

Progetto S10 – L5

Titolo:

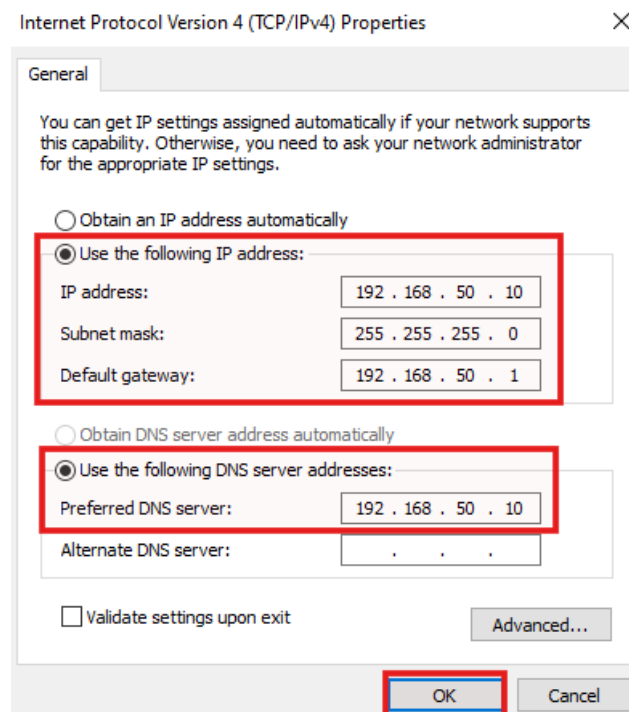
Windows Server 2022 – Active Directory, Gruppi (Team Cybersecurity) e Permessi su Condivisioni

Introduzione:

In questo esercizio configuro un dominio Active Directory, creo OU, utenti e **gruppi orientati a un team Cybersecurity**, imposto una struttura di cartelle condivise e applico permessi coerenti con le policy, verificando tutto da un client Windows in dominio.

Prerequisiti (ambiente)

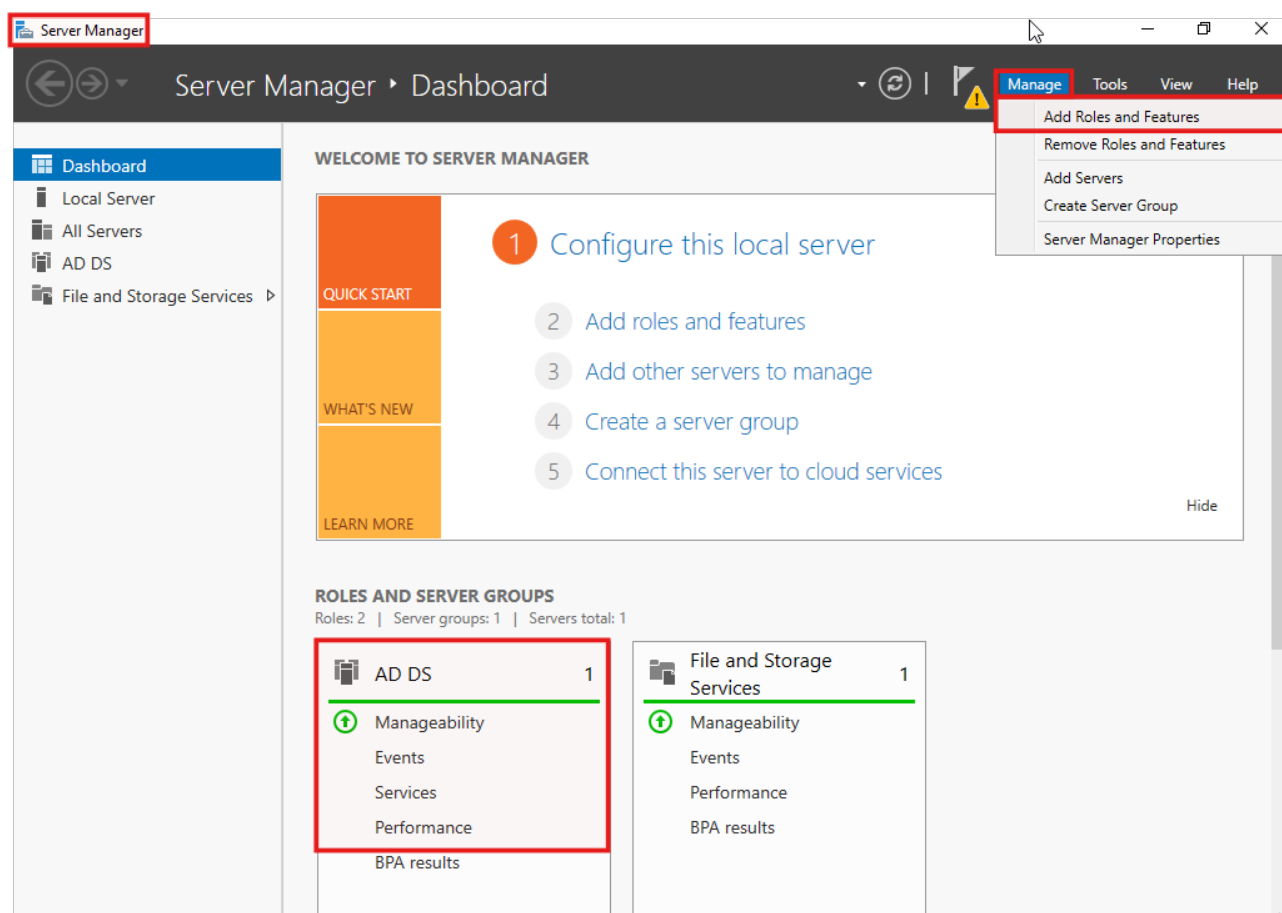
1. Accedo a **Windows Server 2022** con account **Administrator**.
2. Verifico che la scheda di rete della VM sia in **Rete interna**.
3. Imposto l'IP del server **statico** e come DNS primario metto **l'IP del server stesso** (il server farà da DNS).



- IP statico + DNS = IP del server
-

1) Installazione Active Directory Domain Services (AD DS)

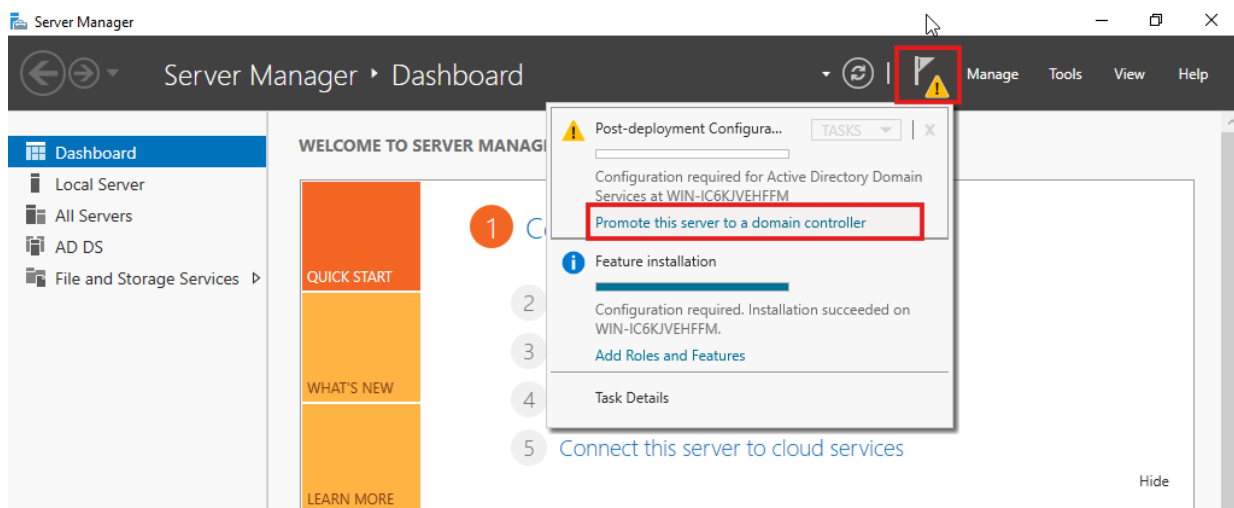
1. Apro **Server Manager**.
2. Clicco **Manage** → **Add Roles and Features**.
3. Vado avanti con **Next** fino a **Server Roles**.
4. Seleziono **Active Directory Domain Services**.
5. Quando richiesto, clicco **Add Features**.
6. Continuo **Next** → **Install**.
7. A fine installazione clicco **Close**.

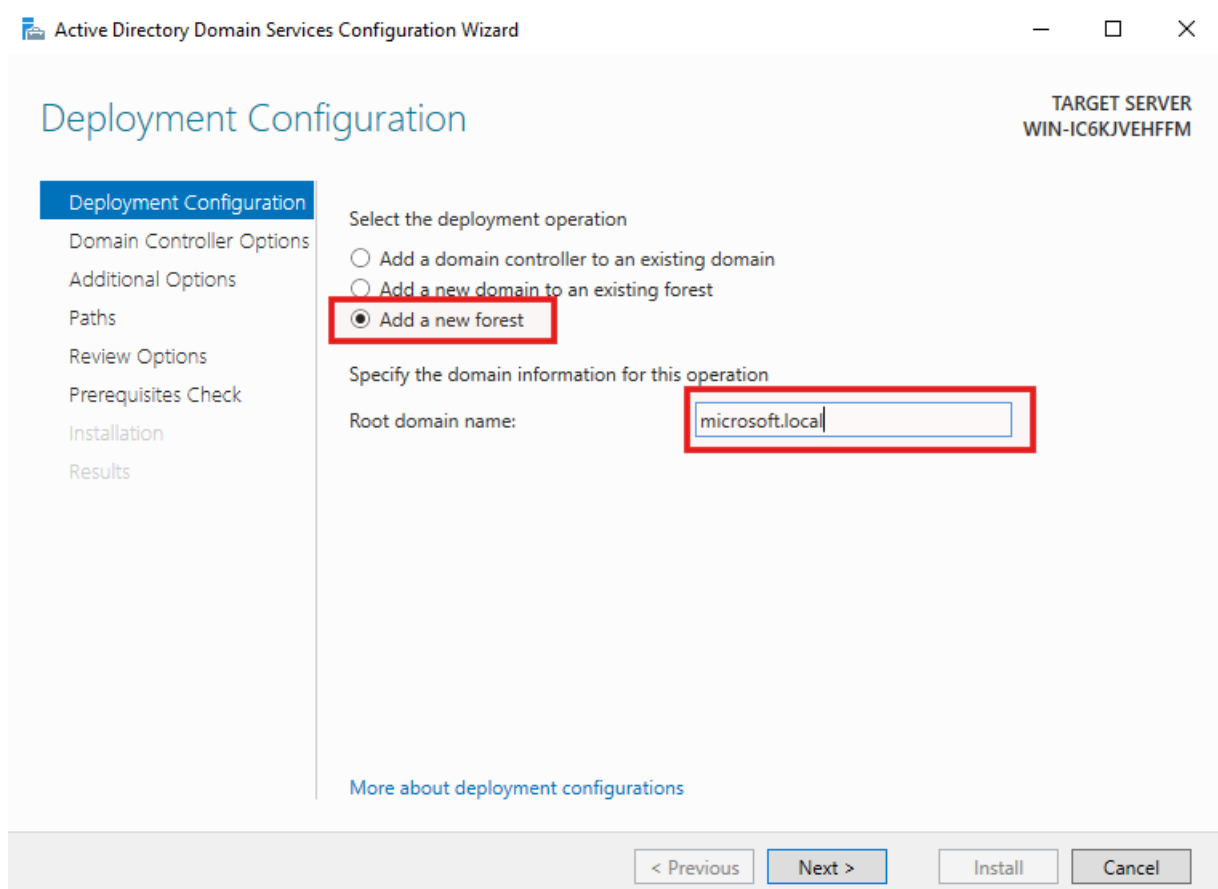
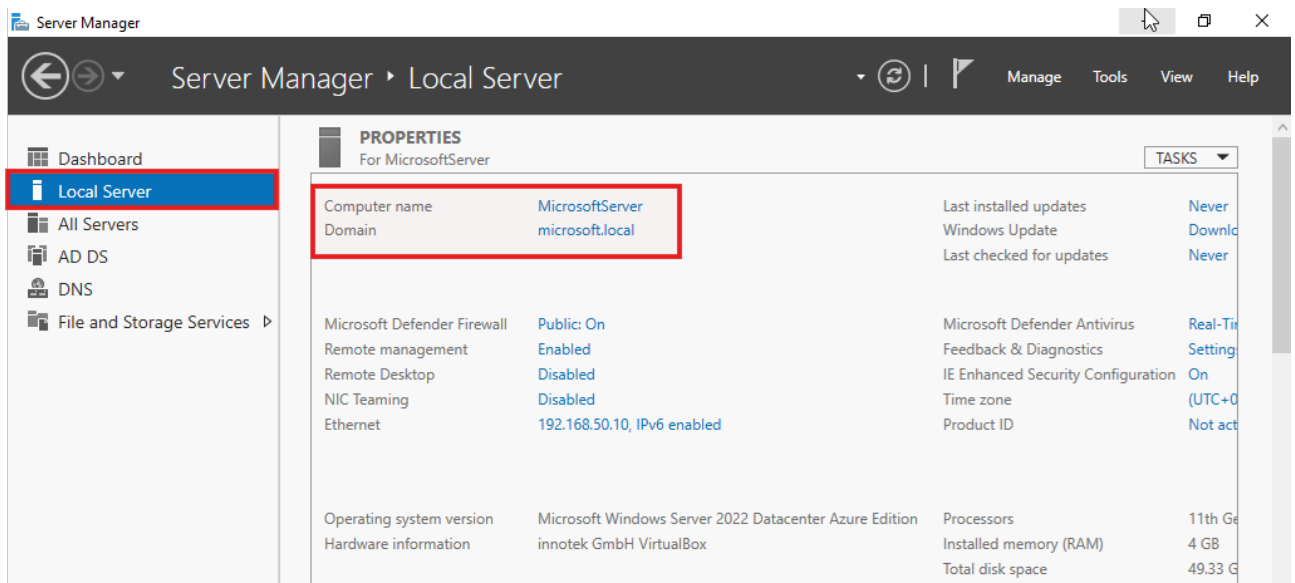


- Ruolo AD DS selezionato
- Install completata

2) Promozione a Domain Controller e creazione foresta/dominio

1. In Server Manager clicco la notifica (triangolo giallo) e seleziono **Promote this server to a domain controller**.
2. Scelgo **Add a new forest**.
3. Inserisco il nome dominio, ad esempio: **microsoft.local** (il mio dominio scelto).
4. Imposto la **DSRM password** (diversa dalle altre).
5. Lascio le opzioni di default e clicco **Next** fino a **Install**.
6. Il server si riavvia.



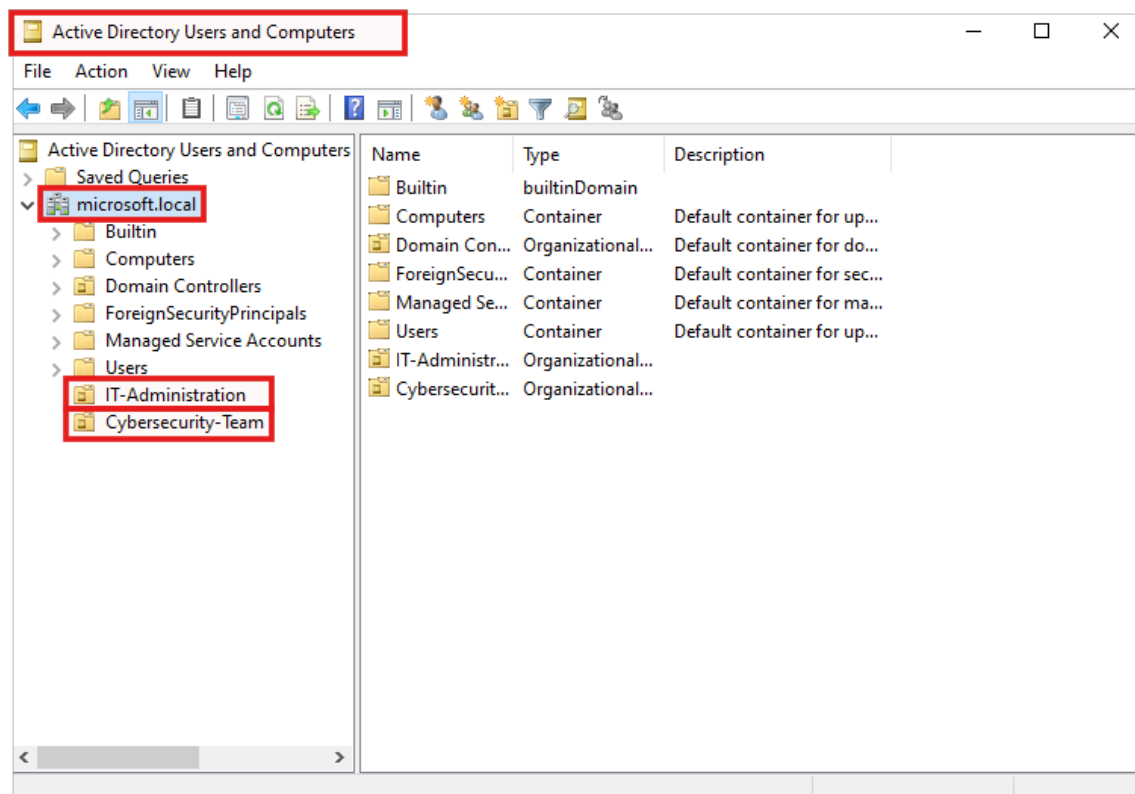
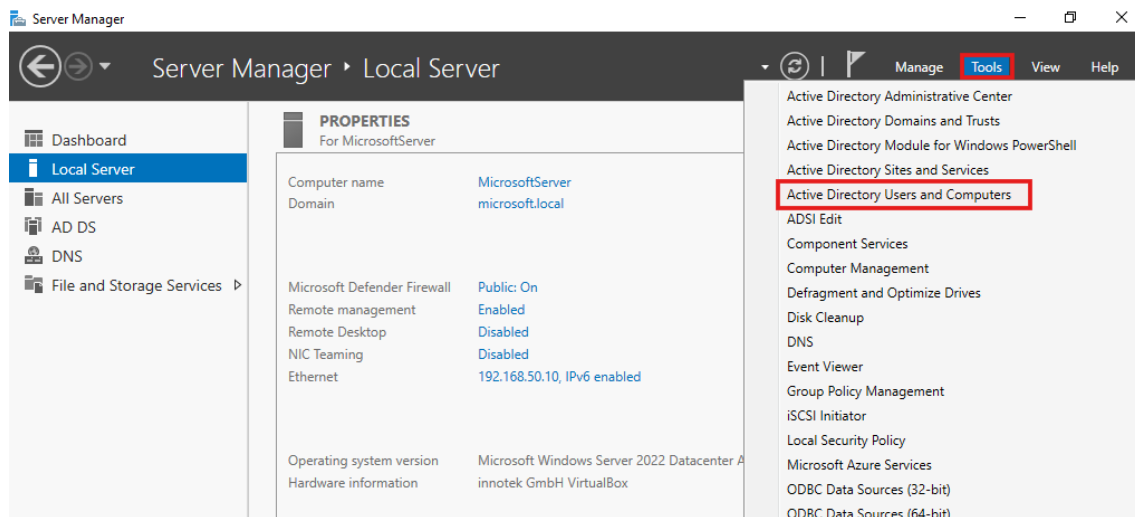


- Schermata Promote this server to a domain controller.
- Schermata “Add a new forest”
- Nome dominio (**microsoft.local**)

3) Creazione OU (struttura organizzativa)

Qui introduco il riferimento al team Cybersecurity.

1. Apro **Tools** → **Active Directory Users and Computers (ADUC)**.
2. Espando il dominio **microsoft.local**.
3. Tasto destro sul dominio → **New** → **Organizational Unit**.
4. Creo queste OU:
 - **IT-Administration**
 - **Cybersecurity-Team** (OU dedicata al team Security/SOC/IR)



- OU (**IT-Administrator** e **Cybersecurity-Team**) create e visibili sotto il dominio

4) Creazione utenti (esempi)

4.1 Utenti IT-Administration

1. Entro in **OU IT-Administration**.
2. Tasto destro → **New** → **User**.
3. Creo due utenti, ad esempio:
 - **Federica Rossi** (federica.rossi)
 - **Martina Bianchi** (martina.bianchi)
4. Imposto una password e **spunto** “User must change password at next logon”
5. Gli utenti **IT-Administration** sono configurati con password iniziale e obbligo di cambio al primo accesso per garantire che la password definitiva sia scelta solo dall’utente, assicurando riservatezza e maggiore sicurezza su account con privilegi elevati

The image displays two side-by-side screenshots of the 'New Object - User' dialog box in Active Directory, illustrating the configuration steps for a new user.

Left Screenshot: The dialog box shows the 'Create in' field set to 'microsoft.local/IT-Administration'. The 'First name' is 'Federica', 'Last name' is 'Rossi', and 'Full name' is 'Federica Rossi'. The 'User logon name' field is highlighted with a red box and contains 'federica.rossi'. The 'User logon name (pre-Windows 2000)' field contains 'MICROSOFT\'. The 'Next >' button is highlighted.

Right Screenshot: The dialog box shows the 'Password' and 'Confirm password' fields, both containing masked text. The 'User must change password at next logon' checkbox is checked and highlighted with a red box. Other options like 'User cannot change password', 'Password never expires', and 'Account is disabled' are unchecked. The 'Next >' button is highlighted.

New Object - User

Create in: microsoft.local/IT-Administration

First name:

Initials:

Last name:

Full name:

User logon name:

@microsoft.local

User logon name (pre-Windows 2000):

< Back

Next >

Cancel

New Object - User

Create in: microsoft.local/IT-Administration

Password:

Confirm password:

☒ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back

Next >

Cancel

4.2 Utenti Cybersecurity-Team

1. Entro in **OU Cybersecurity-Team**.
2. **New** → **User** e creo due utenti, ad esempio:
 - **Elliot SOC** (elliott.soc)
 - **Condor IR** (condor.ir)
3. Anche qui: password iniziale + **tolta la spunta** su "User must change password at next logon"
4. Gli account del team Cybersecurity sono stati configurati con **password predefinita controllata dall'amministratore per finalità di laboratorio e test controllati**.

New Object - User

Create in: microsoft.local/Cybersecurity-Team

First name:

Initials:

Last name:

Full name:

User logon name:

@microsoft.local

User logon name (pre-Windows 2000):

< Back

Next >

Cancel

New Object - User

Create in: microsoft.local/Cybersecurity-Team

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

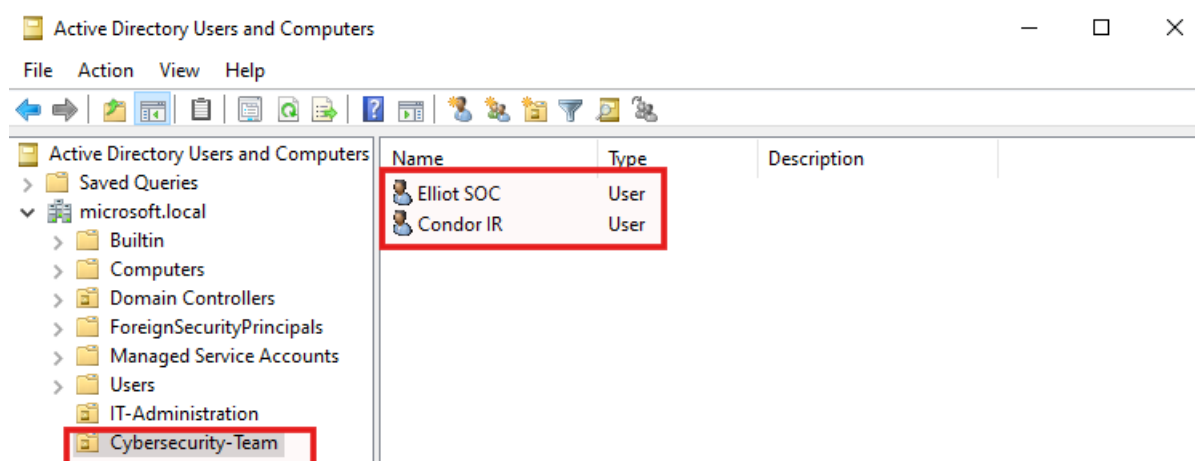
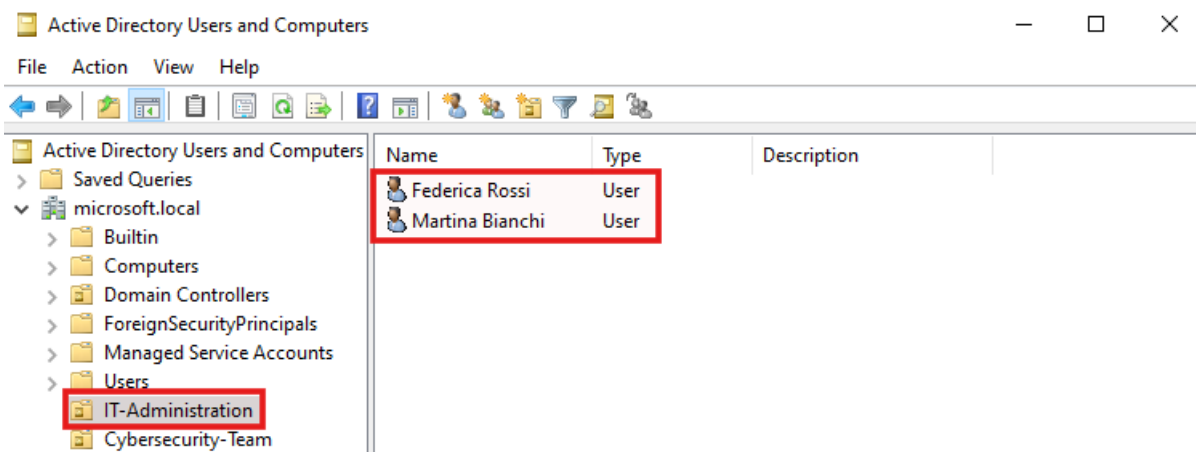
☐ Account is disabled

< Back

Next >

Cancel

A seguire la lista utenti dentro ogni OU



5) Creazione gruppi (con riferimento al team Cybersecurity)

Qui creo i gruppi “ruolo” e ci aggiungo gli utenti.

5.1 Gruppo IT

1. Entro in **OU IT-Administration**.
2. Tasto destro → **New** → **Group**.
3. Nome gruppo: **IT-Admins**
4. Lascio **Group scope** e **Group type** su impostazioni standard (Security Group).
5. Apro le proprietà del gruppo → **Members** → **Add**.
6. Aggiungo: **Federica;Martina** (separati da ; sulla stessa riga).
7. Eseguo il **Check Names** per confermare

Figura 1

New Object - Group

Create in: microsoft.local/IT-Administration

Group name: IT-Admins

Group name (pre-Windows 2000): IT-Admins

Group scope

☐ Domain local

☒ Global

☐ Universal

Group type

☒ Security

☐ Distribution

OK Cancel

Figura 2

Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type: Users, Service Accounts, Groups, or Other objects

Object Types...

From this location: microsoft.local

Locations...

Enter the object names to select (examples):

Federica Rossi (federica.rossi@microsoft.local);
Martina Bianchi (martina.bianchi@microsoft.local)

Check Names

Advanced... OK Cancel

Figura 3

IT-Admins Properties

General Members Member Of Managed By

Members:

Name	Active Directory Domain Services Folder
Federica Rossi	microsoft.local/IT-Administration
Martina Bianchi	microsoft.local/IT-Administration

Add... Remove

OK Cancel Apply

5.2 Gruppo Cybersecurity (SOC/IR)

1. Entro in **OU Cybersecurity-Team**.
2. **New** → **Group**.
3. Nome gruppo: **Cybersecurity-SOC**
4. **Members** → **Add**.
5. Aggiungo: **Elliot;Condor**.
6. Eseguo il **Check Names** per confermare

Figura 1

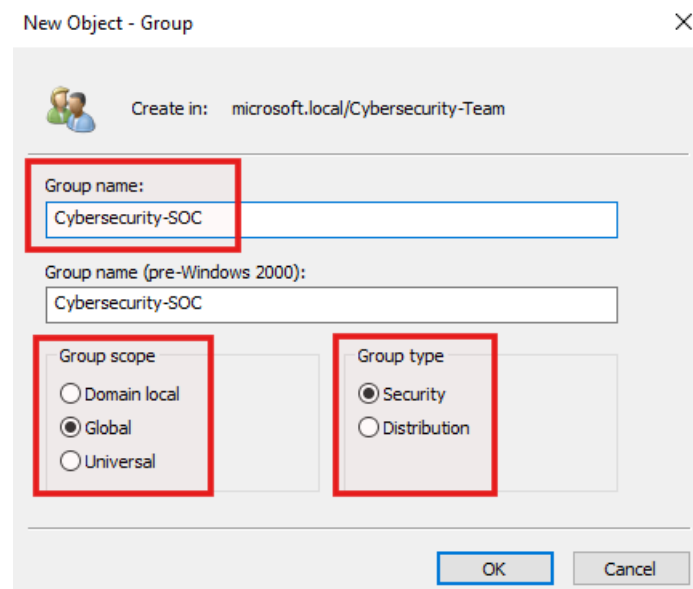
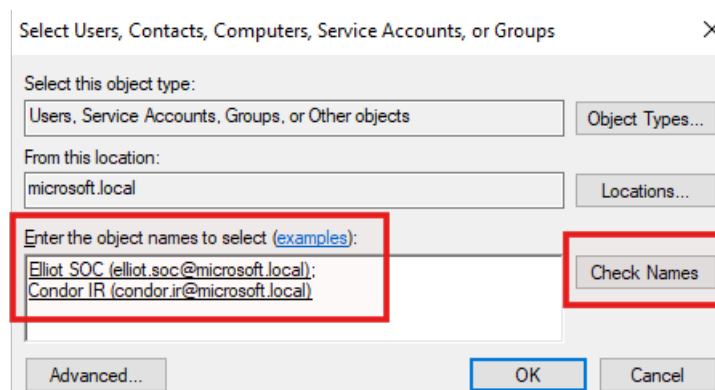


Figura 2



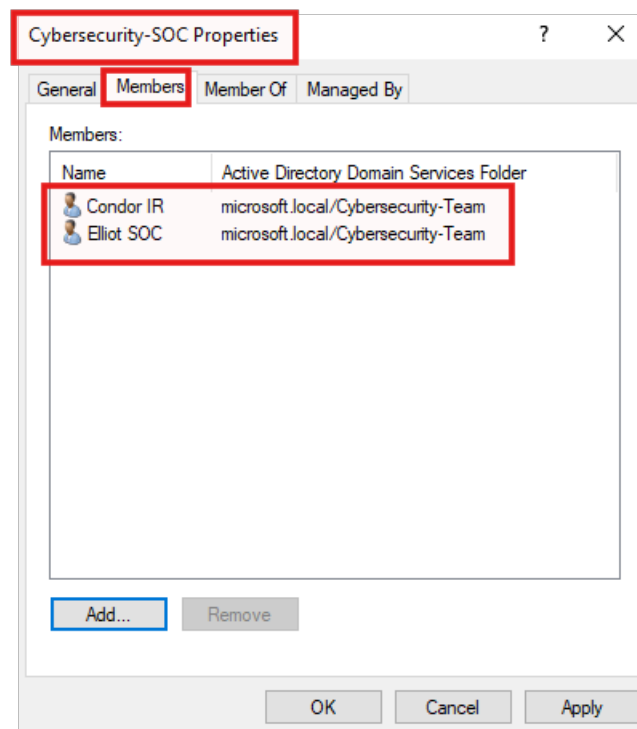
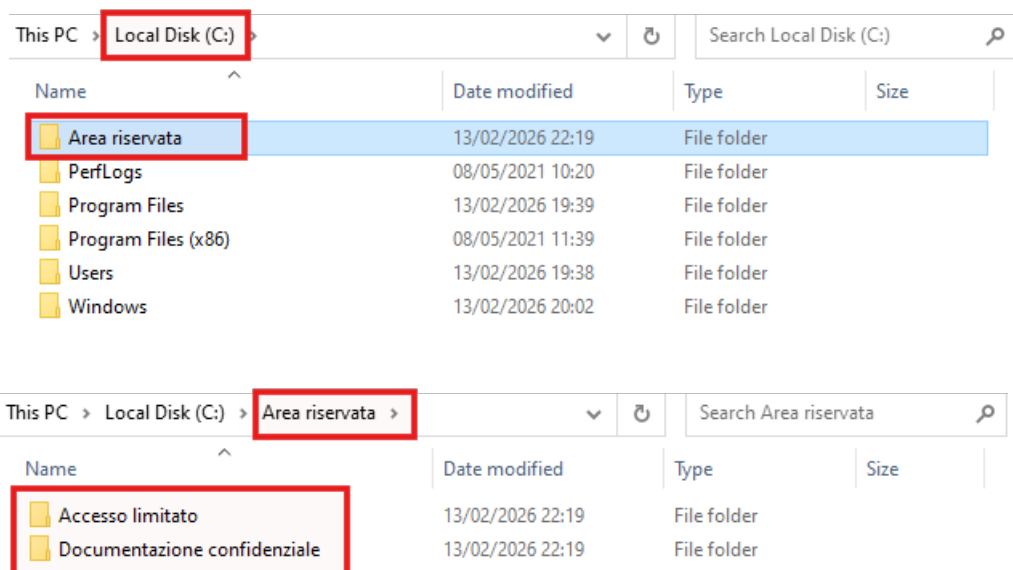


Figura 3

6) Creazione cartelle sul server (struttura dati)

1. Sul server apro **File Explorer**.
2. Creo una cartella principale: **Area riservata**.
3. Dentro creo due sottocartelle:
 - **Documentazione confidenziale**
 - **Accesso limitato**
4. (Facoltativo) Inserisco 1–2 file di test dentro ogni cartella per rendere evidente la verifica.



- Struttura cartelle completa

7) Condivisione e permessi (Sharing + Security)

Concetto chiave: quando si accede via rete conta l'intersezione tra **Sharing** e **Security/NTFS** (vince la più restrittiva).

7.1 Condivisione (Sharing) – Documentazione confidenziale

1. Tasto destro su **Documentazione confidenziale** → **Properties**.
2. Tab **Sharing** → **Advanced Sharing**.
3. Spunto **Share this folder**.
4. Clicco **Permissions**.
5. Seleziono **Everyone** → **Remove**
6. Clicco **Add** e aggiungo **IT-Admins**.
7. Concedo **Full Control** al gruppo (lato sharing).
8. **Apply** → **OK**.

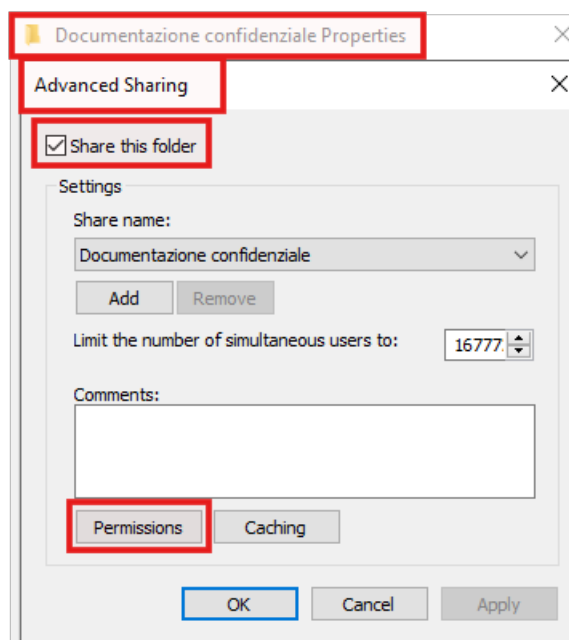


Figura 1

Figura 2

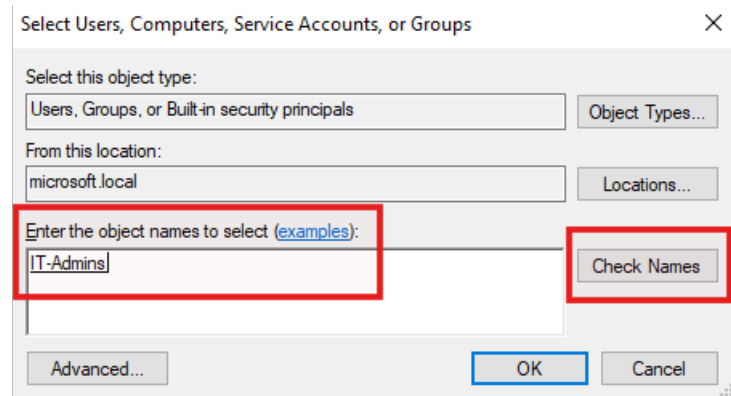
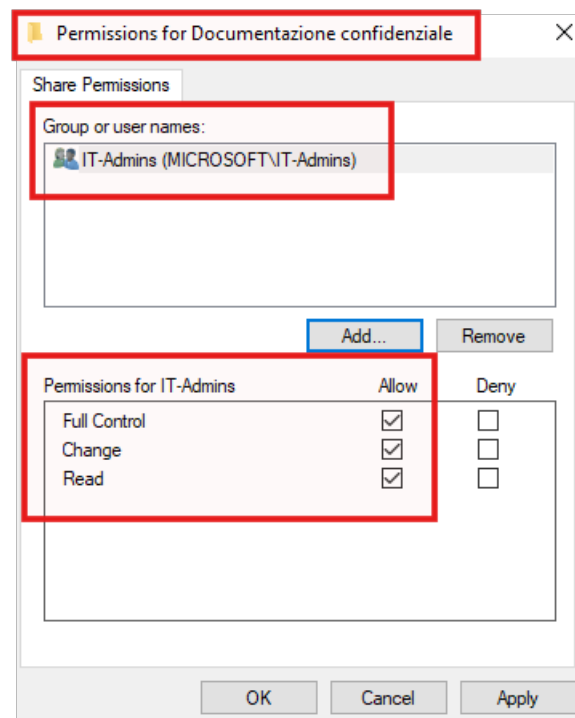


Figura 3



La cartella “**Documentazione confidenziale**” è stata condivisa assegnando i permessi al gruppo **IT-Admins**, garantendo accesso completo ai membri del reparto amministrativo IT. L’assegnazione è stata effettuata a livello di gruppo per semplificare la gestione centralizzata degli accessi e applicare il principio del least privilege.

7.2 Condivisione (Sharing) – Accesso limitato

1. Stessa procedura su **Accesso limitato**.
2. Rimuovo **Everyone**.
3. Aggiungo **Cybersecurity-SOC**.
4. Do **Full Control** (lato sharing).
5. **Apply** → **OK**.

Figura 1

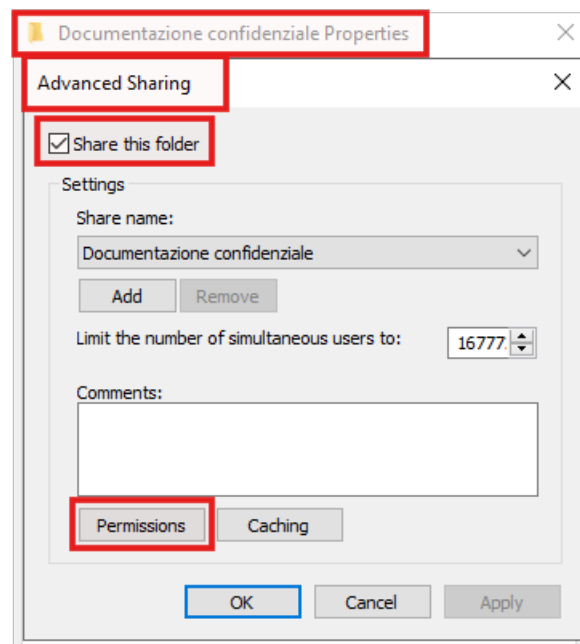


Figura 2

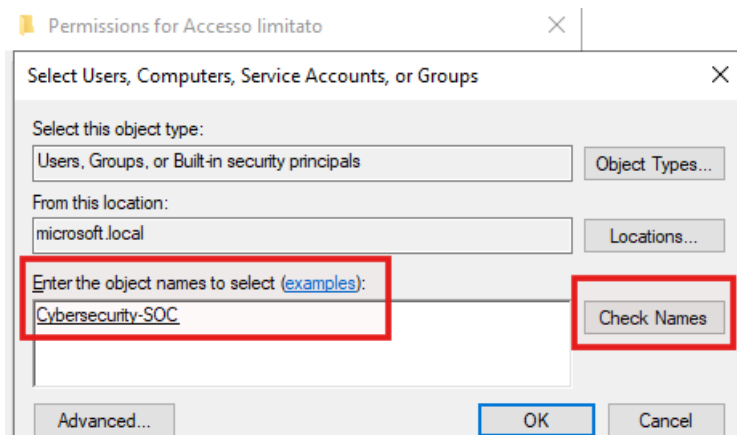
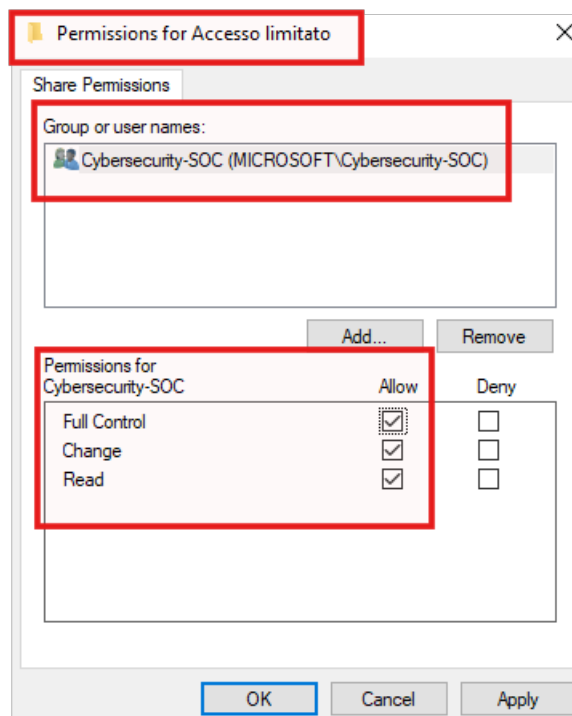


Figura 3



La cartella “**Accesso limitato**” è stata condivisa assegnando i permessi al gruppo **Cybersecurity-SOC**, riservando l’accesso esclusivamente ai membri del team Cybersecurity. Questa configurazione consente la separazione dei privilegi tra reparti e rafforza il controllo sugli asset sensibili.

8) Join del client Windows al dominio (e rete corretta)

1. Avvio **Windows 10 Pro** client.
2. Imposto anche qui la scheda in **Rete interna** (stessa rete del server).
3. Imposto IP del client nella stessa subnet del server e come DNS metto **IP del server**.
4. Rinomino il PC (**CLIENT-SECURITY**).
5. Metto il PC in dominio:
 - **Sistema → Rinomina questo PC (avanzate) → Cambiamenti dominio/nome computer**
 - Inserisco: **microsoft.local**
6. Quando chiede credenziali inserisco **Administrator** + password del server.
7. Riavvio.

Proprietà - Protocollo Internet versione 4 (TCP/IPv4)

Generale

È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.

☐ Ottieni automaticamente un indirizzo IP

☒ Utilizza il seguente indirizzo IP:

Indirizzo IP: 192 . 168 . 50 . 20

Subnet mask: 255 . 255 . 255 . 0

Gateway predefinito: 192 . 168 . 50 . 1

☐ Ottieni indirizzo server DNS automaticamente

☒ Utilizza i seguenti indirizzi server DNS:

Server DNS preferito: 192 . 168 . 50 . 10

Server DNS alternativo: . . .

☐ Convalida impostazioni all'uscita

Avanzate...

OK Annulla

Cambiamenti dominio/nome computer

È possibile modificare il nome e l'appartenenza del computer. Le modifiche potrebbero compromettere l'accesso alle risorse di rete.

Nome computer: CLIENT-SECURITY

Nome completo computer: CLIENT-SECURITY

Altro...

Membro di

☒ Dominio: microsoft.local

☐ Gruppo di lavoro: WORKGROUP

OK Annulla

Sicurezza di Windows

Cambiamenti dominio/nome computer

Immettere il nome e la password di un account con autorizzazione di accesso al dominio.

Administrator

.....

OK Annulla

Cambiamenti dominio/nome computer

È possibile modificare il nome e l'appartenenza del computer. Le modifiche potrebbero compromettere l'accesso alle risorse di rete.

Nome computer: CLIENT-SECURITY

Nome completo computer: CLIENT-SECURITY

Altro...

Membro di

☒ Dominio: microsoft.local

☐ Cambiamenti dominio/nome computer

Domino microsoft.local.

OK

Output:

- IP client, DNS del client = IP server
- Rinomina PC: CLIENT-SECURITY
- Dominio: microsoft.local

**Ping verso
192.168.50.10
(Server)
funzionante**

```
C:\Windows\system32>ping 192.168.50.10

Esecuzione di Ping 192.168.50.10 con 32 byte di dati:
Risposta da 192.168.50.10: byte=32 durata=1ms TTL=128
Risposta da 192.168.50.10: byte=32 durata=1ms TTL=128
Risposta da 192.168.50.10: byte=32 durata=2ms TTL=128
Risposta da 192.168.50.10: byte=32 durata=3ms TTL=128

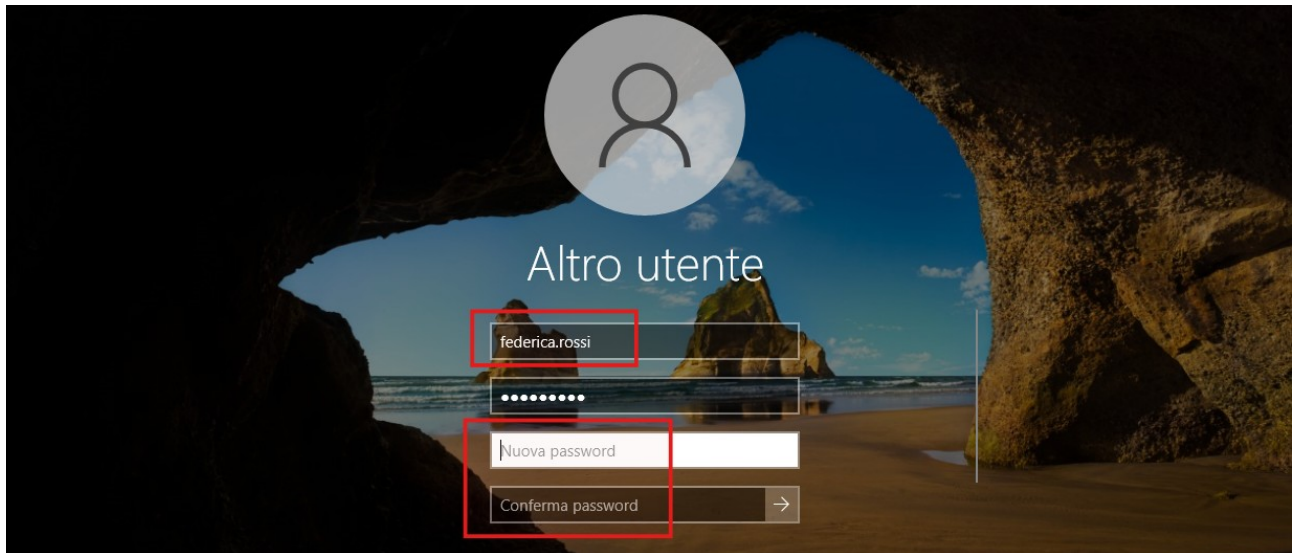
Statistiche Ping per 192.168.50.10:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 1ms, Massimo = 3ms, Medio = 1ms

C:\Windows\system32>
```

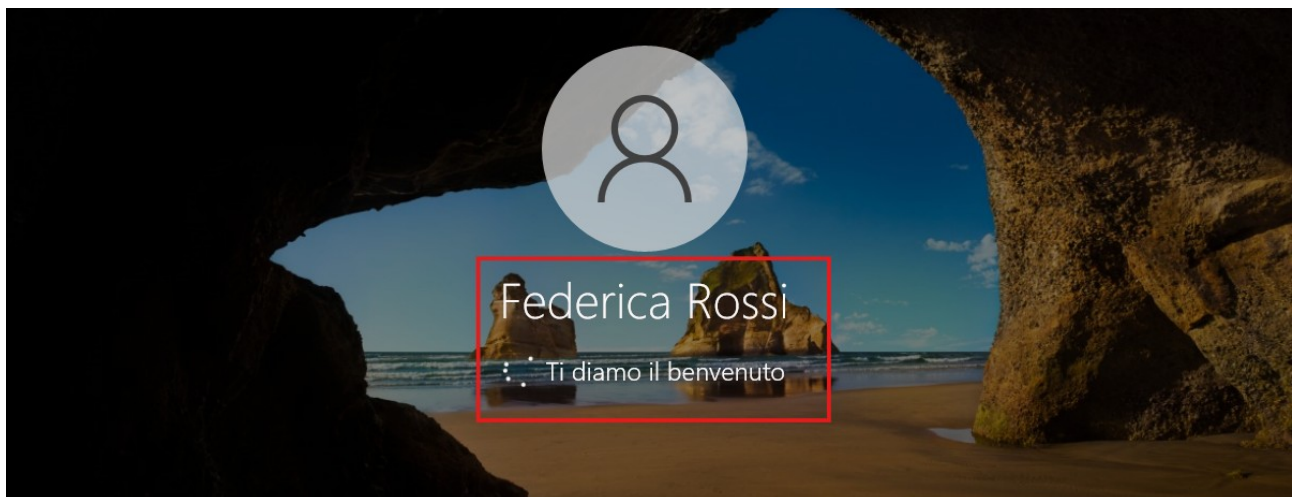

9) Verifica accessi (test pratici)

9.1 Test come utente IT (Federica)

1. Sul client faccio login (Altro utente) con **federica.rossi**
2. Al primo accesso cambio password.



Schermata di login di Federica Rossi



Schermata di login di Federica Rossi durante l'accesso



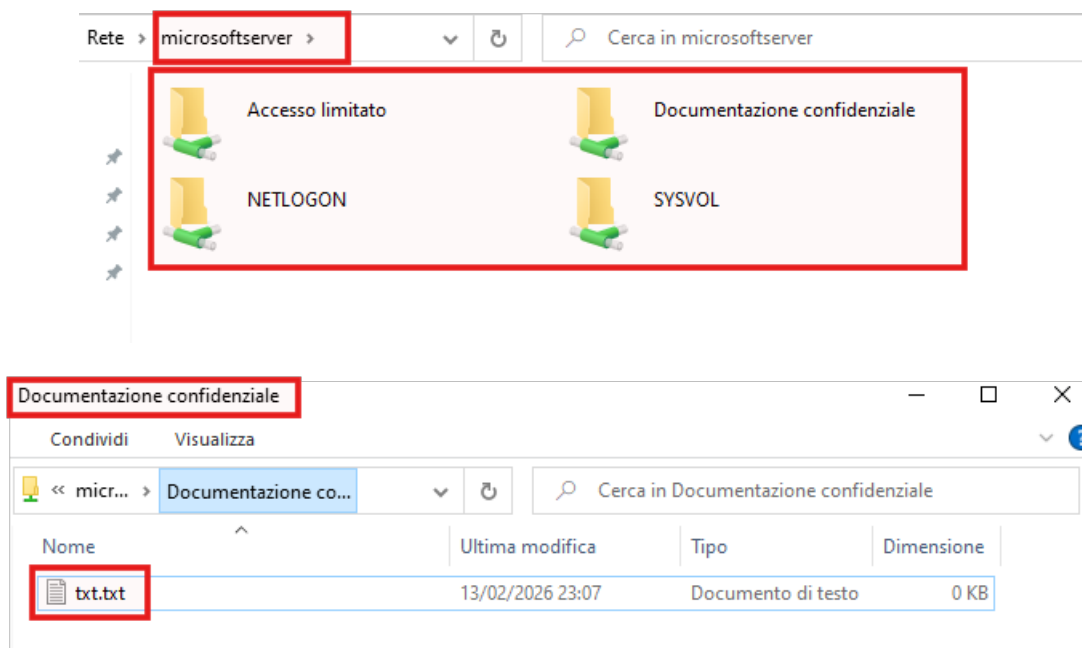
10) Accesso alle condivisioni e verifica dei permessi (Utente Federica)

Dopo aver effettuato correttamente il login sul client Windows 10 con l'account di dominio **Federica**, ho proceduto alla verifica dell'accesso alle risorse condivise sul Domain Controller. Dal client ho aperto la cartella "File Explorer" e ho digitato:

\\microsoftserver

Sono state visualizzate le cartelle condivise:

- **Documentazione confidenziale**
- **Accesso limitato**
- NETLOGON
- SYSVOL



Verifica accesso a “Documentazione confidenziale”

Ho effettuato l’accesso alla cartella **Documentazione confidenziale**.

L’accesso è avvenuto correttamente e ho potuto visualizzare e modificare il file presente (txt.txt), dimostrando che l’**utente Federica dispone delle autorizzazioni previste**.

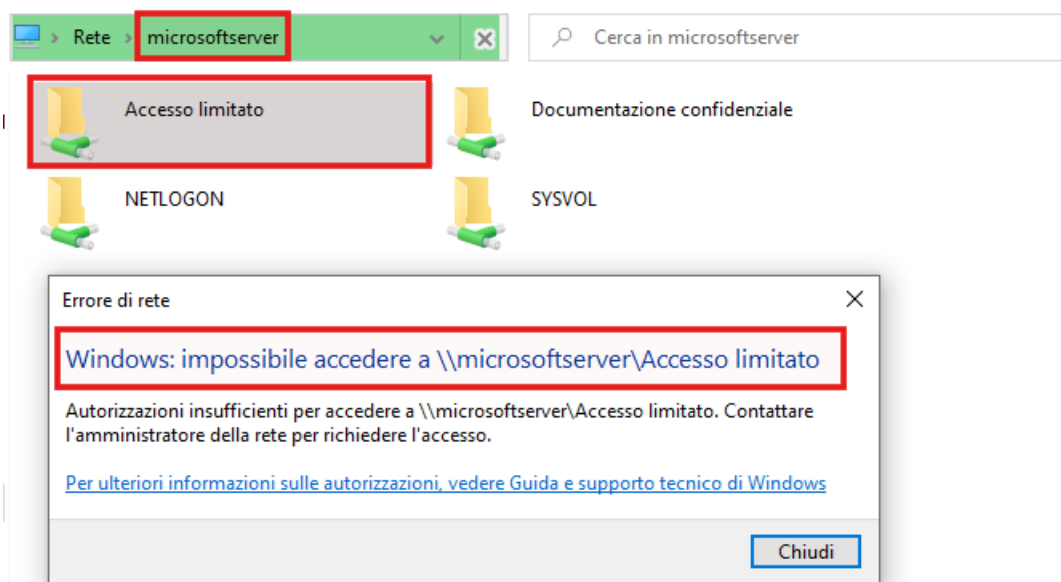
Verifica accesso a “Accesso limitato”

Successivamente ho tentato di accedere alla cartella **Accesso limitato**.

Il sistema ha restituito il messaggio:

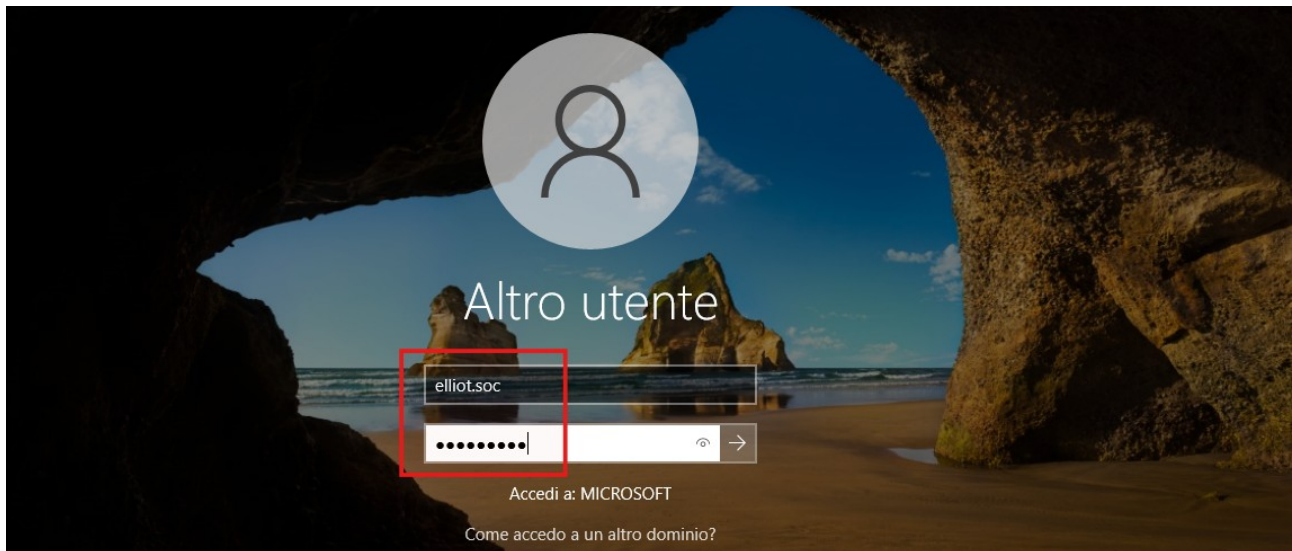
Autorizzazioni insufficienti per accedere a \\microsoftserver\\Accesso limitato

Questo comportamento conferma che **Federica non appartiene al gruppo Cybersecurity-Team** e che i permessi di sicurezza sono configurati correttamente.

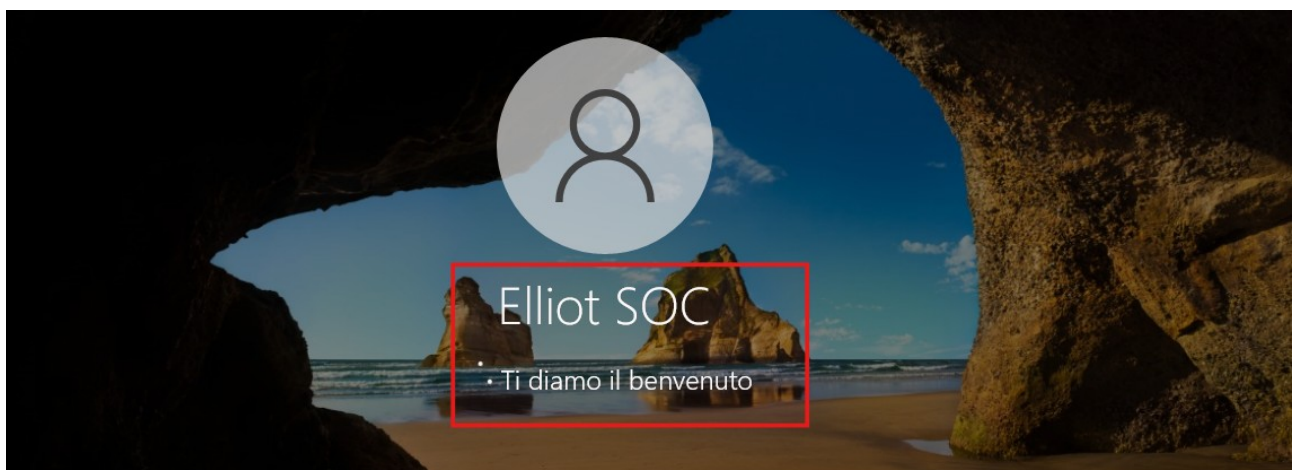


10.1) Test come utente Cybersecurity (Elliot)

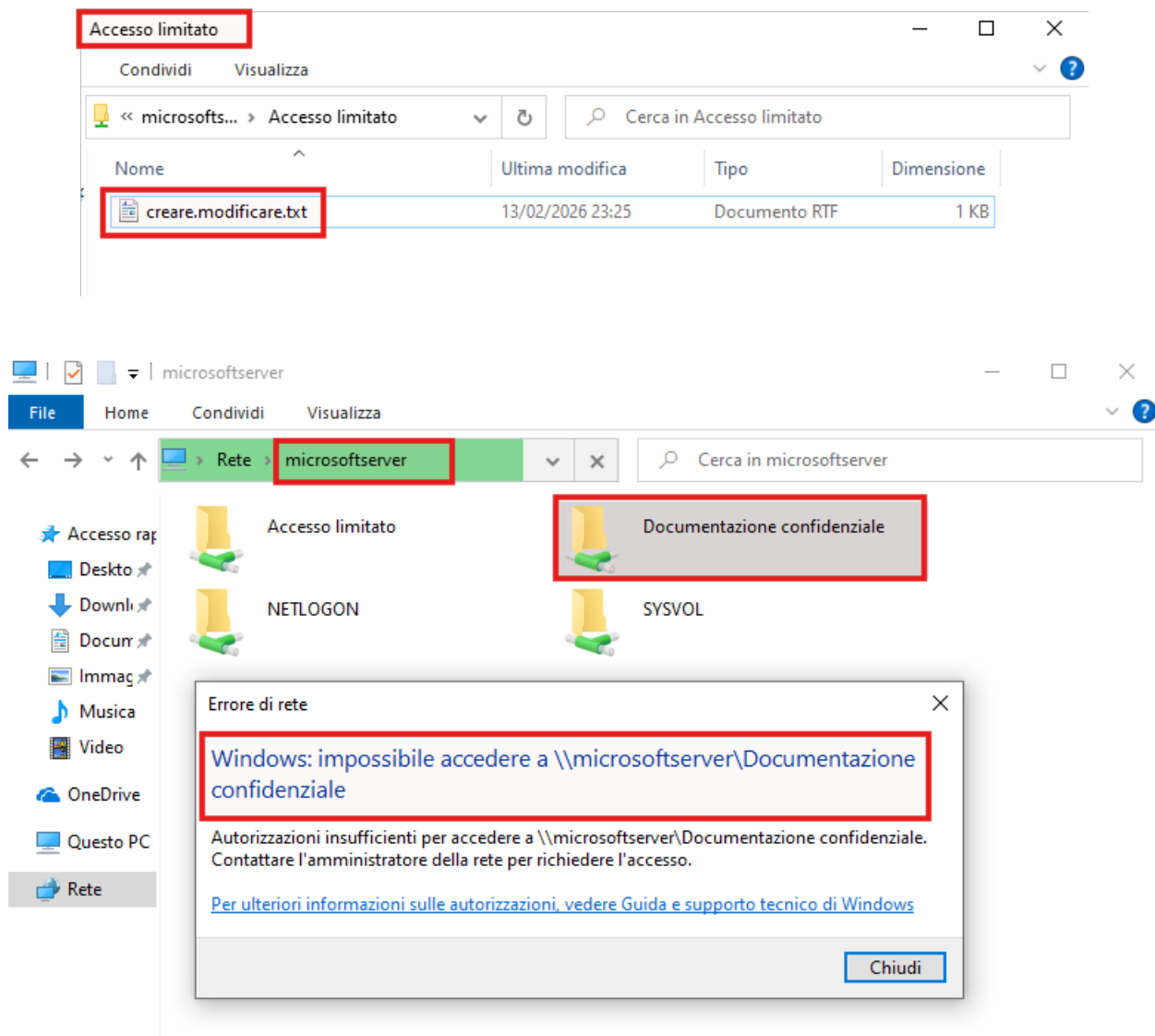
1. Logout, login con **elliott.soc**.
2. Apro **Accesso limitato**:
 - Creo/modifico file → **OK**
3. Provo **Documentazione confidenziale**:
 - Deve risultare **negato**.



Schermata di login di Elliot SOC



Schermata di login di Elliot SOC durante l'accesso



Output

- **Accesso riuscito + creazione file nella cartella Accesso limitato**
- **Messaggio di accesso negato nella cartella Documentazione confidenziale**

Breve documentazione (perché ho scelto questi permessi)

- Ho assegnato i permessi **a gruppi** e non a singoli utenti per semplificare gestione, coerenza e sicurezza.
 - Ho separato i dati per responsabilità: **IT-Admins** gestisce “**Documentazione confidenziale**”, mentre il **Cybersecurity-Team** gestisce “**Accesso limitato**”, applicando il principio del **least privilege**.
-

Conclusioni:

Nel presente progetto ho configurato correttamente un ambiente **Windows Server 2022 con Active Directory**, creando gruppi distinti (**IT-Admins e Cybersecurity-SOC**) e assegnando loro permessi differenziati su risorse condivise.

Ho verificato il corretto funzionamento delle autorizzazioni tramite utenti di prova, dimostrando che **ogni gruppo dispone esclusivamente dei privilegi assegnati, nel rispetto del principio del least privilege.**

Durante la configurazione ho riscontrato inizialmente un **problema di comunicazione tra client e server, risolto correggendo la configurazione della rete interna delle macchine virtuali tramite l'attivazione dell'opzione: cavo virtuale collegato.**

L'esercizio ha permesso di **comprendere l'importanza della gestione centralizzata dei gruppi e dell'assegnazione dei permessi per garantire sicurezza, organizzazione e controllo degli accessi in ambiente Windows Server.**