REPORT TECNICO

Windows Server

Redatto da: *Nicolò Calì Cybersecurity Student*

Data: *13/02/2026*

Oggetto: *Configurazione Infrastruttura Windows Server 2022: Implementazione Active Directory, Gestione Utenti e ACL.*

1. Introduzione

Il presente report documenta le attività svolte durante il laboratorio di **Windows Server 2022**. L'obiettivo dell'esercitazione è simulare la creazione e la messa in sicurezza di un ambiente aziendale basato su dominio, utilizzando macchine virtuali per replicare un'infrastruttura di rete reale.

Per rendere lo scenario coerente con un ambiente gerarchico e controllato, è stato scelto il tema **"Fallout"**. Il server agirà come il computer centrale di un *Vault* (rifugio antiatomico), dove è necessario gestire rigorosamente i permessi:

- **L'Overseer (Supervisore):** Deve avere accesso completo ai documenti sensibili.
- **I Vault Dwellers (Abitanti):** Devono poter accedere solo alle informazioni pubbliche e non ai segreti del Vault.

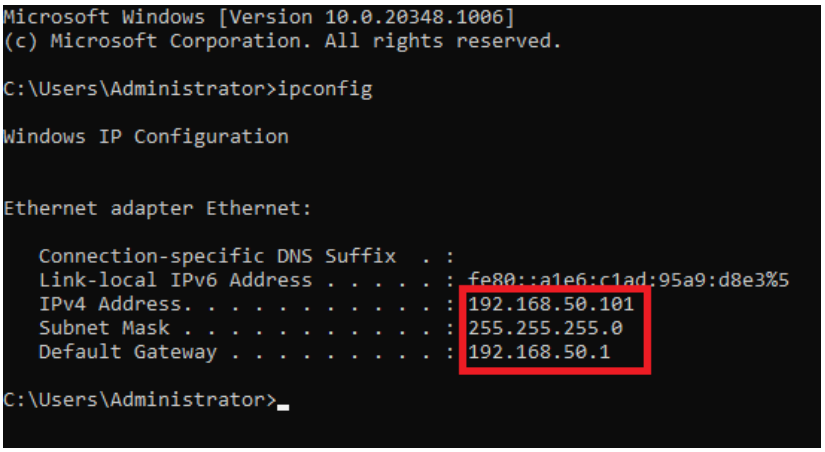
Gli obiettivi tecnici raggiunti includono:

- Configurazione di rete statica.
- Promozione del server a Domain Controller (**Active Directory**).
- Creazione di Organizational Units (**OU**), Utenti e Gruppi.
- Configurazione dei permessi **NTFS** e di condivisione (**ACL**) per segregare l'accesso ai dati.
- Esecuzione di un Test che permette di dimostrare la corretta configurazione del server.

2. Configurazione di Rete e Preparazione del Server

Il primo passo fondamentale per configurare un Server è l'assegnazione di un indirizzo **IP statico**, necessario affinché il server sia sempre raggiungibile dai client e possa risolvere correttamente le richieste DNS.

Nelle impostazioni della scheda di rete, è stato assegnato l'indirizzo IPv4 **192.168.50.101** con subnet mask **255.255.255.0** e gateway **192.168.50.1**.



ig 1. IP statico del Server

3. Creazione del Dominio "Fallout.local"

Una volta configurata la rete, è stato installato il ruolo **Active Directory Domain Services (AD DS)**. Tramite il wizard di configurazione, è stata creata una nuova foresta con il nome di dominio radice **Fallout.local**.

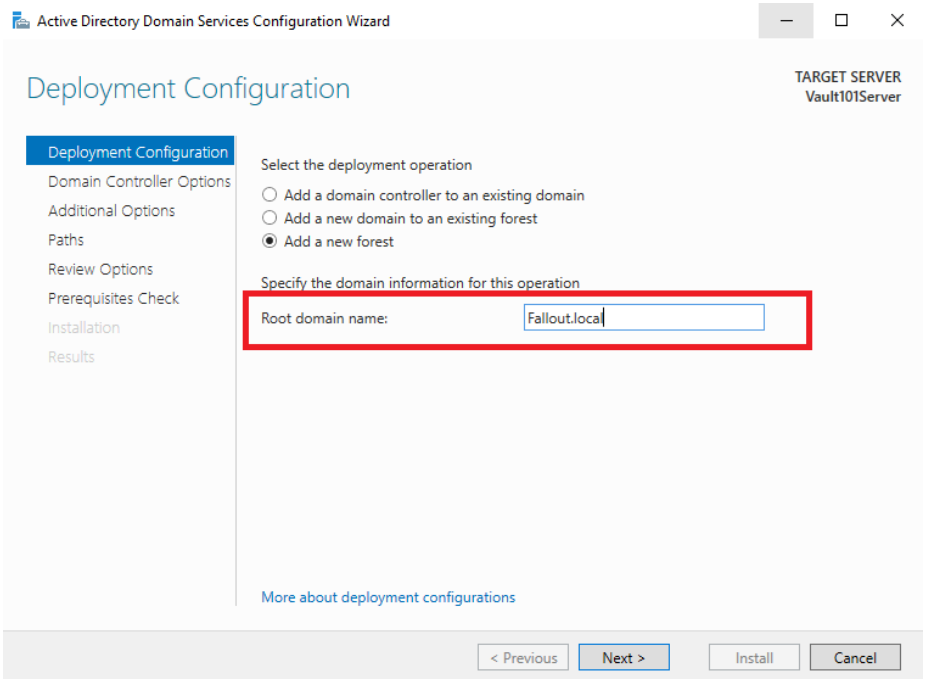


Fig 2. Creazione del Domain Fallout.local

Al termine dell'installazione e dopo il riavvio obbligatorio, il server è diventato operativo come Domain Controller. L'accesso è stato effettuato con l'account **FALLOUT\Administrator**.

Fig 3. Login Server

4. Struttura Active Directory: Organizzazione ed Utenti

Accedendo alla console **Active Directory Users and Computers**, è stata definita una struttura gerarchica per organizzare le risorse del “Vault”.

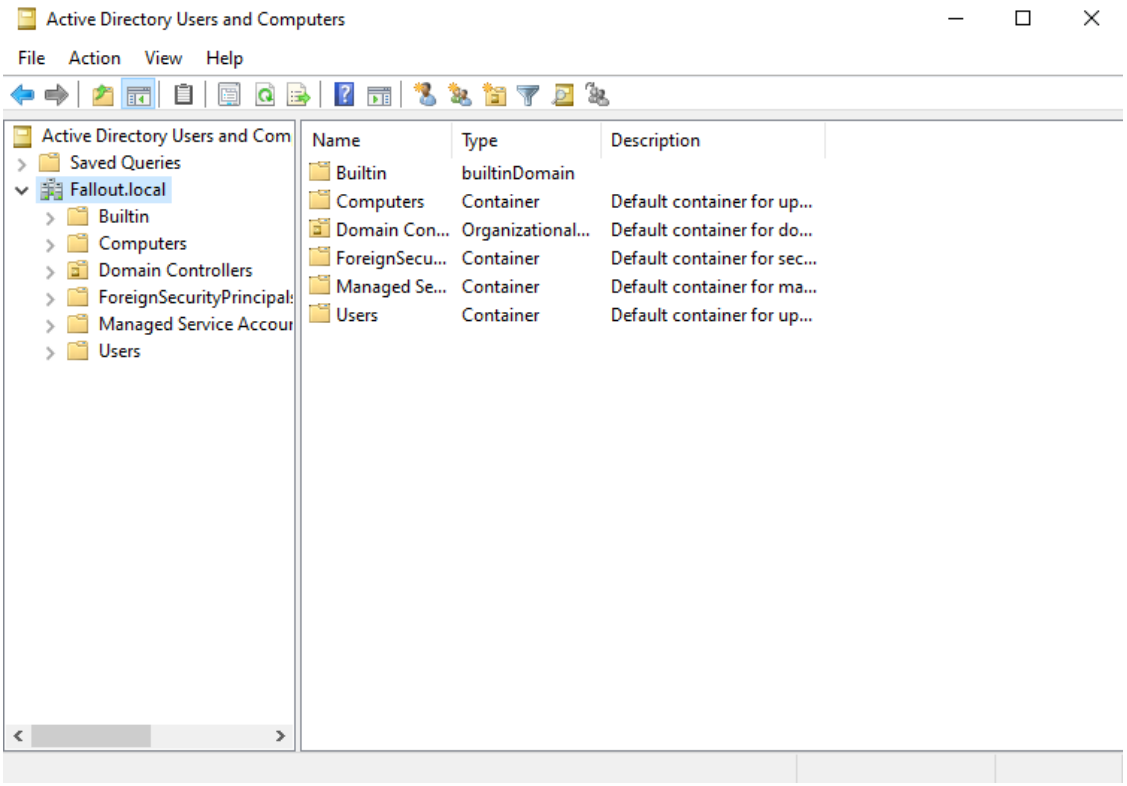


Fig 4. Accedere ad Active Directory

Sono state create due Organizational Units (OU) principali per separare i ruoli:

1. **Overseer:** Contiene gli utenti con privilegi amministrativi o di alto livello.
2. **Vault Dwellers:** Contiene gli utenti standard.

All'interno della OU Overseer è stato creato l'utente **Hank MacLean** (il Supervisore), mentre nella OU Vault Dwellers sono stati creati gli utenti **Lucy MacLean**, **Albert Cole** e **Amata Almodovar**.

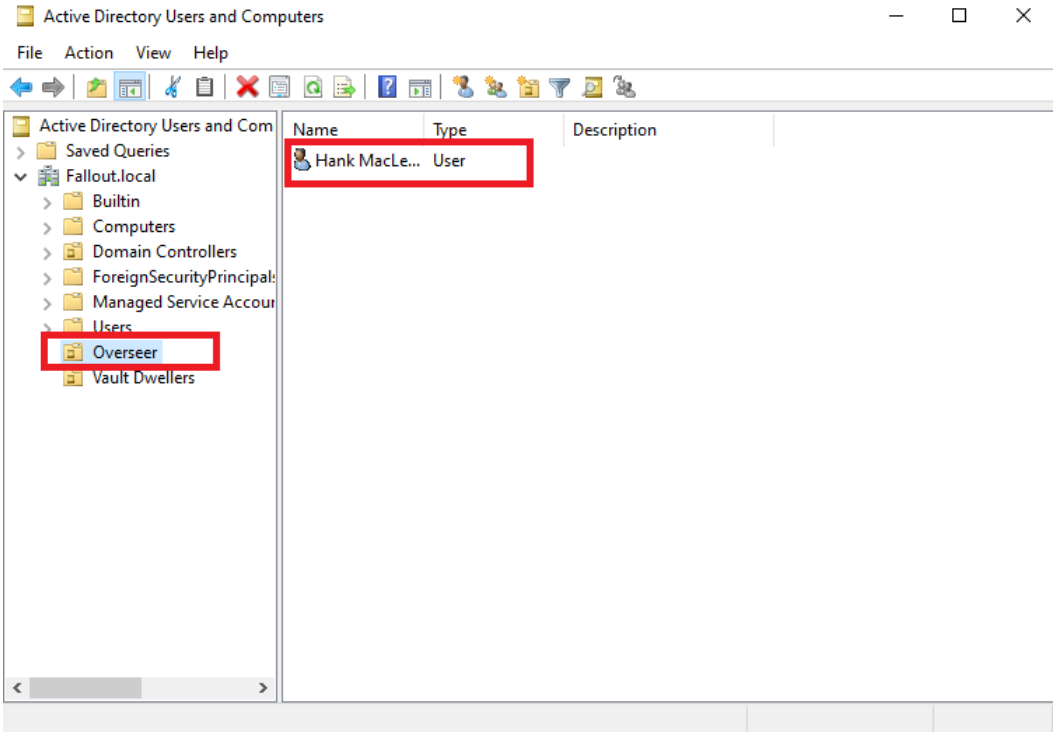


Fig 5. Creazione Organizzazione Overseer e User

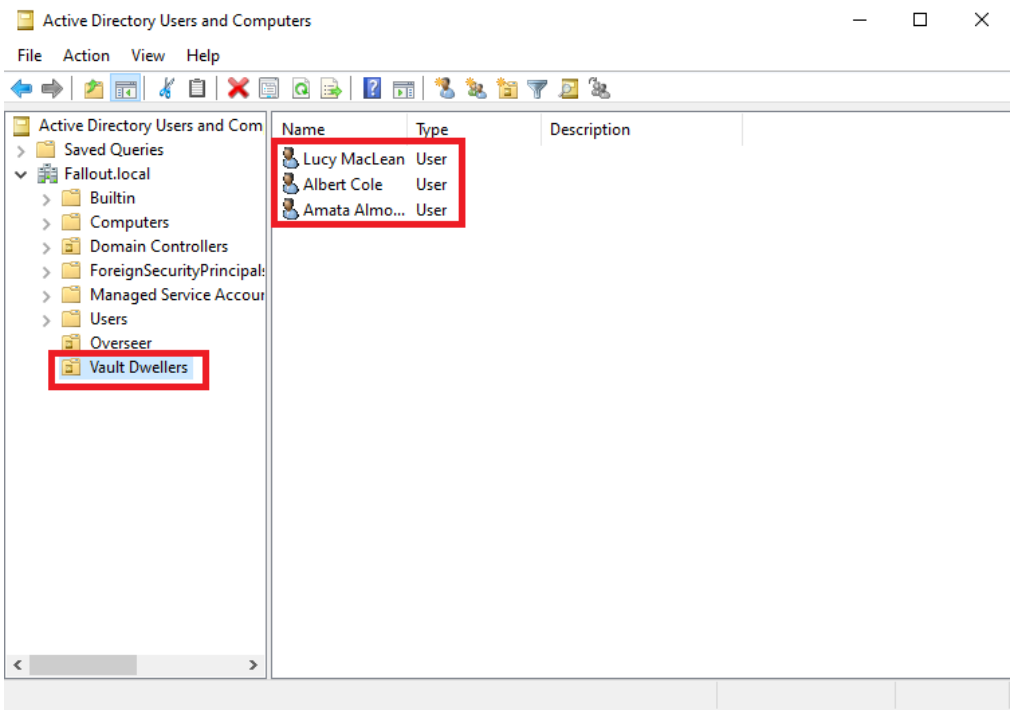


Fig 6. Creazione Organizzazione Vault Dwellers e User

Per facilitare la gestione dei permessi, è stato creato un **Gruppo di Sicurezza** chiamato **"Abitanti"**, nel quale sono stati inseriti gli utenti standard (Lucy, Albert, Amata). L'uso dei gruppi è una best practice che evita di dover assegnare permessi a ogni singolo utente manualmente.

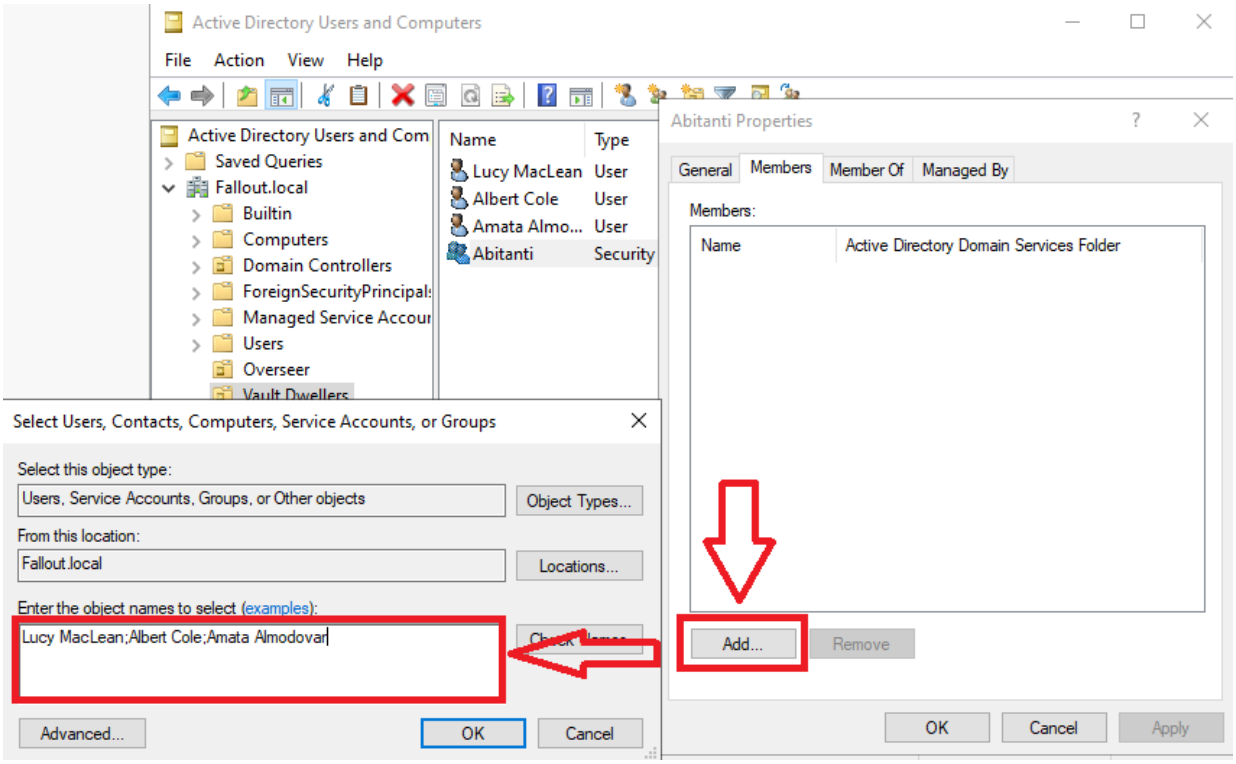


Fig 7. *Creazione Gruppi*

Seguendo la medesima procedura operativa, è stato creato un secondo Gruppo di Sicurezza denominato **"Supervisori"**. All'interno di questo gruppo è stato aggiunto l'utente **Hank MacLean**.

Questa operazione è fondamentale per garantire una corretta segregazione dei ruoli: in futuro, i permessi di accesso alla cartella "Top Secret" verranno assegnati direttamente al gruppo Supervisori e non al singolo utente Hank, facilitando la gestione amministrativa qualora il ruolo di Overseer dovesse passare a un altro utente.

5. Struttura Active Directory: Organizzazione ed Utenti

Sul disco locale del server è stata creata una cartella radice chiamata **Vault Tech Documents**, contenente due sottocartelle con livelli di sicurezza differenti:

- **Top Secret:** Dati riservati solo al Supervisore.
- **Vault Events:** Dati pubblici per tutti gli abitanti.

Per la cartella **Top Secret**, sono state modificate le impostazioni di **Condivisione Avanzata** e i permessi di sicurezza. È stato rimosso l'accesso al gruppo **Everyone** ed è stato aggiunto esplicitamente solo l'utente "*Sovrintendente*" con controllo completo, negando o omettendo l'accesso agli altri gruppi.

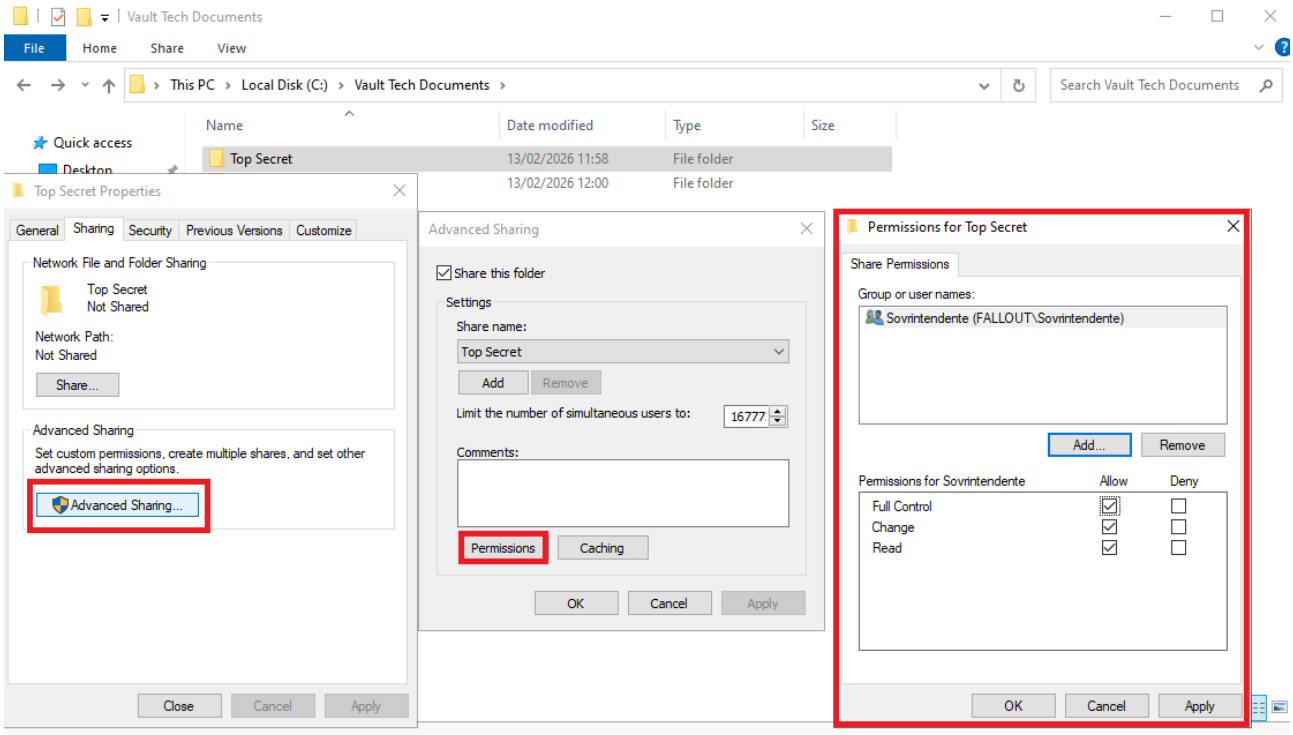


Fig 8. Permessi della cartella Top Secret

6. Testing e Verifica degli Accessi

Per verificare la corretta applicazione delle **policy di sicurezza**, sono stati effettuati test di accesso con due account diversi.

Test A: Accesso Utente Standard

Fig 9. Login come Utente Lucy MacLean

Effettuando il login su una macchina client con l'utente **Lucy MacLean** (membro del gruppo *Abitanti*) L'utente riesce a visualizzare le cartelle di rete condivise dal server **Vault101Server**.

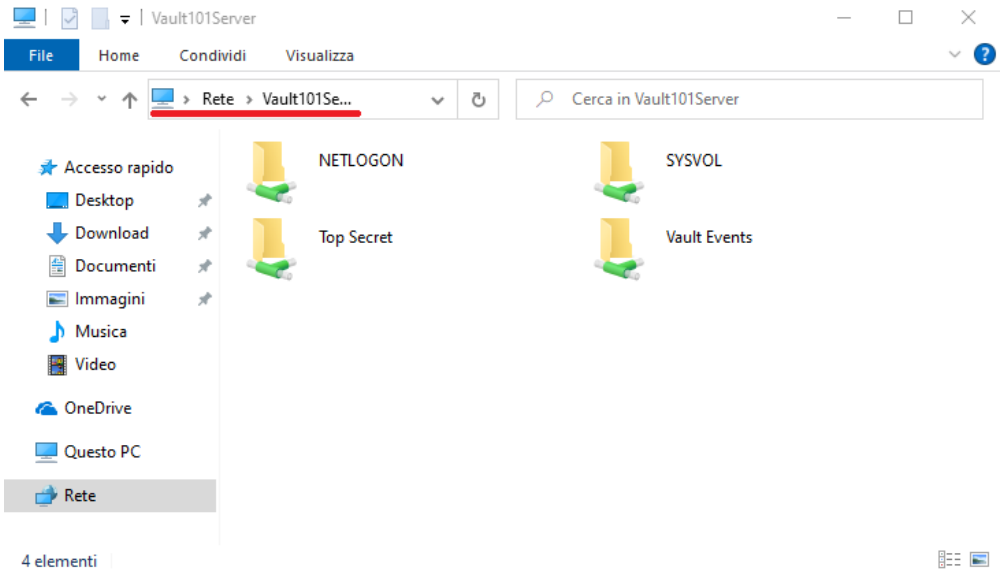


Fig 10. Accesso alle cartelle del server

Tentando di aprire la cartella **Top Secret**, il sistema restituisce correttamente un errore di "Accesso Negato", confermando che le restrizioni sono attive.

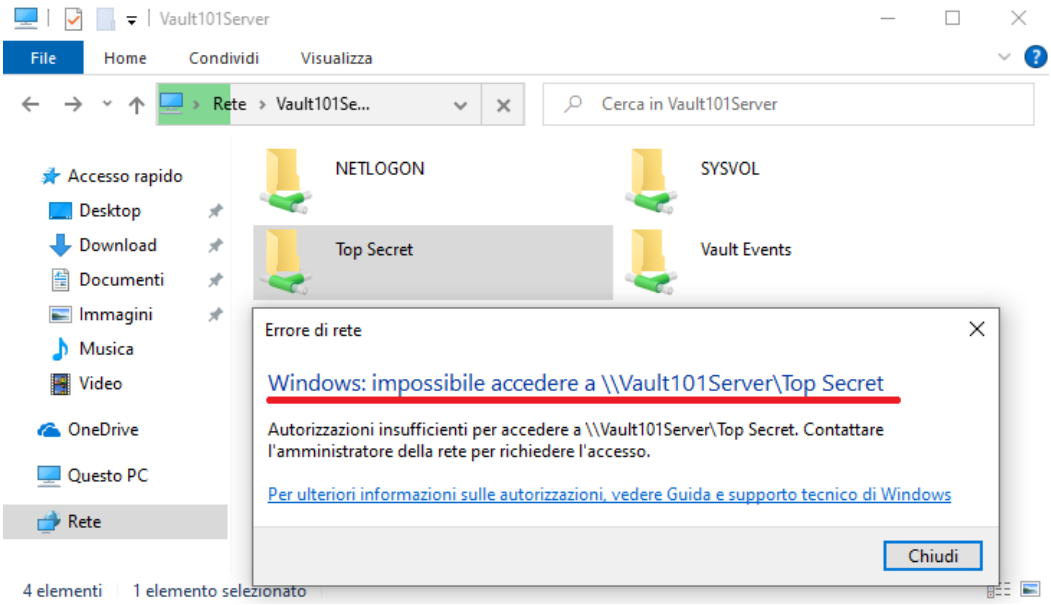


Fig 11. Accesso negato per la cartella Top Secret

Al contrario, l'accesso alla cartella pubblica **Vault Events** è consentito.

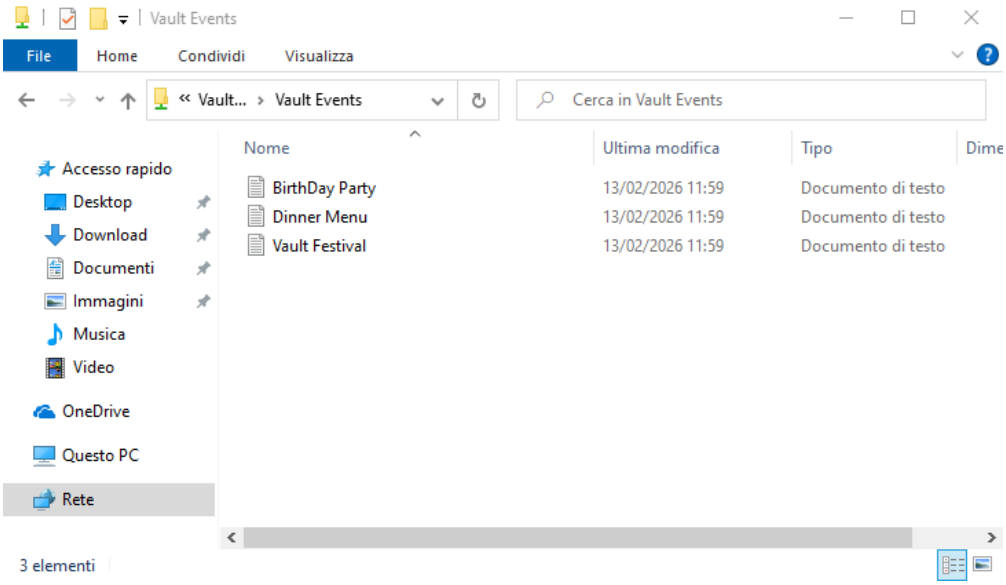


Fig 12. Accesso consentito per la cartella Vault Events

Test B: Accesso Utente Privilegiato

Fig 13. Login come Utente Hank MacLean

Effettuando il logout e rientrando come **Hank MacLean** (Overseer) notiamo subito come l'utente ha pieno accesso alla cartella **Top Secret** e può visualizzare i file riservati (come "Water Chip" e "Experiments"), dimostrando che la configurazione dei permessi basata sui ruoli funziona correttamente.

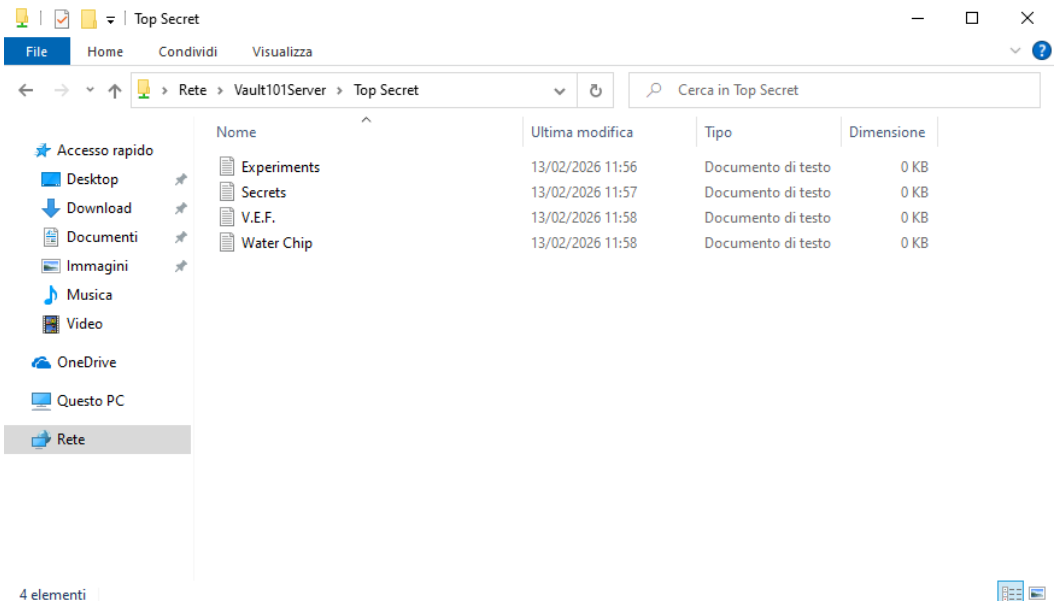


Fig 14. Libero Accesso a cartella Top Secret

7. Conclusione e Considerazioni

L'esercitazione ha permesso di configurare con successo un server Windows 2022 in ambiente simulato. Attraverso la creazione del dominio **Fallout.local**, è stato possibile centralizzare la gestione delle identità.

I test finali confermano che:

1. Il server è correttamente raggiungibile in rete.
2. La struttura delle Organizational Unit rispecchia la gerarchia aziendale (o, in questo caso, del Vault).
3. I permessi sulle cartelle impediscono accessi non autorizzati, garantendo la confidenzialità dei **dati sensibili** e la disponibilità dei **dati pubblici**.

Questa configurazione rispetta il principio del ***Least Privilege*** (privilegio minimo), fondamentale nella cybersecurity per ridurre la superficie di attacco interna.

L'attività si è svolta linearmente e **non sono state riscontrate problematiche tecniche o errori di configurazione** durante le fasi di setup e testing.