WINDOWS SERVER&CLIENT

Introduzione:

Il presente report descrive i concetti fondamentali e le competenze tecniche acquisite attraverso la configurazione integrata di un'infrastruttura Network–Server–Client in ambiente Windows Server.

L'obiettivo delle attività svolte è comprendere come progettare e implementare un sistema centralizzato di gestione delle identità, delle risorse e dei permessi all'interno di una rete aziendale strutturata. Attraverso l'installazione e la configurazione di Windows Server con **Active Directory Domain Services**, viene introdotto il modello di dominio come strumento per l'autenticazione e l'autorizzazione centralizzata di utenti e dispositivi.

Nel corso delle configurazioni vengono approfonditi i seguenti concetti chiave:

- Architettura client-server in ambiente di dominio
- Ruolo del Domain Controller e funzionamento di Active Directory
- Strutturazione logica tramite foresta, dominio e Unità Organizzative (OU)
- Gestione di utenti e gruppi secondo criteri organizzativi
- Assegnazione e controllo dei permessi mediante gruppi di sicurezza
- Differenza tra permessi di condivisione (Sharing) e permessi NTFS (Security)
- Join di un client al dominio e verifica dell'autenticazione centralizzata
- Implementazione del principio del minimo privilegio (Least Privilege)

L'approccio adottato consente di comprendere non solo le procedure operative, ma anche la logica strutturale che regola la sicurezza e la gestione delle risorse in un'infrastruttura aziendale. L'integrazione tra rete, server e client permette di osservare in modo pratico il funzionamento dei meccanismi di controllo degli accessi, della segmentazione logica degli utenti e della protezione dei dati.

Il report fornisce quindi una visione sistemica dell'ambiente configurato, evidenziando come una corretta progettazione dell'architettura di dominio rappresenti un elemento essenziale per garantire sicurezza, scalabilità e governabilità dell'infrastruttura IT.

CONFIGURAZIONE PERMESSI

1) Obiettivo del laboratorio

1. Creare un **dominio Active Directory** (foresta + dominio).
2. Organizzare utenti con **OU** (reparti).
3. Creare **gruppi** per gestire permessi in modo scalabile.
4. Creare **cartelle** con accessi differenziati.
5. Collegare un **client Windows** al dominio e verificare che i permessi funzionino.

---

2) Server: base logica (non settaggi estetici)

2.1 Installazione Windows Server 2022 (solo concetto)

- Il server diventa la macchina "centrale" su cui si installera' i ruoli necessari.

2.2 Installazione ruolo Active Directory Domain Services (AD DS)

1. In Server Manager su **Add Roles and Features**.
2. Selezionare **Active Directory Domain Services** (aggiungendo le feature richieste).
3. Installare **Active Directory Domain Services**.

Perché: AD DS è ciò che abilita gestione centralizzata di utenti/computer/gruppi e policy

---

3) Dominio e foresta (struttura "top level")

3.1 Creazione della foresta/dominio

1. Dopo l'installazione AD DS, di fa la **promozione a Domain Controller**.
2. Creare una **nuova foresta** e impostre un nome (esempio : `Epicode.local`).
3. Impostare la password di ripristino (DSRM).

Cosa ottieni: un dominio dove tutte le identità (utenti/computer) possono essere gestite centralmente.

---

4) Strutturazione in OU (repliche dell'organizzazione)

4.1 Creazione delle OU

1. Dentro il dominio/foresta Creare le **OU**:
    - `Amministrazione`
    - `Hacker1`

Idea chiave: le OU servono per ordinare oggetti (utenti/computer/gruppi) e applicare policy in modo mirato.

---

5) Utenti (identità) dentro le OU

5.1 Creazione utenti in "Amministrazione"

1. Creare l'utente `Chiara`
2. Creare l'utente `Marina`
3. Impostare "**cambia password al primo accesso**" (principio: l'admin non dovrebbe conoscere la password finale dell'utente).

5.2 Creazione utenti in "Hacker1"

1. Creare l'utente `Elliot`
2. Creare l'utente `Condor`

✅ **Risultato atteso:**

- OU Amministrazione → Chiara, Marina
- OU Hacker1 → Elliot, Condor

---

6) I Gruppi (il trucco per non impazzire coi permessi)

6.1 Creazione gruppi nelle rispettive OU

1. In `Amministrazione` Creare il gruppo **Mitiche**
2. In `Hacker1` Creare il gruppo **Robot**

6.2 Aggiunta membri ai gruppi

- **Mitiche**: Chiara + Marina
- **Robot**: Elliot + Condor

Perché è fondamentale: assegnare permessi ai gruppi, non ai singoli utenti. È più pulito, più sicuro, più manutenibile.

---

7) Cartelle (risorse) e modello di accesso desiderato

7.1 Creazione struttura cartelle sul server

1. Creare cartella principale: `Dati Sensibili`
2. Dentro Creare due sottocartelle:
    - `Dati Segreti`
    - `Dati Top`

7.2 Regole di accesso (policy aziendale dell'esempio)

- `Dati Sensibili`: **tutti** possono vedere l'elenco (visibilità generale)
- `Dati Segreti`: accesso/modifica **solo** gruppo **Mitiche**
- `Dati Top`: accesso/modifica **solo** gruppo **Robot**

Questa è la "matrice permessi" che poi si va a implementare.

---

8) Permessi: Sharing vs Security (NTFS) e regola del "più restrittivo"

8.1 Due livelli di permessi

1. **Sharing permissions** (solo quando si accede via rete)
2. **Security/NTFS permissions** (valgono localmente e via rete, più granulari)

8.2 Regola cruciale

Quando si accedw a una cartella condivisa via rete, l'accesso finale è:

intersezione tra permessi di Sharing e permessi NTFS (vince il più restrittivo)

Conclusione : i permessi più importanti da impostare bene sono quelli **NTFS**.

8.3 Logica operativa (alto livello)

1. Rimuovere **Everyone** dove non ha senso (eviti accesso "universale").
2. Aggiungere il **gruppo corretto** (Mitiche o Robot) alla cartella corretta.
3. Concedere il livello richiesto (lettura/modifica/controllo completo) in base alla policy.

---

9) Client: ingresso nel dominio (solo parte utile)

9.1 Aggiunta del client al dominio

1. Rinominare il PC (nome host sensato).
2. Lo si **mette a dominio** inserendo credenziali di un account autorizzato (tipicamente Administrator/Domain Admin per l'operazione).

Risultato: il client ora autentica gli utenti contro Active Directory.

---

10) Verifica finale (test "reale" dei permessi)

10.1 Test con un utente del gruppo Robot (Elliot)

1. Login sul client come **Elliot** (al primo accesso si cambia password).
2. Accedere alla condivisione sul server.
3. Verificare se:
    - Elliot **può** leggere/modificare `Dati Top`
    - Elliot **non può** accedere/modificare `Dati Segreti`

Se succede esattamente questo, la struttura utenti→gruppi→permessi è coerente.