

Creazione e Gestione di Gruppi in Windows Server 2022

Introduzione e Obiettivo della Lezione

Lo scopo primario di questa esercitazione è familiarizzare con gli strumenti e le procedure di gestione dei gruppi di utenti all'interno dell'ambiente Windows Server 2022.

La gestione degli utenti e dei gruppi è un aspetto fondamentale dell'amministrazione di qualsiasi sistema operativo, specialmente in ambienti aziendali che utilizzano Windows Server 2022. L'organizzazione efficiente degli account utente in gruppi logici non solo semplifica l'amministrazione quotidiana, ma è anche un pilastro essenziale per mantenere la sicurezza e l'integrità delle risorse di sistema.

Durante questo esercizio ho potuto applicare concretamente i principi del controllo degli accessi basato sui ruoli (RBAC), comprendendo come la corretta configurazione dei gruppi e dei permessi NTFS possa proteggere efficacemente le risorse aziendali da accessi non autorizzati.

Configurazione dell'Ambiente e Creazione degli Oggetti

Prima di iniziare l'esercitazione, ho effettuato l'accesso all'ambiente Windows Server 2022 con i permessi amministrativi necessari per gestire utenti, gruppi e risorse di sistema.

Creazione dei Gruppi di Sicurezza

Ho deciso di creare due gruppi di sicurezza distinti, ispirandomi allo scenario aziendale CyberLab S.r.l., in cui sono presenti due ruoli principali: gli analisti del Security Operation Center e gli amministratori di infrastruttura.

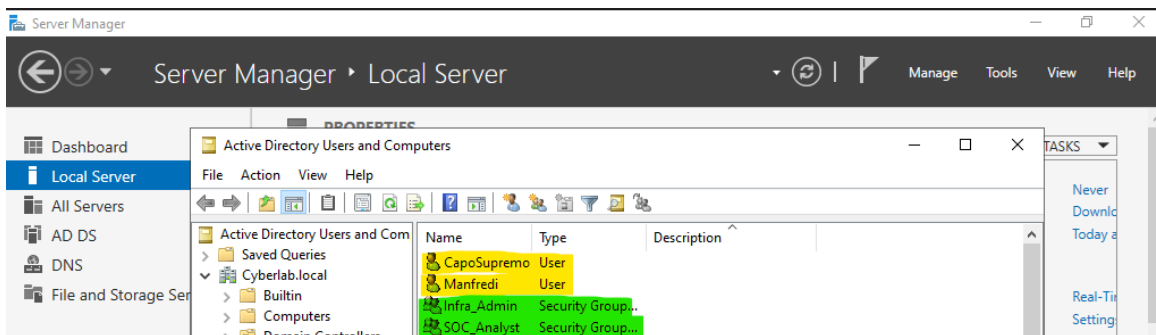
I gruppi scelti riflettono chiaramente i loro ruoli e responsabilità all'interno dell'organizzazione:

Gruppo	Scopo (Ruolo)	Membri Assegnati	Privilegio
SOC_Analyst	Analisi dati di sicurezza e monitoraggio log	Manfredi	Standard (Operativo)
Infra_Admin	Amministrazione infrastruttura e gestione server	CapoSupremo	Elevato (Amministrativo)

Creazione degli Utenti

Per ogni gruppo ho creato due utenti di test in Active Directory Users and Computers. La procedura seguita è stata la seguente:

1. Apertura della console ADUC tramite Server Manager → Tools → Active Directory Users and Computers
2. Click destro sul contenitore Users → New → User
3. Compilazione dei campi richiesti (nome, cognome, username di logon)
4. Assegnazione dell'utente al gruppo appropriato tramite la scheda Member Of nelle proprietà dell'utente.



Evidenziati Utenti(giallo) e Gruppi(verde)

Assegnazione dei Permessi e Architettura dei Dati

Per testare l'efficacia della gestione dei gruppi, ho creato due cartelle sul server (unità C:) che rappresentano diversi livelli di sensibilità dei dati. I permessi sono stati configurati utilizzando le Autorizzazioni NTFS (New Technology File System).

Architettura dei Permessi Implementata

C:\SOC_Data (Cartella Operativa per Analisti)

Funzione: Contiene log di sicurezza, report di analisi e strumenti di monitoraggio accessibili agli analisti del Security Operation Center.

Gruppi Assegnati: SOC_Analyst

Permessi NTFS:

- Read & Execute: Consentito
- List folder contents: Consentito
- Read: Consentito
- Write: Consentito
- Modify: Negato

- Full Control: Negato

Motivazione della scelta: Gli analisti devono poter leggere i log di sistema, eseguire tool di analisi che scrivono output nella cartella, e salvare report. Tuttavia non devono poter modificare i permessi della cartella o cancellare l'intera struttura, in quanto questo rappresenterebbe un rischio per l'integrità dei dati di sicurezza. Limitando i privilegi a Write senza Modify, si impedisce anche la cancellazione accidentale o malevola di file critici.

C:\Infra_AdminTools (Cartella Amministrativa)

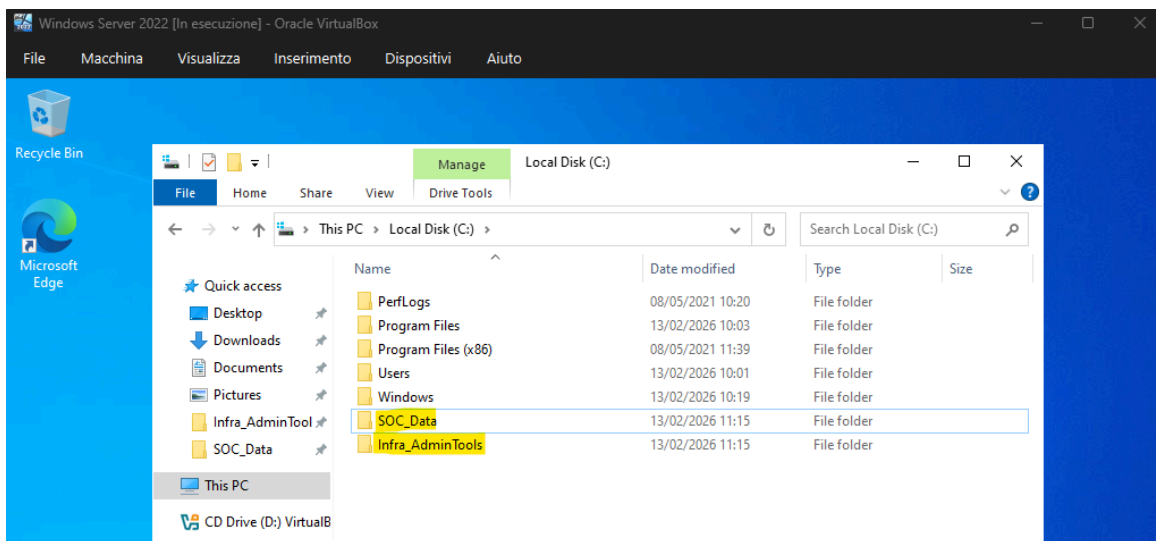
Funzione: Contiene script di amministrazione, strumenti di configurazione e documentazione tecnica accessibile solo agli amministratori di infrastruttura.

Gruppi Assegnati: Infra_Admin

Permessi NTFS:

- Full Control: Consentito (include automaticamente tutti i permessi sottostanti)

Motivazione della scelta: Gli amministratori di infrastruttura necessitano di controllo completo sulla cartella degli strumenti amministrativi per poter aggiungere nuovi script, aggiornare tool, modificare configurazioni e gestire la struttura della cartella stessa. Il Full Control include anche la capacità di modificare i permessi, essenziale per l'amministrazione a lungo termine.



Cartelle create in C:

Implementazione Tecnica dei Permessi

Dopo aver creato le cartelle sul server, ho proceduto con la configurazione dei permessi seguendo questi passaggi:

1. Click destro sulla cartella → Properties → Security
2. Click su "Advanced" per aprire le impostazioni avanzate di sicurezza
3. Disabilitazione dell'ereditarietà tramite il pulsante "Disable inheritance"

4. Selezione dell'opzione "Remove all inherited permissions from this object"
5. Rimozione dei permessi generici preesistenti (Users, CREATOR OWNER, Authenticated Users)
6. Aggiunta esplicita dei gruppi creati tramite il pulsante "Add"
7. Configurazione dei permessi specifici per ciascun gruppo
8. Applicazione delle modifiche e verifica della configurazione finale

Questo passo di disabilitazione dell'ereditarietà e rimozione dei permessi generici è cruciale per la sicurezza, in quanto garantisce che solo i gruppi esplicitamente definiti controllino l'accesso. In un ambiente di produzione reale, lasciare permessi ereditati o generici rappresenta una vulnerabilità, poiché utenti non previsti potrebbero ottenere accesso a risorse sensibili.

Verifica Remota e Risultati dei Test

I test sono stati eseguiti accedendo da una macchina client remota e utilizzando i percorsi di rete UNC (\\EPICODESERVER\Nome_Cartella_Shared), che rappresenta il metodo più realistico per simulare l'accesso di un utente di dominio alle risorse condivise del server.

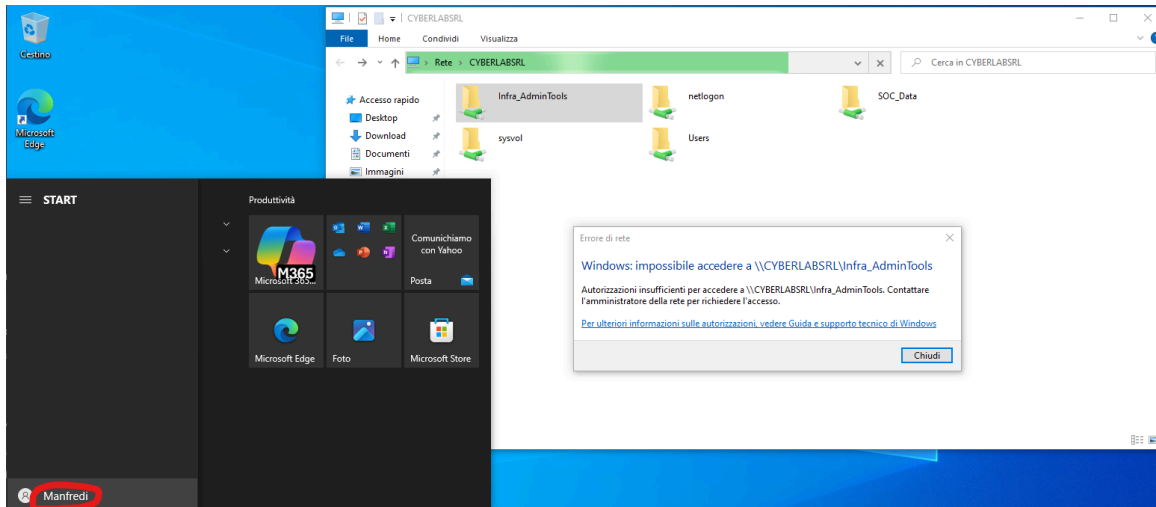
Test sulla Cartella SOC_Data

Utente di Test	Accesso alla Cartella	Tentativo di Modifica	Risultato Verificato
Manfredi (SOC_Analyst)	Consentito	Consentito (creazione file)	Corretto

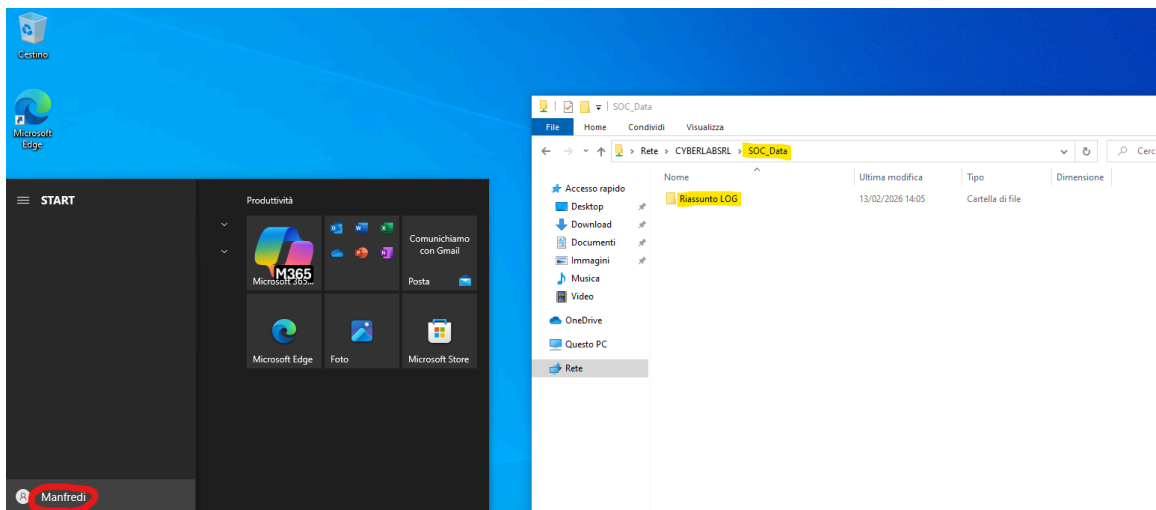
Il test ha confermato che gli utenti del gruppo SOC_Analyst possono accedere alla loro cartella di lavoro e creare file di report o log.

Test sulla Cartella Infra_AdminTools

Utente di Test	Accesso	Modifica	Cambio Permessi
Manfredi (SOC_Analyst)	Negato	N/A	N/A
CapoSupremo (Infra_Admin)	Consentito	Consentito	Consentito



Accesso negato con l'utente Manfredi



Accesso consentito + creazione cartella "Riassunto LOG" con l'utente Manfredi

Anche in questo caso i risultati sono stati conformi alle aspettative: gli analisti non possono accedere agli strumenti amministrativi, mentre gli amministratori hanno pieno controllo sulla cartella dedicata alla gestione dell'infrastruttura.

Analisi della Sicurezza e Principi Applicati

Principio del Privilegio Minimo (Least Privilege)

L'intera architettura implementata si basa sul principio fondamentale del privilegio minimo: ogni utente riceve solo i permessi strettamente necessari per svolgere le proprie mansioni lavorative, niente di più. Questo approccio:

- Riduce la superficie di attacco in caso di compromissione delle credenziali

- Limita i danni potenziali causati da errori umani accidentali
- Facilita l'auditing e la tracciabilità delle azioni
- Semplifica la gestione delle conformità normative (GDPR, ISO 27001, etc.)

Separazione dei Ruoli (Separation of Duties)

Ho implementato una chiara separazione tra ruoli operativi (analisti) e ruoli amministrativi (amministratori di infrastruttura). Questa separazione previene conflitti di interesse e garantisce che nessun singolo utente abbia accesso completo a tutte le risorse critiche del sistema.

In ottica di Cyber Security, la strategia adottata assicura che un utente compromesso o un attacco informatico che sfrutti le credenziali di un utente standard (SOC_Analyst) non possa in alcun modo accedere o danneggiare i dati amministrativi custoditi nella cartella `Infra_AdminTools`. Questo limita il potenziale danno (o la "superficie d'attacco") e protegge l'integrità del sistema.

Controllo degli Accessi Basato sui Ruoli (RBAC)

L'utilizzo dei gruppi di sicurezza invece dell'assegnazione diretta dei permessi ai singoli utenti implementa il modello RBAC (Role-Based Access Control). I vantaggi di questo approccio includono:

- Scalabilità: aggiungere un nuovo analista richiede solo l'inserimento nel gruppo `SOC_Analyst`
- Consistenza: tutti i membri dello stesso gruppo hanno identici permessi
- Manutenibilità: modificare i permessi di un ruolo impatta automaticamente tutti i membri
- Tracciabilità: è facile identificare quali risorse sono accessibili a quale ruolo

Problemi Riscontrati e Soluzioni Implementate

Problema: Accesso Negato Inaspettato

Durante i primi test, ho riscontrato che l'utente `manfredi.lp` non riusciva ad accedere alla cartella `SOC_Data` nonostante fosse membro del gruppo `SOC_Analyst` che avrebbe dovuto avere i permessi.

Causa identificata: Verificando le proprietà di sicurezza della cartella, ho scoperto che il gruppo `SOC_Analyst` non era stato aggiunto correttamente alla lista dei permessi NTFS. Probabilmente durante la configurazione iniziale avevo salvato le modifiche prima di completare l'aggiunta del gruppo.

Soluzione applicata: Ho riaperto le proprietà della cartella, scheda Security, e ho aggiunto esplicitamente il gruppo `SOC_Analyst` con i permessi corretti (Read & Execute, List folder contents, Read, Write). Dopo aver applicato le modifiche e atteso la propagazione dei permessi (circa 30 secondi), l'accesso ha funzionato correttamente.

Problema: Conflitto tra Permessi Espliciti ed Ereditati

In una fase iniziale della configurazione, prima di disabilitare completamente l'ereditarietà, ho notato comportamenti inaspettati nei permessi effettivi degli utenti. Alcuni utenti sembravano avere più accessi del previsto.

Causa identificata: I permessi ereditati dal contenitore padre (l'unità C:) si combinavano con i permessi espliciti che stavo configurando, creando una situazione di permessi cumulativi non prevista.

Soluzione applicata: Ho seguito la procedura corretta di disabilitazione dell'ereditarietà per tutte le cartelle di test:

1. Advanced Security Settings della cartella
2. Disable inheritance
3. Remove all inherited permissions
4. Aggiunta esplicita solo dei gruppi necessari con permessi specifici

Questo ha eliminato ogni ambiguità e garantito che solo i permessi esplicitamente configurati fossero attivi.

Problema: Ritardo nella Propagazione dei Permessi

Dopo aver modificato i permessi di una cartella, ho notato che l'utente di test continuava a ricevere "Access Denied" per alcuni secondi anche dopo l'applicazione delle modifiche.

Causa identificata: Windows Server e Active Directory utilizzano meccanismi di caching dei permessi per ottimizzare le performance. Le modifiche ai permessi non sono sempre istantanee.

Soluzione applicata: Ho adottato le seguenti pratiche:

- Attendere 30-60 secondi dopo ogni modifica ai permessi prima di ritestare
- Eseguire il comando `gpupdate /force` sulla macchina client per forzare l'aggiornamento delle policy
- In casi persistenti, eseguire logout e nuovo login dell'utente per forzare la rigenerazione del token di accesso

Conclusioni e Considerazioni Finali

Questo progetto ha pienamente raggiunto l'obiettivo di applicare la gestione dei gruppi per definire i privilegi in un ambiente Windows Server 2022. La creazione di gruppi di sicurezza (SOC_Analyst vs. Infra_Admin) e l'attenta configurazione delle autorizzazioni NTFS hanno dimostrato l'efficacia del Controllo degli Accessi Basato sui Ruoli (RBAC - Role-Based Access Control).

Ho compreso concretamente come una corretta gestione dei gruppi e dei permessi non sia solo una questione di organizzazione amministrativa, ma rappresenti un elemento

fondamentale della strategia di sicurezza complessiva di un'infrastruttura IT. La possibilità di limitare l'accesso alle risorse sensibili, garantire la separazione dei ruoli e implementare il principio del privilegio minimo sono tutti fattori che contribuiscono significativamente alla resilienza del sistema contro attacchi informatici e errori operativi.

L'esercizio mi ha anche permesso di apprezzare l'importanza della pianificazione iniziale: definire chiaramente i ruoli, le responsabilità e le necessità di accesso prima di implementare la struttura tecnica ha reso il processo molto più fluido e ha ridotto il numero di correzioni necessarie.