

Report: Configurazione di Gruppi e Permessi su Windows Server

Descrizione dell'ambiente

1. **Nome server:** APServer
 - Dominio configurato: **AP.local**
 - Sistema operativo: Windows Server 2022
 - Componenti installati: Active Directory Domain Services (AD DS), strumenti di gestione delle policy e dei gruppi.
 2. **Struttura del file system:**

Il disco del server è stato organizzato con due directory principali per la gestione dei dati:

 - **SECDATA** (dati di sicurezza)
 - **AMMDATA** (dati amministrativi)
 3. All'interno di ciascuna directory principale sono presenti sottocartelle dedicate ai diversi livelli di accesso:
 - **ResponsabileSEC** e **UtenteSEC** in **SECDATA**
 - **ResponsabileAMM** e **UtenteAMM** in **AMMDATA**
-

Gruppi creati

Sono stati definiti due gruppi per gestire gli accessi e i permessi:

1. **SecurityTeam:**
 - Scopo: Gestione della sicurezza dei dati, policy di sistema e documentazione riservata.
 - Membri: Utenti responsabili della sicurezza.
2. **DataManager:**
 - Scopo: Gestione dei dati amministrativi, budget e documentazione interna aziendale.
 - Membri: Responsabili e utenti operativi del team amministrativo.

Permessi assegnati

1. SECDATA

- **Cartella principale:** Solo il gruppo **SecurityTeam** può accedere a questa directory.
 - **ResponsabileSEC:**
 - Permessi completi: lettura, scrittura, modifica ed eliminazione.
 - Scopo: Garantire la gestione completa dei dati di sicurezza.
 - **UtenteSEC:**
 - Permessi limitati: lettura e scrittura (senza possibilità di eliminare o modificare file critici).
 - Scopo: Accesso operativo ai file relativi alla sicurezza aziendale.

2. AMMDATA

- **Cartella principale:** Solo il gruppo **DataManager** può accedere a questa directory.
 - **ResponsabileAMM:**
 - Permessi completi: lettura, scrittura, modifica ed eliminazione.
 - Scopo: Gestione strategica dei dati amministrativi e finanziari.
 - **UtenteAMM:**
 - Permessi limitati: lettura e scrittura (senza possibilità di eliminare o modificare file critici).
 - Scopo: Gestione operativa dei file amministrativi.

Test e verifica

Sono stati effettuati i seguenti test per garantire il corretto funzionamento dell'ambiente:

1. Verifica accessi:

- Utenti non autorizzati hanno riscontrato errori di accesso alle cartelle protette, garantendo che i permessi funzionino correttamente.

2. Test di lettura/scrittura:

- Gli utenti autorizzati possono leggere e scrivere all'interno delle loro cartelle assegnate.

3. Conformità ai ruoli:

- I responsabili possono gestire i file con accesso completo, mentre gli utenti hanno un accesso limitato.

Conclusioni

La configurazione è stata completata con successo, garantendo:

- **Sicurezza:** I dati sensibili sono protetti da accessi non autorizzati.
- **Organizzazione:** La struttura delle cartelle è chiara e consente una gestione efficace dei dati.
- **Efficienza:** I permessi sono definiti in modo da rispettare i ruoli dei gruppi e ottimizzare le operazioni.



