Gestione dei Gruppi e Controllo degli Accessi

Implementazione di un modello RBAC in Windows Server 2022

Ardelean Pop Catalin
Master in Cyber Security Specialist – Epicode

13 febbraio 2026

Indice

1 Traccia dell'esercizio

L'esercizio ha l'obiettivo di applicare le basi della gestione dei gruppi di sicurezza in Windows Server 2022. I passaggi da seguire sono i seguenti:

- Creare gruppi utenti coerenti con ruoli organizzativi definiti.
- Assegnare permessi differenziati alle risorse, rispettando il principio del **Least Privilege**.
- Verificare operativamente i permessi tramite utenti di test per confermare la corretta applicazione delle policy.

L'implementazione segue un modello di **Role-Based Access Control (RBAC)** volto a controllare e segmentare gli accessi in maniera strutturata e sicura.

2 Scenario di laboratorio

L'ambiente di laboratorio è stato predisposto per simulare un contesto enterprise con controllo centralizzato tramite Active Directory. Le caratteristiche principali sono le seguenti:

- **Domain Controller**: Windows Server 2022 Standard.
- **Dominio**: `Epicode.local`.
- **IP Server**: 192.168.50.2.
- **Client di test**: Windows 10 Pro, IP 192.168.50.3.

Servizi principali attivi sul Domain Controller:

- Active Directory Domain Services (AD DS) – gestione centralizzata degli account e dei gruppi.
- DNS integrato – risoluzione dei nomi interna al dominio.

Utenti di test creati per la verifica delle policy:

- Luca Verdi – dipartimento Marketing.
- Valerio Neri – dipartimento Sviluppo.

3 Creazione dei gruppi

I gruppi di sicurezza sono stati creati tramite lo strumento **Active Directory Users and Computers (dsa.msc)**.

Tipologia dei gruppi:

- Security Group
- Scope: Global

Gruppi creati:

- Marketing – destinato agli utenti del reparto Marketing.
- Sviluppo – destinato agli utenti del reparto Sviluppo.

La creazione dei gruppi consente una gestione centralizzata dei permessi, riducendo il rischio di accessi non autorizzati e semplificando l'applicazione di policy di sicurezza coerenti con il modello RBAC.

4 Configurazione delle risorse condivise

La configurazione delle risorse condivise è avvenuta tramite la creazione di directory dedicate sul server e l'applicazione di permessi sia a livello di condivisione (SMB) sia a livello di sicurezza (NTFS). È fondamentale comprendere che l'accesso effettivo di un utente a una risorsa condivisa è determinato dall'intersezione tra i permessi di condivisione e i permessi NTFS, dove vince sempre il livello più restrittivo.

4.1 Creazione delle directory sul server

Sono state create le seguenti cartelle sul volume locale del Domain Controller:

- **C:\DatiSensibili\Marketing**
- **C:\DatiSensibili\Sviluppo**

4.2 Configurazione della condivisione (Sharing)

Per ciascuna directory:

1. Accedere al server con credenziali amministrative.
2. Fare clic con il tasto destro sulla cartella da condividere e selezionare *Proprietà*.
3. Nella scheda *Condivisione*, cliccare su *Condivisione avanzata...*.

4. Abilitare *Condividi questa cartella* e assegnare un nome alla share.
5. Cliccare su *Autorizzazioni* e rimuovere il gruppo *Everyone* se presente.
6. Inserire i gruppi di sicurezza appropriati e assegnare i permessi di condivisione (Lettura o Modifica) in base alle policy aziendali.

4.3 Configurazione dei permessi di sicurezza (NTFS)

A livello di filesystem NTFS:

1. Nella scheda *Sicurezza*, cliccare su *Modifica...*.
2. Rimuovere eventuali gruppi non autorizzati (es. *Domain Users*) per evitare accessi non voluti.
3. Aggiungere i gruppi di sicurezza creati in Active Directory (Marketing, Sviluppo).
4. Assegnare i permessi NTFS appropriati:
   - *Marketing* – permessi coerenti con le policy di accesso limitato.
   - *Sviluppo* – permessi completi o specifici per le attività richieste.
5. Verificare che la propagazione dei permessi sia impostata in modo corretto su sottocartelle e file in base ai requisiti di accesso.

4.4 Considerazioni di sicurezza

- Le autorizzazioni di condivisione e quelle NTFS sono ambiti distinti: i permessi di condivisione regolano l'accesso sulla rete, mentre i permessi NTFS controllano l'accesso a livello di file system.
- In un contesto di dominio, è buona prassi assegnare i permessi tramite gruppi di sicurezza piuttosto che direttamente agli utenti, migliorando il controllo e semplificando la gestione.
- L'accesso effettivo è sempre determinato dall'intersezione tra i permessi di condivisione e quelli NTFS: ad esempio, se la condivisione concede solo Lettura e NTFS concede Modifica, l'accesso effettivo sarà Limitato alla Lettura.

5 Permessi assegnati al gruppo Marketing

Il gruppo **Marketing** è stato configurato per supportare attività di sviluppo e testing, garantendo accesso completo alle risorse necessarie e possibilità di connessione remota.

5.1 Accesso file e cartelle

Directory di riferimento:

```
C:\DatiSensibili\Marketing
```

Permessi NTFS assegnati:

- **Full Control** – consente lettura, scrittura, creazione, eliminazione di file e sottocartelle.
- Gestione permessi ACL – possibilità di modificare i permessi su file e cartelle, se necessario per attività di sviluppo.

Permessi di condivisione (Sharing):

- La cartella è condivisa tramite *Advanced Sharing* con accesso completo al gruppo Marketing.
- I permessi di condivisione e NTFS sono configurati per garantire che il Full Control venga applicato solo agli utenti appartenenti al gruppo.

5.2 Restrizioni applicative

Per garantire la sicurezza e limitare l'esecuzione di software non autorizzato, sono state applicate **Software Restriction Policies (SRP)** con configurazione specifica:

- **Default Security Level: Disallowed** – tutte le applicazioni non esplicitamente consentite sono bloccate.
- **Percorsi consentiti**:
  - C:\Program Files\Microsoft Office
  - C:\Windows
- Questa configurazione consente agli utenti Marketing di utilizzare esclusivamente applicazioni Office necessarie per le attività quotidiane, limitando ogni altro software non autorizzato.

Benefici di questa configurazione: Limitare l'esecuzione delle applicazioni ai soli programmi Office riduce significativamente la superficie d'attacco lato client. Gli utenti Marketing non possono eseguire software non autorizzato, prevenendo l'esecuzione di tool potenzialmente malevoli o script dannosi. Questa configurazione supporta la politica di **Least Privilege** e semplifica il monitoraggio del comportamento applicativo tramite strumenti di endpoint security.

5.3 Blocco strumenti di sistema

Attraverso GPO sono stati applicati i seguenti vincoli:

- Prevent access to command prompt – impedisce l'uso di CMD o PowerShell per operazioni potenzialmente rischiose.
- Prevent access to registry editing tools – limita modifiche al registro di sistema, prevenendo configurazioni non autorizzate.

6 Permessi assegnati al gruppo Sviluppo

Il gruppo **Sviluppo** è stato configurato per supportare attività di sviluppo e testing, garantendo accesso completo alle risorse necessarie e possibilità di connessione remota.

6.1 Accesso file e cartelle

Directory di riferimento:

```
C:\DatiSensibili\Sviluppo
```

Permessi NTFS assegnati:

- **Full Control** – consente lettura, scrittura, creazione, eliminazione di file e sottocartelle.
- Gestione permessi ACL – possibilità di modificare i permessi su file e cartelle, se necessario per attività di sviluppo.

Permessi di condivisione (Sharing):

- La cartella è condivisa tramite *Advanced Sharing* con accesso completo al gruppo Sviluppo.
- I permessi di condivisione e NTFS sono configurati per garantire che il Full Control venga applicato solo agli utenti appartenenti al gruppo.

6.2 Accesso RDP

Per consentire l'accesso remoto al server, il gruppo Sviluppo è stato aggiunto al gruppo locale `Remote Desktop Users` tramite:

```
net localgroup "Remote Desktop Users" Sviluppo /add
```

Monitoraggio eventi consigliato:

- **4624 – Logon riuscito**: tracciamento degli accessi autorizzati.
- **4625 – Logon fallito**: rilevamento tentativi di accesso non autorizzati o brute force.
- **4672 – Privilegi speciali assegnati**: monitoraggio sessioni con diritti elevati.

Note operative: L'RDP è abilitato solo per gli utenti Sviluppo, con monitoraggio continuo degli eventi di logon e privilegi. Si raccomanda di integrare queste informazioni in un sistema SIEM per rilevare anomalie comportamentali.

6.3 Accesso applicativo

Software Restriction Policies: non applicate, in quanto gli utenti necessitano di utilizzare strumenti di sviluppo e amministrazione.

Permessi applicativi:

- IDE e strumenti di sviluppo (Visual Studio, IntelliJ, ecc.)
- Utility di scripting e terminale (PowerShell, CMD)
- Software di testing e debug

Commento tecnico: L'assenza di restrizioni applicative aumenta la flessibilità operativa ma implica che sia necessario un monitoraggio continuo tramite audit di processi e controllo esecuzione software per prevenire l'utilizzo di applicazioni non autorizzate.

7 Verifica delle configurazioni

La verifica delle configurazioni è stata eseguita con un approccio operativo completo, simulando l'attività quotidiana degli utenti dei gruppi Marketing e Sviluppo. L'obiettivo è stato confermare l'efficace applicazione di permessi NTFS, sharing, GPO e restrizioni applicative, garantendo conformità al principio di **Least Privilege**.

7.1 Preparazione degli utenti di test

1. Creazione degli utenti di prova in Active Directory:
   - **Luca Verdi** – gruppo Marketing
   - **Valerio Neri** – gruppo Sviluppo
2. Impostazione di password temporanee sicure per entrambi gli utenti.

3. Configurazione obbligatoria di cambio password al primo login, per conformità alle best practice di sicurezza.

4. Verifica dell'appartenenza ai rispettivi gruppi tramite:

```
whoami /groups
```

7.2 Aggiornamento policy e sincronizzazione GPO

Per assicurare che tutte le modifiche fossero attive sul client Windows 10:

```
gpupdate /force   # Aggiorna immediatamente le Group Policy
gpresult /r       # Controlla le policy applicate all'utente
```

Eventuali errori nella propagazione delle GPO sono stati risolti tramite Security Filtering e aggiunta di `Authenticated Users` con permesso Read.

7.3 Test del gruppo Marketing

1. Login su client Windows 10 con credenziali di Luca Verdi.

2. Cambio obbligatorio della password temporanea.

3. Accesso alle cartelle condivise:

   - **C:\DatiSensibili\Marketing:** Accesso consentito (Full Control).
   - **C:\DatiSensibili\Sviluppo:** Accesso negato.

4. Esecuzione applicazioni:

   - Consentito: Microsoft Office.
   - Negato: CMD, PowerShell, Regedit e altri strumenti di amministrazione.

5. Accesso remoto (RDP) al server: Negato.

Esito: tutte le restrizioni e permessi previste per Marketing sono state correttamente applicate. L'utente può operare solo all'interno delle risorse e applicazioni autorizzate.

7.4 Test del gruppo Sviluppo

1. Login su client Windows 10 con credenziali di Valerio Neri.

2. Cambio obbligatorio della password temporanea.

3. Accesso alle cartelle condivise:

- **C:\DatiSensibili\Sviluppo:** Accesso consentito (Full Control).
- **C:\DatiSensibili\Marketing:** Accesso negato.

4. Esecuzione applicazioni:
   - Consentito: IDE, strumenti di sviluppo, CMD, PowerShell, software di testing e debug.
   - Negato: strumenti di amministrazione non necessari (accesso al registro o configurazioni critiche tramite GPO).
5. Accesso remoto (RDP) al server: Consentito, con monitoraggio continuo tramite eventi 4624, 4625 e 4672.

Esito: il gruppo Sviluppo ha accesso completo alle risorse necessarie per attività di sviluppo e testing, mantenendo blocchi su strumenti di sistema sensibili non richiesti.

7.5 Commento tecnico

- I permessi NTFS e di sharing sono stati applicati correttamente e testati tramite accessi diretti e strumenti di amministrazione.
- Le restrizioni applicative rispettano le policy di sicurezza definite: Marketing limitato a Office, Sviluppo libero ma controllato.
- Il login con password temporanea e cambio obbligatorio garantisce sicurezza iniziale delle credenziali.
- L'accesso RDP è segmentato correttamente, con monitoraggio degli eventi di logon per prevenzione di accessi non autorizzati.
- La procedura di verifica conferma la piena conformità al modello RBAC implementato e alle best practice di sicurezza lato client e server.

8 Problemi riscontrati e soluzioni

Durante la fase di implementazione e verifica dei gruppi Marketing e Sviluppo sono stati riscontrati alcuni problemi operativi, risolti seguendo procedure standard di troubleshooting in ambiente Active Directory e Group Policy.

8.1 GPO non applicata correttamente

Sintomo: le restrizioni su CMD e Regedit non venivano rispettate dagli utenti Marketing.

Diagnosi: tramite `gpresult /r` è stato osservato che il filtro di sicurezza (Security Filtering) non includeva correttamente gli utenti del gruppo Marketing.

Soluzione:

1. Aggiunta del gruppo `Authenticated Users` con permesso Read nella sezione Security Filtering della GPO.
2. Forzato aggiornamento delle policy client tramite:

```
gpupdate /force
```

3. Verifica dell'applicazione tramite login utente di test e test restrizioni applicative.

8.2 SRP non attiva

Sintomo: le Software Restriction Policies configurate per il gruppo Marketing non venivano applicate.

Diagnosi: il servizio `Application Identity` necessario per le SRP era disabilitato.

Soluzione:

1. Abilitato e avviato il servizio `Application Identity`:

```
services.msc
# Impostare Application Identity su Automatic e Avviare il
    servizio
```

2. Forzato aggiornamento GPO:

```
gpupdate /force
```

3. Confermata applicazione delle SRP tramite tentativi di esecuzione di applicazioni non consentite (bloccate correttamente) e applicazioni Office (consentite).

8.3 Problemi DNS e risoluzione nomi

Sintomo: durante i test su client Windows 10, alcune condivisioni di rete non erano immediatamente accessibili tramite nome server (
`Epicode.local`).

Diagnosi: cache DNS locale non aggiornata e registrazioni DNS del server non propagate.

Soluzione:

1. Pulizia della cache DNS locale:

```
ipconfig /flushdns
```

2. Registrazione forzata dei record DNS del server:

```
ipconfig /registerdns
```

3. Verifica risoluzione dei nomi e accesso alle cartelle condivise tramite percorso UNC.

8.4 Commento tecnico

I problemi riscontrati sono tipici in un ambiente Active Directory appena configurato:

- La mancata applicazione delle GPO è spesso causata da filtri di sicurezza incompleti o assenza di diritti di lettura su utenti e gruppi.
- Le SRP richiedono il servizio `Application Identity` attivo su tutti i client per funzionare correttamente.
- La risoluzione dei nomi DNS è critica per l'accesso alle risorse condivise; la propagazione delle modifiche può richiedere forzature manuali.

L'implementazione delle soluzioni sopra descritte ha permesso di ristabilire il corretto comportamento dei gruppi e delle policy, garantendo la sicurezza e la conformità ai requisiti dell'esercizio.

9 Conclusioni

L'implementazione dei gruppi **Marketing** e **Sviluppo** in Windows Server 2022 ha permesso di configurare un modello di accesso basato sui ruoli (RBAC), garantendo separazione dei privilegi, sicurezza e controllo operativo sulle risorse aziendali.

9.1 Benefici ottenuti

- **Segmentazione dei privilegi:** ogni gruppo ha accesso solo alle risorse pertinenti al proprio ruolo, riducendo il rischio di accessi non autorizzati.
- **Least Privilege:** gli utenti Marketing non possono eseguire applicazioni o strumenti di sistema non autorizzati, mentre gli utenti Sviluppo hanno accesso controllato a strumenti di sviluppo necessari.
- **Controllo RDP e accesso remoto:** l'accesso remoto è stato limitato al gruppo Sviluppo, con monitoraggio continuo degli eventi di logon e privilegi.

- **Riduzione della superficie di attacco:** restrizioni applicative e ACL NTFS garantiscono che solo gli utenti autorizzati possano interagire con le risorse critiche.
- **Tracciabilità e audit:** configurazione degli eventi di sicurezza (4624, 4625, 4672) e controllo dei log per rilevare comportamenti anomali.

9.2 Best practice applicate

- Creazione di **Security Groups** con scope appropriato e permessi NTFS coerenti.
- Configurazione di **Software Restriction Policies** per limitare l'esecuzione di software non autorizzato.
- Utilizzo di **Group Policy Objects (GPO)** per applicare restrizioni operative e vincoli di sicurezza.
- Implementazione di accesso remoto selettivo tramite `Remote Desktop Users`, garantendo monitoraggio e tracciabilità.
- Verifica dei permessi tramite login di test, reimpostazione password e audit dei tentativi di accesso.

9.3 Considerazioni finali

L'esercizio ha dimostrato che un approccio RBAC ben strutturato in Active Directory consente di:

- Migliorare la sicurezza complessiva dell'infrastruttura server.
- Prevenire l'esecuzione di software non autorizzato e la modifica di configurazioni critiche.
- Fornire agli sviluppatori la flessibilità necessaria senza compromettere la sicurezza degli altri reparti.

Questa implementazione rappresenta una base solida per la gestione sicura degli accessi in un contesto enterprise, in linea con i principi di **cyber security governance** e di protezione delle risorse digitali.