

Windows Server

Executive Summary

Il presente report documenta le fasi di configurazione di un ambiente **Windows Server** finalizzato alla gestione sicura e ottimizzata delle risorse e degli accessi. L'obiettivo principale del progetto è la creazione di gruppi e l'assegnazione di permessi specifici all'interno di un dominio denominato **pentagon.gov**.

Obiettivo

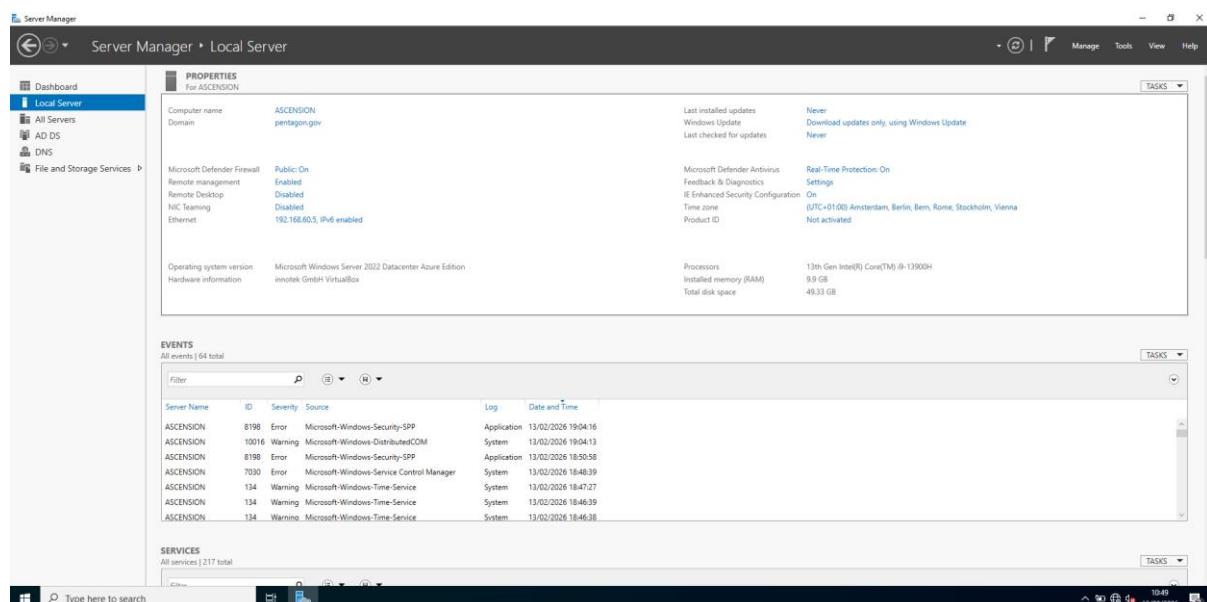
Creare gruppi, assegnare permessi specifici per una gestione dei gruppi e di sicurezza ottimale

Strumenti laboratorio

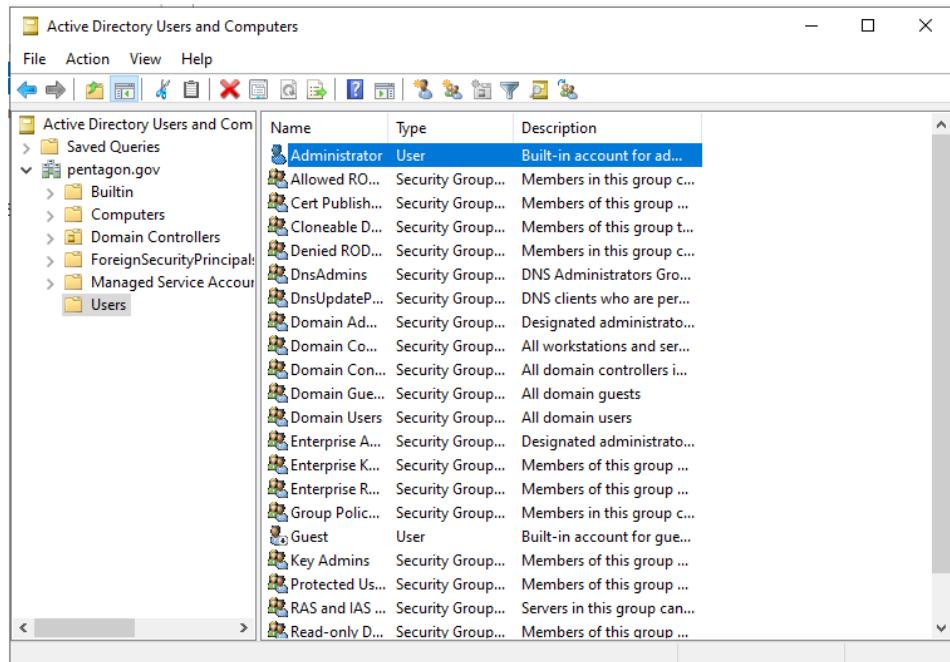
Windows Server 2022: macchina per gestione gruppi e permessi

Windows 10 Pro N: macchina per simulazione utenti

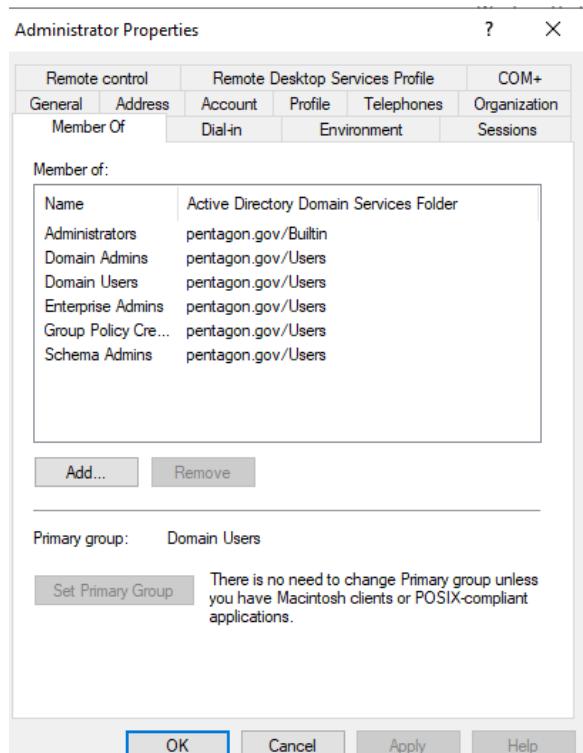
Fase1 – Accesso a Windows Server



*Fig.1 Pagina principale post configurazione



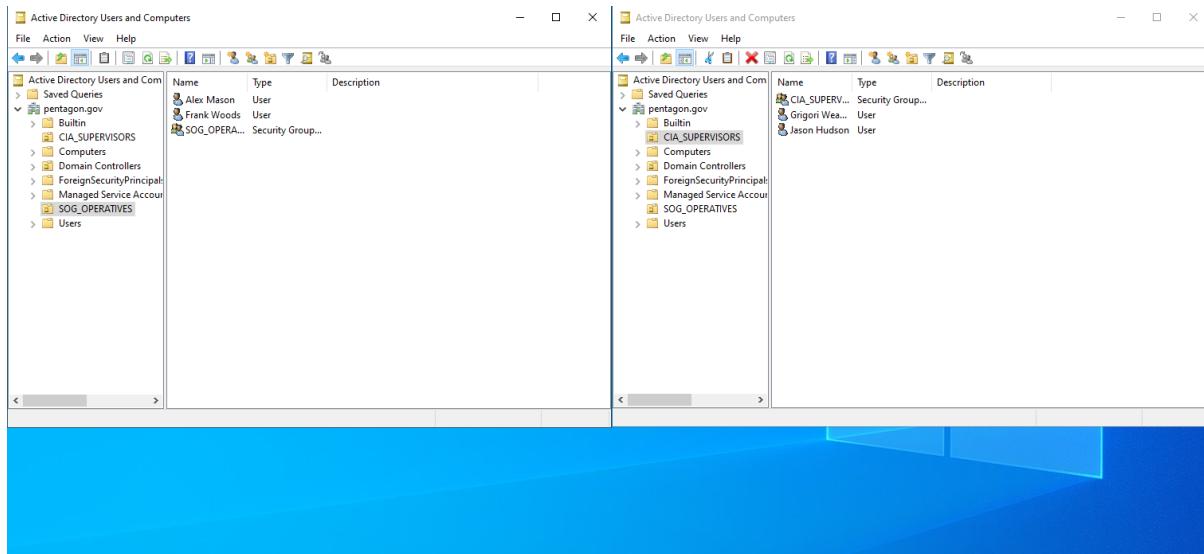
*Fig.2 Verifica permessi amministrativi



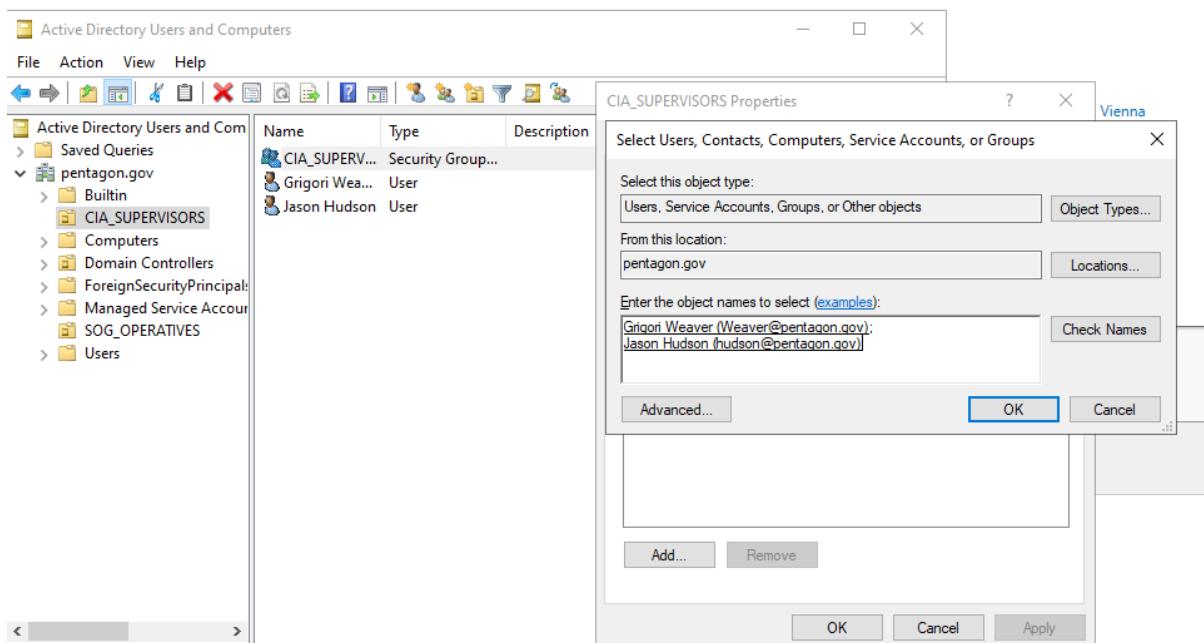
*Fig.3 Verifica permessi amministrativi

Una volta reso operativo il server **ASCENSION**, il primo passo ha riguardato il **controllo dei permessi amministrativi**. È stato confermato l'accesso con privilegi elevati, condizione necessaria per poter procedere alla creazione di gruppi e alla loro gestione.

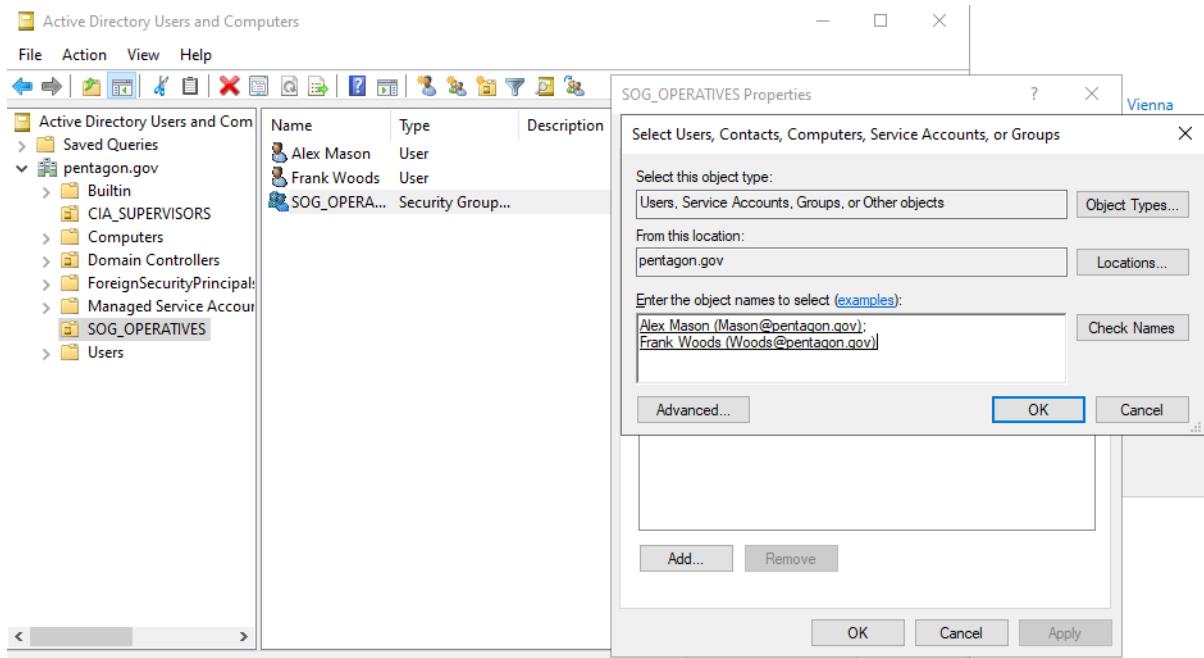
Fase2 – Creazione Gruppi



*Fig.4 Creazione Utenti e Gruppi



*Fig.5 Configurazione gruppo CIA



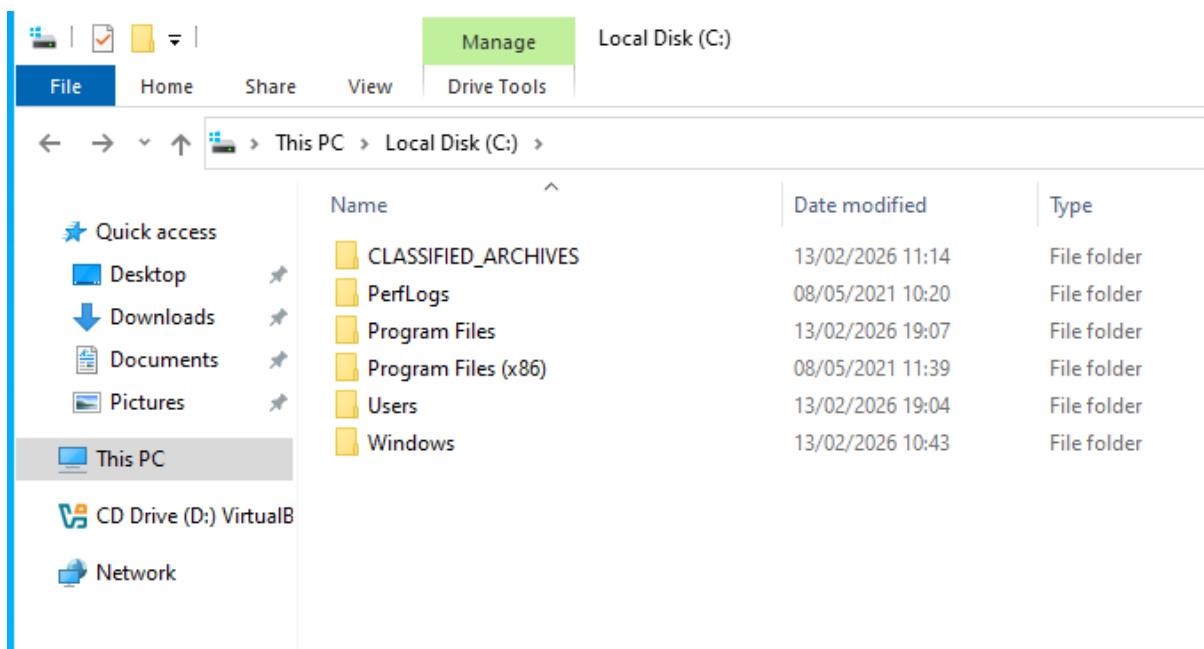
*Fig.6 Configurazione gruppo SOG

Per garantire una gestione ordinata delle risorse, sono state create due **Organizational Unit** distinte: **CIA_SUPERVISORS** e **SOG_OPERATIVES**. All'interno di ciascuna unità sono stati inseriti i relativi account utente:

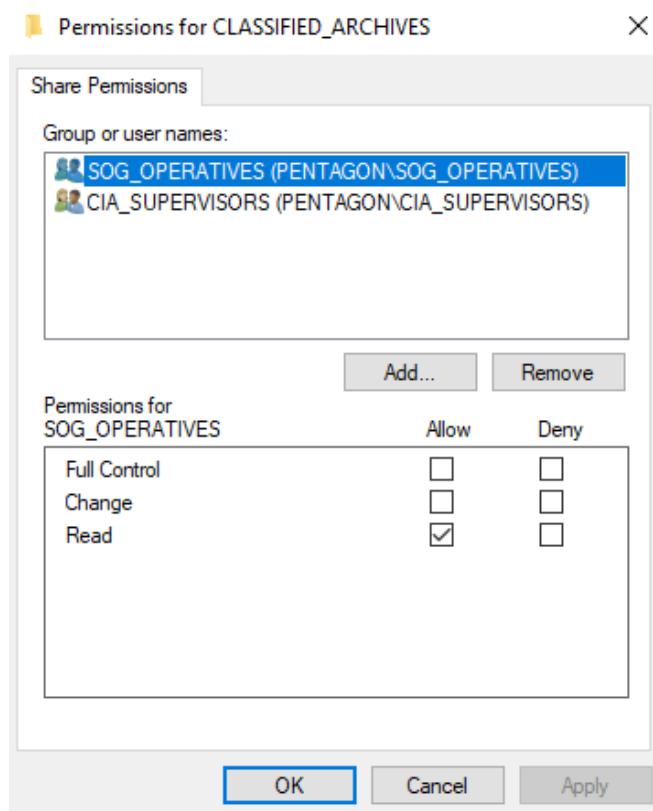
1. **Hudson e Weaver:** CIA_SUPERVISORS
- 2 . **Mason e Woods:** SOG_OPERATIVES

Infine, ogni utente è stato associato al rispettivo **Gruppo** per facilitare l'assegnazione dei permessi.

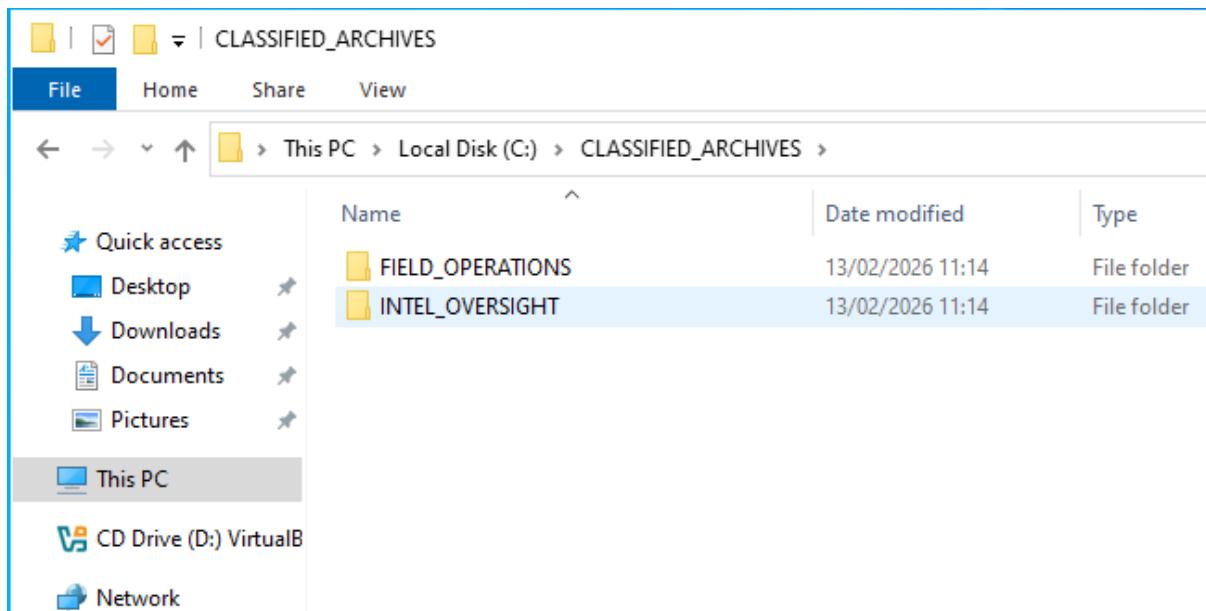
Fase3 – Assegnazione Permessi



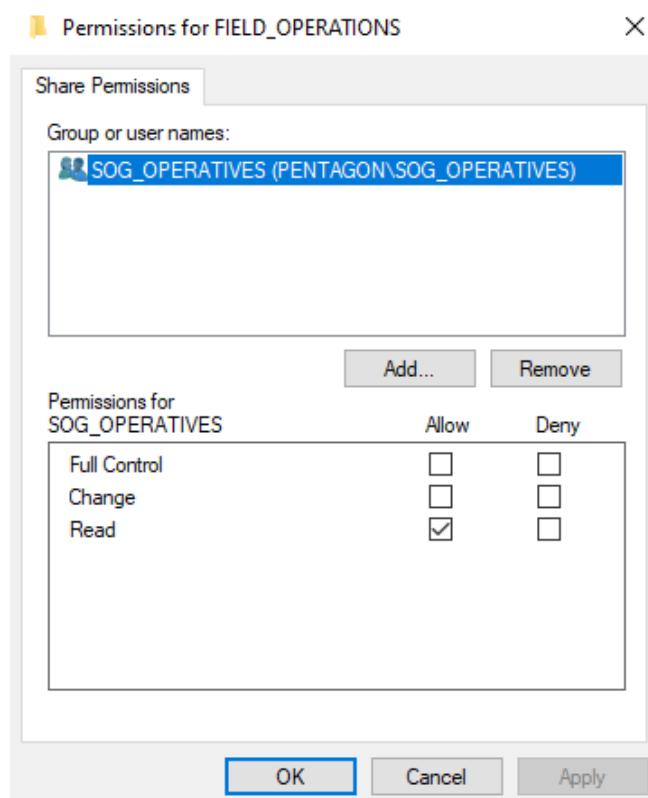
*Fig. 7 Creazione cartella condivisa



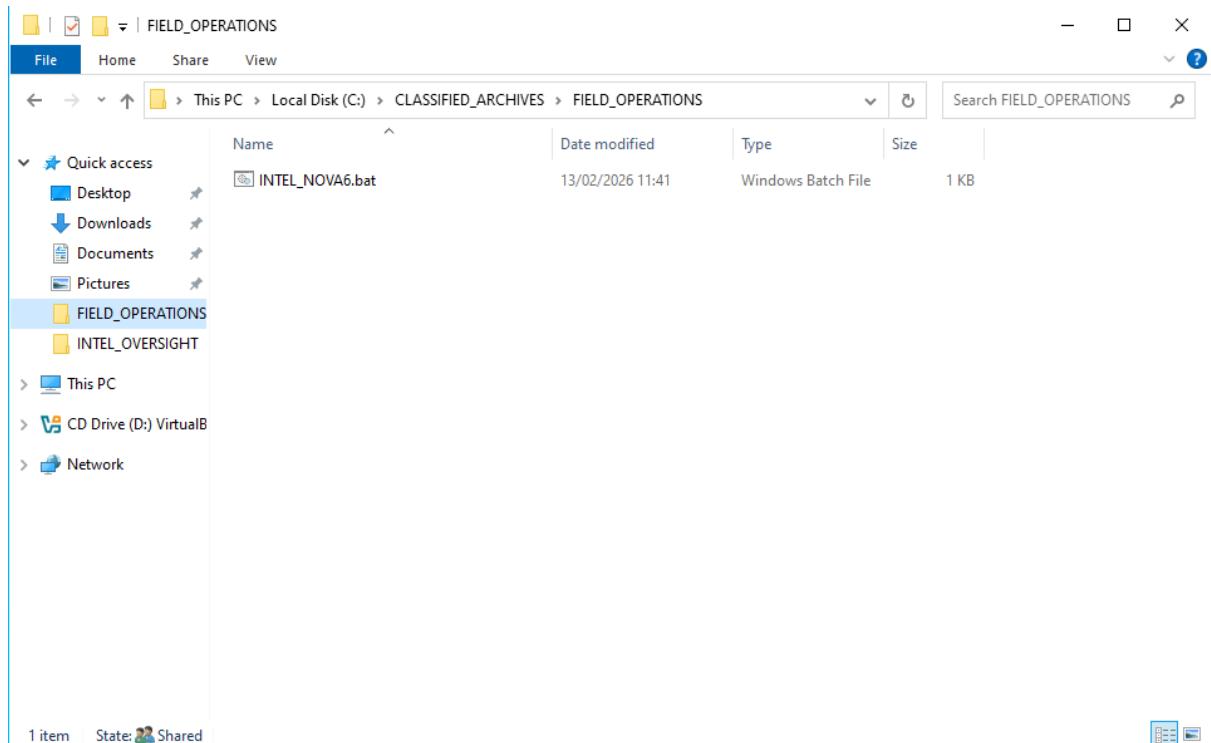
*Fig. 8 Assegnazione utenti



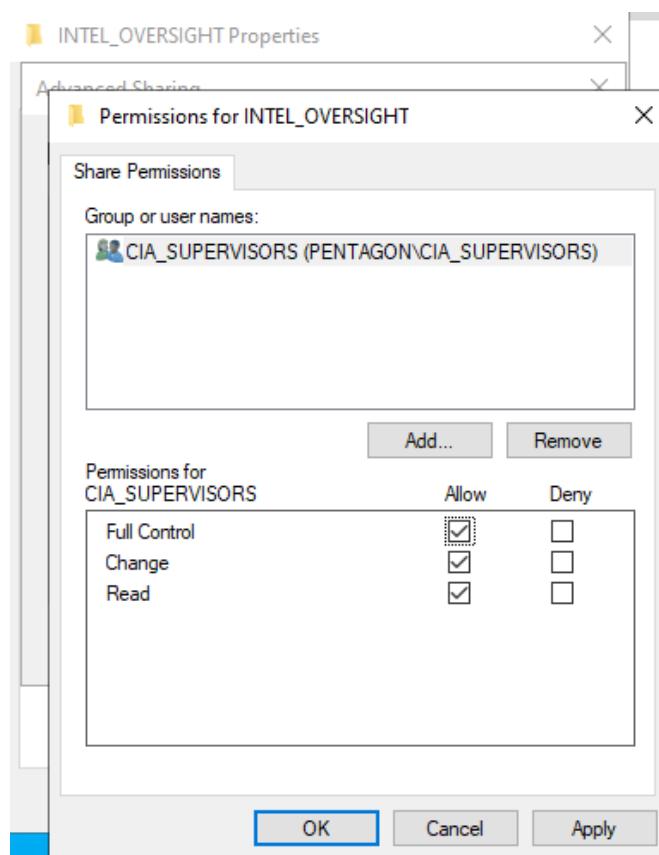
*Fig.9 Creazione cartelle separate



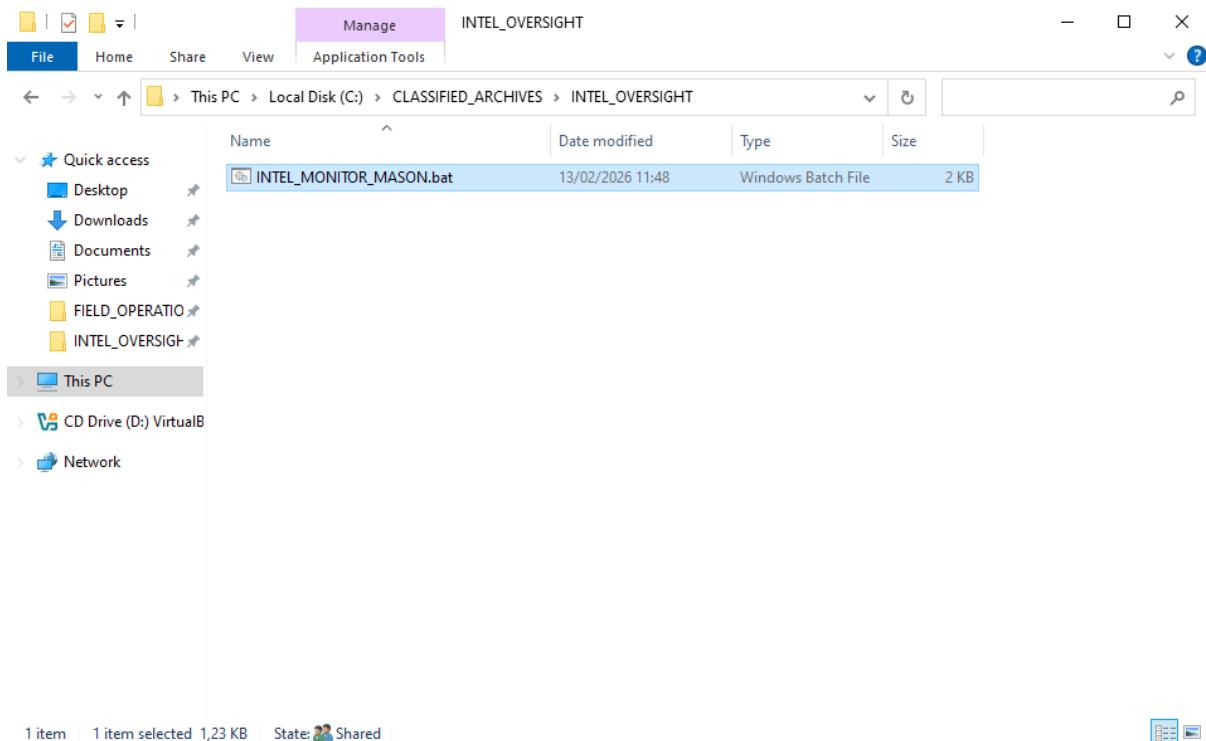
*Fig.10 Assegnazione permessi SOG



*Fig. 11 Creazione file SOG



*Fig. 12 Assegnazione permessi CIA



*Fig. 13 Creazione file CIA

È stata creata una cartella principale accessibile solo ai due reparti. (**CLASSIFIED_ARCHIVE**). Per garantire la massima sicurezza, i permessi sono stati configurati in modalità Solo Lettura per i gruppi **CIA_SUPERVISORS** e **SOG_OPERATIVES** per impedire in caso di compromissione di un utente di alterare la struttura della directory.

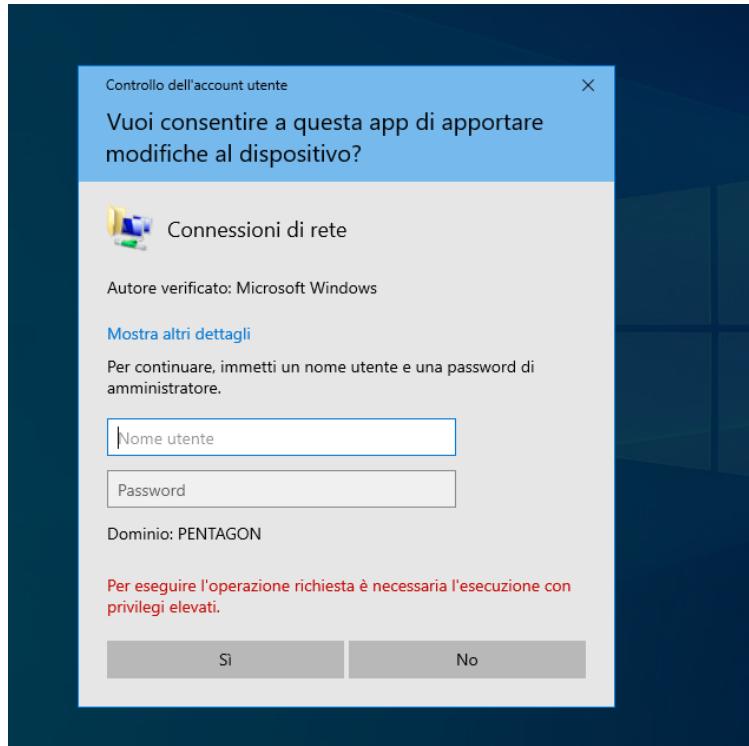
All'interno di **INTEL_OVERSIGHT**, sono stati assegnati permessi di Controllo Completo esclusivamente al gruppo **CIA** poiché, essendo coordinatori e supervisori, gli agenti della CIA devono poter aggiornare i file Intel, caricare nuovi rapporti e gestire il ciclo di vita dei documenti.

In **FIELD_OPERATIONS**, l'accesso è stato limitato al solo gruppo **SOG** con permessi di sola **revisione** dato che sono considerati elementi operativi sul campo ed il loro compito è esclusivamente ricevere ed eseguire gli ordini.

In conformità con le direttive del **Pentagono**, ogni sottocartella contiene un file **.bat** configurato per **l'autodistruzione istantanea**.

Lo script viene eseguito correttamente e, una volta terminata la lettura, rimuove sé stesso dal server, lasciando la directory vuota.

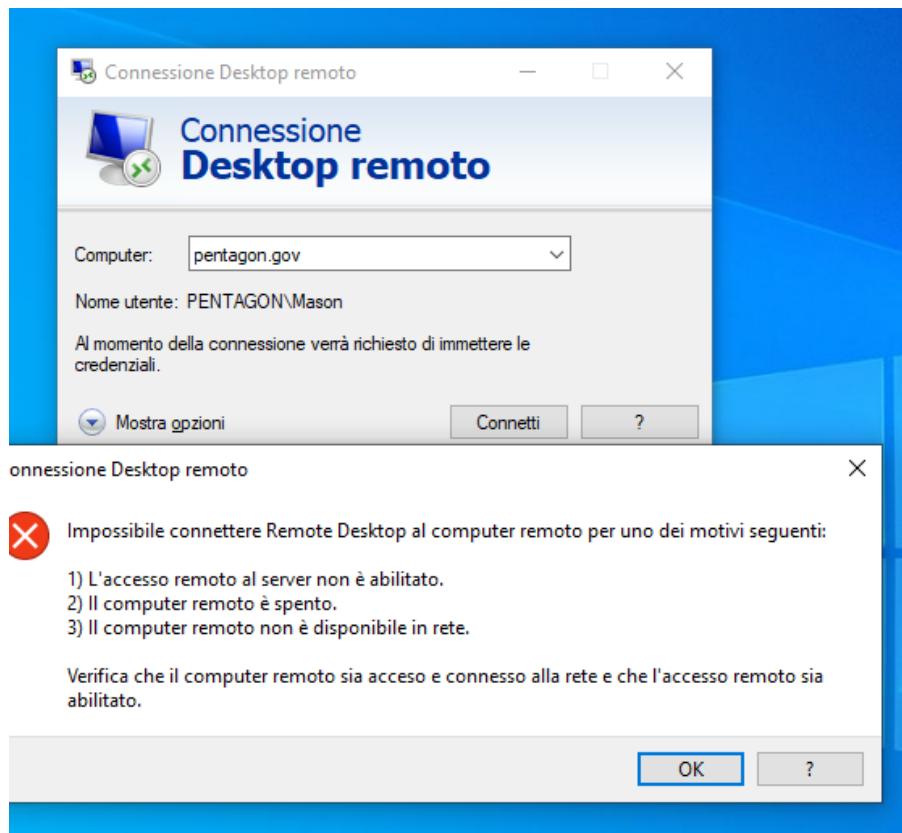
I gruppi **CIA_SUPERVISORS** e **SOG_OPERATIVES** non hanno permessi di amministrazione sul sistema, questo per garantire la stabilità del server. Solo l'utente **Administrator** può farlo.



*Fig.14 Prova configurazione rete

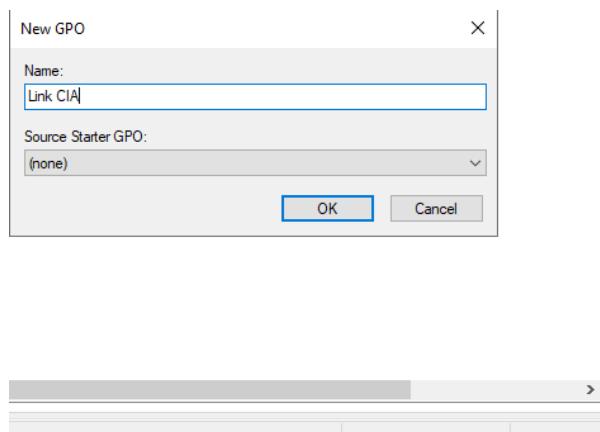


*Fig. 15 Prova esecuzione software

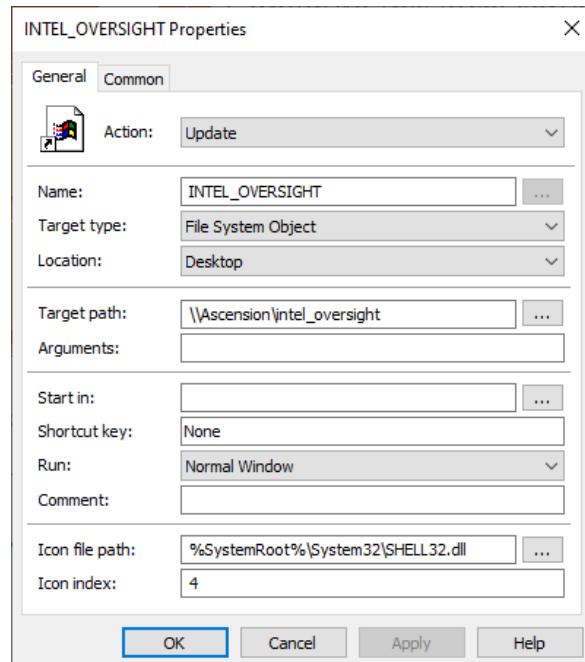


*Fig. 16 Prova remote desktop

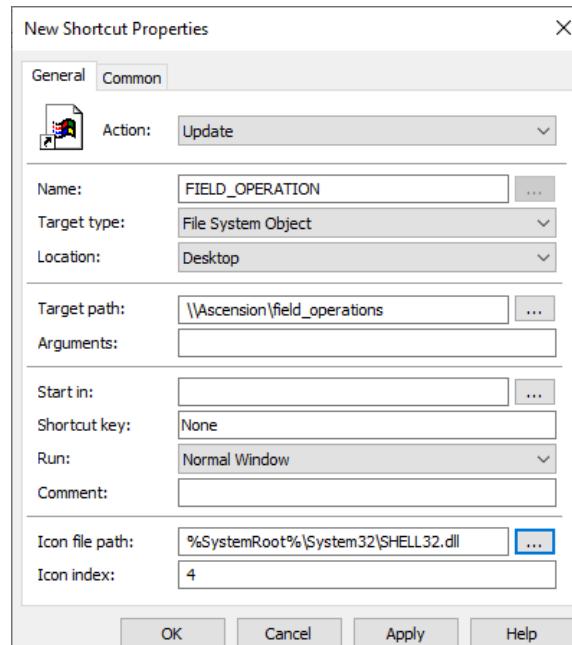
FASE4- Creazione collegamento cartella



*Fig. 17 Creazione link cartelle



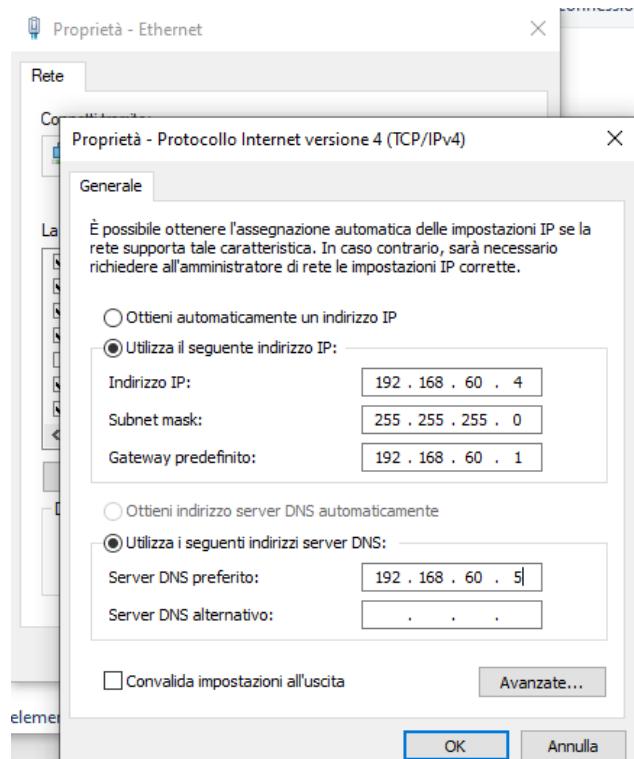
*Fig. 18 Configurazione link cartella CIA



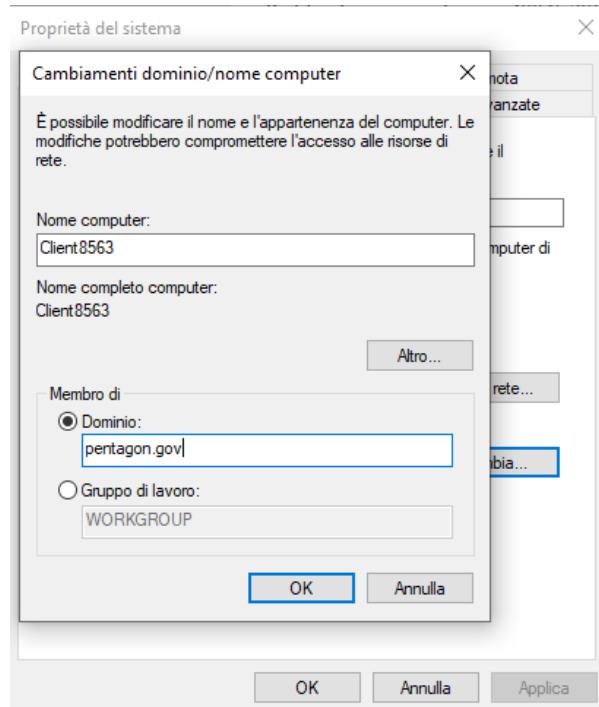
*Fig. 19 Configurazione link cartella SOG

Al fine di ottimizzare l'operatività degli utenti, sono stati configurati i collegamenti delle rispettive cartelle. Questo passaggio permette di visualizzare la cartella specifica sul desktop dell'utente, garantendo un accesso immediato al momento del login.

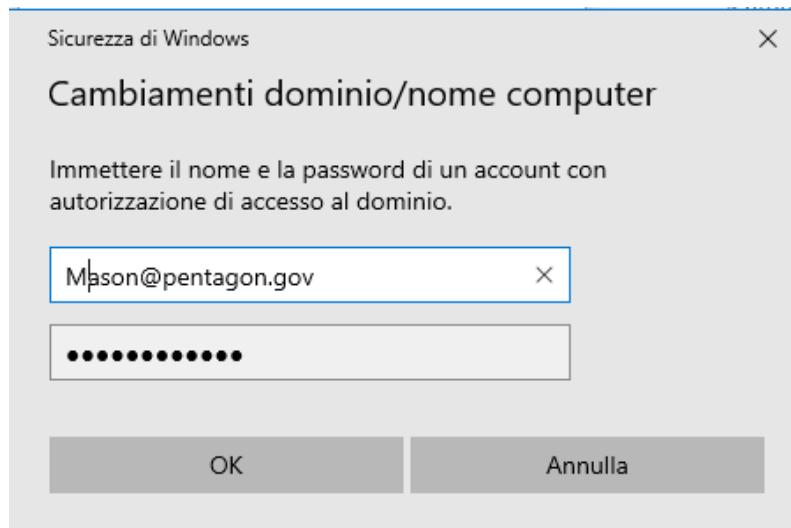
FASE5 – Configurazione macchina utente



*Fig.20 Configurazione rete macchina



*Fig.21 Configurazione dominio

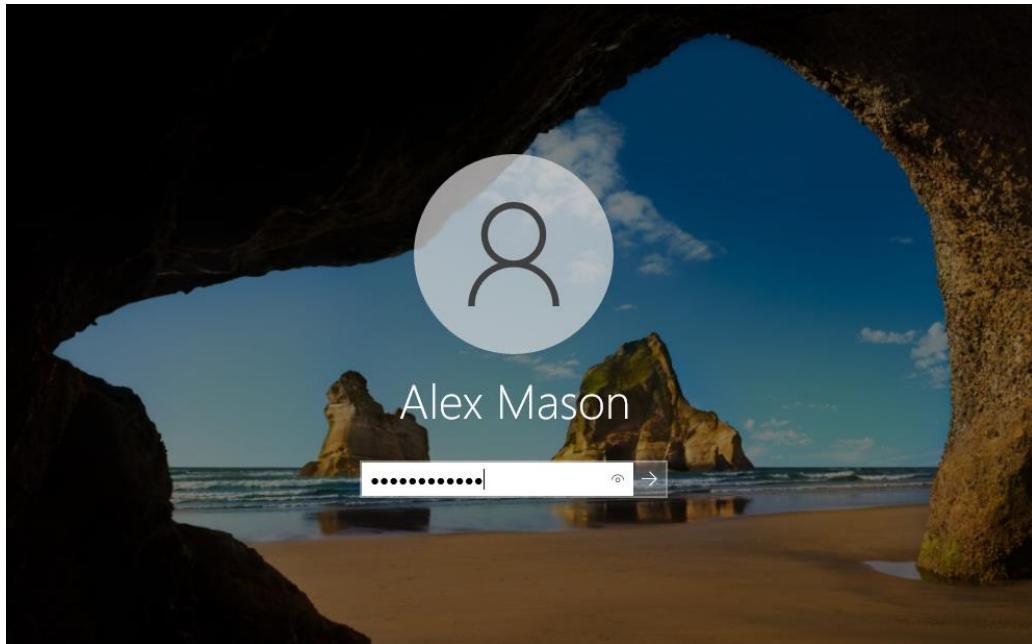


*Fig.22 Configurazione utente

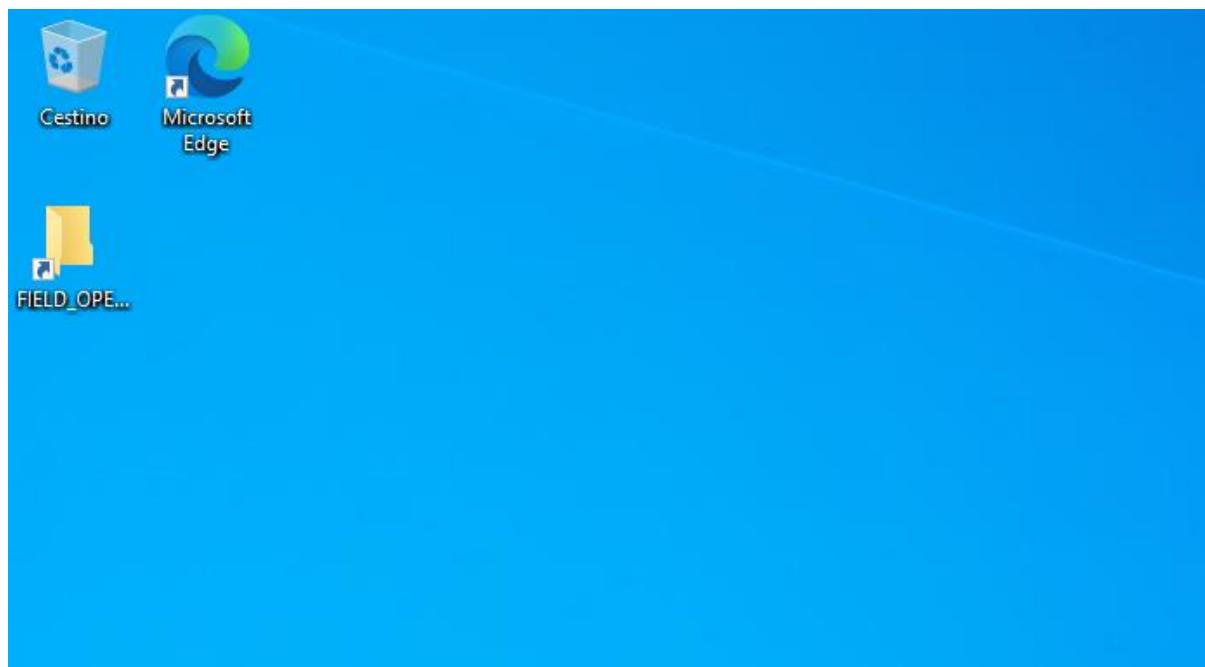
Completata la configurazione lato server, si è proceduto alla preparazione del client impostando un **indirizzo IP statico** corrispondente con la sottorete del server. Una volta stabilita la connessione, la macchina è stata aggiunta al dominio **pentagon.gov**, permettendo così l'autenticazione dell'utente **Mason** con le credenziali configurate in **Active Directory**.

Lo stesso protocollo è stato seguito per l'utente **Hudson**, permettendo anche a quest'ultimo di autenticarsi dal proprio client.

Fase6 – Verifica permessi

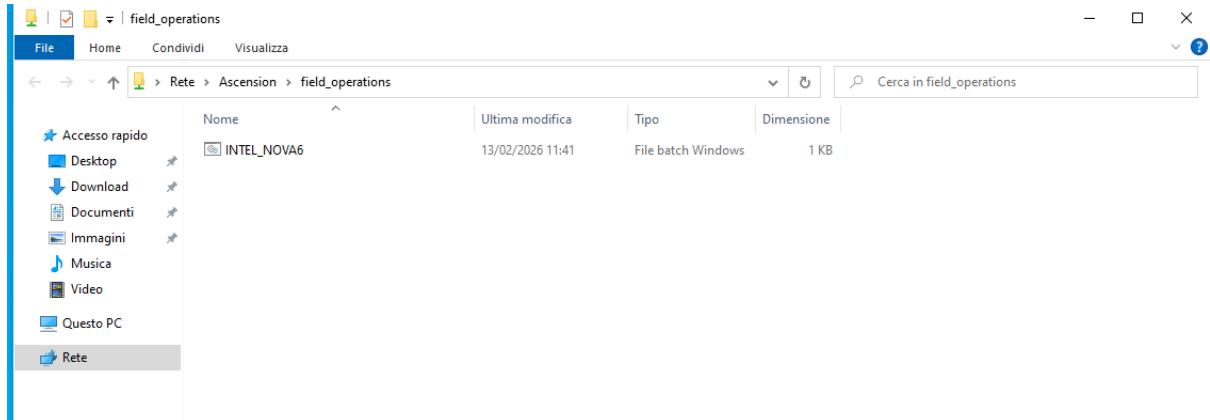


*Fig.23 Accesso utente Mason



*Fig.24 Desktop utente Mason

Come evidenziato nella **Fig. 24**, al momento del login, l'interfaccia desktop dell'utente **Mason** presenta il **collegamento diretto**, garantendo l'accesso immediato alle risorse riservate al gruppo **SOG**.



*Fig.25 Verifica contenuto cartella SOG

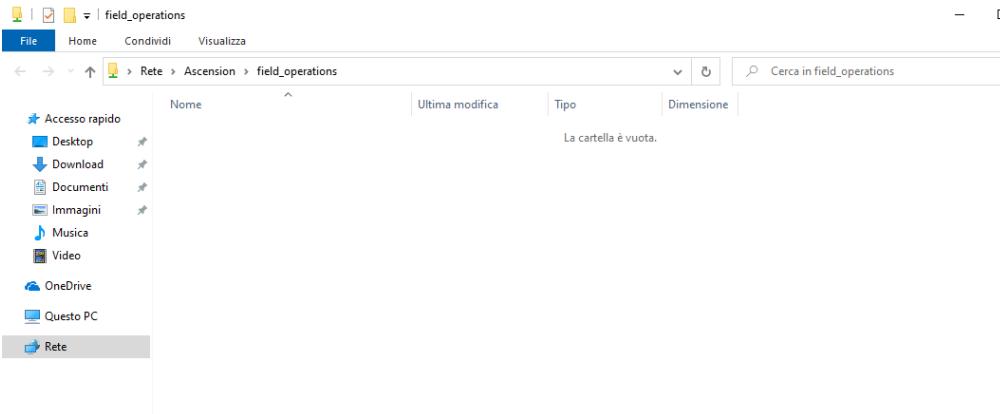
```
#####
#
#          PENTAGON DATA STREAM: INTEL_8-15
#
#####
SOG OPERATIVE: MASON, A.;WOODS, F.

L'obiettivo e' la base di test di armi chimiche russa.
Coordinate: 45.3900 N, 59.4400 E.
Distruggete i campioni di Nova-6 e caricate i dati.

ATTENZIONE: Una volta chiuso questo terminale,
questo file sara eliminato permanentemente per
evitare che cada in mani nemiche.

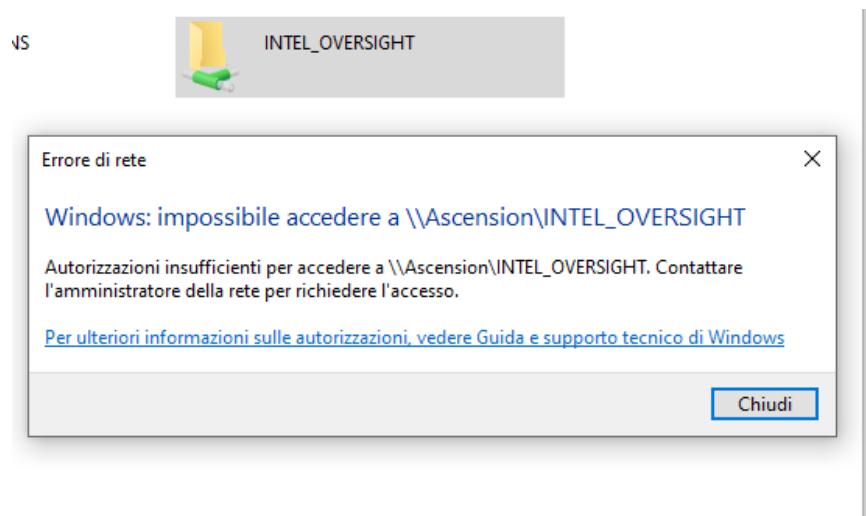
=====
Premere qualsiasi tasto per confermare la lettura e distruggere...
```

*Fig.26 Avvio file



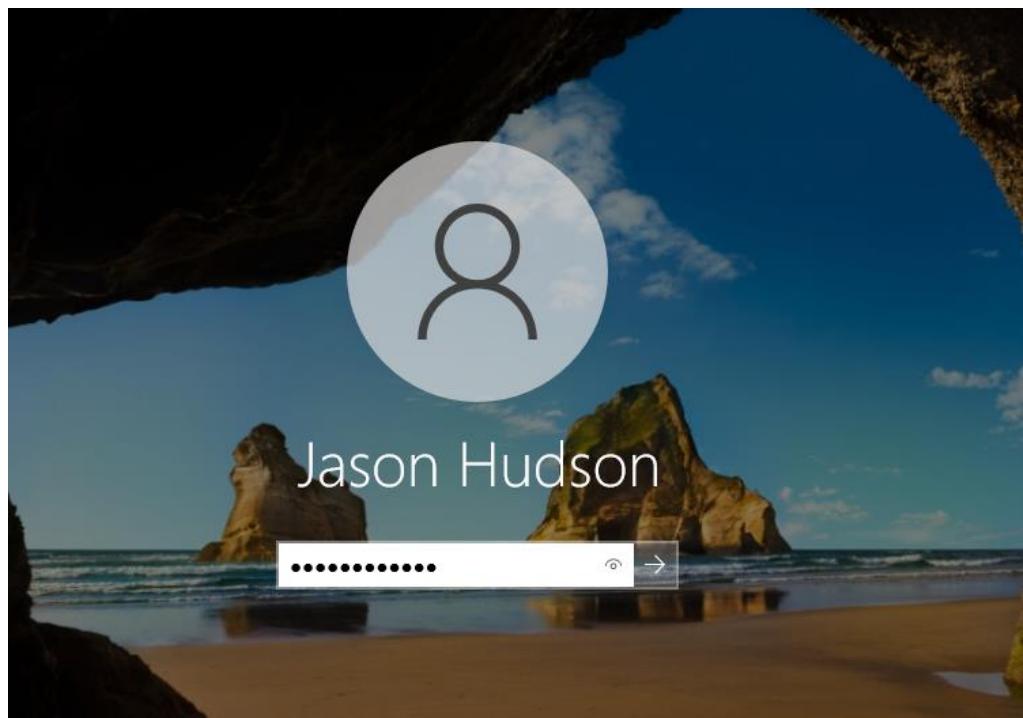
*Fig.27 Contenuto cartella post esecuzione

Come documentato nelle immagini, l'utente avvia il file per leggere l'Intel della missione. Una volta conclusa la lettura, il sistema innesca un protocollo di **autoeliminazione** del file per eliminare ogni traccia di informazioni in caso di compromissione dell'utente.

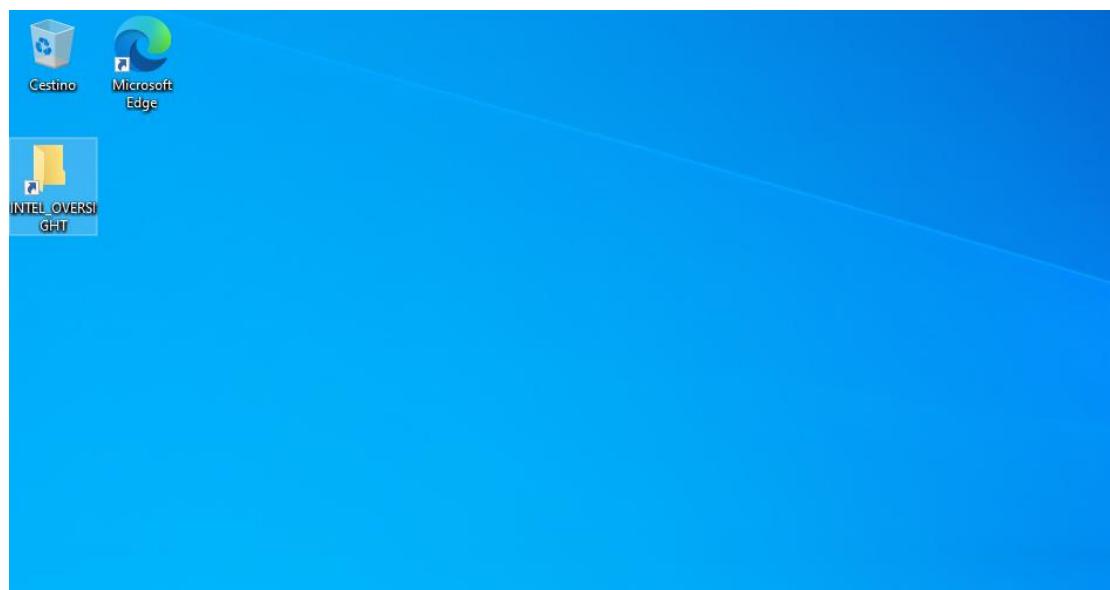


*Fig.28 Accesso cartella CIA con utente Mason

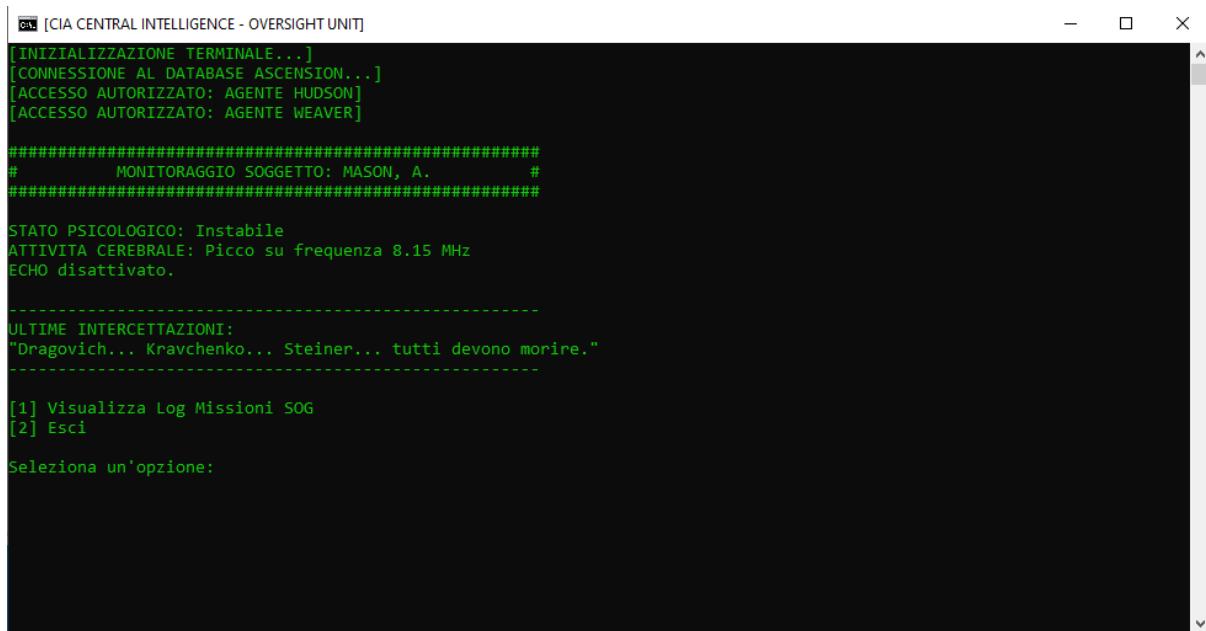
Si è proceduto inoltre alla **verifica delle policy di sicurezza**, come previsto dalla configurazione, il sistema ha impedito l'apertura della cartella riservata alla **CIA** da parte di utenti appartenenti al gruppo **SOG**.



*Fig.29 Accesso utente Hudson



*Fig.30 Desktop utente Hudson



```
[cia] [CIA CENTRAL INTELLIGENCE - OVERSIGHT UNIT]
[INIZIALIZZAZIONE TERMINALE...]
[CONNESSIONE AL DATABASE ASCENSION...]
[ACCESSO AUTORIZZATO: AGENTE HUDSON]
[ACCESSO AUTORIZZATO: AGENTE WEAVER]

#####
#      MONITORAGGIO SOGGETTO: MASON, A.      #
#####

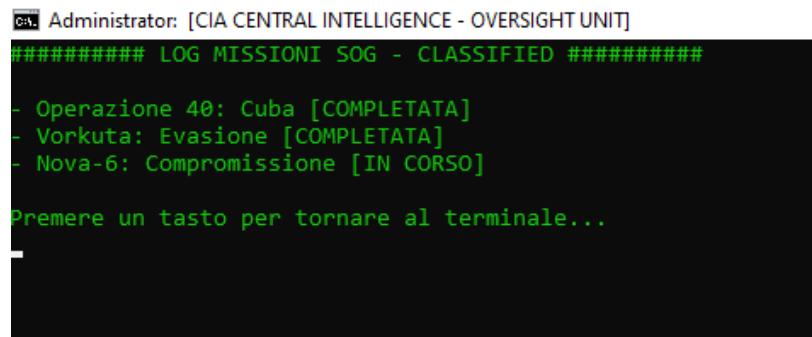
STATO PSICOLOGICO: Instabile
ATTIVITA CEREBRALE: Picco su frequenza 8.15 MHz
ECHO disattivato.

-----
ULTIME INTERCETTAZIONI:
"Dragovich... Kravchenko... Steiner... tutti devono morire."
-----

[1] Visualizza Log Missioni SOG
[2] Esci

Seleziona un'opzione:
```

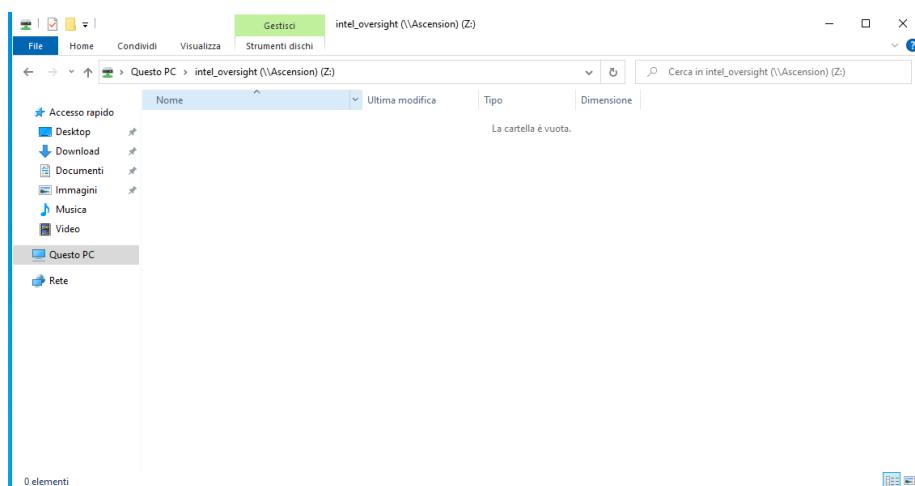
*Fig.31 Avvio file



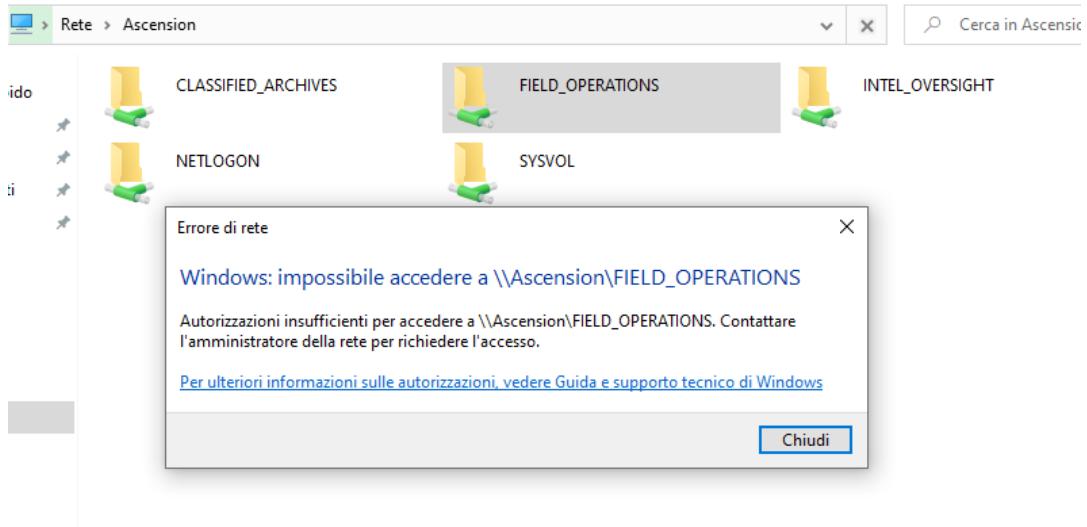
```
[cia] Administrator: [CIA CENTRAL INTELLIGENCE - OVERSIGHT UNIT]
#####
# LOG MISSIONI SOG - CLASSIFIED #####
- Operazione 40: Cuba [COMPLETATA]
- Vorkuta: Evasione [COMPLETATA]
- Nova-6: Compromissione [IN CORSO]

Premere un tasto per tornare al terminale...
-
```

*Fig.32 Avvio file



*Fig.33 Contenuto cartella post esecuzione



*Fig.34 Accesso cartella SOG con utente Hudson

I medesimi test di validazione sono stati eseguiti con successo anche per l'utente **Hudson**, confermando la coerenza dei permessi di accesso e l'isolamento dei dati tra i due reparti.

Conclusione

In conclusione, l'attività svolta ha permesso la corretta implementazione e gestione dei permessi all'interno di **Active Directory**. La configurazione ha garantito un funzionamento ottimale e sicuro per entrambi i gruppi operativi, assicurando che ogni utente potesse accedere esclusivamente alle risorse di propria competenza. Queste policy vengono inoltre confermate anche dagli esiti riscontrati durante la fase di testing.