

Report: Configurazione Sicurezza e Gestione Accessi

Progetto: Gestione Privilegiata e Controllo Accessi su Windows Server 2022

Host Identificato: SimpsonServer

Dominio: Simpson.local

Data di Emissione: 14 Febbraio 2026

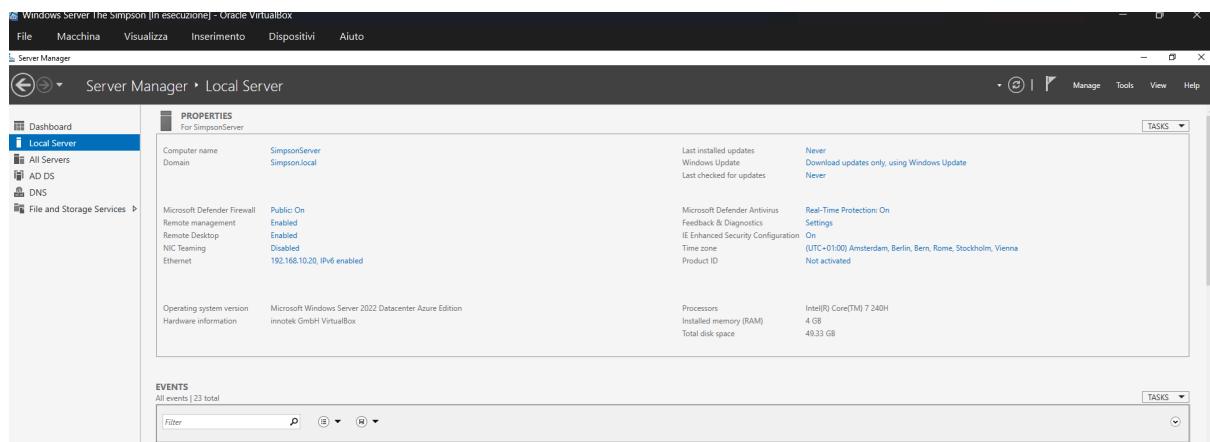
1. Executive Summary

L'attività ha riguardato il deployment di una struttura di **Role-Based Access Control (RBAC)** finalizzata alla protezione degli asset informativi e alla gestione delle identità. Sono stati definiti due profili di accesso distinti per i dipartimenti di Amministrazione e Sicurezza, applicando il principio del minimo privilegio per il personale operativo e garantendo la piena operatività al personale amministrativo.

2. Infrastruttura di Dominio e Identità

La configurazione ha previsto la creazione di un ecosistema centralizzato per la gestione degli oggetti.

- Naming Convention:** Il server è stato rinominato **SimpsonServer** per garantire la tracciabilità nei log di audit.



- **Active Directory (AD DS):** È stata implementata una struttura a Unità Organizzative (OU) per separare logicamente le funzioni aziendali.
 - **OU Amministrazione:** Contenitore per account ad alto privilegio come **Mr Burns**.
 - **OU Sicurezza:** Contenitore per i gruppi preposti alla vigilanza dei dati.

Server Manager > Dashboard

Active Directory Users and Computers

Name	Type	Description
Amministraz...	Organizational...	
Builtin	builtinDomain	
Computers	Container	Default container for do...
Domain Con...	Organizational...	Default container for sec...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Sicurezza	Organizational...	
Users	Container	Default container for up...
Utenti Stand...	Organizational...	

Storage 1 Availability

Local Server 1 Manageability

All Servers 1 Manageability

Server Manager > Dashboard

Active Directory Users and Computers

New Object - User

Name	Type	Description
Montgomery	User	

Create in: Simpson.local/Amministrazione

First name: Montgomery Initials:

Last name: Burns

Full name: Montgomery Burns

User logon name: Mr Burns@Simpson.local

User logon name (pre-Windows 2000):

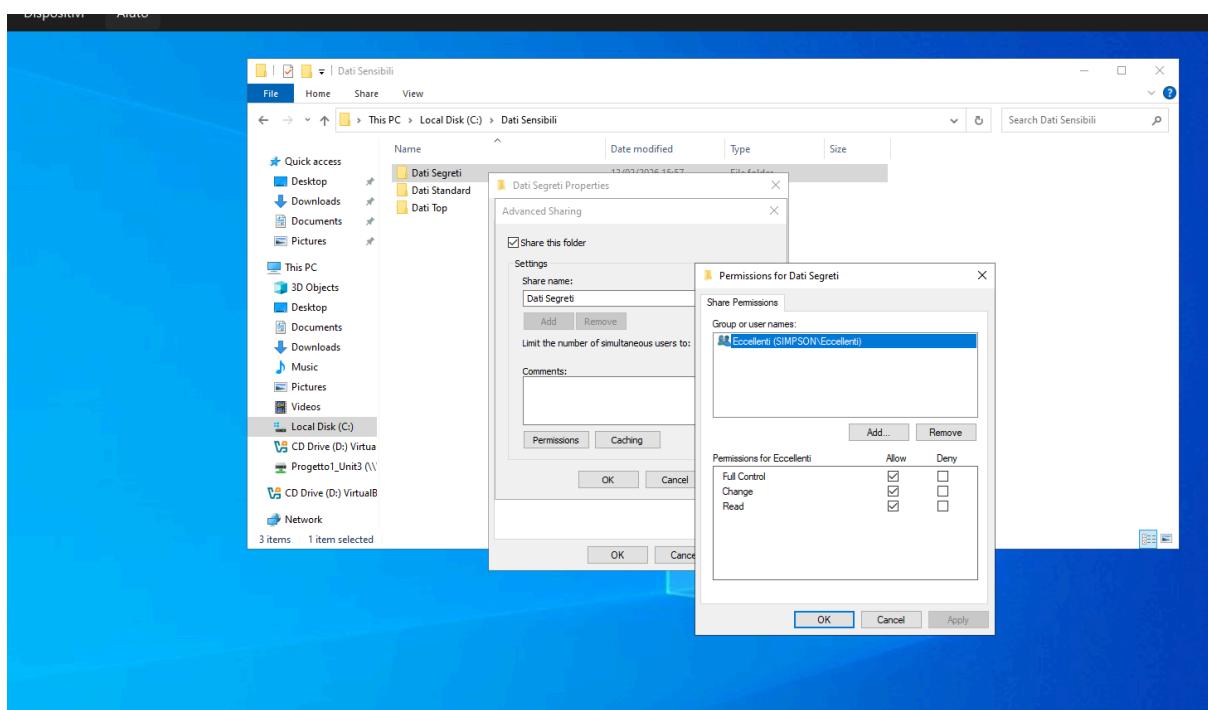
3. Matrice delle Autorizzazioni e Permessi

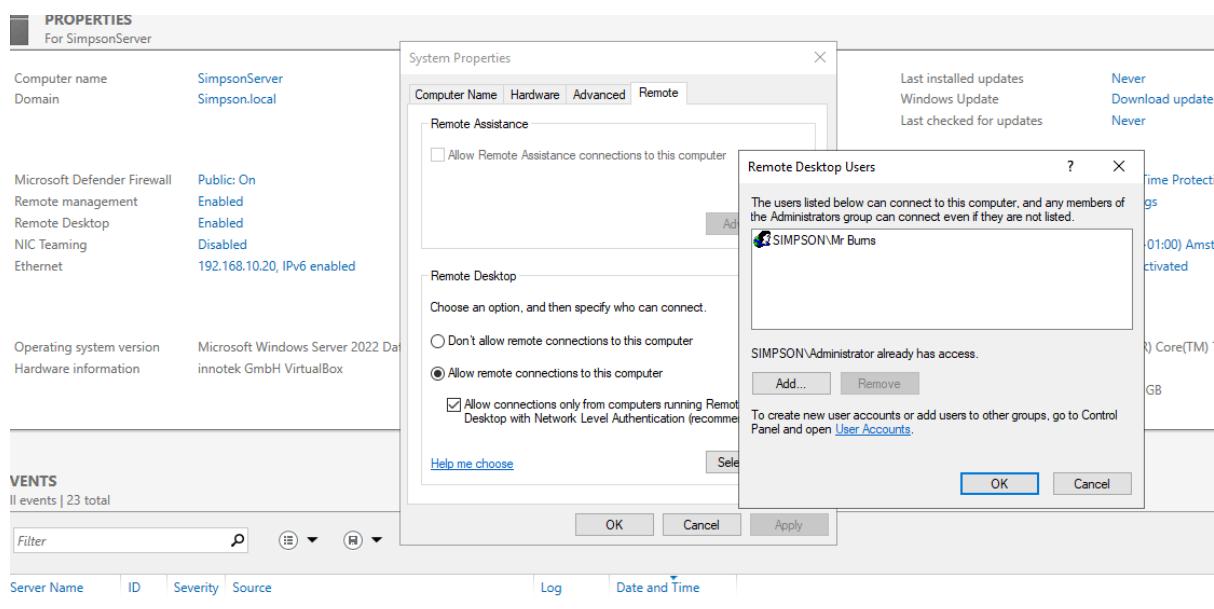
In base ai requisiti tecnici, è stata definita la seguente matrice di accesso per i gruppi di sicurezza:

3.1 Profilo: Amministrazione (Gruppo "Eccellenti")

Il gruppo dispone di un controllo totale sul sistema per consentire la manutenzione e la gestione strategica.

- Accesso File/Cartelle:** Possiede "Full Control" sulla cartella **C:\Dati Sensibili\Dati Segreti**.
- Esecuzione Programmi:** Autorizzato all'esecuzione di software di sistema e gestionali critici.
- Modifiche Impostazioni:** Permesso di alterare configurazioni di registro, servizi e policy di gruppo.
- Accesso Remoto (RDP):** Abilitato tramite l'impostazione "Allow remote connections" con **Network Level Authentication (NLA)** attivo.

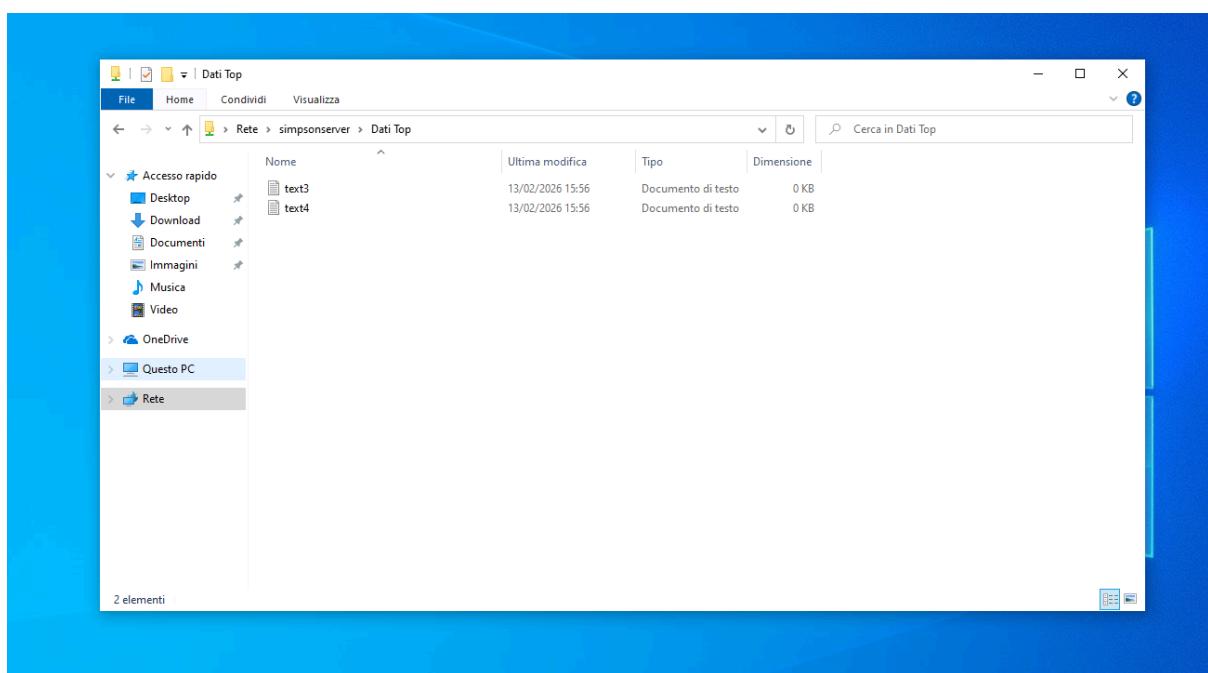
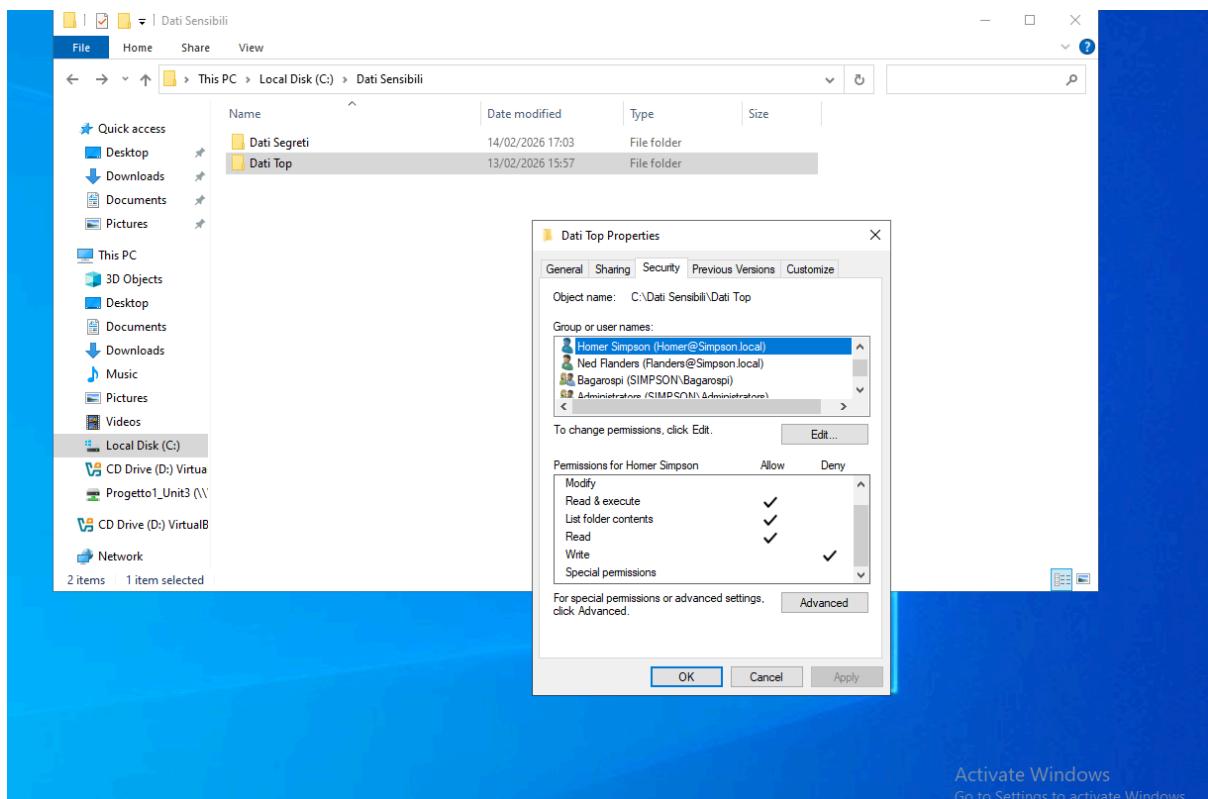


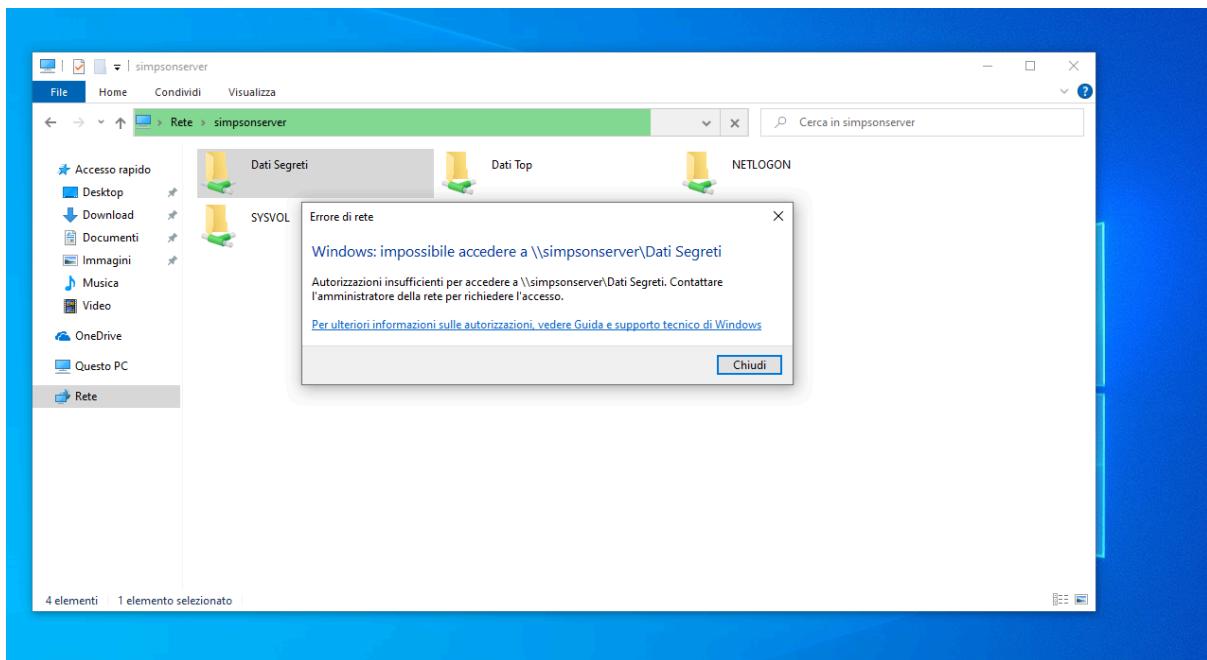


3.2 Profilo: Sicurezza (Gruppo "Bagarospi")

Il gruppo opera in un ambiente ristretto, limitato esclusivamente alle funzioni di monitoraggio.

- Accesso File/Cartelle:** "Full Control" limitato alla sottocartella **C:\Dati Sensibili\Top**.
- Esecuzione Programmi:** Limitato a strumenti di analisi e programmi specifici approvati.
- Restrizioni Critiche:** Non autorizzato a modificare le impostazioni di sistema né ad accedere al server via Desktop Remoto (RDP).





4. Approfondimento Tecnico sulle Scelte di Configurazione

4.1 Gestione del File System (NTFS & Share)

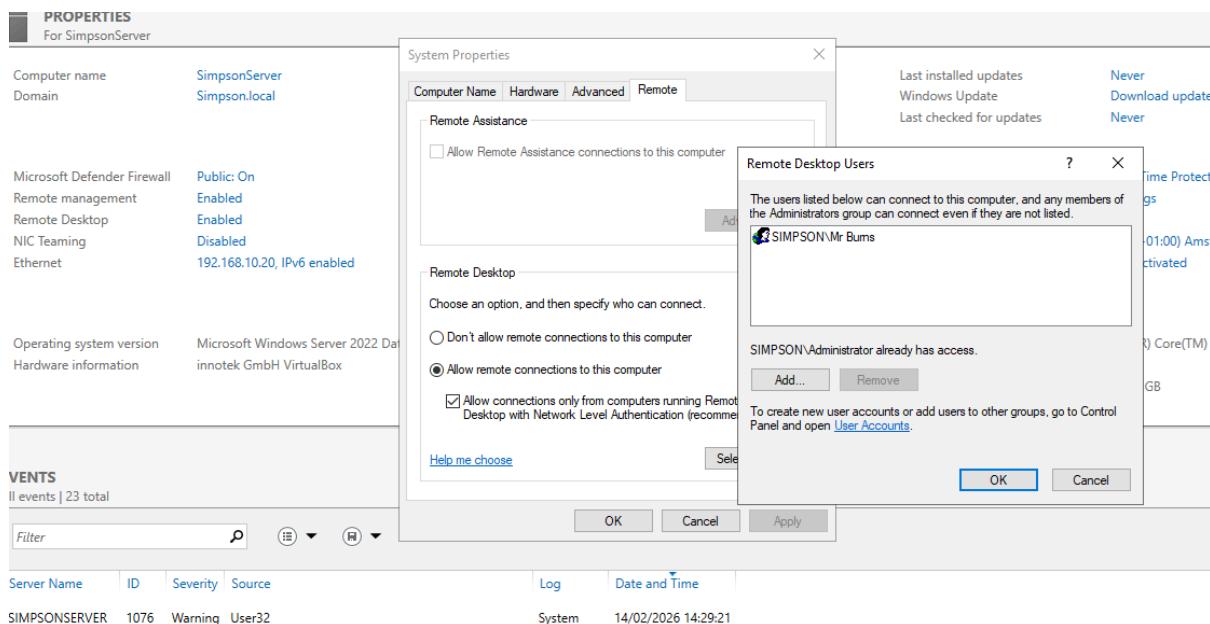
Per isolare i dati segreti, è stata applicata una combinazione di permessi di condivisione e liste di controllo accessi (ACL).

- L'assegnazione del **Full Control** al gruppo **Eccellenti** sulla cartella **Dati Segreti** è stata scelta per permettere la gestione del ciclo di vita dei dati (creazione, modifica, cancellazione e assegnazione permessi).
- La segregazione è garantita dal fatto che il gruppo **Bagarospi** non compare nelle ACL della cartella amministrativa, risultando in un "Access Denied"隐式.

4.2 Hardening dell'Accesso Remoto (RDP)

L'accesso remoto è stato configurato nella scheda "Remote" delle proprietà di sistema.

- **Scelta Professionale:** L'attivazione dell'**NLA (Network Level Authentication)** garantisce che l'autenticazione avvenga prima della creazione della sessione RDP, proteggendo il server da vulnerabilità note come "BlueKeep".
- **Limitazione:** Solo i membri del gruppo **Eccellenti** sono stati aggiunti al gruppo locale *Remote Desktop Users*, impedendo ai **Bagarospi** di stabilire connessioni interattive.



4.3 Controllo dell'Esecuzione e Impostazioni

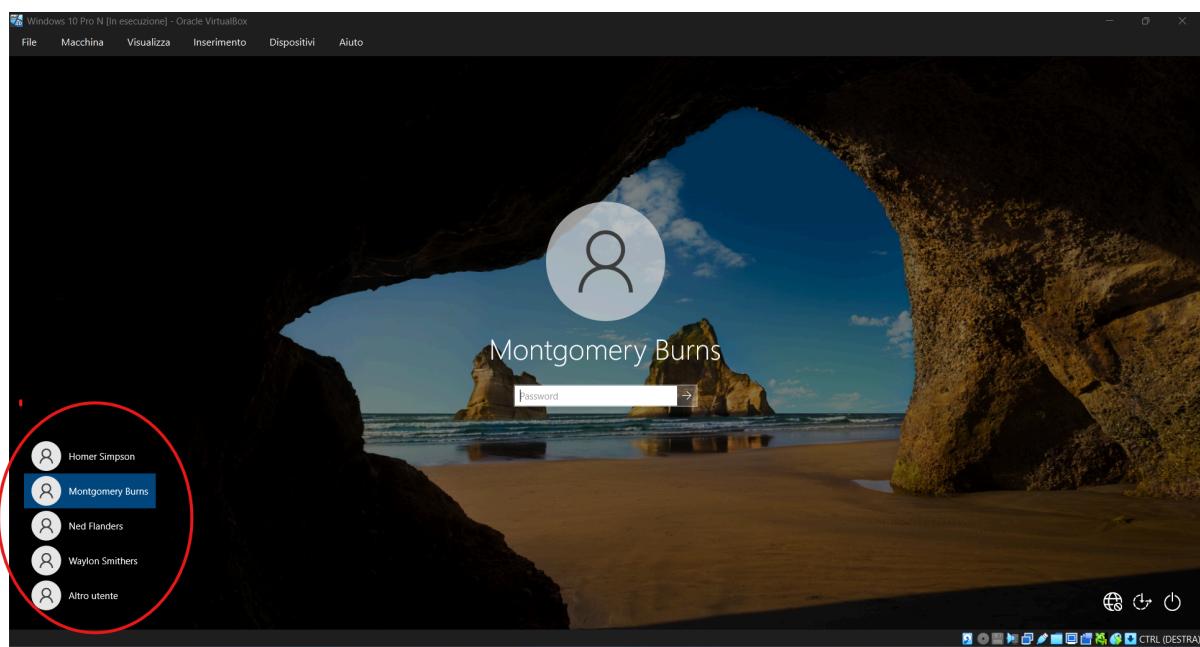
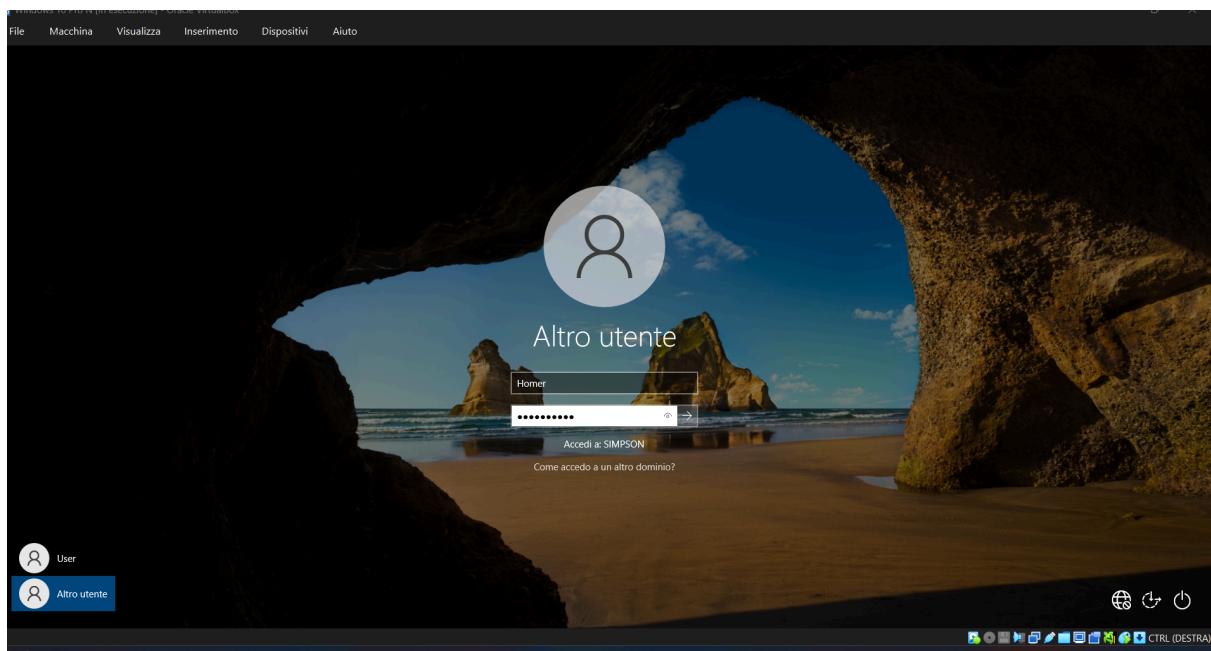
Per impedire al gruppo Sicurezza di modificare il sistema, si è fatto affidamento sui privilegi standard degli utenti di dominio in Windows Server 2022.

- Mentre gli **Eccellenti** possono invocare il prompt dei comandi con privilegi elevati (UAC), i **Bagarospi** sono vincolati a un ambiente non amministrativo, impedendo modifiche a C:\Windows o al Registro di Sistema.

5. Verifica e Validazione

La validazione finale ha confermato il successo dell'implementazione:

- Logon Test:** Gli utenti hanno effettuato l'accesso tramite client e sono riusciti a sfruttare i permessi concessi



2. **Test:** Confermata l'impossibilità di connessione remota per gli account appartenenti esclusivamente al gruppo **Bagarospi**.
3. **Audit dei Gruppi:** La console *Active Directory Users and Computers* mostra la corretta gerarchia di appartenenza, prevenendo il fenomeno del "Privilege Creep".

The screenshot displays two windows side-by-side. On the left is the 'Local Server' properties page for 'SimpsonServer'. It shows basic server details like computer name, domain, and network configuration. Below this is an 'EVENTS' section listing three recent logs. On the right is the 'Active Directory Users and Computers' management console, which lists users and groups within the 'Simpson.local' domain.

Local Server Properties (Left Window)

- Computer name: SimpsonServer
- Domain: Simpson.local
- Microsoft Defender Firewall: Public: On
- Remote management: Enabled
- Remote Desktop: Enabled
- NIC Teaming: Disabled
- Ethernet: 192.168.10.20, IPv6 enabled
- Operating system version: Microsoft Windows Server 2022
- Hardware information: innoteck GmbH VirtualBox

Events (Left Window)

Server Name	ID	Severity	Source
SIMPSONSERVER	1076	Warning	User32
SIMPSONSERVER	8198	Error	Microsoft-Windows-Security-SPP
SIMPSONSERVER	10016	Warning	Microsoft-Windows-DistributedCOM

Active Directory Users and Computers (Right Window)

Name	Type	Description
Bagarosp... (Security Group)	Security Group...	
Homer Simp... (User)	User	
Ned Flanders (User)	User	

6. Conclusioni

La configurazione di **SimpsonServer** rispetta i più alti standard di sicurezza per la segregazione dei ruoli. L'ambiente risulta protetto sia a livello di file system che di accesso perimetrale, garantendo che le funzioni amministrative rimangano isolate dalle funzioni operative di sicurezza.