

REPORT S10/L5

Windows Server

Traccia

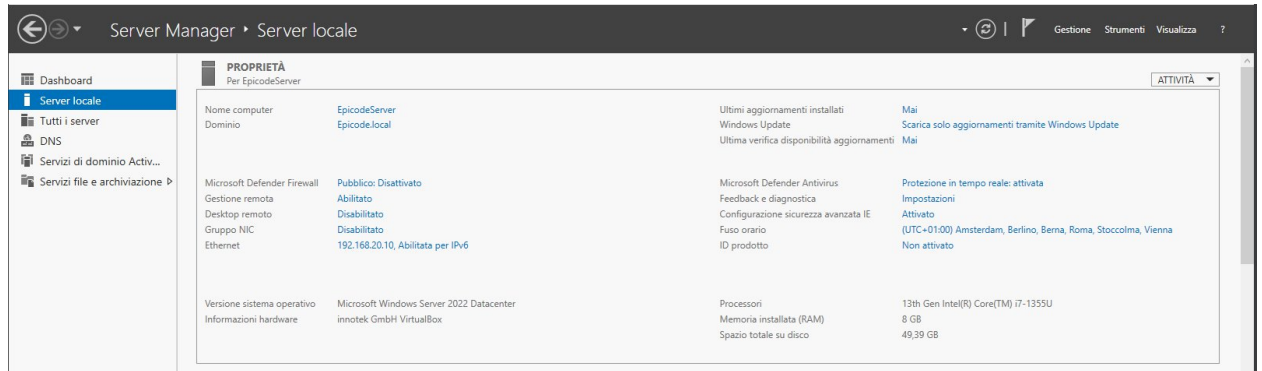
Lo scopo di questo esercizio è di familiarizzare con la gestione dei gruppi di utenti in Windows Server 2022. Imparerai a creare gruppi, assegnare loro permessi specifici e comprendere l'importanza della gestione dei gruppi per la sicurezza e l'amministrazione del sistema.

Istruzioni

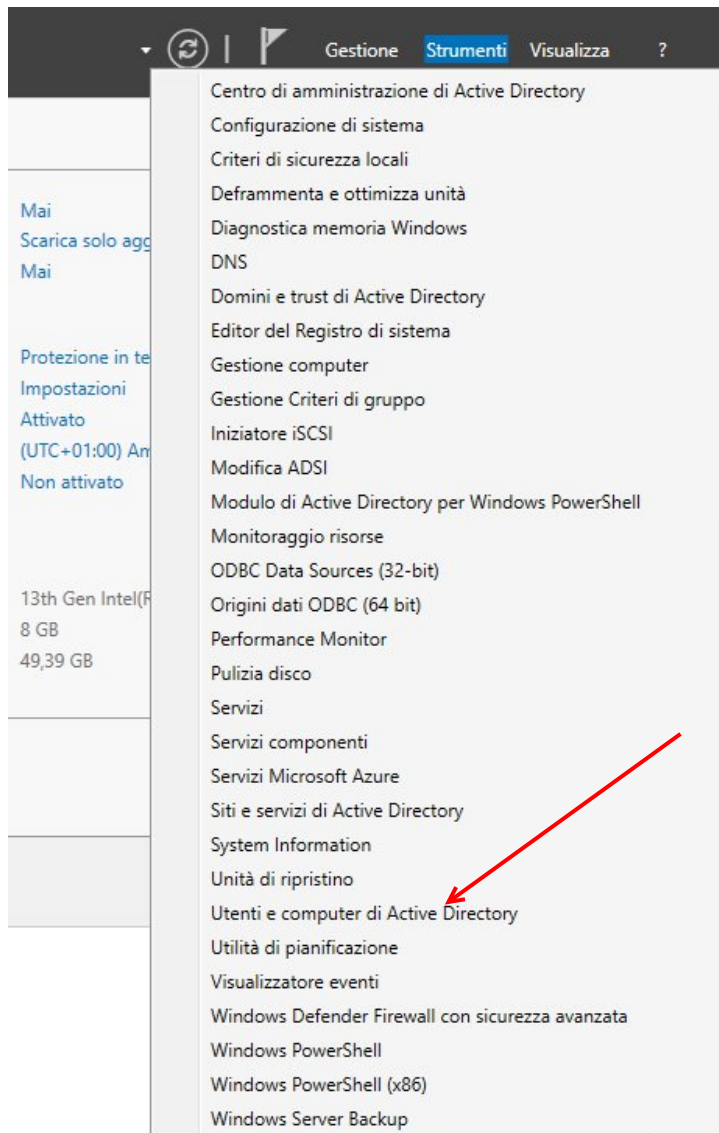
1. Preparazione:
 - Accedi al tuo ambiente Windows Server 2022.
 - Assicurati di avere i permessi amministrativi necessari per creare e gestire gruppi.
2. Creazione dei Gruppi:
 - Crea due gruppi distinti. Puoi scegliere i nomi che preferisci per questi gruppi, ma assicurati che i nomi siano significativi 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.
 - Verifica che altri utenti non possano accedere a quelle risorse.
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.

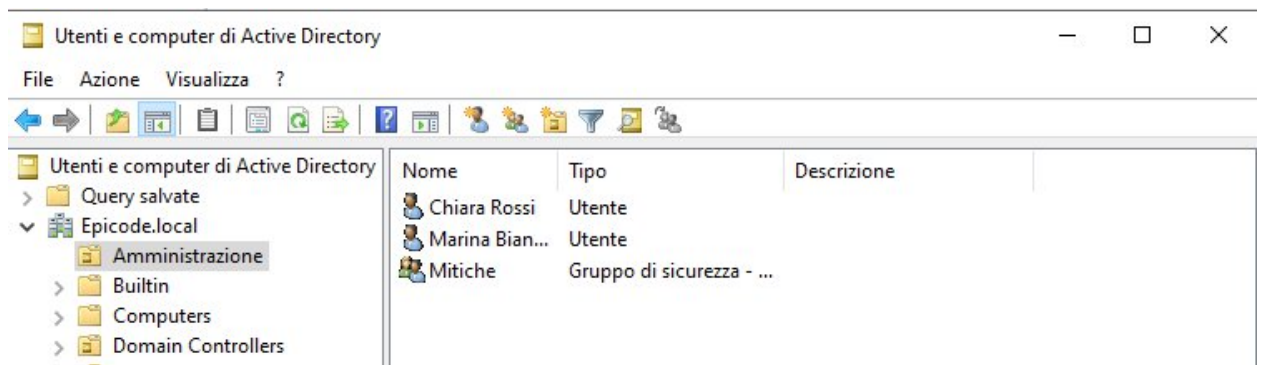
Svolgimento

Partiamo dal server che abbiamo già creato nell'esercizio mercoledì, in cui abbiamo creato il server e EpicodeServer e il dominio Epicode.local

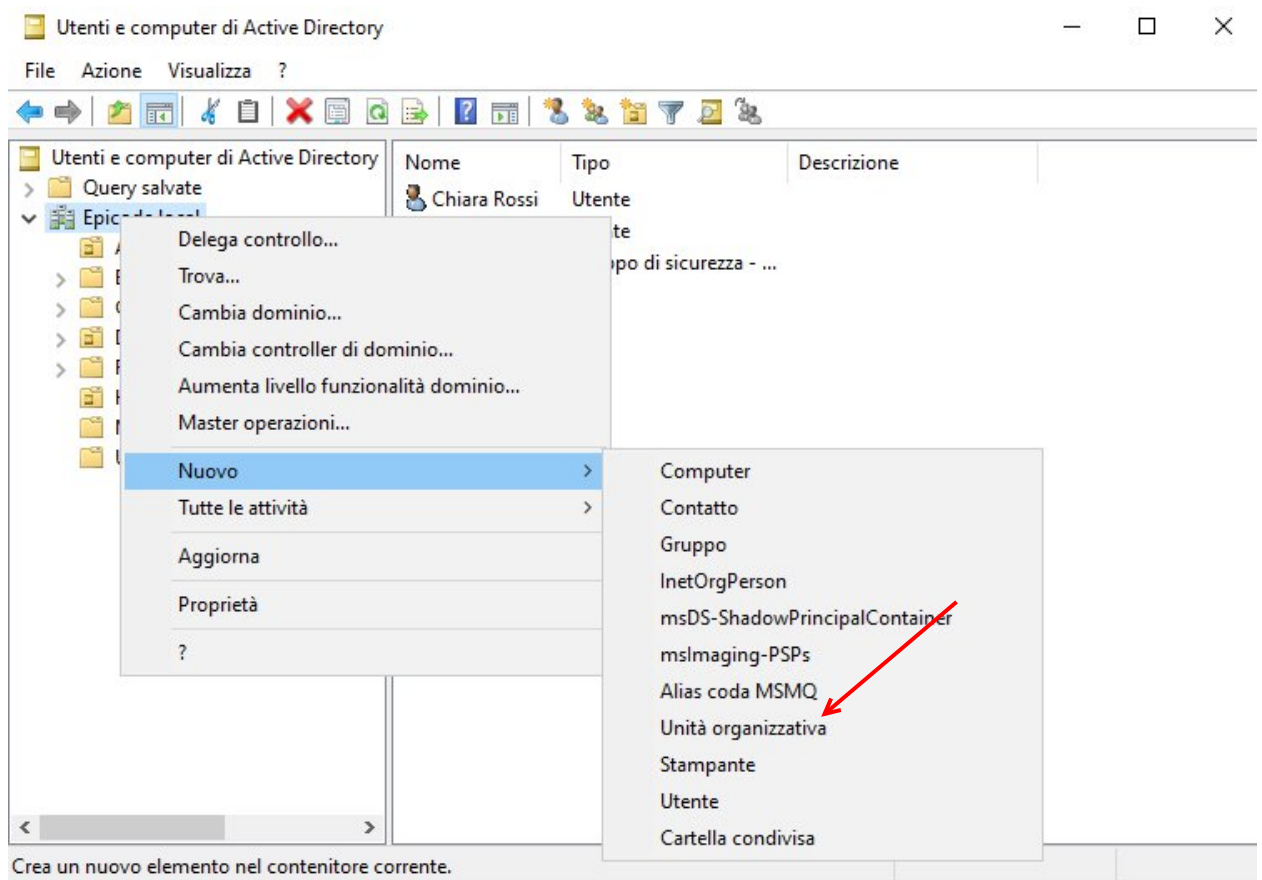


Creiamo i gruppi e gli utenti:






Nella finestra di *Utenti e computer di Active Directory* ritroviamo quanto fatto in precedenza, ovvero le *Unità organizzative* **Amministrazione** e **Hacker1**. Ne creiamo due nuove così da avere profili puliti per questo esercizi



Le nomineremo **Marketing** e **Sviluppatori**

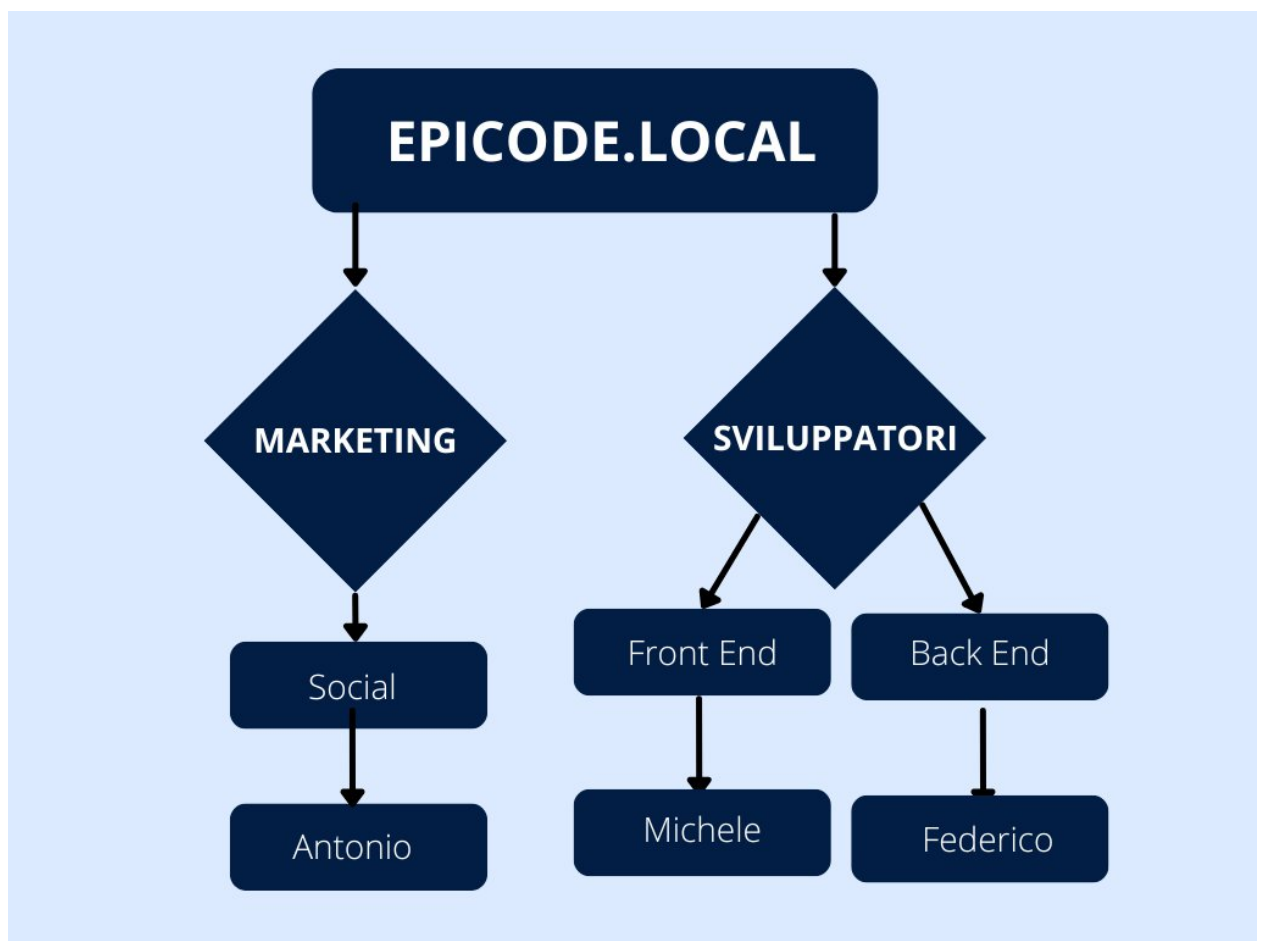
Nuovo oggetto Unità organizzativa ✕

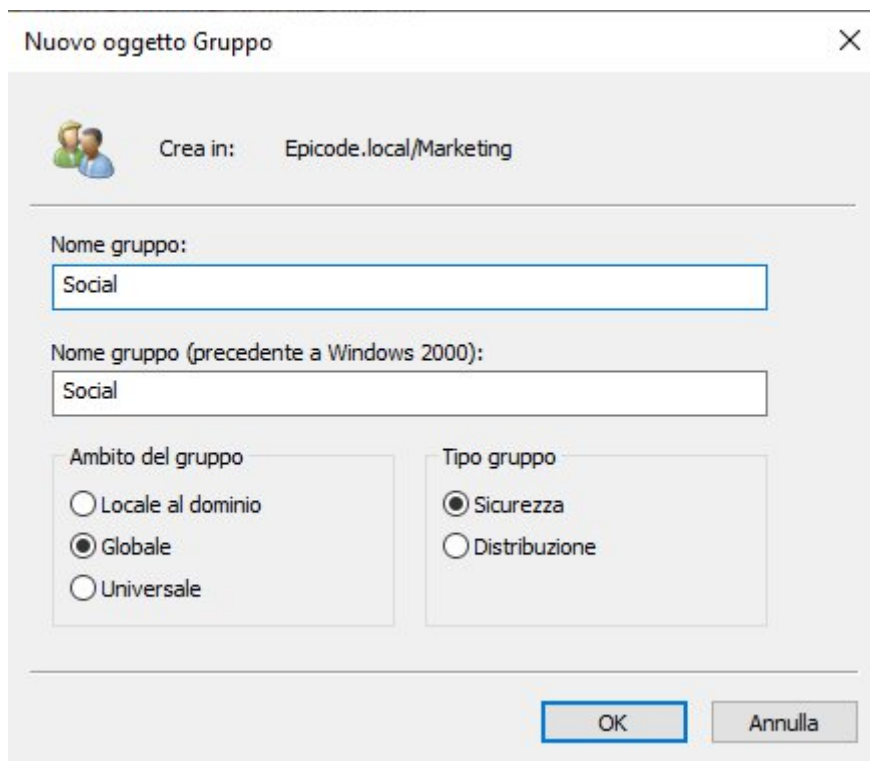
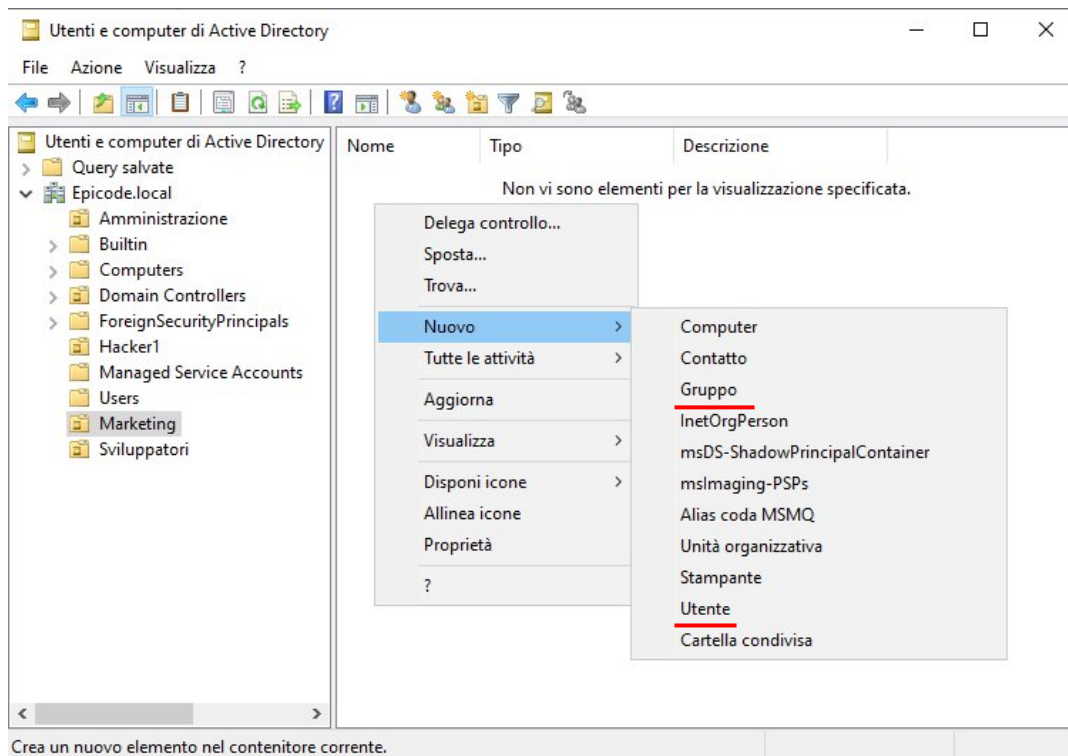
 Crea in: Epicode.local/

Nome:

☒ Proteggi contenitore da eliminazioni accidentali


All'interno di queste unità andiamo a creare i rispettivi gruppi e utenti che saranno così organizzati:





Nuovo oggetto Utente



 Crea in: Epicode.local/Marketing

Nome: Iniziali:

Cognome:

Nome completo:

Nome accesso utente:


Nome accesso utente (precedente a Windows 2000):

< Indietro **Avanti >** Annulla

Nella creazione dell'utente ricordiamo di inserire una password standard e di lasciare l'opzione di cambiare questa password al primo accesso, così che ogni utente possa inserire una password personale e sicura.

Nuovo oggetto Utente



 Crea in: Epicode.local/Marketing

Password:

Conferma password:

☒ Cambiamento obbligatorio password all'accesso successivo

☐ Cambiamento password non consentito

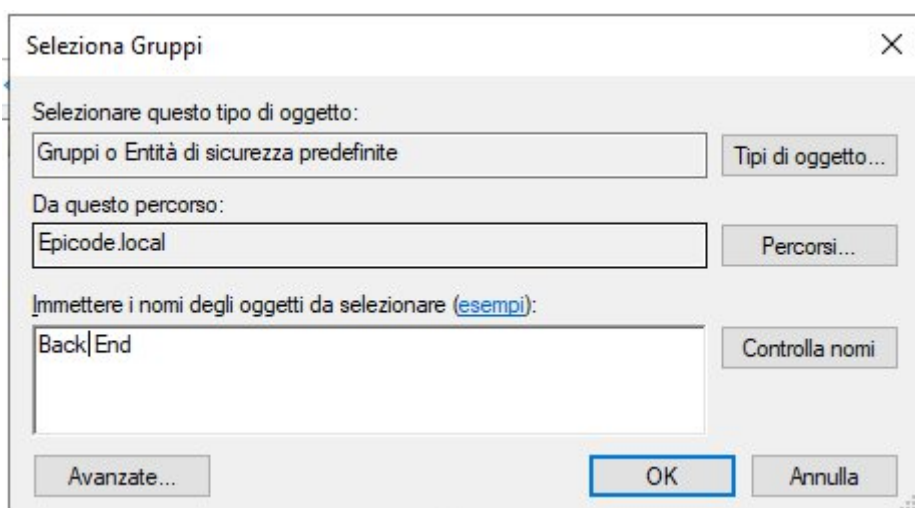
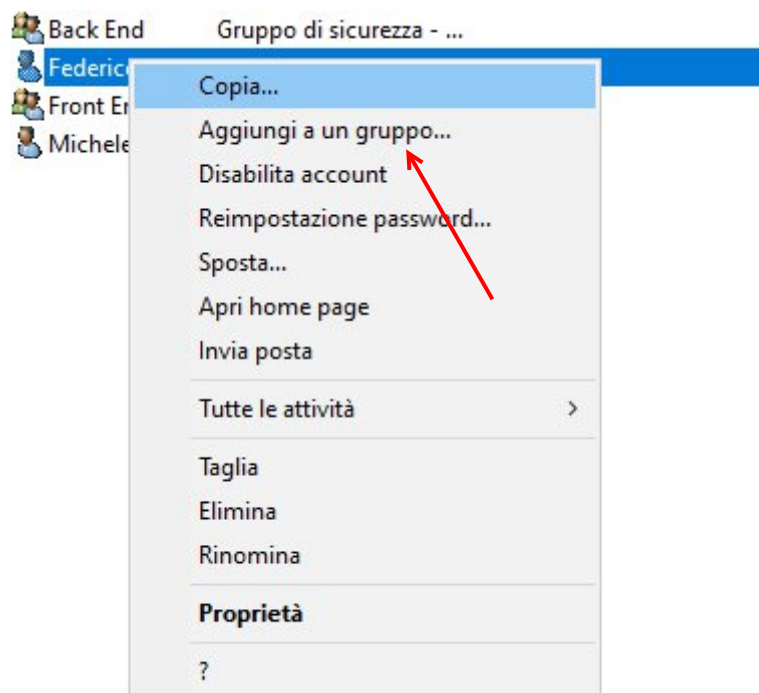
☐ Nessuna scadenza password

☐ Account disabilitato

< Indietro **Avanti >** Annulla

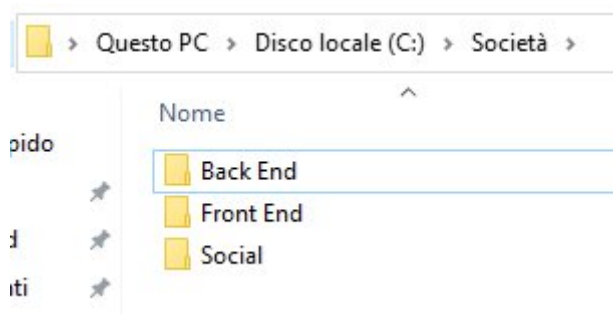
Ripetiamo queste operazioni per tutti gli utenti e i gruppi così da avere l'organizzazione aziendale come nello schema in alto.

Ora aggiungiamo gli utenti ai vari gruppi:

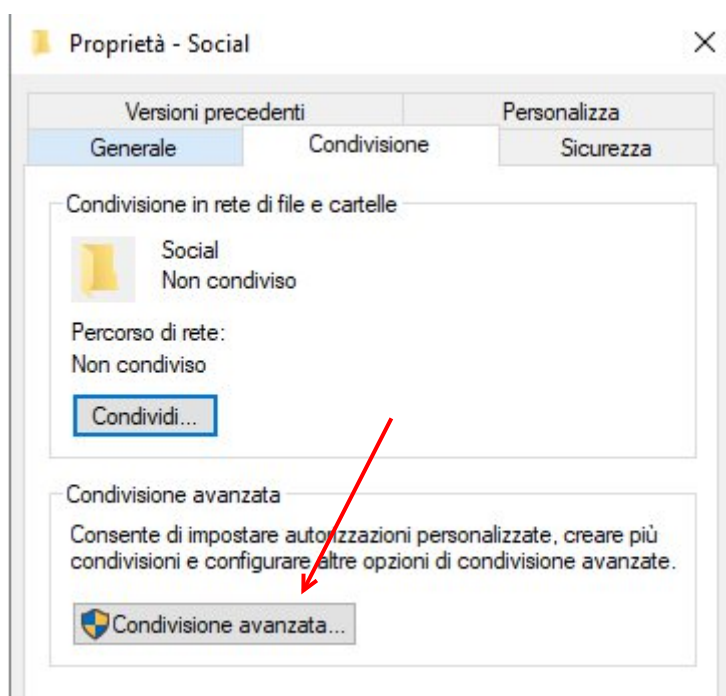


Ora possiamo creare sul server le cartelle da associare ai gruppi e agli utenti creati con i rispettivi permessi d'accesso e utilizzo.

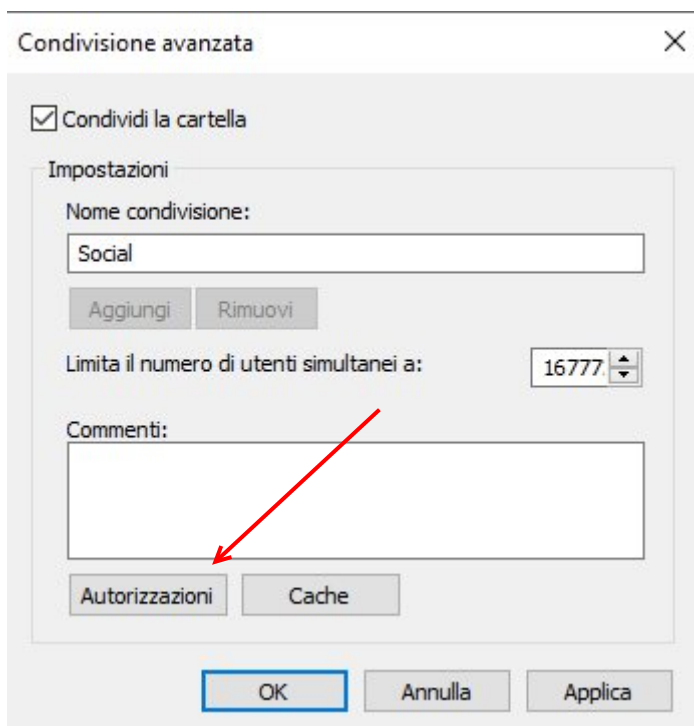
Chiameremo la cartella principale **Società** e useremo i nomi dei gruppi e degli utenti specifici per le sottocartelle.



Diamo i permessi di accesso e utilizzo dalle opzioni di *Condivisione Avanzata* delle sotto cartelle:



E poi andiamo su *Autorizzazioni*



Qua vediamo che le impostazioni di default prevedono la condivisione al gruppo *Everyone* con permessi di sola lettura. Nel nostro caso cancelliamo *Everyone*, perché questo gruppo include tutti gli utenti anche i non autenticati. Facendo questo passaggio otterremo maggiore sicurezza e controllo, prevenendo attacchi interni o perdita di dati, in conformità con le normative.

Aggiungiamo quindi il gruppo *Social* alla relativa cartella, poi diamo la sola autorizzazione di lettura:

Seleziona Utenti, Computer, Account servizio o Gruppi

Selezionare questo tipo di oggetto:
Utenti, Gruppi o Entità di sicurezza predefinite

Da questo percorso:
Epicode.local

Immettere i nomi degli oggetti da selezionare (esempi):
Social

Avanzate... OK Annulla

Autorizzazioni per Social	Consenti	Nega
Controllo completo	<input type="checkbox"/>	<input type="checkbox"/>
Modifica	<input type="checkbox"/>	<input type="checkbox"/>
Lettura	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Con lo stesso metodo neghiamo agli altri gruppi l'accesso e la modifica di questa cartella e delle relative sotto cartelle:

Seleziona Utenti, Computer, Account servizio o Gruppi

Selezionare questo tipo di oggetto:
Utenti, Gruppi o Entità di sicurezza predefinite

Da questo percorso:
Epicode.local

Immettere i nomi degli oggetti da selezionare (esempi):
Front End;Back End

Avanzate... OK Annulla

Utenti e gruppi:

Back End (EPICODE\BACK_END)
Front End (EPICODE\FRONT_END)
Social (EPICODE\Social)

Aggiungi... Rimuovi

Autorizzazioni per Front End

	Consenti	Nega
Controllo completo	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Modifica	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Lettura	<input type="checkbox"/>	<input checked="" type="checkbox"/>

In questo modo tutti gli utenti non appartenenti al gruppo *Social* non avranno accesso a questo “spazio” della *Società*.

Ripetiamo questi passaggi anche per le altre cartelle in modo che gli utenti appartenenti allo stesso gruppo possono soltanto leggere, mentre abilitiamo la modifica alla cartella specifica dell’utente. In questo modo, ad esempio, se all’interno del gruppo *Social* appartengono più utenti, ognuno di loro può vedere il contenuto della cartella principale, ma potrà modificare soltanto i files contenuti nella sua cartella specifica.

Autorizzazioni per Antonio

Autorizzazioni condivisione

Utenti e gruppi:

Antonio (Antonio@Epicode.local)

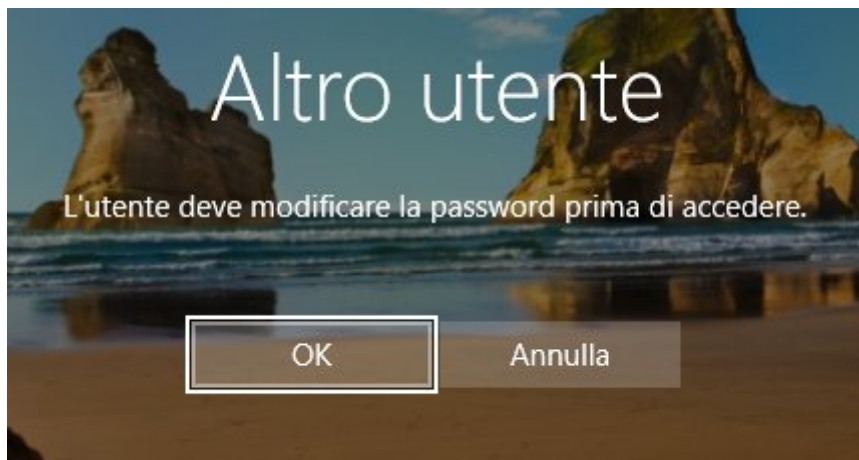
Autorizzazioni per Antonio

	Consenti	Nega
Controllo completo	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modifica	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lettura	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Con queste impostazioni, pertanto, l’utente *Antonio* potrà vedere il contenuto della cartella principale *Società*, della sotto cartella *Social*, ma potrà modificare soltanto i files contenuti nella sua specifica cartella.

Verifichiamo, da Windows 10 Pro, la valenza delle configurazioni fatte. Accederemo con l'account di Antonio, che ricordiamo fa parte del gruppo Social, e proveremo ad accedere e a modificare files nella sua cartella, e anche in quelle di altri utenti.

Come previsto, al primo accesso di *Antonio* ci viene chiesto di cambiare la password:



Proseguiamo nell'operazione, logghiamoci e attiviamo le icone di Questo PC e Rete sul desktop.



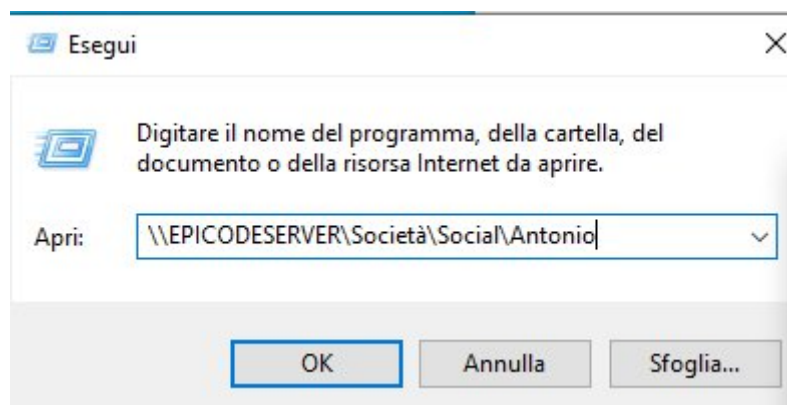
Verifichiamo che il server riesce a pingare il pc client

```
C:\Users\Administrator>ping 192.168.20.30

Esecuzione di Ping 192.168.20.30 con 32 byte di dati:
Risposta da 192.168.20.30: byte=32 durata=1ms TTL=128
Risposta da 192.168.20.30: byte=32 durata=1ms TTL=128
Risposta da 192.168.20.30: byte=32 durata=1ms TTL=128

Statistiche Ping per 192.168.20.30:
    Pacchetti: Trasmessi = 3, Ricevuti = 3,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 1ms, Massimo = 1ms, Medio = 1ms
```

Ora tramite il comando Win + R e inserendo il link della cartella condivisa per l'utente Antonio possiamo entrare nel suo spazio personale sul server e da lì cominciare ad esplorare.

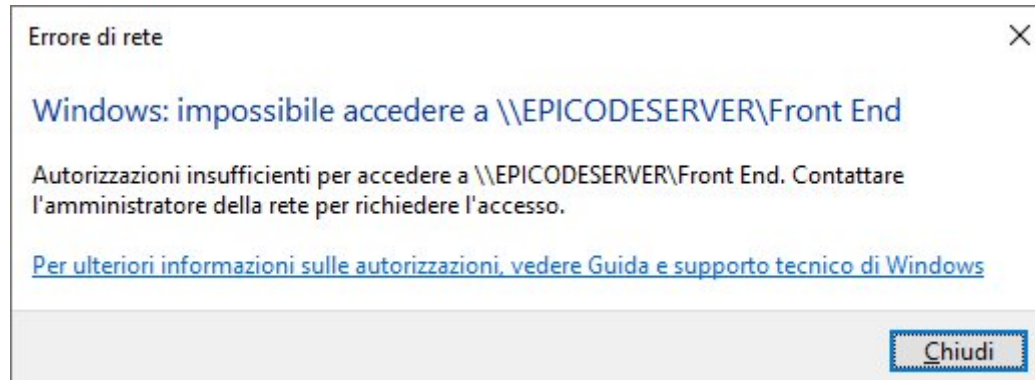


Nella cartella che si apre possiamo modificare qualunque files perchè abbiamo le autorizzazioni sia di lettura che di scrittura.

Creiamo infatti un nuovo documento txt e verifichiamo lato server se lo troviamo nella cartella di Antonio:

Nome	Ultima modifica	tipo	Dimensione
 Nuovo documento di testo	14/02/2025 13:43	Documento di testo	0 KB

Ora se proviamo ad accedere ad una delle cartelle appartenenti ad un gruppo diverso da quello a cui appartiene *Antonio* otteniamo un errore, proprio perchè non abbiamo i diritti di accesso.



Quindi dato che abbiamo bloccato l'accesso alla cartella principale del gruppo Front End, va da sè che non possiamo nemmeno vedere o modificare i files e le sotto cartelle in essa contenuti.