

Report Tecnico: Configurazione Client e Verifica ACL (Access Control Lists)

Studente: Nicola Cassandra

Data: 11 Febbraio 2026

Oggetto: Verifica configurazione di rete e test dei privilegi di accesso su Windows Server 2022

1. Introduzione: L'Importanza della Configurazione e dei Permessi

Questo report documenta la fase finale dell'esercizio di configurazione su Windows Server 2022. L'obiettivo non è solo garantire che le macchine comunichino, ma assicurare che i principi della **CIA Triad** (Confidentiality, Integrity, Availability) siano rispettati, con particolare enfasi sulla *Confidenzialità*.

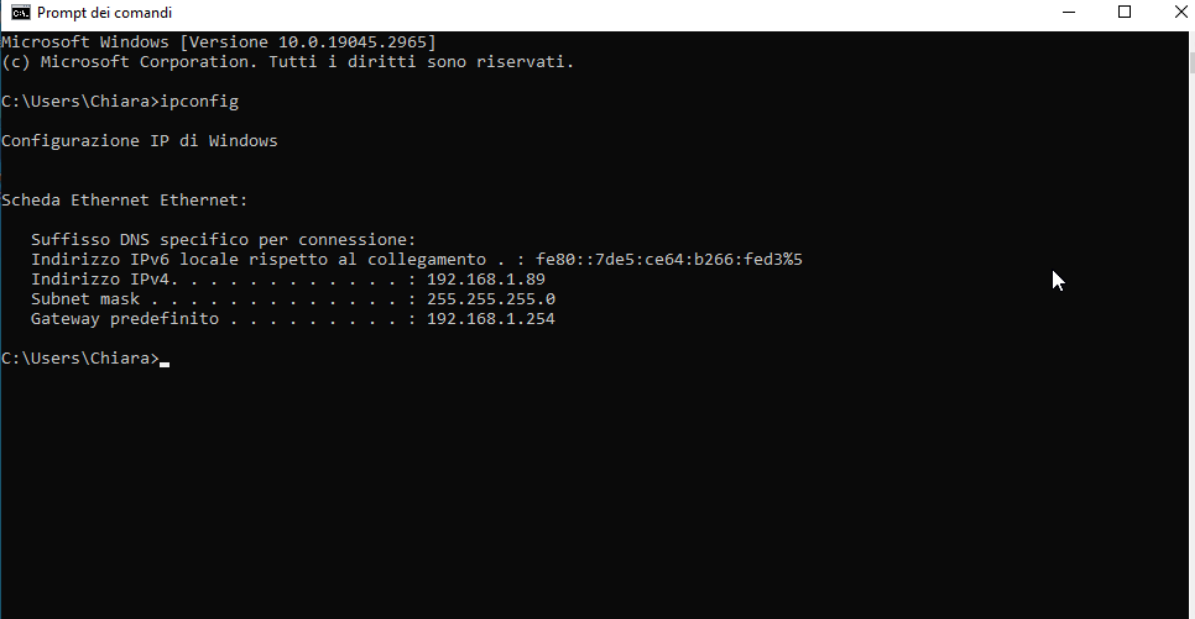
Nel mondo della Cyber Security, una configurazione di rete corretta è il prerequisito per qualsiasi servizio, ma la gestione dei permessi (Authorization) è ciò che protegge i dati sensibili.

In questo scenario, stiamo applicando il **Principio del Privilegio Minimo (Principle of Least Privilege)**: un utente (Chiara) deve avere accesso *solo* alle risorse necessarie per il suo ruolo e a nient'altro. Un errore di "Accesso Negato" non è sempre un fallimento tecnico; in sicurezza, spesso è la prova che il sistema di difesa sta funzionando correttamente.

2. Analisi Tecnica delle Evidenze

Di seguito analizziamo gli screenshot prodotti durante la sessione di verifica, come richiesto dalla traccia.

A. Configurazione di Rete (Network Configuration)



```
Prompt dei comandi
Microsoft Windows [Versione 10.0.19045.2965]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\Chiara>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::7de5:ce64:b266:fed3%5
    Indirizzo IPv4. . . . . : 192.168.1.89
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.254

C:\Users\Chiara>
```

Fig 1. Output del comando `ipconfig` dal prompt dei comandi dell'utente Chiara. Si evidenzia l'indirizzo IPv4 configurato (192.168.1.89) e la connettività con il Gateway (192.168.1.254).

Dall'analisi del prompt dei comandi (`ipconfig`), emerge che la workstation dell'utente *Chiara* è correttamente configurata per operare nella rete aziendale.

- **Indirizzo IPv4:** 192.168.1.89
- **Subnet Mask:** 255.255.255.0 (o /24)
- **Gateway Predefinito:** 192.168.1.254

La macchina ha un IP statico valido che le permette di comunicare con il server che è sulla stessa sottorete.

B. Verifica Accesso Risorse Autorizzate

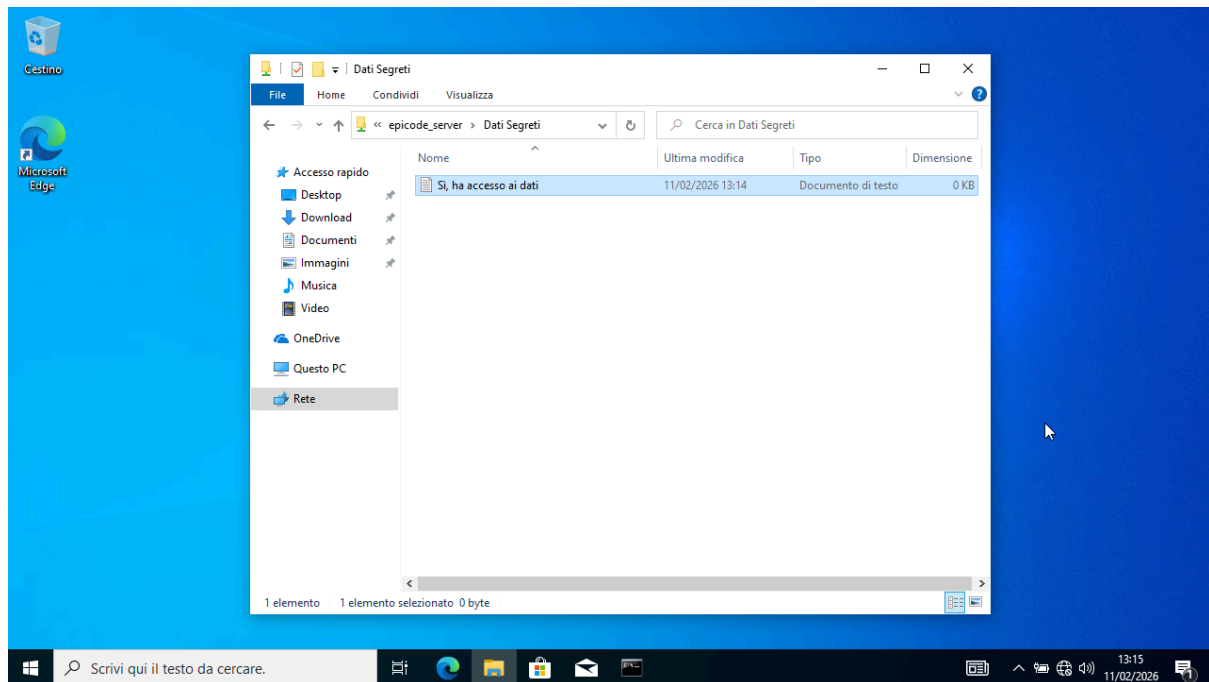


Fig 2. Esplora Risorse mostra l'accesso riuscito alla cartella di rete condivisa `\\epicode_server\Dati Segreti`. All'interno è visibile il file di test creato dall'utente, confermando i permessi di Lettura e Scrittura.

L'utente ha tentato l'accesso alla risorsa di rete condivisa `\\epicode_server\Dati Segreti`.

- **Esito:** Accesso Riuscito.
- **Contenuto:** È visibile un file di testo creato alle 13:14 del 11/02/2026 denominato "Si, ha accesso ai dati".

Questo conferma che le **Share Permissions** (permessi di condivisione) e le **NTFS Permissions** (permessi sul file system) sono state configurate correttamente per consentire a Chiara la lettura (e probabilmente la scrittura) in questa cartella. L'obiettivo di verificare che "Chiara abbia accesso alle risorse previste" è stato raggiunto.

C. Verifica Negazione Accesso (Access Control Enforcement)

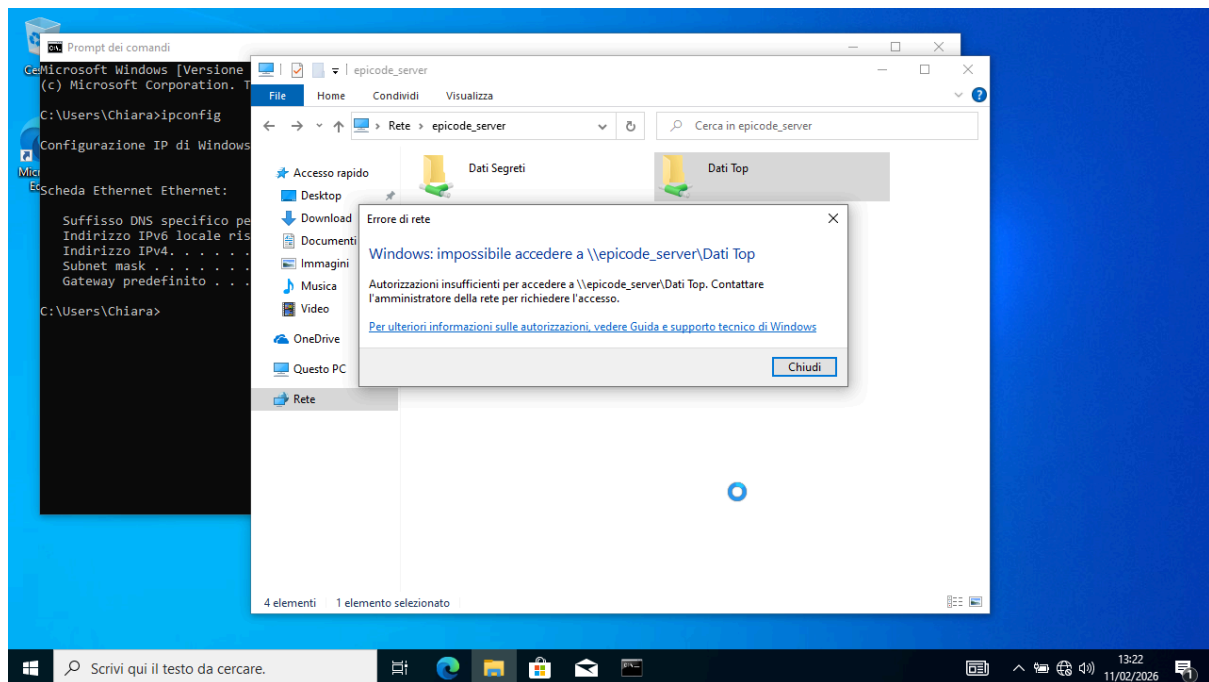


Fig. 3. Tentativo di accesso alla risorsa riservata `\\epicode_server\Dati Top`. Il sistema risponde con un messaggio di errore "Accesso Negato", confermando che l'utente Chiara non possiede le autorizzazioni necessarie.

L'utente ha tentato l'accesso alla risorsa `\\epicode_server\Dati Top`.

- **Esito:** Accesso Negato ("*Windows: impossibile accedere a... Autorizzazioni insufficienti*").
- **Analisi:** Il sistema ha bloccato la richiesta.

Questo è un risultato dimostra che l'utente Chiara non fa parte del gruppo di sicurezza autorizzato per i dati "Top" (probabilmente riservati agli amministratori o al management). Il sistema ha applicato correttamente le restrizioni, proteggendo la risorsa da accessi non autorizzati.

3. Conclusione

L'esercitazione ha dimostrato con successo che:

1. Il client è correttamente unito alla rete e comunicante con il server.
2. L'autenticazione dell'utente *Chiara* avviene correttamente.
3. Il sistema di autorizzazione discrimina correttamente tra le risorse accessibili ("Dati Segreti") e quelle proibite ("Dati Top").

La configurazione del Windows Server 2022 rispetta i requisiti di sicurezza e segmentazione dei dati richiesti.