

REPORT TECNICO: AMMINISTRAZIONE E SICUREZZA WINDOWS SERVER

Ambiente: Windows Server 2022 | Windows Pro N

Dominio: azeroth.local | **Obiettivo:** Gestione Gruppi, Utenti e Permessi

Allievo: Giuseppe Monaco

1. INTRODUZIONE

Lo scopo di questo esercizio è acquisire familiarità con la gestione dei gruppi di utenti in ambiente Windows Server 2022. L'amministrazione corretta dei gruppi è fondamentale per la sicurezza del sistema, in quanto permette di assegnare permessi specifici in modo scalabile e organizzato.

Per rendere l'esercitazione più coinvolgente e intuitiva, abbiamo simulato un'infrastruttura basata sul mondo di **World of Warcraft**, configurando il dominio all'interno della **Foresta di Azeroth**. In questo scenario, il server è stato trasformato nel fulcro gestionale delle fazioni contrapposte, **"Alleanza"** e **"Orda"**. Questa scelta permette di applicare criteri di segregazione dei dati e controllo degli accessi basati sui ruoli in modo netto: la separazione tra le fazioni simula la protezione di segreti militari e documenti diplomatici, dove ogni utente (eroe) può accedere esclusivamente alle risorse della propria capitale, garantendo l'integrità del sistema contro intrusioni della fazione avversaria.

2. PREPARAZIONE E REQUISITI

Prima di procedere alla configurazione logica, l'ambiente di laboratorio è stato isolato per garantire la sicurezza delle operazioni di test.

- **Configurazione Rete:** Il server è stato configurato su una rete interna denominata "intnet" per simulare un perimetro aziendale protetto.
- **Privilegi:** Le operazioni sono state eseguite con privilegi amministrativi, necessari per la creazione e gestione di oggetti Active Directory.

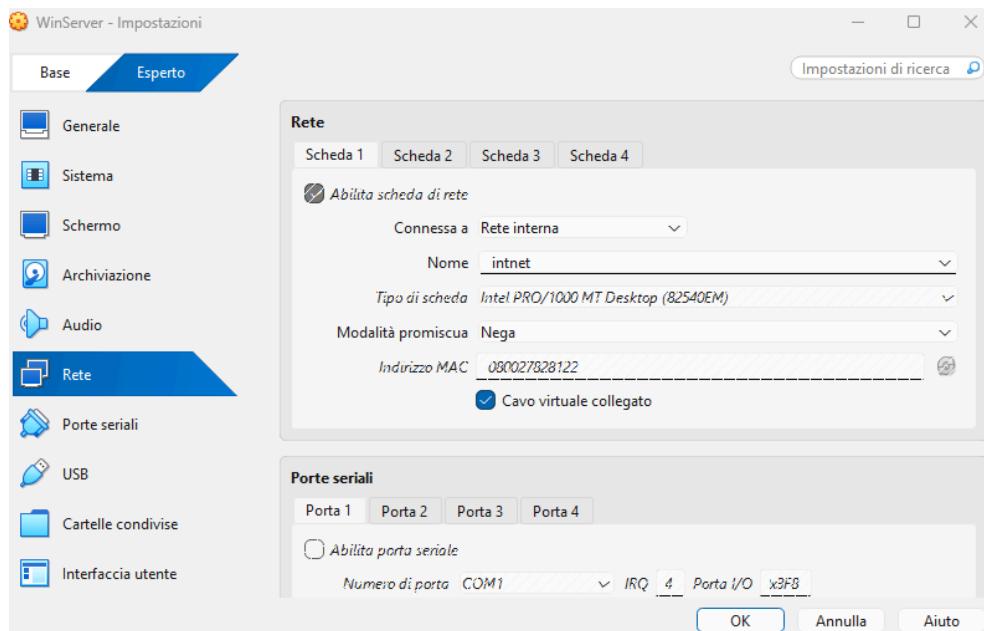


Fig. 1: Pannello delle impostazioni della macchina virtuale che mostra l'abilitazione della scheda di rete connessa alla "Rete interna" con nome "intnet".

3. CREAZIONE DEI GRUPPI E GESTIONE UTENTI

In questa fase sono stati creati gruppi distinti con nomi significativi per riflettere la loro funzione e il loro ruolo all'interno dell'organizzazione, come richiesto dall'obiettivo dell'esercizio.

3.1 Creazione delle Unità Organizzative (OU)

Per una gestione ordinata e gerarchica, sono stati creati dei contenitori logici (OU) che suddividono gli utenti in base alla loro affiliazione e dipartimento.

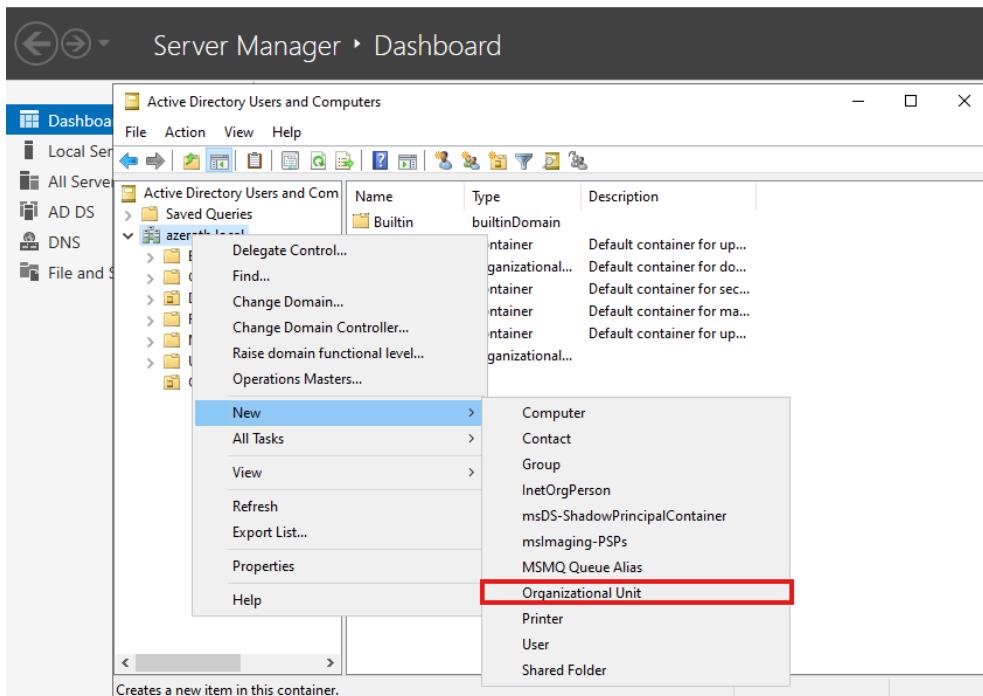


Fig. 2: Procedura di creazione di una **Organizational Unit** nel dominio per ospitare i nuovi oggetti di Active Directory.

1. Aprire lo strumento **Active Directory Users and Computers** dal menu *Tools* del Server Manager.
2. Fare clic destro sul dominio `azeroth.local` -> **New** -> **Organizational Unit**.
3. Sono state create le OU principali "**Alleanza**" e "**Orda**", all'interno delle quali sono state successivamente create le sotto-OU per le capitali (es. Sepulcro, Orgrimmar, Dalaran).

3.2 Configurazione dei Gruppi di Sicurezza

I gruppi rappresentano il fulcro della gestione dei permessi nel sistema. Invece di assegnare accessi ai singoli utenti, i privilegi vengono concessi a livello di gruppo per garantire scalabilità e una gestione centralizzata.

Standard di Sicurezza e Sharing: La divisione in gruppi è stata effettuata per garantire che ad ogni utente appartenente a un determinato schieramento venissero applicati **standard di sicurezza e criteri di sharing differenziati per fazione, ma omogenei per i membri dello stesso gruppo**.

- **Differenziazione:** Gli utenti del gruppo *Crimine* hanno accesso a risorse totalmente diverse rispetto a quelli del gruppo *Giustizia*.
- **Omogeneità:** Grazie all'appartenenza al gruppo, ogni nuovo "eroe" aggiunto (es. tramite lo script .bat) riceve istantaneamente lo stesso set di permessi, lo stesso sfondo e le stesse restrizioni dei suoi

compagni, eliminando discrepanze manuali e potenziali falle di sicurezza.

Sono stati creati i gruppi **Crimine** (per gli utenti dell'Orda) e **Giustizia** (per gli utenti dell'Alleanza).

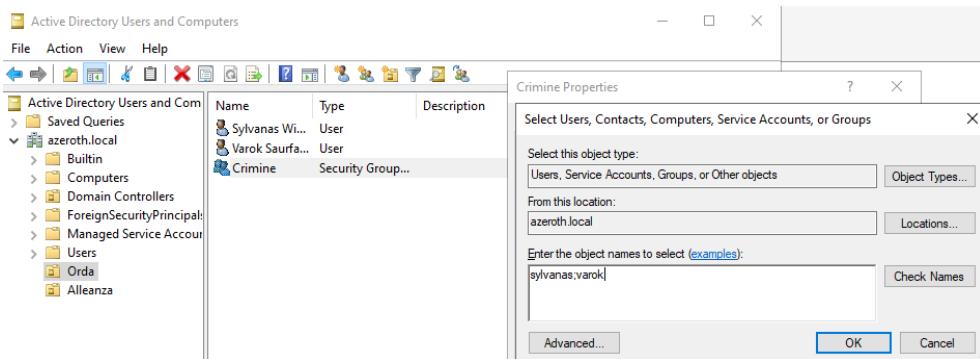


Fig. 3: Finestra delle proprietà dei gruppi durante la fase di popolamento dei membri per l'amministrazione dei permessi.

3.3 Gestione e Inserimento Utenti

Gli account utente sono stati configurati seguendo standard di sicurezza per la verifica dei permessi.

1. Fare clic destro nell'OU scelta -> **New -> User**.
2. Inserire Nome, Cognome e impostare il **User Logon Name** univoco.
3. Configurare una password complessa e attivare l'opzione "User must change password at next logon" per garantire la riservatezza delle credenziali al primo accesso.

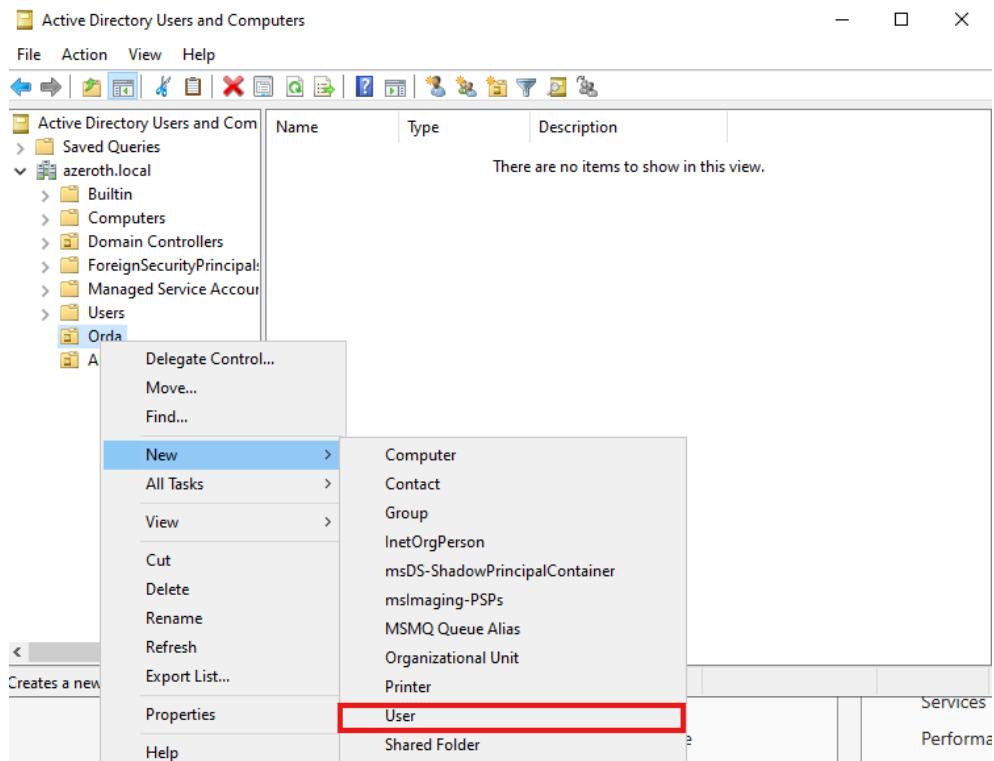


Fig. 4: Interfaccia di creazione utente in Active Directory.

Fig. 5: Configurazione delle policy della password per garantire che l'identità dell'utente sia protetta fin dal primo login.

AUTOMAZIONE TRAMITE SCRIPT BATCH (.BAT)

Per accelerare il processo di popolamento del dominio e garantire che ogni utente venisse creato con i metadati corretti (Titolo, Dipartimento e Gruppo di appartenenza), è stato implementato un file **Batch**. Questo file

automatizza la creazione delle OU mancanti e l'inserimento degli utenti, riducendo il margine di errore umano tipico della configurazione manuale.

```
Crea_Esercito.txt - Notepad
File Edit Format View Help
echo off
title Configurazione Eserciti di Azeroth
echo -----
echo COSTRUZIONE CAPITALI E RECLUTAMENTO EROI
echo -----

:: Definiamo le variabili principali
set DOMAINIO=DC=azeroth,DC=local
set PASSWORD=Zaqxswe123!

echo.
echo [1/3] Creazione Sotto-OUs (Capitali)...
powershell -Command "New-ADOrganizationalUnit -Name 'Sepulcra' -Path 'OU=Orda,%DOMAINIO%' -ErrorAction SilentlyContinue"
powershell -Command "New-ADOrganizationalUnit -Name 'Orgrimmar' -Path 'OU=Orda,%DOMAINIO%' -ErrorAction SilentlyContinue"
powershell -Command "New-ADOrganizationalUnit -Name 'Dalaran' -Path 'OU=Alleanza,%DOMAINIO%' -ErrorAction SilentlyContinue"

echo [2/3] Reclutamento campioni dell'Orda...
powershell -Command "$pw = ConvertTo-SecureString '%PASSWORD%' -AsPlainText -Force; New-ADUser -Name 'Putress' -SamAccountName 'putress' -Path 'OU=Sepulcra,OU=Orda,%DOMAINIO%'"
powershell -Command "$pw = ConvertTo-SecureString '%PASSWORD%' -AsPlainText -Force; New-ADUser -Name 'Baine' -SamAccountName 'baine' -Path 'OU=Orgrimmar,OU=Orda,%DOMAINIO%' -Ac
powershell -Command "Add-ADGroupMember -Identity 'Crimine' -Members 'putress', 'baine'"

echo [3/3] Reclutamento campioni dell'Alleanza...
powershell -Command "$pw = ConvertTo-SecureString '%PASSWORD%' -AsPlainText -Force; New-ADUser -Name 'Khadgar' -SamAccountName 'khadgar' -Path 'OU=Dalaran,OU=Alleanza,%DOMAINIO'
powershell -Command "$pw = ConvertTo-SecureString '%PASSWORD%' -AsPlainText -Force; New-ADUser -Name 'Anduin' -SamAccountName 'anduin' -Path 'OU=Alleanza,%DOMAINIO%' -AccountPa
powershell -Command "Add-ADGroupMember -Identity 'Giustizia' -Members 'khadgar', 'anduin'

echo.
echo =====
echo OPERAZIONE COMPLETATA! Per l'onore di Azeroth.
echo =====
pause
```

Fig. 6: Visualizzazione dello script Crea_Esercito.bat in TXT

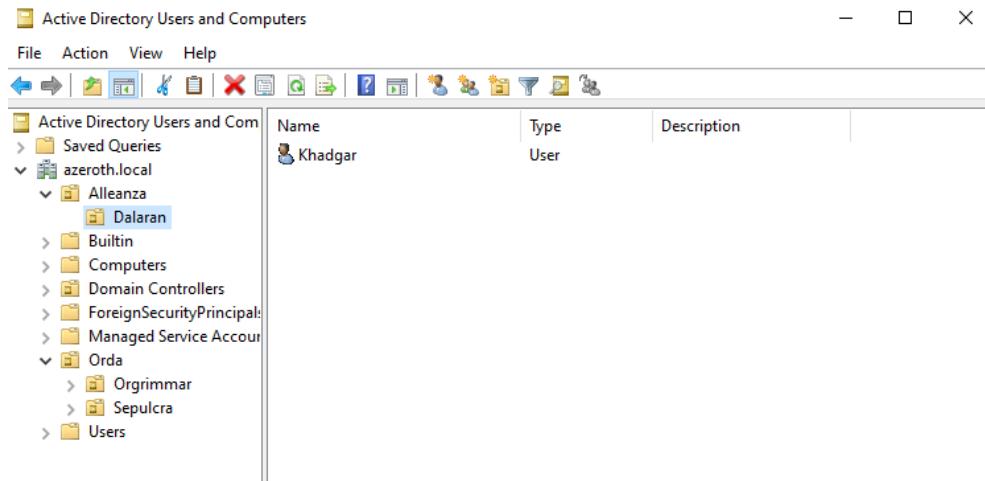


Fig. 7: Visualizzazione della gerarchia delle OU creata per strutturare il sistema in fazioni e città post esecuzione .bat

4. ASSEGNAZIONE PERMESSI E SICUREZZA DATI

Per ogni gruppo sono stati definiti permessi specifici riguardanti l'accesso a file e cartelle.

4.1 Configurazione NTFS e Standard di Sicurezza

Per ogni gruppo sono stati definiti permessi specifici riguardanti l'accesso a file e cartelle, assicurando che l'amministrazione del sistema segua criteri di sicurezza rigorosi.

- **Metodologia di Segregazione:** La sicurezza del sistema è stata garantita tramite la rimozione dei gruppi predefiniti "**Users**" ed "**Everyone**" dalla lista di controllo degli accessi (ACL) delle cartelle **Codice** e **Inquisizione**. Questa operazione assicura che nessun utente del dominio possa accedere alle risorse per il solo fatto di essere autenticato nel sistema.
- **Standard di Sharing Omogenei:** La divisione in gruppi è stata effettuata per garantire che ad ogni utente dello stesso schieramento venissero applicati standard di sicurezza e criteri di condivisione omogenei. Grazie a questa struttura, ogni nuovo utente aggiunto (anche tramite automazione script) riceve istantaneamente lo stesso set di permessi del proprio gruppo, eliminando discrepanze manuali e potenziali falle di sicurezza.
- **Permessi Esplicativi:** Sebbene l'ereditarietà rimanga attiva per scopi amministrativi, la riservatezza dei dati è totale poiché l'accesso è concesso esclusivamente tramite **permessi esplicativi** assegnati ai gruppi di sicurezza **Giustizia** e **Crimine**.

4.2 Verifica dell'Accesso

La verifica ha confermato che gli utenti autorizzati visualizzano i propri documenti, mentre i tentativi di accesso non autorizzato vengono bloccati.

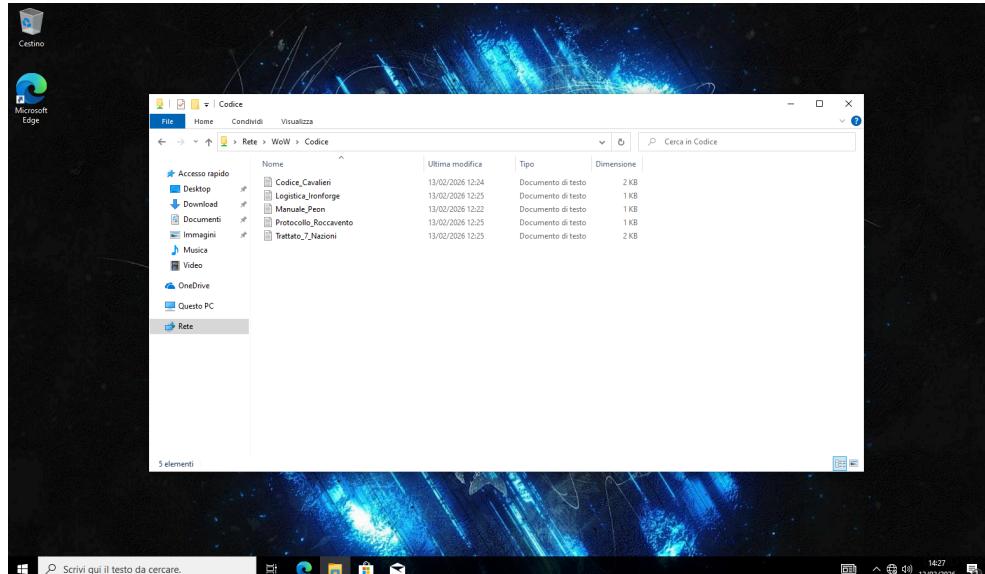


Fig. 8: Esplora file che mostra l'accesso riuscito alla cartella di rete 'Codice' con la visualizzazione dei file sensibili (Protocollo_Roccavento, Trattato_7_Nazioni, ecc.).

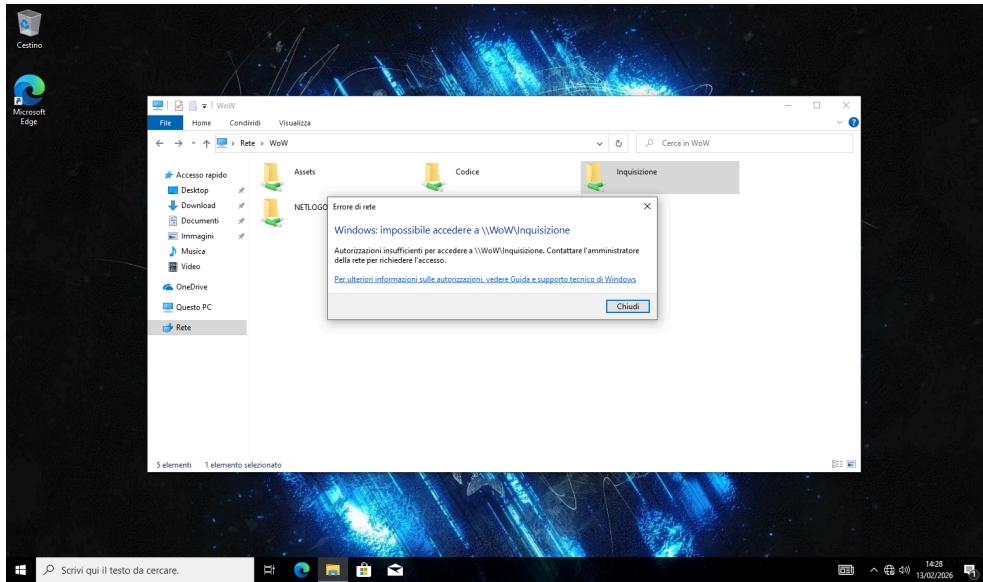


Fig. 9: Messaggio di errore di Windows che nega l'accesso alla cartella 'Inquisizione' a causa di autorizzazioni insufficienti, confermando la corretta configurazione della sicurezza.

5. GESTIONE AMBIENTE E VERIFICA FINALE

Tramite le Group Policy e gli script di logon, è stata personalizzata l'esperienza utente in base all'appartenenza ai gruppi. Nello specifico, sono stati aggiungi un Background per l'Orda ed uno per l'Alleanza, e sono stati impostati messaggi di Logon personalizzati in base al gruppo di appartenenza.

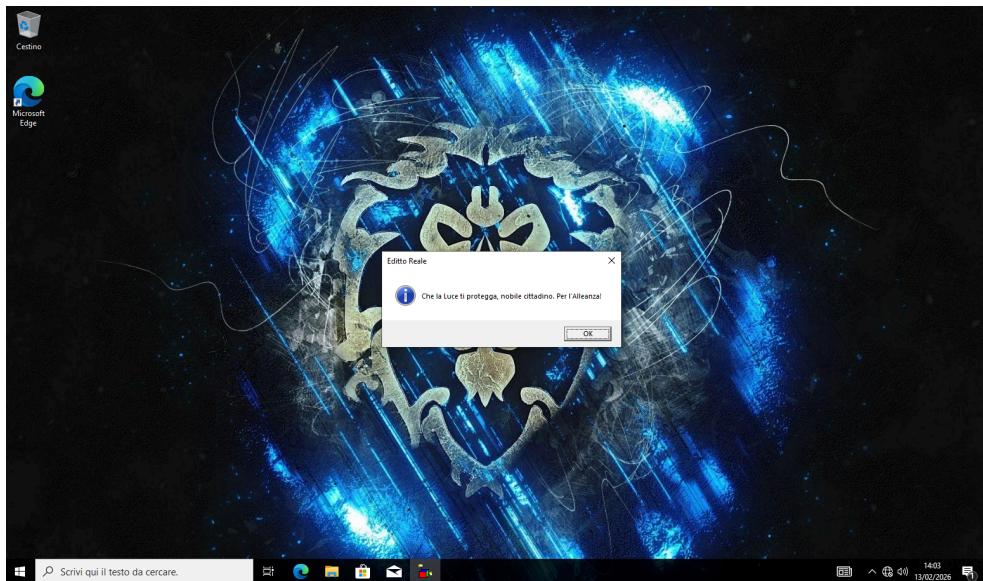


Fig. 10: Desktop dell'Alleanza al momento del logon, che mostra il vessillo blu come sfondo e il messaggio popup 'Editto Reale' configurato tramite script .vbs.

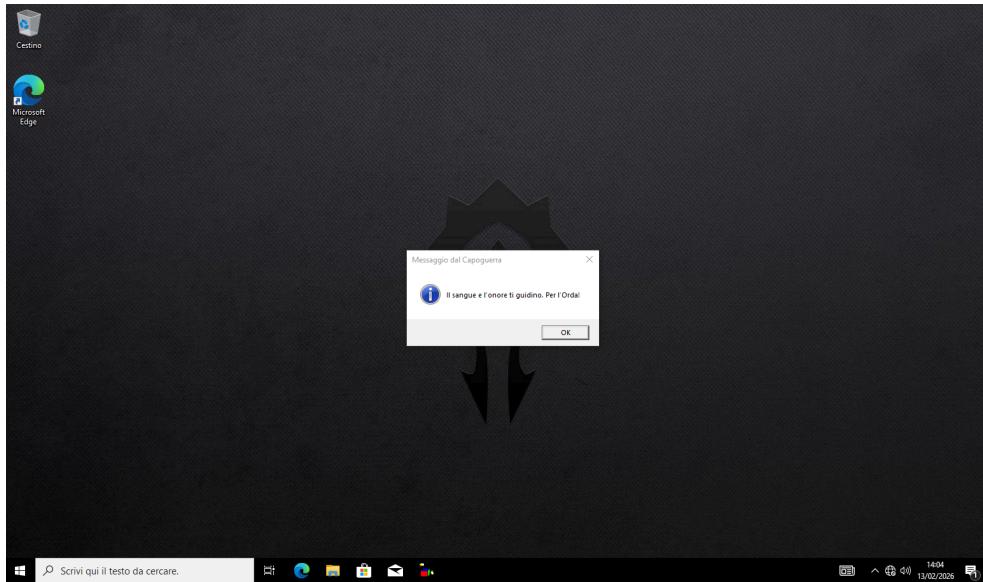


Fig. 11: Desktop dell'Orda che mostra lo sfondo personalizzato e il popup di benvenuto 'Messaggio dal Capoguerra' eseguito correttamente all'accesso.

6. DOCUMENTAZIONE E CONCLUSIONI FINALI

L'obiettivo dell'esercizio è stato pienamente raggiunto, trasformando una configurazione iniziale in un'infrastruttura di dominio completa, popolata e automatizzata.

6.1 Struttura Finale dell'Infrastruttura "WoW"

Grazie all'integrazione tra configurazione manuale e automazione tramite script batch, il server `azeroth.local` presenta ora la seguente gerarchia definitiva:

- **Gruppi di Sicurezza principali:**
 - **Giustizia:** Amministra i permessi degli utenti dell'Alleanza (Varian, Anduin, Khadgar).
 - **Crimine:** Amministra i permessi degli utenti dell'Orda (Sylvanas, Varok, Putress, Baine).
- **Organizzazione Territoriale (Unità Organizzative):**
 - **Alleanza:** Contenitore radice che include le sotto-OUs *Dalaran* e gli utenti diplomatici.
 - **Orda:** Contenitore radice che include le sotto-OUs *Sepulcras* e *Orggrimmar*.

6.2 Risultati della Segregazione e Sicurezza Dati

L'implementazione dei permessi NTFS, combinata con la disabilitazione dell'ereditarietà, ha prodotto i seguenti risultati operativi:

1. **Controllo degli Accessi Rigo**: La sicurezza è garantita dall'interruzione dell'ereditarietà sulle cartelle **Codice** e **Inquisizione**. Ogni gruppo possiede permessi di "Modifica" esclusivamente sulla propria cartella di pertinenza, mentre l'accesso alla cartella della fazione opposta è esplicitamente negato dal sistema.
2. **Verifica dei Permessi**: I test effettuati hanno confermato che un utente del gruppo *Crimine* (Orda) riceve un errore di rete immediato se tenta di accedere ai documenti del **Codice**, garantendo la protezione dei dati sensibili.
3. **Automazione e Personalizzazione**: L'utilizzo di script di logon differenziati ha confermato la capacità del sistema di distinguere gli utenti in base al gruppo, applicando sfondi desktop e messaggi di benvenuto specifici (es. "Editto Reale" per l'Alleanza).

6.3 Risoluzione Problematiche Tecniche

Durante le fasi di test è stata risolta la problematica relativa alla distribuzione degli sfondi desktop. La soluzione è consistita nel migrare gli asset grafici in una cartella condivisa accessibile tramite **percorso UNC** (`\WoW\Assets`), garantendo che le Group Policy possano applicare correttamente le risorse ai client senza dipendere da percorsi locali inaccessibili agli utenti standard.

Considerazioni Finali: Il progetto ha dimostrato che la gestione granulare dei gruppi è il pilastro fondamentale per amministrare un sistema Windows Server in modo sicuro e scalabile. L'integrazione del file **Batch** ha permesso di passare da un ambiente statico a uno dinamico, garantendo l'omogeneità di tutti gli account creati nel dominio.