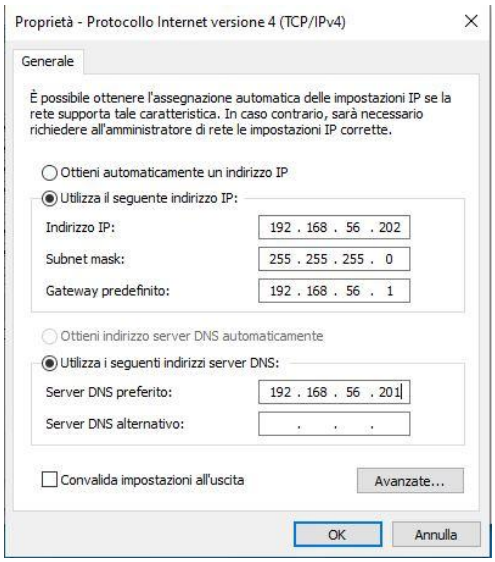
Windows Server 2022

Obiettivo: Incrementare un'infrastruttura Active Directory su **Windows Server 2022** considerando i seguenti permessi:
Accesso ai file e alle cartelle.
Esecuzione di programmi specifici.
Modifiche alle impostazioni di sistema.
Accesso remoto al server.

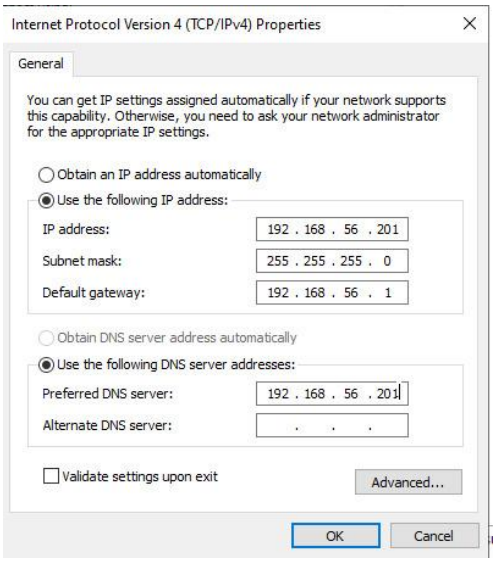
Macchine utilizzate e configurazione: Le macchine utilizzate sono state Windows Server 2022 che gestisce e supporta la rete e l'infrastruttura aziendale, Windows 10 in questo caso per simulare l'ipotetico Computer lato client di un lavoratore e pfSense come router.

Le macchine sono state configurate in **Rete Interna**, assegnando a ciascuna di esse un IP statico e come **DNS** lo stesso IP assegnato lato Server.

IP & DNS Client



IP & DNS Server

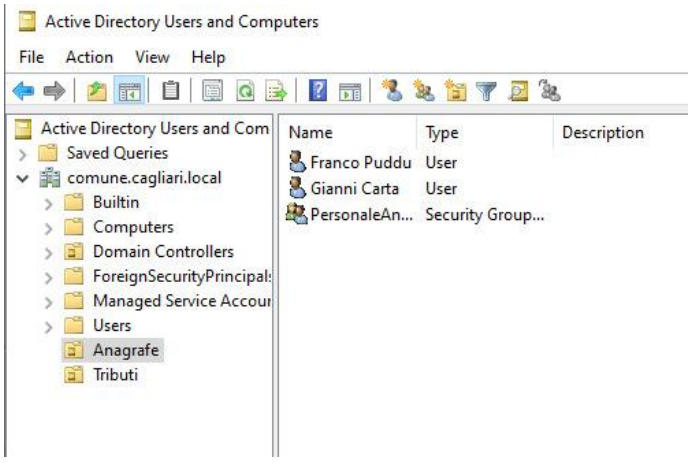


Gli IP sono stati confermati tramite l'utilizzo di **ipconfig** tramite **cmd.** Per questioni di praticità e semplicità del report, alcuni passaggi meno influenti e di verifica implementare verranno descritti ma non specificati da Screenshot.

Configurazione del Server & Struttura della gestione centralizzata dei gruppi e utenti: E' stato aggiunto il dominio al Server, in questo caso **comune.cagliari.local**, il PC è stato rinominato con il nome inerente, in quanto l'infrastruttura è basata interamente sul Comune di Cagliari.

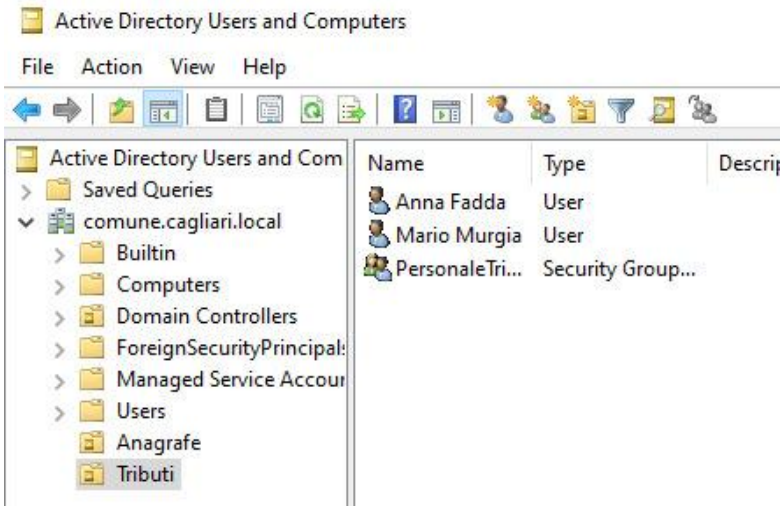
Successivamente, quindi, dopo aver creato la **Foresta**, sono state create 2 **OU** (Organizational Unit), le quali sarebbero **Anagrafe** e **Tributi**, due principali uffici distinti del Comune.
Dentro ciascun OU sono stati creati gli utenti, in questo caso per l'Anagrafe abbiamo:

1) Franco Puddu
2) Gianni Carta



Come si può vedere dallo Screenshot, gli utenti sono stati inseriti all'interno del gruppo **PersonaleAnagrafe**, e assegnati i Permessi, in questo caso si è optato per un **Full Control**, per poi successivamente creare delle Policy che negherebbero l'utilizzo di alcuni programmi o

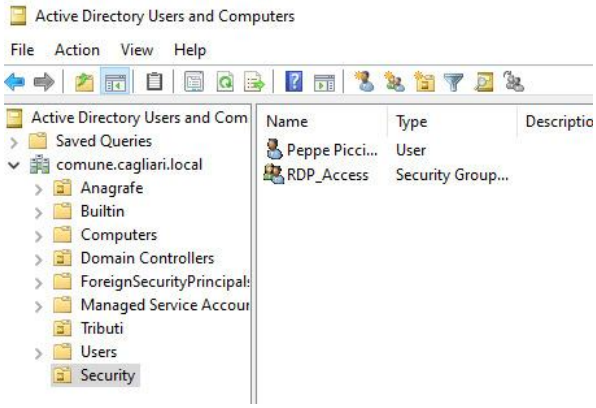
comunque modifiche alle impostazioni che potrebbero comportare un rischio per quanto riguarda la Sicurezza.
La stessa configurazione, sempre con l'accesso Full Control, è stata effettuata per l'OU Tributi.



Anna Fadda e Mario Murgia in questo caso, sono stati quindi aggiunti al gruppo **PersonaleTributi**.

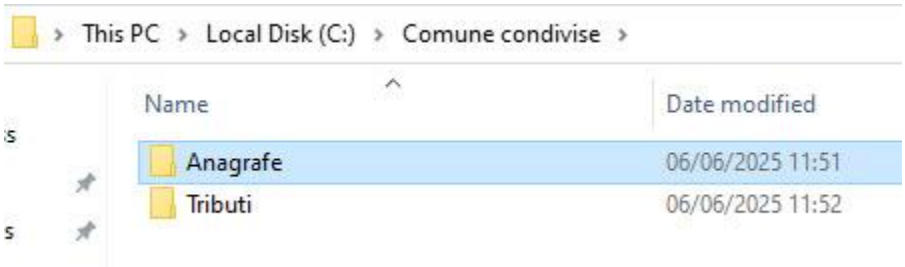
Abbiamo quindi 2 Unità Organizzative distinte, le quali contenenti gli utenti stessi e i gruppi.

E' stato inoltre creata una terza unità organizzativa, la quale servirebbe per la Sicurezza, gestita da Peppe Piccioni.
Ciò comporterebbe una divisione dei permessi più facilitata e l'eventuale gestione del Server possibile solo per quest'ultima OU.
Solo Peppe infatti ha il pieno controllo del Server.



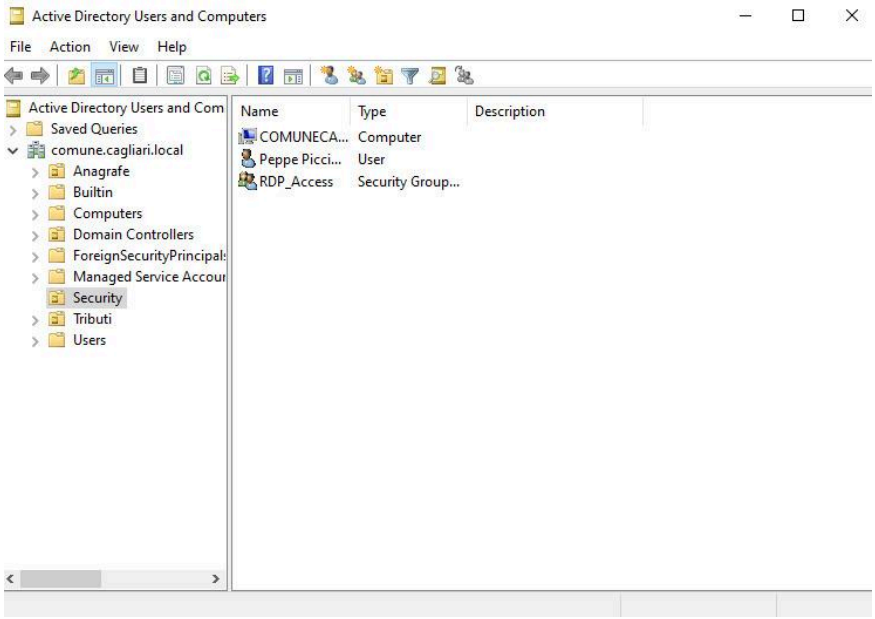
Peppe in questo momento è in pausa caffè quindi spiegherò tra poco con il suo aiuto l'implemento di una questa **OU**.

Creazione delle Cartelle condivise: Una volta configurate le OU, gli user e i gruppi, sono state create delle Cartelle condivise.
Ad ognuna delle Cartelle è stato rimosso **Everyone** e applicato il gruppo di appartenenza, con i permessi in Full Control.
Questo perchè ciascun gruppo può accedere ed operare **solo ed esclusivamente all'interno della Cartella relativa alla propria OU** e per questioni lavorative, è necessario abilitare anche i permessi di execute e write ad ognuno di essi.

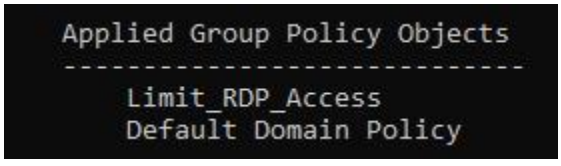


Ad avvenuta prova, Franco ha accesso alla cartella Anagrafe ma non alla cartella Tributi e viceversa con gli utenti della Cartella Tributi.
L'organizzazione in queste infrastrutture è basata principalmente sui permessi.

Gestione delle Policy: Perciò, per quanto detto prima, oltre all'accesso ai File e alle Directory, sono state prese in considerazione anche l'esecuzione di programmi specifici e l'accesso remoto al Server.
Per quanto riguarda quest'ultima, è stata configurata una Policy all'interno della OU stessa, importando anche il **Server Centrale** qui dentro.

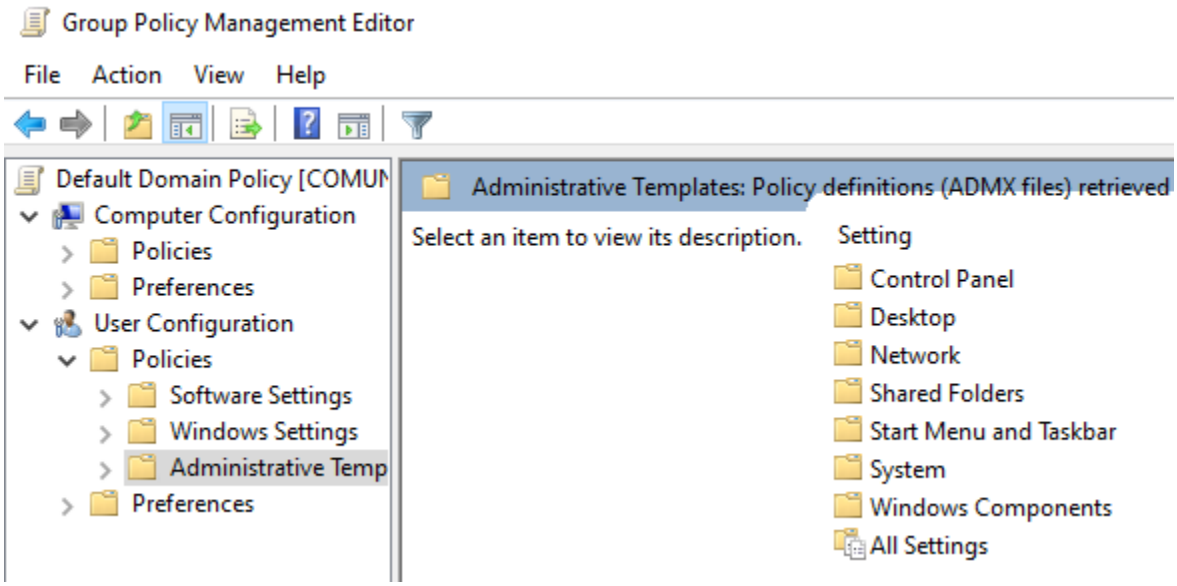


Ciò infatti, darebbe l'accesso al Server solamente a Peppe Piccioni, evitando il Remote Desktop Access indesiderato per evitare intrusioni interne.
Per forzare l'avvio della Policy applicata, è stato eseguito il comando sul cmd del Server **gpupdate /force** e con il corrispondente comando relativo al risultato **gpresult /r** si è confermata l'applicazione.

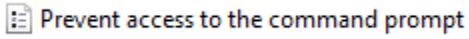


Stessa procedura è stata effettuata per l'esecuzione di programmi specifici, in particolare è stata rimossa l'opzione di aprire il **cmd**, il **Control Panel** e le **Impostazioni di Rete**.

Dopo vari tentativi, sia da **AppLocker**, sia da nuove **GPO** linkate nella OU desiderata, purtroppo falliti, è stato sufficiente applicarli come modifica al **Default Domain Policy**.
Il percorso è stato il seguente:

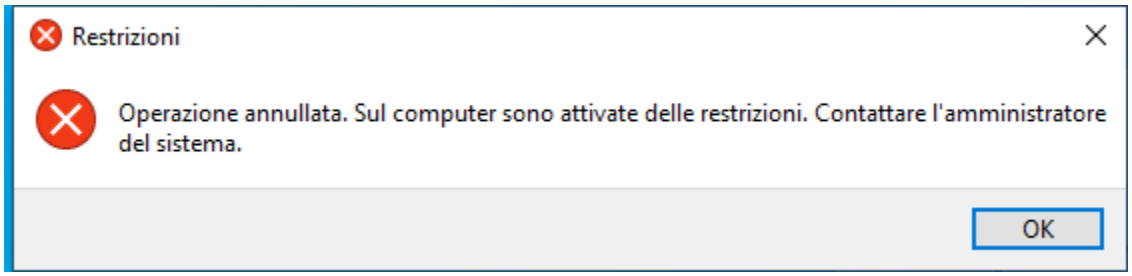


In **System**, è stato bloccato l'accesso al **cmd**:



mentre in **Control Panel**, quello al Pannello di Controllo appunto:

Con il seguente risultato in fase di tentativo di apertura **lato Client**,



E' stata implementata inoltre, una Policy che ridurrebbe il rischio di Malware da parte di **Unità Esterne**, impedendo la scrittura.
Il tutto non è stato testato in quanto la Simulazione è stata effettuata all'interno di una singola Vbox.