

WINDOWS SERVER

Traccia: Lo scopo di questo esercizio è di familiarizzare con la gestione dei gruppi di utenti in Windows Server 2022. Imparerai a creare gruppi, assegnare loro permessi specifici e comprendere l'importanza della gestione dei gruppi per la sicurezza e l'amministrazione del sistema

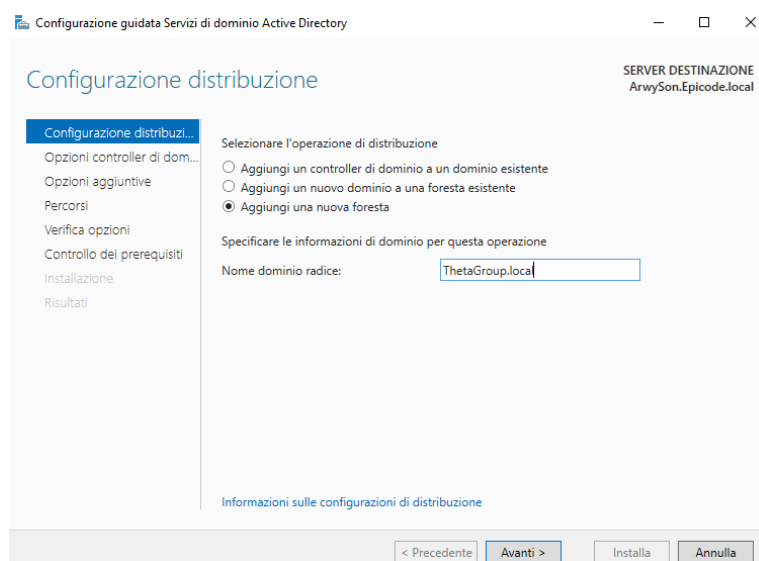
1. Introduzione
2. Preparazione dell'ambiente
3. Creazione dei gruppi
4. Somministrazione dei permessi
5. Accesso agli account e verifica dei permessi
6. Conclusioni

1. Introduzione

Nel progetto odierno si chiede di acquisire familiarità con la gestione dei gruppi di utenti all'interno di Windows Server 2022. La gestione efficace dei gruppi è un aspetto fondamentale per amministrare in modo sicuro ed efficiente un sistema basato su Active Directory, distribuendo permessi ed autorizzazioni ai vari utenti. Attraverso questo esercizio, verranno illustrate le procedure per creare gruppi di utenti, assegnare loro specifici permessi e comprendere come tali configurazioni possano migliorare la sicurezza e facilitare l'amministrazione delle risorse di rete.

2. Preparazione ambiente

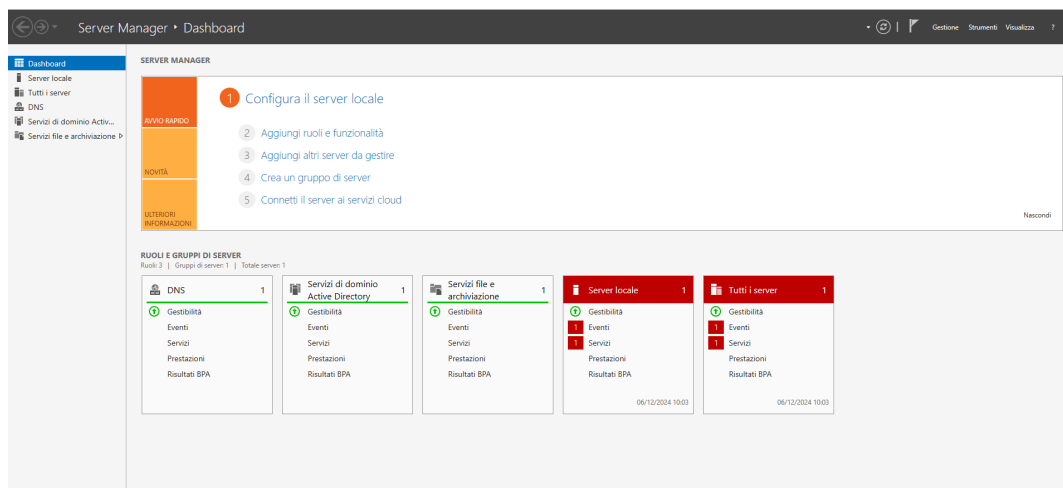
Come primo passaggio, è stata creata una nuova Active Directory con all'interno la sua foresta, per ipotesi appartenente all'azienda Thetha Group. Il dominio di tale foresta si chiamerà *ThetaGroup.local*.



Quando si parla di *Active Directory* (AD) è un servizio di directory sviluppato da Microsoft, utilizzato per organizzare utenti, computer, gruppi ed altre risorse all'interno di una rete, si tratta di uno degli strumenti fondamentali per l'amministrazione di un ambiente Windows Server, consentendo la gestione centralizzata delle risorse e dei servizi in una rete aziendale.

Per *foresta*, si intende il livello più alto dell'infrastruttura logica all'interno di un ambiente Active Directory, si tratta di un insieme di uno o più domini che condividono una struttura comune di directory, ma che possono essere gestiti in modo indipendente. Una foresta rappresenta l'intera Active Directory e fornisce i confini per la gestione di sicurezza, policy e condivisione tra i vari domini.

Una volta creata la nuova foresta, potremo visualizzarla nella dashboard di Server Manager.

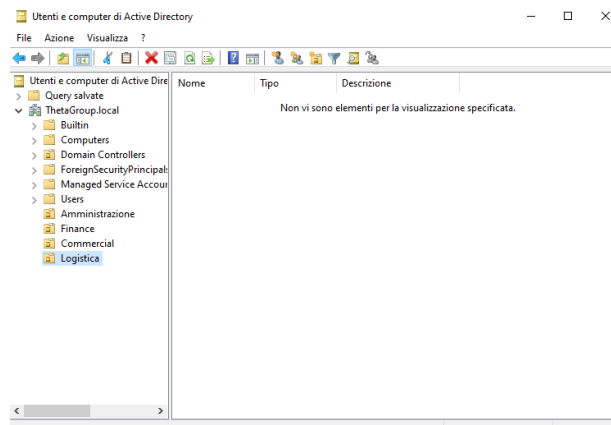


3. Creazione dei Gruppi




Il passo successivo sarà la creazione dei gruppi interni all'organizzazione, procedura importante al fine di assegnare i vari permessi ed autorizzazioni all'accesso di cartelle, file, programmi, impostazioni di sistema o accesso remoto ai server, a seconda dei compiti svolti da ciascun gruppo.




I gruppi che sono stati creati si divideranno in:




- Amministrazione;
- Finance;
- Commercial;
- Logistica.






Nell'immagine precedente sono state create le unità organizzative, nelle quali sono stati aggiunti gli utenti che apparterranno a quella unità. Al suo interno verrà anche creato il gruppo a cui verranno aggiunti gli utenti. Questo tipo di impostazione consente di creare anche più gruppi diversi all'interno di ciascuna unità, in base alle esigenze e struttura della compagnia. Di seguito vedremo la composizione di ciascuna unità nel caso preso in esame, con il relativo gruppo di appartenenza. Per ogni utente è stata inserita l'impostazione che li obbligherà a cambiare password al primo accesso.

Nome	Tipo	Descrizione
 Amministraz...	Gruppo di sicu...	
 Martina Rossi	Utente	
 Sonia Laterza	Utente	

Nome	Tipo	Descrizione
 Filippo Bian...	Utente	
 Paola Verdi	Utente	
 Finance	Gruppo di sicu...	

Nome	Tipo	Descrizione
 Commercial	Gruppo di sicu...	
 Gianni Gialli	Utente	
 Katia Viola	Utente	

Nome	Tipo	Descrizione
 Logistica	Gruppo di sicu...	
 Luca Celeste	Utente	
 Ugo Blu	Utente	

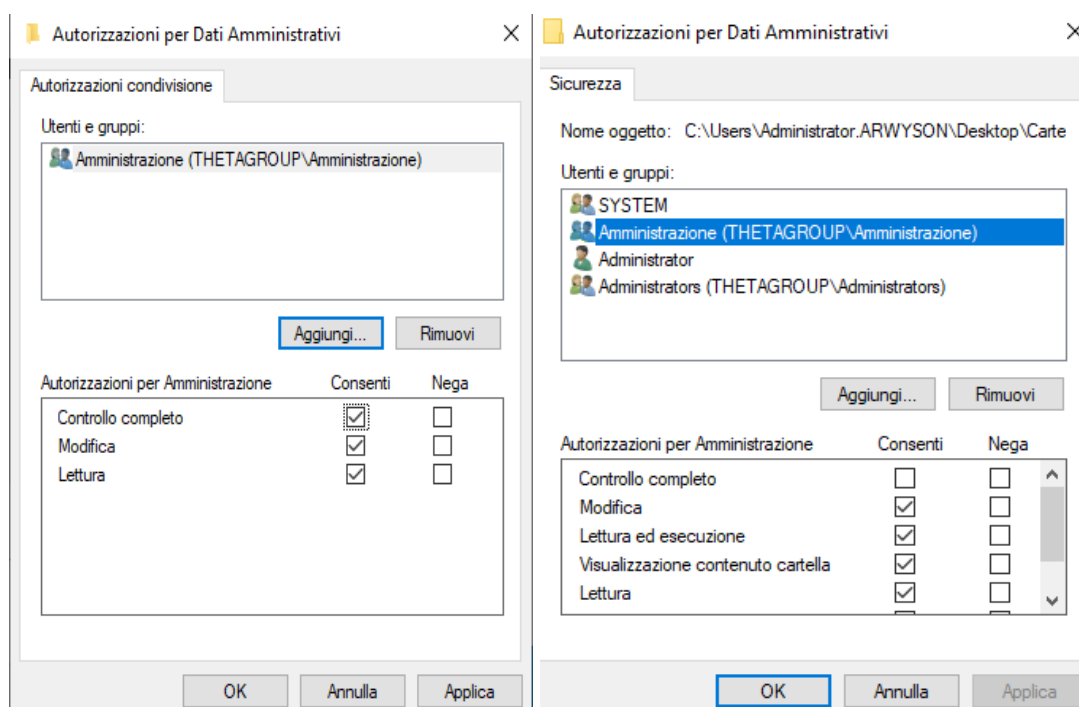
4. Somministrazione dei permessi

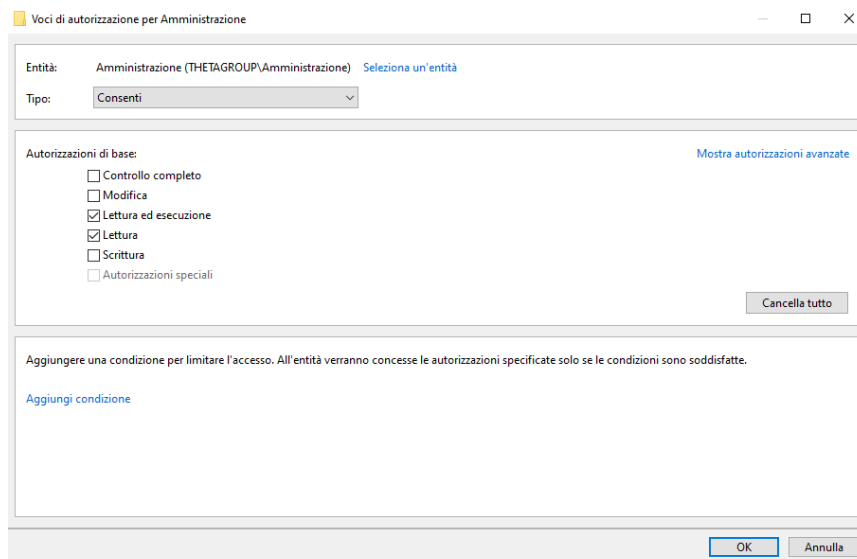
Dopo la creazione dei gruppi, si andrà a creare le cartelle ed i file che saranno condivisi con gli utenti appartenenti al server, andremo a realizzare una cartella sul Desktop nella quale verranno aggiunte, per ogni gruppo, una cartella dedicata, con nomi facilmente riconoscibili. La cartella principale la chiameremo *Cartella Theta Group*. Si dividerà nelle seguenti sotto-cartelle:

- Dati Amministrativi (contenente il file Amministrazione);
- Dati Finance (contenente il file Finance);
- Dati Commercial (contenente il file Commercial);
- Dati Logistica (contenente il file Logistica).

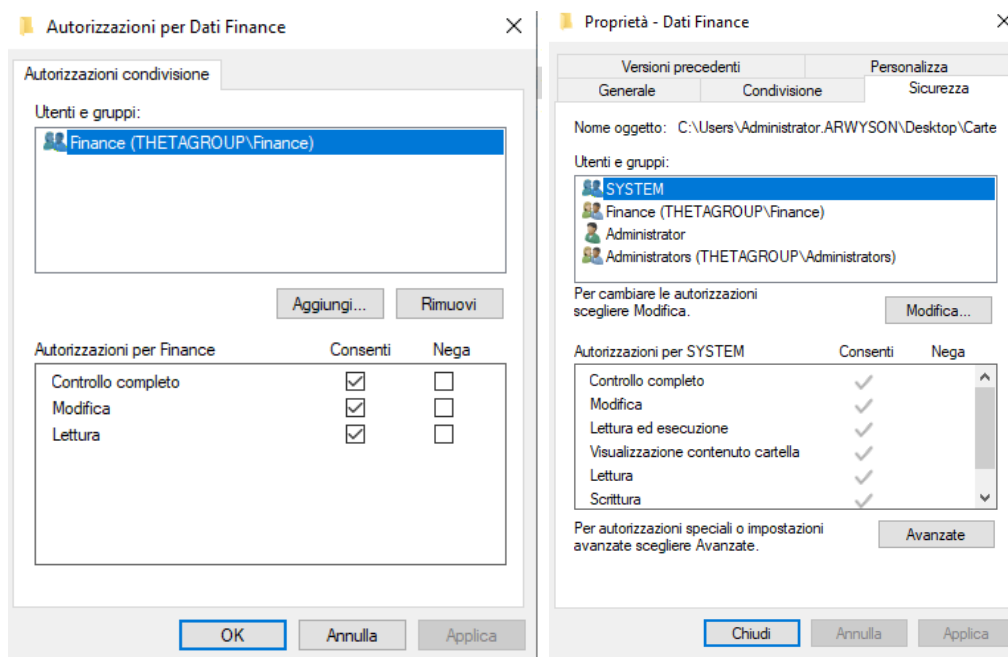
Il passaggio successivo sarà la somministrazione dei permessi per ogni cartella. Come facilmente intuibile, saranno impostati i permessi associando il nome della cartella al nome del gruppo, cliccando su *Proprietà* di ogni cartella, avremo accesso ai permessi di condivisione e di sicurezza.

Di seguito si vedranno come sono stati assegnati i permessi nella cartella Dati Amministrativi e nel relativo file, e nella cartella Finance, facendo due esempi distinti. Nella cartella *Dati Amministrativi* saranno impostati tutti i permessi completi, di lettura e modifica del contenuto, differenziando i permessi del file, il quale avrà permessi di sola lettura da parte degli utenti del gruppo. Tale permesso serve nel caso non si volesse far manomettere i file dagli utenti di quel gruppo.





Per la cartella *Dati Finance* invece lasceremo accesso completo alla cartella e, per estensione automatica, ai file, permettendo sia lettura che modifica. Tali permessi hanno la funzione di permettere agli utenti la modifica di tali file, qualora fosse necessario.

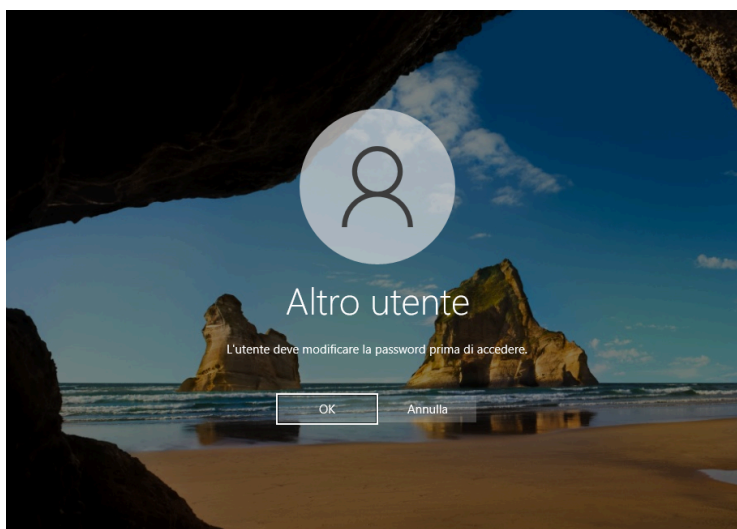


I permessi dati agli altri gruppi, saranno gli stessi dati al gruppo Finance.

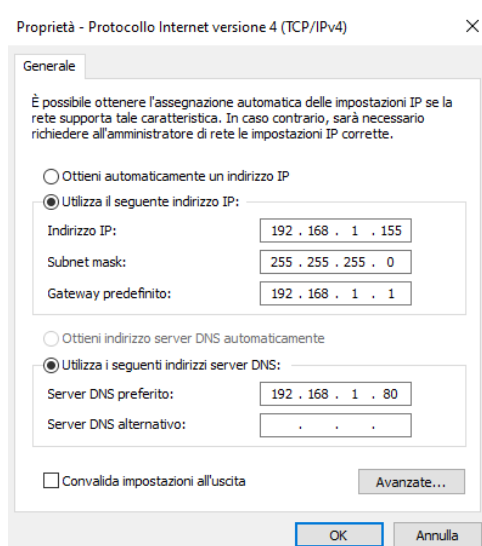
5. Accesso agli account degli utenti e verifica del funzionamento dei permessi

Per poter accedere agli account appena creati, come accennato precedentemente, sarà necessaria la modifica della password.

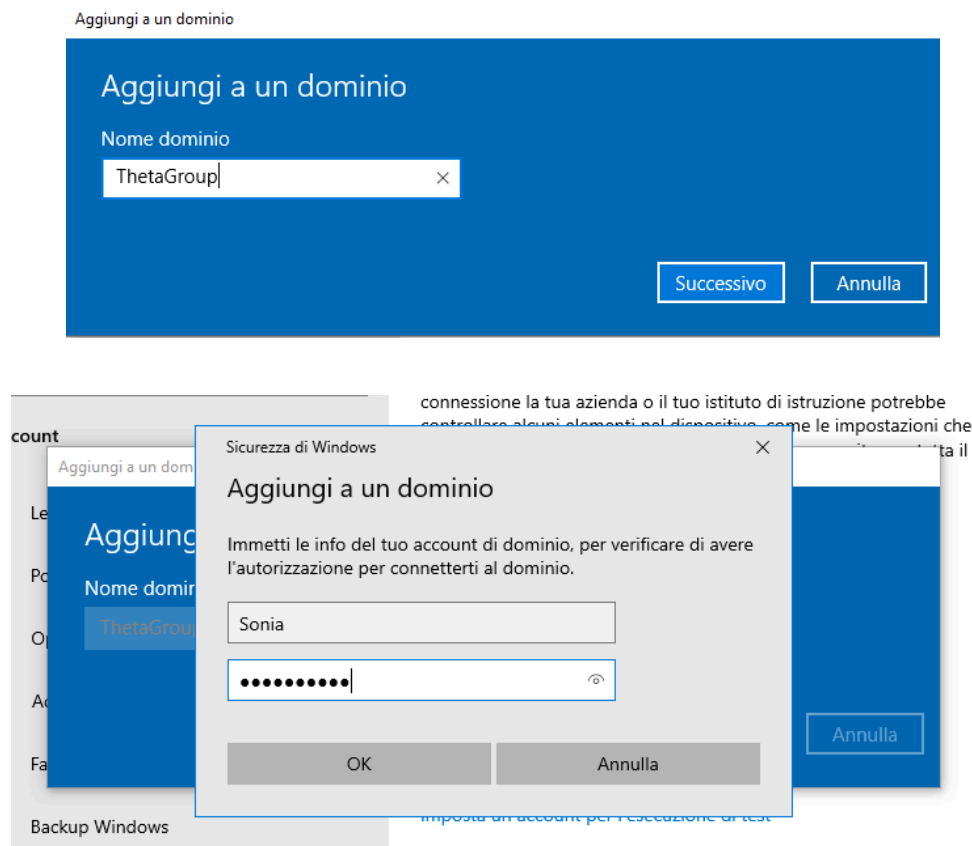
Verrà eseguita la disconnessione da Windows Server per poi accedere da un altro account, inserendo il nome designato all'interno del Server Manager.



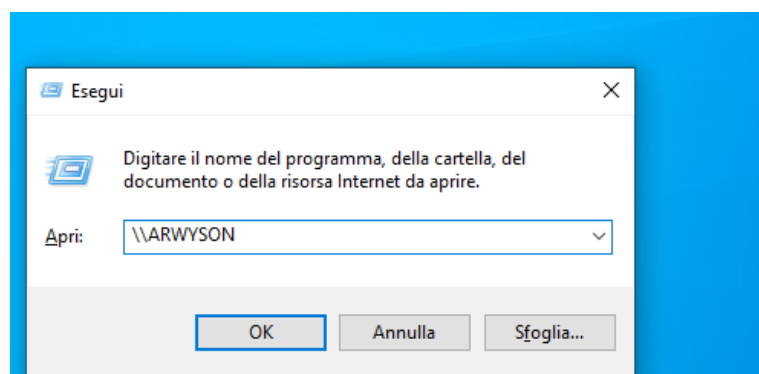
Una volta eseguito questo passaggio, l'account è attivo, e potrà essere inserito all'interno della macchina Windows 10 Pro. Per farlo per prima cosa si dovrà impostare la macchina sulla stessa rete del Server utilizzando l'IP del Server stesso come DNS. L'indirizzo IP della macchina Windows 10 Pro dovrà essere statico, quindi affidato manualmente per scongiurare eventuali cambiamenti automatici.

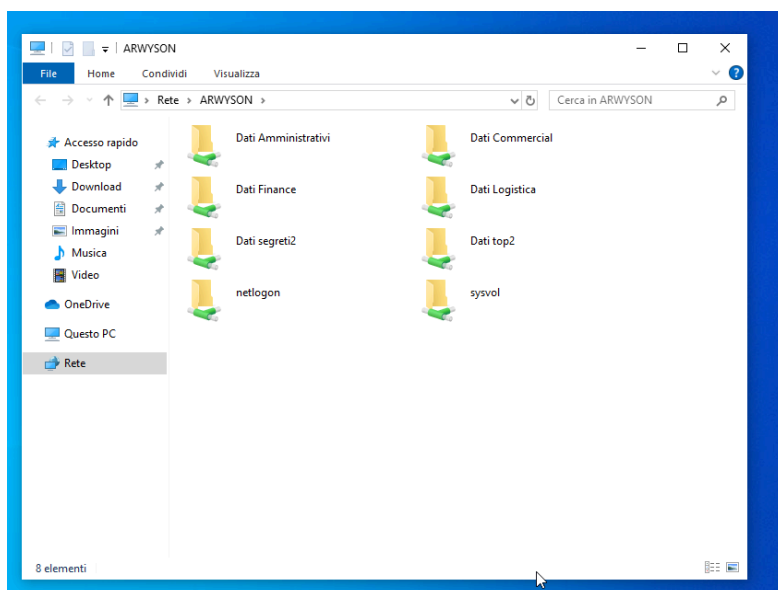


Dopodichè dovremo effettuare la ricerca del Dominio della foresta creata all'inizio dell'esercizio.



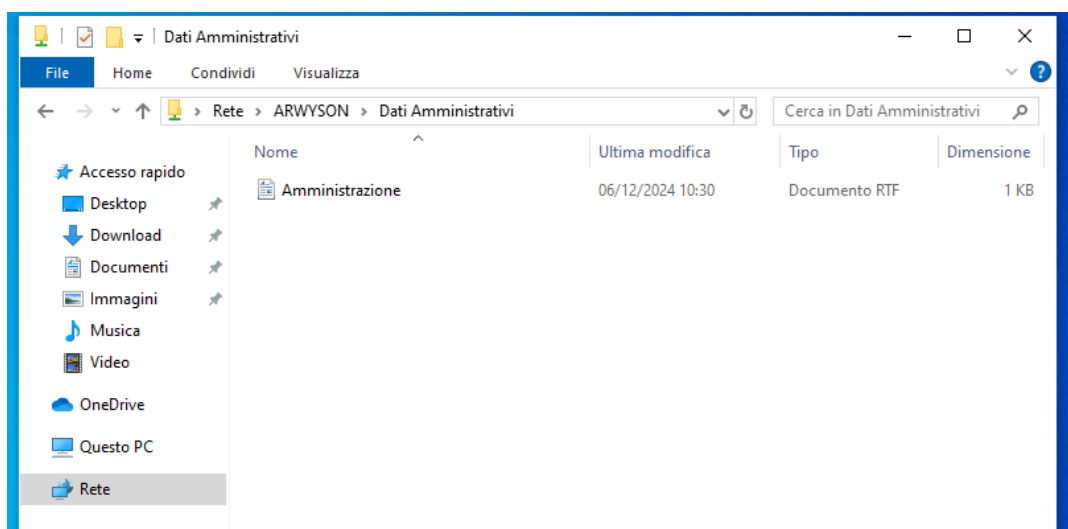
Dopo che saranno stati inseriti i dati dell'account interessato, la macchina si riavvierà per aggiungerlo al suo avvio in maniera da consentire l'accesso al Server. Una volta all'interno, andremo alla ricerca del Server scrivendo \\<<Nome_server>> per accedere alle cartelle condivise.



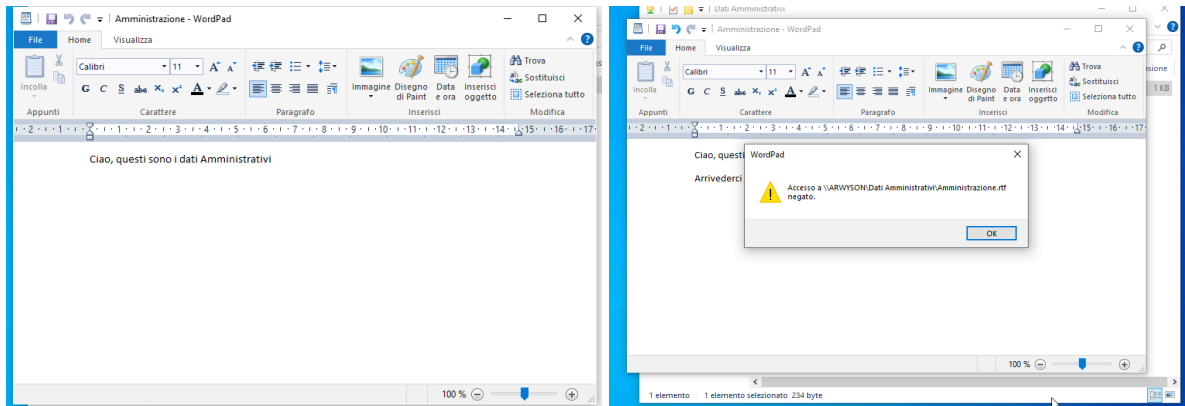


Finalmente sarà possibile visualizzare le cartelle condivise sul Desktop del Server. Ora si andrà ad eseguire i test di accessibilità dei dati, per verificare che le impostazioni siano state messe in maniera corretta e se gli account si comportano seguendo le regole assegnate.

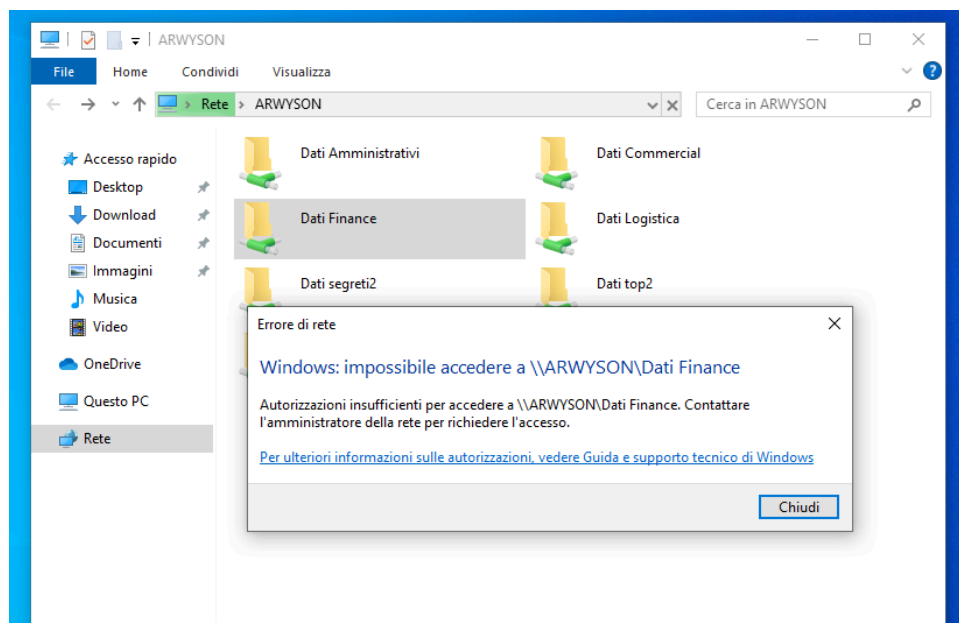
Per prima cosa si è proceduto col controllo di accesso sulla cartella Dati Amministrativi, di cui l'utente selezionato fa parte. Come si può vedere nell'immagine seguente, il file al suo interno sarà visibile, quindi l'accesso viene eseguito con successo.



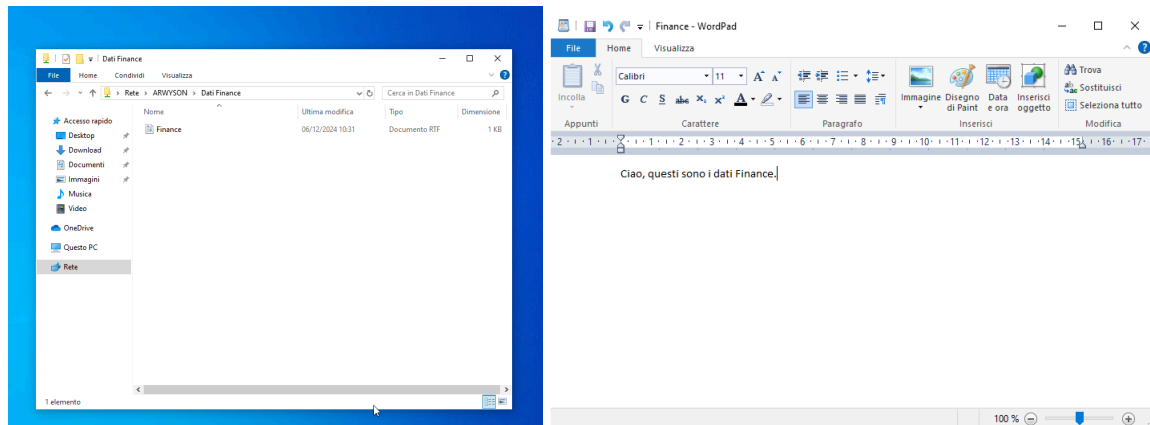
Di seguito si è andato a verificare che sia possibile la lettura del file, ma non la modifica. Aprendo il file e tentando di modificarlo, questo è ciò che avverrà, l'output che restituirà dopo la modifica sarà un messaggio di errore. Ciò dimostra che le impostazioni accennate precedentemente sono state inserite in maniera corretta.



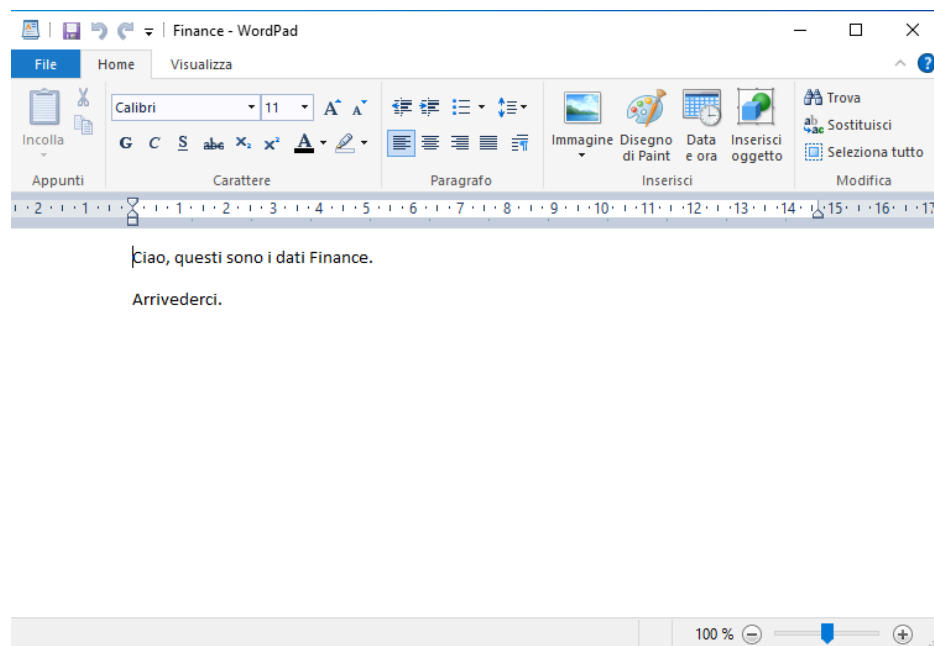
Per verificare che anche le altre impostazioni siano state messe correttamente, si farà la prova di apertura delle cartelle senza permessi di accesso per gli utenti appartenenti all'Amministrazione. Il messaggio restituito sarà un messaggio d'errore, ancora a conferma delle impostazioni inserite.



Per eseguire una ulteriore prova, si è provato ad accedere con un utente appartenente al gruppo Finance, il quale avrà come permessi completi di lettura e modifica solo quelli appartenenti alla propria cartella. Come possiamo notare, tutto viene aperto correttamente.



Per verificare che la modifica ai file sia abilitata, si andrà a modificare e salvare il file, il quale, questa volta, non mostrerà messaggi d'errore, come da permessi impostati.



6. Conclusioni

Attraverso questo esercizio è stato possibile comprendere l'importanza della gestione centralizzata degli utenti e dei gruppi in un ambiente Windows Server 2022 basato su Active Directory.

La creazione di gruppi organizzati in base ai reparti aziendali, come Amministrazione, Finance, Commercial e Logistica, ha consentito di definire in modo chiaro e strutturato i permessi e le autorizzazioni per ciascun gruppo. Questo approccio ha dimostrato come la gestione dei gruppi semplifichi l'amministrazione delle risorse, garantendo un controllo sicuro e preciso sull'accesso a file e cartelle. L'esercizio ha messo in evidenza come la configurazione corretta dei permessi sia fondamentale per prevenire accessi non autorizzati e mantenere l'integrità delle informazioni aziendali. I test effettuati hanno confermato che le impostazioni applicate sono state implementate con successo, rispettando le regole di accesso predefinite per ciascun gruppo. Inoltre, l'integrazione degli account utente in un ambiente Windows 10 Pro ha dimostrato la flessibilità e l'efficacia dell'infrastruttura basata su Active Directory nel gestire utenti e risorse distribuite.

In conclusione, questo progetto ha fornito un'esperienza pratica sulla configurazione e gestione degli utenti in un ambiente aziendale, rafforzando la comprensione dell'architettura e delle funzionalità di Active Directory, nonché l'importanza della sicurezza nell'amministrazione dei sistemi IT.

*Progetto a cura di
Sonia Laterza*