Report di Progetto: Implementazione di un'Infrastruttura di Dominio su Active Directory con Gestione Ruoli e Risorse

Data: 6 Giugno 2025

Autore: Stefano Gugliotta

Oggetto: Documentazione dell'implementazione di un'infrastruttura di dominio basata su Windows Server 2022 e Windows 10 Client per la gestione centralizzata di utenti, gruppi, permessi e criteri di gruppo, ispirata al contesto di Final Fantasy VII e VIII.

---

1. Introduzione al Progetto

Il presente report documenta le fasi di progettazione, implementazione e verifica di un'infrastruttura di rete simulata, basata su un ambiente Microsoft Windows Server 2022 come Domain Controller e un client Windows 10 Debloated. L'obiettivo principale era quello di creare un ambiente controllato che riproducesse scenari di gestione utenti e risorse tipici di un'organizzazione, con una particolare attenzione alla granularità dei permessi e all'applicazione centralizzata dei criteri. Per rendere il progetto più coinvolgente e didattico, la struttura e la nomenclatura sono state ispirate all'universo dei videogiochi Final Fantasy VII e VIII, attribuendo ruoli specifici ai vari dipartimenti e personaggi.

Questo progetto mira a dimostrare la capacità di:

- Configurare un Domain Controller (DC) e un servizio DNS integrato, pilastri di un'infrastruttura di dominio robusta.
- Strutturare logicamente un'organizzazione tramite Unità Organizzative (OU), migliorando la gestibilità.
- Creare e gestire account utente e gruppi di sicurezza in Active Directory, essenziali per il controllo degli accessi.
- Implementare permessi di accesso granulari su risorse condivise (cartelle) utilizzando i principi dei permessi NTFS e di condivisione, garantendo la sicurezza dei dati.
- Applicare criteri di gruppo (GPO) per configurare centralmente le impostazioni utente e computer, automatizzando la gestione delle policy.
- Diagnosticare e risolvere problematiche comuni relative all'accesso e all'applicazione dei criteri, dimostrando capacità di troubleshooting.

2. Architettura della Soluzione

L'infrastruttura è stata realizzata utilizzando due macchine virtuali, configurate per emulare un ambiente di rete aziendale standard:

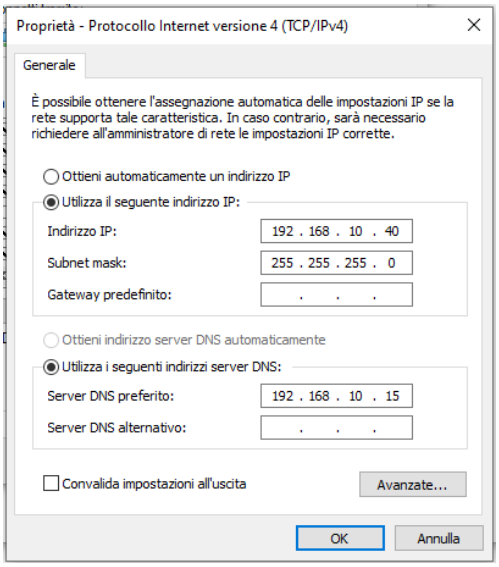
- **Server:** Una VM Windows Server 2022 Standard, configurata per ospitare il ruolo di Domain Controller (DC) e il servizio DNS per il dominio midgar.local. Il server è stato denominato MidgarServer.
- **Client:** Una VM Windows 10 Debloated, selezionata per la sua leggerezza ma anche come caso di studio per potenziali problematiche di compatibilità con le GPO. Il client è stato unito al dominio midgar.local e denominato WorldofFinalFantasy.

Entrambe le macchine virtuali operano su una rete interna isolata, con il Domain Controller che funge da server DNS primario per garantire la corretta risoluzione dei nomi e l'autenticazione nel dominio.

2.1 Configurazione della Rete

Una configurazione di rete accurata è stata il primo passo per garantire la corretta comunicazione e l'integrazione delle macchine nell'ambiente di dominio.

Server (MidgarServer): Al server è stato assegnato un indirizzo IP statico (192.168.10.15). Il DNS primario è stato configurato per puntare a se stesso (utilizzando l'indirizzo di loopback 127.0.0.1 o il suo IP statico 192.168.10.15), essenziale per la corretta operatività dei servizi di Active Directory Domain Services (AD DS) e DNS integrato. Questo garantisce che il server possa risolvere correttamente i nomi all'interno del proprio dominio.



Client (WorldOfFinalFantasy): Anche il client Windows 10 è stato configurato con un indirizzo IP statico (192.168.10.40) sulla stessa sottorete del server (255.255.255.0). Crucialmente, il server DNS preferito del client è stato impostato sull'indirizzo IP del Domain Controller (192.168.10.15), consentendogli di individuare i servizi di Active Directory e di risolvere i nomi di dominio per l'autenticazione.

3. Implementazione di Active Directory su Windows Server 2022

La configurazione del Domain Controller è il cuore dell'infrastruttura, permettendo la gestione centralizzata degli utenti e delle risorse.

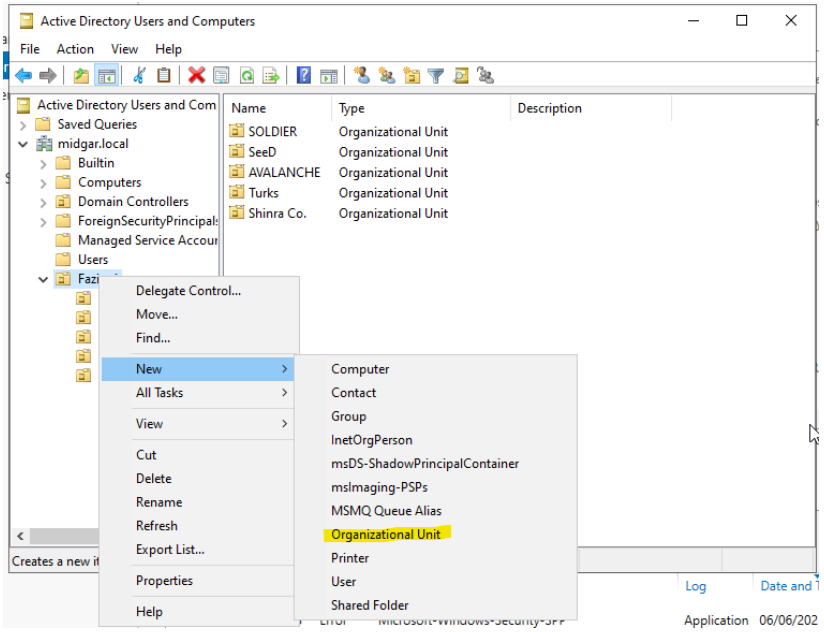
3.1 Promozione a Domain Controller e Creazione della Foresta

Il server Windows Server 2022 è stato promosso a Domain Controller, creando una nuova foresta con il nome di dominio radice midgar.local. Durante questo processo, è stata impostata la password per la modalità di ripristino dei servizi di directory (DSRM), una misura di sicurezza fondamentale per il ripristino del dominio.

3.2 Struttura delle Unità Organizzative (OU)

Per replicare una struttura organizzativa chiara e consentire un'applicazione granulare dei criteri di gruppo e dei permessi, sono state create diverse Unità Organizzative (OU) all'interno del dominio midgar.local. La struttura gerarchica è stata progettata come segue:

- **Fazioni**: OU principale che racchiude tutte le divisioni operative.
    - **SOLDIER**: Per i guerrieri d'élite (es. Cloud Strife, Sephiroth).
    - **SeeD**: Per i mercenari addestrati dell'accademia (es. Squall Leonhart).
    - **AVALANCHE**: Per il gruppo ribelle.
    - **Turks**: Per la divisione investigativa e di intelligence della Shinra.

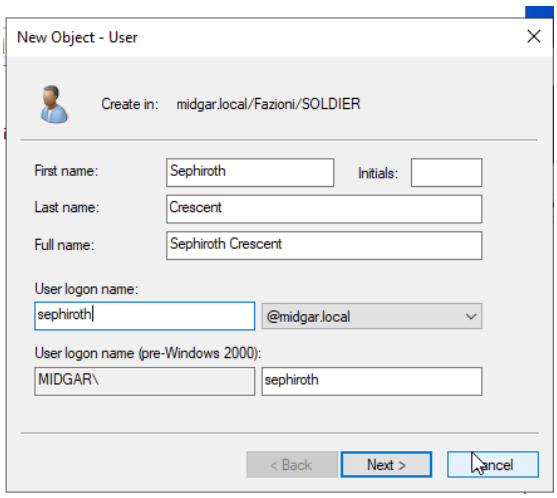


    - **Shinra Co.**: Per la direzione e il personale amministrativo della Shinra.

Questa organizzazione logica facilita l'applicazione mirata di Group Policy Objects (GPO) e la delega dell'amministrazione.

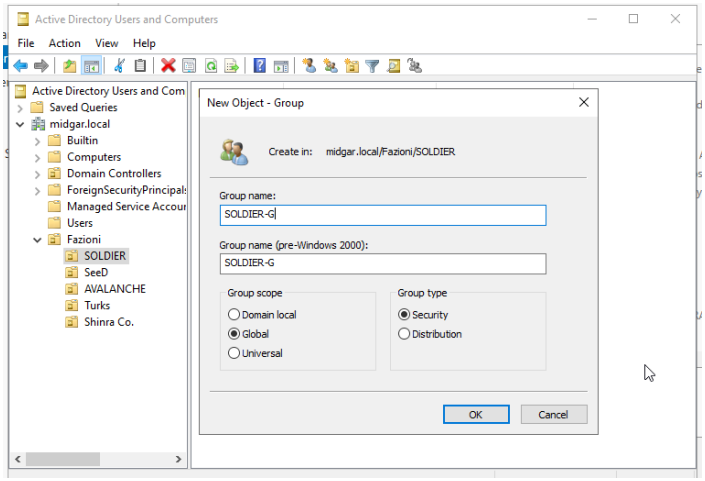
3.3 Creazione di Utenti e Gruppi di Sicurezza

All'interno di ciascuna OU, sono stati creati specifici account utente e gruppi di sicurezza. Gli utenti sono stati assegnati ai rispettivi gruppi, che a loro volta sono stati utilizzati per gestire l'accesso alle risorse condivise. Questo approccio basato sui gruppi semplifica la gestione dei permessi, specialmente in ambienti con numerosi utenti.



- **Utenti Esempi:**
    - Cloud Strife (OU SOLDIER)
    - Sephiroth Crescent (OU SOLDIER)
    - Squall Leonhart (OU SeeD)
    - Barret Wallace (OU AVALANCHE)
    - Reno Turks (OU Turks)
    - Rufus Shinra (OU Shinra Co.)

- **Gruppi di Sicurezza:** Per ogni fazione/dipartimento, è stato creato un gruppo di sicurezza Globale. Gli utenti sono stati resi membri del loro gruppo corrispondente (es. Cloud Strife e Sephiroth Crescent sono membri di SOLDIER-G).
    - SOLDIER-G
    - SeeD-G
    - AVALANCHE-G
    - Turks-G
    - Shinra Co. (per il gruppo di gestione)



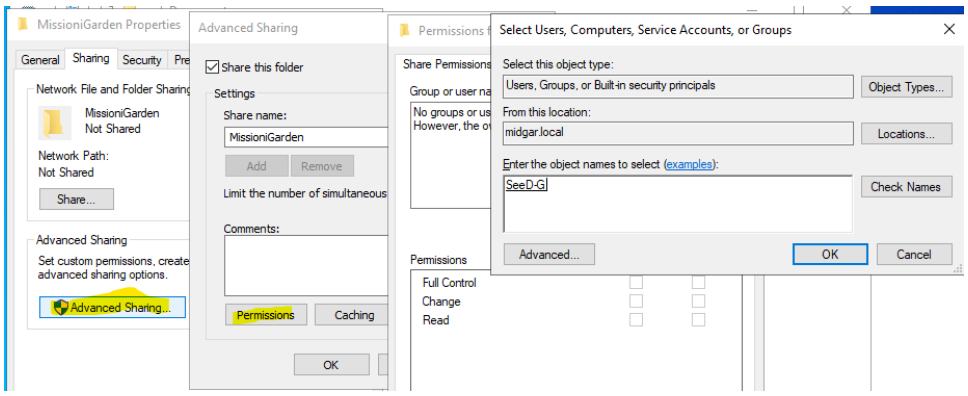
4. Gestione delle Cartelle Condivise e Permessi NTFS

Per controllare l'accesso ai dati sensibili e operativi, sono state create diverse cartelle sul server, con permessi configurati in modo granulare per garantire che solo i gruppi autorizzati potessero accedervi. Le cartelle sono state collocate all'interno della cartella C:\Users\Administrator\Documents\ del server per comodità.

Le cartelle create e i gruppi associati sono:

- **DatiMako**: Accesso per il gruppo SOLDIER-G.
- **MissioniGarden**: Accesso per il gruppo SeeD-G.
- **CovoRibelle**: Accesso per il gruppo AVALANCHE-G.
- **FileConfidenziali**: Accesso per il gruppo Turks-G.
- **ProgettoJenova**: Accesso per il gruppo Shinra Co..

4.1 Configurazione dei Permessi di Condivisione (Share Permissions)

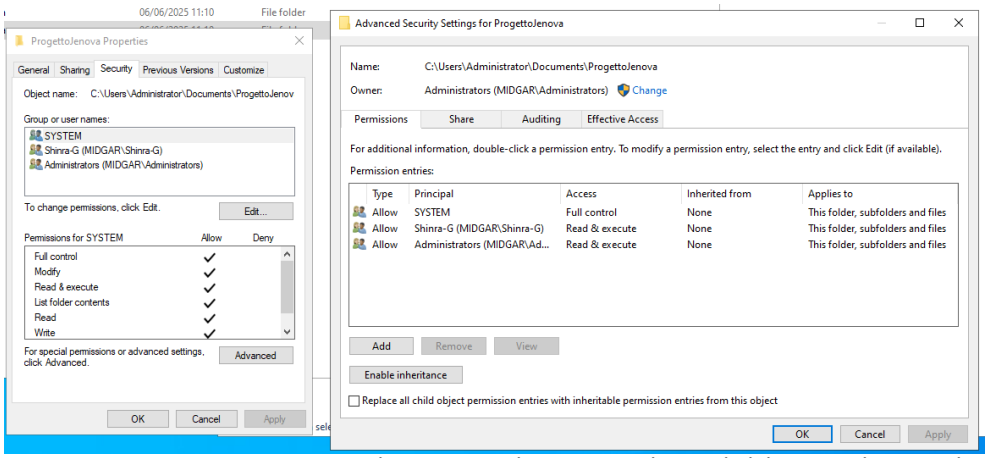


Per ciascuna cartella, i permessi di condivisione sono stati configurati per consentire l'accesso di rete solo ai gruppi specifici (e al gruppo Administrators per la gestione). Questo garantisce un primo livello di protezione a livello di rete. Per semplicità e per affidare il controllo granulare ai permessi NTFS, in alcuni

casi è stato concesso il controllo completo al gruppo Everyone a livello di condivisione, delegando interamente la sicurezza effettiva ai permessi NTFS.

4.2 Configurazione dei Permessi NTFS (File System Permissions)

Questa è stata la fase più critica per la gestione della sicurezza dei dati. Per ogni cartella, l'ereditarietà dei permessi è stata **disabilitata** dalla cartella padre

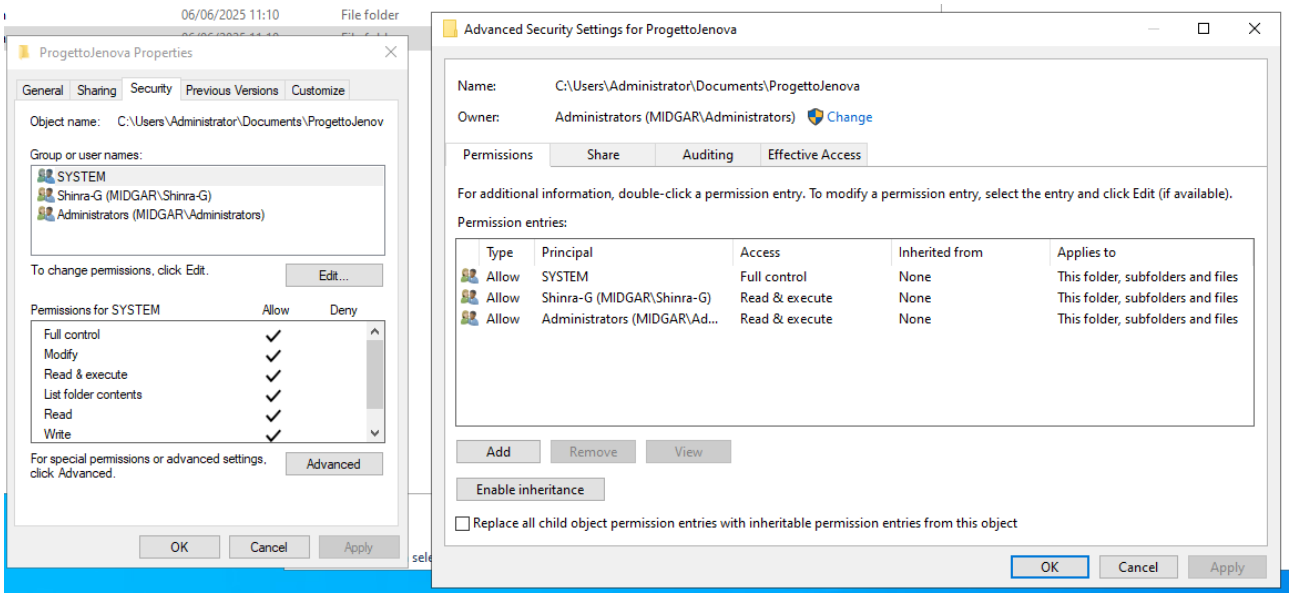


(C:\Users\Administrator\Documents\) e sono stati assegnati permessi espliciti solo ai gruppi desiderati, garantendo un controllo preciso.

Per ogni cartella, i permessi NTFS sono stati configurati come segue:

- **SYSTEM**: Controllo Completo (necessario per le operazioni di sistema).
- **Administrators** (o Domain Admins): Controllo Completo (per la gestione da parte degli amministratori del dominio).
- **Gruppo specifico** (es. SOLDIER-G per DatiMako, Shinra Co. per ProgettoJenova): Controllo Completo.

È stato assicurato che nessun altro gruppo generico (come Users, Authenticated Users, Everyone) avesse permessi su queste cartelle, a meno che non fosse strettamente necessario per un accesso generico di sola lettura.



5. Integrazione del Client nel Dominio

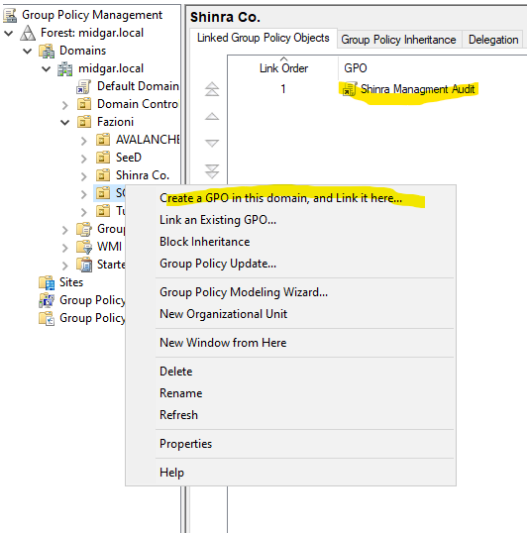
Il client Windows 10 Debloated è stato configurato per diventare un membro del dominio midgar.local, consentendo agli utenti creati in Active Directory di autenticarsi sulla macchina client e accedere alle risorse di dominio.

5.1 Unione al Dominio

Il nome del computer client è stato modificato in WorldofFinalFantasy. Successivamente, il client è stato unito al dominio midgar.local utilizzando le credenziali di un account amministrativo del dominio (es. l'account Administrator di midgar.local).

6. Implementazione dei Criteri di Gruppo (GPO)

Per dimostrare la gestione centralizzata delle configurazioni, sono state create e collegate delle Group Policy Objects (GPO) alle Unità Organizzative pertinenti.

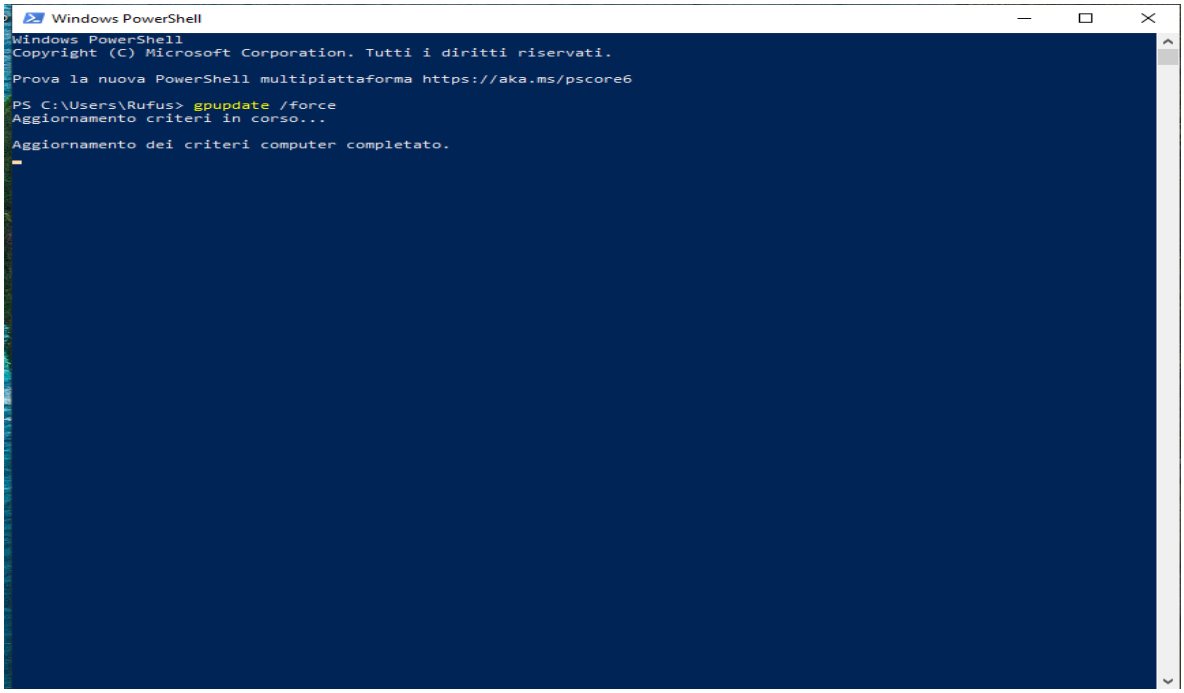


6.1 Creazione e Collegamento della GPO

È stata creata una GPO denominata Shinra Management Audit e collegata all'OU Shinra Co., con l'intento di applicare specifiche policy agli utenti di quella fazione. Ulteriori GPO possono essere create e collegate per altre OU, definendo impostazioni specifiche per ciascun ruolo.

6.2 Applicazione dei Criteri

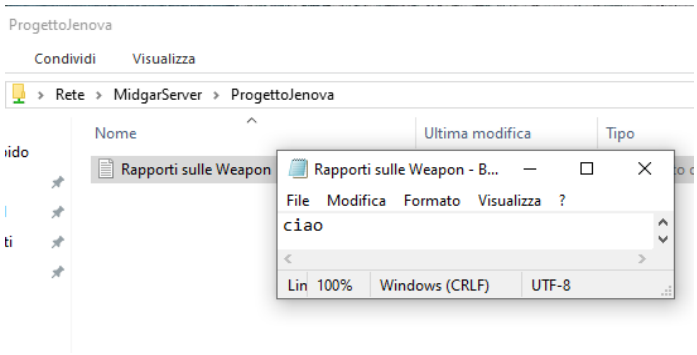
Per forzare l'applicazione immediata dei nuovi criteri sul client, è stato eseguito il comando gpupdate /force sul client Windows 10, assicurando che le impostazioni fossero scaricate e applicate.



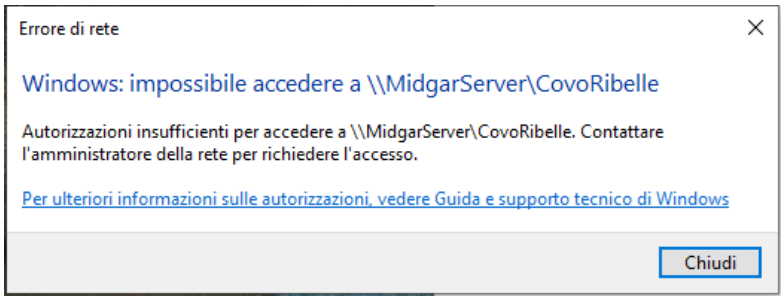
7. Test e Verifica Funzionale

La fase di test è stata cruciale per convalidare l'efficacia delle configurazioni implementate e assicurarsi che gli utenti avessero i permessi appropriati.

7.1 Test di Accesso alle Cartelle Condivise



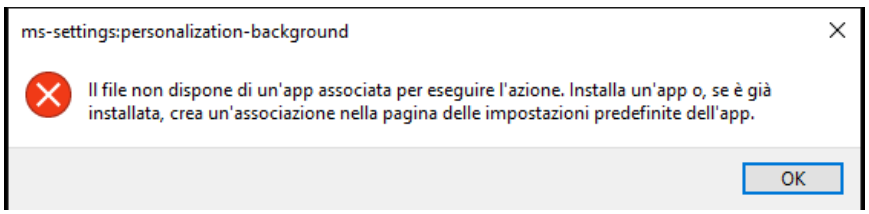
- **Accesso Riuscito:** L'utente Rufus Shinra, membro del gruppo Shinra Co., ha effettuato l'accesso al client WorldOfFinalFantasy e ha navigato con successo alla cartella \\MidgarServer\ProgettoJenova. Ha potuto creare e modificare file all'interno di questa cartella, confermando che i permessi di Controllo Completo erano stati correttamente applicati per il suo gruppo.
- **Accesso Negato:** Successivi test con Rufus Shinra (e analogamente con altri utenti su cartelle non autorizzate) hanno confermato che l'accesso alle altre cartelle condivise (es. DatiMako, MissioniGarden) veniva correttamente negato. Questo dimostra l'efficacia della configurazione dei permessi NTFS combinata con i permessi di condivisione, impedendo l'accesso non autorizzato ai dati specifici di altre fazioni.



7.2 Test dell'Applicazione delle GPO

I test hanno mostrato che le GPO base (come la disabilitazione dell'accesso al Pannello di controllo, se implementata) venivano applicate correttamente sul client Windows 10 Debloated, a dimostrazione che il sistema client riceveva ed elaborava i criteri di gruppo dal Domain Controller.

- **Problematica dello Sfondo Desktop:** È stato riscontrato un problema specifico con l'applicazione della GPO relativa all'impostazione dello sfondo desktop. Nonostante la GPO fosse correttamente configurata e applicata dal server, il client Windows 10 Debloated non ha modificato lo sfondo. Questo è stato diagnosticato come una limitazione specifica della versione "Debloated" di Windows 10, che probabilmente ha rimosso o disabilitato componenti del sistema operativo



responsabili della gestione della personalizzazione dell'interfaccia utente in risposta ai criteri di gruppo. Il tentativo di accedere alle impostazioni di personalizzazione del sistema operativo ha generato un errore indicando l'assenza di un'app associata per l'azione.

8. Sfide Incontrate e Soluzioni Adottate

Durante l'implementazione e il test, sono state incontrate alcune sfide che hanno richiesto debugging e comprensione approfondita dei meccanismi di Active Directory e Windows.

- **Accesso Inaspettato alle Cartelle:** Inizialmente, gli utenti potevano accedere a cartelle non autorizzate. La diagnosi ha rivelato che la causa principale erano i permessi NTFS ereditati dalle cartelle genitore (C:\Users\Administrator\Documents\) che concedevano permessi generici a gruppi come Users o Authenticated Users.
    - **Soluzione:** Questo problema è stato risolto disabilitando esplicitamente l'ereditarietà dei permessi per ogni singola cartella condivisa e riapplicando manualmente solo i permessi necessari a SYSTEM, Administrators e al gruppo specifico di sicurezza designato, con "Controllo Completo". Questo ha garantito una segregazione rigorosa degli accessi.
- **Connettività Iniziale (Percorso di Rete):** Durante i primi test di accesso alle condivisioni, si è riscontrato un problema di connettività, con errori di "percorso non trovato".
    - **Soluzione:** La causa è stata identificata nell'utilizzo di \\dominio\ anziché \\nomeserver\ o \\IPserver\ per accedere alle condivisioni. L'adozione del percorso UNC diretto \\MidgarServer\NomeCondivisione ha risolto il problema, consentendo il corretto instradamento delle richieste.
- **Applicazione della GPO dello Sfondo Desktop sulla VM Debloated:** Come dettagliato in precedenza, l'impostazione dello sfondo desktop tramite GPO non è stata applicata.
    - **Soluzione:** Dopo aver verificato la corretta configurazione della GPO sul server, l'accessibilità del percorso UNC dell'immagine e la corretta ricezione della GPO da parte del client (gpupdate /force), è stato concluso che la causa risiedeva nelle modifiche profonde apportate dalla versione "Debloated" di Windows 10. La rimozione di componenti di personalizzazione o servizi correlati impedisce al sistema di elaborare questa specifica impostazione. Nonostante il problema non sia stato risolvibile con le GPO standard su questa VM, la comprensione del problema e la sua documentazione dimostrano la capacità di identificare e analizzare le limitazioni di un ambiente specifico.

9. Conclusioni

Il progetto ha permesso di implementare con successo un'infrastruttura di dominio funzionante, dimostrando le capacità di gestione di Active Directory, dalla creazione di OU, utenti e gruppi, all'applicazione di permessi granulari su risorse condivise e alla configurazione di criteri di gruppo. Le sfide incontrate e le relative soluzioni adottate hanno arricchito l'esperienza, fornendo preziose lezioni sul troubleshooting e sull'importanza di comprendere a fondo il comportamento dei sistemi operativi, specialmente in versioni modificate come la "Debloated".

L'ambiente di Final Fantasy ha fornito un contesto divertente e funzionale per esplorare concetti di sicurezza e gestione delle risorse che sono direttamente applicabili in contesti aziendali reali. Il sistema è ora pronto per supportare ulteriori espansioni e policy più complesse, fungendo da solida base per future esplorazioni nel campo dell'amministrazione di rete.