

Progetto S10/L5

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.).

Progetto S10/L5

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.
 - Verifica che altri utenti non possano accedere a quelle risorse.

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.

1) Preparazione

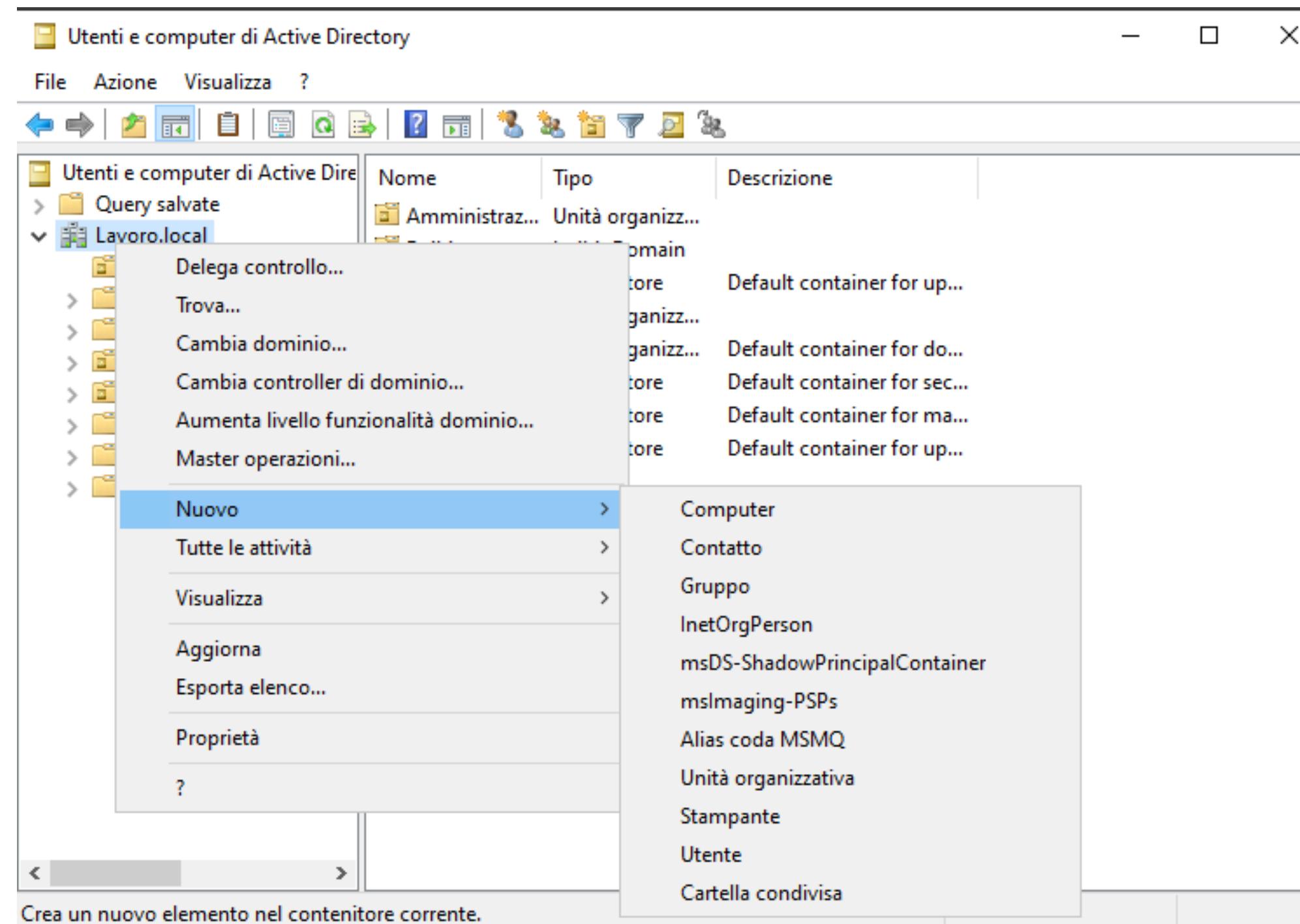
Accediamo a Windows Server con credenziali di Amministratore e una volta entrati, procediamo con la configurazione dei gruppi.

The screenshot shows the Windows Server Manager interface. The left navigation pane is visible with options like Dashboard, Server locale (which is selected and highlighted in blue), Tutti i server, DNS, Servizi di dominio Active..., and Servizi file e archiviazione. The main content area displays the properties of the local server (WIN-DHCV0IKDA28). The title bar says "Server Manager > Server locale". The top right has icons for Refresh, Stop, Start, Gestione, Strumenti, Visualizza, and Help. A dropdown menu "ATTIVITÀ" is open. The properties table includes sections for General, Firewall & Network, System, and Hardware. Key details shown include:

General	Firewall & Network	System	Hardware
Nome computer: WIN-DHCV0IKDA28 Dominio: Lavoro.local	Microsoft Defender Firewall: Pubblico: Attivato Gestione remota: Abilitato Desktop remoto: Disabilitato Gruppo NIC: Disabilitato Ethernet: 192.168.1.120, Abilitata per IPv6	Ultimi aggiornamenti installati: Windows Update Ultima verifica disponibilità aggiornamenti	Microsoft Defender Antivirus Feedback e diagnostica Configurazione sicurezza avanzata IE Fuso orario ID prodotto
Versione sistema operativo: Microsoft Windows Server 2022 Datacenter Evaluation	Informazioni hardware: innotek GmbH VirtualBox	Processori: 12t Memoria installata (RAM): 8 G Spazio totale su disco: 49,	

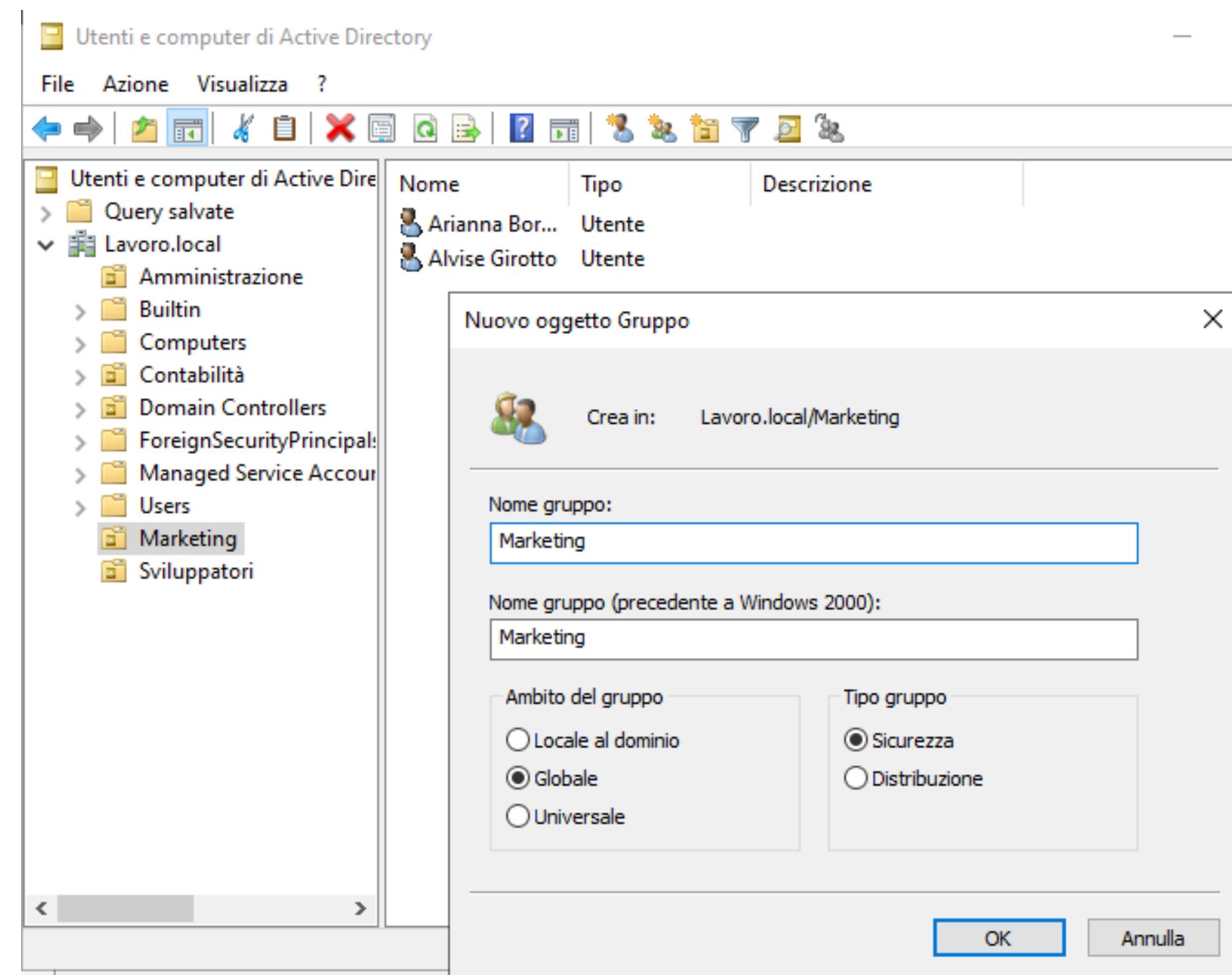
2) Creazione dei gruppi

Sul server locale, già precedentemente creato e intitolato **Lavoro.local**, andiamo a creare due unità organizzative, che andranno a contenere i due gruppi distinti: uno si intitolerà “**Sviluppatori**”, mentre l’altro “**Marketing**”.



2) Creazione dei gruppi

Creiamo la prima unità, ovvero **Marketing**, inserendo all'interno due utenti creati da noi.



2) Creazione dei gruppi

I due utenti, a solo scopo di esempio, si chiameranno Arianna Borgarelli e Alvise Girotto.

Nuovo oggetto Utente

Crea in: Lavoro.local/Marketing

Nome: Arianna Iniziali:

Cognome: Borgarelli

Nome completo: Arianna Borgarelli

Nome accesso utente: @Lavoro.local

Nome accesso utente (precedente a Windows 2000): LAVORO\

< Indietro Avanti > Annulla

Nuovo oggetto Utente

Crea in: Lavoro.local/Marketing

Nome: Alvise Iniziali:

Cognome: Girotto

Nome completo: Alvise Girotto

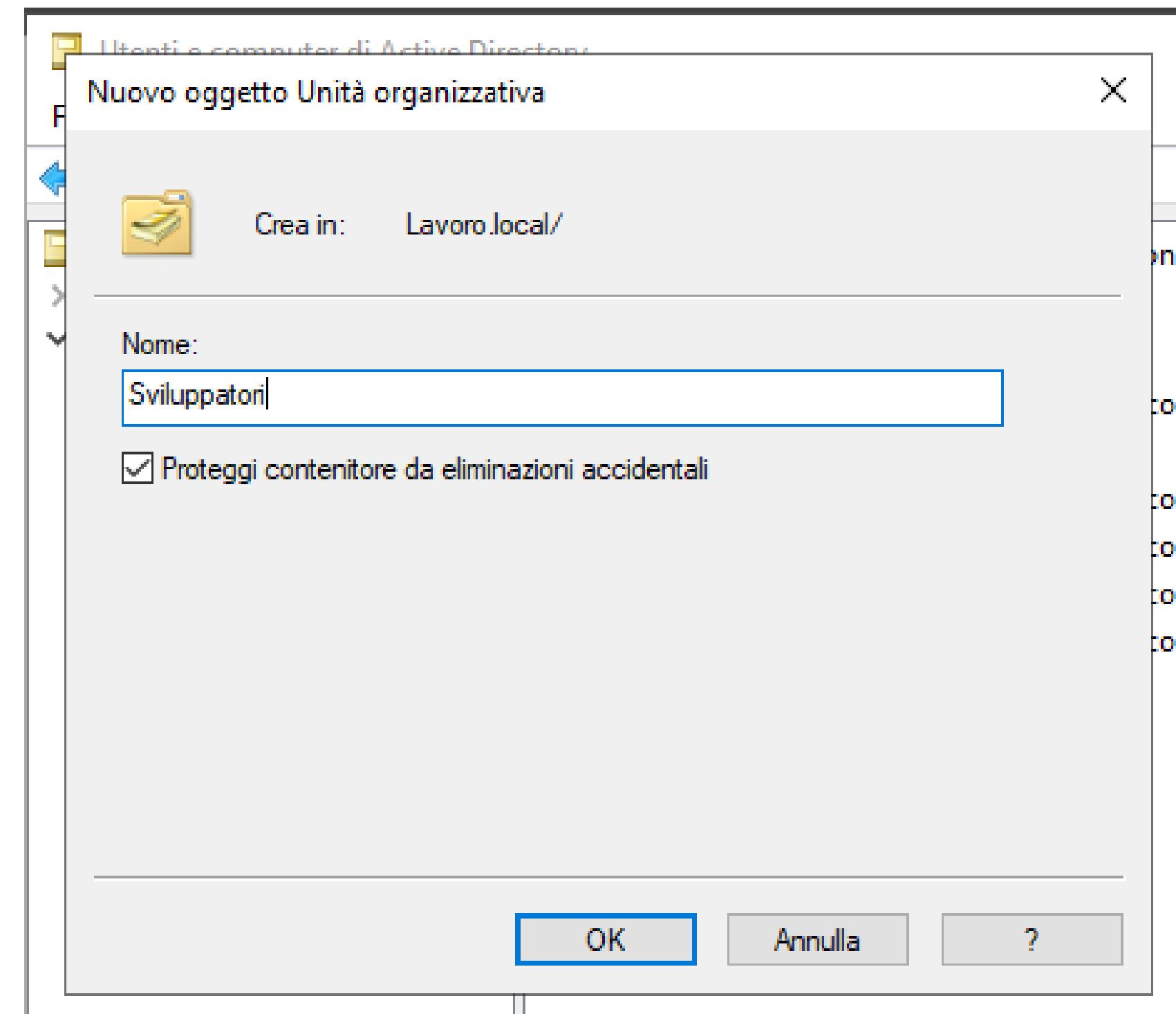
Nome accesso utente: @Lavoro.local

Nome accesso utente (precedente a Windows 2000): LAVORO\

< Indietro Avanti > Annulla

2) Creazione dei gruppi

Ripetiamo le stesse operazioni precedenti con la seconda unità organizzativa, ovvero “**Sviluppatori**”



2) Creazione dei gruppi

Questa unità conterrà invece gli utenti Mark Strong e John Doe.

Nuovo oggetto Utente

Crea in: Lavoro.local/Sviluppatori

Nome: Iniziali:
Cognome:
Nome completo:

Nome accesso utente:

Nome accesso utente (precedente a Windows 2000):

< Indietro Annulla

Nuovo oggetto Utente

Crea in: Lavoro.local/Sviluppatori

Nome: Iniziali:
Cognome:
Nome completo:

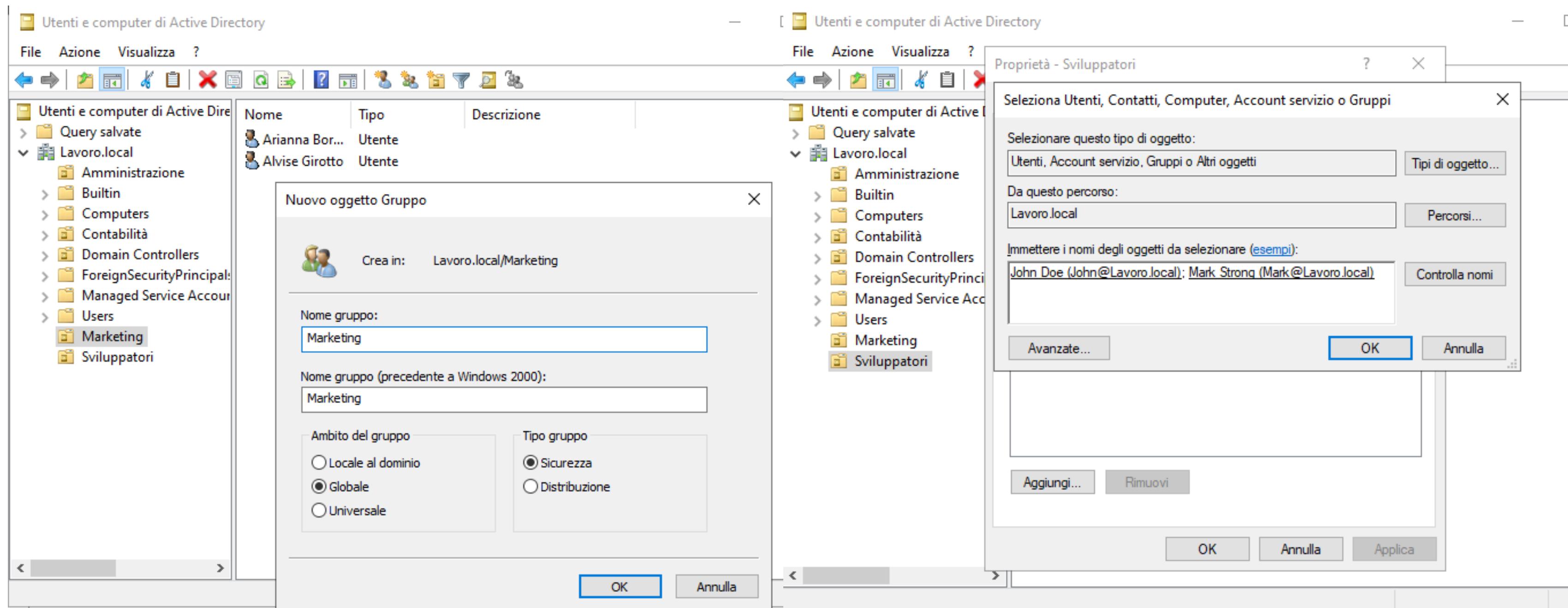
Nome accesso utente:

Nome accesso utente (precedente a Windows 2000):

< Indietro Annulla

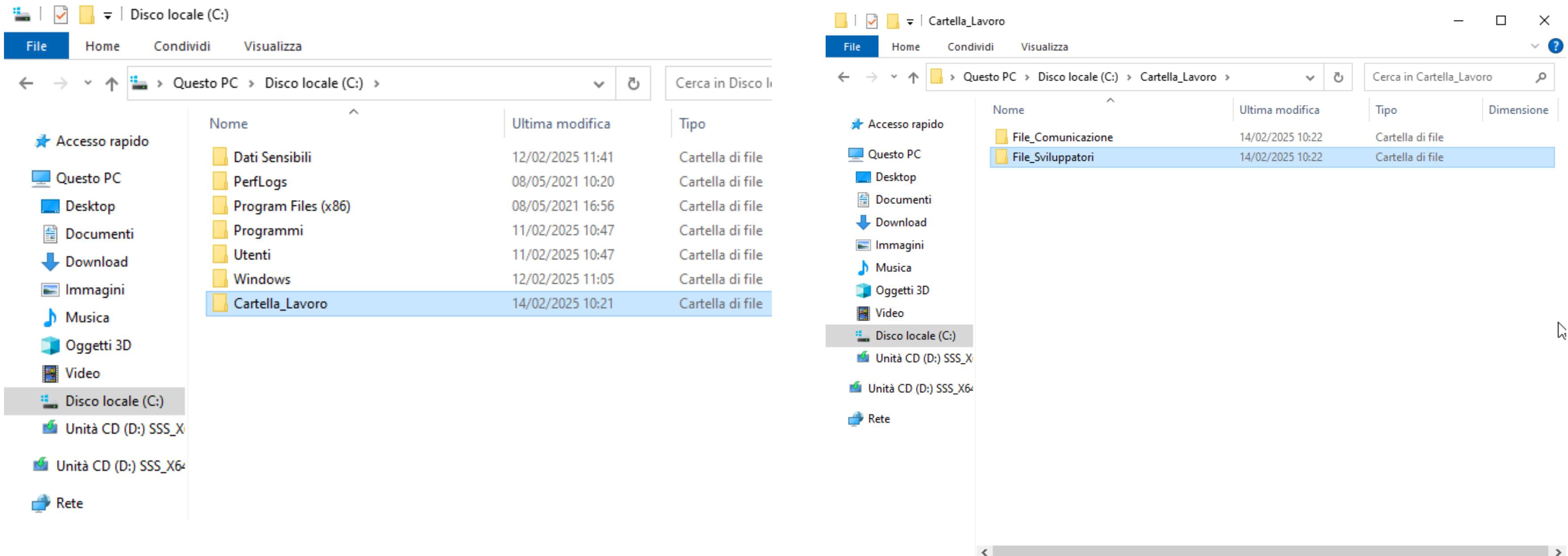
2) Creazione dei gruppi

All'interno delle due unità organizzative creiamo i due gruppi con i medesimi nomi e inseriamo dentro i due utenti creati per ciascuna unità. E' sempre bene cliccare su "**Controllo nomi**" perché è possibile sbagliarsi nella digitazione e in questo modo gli utenti non verrebbero inseriti correttamente.



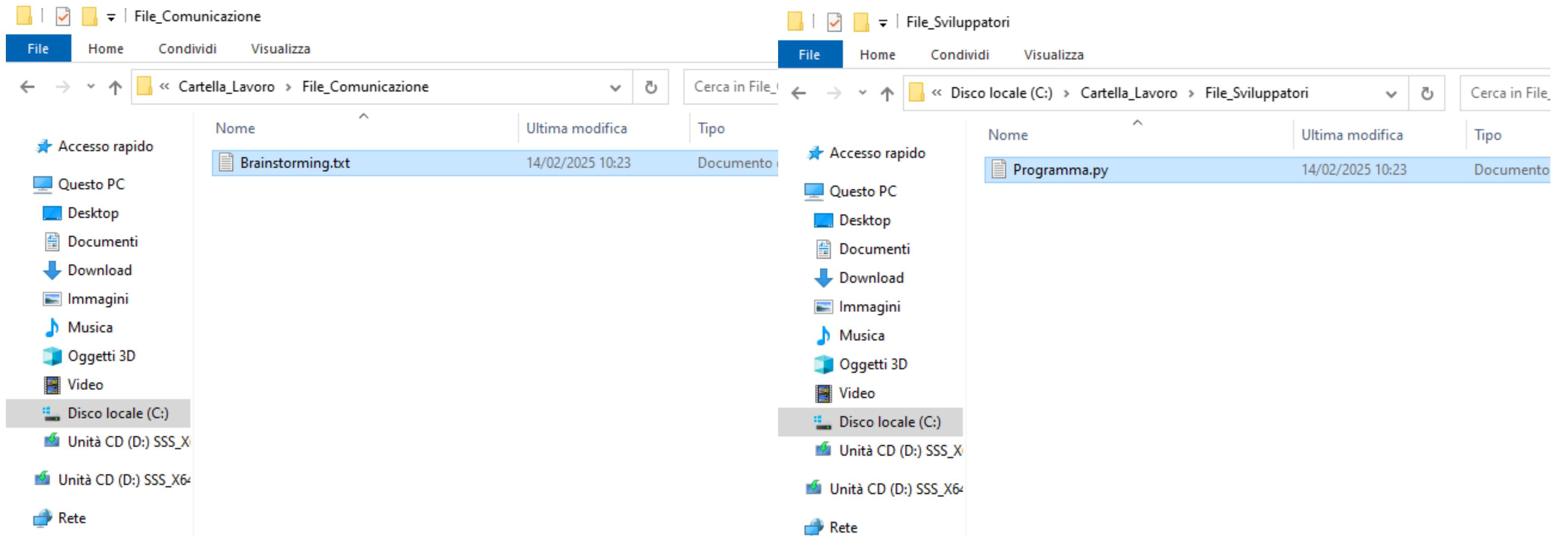
3) Assegnazione dei permessi

Ora che abbiamo creato i due gruppi, sfruttiamo le potenzialità dell'Active Directory andando a creare nell'unità locale del server un file chiamato "**Cartella_lavoro**". Al suo interno creeremo altre due sottocartelle denominate **File_Comunicazione** e **File_Sviluppatori**.



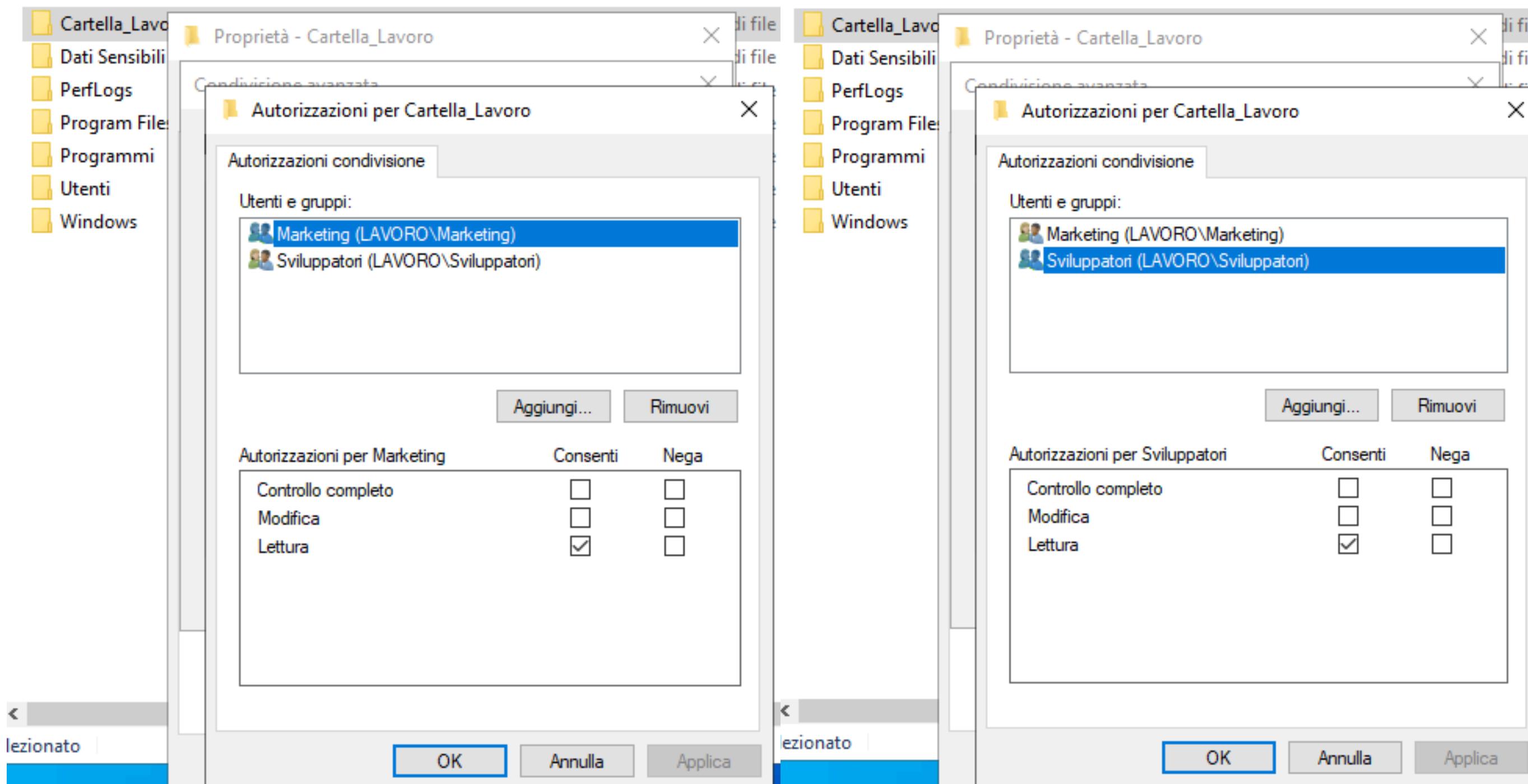
3) Assegnazione dei permessi

La prima conterrà un file testo fittizio denominato “**Brainstorming.txt**”, mentre la seconda sottocartella conterrà un file chiamato “**Programma.py**”.



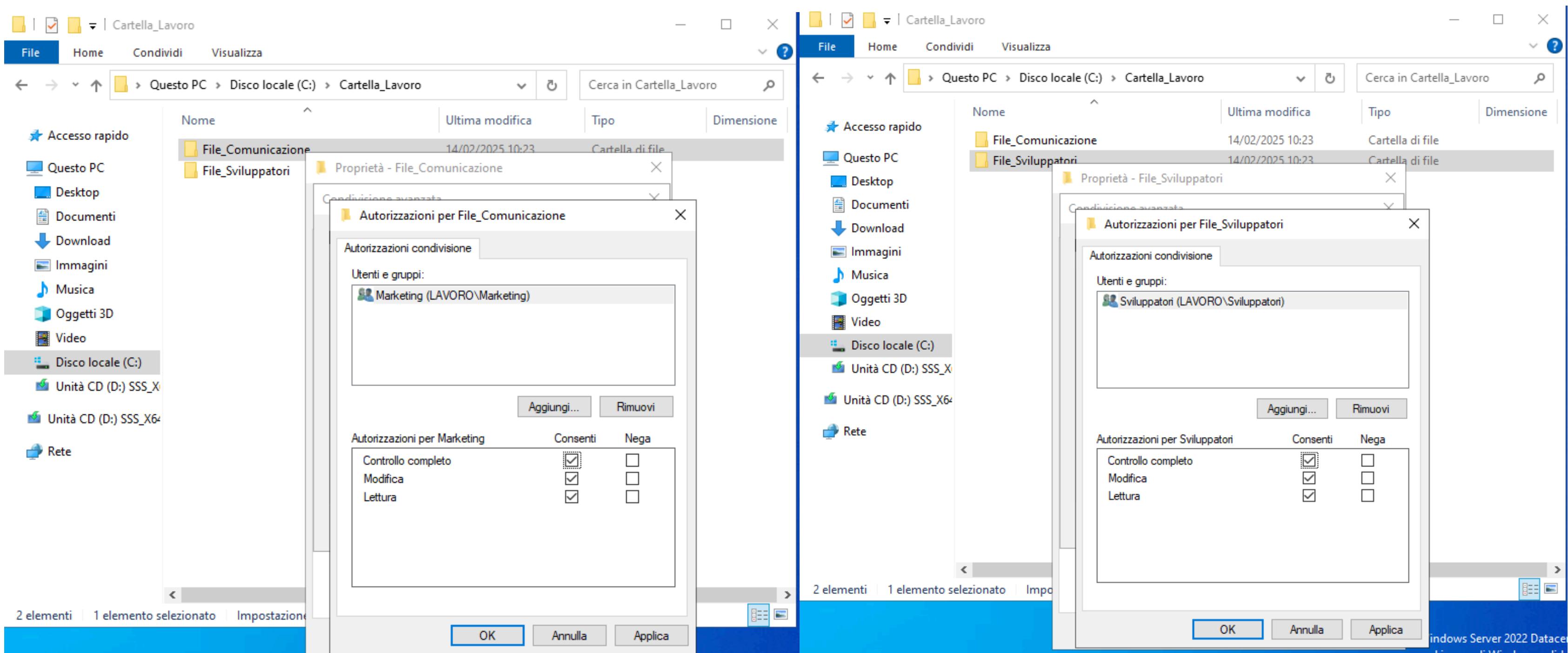
3) Assegnazione dei permessi

Arrivati a questo punto bisogna eseguire un'operazione fondamentale, andando a inserire nelle opzioni di condivisione della “**Cartella_lavoro**” i due gruppi ma con opzioni di sola lettura, ed eliminando ovviamente il gruppo “**Everyone**”, altrimenti qualunque utente potrebbe leggerla.



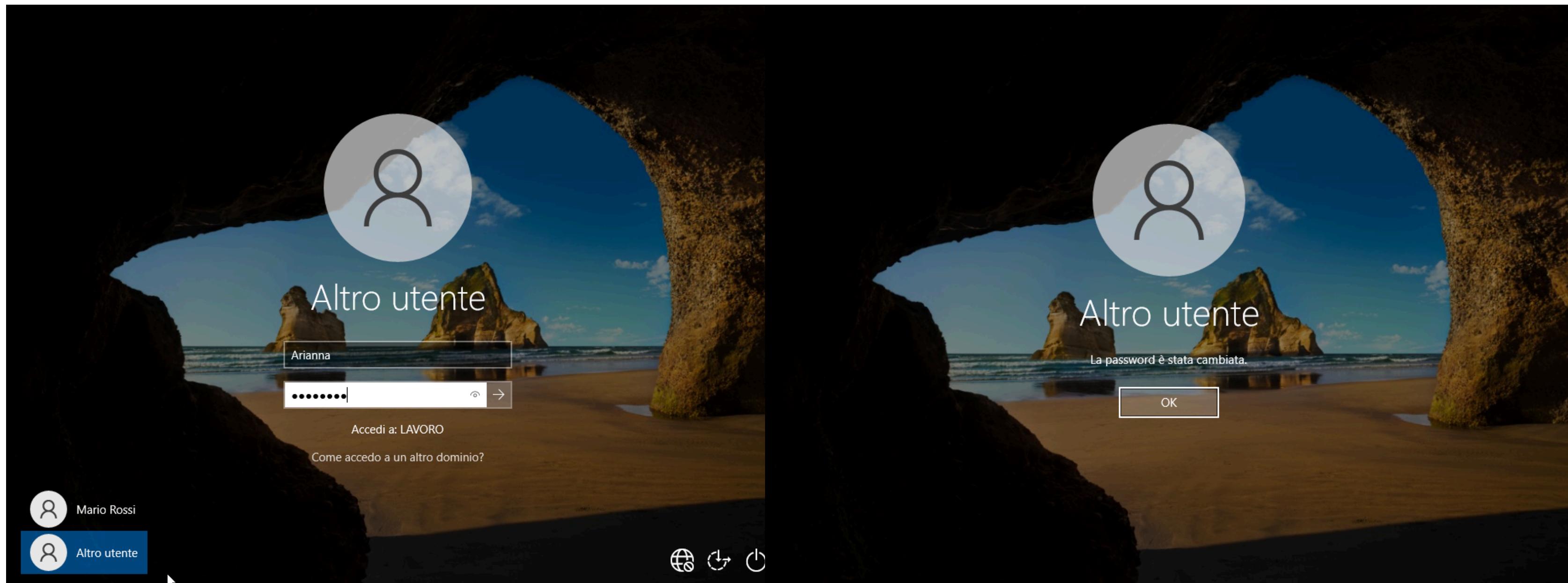
3) Assegnazione dei permessi

Mentre per le altre due sottocartelle inseriamo nel **File_Comunicazione** solamente il gruppo **Marketing**, con controllo completo; mentre per il **File_Sviluppatori** inseriamo solo il gruppo **Sviluppatori**, nuovamente con controllo completo.



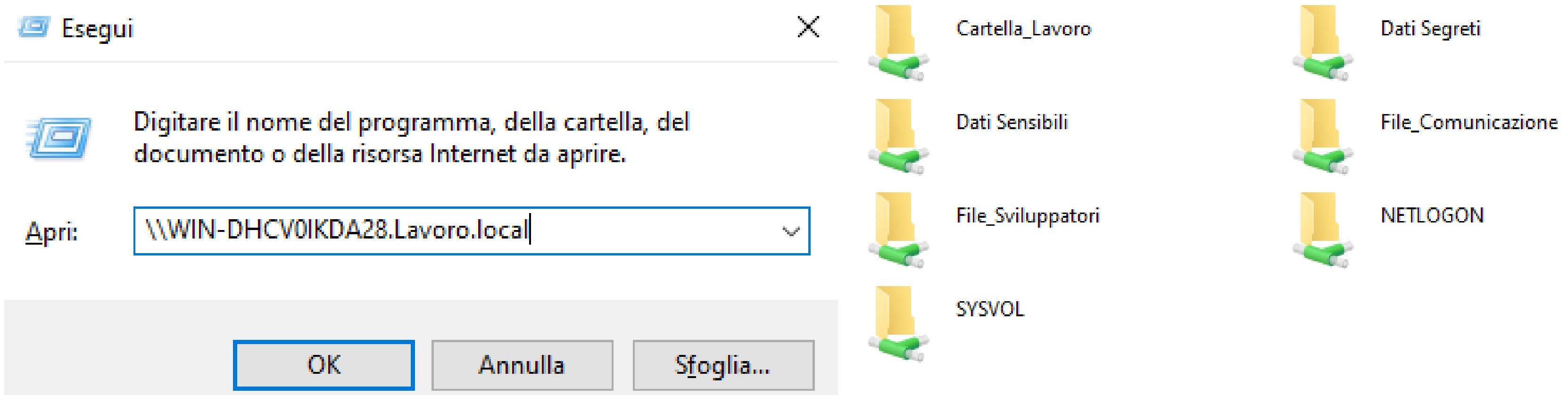
4) Verifica

Ora, verifichiamo che l'accesso alle risorse sia andato a buon fine facendo una prova: accediamo alla macchina Windows 10 Pro con le credenziali create da noi, e come vediamo ci chiederà di cambiare la password poiché questo è il nostro primo accesso, proprio come ci aspettavamo.



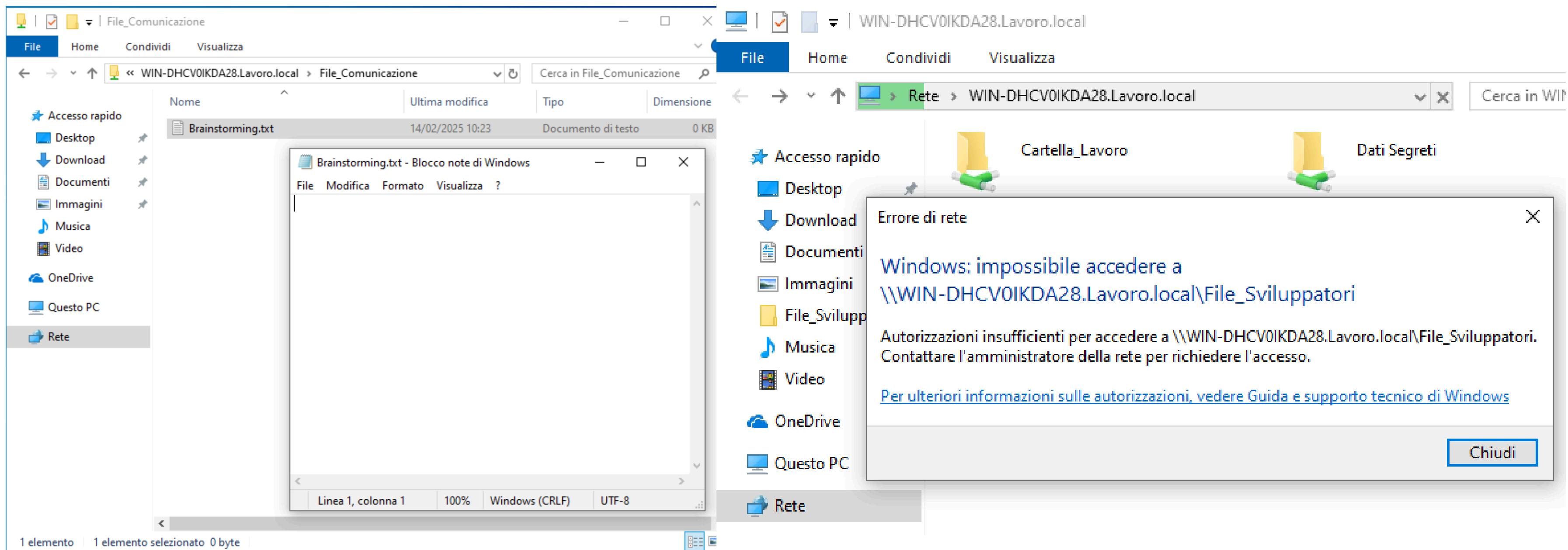
4) Verifica

Una volta effettuato l'accesso, digitiamo i tasti **WIN+R** ed accediamo alla risorsa server con il nome del computer e il nome del server locale. Ecco dunque che troveremo le cartelle create in precedenza.



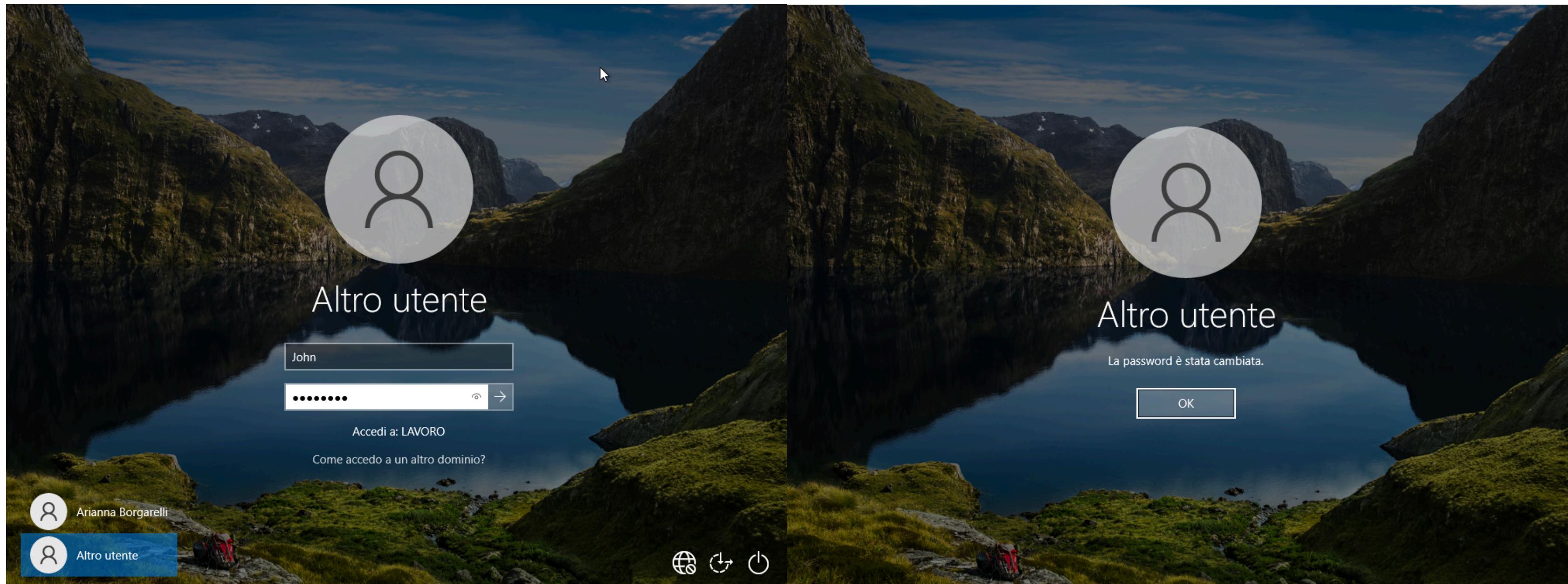
4) Verifica

Ricordandoci che, essendo l'utente Arianna, ci dovremmo aspettare di avere accesso solo alla cartella **File_Comunicazione**. Infatti, provando ad accedere potremo vedere e modificare il file **Brainstorming.txt** al suo interno. Di contro, non dovremmo aver accesso al **File_Sviluppatori**. Infatti se provassimo ad accedere riceveremmo questo messaggio di errore.



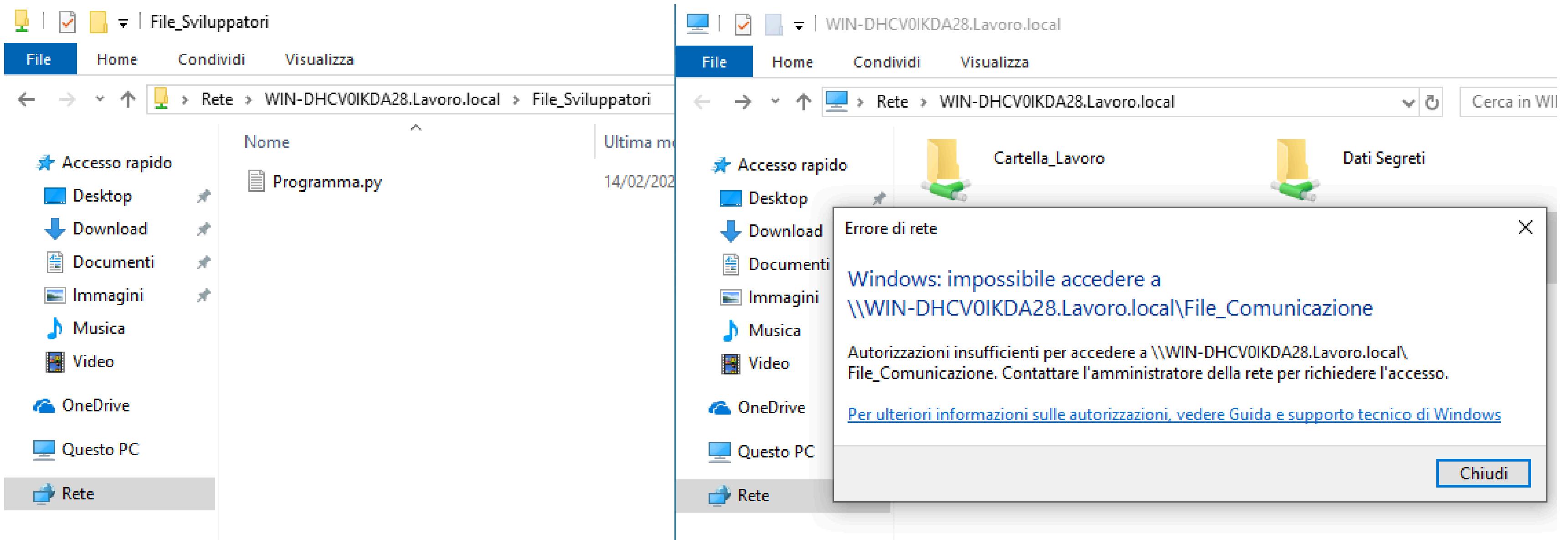
4) Verifica

Volendo fare una controprova, vediamo adesso cosa succederebbe se provassimo ad accedere con l'utente **John Doe**.



4) Verifica

Questa volta, accade l'esatto opposto: riusciamo ad entrare nel **File_Sviluppatori** con al suo interno il file **Programma.py** ma non nella cartella **File_Comunicazione**. Esattamente come avevamo configurato secondo i nostri criteri di condivisione.



5) Documentazione

In conclusione: ciò che abbiamo fatto è stato creare una cartella di lavoro condivisa con al suo interno due sottocartelle alle quali solamente i gruppi di lavoro designati potessero accedervi.

Eseguire questo tipo di configurazione è importante in azienda poiché riduce la superficie d'attacco e rispetta i principi dettati dalle norme di sicurezza e privacy.

Infatti questa configurazione effettuata da noi, essendo amministratori di sistema, rispetta i criteri di sicurezza dettati dalla **IAM** (Identity and Access Management) e, in maniera trasversale, anche dal **GDPR**.

Bonus

Obiettivo

Lo scopo di questo esercizio è analizzare il seguente file di log con Splunk e :

1. Notare e documentare evidenze di anomalie o attacchi
2. Preparare un report TECNICO DETTAGLIATO per spiegare le remediation (non voglio tipo "installare MFA" ma voglio dei passi per implementare una soluzione, a livello pratico).
3. Creare una conclusione PER I MANAGER che indica brevemente le anomalie/attacchi coprire le situazioni (descritte dal file log).

File1: <https://mega.nz/file/wapzyZzA#MyjJHoNfGs> rilevati e delle remediation per -3UpORTf1sduGdYGajTXdB8hHxTpFpfM

Bonus

L'esercizio bonus sarà purtroppo incompleto e riguarderà solamente il punto 1, data la mancanza di tempo e informazioni necessarie per completare i punti 2 e 3. Ad ogni modo, osservando su Splunk l'analisi dei log ciò che balza all'occhio è che le richieste sono tutte di tipo **ftp**. Le richieste partono da più host attaccanti e raggiungono più host destinatari. Spesso

partono da un utente **anonymous** e sono frequenti le richieste **RETR**, **STOR** e **DELE**, che sono tutti metodi ftp. Essi riguardano operazioni di download, upload ed eliminazione di file; spesso però danno l'errore “**Operation not permitted**”.

Sembra dunque che l'utente attaccante stesse andando a "caccia" di qualche file vulnerabile in modo da eliminarlo e sostituendolo caricando un presunto file malevolo ma senza successo. Potrebbe dunque essere un tentativo di eseguire un malware di qualche genere. Sfortunatamente non sono riuscito a reperire ulteriori informazioni in modo da presentare un quadro più generale.

i	Ora	Evento
>	14/02/25 10:45:10,000	1331992579.620000 C9Jq442ff1JhSB0UA8 192.168.202.138 55780 192.168.25.101 21 anonymous justinwray@justinwray.com STOR f tp://192.168.25.101/dept/www/html/x.php - - 550 x.php: Operation not permitted - - - - Fx7EWx1coA7eyCvPX host = si-i-01e92308449c65881prd-p-by1b3.splunkcloud.com source = File1.log sourcetype = Prova
>	14/02/25 10:45:10,000	1331921049.880000 Cu0Czp1W7hIKmYtQpb 192.168.25.254 1721 192.168.202.78 21 spatiald <hidden> STOR ftp://192.168.20 2.78./stuff - - 550 stuff: Permission denied - - - - host = si-i-01e92308449c65881prd-p-by1b3.splunkcloud.com source = File1.log sourcetype = Prova
>	14/02/25 10:45:10,000	1331909396.160000 CVHMp01B6ylGqaAJje 192.168.202.102 4970 192.168.28.101 21 ftp password@example.com STOR ftp://192.168.28. 101/dept/env/lib/python2.7/site-packages/flask/testsuite/test_apps/moduleapp/apps/admin/static/css/.ftpde854Us - - 550 /dept/env/lib/pyt hon2.7/site-packages/flask/testsuite/test_apps/moduleapp/apps/admin/static/css/.ftpde854Us: Operation not permitted - - - - FymT07Uu2XCI suyx2 host = si-i-01e92308449c65881prd-p-by1b3.splunkcloud.com source = File1.log sourcetype = Prova
>	14/02/25 10:45:10,000	1331909396.150000 CVHMp01B6ylGqaAJje 192.168.202.102 4970 192.168.28.101 21 ftp password@example.com STOR ftp://192.168.28. 101/dept/env/lib/python2.7/site-packages/flask/testsuite/test_apps/blueprintapp/apps/frontend/templates/frontend/.ftpde854Us - - 550 / dept/env/lib/python2.7/site-packages/flask/testsuite/test_apps/blueprintapp/apps/frontend/templates/frontend/.ftpde854Us: Operation not permitted - - - - FymT07Uu2XCI suyx2 host = si-i-01e92308449c65881prd-p-by1b3.splunkcloud.com source = File1.log sourcetype = Prova