REPORT DI LABORATORIO: Gestione Identità e Accessi (IAM) in Windows Server 2022

Studente: Rocco Paolo Caccamo

Modulo: Hardening di Active Directory & Access Control

Data: 13 Febbraio 2026

---

1. Executive Summary

L'obiettivo di questo laboratorio è configurare un'infrastruttura di dominio sicura (Active Directory), applicando il principio del **Least Privilege** (Privilegio Minimo). L'esercitazione simula uno scenario aziendale reale in cui è necessario segregare l'accesso ai dati tra diversi dipartimenti (Sviluppatori vs Auditor) e configurare correttamente le autorizzazioni di rete e locali.

---

2. Architettura di Rete e Configurazione

L'ambiente di laboratorio è isolato e costituito da due nodi principali. La configurazione statica degli indirizzi IP è essenziale per garantire la corretta risoluzione dei nomi DNS all'interno del dominio.

2.1 Topologia

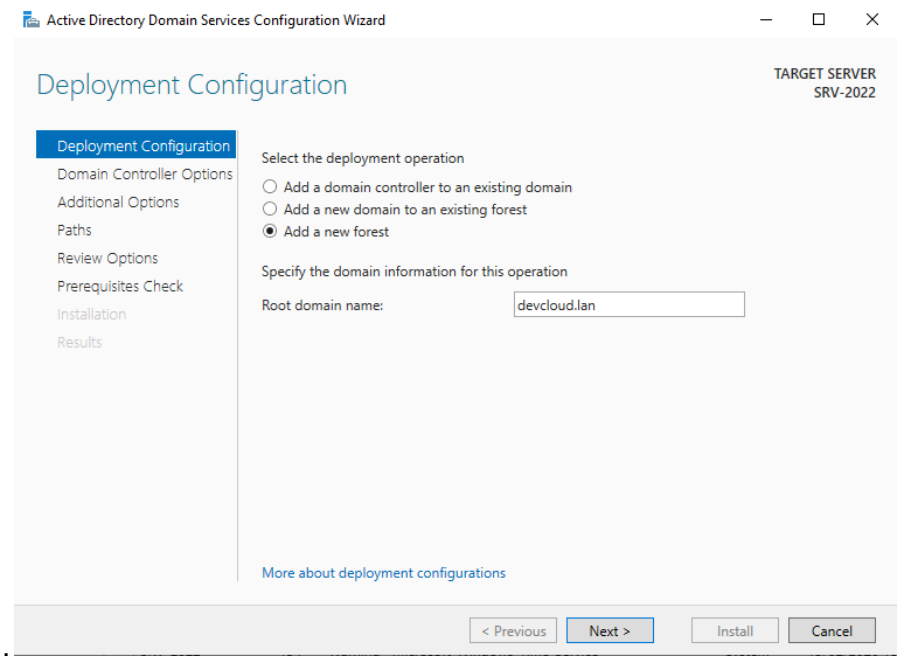
- **Server (Domain Controller):** `SRV-2022`
  - **IP:** `192.168.50.2` / 24
  - **Ruolo:** AD DS, DNS Server
- **Client (Workstation Utente):** Windows 10/11
  - **IP:** `192.168.50.3` / 24
  - **DNS Primario:** `192.168.50.2` (Punta al DC per risolvere il dominio)

```
Microsoft Windows [Version 10.0.20348.1006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::44b1:80c5:d14e:5d1b%6
   IPv4 Address. . . . . . . . . . . : 192.168.50.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.1

C:\Users\Administrator>
```

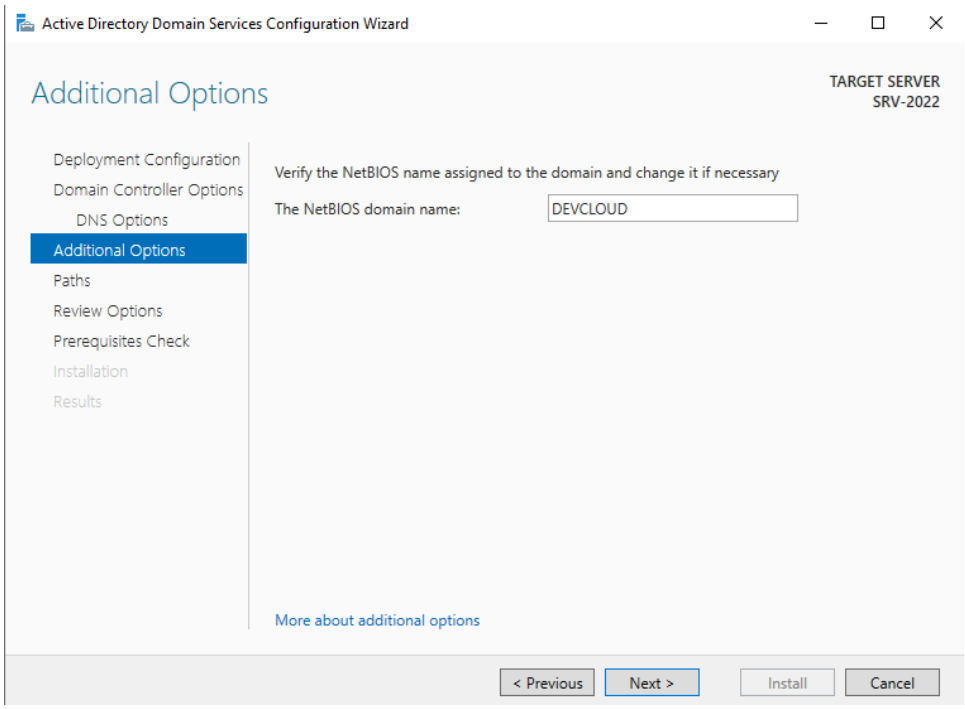
cmd con output di ipconfig del Server

2.2 Setup del Dominio

Il server è stato promosso a Domain Controller creando una nuova foresta denominata `devcloud.lan`



- **NetBIOS Name:** `DEVCLOUD`



---

3. Gestione Identità (Users & Groups)

Per evitare l'uso di account generici, è stata implementata una struttura gerarchica basata su **Organizational Units (OU)**.

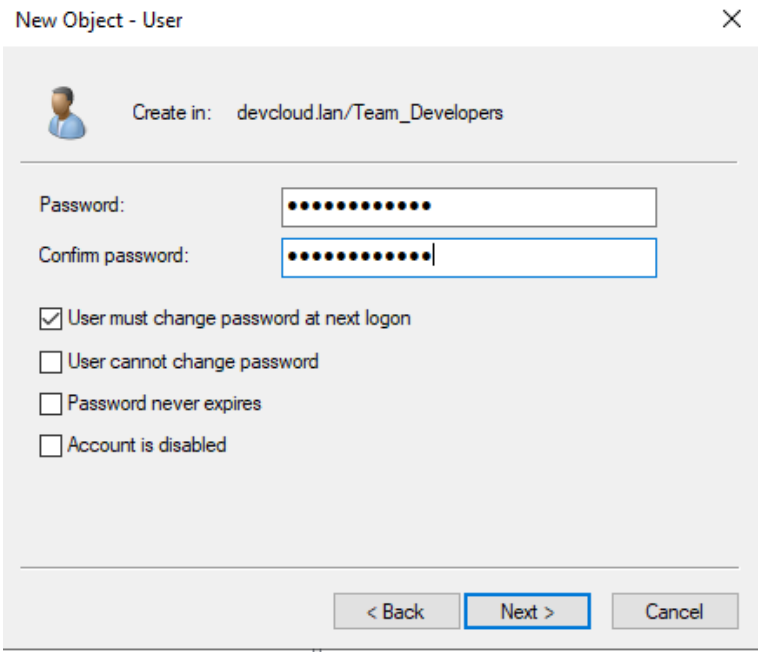
3.1 Creazione Utenti

Sono stati creati account specifici per simulare i ruoli aziendali:

- **OU Team_Developers:** *Mario Rossi*, *Stefano Neri*
- **OU Team_Auditors:** *Elisa Verdi*

3.2 Security Policy

È stata applicata la policy "User must change password at next logon". Questo obbliga l'utente a impostare una password privata al primo accesso, garantendo la non ripudiabilità delle azioni successive.



Creazione utente con opzione cambio password al primo avvio

---

4. Gestione delle Autorizzazioni (Access Control)

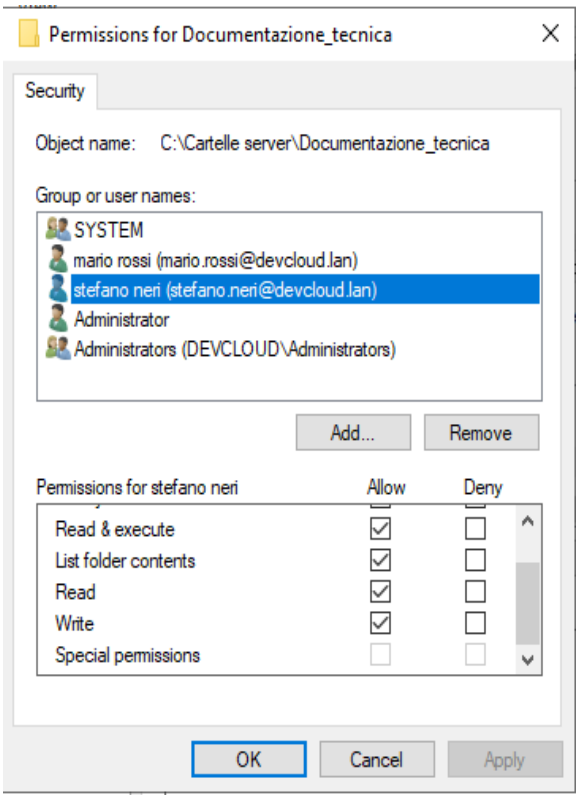
Il cuore dell'esercizio è la configurazione dei permessi sulle cartelle condivise `\\SRV-2022\Documentazione_tecnica` e `\\SRV-2022\Audit_logs`.

4.1 Logica dei Permessi

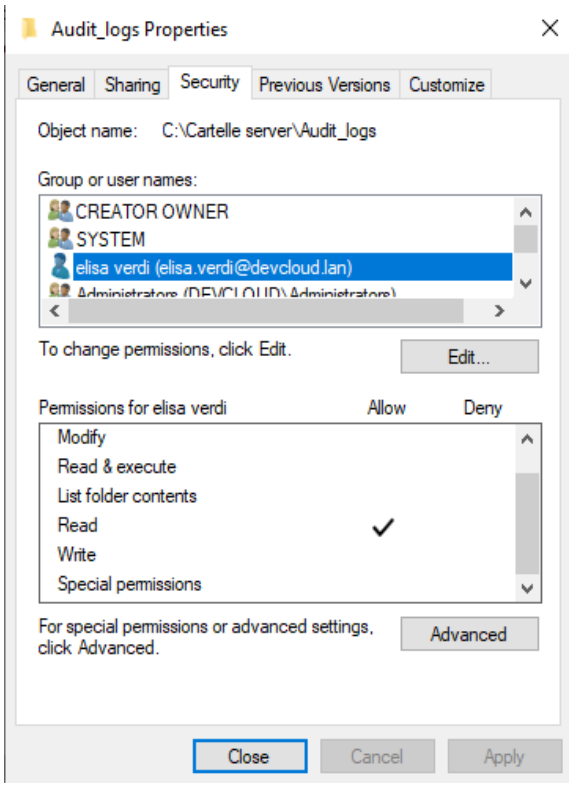
Abbiamo distinto tra:

1. **Share Permissions:** Chi può "entrare dalla porta di rete".
2. **NTFS Security:** Chi può "aprire il cassetto" una volta entrato.

Per la cartella `Documentazione_tecnica`, agli sviluppatori (Mario e Stefano) sono stati concessi permessi di Lettura e Modifica.



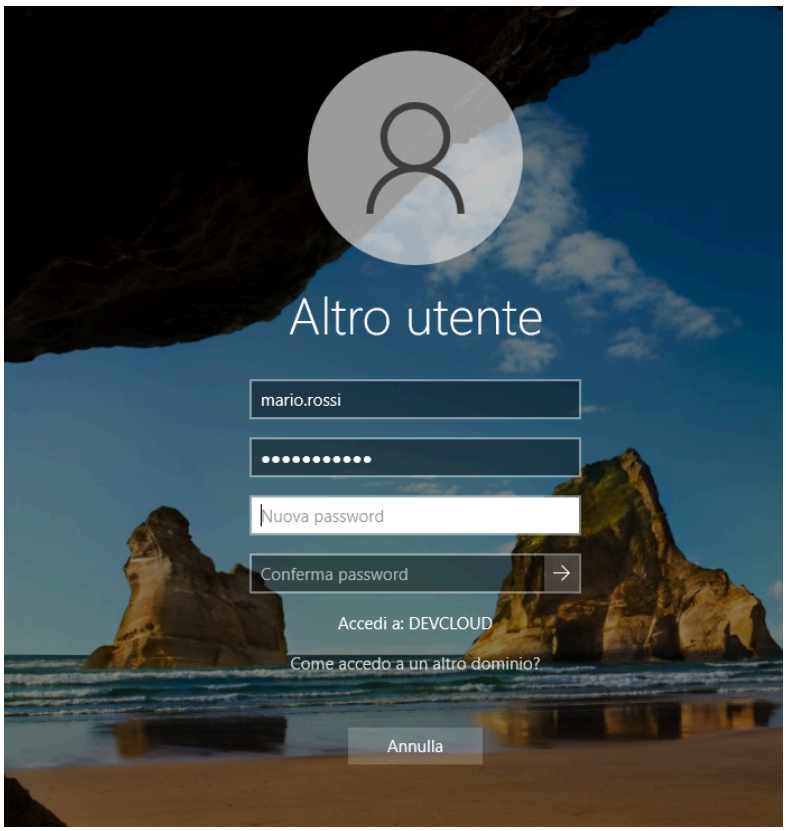
Per la cartella `Audit_logs`, l'utente *Elisa Verdi* ha permessi NTFS di lettura, ma l'accesso è stato ristretto per testare la propagazione dei diritti.



---

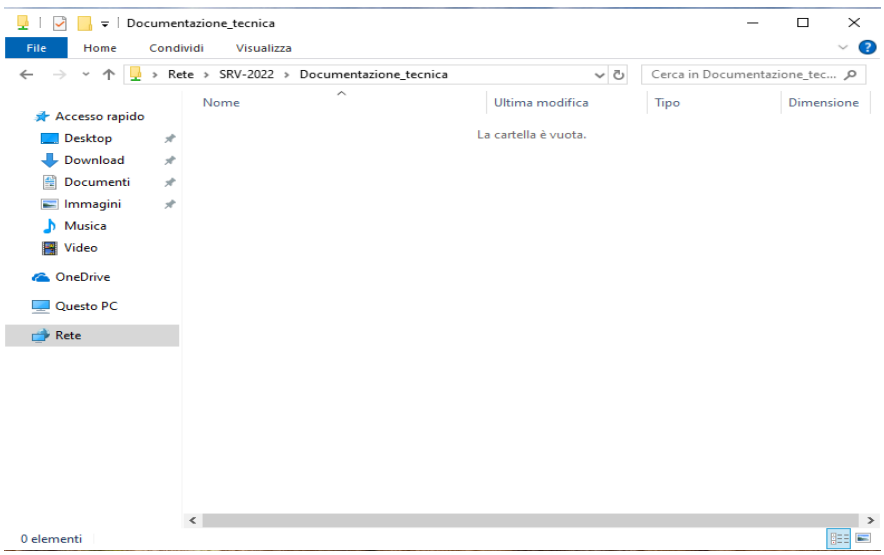
5. Verifica e Testing (Proof of Concept)

I test sono stati eseguiti dalla **macchina Client (192.168.50.3)** loggata nel dominio.



5.1 Accesso Concesso

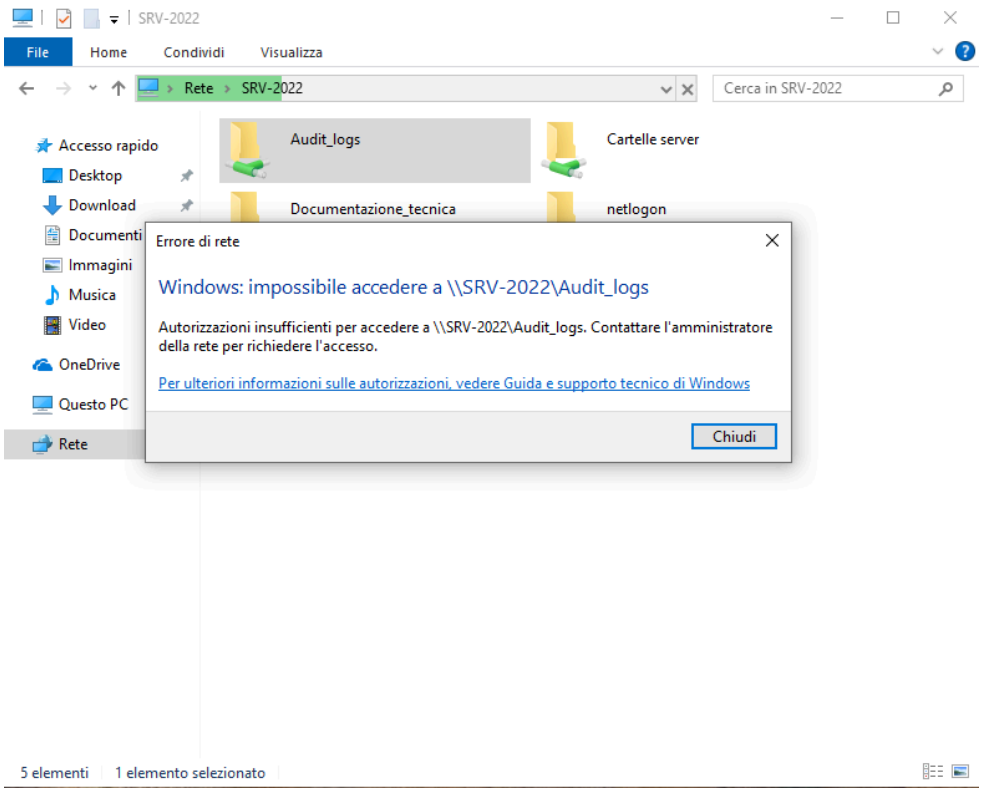
L'utente *Mario Rossi* effettua il login al dominio `DEVCLOUD`. Tenta l'accesso alla risorsa `\\SRV-2022\Documentazione_tecnica`.



Accesso garantito. L'utente visualizza il contenuto.

5.2 Accesso Negato

Tentativo di accesso alla risorsa protetta `\\SRV-2022\Audit_logs` con utente non autorizzato o con permessi Share insufficienti.



- **Risultato:** Errore "Impossibile accedere".
- **Analisi Tecnica:** Windows combina i permessi Share e NTFS e applica sempre la **regola più restrittiva**. Se NTFS dice "Full Control" ma Share dice "Read Only", l'utente avrà solo "Read Only" via rete.

---

6. Conclusioni Didattiche

Questo laboratorio ha dimostrato che:

1. **La rete non basta:** Avere il ping (connettività IP tra 50.2 e 50.3) non significa avere l'accesso ai dati.
2. **Layers of Defense:** La sicurezza è a strati. Share Permissions proteggono l'accesso remoto; NTFS Permissions proteggono il file system locale.
3. **Configurazione DNS:** Senza il DNS corretto sul client, l'autenticazione Kerberos al dominio fallisce a monte.