

Report Esercizio 14/02/2025

Creazione e Gestione Gruppi Windows Server 2022

Leonardo Catalano

“La traccia di oggi ci chiede di effettuare una gestione di gruppi di utenti in Windows Server 2022, ad ogni gruppo andranno applicati permessi specifici “Permessi di Lettura, Scrittura ed Esecuzione” e si dovrà creare una gestione dei gruppi per garantire la sicurezza e l’amministrazione del sistema.”

Le fasi da effettuare saranno le seguenti:

1. Preparazione Macchina Windows Server 2022.

Accesso alla macchina Windows Server 2022 con utente amministrativo.

2. Creazione dei Gruppi:

Creare due gruppi distinti con nomi significativi rispetto alla loro funzione (“Amministratori”, “UtentiStandard”).

3. Creazione degli utenti dei Gruppi:

Creare uno o più utenti per i gruppi.

4. Assegnazione dei Permessi:

Per ogni gruppo, assegnare permessi specifici e spiegare il motivo della scelta considerata, basandoci sui seguenti aspetti:

- Accesso ai File e alle Cartelle.
- Esecuzione di programmi specifici.
- Modifiche alle impostazioni di sistema.
- Accesso remoto al server.

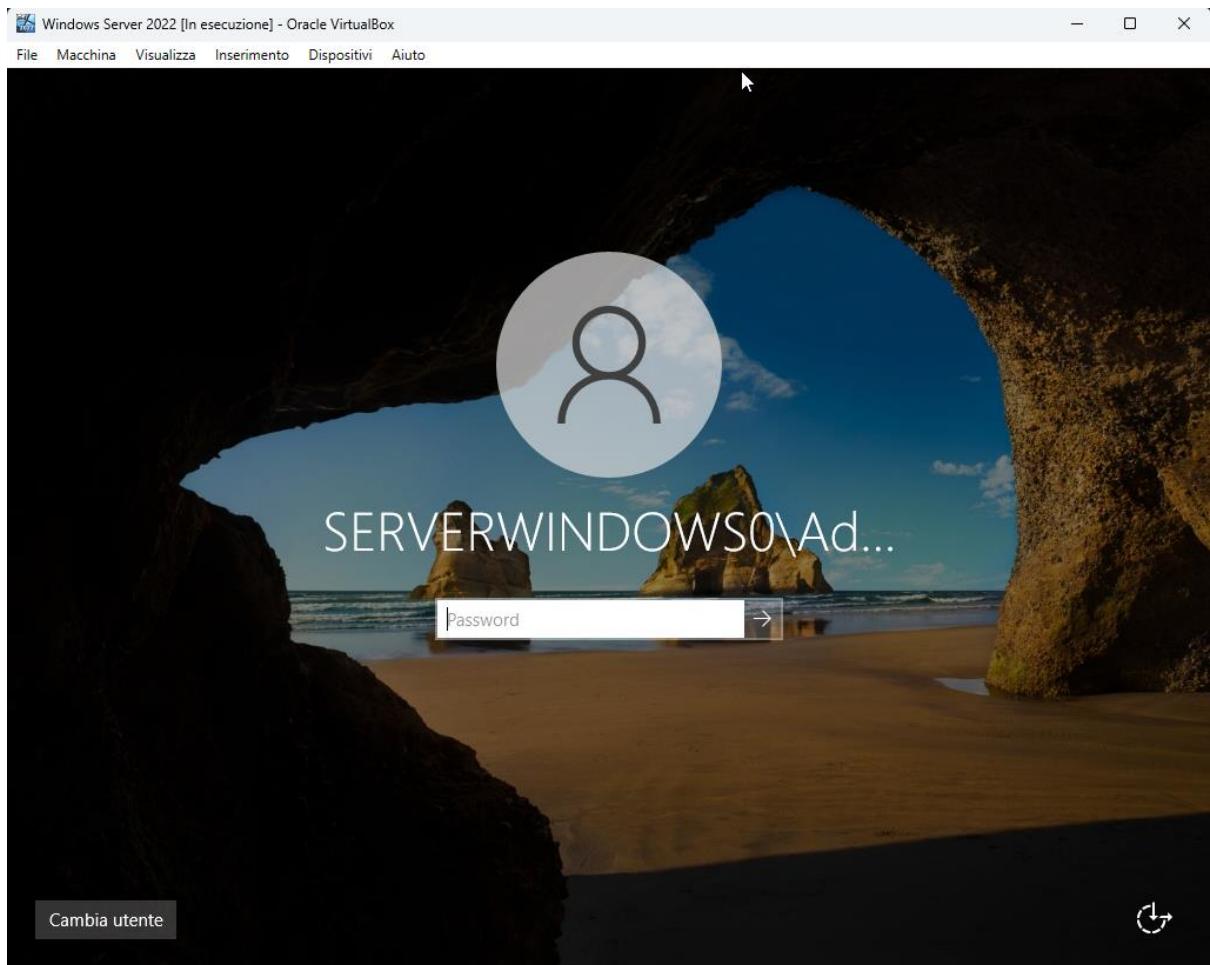
5. Test sui permessi effettuati:

Una volta creati i gruppi e gli utenti ad essi e assegnati i permessi specifici, effettuare dei test per verificare che le impostazioni configurate siano corrette.

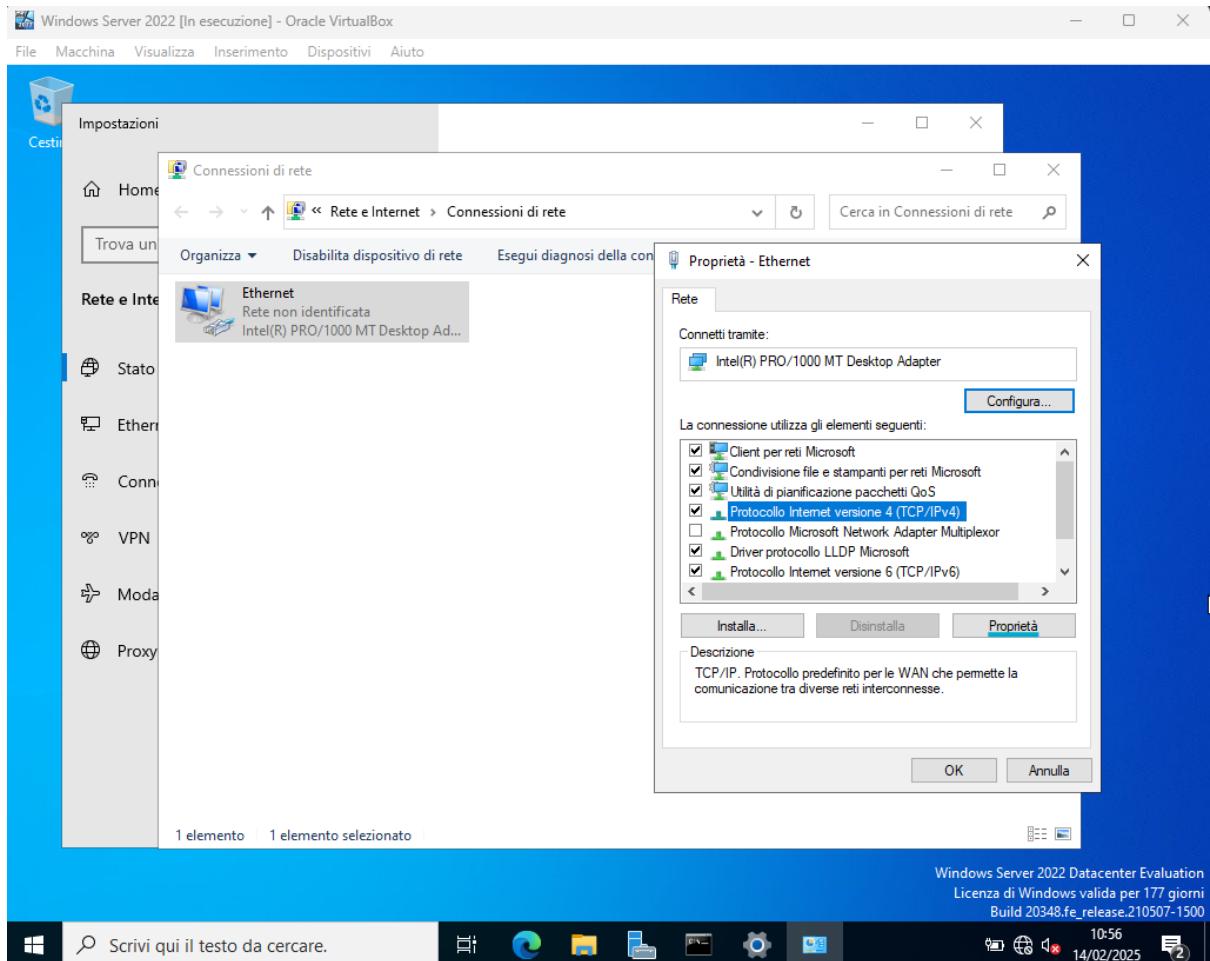
Per far ciò andrò a verificare se gli utenti possano accedere o meno alle risorse assegnate al loro specifico gruppo e alle risorse assegnate agli altri gruppi.

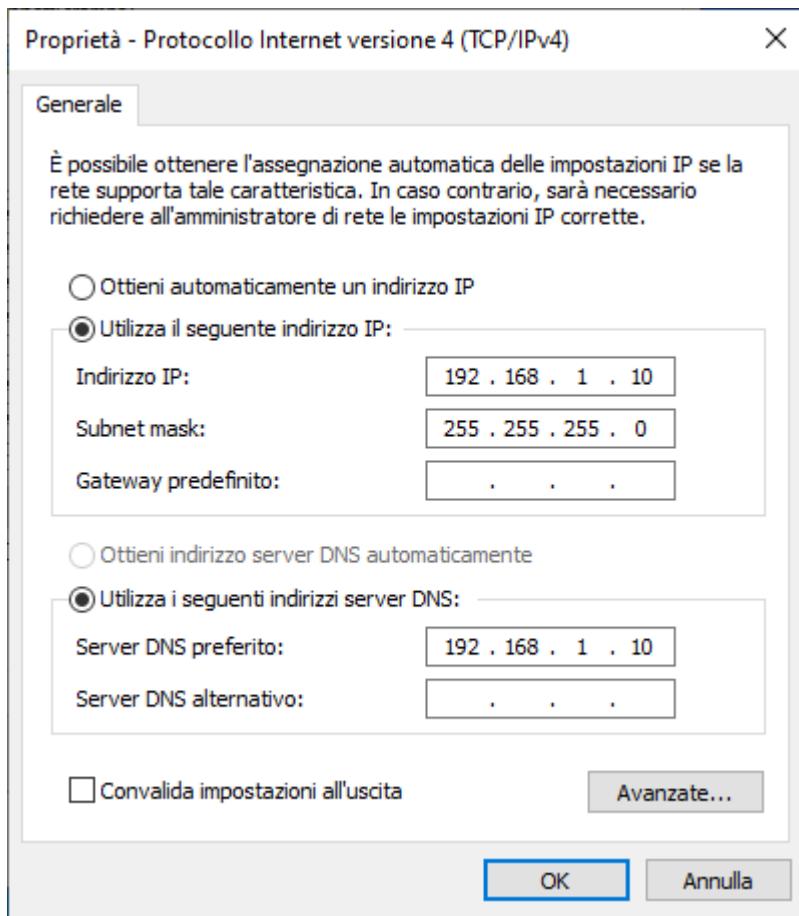
-Macchina Windows Server 2022:

Per poter effettuare l’esercizio come prima fase si va ad accedere e verificare la configurazione della macchina Windows Server 2022.

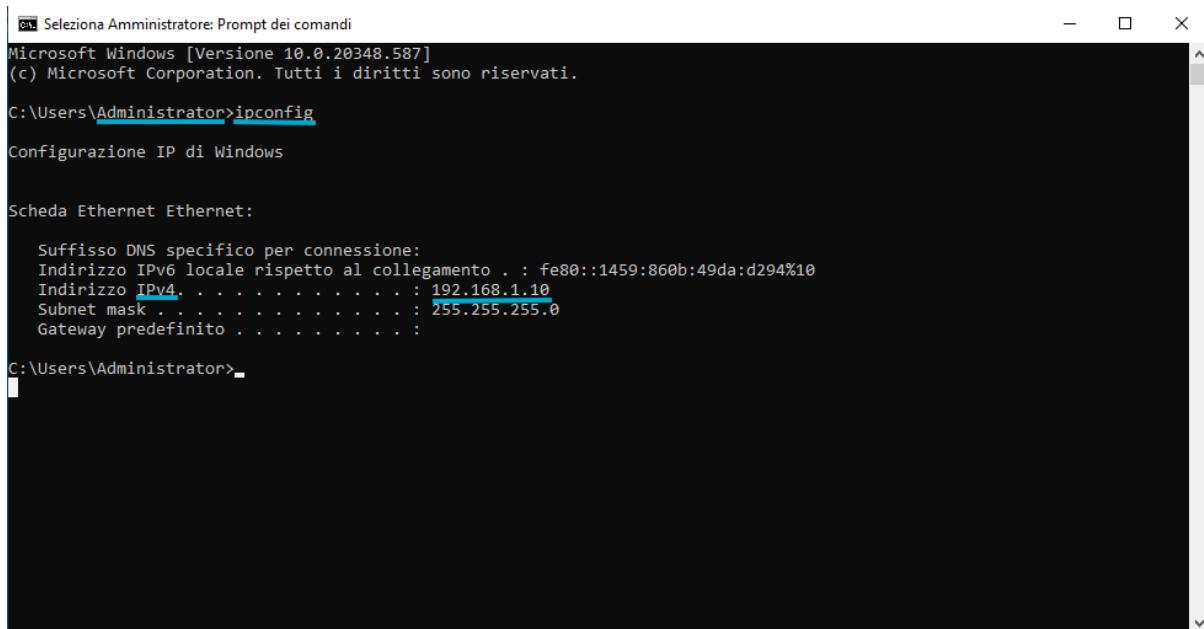


Post Login vado sulle impostazioni della scheda di rete e vado a configurare l'indirizzo ipv4 e il Dns (che saranno uguali perchè il Server fungerà anche da Server DNS).





Eseguiamo un “ipconfig” da cmd per verificare se i settaggi sono stati configurati correttamente:



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

C:\Users\Administrator>ipconfig

Configurazione IP di Windows

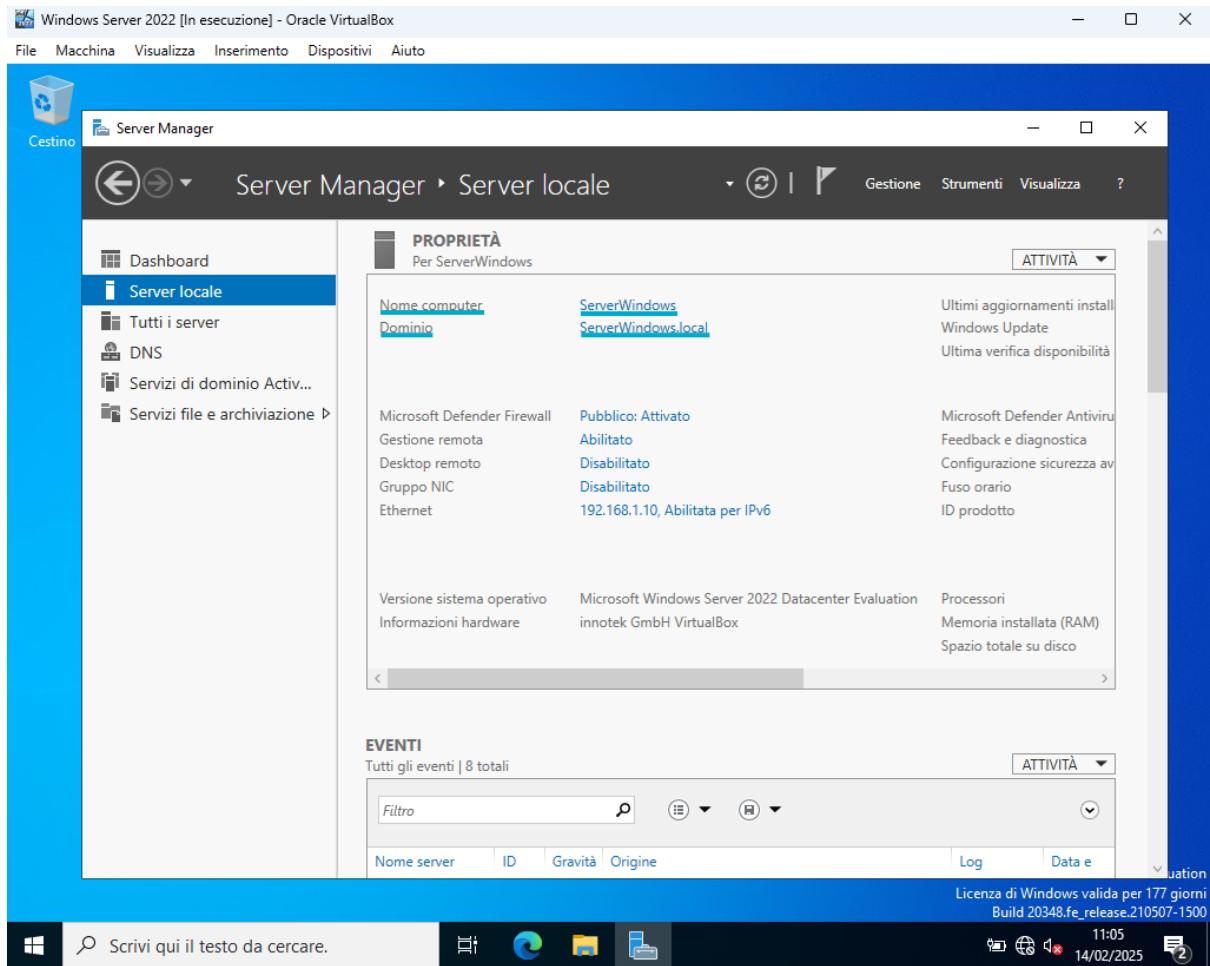
Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::1459:860b:49da:d294%10
    Indirizzo IPv4 . . . . . : 192.168.1.10
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

C:\Users\Administrator>
```

Tramite l'ipconfig vediamo che siamo utenti amministratori e che la configurazione dell'indirizzo Ip è avvenuta correttamente.

Successivamente ci spostiamo nel software “Server Manager” e andiamo a verificare la configurazione già creata. (I settaggi del dominio e la foresta sono gli stessi del precedente esercizio).

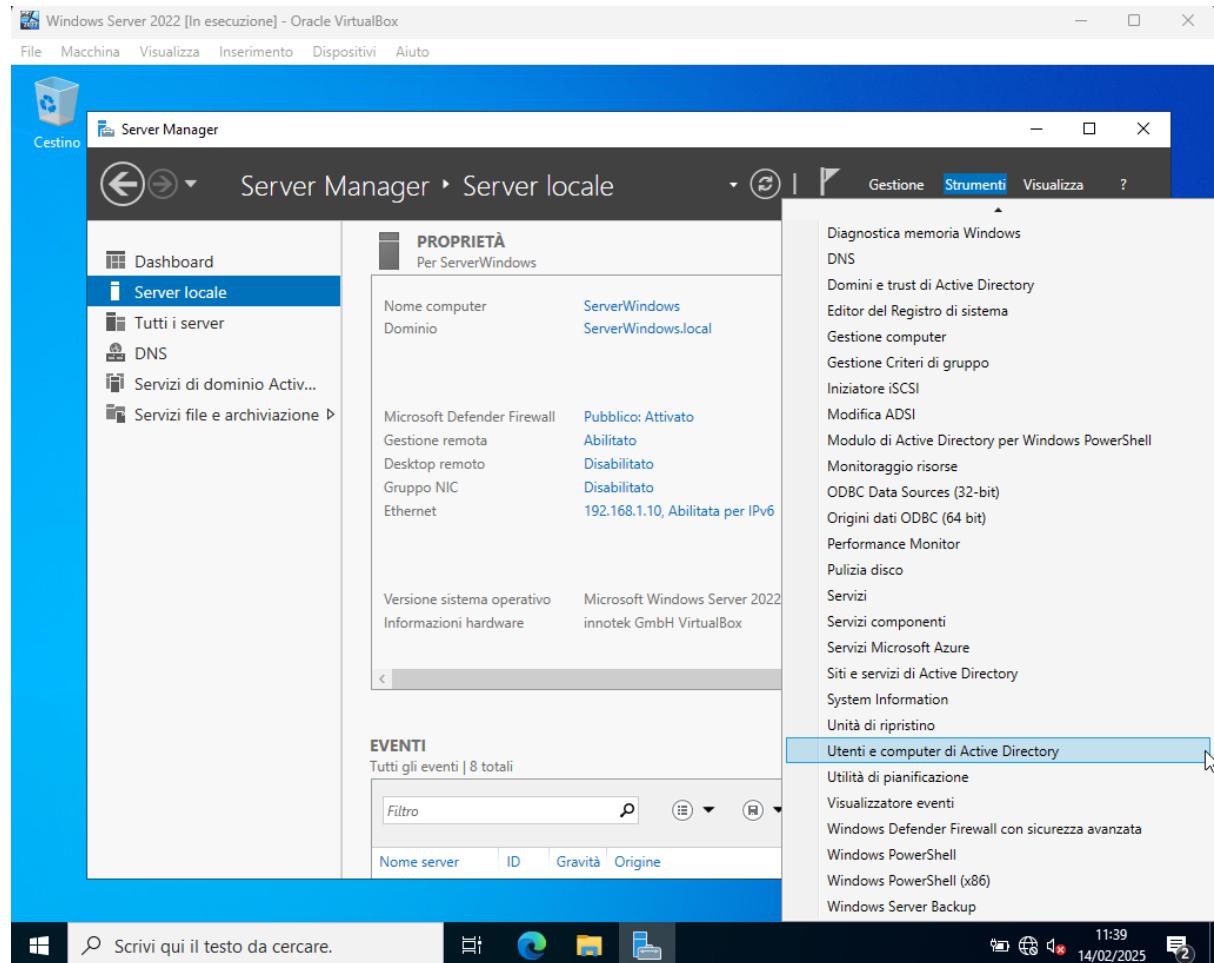


Come Nome della macchina Server abbiamo "ServerWindows" e come nome del Dominio del Server abbiamo "ServerWindows.local", esso ci servirà dopo per andare ad effettuare i test dei gruppi con gli utenti dalla Macchina Windows 10 Pro per accedere alle directory.

L'active Directory è già stata creata e come nome foresta abbiamo "SERVERWINDOWS0" (il check è già stato alla radice quando ci si è andato a loggare sul server 1* screen).

-Creazione dei Gruppi:

Ora andiamo a Creare le 2 sezioni dei gruppi e i sottogruppi per una gestione più ottimale e organizzata, per poi andare a creare gli utenti e gestire i permessi.

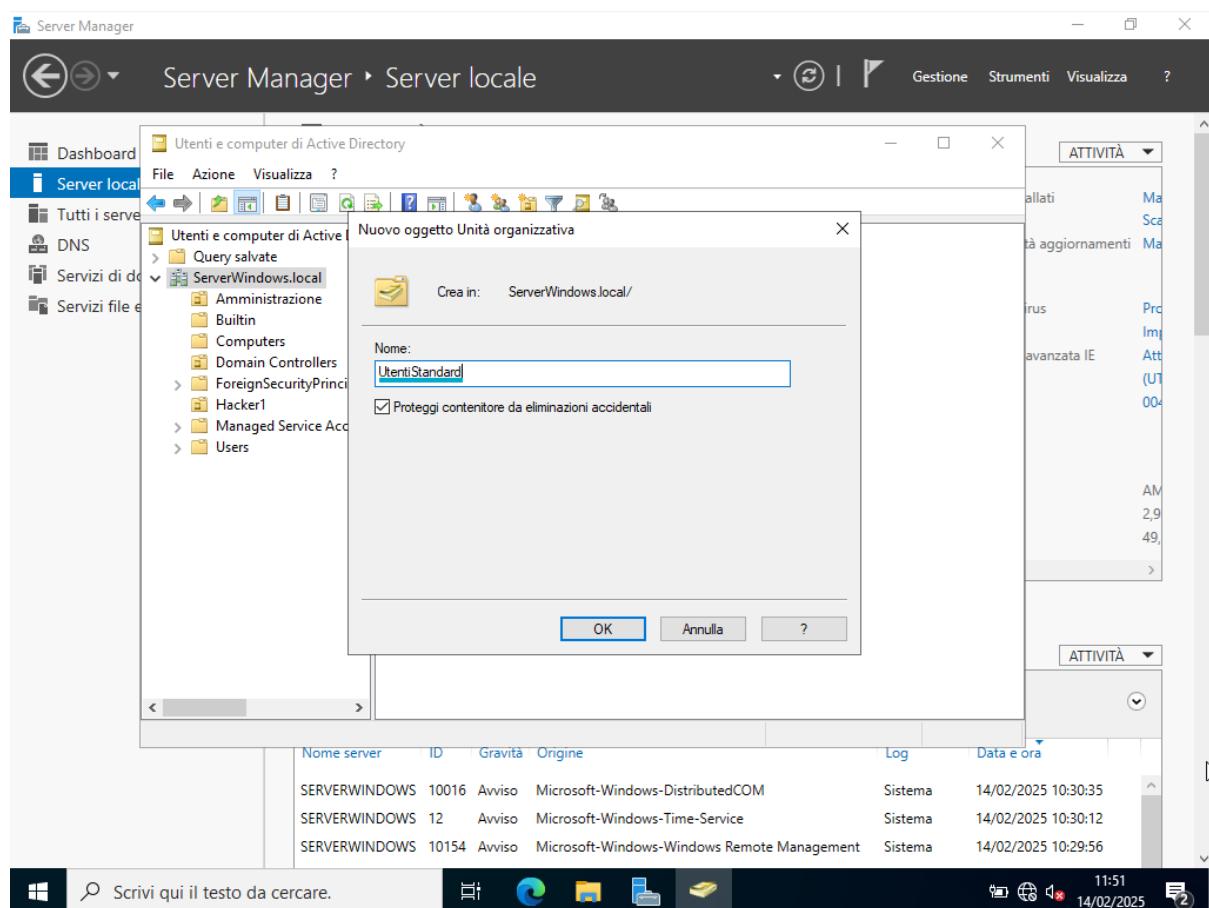
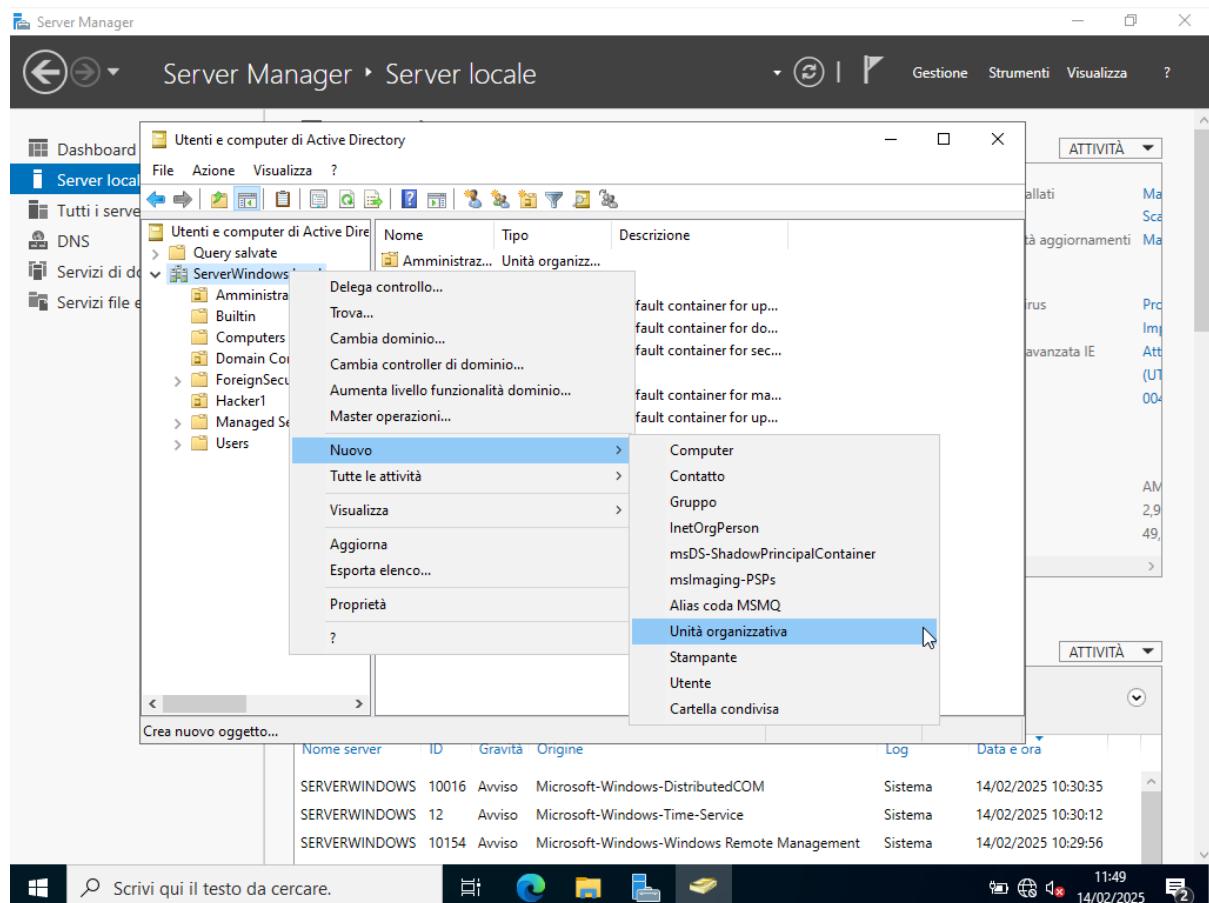


The screenshot shows the Windows Server Manager interface. The left sidebar has 'Server locale' selected. The main area shows the 'Utenti e computer di Active Directory' section for the domain 'ServerWindows.local'. The tree view on the left includes 'Amministrazione', 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Hacker1', 'Managed Service Account', and 'Users'. The main pane lists objects with columns for 'Nome', 'Tipo', and 'Descrizione'. On the right, there are two activity panes and a log window at the bottom showing system events.

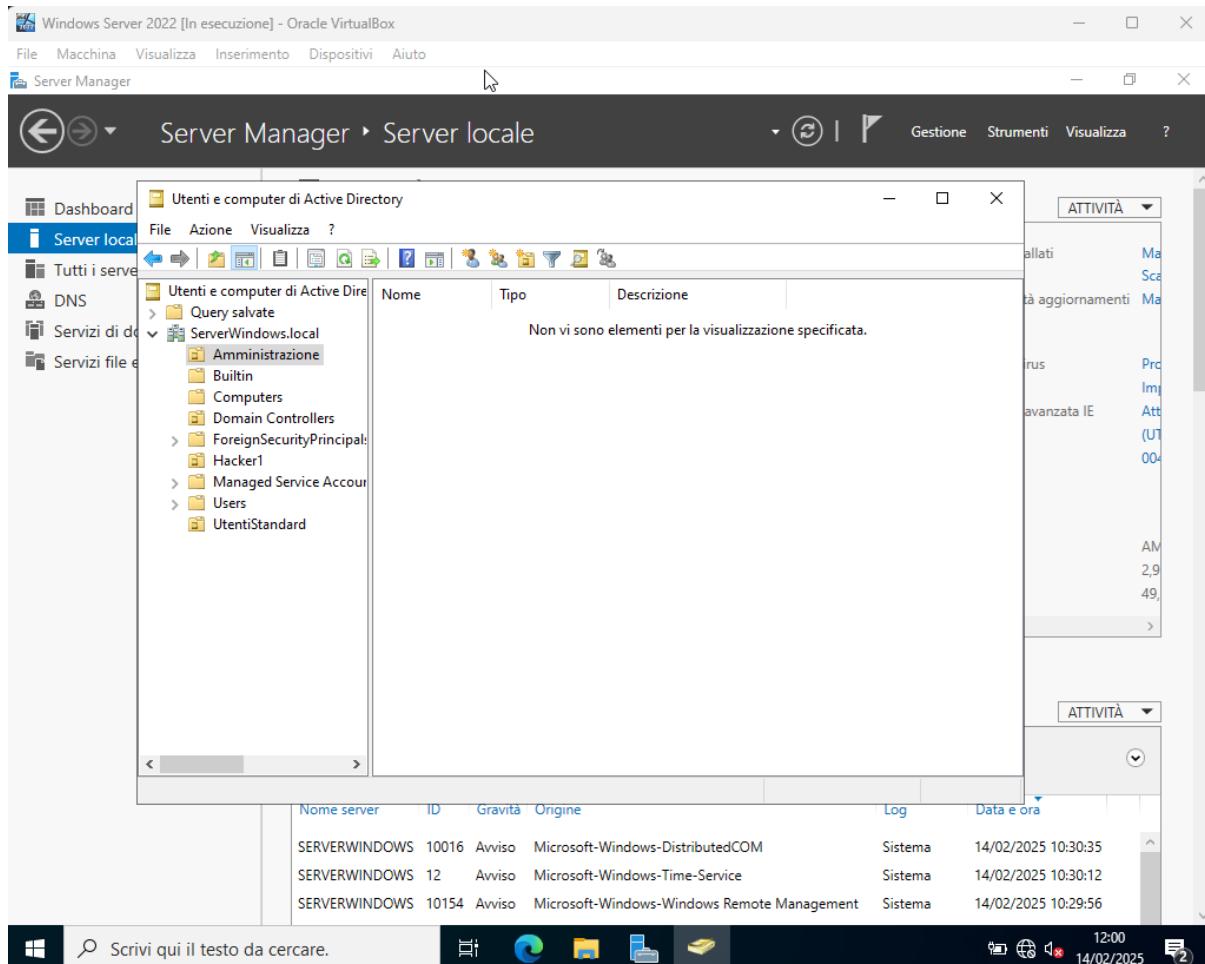
Nome	Tipo	Descrizione
Amministraz...	Unità organizz...	
Builtin	builtinDomain	
Computers	Contenitore	Default container for up...
Domain Con...	Unità organizz...	Default container for do...
ForeignSecu...	Contenitore	Default container for sec...
Hacker1	Unità organizz...	
Managed Se...	Contenitore	Default container for ma...
Users	Contenitore	Default container for up...

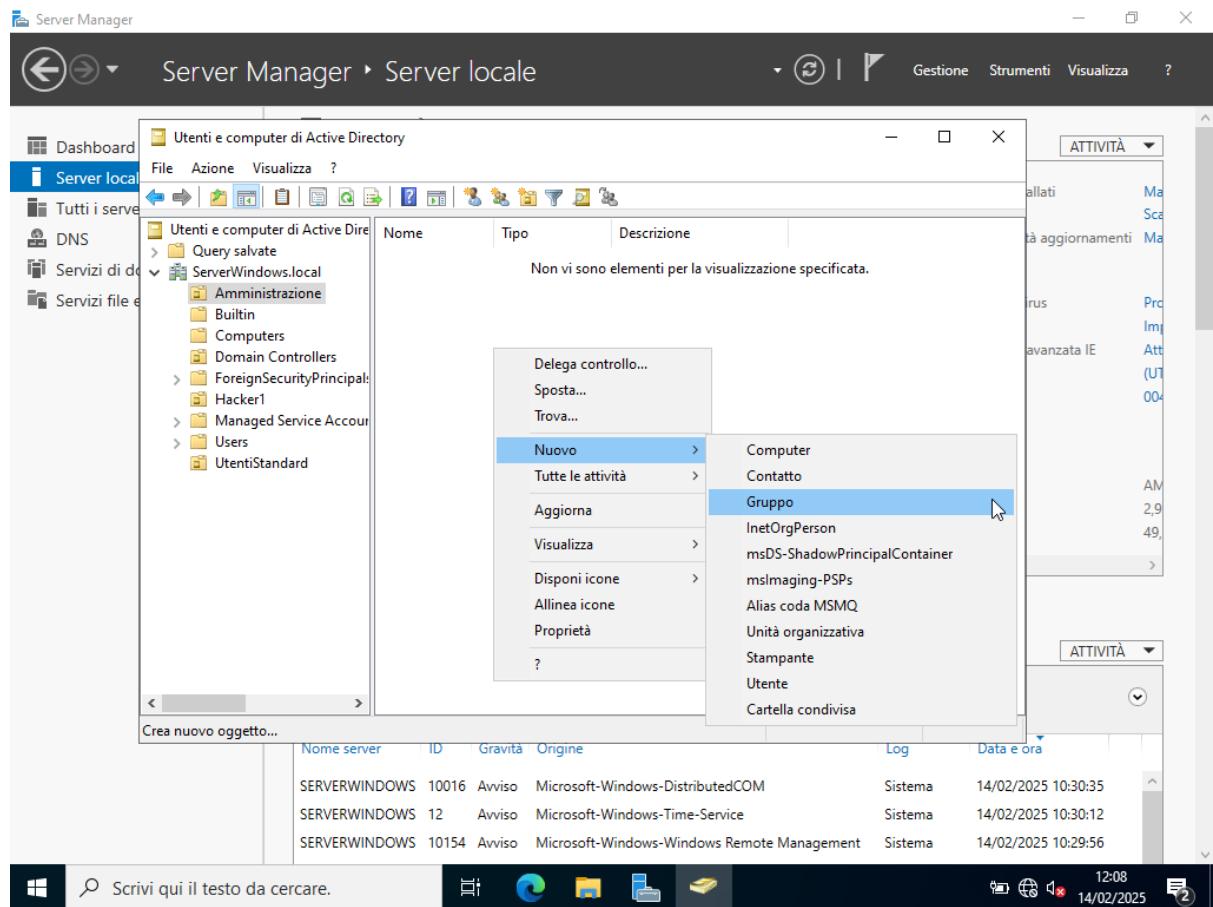
Nome server	ID	Gravità	Origine	Log	Data e ora
SERVERWINDOWS	10016	Avviso	Microsoft-Windows-DistributedCOM	Sistema	14/02/2025 10:30:35
SERVERWINDOWS	12	Avviso	Microsoft-Windows-Time-Service	Sistema	14/02/2025 10:30:12
SERVERWINDOWS	10154	Avviso	Microsoft-Windows-Windows Remote Management	Sistema	14/02/2025 10:29:56

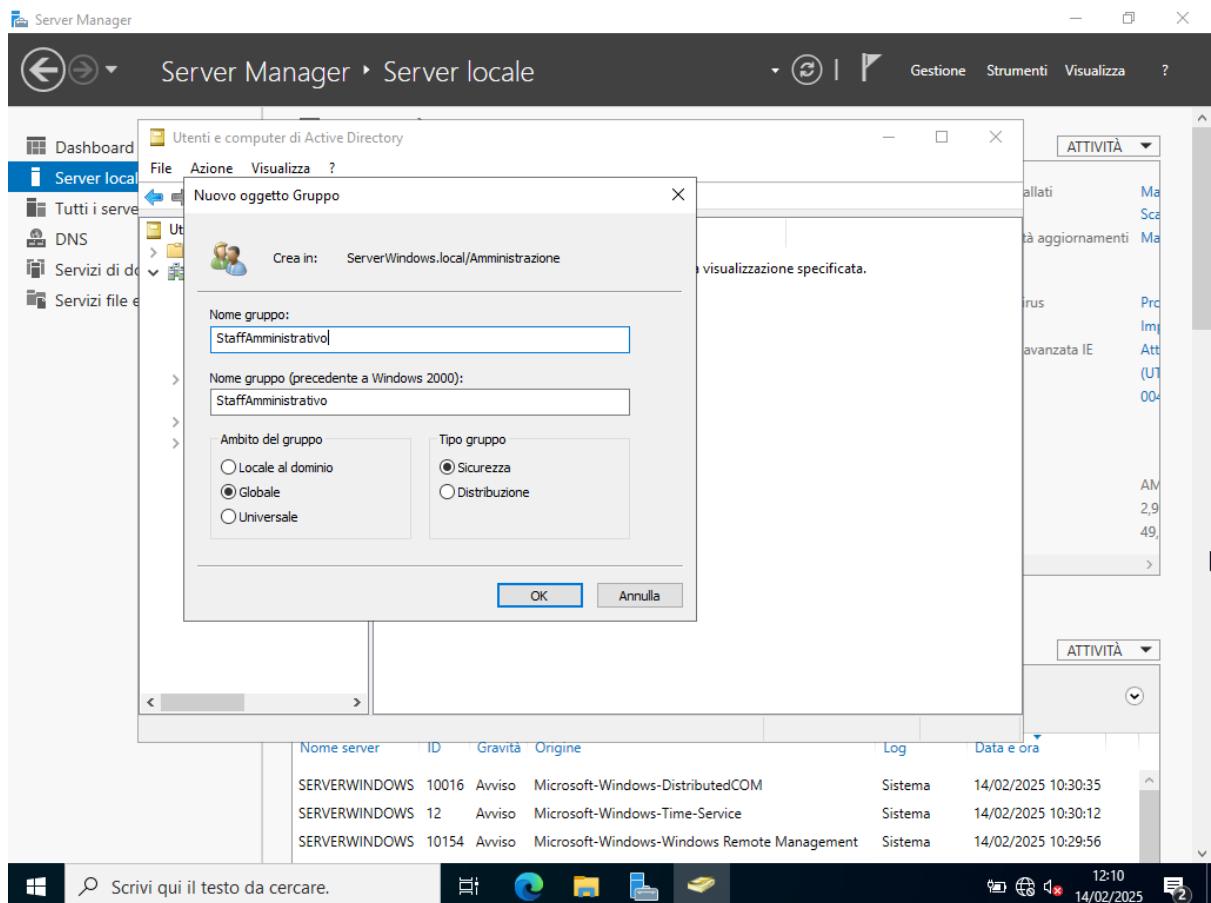
Come Foresta/Dominio abbiamo "ServerWindows.local" e abbiamo già creato la sezione "Amministrazione" (dentro essa andrà a creare il Gruppo "StaffAmministrativo" e i vari utenti), quindi come prima cosa vado a Creare la sezione "UtentiStandard".



Ora andiamo a creare il gruppo “StaffAmministrativo” all’interno della sezione “Amministrazione” per poi andare a creare gli utenti.







Ora andiamo a creare gli utenti dello Staff amministrativo "Daniele Attampato Franco Mastroianni":

Server Manager

Server Manager • Server locale

Dashboard Server locale

Tutti i servizi DNS Servizi di database Servizi file e dati

Utenti e computer di Active Directory

File Azione Visualizza ?

Utenti e computer di Active Directory

Nome Tipo Descrizione

StaffAmmin... Gruppo di sicurezza

Amministrazione BuiltIn Computers Domain Controllers ForeignSecurityPrincipal Hacker1 Managed Service Account Users UtentiStandard

Delega controllo... Sposta... Trova...

Nuovo > Tutte le attività > Aggiorna Esporta elenco... Visualizza > Disponi icone > Allinea icone Proprietà ? Utente Cartella condivisa

Computer Contatto Gruppo InetOrgPerson msDS-ShadowPrincipalContainer msImaging-SPS Alias coda MSMQ Unità organizzativa Stampante

Crea nuovo oggetto...

Nome server ID Gravità Origine Log Data e ora

SERVERWINDOWS 10016 Avviso Microsoft-Windows-DistributedCOM Sistema 14/02/2025 10:30:35

SERVERWINDOWS 12 Avviso Microsoft-Windows-Time-Service Sistema 14/02/2025 10:30:12

SERVERWINDOWS 10154 Avviso Microsoft-Windows-Windows Remote Management Sistema 14/02/2025 10:29:56

Scrivi qui il testo da cercare.

12:19 14/02/2025

Server Manager

Server Manager • Server locale

Dashboard Server locale

Tutti i servizi DNS Servizi di database Servizi file e dati

Utenti e computer di Active Directory

Nuovo oggetto Utente

Nome Nome accesso utente:

Daniele Daniele@ServerWindows.local

Cognome Nome accesso utente (precedente a Windows 2000):

Attampato SERVERWINDOWS0\ Daniele

< Indietro Avanti > Annulla

Nome server ID Gravità Origine Log Data e ora

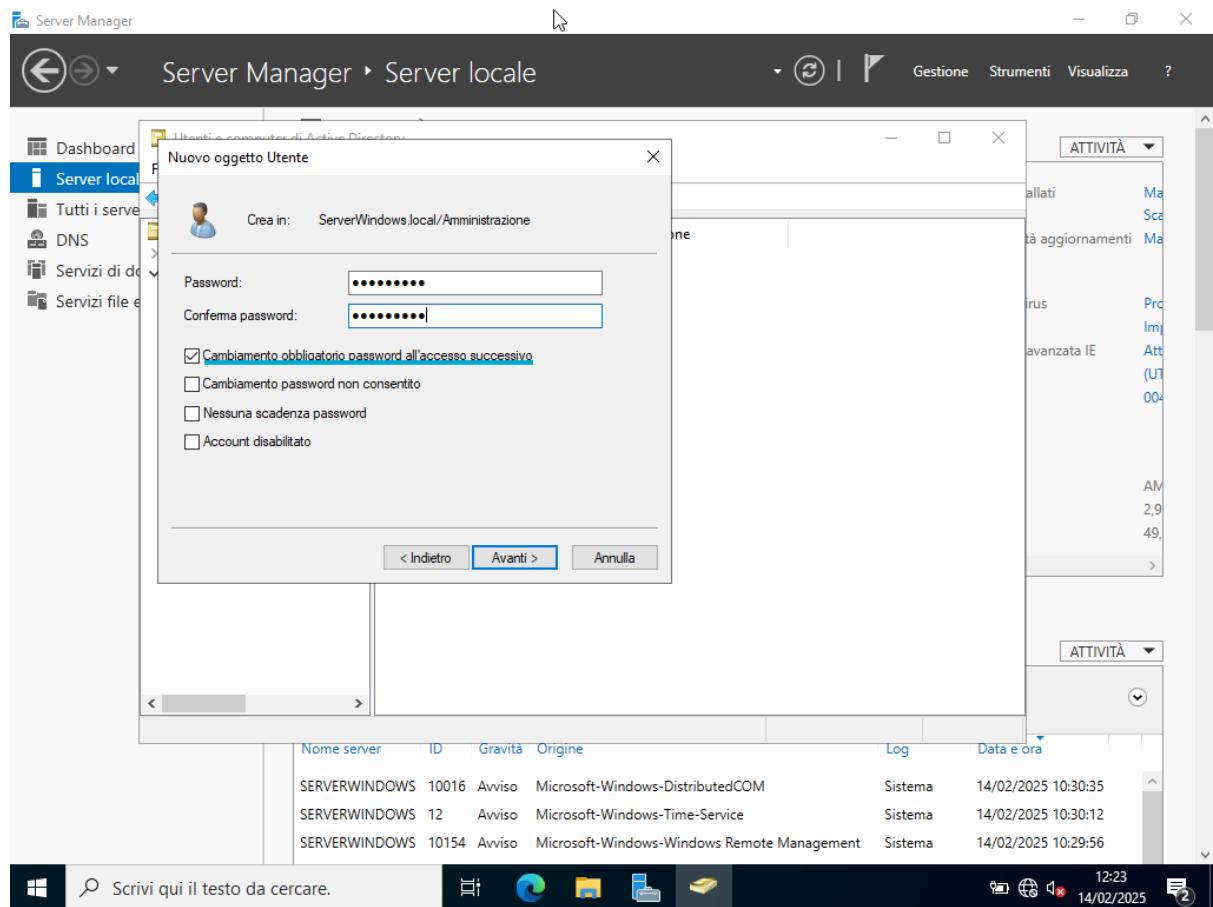
SERVERWINDOWS 10016 Avviso Microsoft-Windows-DistributedCOM Sistema 14/02/2025 10:30:35

SERVERWINDOWS 12 Avviso Microsoft-Windows-Time-Service Sistema 14/02/2025 10:30:12

SERVERWINDOWS 10154 Avviso Microsoft-Windows-Windows Remote Management Sistema 14/02/2025 10:29:56

Scrivi qui il testo da cercare.

12:20 14/02/2025



Server Manager

Server Manager • Server locale

Dashboard

Tutti i servizi

DNS

Servizi di dominio

Servizi file e dati

Utenti e computer di Active Directory

File Azione Visualizza ?

Utenti e computer di Active Directory

Nome Tipo Descrizione

Daniele Att... Utente

StaffAmmini... Gruppo di sicurezza

Amministrazione

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipal

Hacker1

Managed Service Account

Users

UtentiStandard

Attività

allati

Ma

Sc

tà aggiornamenti

Ma

rus

Pro

Im

Att

(UT

004

AM

2,9

49,

AV

ATTIVITÀ

Nome server ID Gravità Origine Log Data e ora

SERVERWINDOWS 10016 Avviso Microsoft-Windows-DistributedCOM Sistema 14/02/2025 10:30:35

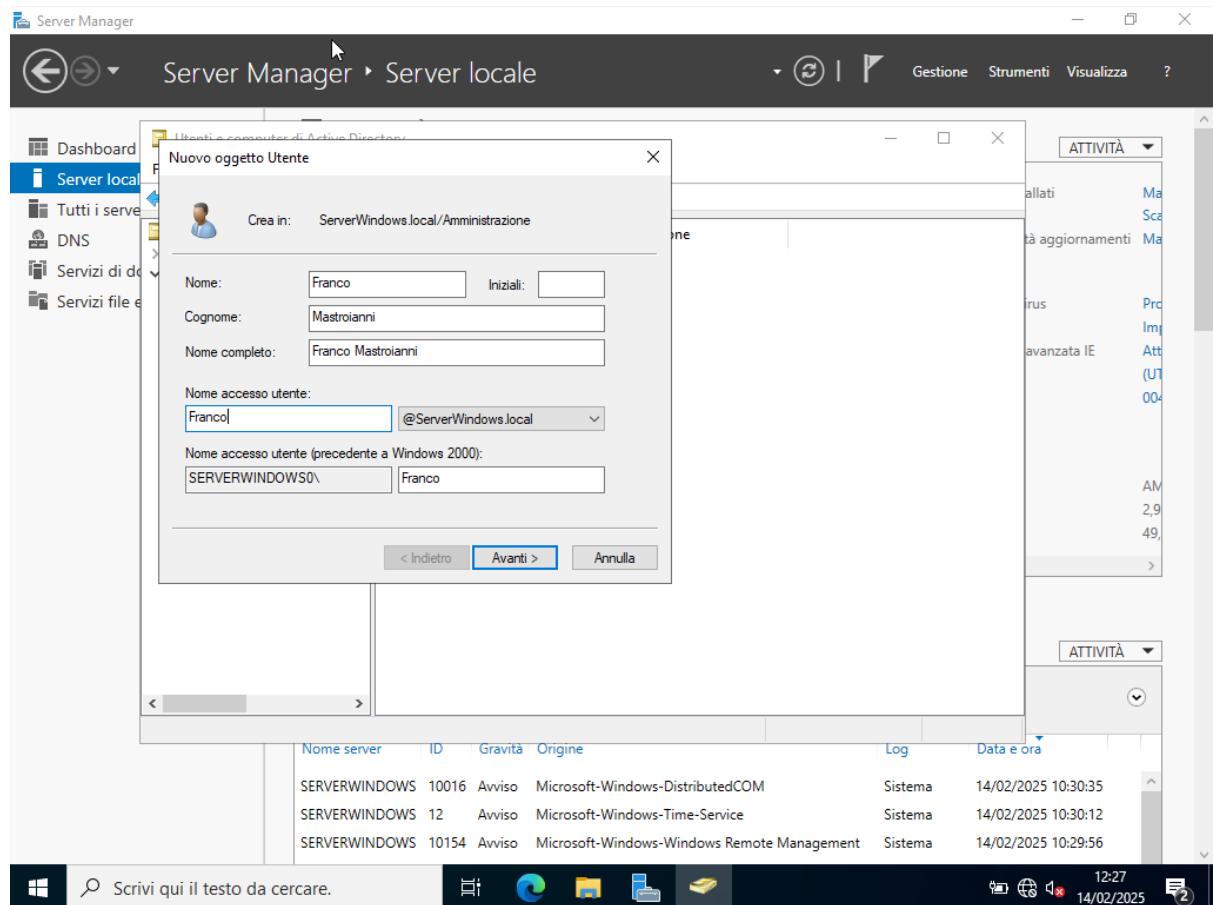
SERVERWINDOWS 12 Avviso Microsoft-Windows-Time-Service Sistema 14/02/2025 10:30:12

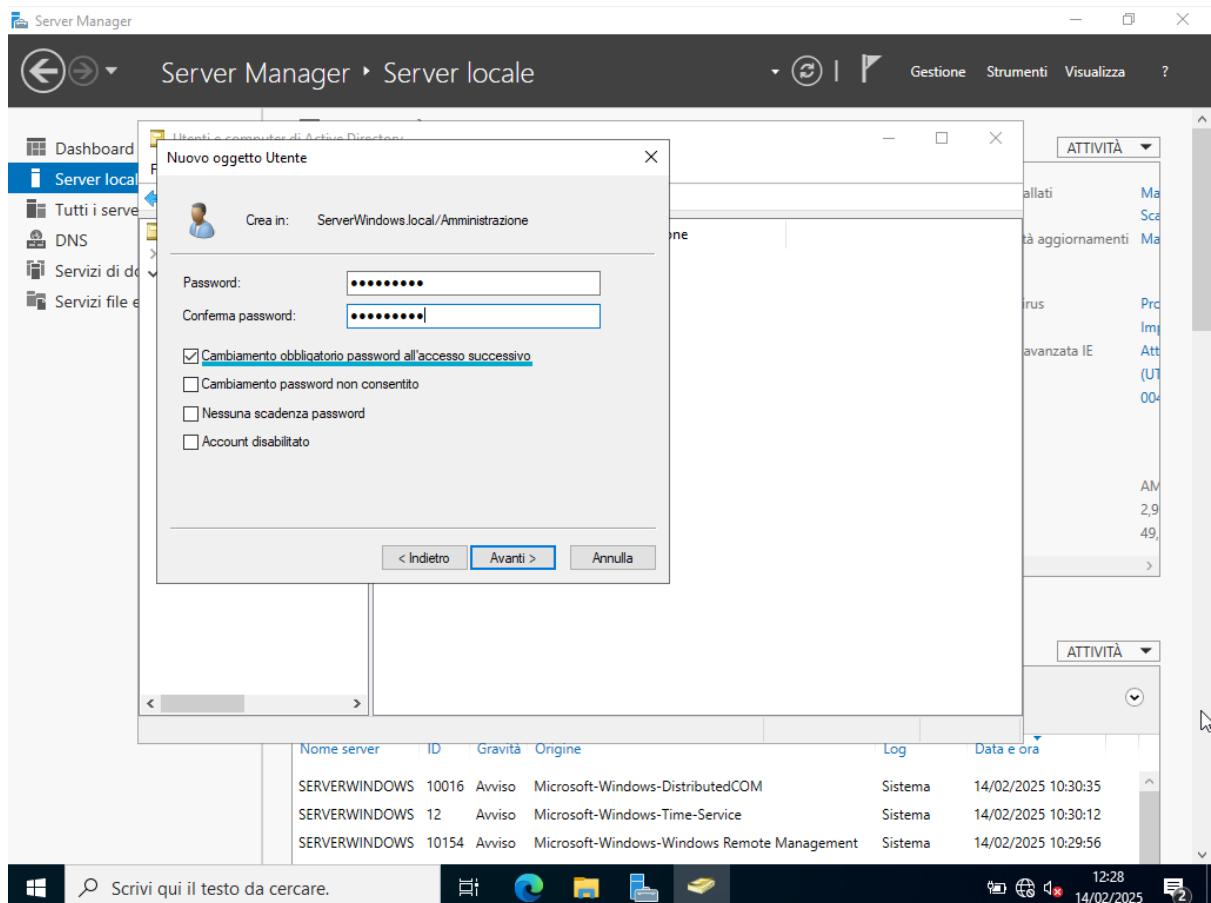
SERVERWINDOWS 10154 Avviso Microsoft-Windows-Windows Remote Management Sistema 14/02/2025 10:29:56

Scrivi qui il testo da cercare.

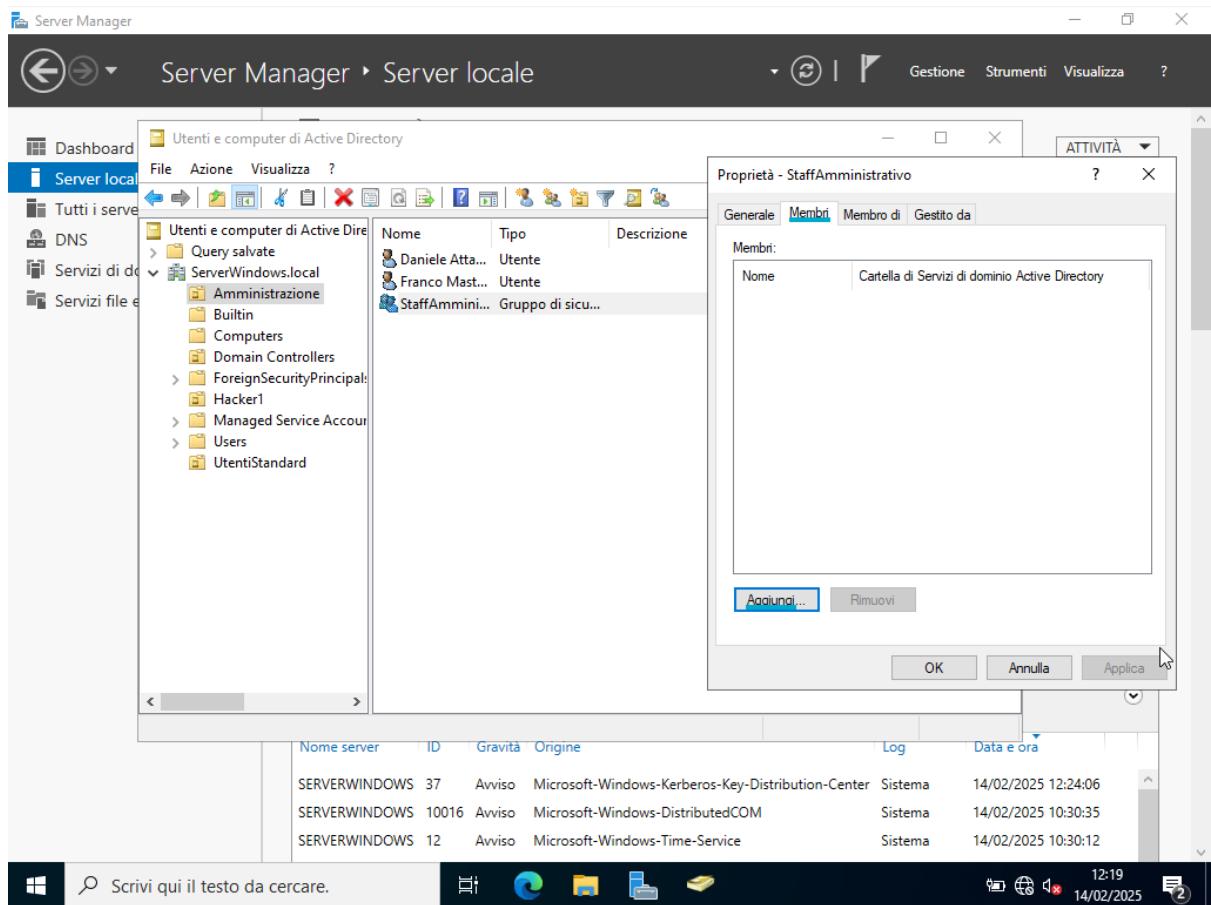
12:25 14/02/2025

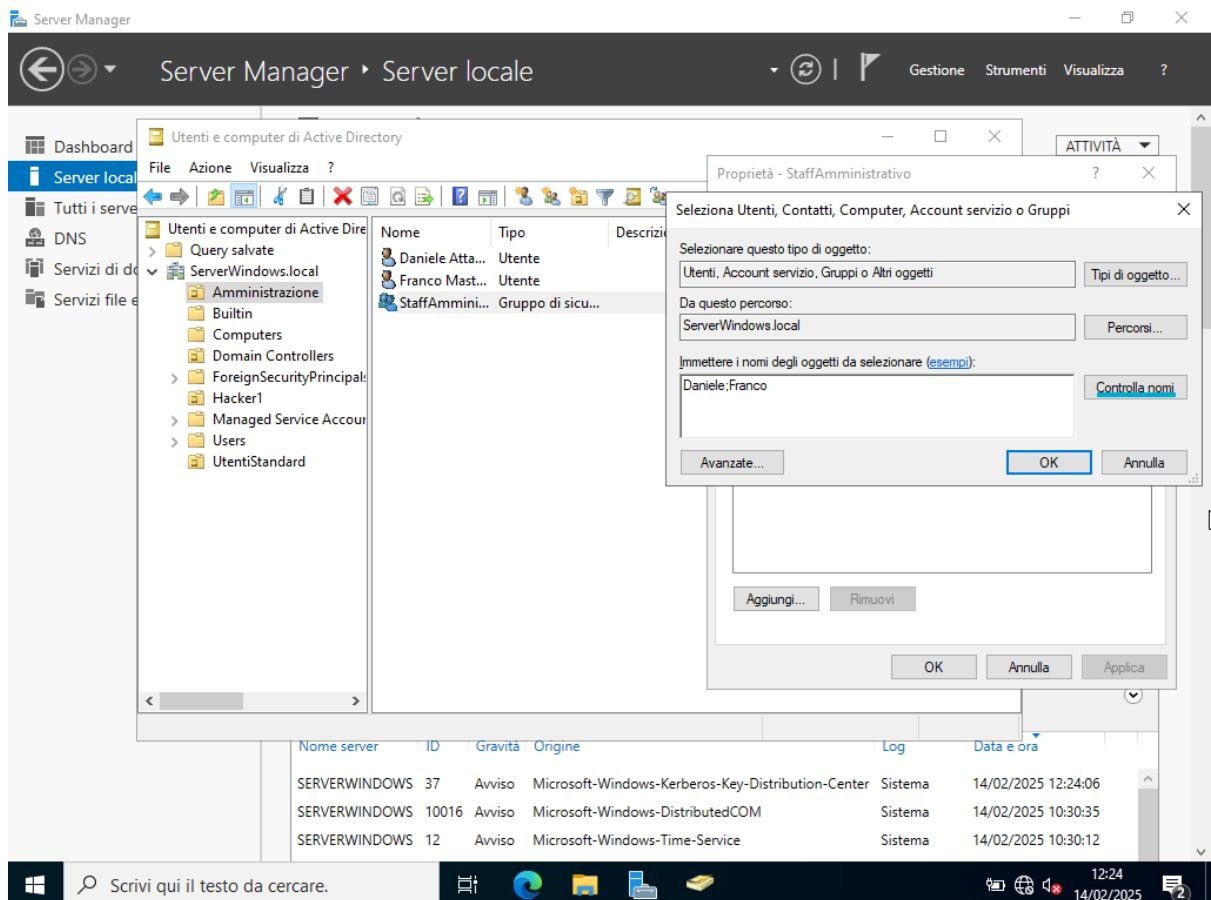
Stesso procedimento per la creazione del 2° utente "Franco Mastroianni":



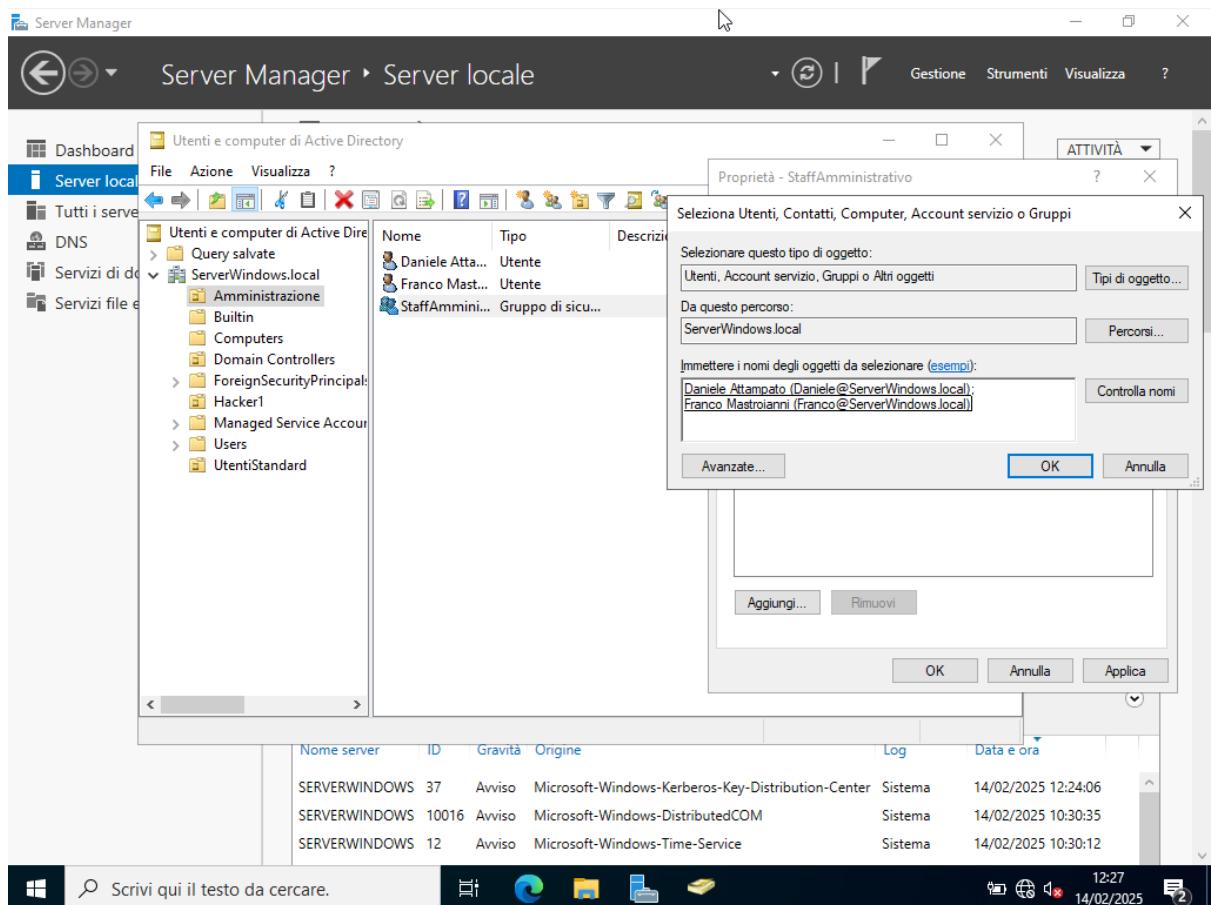


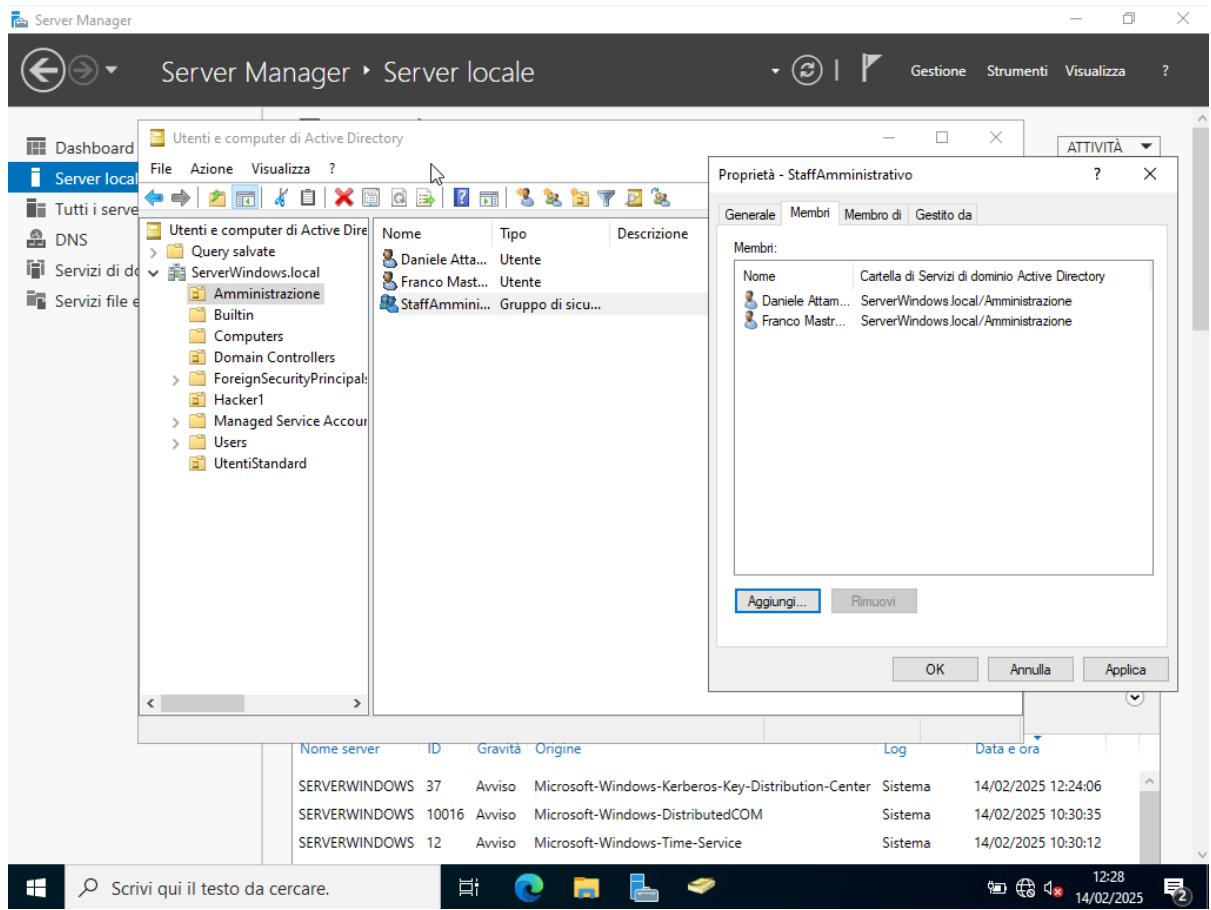
Ora andiamo ad inserire gli utenti nel gruppo "StaffAmministrativo":



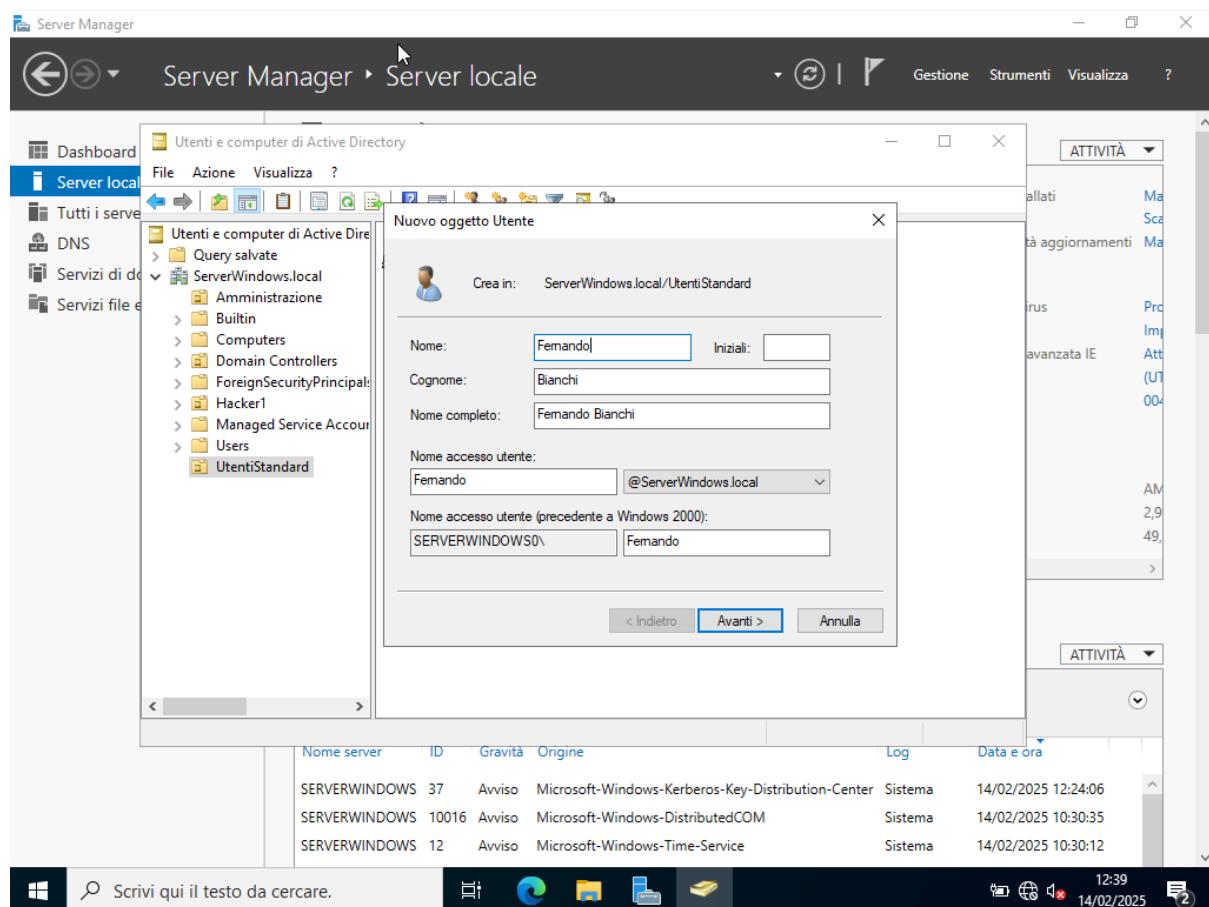
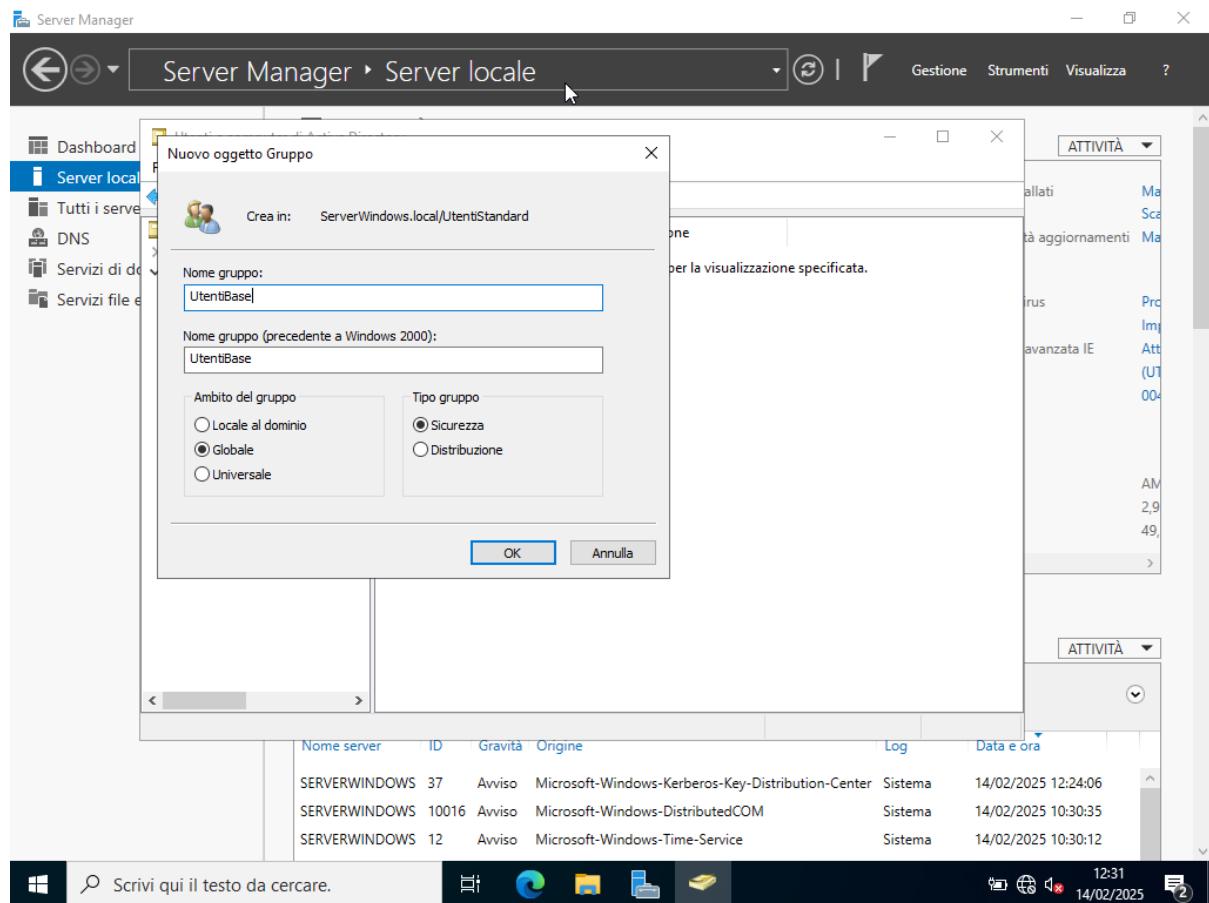


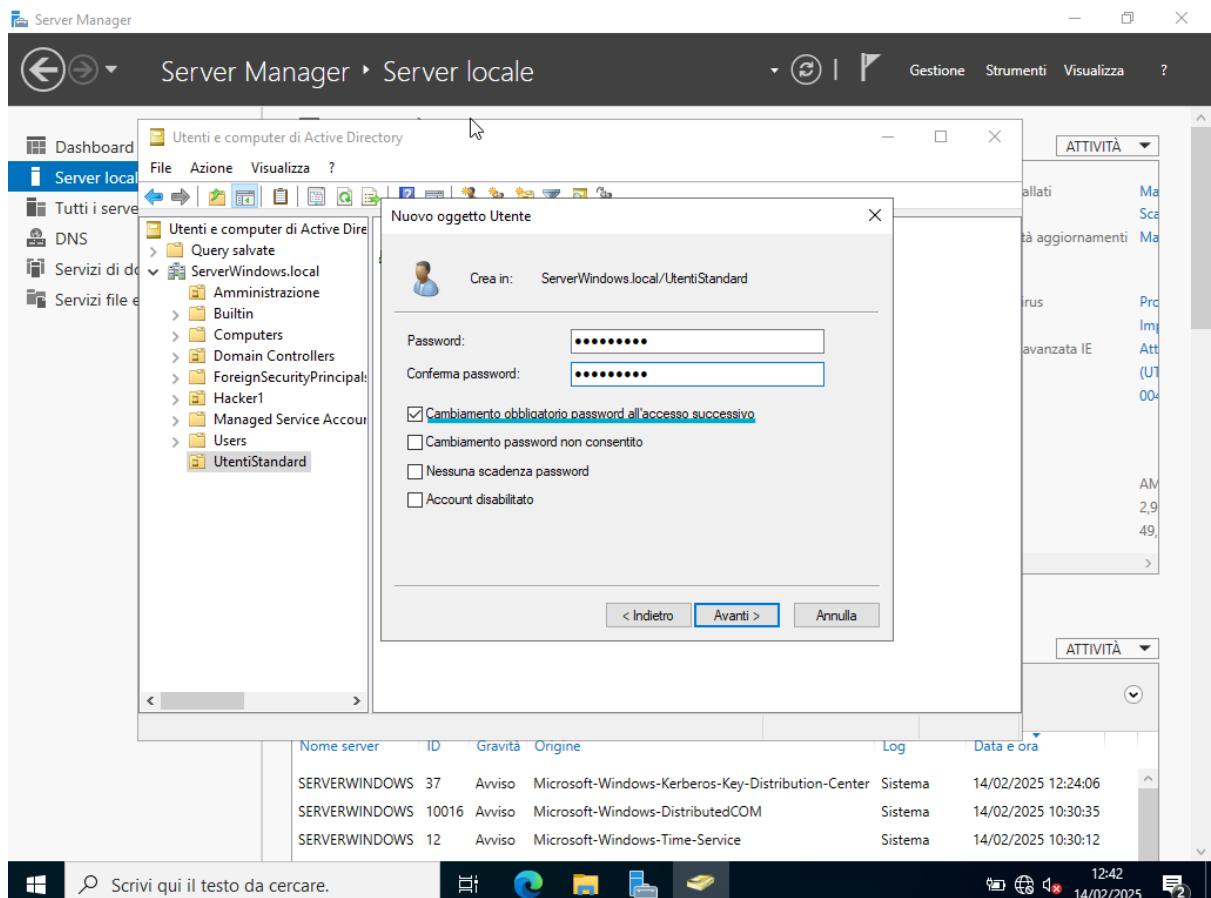
(Per aggiungere più utenti insieme si utilizza il ; tra i nomi e con l'opzione "Controlla nomi" verifichiamo se i nomi inseriti sono corretti).



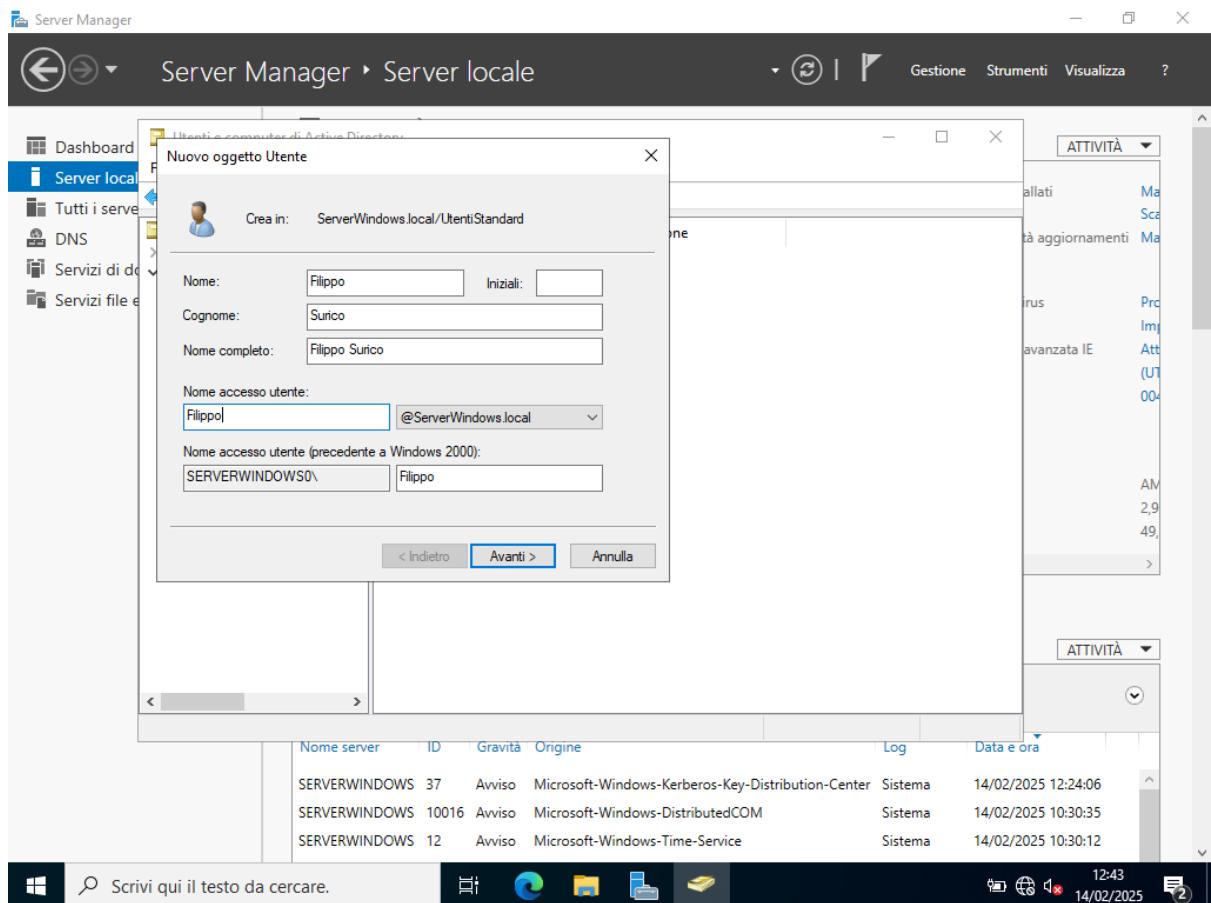


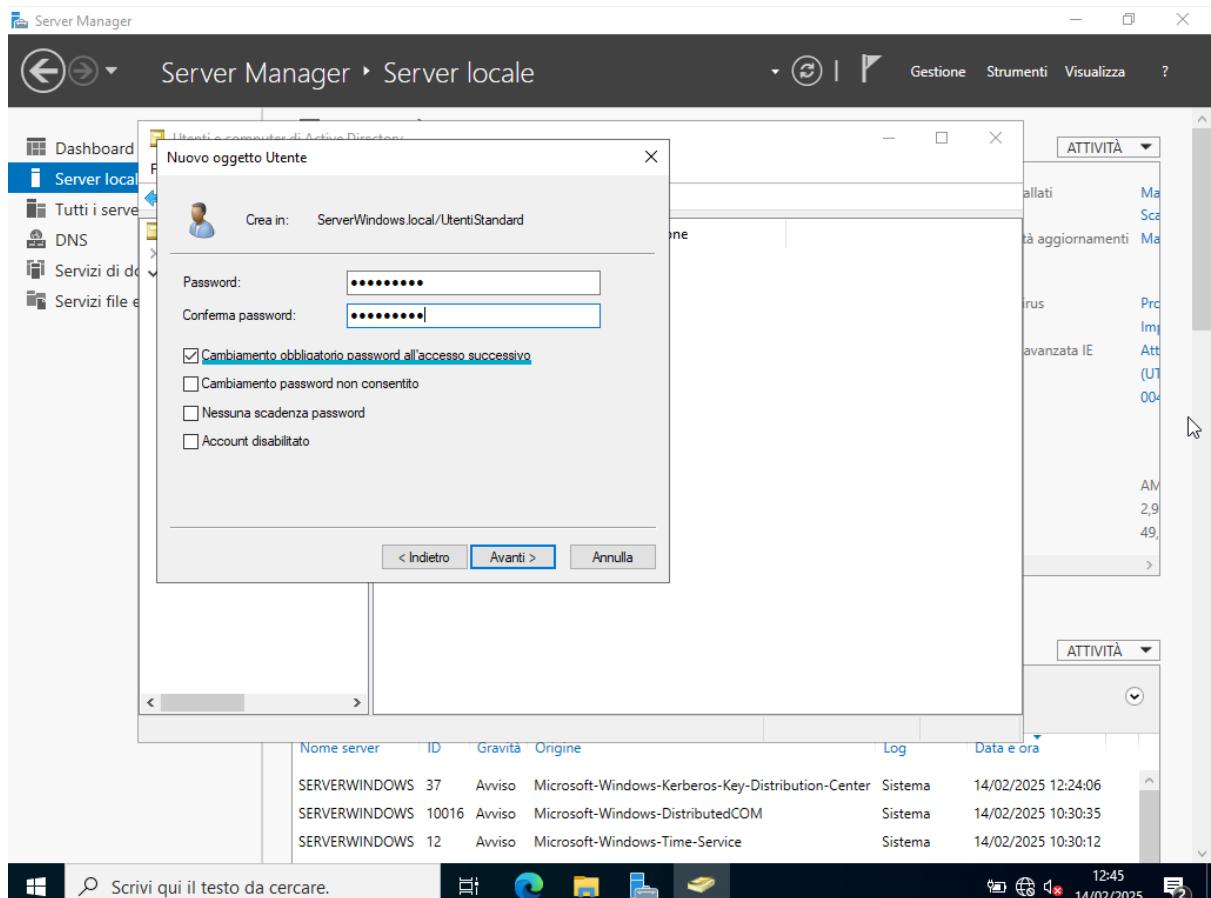
Si ripete il medesimo procedimento sulla sezione “UtentiStandard” per creare il gruppo “UtentiBase” e i relativi utenti “Fernando Bianchi, Filippo Surico”.



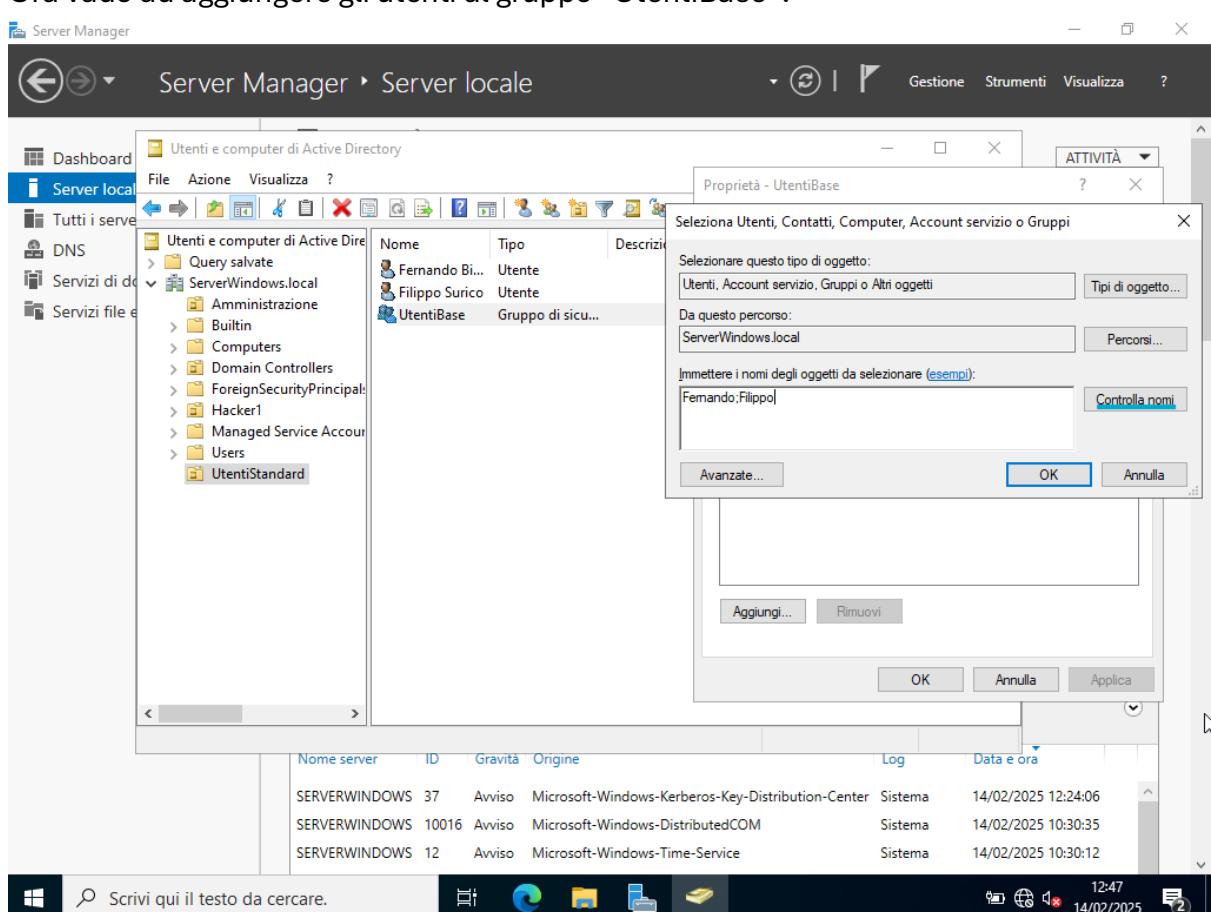


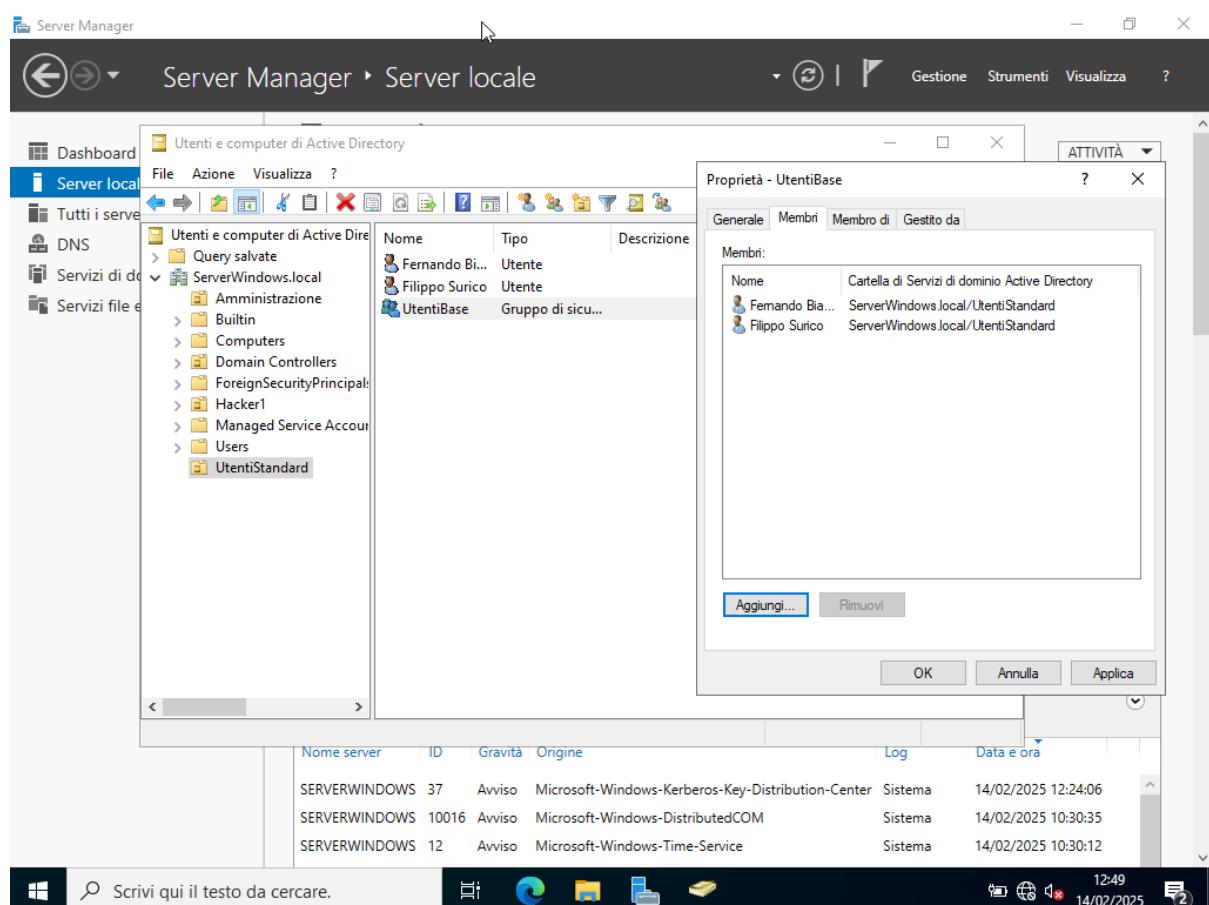
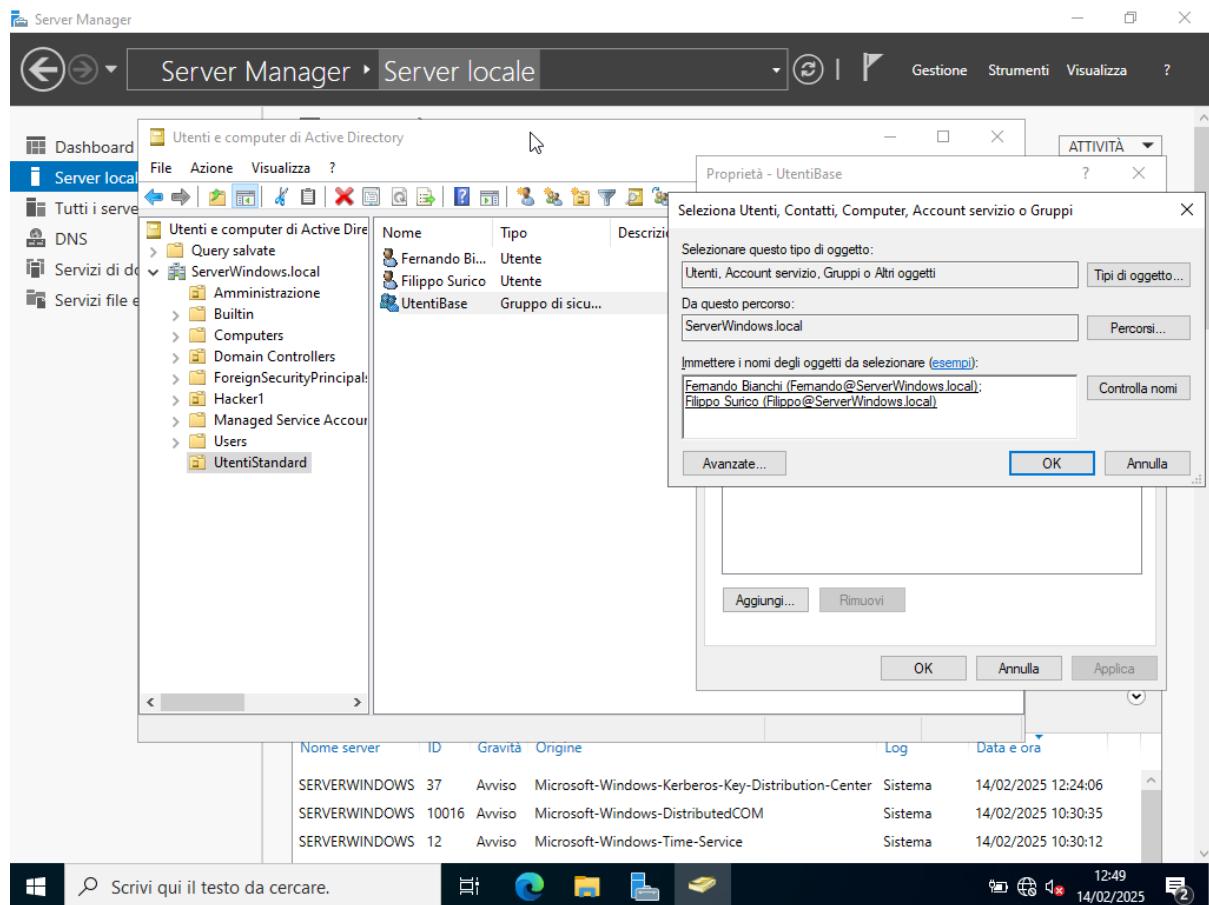
Stesso procedimento per l'altro utente "Filippo Surico":





Ora vado ad aggiungere gli utenti al gruppo "UtentiBase":



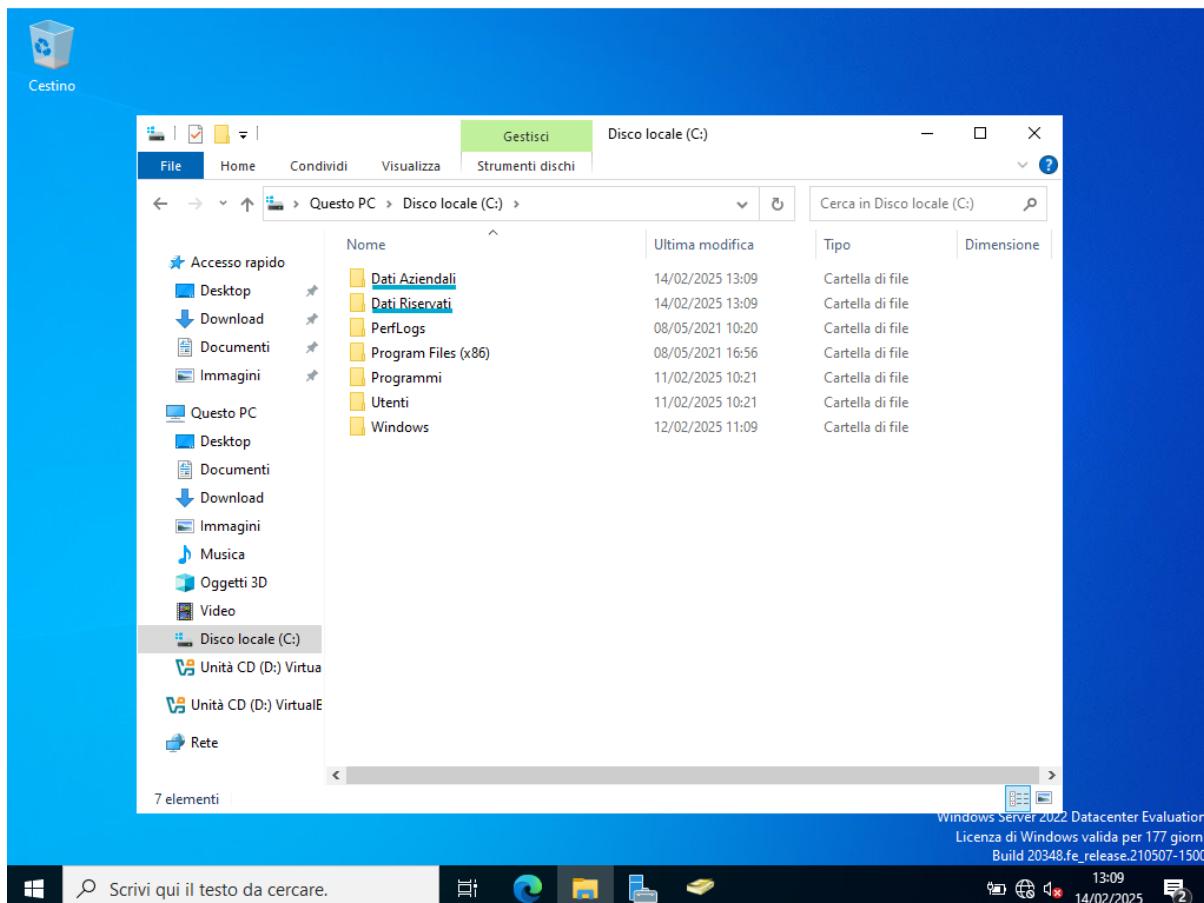


-Creazione Cartelle e Policy:

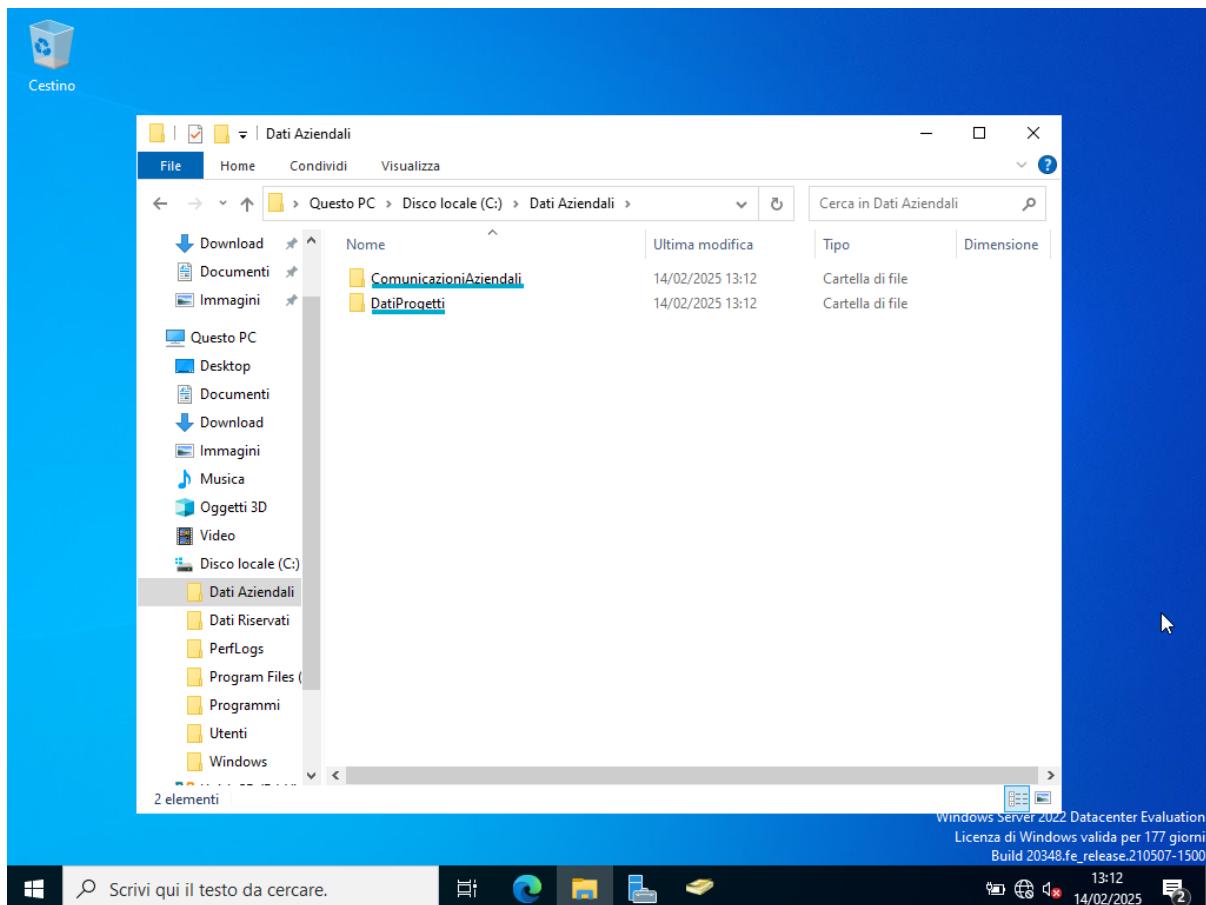
Andremo a creare due Directory “Dati Aziendali, Dati Riservati” dove all’interno creeremo altre cartelle , in seguito andrò a definire le policy di sicurezza dei permessi, per vedere chi può vedere/modificare/eseguire le directory/file.

La Directory Dati Aziendali sarà riservata maggiormente ai dati creati dagli Utenti Base, e alle comunicazioni per tutta l’azienda.

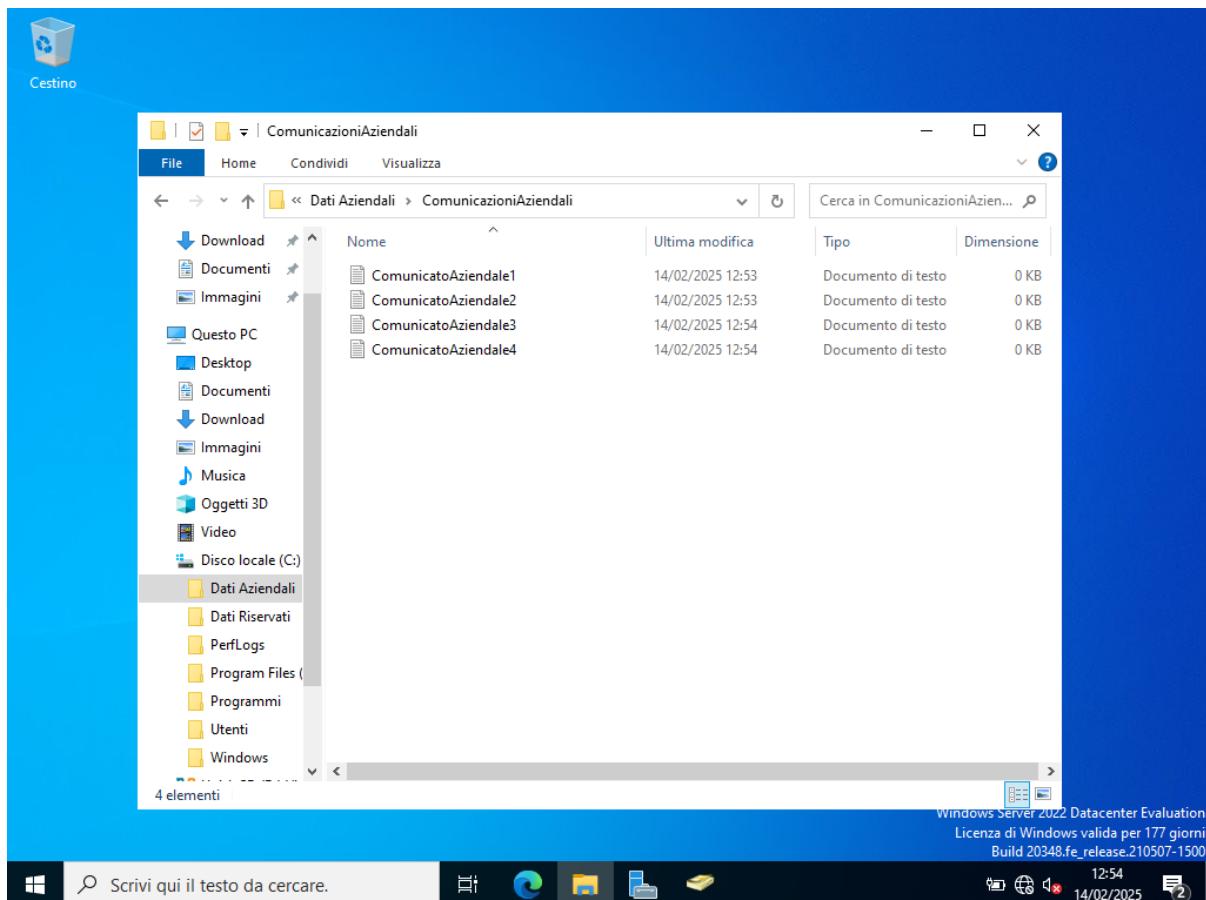
La Directory Dati Riservati sarà riservata solamente allo Staff amministrativo e non sarà accessibile agli Utenti Base.



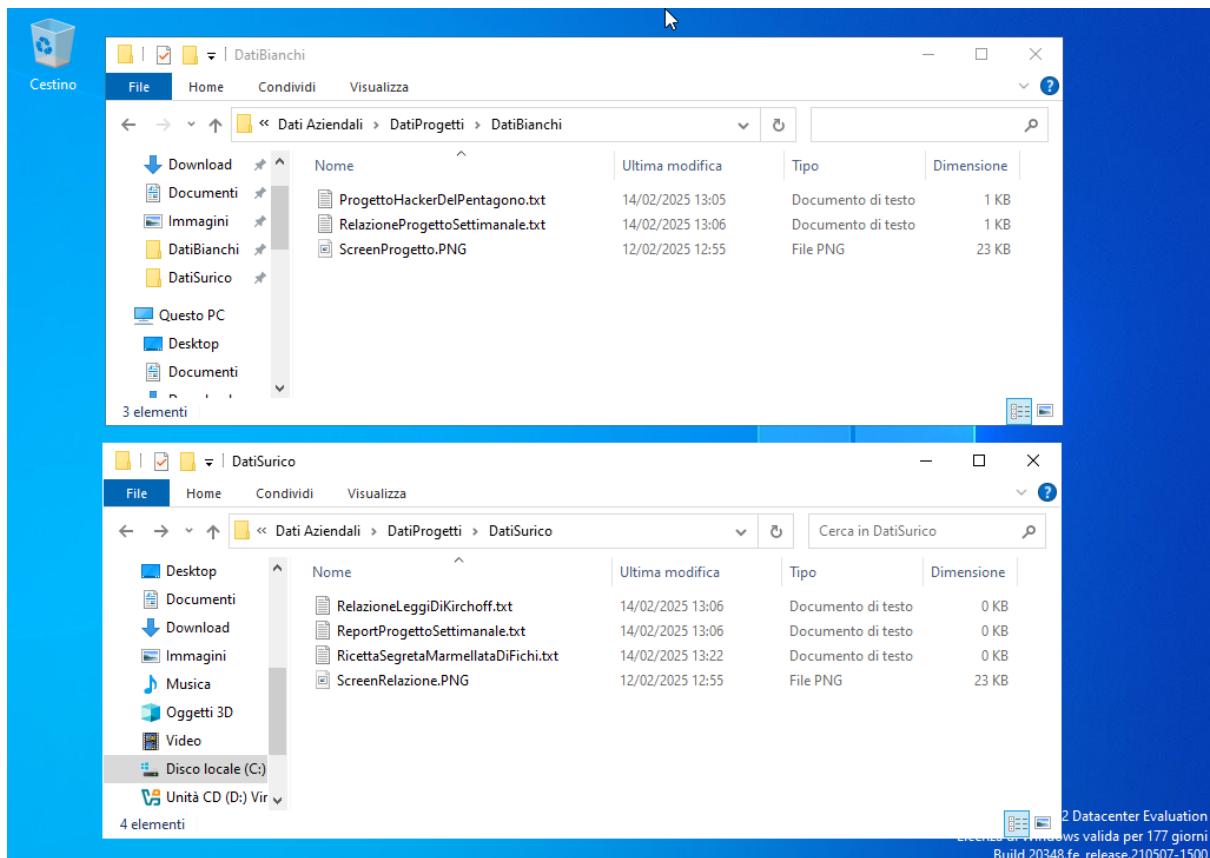
All’interno dei Dati Aziendali creerò due cartelle ”ComunicazioniAziendali”, ”DatiProgetti”.



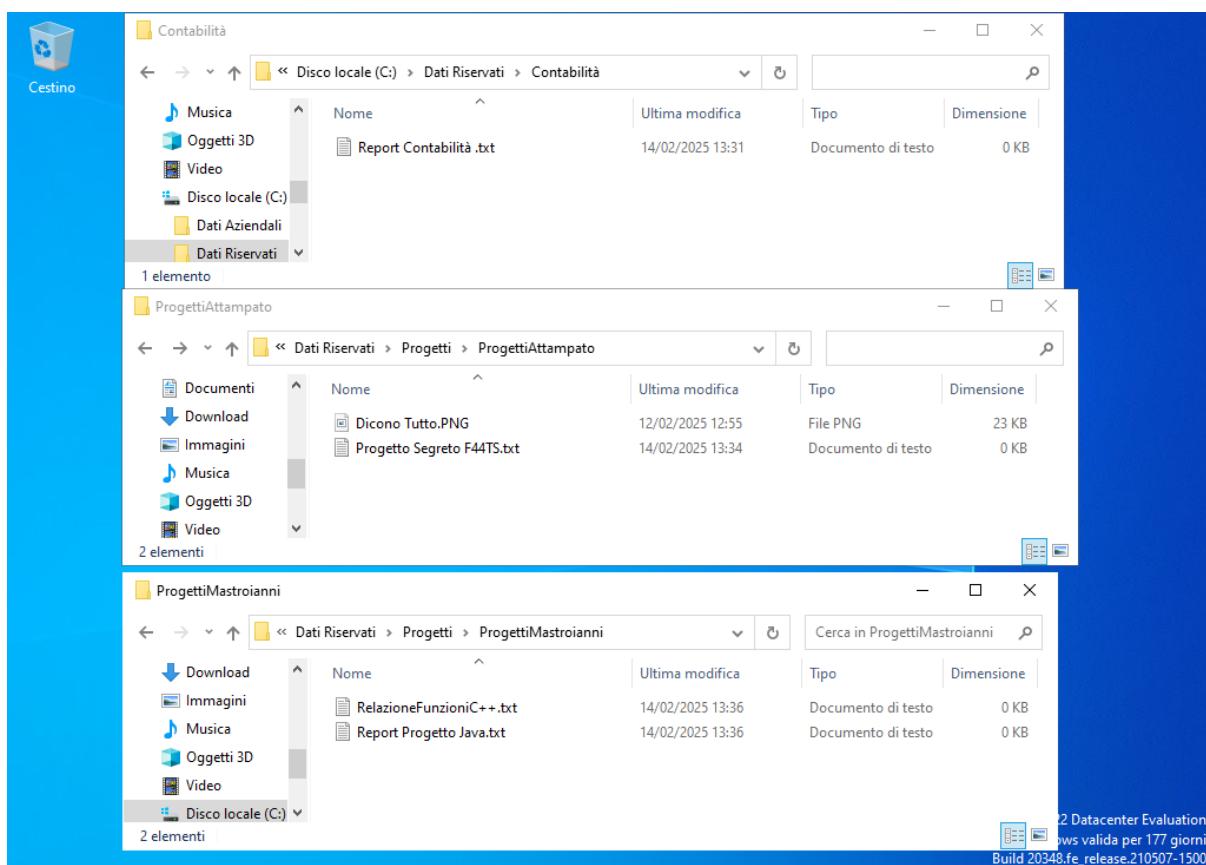
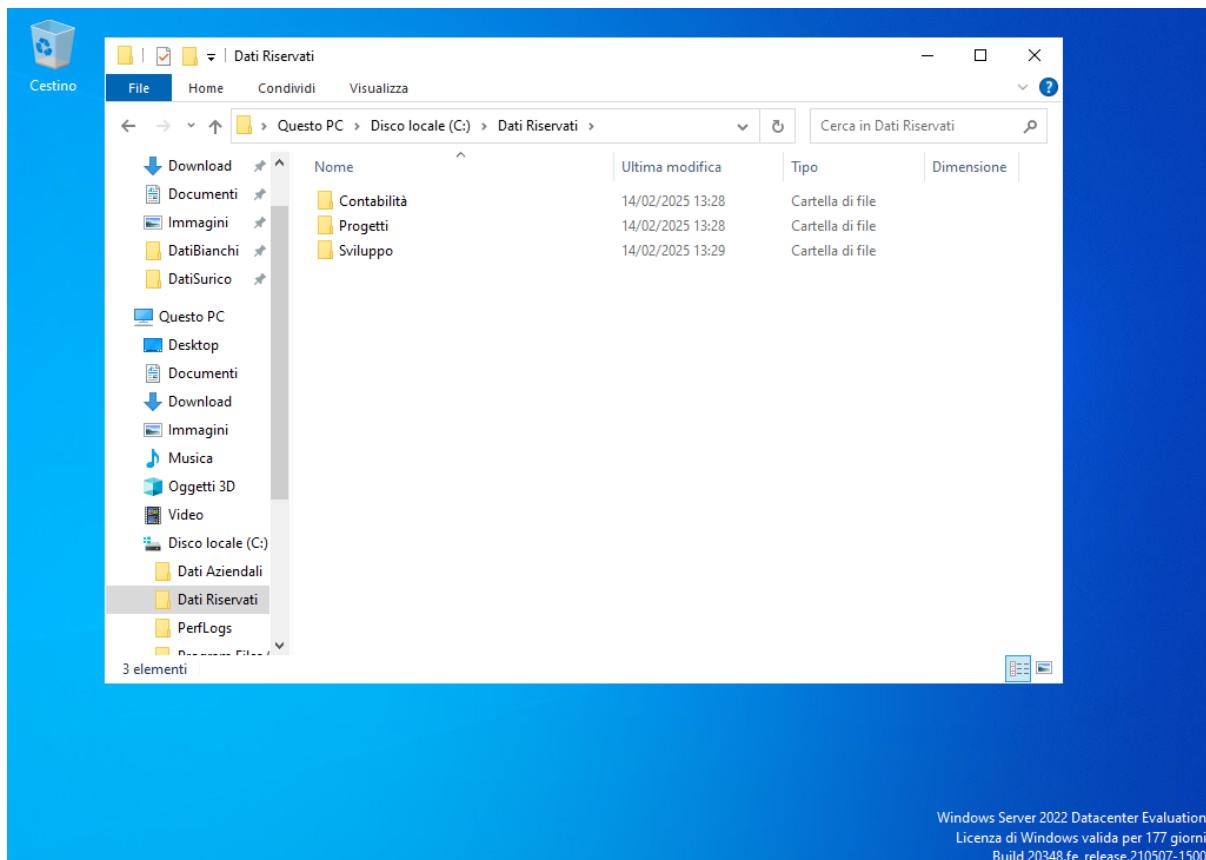
All'interno di "ComunicazioniAziendali" troveremo dei Comunicati Ufficiali a livello aziendale, quindi i permessi saranno che lo Staff Amministrativo può leggere e modificare i file all'interno della cartella, mentre gli Utenti Base potranno solamente leggere i Comunicati ma non modificarli.



Nella cartella DatiProgetti ci saranno i dati creati dagli Utenti Base (quindi a livello di permessi qui gli Utenti Base avranno il permesso di leggere, scrivere, eseguire. Lo staff Amministrativo a scopo di supervisione anch'essi avranno pieni permessi in questa directory).

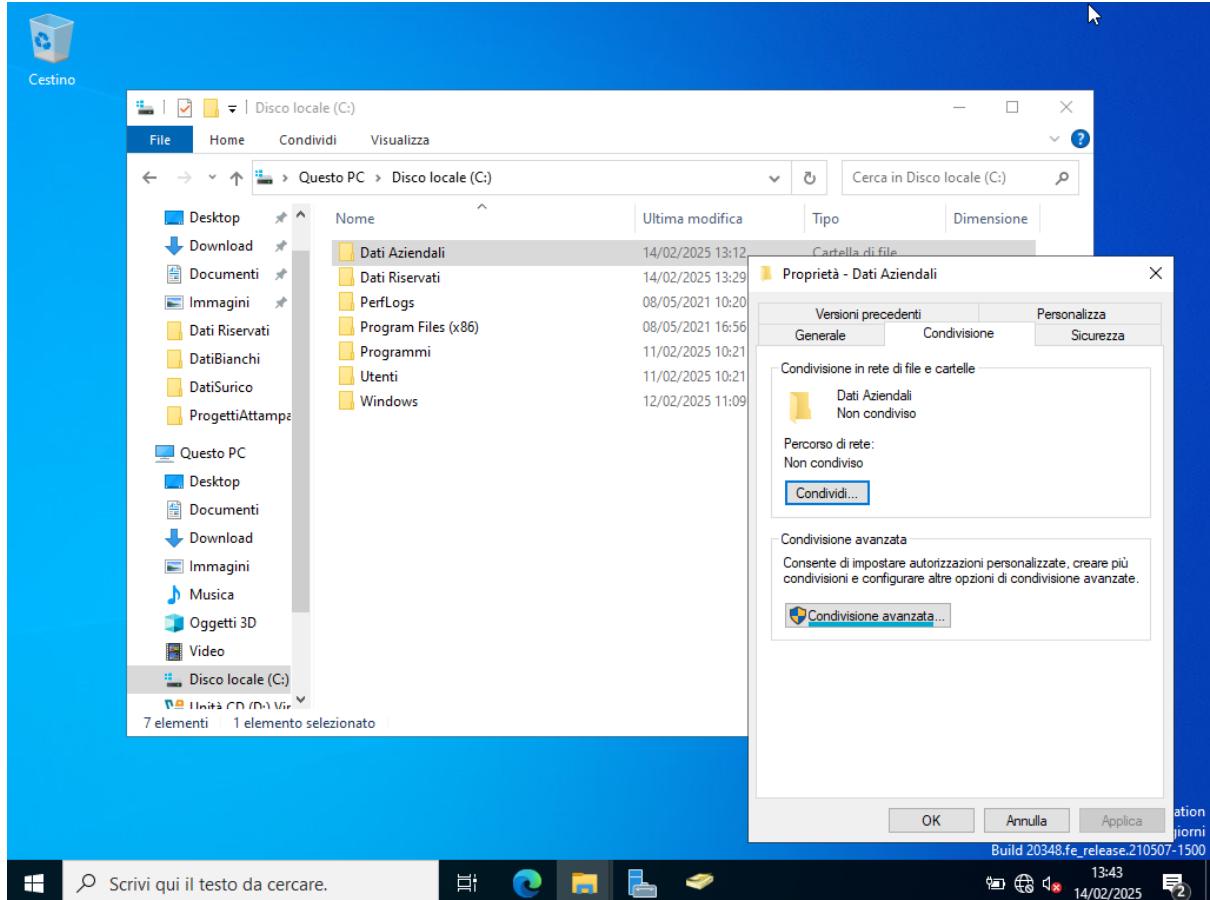


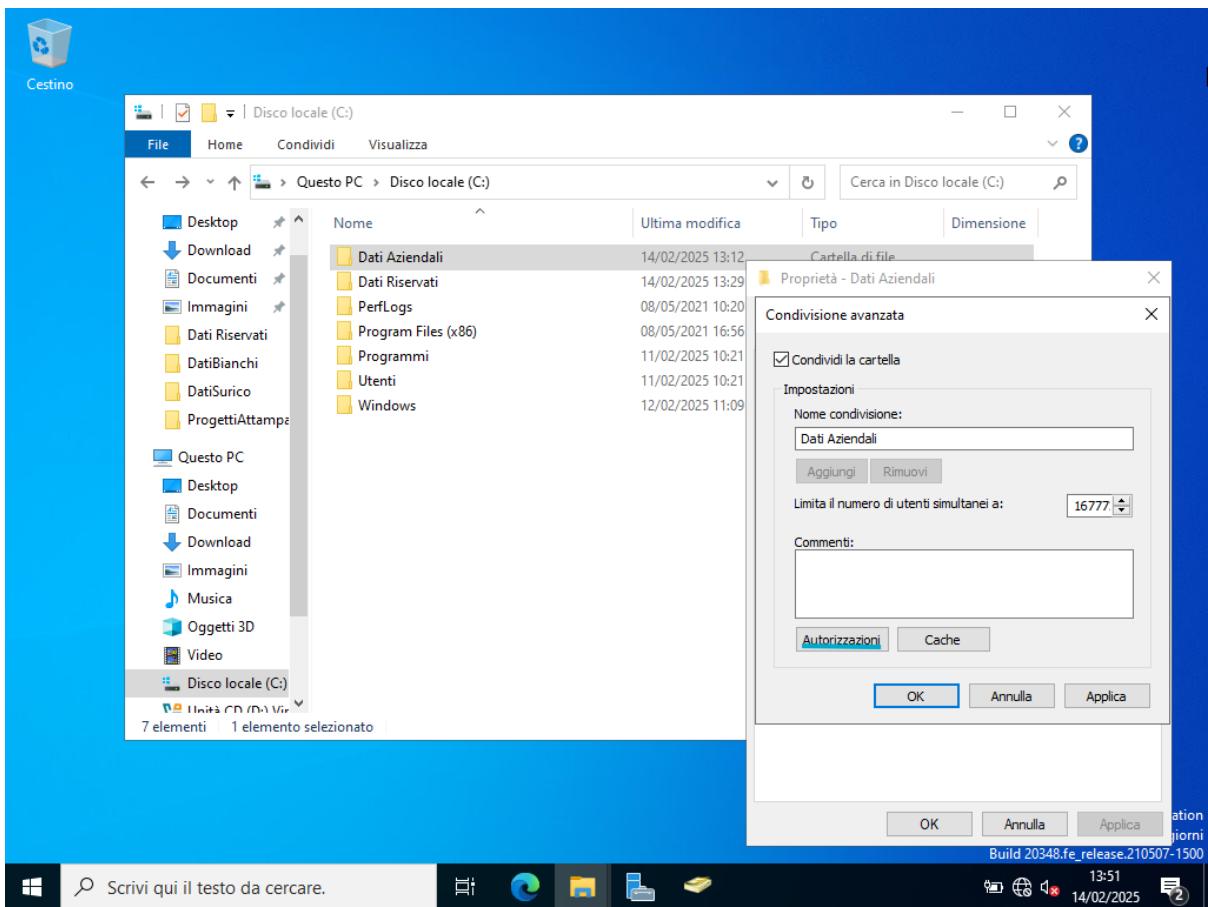
Tornando ai “Dati Riservati” directory riservata allo Staff Amministrativo, ci saranno le seguenti directory con file contenenti informazioni riservate sulla Contabilità, Progetti, Sviluppo.

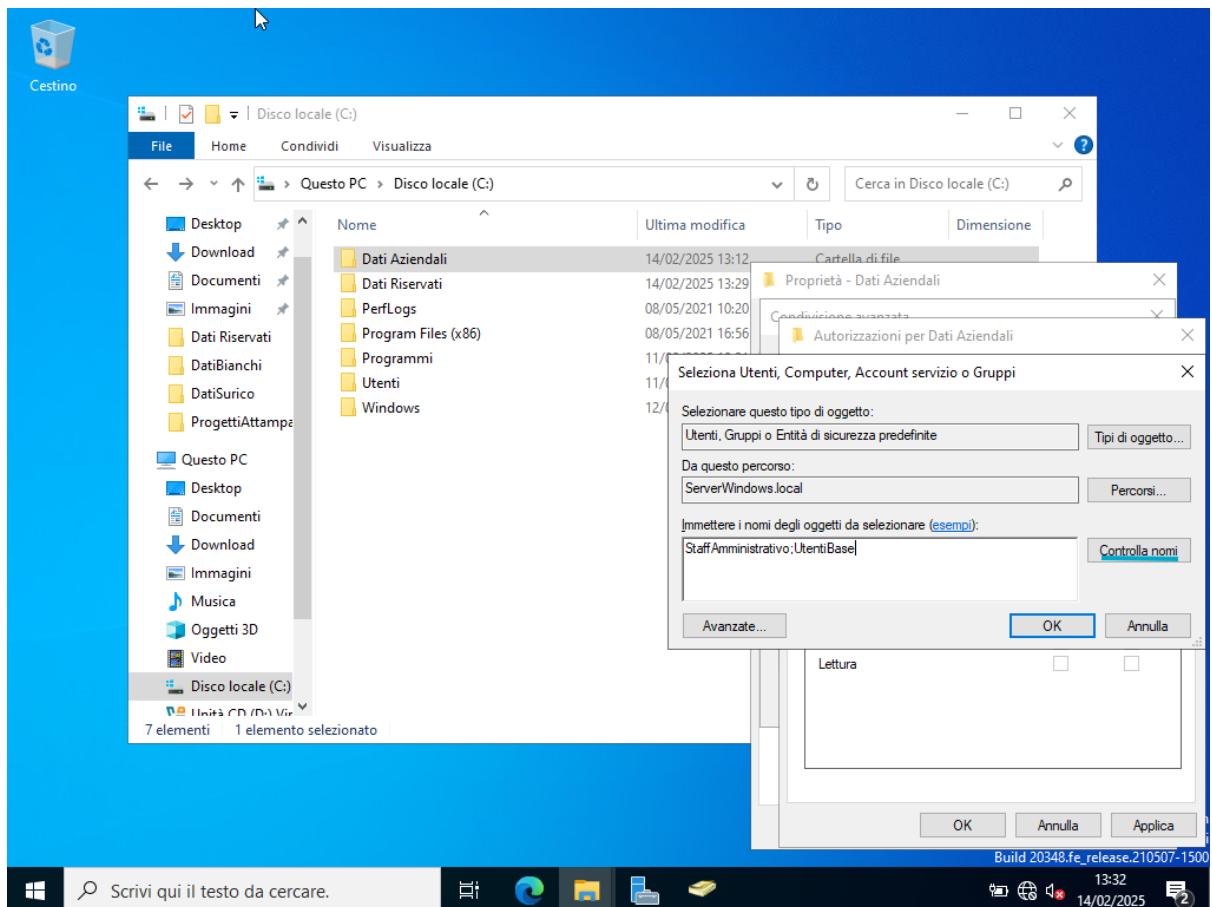


-Creazione e Gestione Policy delle Cartelle/File:

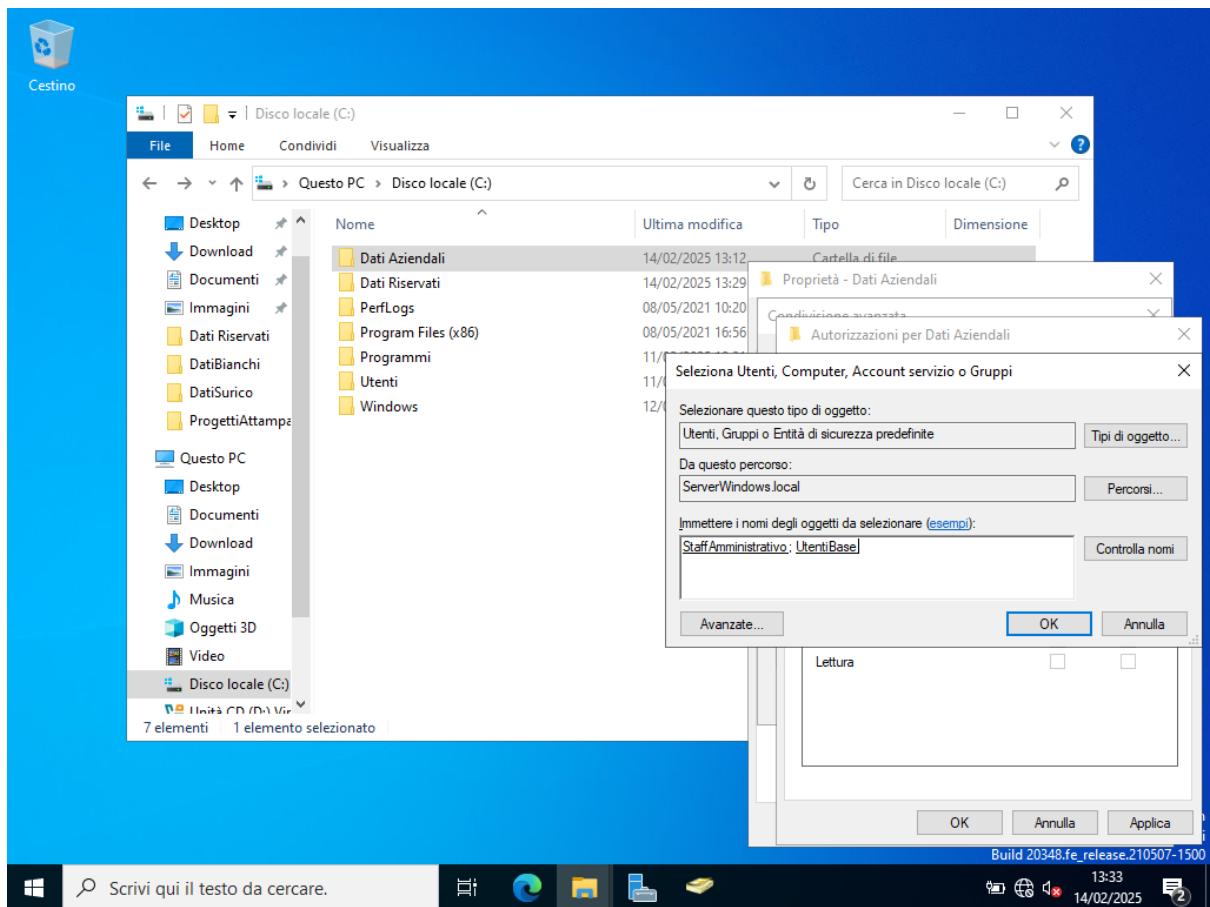
Partendo dalla directory “Dati Aziendali” tutti avranno il permesso di accederci, ma solo al gruppo amministrativo potranno creare e modificare i file all’interno della Directory, gli utenti singoli avranno il permesso di creare e modificare file e cartelle all’interno della loro Directory designata (“DatiBianchi, DatiSurico”).

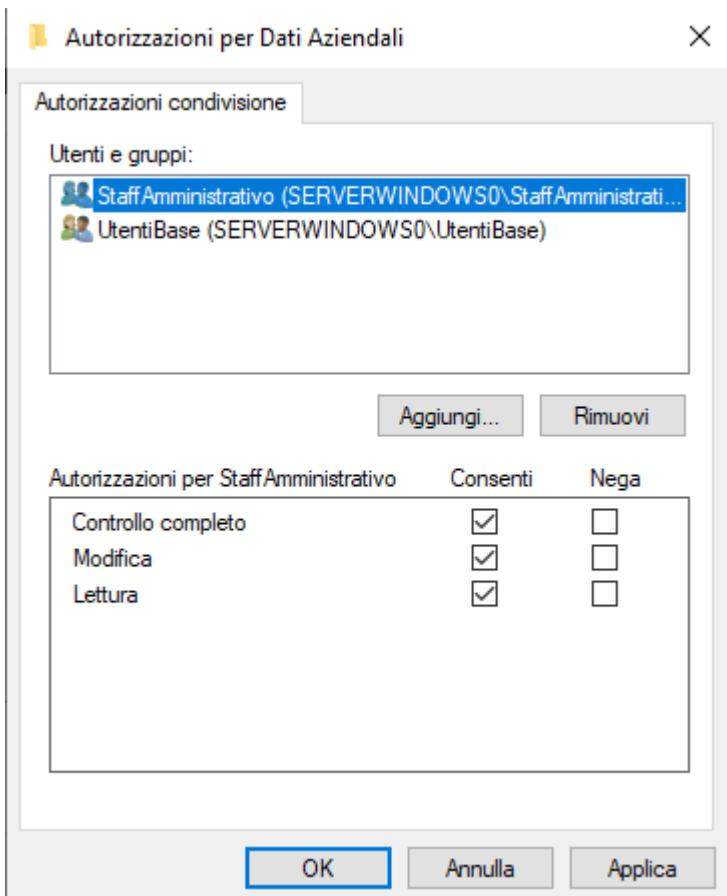


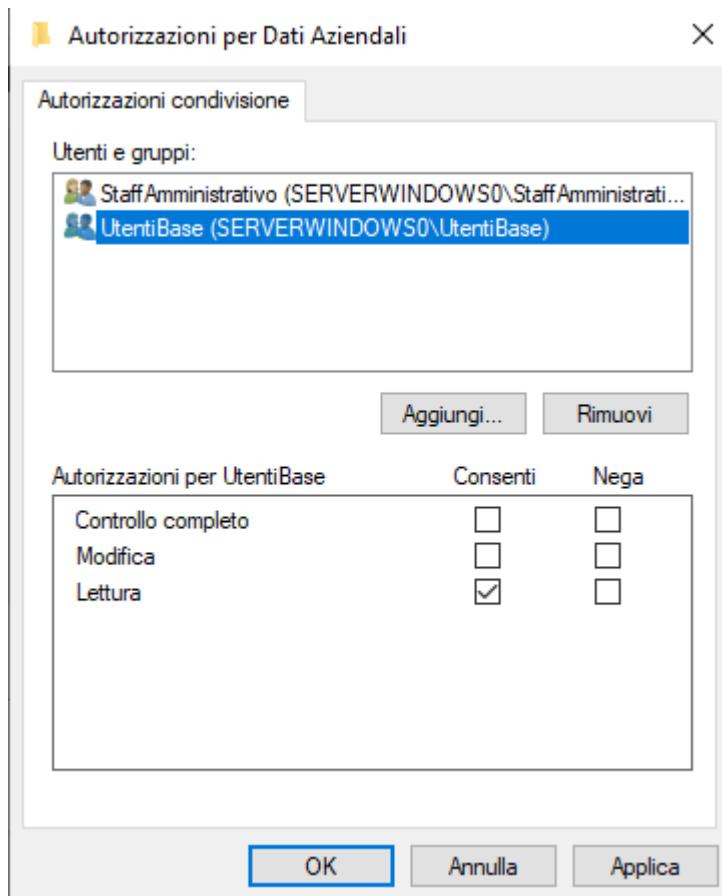




(Check controllo nomi):





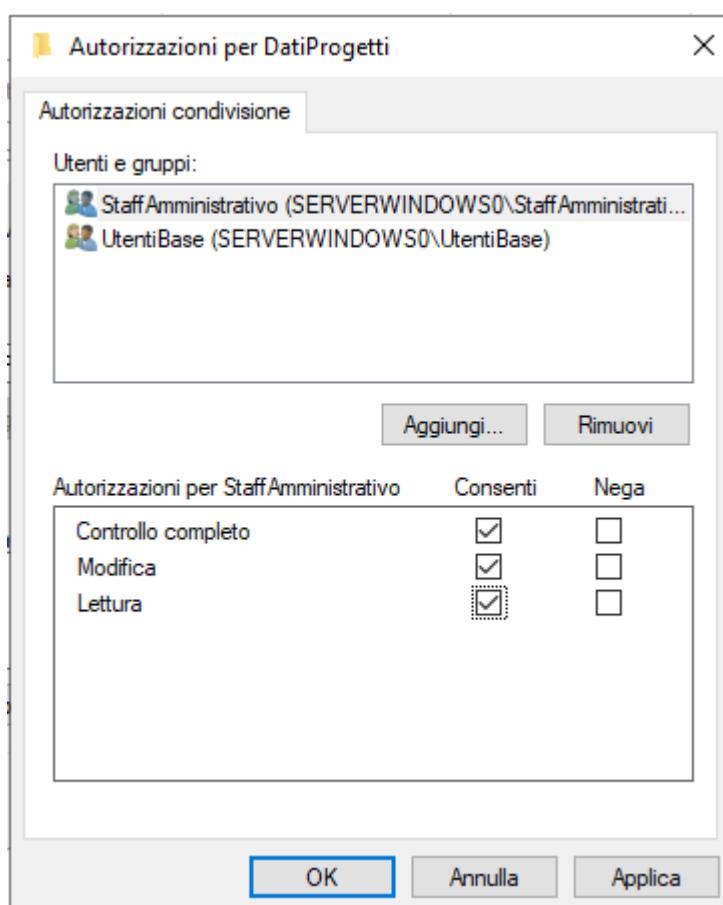
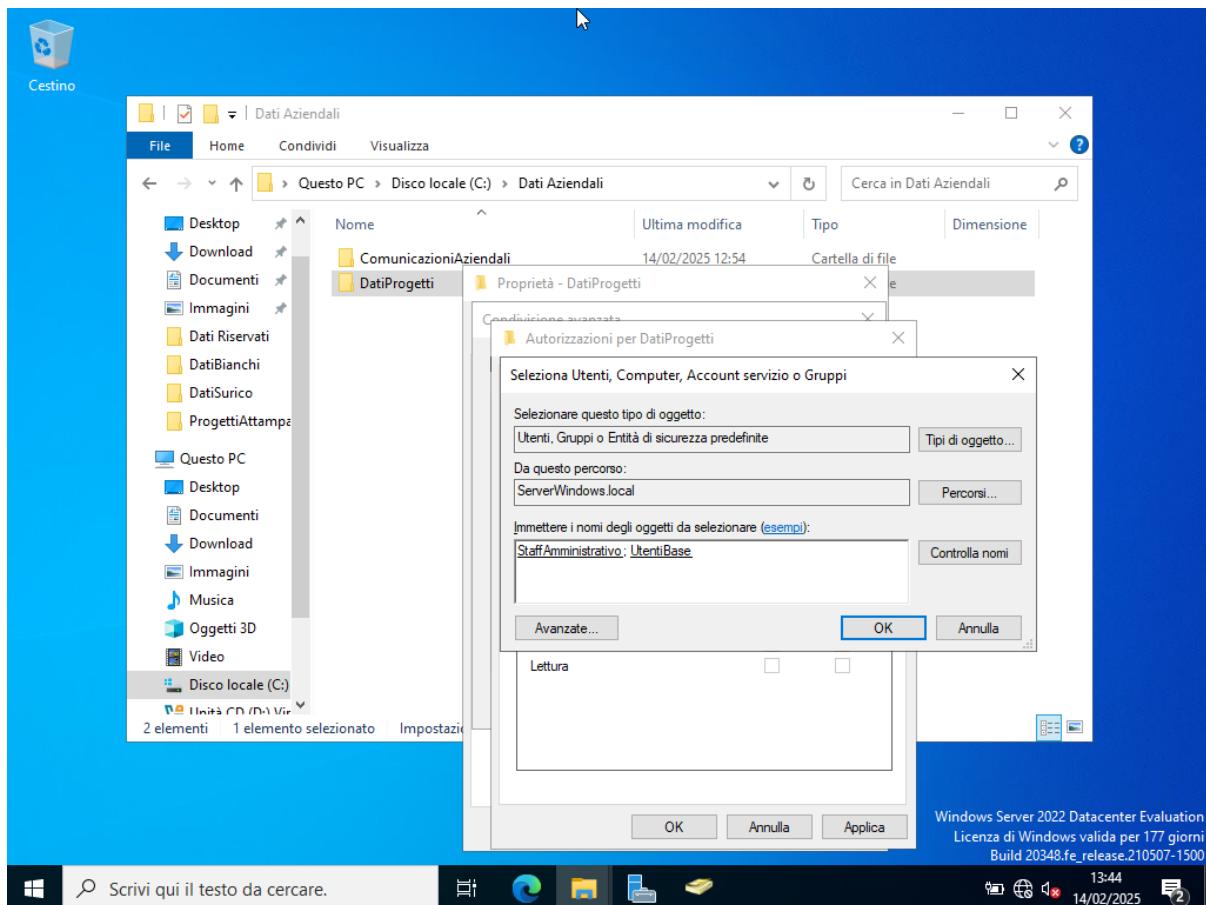


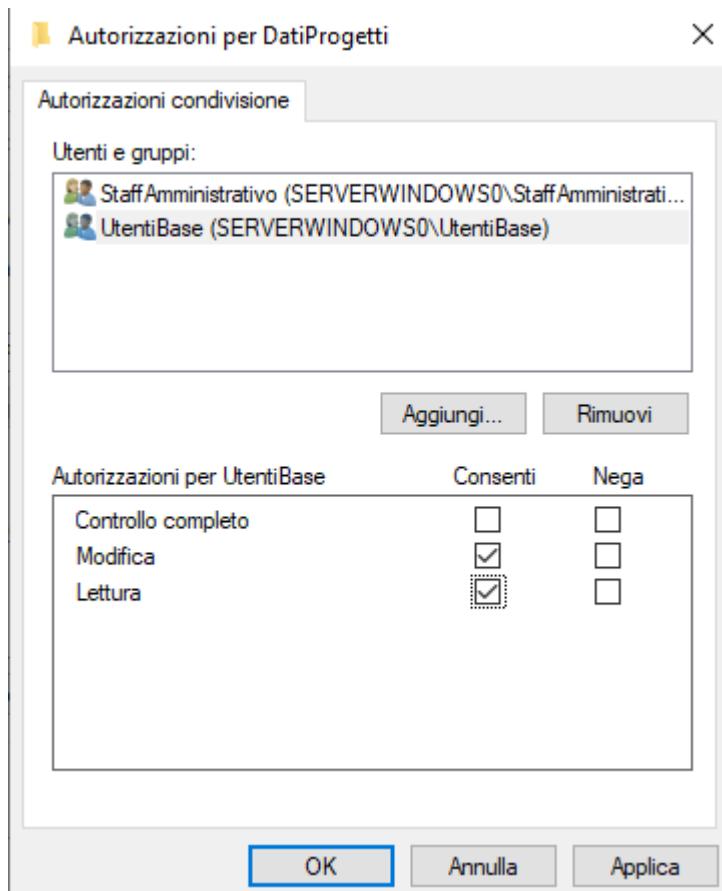
-Permessi Directory “ComunicazioniAziendali / DatiProgetti”:

Andando internamente alla Directory “Dati Aziendali, dobbiamo settare le sottodirectory “ComunicazioniAziendali / DatiProgetti” con permessi differenti.

-ComunicazioniAziendali --> deve essere visibile anche agli UtentiBase ma non potranno modificare il contenuto, mentre lo StaffAmministrativo avranno tutti i permessi.

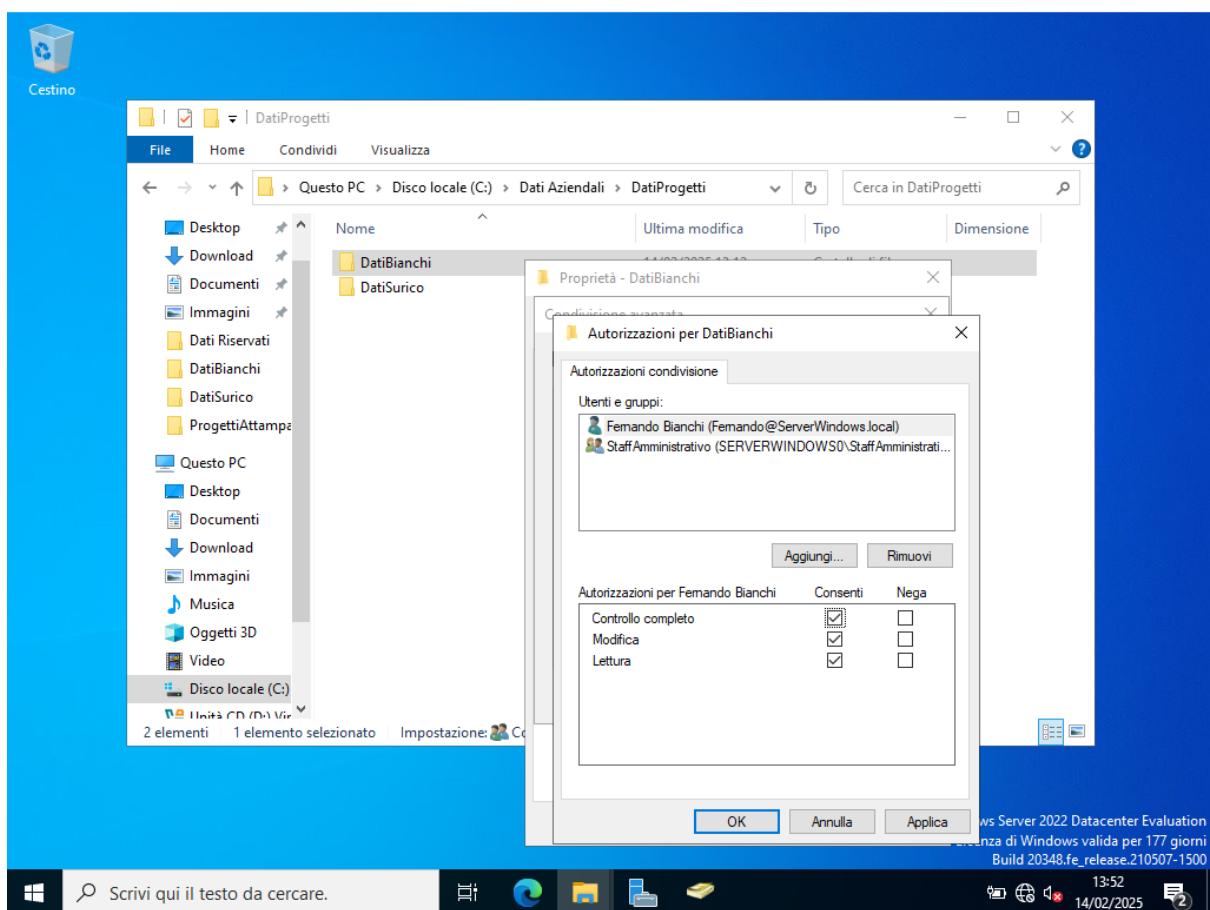
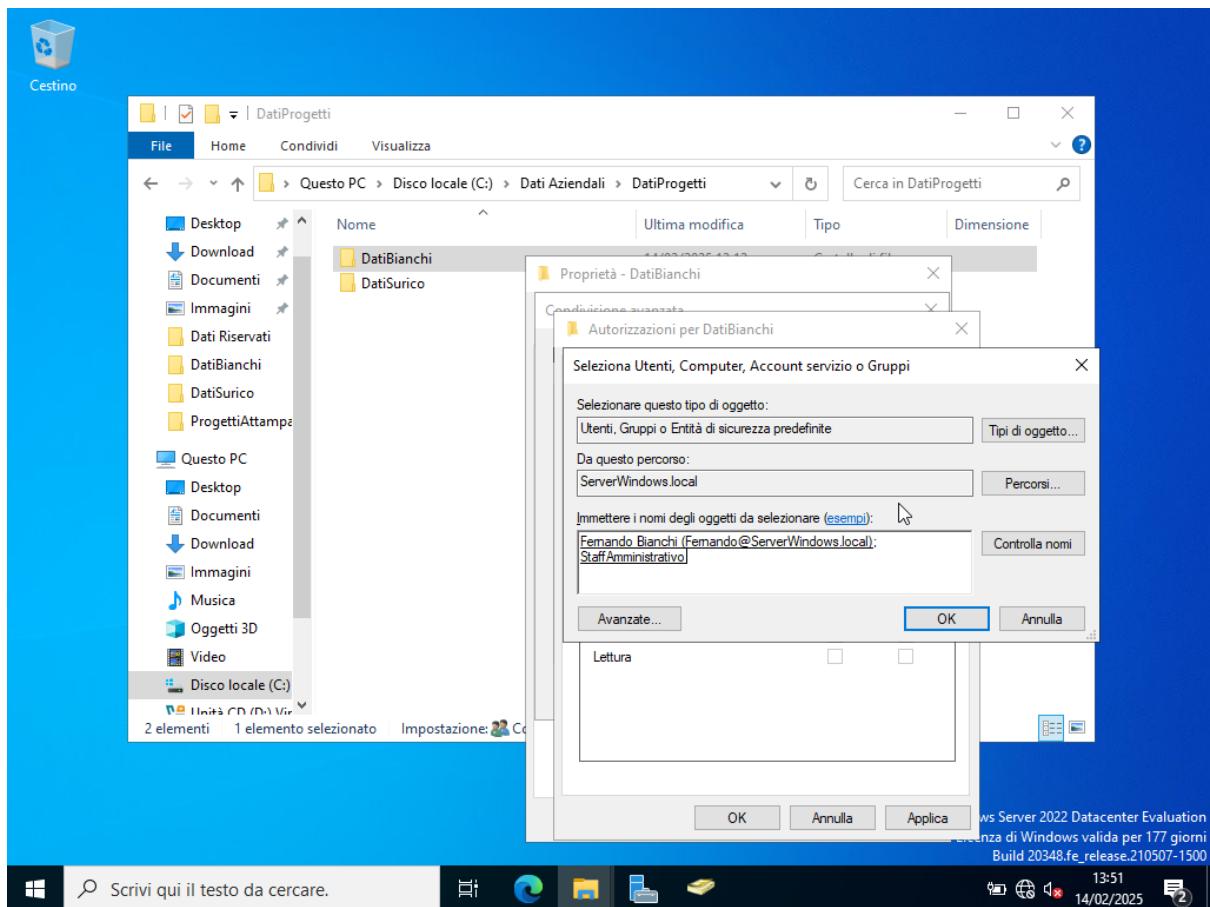
-DatiProgetti --> deve essere visibile e modificabile dagli UtentiBase e per uno scopo di supervisione anche lo StaffAmministrativo avrà i permessi.

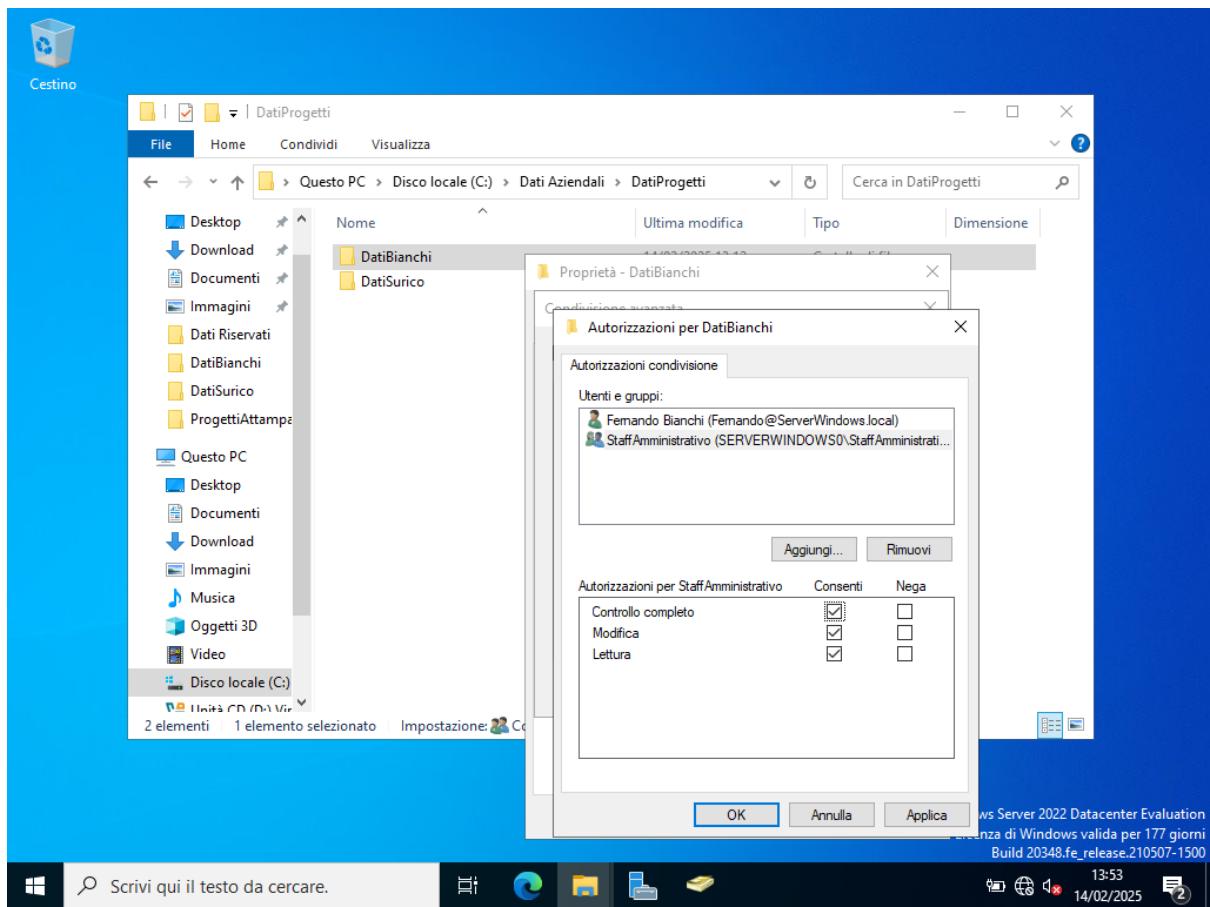




Dentro la cartella DatiProgetti ci saranno le sottocartelle specifiche degli utenti “DatiBianchi / DatiSurico”, queste cartelle sono private dei singoli specifici utenti quindi non potranno essere viste dagli altri utenti base, ma lo staff amministrativo per uno scopo di supervisione avrà poteri di modifica lettura ed esecuzione delle directory.

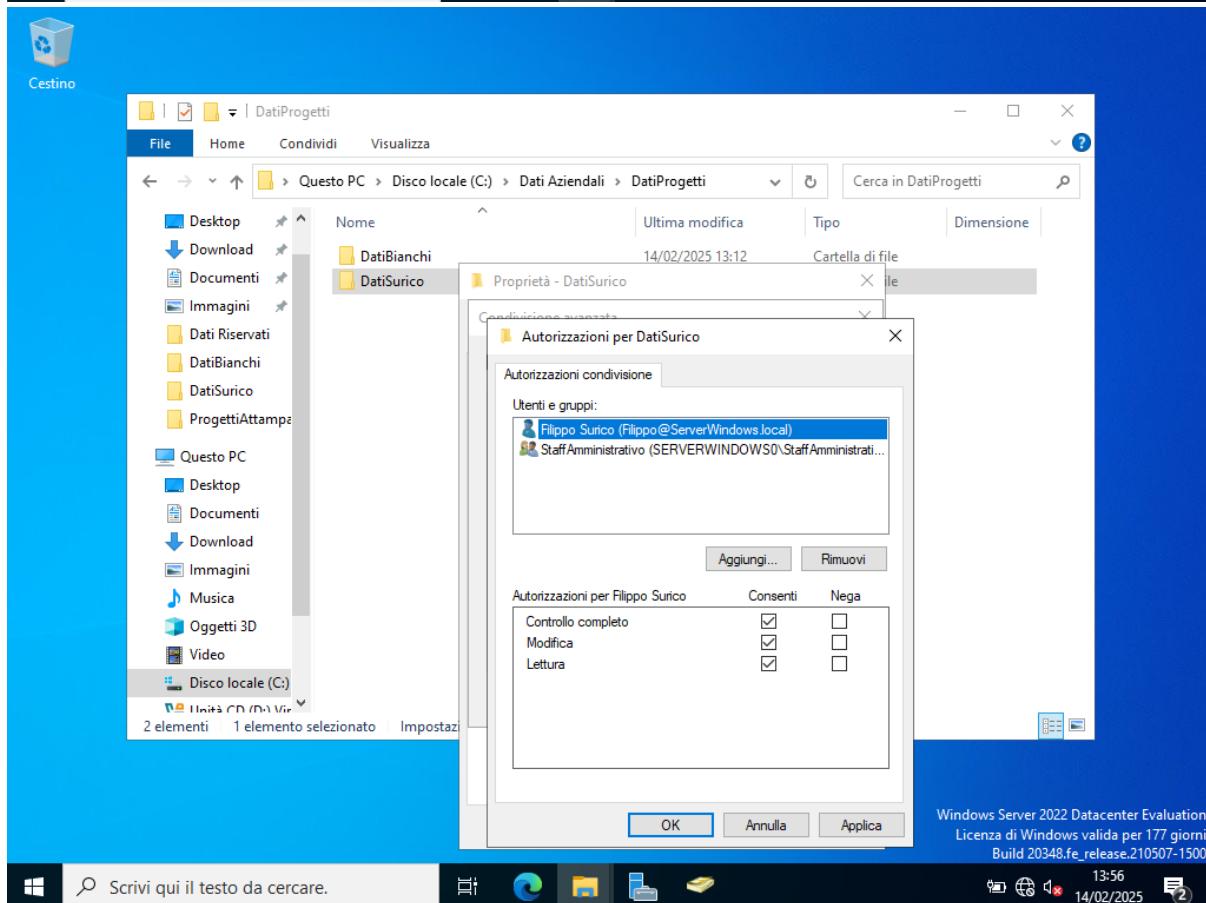
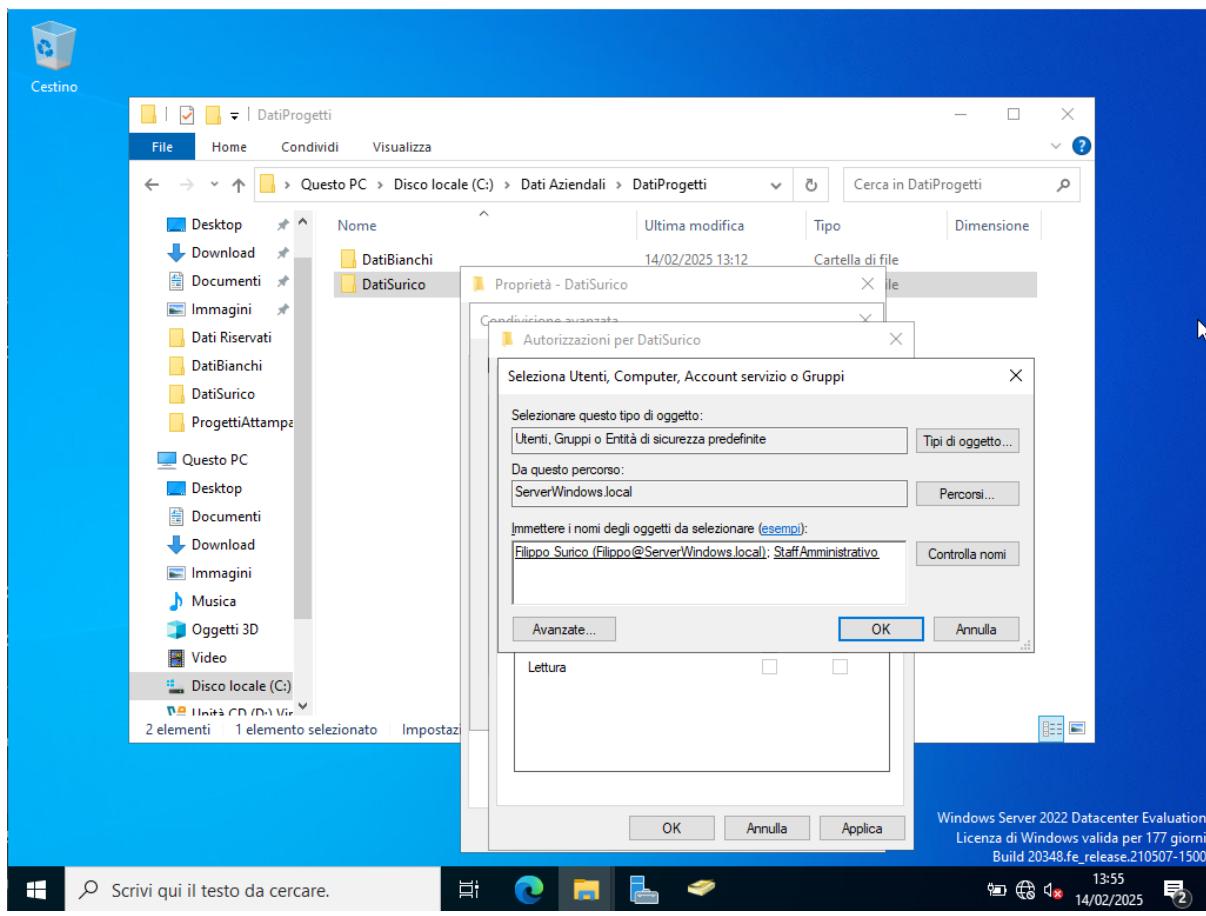
-Directory “DatiBianchi”:

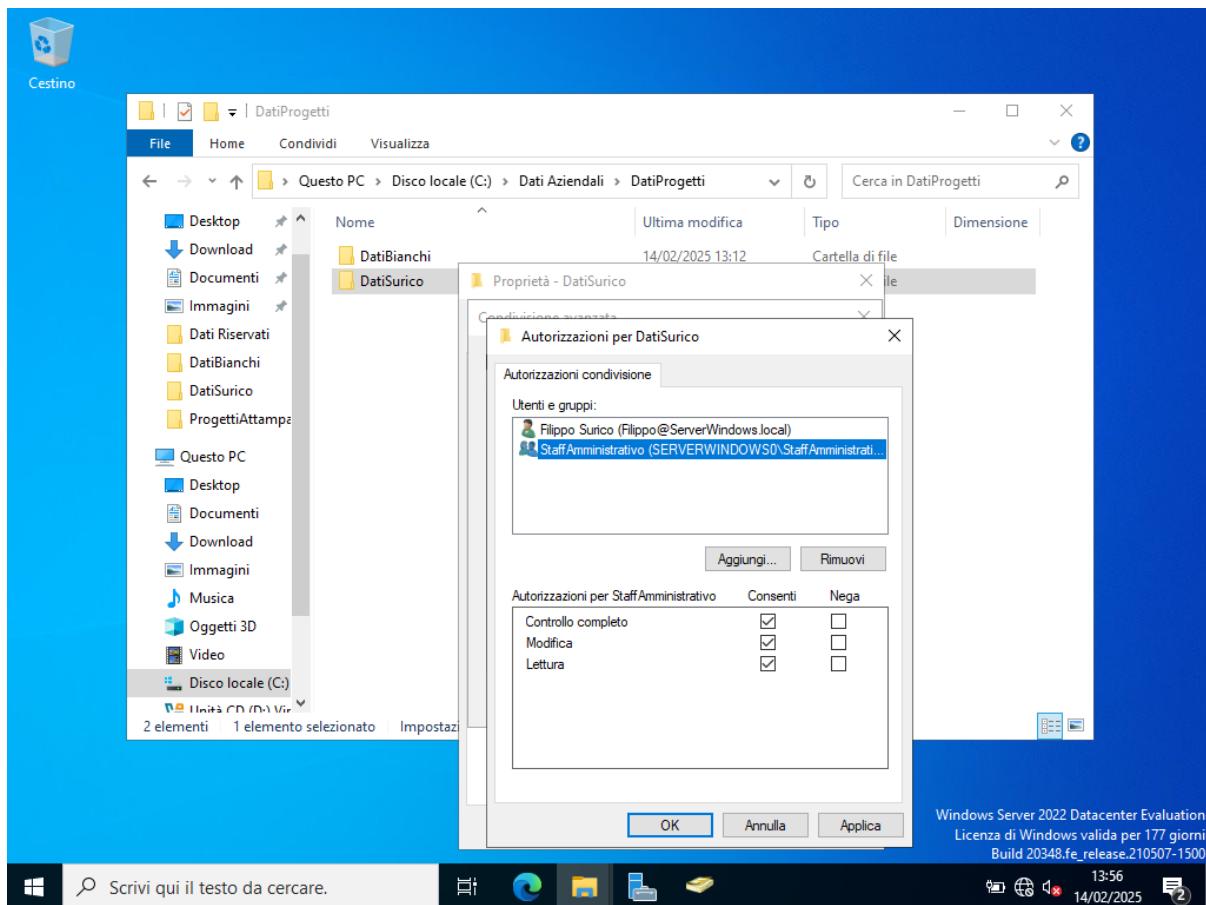




-Directory “DatiSurico”:

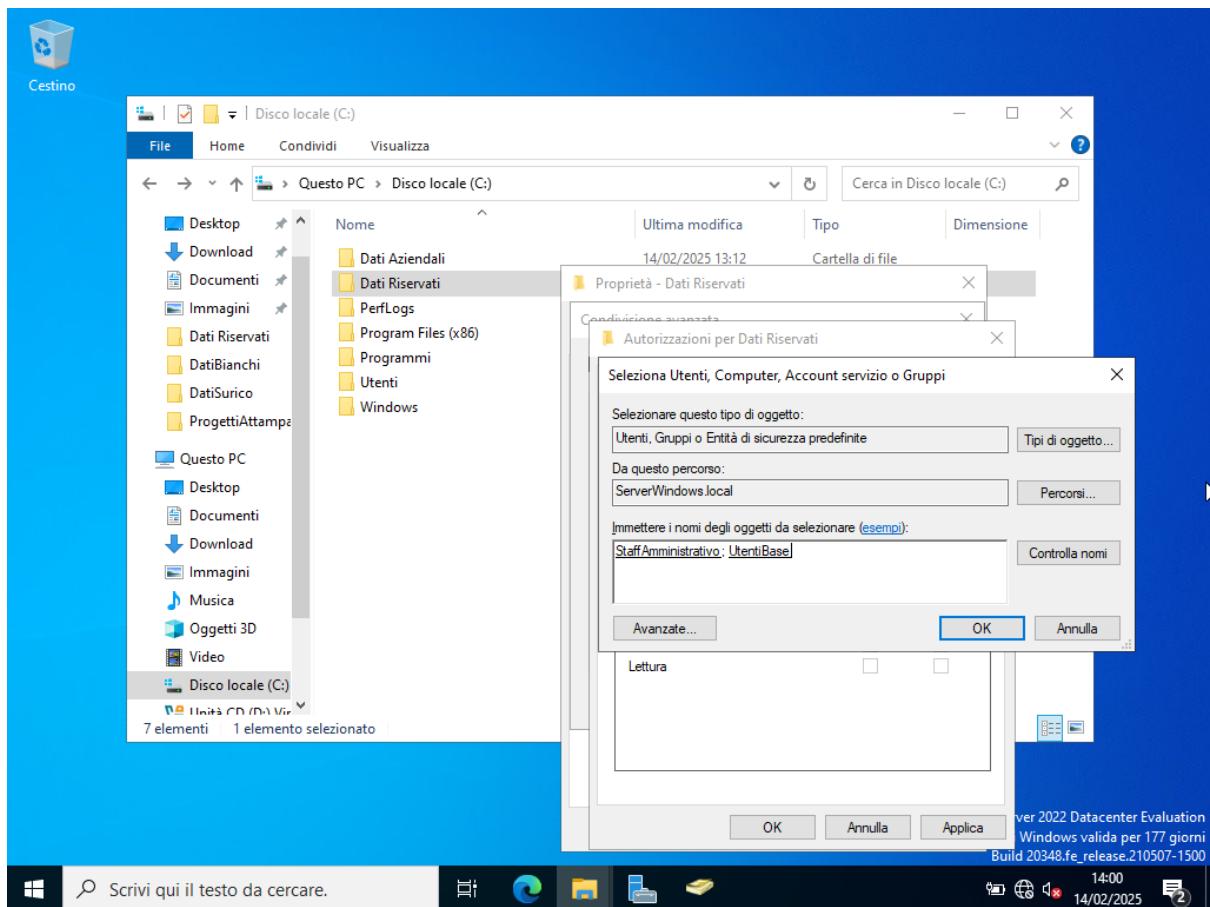
Stesso procedimento precedente:

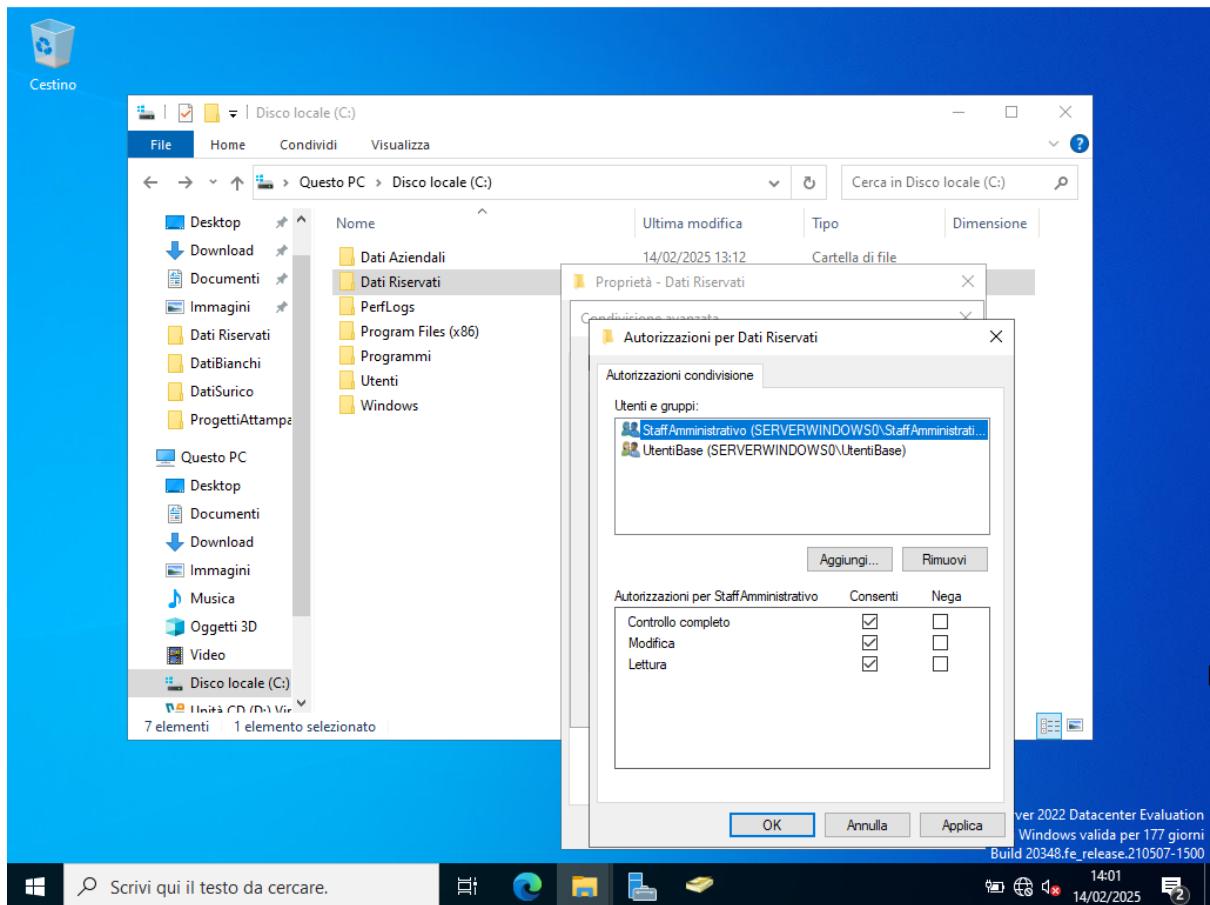


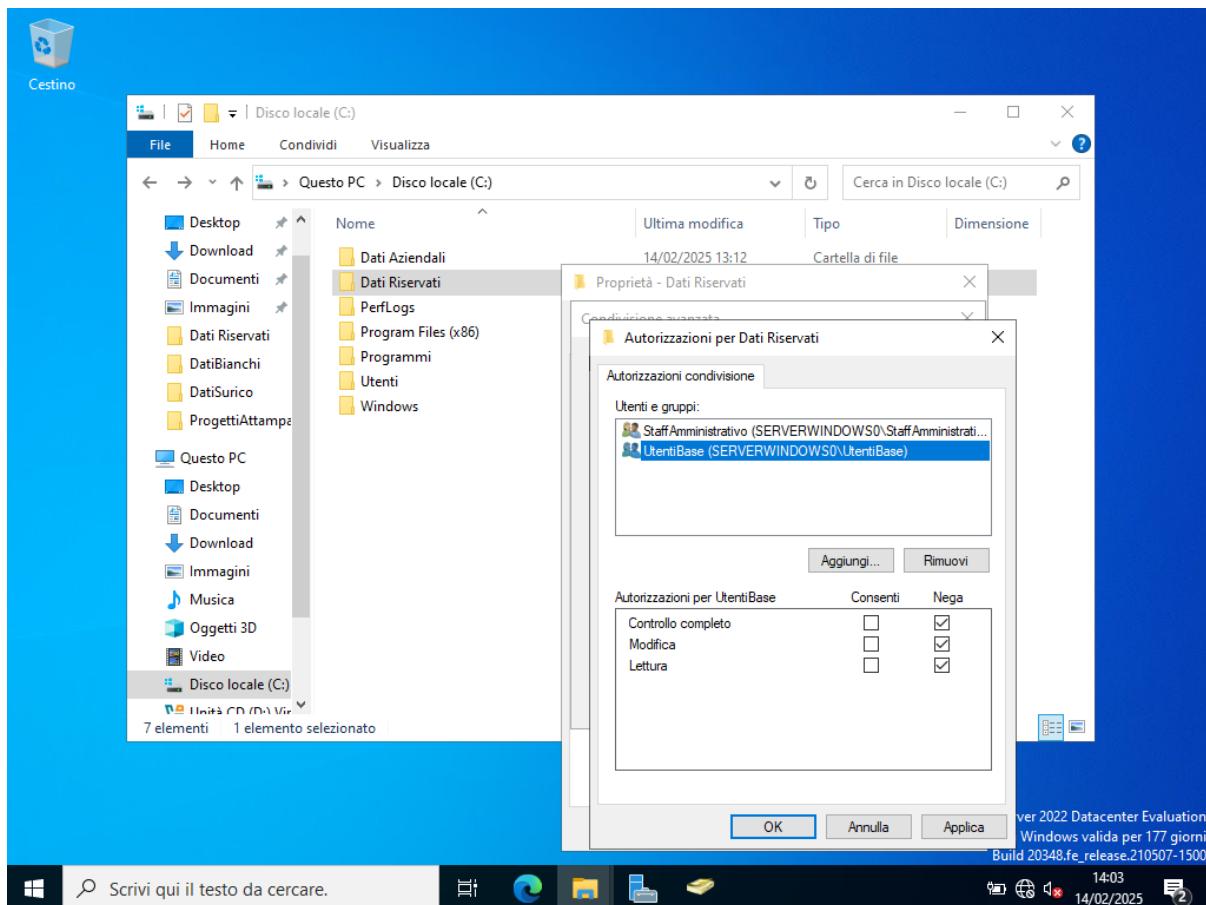


-Directory "Dati Riservati":

Nella directory Dati Riservati sarà accessibile soltanto dallo Staff Amministrativo, che avrà il permesso di leggere, modificare ed eseguire file/directory all'interno di essa. Gli UtentiBase non avranno alcun permesso di accesso alla directory.

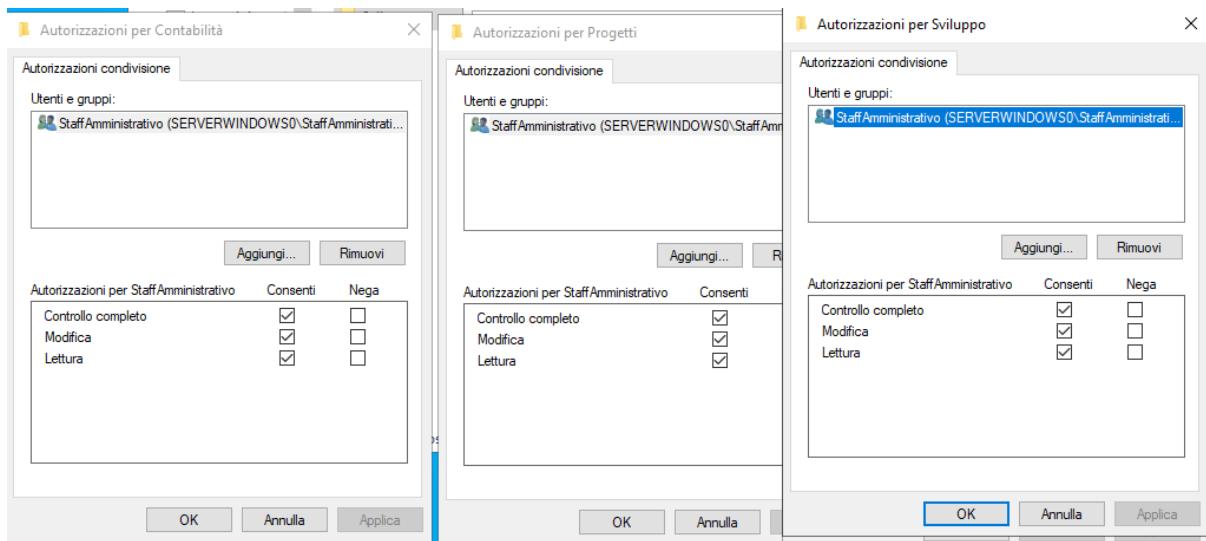






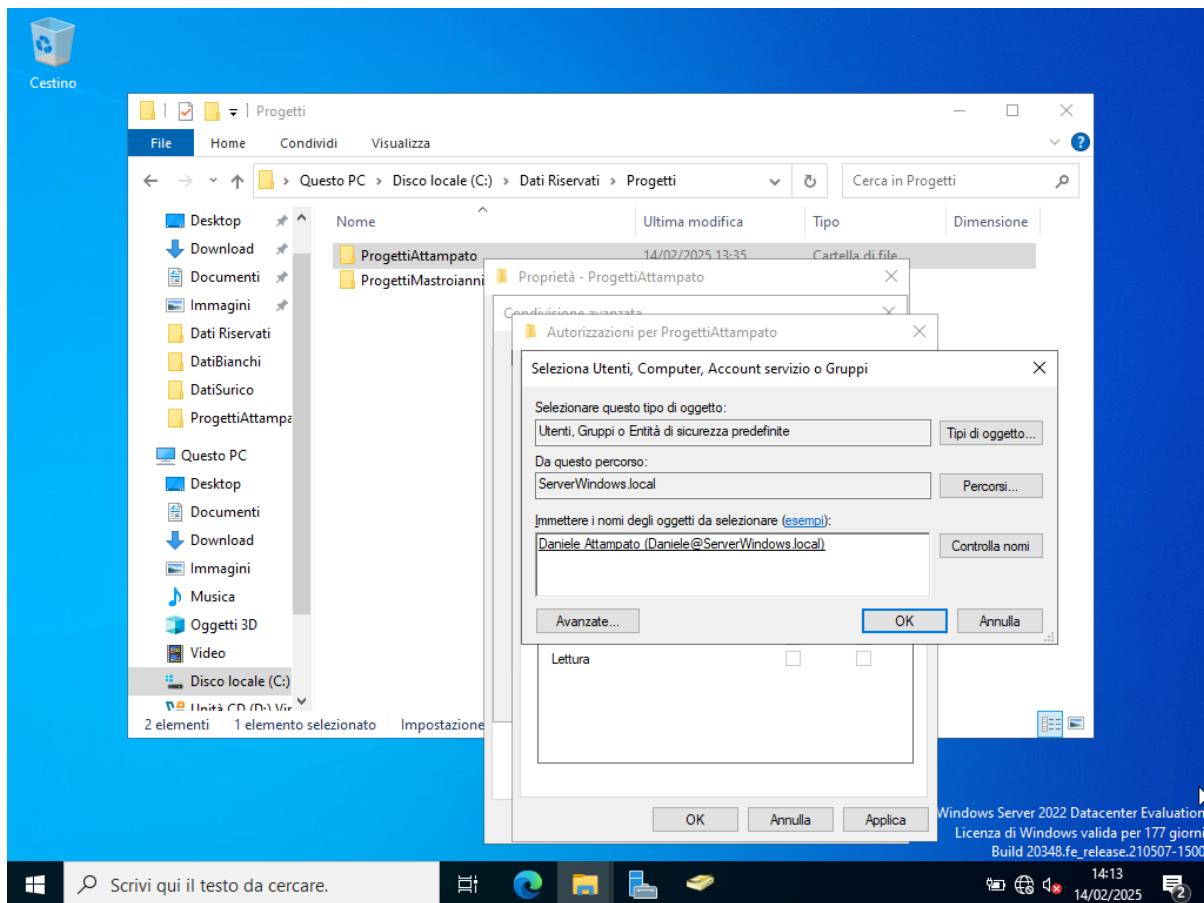
-Directory “Contabilità / Progetti / Sviluppo”:

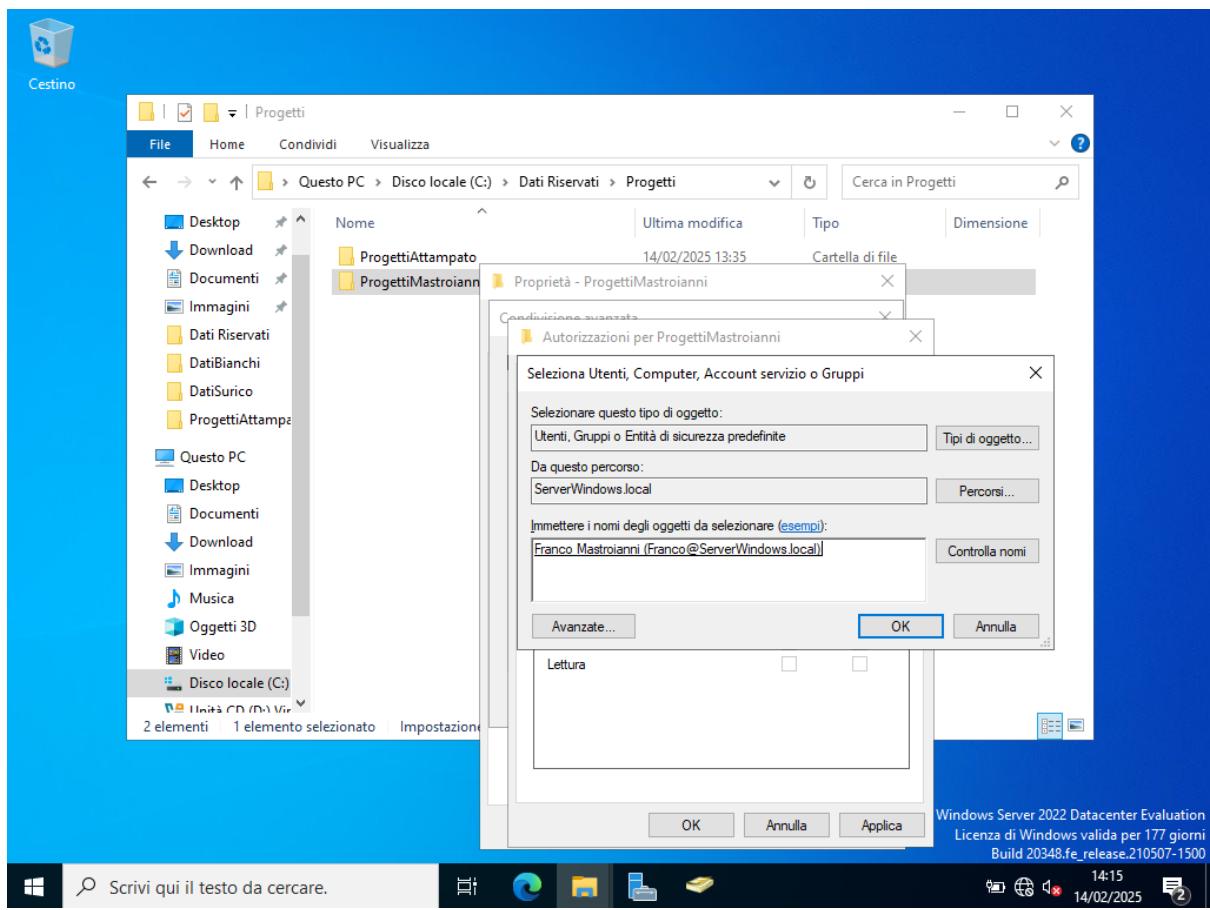
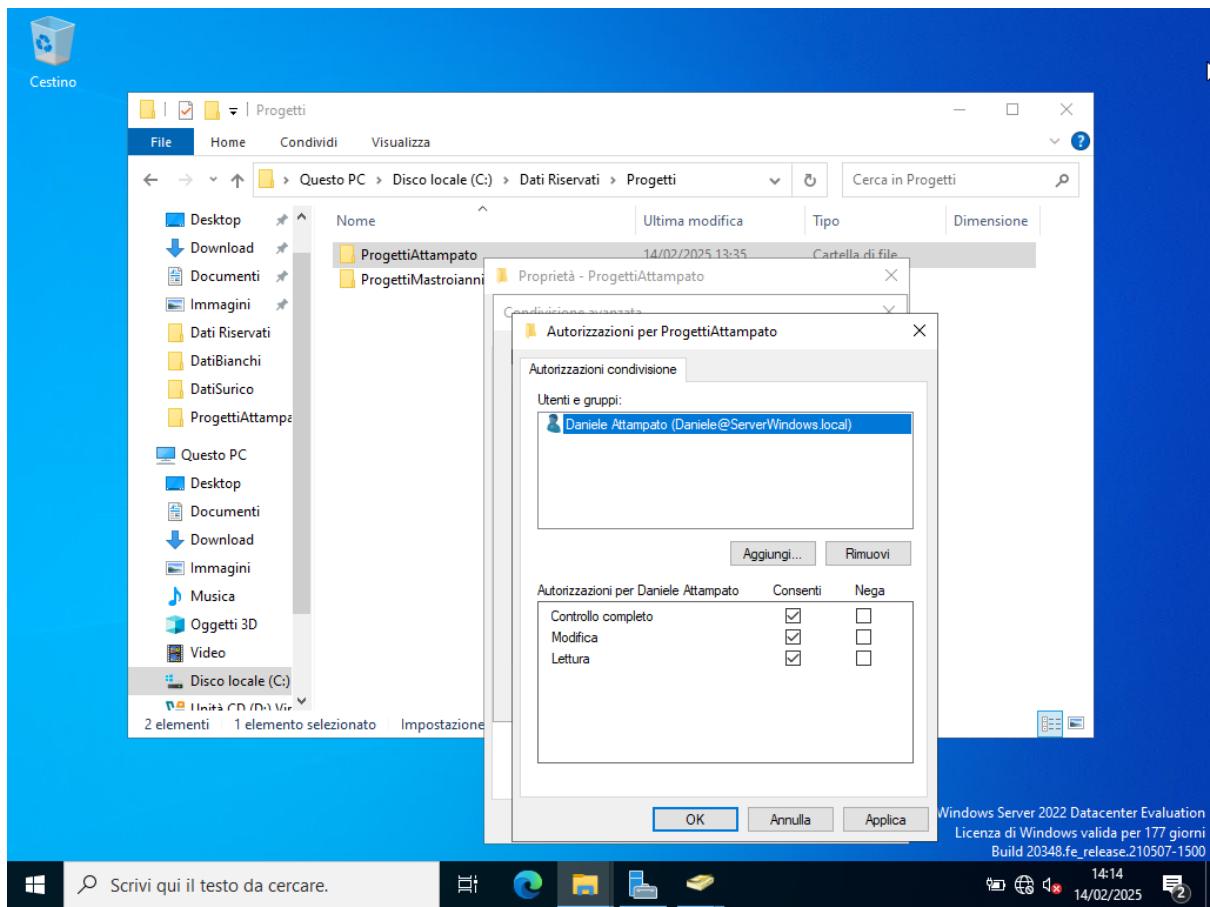
In queste Directory andiamo a settare i permessi di lettura, scrittura, esecuzione allo Staff Amministrativo.

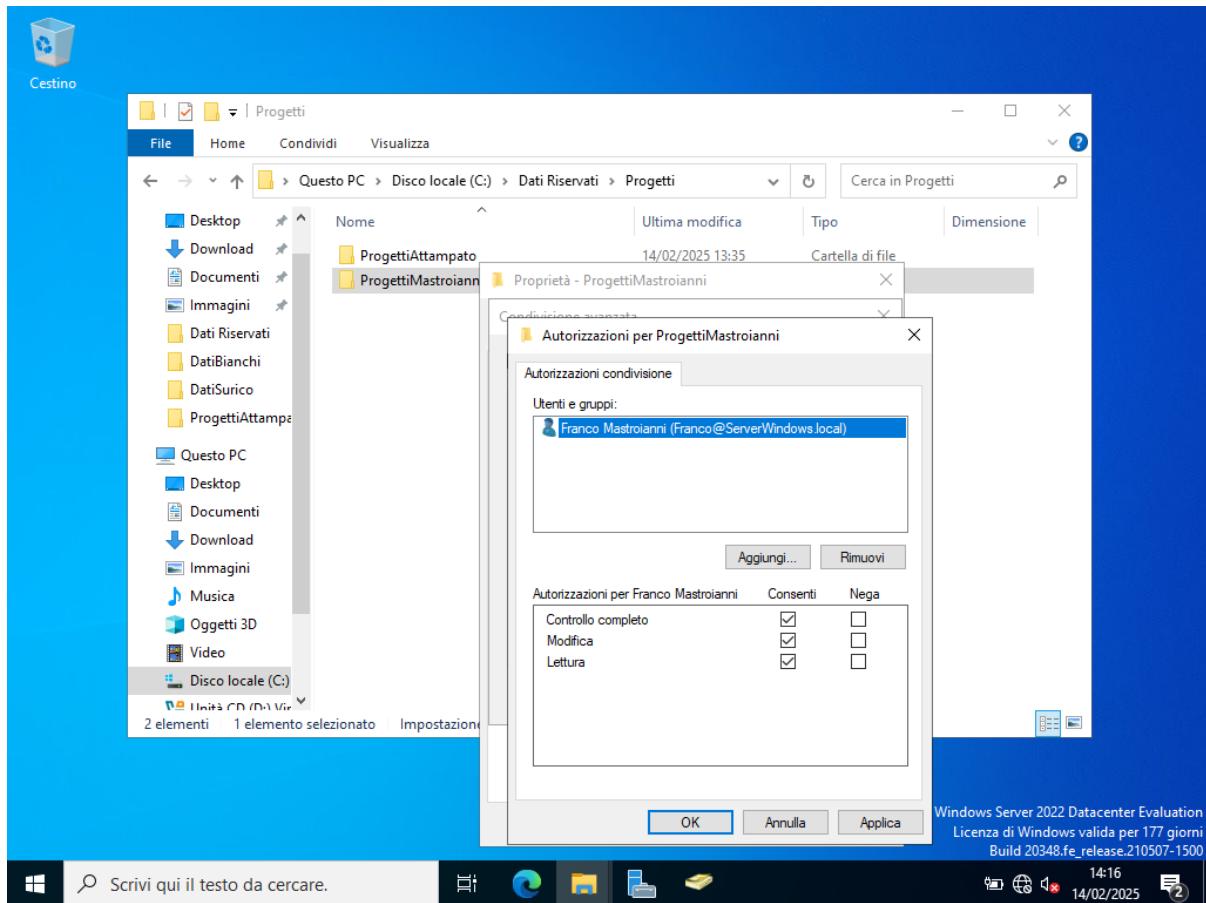


-Directory “ProgettiAttampato /ProgettiMastroianni”:

Queste Directory sono private per gli utenti specifici dello Staff Amministrativo quindi soltanto gli utenti proprietari potranno accederci.







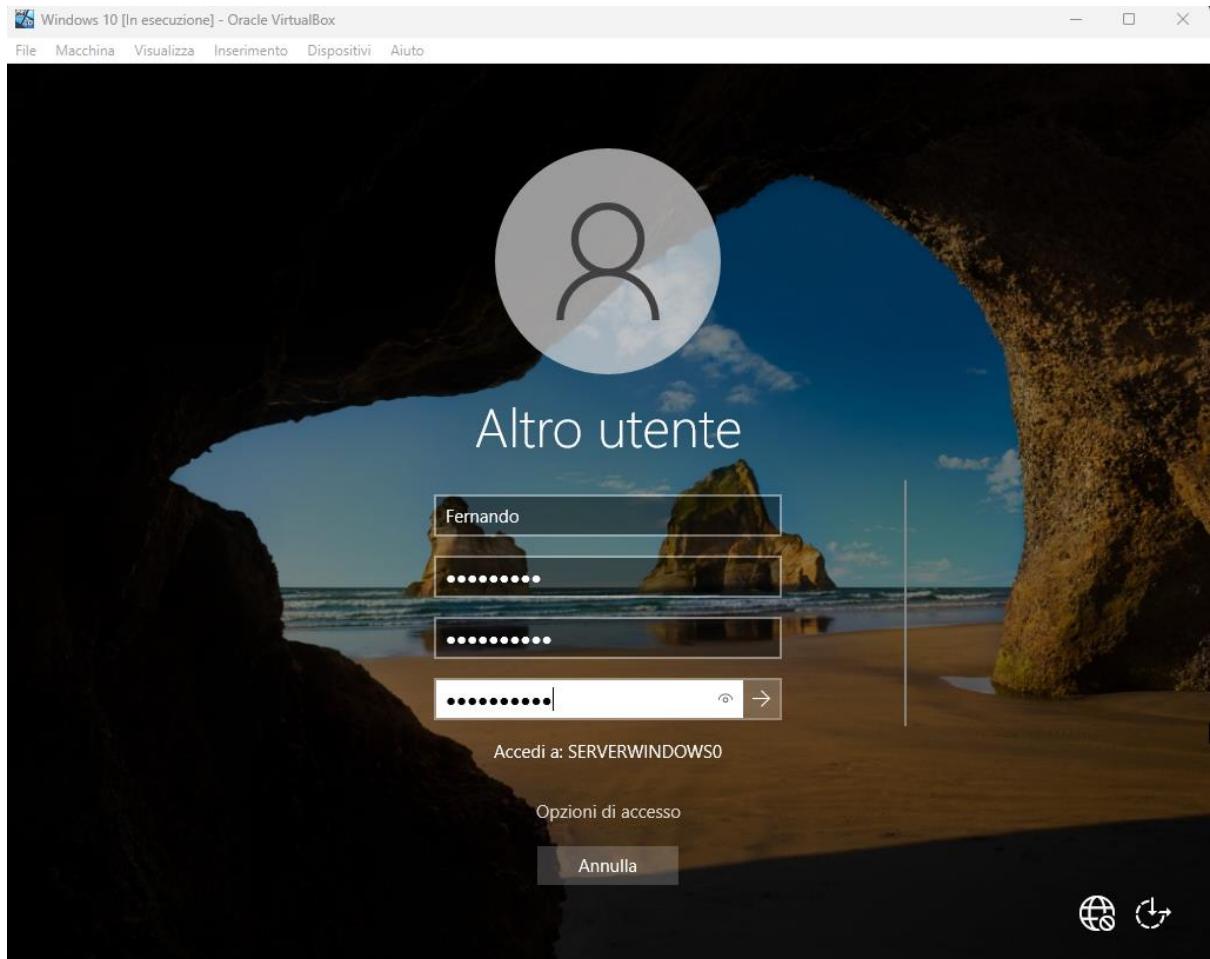
Tutti i permessi ora sono stati settati.

-Test Policy di Sicurezza Aziendale:

Per testare che il tutto è stato configurato correttamente, proverò dalla macchina Windows 10 Pro, ad accedere con due utenti: "Daniele" che fa parte dello StaffAmministrativo e "Fernando" che fa parte degli UtentiBase.

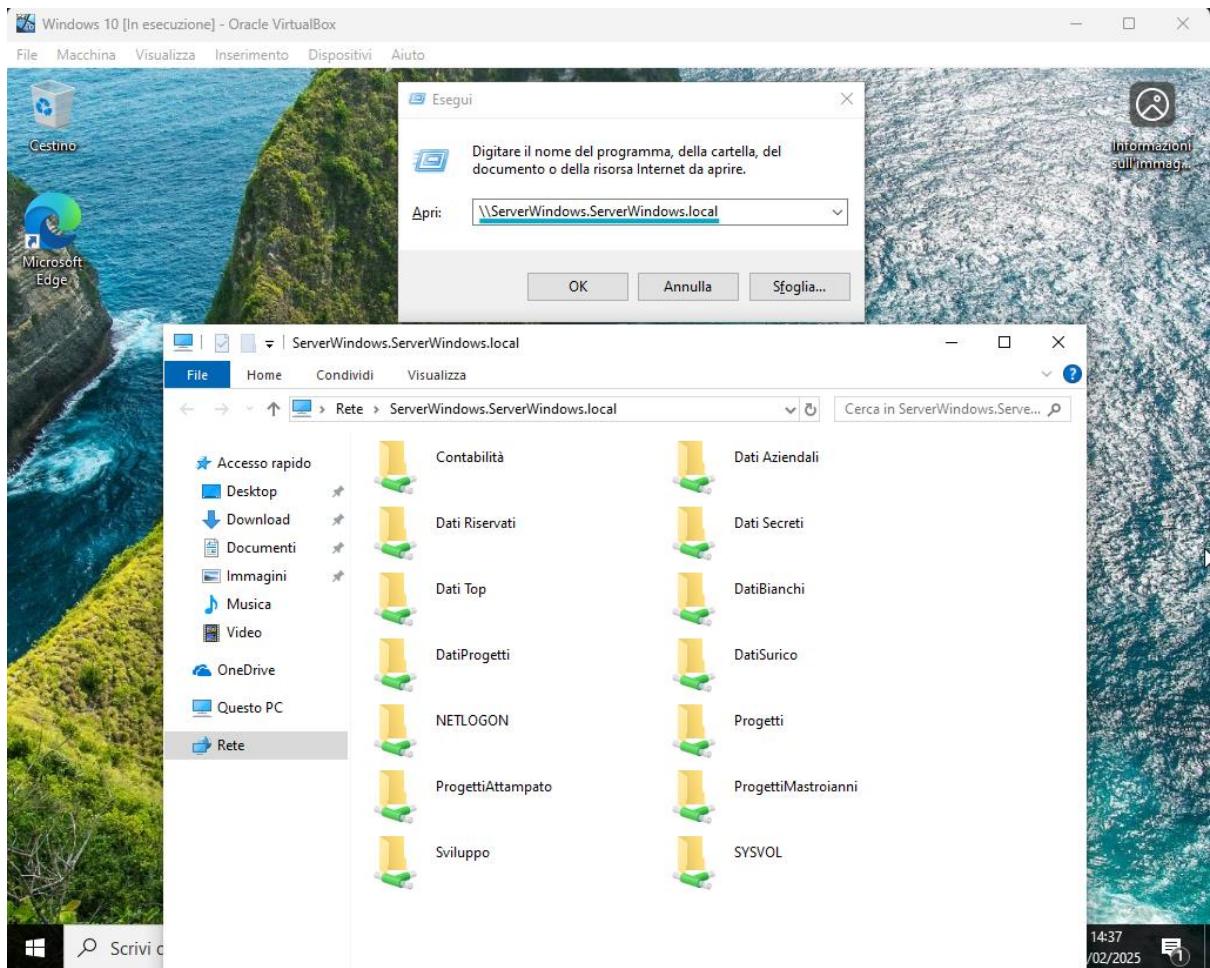
-Test UtenteBase "Fernando":

Da Windows 10 andiamo ad effettuare il 1* login con l'utente, il sistema ci chiederà di modificare la password:

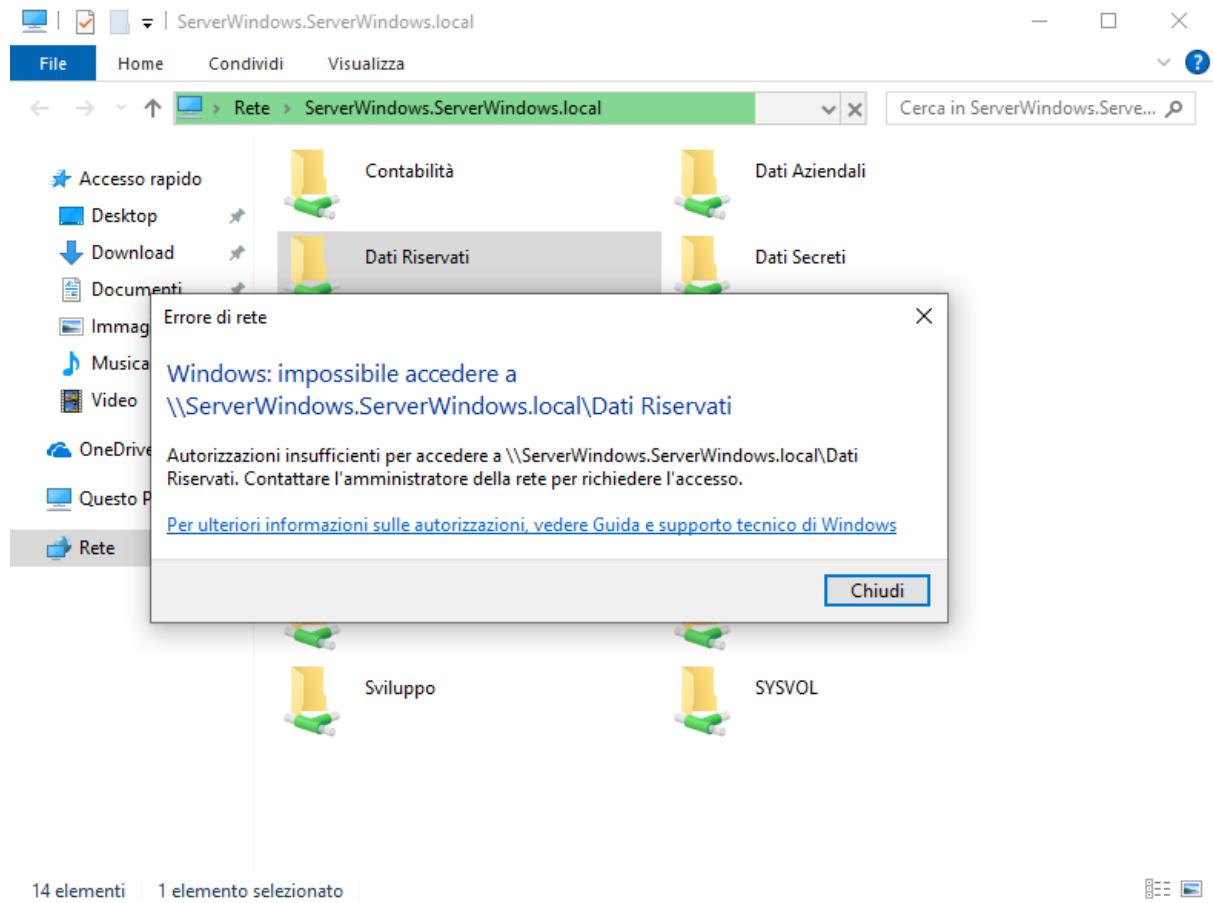


(La Macchina Windows 10 è già settata con il domino e l'indirizzo ip nella stessa rete della macchina Windows Server "192.168.1.11").

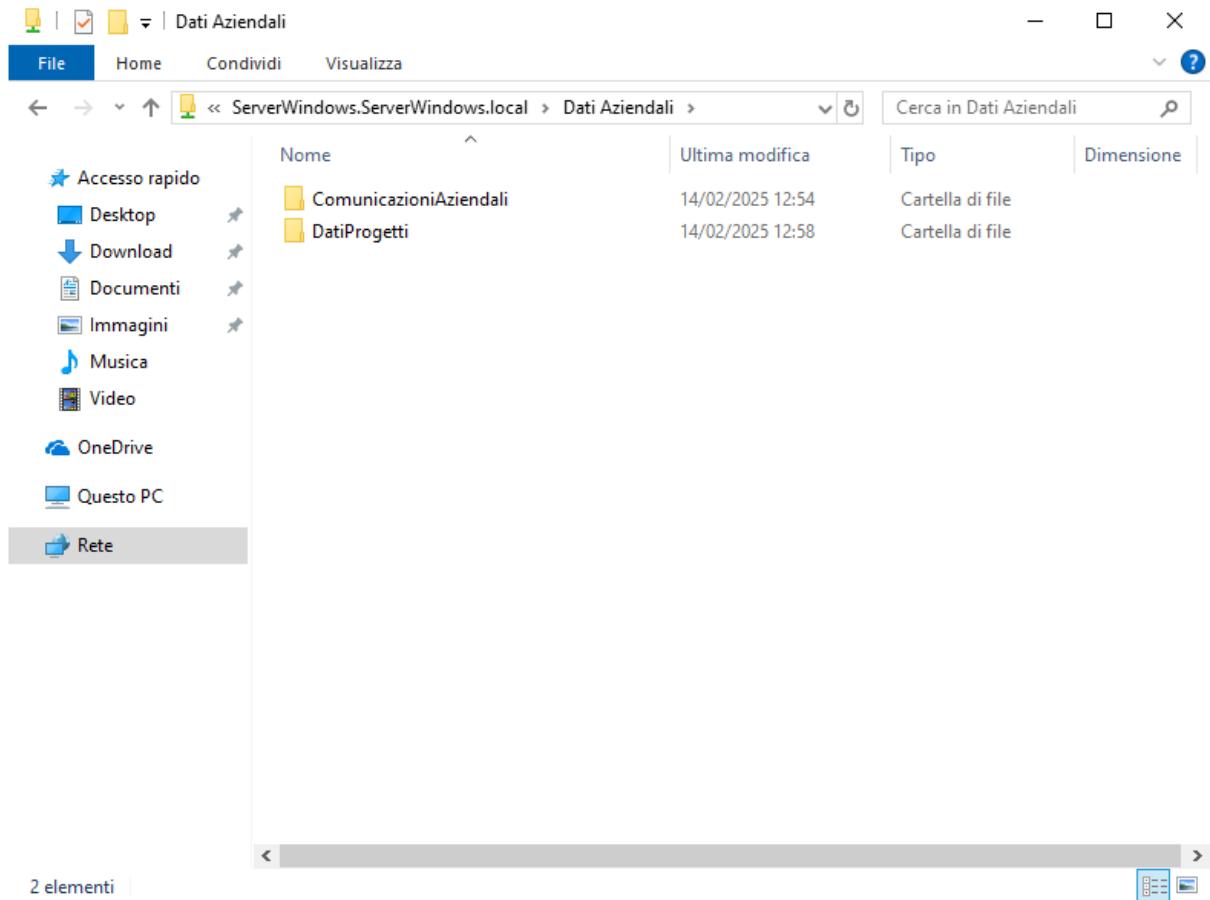
Per accedere alla directory di rete dalla barra di ricerca cerchiamo “Esegui” e inseriamo il percorso del Server, \\ServerWindows.ServerWindows.local .



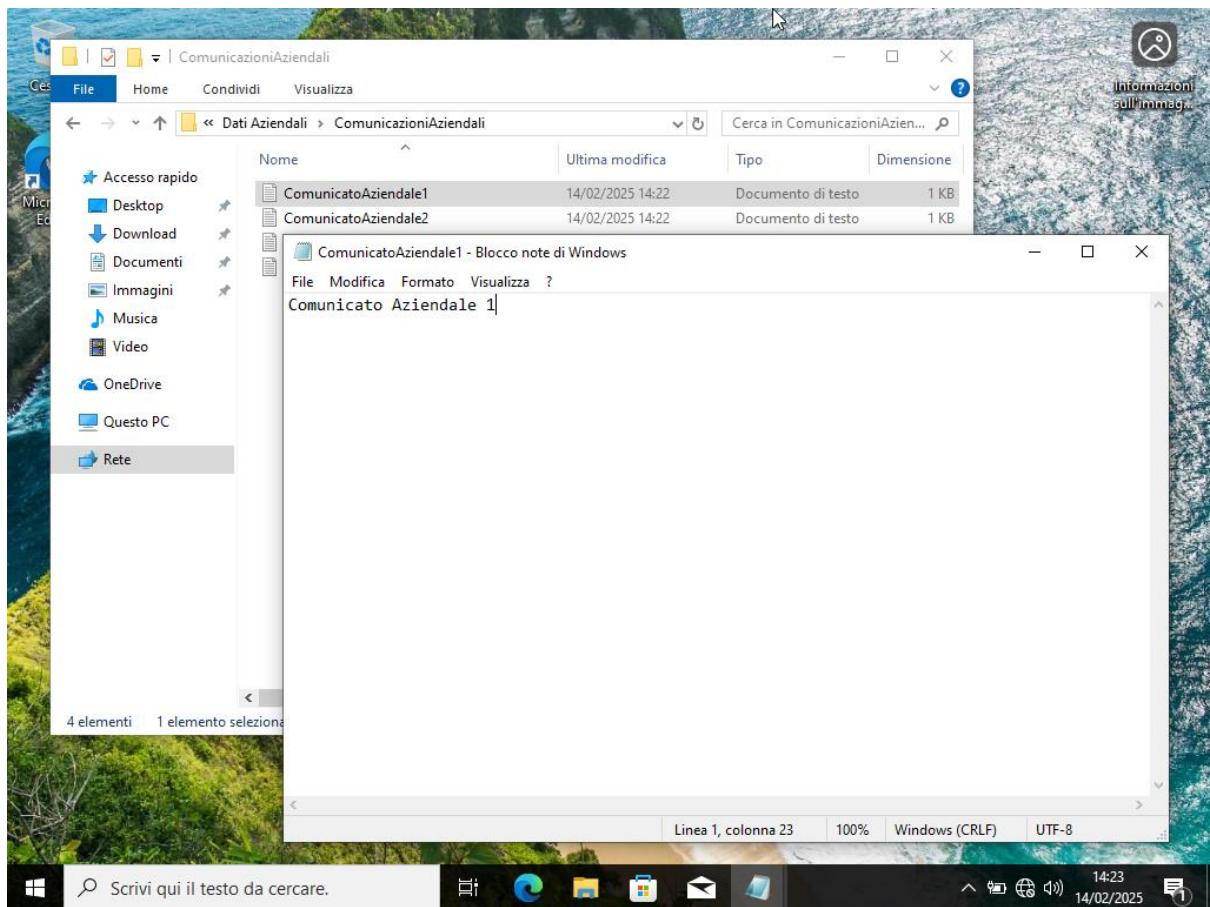
Se proviamo ad accedere alla directory "Dati Riservati" ci apparirà un avviso di errore perché non disponiamo i permessi per accedere:



Riusciamo ad accedere alla directory Dati Aziendali perché disponiamo i permessi:

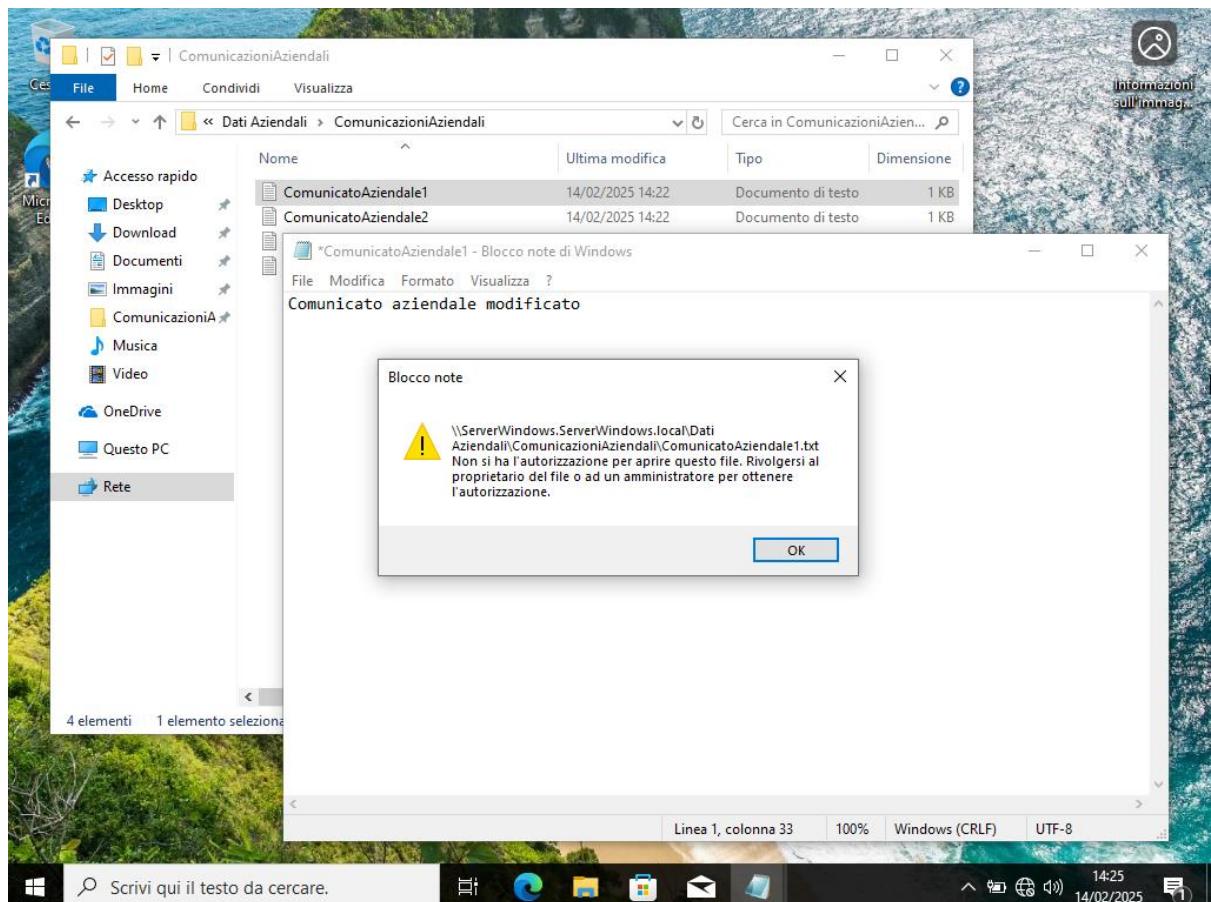


Se proviamo ad accedere ai comunicati aziendali potremmo leggere il contenuto dei file, ma non modificarlo:

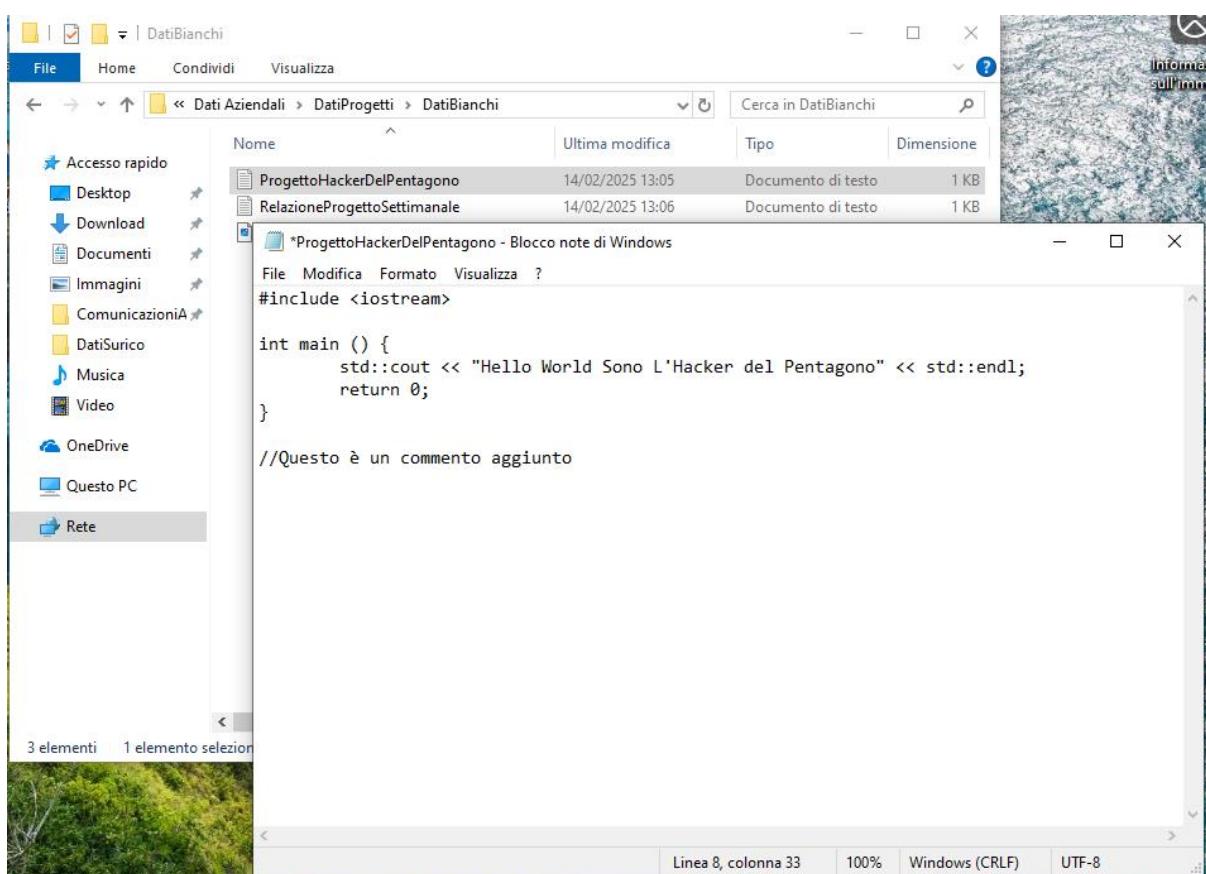
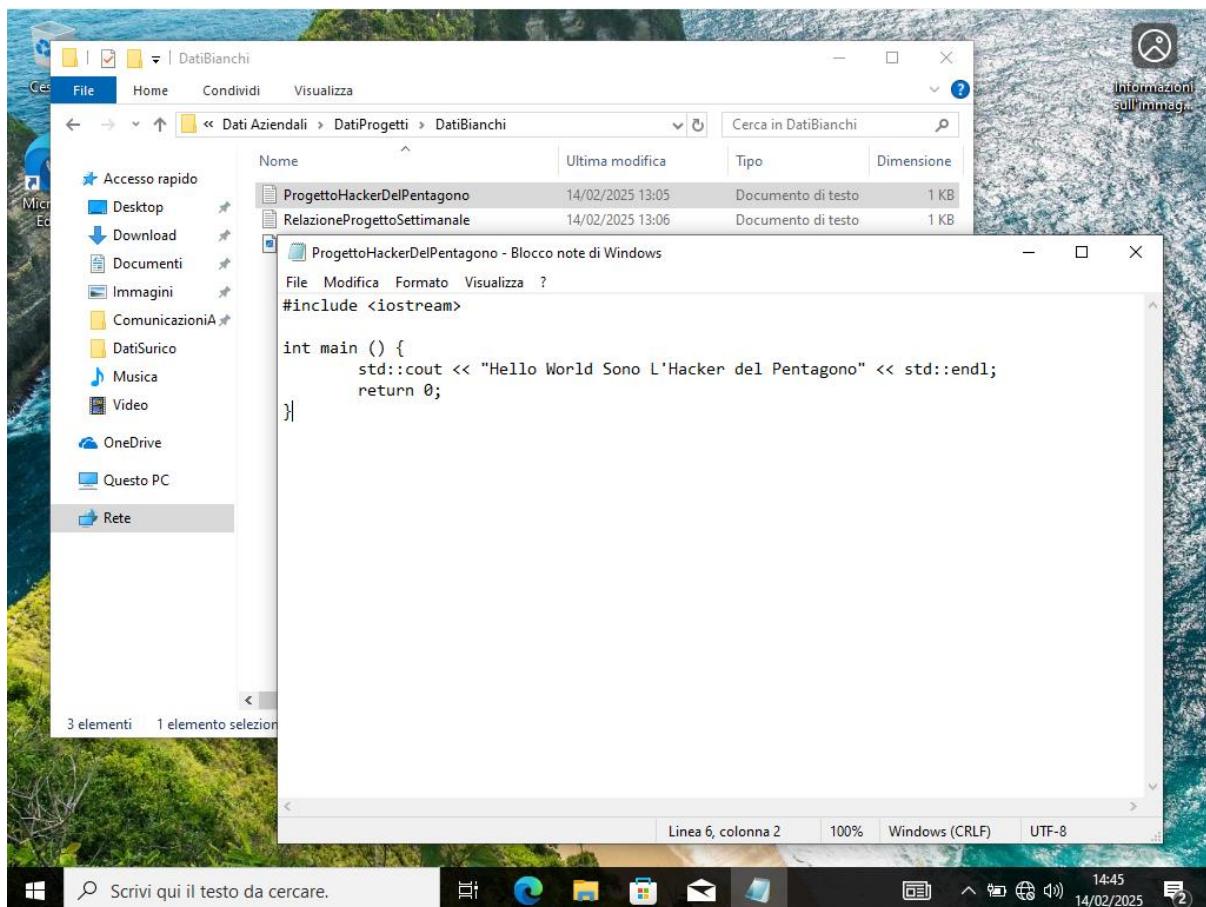


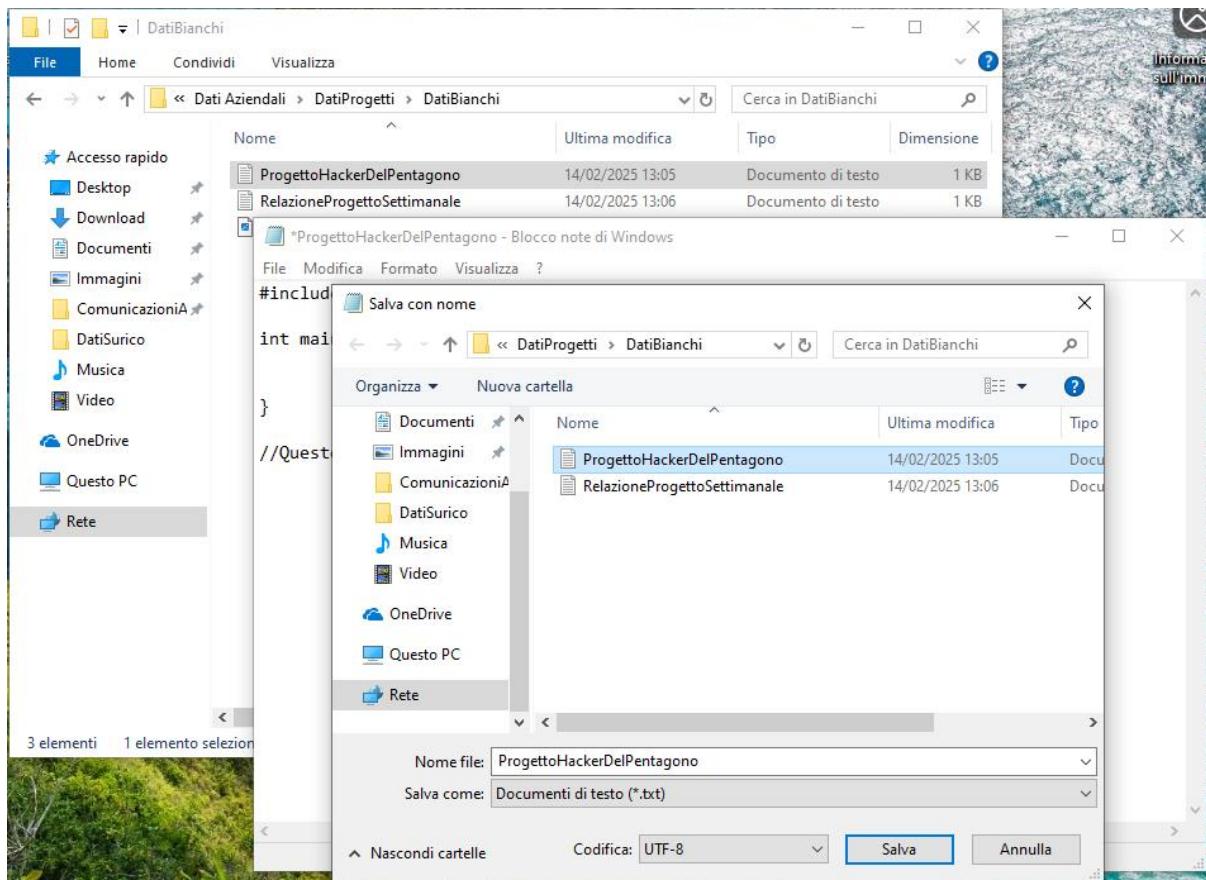
Se proviamo ad andare ad effettuare una modifica e a salvare il file ci darà errore

perchè disponiamo soltanto dei permessi di lettura:

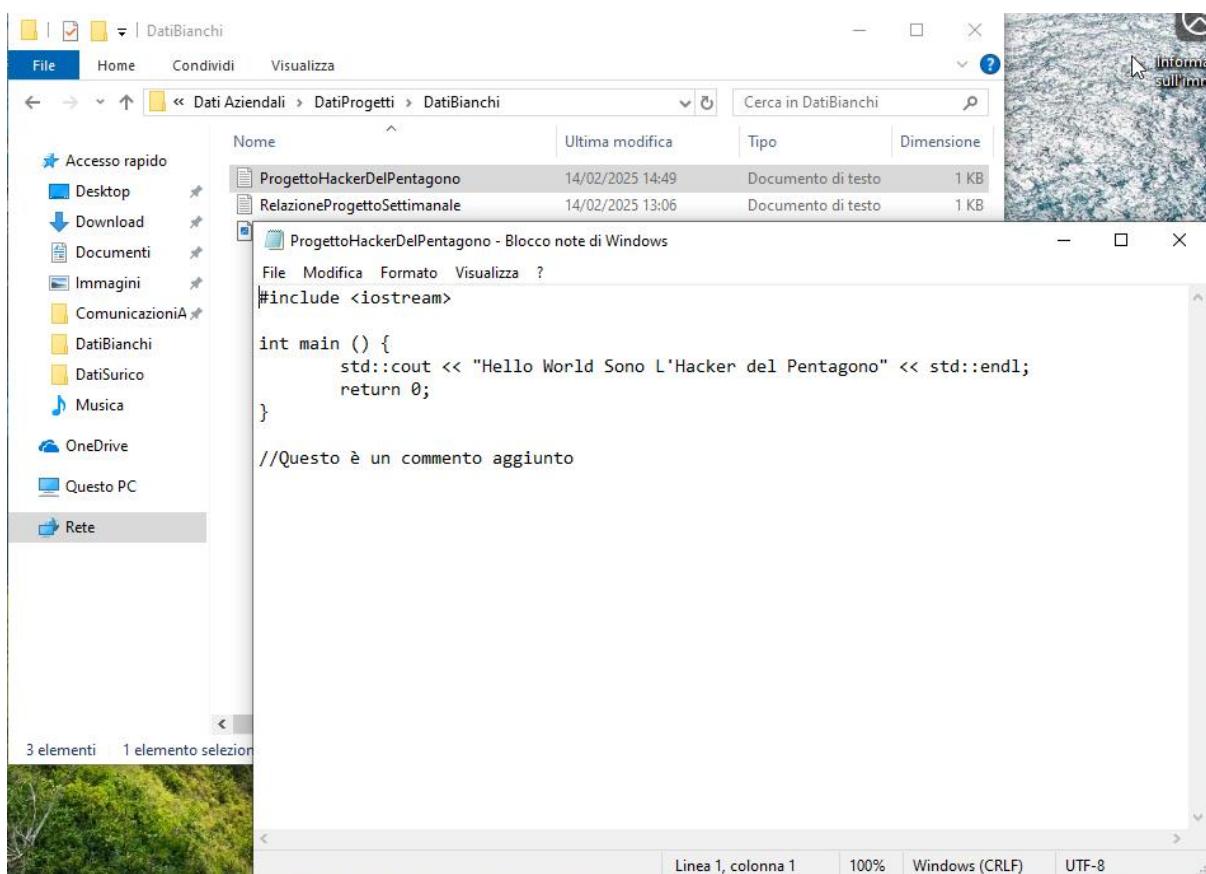


Ora se proviamo ad accedere alla directory “DatiBianchi”, potremmo leggerne il contenuto dei file e modificarli.



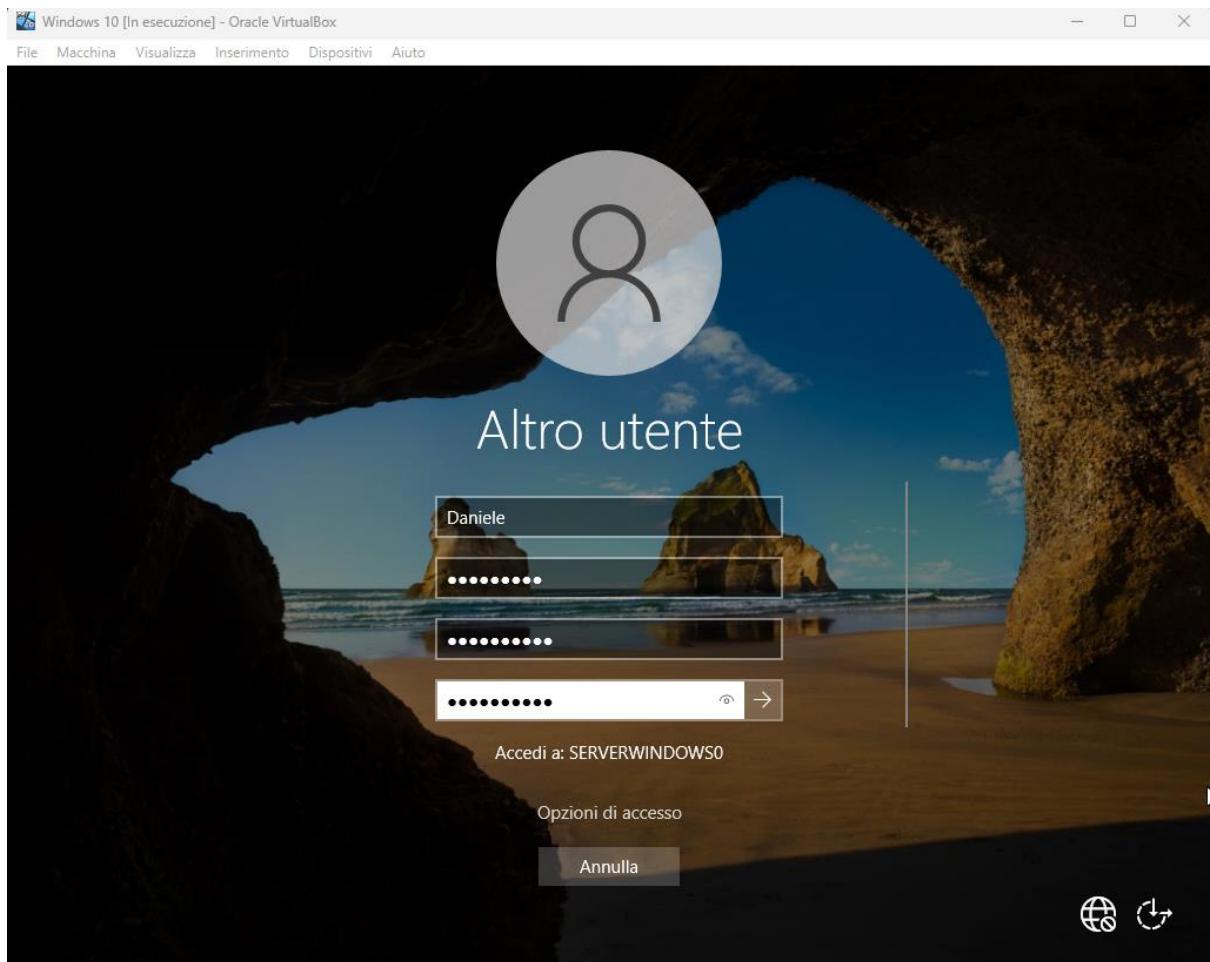


Riaprendo il file la modifica sarà effettuata:

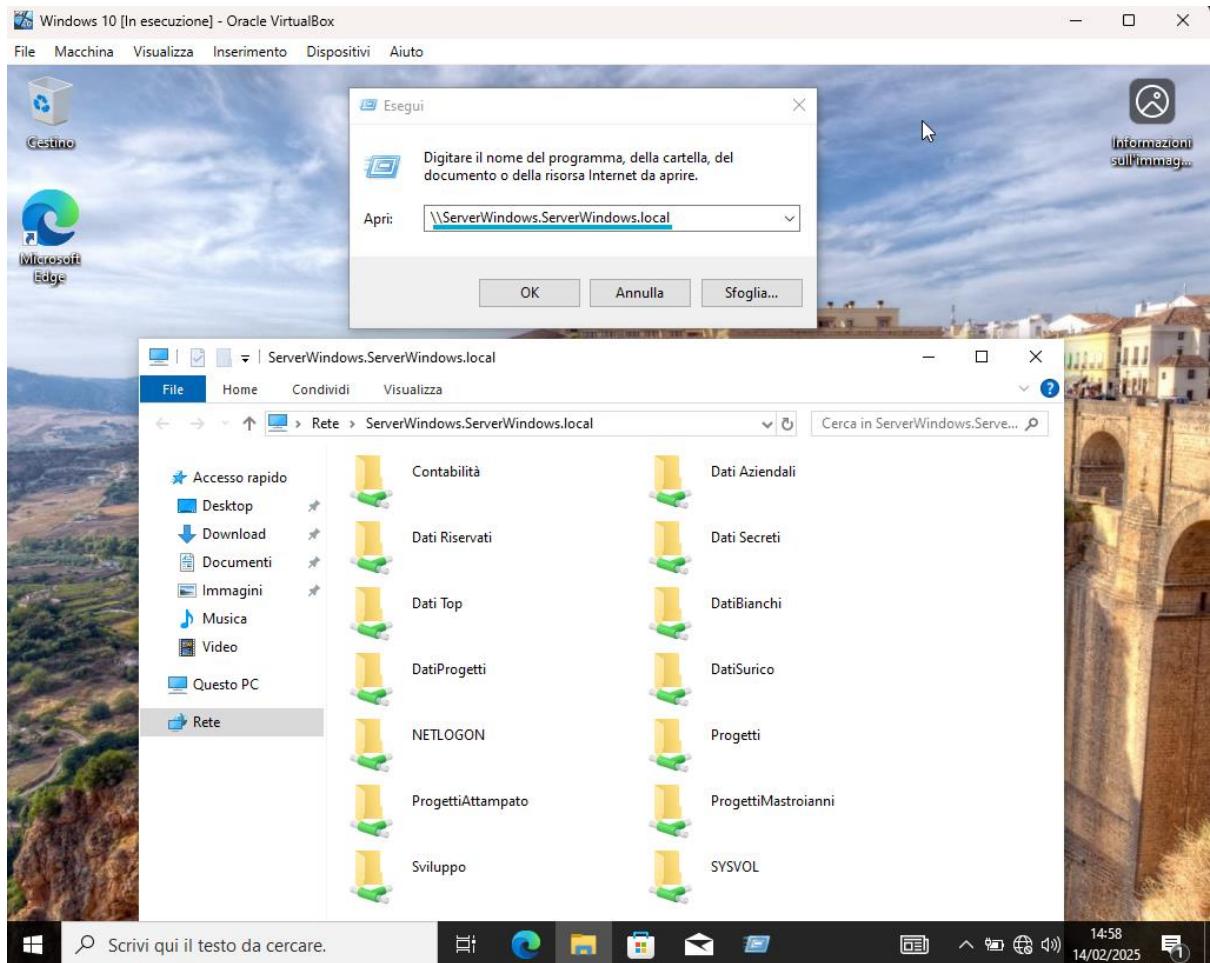


-Test Utente StaffAmministrativo “Daniele”:

Da Windows 10 andiamo ad effettuare il 1* login con l’utente, il sistema ci chiederà di modificare la password:

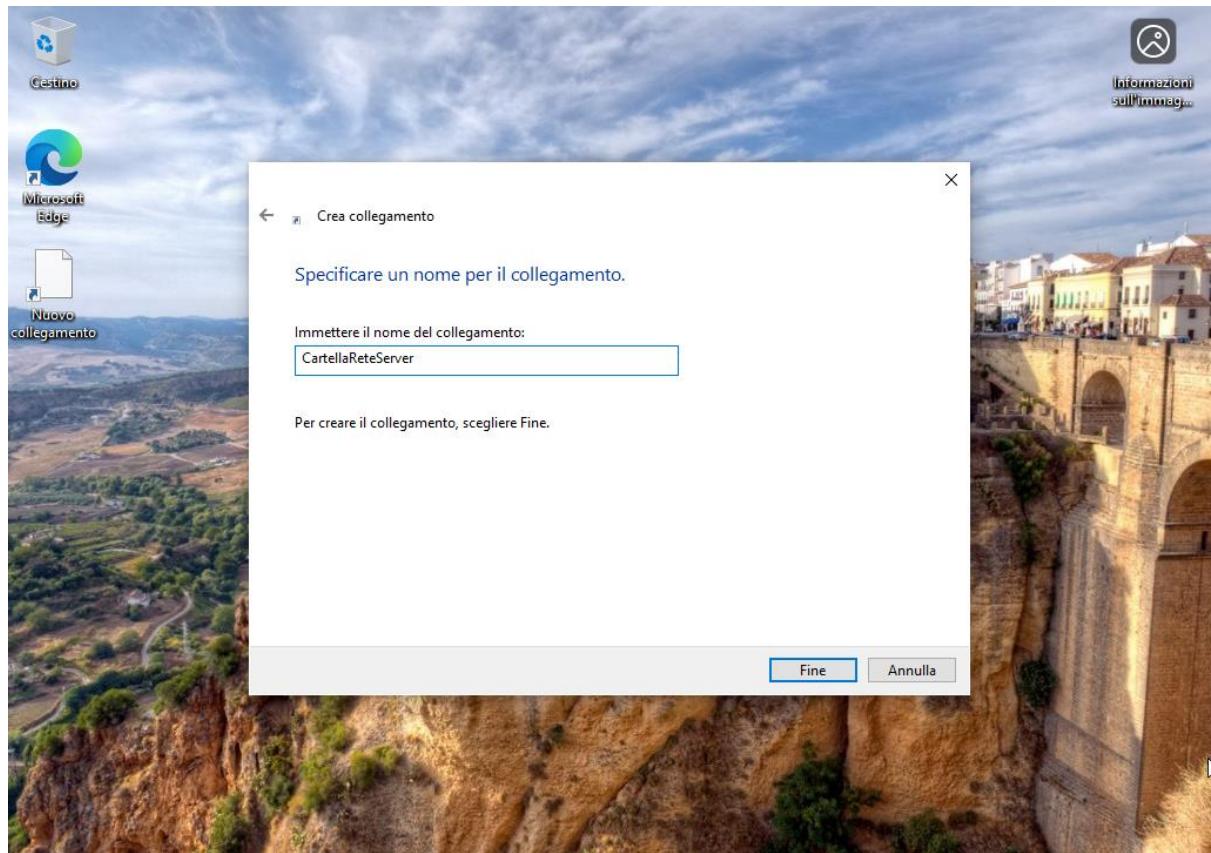


Per accedere alla directory di rete dalla barra di ricerca cerchiamo “Eseguì” e inseriamo il percorso del Server, \\ServerWindows.ServerWindows.local .

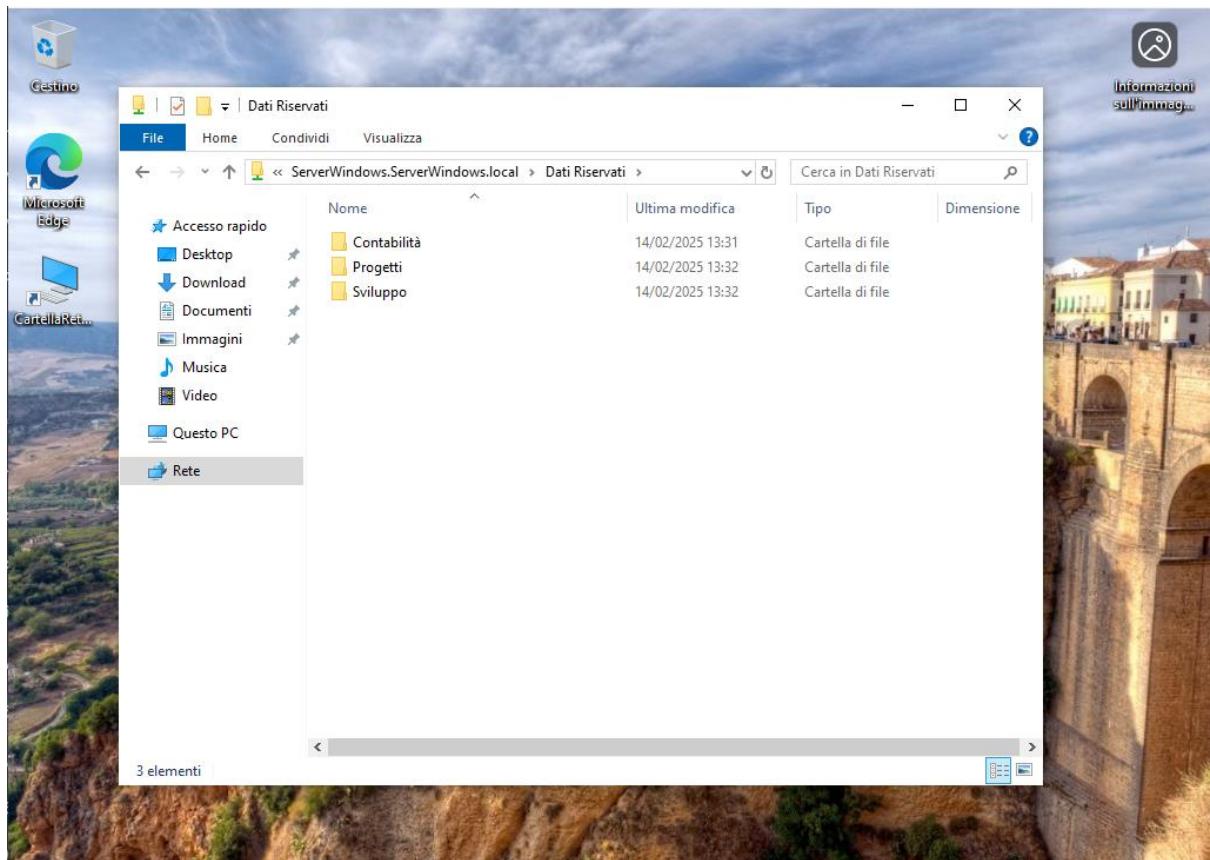


Per evitare di effettuare sempre l'accesso il path del server, possiamo creare una cartella da desktop che fungerà da cartella di Rete con il path del server già pre-

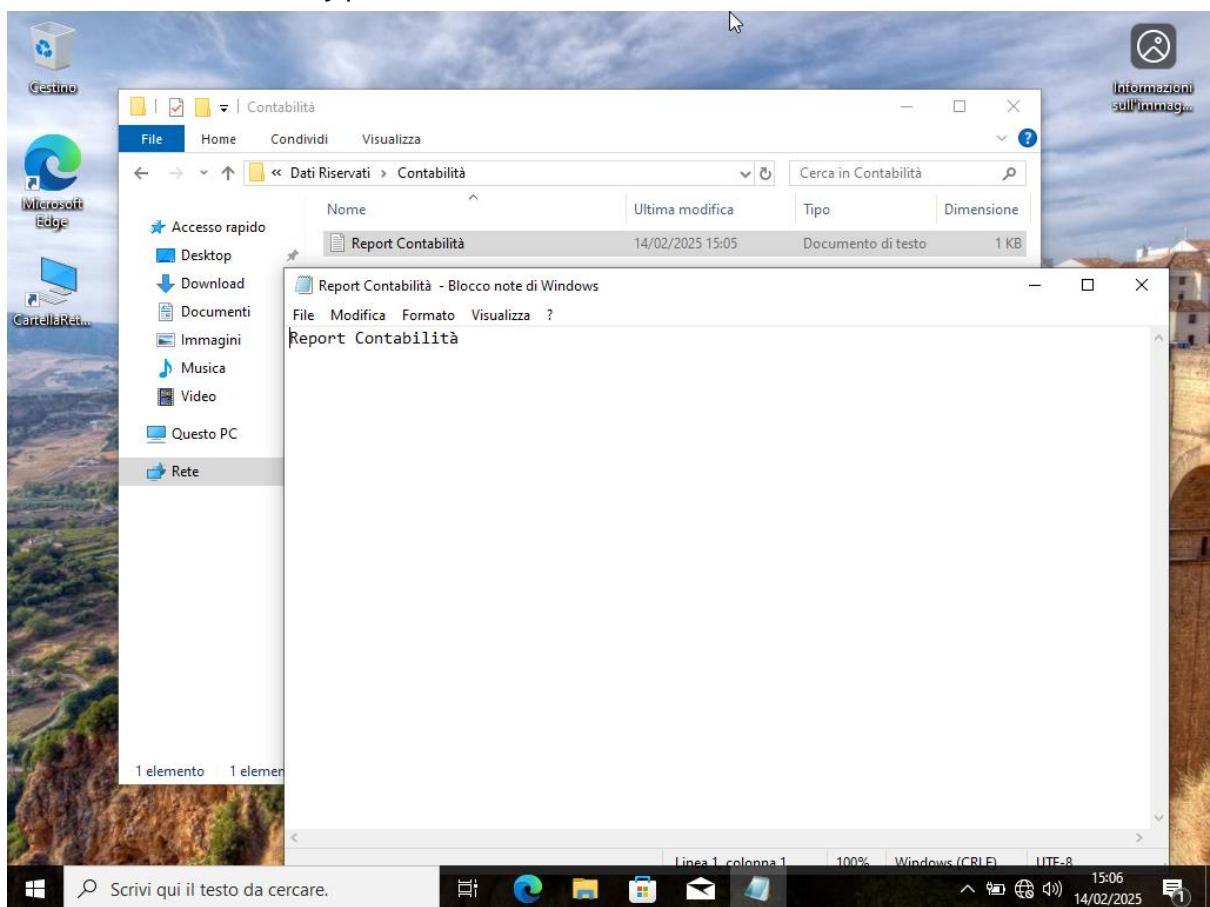
impostato.

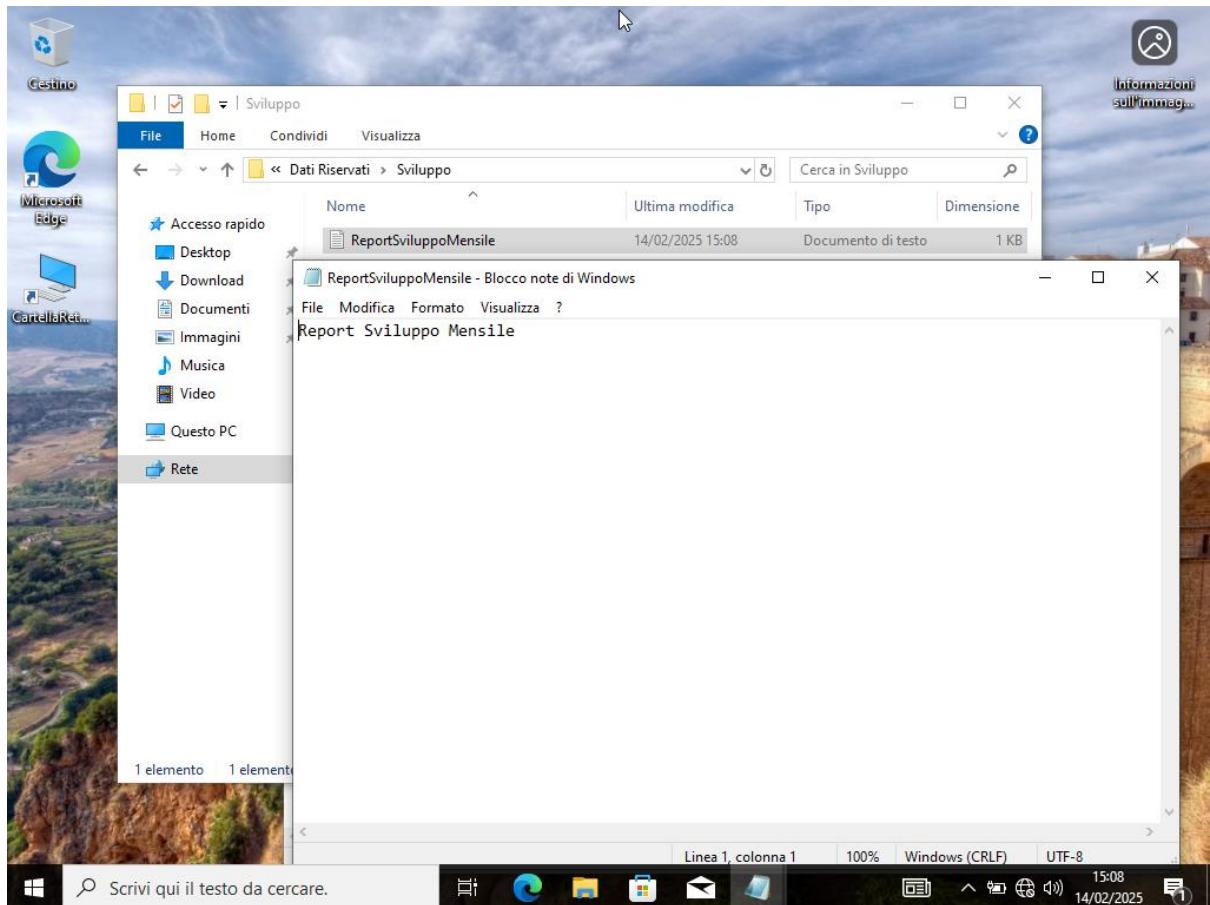


Se facciamo il test di accedere alla directory “Dati Riservati” essendo che abbiamo i permessi riusciamo ad accedere:

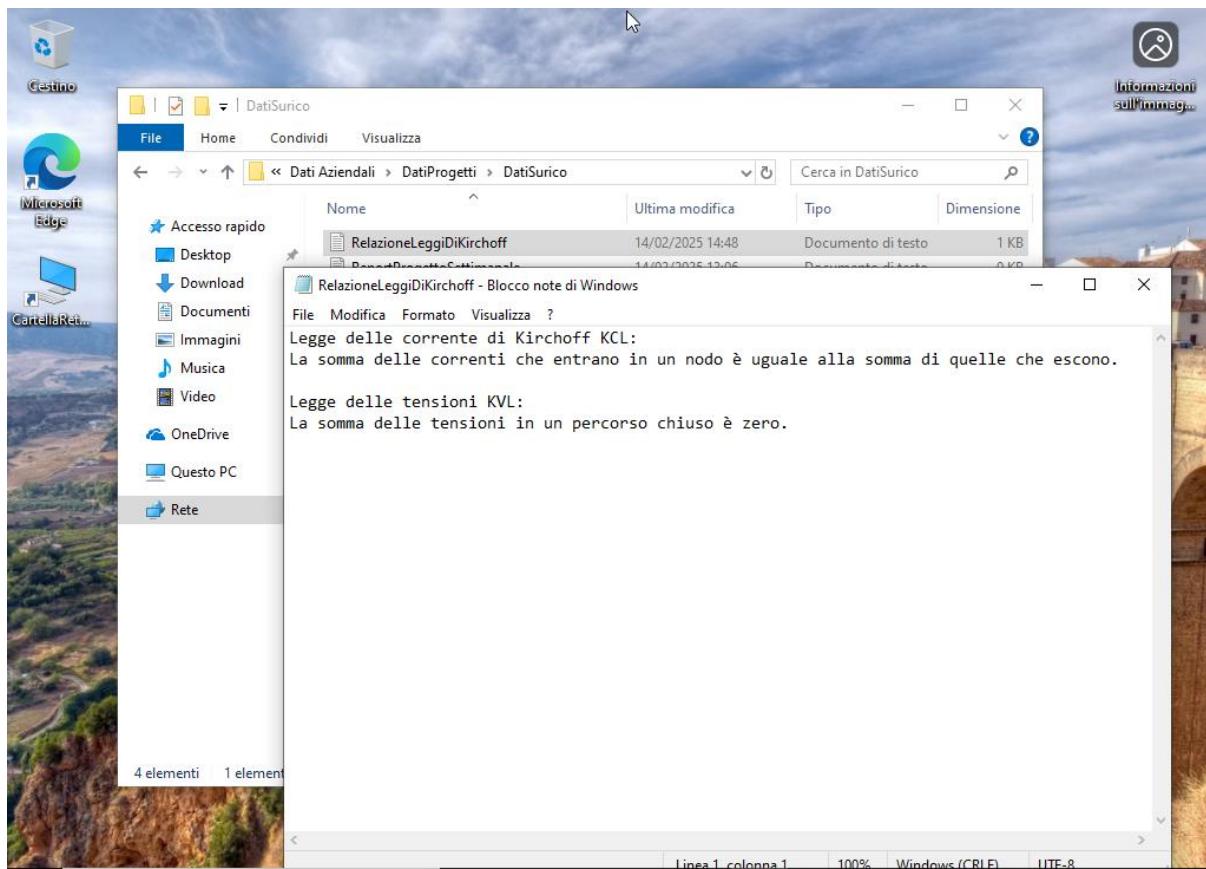


Entrando nelle directory potremmo vedere i contenuti dei file:





Se facciamo il test e proviamo ad accedere alle cartelle designate agli utenti base “DatiSurico” riusciremo ad accedere e a visionare il contenuto dei file:



-Conclusioni:

Effettuando i test i settaggi dei permessi sono stati validati.

In sintesi un grafico dei permessi effettuati:

Legenda:

L=Lettura

M=Modifica

E=Esecuzione

X=Nessun Accesso

Utenti:	Dati Aziendali	Comunicazioni Aziendali	Dati Progetti
Daniele	L , M , E	L , M , E	L , M , E
Franco	L , M , E	L , M , E	L , M , E
Fernando	L	L	L , M , E
Surico	L	L	L , M , E

Utenti:	Dati Riservati	Contabilità	Progetti	Sviluppo
Daniele	L , M , E	L , M , E	L , M , E	L , M , E
Franco	L , M , E	L , M , E	L , M , E	L , M , E
Fernando	X	X	X	X
Surico	X	X	X	X

Gli utenti che appartengono alla categoria “StaffAmministrativo”, hanno pieni poteri per un concetto di supervisione, ma ciò comporta un rischio perchè in caso di attacco ad un utente amministrativo e una conseguenza di credenziali rubate, si andrà ad avere accesso ai dati aziendali riservati.

Quindi è necessario monitorare costantemente gli accessi di login amministrativi e definire delle politiche interne aziendali di cambio password frequenti per gli utenti amministrativi.

-Possibile Miglioramento:

Si potrebbe migliorare il sistema e ridurre il rischio legato all’accesso illimitato da parte dello “StaffAmministrativo”, andando a creare dei sotto gruppi interni, e fornire agli utenti dei ruoli amministrativi soltanto su determinate sezioni, per es. Avere soltanto un amministratore che gestisce la “Contabilità”, ma non ha accesso privilegiati alle altre sezioni, e così anche per le altre sezioni “Progetti” e “Sviluppo”.