

Relazione Tecnica Illustrata – Configurazione Dominio Active Directory

Introduzione

Nel presente documento viene illustrato in modo discorsivo e dettagliato il processo di configurazione di un ambiente Windows Server 2022 con dominio Active Directory. Il lavoro ha previsto diverse fasi: la preparazione della rete, la creazione della foresta e del dominio, la definizione di utenti e gruppi, la configurazione di cartelle condivise con relativi permessi, l'applicazione di Group Policy, l'abilitazione dell'accesso remoto e infine la verifica degli accessi e dei permessi da parte di un client unito al dominio. Ogni passaggio è accompagnato da screenshot esplicativi e da una descrizione chiara delle operazioni svolte.

1) Configurazione di Rete: Server e Client

Per consentire la corretta comunicazione tra server e client, è stato necessario configurare indirizzi IP statici. Il server è stato impostato con l'indirizzo 192.168.50.10, gateway 192.168.50.1 e DNS locale. Il client, invece, ha ricevuto l'indirizzo 192.168.50.30 con lo stesso gateway e con il DNS puntato al server. Questa configurazione garantisce che entrambi i dispositivi si trovino sulla stessa rete e che il client possa risolvere correttamente i nomi tramite il DNS del server.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:	192 . 168 . 50 . 10
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 50 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:	127 . 0 . 0 . 1
Alternate DNS server:	. . .

☐ Validate settings upon exit

Advanced...

OK Cancel

Figura 1 – Configurazione IP sul server (192.168.50.10).

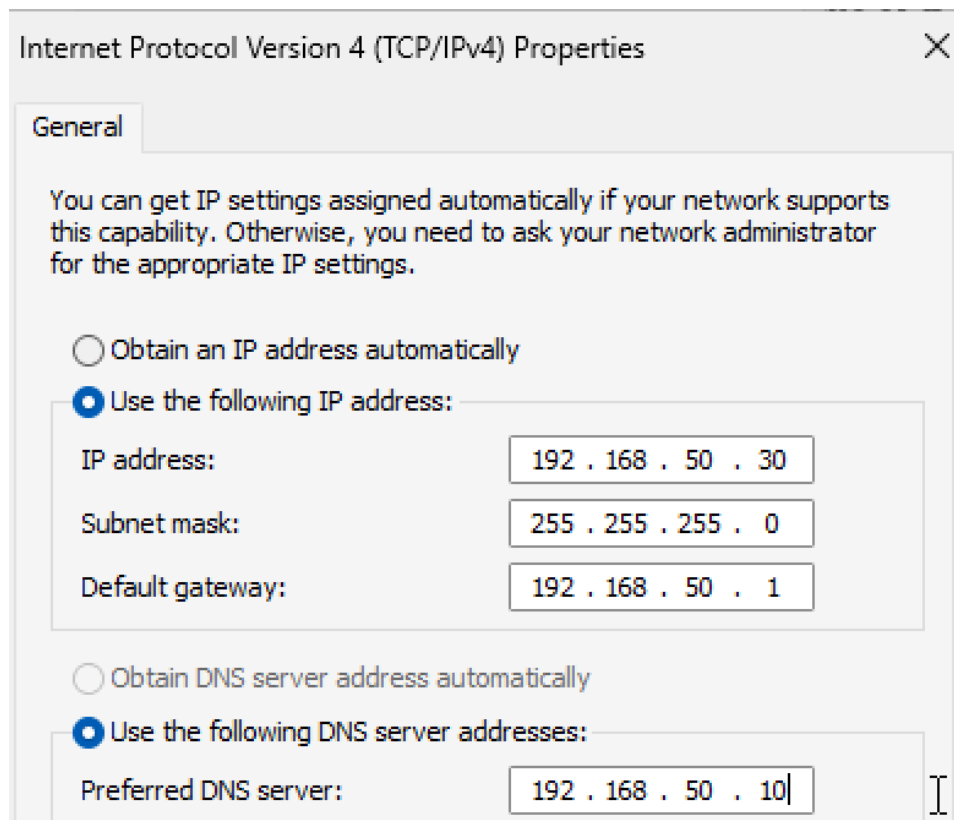


Figura 2 – Configurazione IP sul client (192.168.50.30).

2) Verifica della Connettività

Una volta configurata la rete, ho verificato la comunicazione tra client e server tramite il comando ping. Dal client è stato eseguito un ping verso l'indirizzo IP del server, ottenendo risposte regolari senza perdita di pacchetti. Questo ha confermato che la rete era configurata correttamente e che i due sistemi potevano comunicare senza problemi.

```
PS C:\Users\Pippo> ping 192.168.50.10

Pinging 192.168.50.10 with 32 bytes of data:
Reply from 192.168.50.10: bytes=32 time=4ms TTL=128
Reply from 192.168.50.10: bytes=32 time=1ms TTL=128
Reply from 192.168.50.10: bytes=32 time=1ms TTL=128
Reply from 192.168.50.10: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.50.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figura 3 – Ping riuscito dal client verso il server.

3) Creazione della Foresta e del Dominio

Il passo successivo ha riguardato l'installazione dei ruoli Active Directory Domain Services (AD DS) e DNS sul server. Tramite il wizard di configurazione è stata creata una nuova foresta con dominio radice 'unknown.local'. Al termine della procedura, il server è diventato un Domain Controller, responsabile della gestione centralizzata degli utenti, dei gruppi e delle policy di sicurezza. Questo passaggio è fondamentale per garantire un'infrastruttura di rete organizzata e sicura.

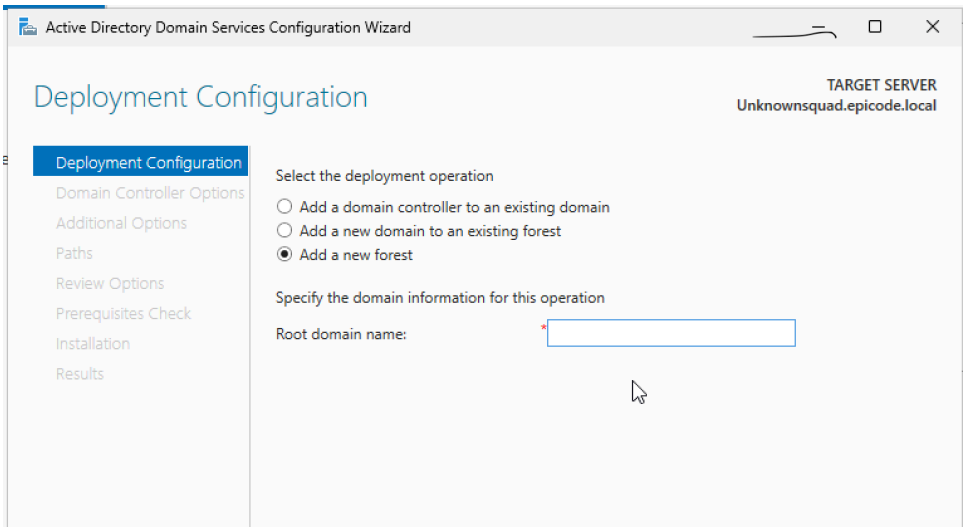


Figura 4 – Wizard di creazione di una nuova foresta.

Computer name	Unknownsquad
Domain	unknown.local
Microsoft Defender Firewall	Public: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet	192.168.50.10
Azure Arc Management	Disabled
Remote SSH Access	Disabled

Figura 5 – Configurazione dominio 'unknown.local'.

Select server roles

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more roles to install on the s

Roles


- ☐ Active Directory Certificate Service
- ☒ Active Directory Domain Services (
- ☐ Active Directory Federation Service
- ☐ Active Directory Lightweight Direc
- ☐ Active Directory Rights Manageme
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☒ DNS Server (Installed)
- ☐ Fax Server
- ▷ ☒ File and Storage Services (2 of 12 i
- ☐ Host Guardian Service

Figura 6 – Riepilogo installazione AD DS e DNS.

4) Creazione degli Utenti

Una volta creato il dominio, ho provveduto alla definizione degli utenti che vi appartengono. Sono stati creati diversi account, tra cui 'Pippo', 'Al' e 'Johnny', collocati nelle rispettive Unità Organizzative. Per ciascun utente è stata impostata una password iniziale, con l'obbligo di modificarla al primo accesso. Questa procedura consente di aumentare la sicurezza, garantendo che ciascun utente scelga una password personale.

New Object - User ✕

 Create in: unknown.local/Amministrazione

First name: Initials:

Last name:


Full name:

User logon name: ▼


User logon name (pre-Windows 2000):

Figura 7 – Creazione utente 'Pippo' (OU Amministrazione).

New Object - User ✕

 Create in: unknown.local/Amministrazione

Password:

Confirm password: 

☒ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

Figura 8 – Impostazione della password con richiesta di cambio al primo accesso.

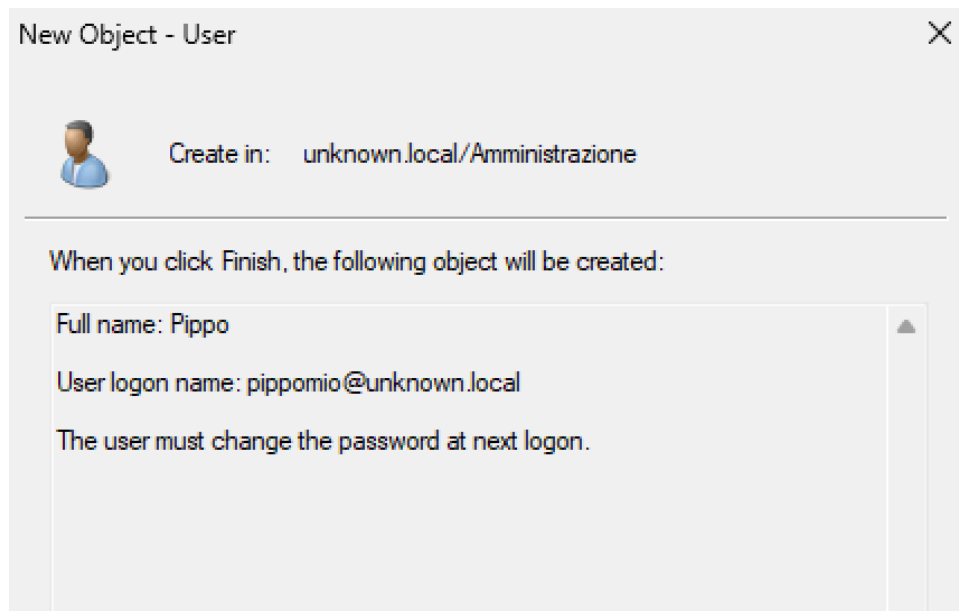


Figura 9 – Conferma della creazione dell'utente 'Pippo'.

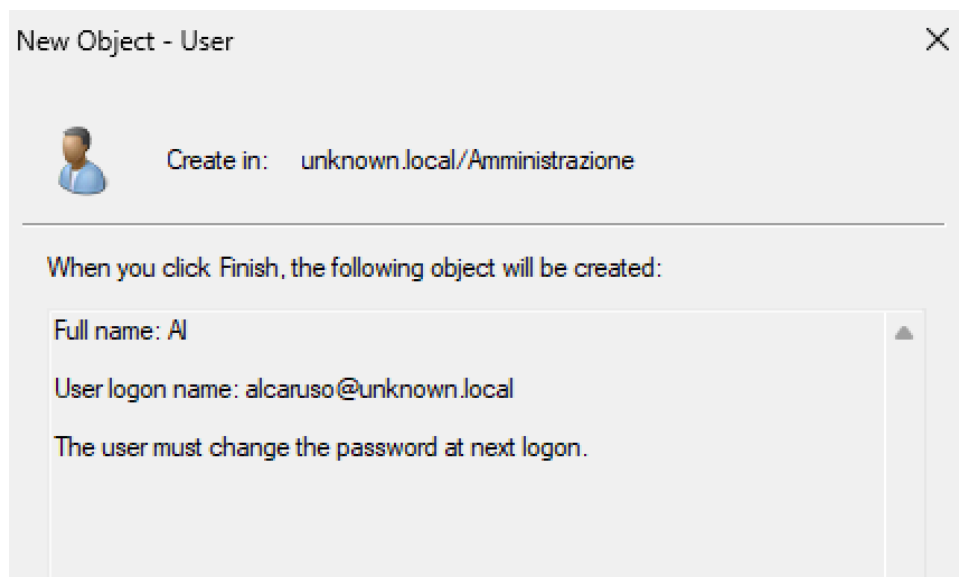
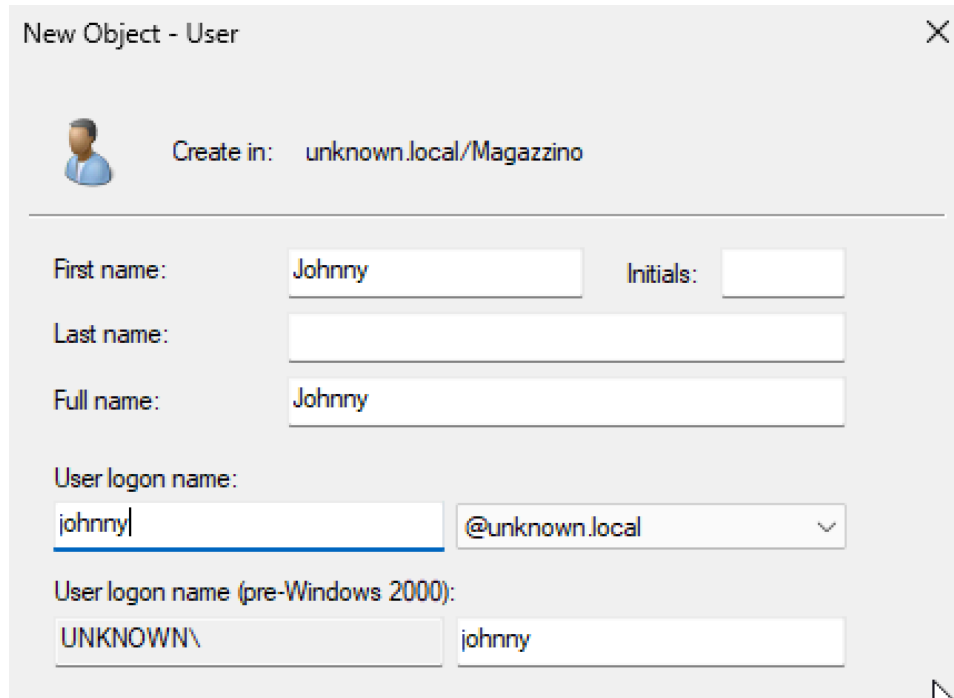


Figura 10 – Creazione dell'utente 'Al'.



New Object - User

Create in: unknown.local/Magazzino

First name: Johnny Initials:

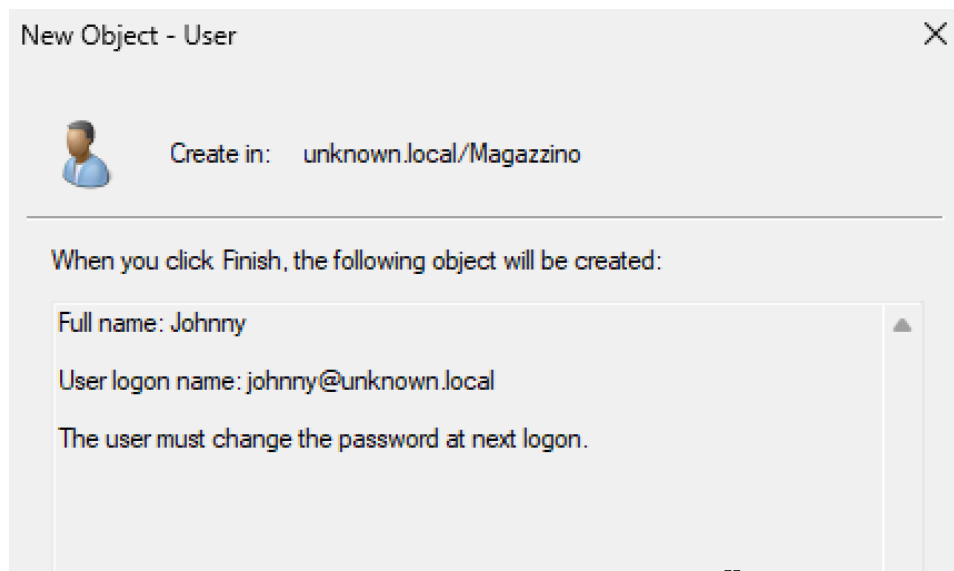
Last name:

Full name: Johnny

User logon name: johnny| @unknown.local

User logon name (pre-Windows 2000): UNKNOWN\ johnny

Figura 11 – Creazione utente 'Johnny' (OU Magazzino).



New Object - User

Create in: unknown.local/Magazzino

When you click Finish, the following object will be created:

Full name: Johnny

User logon name: johnny@unknown.local


The user must change the password at next logon.

Figura 12 – Conferma della creazione dell'utente 'Johnny'.

5) Creazione dei Gruppi

Per una gestione efficiente dei permessi, gli utenti sono stati organizzati in gruppi di sicurezza. Sono stati creati, ad esempio, i gruppi 'I corti' e 'Gastani Frinzi', che raggruppano utenti con esigenze simili. In questo modo è possibile assegnare i permessi a livello di gruppo, semplificando notevolmente la gestione e riducendo il rischio di errori.

New Object - Group ✕

 Create in: unknown.local/Amministrazione

Group name:

Group name (pre-Windows 2000):

Group scope

☐ Domain local

☒ Global

☐ Universal

Group type

☒ Security

☐ Distribution





Figura 13 – Creazione gruppo 'I corti'.

New Object - Group ✕

 Create in: unknown.local/Magazzino

Group name:

Group name (pre-Windows 2000):

Group scope

☐ Domain local

☒ Global

☐ Universal

Group type

☒ Security

☐ Distribution




Figura 14 – Creazione gruppo 'Gastani Frinzi'.

6) Cartelle Condivise e Permessi

Per permettere la condivisione di file all'interno dei reparti, sono state create cartelle condivise sul server. A ciascuna cartella sono stati assegnati permessi specifici in base al gruppo di appartenenza. Ad esempio, la cartella '3 Uomini e una gamba' è stata resa accessibile esclusivamente al gruppo 'I corti', mentre 'Chiedimi se sono felice' è stata riservata al gruppo 'Gastani Frinzi'. Questa organizzazione assicura che ogni utente possa accedere solo alle risorse necessarie.

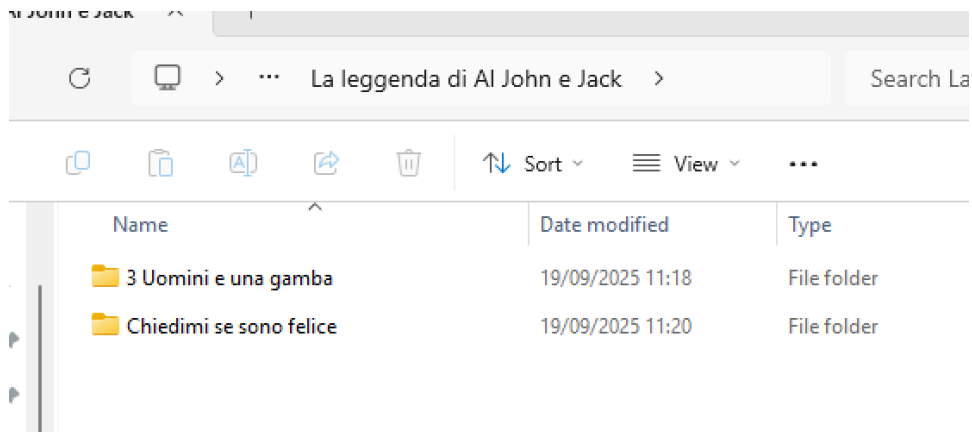


Figura 15 – Creazione delle cartelle condivise.

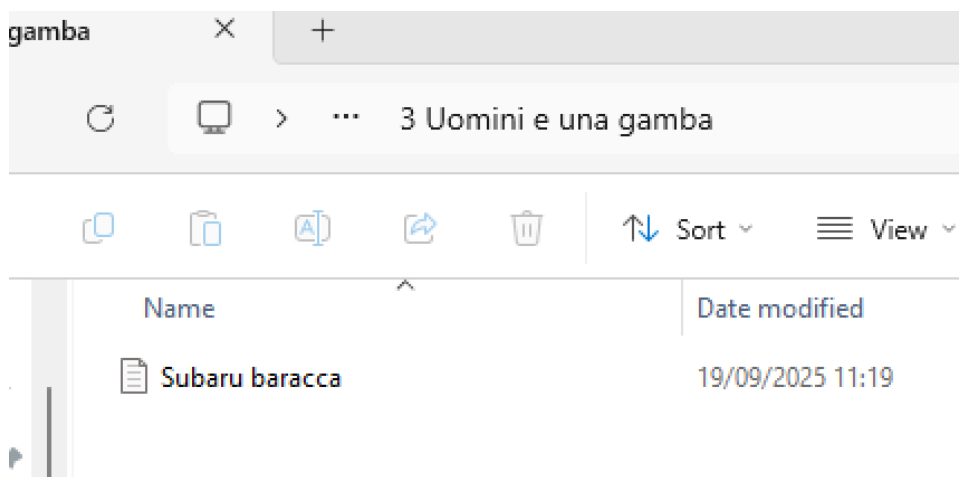


Figura 16 – Contenuto cartella '3 Uomini e una gamba'.

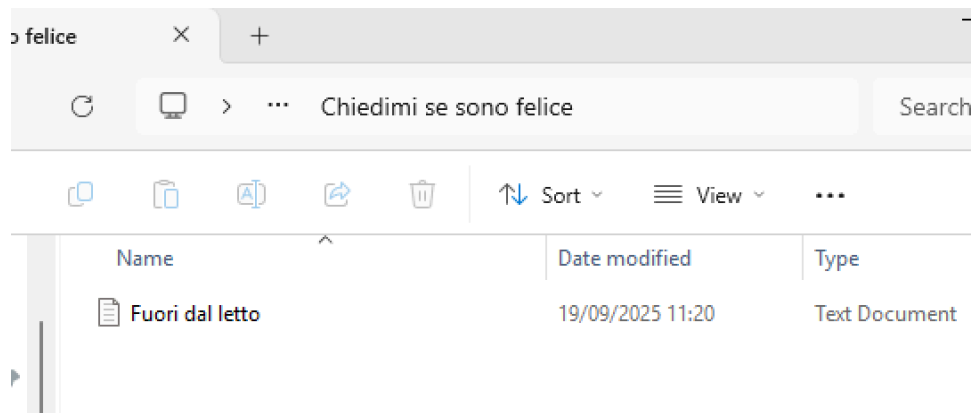


Figura 17 – Contenuto cartella 'Chiedimi se sono felice'.

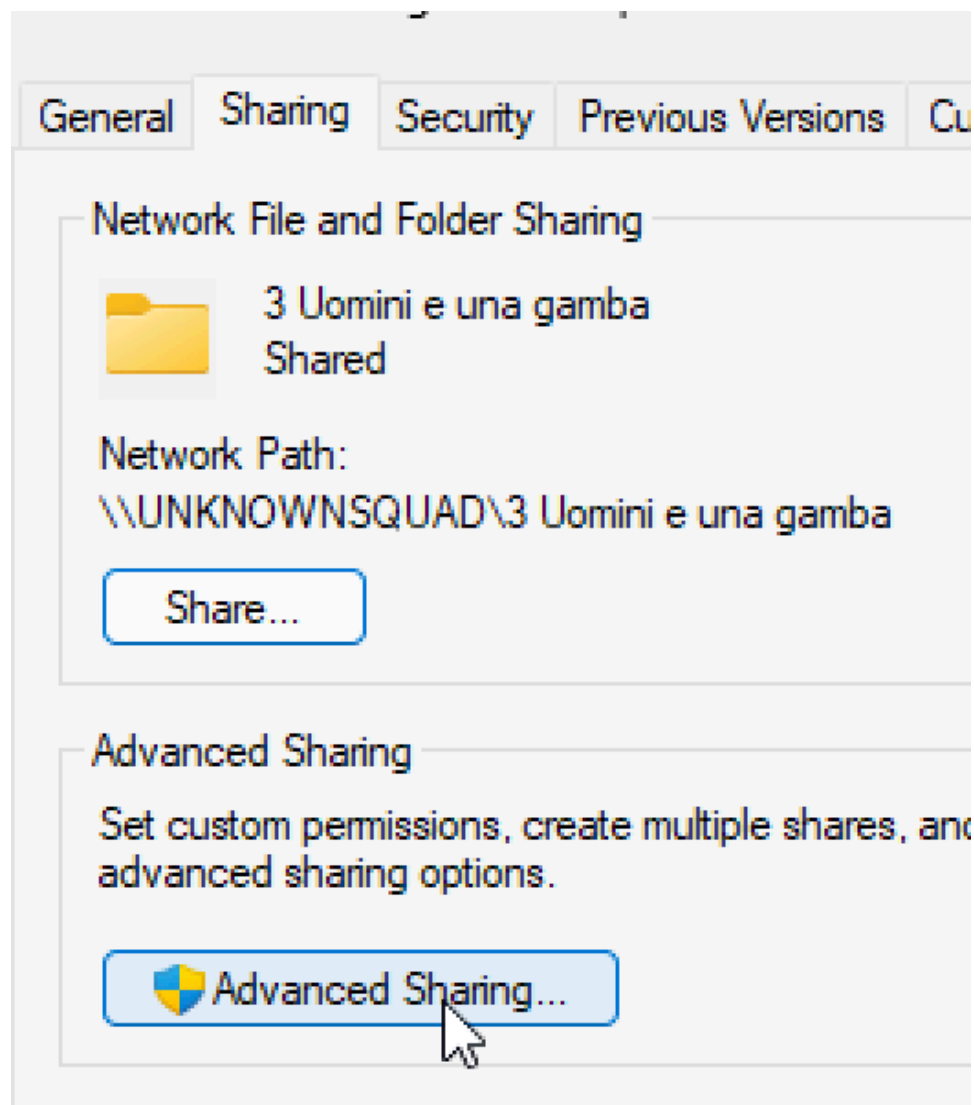


Figura 18 – Condivisione '3 Uomini e una gamba'.

Advanced Sharing

☒ Share this folder

Settings

Share name:

3 Uomini e una gamba

Add Remove

Limit the number of simultaneous users to: 1

Comments:

Permissions Caching

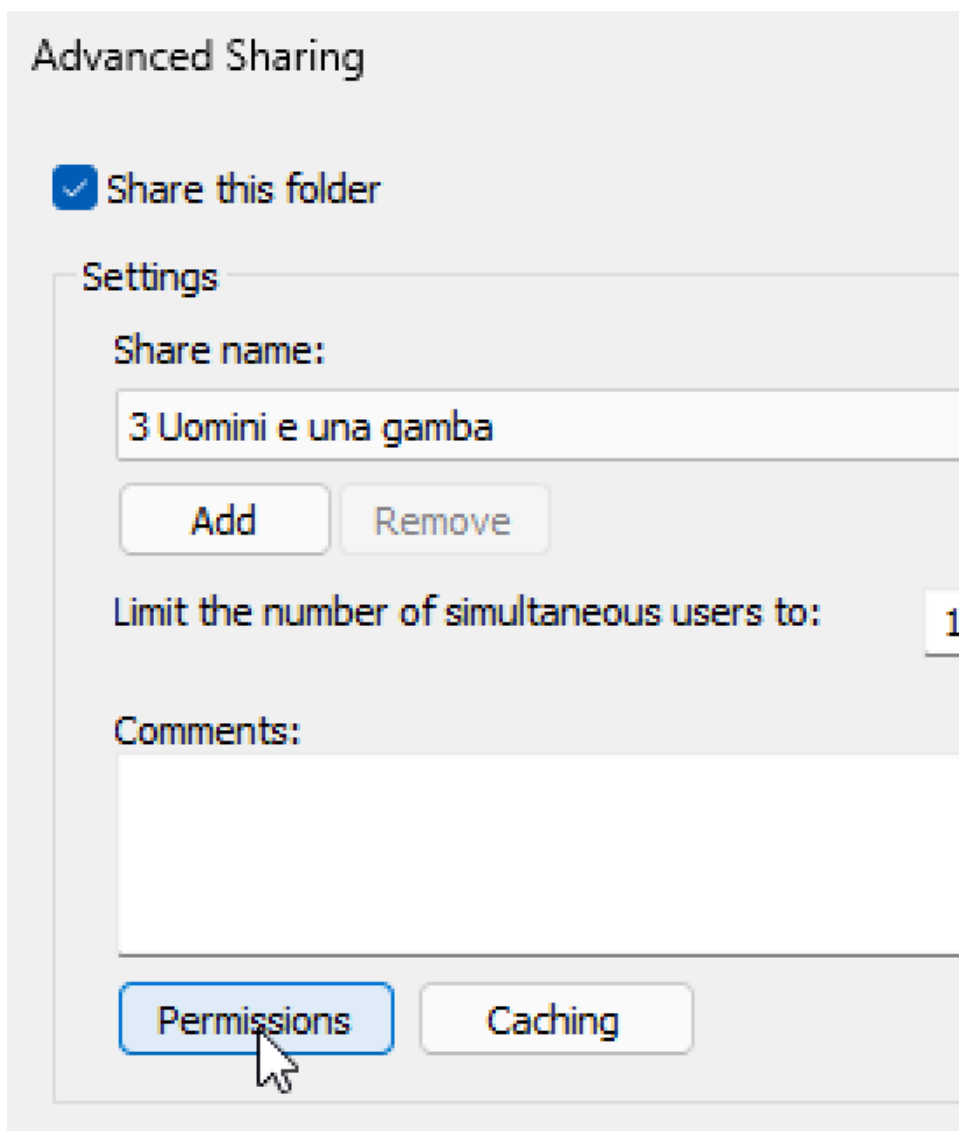


Figura 19 – Abilitazione della condivisione avanzata.

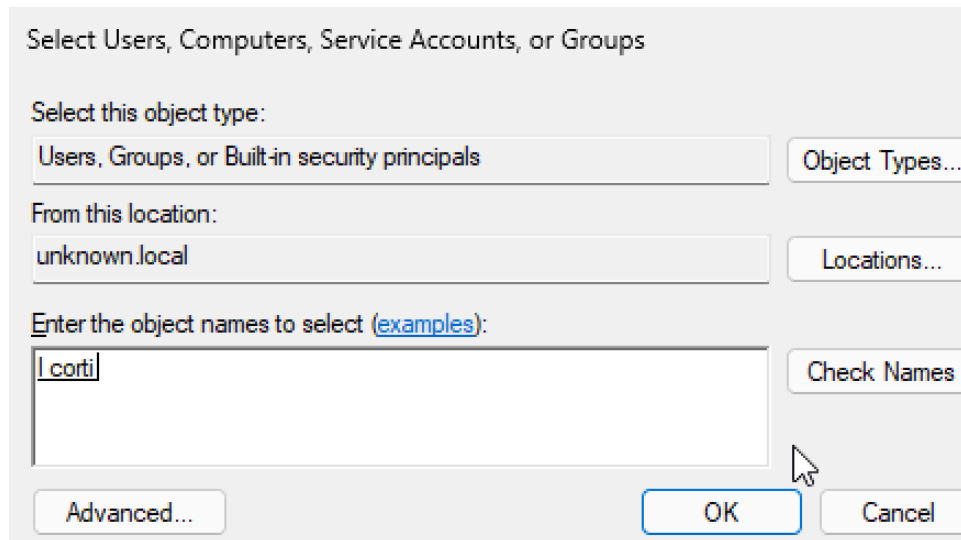


Figura 20 – Permessi assegnati al gruppo 'I corti'.

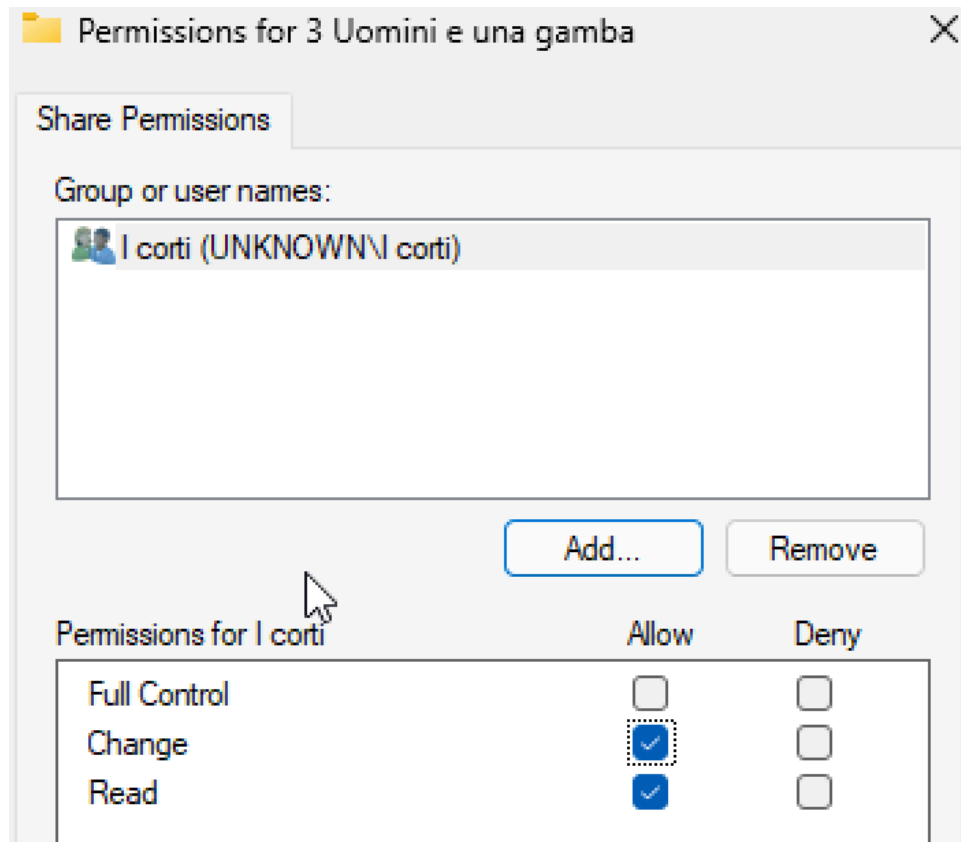


Figura 21 – Dettaglio dei permessi di lettura/scrittura.

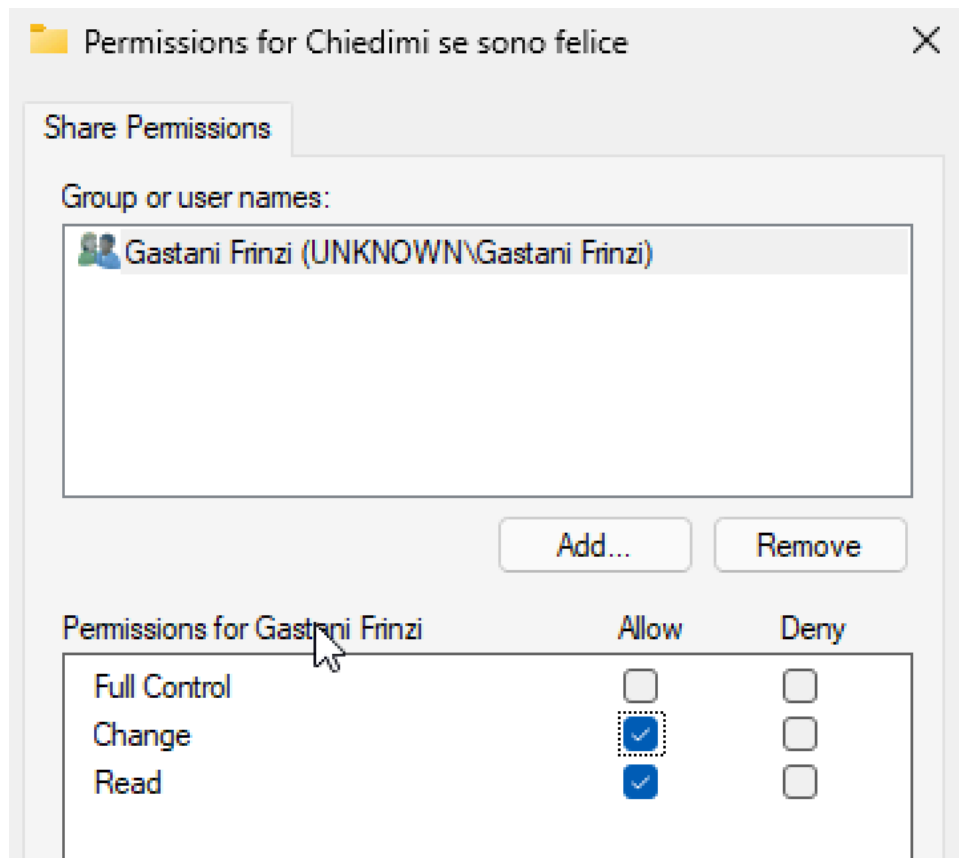


Figura 22 – Permessi assegnati al gruppo 'Gastani Frinzi'.

7) Configurazione delle Group Policy

Per applicare regole e restrizioni specifiche ai vari reparti, sono state utilizzate le Group Policy. Attraverso la console di gestione, sono state definite policy differenziate per le OU 'Amministrazione' e 'Magazzino'. In questo modo, ad esempio, è possibile concedere determinate autorizzazioni agli utenti dell'amministrazione e limitare alcune funzionalità per gli utenti del magazzino.

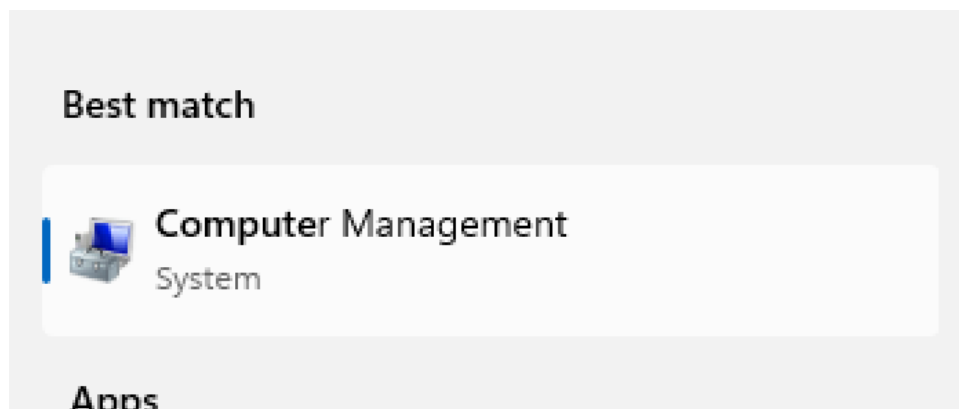


Figura 23 – Apertura della console di amministrazione.

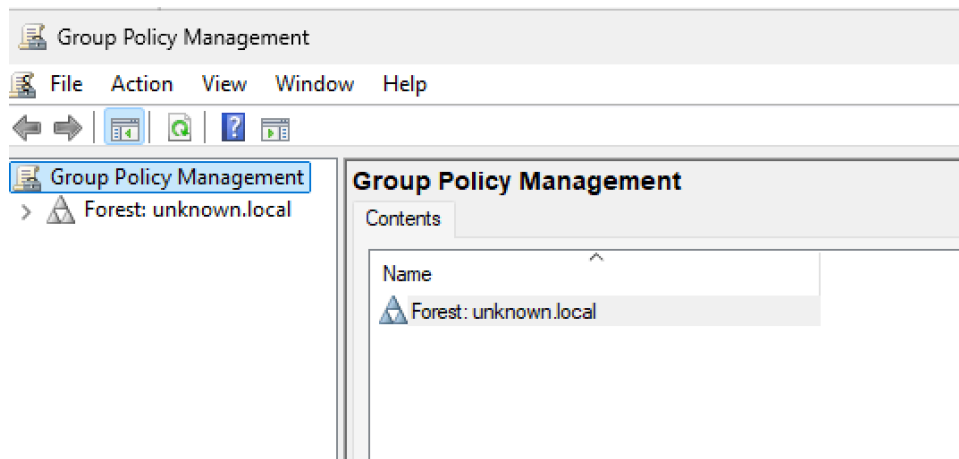


Figura 24 – Console Group Policy Management.

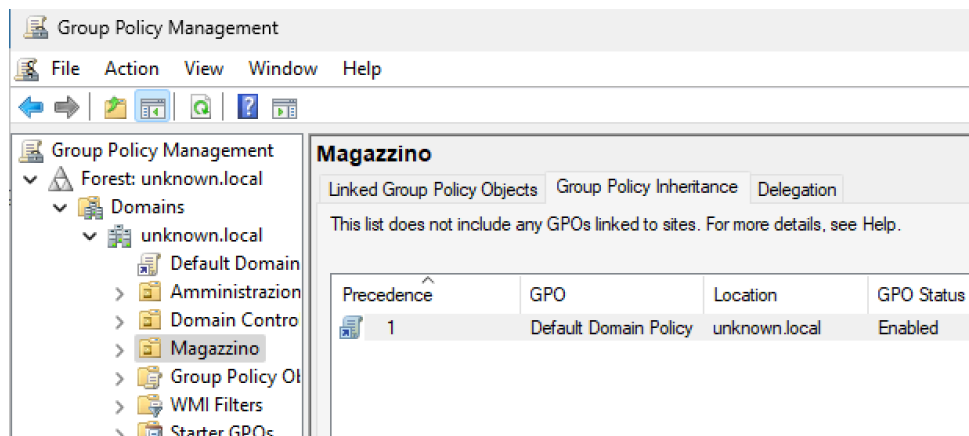


Figura 25 – Policy applicate all'OU Magazzino.

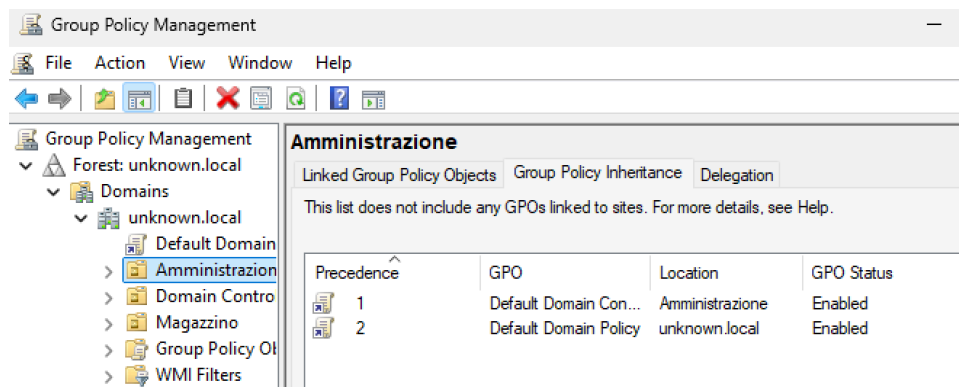


Figura 26 – Policy applicate all'OU Amministrazione.

8) Abilitazione dell'Accesso Remoto (RDP)

Un ulteriore passaggio ha riguardato la configurazione dell'accesso remoto tramite Remote Desktop. È stata abilitata l'opzione sul server e il gruppo 'I corti' è stato autorizzato ad accedere tramite RDP. Questa configurazione è stata completata anche attraverso le Local Security Policy, che hanno confermato il diritto di accesso al servizio Remote Desktop per gli utenti del gruppo. Dal lato client, è stata avviata una connessione remota verso il server e sono state inserite le credenziali di un utente di dominio, verificando il corretto funzionamento.

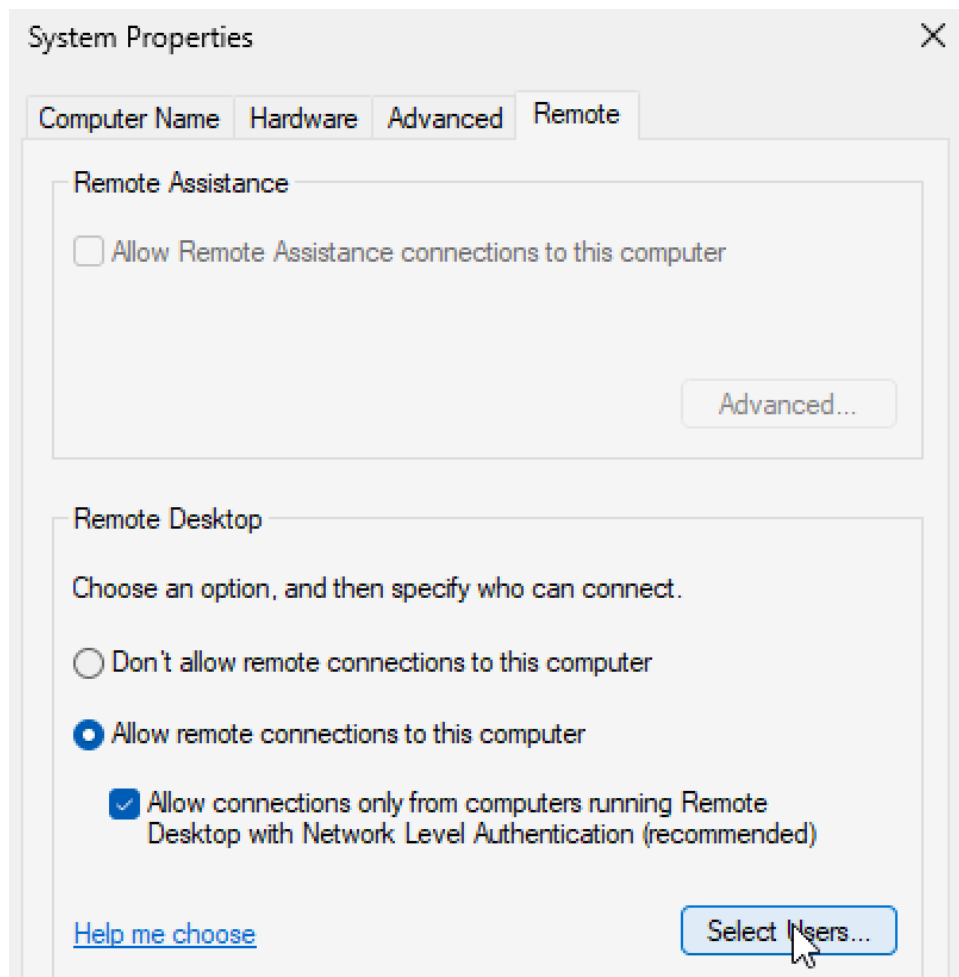


Figura 27 – Abilitazione Remote Desktop sul server.

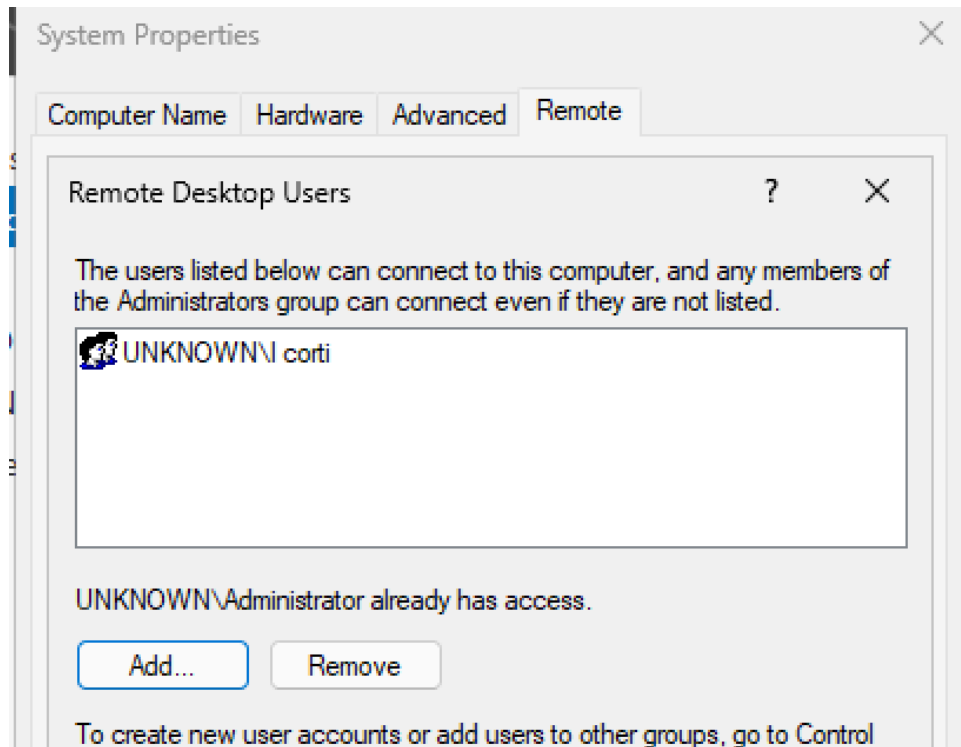


Figura 28 – Aggiunta del gruppo 'I corti' tra i Remote Desktop Users.

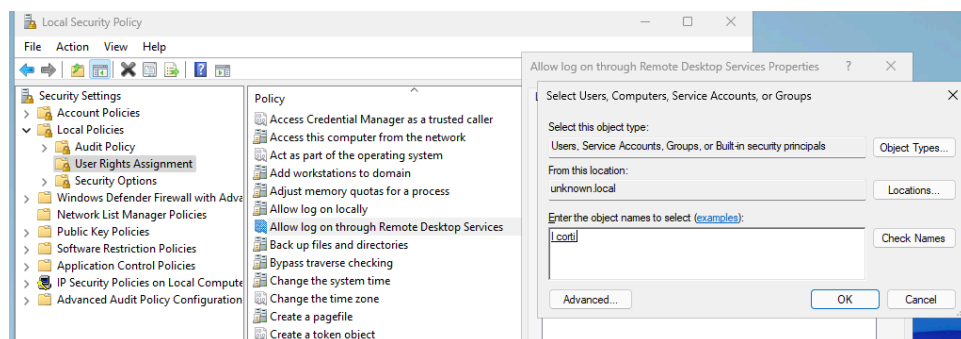


Figura 29 – Local Security Policy – autorizzazione RDP per il gruppo 'I corti'.

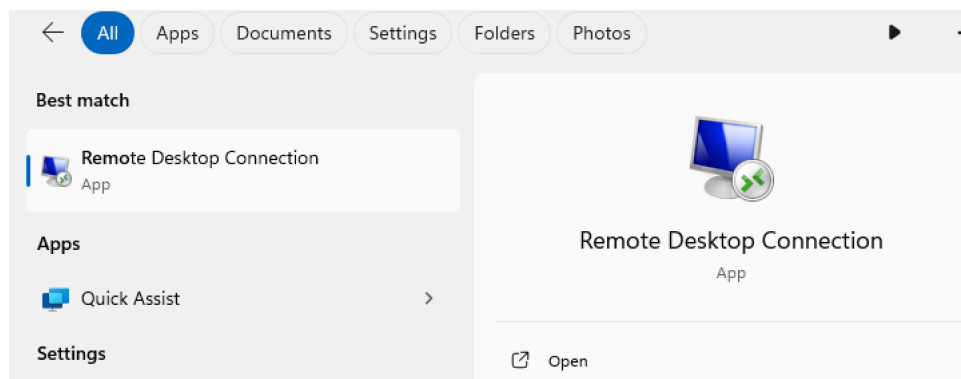


Figura 30 – Avvio connessione RDP dal client.

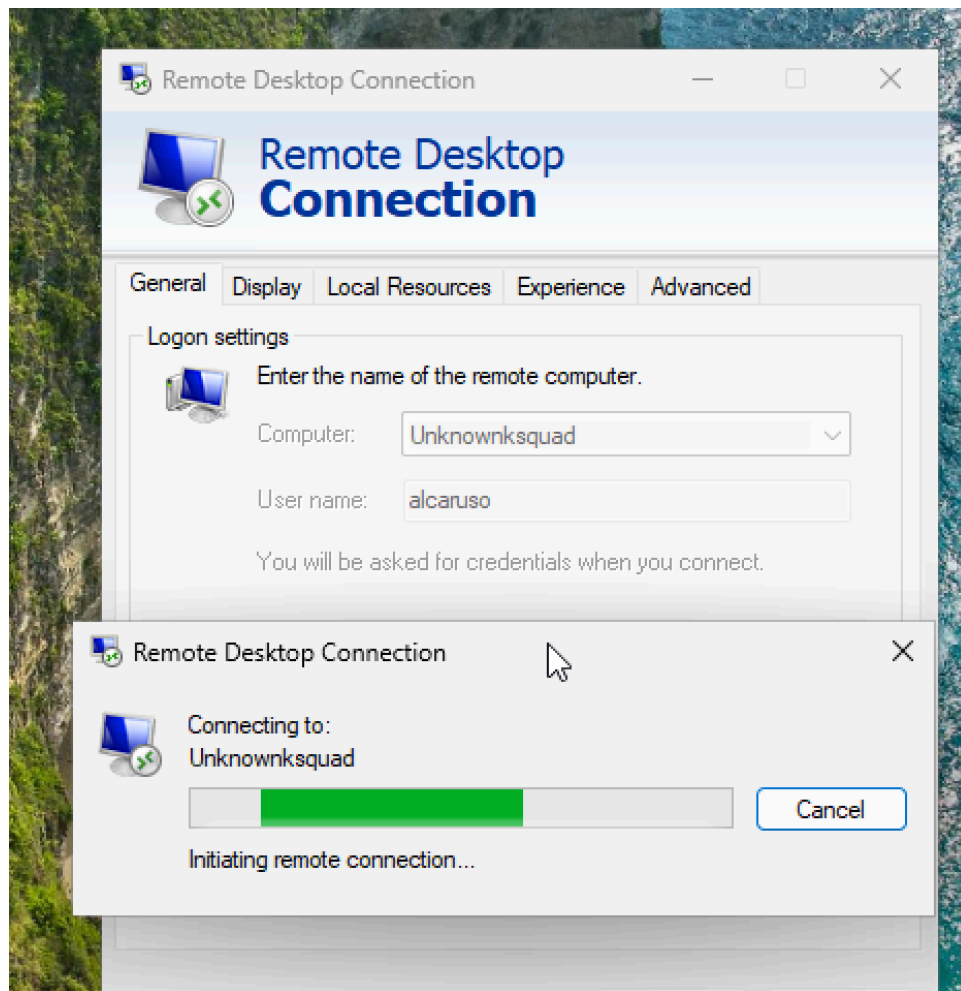


Figura 31 – Connessione remota verso il server 'Unknownsquad'.

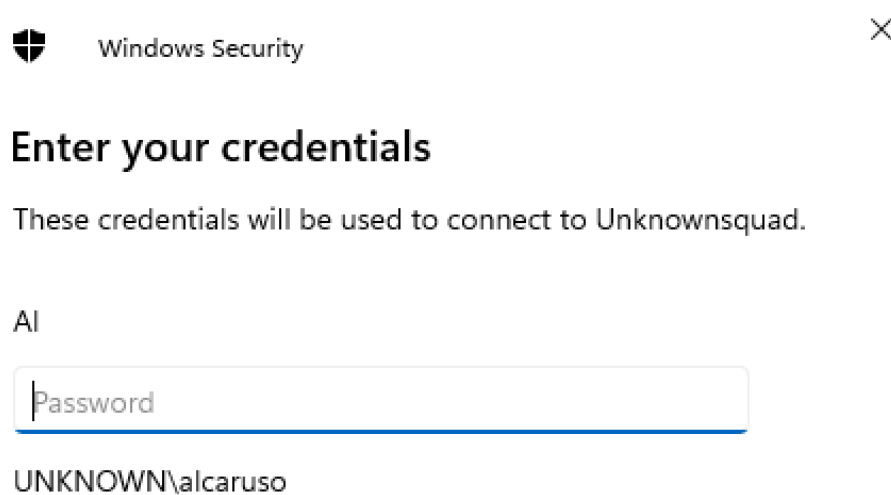


Figura 32 – Inserimento delle credenziali dell'utente di dominio.

9) Accesso al Server dal Client e Verifica dei Permessi

Infine, il client è stato unito al dominio e sono stati effettuati test di accesso alle cartelle condivise e alle applicazioni. Con l'utente 'alcaruso' è stato possibile verificare che i permessi impostati funzionano correttamente: l'utente poteva accedere e modificare i file nelle cartelle autorizzate, mentre l'accesso veniva negato per le cartelle non pertinenti al suo gruppo di appartenenza. Lo stesso principio è stato applicato alle applicazioni, garantendo che solo gli utenti autorizzati potessero eseguirle.

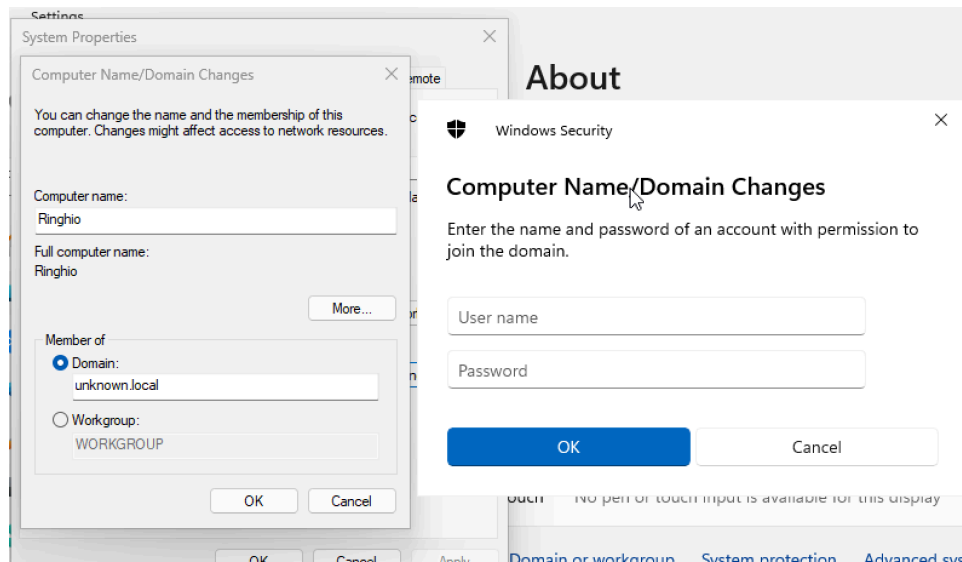


Figura 33 – Join del client al dominio con credenziali amministrative.

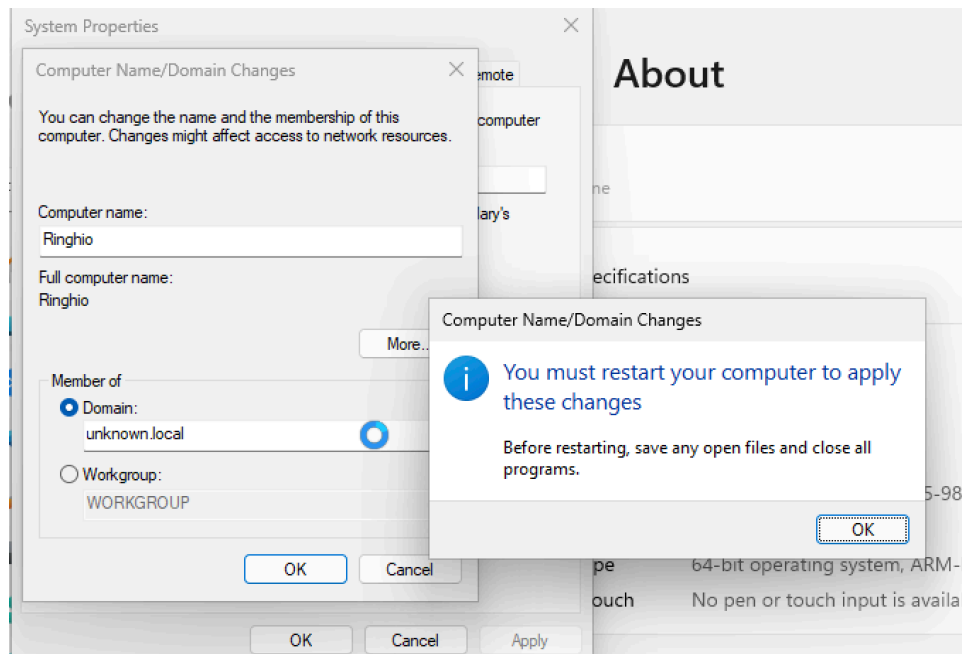


Figura 34 – Richiesta riavvio dopo il join al dominio.

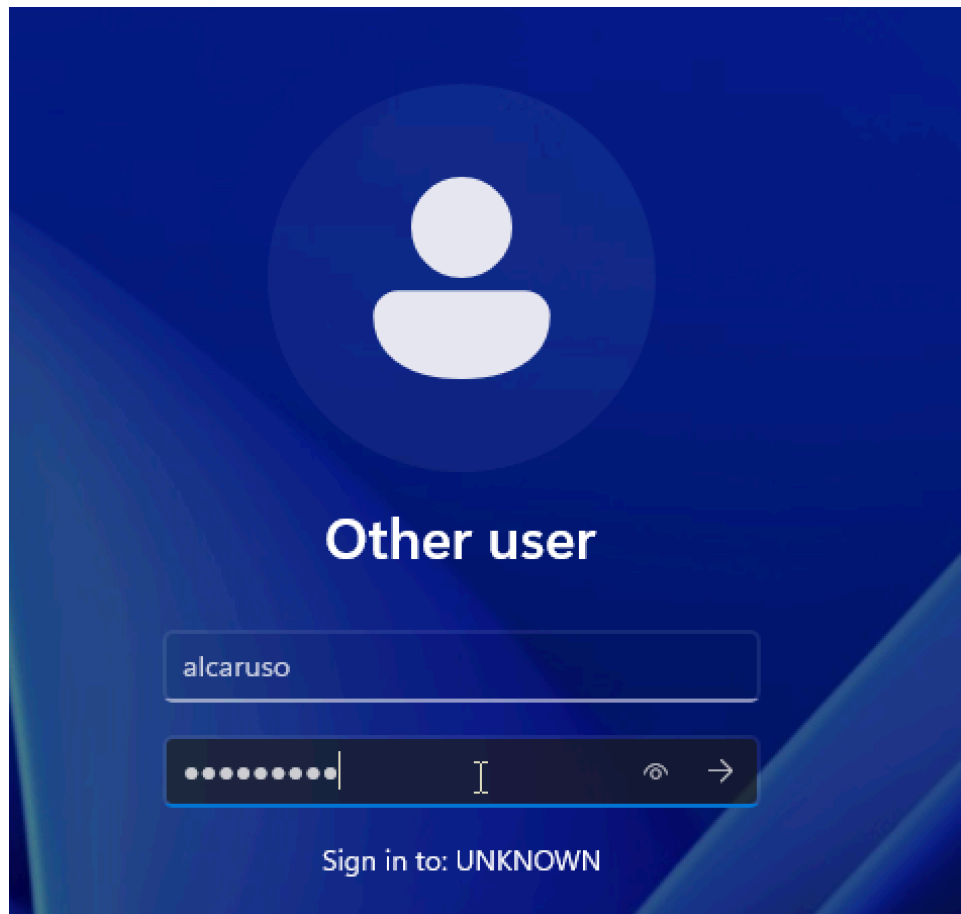


Figura 35 – Login del client con l'utente di dominio 'alcaruso'.

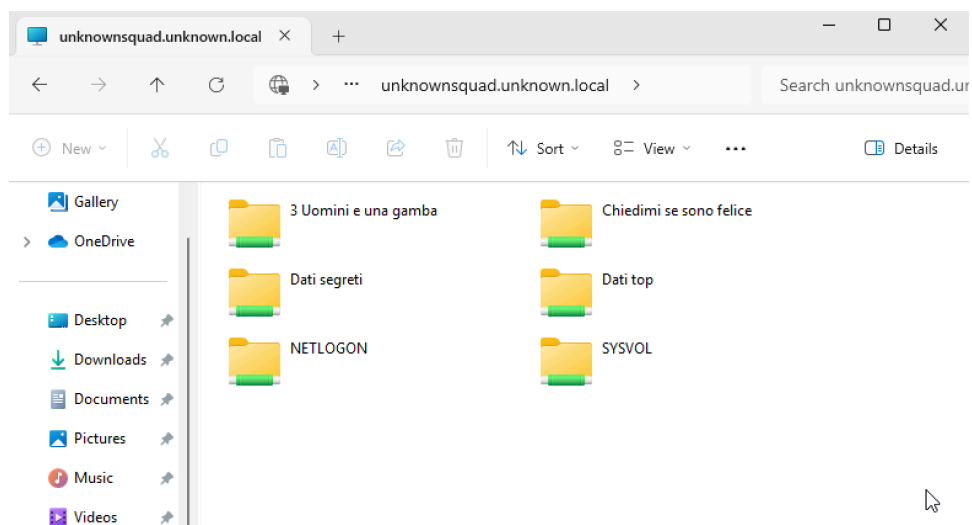


Figura 36 – Visualizzazione delle share disponibili dal client.

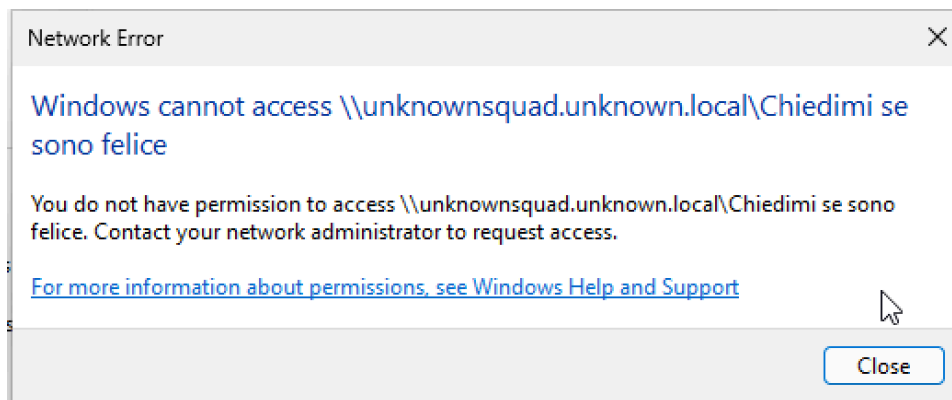


Figura 37 – Accesso negato a cartella non autorizzata.

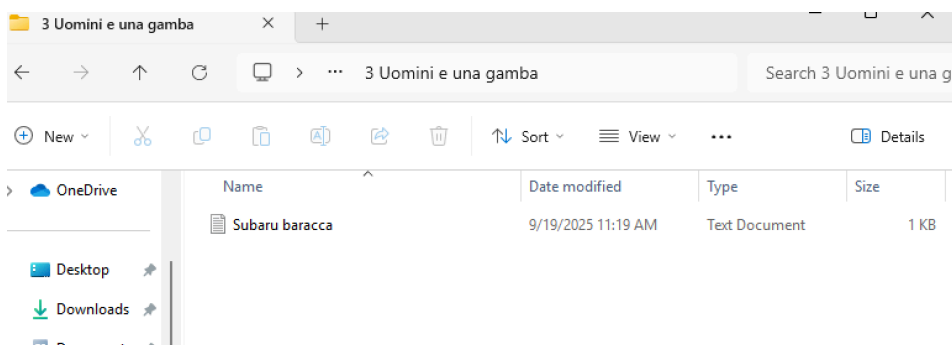


Figura 38 – Accesso a cartella autorizzata.

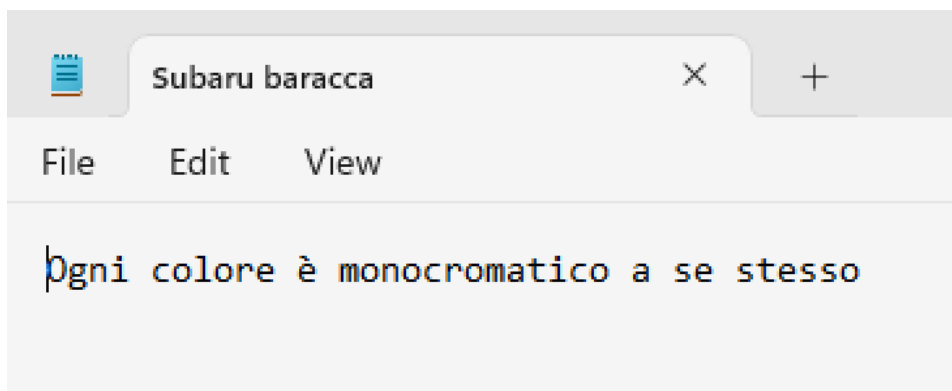


Figura 39 – Modifica di un file condiviso dal client.

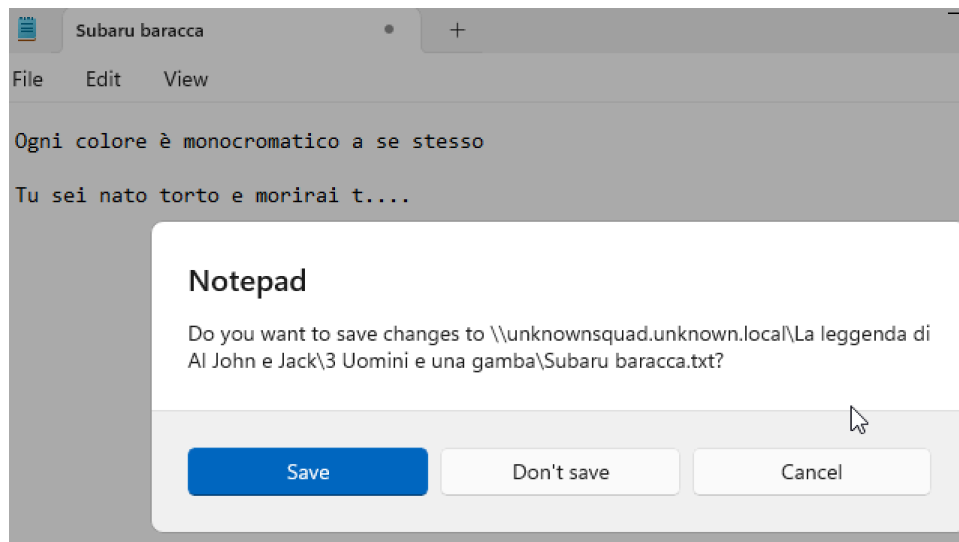


Figura 40 – Salvataggio delle modifiche al file condiviso.

Conclusioni

La configurazione realizzata ha permesso di implementare un'infrastruttura di dominio Active Directory completa e funzionale. Gli utenti sono stati organizzati in gruppi, con permessi precisi su cartelle e applicazioni. Le Group Policy hanno consentito di applicare regole differenziate per reparto, mentre l'accesso remoto ha reso possibile l'amministrazione e il lavoro a distanza. I test finali dal client hanno confermato la coerenza delle impostazioni e la sicurezza della configurazione.