Report Gestione Identità e Accessi (IAM) su Windows Server 2022

Autore: Nicola Cassandra
Data: 13/02/2026
Progetto: Infrastruttura "Mecna Discography"

1. Obiettivo del Progetto

Lo scopo dell'esercitazione è stato simulare un ambiente aziendale (un'etichetta discografica) applicando il principio del **Least Privilege** (Minimo Privilegio). L'obiettivo era garantire che gli artisti (Utenti) potessero accedere esclusivamente ai progetti (Album) a cui hanno collaborato e, all'interno di essi, modificare solo le tracce (File) di loro competenza, pur mantenendo visibile la struttura completa dell'album.

2. Configurazione Active Directory (IAM)

Per rispecchiare la discografia dell'artista Mecna, è stata creata una struttura gerarchica in Active Directory Users and Computers (ADUC).

- **Organizational Unit (OU):** Creata la OU `Artisti` per contenere le identità.
- **Gruppi di Sicurezza:** Sono stati creati gruppi basati sui "Cast" degli album per gestire l'accesso macroscopico alle cartelle.
    - `GRP_Cast_DiscoInverno`: Include Mecna, Ghemon, Andrea Nardinocchi, ecc.
    - `GRP_Cast_Neverland`: Include Mecna, Luche, Tedua, ecc.

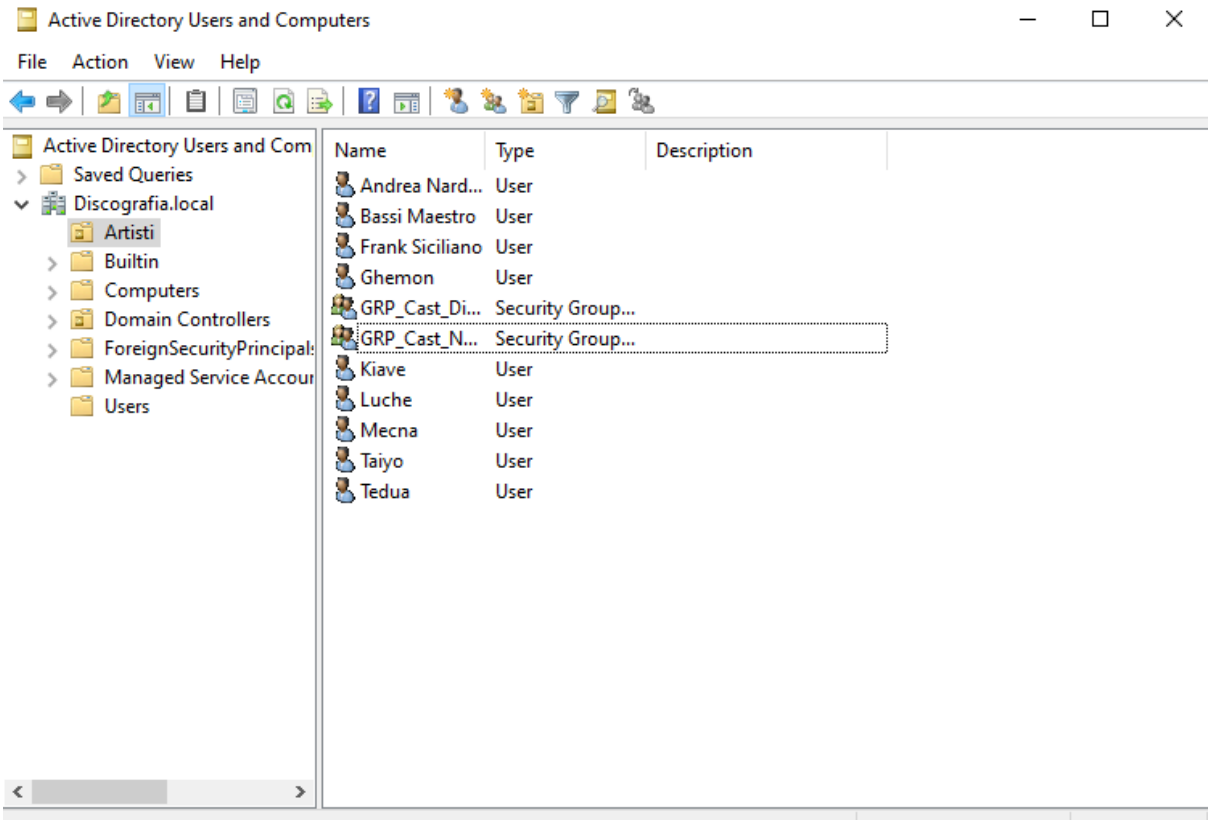

Fig. 1 - Struttura della Organizational Unit con gli utenti (artisti) e i Security Groups creati per la gestione dei permessi.

3. Strategia dei Permessi (ACL e NTFS)

La sicurezza è stata configurata su due livelli distinti per soddisfare il requisito: *"Vedere tutto, toccare solo il proprio"*.

A. Livello Cartella (Browsing)

Alle cartelle radice degli album (es. `Disco_Inverno` e `Neverland`) sono stati assegnati permessi al gruppo `GRP_Cast_...` corrispondente.

- **Permesso:** `List Folder Contents` e `Read`.
- **Risultato:** Gli artisti possono entrare nella cartella dell'album e vedere la lista dei file, ma non hanno permessi di scrittura generici.

B. Livello File (Accesso Granulare)

Per i singoli file `.txt` (le canzoni), è stato necessario deviare dalla configurazione standard.

- **Problema Riscontrato (Ereditarietà):** Inizialmente, utenti come "Ghemon" potevano leggere i testi di "Andrea Nardinocchi" perché ereditavano i permessi di lettura dalla cartella madre.

- **Soluzione Applicata:** È stata **disabilitata l'ereditarietà** sui singoli file critici, convertendo i permessi in espliciti. Successivamente, sono stati rimossi i gruppi generici ed è stato aggiunto esclusivamente l'utente creatore della canzone (es. Andrea Nardinocchi) con permessi `Modify`, oltre agli amministratori.

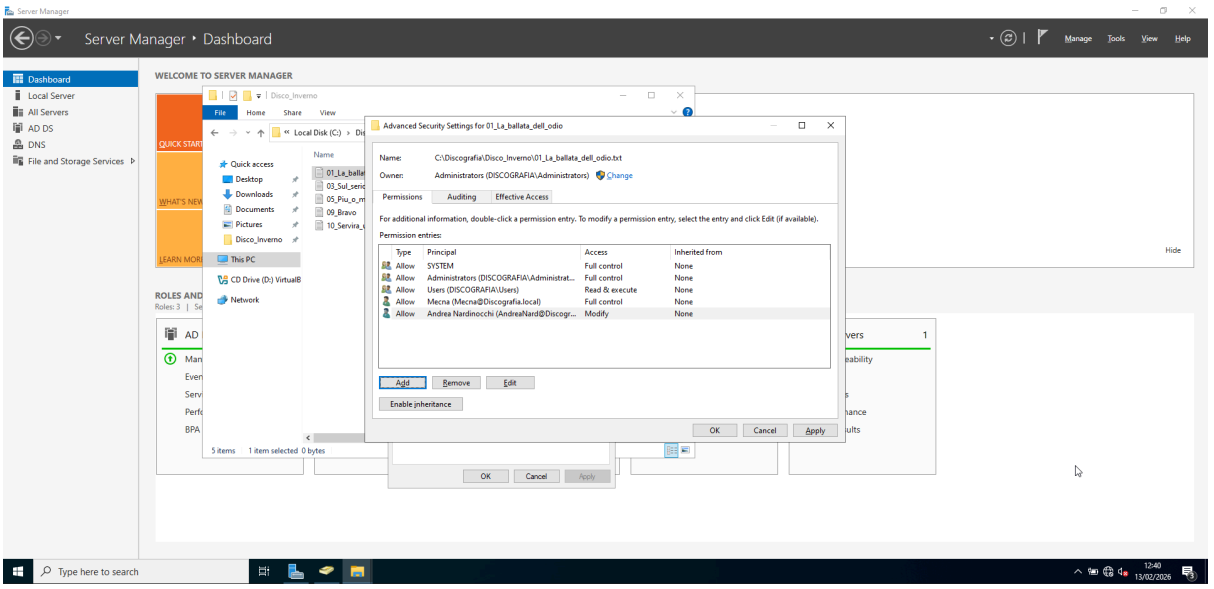

Fig. 2 - Configurazione avanzata di sicurezza: disabilitazione dell'ereditarietà e assegnazione esplicita dei permessi all'utente specifico per il singolo file.

4. Problematiche di Rete e Risoluzione

Durante la fase di test iniziale da una macchina client, è emerso un problema di visibilità delle risorse.

- **Errore:** Nonostante i permessi NTFS fossero corretti, la cartella `Discografia` non appariva esplorando la rete (`\\mecna`).
- **Causa:** Mancava la configurazione della **Condivisione SMB**. I permessi locali (Security) erano pronti, ma la "porta" di rete (Sharing) era chiusa.
- **Risoluzione:** È stata attivata la condivisione avanzata sulla cartella `Discografia`, garantendo che le regole di sicurezza NTFS rimanessero l'unica autorità per il blocco degli accessi.

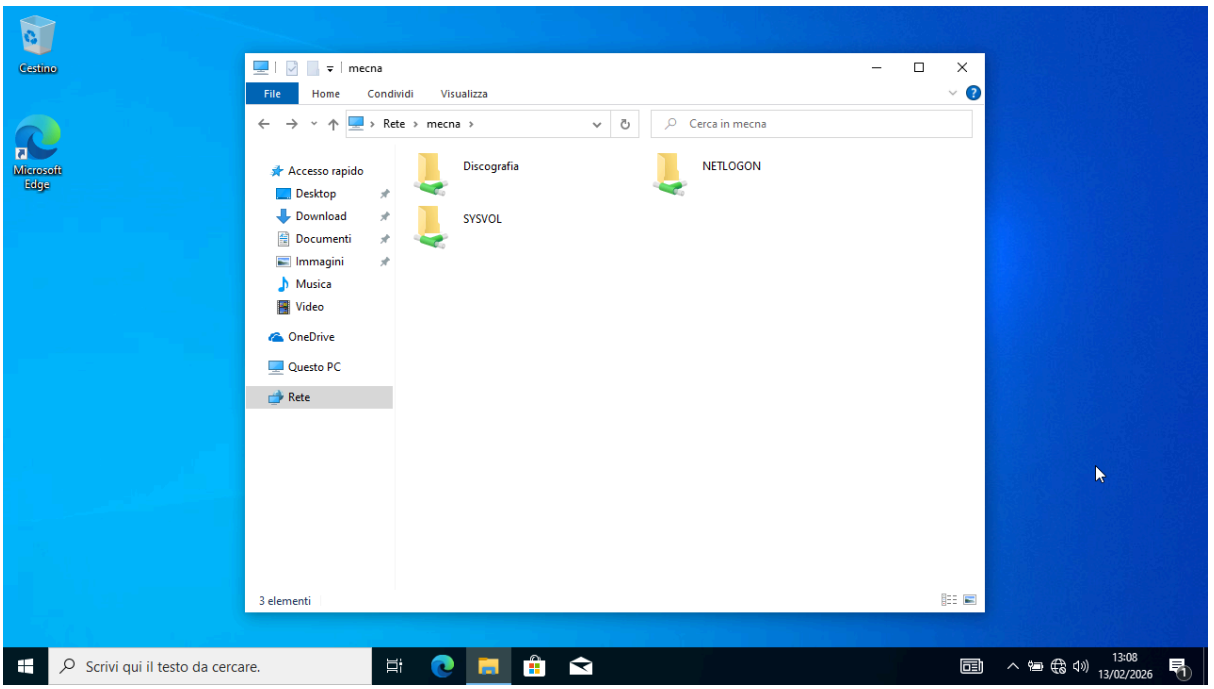

Fig. 3 - Verifica dell'accesso alle risorse di rete dopo la corretta configurazione della condivisione SMB sulla cartella "Discografia".

5. Verifica e Testing (Validation)

Il sistema è stato sottoposto a test di accesso loggandosi con l'utente **Ghemon** (appartenente al cast di *Disco Inverno* ma non di *Neverland*).

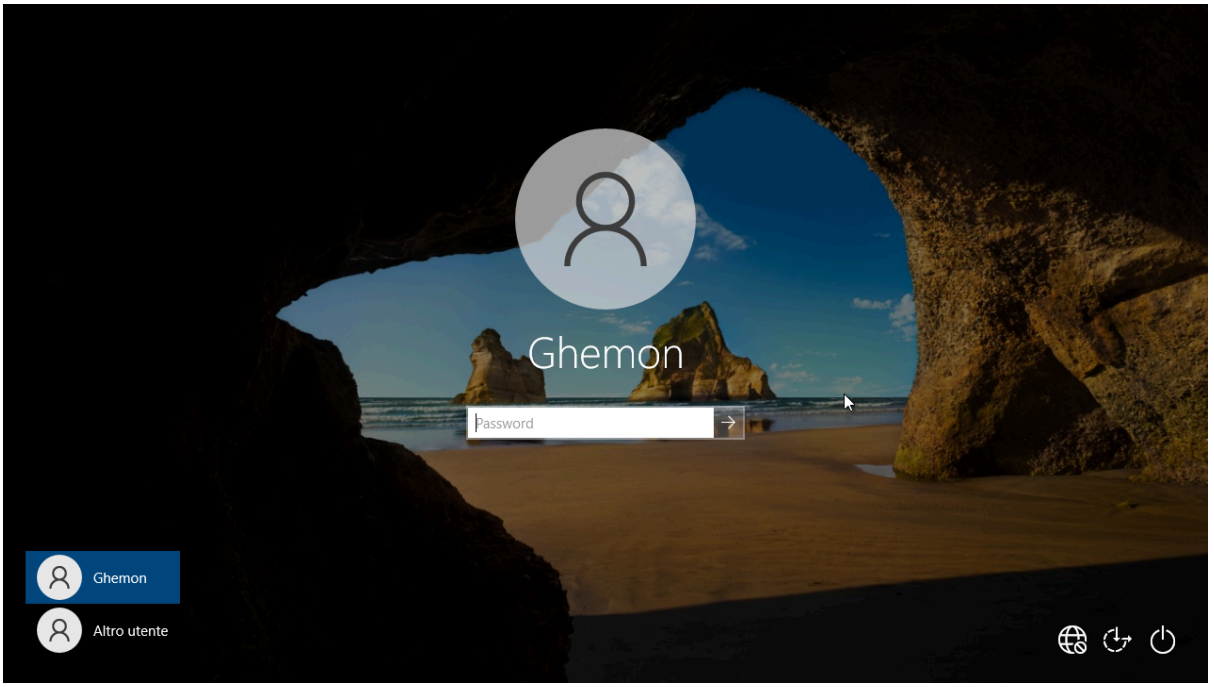

Fig. 4 - Login sul client Windows 10 con le credenziali dell'utente di test "Ghemon".

Test 1: Isolamento tra Album

Tentativo di accesso alla cartella `Neverland` da parte di Ghemon.

- **Esito: NEGATO**. Il sistema ha bloccato correttamente l'utente poiché non fa parte del gruppo `GRP_Cast_Neverland`.

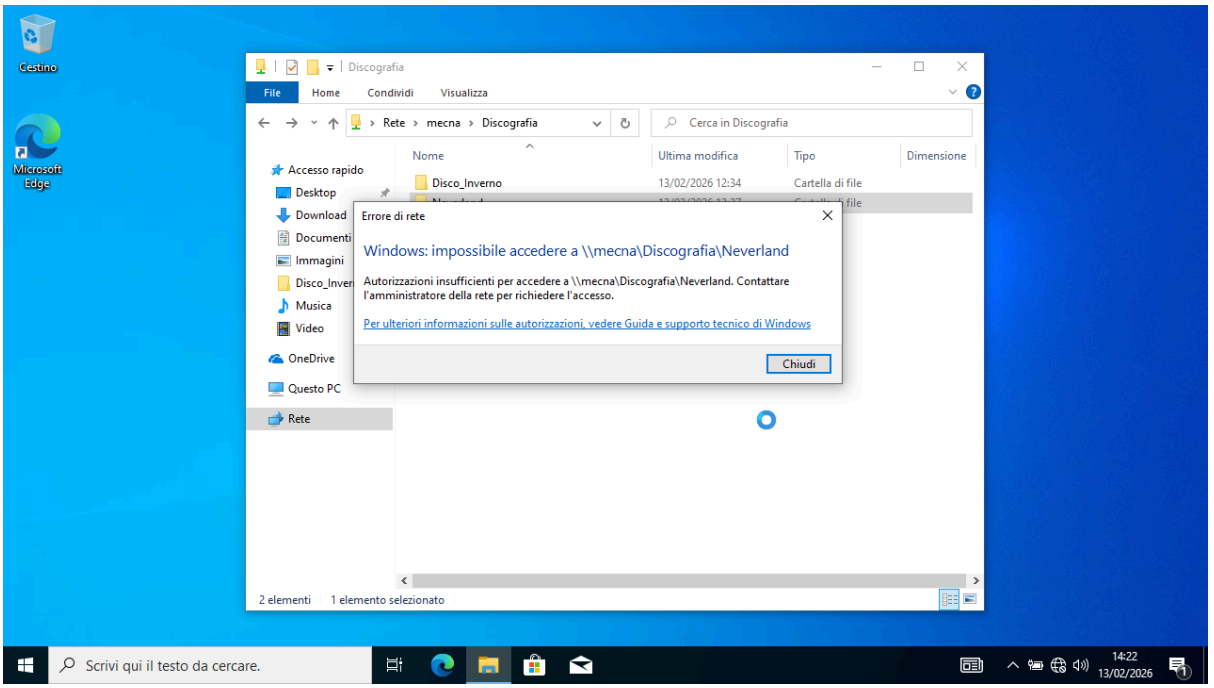

Fig. 5 - Prova di efficacia delle ACL: l'utente viene bloccato tentanto di accedere a un album a cui non ha collaborato.

Test 2: Sicurezza a livello di File (Intra-Album)

Tentativo di apertura del file `05_Piu_o_meno.txt` (di proprietà di Kiave/Frank Siciliano) all'interno della cartella accessibile `Disco_Inverno`.

- **Esito: NEGATO**. Ghemon può vedere il file nell'elenco, ma non può aprirlo, confermando il successo della rottura dell'ereditarietà.

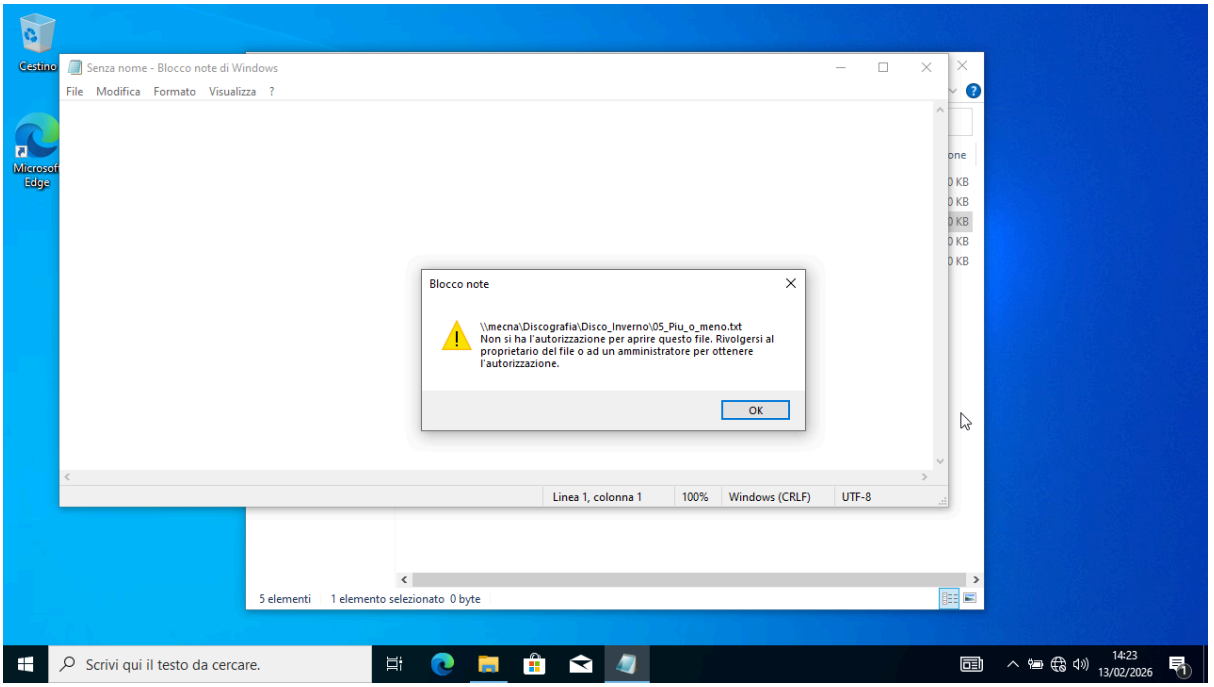

Fig. 6 - Granularità dei permessi: l'utente accede alla cartella ma riceve errore tentando di aprire un file di cui non è proprietario.

6. Conclusioni

L'esercizio ha dimostrato come la combinazione di **Gruppi Active Directory**, gestione dell'**Ereditarietà NTFS** e configurazione delle **Share di Rete** permetta di creare un ambiente sicuro e compartimentato, rispettando rigorosamente le policy di accesso aziendali.