

Obiettivo:

L'obiettivo principale è acquisire una comprensione più approfondita dei gruppi di utenti e dei relativi permessi. Questo aiuterà a rendere il server più sicuro e gestibile in modo centralizzato



1 Preparazione












Per iniziare, accedi al tuo ambiente Windows Server 2022 . Assicurati di avere i permessi amministrativi necessari per creare e gestire i gruppi . Puoi verificare i permessi amministrativi accedendo al Pannello di Controllo e controllando le impostazioni di 'Account Utente' oppure eseguendo il comando 'net user' per visualizzare i dettagli dell'account. A questo scopo, è utile avere una buona conoscenza del pannello di amministrazione e delle funzionalità di gestione degli utenti e gruppi.

Diagramma del Flusso di Preparazione




- **Passo 1:** Accedi al server .
- **Passo 2:** Verifica i permessi amministrativi .
- **Passo 3:** Avvia la gestione di utenti e gruppi .

2 Creazione dei Gruppi

Abbiamo creato due gruppi distinti chiamati "Amministratori" e "UtentiStandard" . Questi nomi sono stati scelti per riflettere i ruoli e le responsabilità degli utenti che saranno inclusi in ciascun gruppo . Scegliere nomi significativi per i gruppi è importante per facilitare la gestione del sistema e la risoluzione dei problemi, poiché rende immediatamente chiaro il ruolo e i permessi di ciascun gruppo:

- **Amministratori:** utenti con permessi elevati per la gestione e configurazione del sistema  .
- **UtentiStandard:** utenti con permessi limitati, utili per svolgere attività quotidiane senza rischiare di compromettere il sistema  .

2.1 Dettagli dei Gruppi Creati

 Nome del Gruppo	 Scopo	 Numero di Membri
Amministratori	Gestione completa del sistema	2
<u>UtentiStandard</u>	Attività operative quotidiane	5

3 Assegnazione dei Permessi

Per ogni gruppo, sono stati assegnati permessi specifici :














- Amministratori:
 - Accesso completo a file e cartelle : Gli amministratori devono poter gestire ogni aspetto del server, inclusa la gestione di tutti i file.
 - Esecuzione di programmi specifici : Permesso di eseguire qualsiasi programma necessario per la gestione del sistema.
 - Modifiche alle impostazioni di sistema : Gli amministratori possono apportare modifiche alle configurazioni di sistema per garantire la sicurezza e l'efficienza.
 - Accesso remoto al server : Accesso remoto consentito per gestire il server anche a distanza.
- UtentiStandard:
 - Accesso limitato a file e cartelle : Accesso solo alle cartelle necessarie per il lavoro quotidiano, per garantire la sicurezza dei dati sensibili.
 - Esecuzione di programmi specifici : Possibilità di eseguire solo applicazioni approvate, per prevenire modifiche non autorizzate.
 - Accesso remoto non consentito : Per motivi di sicurezza, l'accesso remoto non è consentito agli utenti standard.

Tabella dei Permessi Assegnati



 Gruppo	 Accesso File e Cartelle	 Esecuzione Programmi	 Modifiche al Sistema	 Accesso Remoto
Amministratori	Completo	Completo	Completo	Consentito
<u>UtentiStandard</u>	Limitato	Limitato	Nessuno	Non Consentito


Schema dei Permessi

Questo schema mostra la differenziazione dei permessi tra gli Amministratori e gli UtentiStandard per una migliore comprensione delle responsabilità assegnate a ciascun gruppo .





4 Verifica

Per verificare che le impostazioni siano corrette, sono stati creati due utenti di prova .

- User_Admin: Aggiunto al gruppo "Amministratori" .
- User_Standard: Aggiunto al gruppo "UtentiStandard" .

Successivamente, abbiamo effettuato delle verifiche per assicurare che ciascun utente avesse solo i permessi assegnati al gruppo di appartenenza . Abbiamo utilizzato strumenti come 'Gestione Utenti e Gruppi Locali' e il comando 'gpresult' per verificare le impostazioni di sicurezza e i permessi effettivi. Ad esempio, User_Admin è stato in grado di modificare le impostazioni del sistema e accedere a tutte le cartelle, mentre User_Standard ha avuto accesso solo alle cartelle e ai programmi consentiti.

Risultati della Verifica

 Utente	 Gruppo Assegnato	 Permessi Verificati	 Esito
<u>User_Admin</u>	Amministratori	Accesso completo	Successo
User_Standard	UtentiStandard	Accesso limitato	Successo






5 Documentazione

 **Gruppi Creati:** "Amministratori", "UtentiStandard".

 **Permessi Assegnati:**


- Amministratori: Accesso completo, esecuzione di programmi, modifiche al sistema, accesso remoto.
- UtentiStandard: Accesso limitato, esecuzione di programmi limitati, nessuna modifica al sistema, nessun accesso remoto.

 **Passaggi Seguiti:**



1. Accedi al server con privilegi amministrativi .
2. Vai su "Gestione Computer" > "Utenti e Gruppi Locali" .
3. Crea i gruppi "Amministratori" e "UtentiStandard" .
4. Assegna permessi specifici tramite le impostazioni di sicurezza .
5. Crea utenti di prova e aggiungili ai rispettivi gruppi .

 **Schema dei Passaggi Seguiti**



 **Problemi Riscontrati:**

Nessun problema rilevante durante l'esercizio. Tuttavia, è stato necessario assicurarsi che i permessi assegnati fossero corretti durante la verifica, poiché eventuali errori, come la concessione di accessi non autorizzati o la mancata restrizione di permessi critici, avrebbero potuto compromettere la sicurezza del sistema . Ad esempio, un errore nell'assegnazione dei permessi agli utenti standard potrebbe consentire modifiche non autorizzate al sistema, aumentando il rischio di violazioni della sicurezza.

Conclusione



Questo esercizio ha dimostrato l'importanza della gestione dei gruppi per garantire la sicurezza e l'efficienza di un sistema Windows Server . Creare gruppi e assegnare permessi appropriati aiuta a mantenere il controllo su chi può accedere a risorse critiche e a minimizzare i rischi legati a errori umani o ad accessi non autorizzati .

 **Schema Riassuntivo del Sistema di Gestione dei Gruppi**

La gestione dei gruppi è una parte essenziale dell'amministrazione dei server . Una corretta configurazione aiuta a definire i ruoli e a evitare accessi non autorizzati, garantendo un ambiente sicuro e ben gestito .

Appendice

Elenco dei Comandi Utilizzati

 Comando	 Descrizione
<code>net <u>localgroup</u> Administrators</code>	Comando per visualizzare membri del gruppo
<code>net user User_Admin /add</code>	Comando per creare un nuovo utente di prova

Link Utili

[Documentazione Ufficiale di Microsoft](#) 



