



WINDOWS
SERVER

INDICE



01

Introduzione

02

Configurazione del sistema:

- Windows Server / 10
- Foresta
- Utenti e gruppi

03

Policy

04

Test



INTRODUZIONE

INTRODUZIONE

Windows Server è uno dei sistemi operativi più utilizzati per la gestione delle infrastrutture IT nelle aziende.

Una delle sue funzionalità principali è **Active Directory** (AD), un servizio che consente di centralizzare la gestione delle risorse aziendali, degli utenti e delle politiche di sicurezza attraverso la creazione di domini e foreste.

Vedremo i concetti fondamentali legati alla gestione di Windows Server, configurando dominio e foresta in Active Directory. Verranno creati utenti e gruppi e verranno applicate policy di sicurezza e permessi di accesso a file per garantire la protezione e l'efficienza operativa di un sistema.

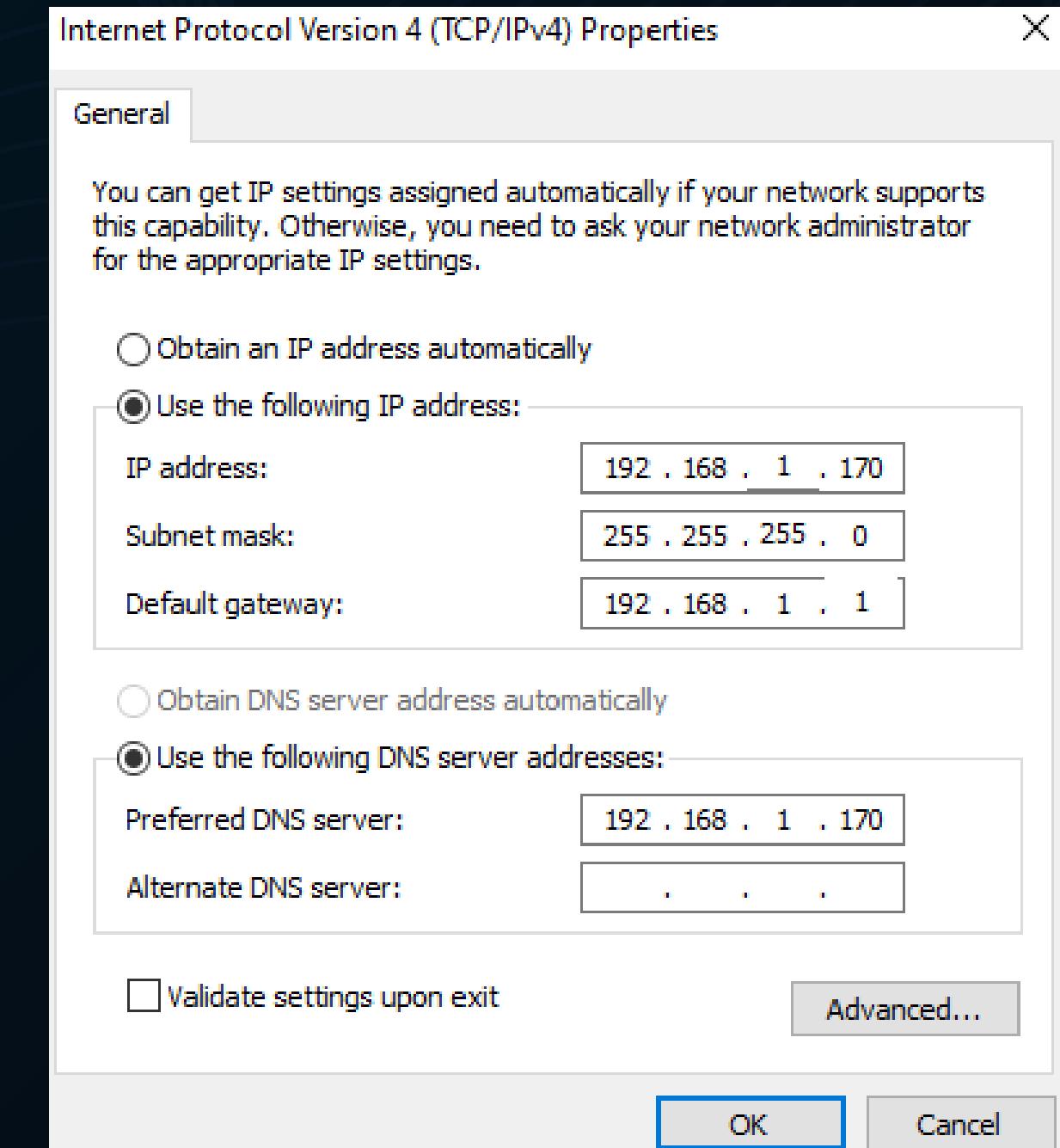
L'obiettivo è fornire una panoramica delle funzionalità offerte da Windows Server e dell'impatto delle politiche su un'infrastruttura IT aziendale, evidenziando come queste configurazioni possano migliorare la sicurezza, il controllo e l'organizzazione delle risorse aziendali.

CONFIGURAZIONE

CONFIGURAZIONE

Iniziamo con la corretta impostazione della rete su Windows Server:

In questo caso ho impostato un indirizzo IP statico e modificato il DNS uguale all'indirizzo IP del server. Si usa questa procedura per il corretto funzionamento di Active directory ottimizzando la gestione della rete.



CONFIGURAZIONE

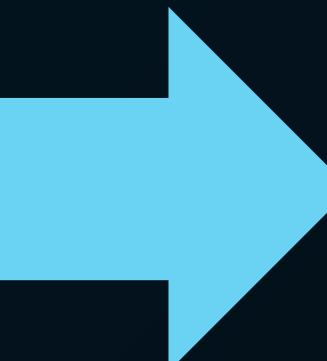
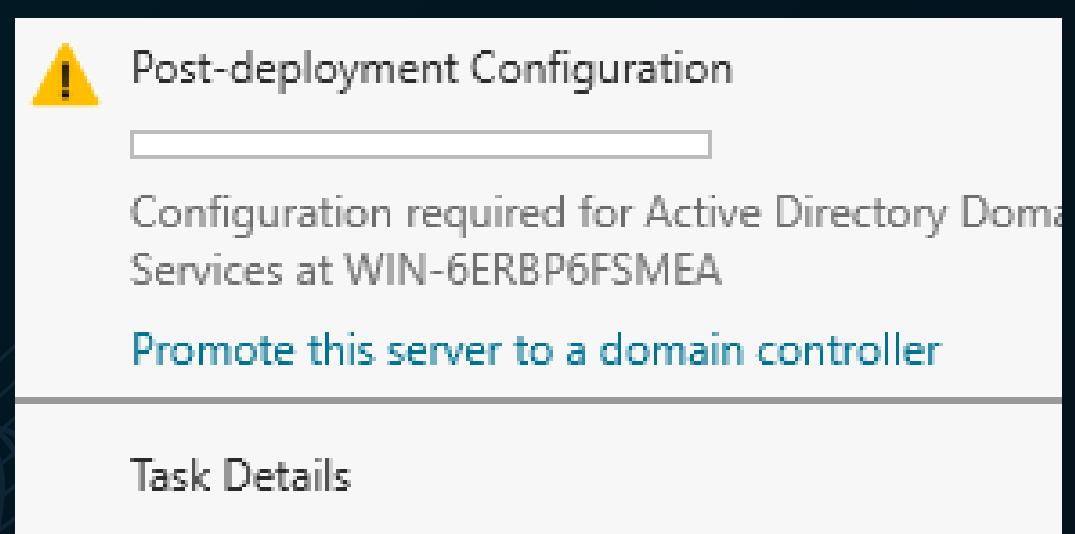
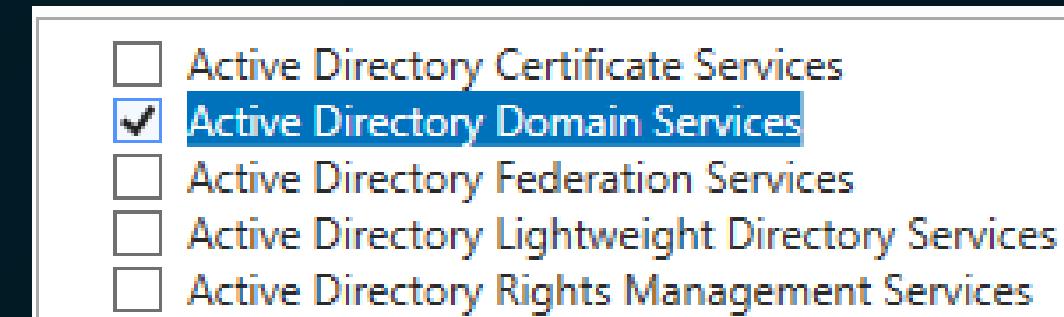
Si procede con la creazione del Dominio e della Foresta.

Ma vediamo cosa si intende con questi due termini.

Questi sono dei concetti utilizzati in Active directory:

- **Dominio:** si intende con dominio un'unità logica che raggruppa utenti, computer e risorse di rete sotto un'unica amministrazione. Ogni dominio ha il suo nome DNS di riferimento (es. Epicode.local) che verrà utilizzato per connettersi ad esso.
- **Forest:** una foresta è un insieme di uno o più domini che condividono una struttura logica comune.

CONFIGURAZIONE



Dopo aver installato Active directory, promuoviamo il server a “Domain controller” e aggiungiamo il dominio ad una foresta. In questo caso, non essendoci altre foreste, ne creeremo una nuova.

Select the deployment operation

Add a domain controller to an existing domain
 Add a new domain to an existing forest
 Add a new forest

Specify the domain information for this operation

Root domain name:

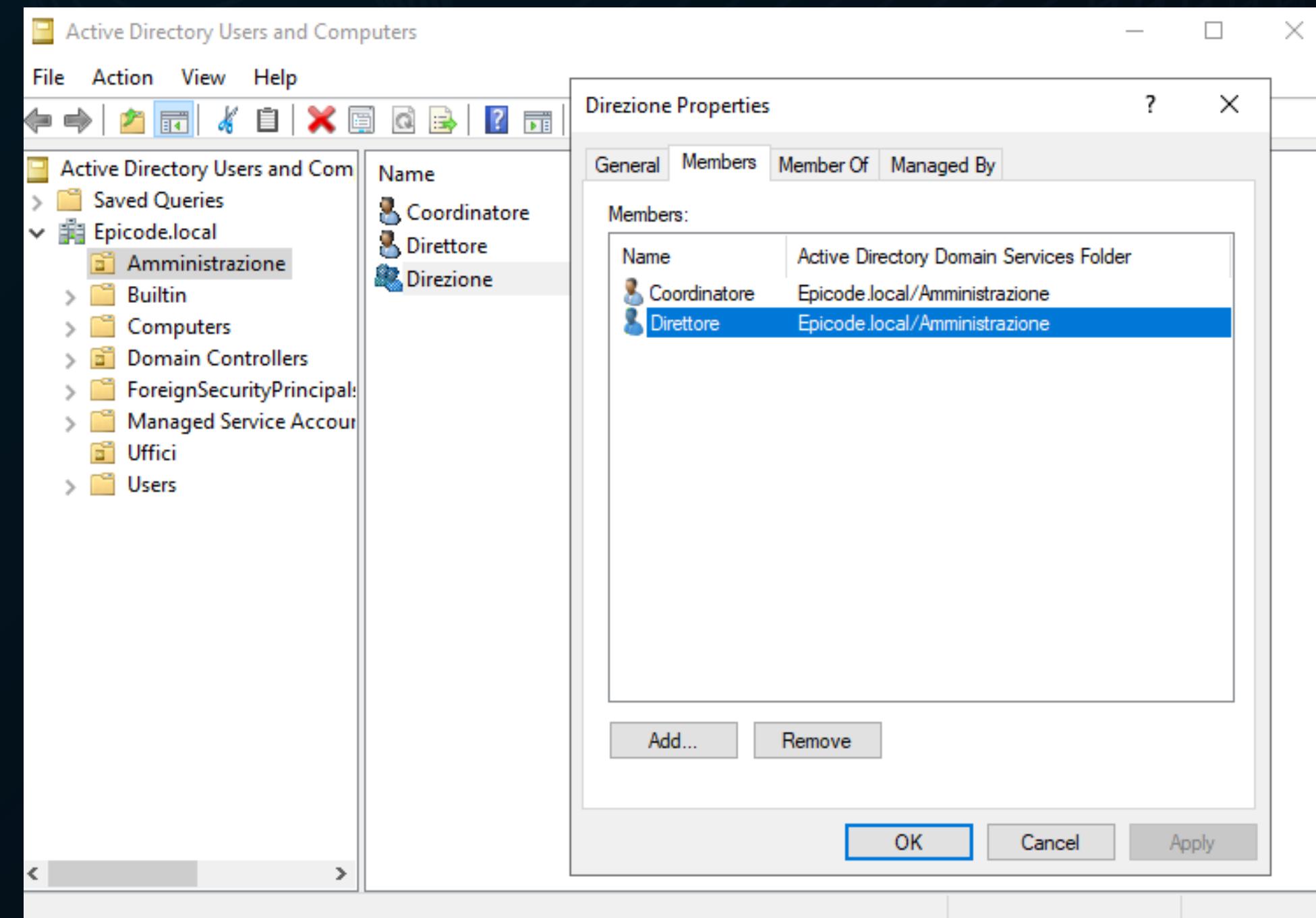
CONFIGURAZIONE

Verifichiamo nel pannello di Windows Server la creazione del dominio e le varie impostazioni.

Computer name	MyServer	Last installed updates	Never
Domain	Epicode.local	Windows Update	Download updates only, using Windows
		Last checked for updates	Never
Microsoft Defender Firewall	Public: On	Microsoft Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC+01:00) Amsterdam, Berlin, Bern,
Ethernet	192.168.1.170	Product ID	00454-40000-00001-AA245 (activated)
Operating system version	Microsoft Windows Server 2022 Standard Evaluation	Processors	12th Gen Intel(R) Core(TM) i7-1255U
Hardware information	innotek GmbH VirtualBox	Installed memory (RAM)	4 GB
		Total disk space	49.39 GB

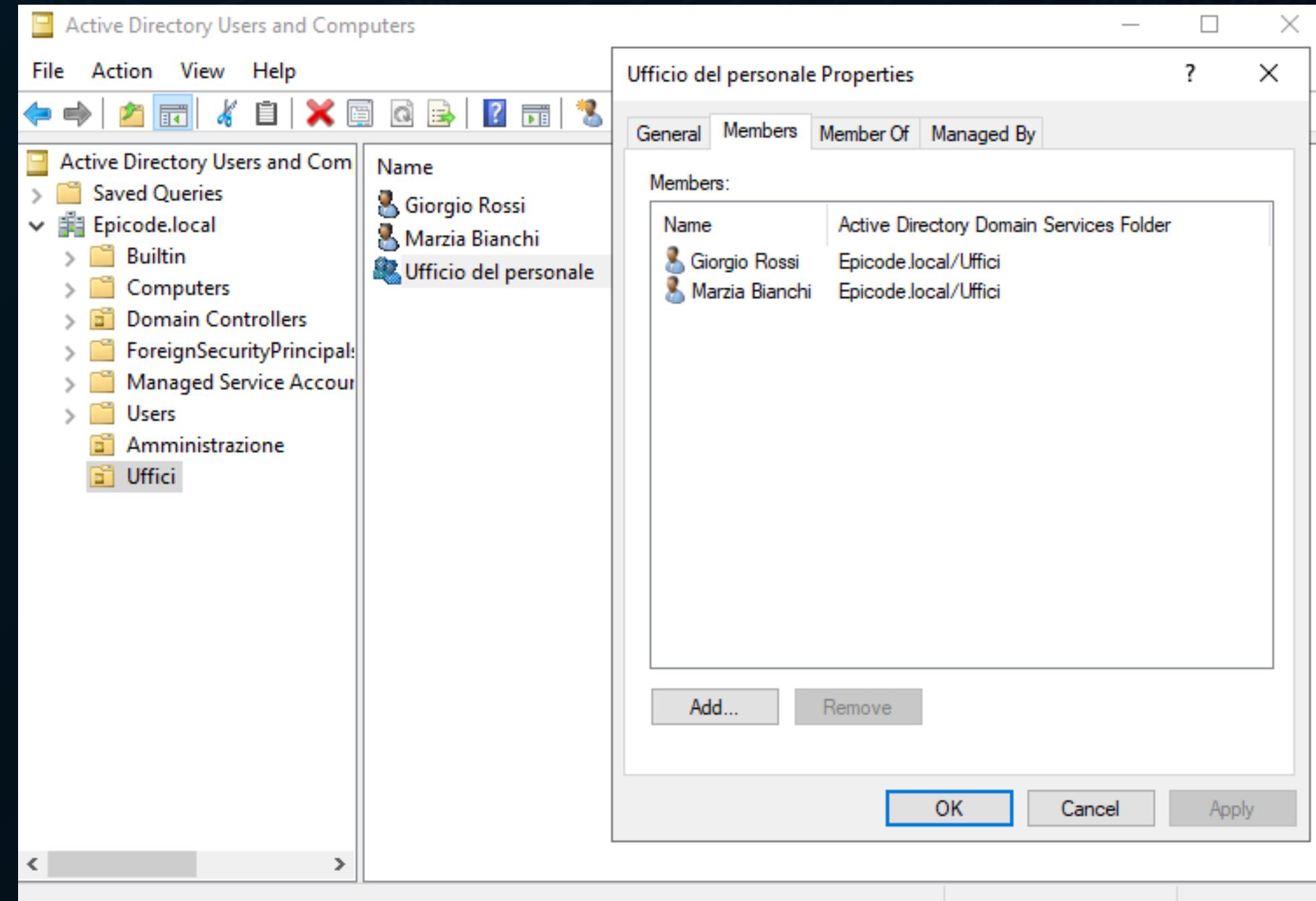
CONFIGURAZIONE

Dopo aver creato correttamente Dominio e Foresta, si può procedere con la creazione degli utenti e andarli ad inserire nei relativi gruppi. In questo caso ho effettuato una simulazione di un ambiente aziendale. Per fare ciò ho inizialmente creato una “Unità Organizzativa” sotto il nome di “Amministrazione”, al suo interno ho creato il gruppo “Direzione” e associati gli utenti relativi a quel reparto aziendale.



CONFIGURAZIONE

Analogamente alla situazione precedente, ho creato un “Unità organizzativa” sotto il nome di “Uffici”, al suo interno ho creato il gruppo “Ufficio del personale” e associati gli utenti relativi a quel reparto aziendale.



PERMESSI & POLICY

PERMESSI & POLICY

Applichiamo quindi permessi e policy ai gruppi appena creati.
Questa è una pratica utile per aumentare la sicurezza del sistema.

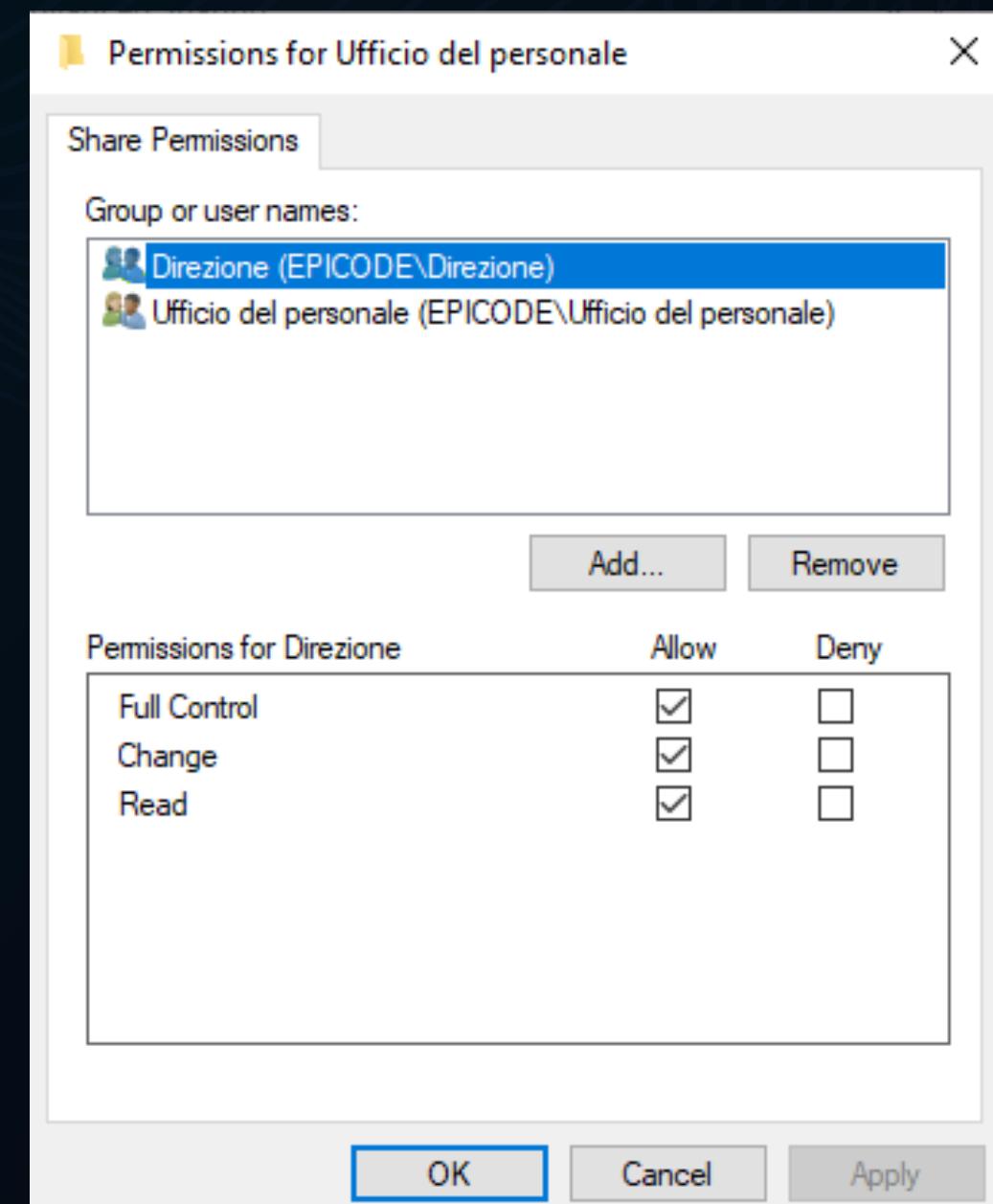
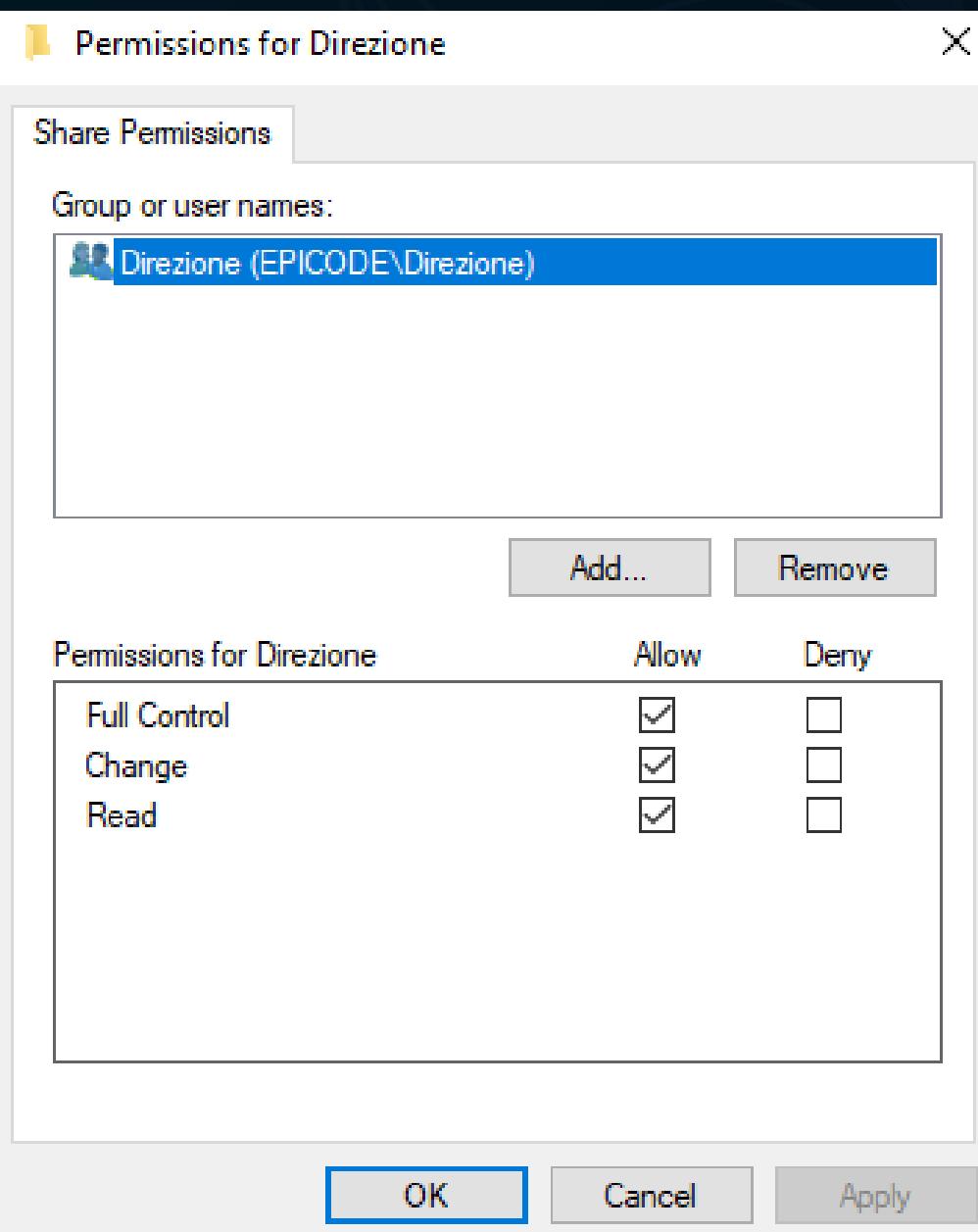
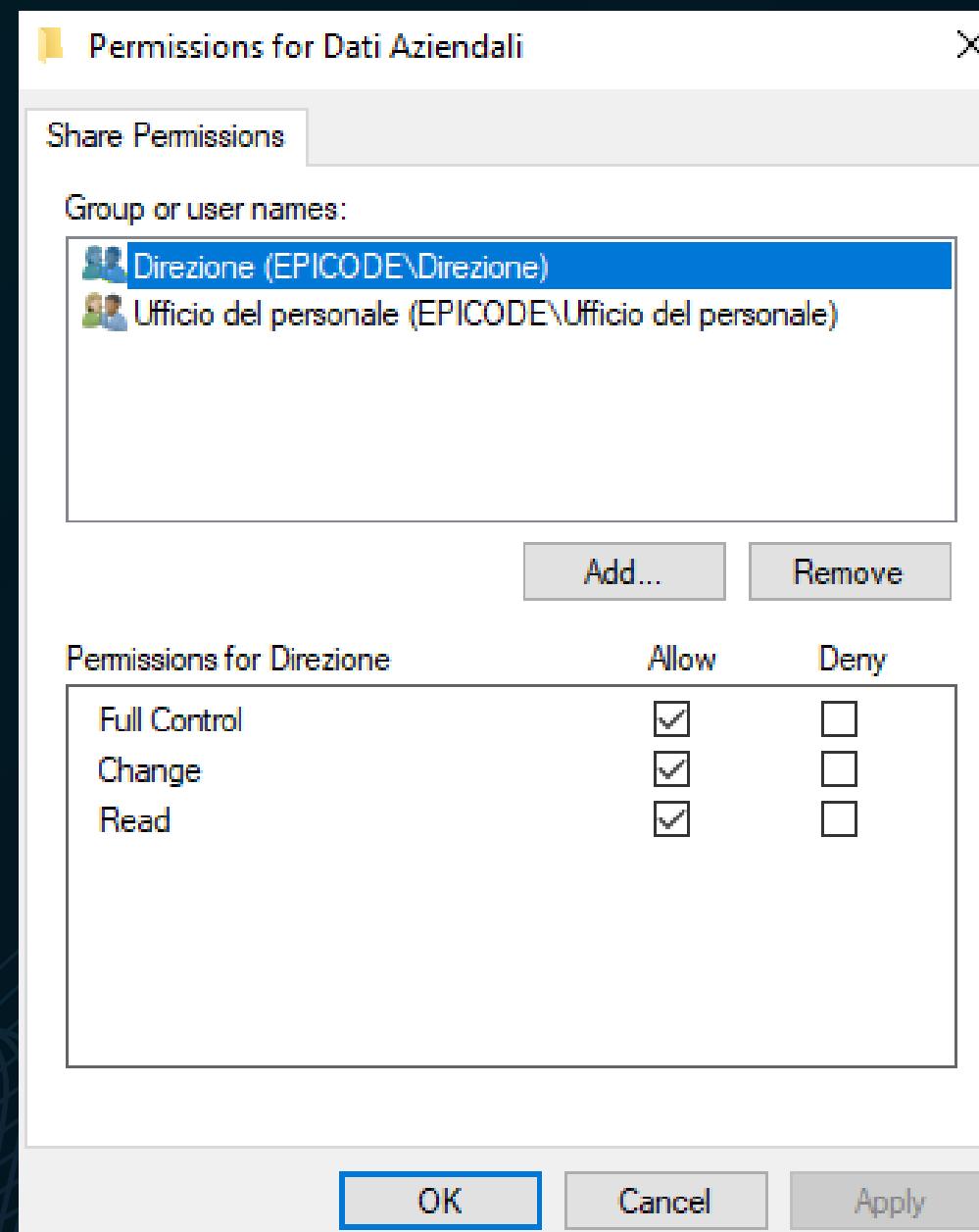
Ho creato in totale 3 cartelle:

- Dati aziendali
- Direzione
- Ufficio del personale

In questo caso ho applicato permessi specifici alle cartelle “Direzione” e “Ufficio del personale” in modo che gli account appartenenti al gruppo Direzione abbiano accesso totale ad entrambe le cartelle. Invece gli utenti appartenenti al gruppo “Ufficio del personale” hanno delle restrizioni sulla cartella “Direzione” per evitare che possano avere l’accesso e vedere o manipolare eventuali file all’interno di essa.

PERMESSI & POLICY

Vediamo nel dettaglio le restrizioni impostate:



PERMESSI & POLICY

Vediamo nel dettaglio le restrizioni impostate:

The screenshot shows the 'Share' dialog for a folder named 'Ufficio del personale'. The folder is located under 'Dati Aziendali'. The 'Share' tab is selected. The 'Name' column lists 'Administrator' and 'Direzione', both with 'Permission Level' set to 'Owner'. Below the table, there is a note: 'Choose people on your network to share with' and 'Type a name and then click Add, or click the arrow to find someone.' An 'Add' button is visible at the bottom right.

The screenshot shows the 'Share' dialog for a folder named 'Ufficio del personale' (highlighted in blue). The folder is located under 'Dati Aziendali'. The 'Share' tab is selected. The 'Name' column lists 'Administrator' and 'Direzione', both with 'Permission Level' set to 'Read/Write'. Below the table, there is a note: 'Choose people on your network to share with' and 'Type a name and then click Add, or click the arrow to find someone.' An 'Add' button is visible at the bottom right.

PERMESSI & POLICY

Aggiungo, inoltre, una restrizione che riguarda solo gli utenti del gruppo “Ufficio del personale”.

Proibisco l’accesso al pannello di controllo per eventuali modifiche al computer in dotazione.

PERMESSI & POLICY

The screenshot shows two windows side-by-side. On the left is a standard Windows Settings dialog box titled "Prohibit access to Control Panel and PC settings". It contains three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". Below these are fields for "Comment" (empty) and "Supported on" (set to "At least Windows 2000"). Under "Options", there is a large text block describing how the setting disables Control Panel programs and PC settings app, and removes them from the Start screen, File Explorer, and Settings charm. At the bottom are "OK", "Cancel", and "Apply" buttons. On the right is the "Group Policy Management Editor" window. The left pane shows a tree structure with "Policies" expanded, showing "Software Settings", "Windows Settings" (with "Control Panel" selected), and "Administrative Templates: Policy". The right pane displays the details for the selected "Control Panel" policy. It has sections for "Setting", "Edit policy setting", "Requirements" (set to "At least Windows 2000"), "Description" (same as the dialog box), and "This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.". A list of settings under "Control Panel" includes "Add or Remove Programs", "Display", "Personalization", "Printers", "Programs", "Regional and Language Options", "Desktop", "Network", "Shared Folders", "Start Menu and Taskbar", "System", "Windows Components", and "All Settings". At the bottom of the right pane, it says "5 setting(s)".



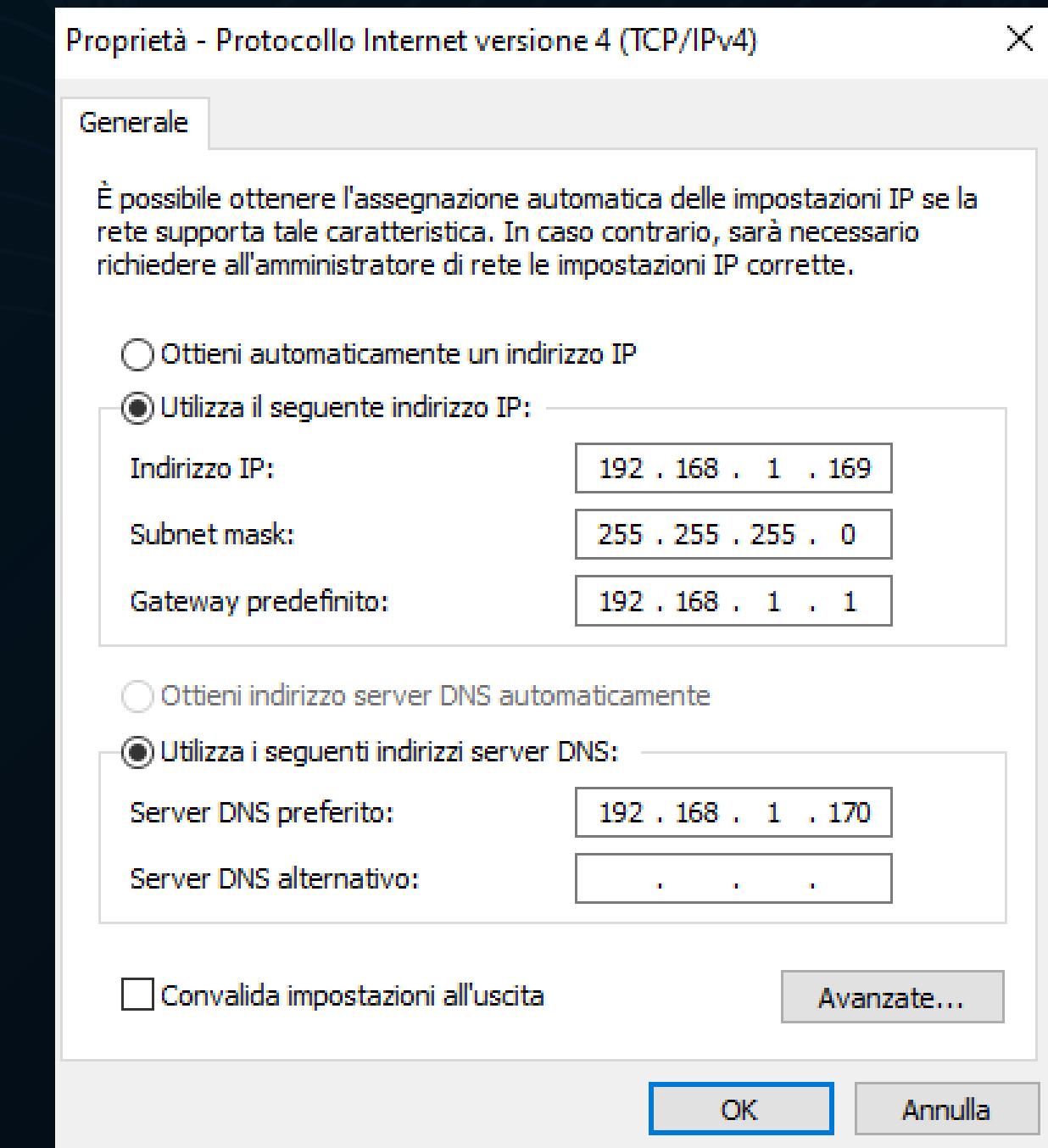
TEST

TEST

Si può finalmente procedere con il test di tutta la rete appena creata.

Utilizzerò un Windows 10 Pro per eseguire le operazioni necessarie.

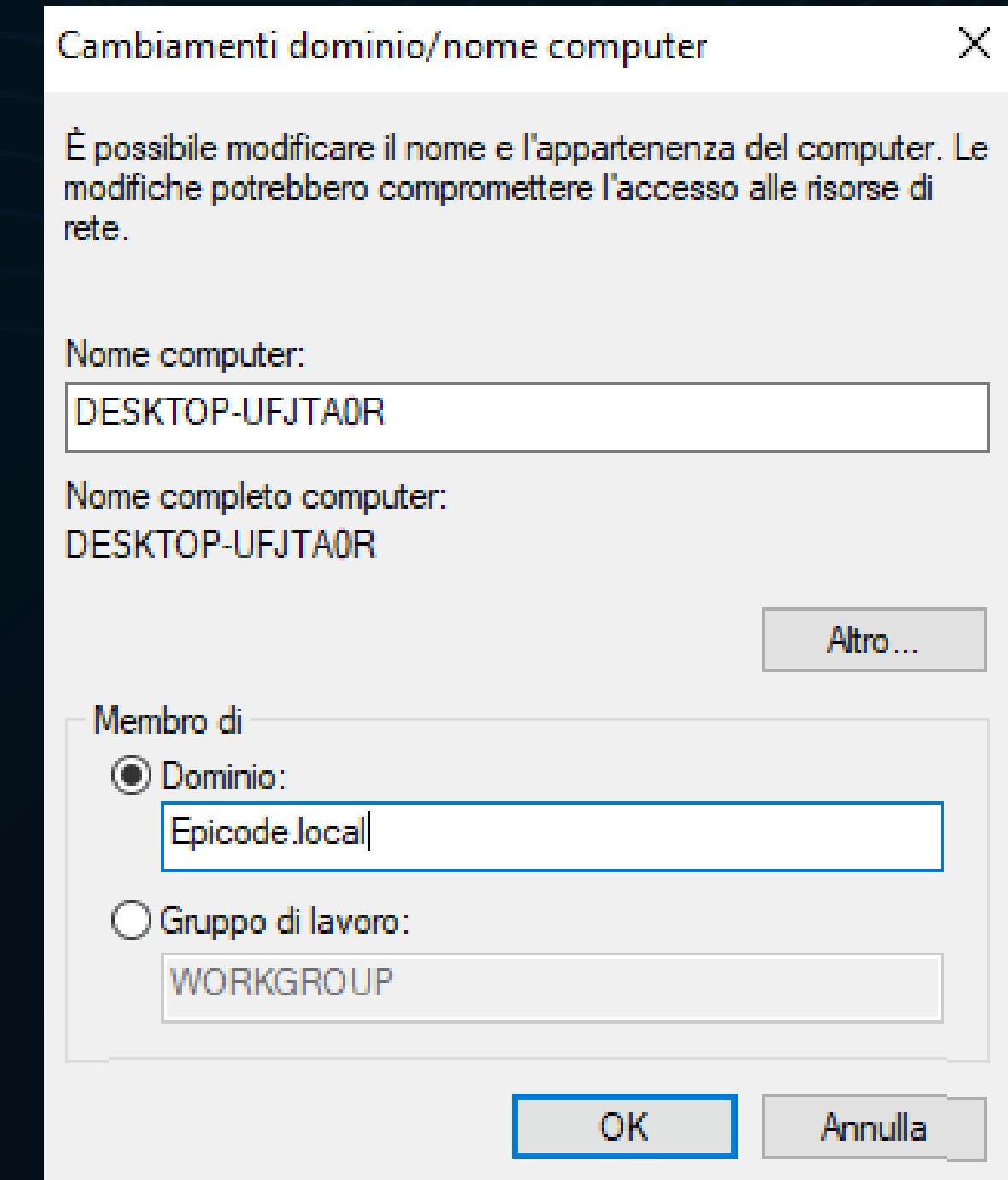
Per prima cosa imposterò un indirizzo IP statico e il DNS come l'indirizzo IP del server in modo da collegarsi ad esso.



TEST

Procedo quindi con il collegamento effettivo al server tramite Dominio.

Qui andrò a mettere il nome di dominio precedentemente creato (Eicode.local) e se non vi sono problemi richiederà nome utente e password da utilizzare per entrare in un account su quel dominio.





TEST

Siamo entrati
correttamente con
l'account del direttore.



Informazioni

Il tuo PC è monitorato e protetto.

[Vedere i dettagli in Sicurezza di Windows](#)

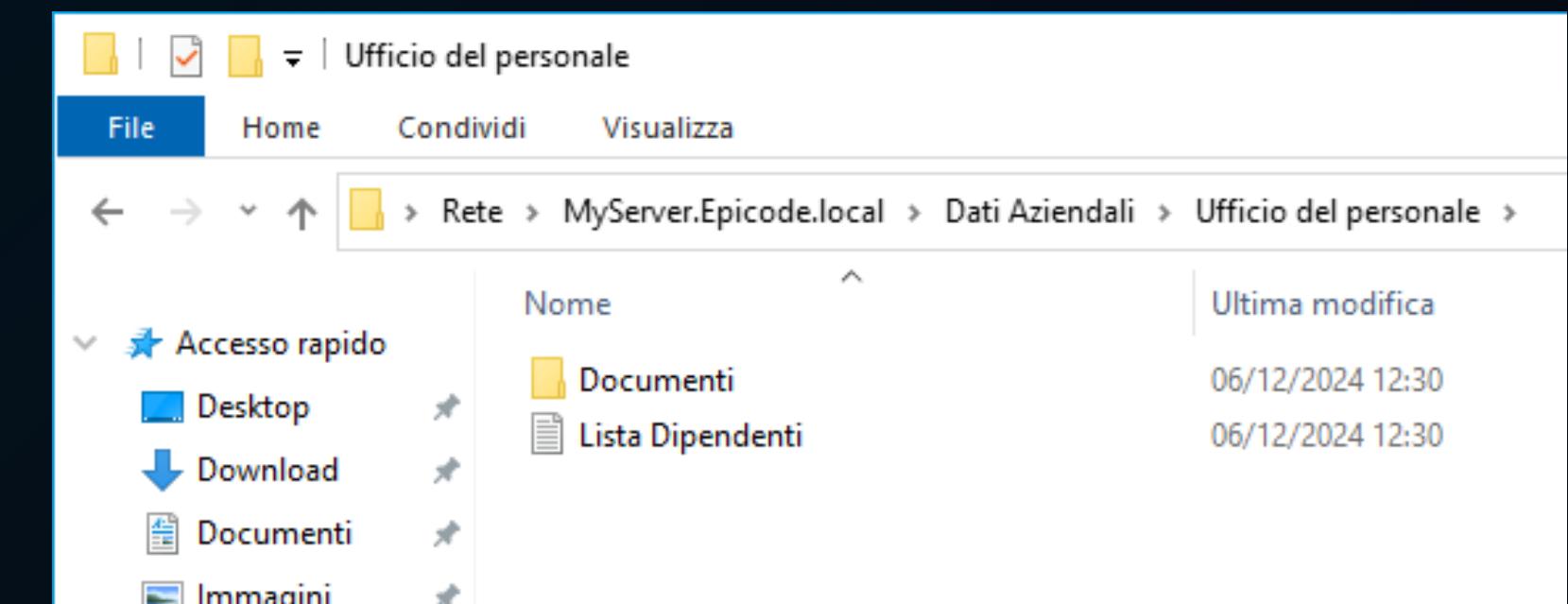
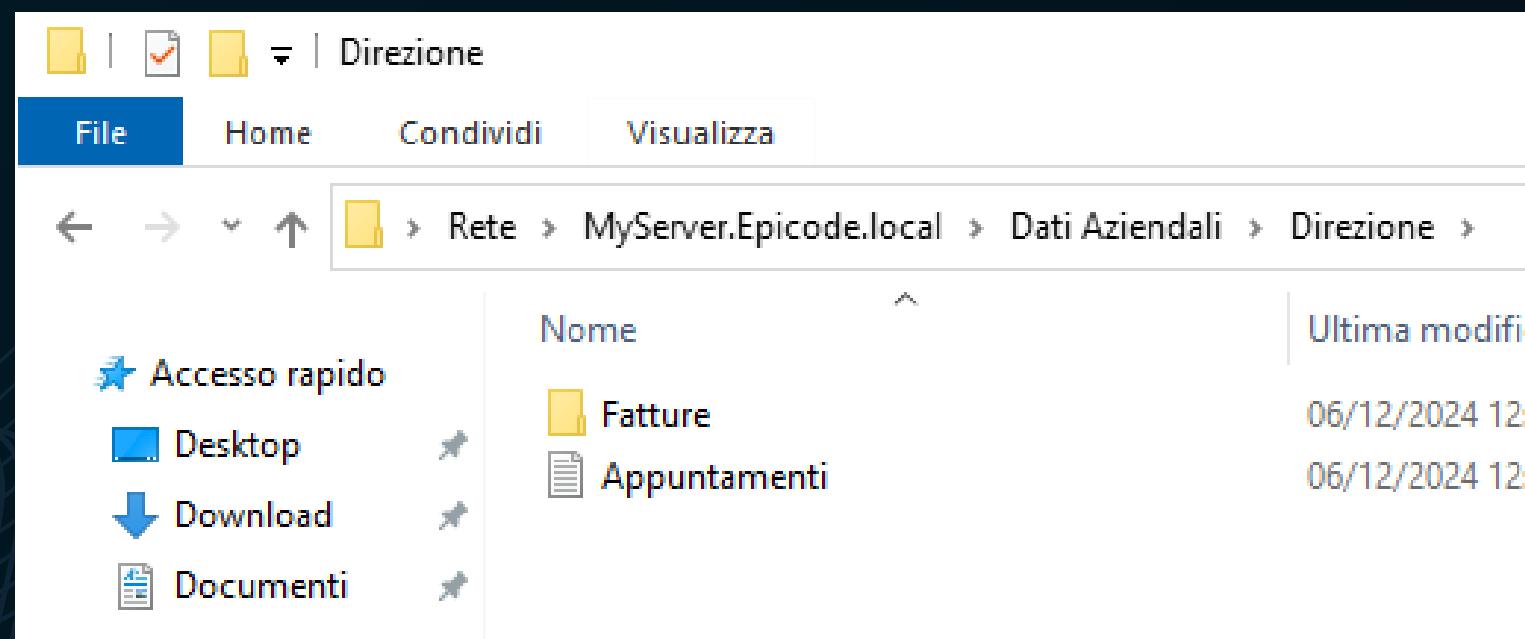
Specifiche dispositivo

Nome dispositivo	DESKTOP-UFJTA0R
Nome completo del dispositivo	DESKTOP-UFJTA0R.Epicode.local
Processore	12th Gen Intel(R) Core(TM) i7-1255U 2.61 GHz
RAM installata	4,00 GB
ID dispositivo	3893A69C-D84F-4225- A287-29BBDD27B645
ID prodotto	00330-80000-00000-AA538
Tipo sistema	Sistema operativo a 64 bit, processore basato su x64
Penna e tocco	Nessun input penna o tocco disponibile per questo schermo

TEST

L'account Direttore, facendo parte del gruppo "Direzione", non dovrebbe avere limitazioni sulla visualizzazione delle cartelle. Non ho applicato restrizioni poichè un direttore, visto il suo ruolo in azienda, potrebbe avere la possibilità di accedere a file e cartelle degli uffici dei suoi dipendenti.

Correttamente ha il permesso ad entrare in entrambe le cartelle.



TEST

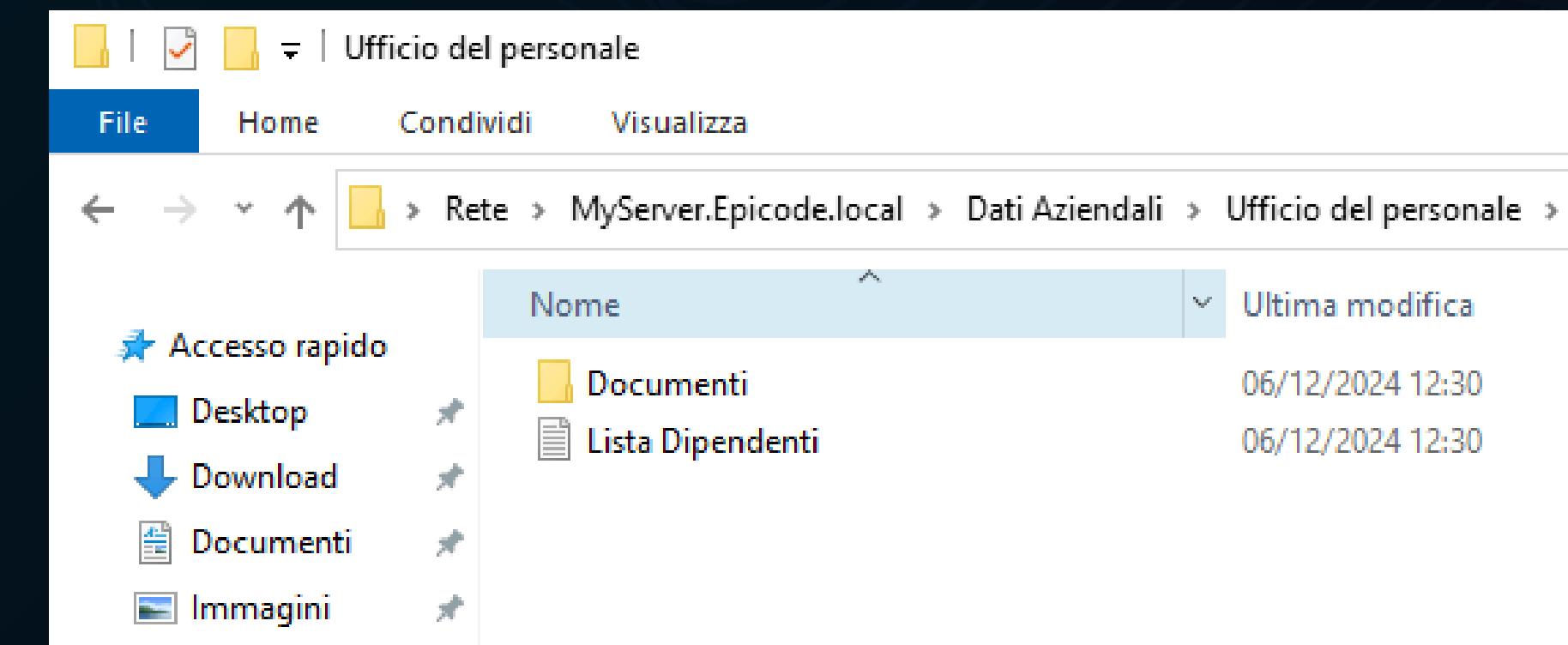
Ora procederò con la verifica delle restrizioni applicate al gruppo “Ufficio del personale”. Effettuerò quindi il login con l'account “Marzia”.



N.B. il primo accesso richiederà la modifica della password dell'account.

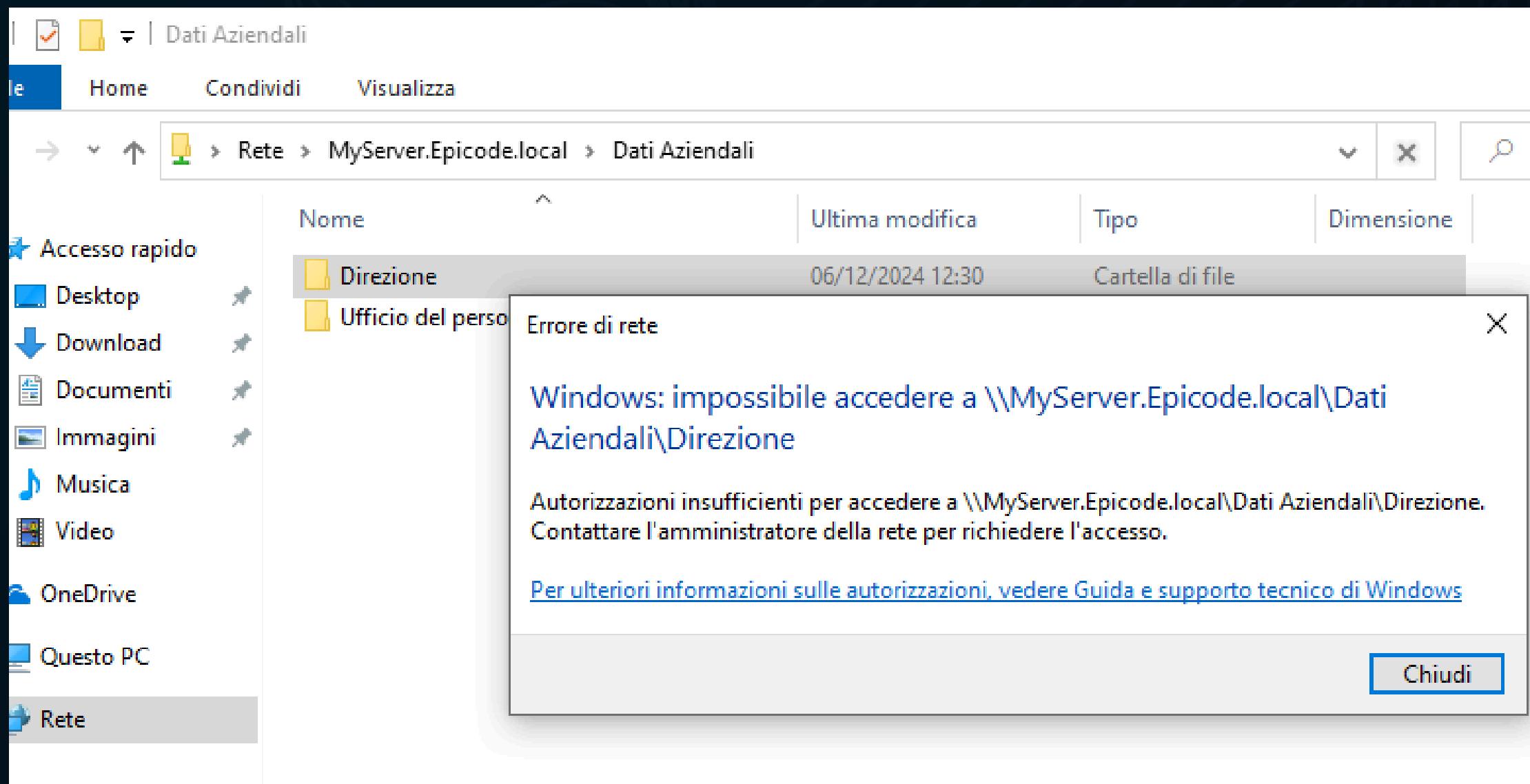
TEST

Una volta effettuato l'accesso proverò quindi ad entrare nelle due cartelle con restrizioni. Nella cartella "Ufficio del personale" entrerò senza problemi.



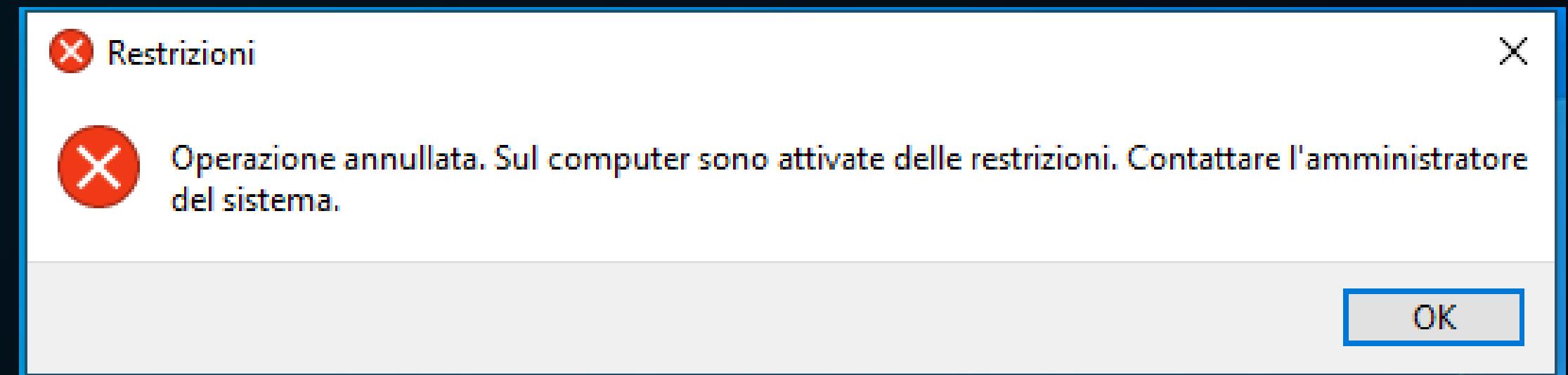
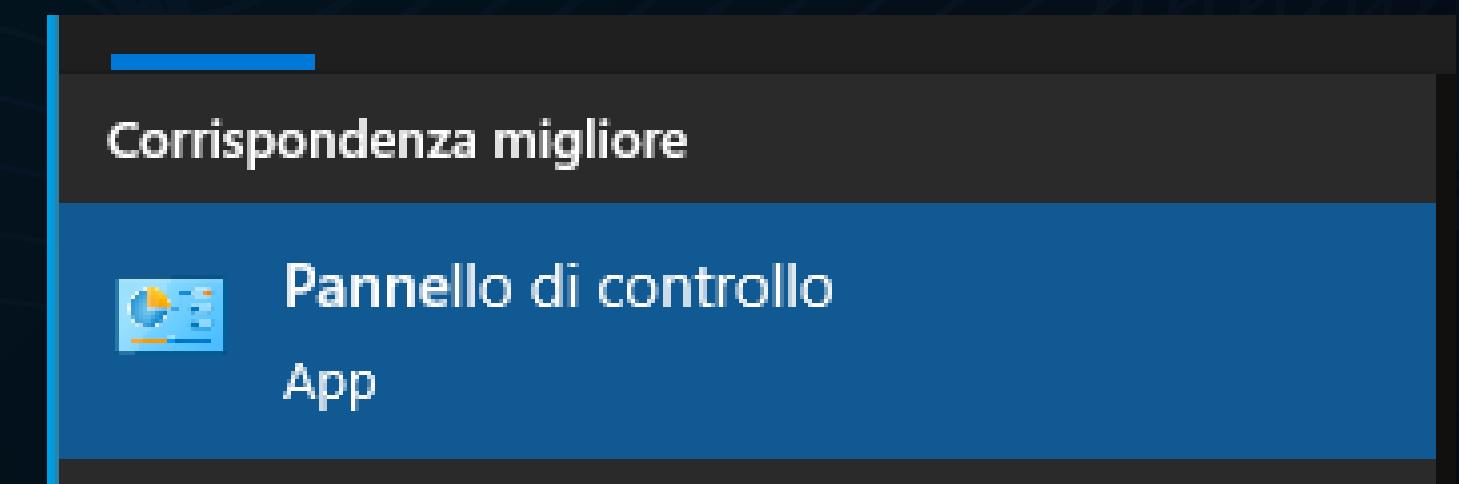
TEST

Nella cartella
direzione invece
non potrò
effettuare l'accesso.



TEST

Infine ho testato l'accesso al pannello di controllo per cambiare impostazioni di sistema ma la restrizione applicata in precedenza non me lo ha permesso.



CONCLUSIONI

CONCLUSIONI

Questa simulazione con Windows Server e Active Directory ha evidenziato l'importanza di una pianificazione accurata e di una gestione centralizzata per garantire un'infrastruttura IT efficiente.

Importante è l'avere cura di ogni impostazione per evitare problemi di interazione tra i sistemi.

Le policy sugli account permettono di controllare l'accesso alle risorse, proteggendo i dati sensibili e migliorando la produttività.

Active directory fornisce gli strumenti essenziali per amministrare reti complesse garantendo sicurezza e controllo.



THANK
YOU