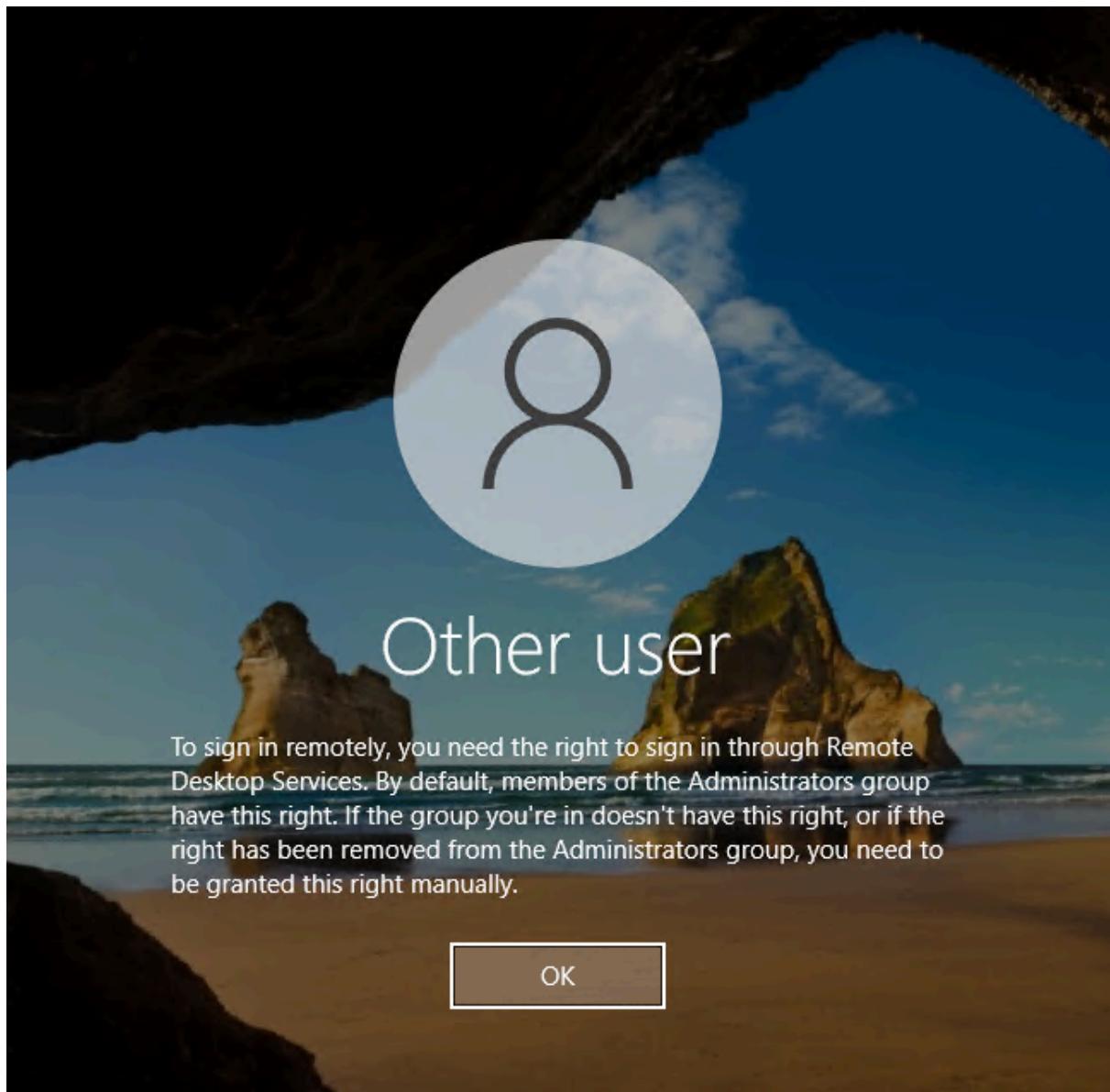
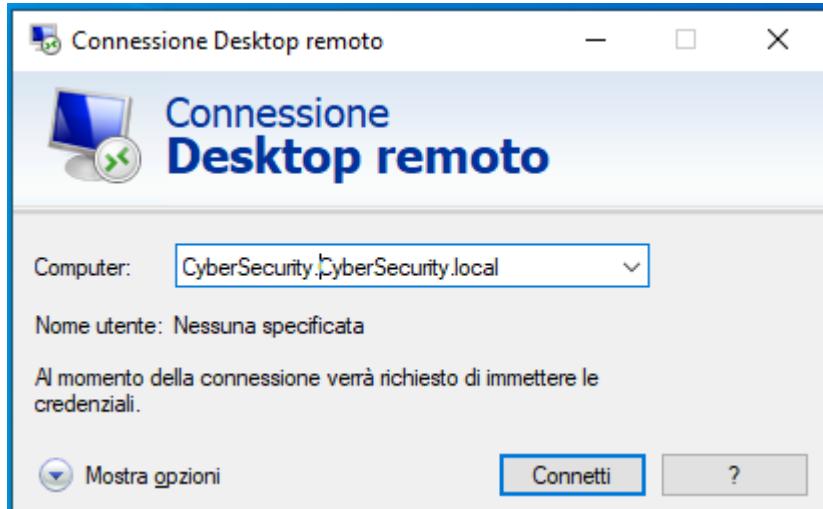


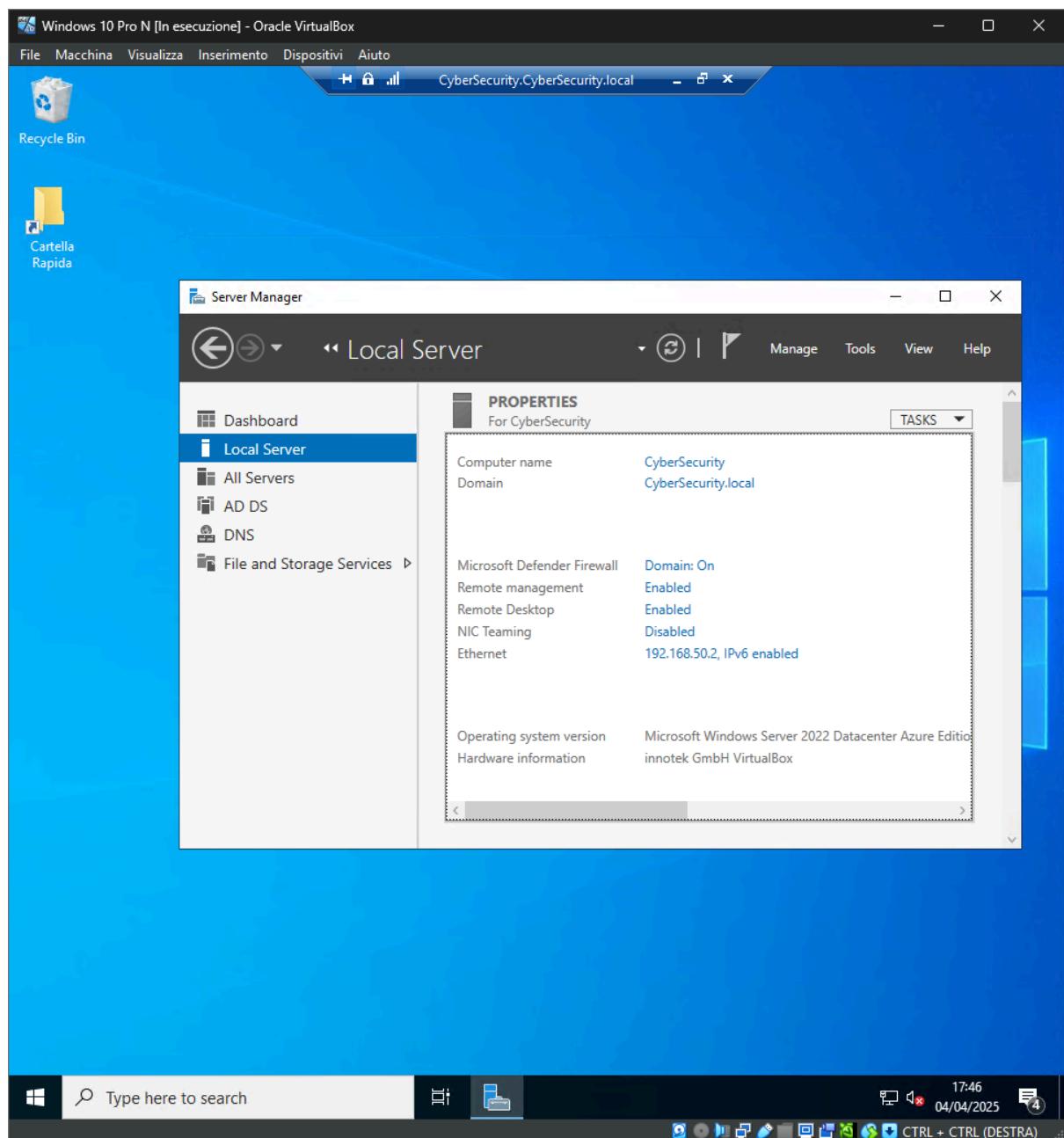
Entrati nel computer client.

Testato l'accesso remoto da un altro dispositivo tramite Remote Desktop Connection (mstsc).



Inserito il nome del computer con il dominio.





Una volta connessi vediamo il desktop in remoto del nostro Windows Server 2022.