

WINDOWS SERVER 2022

- Traccia
- Tema
- Fase 1
- Fase 2
- Fase 3
- Fase 4
- Test
- Conclusione



TRACCIA

In questo esercizio si impara a gestire i gruppi utenti in Windows Server 2022. Dopo aver effettuato l'accesso con privilegi amministrativi, si devono creare due gruppi con nomi significativi e assegnare loro permessi specifici (come accesso a file, esecuzione di programmi, modifiche di sistema o accesso remoto).

Una volta configurati i gruppi, si verifica il funzionamento creando utenti di prova e controllando che abbiano i permessi corretti. Infine, si scrive una breve relazione che descrive i gruppi creati, i permessi assegnati, i passaggi eseguiti e le eventuali difficoltà incontrate.



TEMA

Per questo esercizio ho provato a riprodurre un ambiente di lavoro ispirato alla serie TV **Travelers** e all'organizzazione immaginaria che ha progettato l'intelligenza artificiale quantistica nota come "Il Direttore". L'obiettivo principale è stato strutturare ruoli, cartelle e permessi in Windows Server 2022, in modo da riflettere le responsabilità e le necessità operative di ciascun gruppo. Di seguito racconto passo passo le scelte compiute, partendo dalla creazione dei gruppi fino all'assegnazione degli utenti e dei permessi alle directory su disco locale C:.



TEMA

Il Direttore è un'intelligenza artificiale molto evoluta, creata nel futuro per cercare di salvare l'umanità da una catastrofe. A differenza di un essere umano, non ha emozioni, ma prende decisioni basandosi su calcoli, logica e miliardi di simulazioni. È lui che coordina l'intero programma dei viaggiatori nel tempo, scegliendo chi mandare nel passato e quale missione affidargli.

Il Direttore trasferisce la coscienza dei viaggiatori nei corpi di persone che stanno per morire, così da non alterare troppo la linea temporale. Ogni squadra riceve istruzioni precise, chiamate "missioni", che servono a cambiare il corso degli eventi e prevenire disastri futuri. Per comunicare, spesso prende temporaneamente il controllo di bambini o persone comuni, parlando attraverso di loro. Questo succede solo in situazioni importanti, perché normalmente non interviene direttamente.



FASE 1

Per prima cosa, ho aperto la console Utenti e gruppi locali tramite il comando lusrmgr.msc. Qui ho creato quattro gruppi corrispondenti ai ruoli fondamentali nell'organizzazione immaginaria:

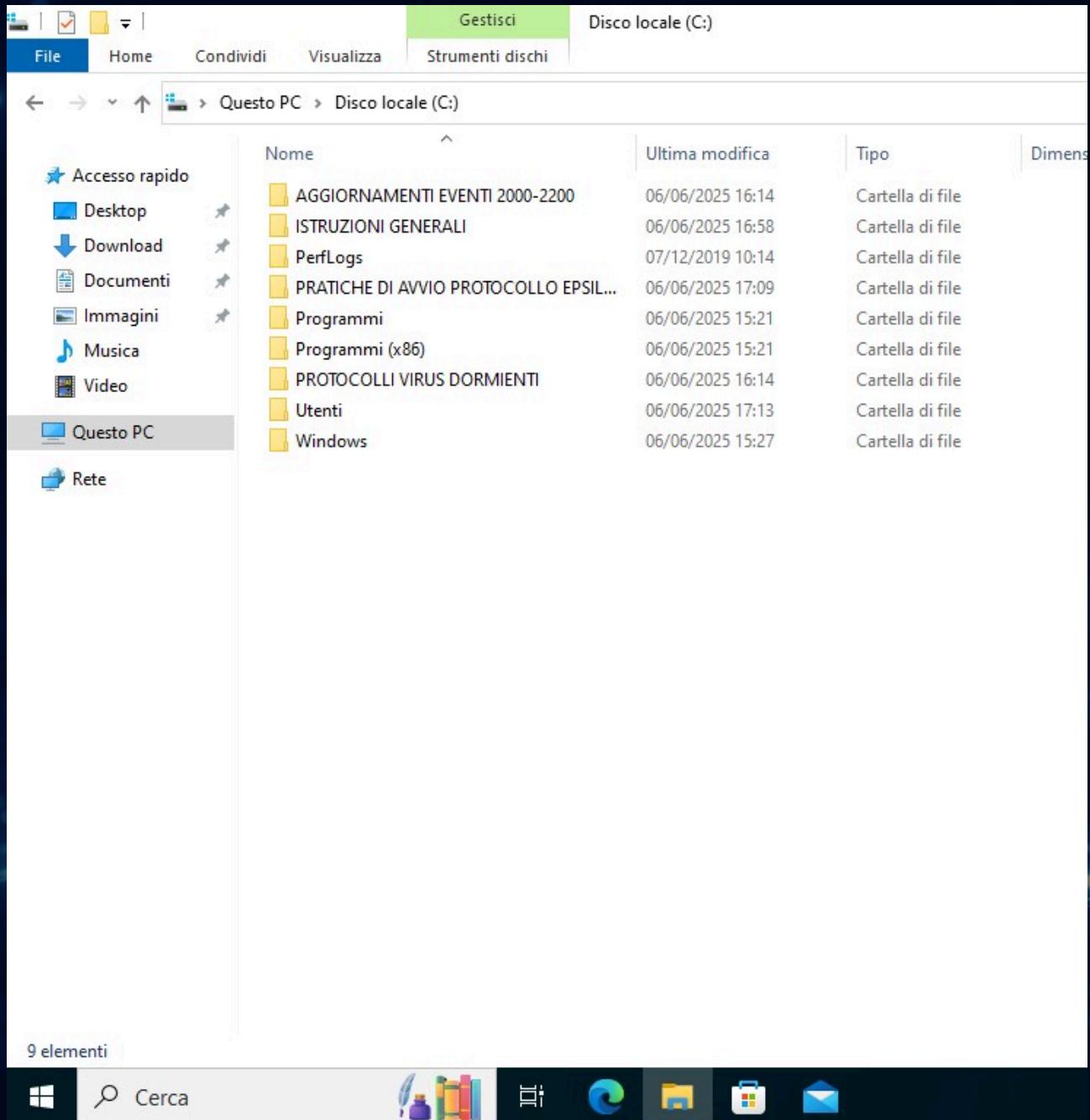
1. **Archivisti**: Gli Archivisti sono incaricati di gestire i protocolli di sicurezza e i codici di avvio per l'isolamento dei dati. Nel contesto del racconto, sono le persone che devono avere sotto controllo i documenti più sensibili nel caso di un attacco alla linea temporale.
2. **Storici**: gli Storici tengono traccia di tutti gli avvenimenti modificati rispetto alla timeline originale; hanno bisogno di accedere a una cartella riservata contenente gli aggiornamenti cronologici. Solo loro possono vedere e modificare questi dati per documentare con precisione ogni cambiamento.
3. **Capisquadra**: I Capisquadra coordinano le operazioni sul campo e devono poter consultare istruzioni generali, visionare protocolli critici (anche se senza poterli modificare) e partecipare alla gestione di emergenze. Rappresentano il livello intermedio tra chi crea protocolli e chi li esegue.
4. **Medici**: infine, i Medici si occupano degli aspetti bio-sanitari e dei protocolli contro eventuali minacce virali dormienti. Devono poter leggere e aggiornare la cartella in cui sono contenuti i protocolli riguardanti spore o virus potenzialmente riattivabili.

Gruppi locali (locale)\Gruppi	
Nome	Descrizione
Administrators	Gli amministratori hanno privilegi...
Amministratori Hyper...	I membri di questo gruppo hanno...
Backup Operators	Al gruppo Backup Operators è co...
Cryptographic Operat...	I membri sono autorizzati a esegu...
Distributed COM Users	Ai membri di questo gruppo è co...
Guests	Gli utenti del gruppo Guests dispon...
IIS_IUSRS	Gruppo predefinito utilizzato da I...
Lettori registri eventi	I membri di questo gruppo posso...
Network Configuration...	I membri di questo gruppo posso...
Operatori assistenza c...	I membri di questo gruppo posso...
Performance Log Users	I membri di questo gruppo posso...
Performance Monitor ...	I membri del gruppo possono acc...
Power Users	Il gruppo Power Users è incluso p...
Proprietari dispositivi	I membri di questo gruppo posso...
Replicator	Supporta la replica dei file in un d...
System Managed Acc...	I membri di questo gruppo vengo...
Users	Gli utenti del gruppo Users non p...
Utenti desktop remoto	Ai membri di questo gruppo è co...
Utenti gestione remota	I membri di questo gruppo posso...
Archivisti	
Capisquadra	
Medici	
Storici	

FASE 2

Una volta stabiliti i quattro gruppi, ho aperto Esplora file e, nella radice del disco locale C:, ho creato quattro nuove directory, ognuna con un nome preciso che rispecchiasse il contenuto e le responsabilità:

1. **AGGIORNAMENTI EVENTI 2000-2200** Contiene i documenti che descrivono come gli eventi sono stati alterati nell'arco di tempo dal 2000 al 2200. Ogni modifica alla linea temporale viene registrata qui dai Storici.
2. **PRATICHE DI AVVIO PROTOCOLLO EPSILON** In questa cartella risiedono i file di script e i codici necessari per avviare il "Protocollo Epsilon", ossia il procedimento di isolamento dei dati in caso di tentativo di attacco alla rete quantistica.
3. **ISTRUZIONI GENERALI** Qui sono raccolte le direttive operative comuni a tutto il personale: linee guida, manuali, regolamenti e procedure standard. I Capisquadra devono poter consultare e aggiornare questo materiale per coordinare il lavoro sul campo.
4. **PROTOCOLLI VIRUS DORMIENTI** Contiene informazioni riservate sui virus che, pur non essendo attivi, vengono monitorati dai Medici. In caso di riattivazione, è qui che troverebbero le istruzioni dettagliate per neutralizzare la minaccia.

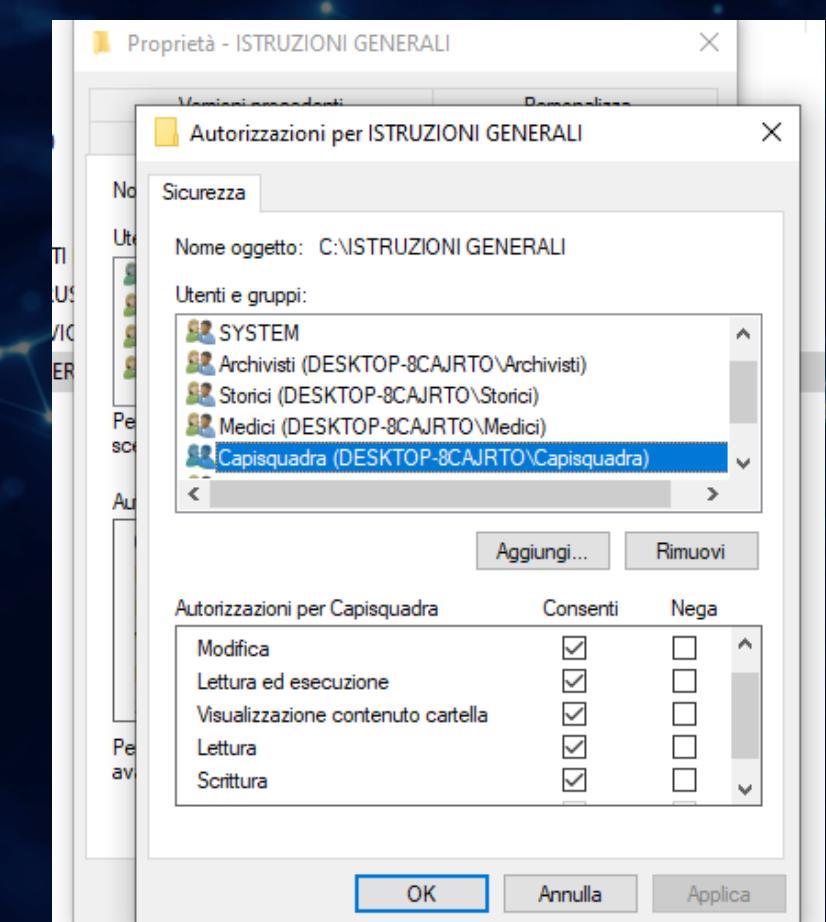
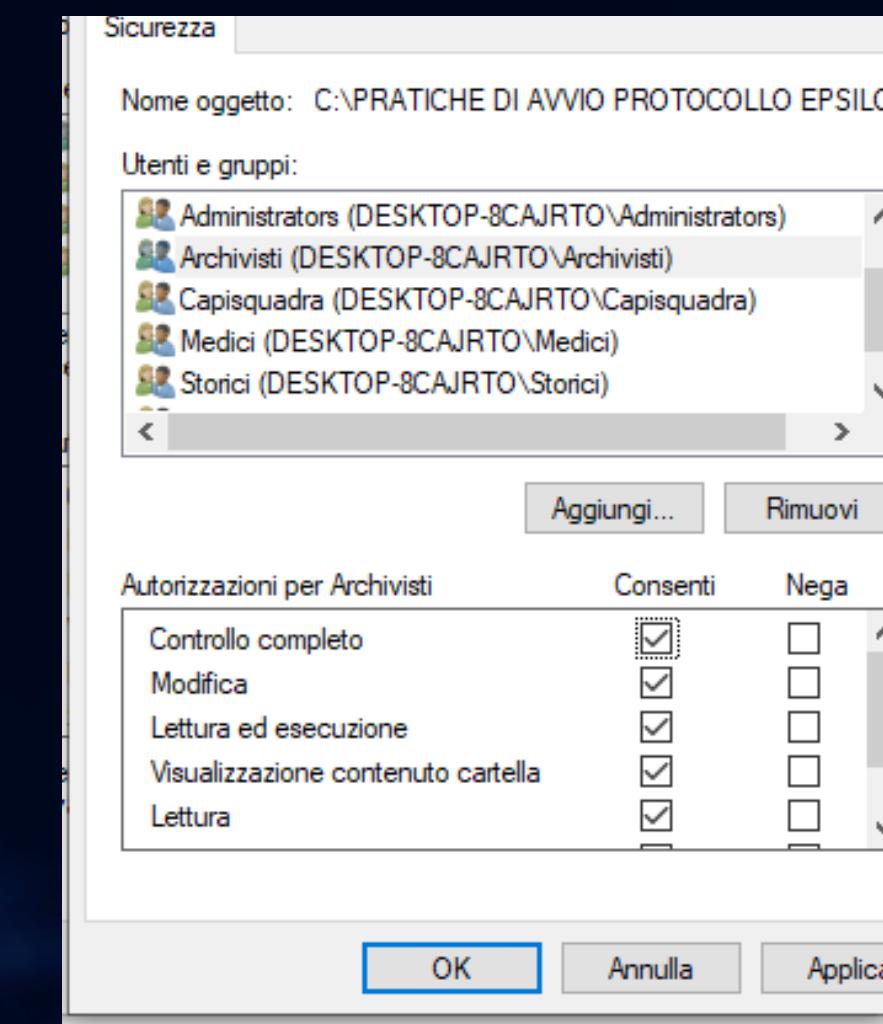
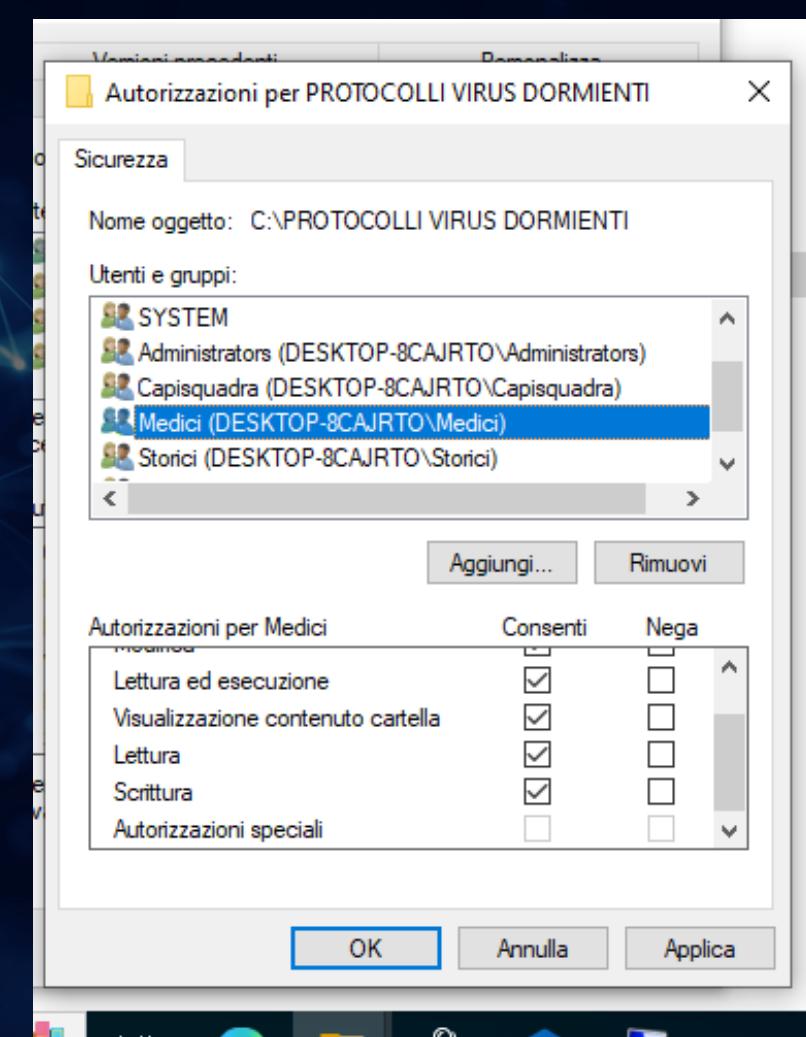
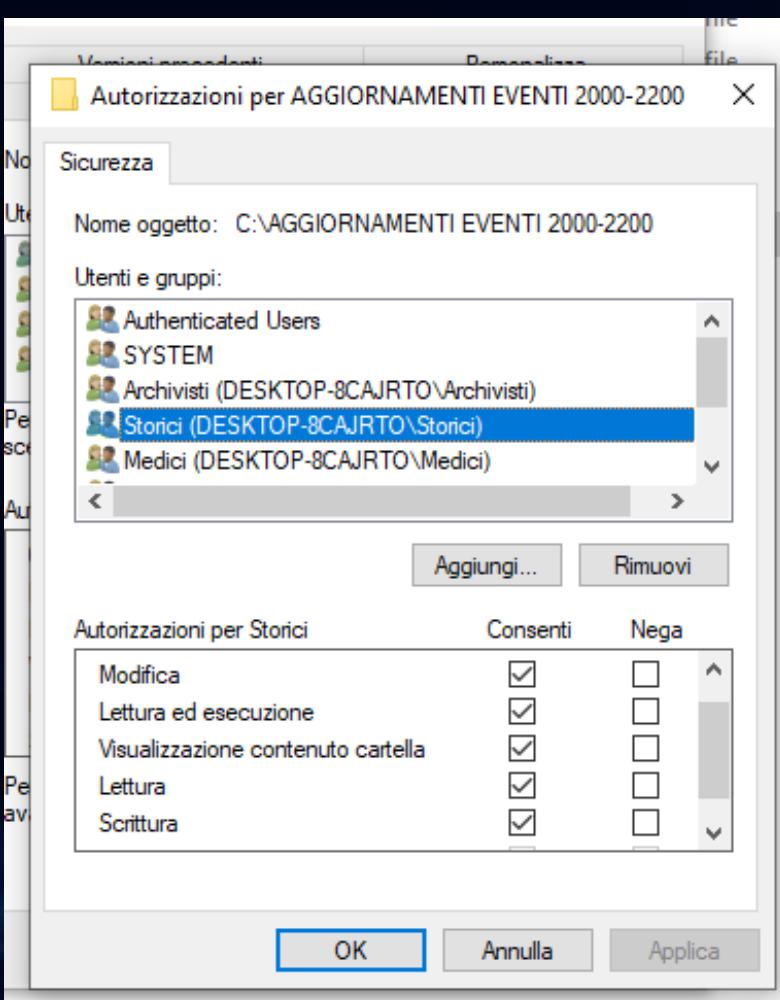


FASE 3

Per ogni cartella ho configurato i permessi in modo da garantire la massima sicurezza e riservatezza, lasciando accessi differenziati a seconda dei ruoli:

- **AGGIORNAMENTI EVENTI 2000-2200** Ho aperto le proprietà della cartella, sono andato nella scheda Sicurezza, ho rimosso i permessi ereditati da "Utenti" e "Administrators" e ho aggiunto solo il gruppo Storici, concedendogli Controllo completo. In questo modo, solo i membri del gruppo Storici possono leggere e scrivere documenti relativi agli eventi cambiati; tutti gli altri gruppi (Archivisti, Capisquadra, Medici) non hanno alcun tipo di accesso.
- **PRATICHE DI AVVIO PROTOCOLLO EPSILON** Qui ho tolto i permessi predefiniti e poi aggiunto il gruppo Archivisti con Controllo completo sulla cartella, perché sono gli unici che devono avere la facoltà di modificare o aggiornare i codici di avvio del Protocollo Epsilon. Inoltre ho aggiunto il gruppo Capisquadra ma soltanto con permessi di Lettura (leggere i file senza poterli modificare). Gli altri gruppi non hanno accesso.
- **ISTRUZIONI GENERALI** Nella scheda Sicurezza ho aggiunto i Capisquadra con Controllo completo, così da permettere loro di aggiornare agilmente le procedure operative. Ho lasciato tutti gli altri (Archivisti, Storici, Medici) con permessi di sola Lettura, in modo che possano consultare le informazioni ma non modificarle.
- **PROTOCOLLI VIRUS DORMIENTI** Ho rimosso tutte le voci eccetto il gruppo Medici, a cui ho concesso Controllo completo, affinché possano aggiornare o aggiungere nuovi protocolli in caso di evoluzioni sanitarie. Ho poi aggiunto i Capisquadra con permessi di Lettura, in modo che possano consultare le indicazioni generali senza poter intervenire sulla struttura dei file. Gli altri gruppi non hanno alcun accesso.

FASE 3



FASE 4

Infine ho creato quattro utenti, uno per ciascun ruolo, sempre tramite la console

Utenti e gruppi locali:

1. Viaggiatore 0024 (utenteArchivista)

- Password: impostata con criteri minimi P@sswOrd2022
- Assegnazione al gruppo Archivisti (attraverso la scheda "Membro di" dell'utente oppure direttamente dal gruppo "Archivisti" → "Aggiungi...").

2. Viaggiatore 1378 (utenteStorico)

- Password: Storico@2200
- Assegnazione al gruppo Storici.

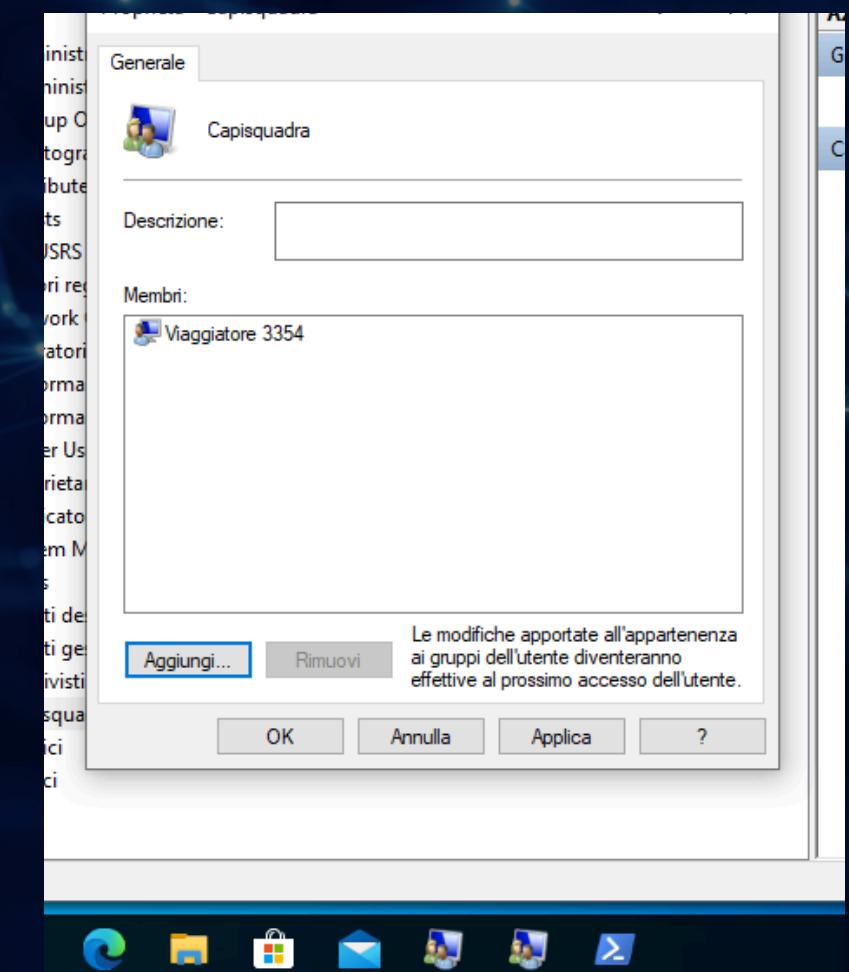
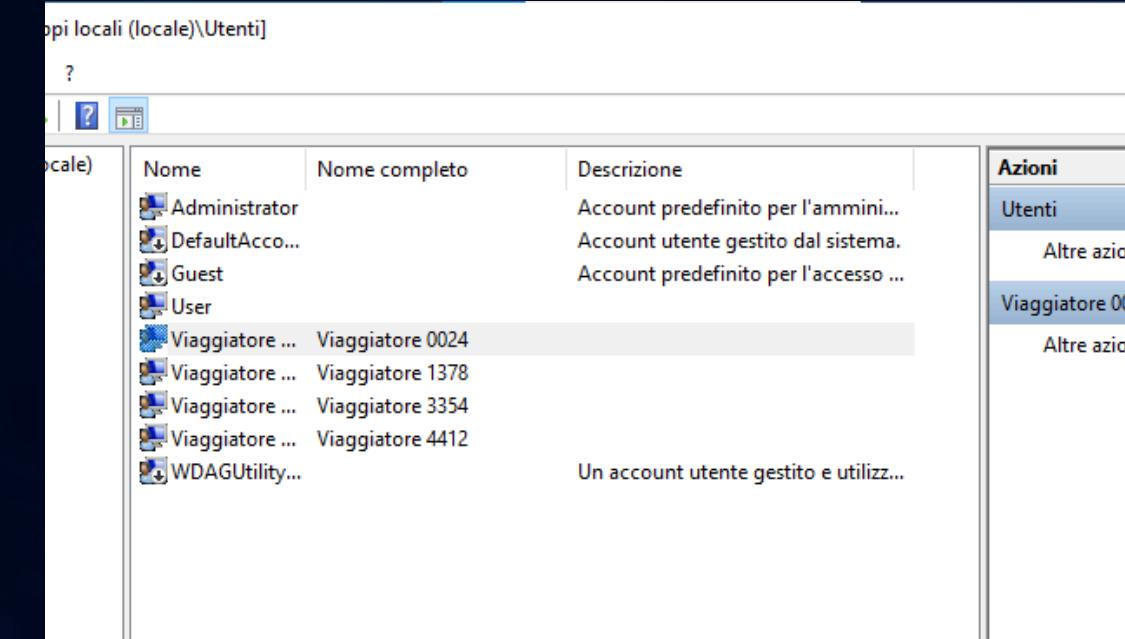
3. Viaggiatore 3354 (utenteCaposquadra)

- Password: CapoSquadra#1
- Assegnazione al gruppo Capisquadra.

4. Viaggiatore 4412 (utenteMedico)

- Password: Medico!2022
- Assegnazione al gruppo Medici.

In ciascun caso ho tolto l'opzione "L'utente deve cambiare password al prossimo accesso" e ho lasciato "Password non scade mai" per semplificare i test.



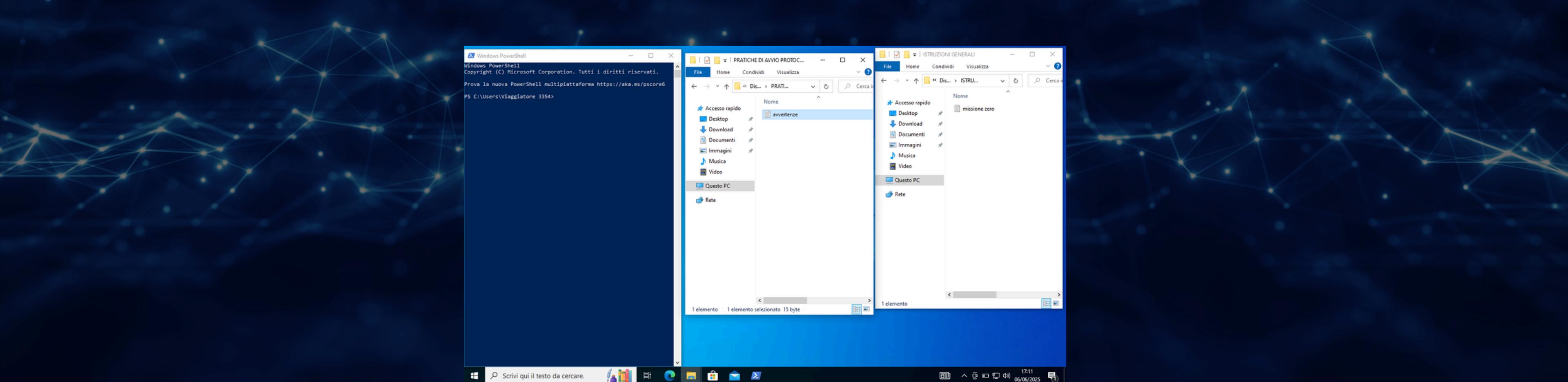
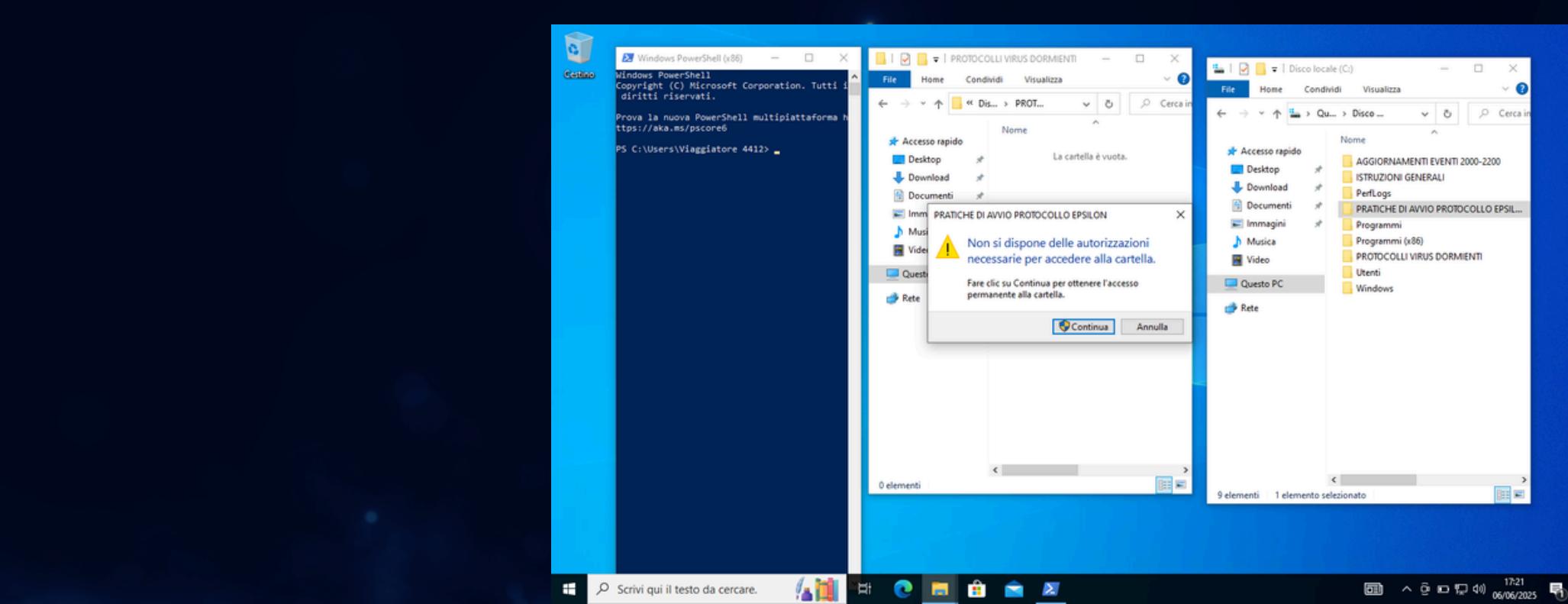
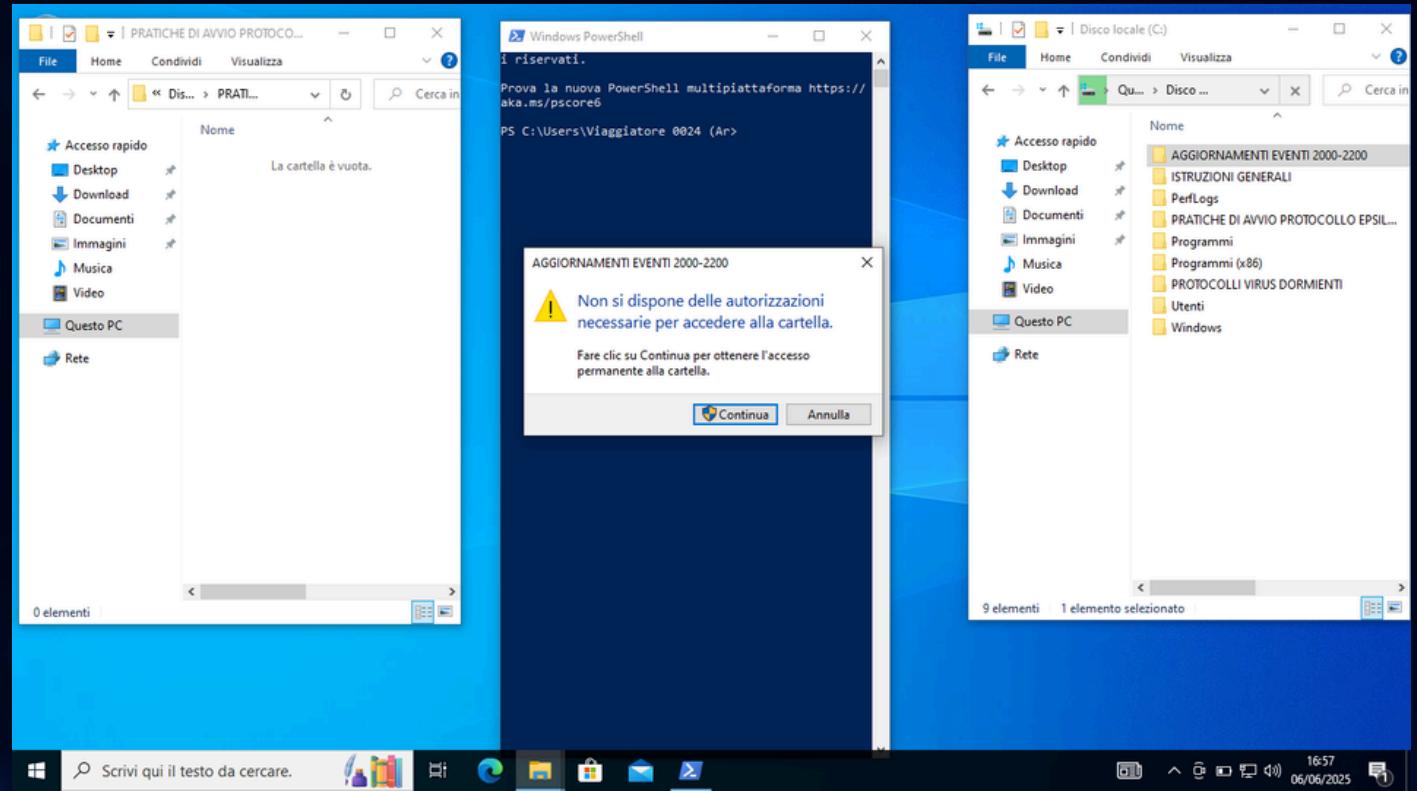
TEST

Dopo aver completato la configurazione, ho eseguito il logout dall'account Administrator e ho effettuato il login con gli account di prova per verificare i permessi:

- Accesso con Viaggiatore 1378 (Storico):
 - Accesso completo alla cartella “AGGIORNAMENTI EVENTI 2000-2200”.
 - Tentativo di accedere alle altre cartelle: accesso rifiutato per “PRATICHE DI AVVIO PROTOCOLLO EPSILON” e “PROTOCOLLI VIRUS DORMIENTI”; può leggere ma non scrivere in “ISTRUZIONI GENERALI”.
- Accesso con Viaggiatore 0024 (Archivista):
 - Controllo completo nella cartella “PRATICHE DI AVVIO PROTOCOLLO EPSILON”.
 - Lettura in “ISTRUZIONI GENERALI”.
 - Nessun accesso a “AGGIORNAMENTI EVENTI 2000-2200” e “PROTOCOLLI VIRUS DORMIENTI”.
- Accesso con Viaggiatore 3354 (Caposquadra):
 - Controllo completo in “ISTRUZIONI GENERALI”.
 - Lettura in “PRATICHE DI AVVIO PROTOCOLLO EPSILON” e “PROTOCOLLI VIRUS DORMIENTI”.
 - Nessun accesso a “AGGIORNAMENTI EVENTI 2000-2200”.
- Accesso con Viaggiatore 4412 (Medico):
 - Controllo completo in “PROTOCOLLI VIRUS DORMIENTI”.
 - Lettura in “ISTRUZIONI GENERALI”.
 - Nessun accesso a “AGGIORNAMENTI EVENTI 2000-2200” e “PRATICHE DI AVVIO PROTOCOLLO EPSILON”.

TEST

TURAZZA GABRIELE



CONCLUSIONE

Per concludere, questo esercizio ha evidenziato l'importanza della gestione strutturata dei gruppi e dei permessi in un ambiente Windows Server 2022.

Organizzare gli utenti secondo ruoli precisi, come nel caso dei gruppi ispirati alla serie Travelers, ha permesso di simulare un sistema efficiente e sicuro, dove ogni utente ha accesso solo alle informazioni di propria competenza. Questo approccio riflette un principio fondamentale della sicurezza: il minimo privilegio.

Durante la configurazione, è stato essenziale prestare attenzione ad alcuni aspetti operativi, come la disattivazione dell'ereditarietà dei permessi quando non necessaria, la corretta assegnazione degli utenti ai gruppi e la verifica pratica degli accessi tramite utenti di prova. Questi passaggi aiutano a evitare errori e a garantire che tutto funzioni come previsto.

Infine, documentare ogni scelta fatta – dai nomi dei gruppi ai permessi assegnati – rende il sistema più facile da gestire e più sicuro nel tempo. Una buona configurazione, infatti, non si basa solo sulla tecnica, ma anche sull'ordine, la logica e la consapevolezza delle conseguenze operative