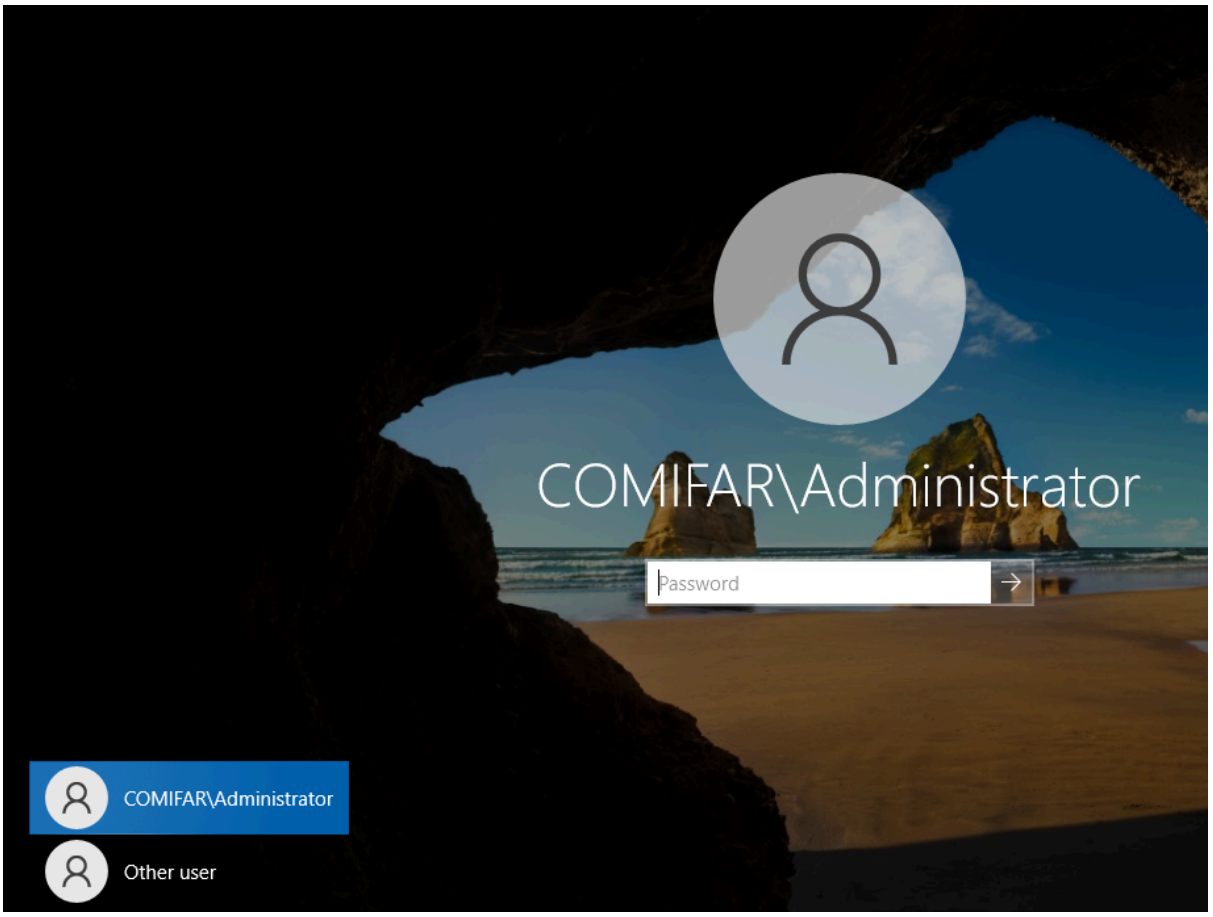
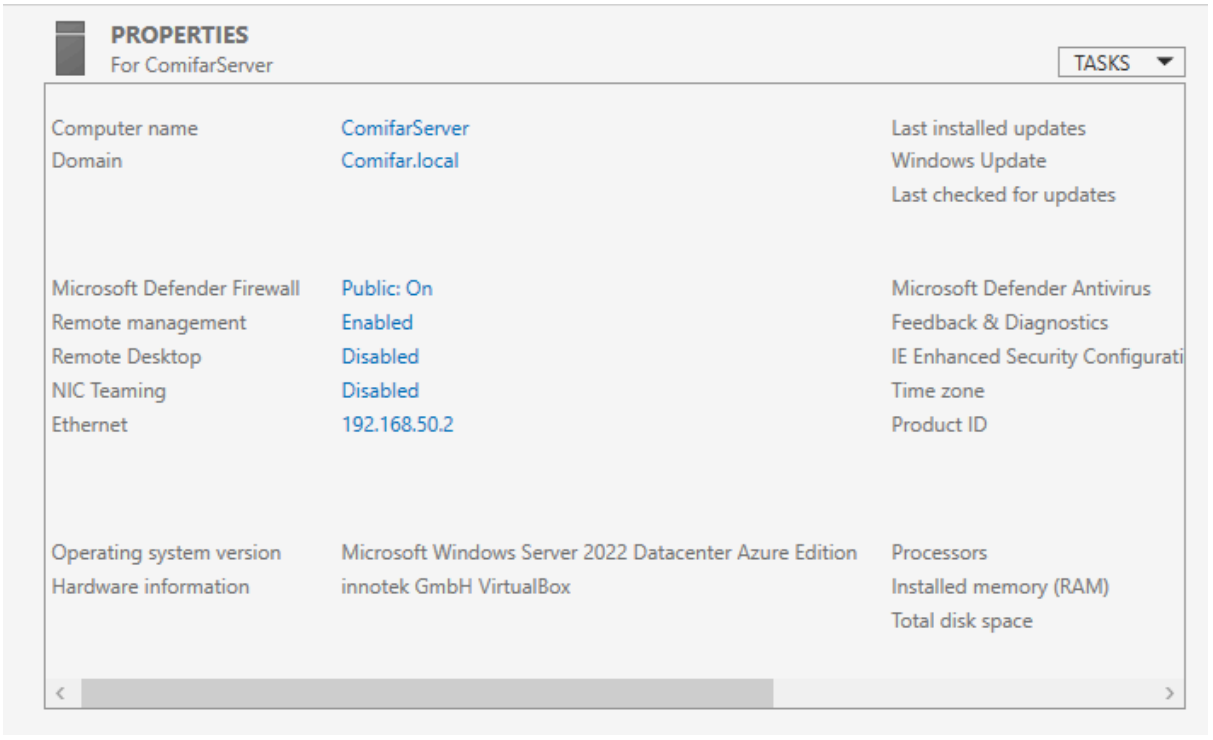
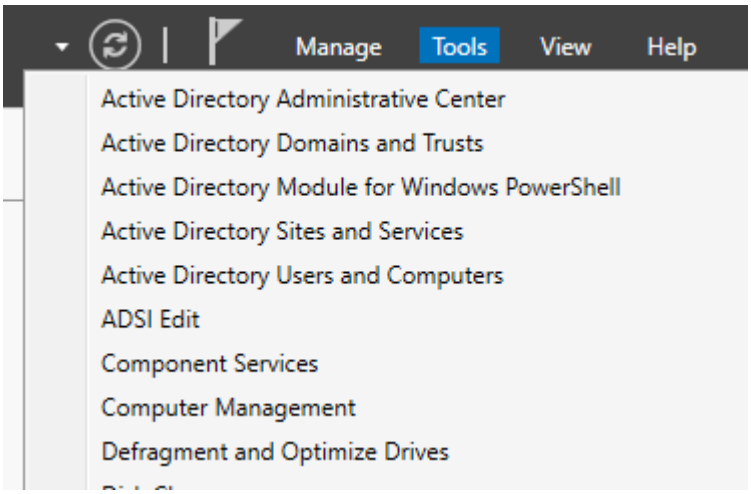
Creazione di Gruppi in Windows Server 2022

Configurato il nostro Windows Server 2022 iniziamo facendo il login come Administrator.

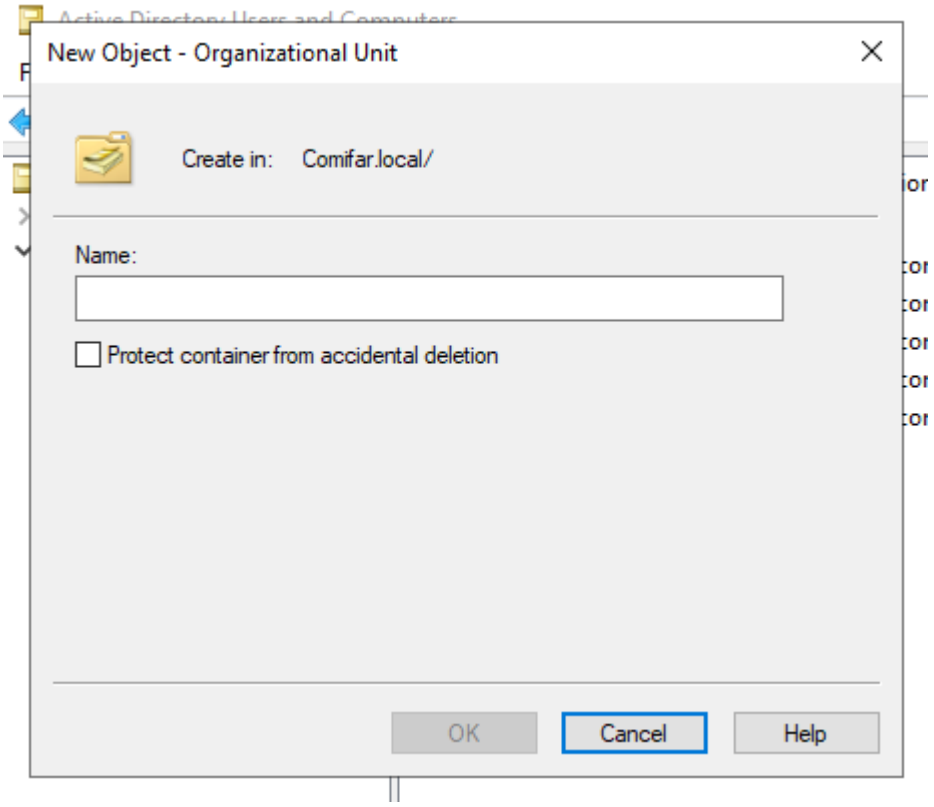




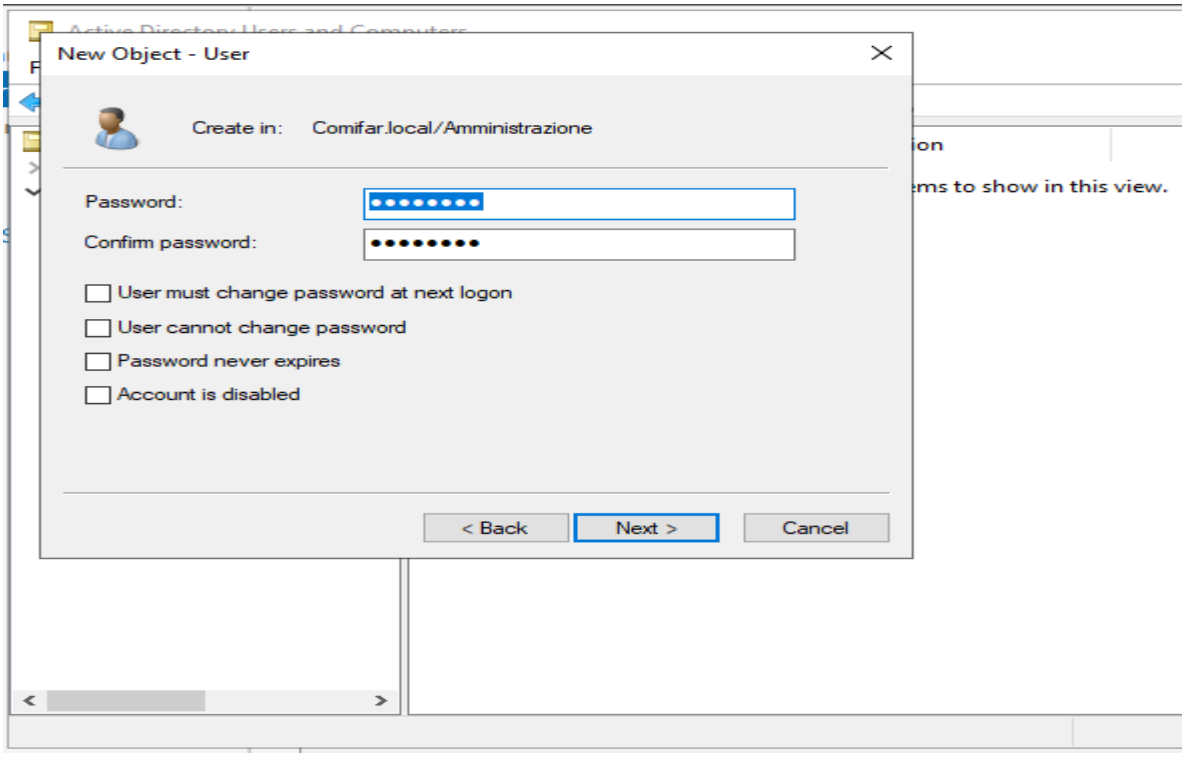
Per creare le cartelle alla quale assegneremo ciascun gruppo/utenti con i relativi permessi, procediamo creando le Organizational Unit.
Nel server manager andiamo su Tools e poi su Active Directory Users and Computers.



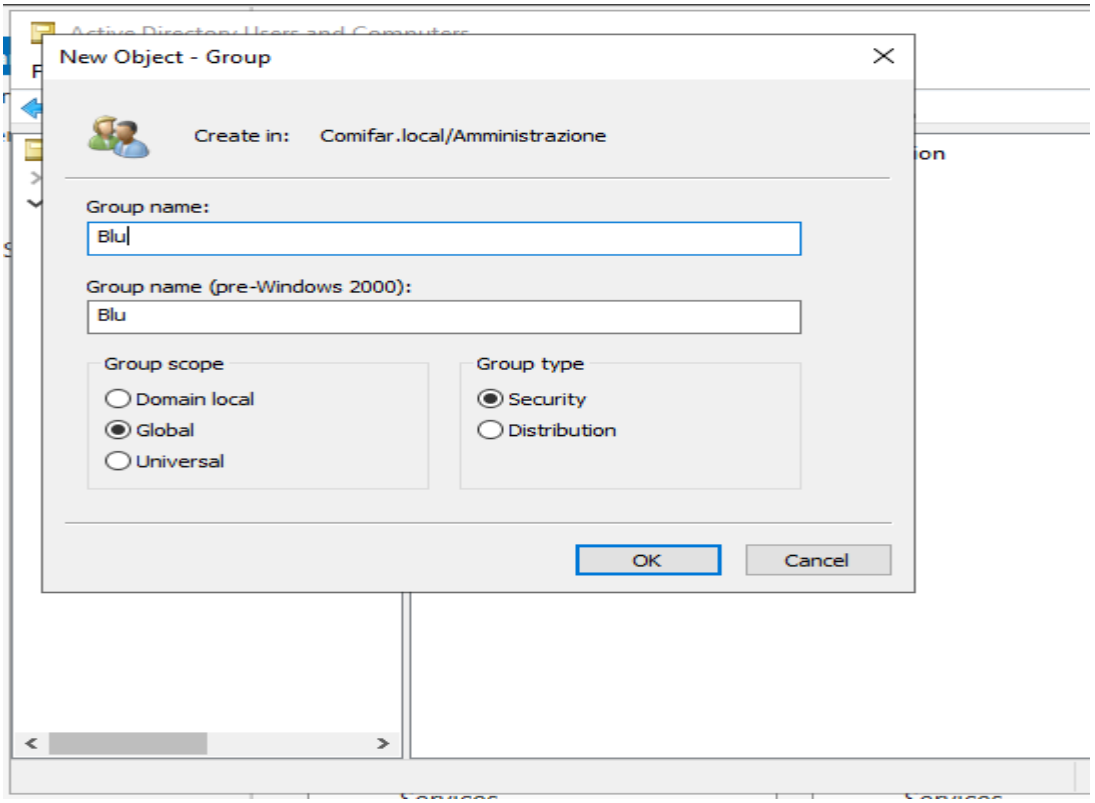
Quindi su Comifar.local con tasto destro faccaimo New, come segue in figura. Facciamo questo procedimento due volte e diamo i nomi Amministrazione e Preposti, nel nostro caso.



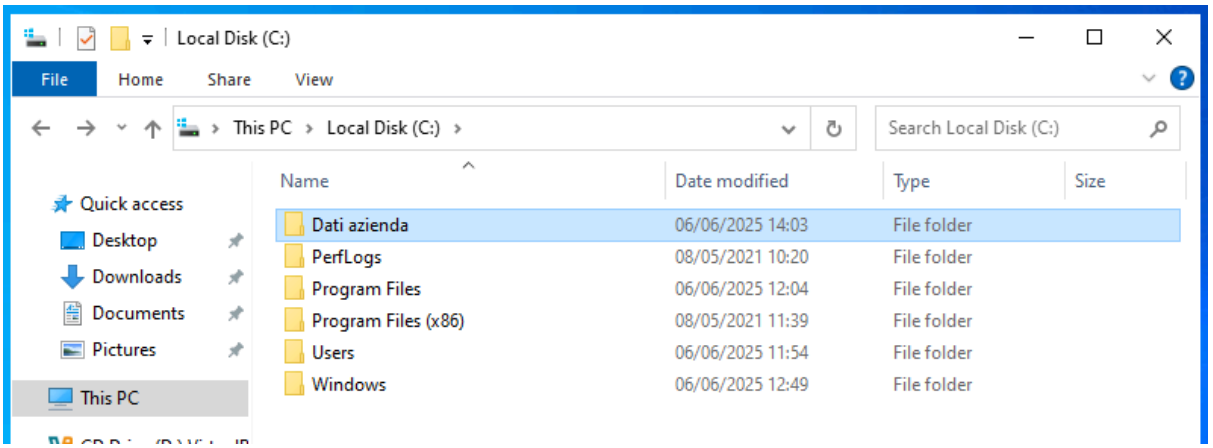
Successivamente all'interno di esse creiamo gli utenti a cui assegneremo nome e password.

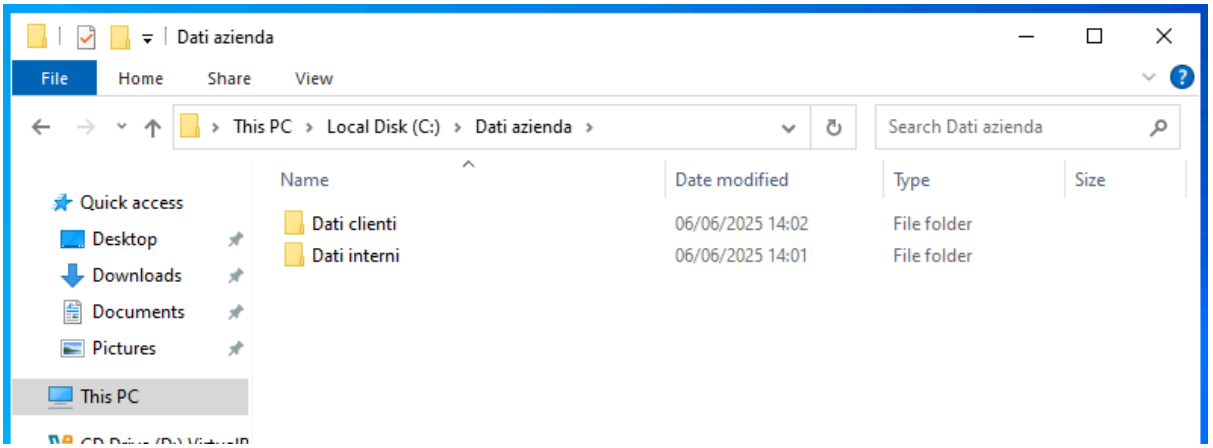


Creati gli utenti li assegniamo al relativo gruppo.

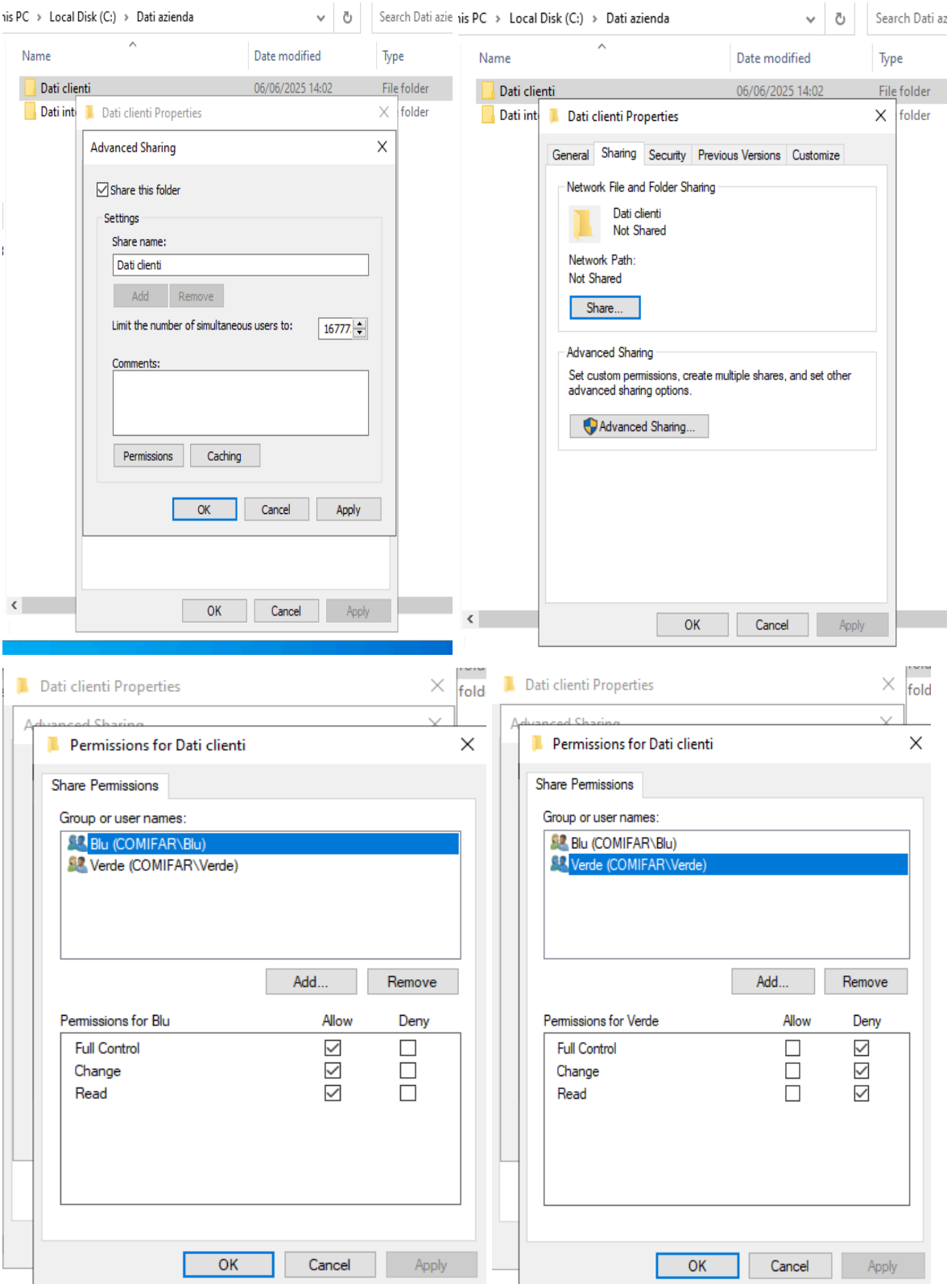


Create le Organization Unit, gli utenti e i gruppi nel disco (C:) creiamo la cartella Dati azienda dove al suo interno creeremo a sua volta altre due cartelle Dati clienti e Dati interni relativi al gruppo Amministrazione (blu) e Preposti (verde).



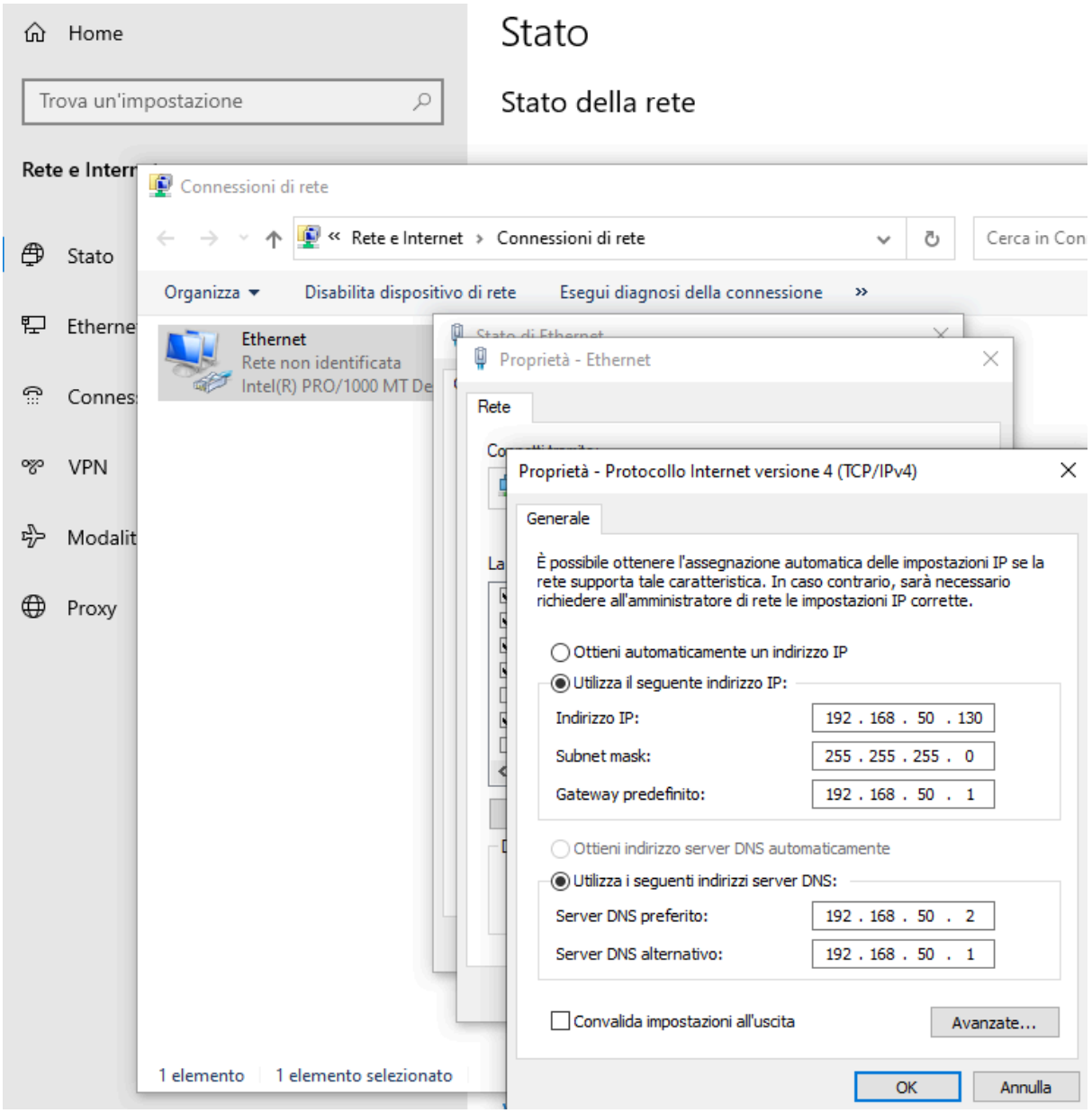


Andiamo a modificare i permessi delle cartelle nelle proprietà.

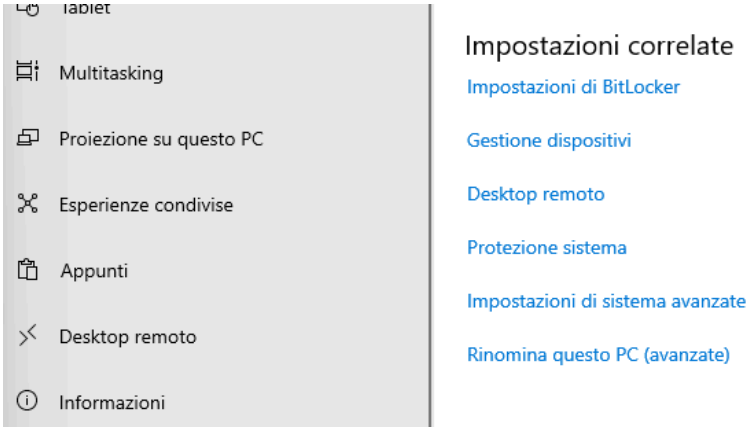


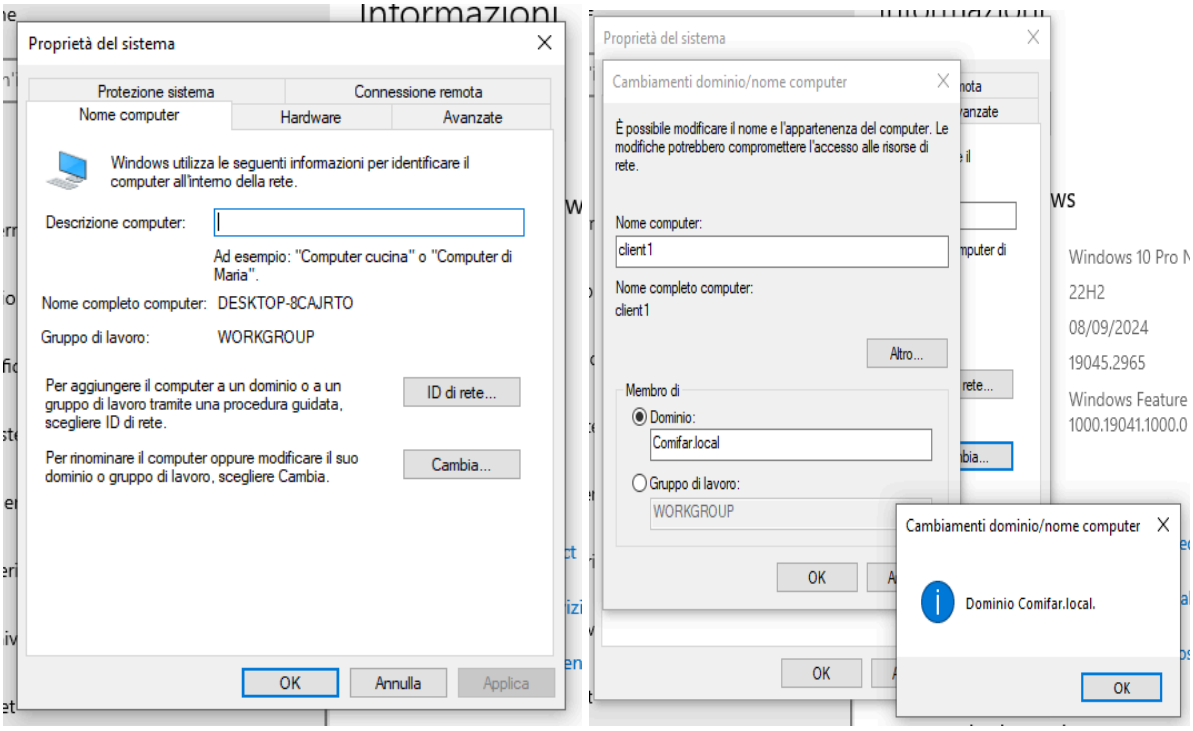
Alla cartella Dati clienti abbiamo dato solo agli amministratori tutti i permessi, ai preposti no, mentre per la cartella Dati interni abbiamo dato sia ad amministratori che preposti i permessi.

Per vedere se questi permessi sono rispettati effettuiamo un accesso remoto al server.
Apriamo un’altra macchina virtuale e configuriamo le impostazioni di rete.

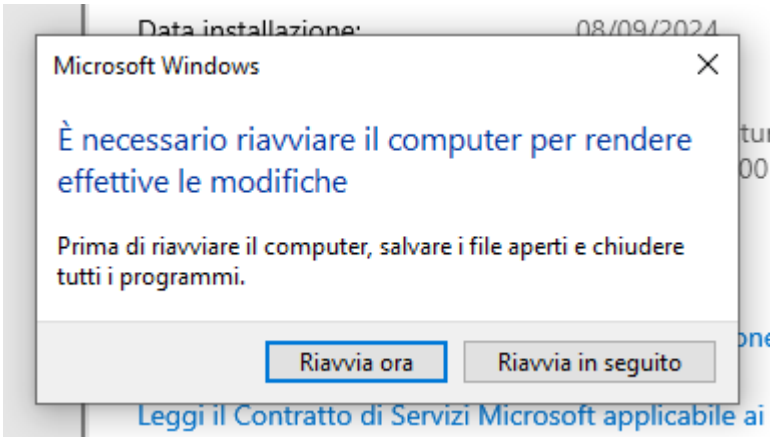


Dalle impostazioni di Windows andiamo su Impostazioni e poi su Impostazioni di sistema avanzate per andare a cambiare dominio.

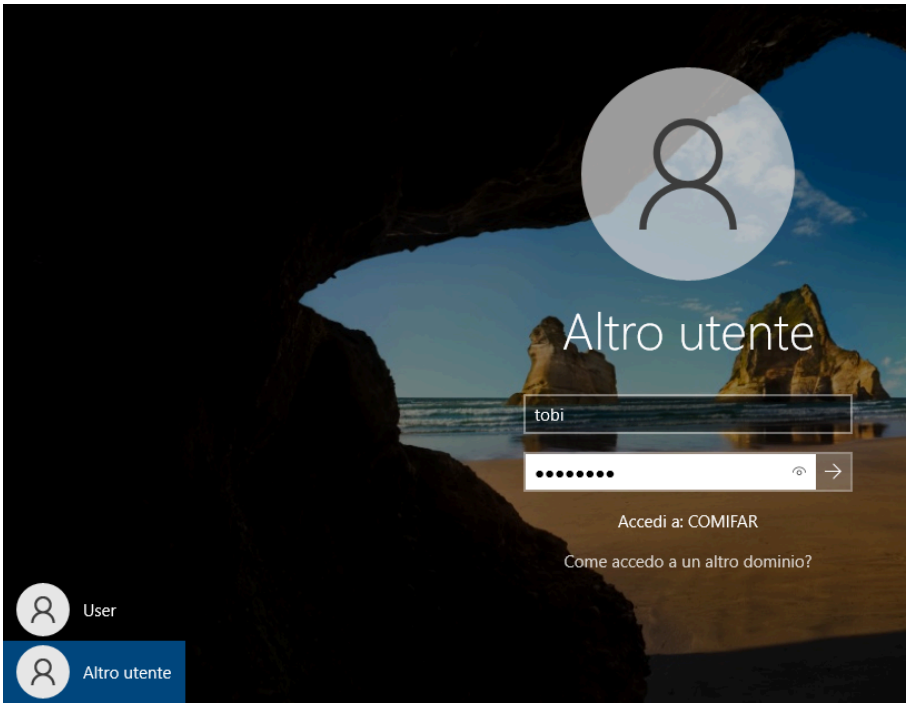


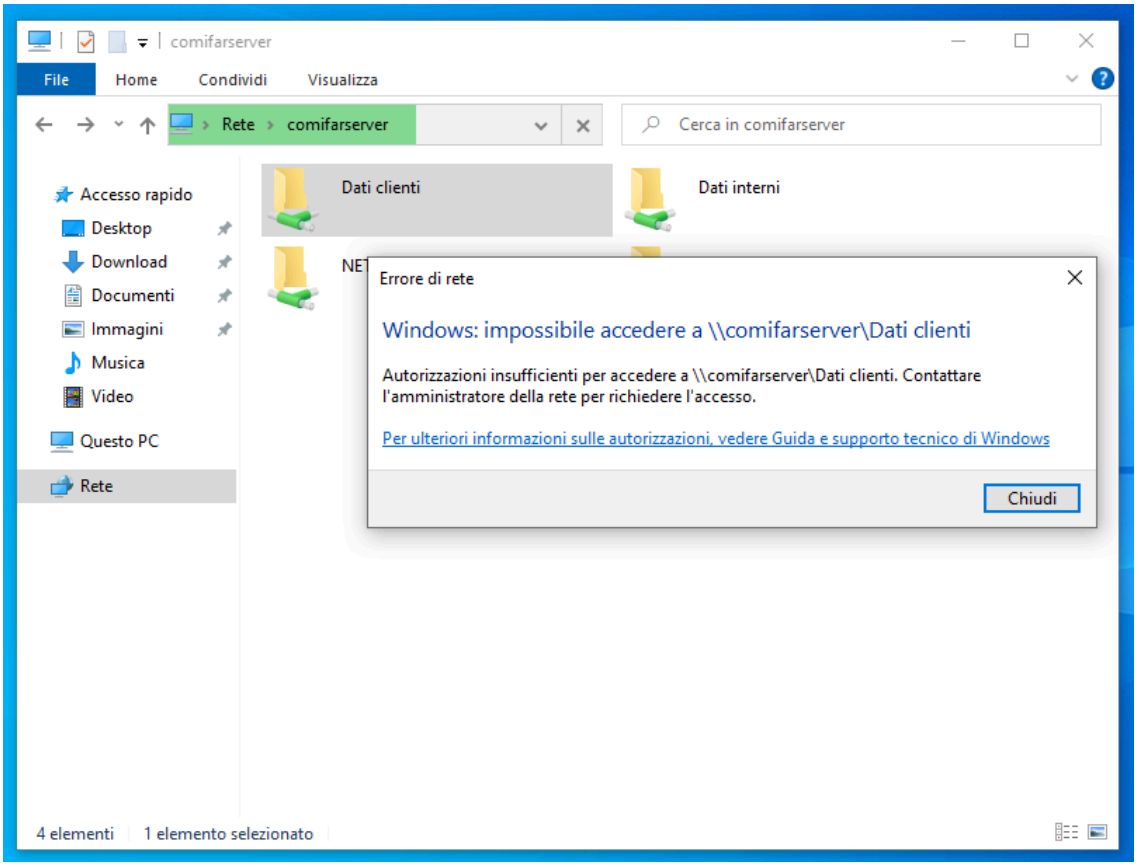


Una volta cambiato farà un riavvio della macchina.



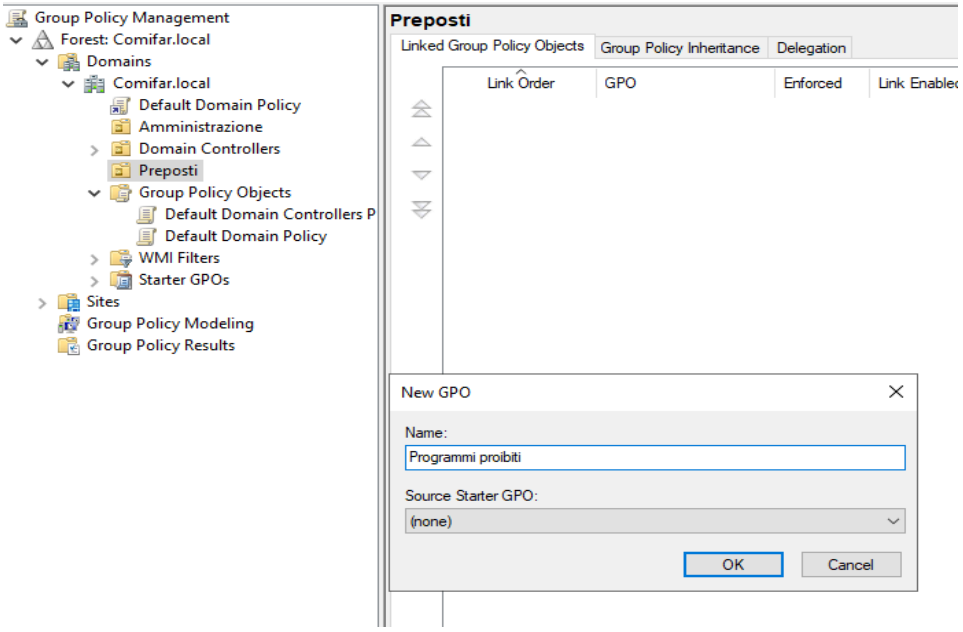
Accediamo con un utente dei Preposti per vedere se i permessi che abbiamo indicato prima sono effettivi.

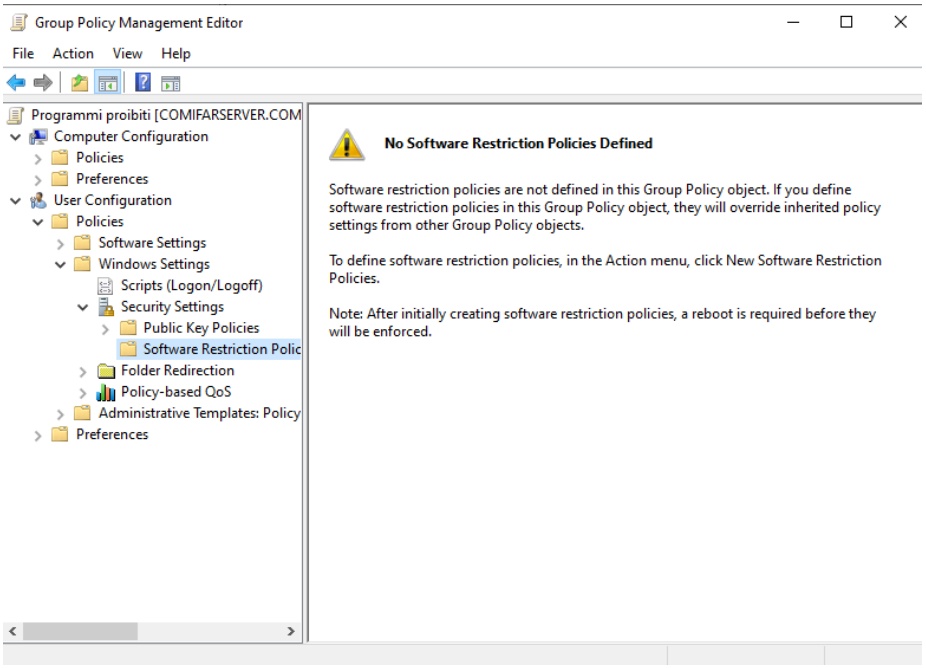




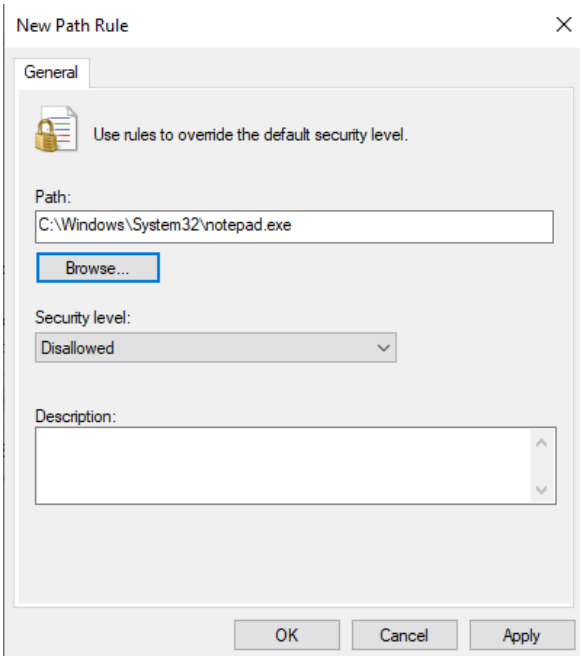
Alla cartella Dati clienti abbiamo dato solo agli amministratori tutti i permessi, ai preposti no, infatti non si riesce ad aprire. Di conseguenza i Dati interni da quest'ultimo sono accessibili e quindi da parte degli amministratori tutte le cartelle sono accessibili.

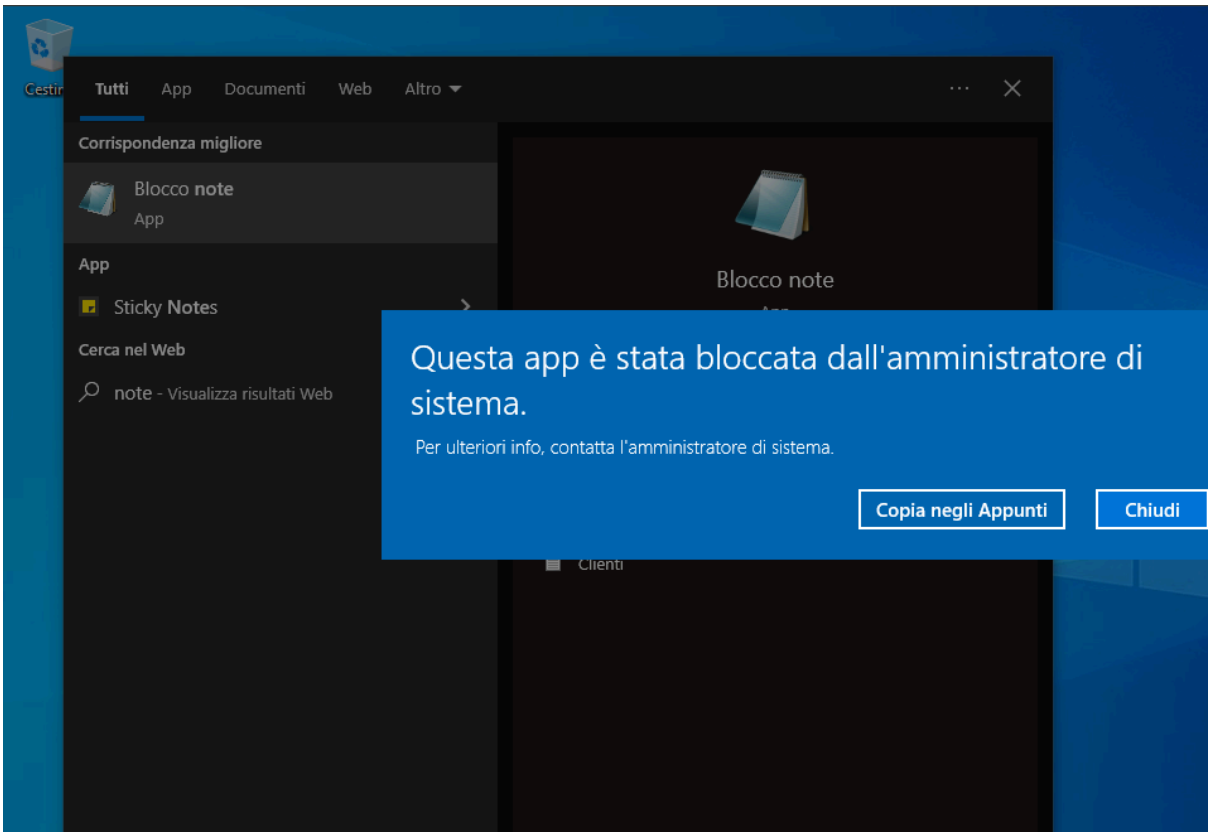
Infine diamo una restrizione al gruppo verde (preposti) inserendo una GPO, con tasto destro e New.





Su Software Restriction Policy aggiungiamo la Path Rule e andiamo a verificare.





L'esercizio di "Creazione di Gruppi in Windows Server 2022" sottolinea l'importanza di una gestione strutturata degli accessi e delle risorse attraverso l'utilizzo di gruppi e l'assegnazione di permessi granulari. Questo approccio non è solo un'utile pratica per la sicurezza informatica, ma offre anche significativi vantaggi operativi e di gestione.

Vantaggi chiave dell'organizzazione del server come suggerito dall'esercizio:

1. Miglioramento della Sicurezza (Principale Vantaggio):

Assegnando permessi specifici a ciascun gruppo (e di conseguenza agli utenti che ne fanno parte), si implementa il principio del minimo privilegio. Questo significa che gli utenti hanno accesso solo alle risorse e alle funzionalità strettamente necessarie per svolgere il proprio lavoro, riducendo drasticamente la superficie di attacco. Se un account utente viene compromesso, il danno potenziale è limitato ai soli permessi assegnati a quel gruppo.

L'esercizio enfatizza l'assegnazione di permessi per "Accesso a file e cartelle", "Esecuzione di programmi specifici", "Modifiche alle impostazioni di sistema" e "Accesso remoto al server". Questa granularità consente di definire con precisione chi può fare cosa, prevenendo accessi non autorizzati o modifiche accidentali/malintenzionate a configurazioni critiche del sistema.

2. Semplificazione della Gestione degli Utenti e dei Permessi:

Invece di dover assegnare permessi individualmente a ogni utente (un compito insostenibile in ambienti con molti utenti), l'organizzazione in gruppi permette di gestire i permessi a livello di gruppo. Quando un utente cambia ruolo o lascia l'organizzazione, è sufficiente spostarlo da un gruppo all'altro o rimuoverlo dal gruppo, e i suoi permessi saranno aggiornati automaticamente.

Questo modello è altamente scalabile. Man mano che l'organizzazione cresce e vengono aggiunti nuovi utenti o dipartimenti, è facile integrarli nei gruppi esistenti o creare nuovi gruppi con set di permessi predefiniti.

3. Coerenza e Riduzione degli Errori:

L'uso dei gruppi promuove la standardizzazione dei permessi all'interno dell'organizzazione. Tutti gli utenti appartenenti a un determinato gruppo avranno lo stesso set di permessi, riducendo la probabilità di configurazioni incoerenti o errori manuali che potrebbero compromettere la sicurezza o la funzionalità.

La documentazione richiesta sui permessi assegnati a ciascun gruppo, con le relative motivazioni, forza la creazione di processi chiari e comprensibili per la gestione degli accessi, facilitando anche l'audit e la conformità.

4. Efficienza Operativa:

Distribuzione Rapida dei Permessi: Quando è necessario concedere un nuovo permesso a un intero dipartimento o a un gruppo di utenti con funzioni simili, è sufficiente modificare i permessi del gruppo corrispondente, anziché intervenire su ogni singolo account utente.

In caso di problemi di accesso, la struttura a gruppi rende più semplice l'identificazione della causa. È possibile verificare rapidamente a quale gruppo appartiene un utente e quali permessi sono stati assegnati a quel gruppo, isolando più facilmente il problema.

5. Facilitazione della Conformità e dell'Audit:

La chiara definizione dei ruoli e dei permessi tramite i gruppi rende molto più semplice dimostrare la conformità a normative interne o esterne (es. GDPR, ISO 27001) che richiedono un controllo stringente sugli accessi ai dati sensibili.

La richiesta di documentazione finale (nomi dei gruppi, permessi assegnati, passaggi eseguiti) è fondamentale per creare un registro completo che può essere utilizzato per audit interni ed esterni, dimostrando che le politiche di sicurezza sono state correttamente implementate e seguite.

Conclusione: L'approccio suggerito dall'esercizio per l'organizzazione del server tramite la creazione di gruppi e l'assegnazione di permessi specifici rappresenta una pietra miliare per qualsiasi ambiente Windows Server 2022. Non solo eleva significativamente il livello di sicurezza riducendo i rischi di accesso non autorizzato, ma ottimizza anche le operazioni IT rendendo la gestione degli utenti e delle risorse più efficiente, scalabile e meno soggetta a errori. Implementare queste pratiche è fondamentale per costruire un'infrastruttura server robusta, sicura e facilmente gestibile.