Report: Policy Windows Server

Tecnico: Victor Rosati

Data: 13 Febbraio 2026

1. Obiettivo dell'Attività

L'obiettivo dell'esercitazione è la messa in sicurezza di un'infrastruttura Windows Server 2022. L'attività si è focalizzata sulla gestione degli accessi basata sui ruoli, l'applicazione del principio del **minimo privilegio** e la risoluzione di criticità legate all'ereditarietà dei permessi e alle policy di dominio.

2. Configurazione Gruppi e Utenti (Active Directory)

Per gestire l'accesso alle risorse, sono stati creati due gruppi di sicurezza globali all'interno dell'Unità Organizzativa (OU) di default:

- **Sec_Ops_Admins**: Destinato agli amministratori di sistema con controllo completo.
- **Audit_Analysts**: Destinato agli analisti con privilegi limitati alla sola consultazione.

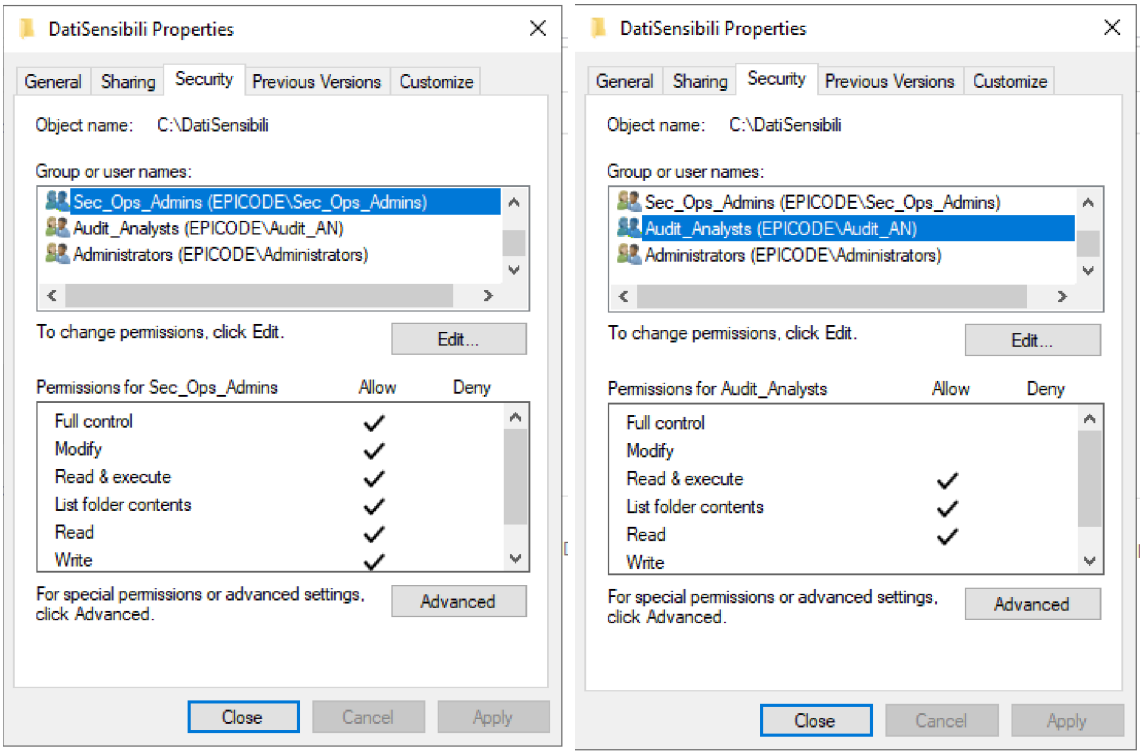
  Sono stati inoltre creati due utenti di test, **TestAdmin** e **TestAuditor**, associati rispettivamente ai gruppi sopra citati per convalidare le policy.

3. Gestione dei Permessi e Sicurezza dei Dati

È stata creata una cartella critica denominata `C:\DatiSensibili`. La configurazione della sicurezza ha seguito step rigorosi per prevenire fughe di dati:

A. Permessi NTFS Granulari

- **Sec_Ops_Admins**: Autorizzazione **Full Control** (Controllo completo).
- **Audit_Analysts**: Autorizzazione **Read & Execute** (Lettura ed esecuzione).



B. Gestione dell'Ereditarietà

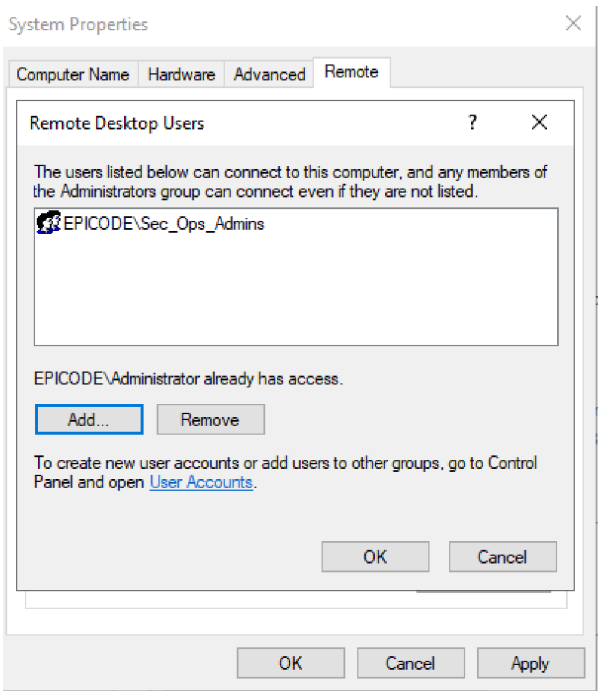
Durante la fase di test, è emersa una vulnerabilità: gli utenti standard potevano ancora scrivere nella cartella a causa dei permessi ereditati dal disco C:.

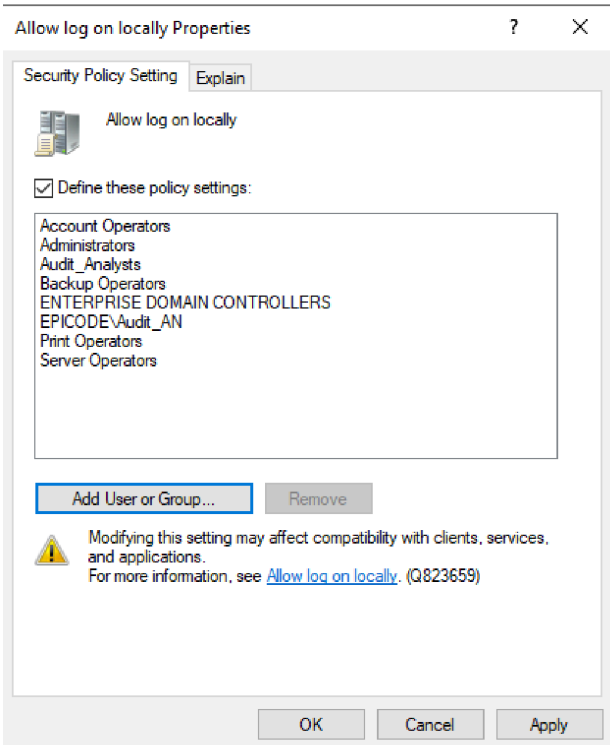
Risoluzione: È stata disabilitata l'ereditarietà (Inheritance) e rimosso il gruppo generico "Users", garantendo che solo i gruppi esplicitamente autorizzati potessero accedere.

4. Accesso Remoto e Policy di Sistema (GPO)

Per permettere l'amministrazione e il monitoraggio del server, sono state configurate le seguenti impostazioni:

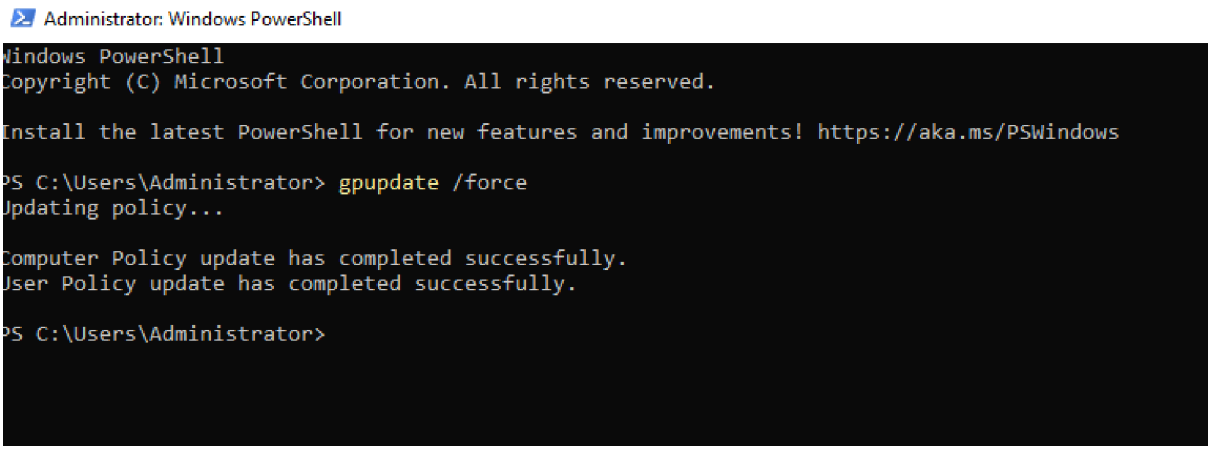
- **Desktop Remoto (RDP)**: Abilitato esclusivamente per il gruppo `Sec_Ops_Admins`.
- **Logon Locale**: Poiché il server opera come Domain Controller, è stata modificata la **Default Domain Controllers Policy** per permettere al gruppo `Audit_Analysts` di effettuare l'accesso locale (GPO: *Allow log on locally*).





Per rendere immediatamente effettive le modifiche apportate alla Group Policy senza attendere il refresh automatico del sistema, è stato eseguito il comando di "Enforcement" tramite PowerShell:

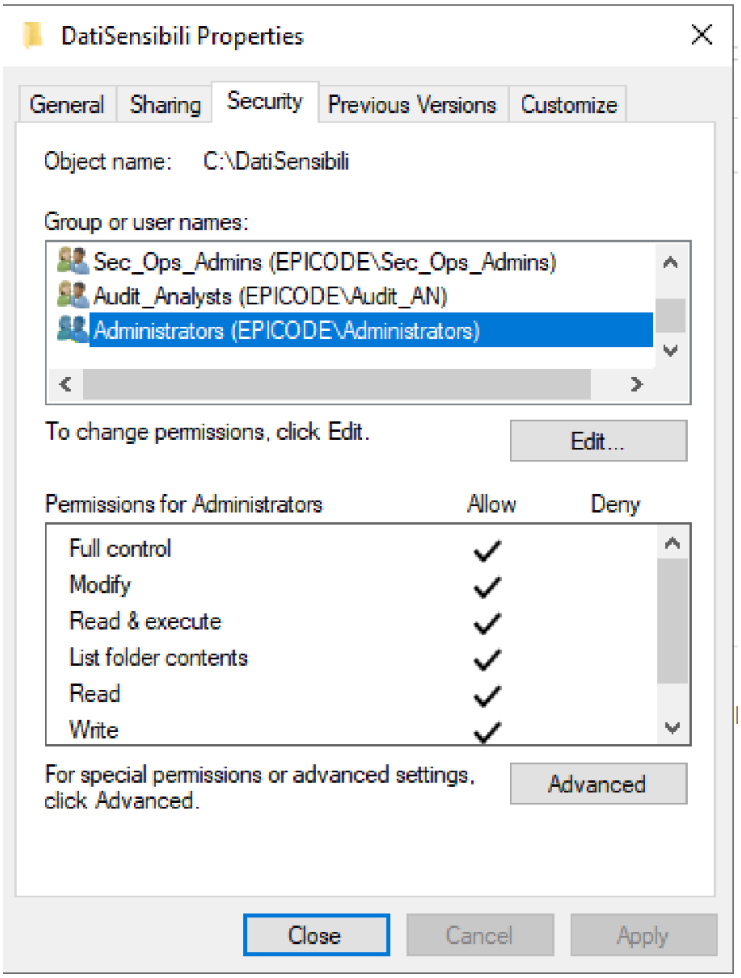
- Comando utilizzato: **`gpupdate /force`**



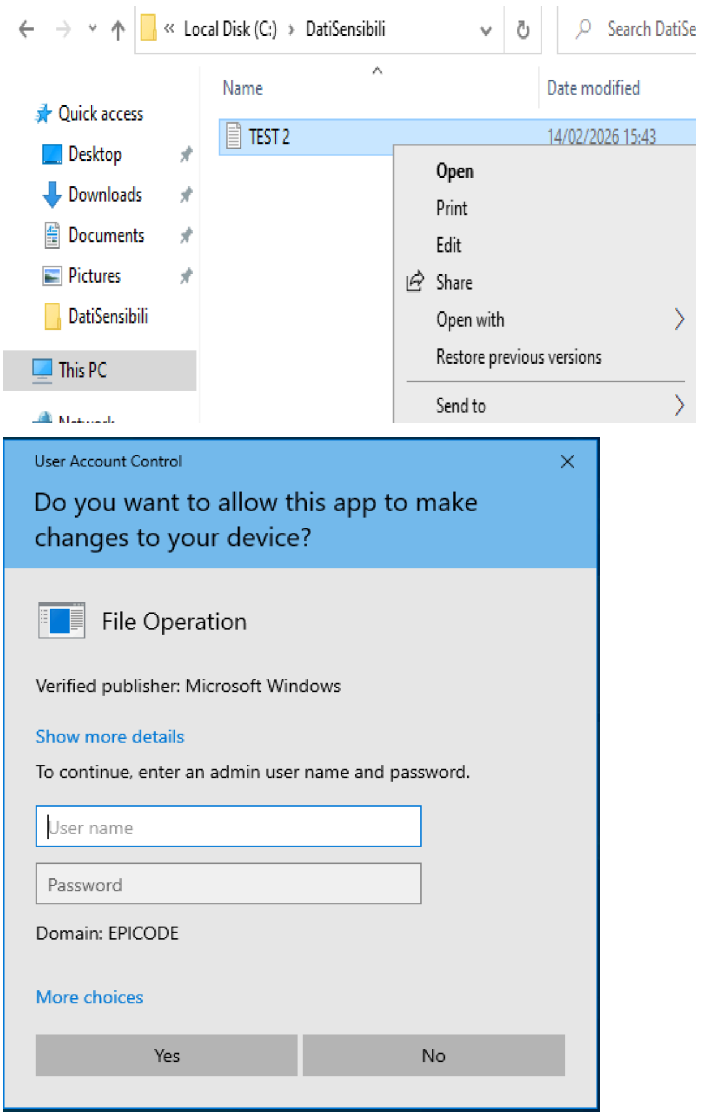
5. Verifica Finale e Risultati

La validazione del sistema è stata eseguita tramite test di accesso incrociato:

1. **Test Amministratore**: L'utente `TestAdmin` ha creato con successo file e cartelle, confermando la piena operatività del ruolo.



2. **Test Auditor**: L'utente `TestAuditor` è stato bloccato dal sistema durante un tentativo di scrittura.



.

6. Conclusioni

L'infrastruttura è ora configurata secondo i criteri di sicurezza richiesti. La corretta gestione dell'ereditarietà e delle Group Policy ha permesso di isolare i dati sensibili, garantendo che il personale di audit possa svolgere le proprie funzioni di controllo senza il rischio di alterare o eliminare accidentalmente file critici.