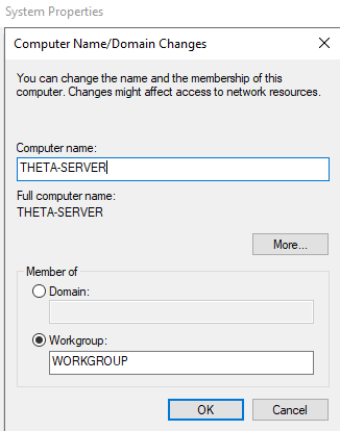
Progetto S10-L5

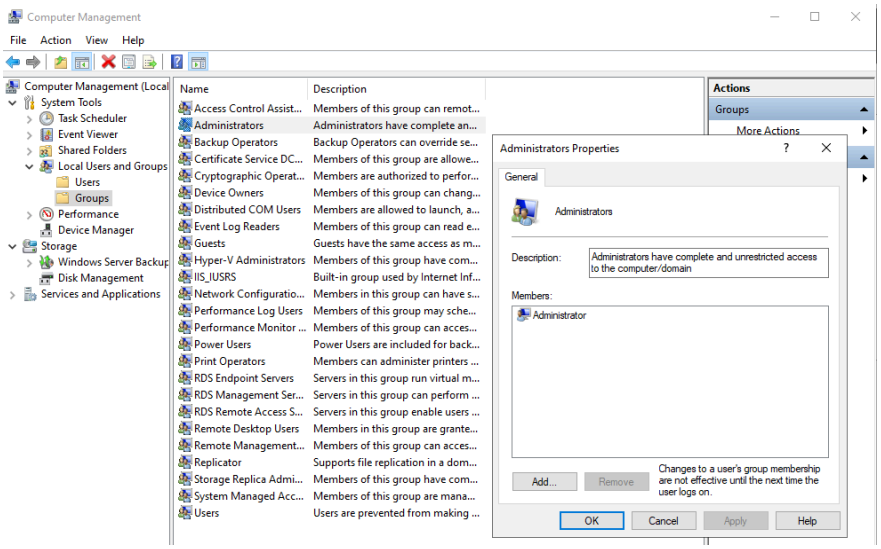
- **Obiettivi**
    1. Creare un ambiente Windows Server 2022
    2. Creare dei gruppi tramite Active Directory immaginando uno scenario reale.
    3. Assegnare permessi specifici.
    4. Verificarne il funzionamento.

- **Progetto**
  Lo scenario da me ideato prende in esame un'azienda di nome Theta, avente un server THETA-SERVER con dominio **theta.local**.
  Si tratta di un'azienda avente due sedi: una a Roma e una a Milano. In ogni sede sono presenti due differenti reparti: Vendite e Finanza.
  Ogni reparto ha accesso a file diversi, non accessibili dagli altri reparti.
  Inoltre la divisione in filiali è fondamentale in quanto THETA utilizza due differenti gestionali, uno per la sede di Roma, al quale la sede di Milano non ha accesso, e uno per la sede di Milano.
  Questi gestionali, in questo caso, saranno simulati da semplici applicazioni.exe: applicazione **calcolatrice** per il gestionale di Milano; applicazione **notepad** per il gestionale di Roma.
  Infine, a parte, abbiamo il reparto IT, il quale ha permessi speciali: accesso a tutte le risorse, modifica file di sistema e accesso remoto al server.

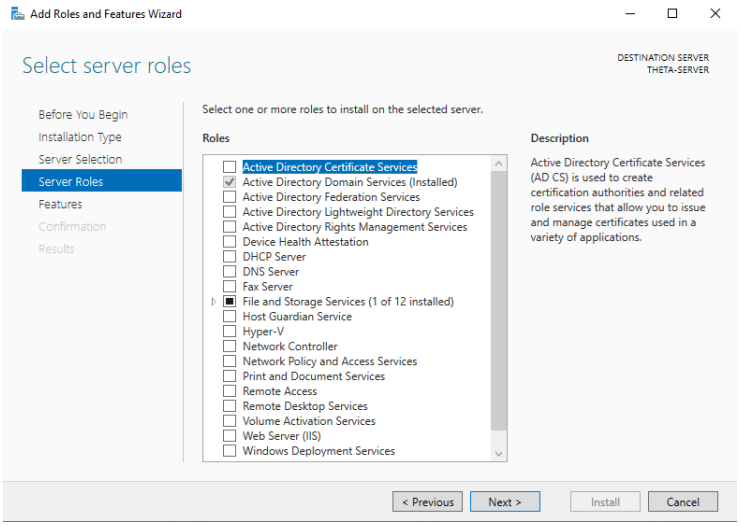
- **Descrizione**
  Per prima cosa ho avviato la macchina Windows Server e ho cambiato il suo nome in THETA-SERVER.



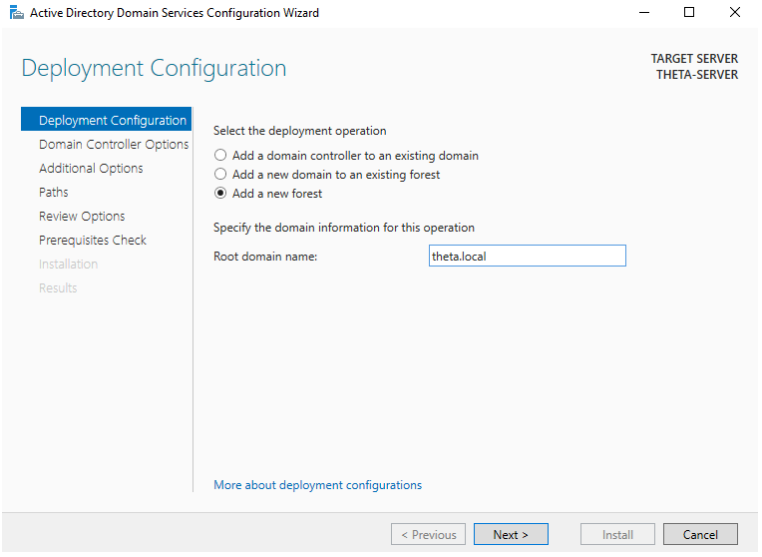
  Ho verificato che il mio utente "**Administrator**" avesse permessi da amministratore, verificando la sua presenza all'interno del gruppo "**Administrators**" tramite il servizio "**Computer Management**".

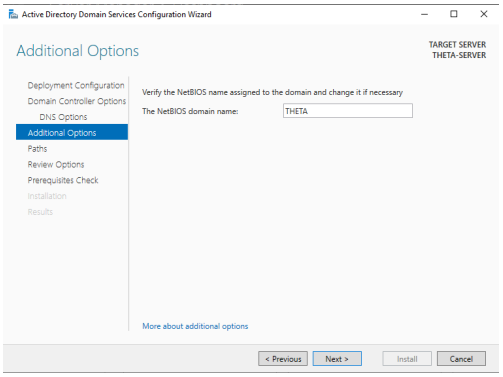


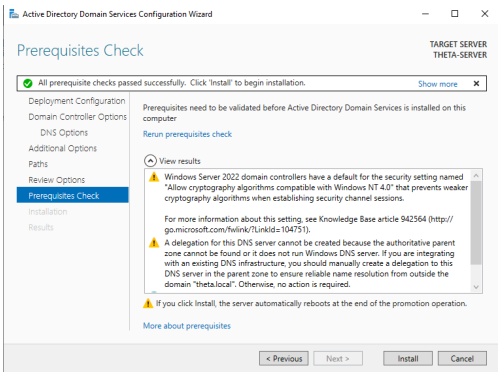
Mi sono recato sul **Server Manager** e ho installato **Active Directory**.



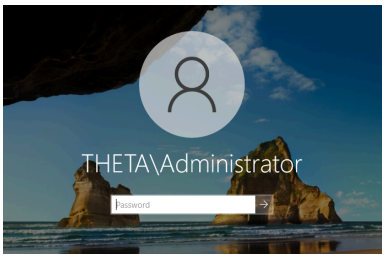
Tramite la sezione “promote this server to a domain controller” ho configurato una nuova foresta con dominio “**theta.local**”

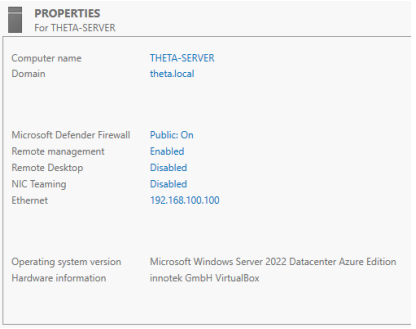






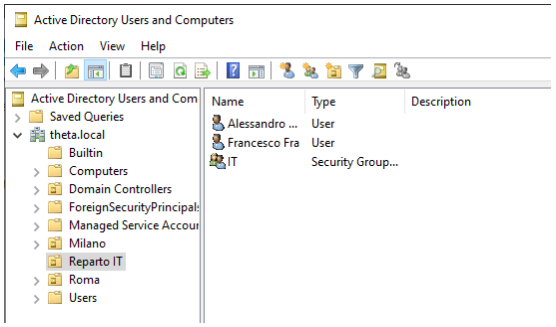
Dopo il riavvio, la schermata appare in questo modo. Abbiamo il nostro server THETA.

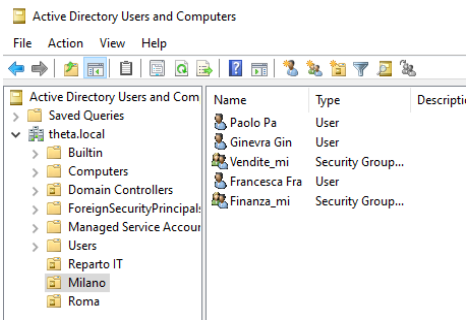


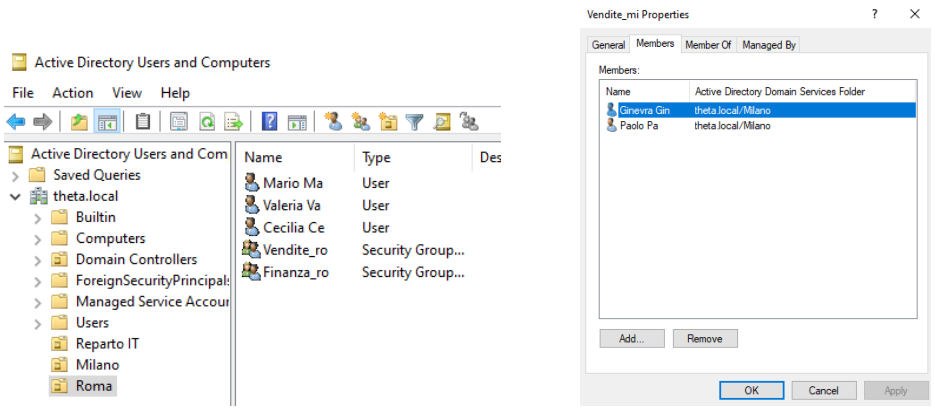


Ho aperto la sezione di Active Directory per la gestione di utenti e gruppi e creato tre **OU** con relativi gruppi e membri:

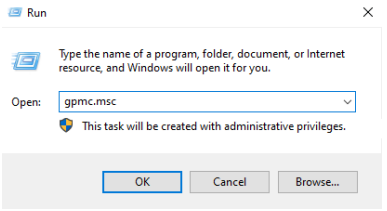
1. **Reparto IT**
    - **Gruppo IT**
        - **Francesco - Alessandro**
2. **Roma**
    - **Vendite_ro**
        - **Mario - Valeria**
    - **Finanza_ro**
        - **Cecilia**
3. **Milano**
    - **Vendite_mi**
        - **Ginevra - Paolo**
    - **Finanza_mi**
        - **Francesca**



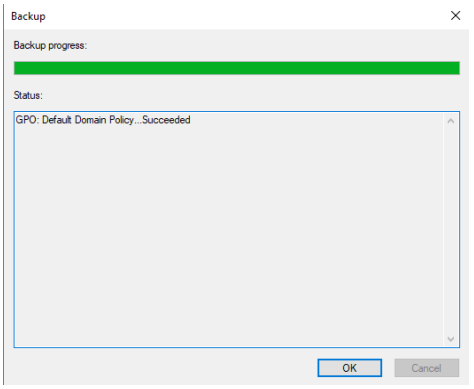




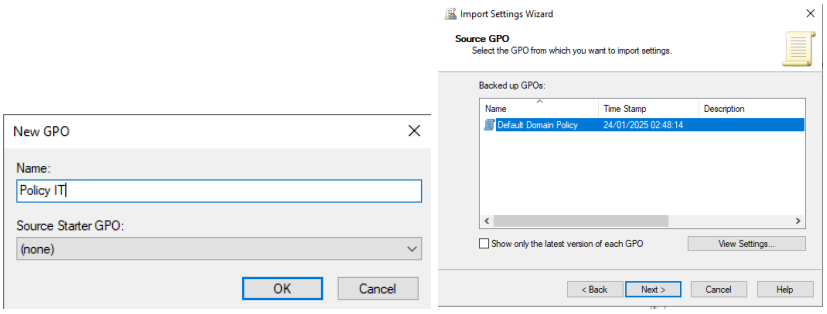
Per impostare delle regole precise per ogni OU, sono andato a lavorare direttamente sulle policy.
Con il comando **gpmc.msc** ho aperto il gestore Policy.



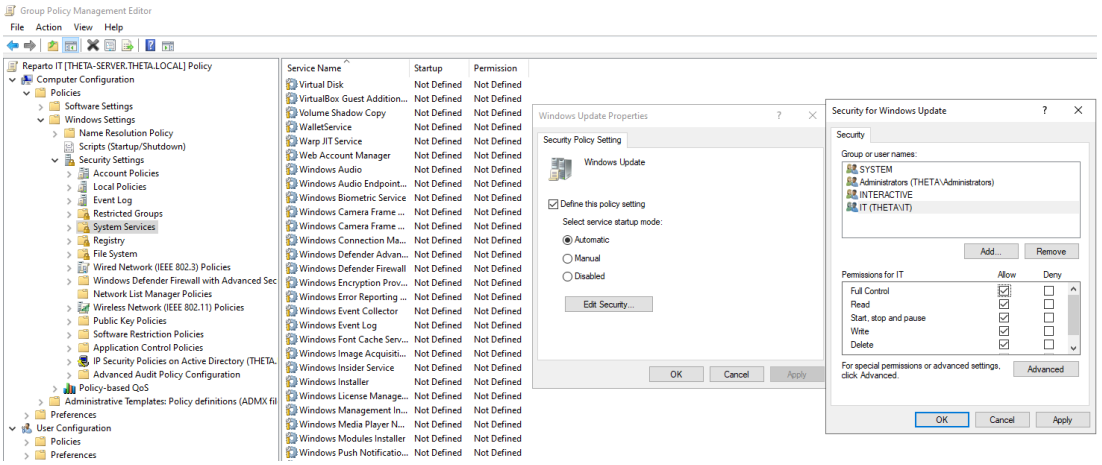
Per poter modificare le GPO in maniera mirata senza perdere le impostazioni di default ma senza andare a modificare in maniera diretta queste ultime, ho fatto un backup delle GPO di default.



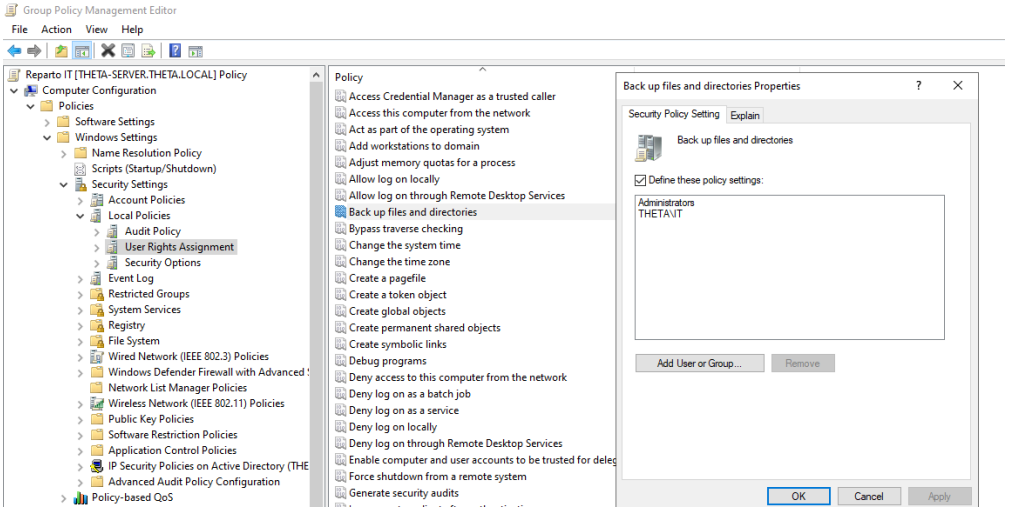
Successivamente, ho creato una nuova GPO con nome **Policy IT** ed ho importato le impostazioni di default sulla nuova GPO (grazie alla copia backup) prima di andare a modificarla.



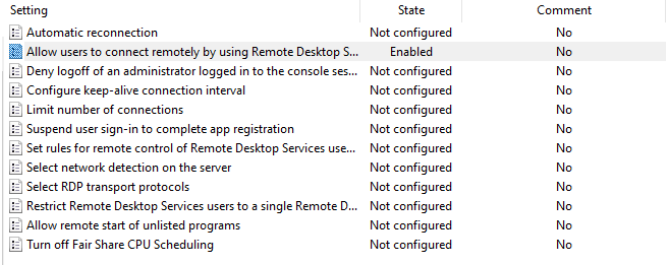
Sono passato così alla modifica della GPO rivolta al reparto IT appena creata.
Ho iniziato modificando alcuni permessi relativi ai servizi di sistema. Ho ad esempio abilitato l'accesso per la gestione degli aggiornamenti tramite **Windows Update** e abilitato i permessi per la gestione di **WMI** (utile per la gestione remota e la diagnostica).



Inoltre, tramite la sezione **Computer Configuration** - **Policies** - **Windows Settings** - **Security Settings** - **Local Policies** - **User Rights Assignment**, ho modificato alcune politiche utili al reparto IT. Ad esempio, tramite la sezione "**Shut down the system**" ho dato il permesso di spegnere il server, mentre tramite la sezione "**Backup file and directories**", ho dato i permessi per il backup dei file.

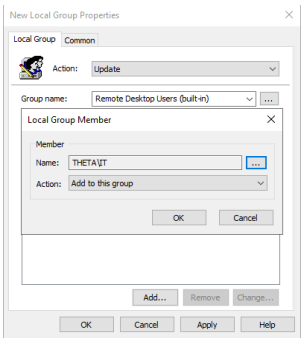


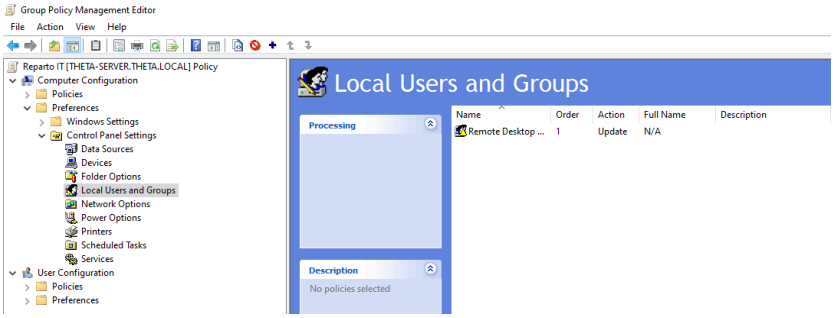
Infine, ho provato ad apportare alcune modifiche per permettere l'accesso remoto al server.
Ho dato il permesso agli utenti di collegarsi tramite **Remote Desktop**.



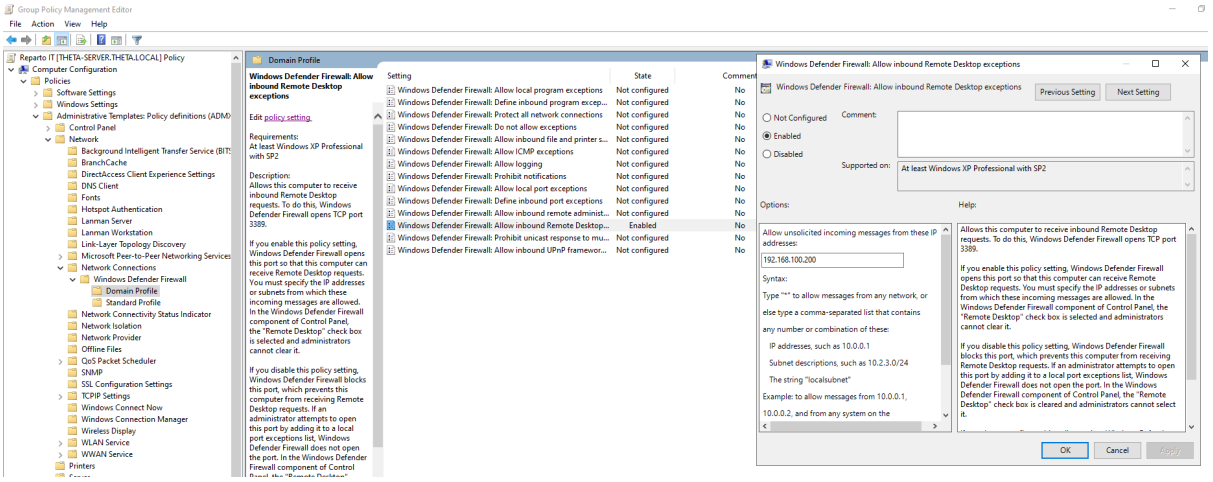
Setting	State	Comment
Automatic reconnection	Not configured	No
Allow users to connect remotely by using Remote Desktop S...	Enabled	No
Deny logoff of an administrator logged in to the console ses...	Not configured	No
Configure keep-alive connection interval	Not configured	No
Limit number of connections	Not configured	No
Suspend user sign-in to complete app registration	Not configured	No
Set rules for remote control of Remote Desktop Services use...	Not configured	No
Select network detection on the server	Not configured	No
Select RDP transport protocols	Not configured	No
Restrict Remote Desktop Services users to a single Remote D...	Not configured	No
Allow remote start of unlisted programs	Not configured	No
Turn off Fair Share CPU Scheduling	Not configured	No

Ho inserito il gruppo “**IT**” tra i gruppi locali affinché venisse riconosciuto come tale.

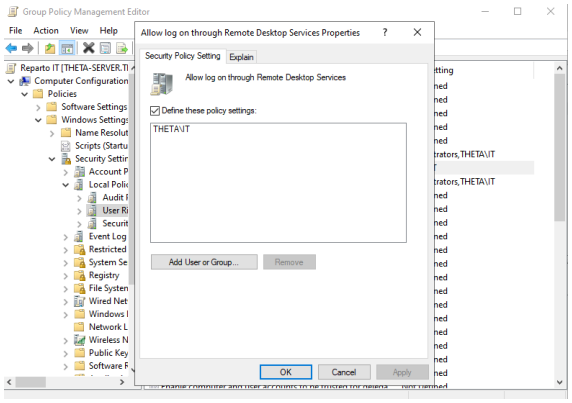




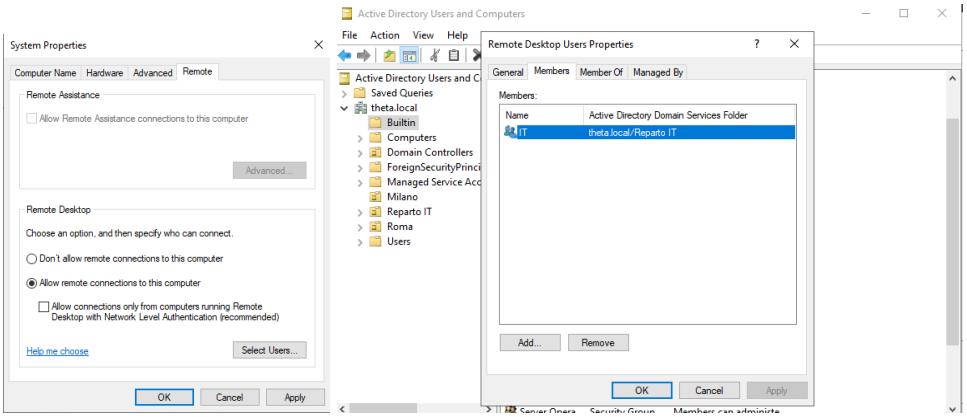
Ho modificato le impostazioni del firewall.



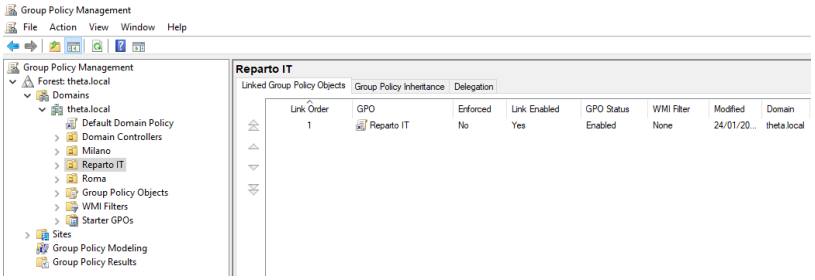
Ho dato i permessi per il log tramite Remote desktop recandomi alla sezione **Computer Configuration - Policies - Windows setting - Security settings - Local policies - User rights assignment**.



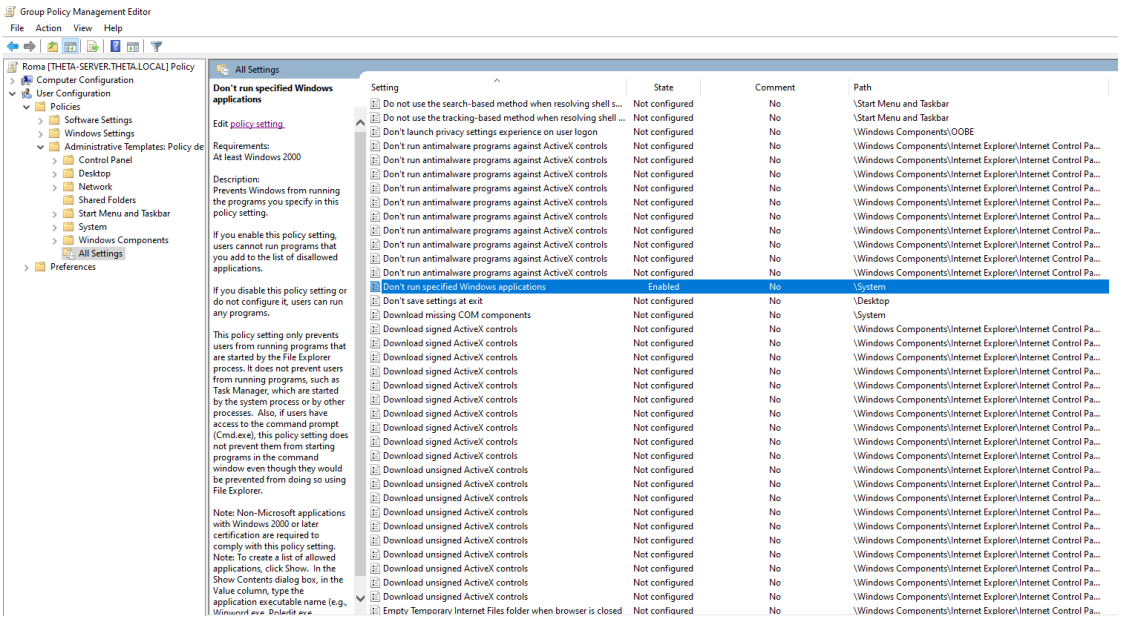
Ho abilitato la funzionalità Remote Desktop tramite Server Manager ed inserito il gruppo interessato nel gruppo **Remote Desktop Users** nella sezione **Builtin** di Active Directory.



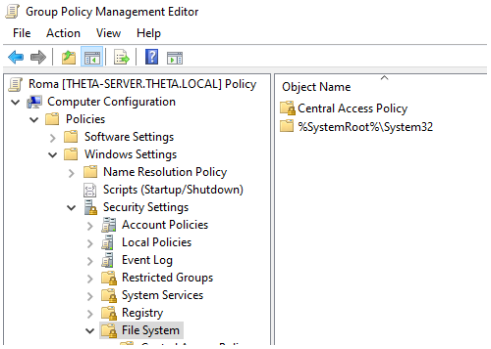
Una volta finiti i tentativi di abilitare l'accesso remoto, ho assegnato la GPO appena creata all'OU "**Reparto IT**"



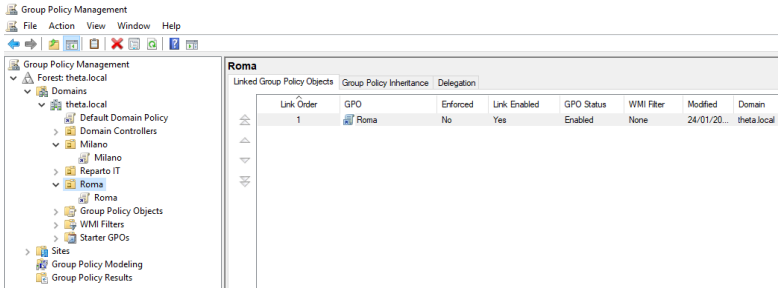
Successivamente sono passato alla modifica delle GPO anche per l'OU "**Roma**". Anche in questo caso ho creato una nuova GPO con nome "Roma" in cui ho importato le impostazioni di default prima di procedere con la modifica.
Tramite GPO ho provato ad impedire l'esecuzione di un programma specifico.
L'impostazione di nostro interesse è in questo caso "**Don't run specified Windows Applications**" nella sezione **Administrative templates** della **User Configuration**.

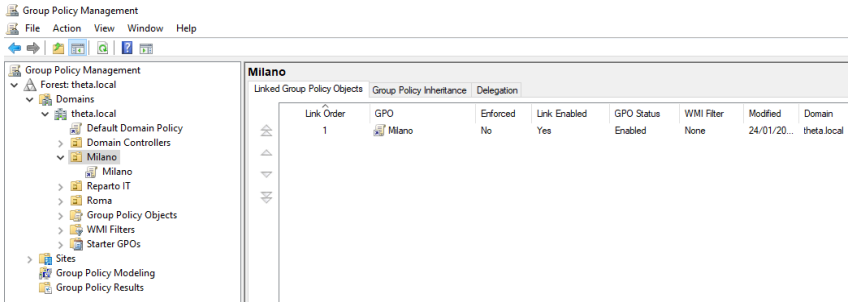


Il tentativo, come detto inizialmente, è stato quello di impedire, in questo caso, l'avvio dell'applicazione calcolatrice (gestionale Milano).
Inoltre ho visto anche che c'era un modo per impedire l'accesso a specifici file e cartelle agendo direttamente sulle regole del File System.
Ho fatto un tentativo di esempio con la cartella **System32** ma senza soffermarmi troppo per mancanza di tempo.

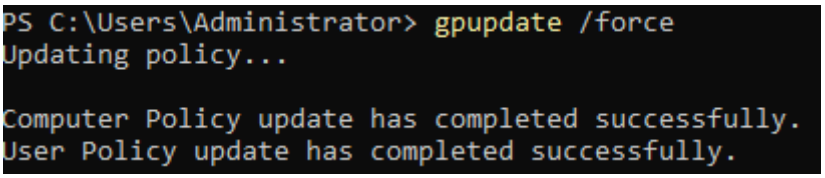


Una volta terminate le modifiche, ho assegnato questa GPO all'OU "Roma".
Ovviamente stesso procedimento è stato seguito per la GPO "**Milano**" con l'unica differenza che, in questo caso, l'applicazione da non far partire era "notepad.exe".



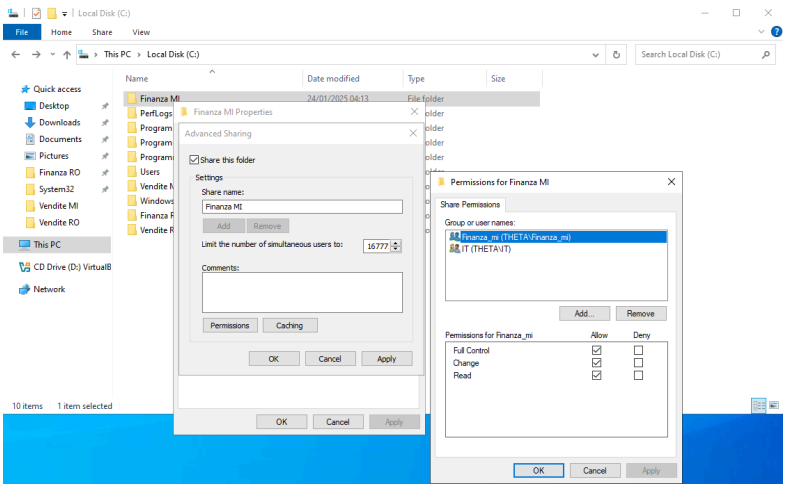


Successivamente ho forzato il caricamento delle nuove Policy tramite Il seguente comando:



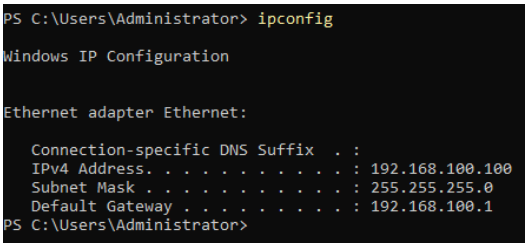
Per la divisione dei file, ho creato quattro differenti cartelle condivise, ognuna specifica per ogni settore: Vendite RO, Finanza RO, Vendite MI e Finanza MI.
Un'ulteriore cartella è stata creata con il nome "**programmi condivisi**", accessibile a tutti, contenente le applicazioni "calcolatrice" e "notepad".

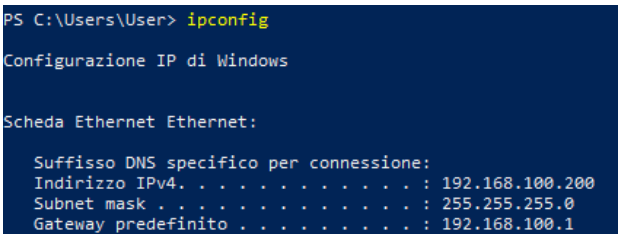
I permessi di tale cartelle sono stati modificati per permettere l'accesso solo al gruppo giusto, come nell'esempio riportato sotto:



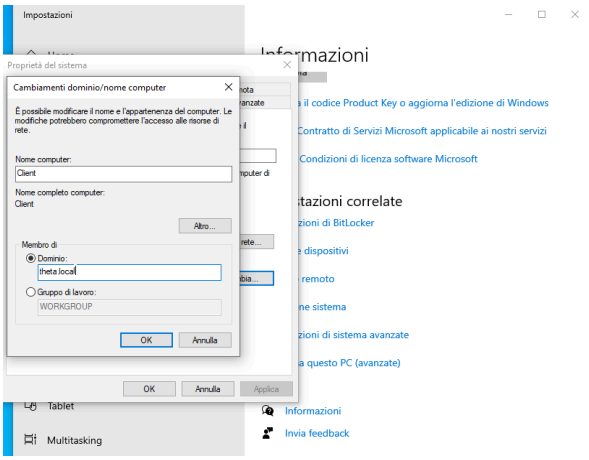
- **Verifica**

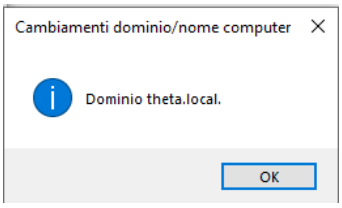
Per verificare che quanto fatto su sia effettivamente funzionante ho avviato una macchina Windows 10. Una volta messe entrambe le macchine sulla rete interna, ho modificato i loro indirizzi IP per metterle nella stessa rete.



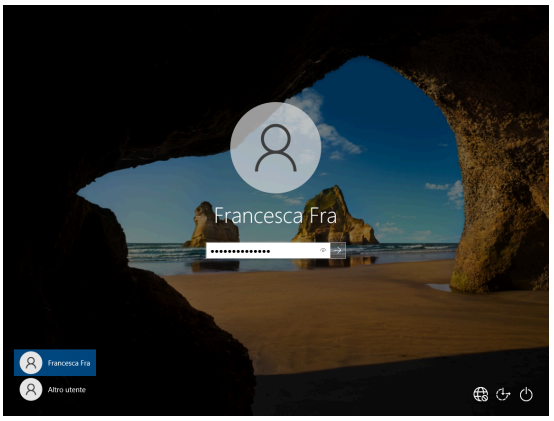


Ho modificato il nome della macchina Windows 10 e l'ho inserita nel dominio **theta.local**

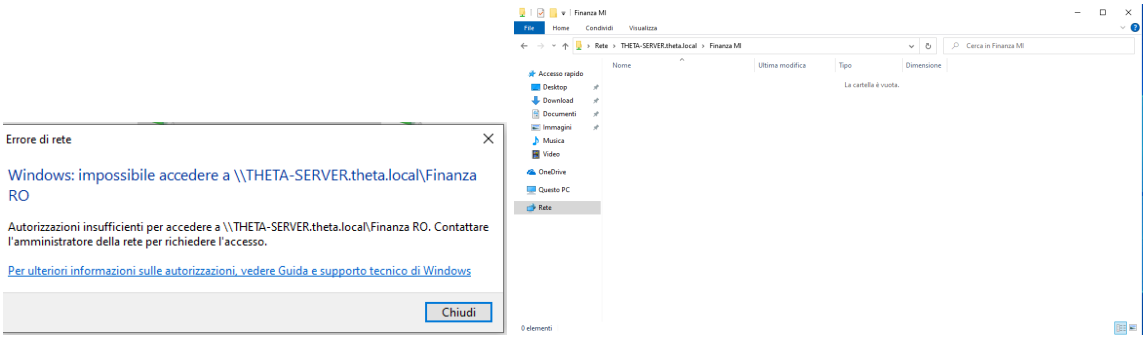




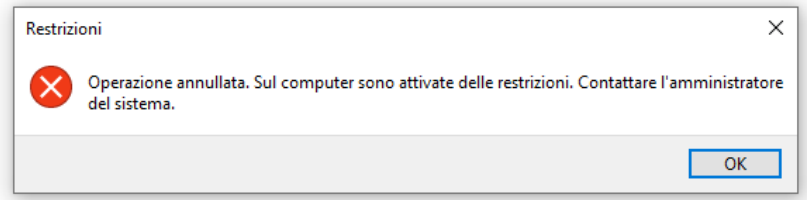
Una volta riavviata la macchina, un primo tentativo è stato effettuato con l'utente "**Francesca**" del reparto finanza della filiale di Milano.



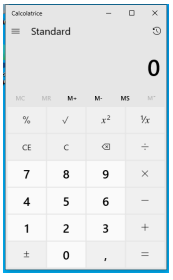
Ho provato a visualizzare le cartelle condivise, ad effettuare l'accesso a cartelle non di sua pertinenza (effettivamente negato) e ad effettuare l'accesso alla cartella di suo interesse. Di seguito i risultati.



Come si può vedere in alto, la cartella a cui è consentito l'accesso è proprio "**Finanza MI**", mentre l'accesso alla cartella "**Finanza RO**" viene negato.
Successivamente mi sono spostato nella cartella "**programmi condivisi**". Ho provato ad avviare l'applicazione notepad (esclusiva di Roma) e il risultato è stato il seguente.

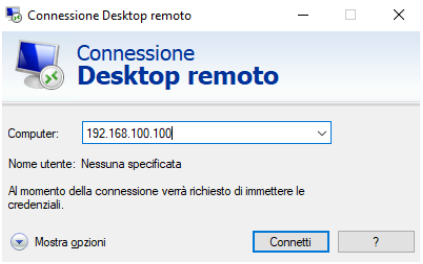


Provando ad avviare l'applicazione calcolatrice ottengo invece il seguente risultato.

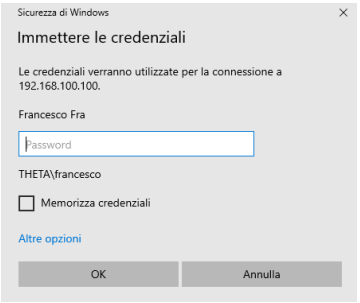


Tutto sembra funzionare correttamente.
Dopo aver effettuato la disconnessione, ho provato ad accedere con l'account "**Francesco**" del reparto IT per provare l'accesso remoto.

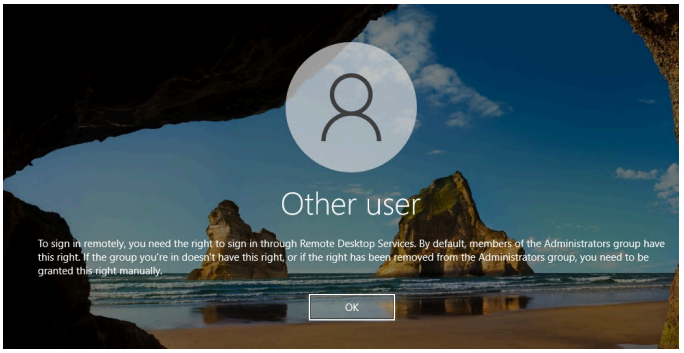
Una volta entrato, tramite il comando **mstc** avvio Remote Desktop ed inserisco l'indirizzo IP del Server.



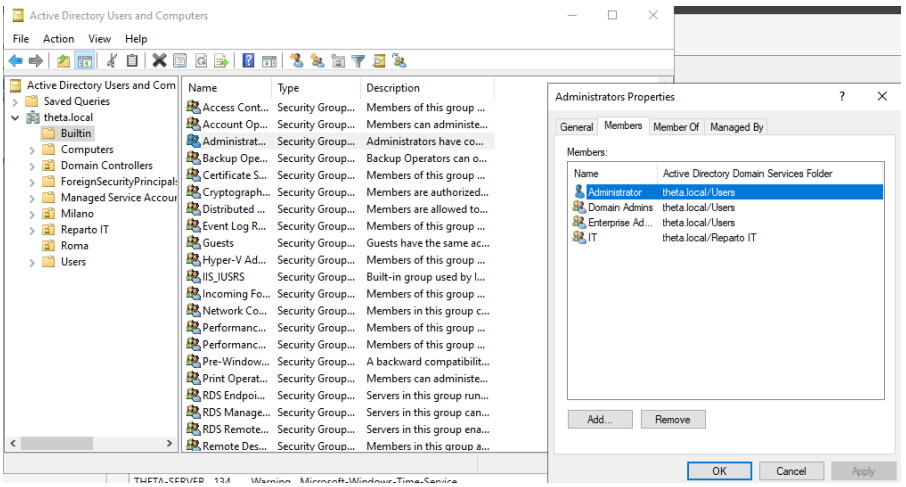
Mi vengono chieste le credenziali.



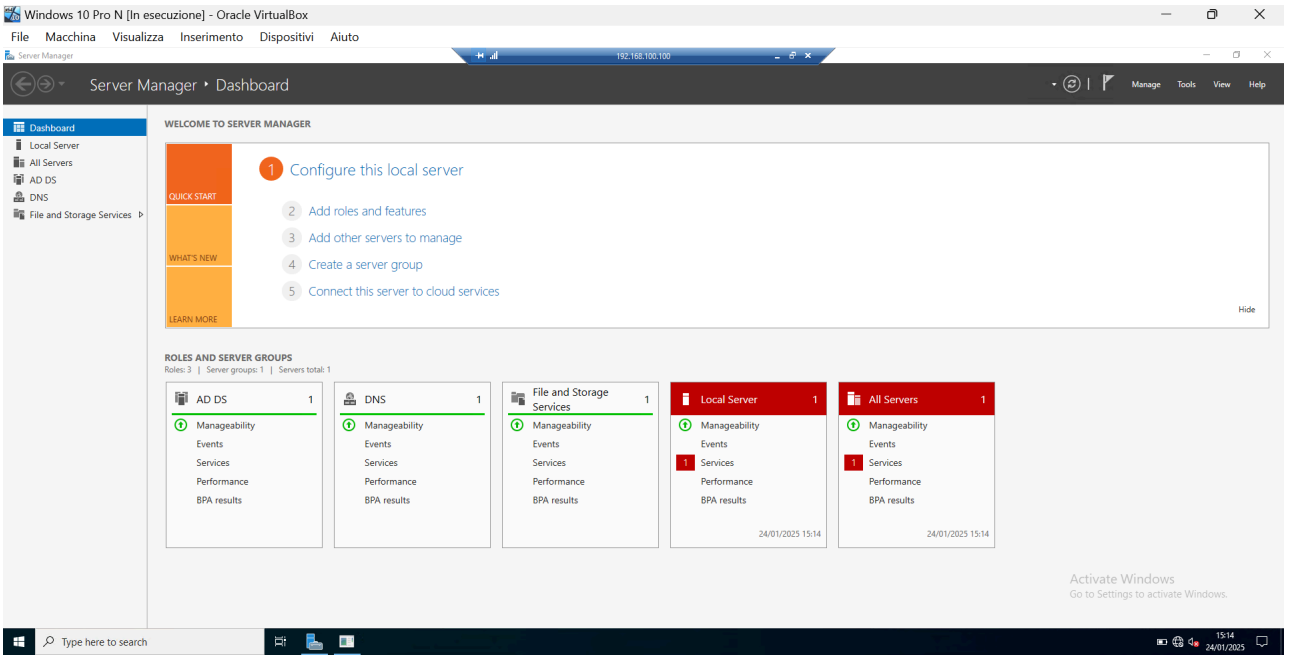
Ma, una volta inserite, il collegamento non riesce. Ad essere precisi, il collegamento avviene, ma non mi viene consentito l'accesso.



Ho bypassato tale problema tornando sulla macchina Windows Server ed inserendo il gruppo “IT” all’interno del gruppo **Administrators** della sezione Builtin di Active Directory, ma non so se si tratta del procedimento corretto.



Una volta fatto ciò, tornando sulla Windows 10 ed accedendo con l’utente Francesco, l’accesso remoto riesce.



Come si può vedere dall’indirizzo IP in alto nell’immagine, stiamo controllando il server da remoto.