S10 – L3

Windows Server 2022: Configurazione + verifica con accesso di Chiara

Introduzione

Nel presente esercizio **ho configurato un ambiente Active Directory su Windows Server 2022, creando dominio, utenti, gruppi e permessi di accesso**, con successiva **verifica tramite login dell'utente Chiara su client Windows 10.**

Prerequisiti (VM e rete)

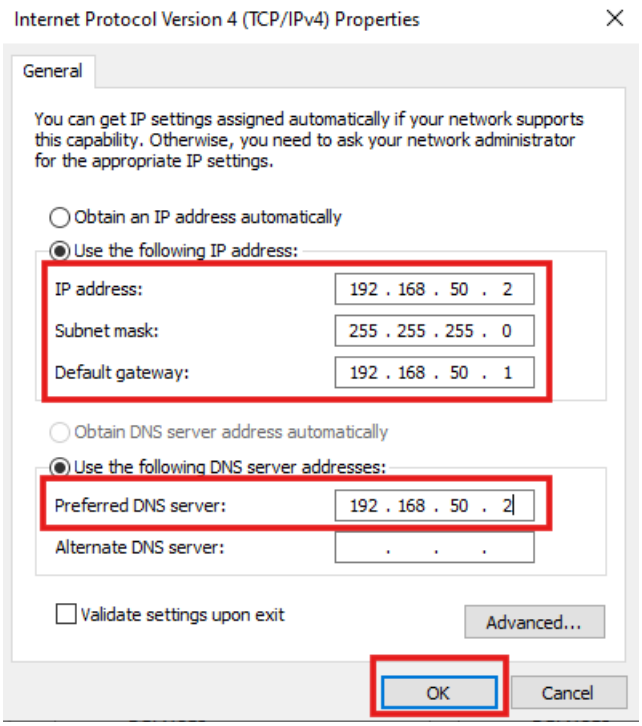
1. **Creo 2 VM**:
    - **Windows Server 2022** (Domain Controller)
    - **Windows 10 Pro** (client)
2. In **VirtualBox/VMware**, imposto per **entrambe** la scheda di rete su **Rete interna** (Internal Network).
3. Avvio il **Server**.

---

1) Configurazione rete e parametri base sul Windows Server 2022

1.1 Imposto IP statico

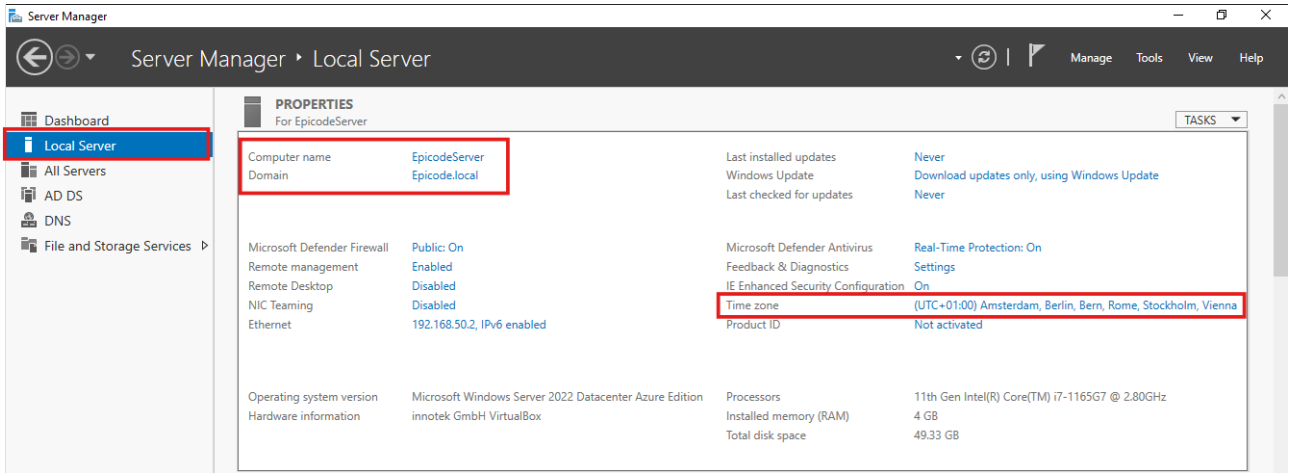
1. Sul Server apro: **Network & Internet settings → Change adapter options**
2. Tasto destro sulla scheda → **Properties**
3. Seleziono **Internet Protocol Version 4 (TCP/IPv4) → Properties**
4. Imposto:
    - **IP statico** (es. `192.168.50.2`)
    - **Subnet** (es. `255.255.255.0`)
    - **DNS primario** = **IP del Server** (`192.168.50.2`) perché il server farà da DNS.



Schermata con **IP/DNS configurati**.

1.2 Rinomino il server e setto time zone

1. Apro **Server Manager → Local Server**
2. Clicco sul nome computer → **Change**
3. Imposto un nome (**`EpicodeServer`**) → OK → **riavvio**
4. Sistemo **data/ora e fuso orario** se necessario.

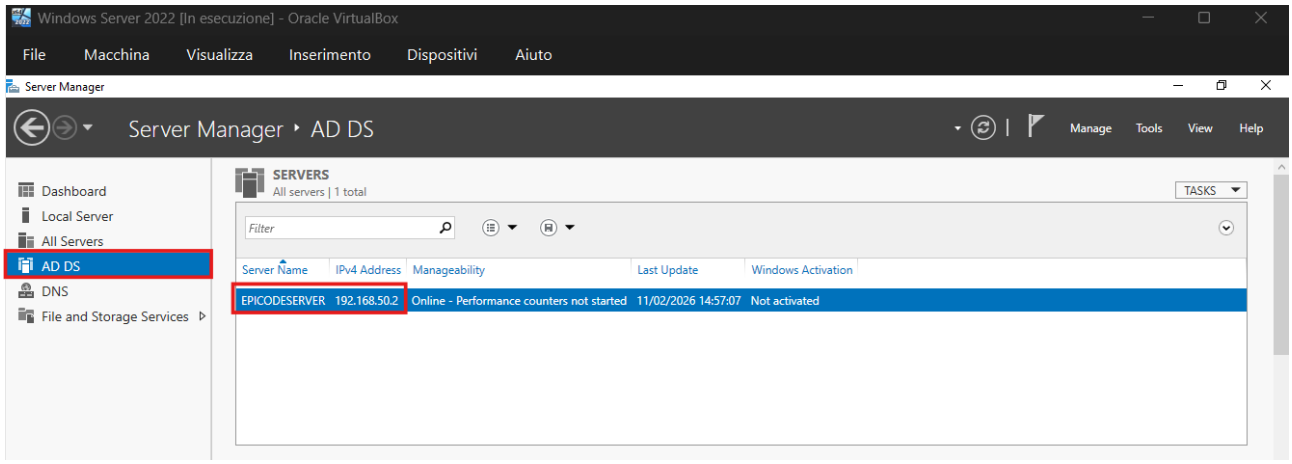


Output nome computer (Local Server) e Time Zone.

---

2) Installazione Active Directory Domain Services (AD DS)

1. In **Server Manager** clicco **Manage** → **Add Roles and Features**
2. Vado avanti con **Next** lasciando default
3. Seleziono **Active Directory Domain Services**
4. Clicco **Add Features**
5. Next → Next → **Install**

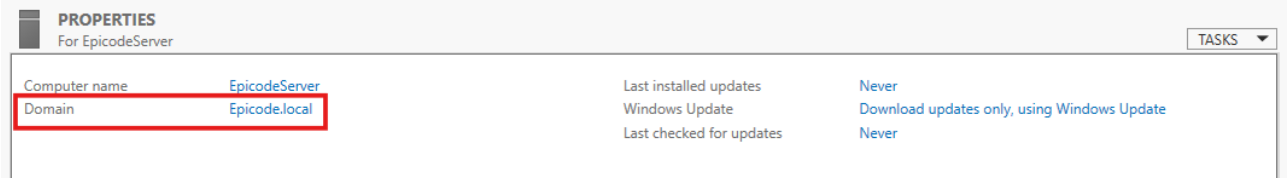


Il ruolo Active Directory Domain Services è stato installato.
Il server è operativo come Domain Controller.

---

3) Promozione a Domain Controller e creazione Foresta/Dominio

1. Finita l'installazione, in Server Manager clicco la notifica (triangolo giallo) → **Promote this server to a domain controller**
2. Scelgo **Add a new forest**
3. Dominio: **`epicode.local`**
4. Imposto la password **Personale** (Directory Services Restore Mode)
5. Lascio default dove indicato → **Install**
6. Al termine: **riavvio automatico**



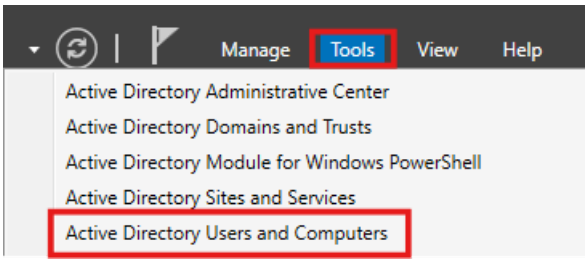
Output promozione a Domain Controller andata a buon fine.

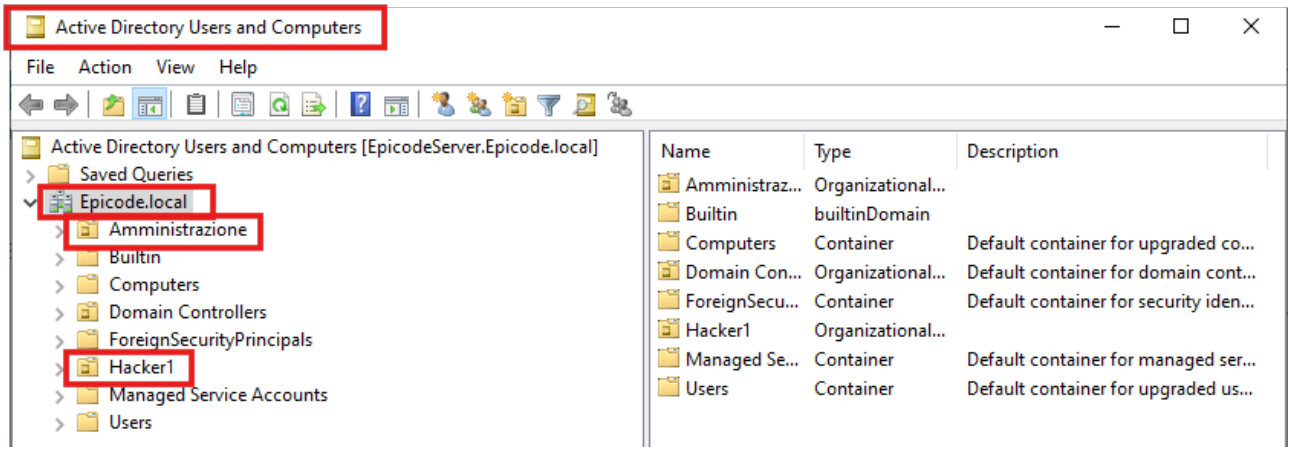
---

4) Creazione OU (Unità Organizzative), utenti e gruppi

4.1 Creo le OU

1. Apro **Tools** → **Active Directory Users and Computers**
2. Espando **`epicode.local`**
3. Tasto destro sul dominio → **New** → **Organizational Unit**
4. Creo:
    - `Amministrazione`
    - `Hacker1`





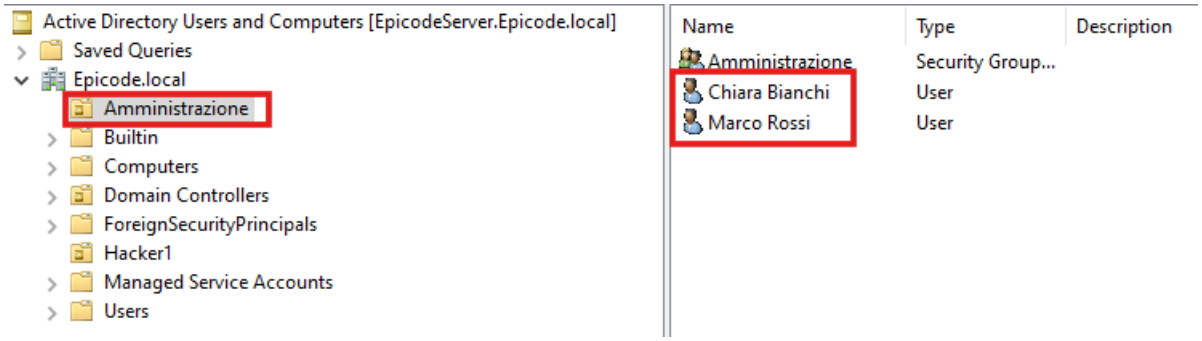
4.2 Creo gli utenti

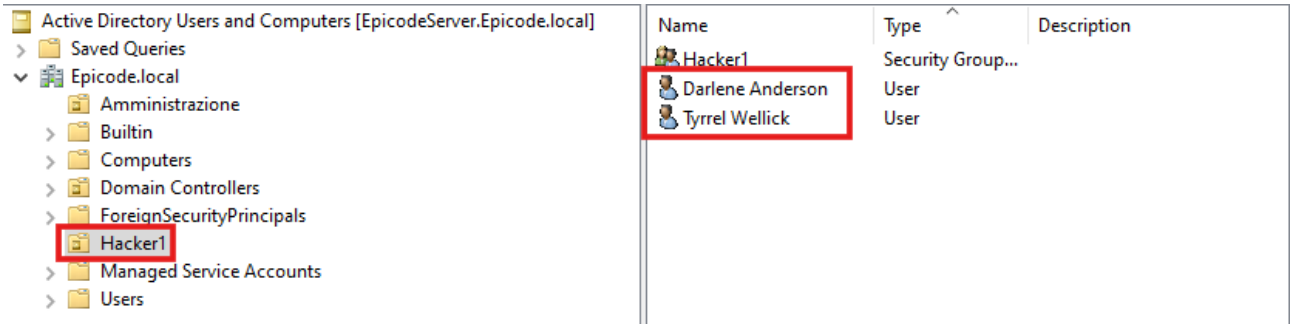
Dentro **Amministrazione** creo:

- **Chiara Bianchi**
- **Marco Rossi**

Dentro **Hacker1** creo:

- **Tyrrel Wellick**
- **Darlene Anderson**





Per ogni utente:

1. Tasto destro OU → **New** → **User**
2. Compilo nome/cognome e username
3. Imposto password
4. Metto flag: **User must be change password at next logon** (così l'admin non "deve conoscere" la password finale) (Chiara Bianchi in Amministrazione non avrà la spunta sul flag mentre gli altri utenti si)

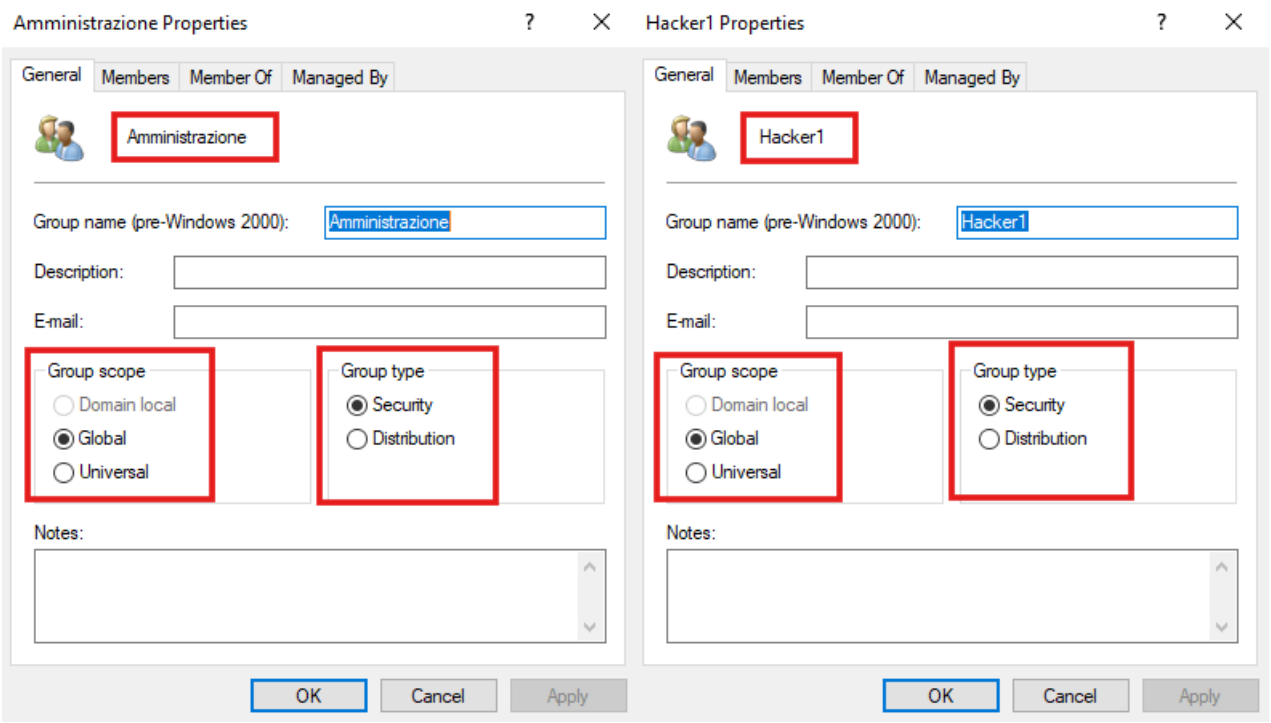
4.3 Creo i gruppi e assegno i membri

Dentro **Amministrazione**:

- gruppo **Amministrazione** → membri: **Chiara** e **Marco**

Dentro **Hacker1**:

- gruppo **Hacker1** → membri: **Darlene** e **Tyrrel**

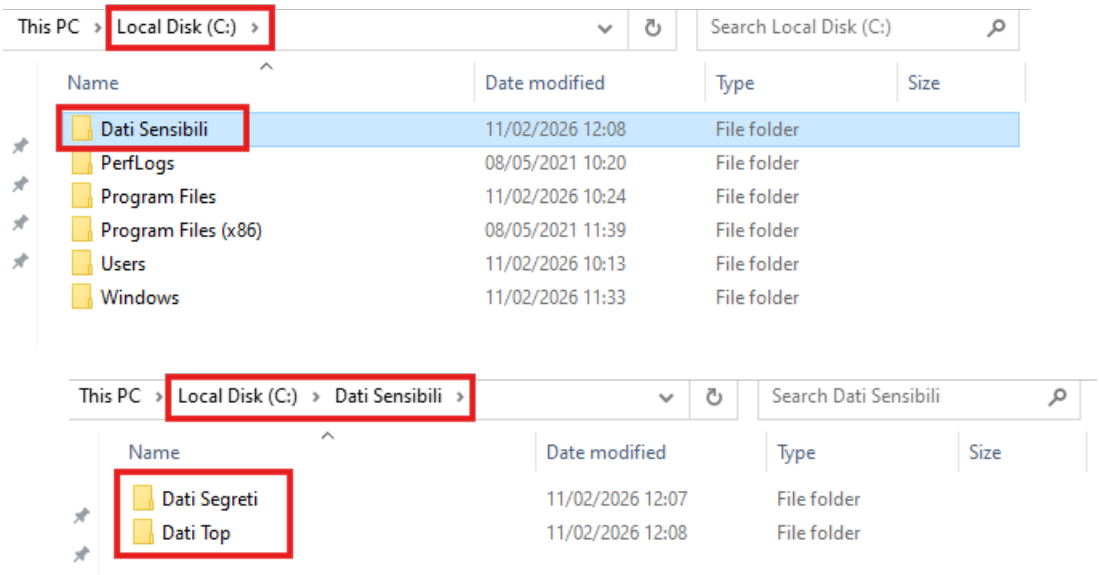


---

5) Creazione cartelle e permessi (policy aziendale)

5.1 Creo struttura cartelle sul Server

1. Sul Server creo una cartella:
   - **`Dati Sensibili`**
2. Dentro creo:
   - **`Dati Segreti`**
   - **`Dati Top`**
3. Metto dentro qualche file “di test” (anche txt va bene)



5.2 Obiettivo permessi

- `Dati Sensibili`: tutti gli utenti possono **vedere** le cartelle contenute
- `Dati Segreti`: accesso/modifica **solo gruppo Amministratore**
- `Dati Top`: accesso/modifica **solo gruppo Hacker1**

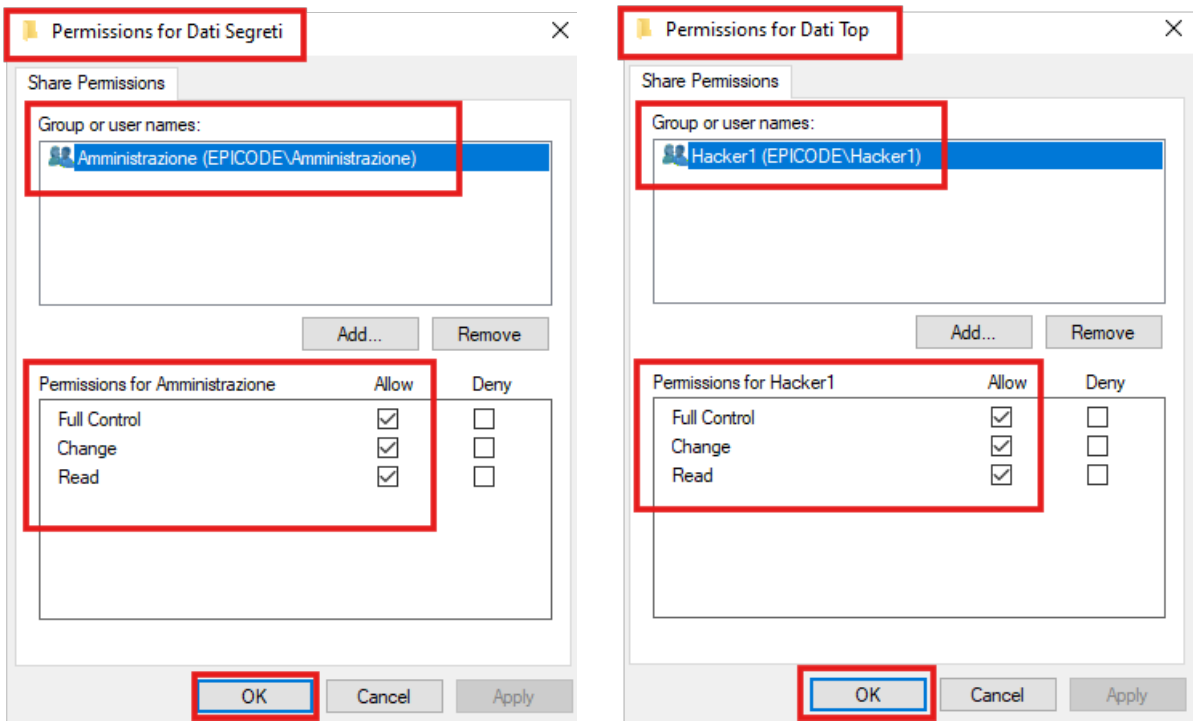
5.3 Condivisione (Sharing) — per Dati Segreti

1. Tasto destro su `Dati Segreti` → **Properties**
2. Tab **Sharing** → **Advanced Sharing**
3. Flag **Share this folder**
4. **Permissions**
5. Seleziono **Everyone** → **Remove**
6. **Add** → inserisco **`Amministratore`** → OK
7. Do **Full Control** (sul livello Sharing) → Apply → OK

5.4 Condivisione (Sharing) — per Dati Top

Stessi identici passi su `Dati Top`, ma:

- rimuovo **Everyone**
- aggiungo **Hacker1**
- Full Control → Apply/OK



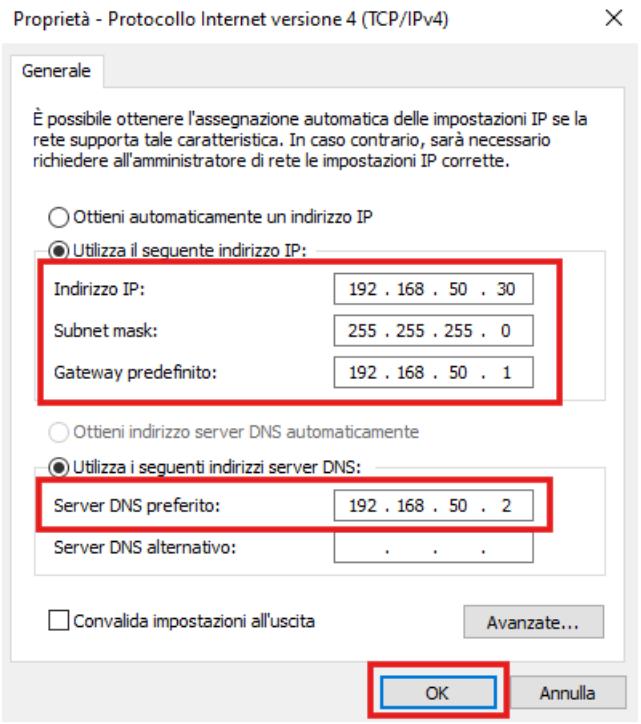
Output permessi per Amministrazione e Hacker1

---

6) Configurazione Windows 10 Pro (client) + join al dominio

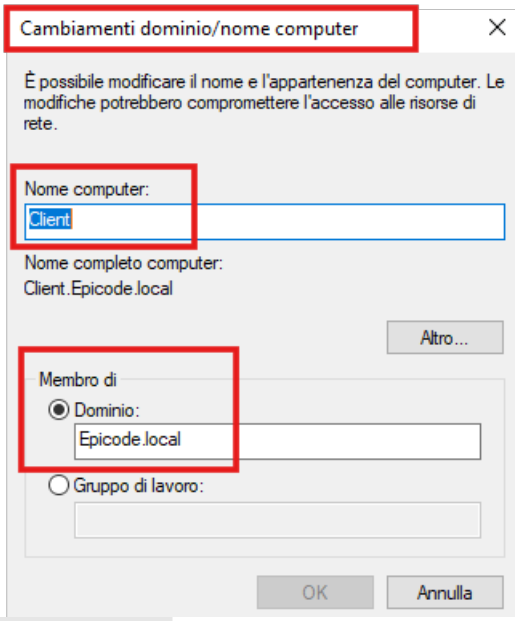
6.1 Rete del client + DNS verso il server

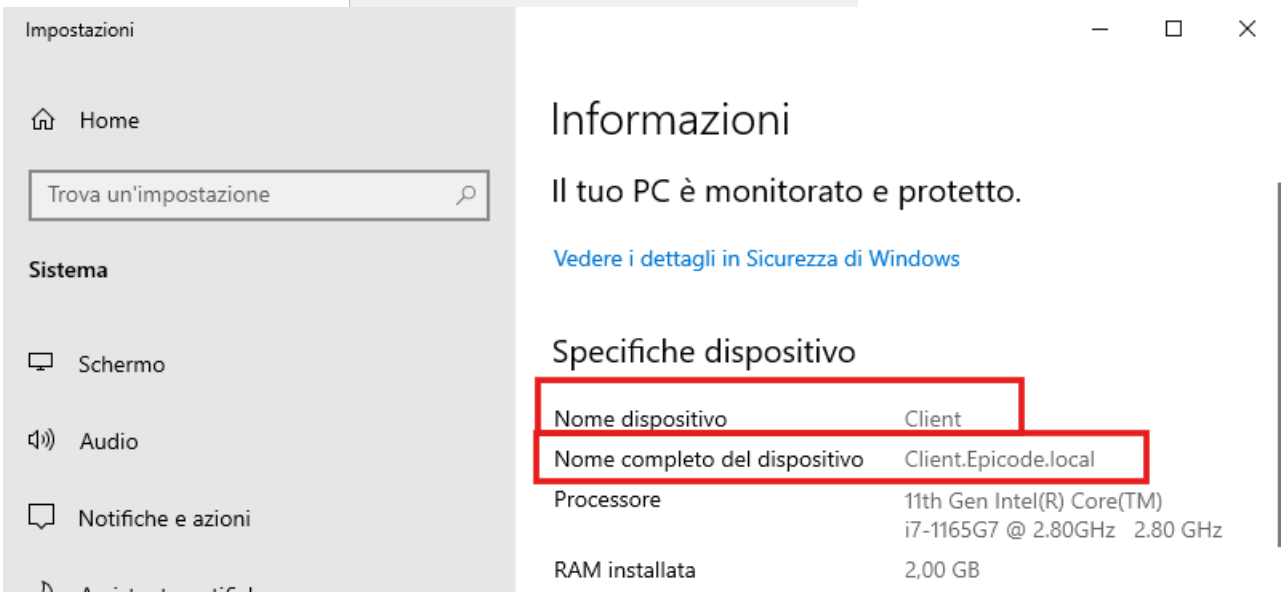
1. Sul client imposto la scheda su **Rete Interna** (stessa rete del server)
2. Imposto **IP statico** nella stessa subnet del server (es. **`192.168.50.30`**)
3. Imposto **DNS primario = IP del server** (**`192.168.50.2`**)



6.2 Nome PC + join dominio

1. Start → cerco **About** / **System**
2. **Rename this PC (advanced)** oppure **Change settings**
3. **Change...**
4. Imposto un nome PC (**Client**)
5. Seleziono **Domain** e scrivo: **`epicode.local`**
6. Quando chiede credenziali inserisco:
    - user: **`Administrator`**
    - password: **quella dell'Administrator del server**
7. Confermo → messaggio di successo → **riavvio**





Output schermate di **nome computer** e **dominio** (prima/dopo o la conferma).

---

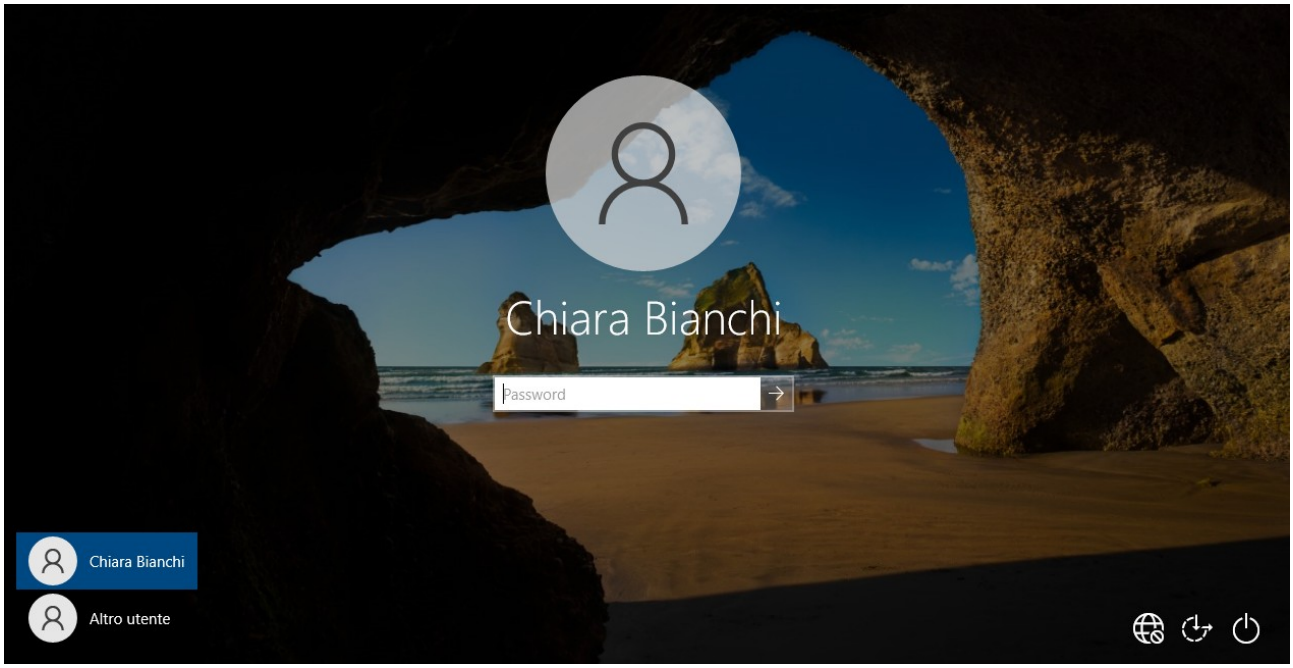
7) Verifica finale richiesta dall’ES: accesso con Chiara + screenshot

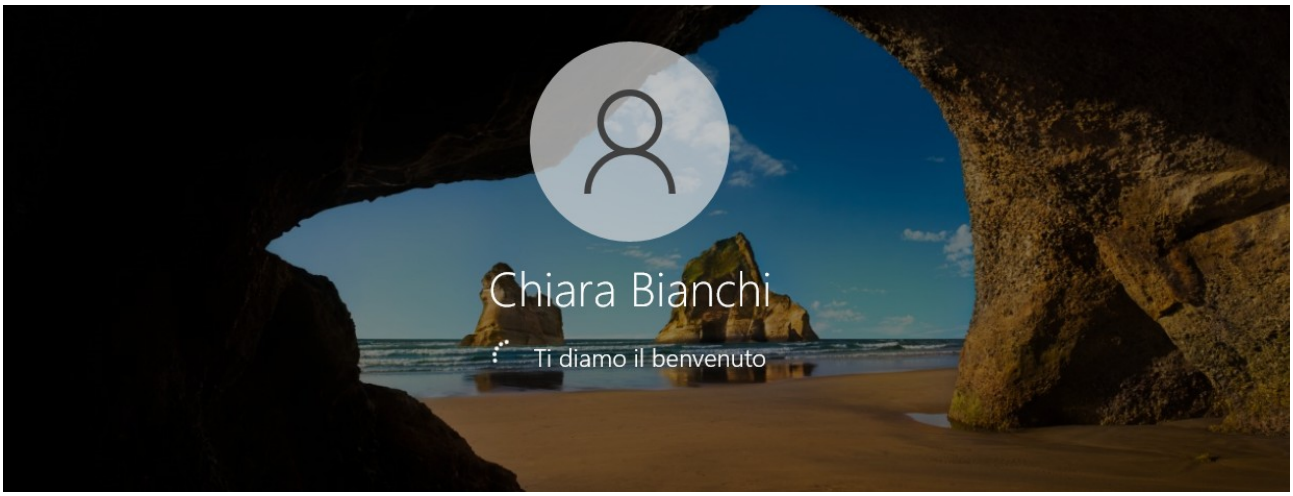
L’esercizio chiede esplicitamente **verifica con accesso di Chiara** e relativi screenshot.

7.1 Login con Chiara

1. Sul client, alla schermata di login seleziono **Other user**
2. Inserisco:
    - `EPICODE\chiara` **oppure** `chiara@epicode.local` (o Chiara Bianchi in base a come appare)
3. Primo accesso: **cambio password** (perché ho messo il flag)

- schermata login di Chiara
- desktop di Chiara dopo accesso





7.2 Accesso alle condivisioni e verifica dei permessi (Utente Chiara)

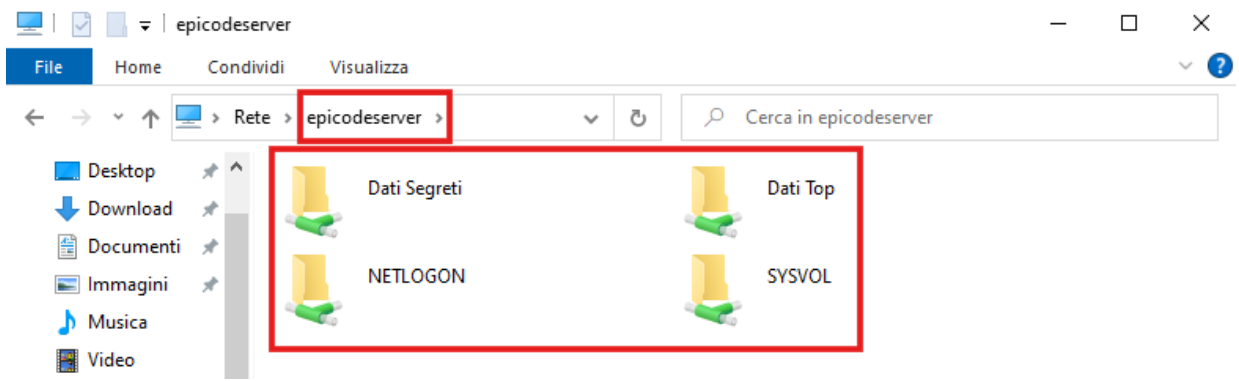
Dopo aver effettuato correttamente il login sul client Windows 10 con l'account di dominio **Chiara**, ho proceduto alla verifica dell'accesso alle risorse condivise sul Domain Controller.

Dal client ho aperto la cartella "File Explorer" e ho digitato:

```
\\epicodeserver
```

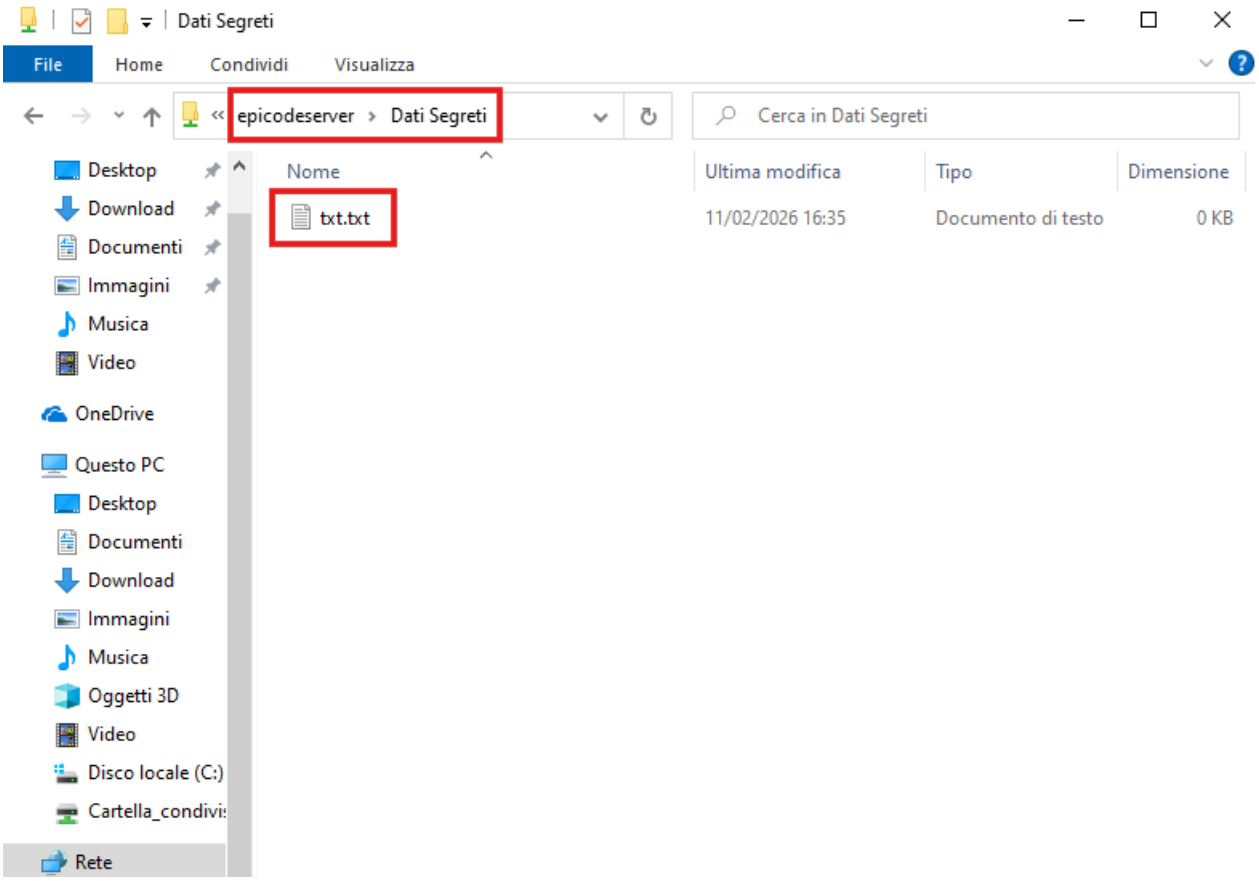
Sono state visualizzate le cartelle condivise:

- Dati Segreti
- Dati Top
- NETLOGON
- SYSVOL



Verifica accesso a “Dati Segreti”

Ho effettuato l’accesso alla cartella **Dati Segreti**.
L’accesso è avvenuto correttamente e ho potuto visualizzare e modificare il file presente (txt.txt), dimostrando che l’utente Chiara dispone delle autorizzazioni previste.

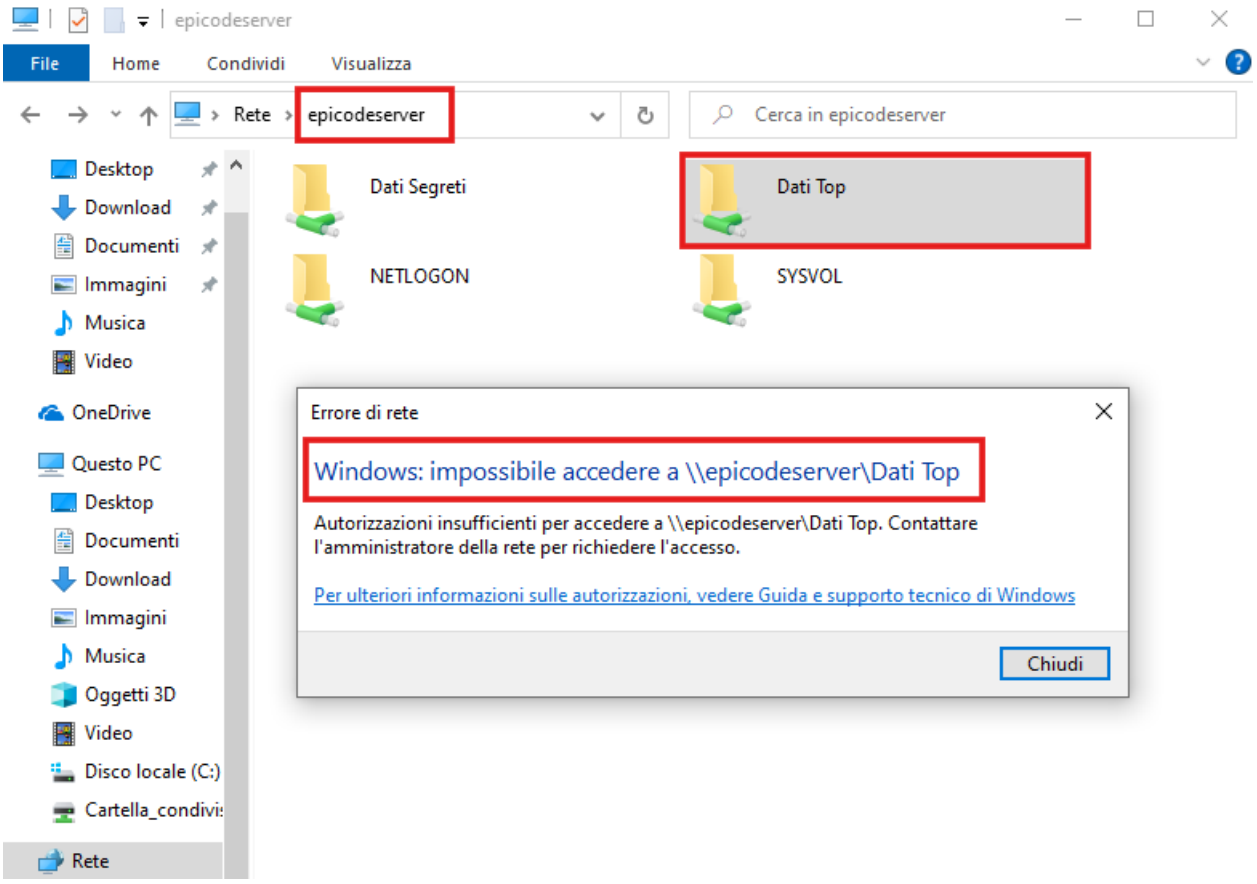


Verifica accesso a “Dati Top”

Successivamente ho tentato di accedere alla cartella **Dati Top**.
Il sistema ha restituito il messaggio:

> **Autorizzazioni insufficienti per accedere a \epicodeserver\Dati Top**

Questo comportamento conferma che **Chiara non appartiene al gruppo Hacker1** e che i permessi di sicurezza sono configurati correttamente.



Esito della verifica:

La configurazione dei gruppi e delle autorizzazioni risulta funzionante:

- **Chiara può accedere solo alle risorse previste dal proprio ruolo.**
- **L’accesso alle cartelle non autorizzate viene correttamente bloccato.**

La gestione dei permessi tramite gruppi di sicurezza in Active Directory è stata implementata correttamente.

Conclusione finale:

L’accesso effettuato con l’account di Chiara ha confermato il corretto funzionamento dei permessi: **accesso consentito alle risorse autorizzate (Dati Segreti) e accesso negato alle risorse non previste (Dati Top).**

La gestione delle autorizzazioni tramite Active Directory e gruppi di sicurezza risulta configurata in modo corretto e funzionante.