Sommario

1. Traccia e Obiettivi

L'obiettivo del progetto è acquisire familiarità con la gestione dei gruppi di utenti in Windows Server 2022.

a. Preparazione
- Accedi al tuo ambiente Windows Server 2022.
- Assicurati di avere i permessi amministrativi necessari per creare e gestire gruppi.

b. 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.).

c. Assegnare i 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.

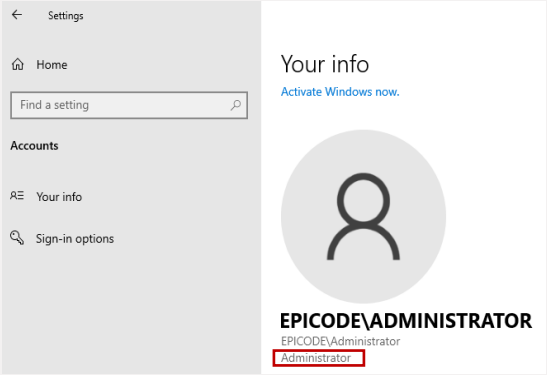
d. Verifica accessi
- Una volta creati i gruppi e assegnati i permessi, verifica che le impostazioni siano corrette. Puoi farlo:
  - Creando utenti di prova e aggiungendoli ai gruppi.
  - Verificando che gli utenti abbiano i permessi assegnati in base al gruppo a cui appartengono.
  - Verifica che altri utenti non possano accedere a quelle risorse.

e. Documenta
- 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.

Nota: L'esercizio è stato sviluppato relativamente al dominio configurato a lezione date le tempistiche, ma è stato realizzato un vademecum a corredo per l'installazione e configurazione di Windows Server 2022 e delle Active Directory.

2. Preparazione

Una volta effettuato l'accesso a Windows Server 2022, verifichiamo di avere privilegi amministrativi accedendo a **Settings -> Accounts -> Your Info.** Notiamo di essere amministratori grazie alla voce **Administrator** sotto al nome utente **EPICODE\Administrator**.

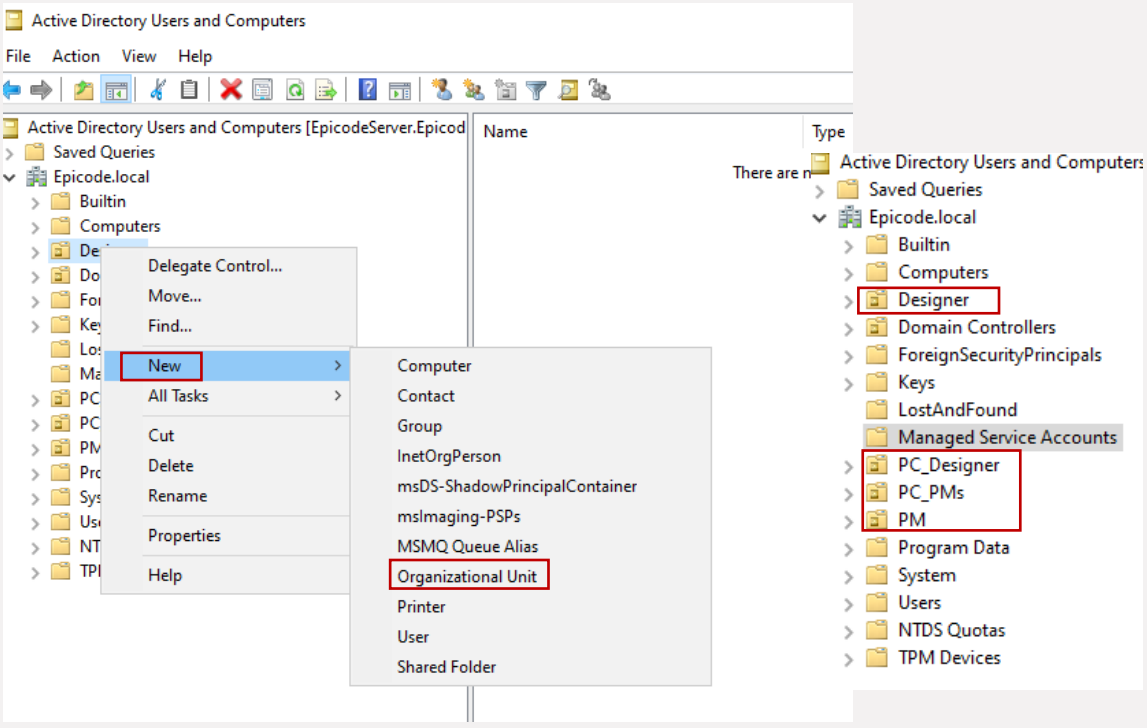


3. Creazione Gruppi

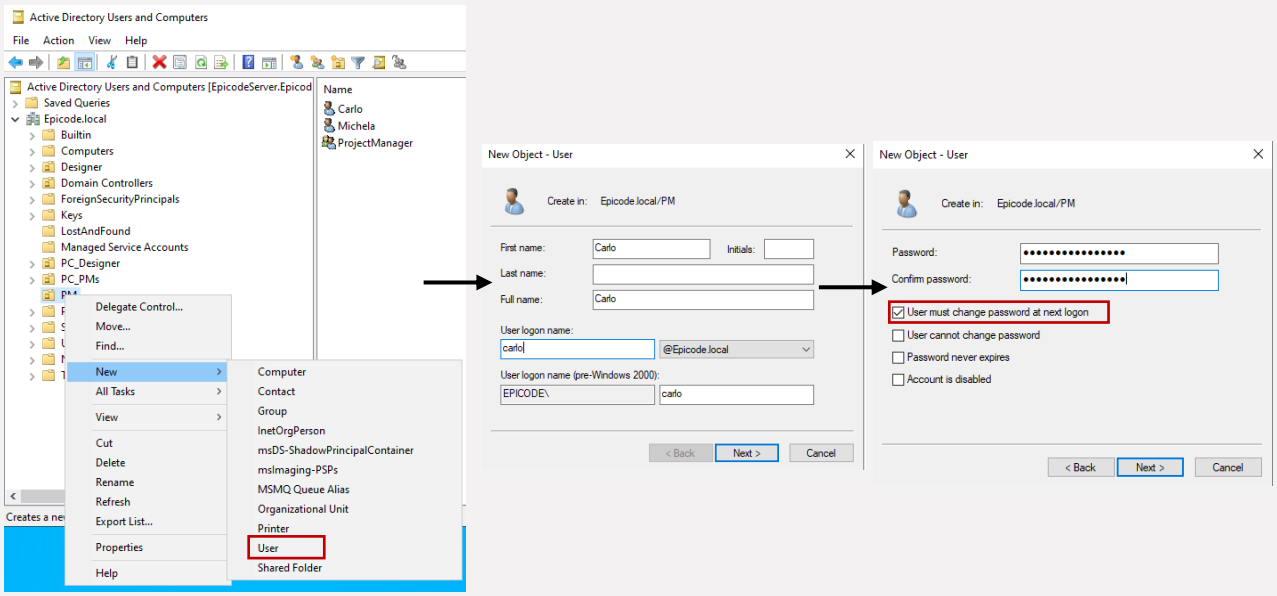
Si procede alla creazione di due gruppi:

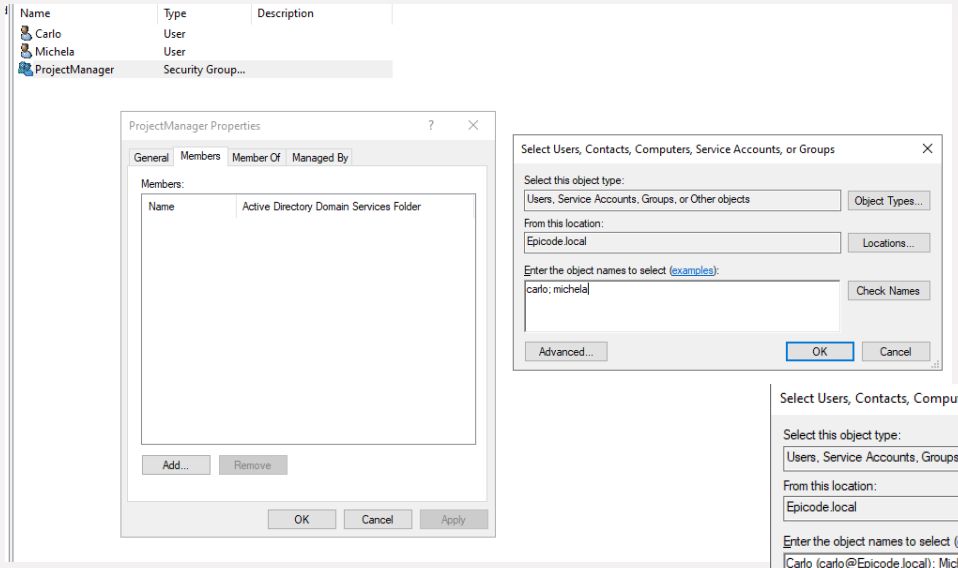
1. **ProjectManager** che conterrà i PM (Project Manager) dell'azienda (Carlo e Michela);
2. **Designer** con i progettisti dell'azienda (Alessandra e Gianfranco).

Si procede con la creazione di 4 **Organizational Unit – OU** che conterranno rispettivamente i PM, i Designer, PC_PM (PC dei Project Manager) e PC_Designer. I primi due conterranno gli user relativi, gli altri i PC degli utenti.

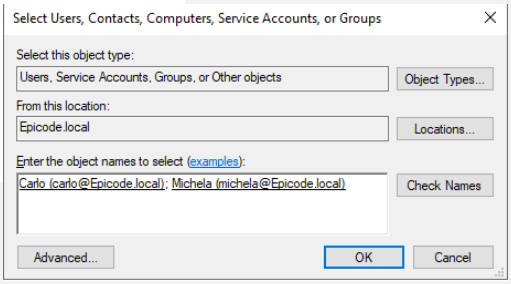


Dopo aver creato le OU, abbiamo inserito gli utenti corrispondenti, assicurandoci di selezionare l'opzione ***User must change password at next logon***, buona pratica per motivi di sicurezza.

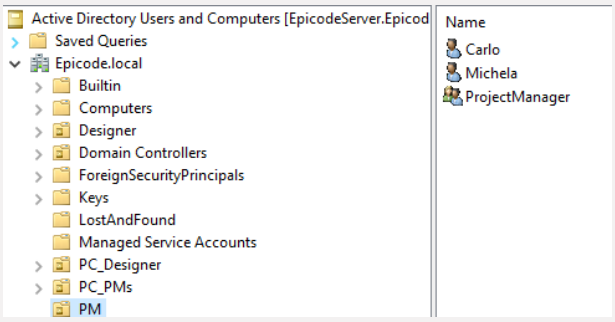


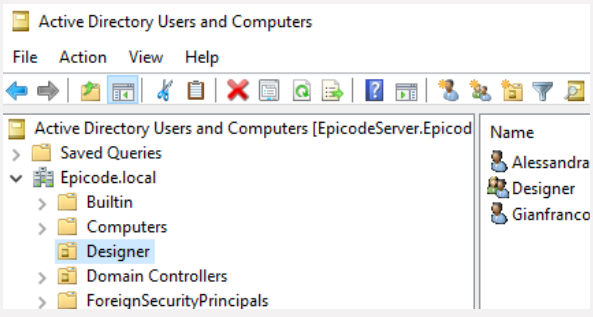


Inserendo i nomi degli utenti, con ***check names*** possiamo attuare la risoluzione dei nomi che in **Active Directory** devono essere unici.

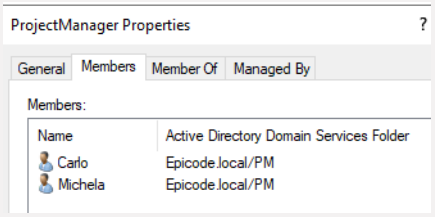


Al termine ci troveremo in questa condizione.



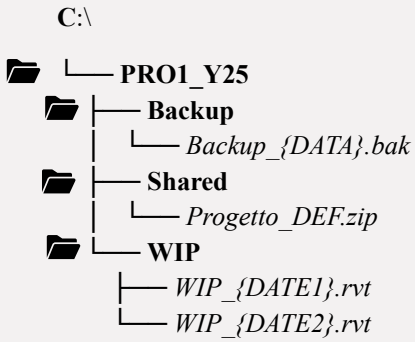


Esplorando le proprietà del gruppo **ProjectManager** troveremo nella sezione ***Members*** i nomi degli utenti appartenenti a quel gruppo.



Ripetiamo lo stesso procedimento per la creazione del gruppo **Designer**, inserendo in questo caso gli user **Gianfranco** e **Alessandra.**

Prima di passare alle impostazioni dei permessi, creiamo una struttura di cartelle e file ai quali verranno associati permessi diversi in relazione alle funzioni degli user definite dai gruppi.



Nota: I file, nonostante l'estensione riportata nel nome, sono file .txt creati per semplicità e per dimostrazione.

Ricordiamo anche il significato dei diversi permessi attribuibili alle cartelle e ai file.

Per le **cartelle:**

Autorizzazione	Leggere / Visualizzare	Scrivere / Creare	Modificare Contenuto	Eliminare	Eseguire Programmi	Modificare Autorizzazioni	Assumere Proprietà
Controllo Completo	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Modifica	Sì	Sì	Sì	Sì	Sì	No	No
Lettura	Sì	No	No	No	Sì	No	No

Per i **file:**

Autorizzazione	Leggere Contenuto	Scrivere Contenuto / Modificare	Eliminare	Eseguire Programma	Modificare Attributi / Proprietà	Modificare Autorizzazioni	Assumere Proprietà
Controllo Completo	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Modifica	Sì	Sì	Sì	Sì	Sì	No	No
Lettura ed Esecuzione	Sì	No	No	Sì	Sì	No	No
Lettura	Sì	No	No	No	Sì	No	No
Scrittura	No	Sì	No	No	Sì	No	No

4. Assegnazione dei Permessi

Andiamo adesso ad assegnare per ogni cartella e file i permessi, considerando di lasciare la possibilità di modificare le autorizzazioni e diventare owner ad un ipotetico gruppo IT.

In particolare assegneremo a:

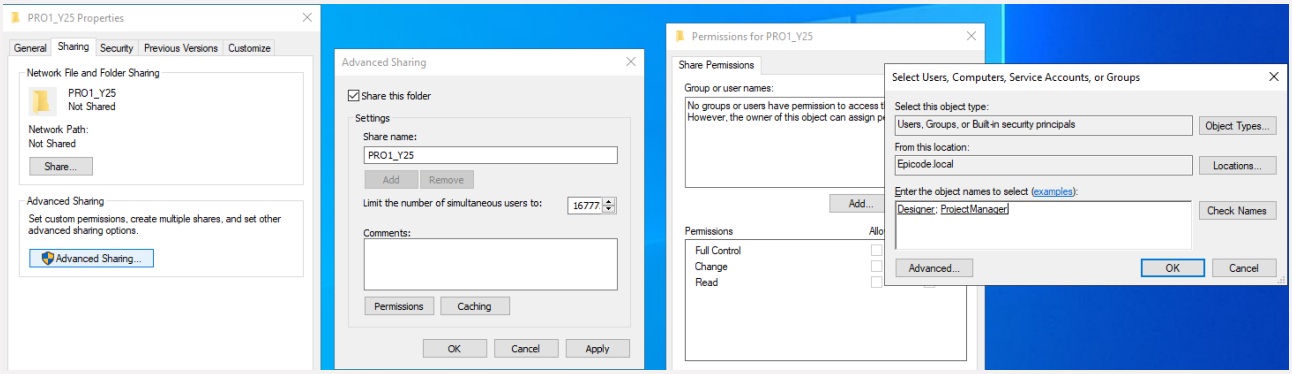
- cartella **PRO1_Y25**, per entrambi i gruppi i permessi ***Change*** (Modifica della tabella precedente) e ***Read*** (Lettura della tabella precedente). Questo perché vogliamo che entrambi i gruppi possano interagire con le cartelle e i file sottostanti.
- Sotto cartella **Backup** i permessi di ***Read*** e ***Change*** solo al gruppo **ProjectManager**. Essendo i PM responsabili della pianificazione, esecuzione e finalizzazione dei progetti, a differenza dei Designer che si occupano esclusivamente della progettazione. Quest'ultimi quindi non avranno accesso alla cartella.
- Sotto cartella **WIP** (Work In Progress) e **Shared**, per entrambi i gruppi i permessi ***Change*** (Modifica della tabella precedente) e ***Read*** (Lettura della tabella precedente). Questo perché vogliamo che entrambi i gruppi possano interagire con i file sottostanti.

Impostiamo ulteriormente i permessi specifici per i file:

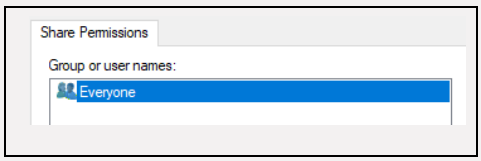
- **Backup_{DATA}.**bak: al gruppo **ProjectManager** sono stati assegnati tutti i permessi, ad eccezione del **Full Control**, tramite la scheda **Security → Edit**. Questo consente loro di aggiornare o eliminare i backup in base allo stato di avanzamento dei progetti.
- **WIP_{DATE1}.rvt** e **WIP_{DATE2}.rvt:** per entrambi il gruppo **ProjectManager** lasciamo solo ***Read***, mentre per il gruppo **Designer** lasciamo tutti i permessi tranne ***Full Control***.
- **Progetto_DEF.zip:** per il gruppo **Designer** imposto solo il permesso ***Read***. Possono solo visualizzare il file del progetto definitivo, senza possibilità di modificarlo, attività riservata ai Project Manager

4.1 Impostazione dei permessi: cartella PRO1_Y25

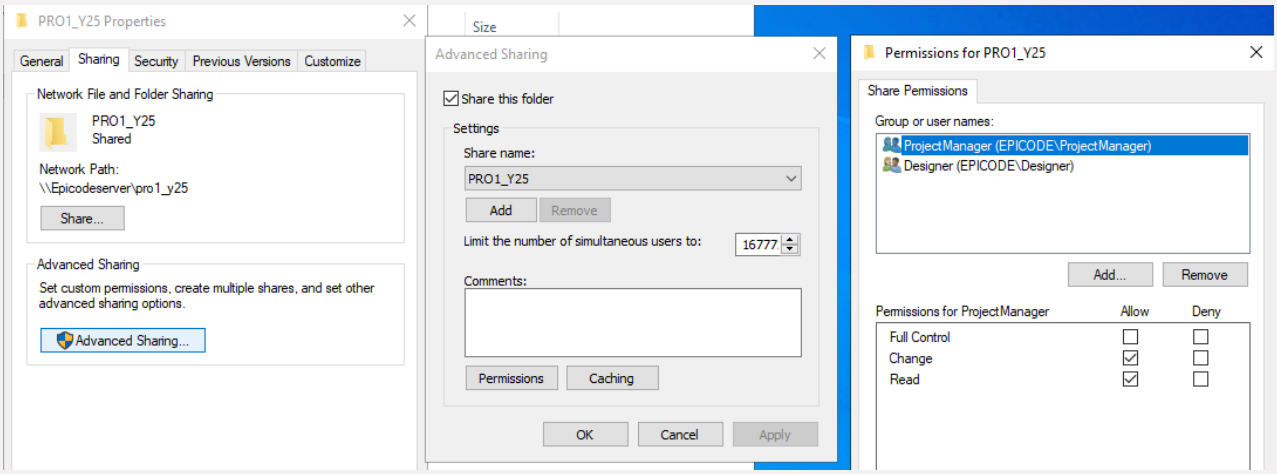
Aggiungiamo i gruppi alla cartella in ***Advanced Sharing -> Permissions -> Add…***

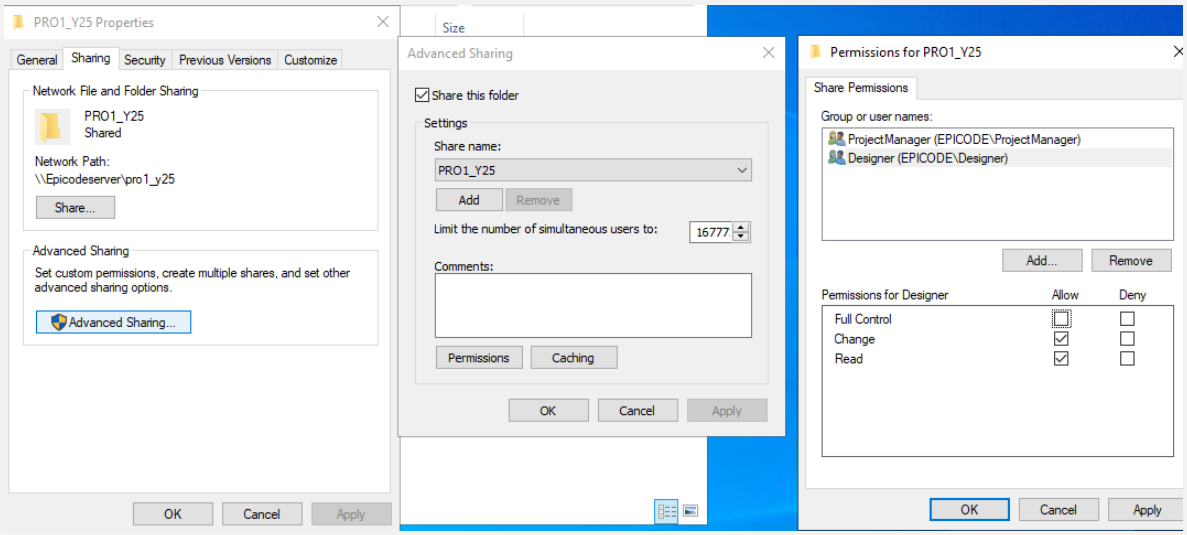


Nota: Eliminare il gruppo Everyone dai permessi poiché concede accesso a chiunque abbia anche solo una sessione sul sistema, senza distinguere ruoli, gruppi o privilegi. Ciò può esporre il sistema ad accessi non controllati.



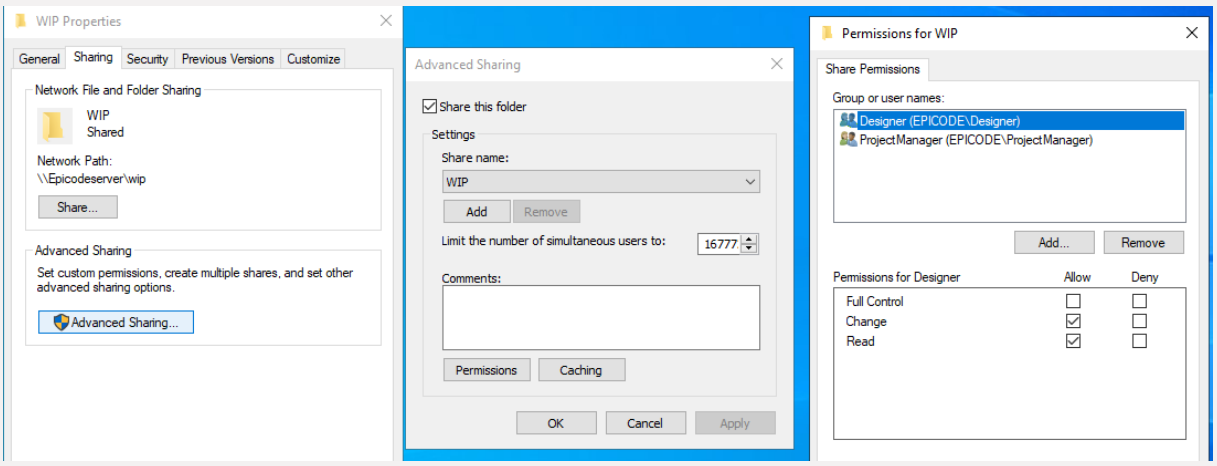
Aggiunti i gruppi impostiamo i loro permessi così come descritti precedentemente.

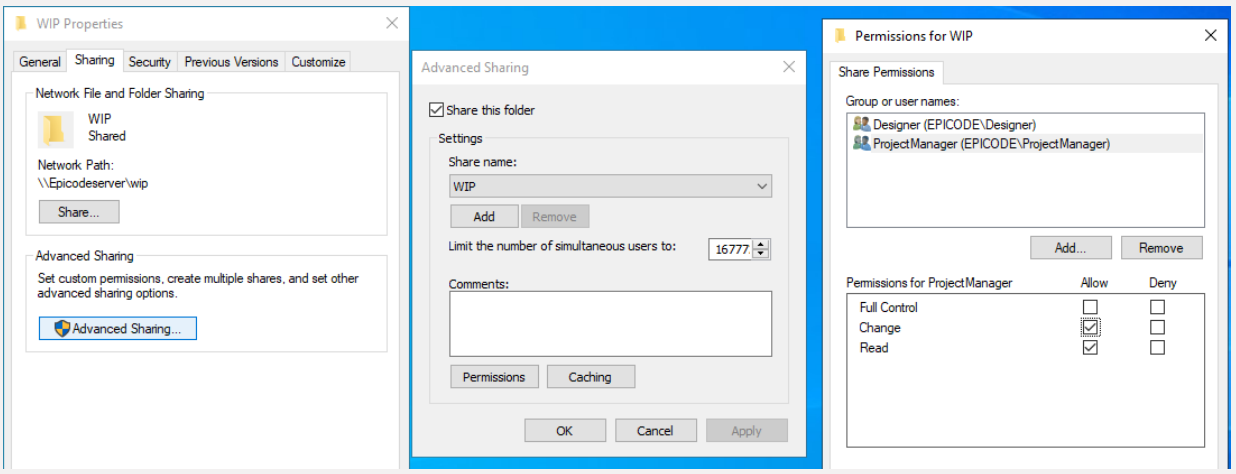




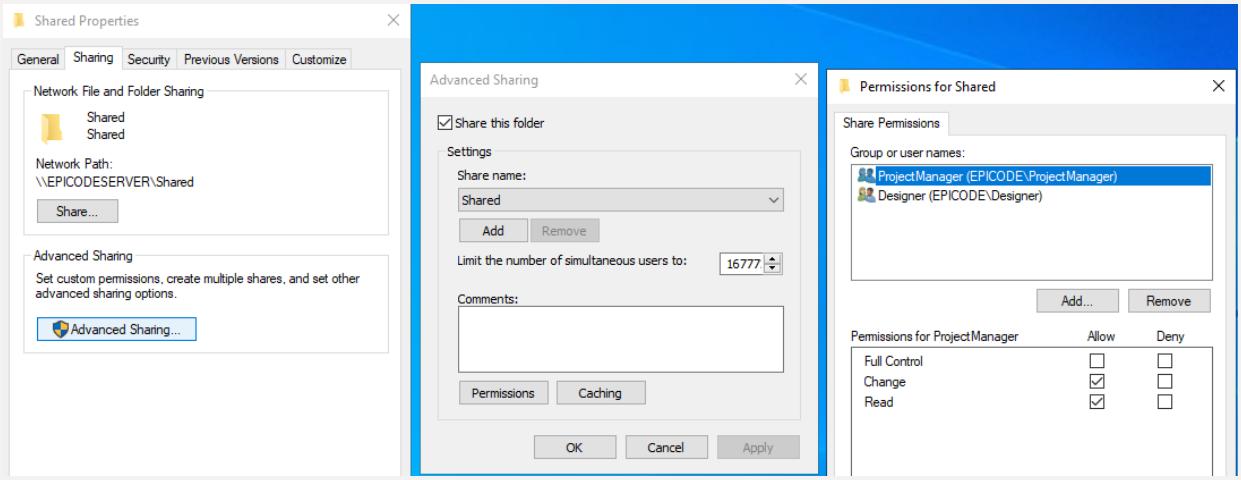
Ripetiamo lo stesso procedimento per le sotto cartelle **WIP**, **Shared** e **Backup.**

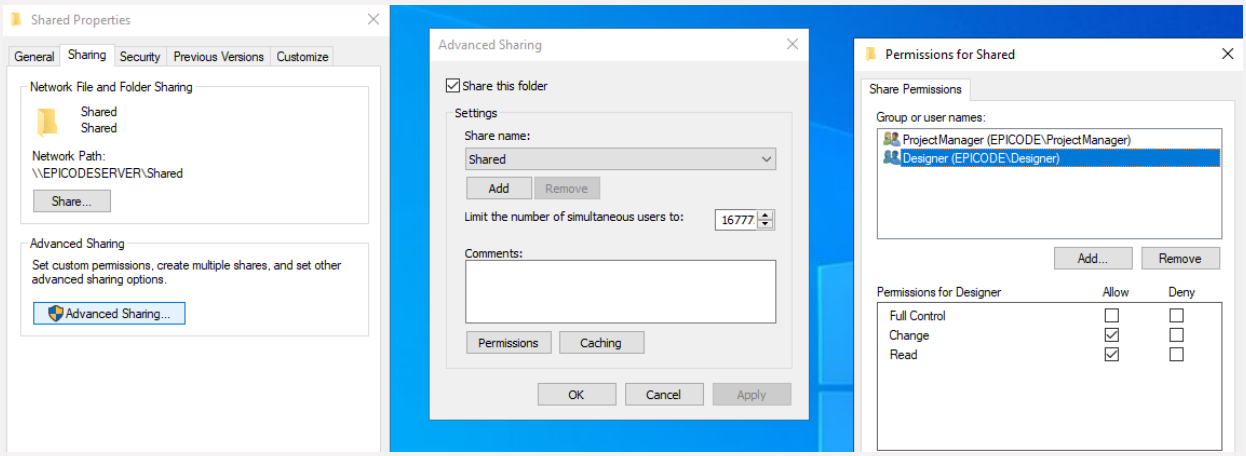
4.2 Impostazione dei permessi: sotto cartella WIP



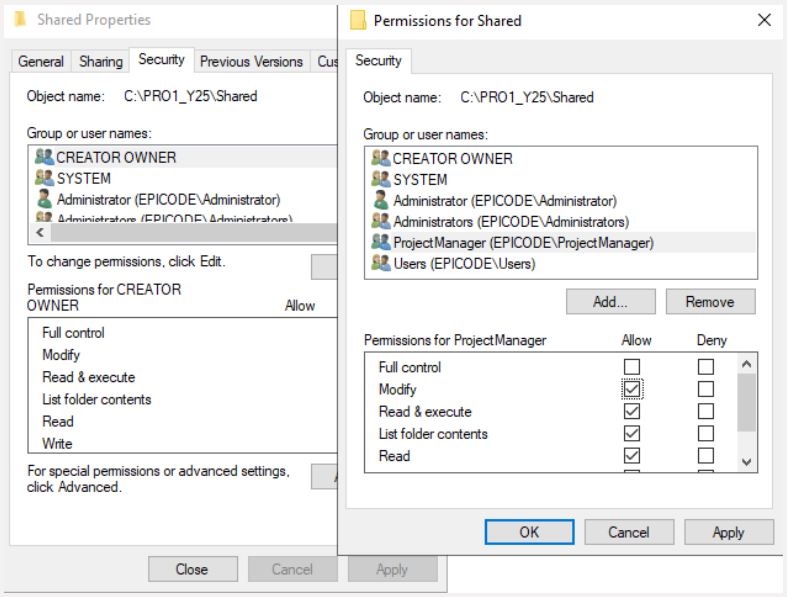


4.3 Impostazione dei permessi: sotto cartella Shared

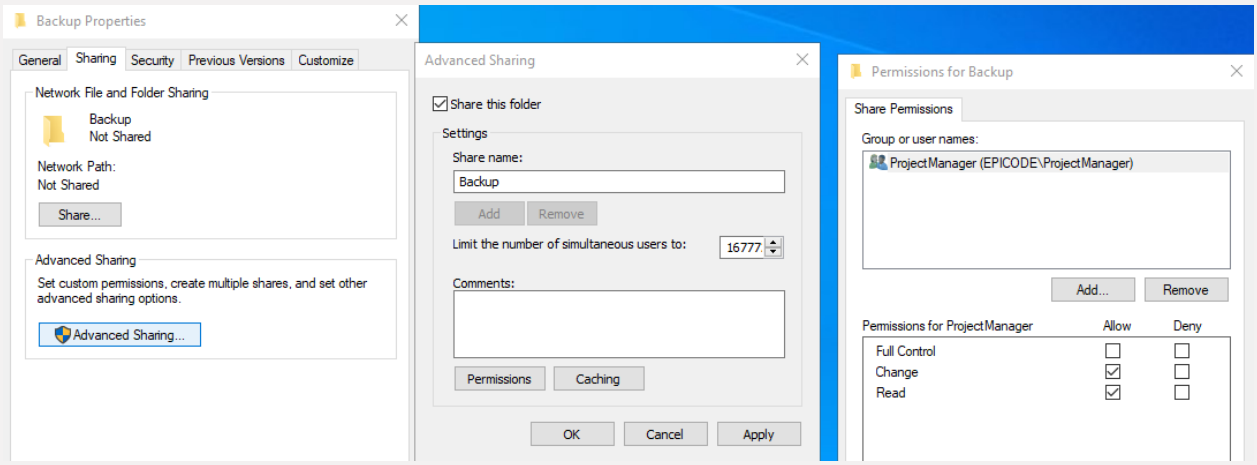




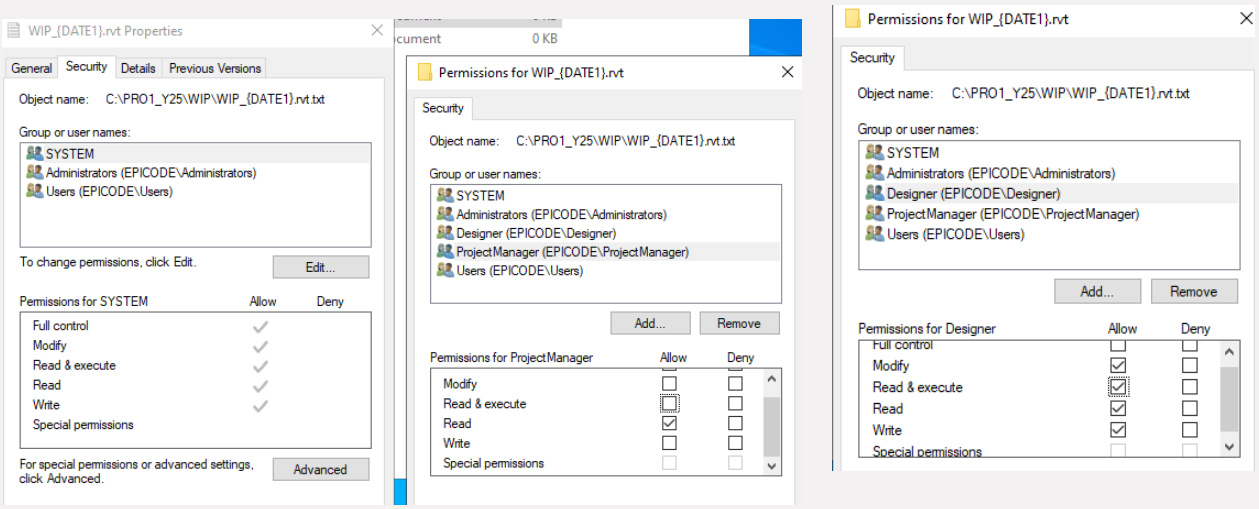
Oltre ad impostare i permessi nella scheda ***Sharing***, nella scheda ***Security*** imposto il permesso ***Modify*** per il gruppo **ProjectManager** così da concedere ai rispettivi utenti di cancellare eventualmente i file creati dagli utenti del gruppo **Designer**.



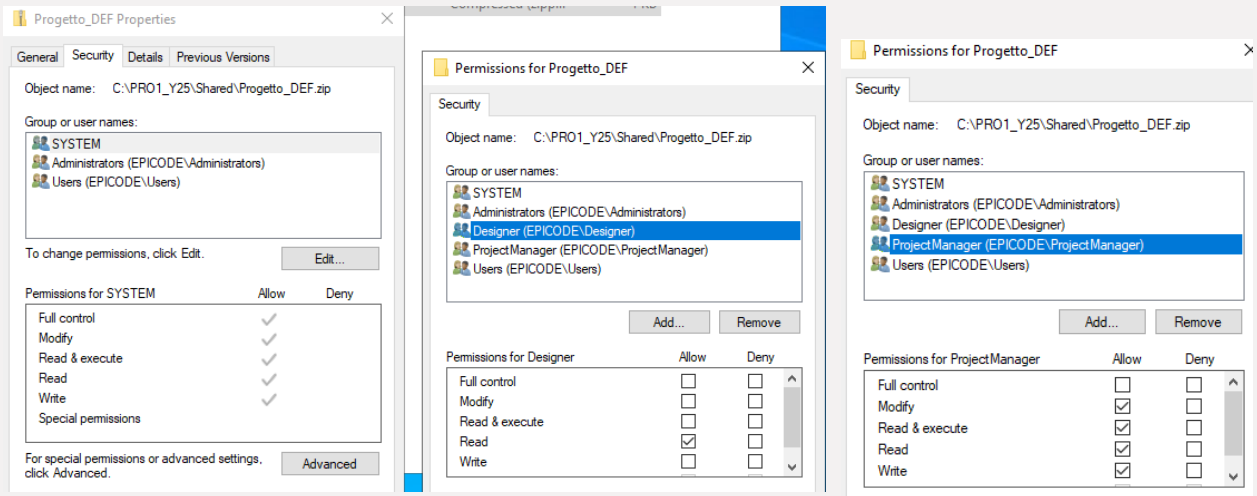
4.4 Impostazione dei permessi: sotto cartella Backup



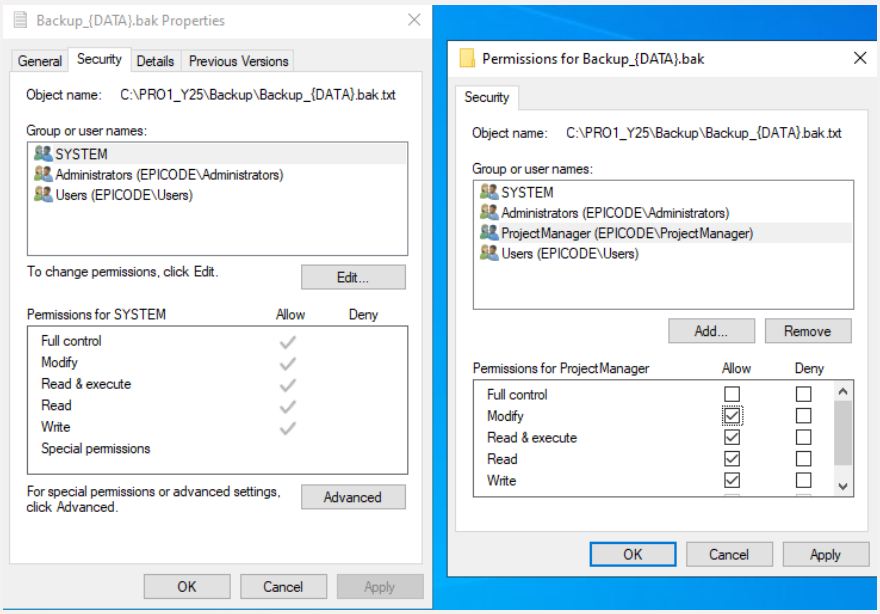
4.5 Impostazione dei permessi: file della sotto cartella WIP



4.6 Impostazione dei permessi: file della sotto cartella Shared



4.7 Impostazione dei permessi: file della sotto cartella Backup

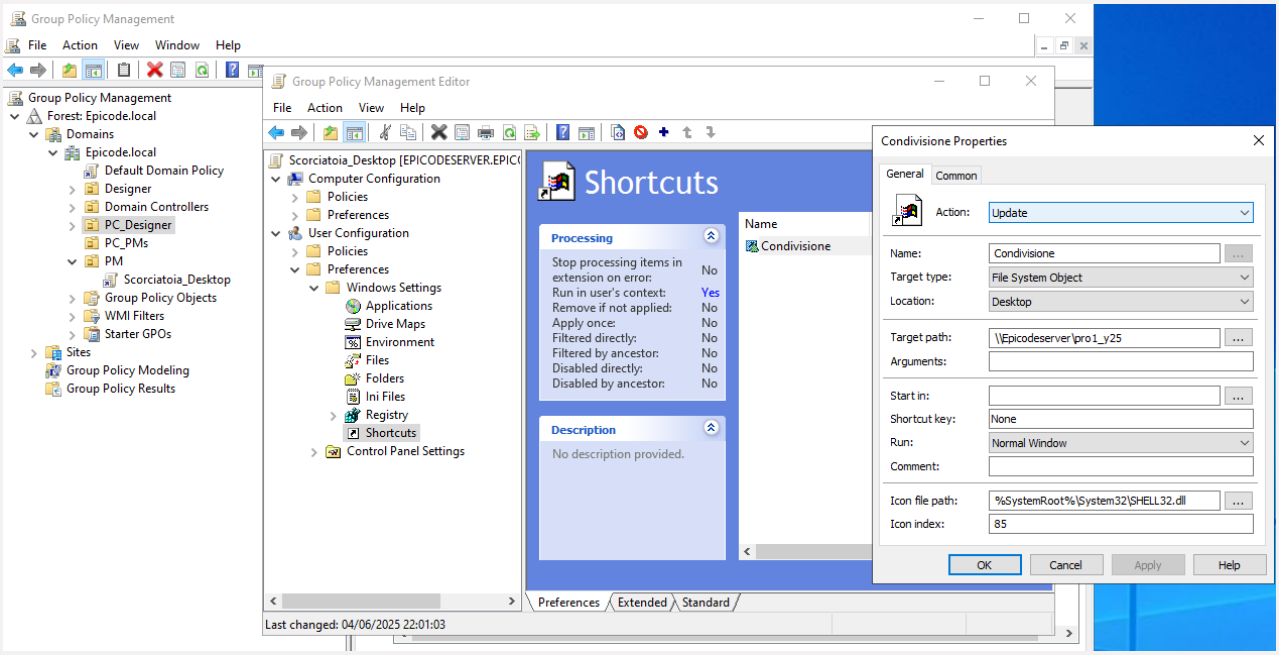


5. Implementazione delle GPO

5.1 Shortcut della cartella condivisa su desktop dell'utente

Nel pannello **Group Policy Management** (GPO) creiamo la policy dopo aver selezionato l'OU desiderata in cui vogliamo inserirla. Quella che vediamo nella UO è solo un collegamento a quella effettiva che possiamo controllare in **Group Policy Objects**.

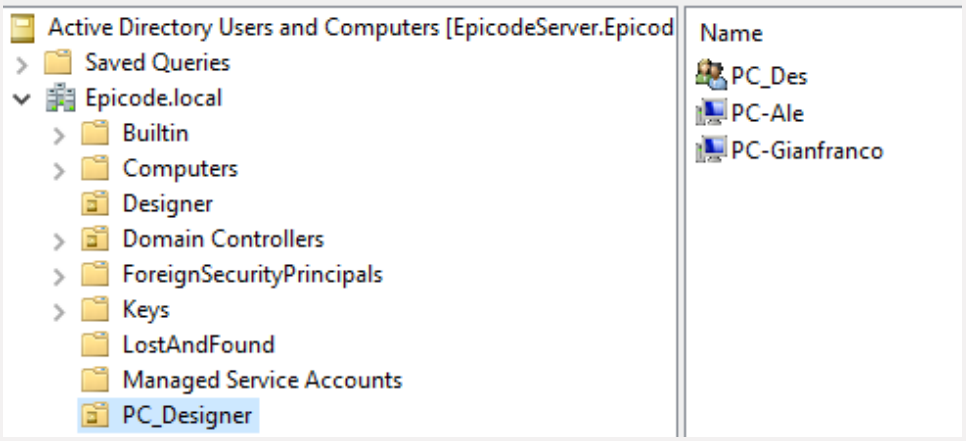
Premendo con tasto destro sulla nuova policy creata e su ***Edit***, possiamo impostarne le caratteristiche e il funzionamento, come nell'immagine sottostante.



Definita la policy la trasportiamo in tutte le OU in cui vogliamo inserirla, nel nostro caso sia nell'unità dei Designer che in quella dei PM.

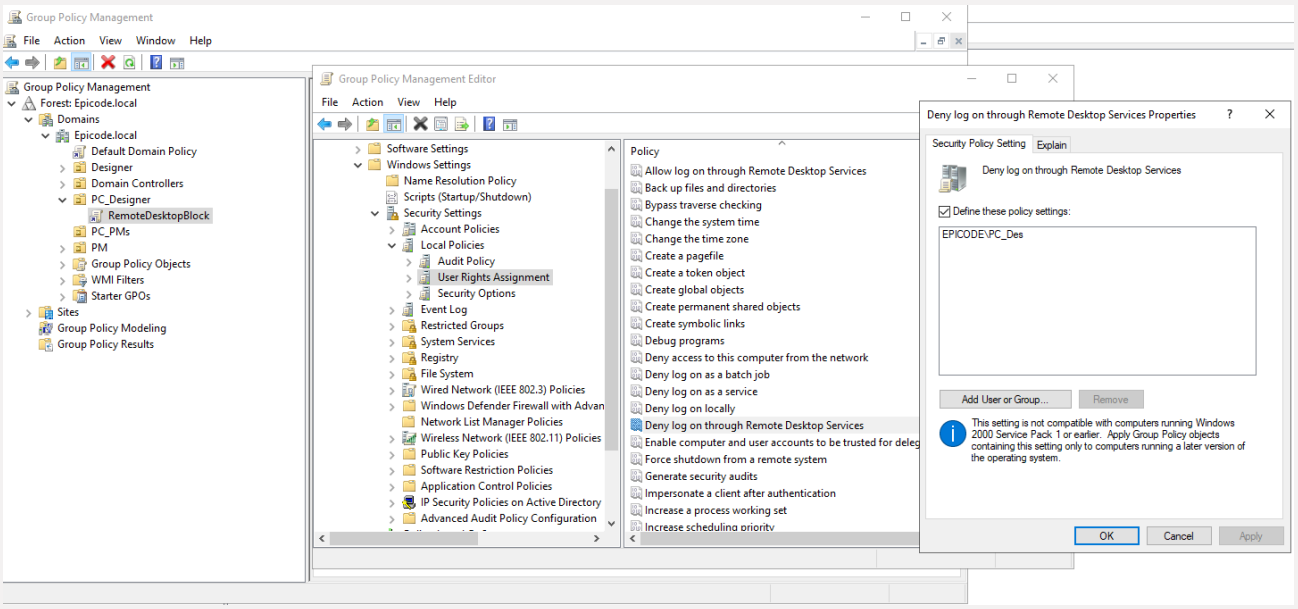
5.2 Impedimento dell'accesso remoto al server

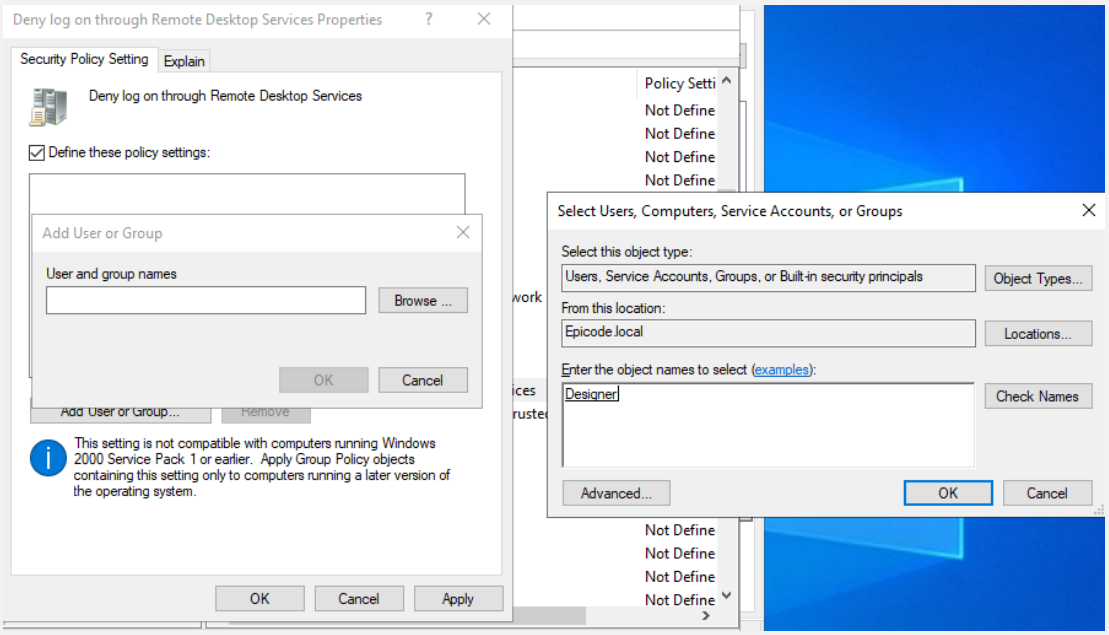
Questa policy riguarda i computer, e non gli utenti, quindi ritorniamo in **Active Directory Users and Computers** e andiamo ad aggiungere i pc relativi ad ogni utente, creando due OU, una per i pc dei Designer e una per i pc dei PM. Aggiungiamo inoltre i primi al gruppo **PC_Des** e i secondi al **PC_PMs**.



Impostiamo ora la policy in Group Policy Management seguendo lo stesso procedimento svolto per la policy relativa alla shortcut vista precedentemente. Questa volta, la policy di interesse si trova nella sezione **Computer Configuration**.

Trovata la policy, aprendo le **Properties** sarà possibile inserire il gruppo dei pc a cui associarla (nel nostro caso PC_Des).

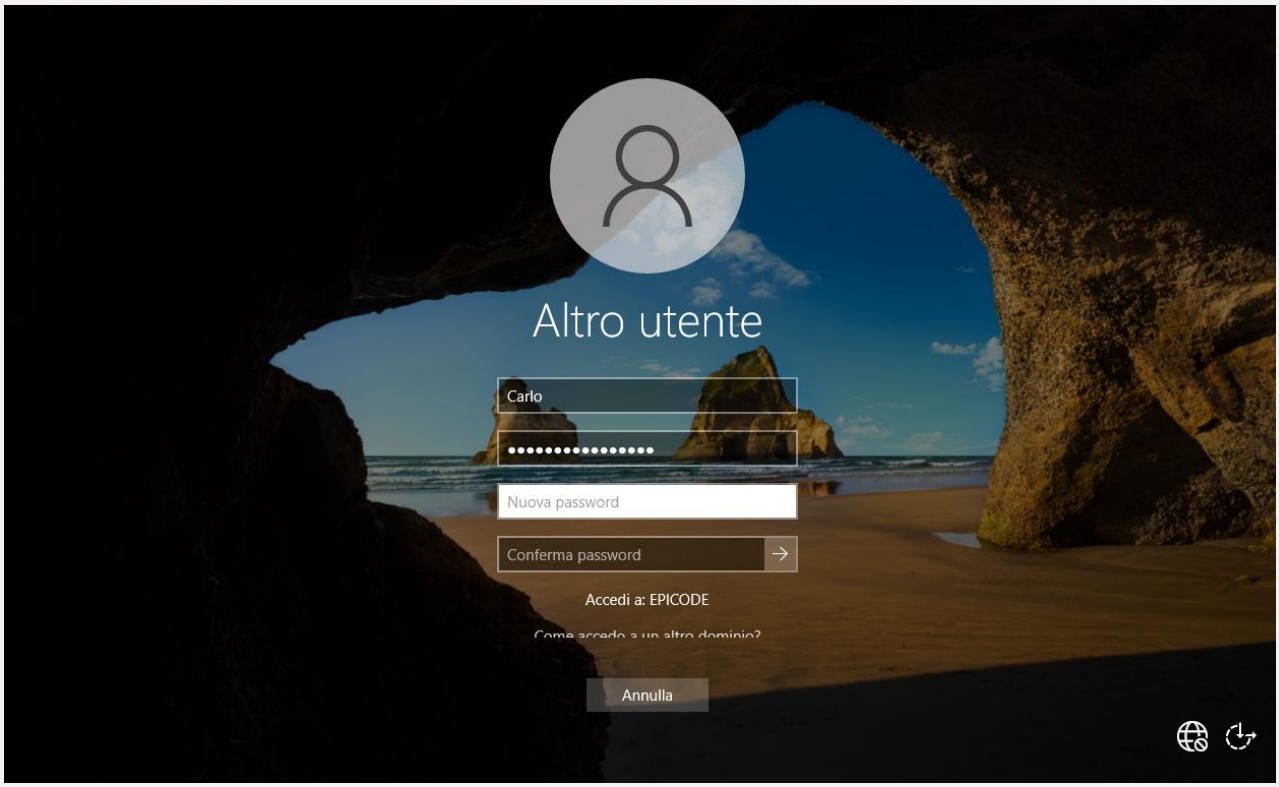




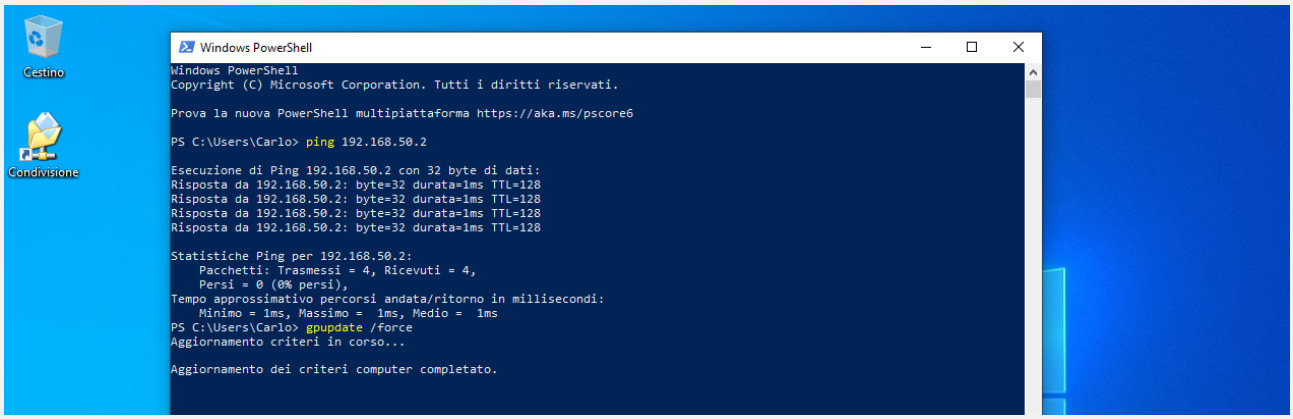
6. Verifica

6.1 Verifica dei permessi e delle policy per il gruppo ProjectManager

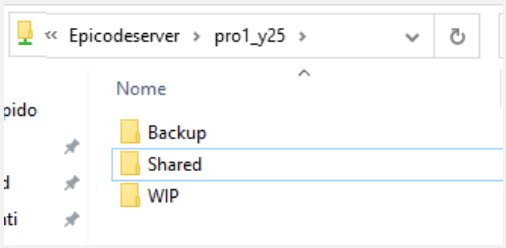
Eseguo l'accesso al PC con l'utente Carlo appartenente al gruppo ProjectManager. Avendo impostato la richiesta di variazione della password al primo ingresso, mi viene richiesto di farlo. La prima impostazione risulta correttamente applicata.



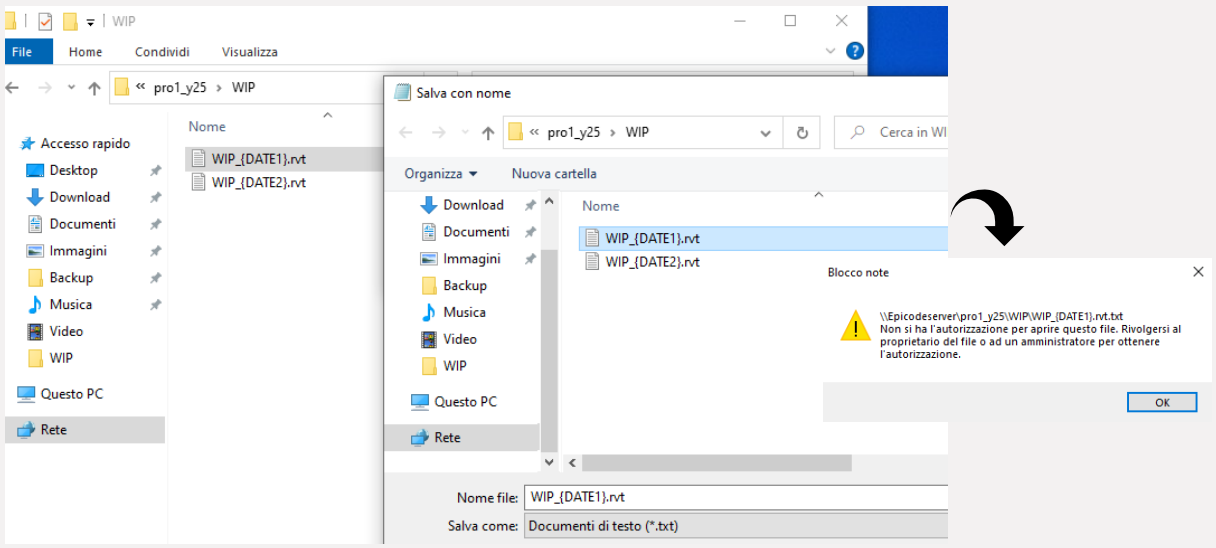
Una volta sul desktop, aprendo **PowerShell** , col comando ***gpupdate /force*** forzo le impostazioni create su Windows Server 2022. In questo modo, il collegamento alla cartella condivisa appare sul desktop, confermando l'applicazione della policy **Scorciatoia_Desktop**.



Accedendo alla cartella, posso verificare la presenza di tutte le sotto cartelle create, e in questo caso, la principale verifica consiste nel tentare di modificare i file WIP_{DATE1}.rvt.



Notiamo che è possibile aprirli, leggerli ma non salvarne le modifiche. Ciò conferma anche le impostazioni su questo utente.

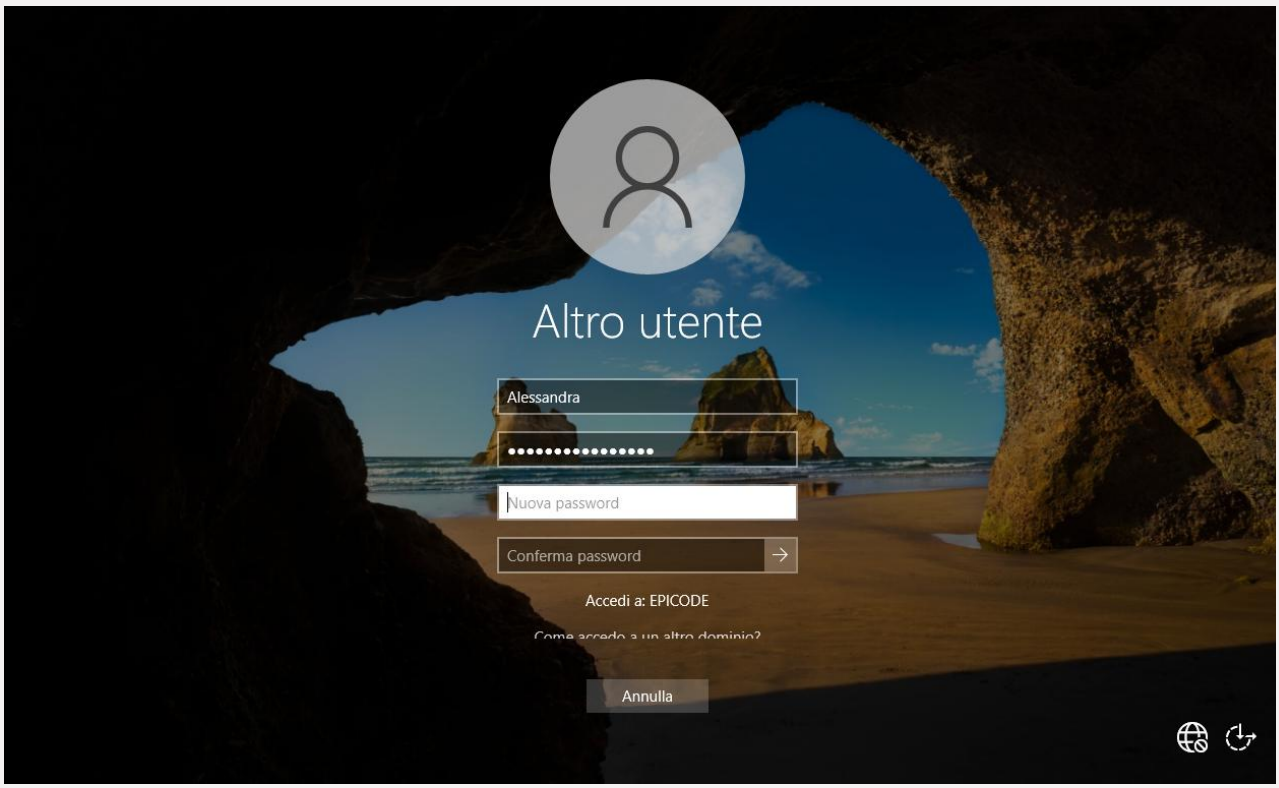


In ultimo, verifichiamo le policy relative al **PC-Carlo** per verificare l'assenza della policy **RemoteDesktopBlock**. Per fare ciò lanciamo in **PowerShell** il comando ***gpresult /r /scope Computer***, non prima di esserci loggati sul pc come amministratori. Nei risultati possiamo notare come la policy non è applicata a questo pc.

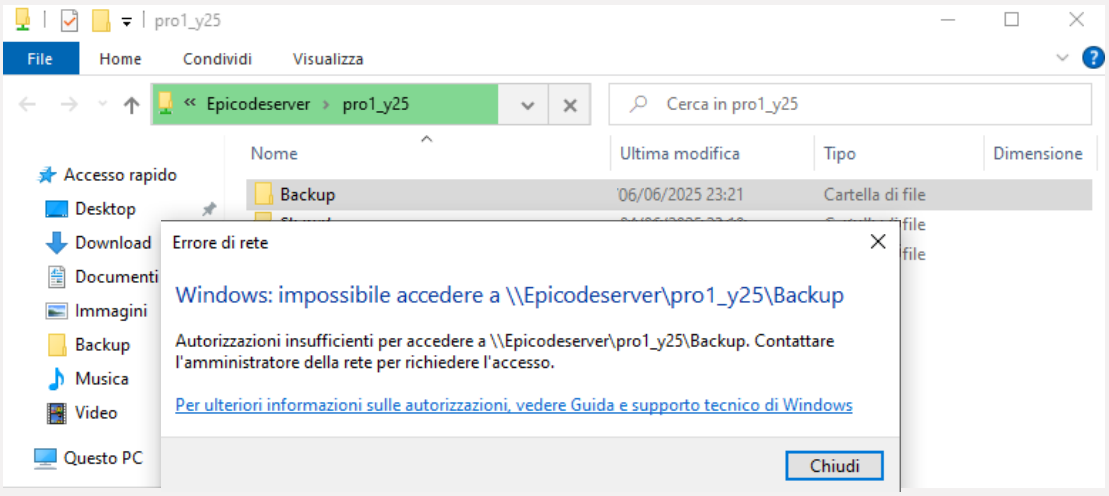
```
IMPOSTAZIONI COMPUTER
---------------------
    CN=PC-Carlo,OU=PC_PMs,DC=Epicode,DC=local
    Ultima applicazione dei
    criteri di gruppo:                  05/06/2025 in 11:40:23
    Criteri di gruppo applicato da:     EpicodeServer.Epicode.local
    Soglia del collegamento lento
    dei criteri di gruppo:              500 kbps
    Nome dominio:                       EPICODE
    Tipo di dominio:                       Windows 2008 o versione successiva

    Oggetti Criteri di gruppo applicati
    -----------------------------------
        Default Domain Policy

    I seguenti oggetti Criteri di gruppo non sono stati
applicati perché sono stati esclusi dal filtro
    --------------------------------------------------------------------------------
        Criteri gruppo locale
            Filtro:  Non applicato (Vuoto)

    Il computer fa parte dei seguenti gruppi di sicurezza
    -----------------------------------------------------
        BUILTIN\Administrators
        Everyone
        BUILTIN\Users
        NT AUTHORITY\NETWORK
        NT AUTHORITY\Authenticated Users
        Questa organizzazione
        PC-CARLO$
        Domain Computers
        PC_ProMan
        Identità con asserzione dell'autorità di autenticazione
        Livello obbligatorio di sistema
```

6.2 Verifica dei permessi e delle policy per il gruppo Designer

Come già avvenuto con l'utente Carlo, anche con l'utente Alessandra, viene richiesto il cambio della password al primo accesso.



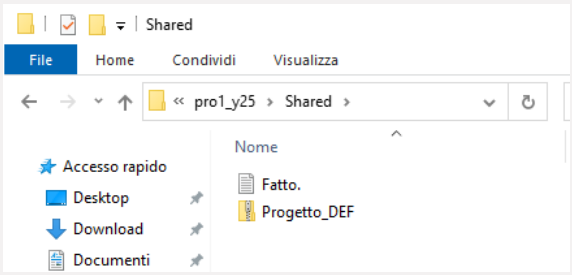
Accedendo alla cartella condivisa sul desktop, posso verificare la presenza di tutte le sotto cartelle create, ma in questo caso, così come impostato nell'**Active Directory** non ho accesso alla cartella **Backup**.



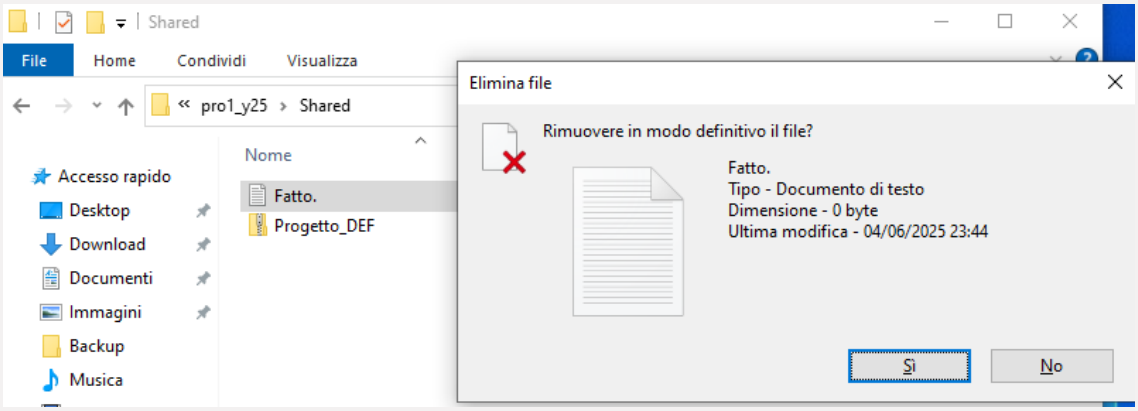
Inoltre, provando ad accedere come Administrator su PC-Ale, posso verificare la presenza della policy **RemoteDesktopBlock**.

```
IMPOSTAZIONI COMPUTER
---------------------
    CN=PC-Ale,OU=PC_Designer,DC=Epicode,DC=local
    Ultima applicazione dei
    criteri di gruppo:                  05/06/2025 in 10:46:08
    Criteri di gruppo applicato da:     EpicodeServer.Epicode.local
    Soglia del collegamento lento
    dei criteri di gruppo:              500 kbps
    Nome dominio:                       EPICODE
    Tipo di dominio:                       Windows 2008 o versione successiva

    Oggetti Criteri di gruppo applicati
    -----------------------------------
        RemoteDesktopBlock
        Default Domain Policy

    I seguenti oggetti Criteri di gruppo non sono stati
applicati perché sono stati esclusi dal filtro
    --------------------------------------------------------------------------------
        Criteri gruppo locale
            Filtro:  Non applicato (Vuoto)

    Il computer fa parte dei seguenti gruppi di sicurezza
    -----------------------------------------------------
        BUILTIN\Administrators
        Everyone
        BUILTIN\Users
        NT AUTHORITY\NETWORK
        NT AUTHORITY\Authenticated Users
        Questa organizzazione
        PC-ALE$
        PC_Des
        Domain Computers
        Identità con asserzione dell'autorità di autenticazione
        Livello obbligatorio di sistema
```

In, per verificare le impostazioni di Security per il gruppo ProjectManager sulla cartella Shared, andiamo a creare un file con estensione ***.txt*** con un nome casuale.



Ritornando sull'utente Carlo, ho la possibilità di eliminare il file perché nei permessi **Security** della cartella Shared ho impostato i permessi di ***Modify***, anche se il file non è creato da un altro utente e quindi è di sua proprietà.



7. Resume: Gestione Gruppi e Permessi in Windows Server 2022

7.1 Gruppi creati

1. **ProjectManager**
   Membri: Carlo, Michela
   Funzione: Gestione, pianificazione e approvazione progetti.
2. **Designer**
   Membri: Alessandra, Gianfranco
   Funzione: Sviluppo e modifica operativa dei progetti.

7.2 Permessi assegnati

Cartella/File	ProjectManager	Designer
PRO1_Y25 (cartella principale)	Lettura + Modifica	Lettura + Modifica
Backup	Lettura + Modifica	Nessun accesso
WIP	Lettura	Lettura + Modifica
Shared	Lettura + Modifica	Lettura + Modifica
Backup_{DATA}.bak	Lettura + Modifica (senza full)	Nessun accesso
WIP_{DATE1}.rvt e WIP_{DATE2}.rvt	Solo Lettura	Lettura + Modifica
Progetto_DEF.zip	Lettura + Modifica	Solo Lettura

Il gruppo **Everyone è stato rimosso** da tutte le cartelle e file per evitare accessi non autorizzati.

Legenda
"Lettura + Modifica" ≈ **Read + Change**,
"Solo Lettura" ≈ **Read**

7.3 Passaggi seguiti per creare e configurare i gruppi

1. **Creazione delle OU (Organizational Units)**:
   - PM per gli utenti ProjectManager.
   - Designer per gli utenti Designer.
   - PC_PM e PC_Designer per associare i computer ai rispettivi gruppi.

2. **Creazione utenti e gruppi**:
   - Utenti creati con obbligo di cambio password al primo accesso.
   - Gruppi di sicurezza ProjectManager e Designer creati e popolati con gli utenti corrispondenti.

3. **Creazione struttura cartelle e file**:
   - In C:\PRO1_Y25, create le sottocartelle Backup, WIP, Shared con i rispettivi file.

4. **Assegnazione permessi NTFS e condivisione**:
   - Permessi specifici assegnati ai gruppi via tab "Sicurezza" e "Condivisione avanzata".

5. **Distribuzione policy tramite GPO**:
   - Shortcut della cartella condivisa sul desktop.
   - Blocco dell'accesso remoto per i computer del gruppo Designer.

6. **Verifica**:
   - Test di accesso e modifica con utenti dei due gruppi.
   - Verifica applicazione delle GPO tramite gpresult.

8. Conclusioni

Durante questo progetto ho appreso come creare, organizzare e gestire gruppi utenti in un'infrastruttura basata su Windows Server 2022. Ho compreso l'importanza di assegnare permessi in base al principio del **least privilege** e di bloccare accessi generici come quello del gruppo **Everyone**. Ho imparato inoltre a distribuire policy tramite **GPO** e a verificare la loro applicazione tramite strumenti come **gpresult**. Questo progetto ha migliorato la mia consapevolezza della sicurezza e della gestione centralizzata degli utenti e delle risorse in ambienti di dominio.