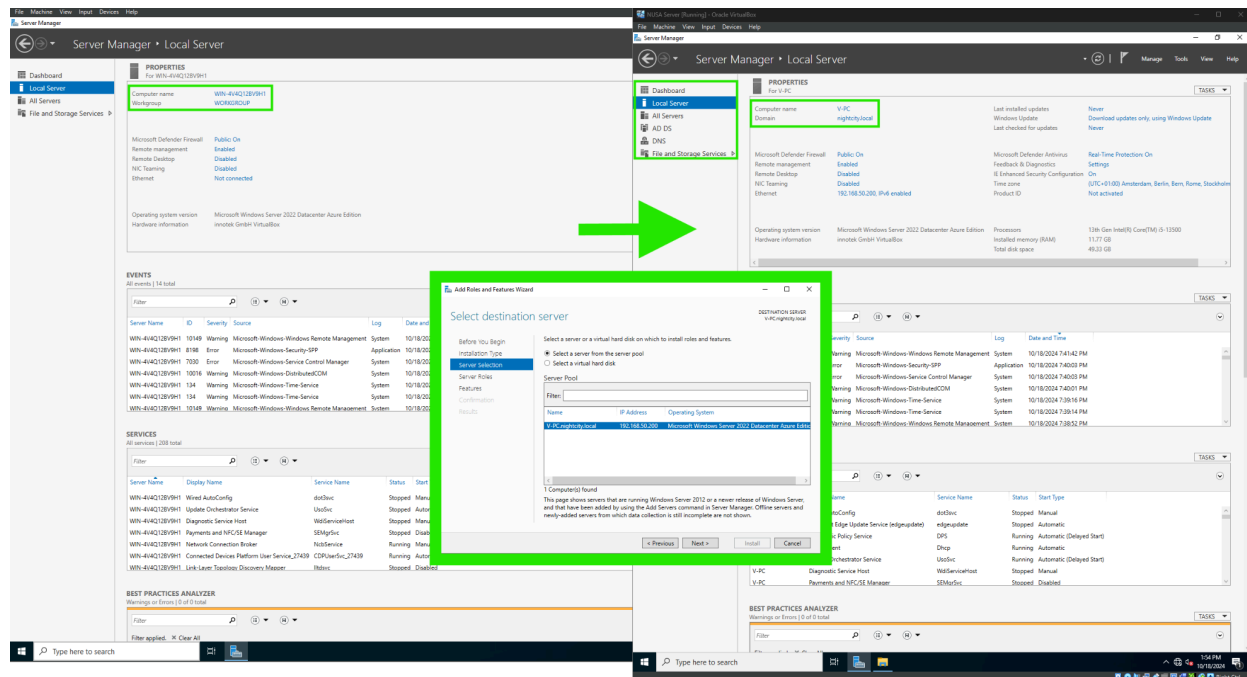


# Report - Creazione e Gestione dei Gruppi in Windows Server 2022 (Versione Cyberpunk 2077)

Oggi andro' a fare dei test per la comprensione del management dei permessi dei vari utenti. Il primo step per lo svolgimento dell'esercizio é stato installare i servizi sul Server Windows, seguendo la procedura ho infine creato il nuovo dominio di una foresta chiamati **nightcity.local**.



Ho proceduto con il login per verificare l'esistenza del nuovo dominio.



Ho creato 2 gruppi separati: **Amministratori** che comprendono gli user **v** e **Johnny Silverhand** e il Gruppo che comprende entrambi gli user **kiroschi** ed il gruppo **UtentiStandard** che comprende gli altri utenti e i gruppi **mox** e **valentinos**.

#### Gruppi Creati:

##### 1. Amministratori

- **Johnny Silverhand** (Capo amministratore)
- **v (Vincent/Valerie)** (Amministratore del sistema e delle risorse)

**GRUPPO Kiroshi** (Gruppo di amministratori con pieni diritti sui sistemi di sicurezza informatica e capacità di monitorare le reti. I membri possono configurare e gestire gli accessi ai dati sensibili.)


## **2. UtentiStandard**

- **Judy Alvarez** (Utente con diritti limitati, ma con accesso a risorse particolari legate al Netwatch)
- **Jackie Welles** (Utente standard con accesso base e possibilità di eseguire programmi legati alla sicurezza)
- **Dante Caruso** (Utente con diritti limitati, ma con accesso a risorse legate alla gestione dei dati aziendali)
- **Evelyn Parker** (Utente standard con accesso a strumenti di marketing e analisi dei dati)
- **Gustavo Orta** (Utente con diritti limitati, abilitato a gestire le comunicazioni interne)
- **Mama Welles** (Utente standard con accesso a informazioni storiche e di contesto sulla città di Night City)
- **Panam Palmer** (Utente con diritti limitati, accesso a risorse legate alla sicurezza del territorio e alle operazioni di guerriglia)

**GRUPPO Mox - Judy Alvarez, Evelyn Parker** (Gruppo di utenti standard con accesso a strumenti di comunicazione e gestione delle relazioni. Hanno la possibilità di interagire con i dati di marketing e vendite, ma con diritti limitati sulla modifica dei sistemi.)

**GRUPPO Valentinos - Jackie Welles, Gustavo Orta** (Gruppo di utenti standard con accesso a informazioni relative alla sicurezza del quartiere. Possono consultare dati e report sulla criminalità, ma non possono apportare modifiche alle configurazioni di sistema.)

New Object - User ✕

 Create in: nightcity.local/Amministratori

---

First name:  Initials:

Last name:


Full name:

User logon name:

User logon name (pre-Windows 2000):

---

New Object - User ✕

 Create in: nightcity.local/UtentiStandard

---

First name:  Initials:

Last name:


Full name:

User logon name:

User logon name (pre-Windows 2000):

---

New Object - User ✕

 Create in: nightcity.local/UtentiStandard

---

Password:

Confirm password:

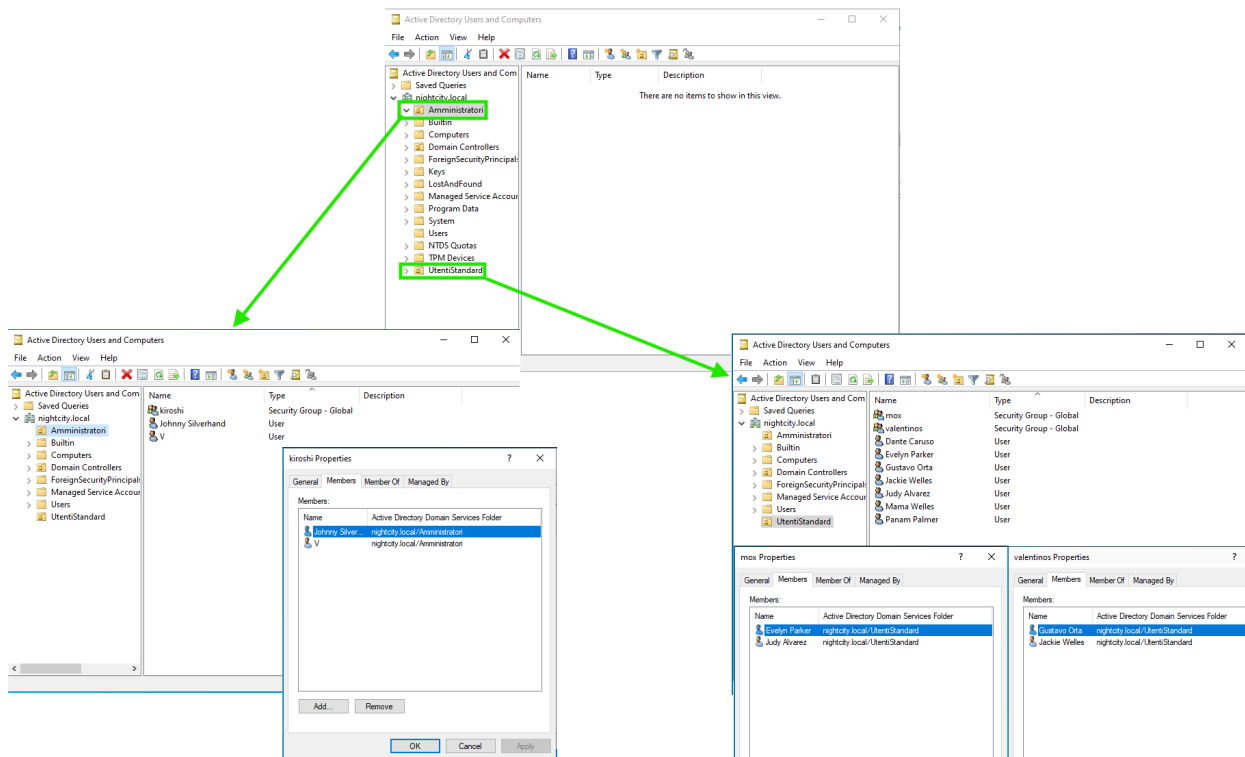
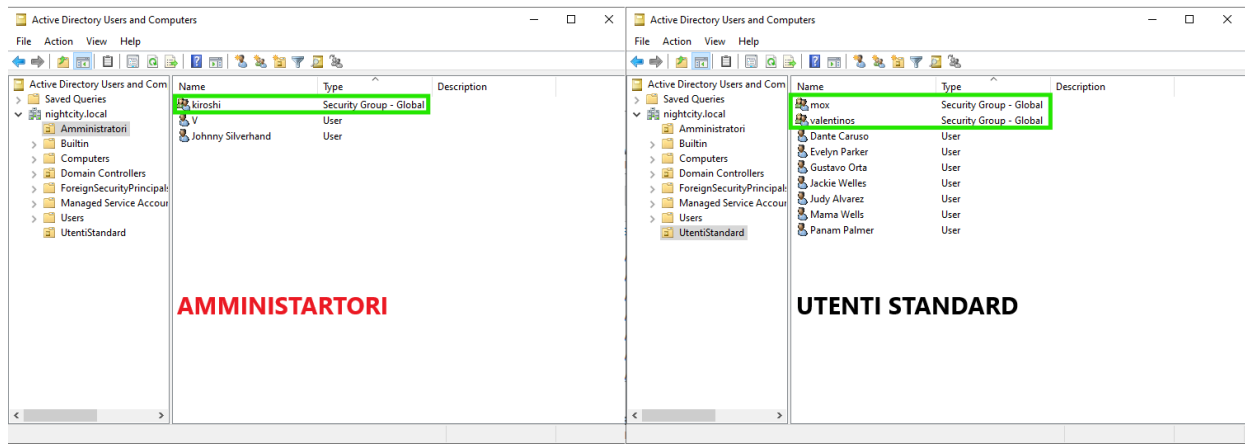
☒ User must change password at next logon

☐ User cannot change password

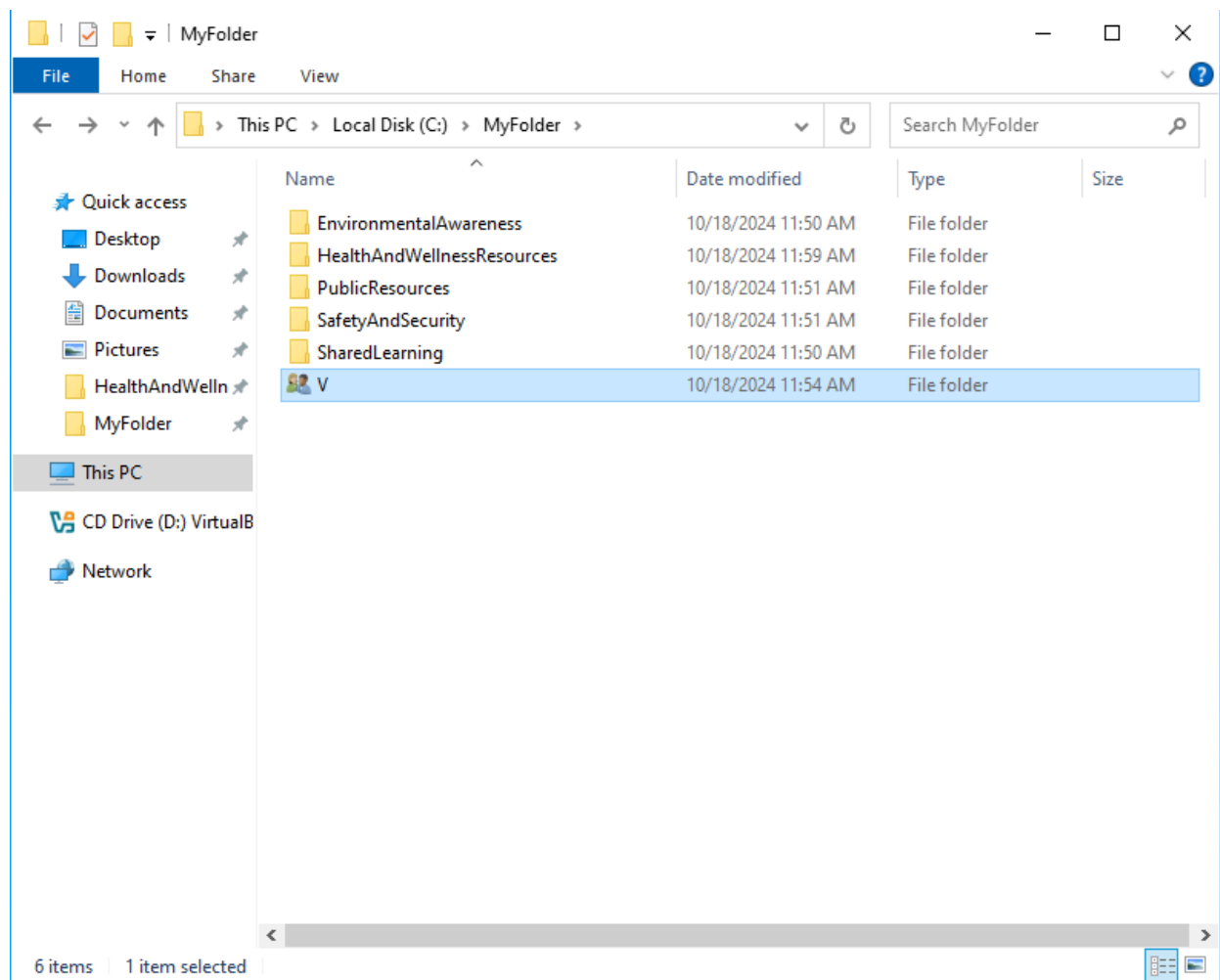
☐ Password never expires

☐ Account is disabled

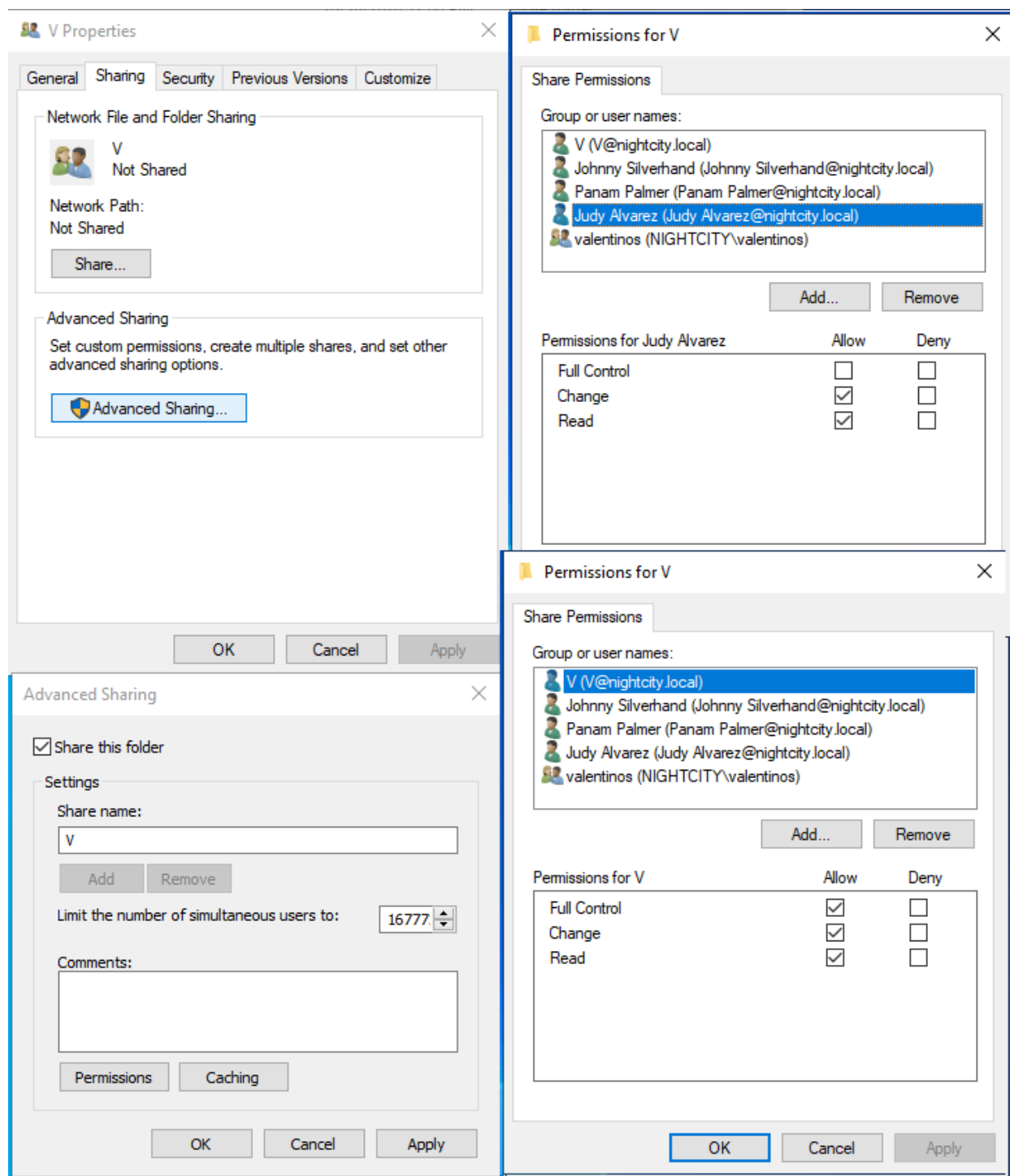
---



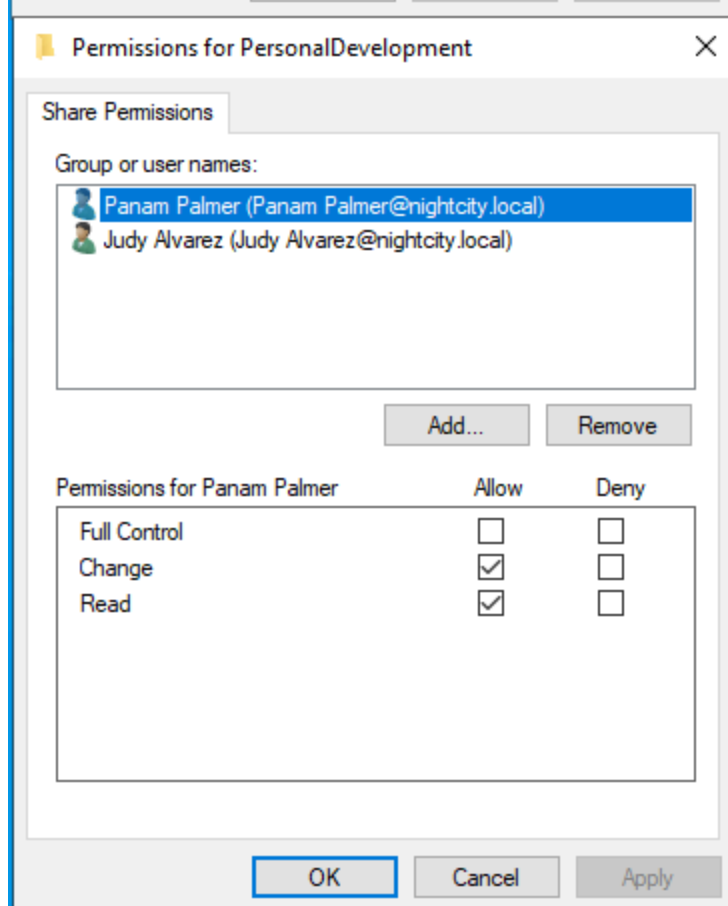
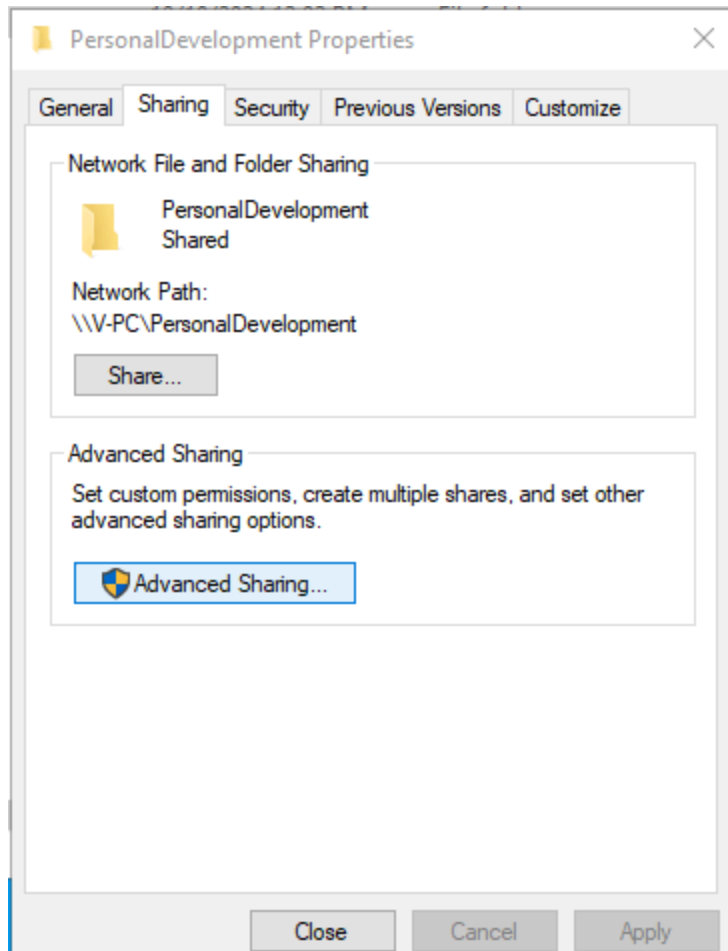
Creata una cartella chiamata **MyFolder** comprensiva di sotto cartelle **v** (intesa come contenuto sensibile) e altre **cartelle** (intese come pubbliche).



Cambiato i permessi di accesso per la cartella **v** che sarà accessibile in permessi change da **Judy Alvarez** e in **full control** dagli **Amministratori**.

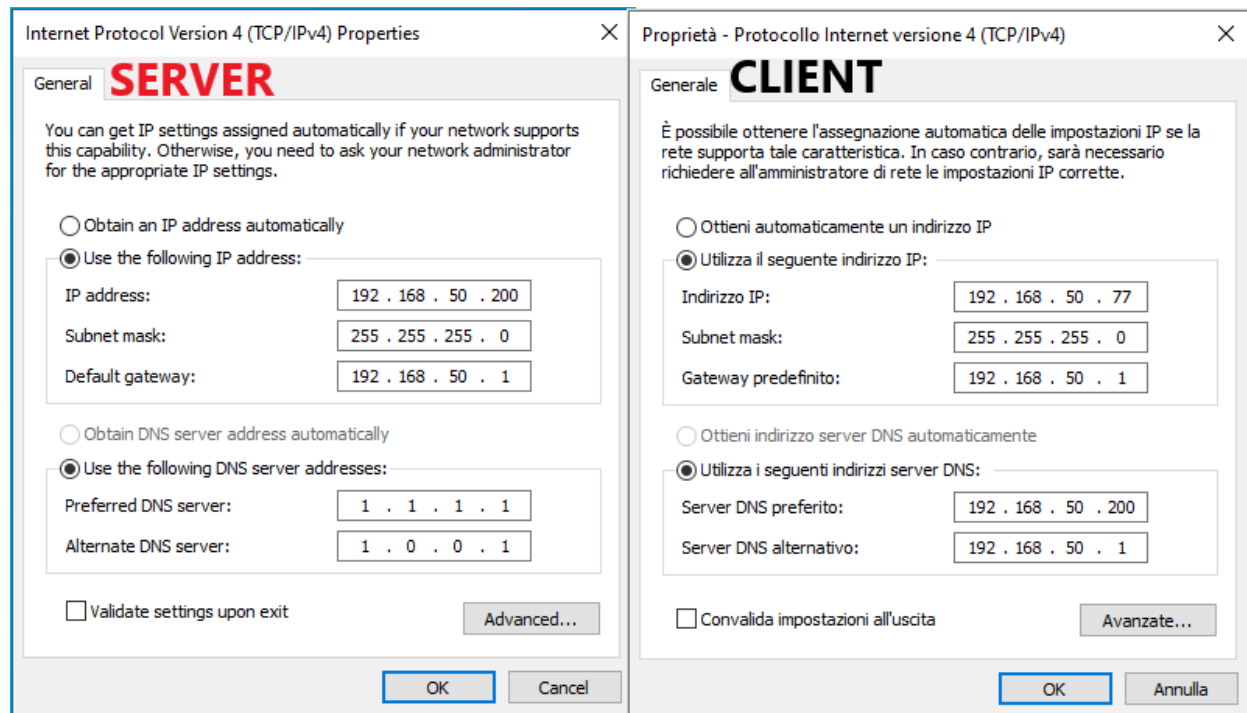


Aggiunti solo 2 utenti alla possibilità di change alla cartella  
**MyFolder/V/PersonalDevelopment**.



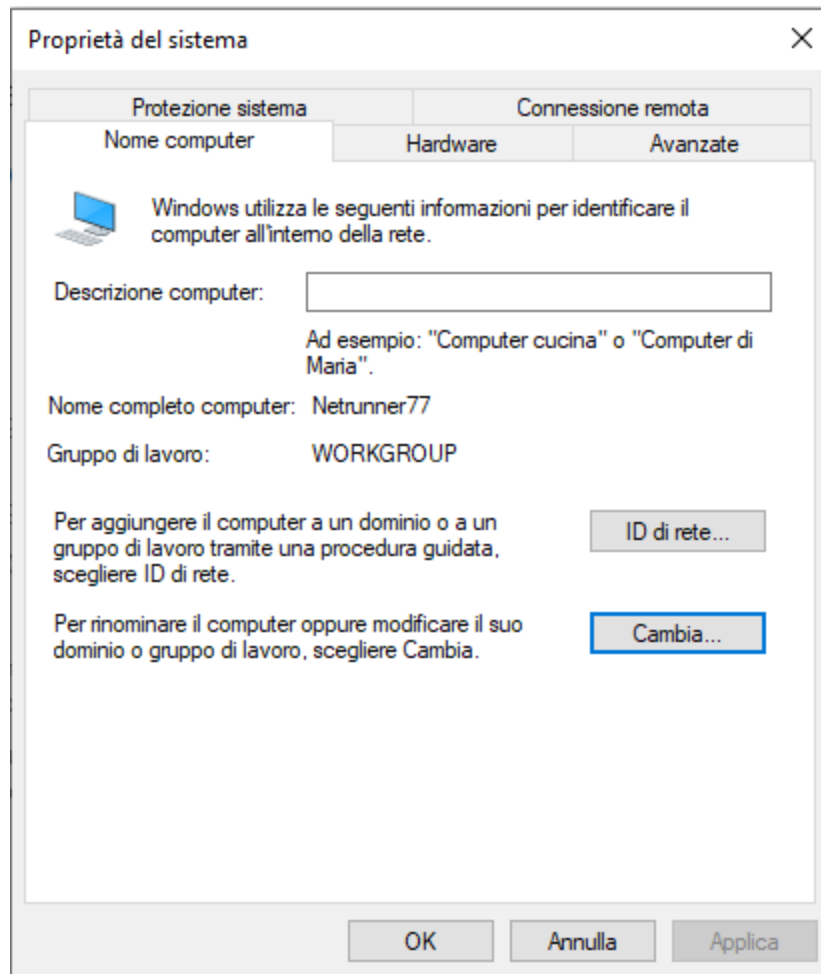


Successivamente ho provveduto a rendere le macchine **server** e **client** comunicanti cambiando i rispettivi ip e rendendoli statici con il client che usera' ip server come DNS.

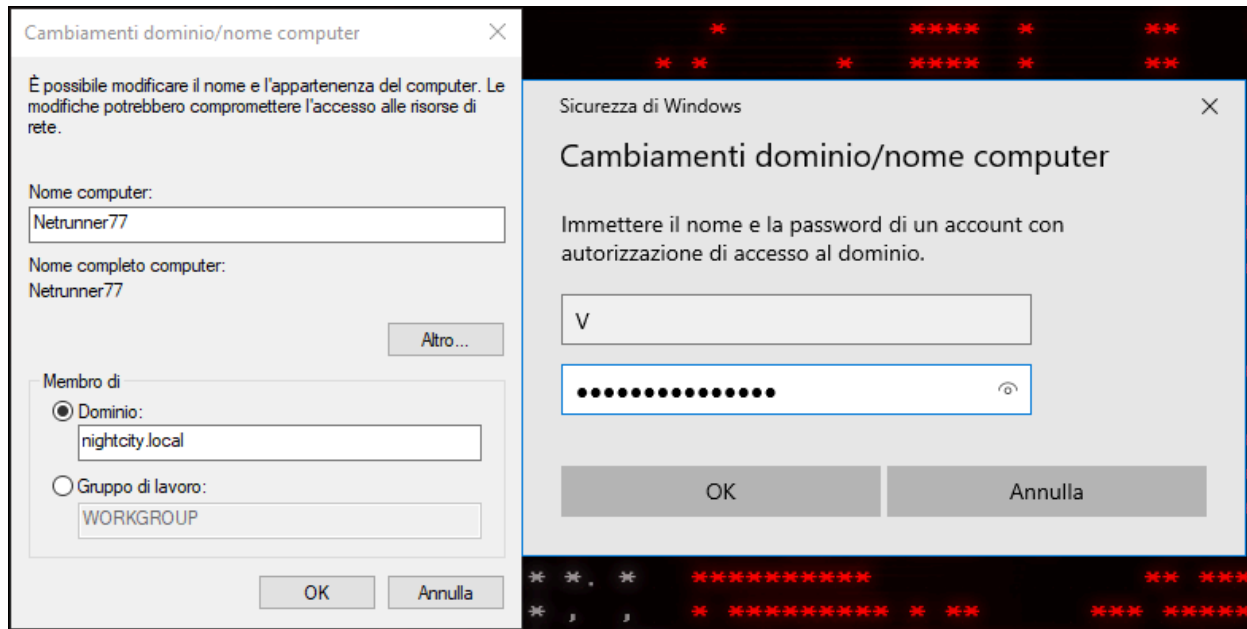


**Prossimo step:** collegarsi del pc **client** al dominio del nostro **server**.

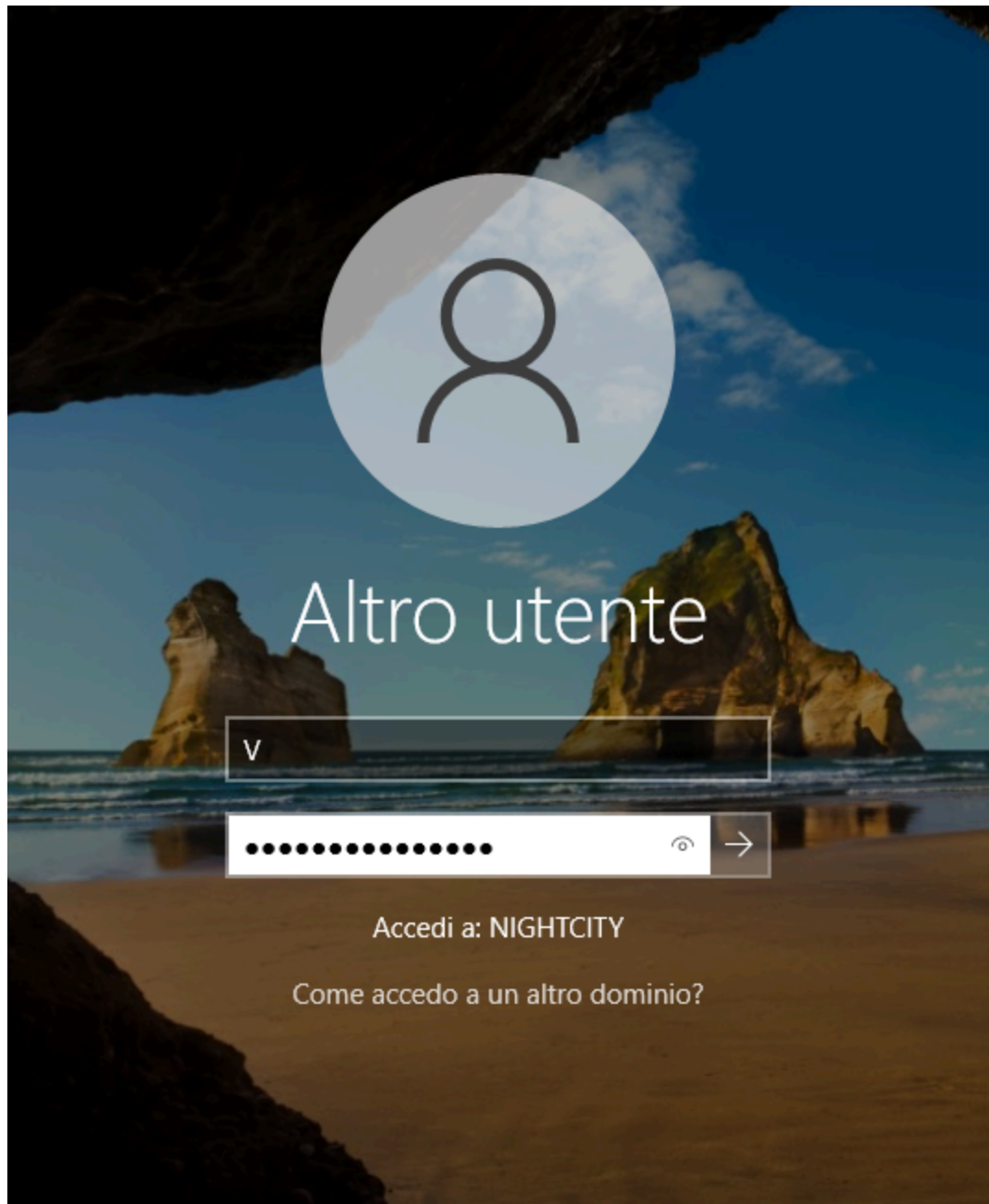
Dalle proprietà di sistema ho cambiato il nome del pc in **Netrunner77**



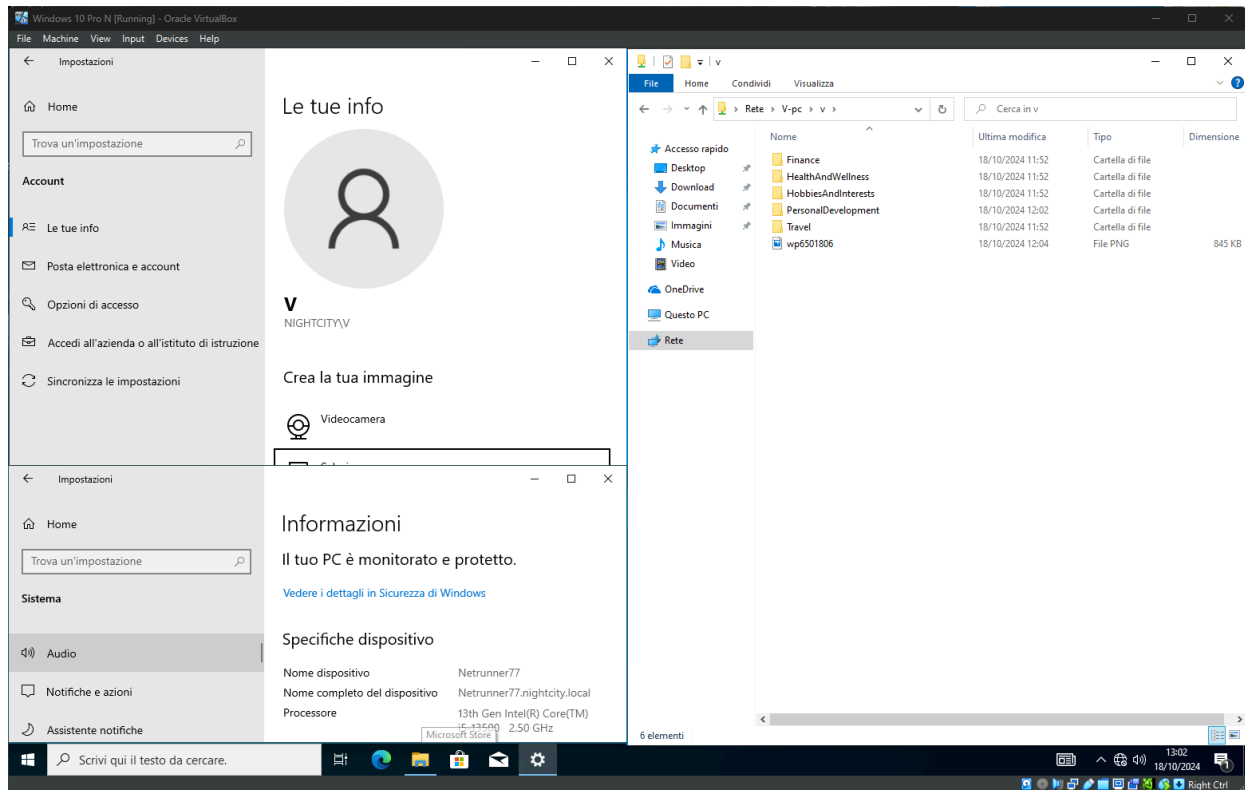
Impostato il dominio in `nightcity.local`



e fatto l'accesso con account **amministratore V**.



Ed ecco che siamo dentro il nostro dominio da pc `client` con user `v`. Con tutti i permessi per tutte le cartelle.



Ho provato successivamente a fare login con un utente di **Utenti Standard** chiamato Judy Alvarez che mi ha chiesto come da impostazioni precedentemente settate il cambio password al primo accesso, cambiata la password sono entrato.



## Altro utente

Judy Alvarez

••••••••••••••••

Nuova password

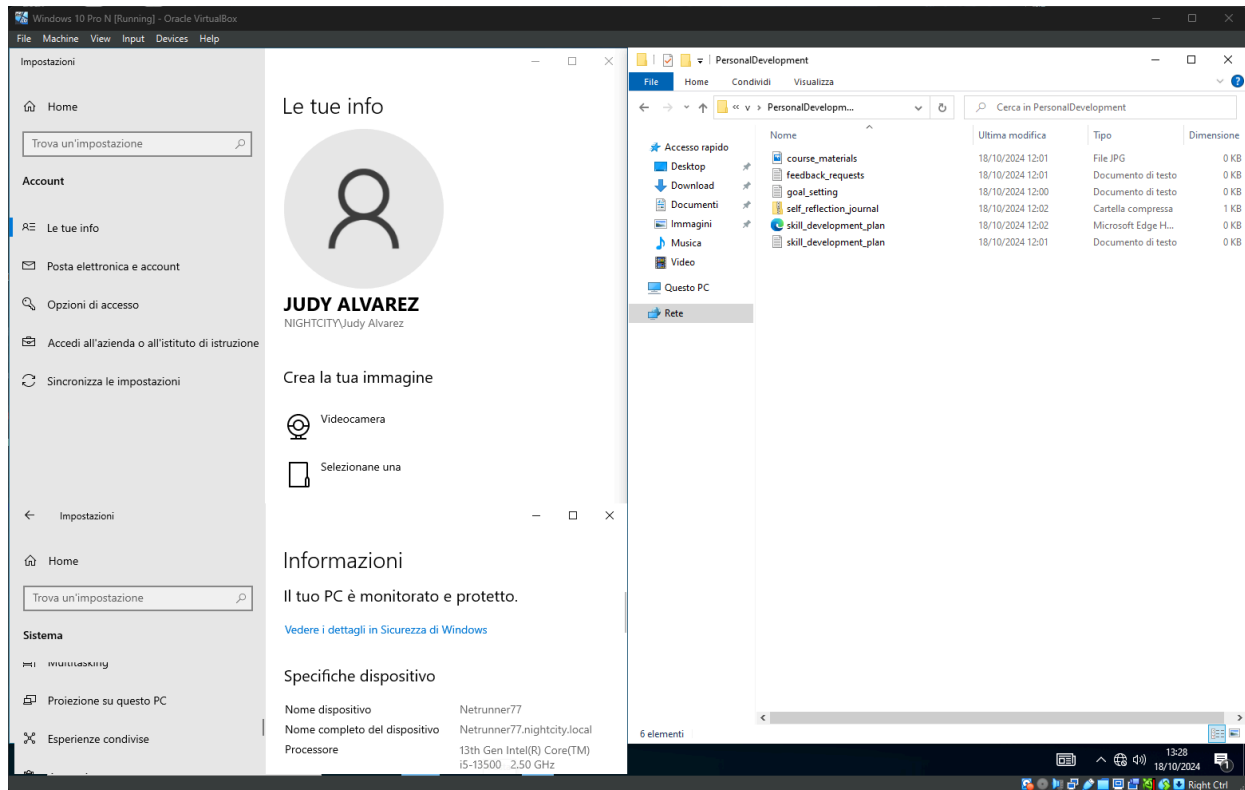
Conferma password



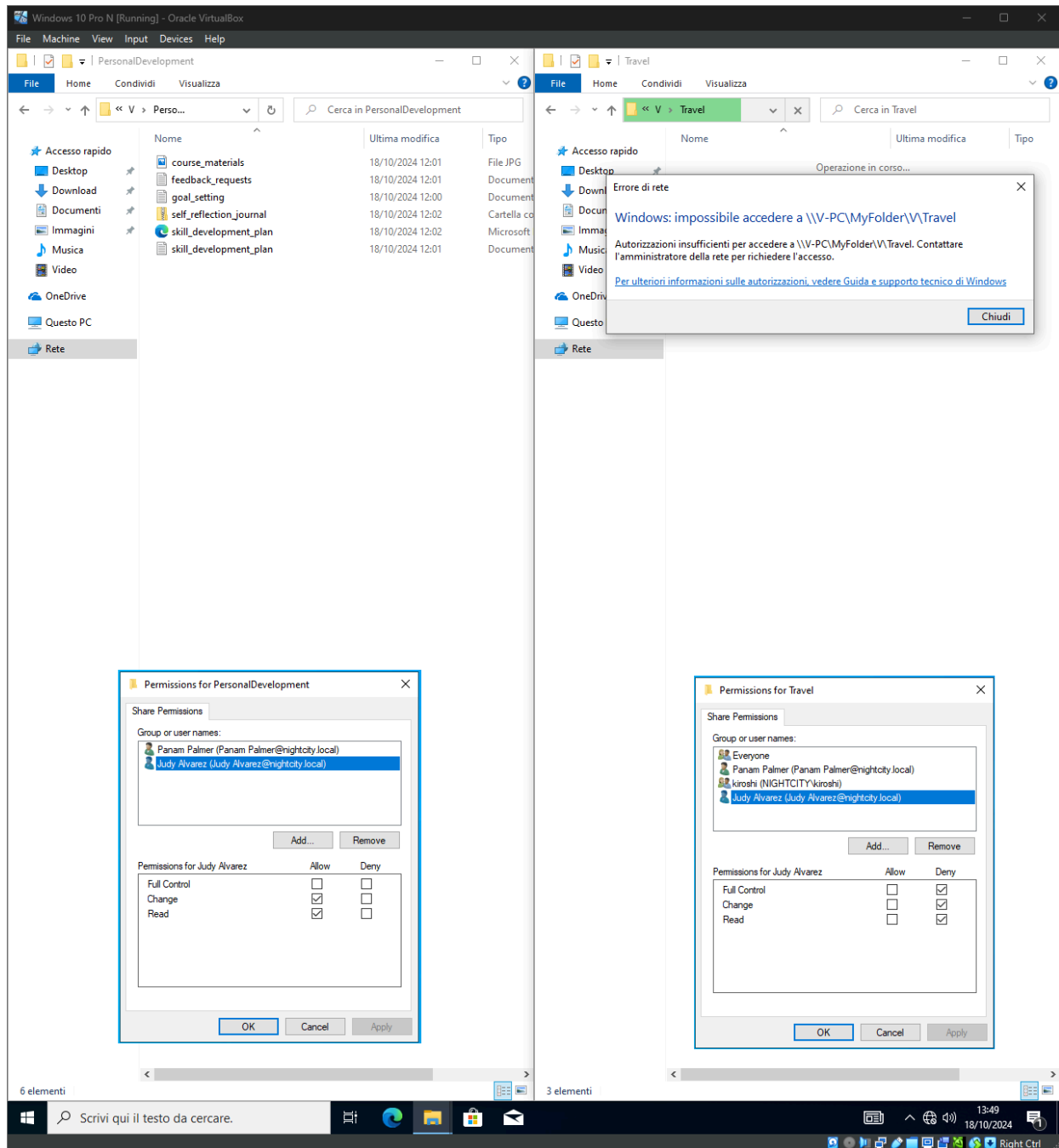
Accedi a: NIGHTCITY

Come accedo a un altro dominio?

Annulla

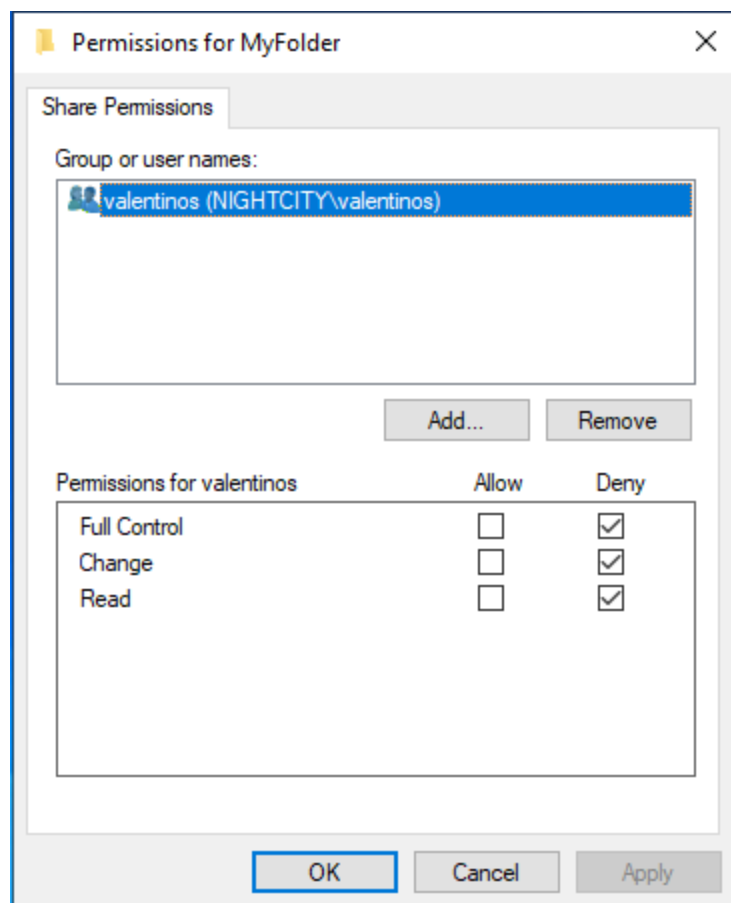


L'utente in questione possiede i permessi per entrare nella cartella **PersonalDevelopment** ed alcune sue sotto cartelle tra le quali **PersonalDevelopment**, ma non alla cartella denominata **Travel**.



Proviamo invece con gli utenti che non hanno nessun permesso ad accedere alla cartella **MyFolder**. Consideriamo **Gustavo Orta** appartenente al gruppo dei **valentinos**.







## Altro utente

Gustavo Orta

.....

.....

.....

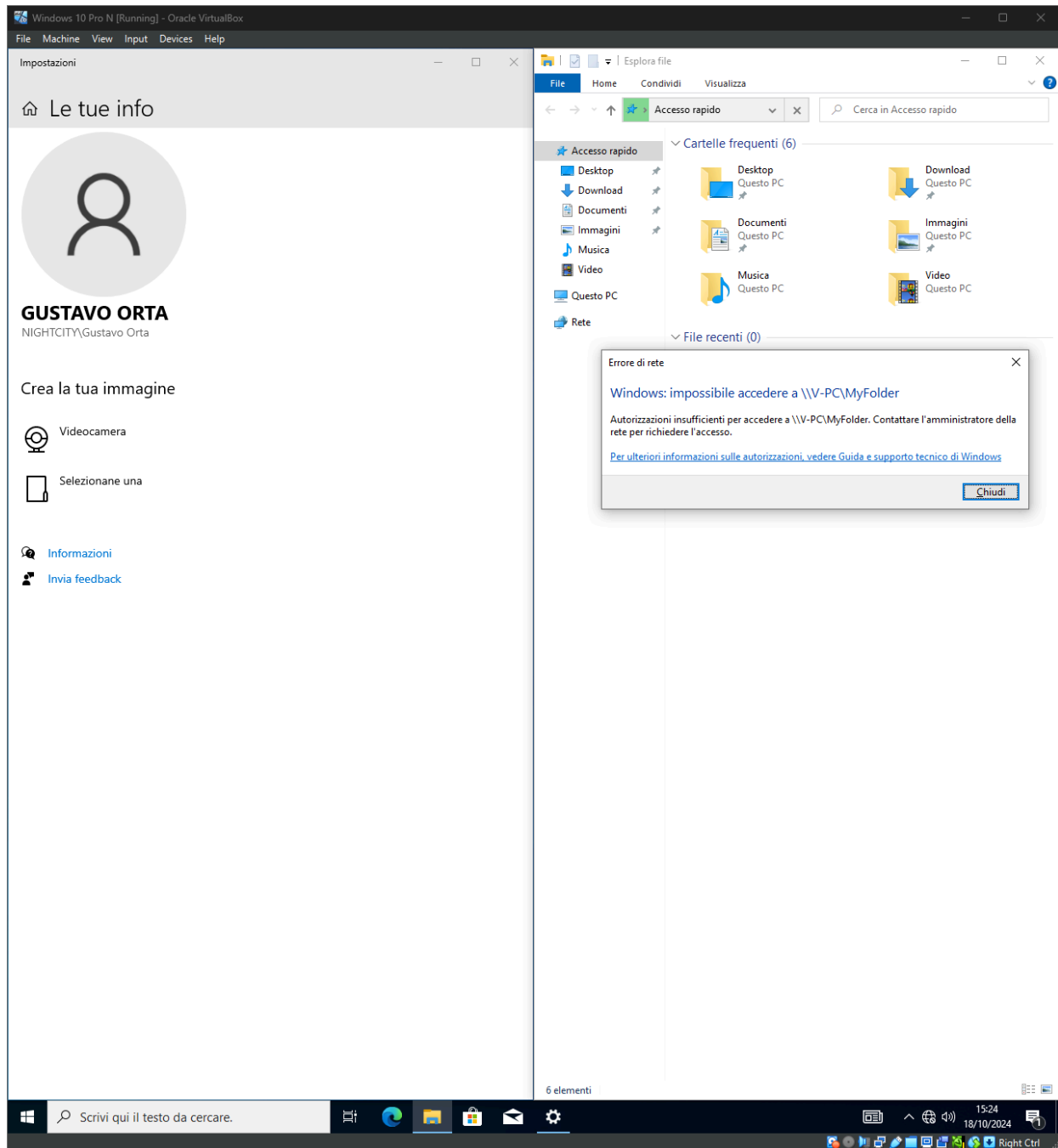


Accedi a: NIGHTCITY

Come accedo a un altro dominio?

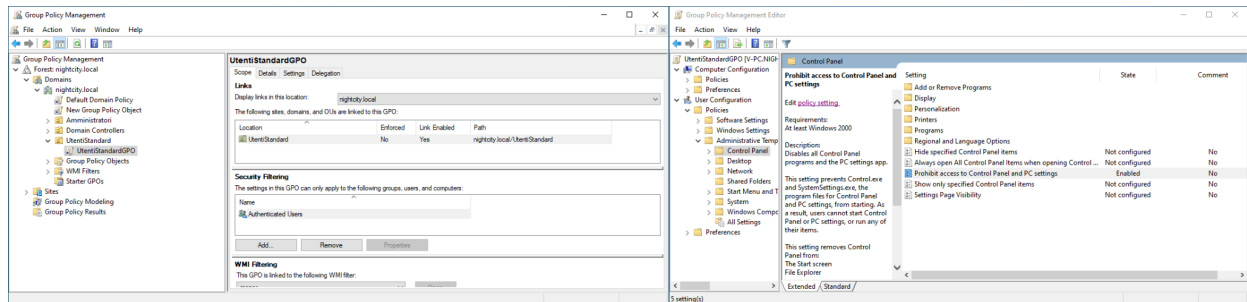
Annulla

Come previsto l'utente con permessi negati sarà in grado comunque di accedere al dominio ma non di accedere alla cartella.

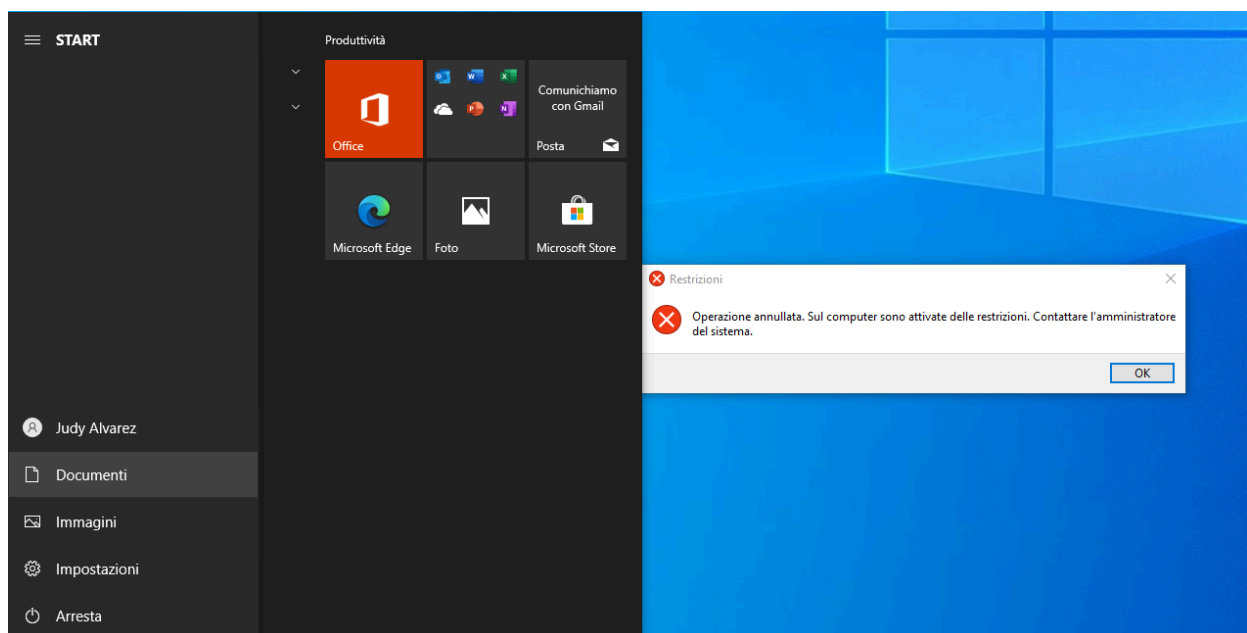


Come ulteriore prova proviamo a negare l'accesso ad un servizio per gli **utentiStandard**.

Crea regola **GPO** per negare l'avvio del pannello di controllo.

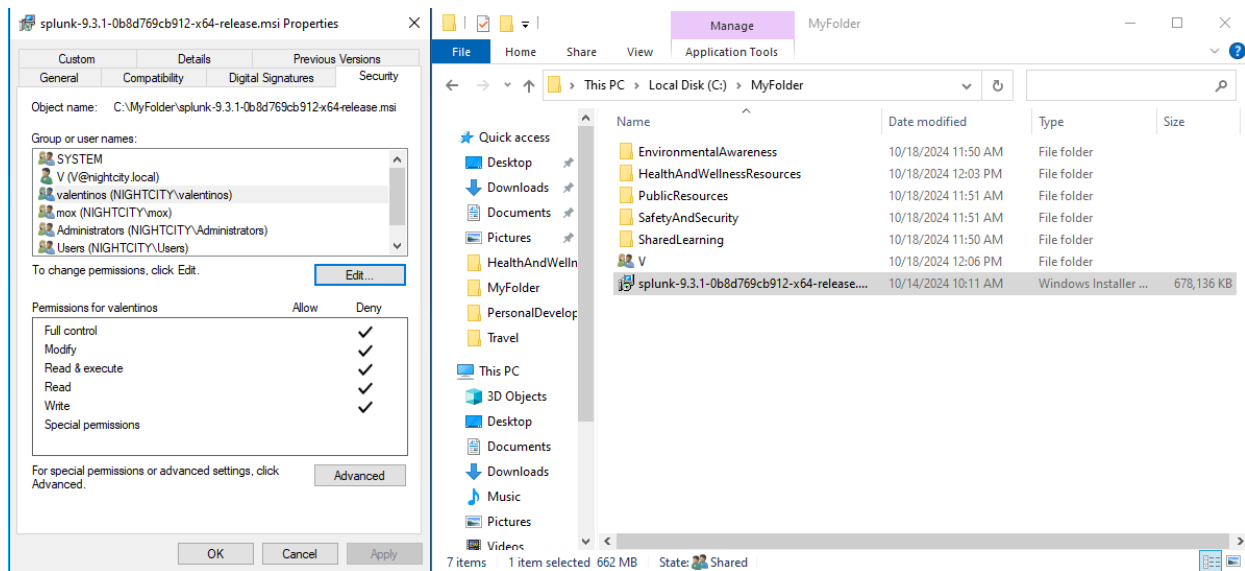


**Judy Alvarez** non potrà accedere al pannello di controllo essendo compresa nella regola **GPO**.

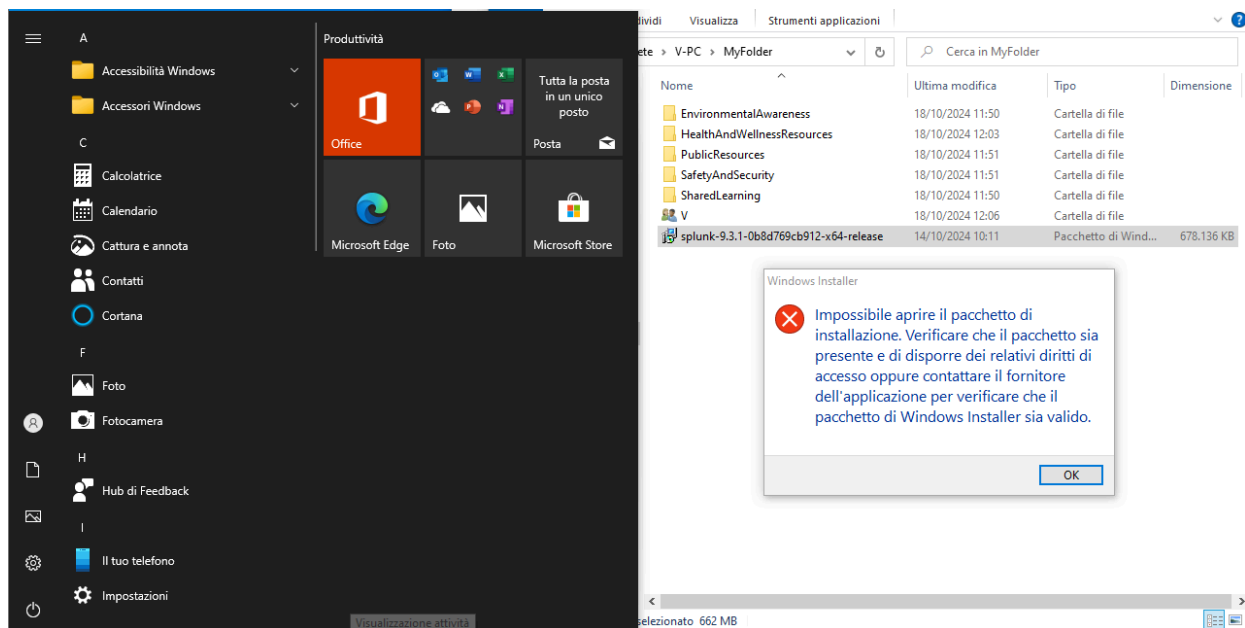


Infine proviamo a negare l'avvio di un eseguibile da parte di **Jackie Welles** del gruppo **valentinos**.

Nego la possibilità da parte di **valentinos** di avviare l'eseguibile dal pannello proprietà dello stesso.



Concludiamo con la prova dei permessi appena negati.



## Conclusione:

L'esercizio ha dimostrato come la gestione accurata dei permessi in un ambiente di dominio sia cruciale per garantire sicurezza e accesso alle risorse aziendali. L'utilizzo di gruppi come **Amministratori**, **UtentiStandard**, e gruppi personalizzati come **mox** e **valentinos** consente un'assegnazione granulare dei permessi, garantendo che ogni utente abbia solo l'accesso necessario per svolgere il proprio lavoro, minimizzando così il rischio di accessi non autorizzati o manipolazioni accidentali di file critici.

In un'ulteriore prova, ho configurato una regola GPO per negare l'accesso al pannello di controllo agli utenti standard, tra cui **Judy Alvarez**, dimostrando la possibilità di limitare funzionalità specifiche del sistema. Come atteso, **Judy** non ha potuto accedere al pannello di controllo, confermando il funzionamento corretto della regola.

Successivamente, ho negato a **Jackie Welles**, appartenente al gruppo **valentinos**, la possibilità di avviare un eseguibile tramite la configurazione delle proprietà dell'eseguibile stesso. **Jackie**, e gli altri membri del gruppo **valentinos**, non sono stati in grado di eseguire l'applicazione in questione, mostrando l'efficacia delle restrizioni basate sui gruppi.

L'unico errore rilevato, riguardante il permesso **Everyone** applicato alla cartella root **MyFolder**, è servito da promemoria sull'importanza di verificare costantemente i permessi assegnati per evitare che configurazioni errate possano compromettere la sicurezza del sistema.

Nel complesso, questo esercizio ha fornito una comprensione più approfondita del management dei permessi e della configurazione del dominio, permettendo una corretta segmentazione dei ruoli all'interno di un'infrastruttura IT complessa come quella simulata in **nightCity.local**. La capacità di configurare i server e di gestire gli accessi garantisce il controllo sulle risorse, aumentando al contempo l'efficienza operativa.

