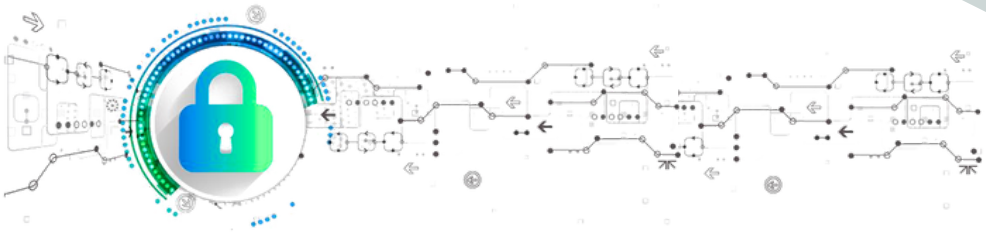


Esercizio per il progetto settimanale Unit 3 - S10 - L5

L'esercizio consiste nel familiarizzare con la gestione dei gruppi di utenti in **Windows Server 2022**. Dovremmo creare gruppi, assegnare loro permessi specifici e comprendere l'importanza della gestione dei gruppi per la sicurezza e l'amministrazione del sistema.
Le varie fasi dell'esercizio comprenderanno la creazione dei gruppi, l'assegnazione dei permessi, la verifica delle impostazioni assegnate e la documentazione.

Windows Server

L'azienda a cui faremo riferimento è: **Renova**, un'azienda moderna e flessibile che offre servizi completi alle imprese, aiutandole a crescere e innovare grazie a un team con competenze diverse e ben coordinate.

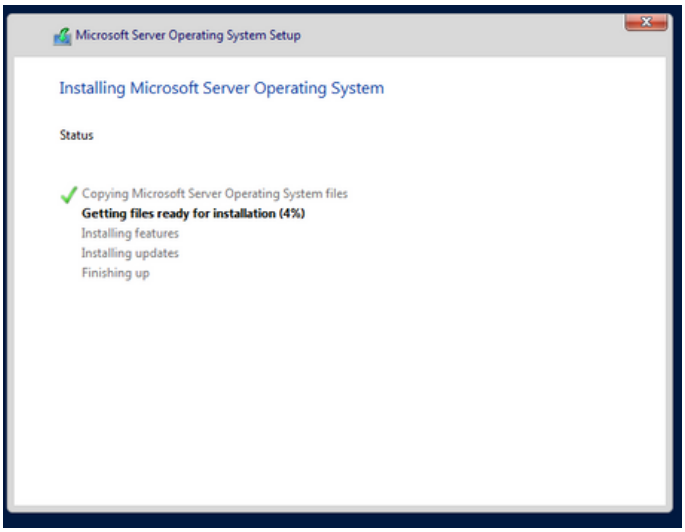
Renova è suddivisa in 3 aree operative, ognuna con compiti specifici:

Marketing e Comunicazione
Si occupa della promozione e dell'immagine delle aziende clienti: crea campagne pubblicitarie, cura i contenuti per i social, progetta loghi, siti e strategie per migliorare la visibilità e attrarre nuovi clienti.

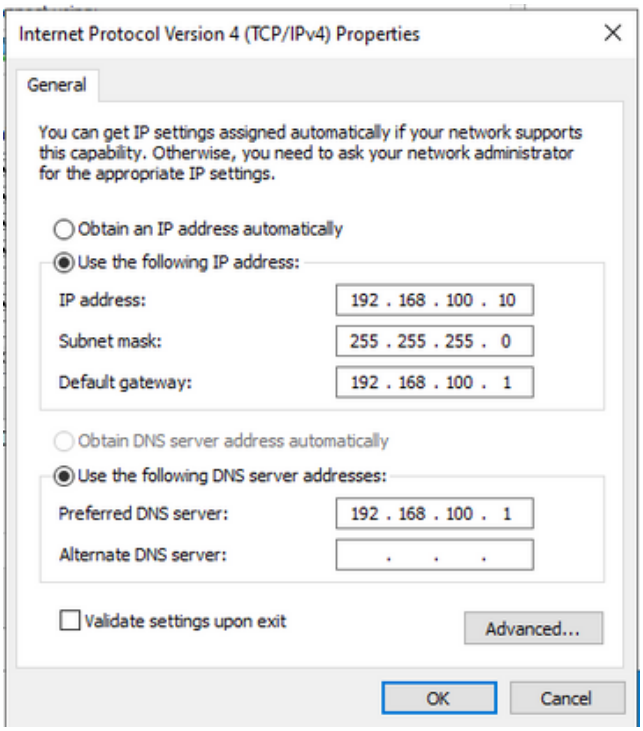
Sviluppo Software e IT
Realizza programmi e strumenti digitali personalizzati, come gestionali, app o piattaforme online, che aiutano le aziende a lavorare meglio e in modo più organizzato.

Amministrazione
Si occupa della contabilità, dei pagamenti, delle fatture e di tutte le attività amministrative. Inoltre, gestisce l'acquisto e l'organizzazione delle attrezzature da ufficio, assicurando che ogni reparto abbia ciò di cui ha bisogno per lavorare al meglio.

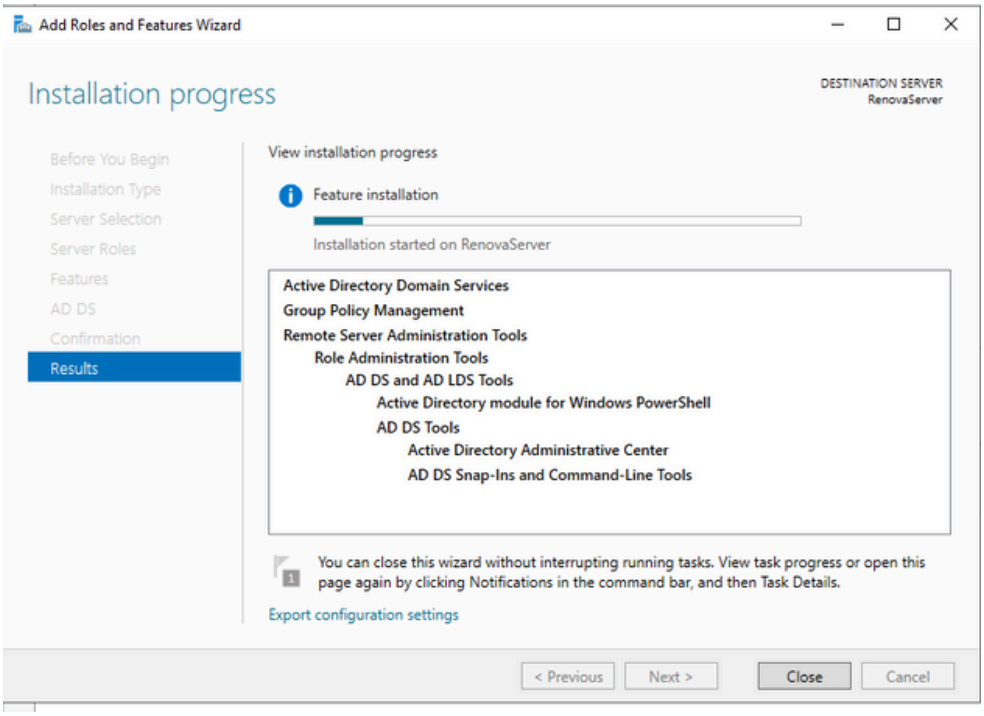
Come prima cosa configuriamo il nostro laboratorio virtuale avviando il **Windows Server** cosi da poterlo usare per il nostro esercizio.



Una volta ottenuto l'accesso al sistema operativo impostando una password per l'utente **Administrator** ci rechiamo sulle impostazioni di rete e configuriamo manualmente gli indirizzi (impostiamo la macchina virtuale su una rete interna)

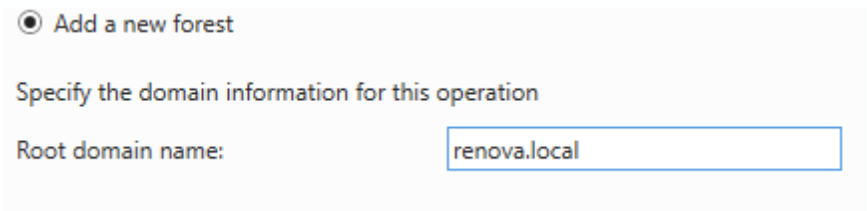


Il prossimo passo sarà cambiare il nome del computer dalle impostazioni del local server chiamandolo **RenovaServer** e successivamente ci servirà installare le **Active Directory** che ci serviranno per la gestione degli utenti e dei gruppi con le relative politiche di sicurezza e Group Policy . Dalla dashboard del server manager clicchiamo su Tools e poi Add Roles e Features e nel processo di installazione abilitiamo l'opzione **Active Directory Domain Service.**

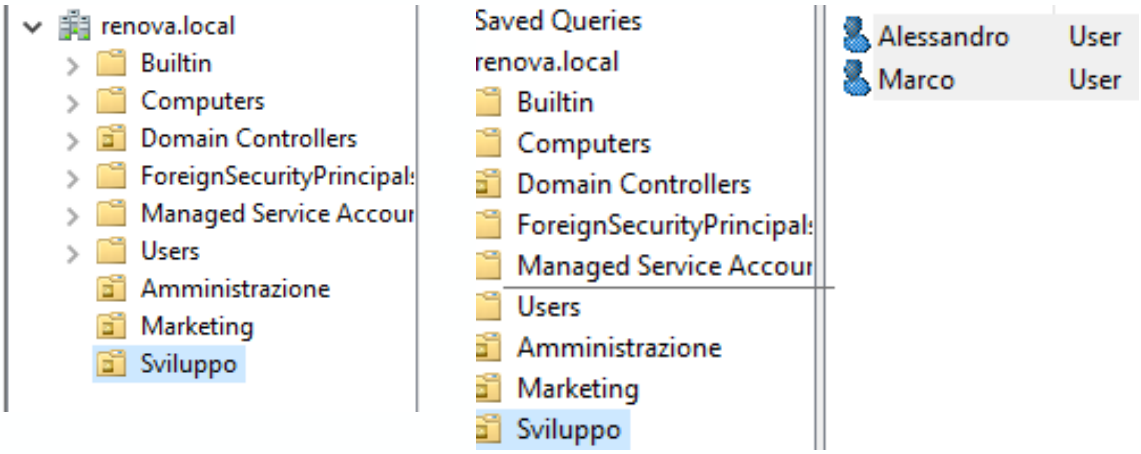


Adesso ci servirà creare la nostra **foresta** ovvero un insieme di domini che condividono la stessa struttura logica comune, creare un **dominio** ci aiuterà a gestire utenti, computer e altre risorse e sono identificati da un nome DNS univoco, le principali funzioni del dominio saranno:

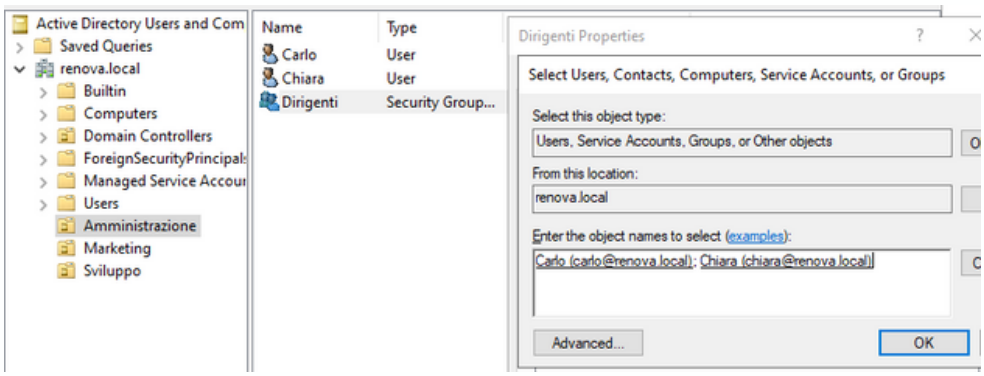
- Autenticazione: Gestisce l'accesso degli utenti alle risorse.
- Policy di Sicurezza: Applica criteri di sicurezza a utenti e computer.
- Replicazione: Sincronizza i dati tra i controller di dominio.



Adesso possiamo entrare nel vivo e creare i nostri **utenti** e **gruppi**, così da facilitare la gestione degli utenti con esigenze simili come nel nostro contesto aziendale, definire chi può accedere a quali risorse e semplificare l'assegnazione delle autorizzazioni.
Accediamo quindi in Tools e Active Directory Users and Computers e per prima cosa creiamo 3 **Organizational Unit** in relazione al nostro contesto aziendale e successivamente gli utenti appartenenti



Adesso sarà importante creare dei **gruppi** con le relative policy aziendale assegnate cosi che quando dovremmo assegnare determinati permessi potremo farlo indirizzi al gruppo rispetto che ai singoli utenti



Al momento la struttura della Foresta e del Dominio è la seguente:

- **RenovaServer**: La Active Directory principale.
- **Renova.local**: La foresta in cui all'interno si trova il dominio con lo stesso nome.
  - **Amministrazione**: OU* creata per il dipartimento amministrativo.
  Carlo: Utente creato nell'OU Amministrazione.
  Chiara: Utente creato nell'OU Amministrazione.
  - **Marketing**: OU creata per il dipartimento di marketing.
  Sofia: Utente creato nell'OU Marketing.
  Giulia: Utente creato nell'OU Marketing.
  - **Sviluppo**: OU creata per il dipartimento di programmazione.
  Alessandro: Utente creato nell'OU Sviluppo.
  Marco: Utente creato nell'OU Sviluppo.

Alla fine, dovremmo ritrovarci con tre Unità Organizzative:

- **Amministrazione** con gli utenti **Carlo e Chiara** che fanno parte del gruppo **Dirigenti** creato all'interno dell'OU **Amministrazione**.
- **Marketing** con gli utenti **Sofia e Giulia** che fanno parte del gruppo **Comunicazione** creato all'interno dell'OU **Marketing**
- **Sviluppo** con gli utenti **Alessandro e Marco** che fanno parte del gruppo **Java** creato all'interno dell'OU **Sviluppo**

Questa struttura ci permette una gestione centralizzata e sicura degli accessi secondo le policy aziendali.

*OU = Organizational Unit - Unità Organizzative

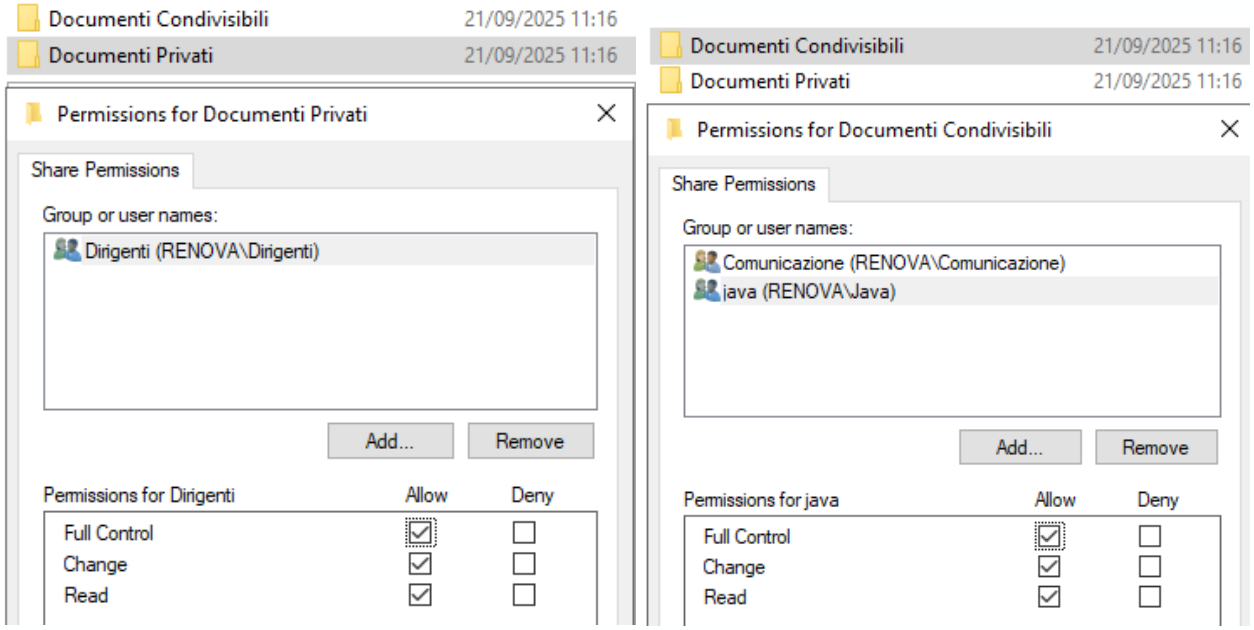
Dopo aver creato gli utenti e i gruppi con i rispettivi membri, procederemo a creare le varie **group policy** di accesso che dovranno rispettare i regolamenti aziendali, definendo chi può vedere cosa, chi può modificare cosa, ecc..
Per applicare le policy nel nostro contesto creo prima una cartella all'interno del server chiamata Dati Riservati . All'interno di questa cartella, ne creo un altra: Documenti Privati, all'interno saranno presenti degli esempi di documenti privati aziendali.

Dopo aver creato le cartelle, andremo a configurare i relativi permessi. Prima di procedere, spiegheremo la differenza tra le due macro categorie di permessi presenti in Windows Server: **Sharing e Security.**

- **Ambito di Applicazione**: I permessi di condivisione si attivano solo quando una risorsa (file o cartella) è accessibile tramite la rete. Al contrario, i permessi di sicurezza (o NTFS) si applicano sempre, sia per l'accesso locale che per quello remoto.
- **Granularità:** I permessi di condivisione sono meno dettagliati, offrendo solo opzioni di base come "Lettura" e "Modifica". I permessi di sicurezza, invece, sono estremamente granulari e permettono di definire con precisione quali azioni possono essere eseguite, offrendo un controllo molto più fine.
- **Effetto Combinato**: Quando un utente accede a una cartella condivisa via rete, il suo livello di accesso è determinato dall'intersezione dei due tipi di permessi. In pratica, il sistema applica sempre il permesso più restrittivo, garantendo che la sicurezza non venga compromessa da un permesso di condivisione troppo ampio.

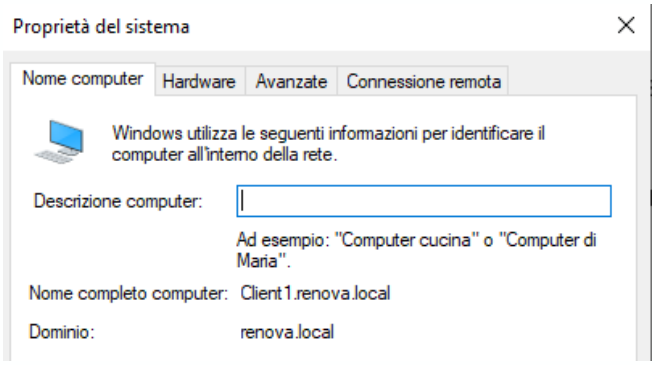
Facciamo l'esempio nella nostra azienda Renova in cui abbiamo la cartella condivisa chiamata "**Dati Riservati**" con all'interno altre 2 cartelle chiamate "Documenti Privati" e "Documenti Condivisibili" e vorremmo assegnare i seguenti permessi:

- **Permessi di Dati Riservati:** Tutti gli utenti potranno vedere le cartelle contenute.
- **Permessi di Documenti Privati:** Accessibile solo al gruppo Dirigenti (Carlo e Chiara) che potrà aprire e modificare i contenuti.
- **Permessi di Documenti Condivisibili**: Accessibile solo al gruppo Comunicazione (Giulia e Sofia) e Java (Alessandro e Marco) che potrà aprire e modificare i contenuti.



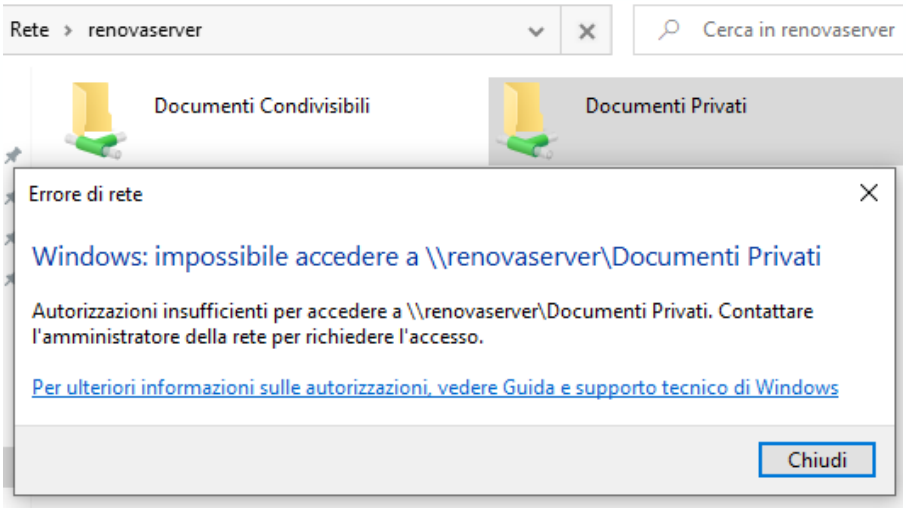
Con queste impostazioni solo i Dirigenti avranno **full control** dei documenti privati mentre per i documenti condividibili aziendali avranno full control i rispettivi gruppi delle Unità di Marketing e Sviluppo (se richiesto anche l'unità di Amministrazione potrà avere accesso ai Documenti Condivisibili)

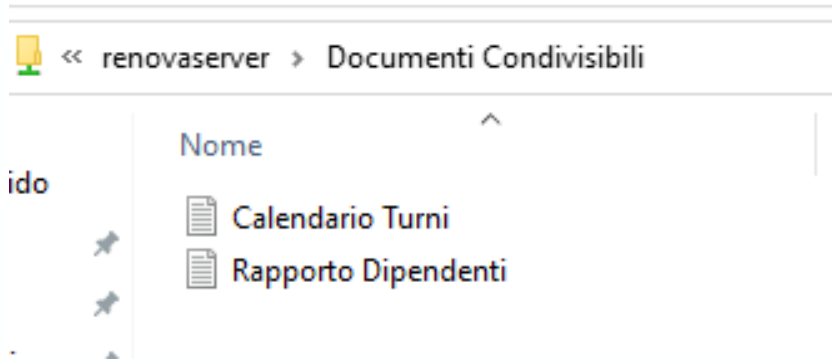
Adesso ci servirà configurare un **client** modificando le impostazioni di rete con il server **DNS** preferito con l'indirizzo IP del windows server e principalmente cambiare nelle impostazioni del nome computer del client e mettere il **dominio renova.local** cosi da collegarsi alla rete e poter accedere con gli user e fare tutte le dovute verifiche.



Una volta riavviata a macchina client si applicheranno le modifiche e potremo fare il **primo accesso** con uno dei nostri utenti della rete, in questo caso accederò con Alessandro che fa parte dell'unità Sviluppo

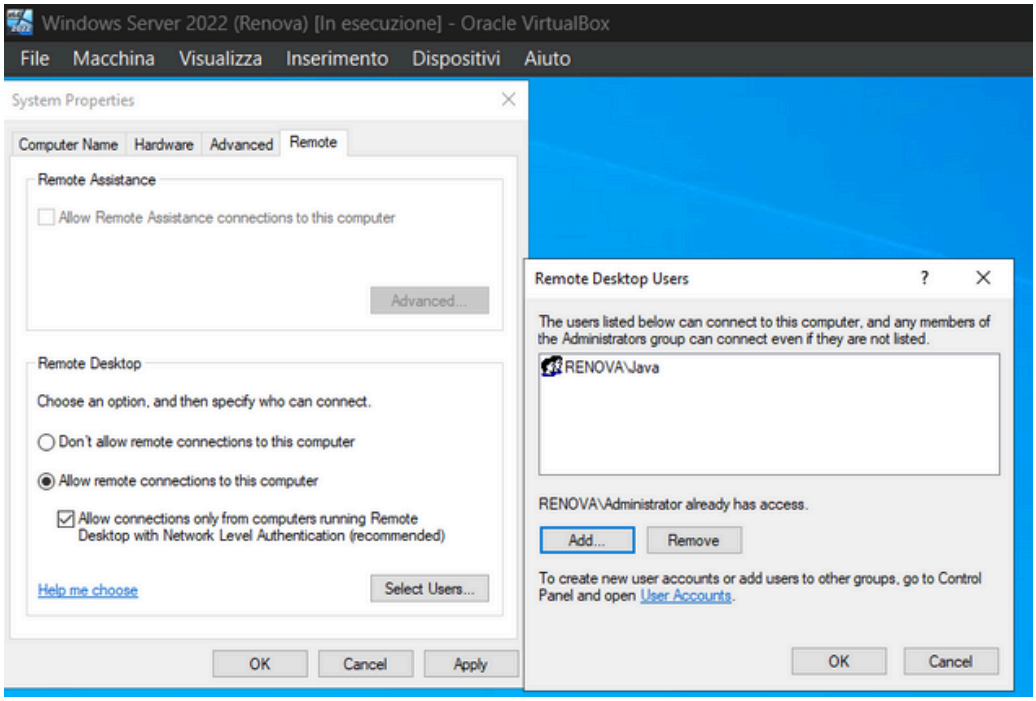
Una volta fatto l'accesso possiamo verificare come la cartella per esempio dei Documenti Privati non sia accessibile da Alessandro mentre invece la cartella dei **Documenti Condivisibili** sia accessibile, rispecchiando le impostazioni di accesso precedentemente configurati.

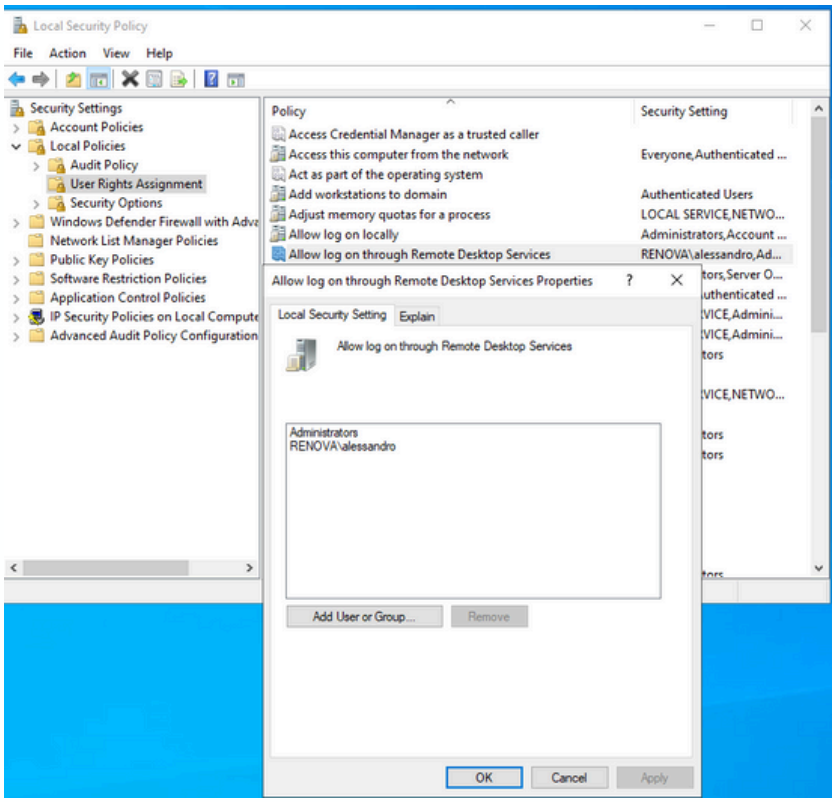




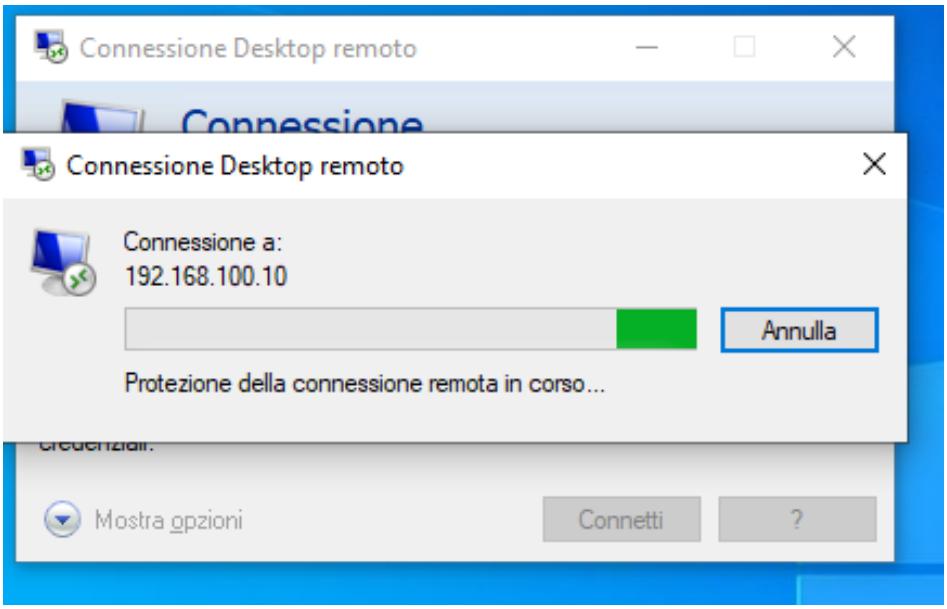
Una volta riavviata a macchina client si applicheranno le modifiche e potremo fare il **primo accesso** con uno dei nostri utenti della rete, in questo caso accederò con Alessandro che fa parte dell'unità Sviluppo

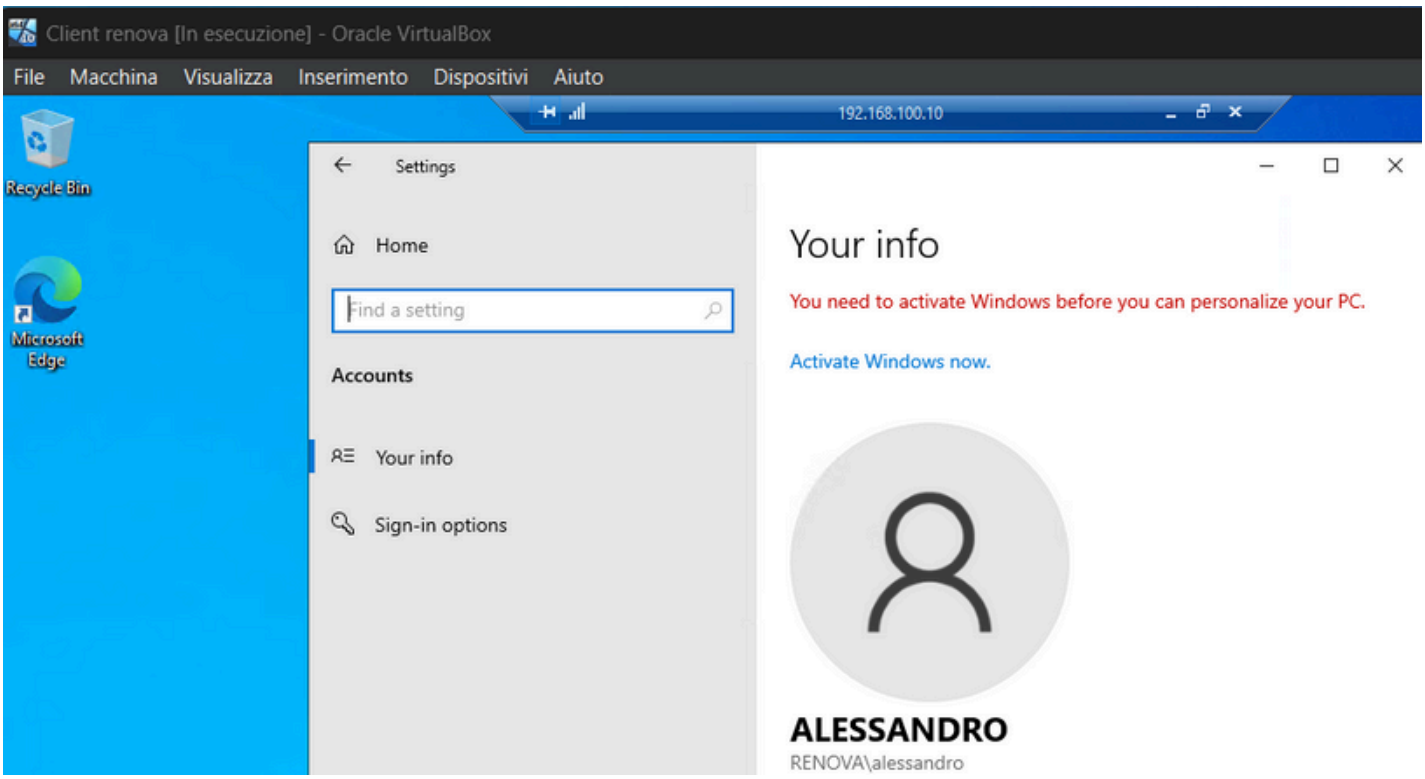
Come prossimo passo daremo all'user Alessandro i permessi per il **controllo da remoto del Server**, accediamo prima alle system properties e successivamente alle Local Security Policy



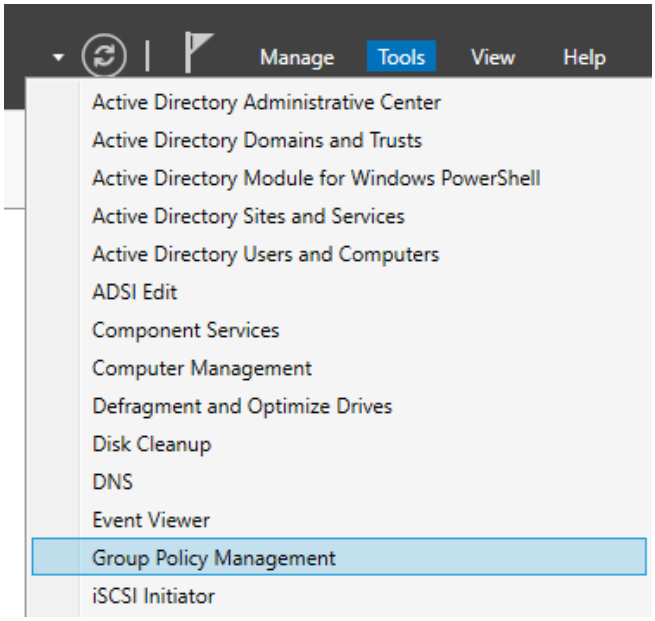


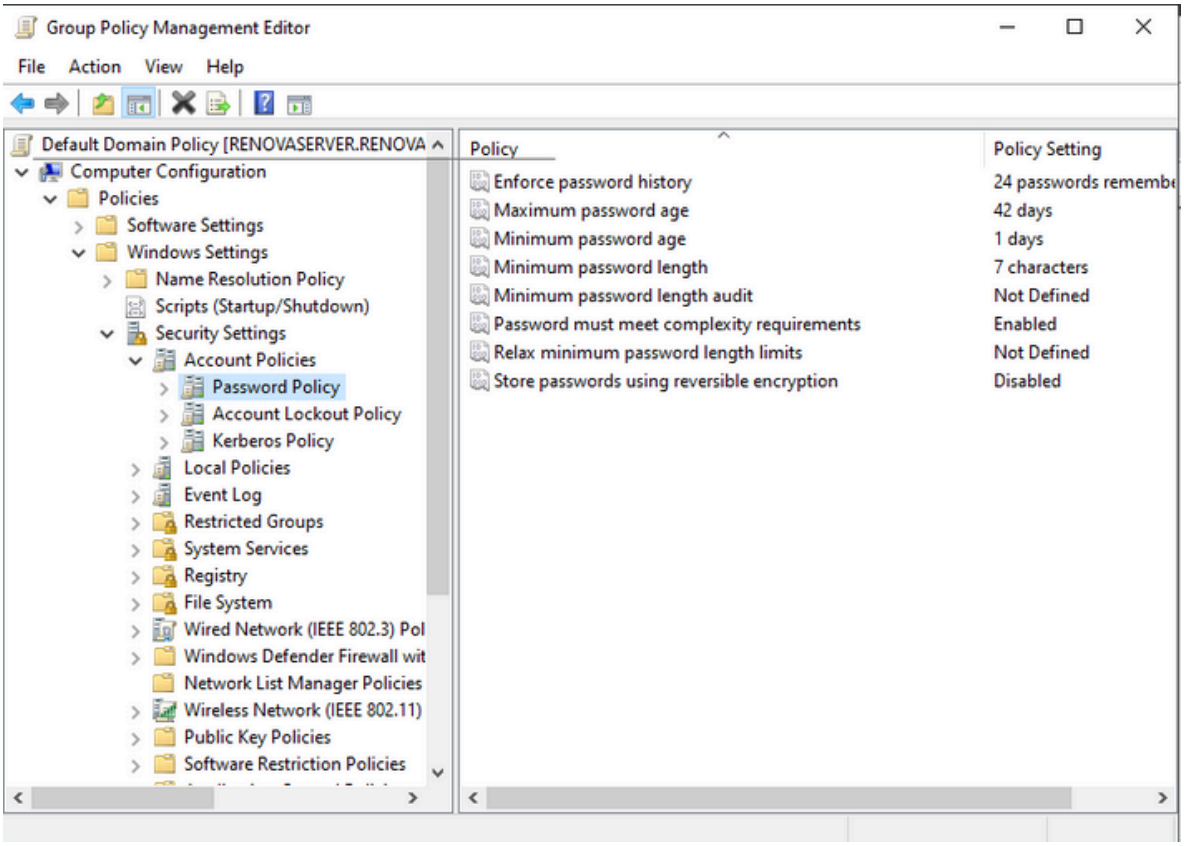
Successivamente facendo la prova a collegarci al **server** vedremo come l'operazione risulta completata



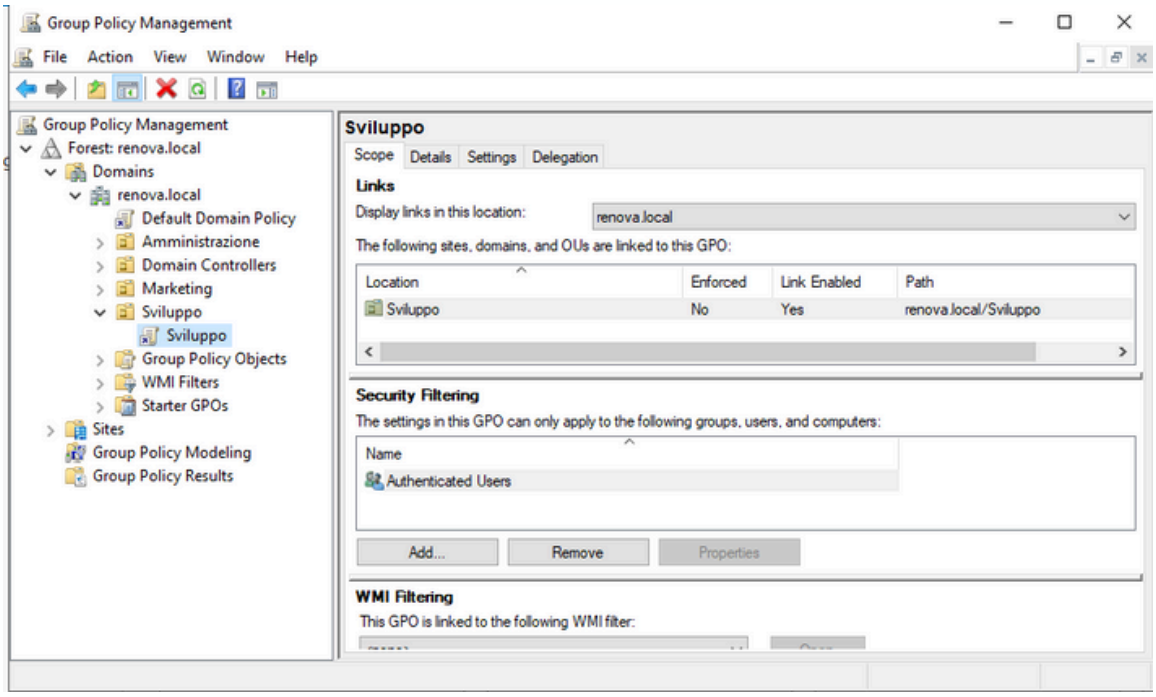


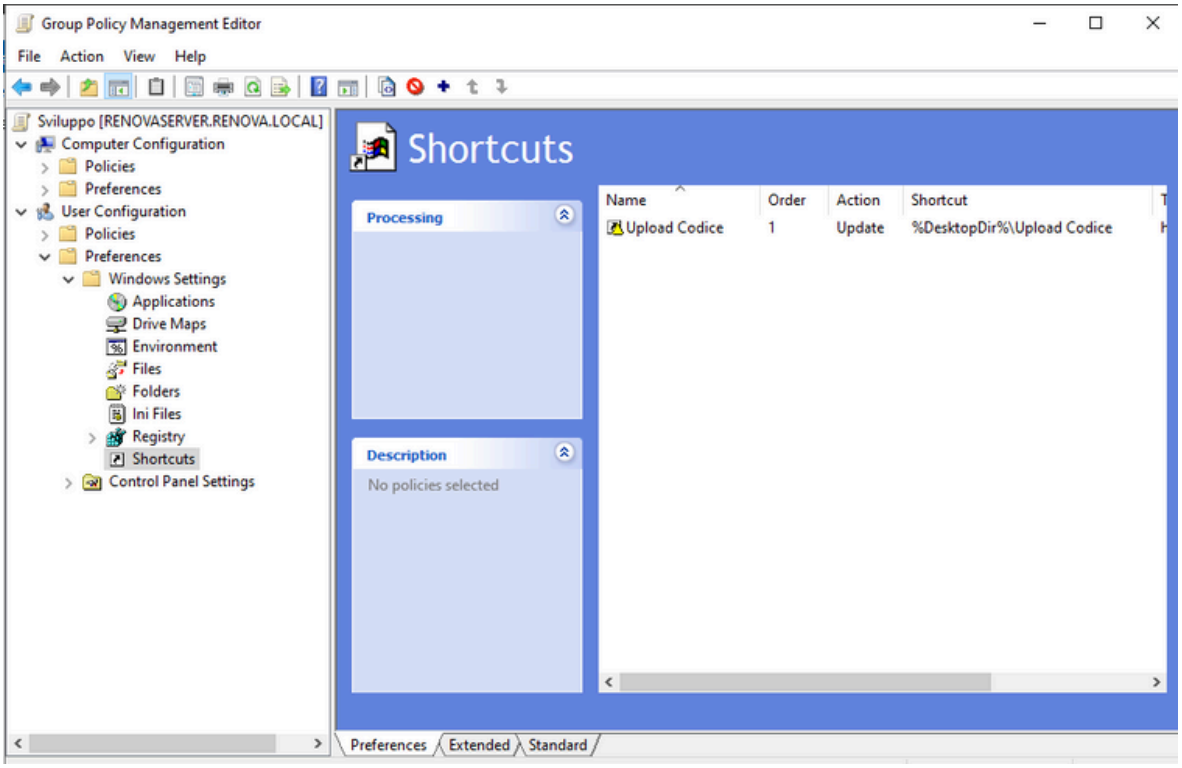
Adesso come prossimo passo andiamo più a fondo implementando le **GPO (Group Policy Objects),** dove è possibile gestire le impostazioni di sicurezza delle password per esempio definendo gli standard di sicurezza



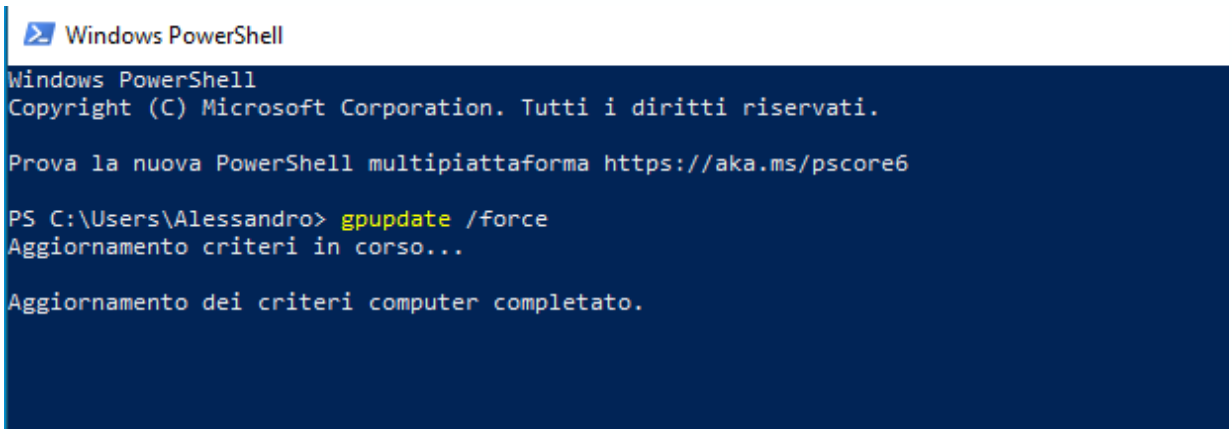


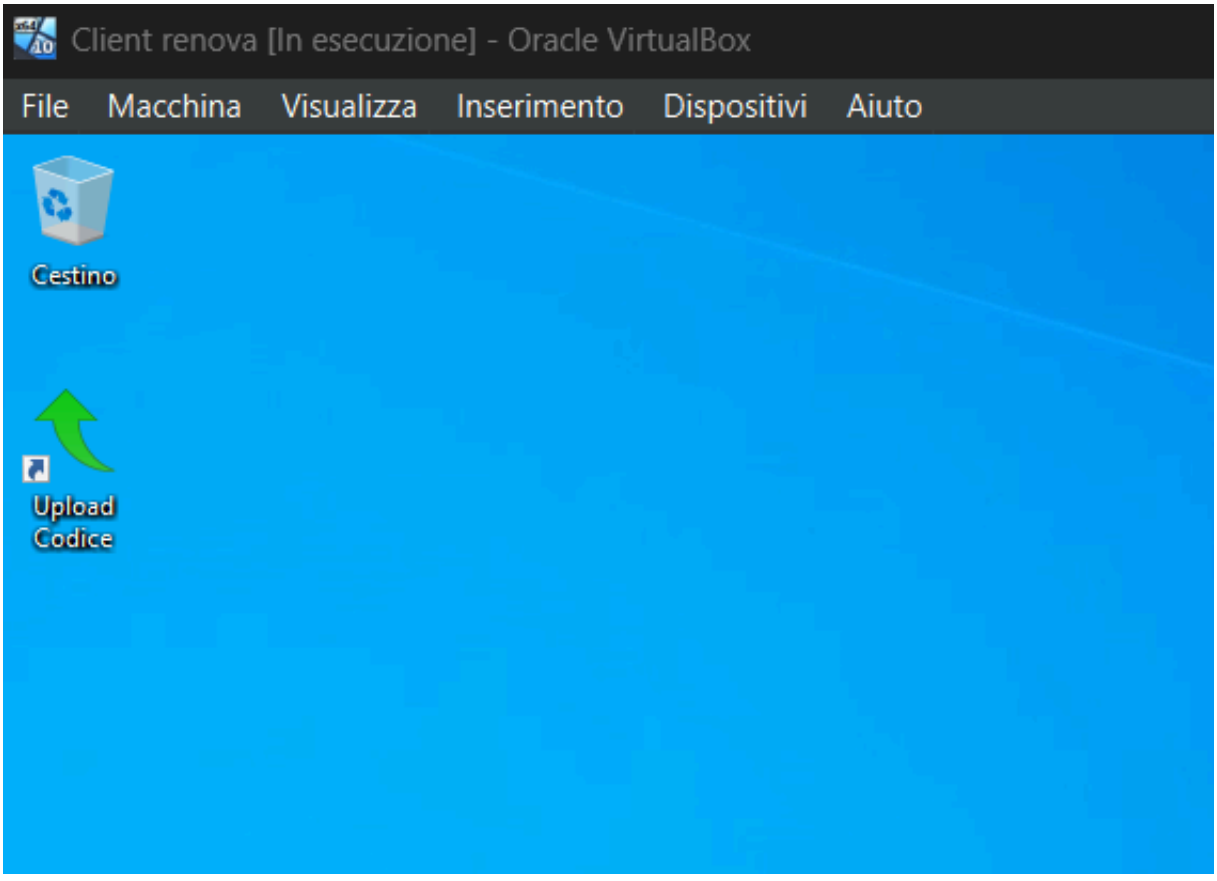
Mettiamo il caso di voler implementare delle GPO ad Alessandro nell'unità di Sviluppo e aggiungere nelle **shortcuts** nel suo desktop





Abbiamo creato una **shortcut** per il Desktop di Alessandro cosi che solo lui avrà il link diretto per l'upload dei codici direttamente nel desktop, quindi forziamo da **powershell** l'azione e cosi dovremo vedere spuntare lo shortcut nel desktop





Windows Server

Windows Server

Le procedure presenti in questo report descrivono la struttura di gestione degli accessi e dei dati dell'azienda **Renova**, implementata tramite **Active Directory.**

La struttura organizzativa si basa sulla creazione di **Unità Organizzative (OU)** per i dipartimenti **Amministrazione, Marketing e Sviluppo**. All'interno di ciascuna OU sono stati creati gli utenti e i relativi gruppi di sicurezza:

- Amministrazione: Gruppo Dirigenti (utenti Carlo e Chiara).
- Marketing: Gruppo Comunicazione (utenti Sofia e Giulia).
- Sviluppo: Gruppo Java (utenti Alessandro e Marco).

Questo approccio consente una gestione centralizzata e basata sui ruoli, fondamentale per l'applicazione delle **Group Policy**.
Per quanto riguarda la gestione dei permessi sui dati, le cartelle sul server sono state configurate con un sistema di **permessi** combinati:

- La cartella "Dati Riservati" permette a tutti gli utenti la visualizzazione delle sottocartelle.
- L'accesso completo alla sottocartella "Documenti Privati" è stato limitato esclusivamente al gruppo Dirigenti.
- L'accesso completo alla sottocartella "Documenti Condivisibili" è stato concesso ai gruppi Comunicazione e Java.

Abbiamo infine consentito all'utente Alessandro l'accesso da **remoto** al server e creato uno **shortcut** tramite **GPO** per il suo Desktop .