S10L5 Progetto Settimanale

Introduzione:

Il compito settimanale, prevedeva l'utilizzo e l'apprendimento di **Windows Server 2022** e dello strumento **Server Manager**, per creare **nuove unità organizzative** e per definire e dare **ruoli** e **permessi** ai vari utenti, dell'ambiente di lavoro.

Cos'è Windows Server 2022?

Windows Server 2022 è un sistema operativo server di Microsoft pensato per garantire sicurezza avanzata, elevate prestazioni e integrazione con il cloud. Progettato per rispondere alle esigenze delle infrastrutture **IT moderne**, sia **locali** che **ibride**.

Tra le sue principali innovazioni, spicca la sicurezza avanzata grazie al modello **Secured-core server**, che sfrutta tecnologie come il **secure boot**, **TPM 2.0** e la **virtualizzazione** per proteggere i dati sensibili. Inoltre, il supporto nativo per **HTTPS** e **TLS 1.3** garantisce una crittografia aggiornata e sicura.

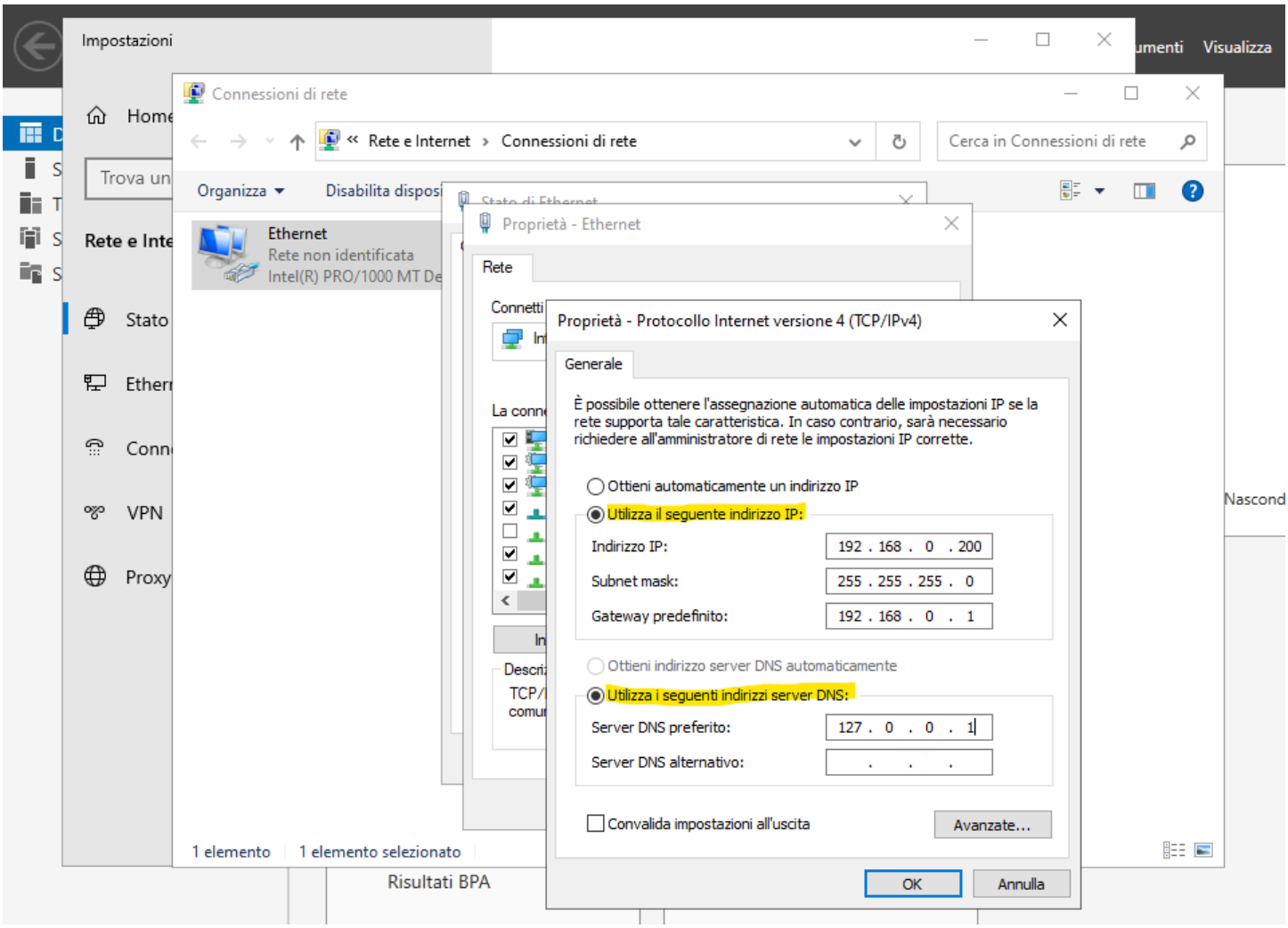
Che cos'è Server Manager?

Server Manager è uno strumento di gestione centralizzato incluso nei sistemi operativi Windows Server. Progettato per facilitare l'amministrazione di server locali e remoti, consente agli amministratori IT di configurare, monitorare e gestire i server da un'unica interfaccia grafica.

Infatti andremo ad utilizzare questo strumento per **definire** e **configurare i ruoli**;

Configurazione unità:

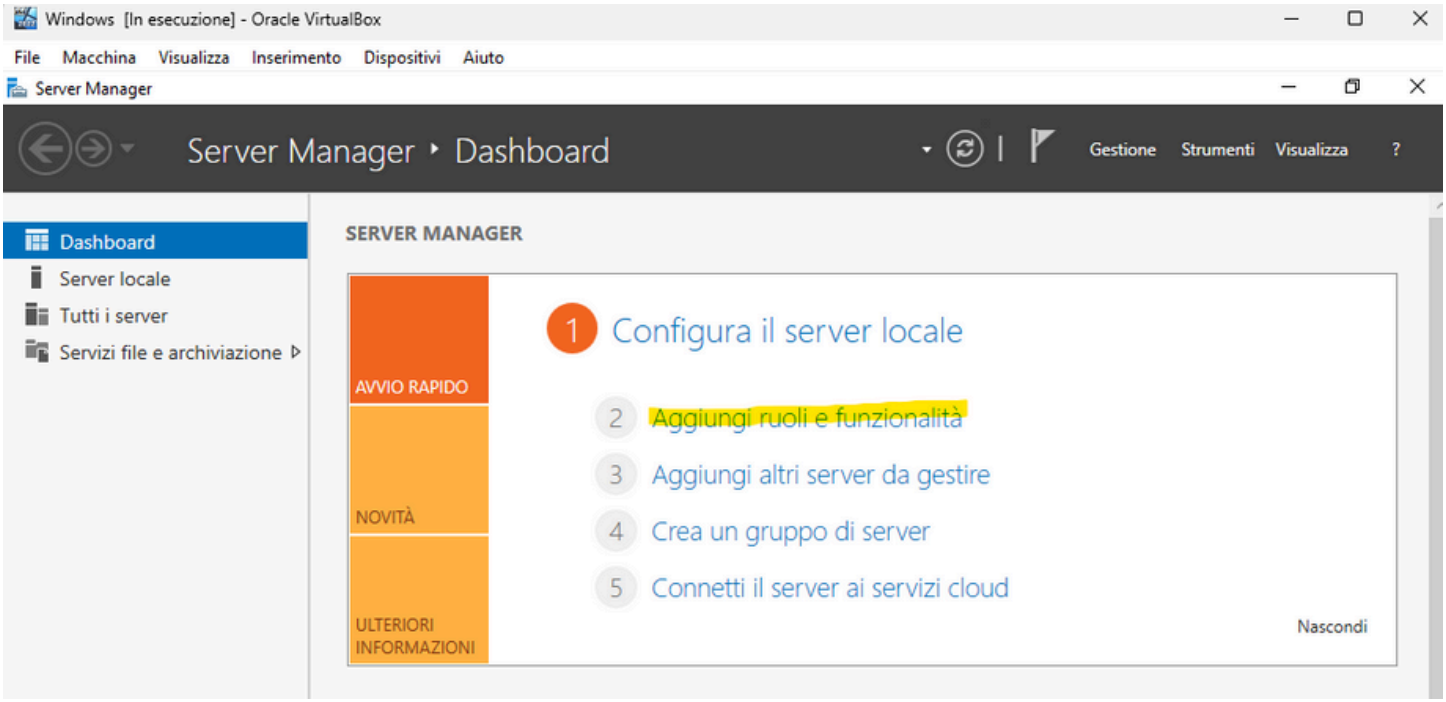
Iniziamo configurando l'indirizzo IP di Windows Server **manualmente** mettendo ovviamente quello della **nostra network**. Andando su **configura scheda di rete**, **proprietà** e poi mettendo **utilizza il seguente indirizzo IP**;



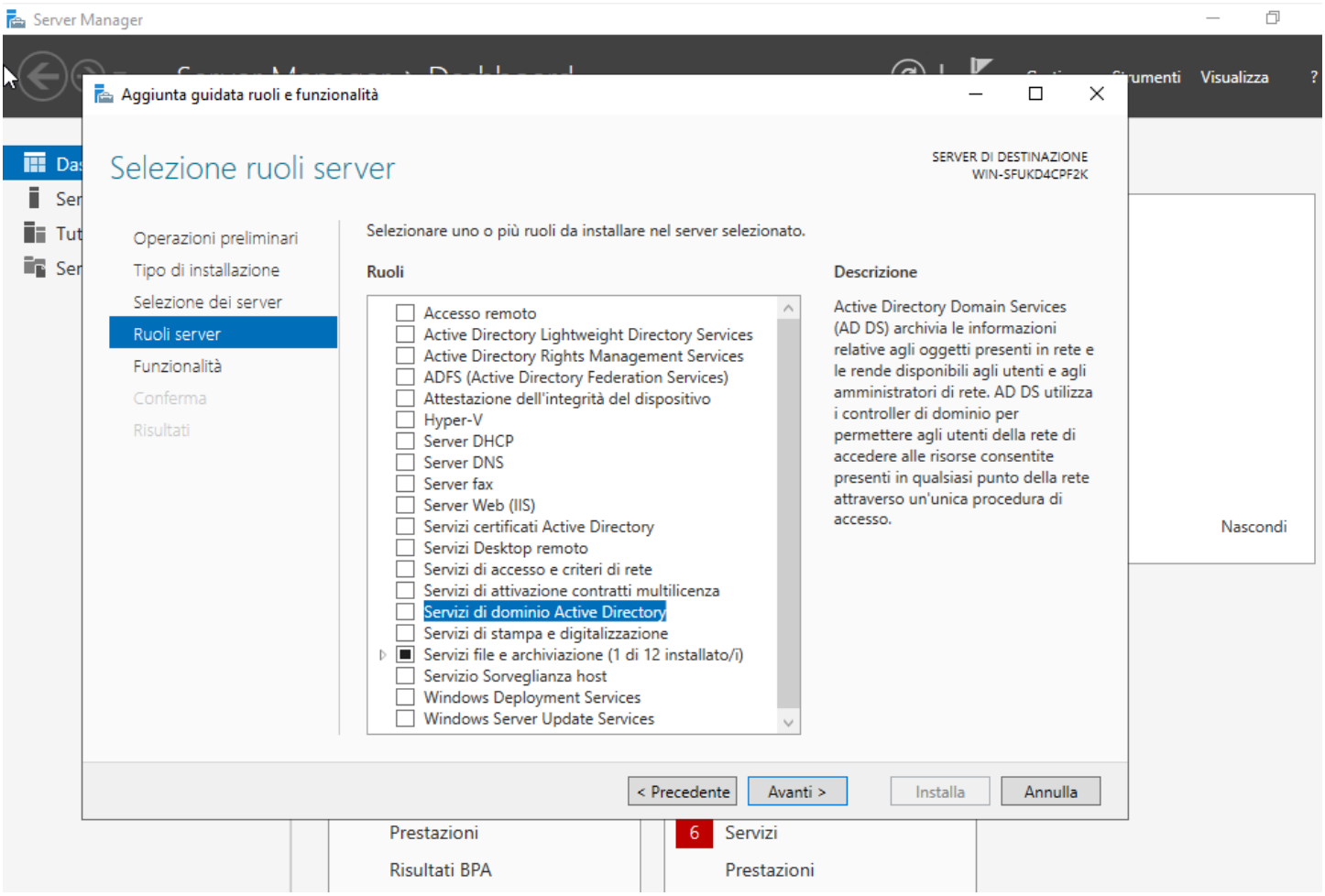
Le modifiche sono state apportate previo **riavvio** della macchina, dopo che dal **cmd** assodo che l'indirizzo IP della macchina è quello che ho inserito io

```
Amministratore: Prompt dei comandi
Microsoft Windows [Versione 10.0.20348.587]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\Administrator>ifconfig
"ifconfig" non è riconosciuto come comando interno o esterno,
 un programma eseguibile o un file batch.

C:\Users\Administrator>ipconfig

Configurazione IP di Windows


Scheda Ethernet Ethernet:

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::2002:c7e2:ba09:373c%6
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.0.200
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . : 192.168.0.1

C:\Users\Administrator>
```

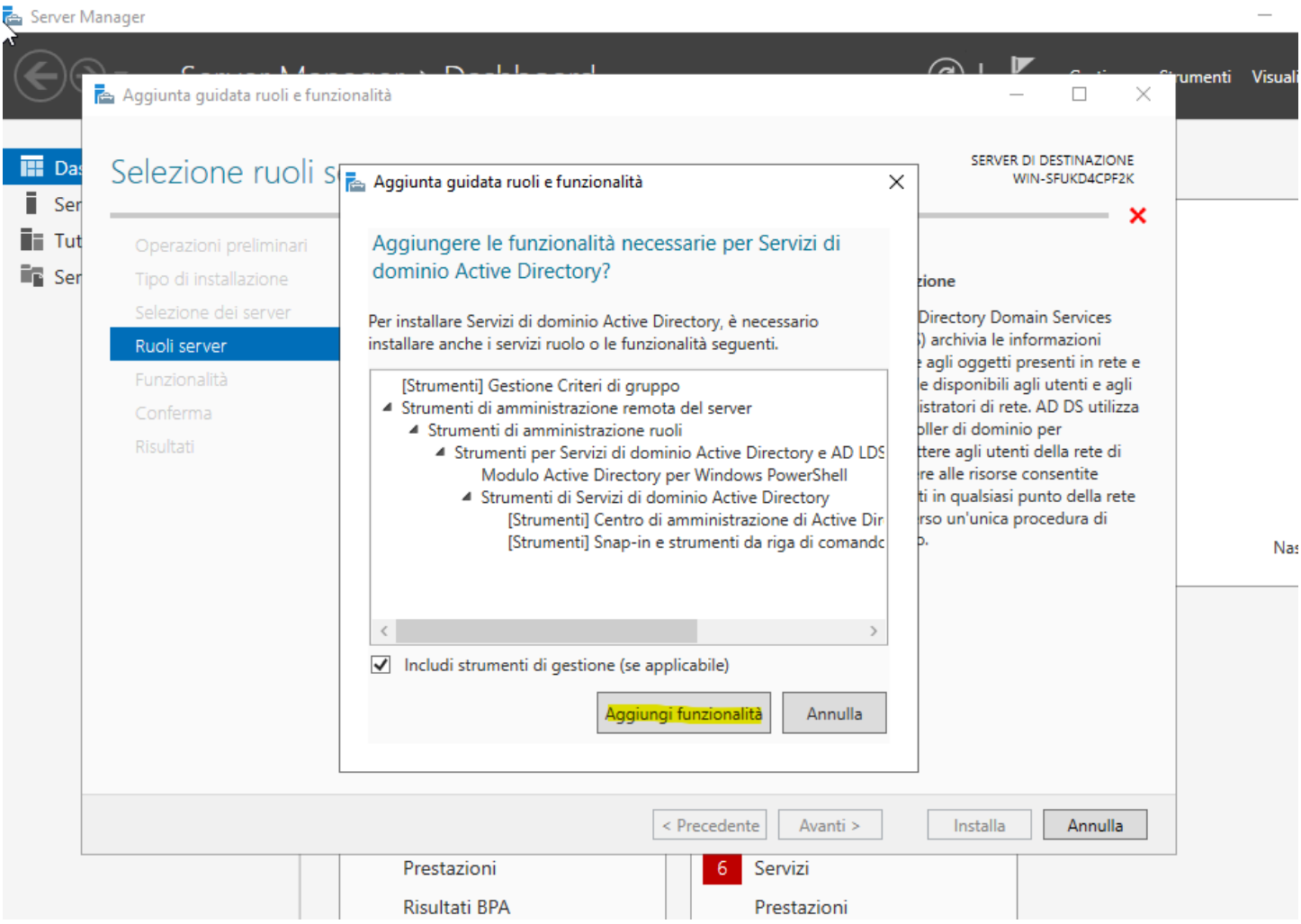
Ora passiamo a Server Manager, dove andremo a creare i ruoli e funzionalità, cliccando appunto su **aggiungi ruoli e funzionalità**;



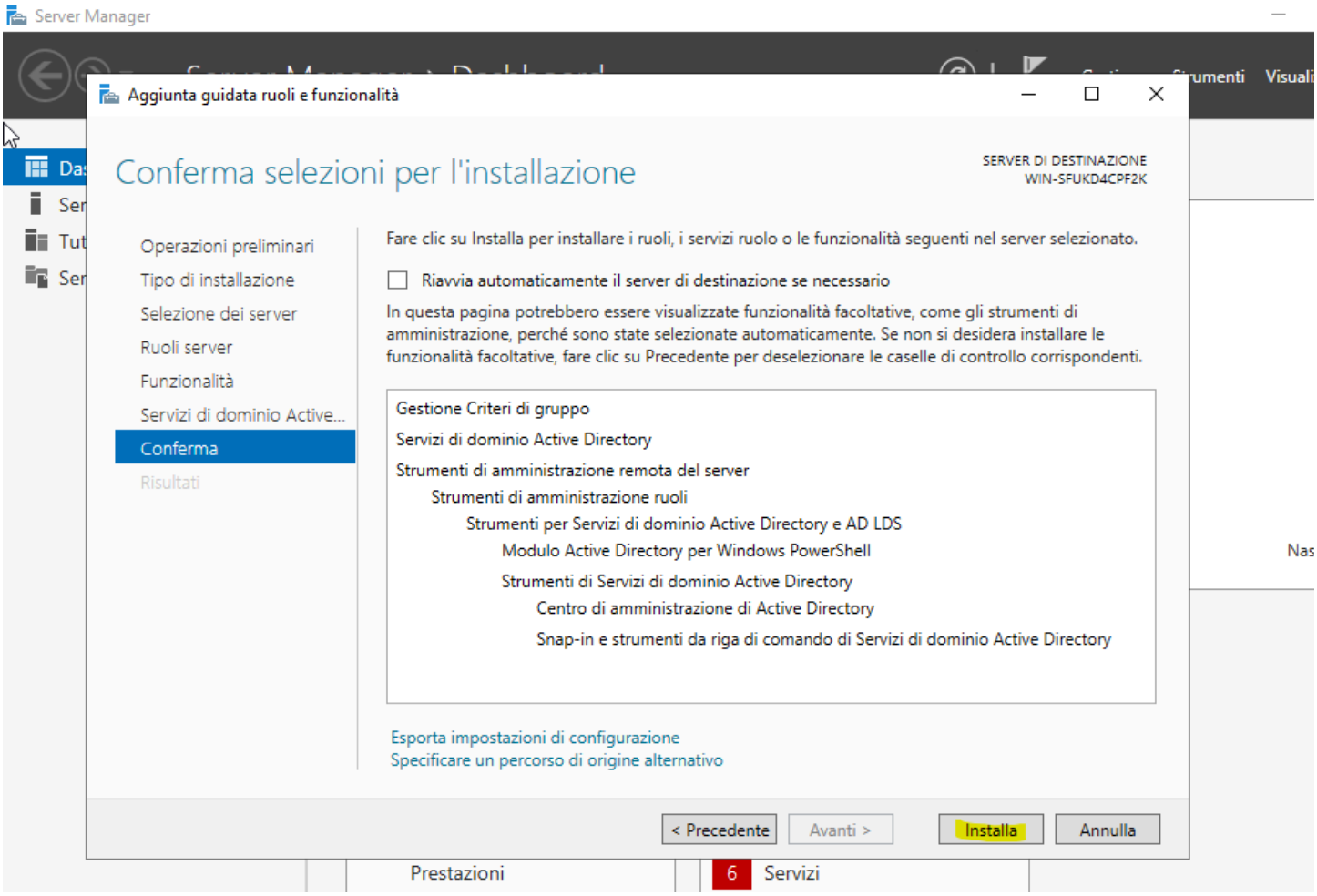
Clicchiamo sempre avanti finche non arriviamo a questa pagine dove andremo ad abilitare il ruolo **Servizi di dominio Active Directory**;



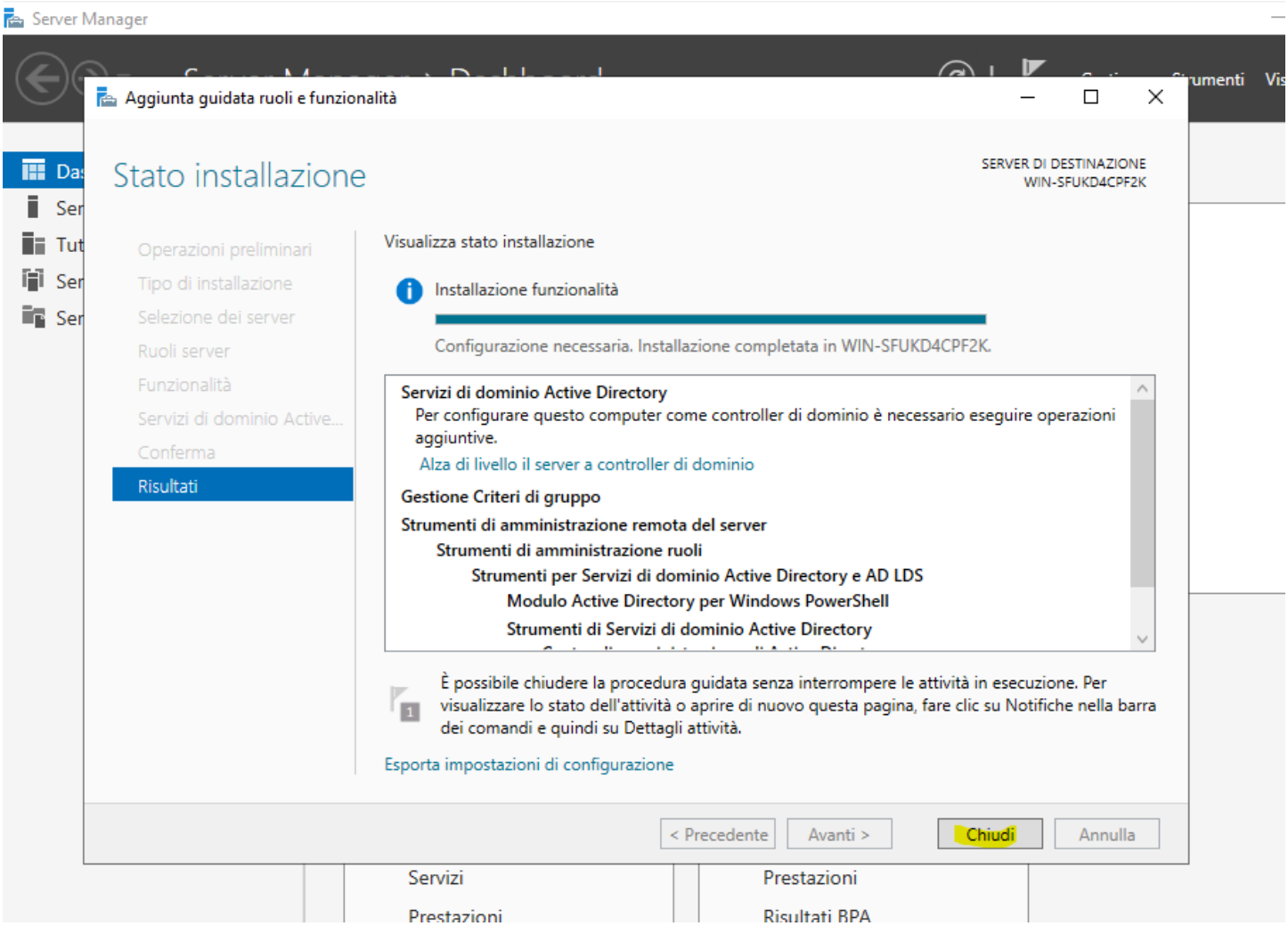
Clicchiamo su **aggiungi funzionalità**;



Ed installiamo:

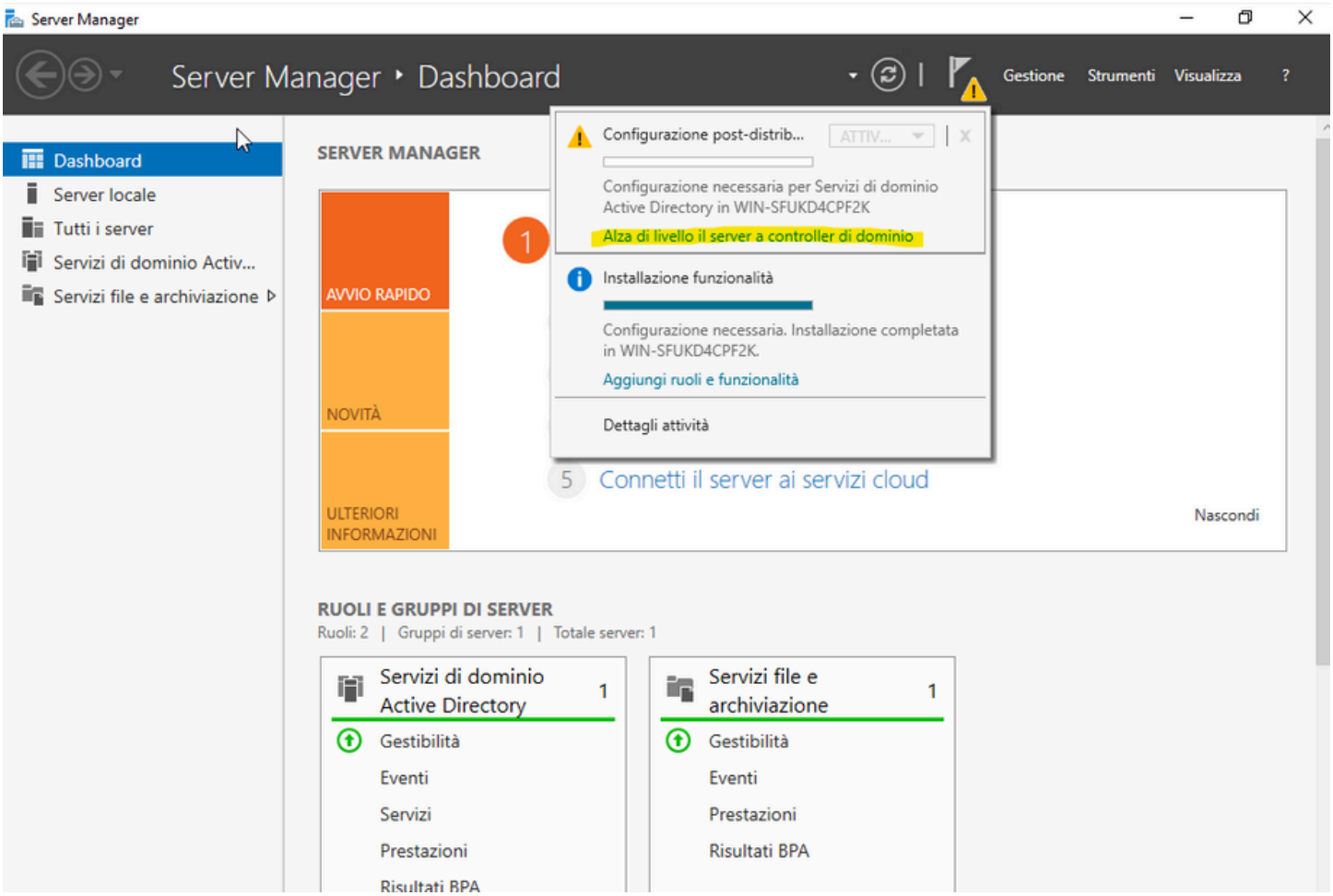


Una volta **completato il download**, possiamo **chiudere** questa pagina;



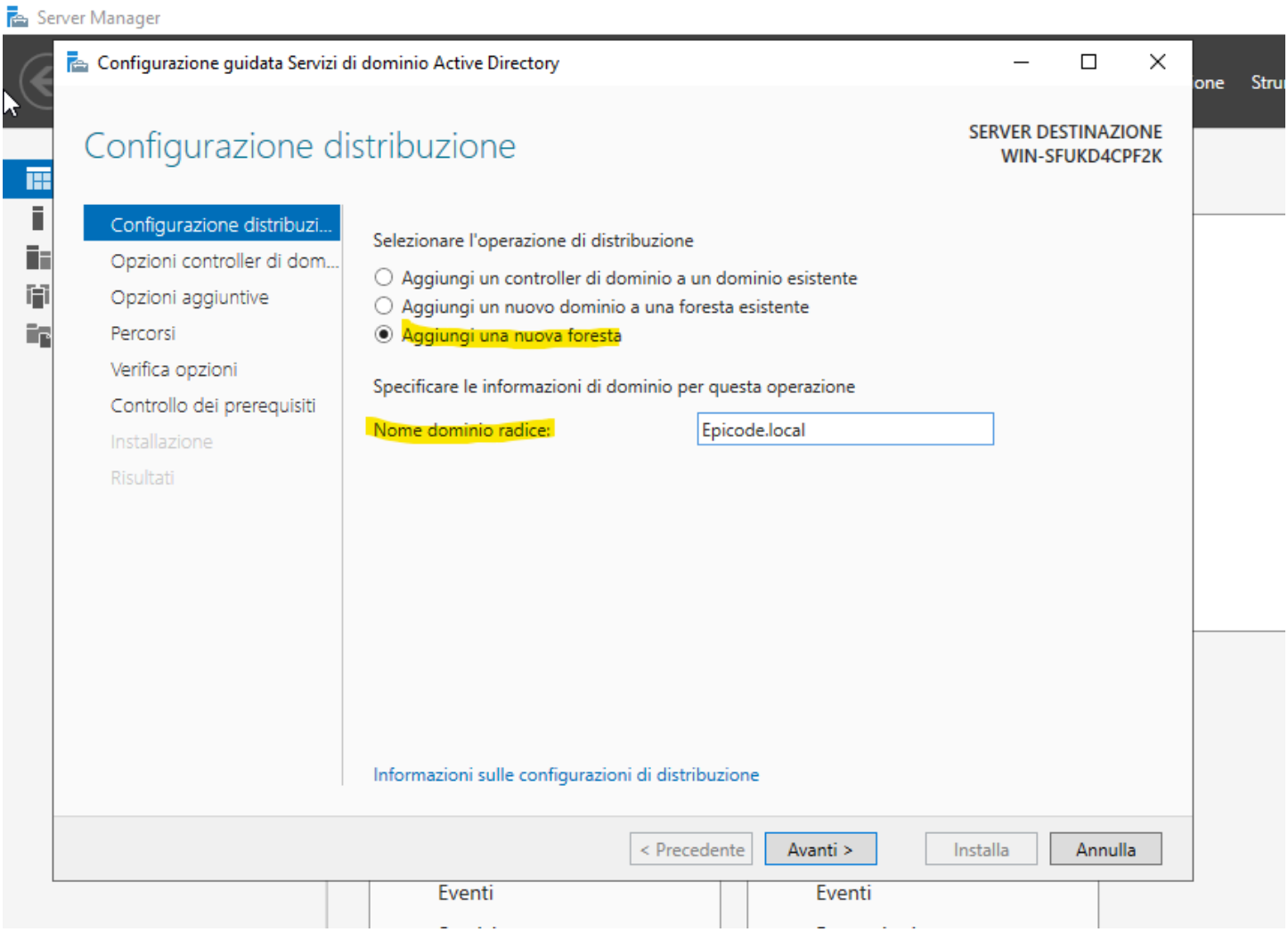
Successivamente ci apparirà questa **flag**, che ci chiederà di alzare di livello il server a **controller di dominio**:

Un **controller di dominio** è un server che gestisce l'autenticazione e l'autorizzazione degli utenti e dei dispositivi in una rete. Funziona come il "cuore" di Active Directory, il sistema di directory di Microsoft, centralizzando la gestione delle identità e delle risorse.

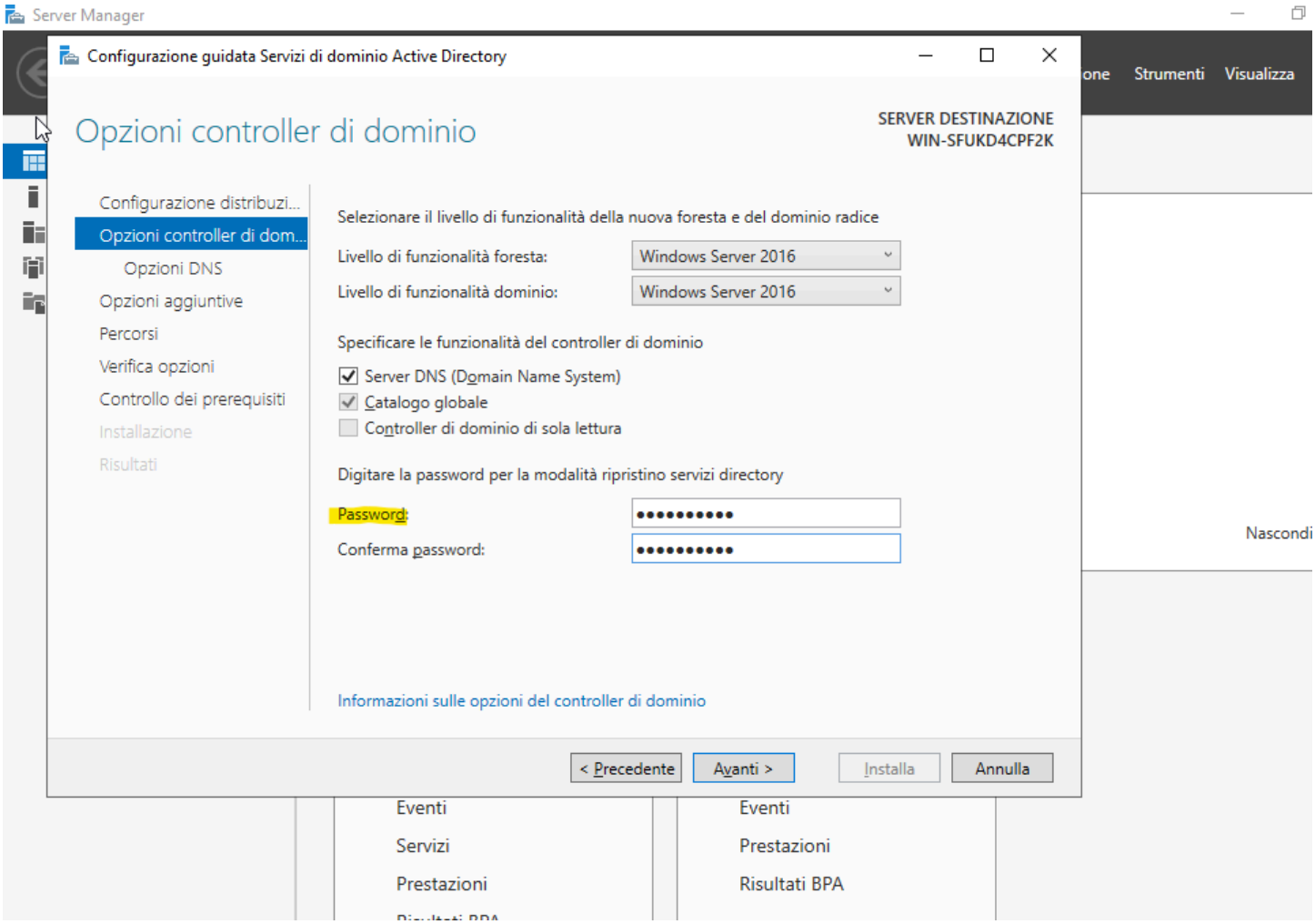


Dopo averci cliccato, scegliamo l'opzione **aggiungi una nuova foresta**. Abbiamo scelto **Epicode.local** come nome per la nostra nuova foresta Active Directory, creando una rete completamente autonoma e separata da qualsiasi altra struttura esterna. Con **Epicode.local**, stiamo stabilendo il dominio principale della nostra infrastruttura, che gestirà tutti gli utenti, dispositivi e risorse all'interno della nostra rete.

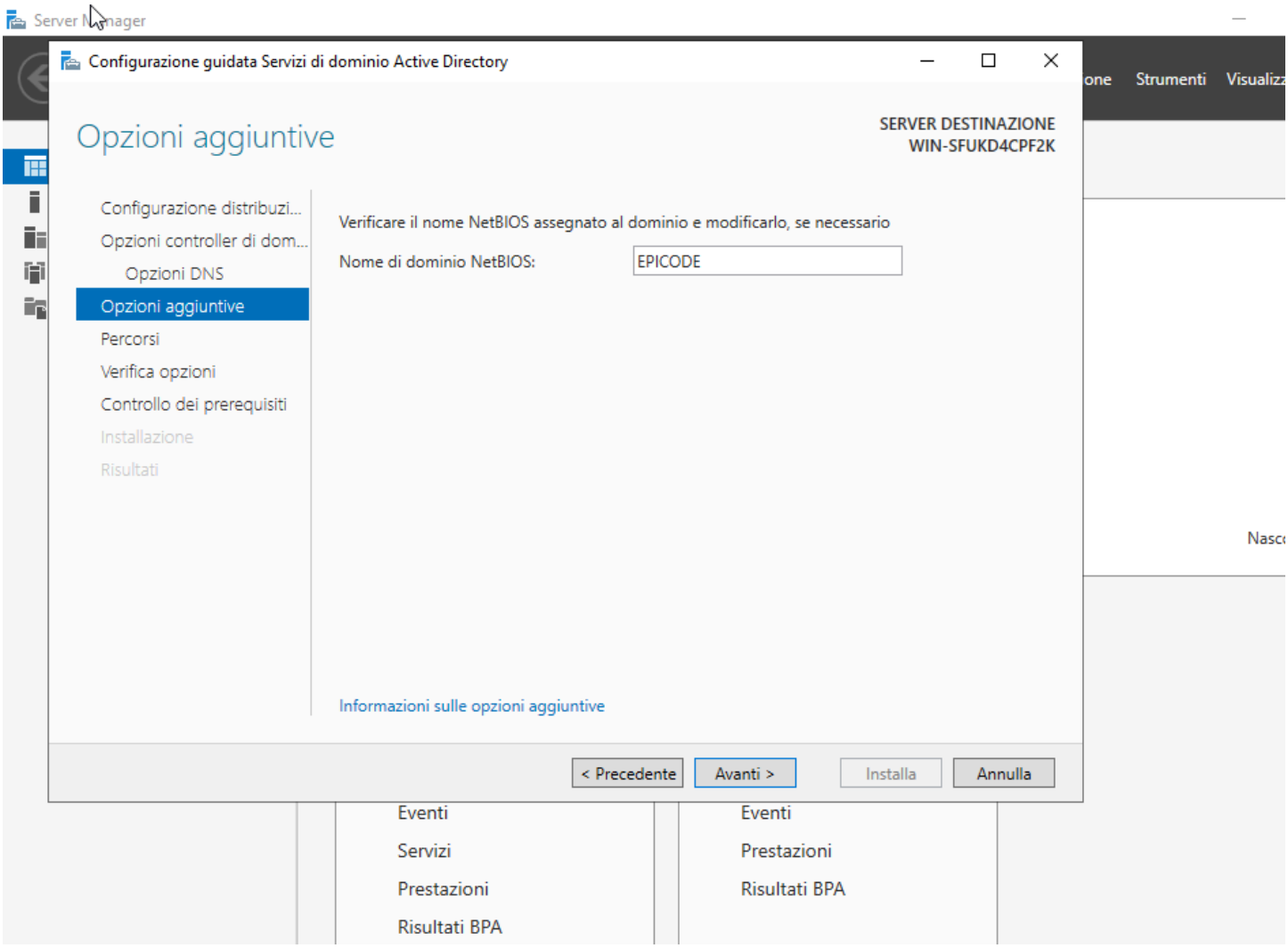
Il dominio **.local** è ideale per ambienti interni, poiché assicura che la nostra rete rimanga isolata da internet, evitando conflitti con altri domini pubblici. In questo modo, possiamo avere il pieno controllo sulla gestione delle risorse e sulla sicurezza senza interferenze esterne.



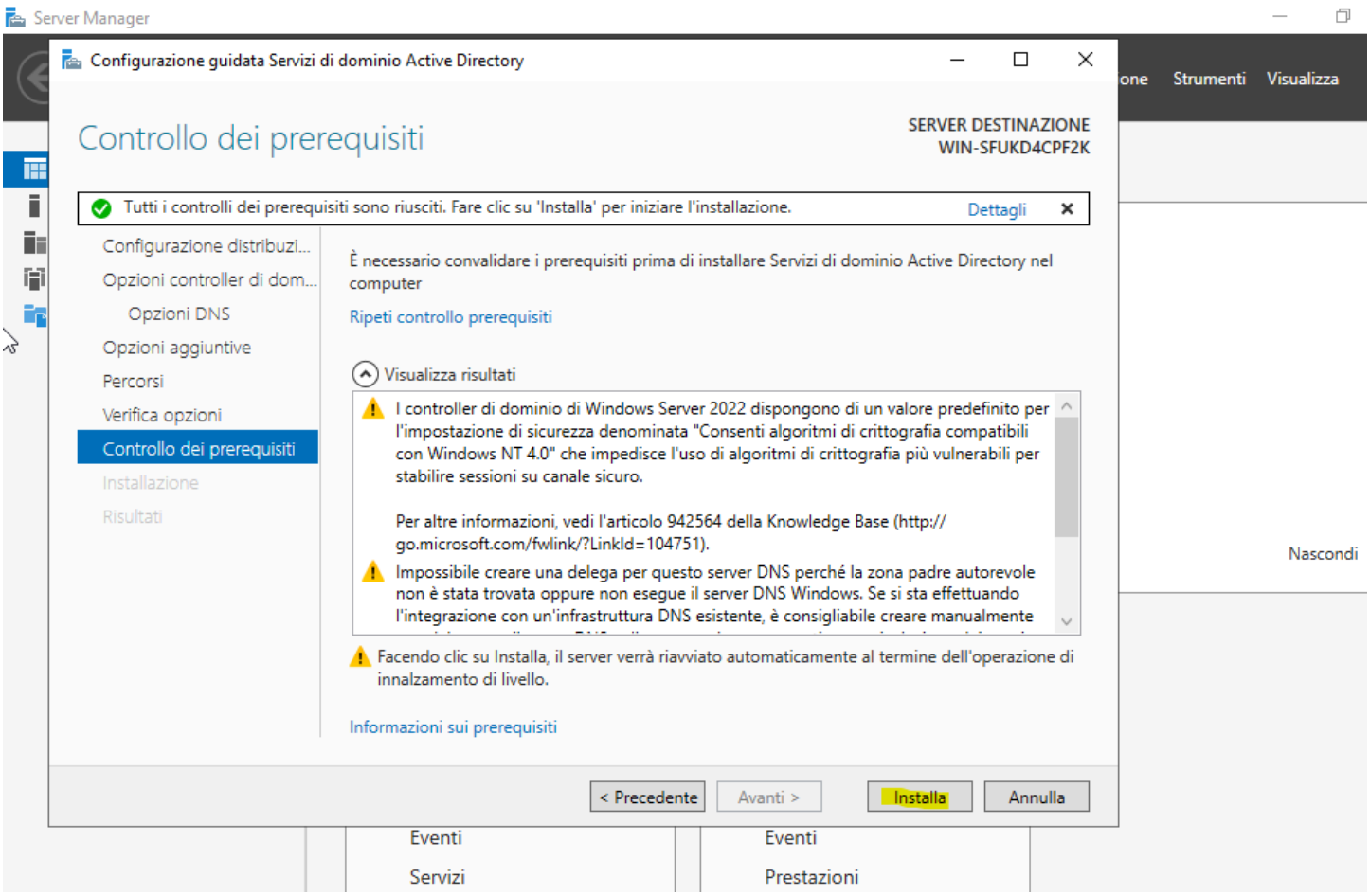
Mettiamo la password per il **ripristino dei servizi directory**:



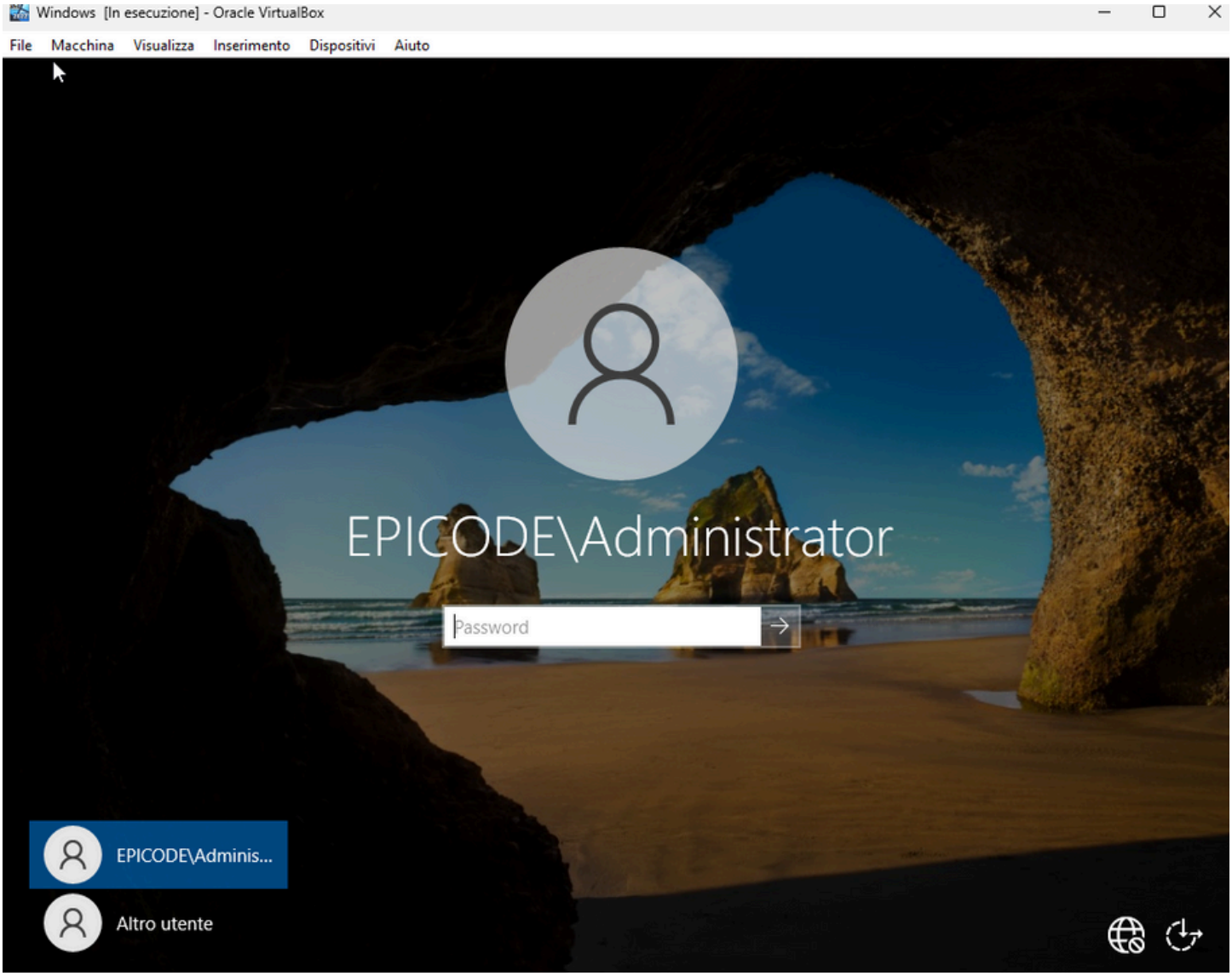
Quando abbiamo scelto **epicode.local** come nome del dominio, il sistema ha automaticamente generato un nome **NETBIOS** abbreviato, che in questo caso è **EPICODE**. Questo nome **NETBIOS** viene usato principalmente per identificare il nostro dominio in ambienti Windows, in particolare nelle operazioni di condivisione di file, gestione delle risorse e comunicazione tra i dispositivi.



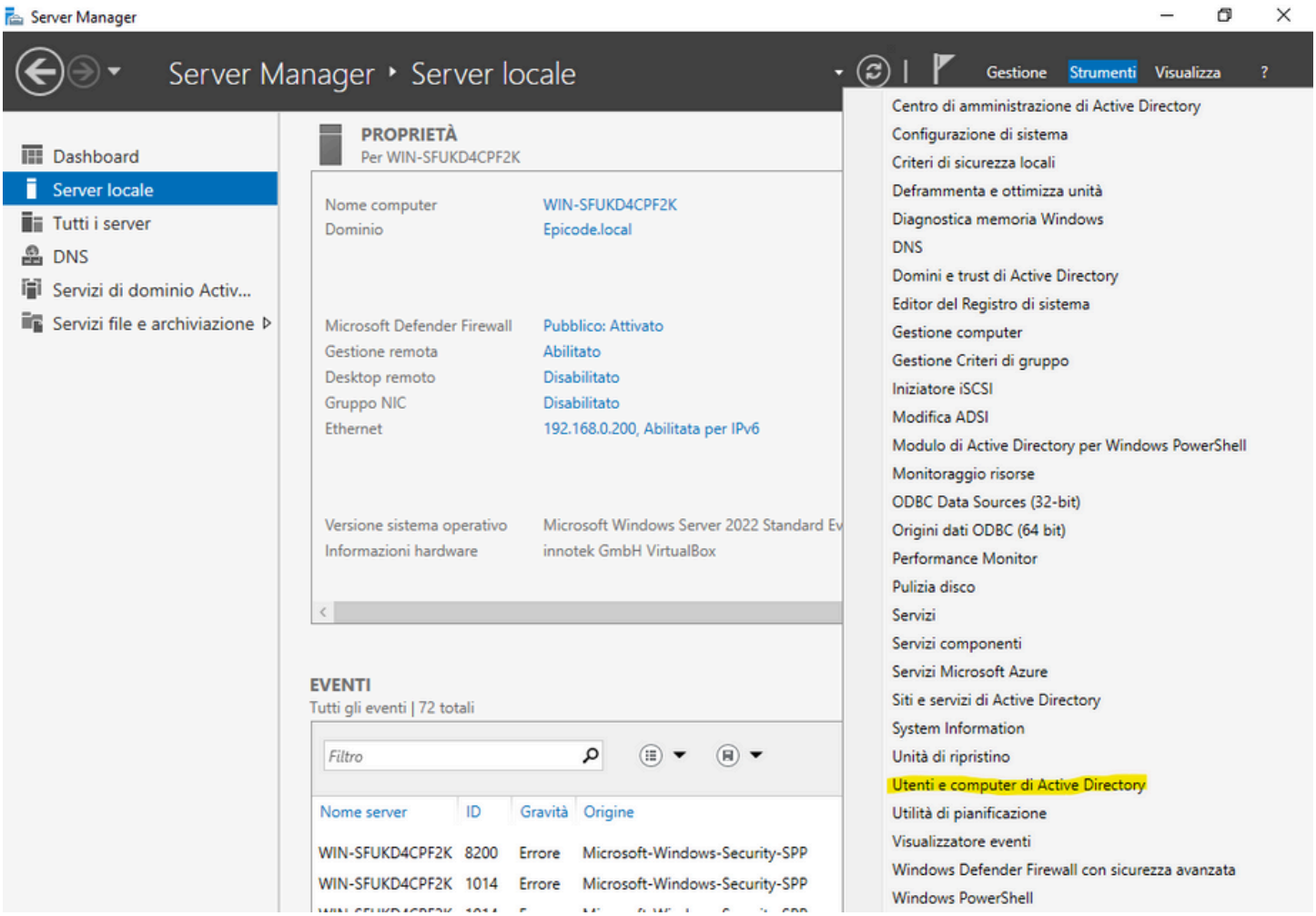
Proseguiamo premendo installa:



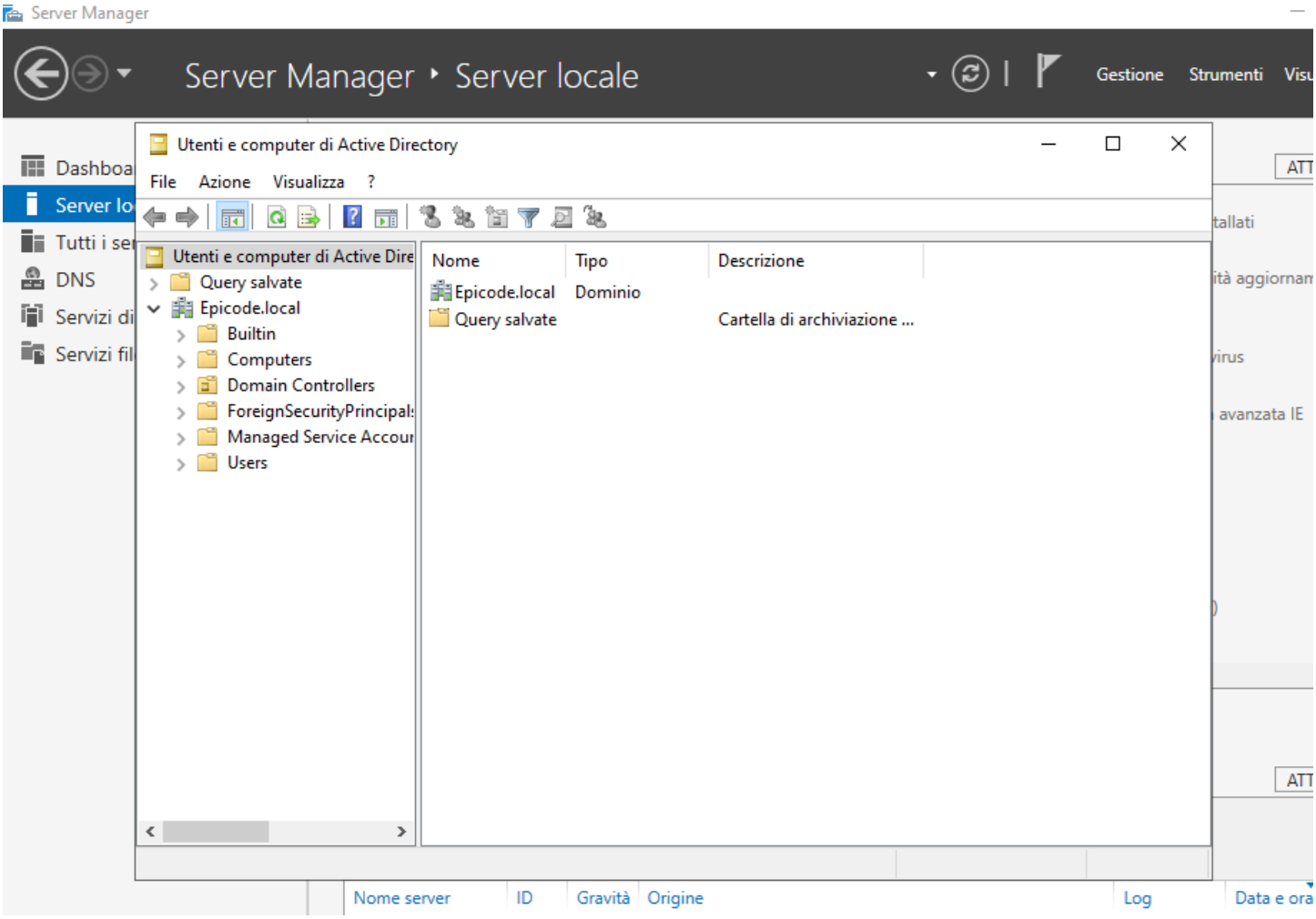
Finita l'installazione verrà riavviata la macchina:



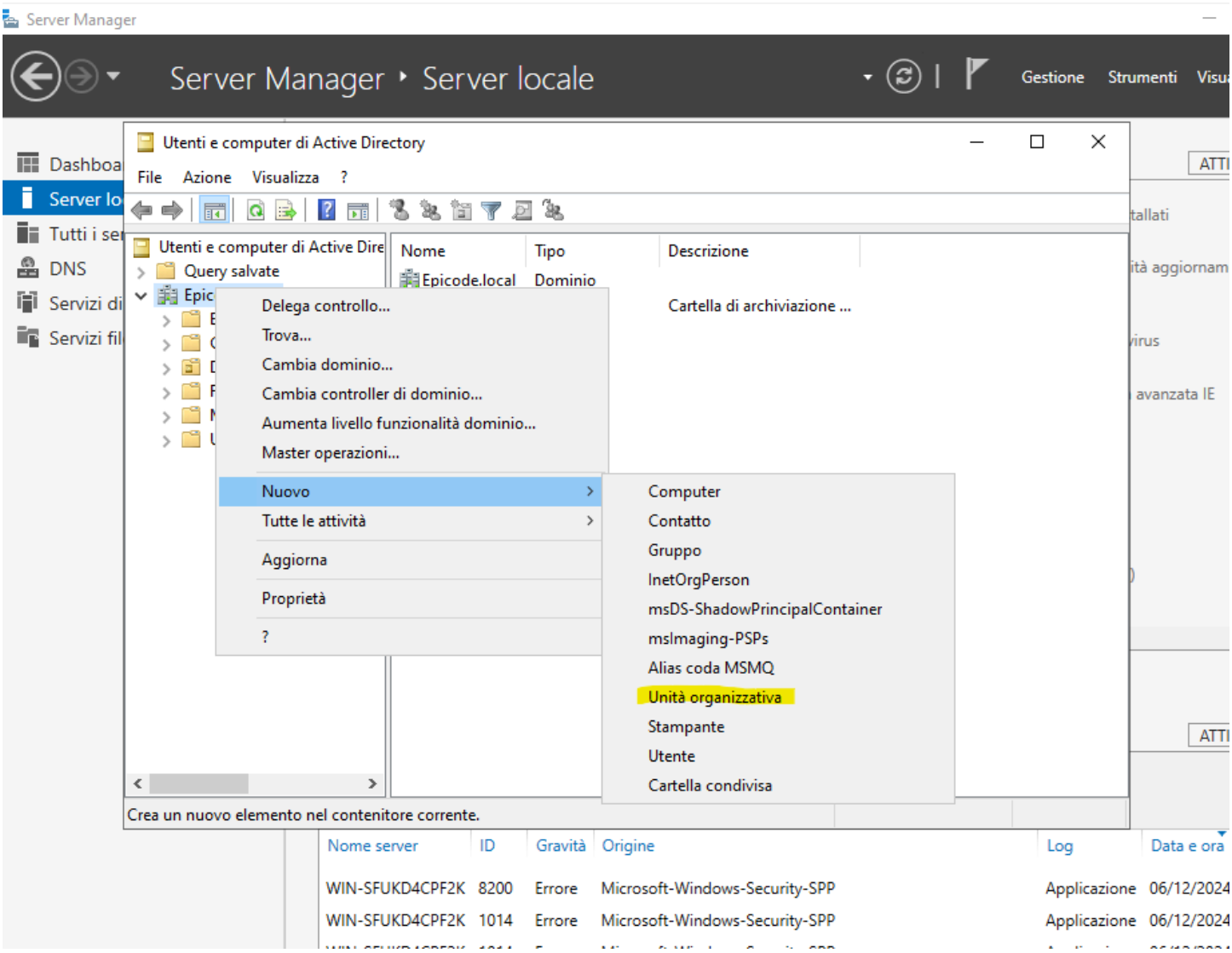
Una volta riavviata la macchina torniamo su **Server Manager**, **strumenti** e **utenti e computer di active directory**. Lo strumento è uno degli strumenti principali per la **gestione** di **Active Directory**. Serve per **amministrare** e **configurare** gli oggetti all'interno di un dominio, come **utenti**, **gruppi**, **computer** e altre **risorse di rete**;



Qui ci verrà mostrato l'insieme delle risorse utenti e computer;



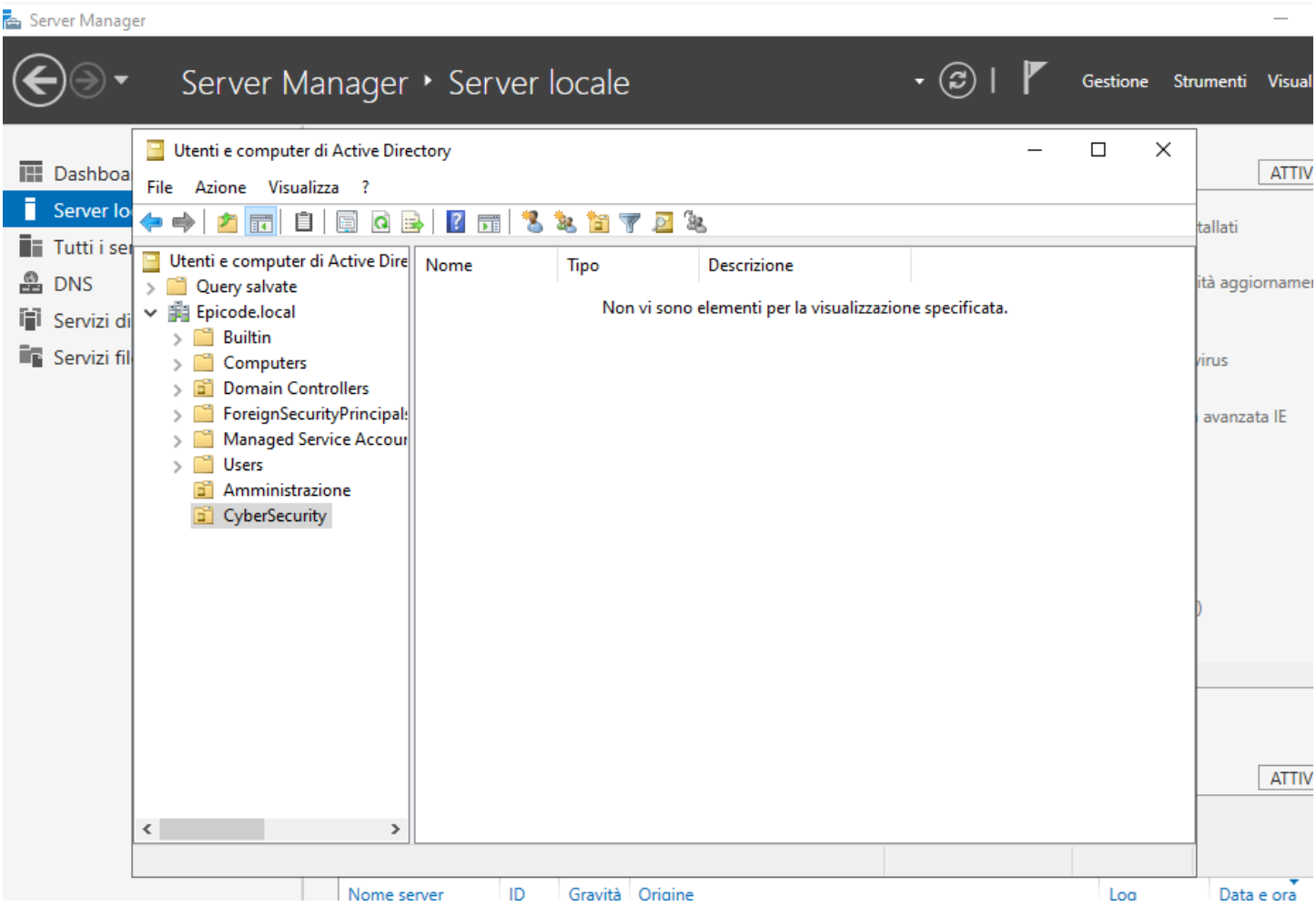
Tasto destro del mouse su **Epicode.local**, **nuovo**, **Unità organizzativa**. Così facendo andremo a creare un nuove **unità organizzative** che poi andremo a configurare. Il termine **unità organizzativa** si riferisce a una **struttura logica** all'interno di **Active Directory** che aiuta a organizzare e gestire oggetti come utenti, gruppi e computer in modo più efficiente. Le unità organizzative permettono di suddividere l'Active Directory in sezioni più piccole, in modo da applicare politiche e configurazioni specifiche a ciascun gruppo.



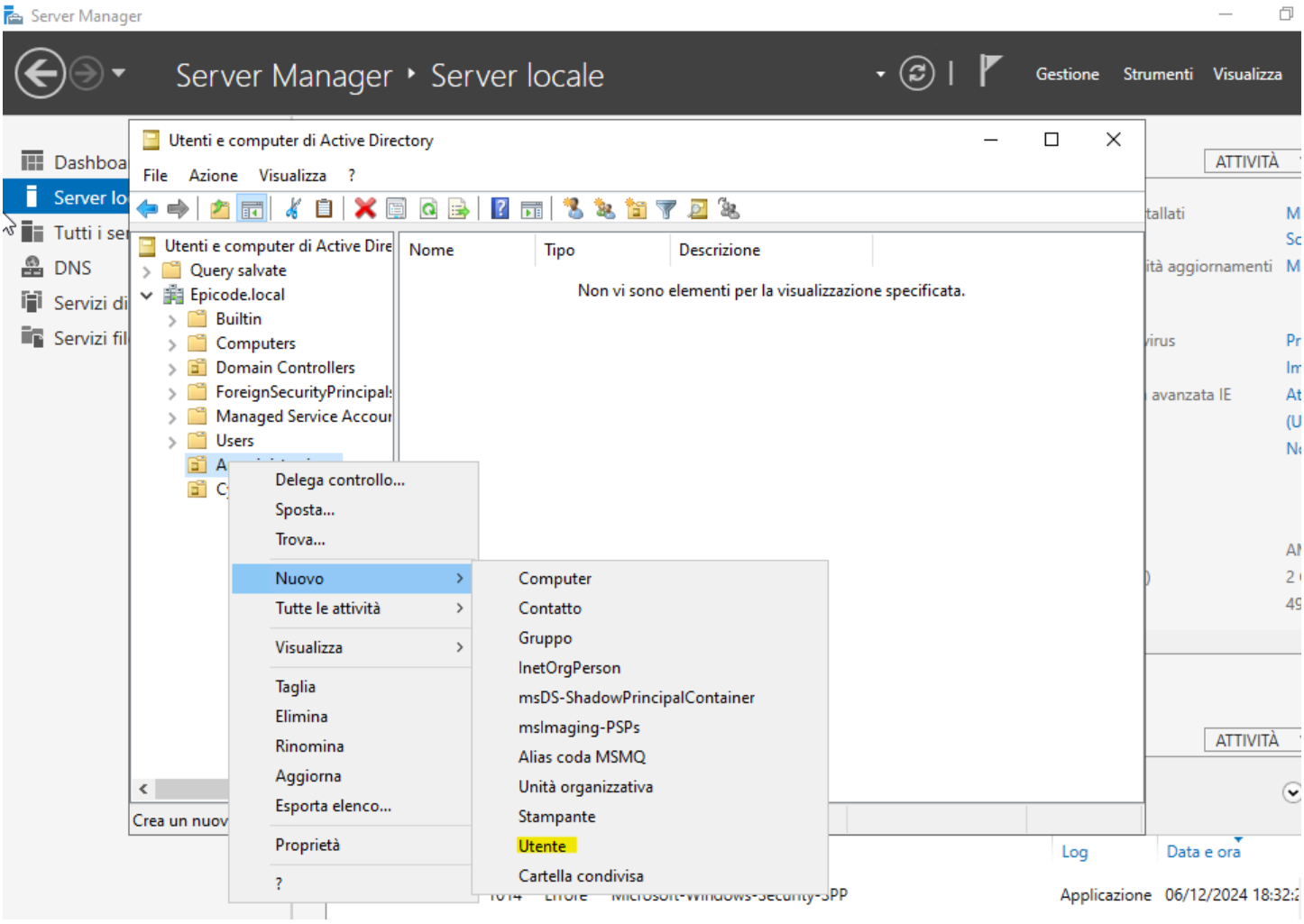
Ne abbiamo create 2:

Amministrazione;

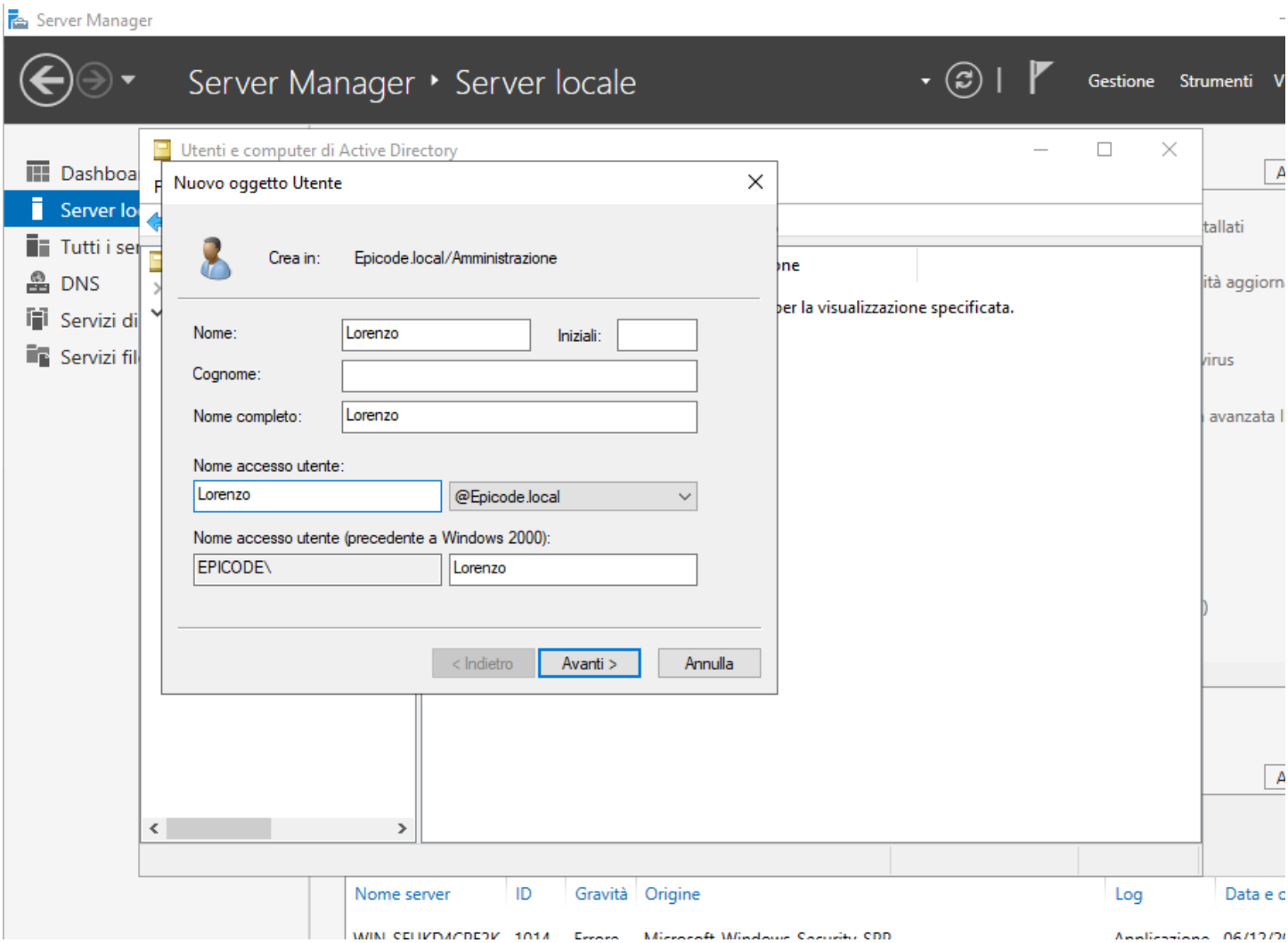
CyberSecurity;



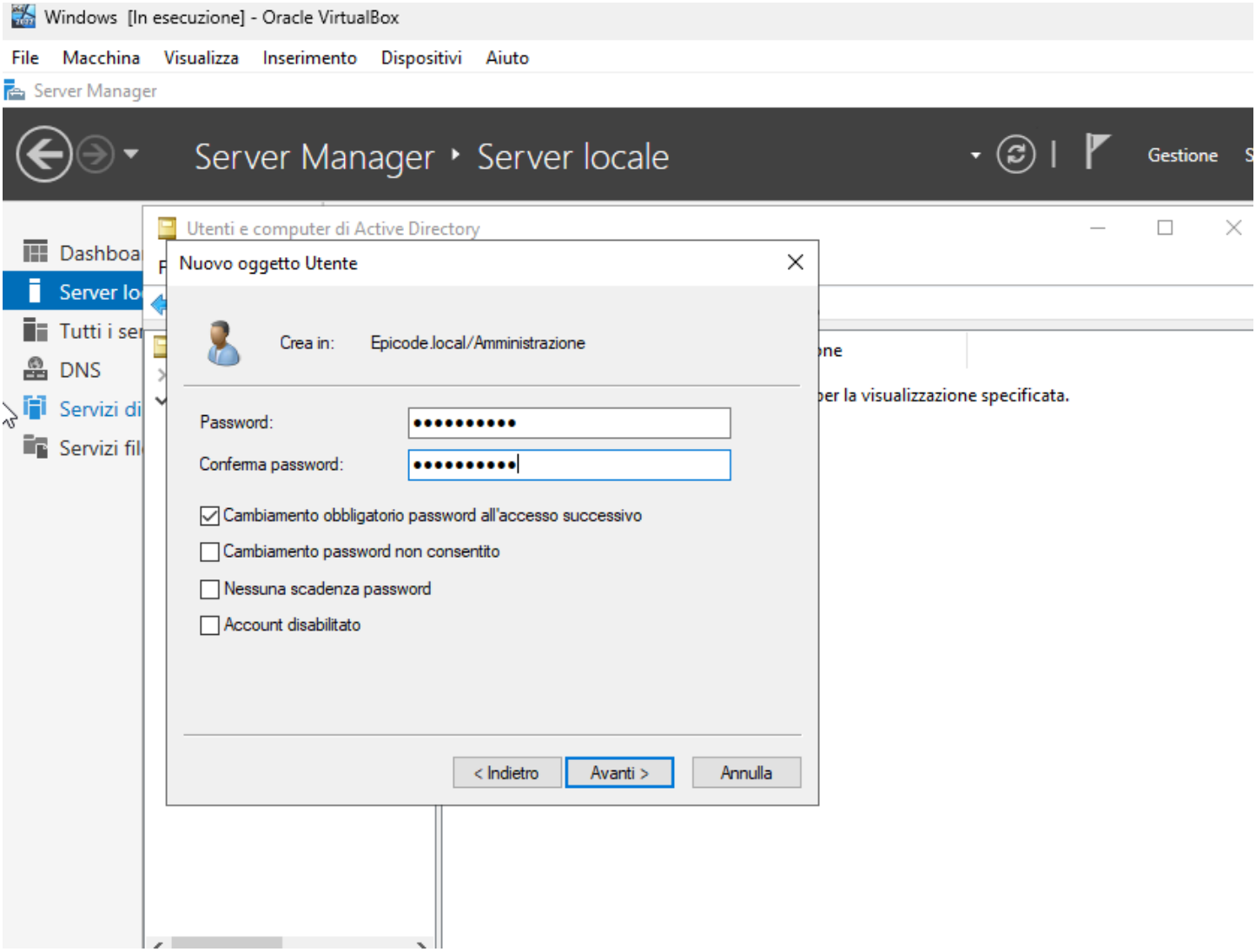
Come una **matriosca** andremo a creare dentro le unità organizzative, gli utenti;



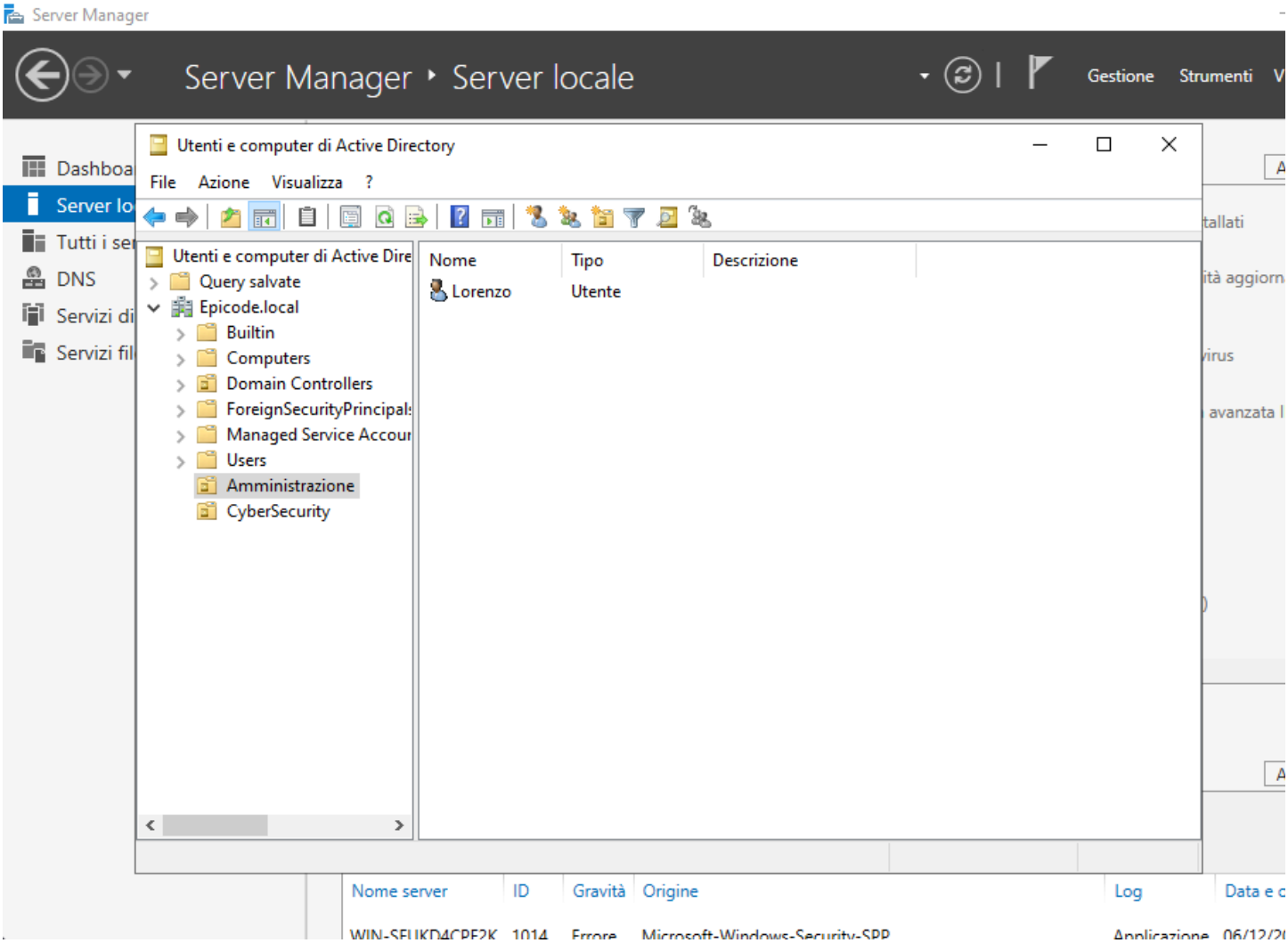
Andiamo ad inserire i **nomi**, ed anche il **nome accesso utente**;



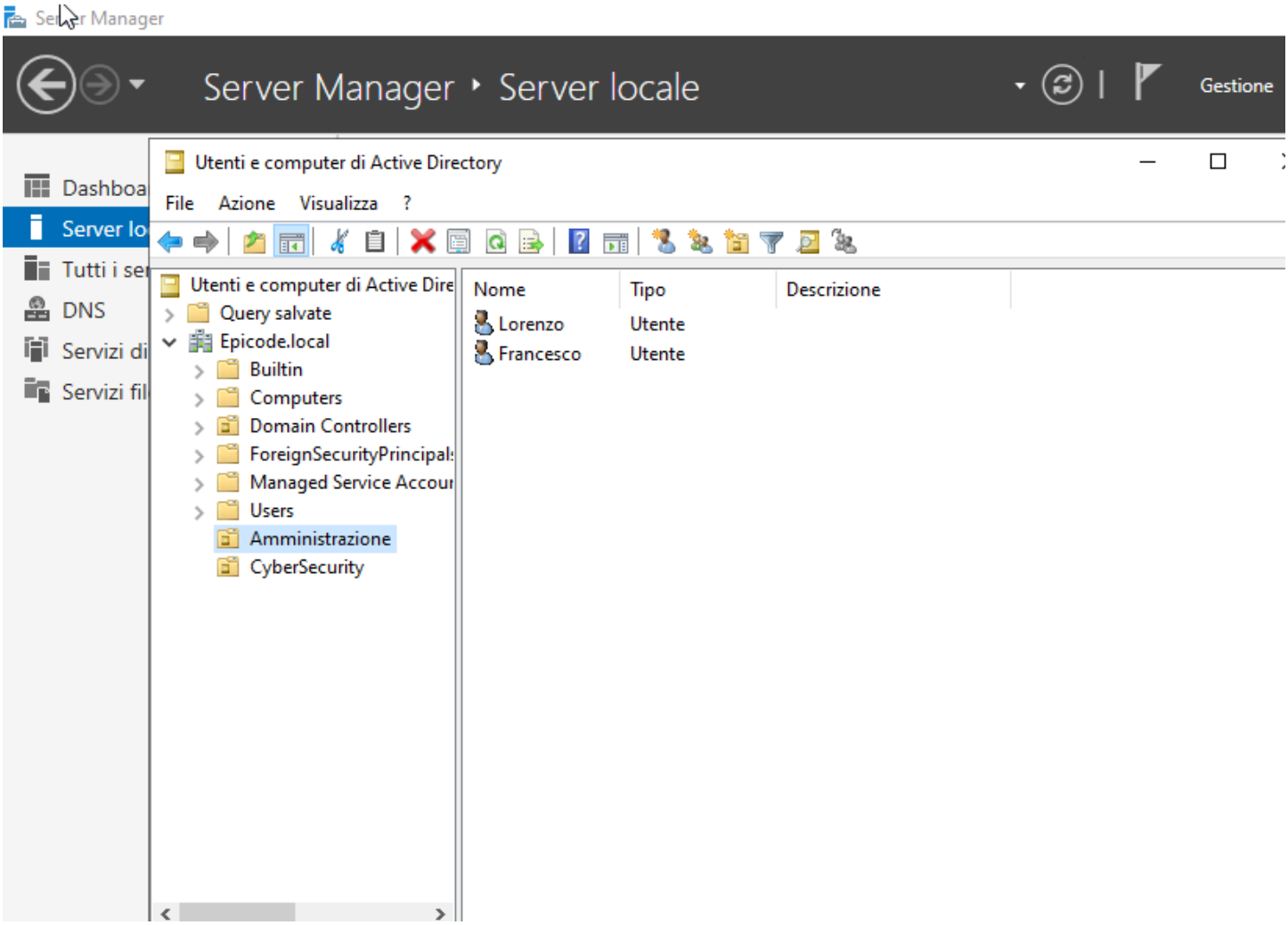
Ed andiamo a fornire anche una **password provvisoria**, che spuntando la flag **“cambiamento obbligatorio password all’accesso successivo”**, l’utente andrà a cambiare al primo accesso;



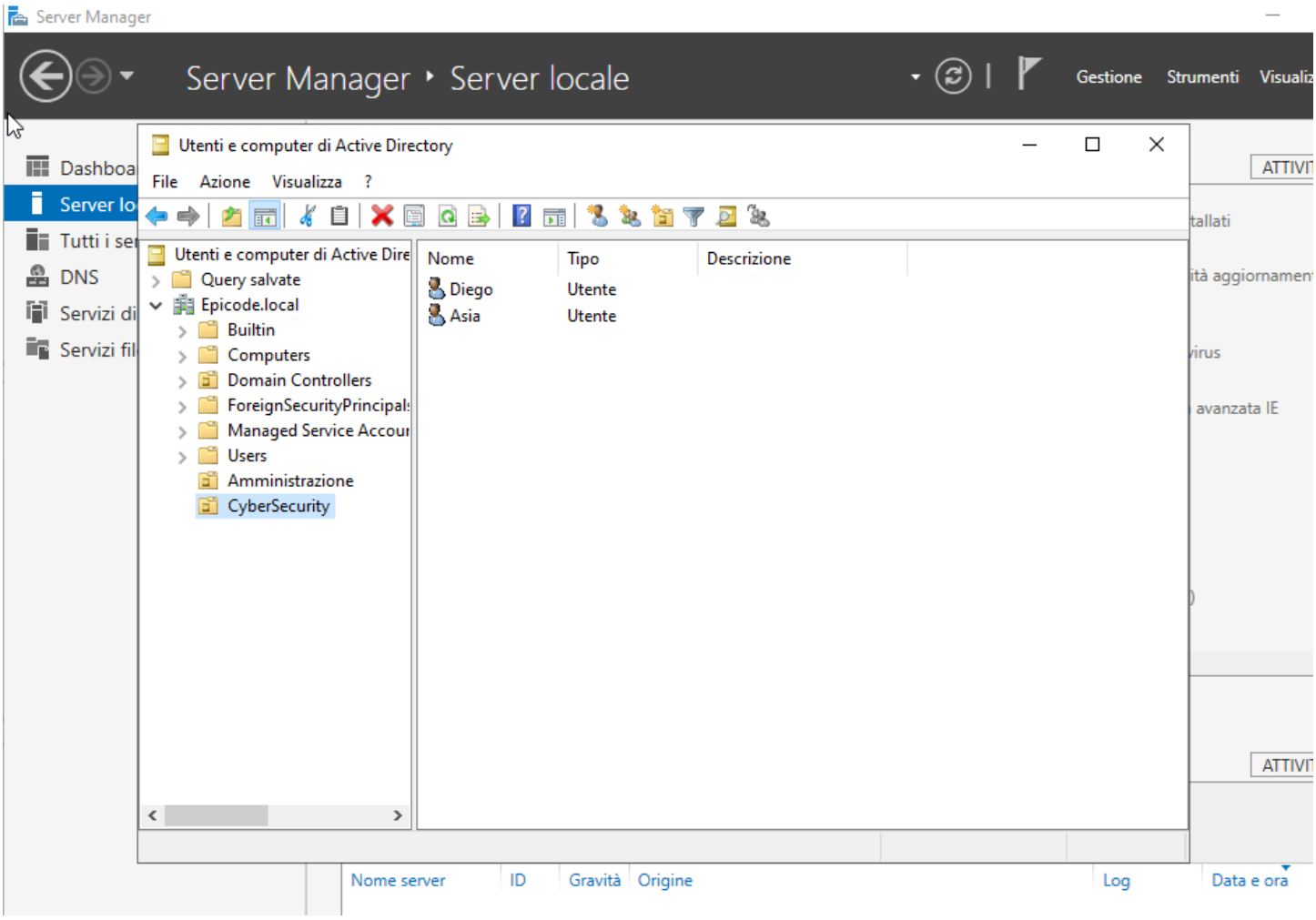
Così facendo abbiamo creato il primo utente, nell'**unità Amministrazione**:



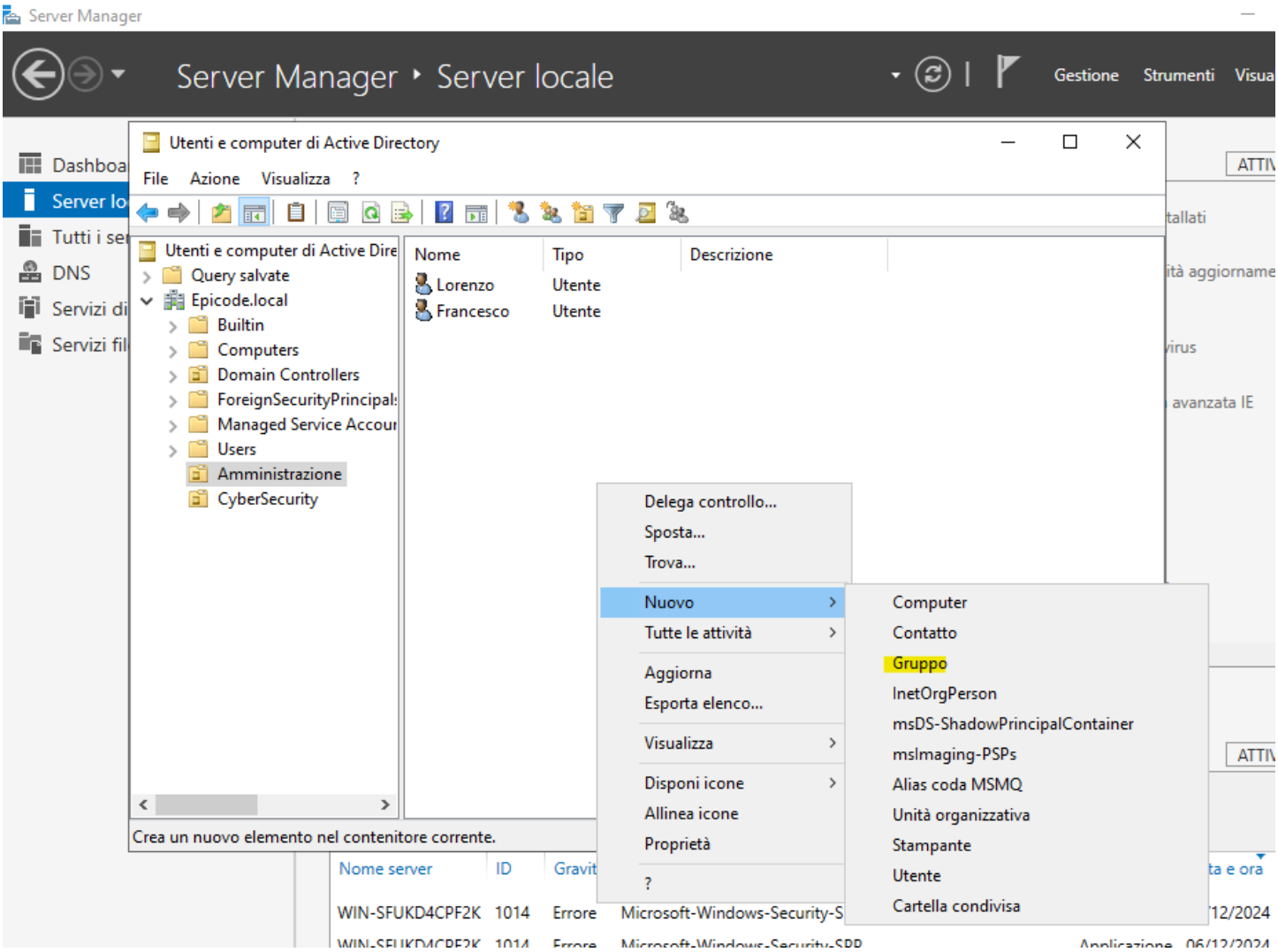
E cosi via per il secondo;



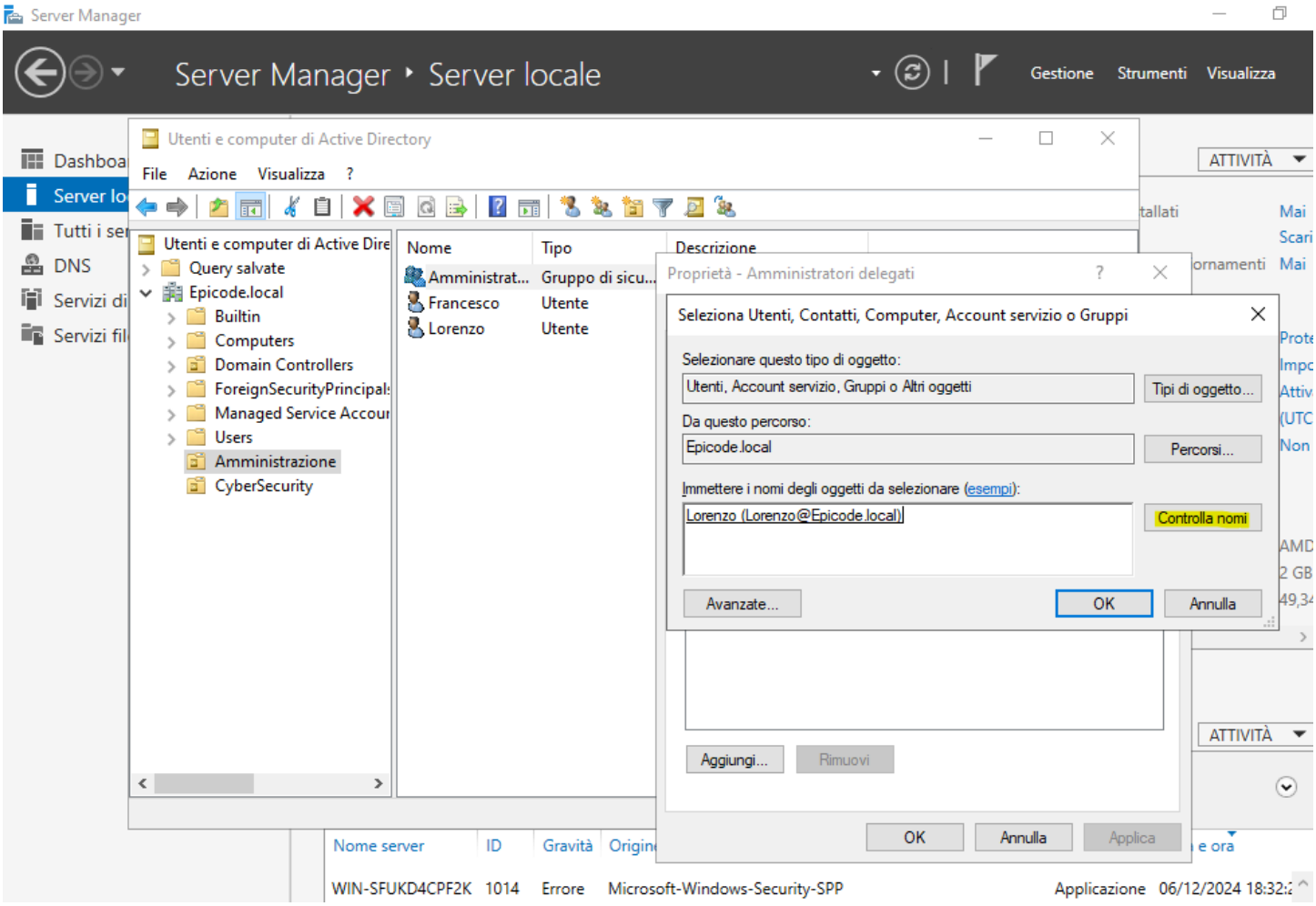
E gli altri 2 nell'unità **CyberSecurity**:



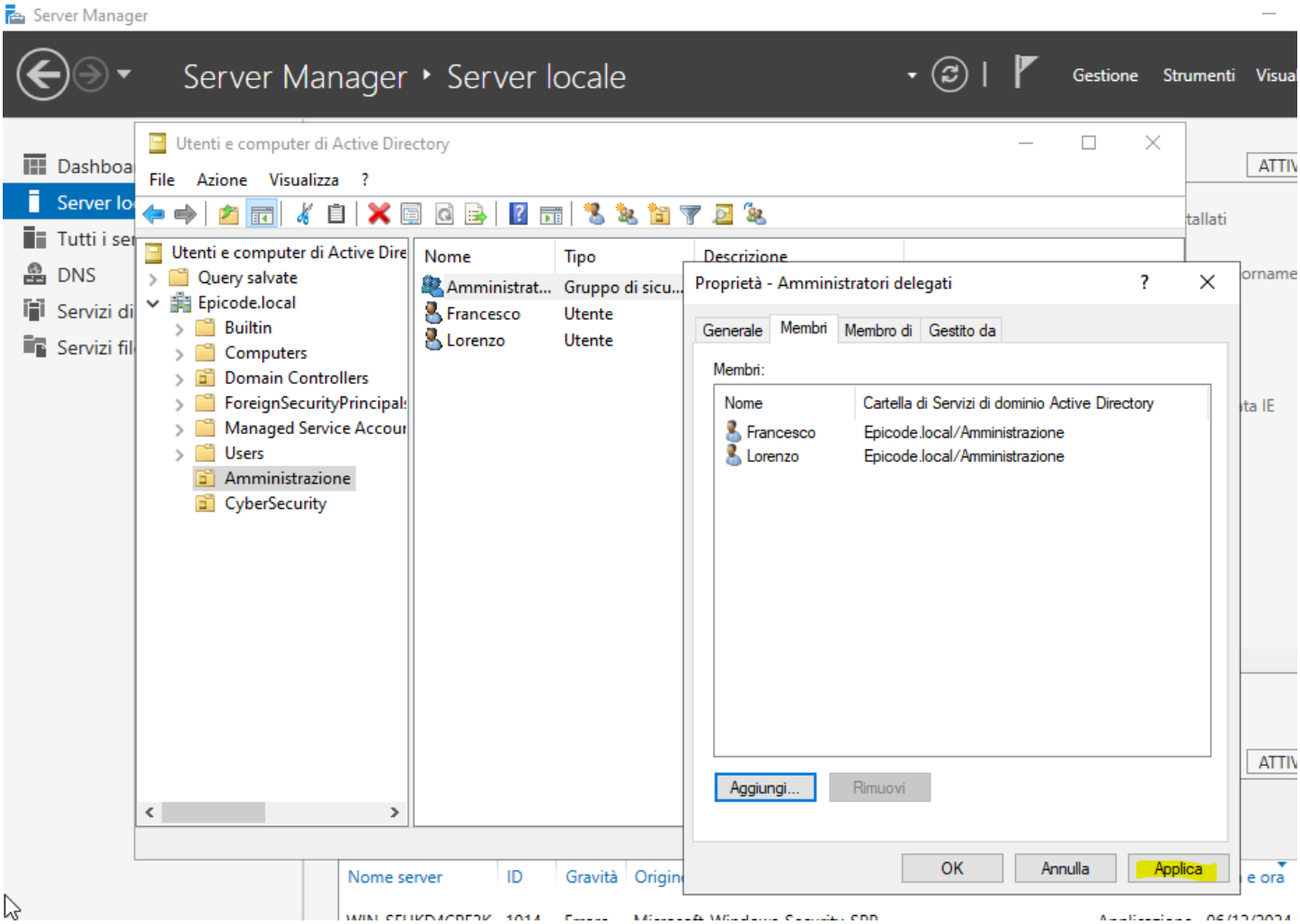
Ora per raggruppare a loro volta questi utenti, creiamo dentro le unità dei **gruppi**;



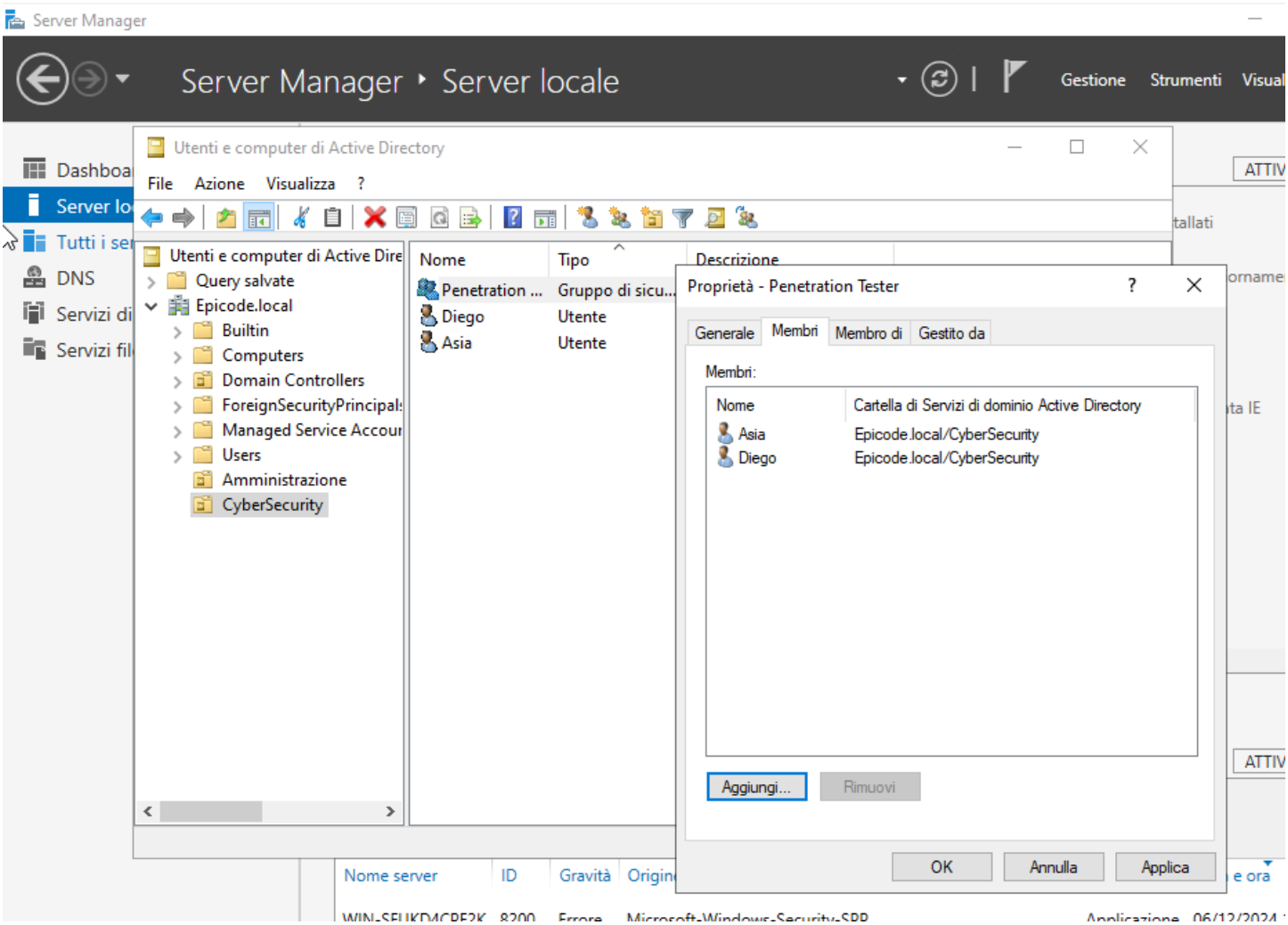
Dopo averlo creato, per inserire gli utenti, ci basterà digitare le iniziale e cliccare cu **controlla nomi**, ed i nomi verranno automaticamente aggiunti;



Per amministrazione;

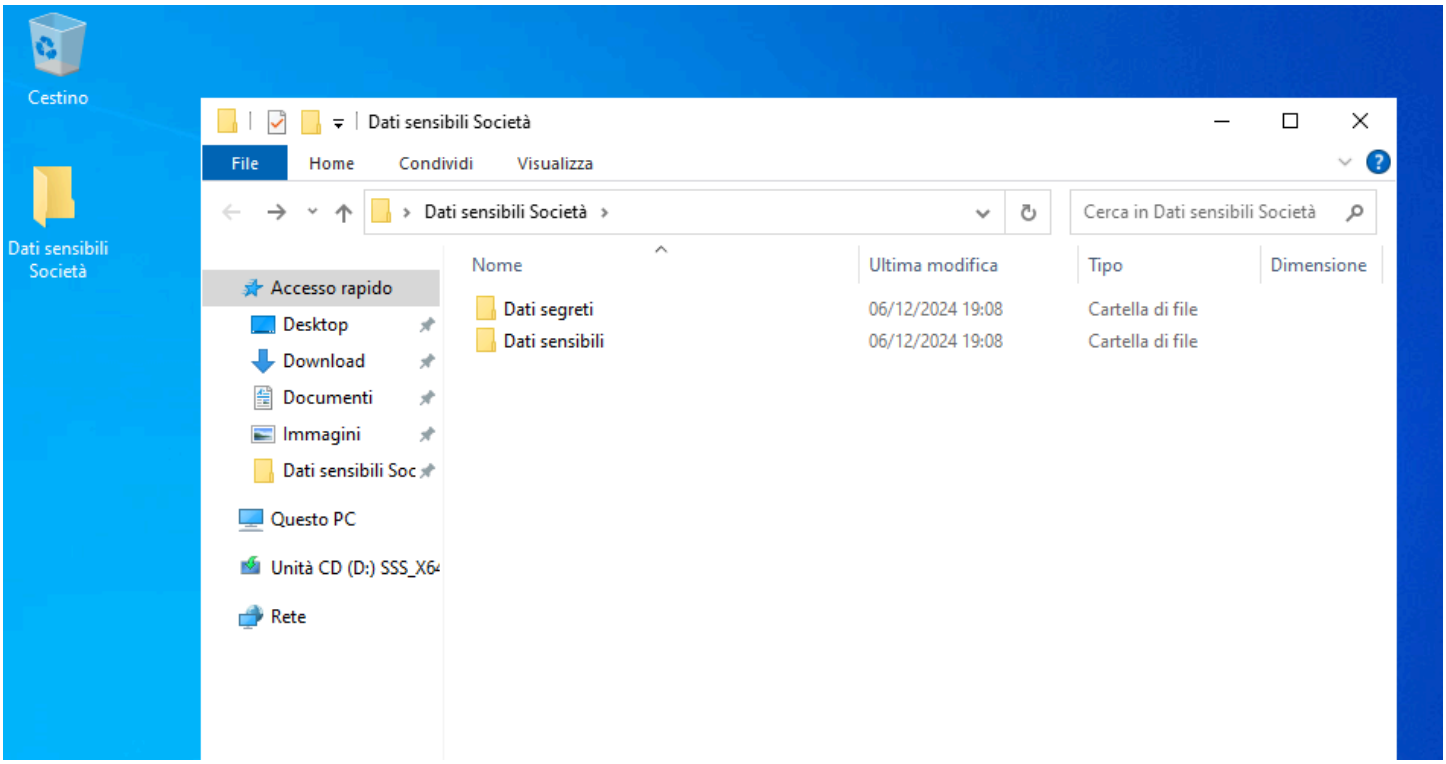


E per il reparto **Penetration Tester**;



Pratica:

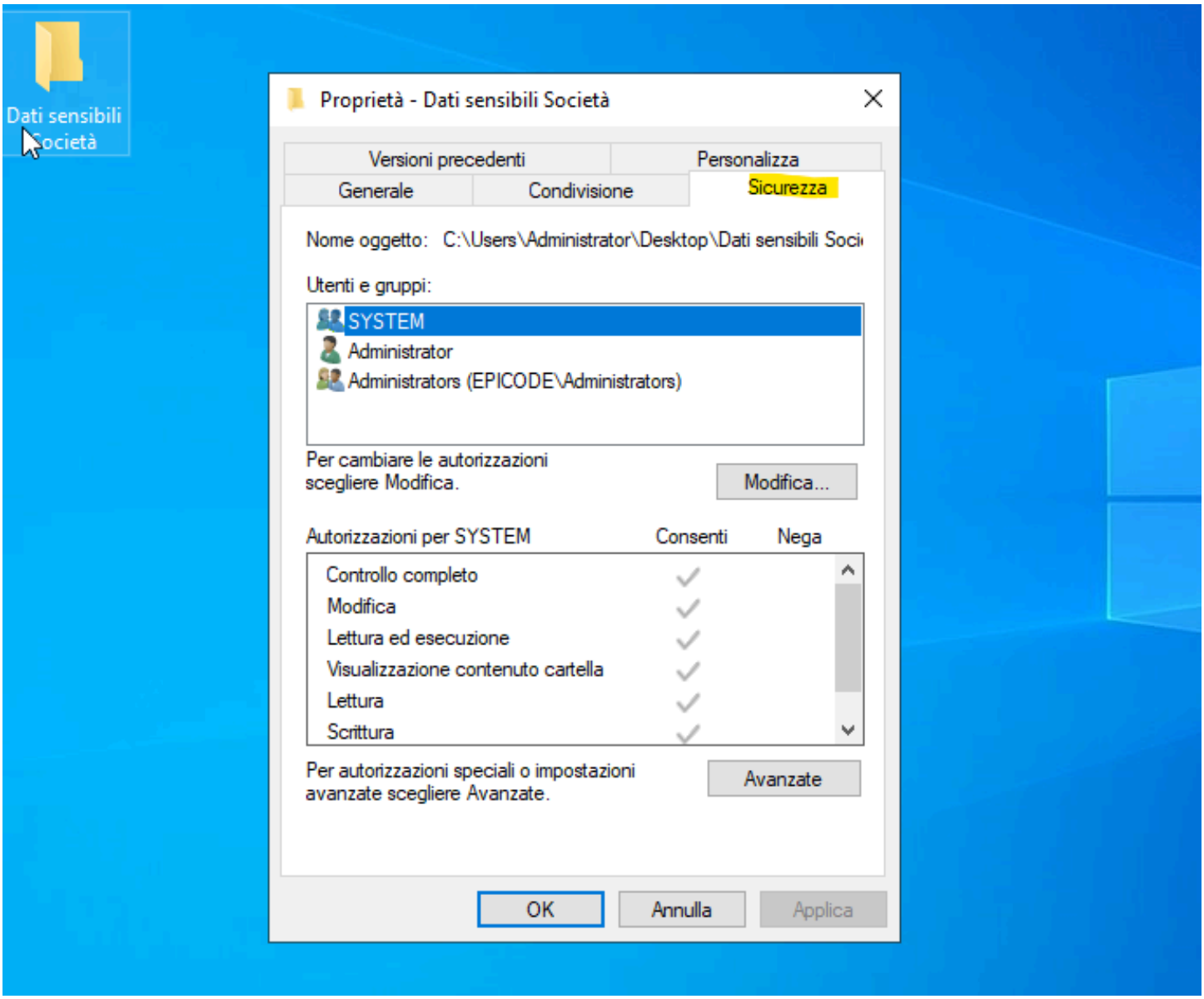
Ora possiamo assegnare i vari ruoli, alle unità ma soprattutto ai gruppi, dopo aver creato questa **cartella** con **2 sottocartelle al suo interno**;



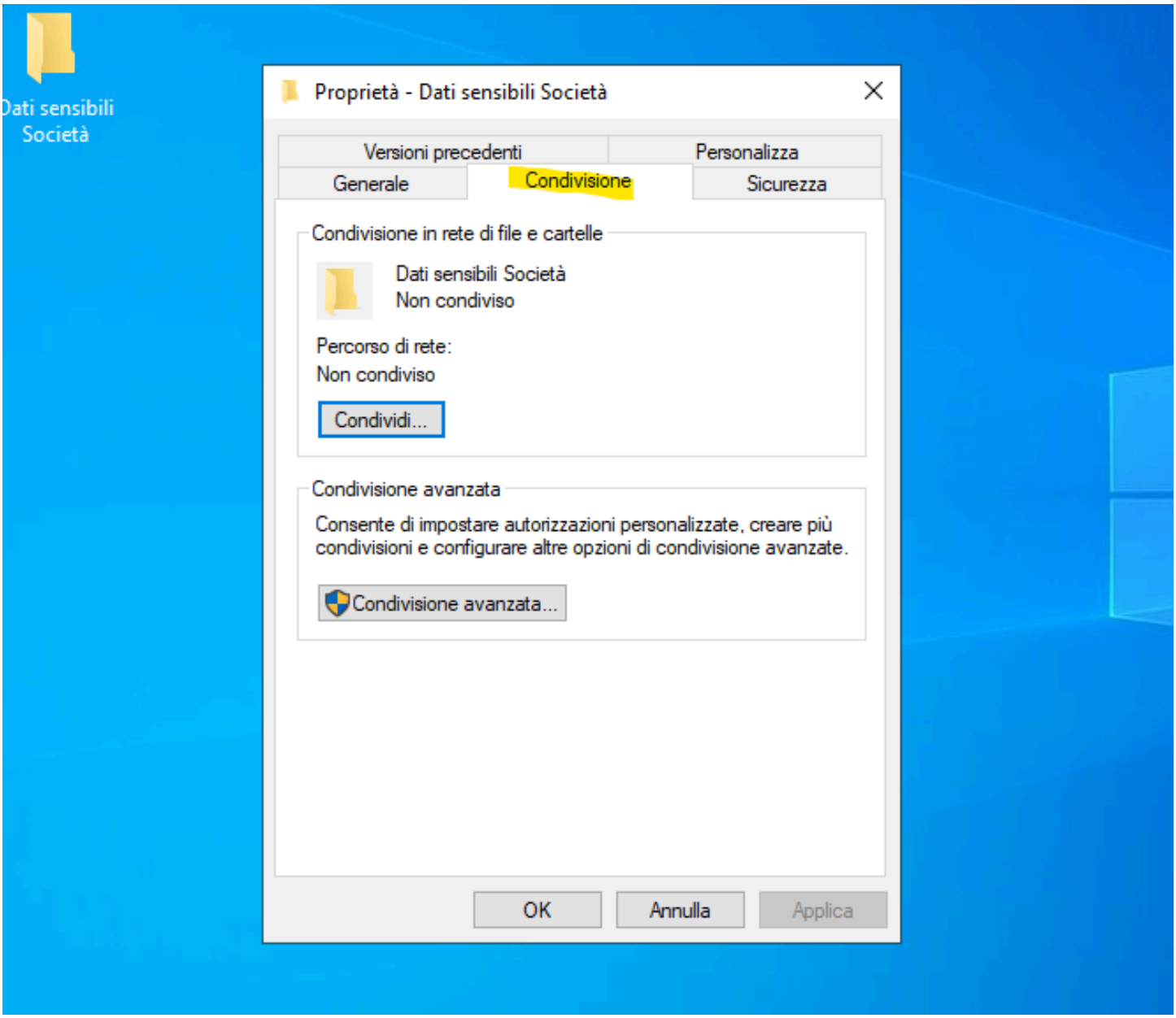
Per configurare i permessi clicchiamo sulla cartella con il **tasto destro del mouse**, **proprietà** e notiamo che troviamo **due tipi di permessi**, i permessi di **condivisione** e di **sicurezza**:

- I permessi di **condivisione** di Windows si applicano quando una cartella o un file viene condiviso in rete. Questi permessi determinano chi può accedere alla risorsa condivisa e con quale livello di accesso, come **lettura**, **scrittura** o **controllo completo**.
- I permessi di **sicurezza** di Windows, invece, riguardano **l'accesso ai file** e alle **cartelle** a livello locale sul disco. Questi permessi controllano chi può **visualizzare**, **modificare** o **eseguire** un file o una cartella, indipendentemente dalla condivisione in rete.

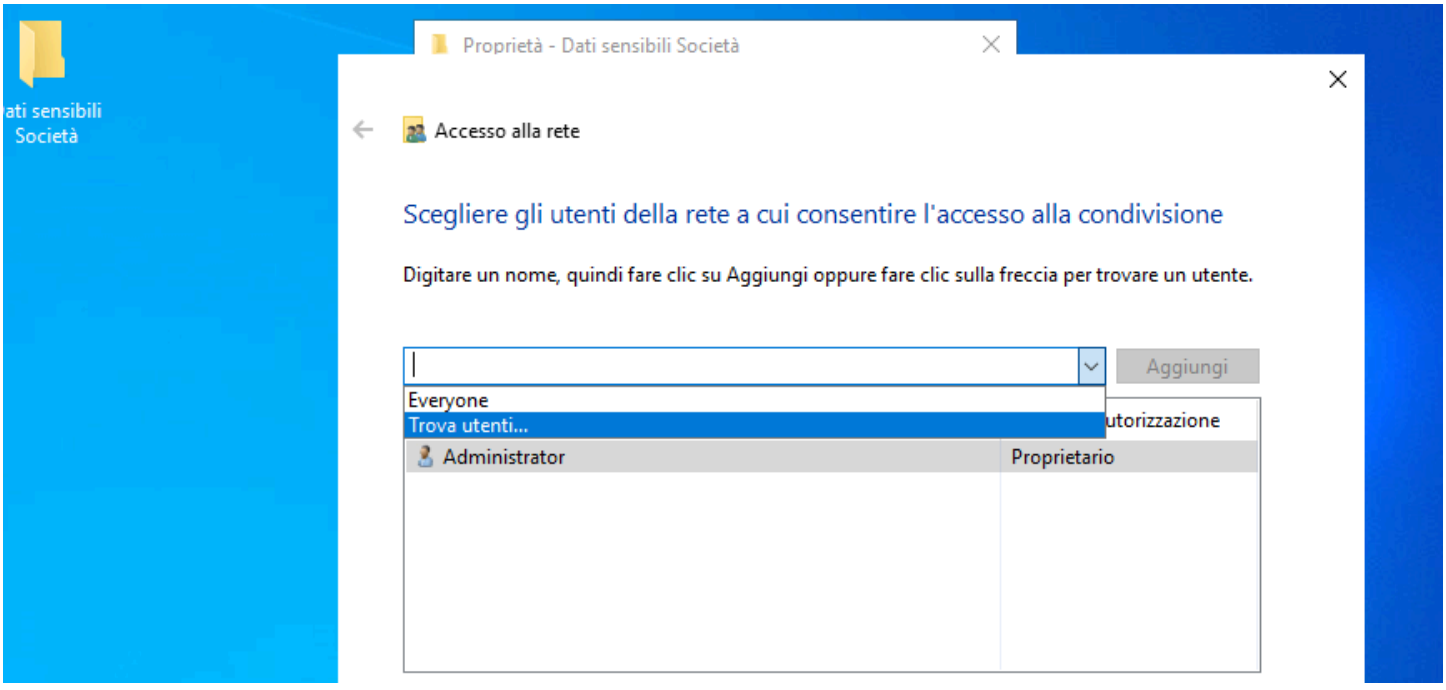
Dato che non troviamo i gruppi da noi creati in sicurezza, dobbiamo andare prima su **condivisione** per aggiungere i due gruppi;



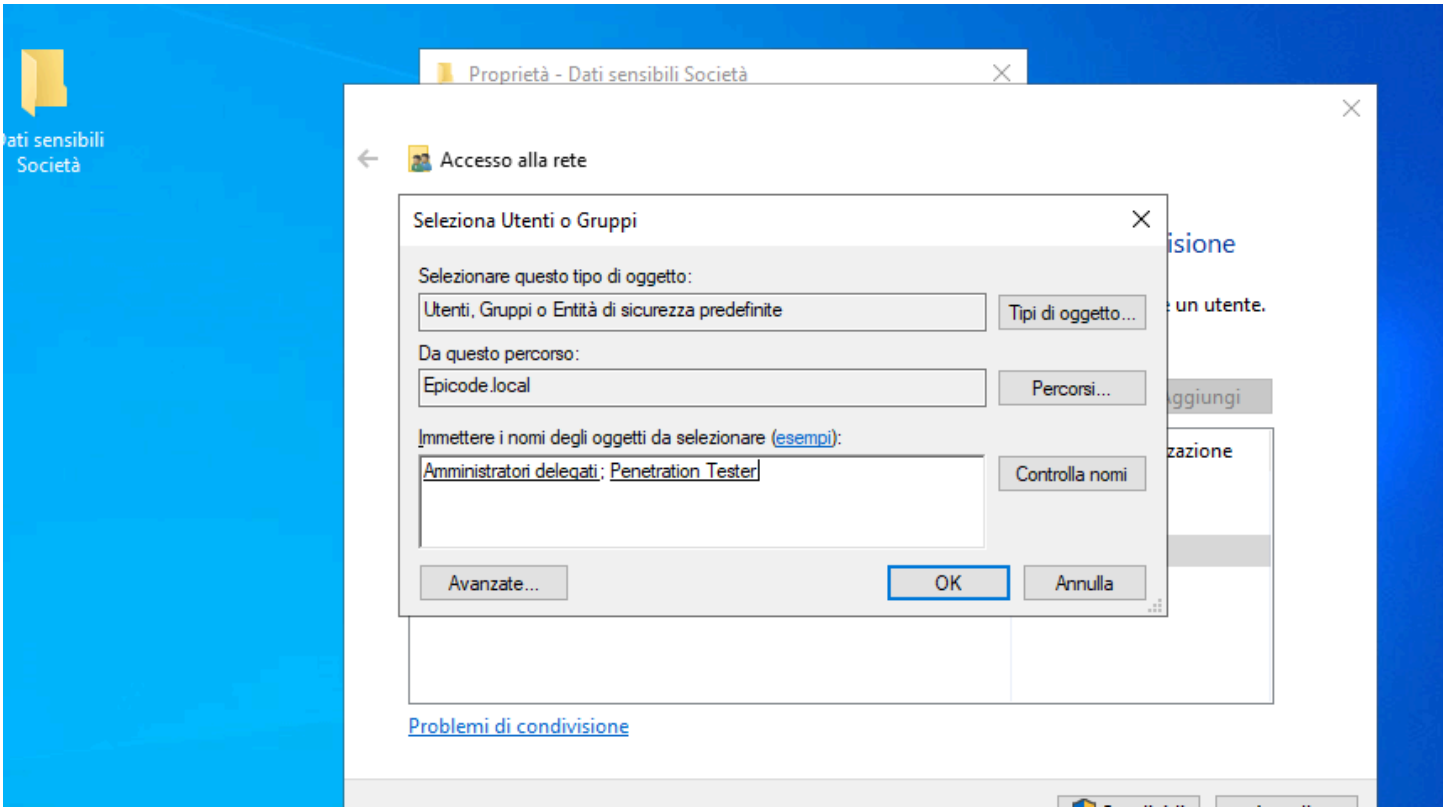
Andiamo su **condivisione avanzata**;



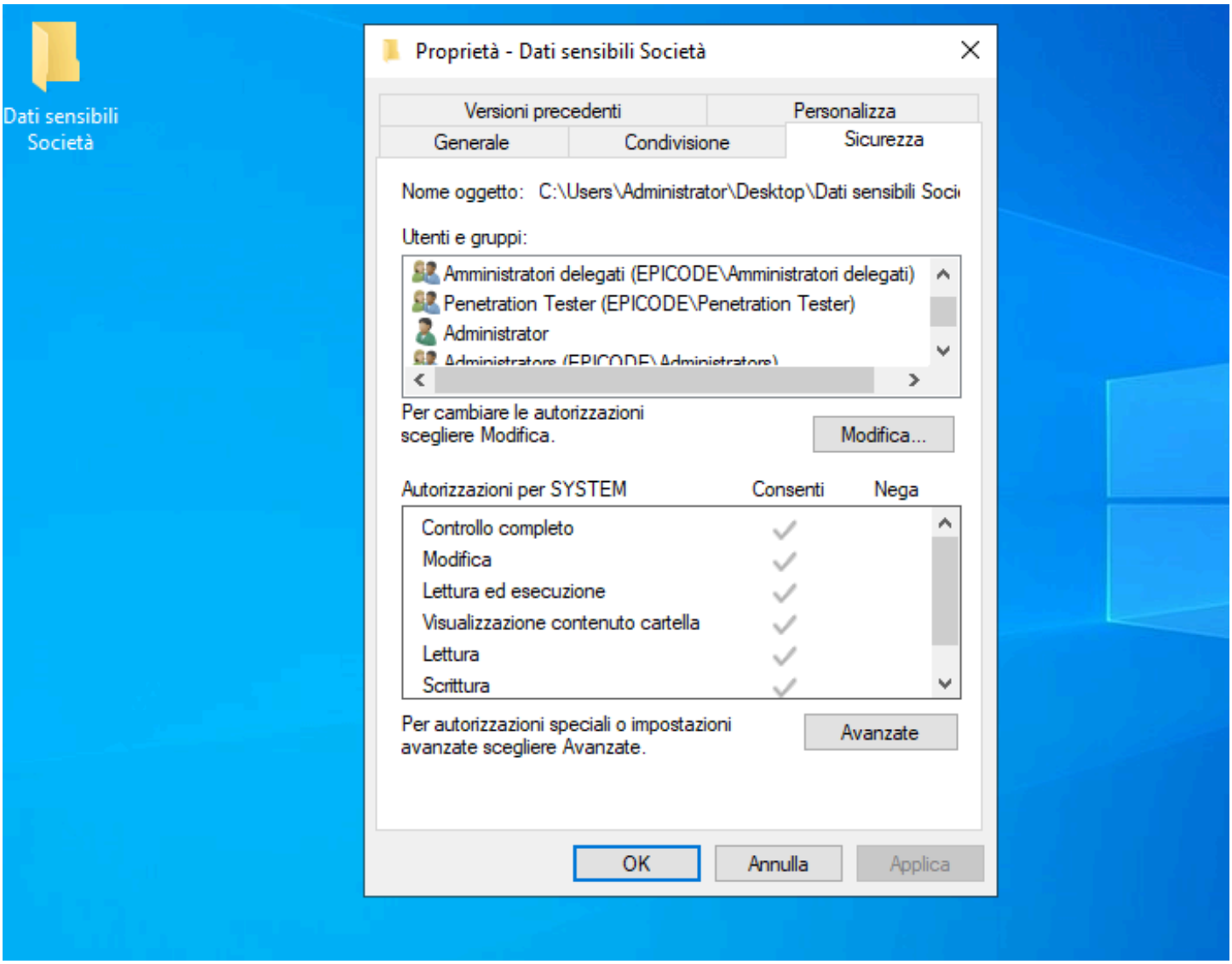
Trova utenti;



E uguale all’aggiunta degli utenti nei gruppi, aggiungiamo i gruppi stessi cercando il loro nome;

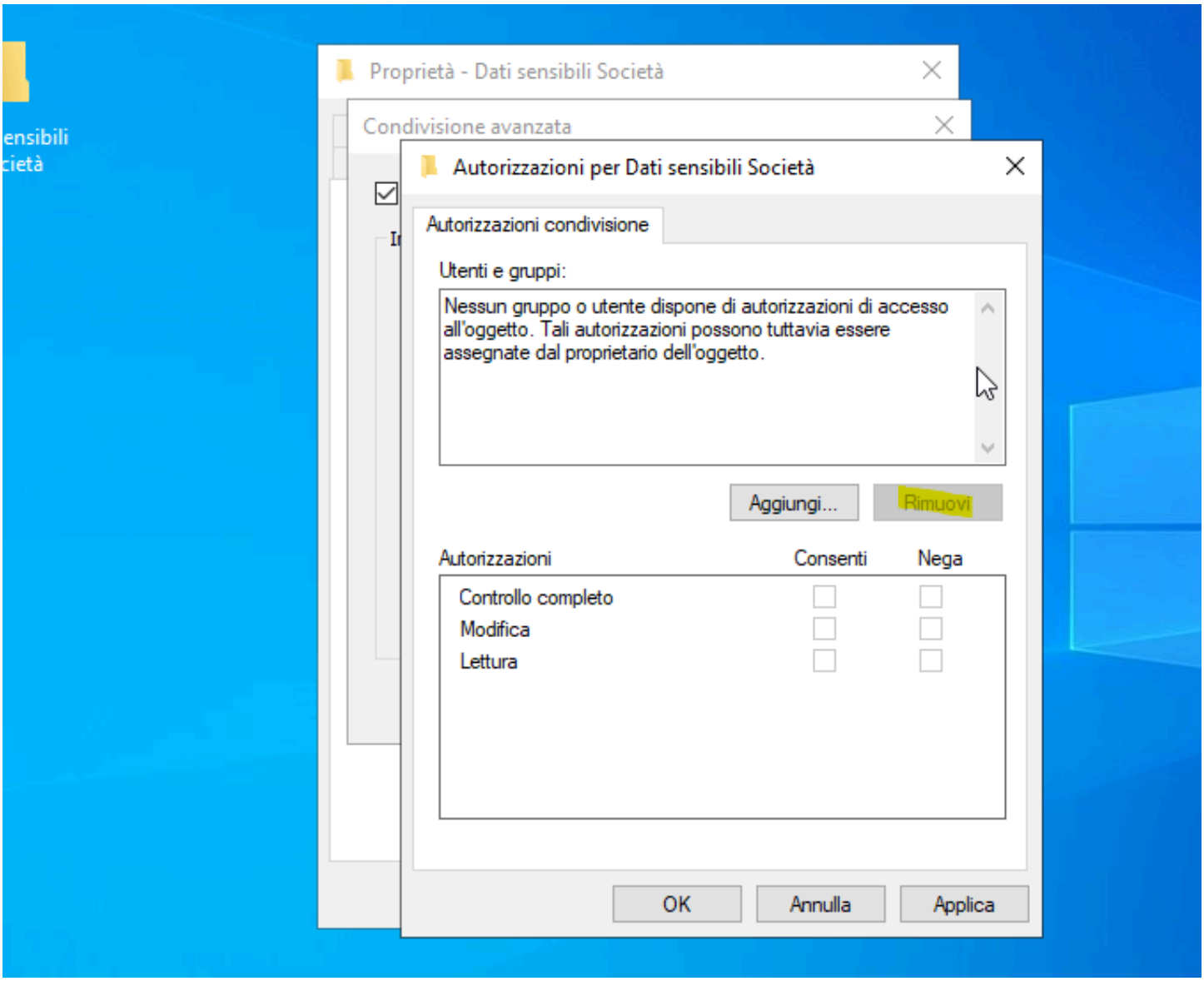


Una volta aggiunti notiamo che ora sono presenti per **fornirgli l’accesso alla cartella e i relativi permessi**;

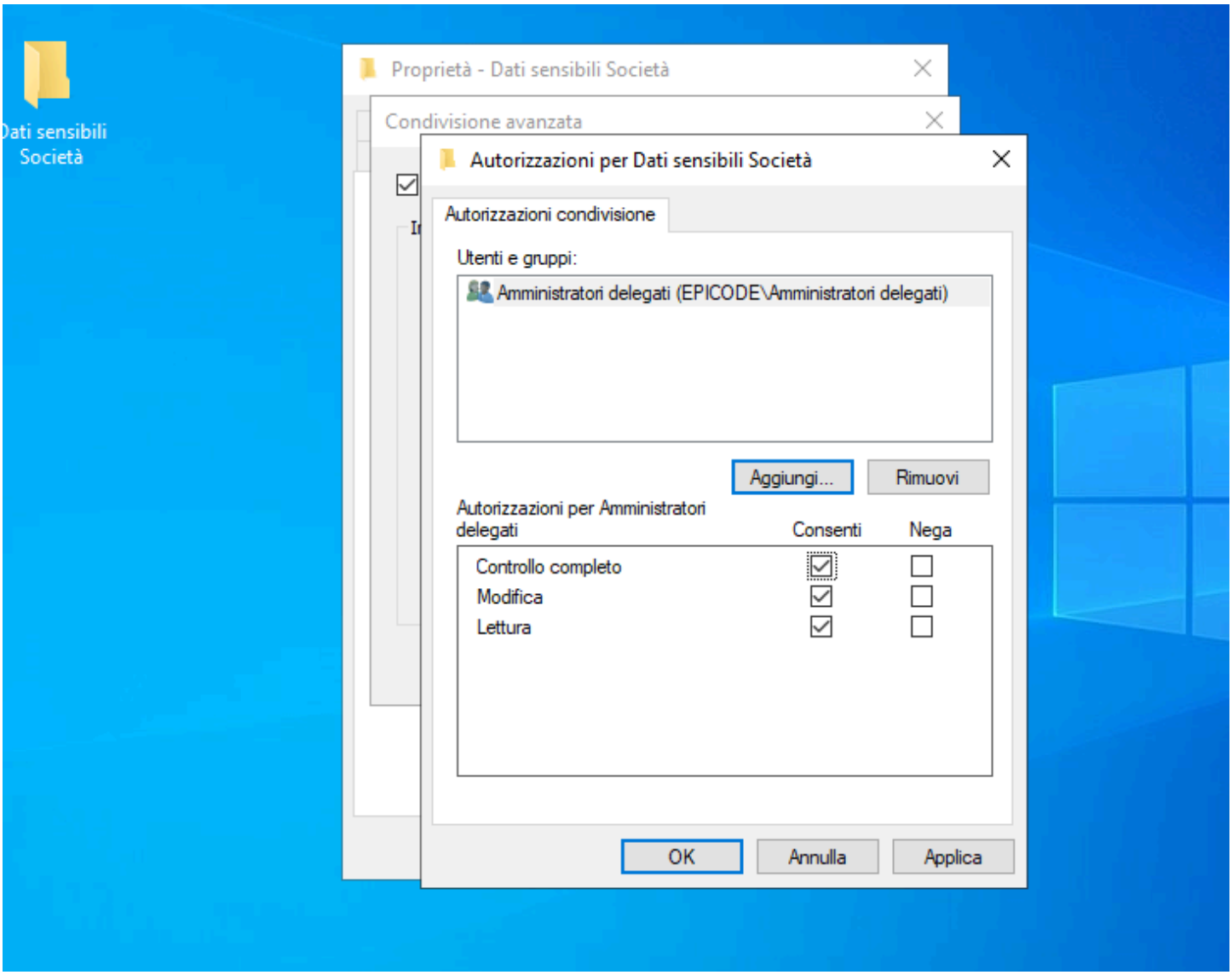


Come passo finale, essendo che in condivisione **è flaggato l'everyone**, ovvero che **tutti possono accedere alla cartella**, lo **togliamo**;

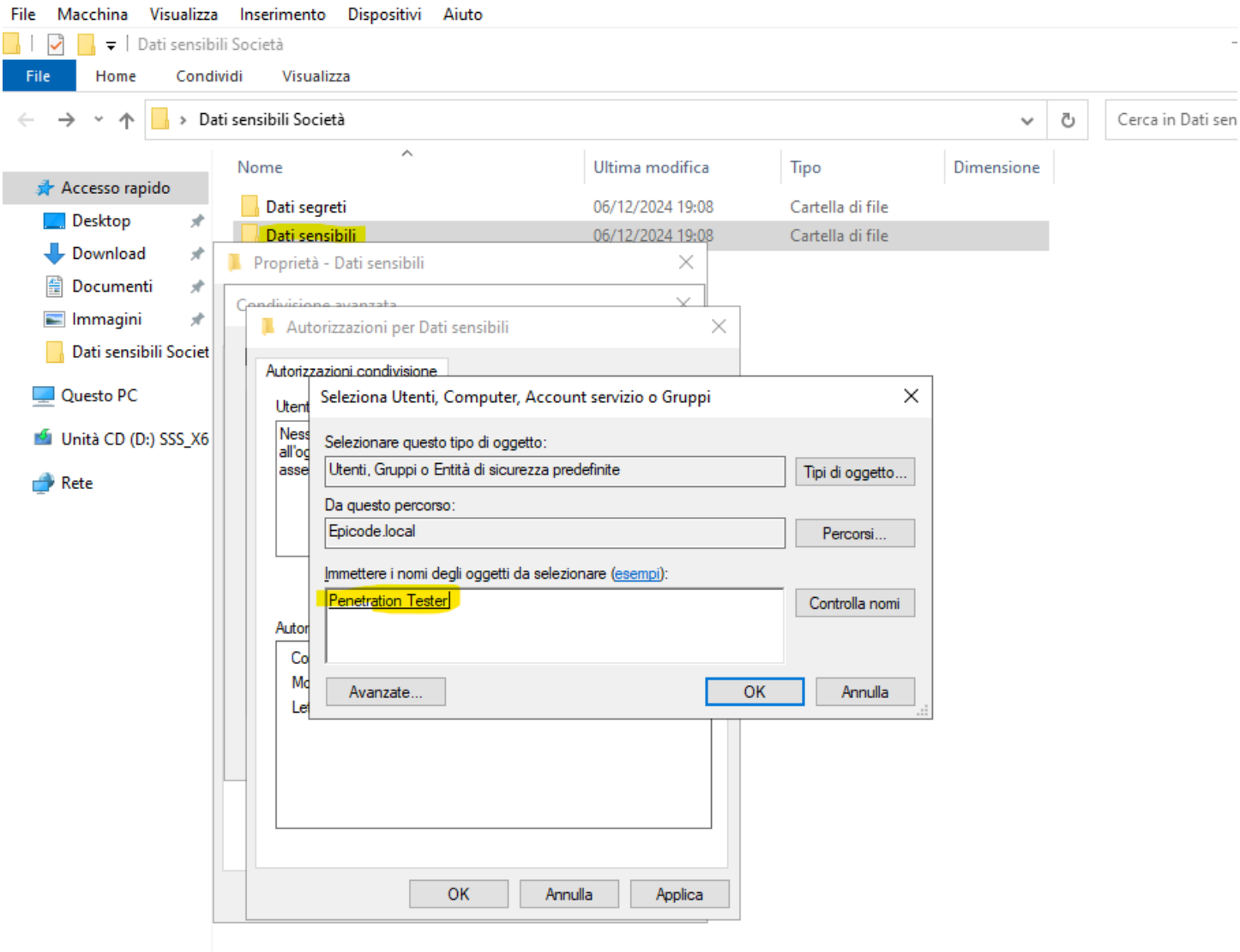
(prima in utenti e gruppi era presente **everyone**)



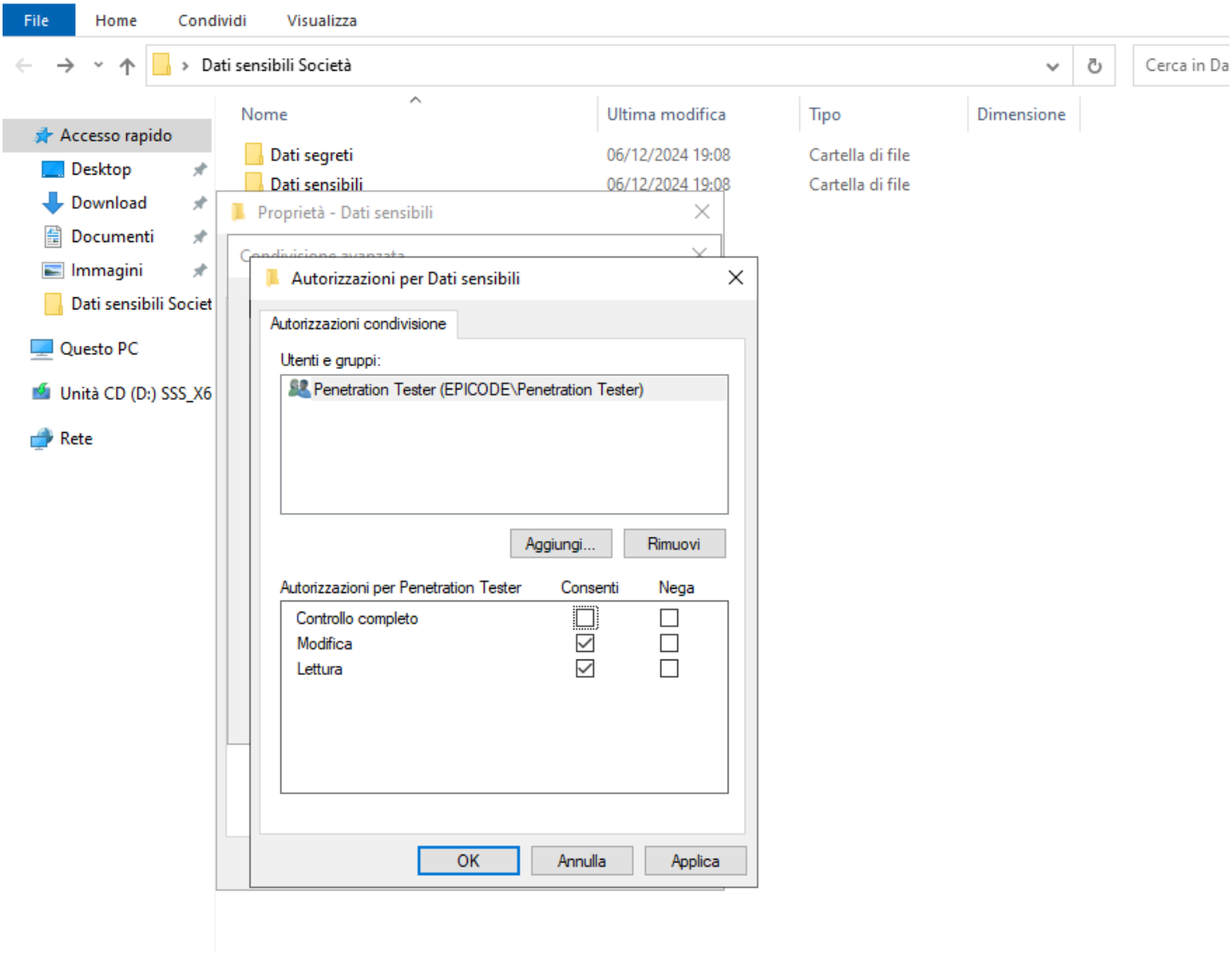
Ora invece aggiungi il gruppo amministratori, e concedo **tutti i permessi** (**controllo completo**);



Mentre al gruppo **penetration tester**;



Forniamo solamente la possibilità di **modifica** e **lettura**, **solamente alla cartella Dati sensibili**;



Conclusione:

In conclusione, questo compito ha permesso di esplorare in modo pratico e approfondito le funzionalità di **Windows Server 2022** e dello strumento **Server Manager**, con l'obiettivo di configurare una rete e gestire in modo efficiente ruoli, permessi e unità organizzative. Abbiamo creato una nuova foresta con il dominio **epicode.local**, trasformato il server in un **controller di dominio** e gestito la sicurezza e l'accesso a risorse condivise.

Abbiamo anche appreso come organizzare gli utenti e le risorse in **unità organizzative** e come assegnare i permessi sia a livello di **condivisione** che di **sicurezza**. L'intero processo ci ha fornito una comprensione pratica della gestione degli accessi e delle risorse in un ambiente Active Directory, preparandoci a gestire e proteggere in modo sicuro un'infrastruttura IT aziendale. Questo compito ci ha permesso di vedere come la teoria venga applicata nella

configurazione di una rete sicura e ben organizzata, fondamentale per un’amministrazione IT efficace.