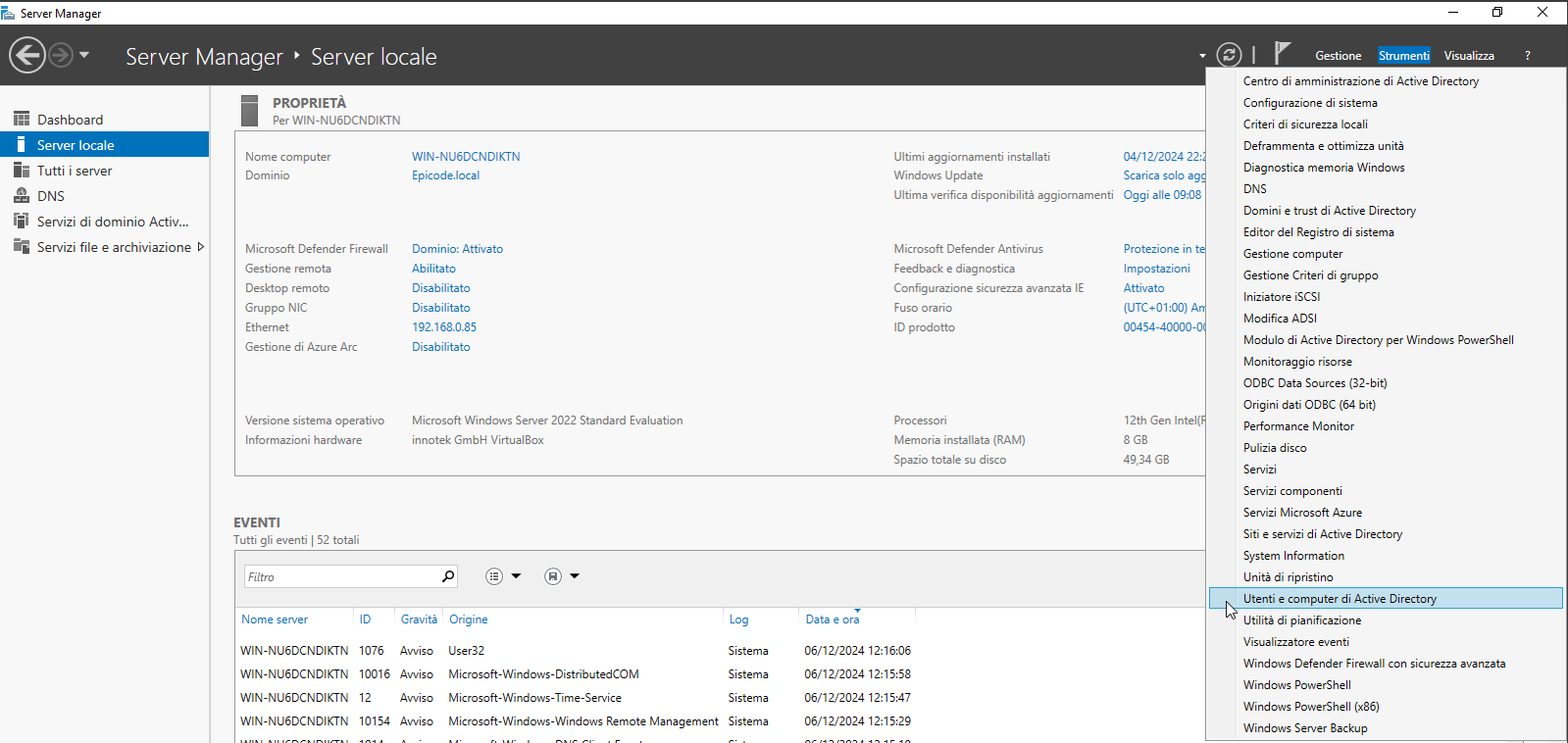
**S10/L5**

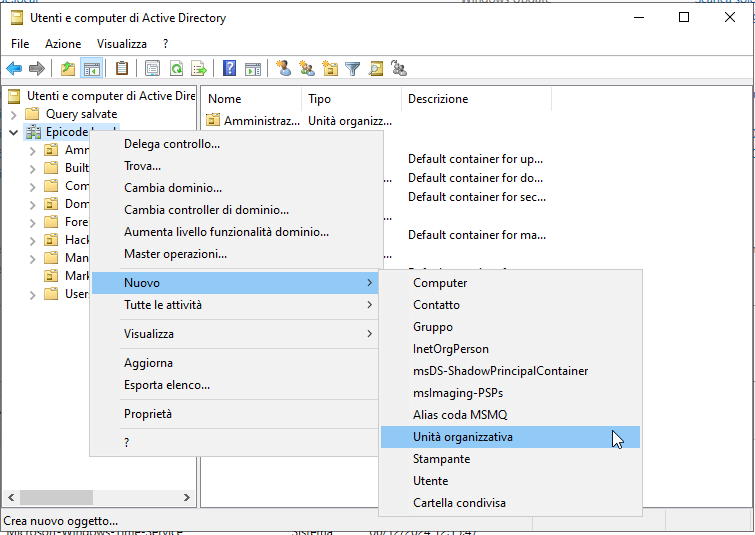
**Windows Server**

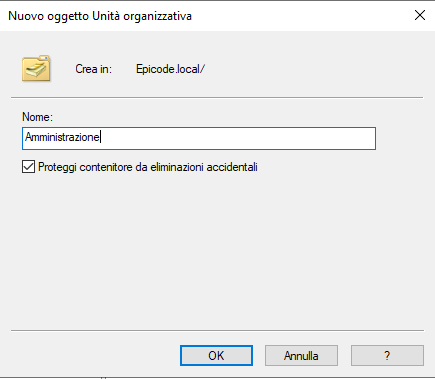
**Guida all’utente**

In questa guida andremo a spiegare come configurare una foresta all’interno di un ambiente lavorativo utilizzando Windows Server.  
  
Vedremo come:  
  
- Crearegruppi di lavoro  
- Assegnare i permessi a ciascun gruppo  
- Effettuare il login su un dispositivo collegato alla foresta  
  
  
**Creazione gruppi lavoro**



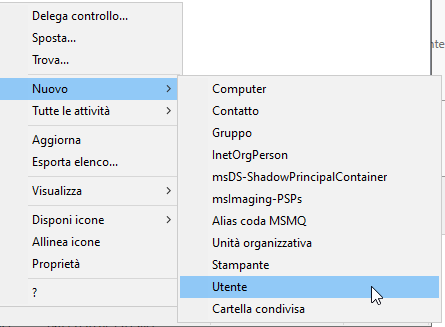
Una volta creata la foresta, sarà necessario creare l’utenza che lavorerà al suo interno.

Per iniziare clicchiamo su “**Strumenti**” all’interno del Server Manager e successivamente selezioniamo “**Utenti e computer di Active Directory**”  
  


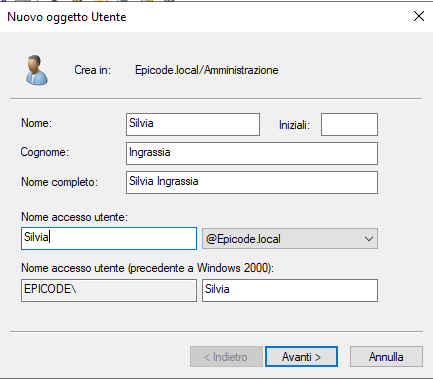
Aperta la finestra “**Utenti e computer di Active Directory**”, clicchiamo col tasto destro sulla nostra foresta (Epicode.local in questo caso). Selezioniamo l’opzione “**Nuovo**” e poi “**Unità organizzativa**”.  
  


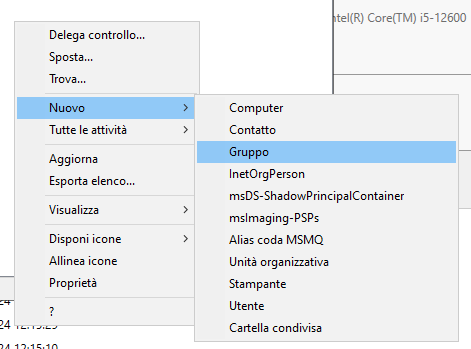
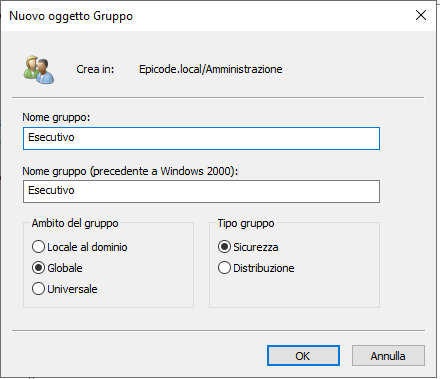
Diamo un nome alla nostra nuova unità e clicchiamo su “**Ok**”

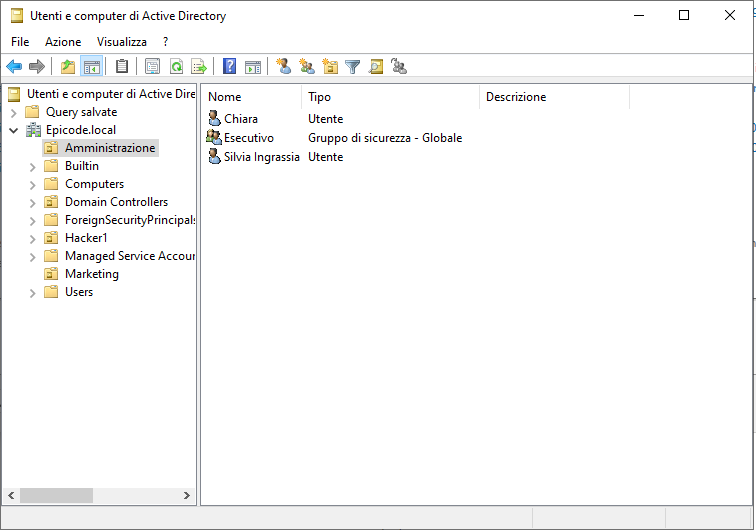
Creata l’unità “**Amministrazione**”, andiamo a creare l’utenza al suo interno. Selezionate “**Nuovo**” facendo tasto destro sull’unità e successivamente “**Utente**”



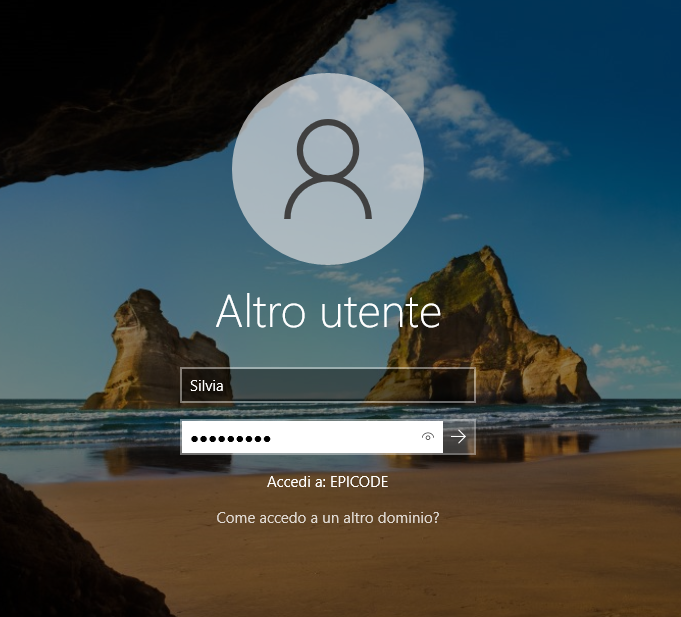
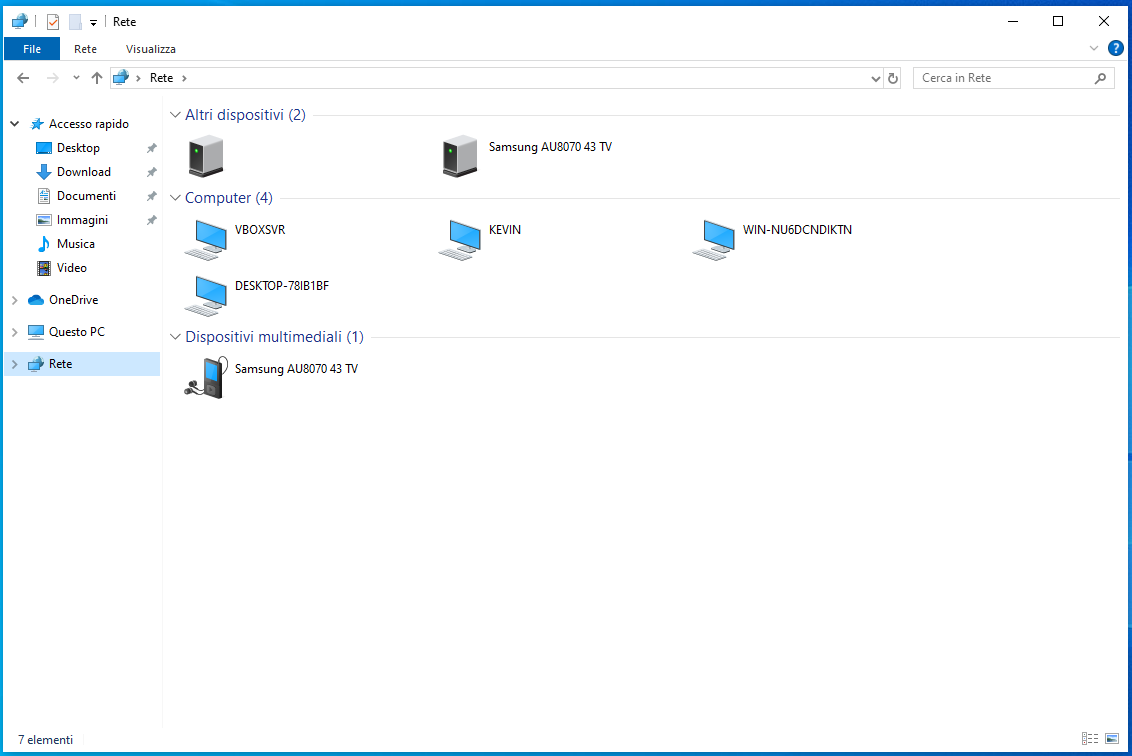
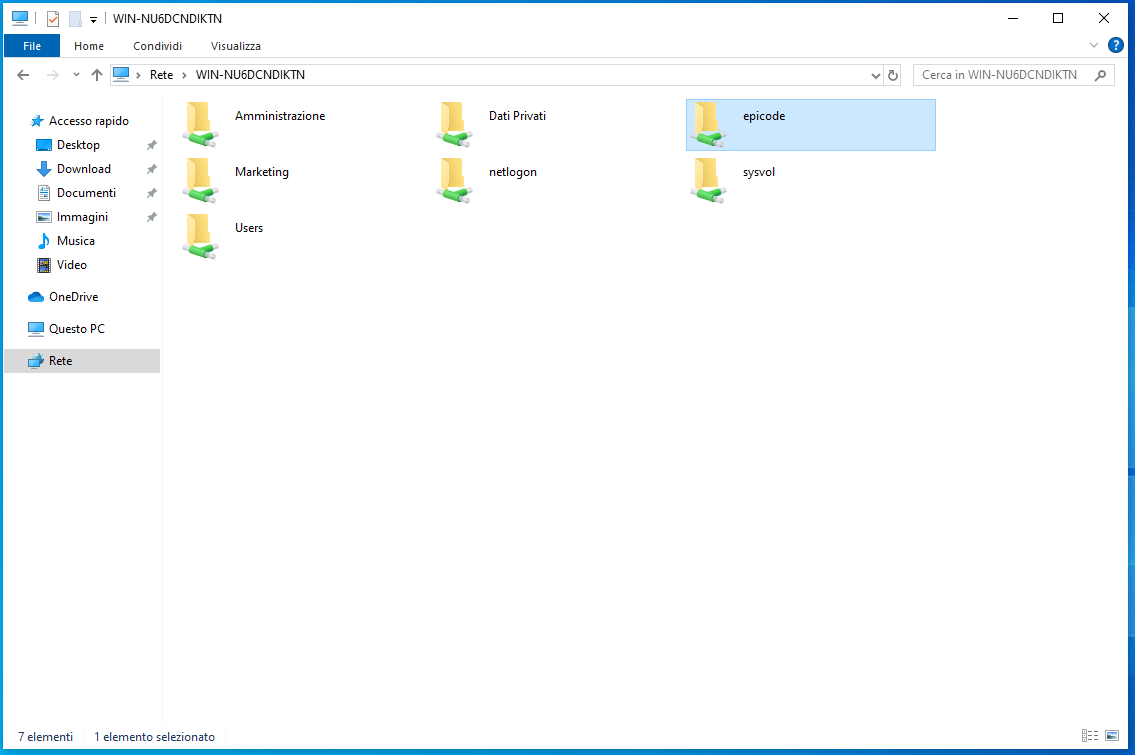
Inseriamo i dati necessari della persona interessata e una password che verrà obbligatoriamente cambiata al primo accesso.

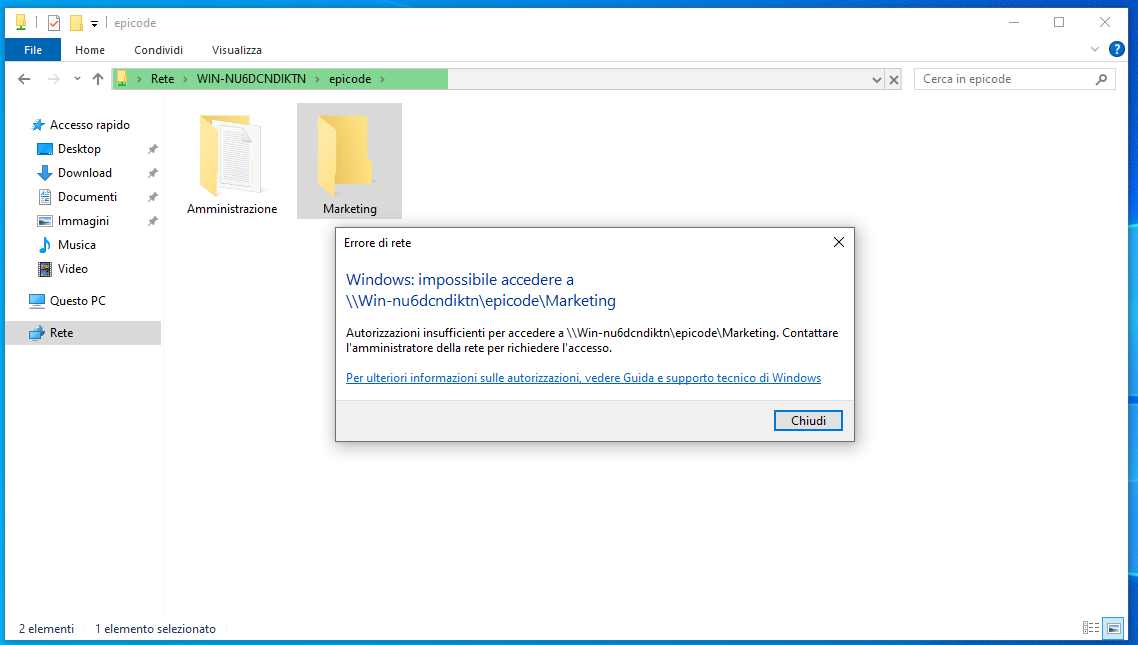


Una volta creati gli utenti sarà necessario assegnare loro un gruppo di appartenenza.  
Sempre all’interno dell’unità “**Amministrazione**” fate tasto destro e selezionate “**Nuovo**” seguito da “**Gruppo**”  
  
  
  
Scegliamo un nome e clicchiamo su “Ok”  
  


Ecco un esempio di Unità organizzativa dove al suo interno sono presenti utenti e gruppi:  
  
  
  
Possiamo notare la presenza di una seconda unità organizzativa di nome “**Marketing**” creata utilizzando il medesimo procedimento.

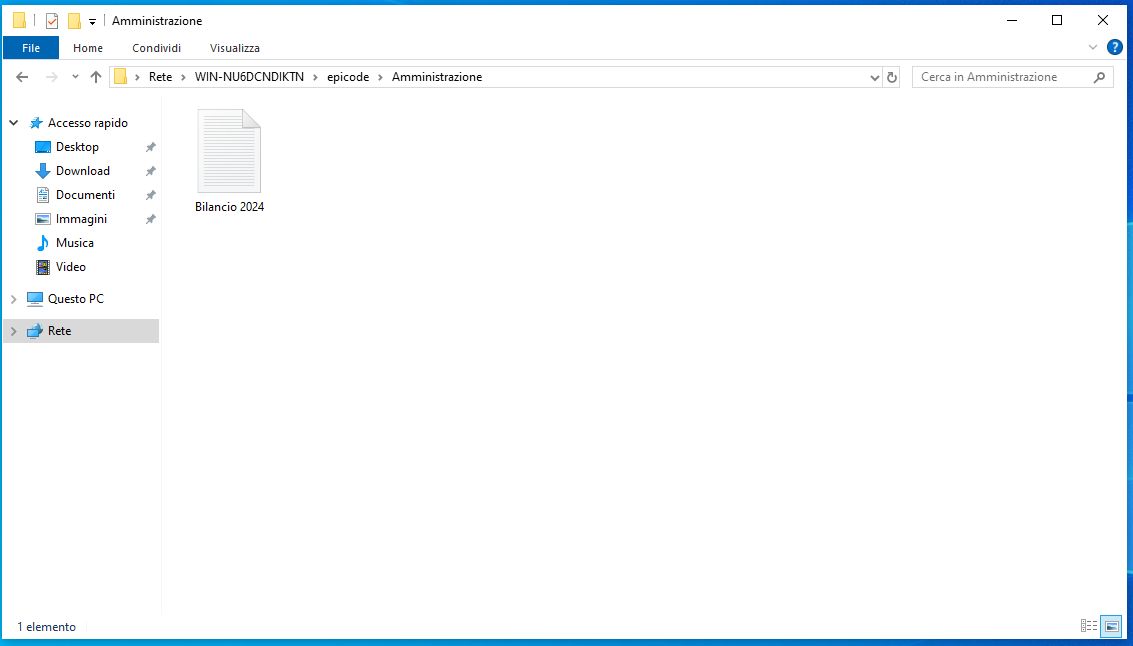
**Effettuare il login su un dispositivo collegato alla foresta**  
Una volta creata l’utenza, i dipendenti saranno in grado di accedere alla foresta da te creata tramite i loro dispositivi precedentemente configurati al Server aziendale.

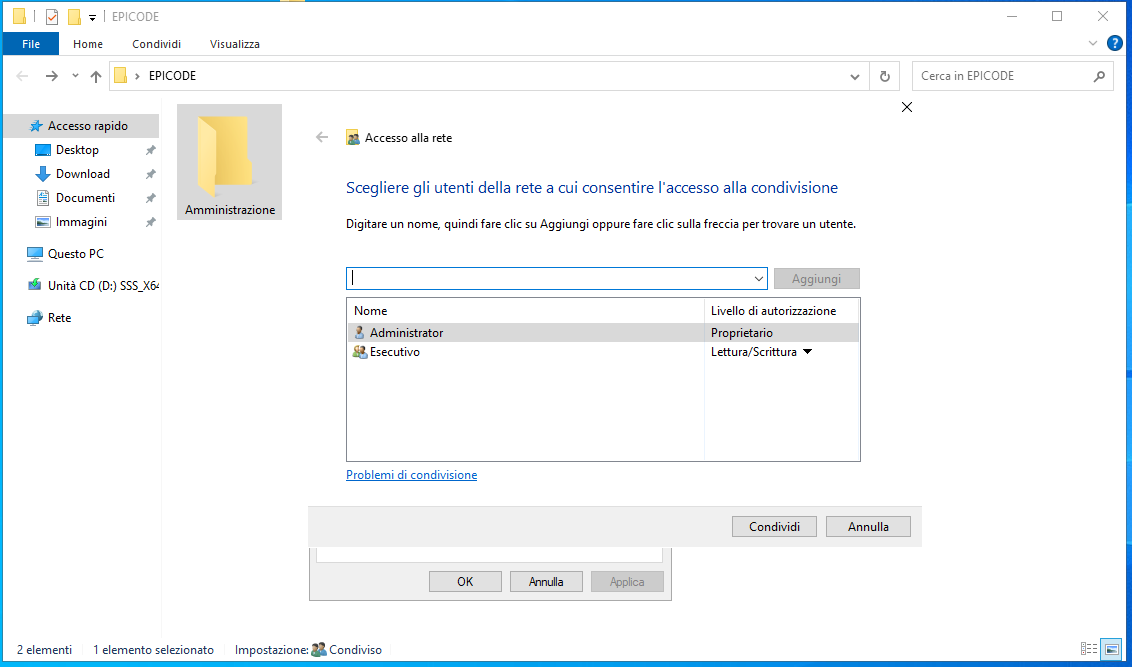
  
  
  
Possiamo adesso procedere all’assegnazione dei permessi per permettere ad ogni gruppo di visualizzare i file inerenti al lavoro.  
  
  
  
Una volta effettuato il login all’interno del dispositivo aziendale, apriamo una cartella nella sezione “Rete” e selezioniamo i file presenti all’interno del server (**WIN-NU6DCNDIKTN** in questo caso)  
  
  
  
Al suo interno troveremo tutte le cartelle presenti all’interno del Server, ma questo non significa che avremo libero accesso a tutte loro.  
  


In questo caso accederemo alla cartella “**Epicode**” che è stata messa a disposizione sia al gruppo “**Amministrazione**”, sia al gruppo “**Marketing**”.  
  


Al suo interno troveremo due cartelle: Amministrazione e Marketing. Silvia, che fa parte del gruppo Amministrazione, non potrà avere accesso alla cartella Marketing anche se presente all’interno della cartella Epicode.

La storia sarà diversa per la cartella amministrazione, dove Silvia potrà tranquillamente accedere e lavorare con i file a lei necessari.

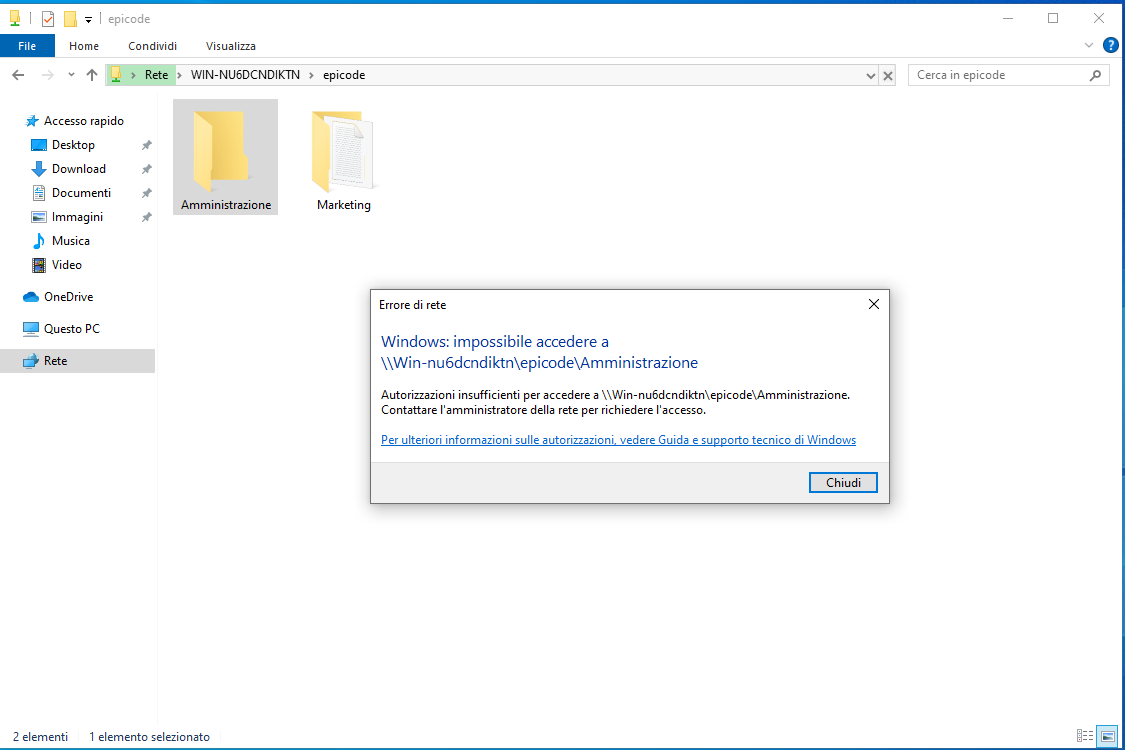


**Assegnare i permessi a ciascun gruppo**Questi sistemi di sicurezza sono stati integrati dall’amministratore di rete.  
Sarà lui a decidere, tramite direttive amministrative, chi può accedere a quale file.  
  


Possiamo notare che il gruppo “**Esecutivo**”, di cui Silvia fa parte, ha permessi di Lettura e scrittura. Ciò le permetterà di accedere ai file all’interno della cartella “**Amministrazione**”.

Stesso procedimento verrà attuato per tutti gli utenti presenti all’interno dell’unità organizzativa “**Marketing**” che, a loro volta, avranno libero accesso alla cartella Marketing, ma non a quella “**Amministrazione**”

Ecco uno screen di Davide, facente parte del team Marketing, che prova ad accedere alla cartella “**Amministrazione**”



**Conclusione**  
  
Garantire che un sistema Windows Server sia configurato correttamente e che ogni dipendente abbia accesso solo ai dati strettamente necessari è fondamentale per proteggere l’integrità e la sicurezza dell’organizzazione. Una configurazione adeguata riduce le vulnerabilità del sistema, limitando il rischio di attacchi informatici e di accessi non autorizzati. Inoltre, applicare il principio del ***least privilege*** (minimo privilegio) minimizza i danni potenziali causati da errori umani o da eventuali compromissioni delle credenziali. Questo approccio non solo tutela i dati sensibili e garantisce la conformità alle normative sulla protezione delle informazioni, ma favorisce anche una gestione più efficiente delle risorse, migliorando la produttività aziendale e la fiducia dei clienti nei confronti dell’organizzazione.