S10-L5
Windows server

Emanuele Benedetti | 14 febbraio 2025

Consegna

Obiettivo

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.

Istruzioni

1. Preparazione
    - Accedi al tuo ambiente Windows Server 2022
    - Assicurati di avere i permessi amministrativi necessari per creare e gestire gruppi
2. Creazione dei gruppi
    - Crea due gruppi distinti. Puoi scegliere i nomi che preferisci per questi gruppi, ma assicurati che i nomi siano significativi per riflettere la loro funzione o ruolo all'interno dell'organizzazione (ad esempio, "Amministratori", "UtentiStandard", "MarketingTeam", "Sviluppatori", ecc.).

3. Assegnazione dei permessi
    - Per ogni gruppo, assegna permessi specifici. Puoi scegliere quali permessi concedere, ma assicurati di considerare i seguenti aspetti:
        - Accesso ai file e alle cartelle
        - Esecuzione di programmi specifici
        - Modifiche alle impostazioni di sistema
        - Accesso remoto al server
    - Documenta i permessi assegnati a ciascun gruppo, spiegando perché hai scelto tali permessi

4. Verifica
    - Una volta creati i gruppi e assegnati i permessi, verifica che le impostazioni siano corrette. Puoi farlo:
        - Creando utenti di prova e aggiungendoli ai gruppi
        - Verificando che gli utenti abbiano i permessi assegnati in base al gruppo a cui appartengono
        - Verificare che gli altri utenti non possano accedere

5. Documentazione
    - Scrivi un breve report che includa:
        - I nomi dei gruppi creati
        - I permessi assegnati a ciascun gruppo
        - I passaggi seguiti per creare e configurare i gruppi
        - Eventuali problemi riscontrati e come li hai risolti

Svolgimento

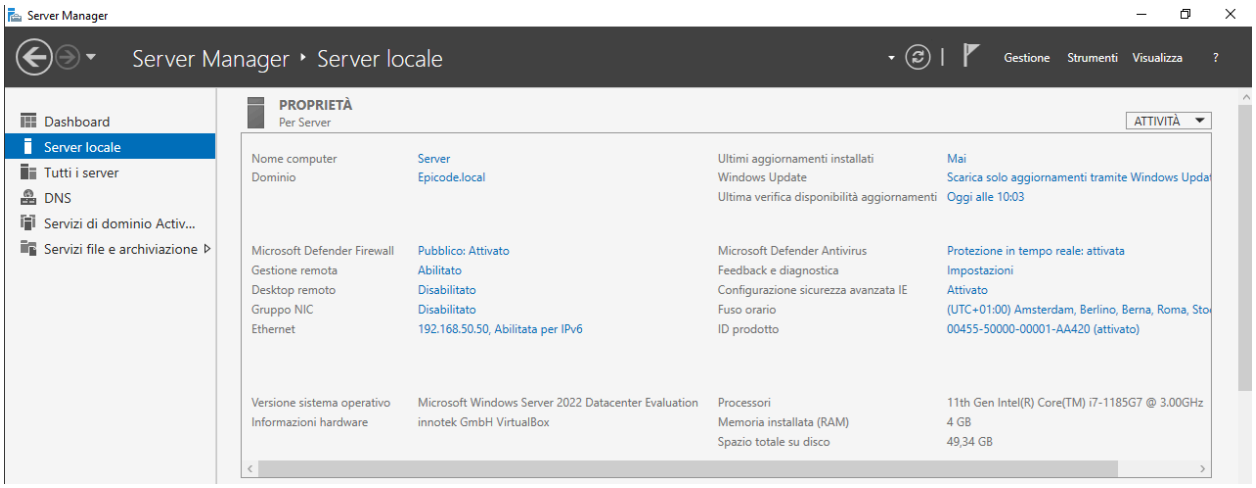
Nel laboratorio di oggi ho utilizzato due macchine virtuali per svolgere quanto richiesto dalla consegna: la prima macchina Windows Server 2022 per gestire i gruppi del dominio e una macchina Windows 10 Pro per l'accesso degli utenti.

Configurazione delle macchine

Ho iniziato il laboratorio impostando le connessioni di rete delle due macchine. Ho assegnato l'indirizzo IP 192.168.50.50/24 staticamente in modo tale da poterlo rendere sempre accessibile dallo stesso indirizzo.

Alla macchina Windows 10 Pro ho assegnato manualmente l'indirizzo 192.168.50.51/24 e impostato l'indirizzo IP del server come server DNS predefinito. Questo passaggio è fondamentale perché ci permette di aggiungere l'host al dominio del server.

Nello screenshot di seguito viene mostrata la configurazione del server



Come si può vedere l'indirizzo IP corrisponde a quello assegnato in precedenza ed è stato creato il dominio *Epicode.local* a cui verranno collegati gli utenti della macchina WIndows 10 PRO.

Dopo aver configurato la macchina host, ho eseguito *ipconfig -all* nel prompt dei comandi per verificare la configurazione di rete completa.

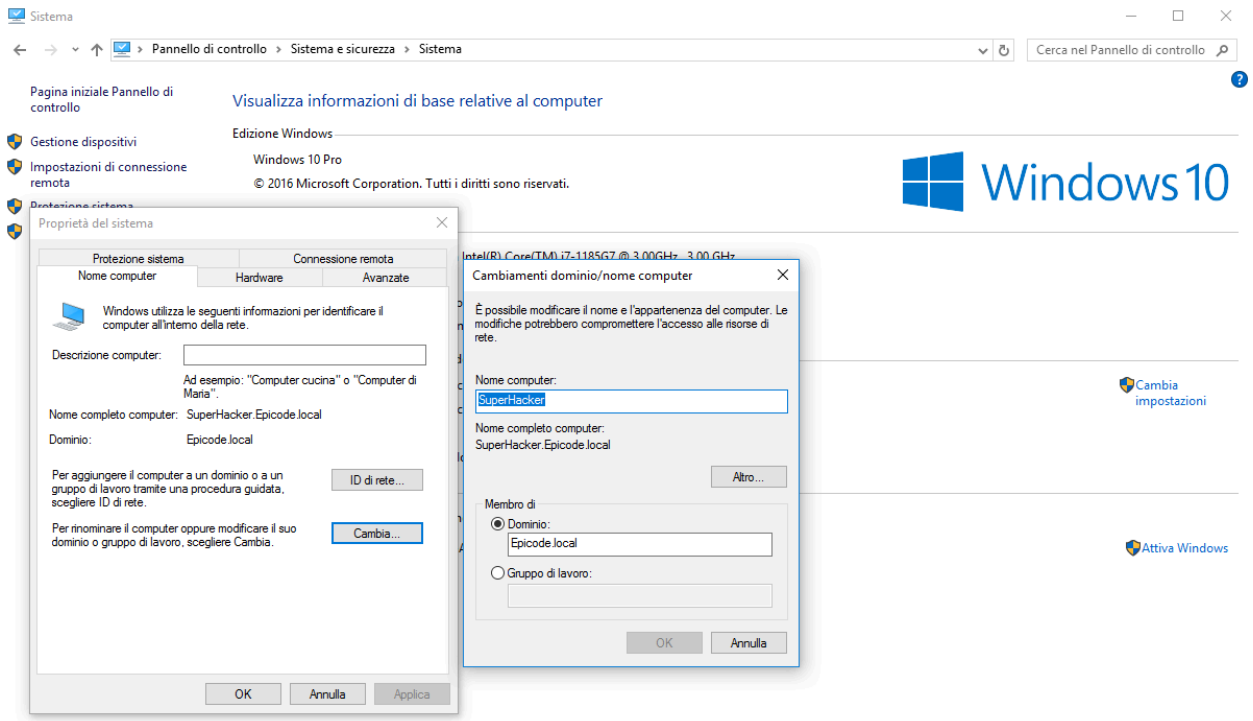
```
Scheda Ethernet Ethernet:

   Suffisso DNS specifico per connessione:
   Descrizione . . . . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Indirizzo fisico. . . . . . . . . . . . : 08-00-27-39-8D-D1
   DHCP abilitato. . . . . . . . . . . . . : No
   Configurazione automatica abilitata   : Sì
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::2de8:52:36ce:2432%12(Preferenziale)
   Indirizzo IPv4. . . . . . . . . . . . . : 192.168.50.51(Preferenziale)
   Subnet mask . . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . . :
   IAID DHCPv6 . . . . . . . . . . . . . . : 50855975
   DUID Client DHCPv6. . . . . . . . . . . : 00-01-00-01-2F-3E-3D-07-08-00-27-39-8D-D1
   Server DNS . . . . . . . . . . . . . . .  : 192.168.50.50
   NetBIOS su TCP/IP . . . . . . . . . . . . : Attivato
```

Aggiungiamo ora il computer host al dominio *Epicode.local* del server.

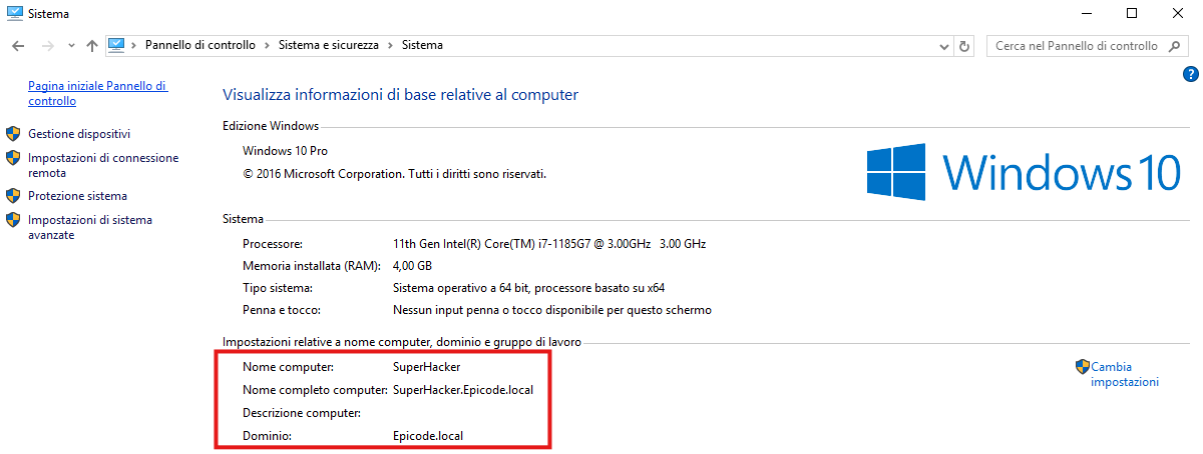
Per aggiungere il dominio andiamo su *Pannello di controllo* > *Sistema e sicurezza* > *Sistema* > *Cambia impostazioni*. Nella finestra che si apre scegliamo la voce *Cambia…*

Scegliamo quindi il nome del computer, se lo vogliamo modificare e impostiamo il dominio sulla base di quello creato nel server, in questo caso *Epicode.local*



L’immagine mostra la corretta configurazione descritta. Salviamo le nuove impostazioni e attendiamo il riavvio della macchina.

Al riavvio possiamo verificare che la modifica abbia avuto successo tornando nelle impostazioni e verificando che il dispositivo appartenga al dominio

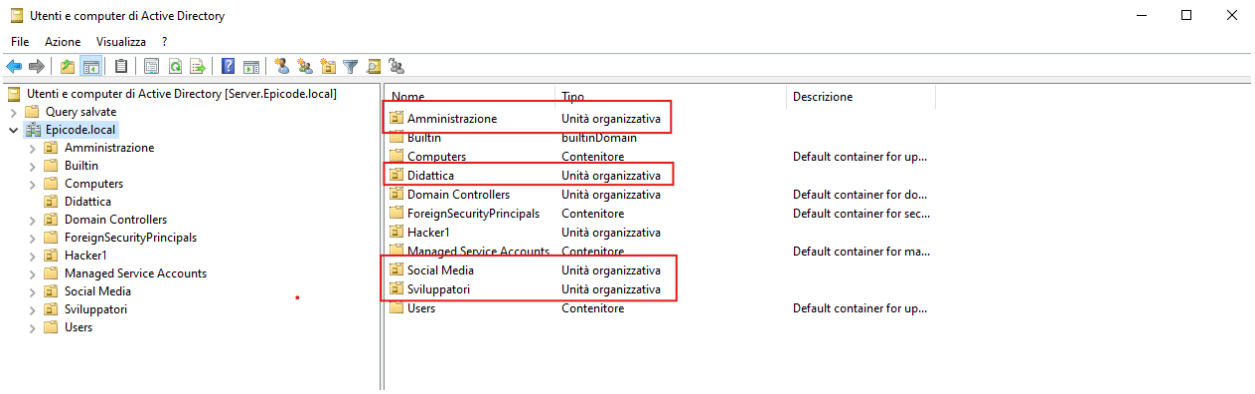


Creazione dei gruppi

Torniamo sulla macchina server per creare e gestire nuovi gruppi.

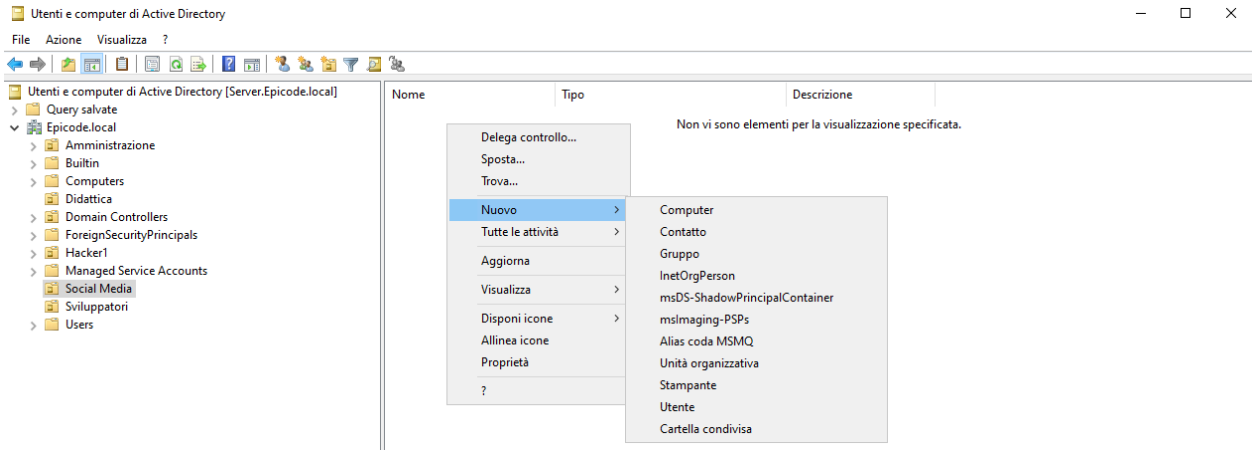
Accediamo alla sezione per configurare i domini tramite *Server Manager* > *Strumenti* > *Utenti e computer di Active Directory*.

Nella sezione a sinistra facciamo click destro sul nome della foresta *Nuovo* > *Unità organizzativa* e inseriamo il nome del reparto che vogliamo aggiungere. Io ho creato le unità organizzative *Amministrazione*, *Sviluppatori*, *Didattica*, *Social Media*.



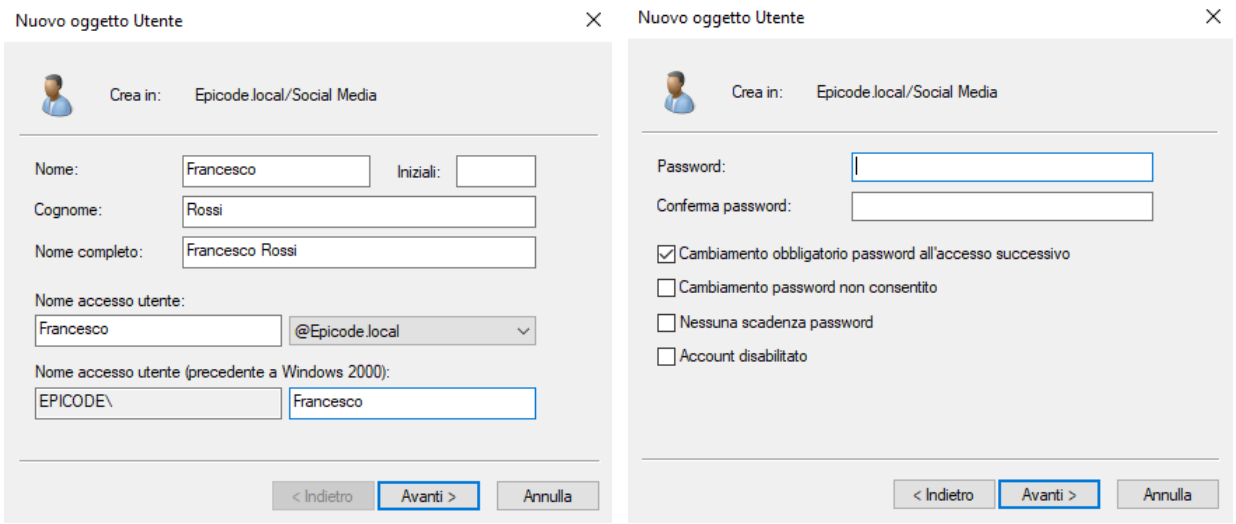
In ogni unità organizzativa andiamo ad inserire tutti gli utenti del dipartimento

Per fare ciò clicchiamo sull'unità organizzativa > *Click destro* > *Nuovo* > *Utente*



Aggiungiamo tutte le informazioni richieste del nuovo utente e quindi *Avanti...*

Andiamo ad impostare la password di login e scegliamo le impostazioni che preferiamo.



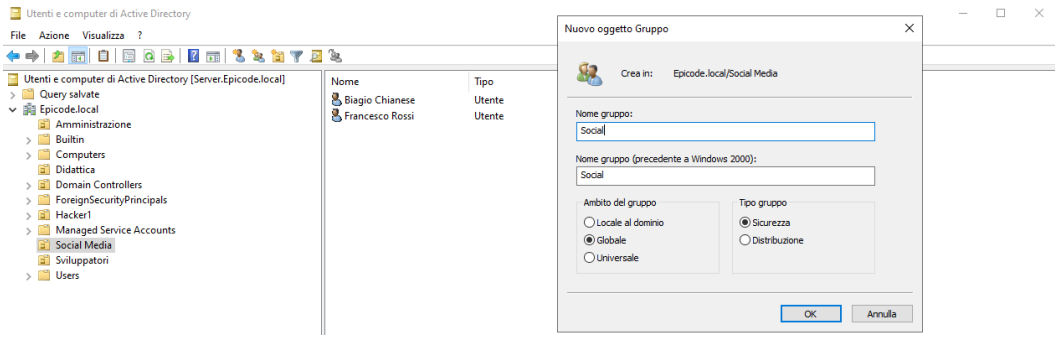
N.B. è importante e vivamente consigliato selezionare la casella *Cambiamento obbligatorio password all'accesso successivo*. Questa impostazione richiede all'utente di modificare la password al primo accesso, per garantire la massima sicurezza e riservatezza dell'account utente.

Scegliamo inoltre di non selezionare la voce *Nessuna scadenza password* in modo tale da seguire le linee guida che consigliano di aggiornare la password dopo un tempo prestabilito.

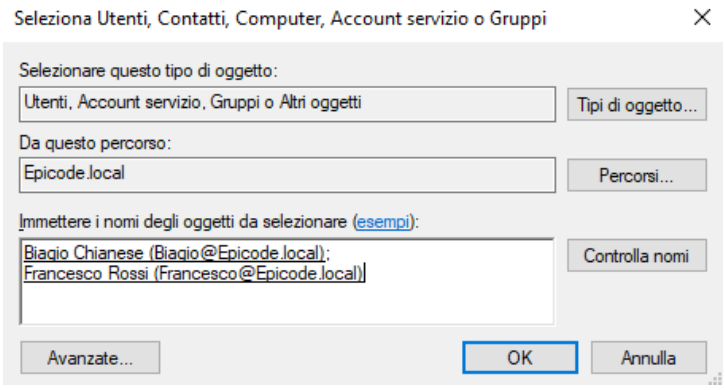
Ripetiamo il procedimento appena descritto per ogni utente delle unità organizzative create in precedenza.

Dopo aver aggiunto tutti i dipendenti aziendali, è finalmente il momento di creare i gruppi.

Scegliamo l'unità da cui partire *Click destro* > *Nuovo* > *Gruppo*. Nella finestra che si apre scegliamo il nome del gruppo, lasciando ambito *Globale* e tipo di gruppo *Sicurezza*.

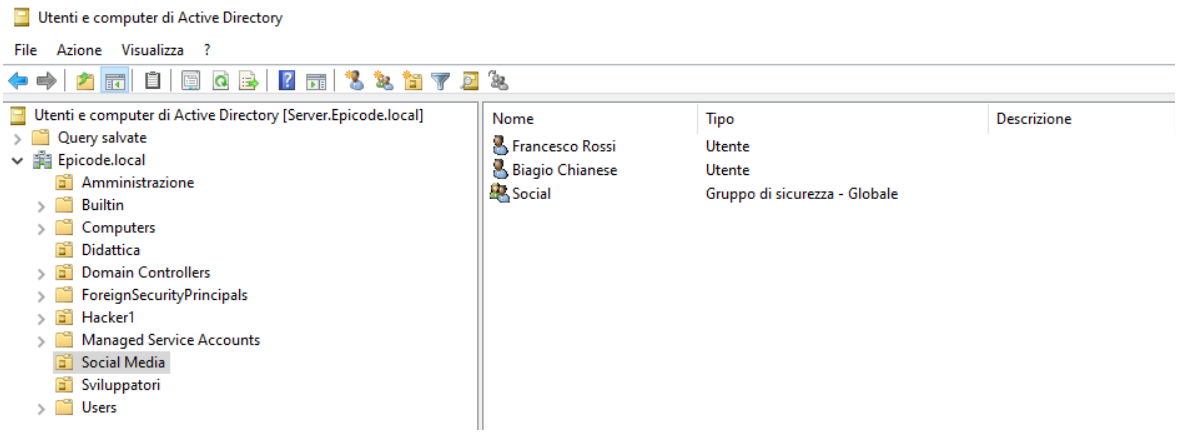


Creato il gruppo, ci clicchiamo due volte e ci spostiamo nella sezione *Membri*. Clicchiamo su *Aggiungi…* ed inseriamo i nomi degli utenti che devono far parte del gruppo, in questo caso *Francesco* e *Biagio* (inseriamo i nomi uno dopo l'altro separati da ";").



Clicchiamo su *Controlla nomi* per verificare che non abbiamo commesso errori di battitura o di inserimento, quindi *OK*, confermiamo con *Applica* e ancora *OK*.

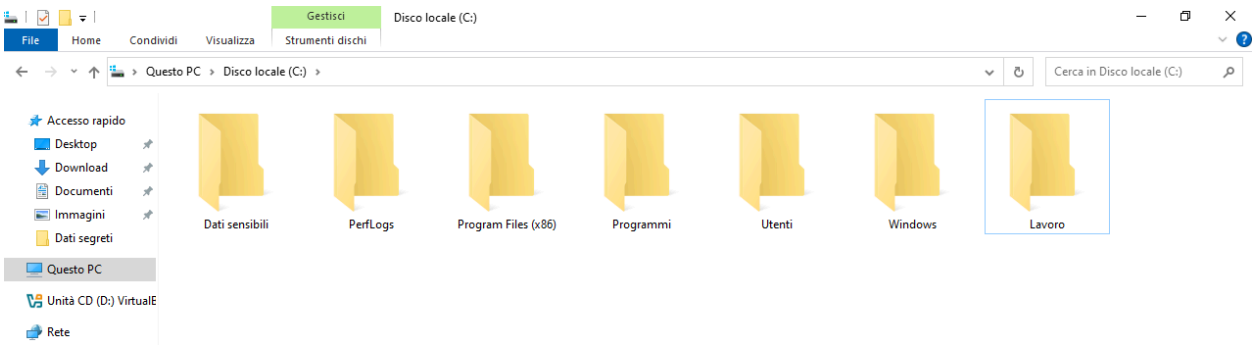
Dopo aver ripetuto i passaggi per ogni unità organizzativa, dovremmo vedere ogni utente e il gruppo appena creato, come mostrato in figura



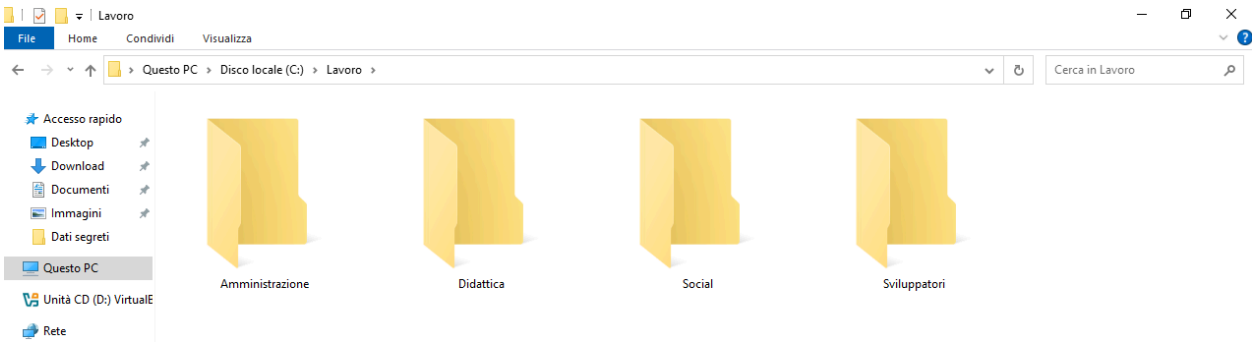
Assegnazione dei permessi

Per prima cosa creiamo delle cartelle condivise a cui assegneremo i permessi specifici per ogni gruppo.

Per semplicità e chiarezza ho scelto di creare le cartelle con il nome del gruppo a cui assegneremo i privilegi maggiori ma non è richiesto né necessario.



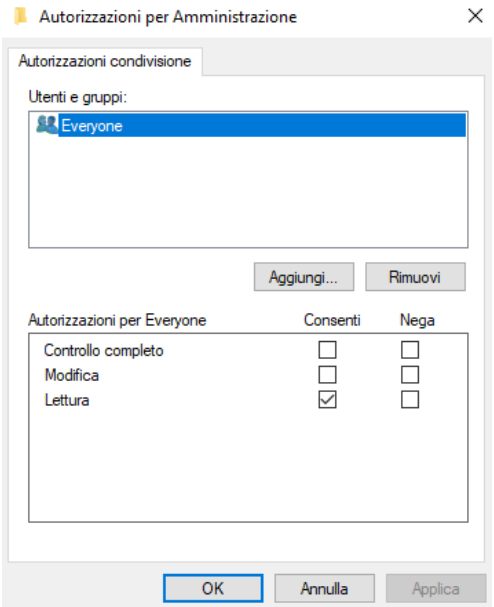
Per prima cosa creo la cartella *Lavoro* che verrà conterrà tutte le cartelle delle unità organizzative. Inserisco in *Lavoro* una cartella per ogni gruppo creato, attribuendo nomi esplicativi del comparto.



Ho scelto di attribuire i permessi nella seguente maniera: il gruppo Amministrazione è più in alto nella gerarchia e può avere il controllo completo della sua cartella di lavoro ed accesso in lettura a tutte le altre cartelle condivise nello spazio di lavoro. Gli altri tre dipartimenti invece sono tutti subordinati all'amministrazione e possono avere accesso (completo) solo alla propria directory, senza poter leggere i file delle altre unità.

Condividiamo la cartella amministrazione con *Click destro* > *Proprietà* > *Condivisione* > *Condivisione avanzata…* > *Condividi la cartella*

A questo punto dobbiamo impostare i permessi di sicurezza in modo tale da seguire le "policy" appena spiegate. Modifichiamo le impostazioni predefinite su *Autorizzazioni*

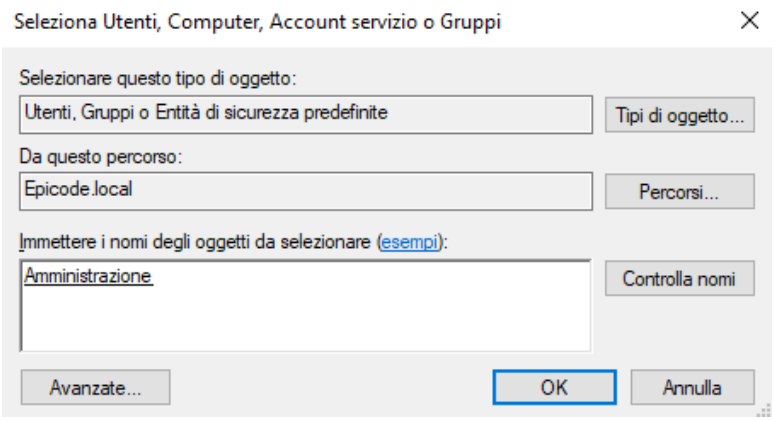


Di default la cartella viene condivisa con "Everyone" ovvero tutti gli utenti, anche quelli non autenticati.

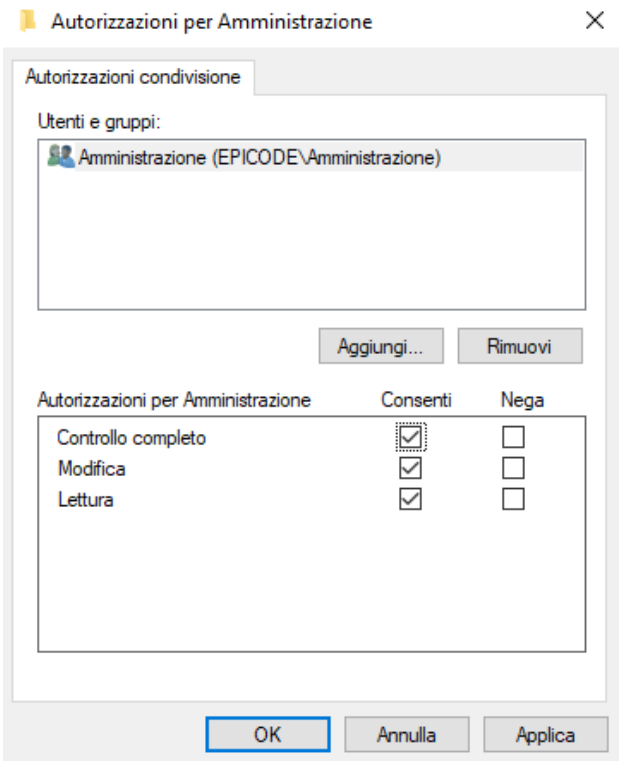
Lasciare questa impostazione sarebbe rischioso per la sicurezza dei dati, che potrebbero essere visualizzati da persone non autorizzate.

Rimuoviamo il gruppo con *Rimuovi* e clicchiamo su *Aggiungi…*

Nel campo apposito vado ad inserire il nome dei gruppi che devono avere i permessi, in questo caso solamente il gruppo *Amministrazione*.



Confermiamo con *OK* e attribuiamo le autorizzazioni *Controllo completo* nella finestra seguente, quindi *Applica* e *OK*.

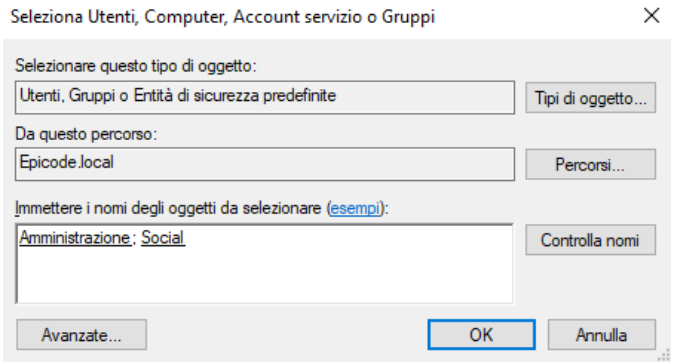


Così facendo permettiamo solo agli utenti inseriti nel gruppo indicato di ottenere le autorizzazioni.

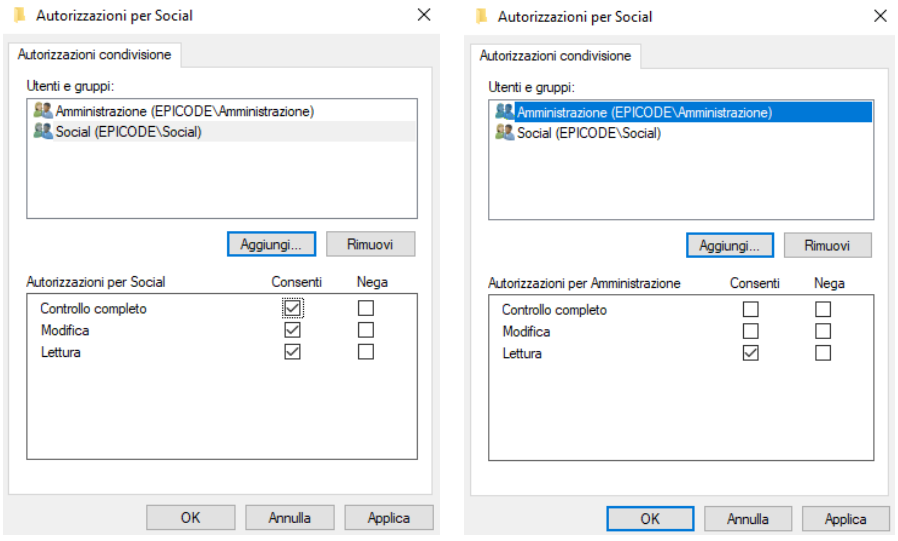
Di seguito mostro il procedimento per una delle tre unità del livello sottostante, il procedimento è da ripetersi per ogni unità modificando di volta in volta il nome del gruppo a cui fornire le autorizzazioni.

Impostiamo quindi le autorizzazioni per la cartella Social dedicata all'unità organizzativa *Social Media*. Come spiegato in precedenza vogliamo che ogni utente del gruppo abbia accesso completo e i dipendenti dell'amministrazione possano leggere il contenuto.

Condividiamo la cartella seguendo i passaggi elencati in precedenza. Anche questa volta rimuoviamo il gruppo *Everyone* per ed aggiungiamo i gruppi *Amministrazione* e *Social*



Forniamo quindi le autorizzazioni come precedentemente stabilito



Dopo aver ripetuto il procedimento per le altre due unità, dovremmo aver impostato tutti i permessi correttamente creando un ambiente di lavoro sicuro e separato.

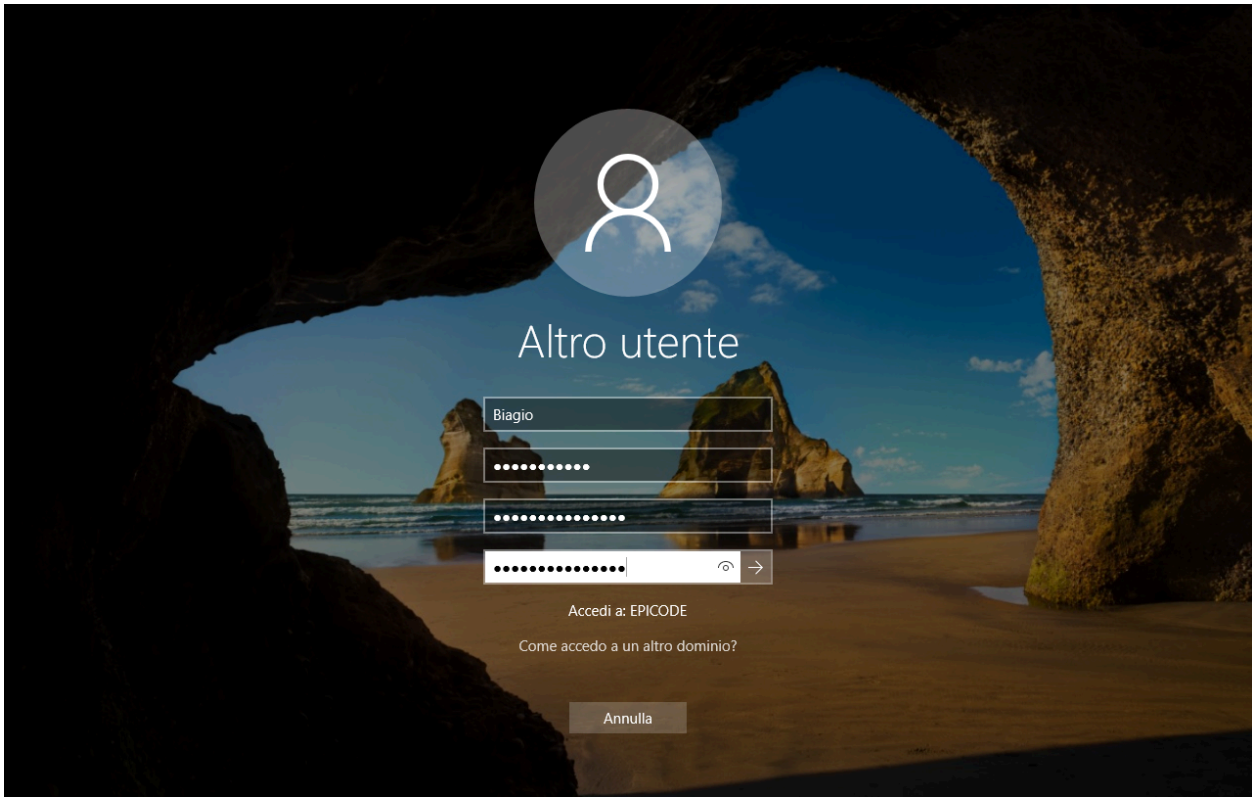
Verifica dei permessi

Proviamo ora a verificare se tutte le configurazioni sono state eseguite correttamente

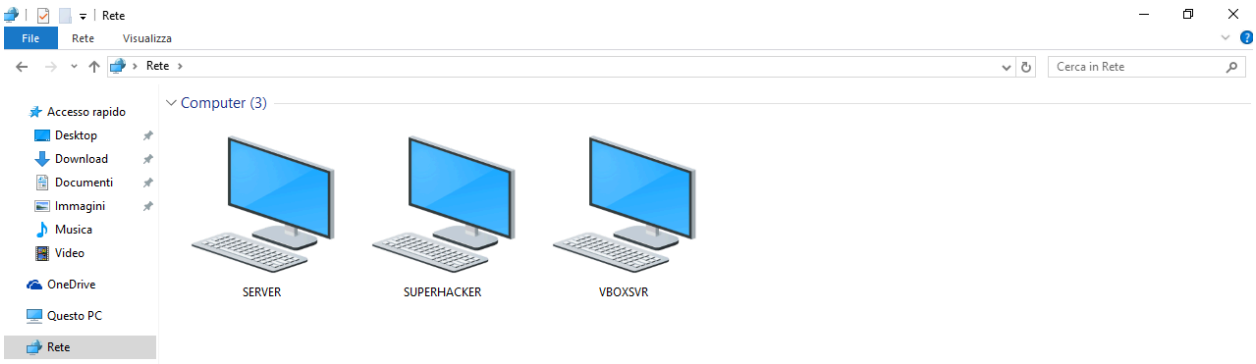
Per prima cosa accediamo sul client con l'utente *Biagio* appartenente al gruppo *Social*. Inseriamo il nome utente nella schermata di accesso e la password preimpostata

Come da nostra configurazione ci viene chiesto di modificare la password al primo accesso e metterne una sicura a scelta.

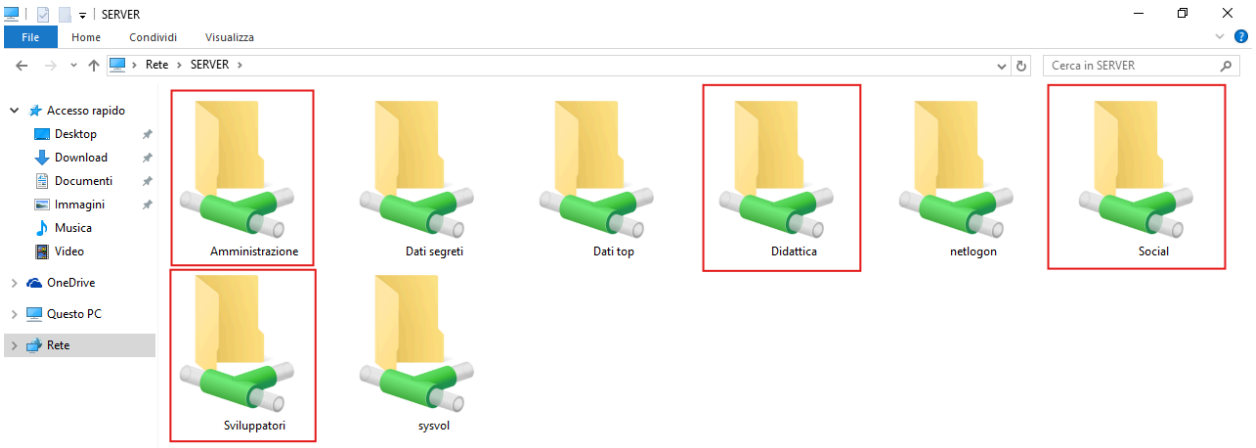
Modifichiamo quindi la password e eseguiamo nuovamente il login



Ad accesso eseguito possiamo accedere alla cartella *Social* condivisa in rete.

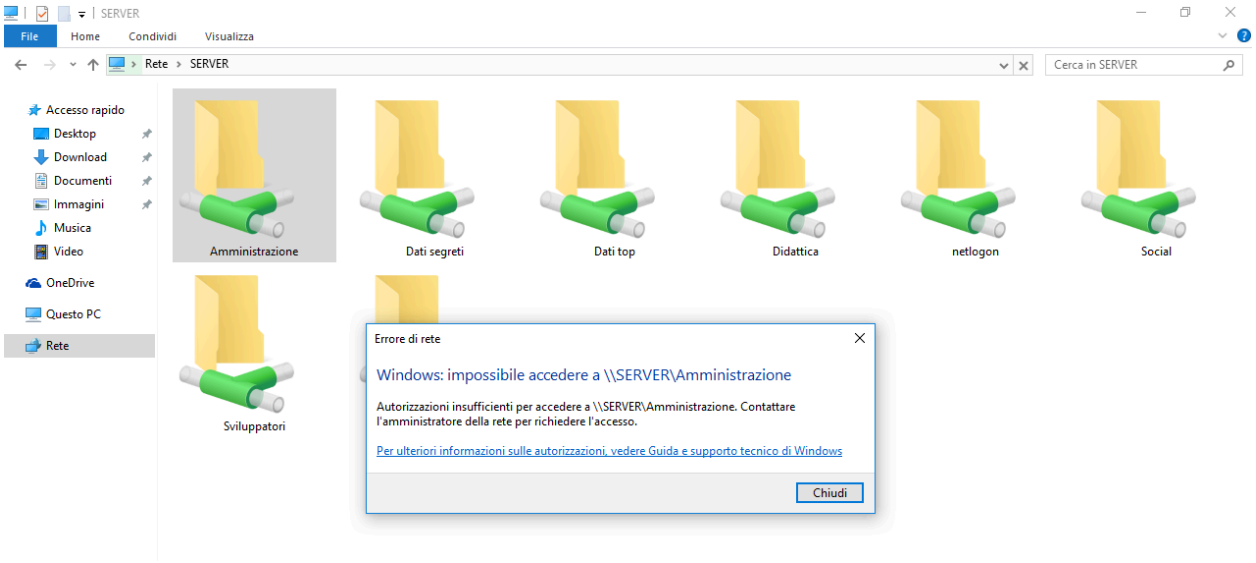


Ricordiamo che il nostro server si chiama *server*, apriamo quindi la risorsa condivisa e possiamo vedere che sono presenti tutte le cartelle che abbiamo condiviso in precedenza



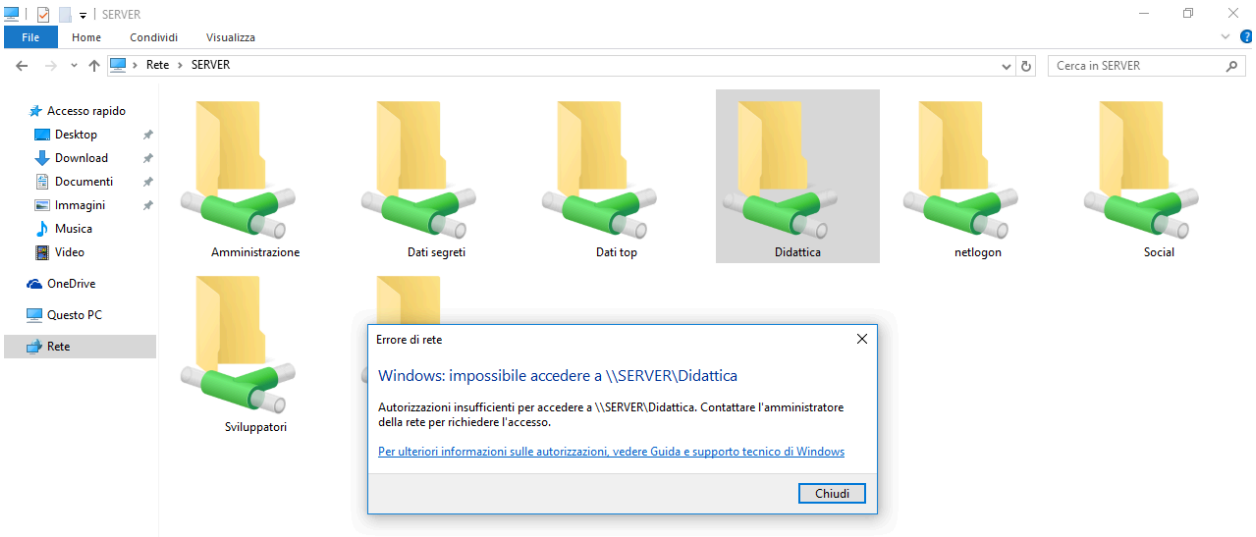
Poiché abbiamo eseguito il login con l'utente *Biagio* del gruppo *Social* dovremmo poter avere accesso esclusivamente alla relativa cartella e non alle altre unità.

Per prima cosa ho provato ad accedere alla cartella *Amministrazione* e come da aspettative, avendo configurato correttamente i permessi, non abbiamo accesso.



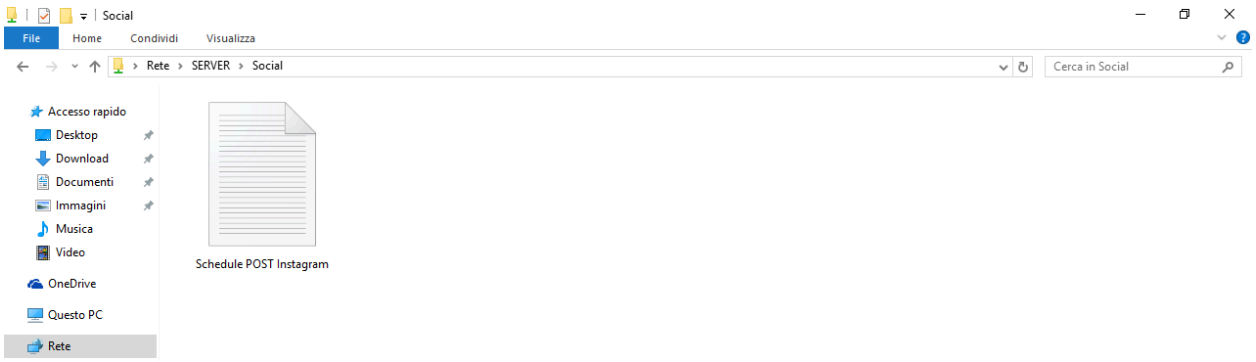
Proviamo ora ad accedere ad una delle cartelle delle unità sullo stesso livello, ad esempio *Didattica*.

Anche in questo caso riceviamo lo stesso messaggio di errore poiché non abbiamo le autorizzazioni di lettura per accedere alla directory



Accediamo quindi alla nostra cartella riservata e non riceviamo alcun errore. Tuttavia per confermare di aver correttamente configurato i permessi, è necessario provare a creare o modificare file all'interno.

Proviamo quindi a creare un nuovo file di testo chiamato *Schedule POST Instagram*



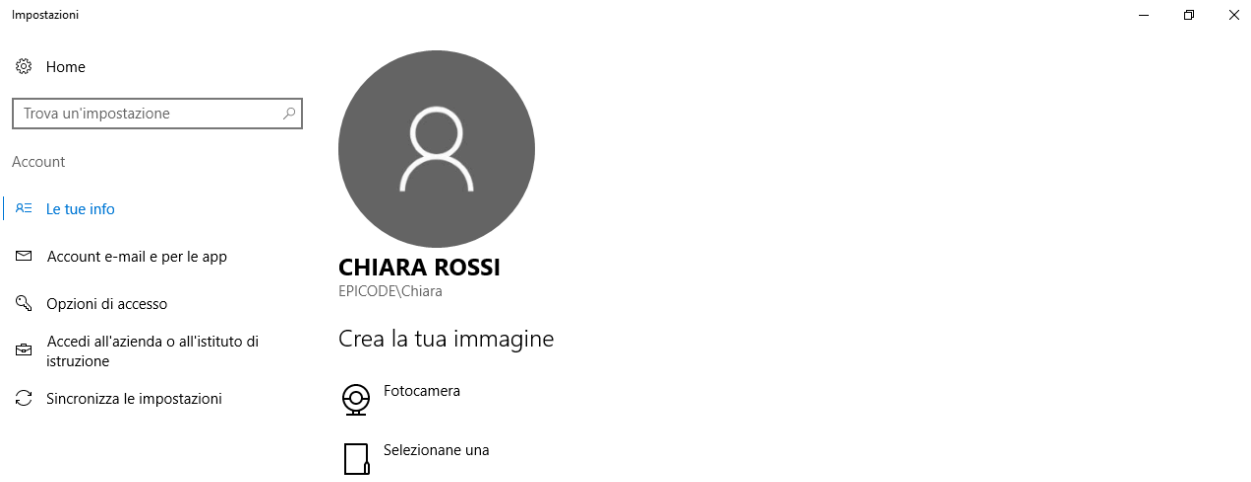
Anche in questo caso abbiamo avuto la conferma che abbiamo tutte le autorizzazioni necessarie e correttamente configurate sul nostro livello di sicurezza.

Proviamo ora a verificare le autorizzazioni per il gruppo *Amministrazione*.

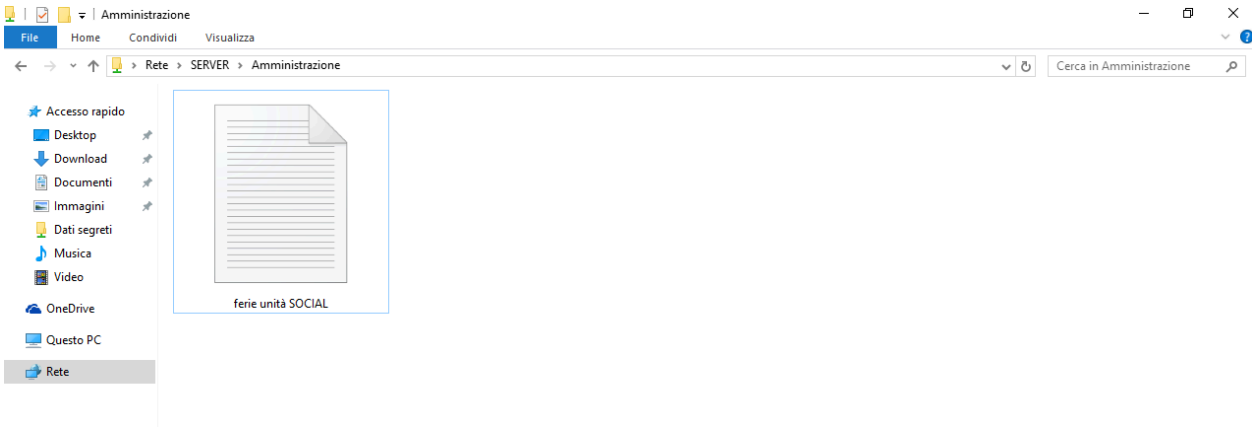
Ricordiamo che in questa simulazione, le policy aziendali di sicurezza prevedono che il gruppo *amministrazione* possa non solo avere accesso completo alla sua directory di lavoro, ma anche poter leggere le directory delle unità sottostanti.

Accediamo quindi con l'account dell'utente *Chiara*.

Poiché mostrato già in precedenza, per rendere l'elaborato meno prolisso, salterò la fase di autenticazione e modifica della password dell'utente. Tuttavia possiamo verificare tramite le impostazioni che siamo realmente autenticati con il nuovo user



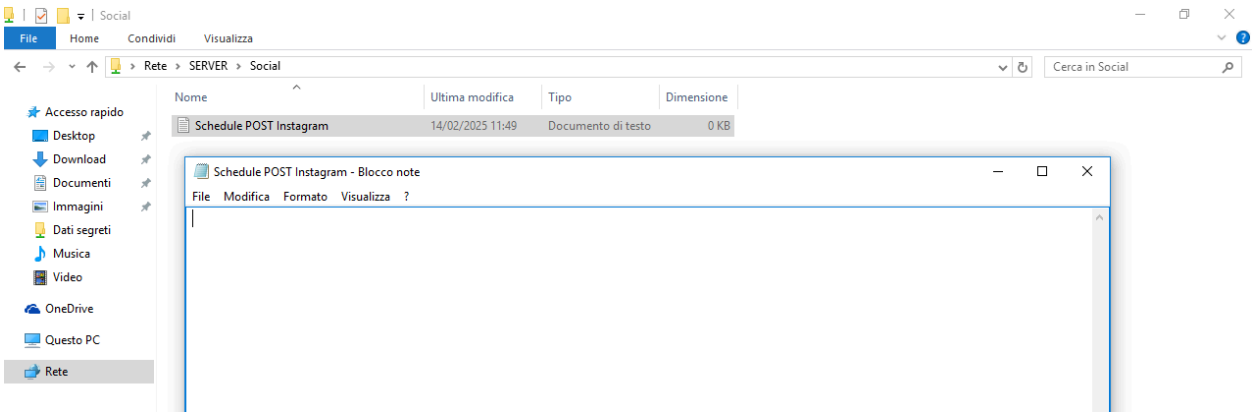
Anche in questo caso accediamo alla risorsa di rete *SERVER*, proviamo ad accedere alla cartella *Amministrazione* e a creare il file di testo *ferie unità SOCIAL*.



Anche in questo caso otteniamo la conferma che i permessi sono stati configurati correttamente.

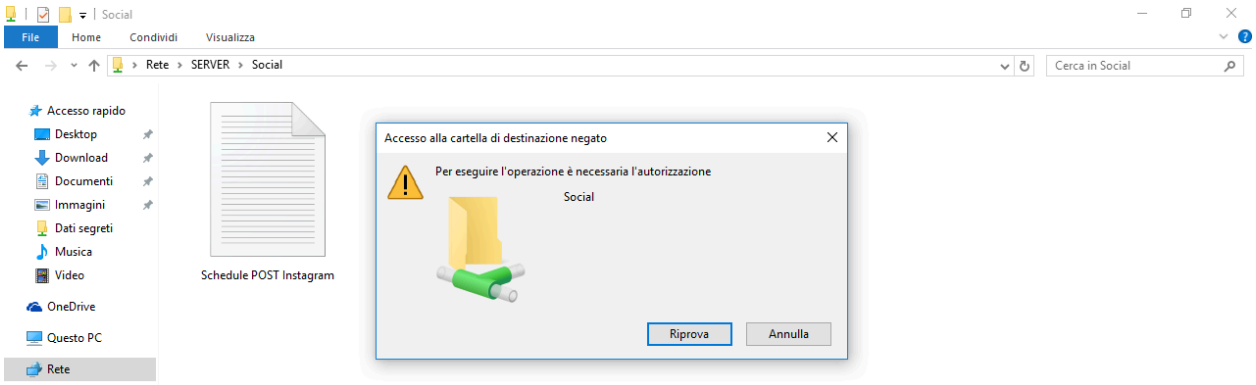
L'ultimo test che ci rimane da fare è la possibilità di leggere il contenuto delle cartelle condivise delle altre unità operative.

Poiché abbiamo già mostrato la creazione del file nella cartella *Social*, proviamo a vedere se riusciamo a visualizzarlo



Come mostrato nello screenshot abbiamo correttamente accesso al file.

Terminiamo infine il report provando ad aggiungere un nuovo file e quindi a scrivere nella cartella *Social*.



Ancora una volta abbiamo ottenuto la conferma che tutti i permessi sono stati correttamente configurati all'interno del dominio.