REPORT TECNICO: Configurazione Infrastruttura e Sicurezza Windows Server 2022

Progetto: Esercitazione S10L5 - Gestione Identità e Accessi

Nome Server: LOTRserver

Dominio: ARDA.local

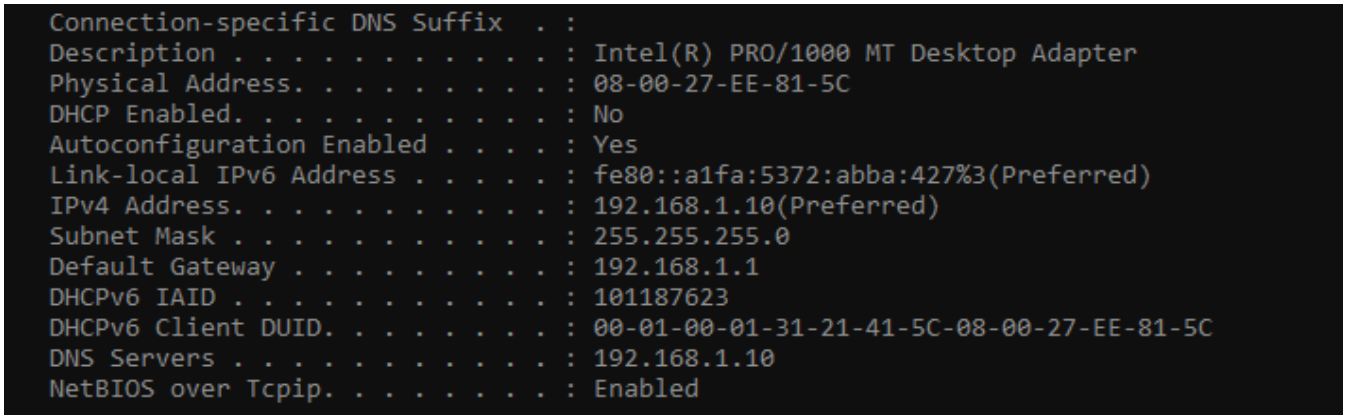
Data: 13 Febbraio 2026

---

1. **Configurazione di Rete e Preliminari**

Per garantire la stabilità dei servizi di dominio, il server è stato configurato con parametri di rete statici:

- **Indirizzo IP (IPv4):** 192.168.10.10
- **Subnet Mask:** 255.255.255.0
- **Gateway:** 192.168.10.1
- **DNS Primario:** 192.168.1.10 (Loopback locale per la risoluzione del dominio).

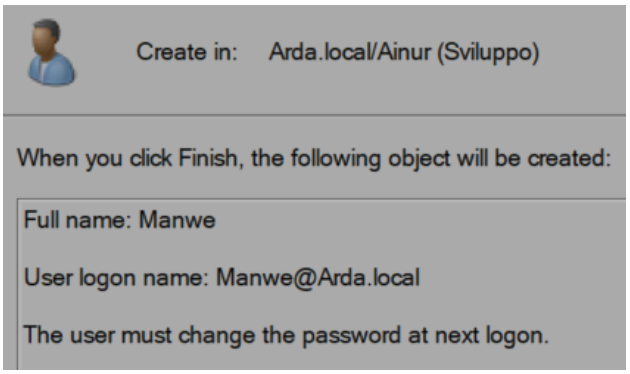


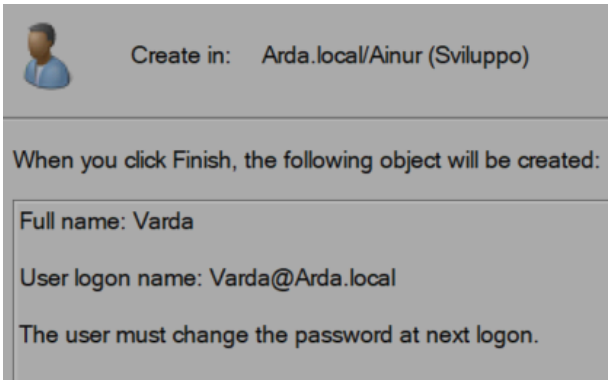
2. **Nomi dei Gruppi ed Utenti Creati**

Sono stati definiti due gruppi di sicurezza principali per rispecchiare la gerarchia aziendale richiesta:

Gruppo A: **Valar (amministratori)**

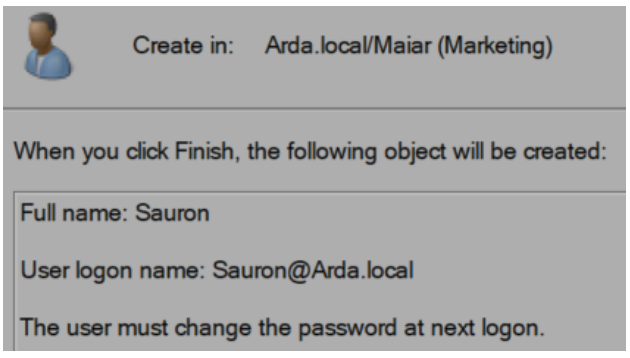
- **Tipologia:** Security Group - Global Scope.
- **Ruolo:** Amministrazione IT e Gestione Infrastruttura.
- **Membri:** Utente Manwe, Utente Varda.
- **Livello Privilegi:** Amministrativo (Membri del gruppo built-in *Administrators*).

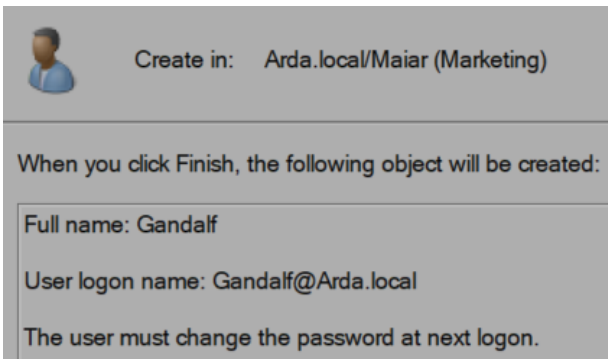




Gruppo B: **Stregoni (marketing)**

- **Tipologia:** Security Group - Global Scope.
- **Ruolo:** Marketing / Operatori Standard.
- **Membri:** Utente Gandalf, Utente Sauron.
- **Livello Privilegi:** Utente Standard (Domain Users) con restrizioni applicate via GPO.





3. **Passaggi Seguiti per Creare e Configurare i Gruppi**

Di seguito la procedura tecnica dettagliata eseguita per raggiungere la configurazione finale.

Fase 1: Creazione Struttura Logica (Active Directory)

1. Apertura della console **Active Directory Users and Computers**.
2. Creazione di due **Unità Organizzative (OU)**: Ainur (per i Valar) e Maiar (per gli Stregoni).
3. All'interno delle OU, creazione dei Gruppi Globali di Sicurezza Valar e Stregoni.
4. Creazione degli oggetti Utente (Manwe, Sauron, ecc.) e loro assegnazione ai rispettivi gruppi tramite la scheda **Member Of**.

4. **Permessi Assegnati a Ciascun Gruppo**

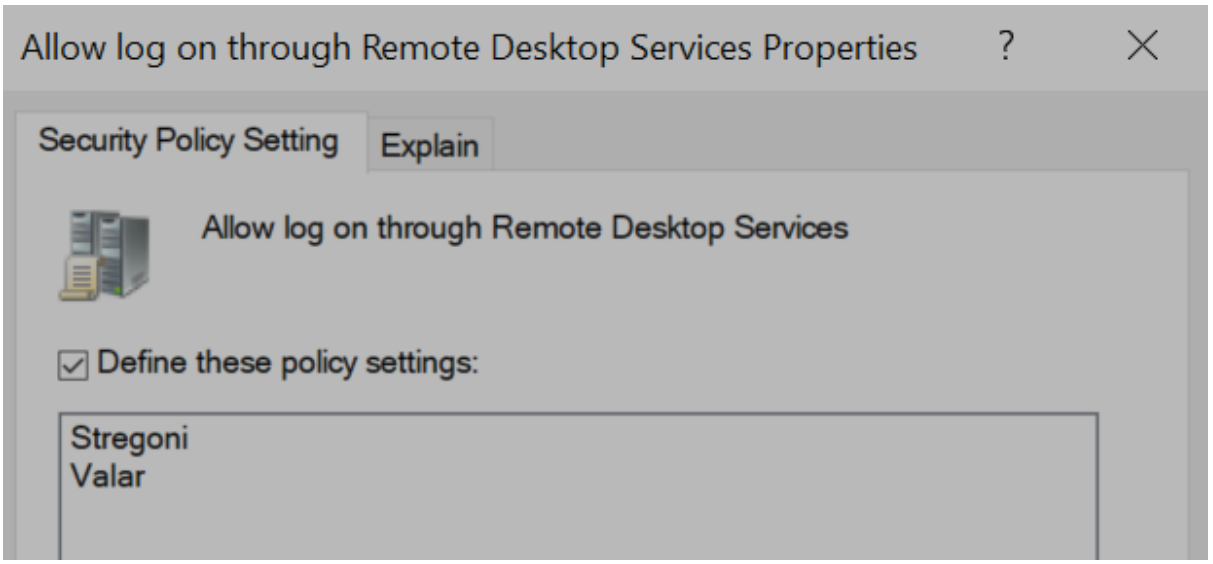
I permessi sono stati distribuiti nel seguente modo.

A. Permessi su File System (NTFS)

- **Cartella C:\Dati Arda\Valinor:**
  - **Gruppo Valar:** Accesso **Full Control** (Controllo Completo).
  - **Gruppo Stregoni: Nessun Accesso** (Access Denied).
- **Cartella C:\Dati Arda\Middle Earth:**
  - **Gruppo Stregoni:** Accesso **Full Control**.
  - **Gruppo Valar:** Accesso **Full Control**.

B. Permessi di Sistema e Policy (GPO)

- **Accesso Remoto (RDP):** Consentito a **entrambi** i gruppi (Valar e Stregoni) tramite la policy *"Allow log on through Remote Desktop Services"*.

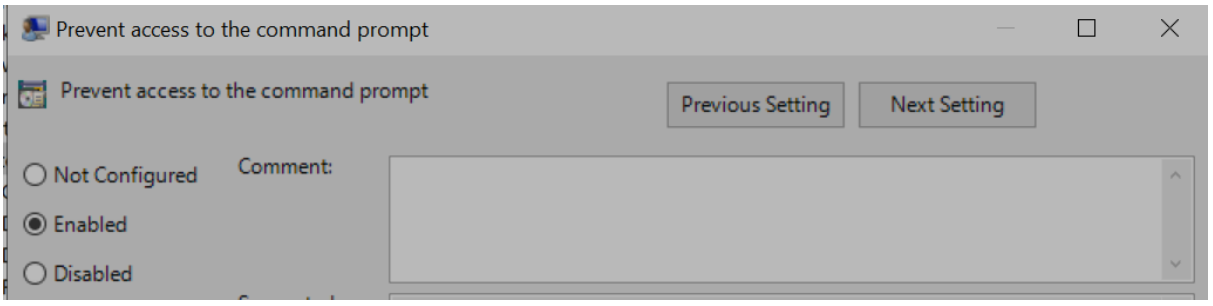


Esecuzione Comandi (CMD):

Valar: **Consentito**.

Stregoni: **Bloccato**. Tentare di aprire il prompt restituisce il messaggio: *"il prompt dei comandi è stato disattivato dall'amministratore"*.

- Creazione di una nuova GPO denominata Blocco_CMD e collegata all'Unità Organizzativa **Maiar**.
- Modifica della GPO in: *User Configuration* > *Policies* > *Administrative Templates* > *System*.
- Impostazione della voce **"Prevent access to the command prompt"** su **Enabled**.
- Applicazione modifiche tramite comando gpupdate /force.



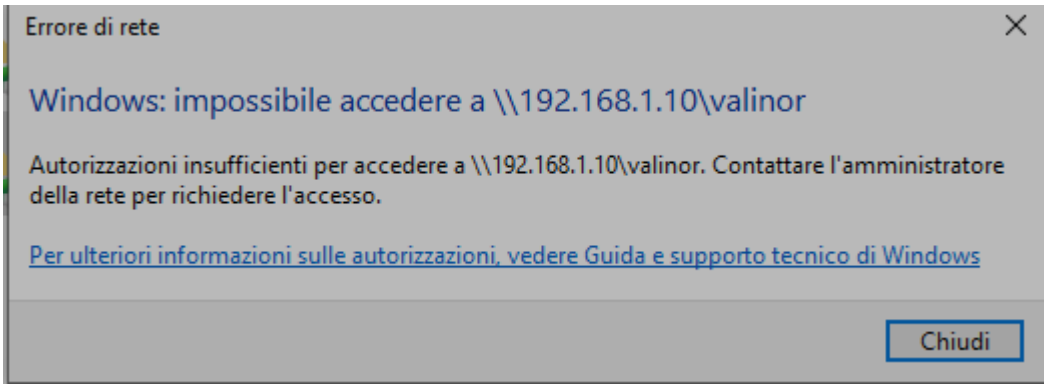
5. **Fase di Testing e Validazione Funzionale**

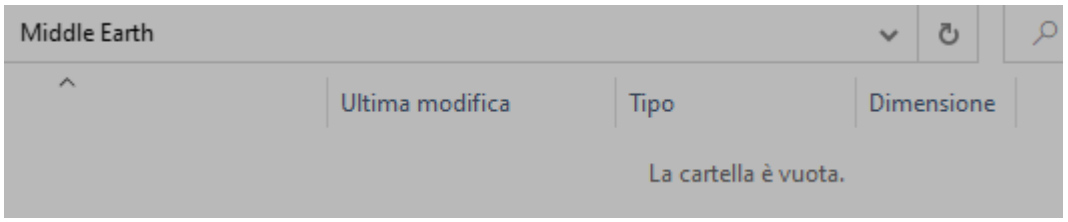
Al fine di certificare la corretta applicazione delle policy di sicurezza e dei permessi NTFS, è stata condotta una sessione di test incrociati utilizzando una workstation client Windows 10 pro aggiunta al dominio ARDA.local. Le verifiche hanno simulato l'operatività quotidiana per confermare l'efficacia delle restrizioni imposte.

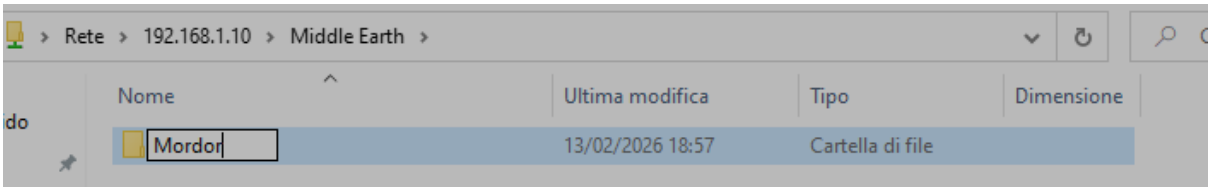
Scenario A: Verifica Profilo Utente Standard

Il test è stato eseguito effettuando il login con l'utente **ARDA\Sauron**, membro del gruppo *Stregoni*, riscontrando i seguenti esiti:

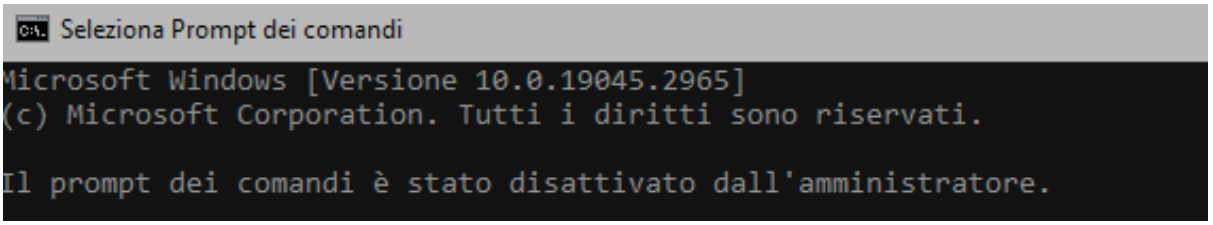
- **Accesso Remoto (RDP):** La connessione al server 192.168.10.10 è avvenuta con successo, confermando la corretta configurazione della policy *Allow log on through Remote Desktop Services*.
- **Sicurezza dei Dati (NTFS):** Il tentativo di accedere alla cartella riservata Valinor è stato **bloccato dal sistema**, restituendo l'errore *"Autorizzazioni insufficienti".* Al contrario, l'accesso alla cartella di competenza Middle Earth è risultato pienamente operativo in lettura e scrittura.







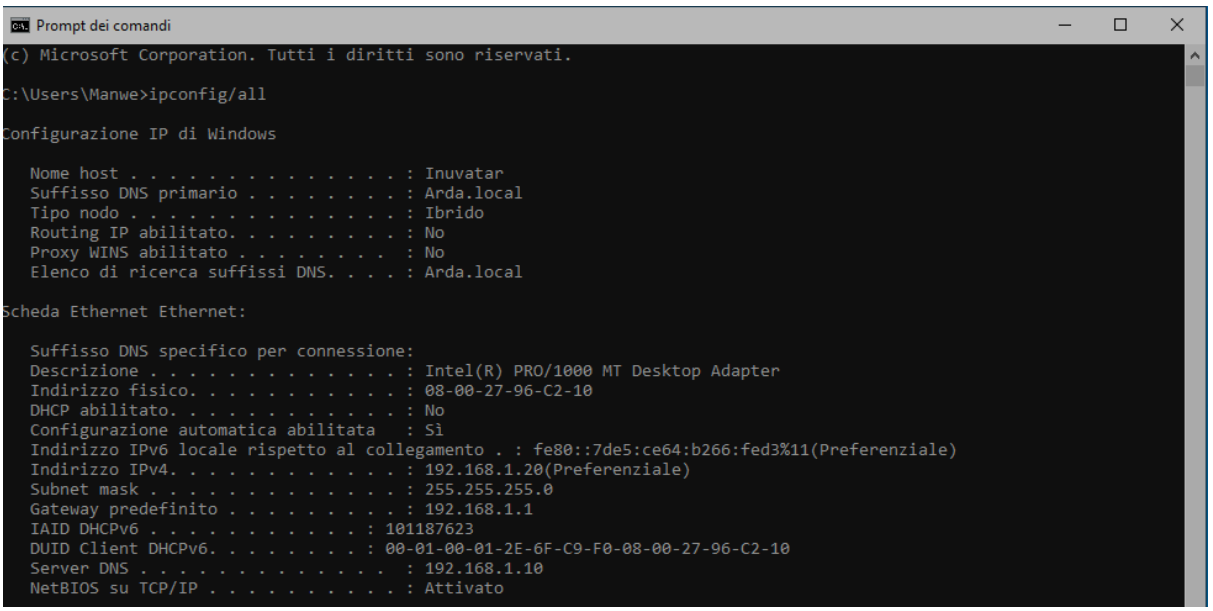
- **Blocco Software (GPO):** Il tentativo di avviare il Prompt dei Comandi (cmd.exe) è stato impedito. Il sistema ha visualizzato il messaggio di restrizione: *"il prompt dei comandi è stato disattivato dall'amministratore"* confermando l'applicazione della Group Policy specifica per l'Unità Organizzativa *Maiar*.



Scenario B: Verifica Profilo Amministrativo

Il test è stato ripetuto con l'utente **Manwe**, membro del gruppo *Valar* e del gruppo *Administrators*, con i seguenti risultati:

- **Gestione File System:** L'utente ha ottenuto accesso completo (*Full Control*) sia alla cartella Valinor che a tutte le risorse di sistema, in virtù dei privilegi amministrativi.
- **Esecuzione Comandi:** L'avvio di cmd.exe e PowerShell è avvenuto senza limitazioni, permettendo la piena gestione del server da riga di comando.



Conclusioni

L'esercitazione ha portato alla realizzazione di un'infrastruttura di dominio **ARDA.local** sicura e gerarchica.

I test finali di conformità hanno confermato i seguenti punti:

1. **Isolamento dei Dati:** La separazione tramite permessi NTFS impedisce efficacemente l'accesso non autorizzato ai documenti riservati (es. l'utente Sauron non può accedere a Valinor).
2. **Sicurezza Operativa:** L'uso delle Group Policy (GPO) ha permesso di limitare la superficie di attacco, impedendo agli utenti standard (Stregoni) di eseguire comandi di sistema tramite CMD o di arrestare il server, pur mantenendo la possibilità di lavorare da remoto.
3. **Gestione Centralizzata:** La struttura basata su Unità Organizzative (OU) permette una gestione scalabile e ordinata delle risorse e dei permessi.