



CYBERSECURITY

# WINDOWS SERVER

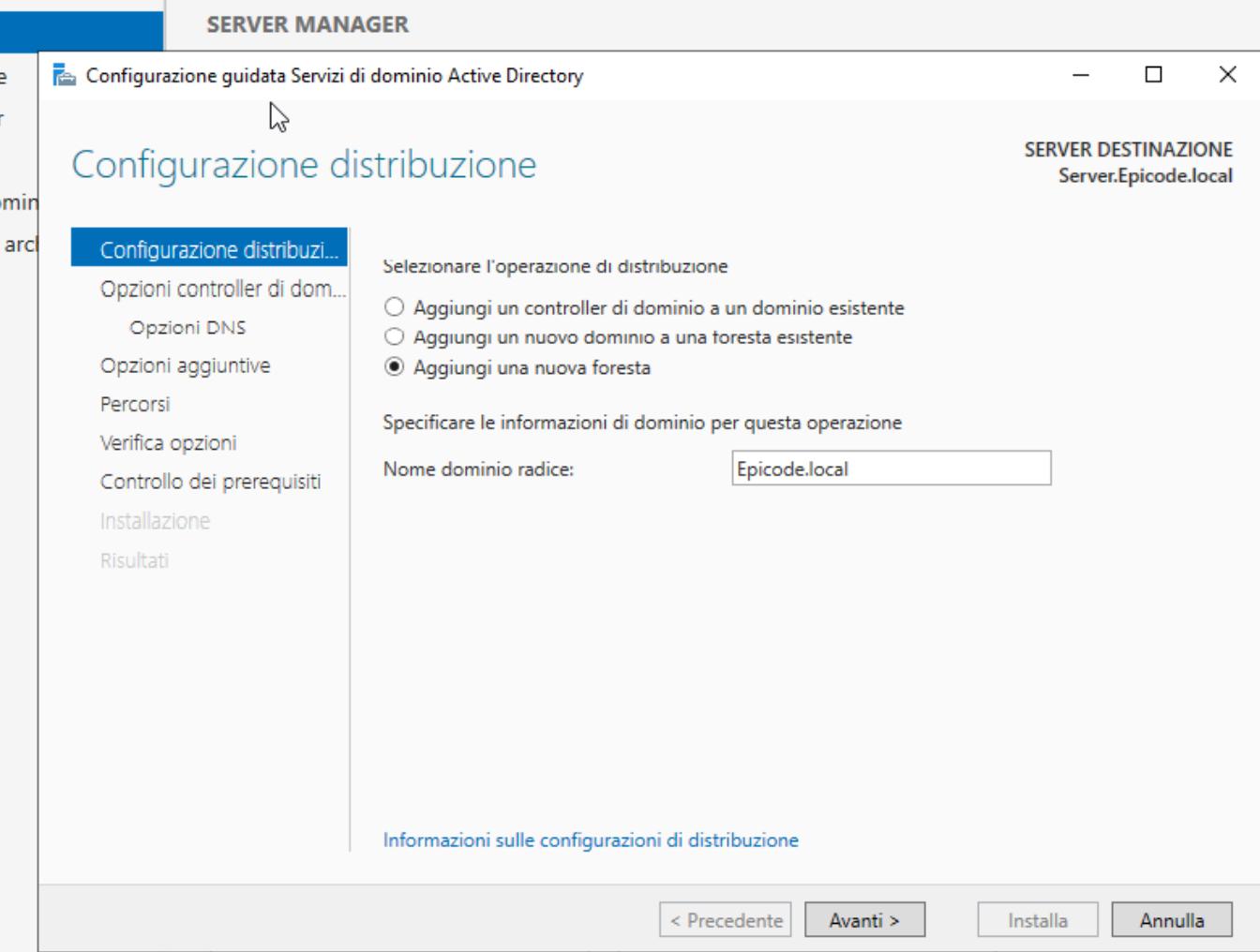
DI CARMINE MALANGONE

# INDICE

- 01** PREPARAZIONE
- 02** CREAZIONE DEI GRUPPI
- 03** ASSEGNAZIONE DEI PERMESSI
- 04** GRUPPO MANAGER
- 05** GRUPPO TEAM1
- 06** CONCLUSIONE

# PREPARAZIONE

*Nome Dominio*



Per l'esecuzione di questa attività, è stato utilizzato un ambiente Windows Server 2022 con i necessari permessi amministrativi per la gestione di utenti e gruppi. Come prima cosa andiamo a creare una foresta con nome di dominio **Eicode.local**

In informatica, una foresta (in inglese *forest*) è un termine utilizzato per descrivere una struttura gerarchica e logica composta da più domini in un sistema di directory, come Active Directory (AD) di Microsoft. È la struttura organizzativa più grande all'interno di un sistema Active Directory ed è progettata per gestire e organizzare risorse su larga scala.

# CREAZIONE GRUPPI

Dopo aver creato le **unità organizzative** andremo a creare gli **utenti** e i **gruppi**.

Creiamo le unità organizzative, una la chiameremo **AMMINISTRAZIONE** e l'altra **SVILUPPATORI**

1

Dopo di che andiamo a creare i gruppi che chiameremo **Team1** in sviluppatori e **Manager** in amministrazione

2

Ora andremo a creare i vari utenti e a dare i permessi ai gruppi

3

# CREAZIONE GRUPPI

Sono stati creati due gruppi distinti:

- **Sviluppatori:** Questo gruppo è stato creato per il team di sviluppatori e avrà meno diversi dal gruppo di amministrazione.
- **Amministrazione:** Questo gruppo rappresenta i membri con ruoli decisionali e accesso a funzioni di gestione aziendale.

The screenshot shows the Windows Server interface with the Active Directory module open. On the left, the navigation pane includes 'Server Manager', 'Dashboard', 'Services', 'Tools', 'Accounts', 'DNS', 'IIS', 'Search', and 'Security'. The main pane displays the 'Utenti e computer di Active Directory' (Active Directory Users and Computers) view for the 'Epicode.local' domain. A tree view on the left lists 'Query salvate', 'Epicode.local' (expanded to show 'amministrazione', 'BuiltIn', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Managed Service Account', 'sviluppatori', and 'Users'), and 'Utenti e computer di Active Directory'. To the right, a table lists four entries: 'Enzo' (Utente), 'Giovanni' (Utente), 'Leo' (Utente), and 'team1' (Gruppo di). Below this is a 'Membri:' section with three users: Enzo, Giovanni, and Leo, all listed under the 'sviluppatori' group. A tab bar at the top right includes 'Generale', 'Membri' (which is selected), 'Membro di', and 'Gestito da'.

This screenshot shows the same ADUC interface. The 'amministrazione' group node is highlighted in blue in the tree view. The table on the right now lists four members: 'Antonio' (Utente), 'Carmine' (Utente), 'francesco' (Utente), and 'Manager' (Gruppo di sicurezza). The 'amministrazione' group is also listed under the 'Epicode.local' domain in the tree view. The 'Generale' tab is selected at the top right.

# ASSEGNAZIONE DEI PERMESSI

In questa fase, abbiamo proceduto con l'assegnazione dei permessi alle cartelle, seguendo questi passaggi:

## Condivisione delle Cartelle:

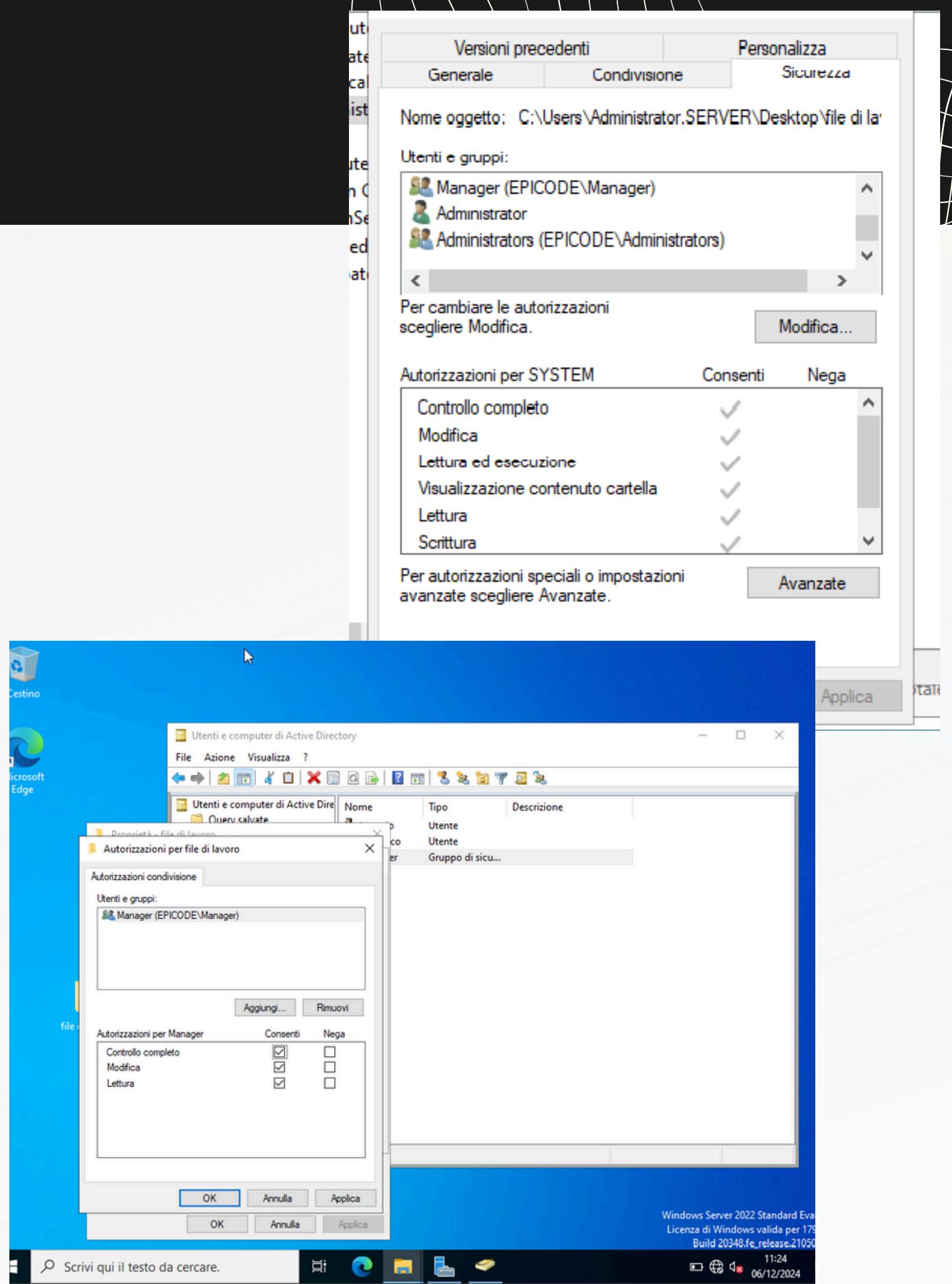
- Per la cartella "**dati di lavoro**", abbiamo rimosso il gruppo predefinito **Everyone** dalla lista dei permessi di condivisione, per garantire che solo gli utenti e i gruppi autorizzati possano accedere alla cartella.
- Successivamente, abbiamo aggiunto i gruppi creati in precedenza alla cartella , concedendo loro i diritti di accesso necessari.

## Impostazioni di Sicurezza:

Abbiamo proceduto con la configurazione delle Impostazioni di Sicurezza per entrambe le cartelle, dove abbiamo ripetuto l'operazione di rimozione del gruppo Everyone e aggiunto i gruppi appropriati. Alla cartella file manager , abbiamo concesso l'accesso al gruppo Manager, mentre alla cartella file team1, l'accesso è consentito al gruppo Sviluppatori. Queste modifiche assicurano che solo i membri specifici di ciascun gruppo possano accedere alle cartelle a loro destinate, rispettando le politiche di sicurezza e di accesso della rete aziendale.

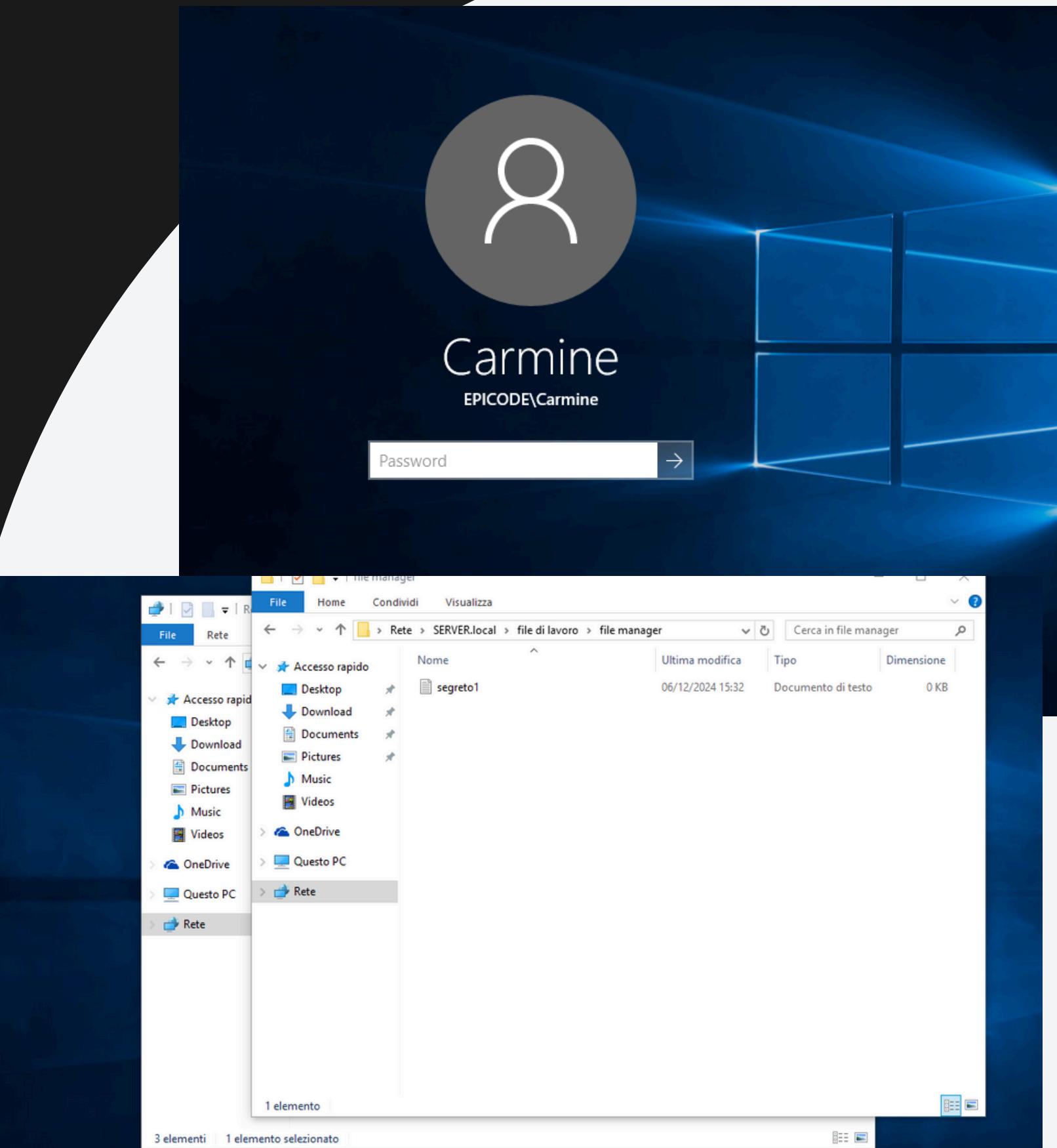
# ESEMPI

Qui possiamo vedere i due tipi di autorizzazione che possiamo dare, quando noi andiamo e digitiamo propria vedremo le voci condividi e sicurezza e li potremo aggiungere i permessi ai vari gruppi/utenti. In base ai permessi che andiamo a dare i gruppi potranno interagire con i file presenti sul server. Successivamente se un utente prova a vedere un file per il quale non ha il permesso apparirà l'errore impossibile accedere al file.



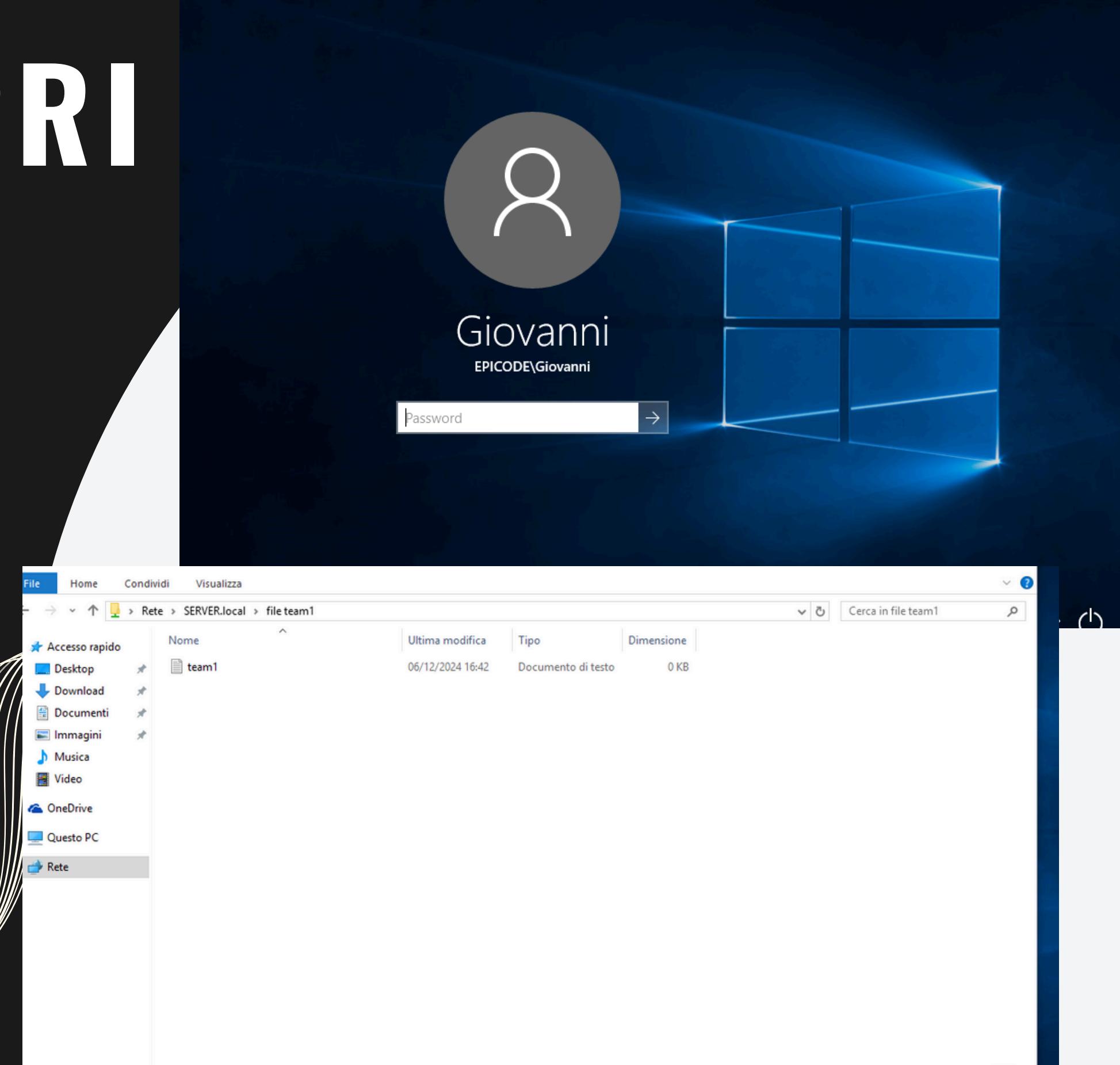
# ACCESSO CON GRUPPO MANAGER

Una volta settati i permessi andremo ad eseguire l'accesso tramite windows 10, useremo un utente del gruppo Manager ovvero Carmine. Una volta effettuato l'accesso useremo il comando win r e cerchiamo \\SERVER.local così da visualizzare le cartelle del server. E con i nostri permessi apriremo la cartella file manager.



# ACCESSO CON GRUPPO SVILUPPATPRI

Ora effettueremo l'accesso con il gruppo degli sviluppatori e tramite il comando citato prima andremo a visualizzare il documento presente nella cartella team1



# CONCLUSIONI



L'attività svolta ha consentito di configurare un'infrastruttura di rete centralizzata e sicura basata su Windows Server 2022 e un client Windows 10. Partendo dalla configurazione del server, abbiamo assegnato un indirizzo IP statico e configurato il DNS per garantire la connettività stabile e la risoluzione dei nomi di dominio.

Abbiamo quindi promosso il server a Controller di Dominio, creando una nuova foresta e il dominio **Eicode.local**, che costituisce il cuore dell'ambiente Active Directory. Successivamente, abbiamo organizzato gli utenti e i gruppi creando due Unità Organizzative (**Sviluppatori** e **Amministrazione**), assegnando utenti e gruppi dedicati, come **Manager** e **Team1**, per semplificare la gestione dei permessi.

Attraverso un'attenta configurazione delle cartelle condivise, sono stati assegnati i permessi di accesso ai gruppi corretti. La verifica finale ha confermato che i permessi funzionano come previsto: gli utenti del gruppo Manager hanno accesso esclusivo alla cartella **File manager**, mentre gli utenti di **Team1** accedono solo alla cartella **File team1**.

Questo processo ha dimostrato la capacità di Windows Server 2022 di gestire un ambiente di rete sicuro ed efficiente, centralizzando l'autenticazione e il controllo degli accessi, migliorando al contempo l'organizzazione e la sicurezza dei dati aziendali.