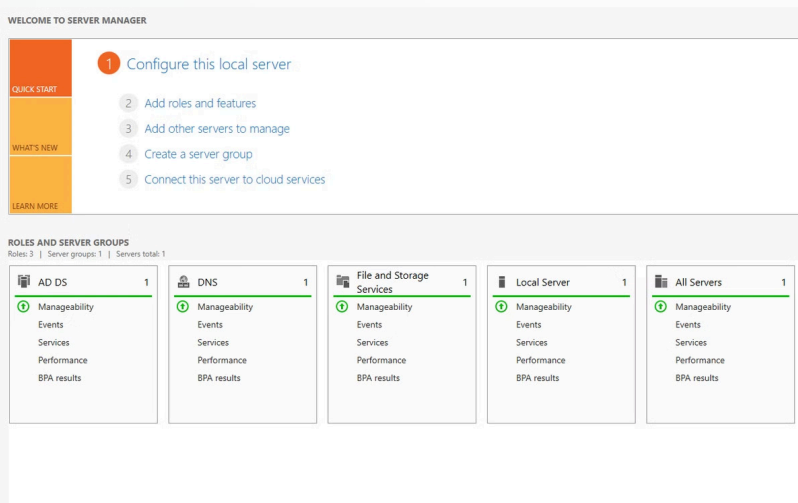


Creazione di Gruppi in Windows Server 2022

In questo esercizio sono stati creati due gruppi in Windows Server 2022: **Amministrazione** e **Utenti Standard**. Sono state assegnate autorizzazioni specifiche per ciascun gruppo, considerando aspetti come l'accesso ai file e alle cartelle, l'esecuzione di programmi specifici, la possibilità di modificare le impostazioni di sistema e l'accesso remoto al server.

La gestione centralizzata dei gruppi semplifica l'amministrazione del sistema e migliora la sicurezza, riducendo il rischio di errori umani.



Panoramica dei Gruppi Creati

Gruppo Amministrazione

Creato per gestire completamente le risorse del server con permessi elevati. L'unico membro del gruppo è Nino, aggiunto come utente di prova per verificare i permessi.

Gruppo Utenti Standard

Creato per fornire un accesso limitato alle risorse di base del server. I membri del gruppo sono Falvio e Gennaro, aggiunti come utenti di prova per verificare i permessi.

Obiettivo della Configurazione

Garantire che ogni gruppo abbia accesso solo alle risorse necessarie per svolgere il proprio ruolo, migliorando la sicurezza e semplificando l'amministrazione.



Permessi del Gruppo Amministrazione



Accesso ai file e alle cartelle

Permesso di Full Control su tutte le cartelle condivise. Questa scelta è stata fatta perché gli amministratori devono poter gestire, modificare e monitorare tutti i file presenti sul server.



Esecuzione di programmi specifici

Accesso completo a tutti i programmi installati sul server, inclusi strumenti di gestione del sistema e software di configurazione. Essenziale per installare, configurare e risolvere problemi.



Modifiche alle impostazioni di sistema

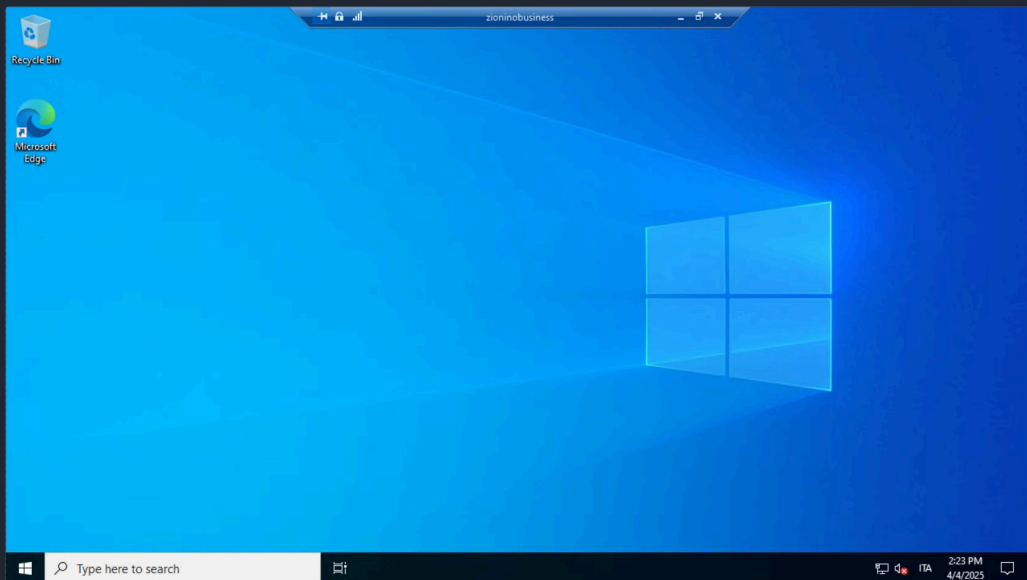
Abilitazione per modificare le impostazioni di rete, installare software e configurare servizi. Necessario per mantenere il server funzionante e sicuro.



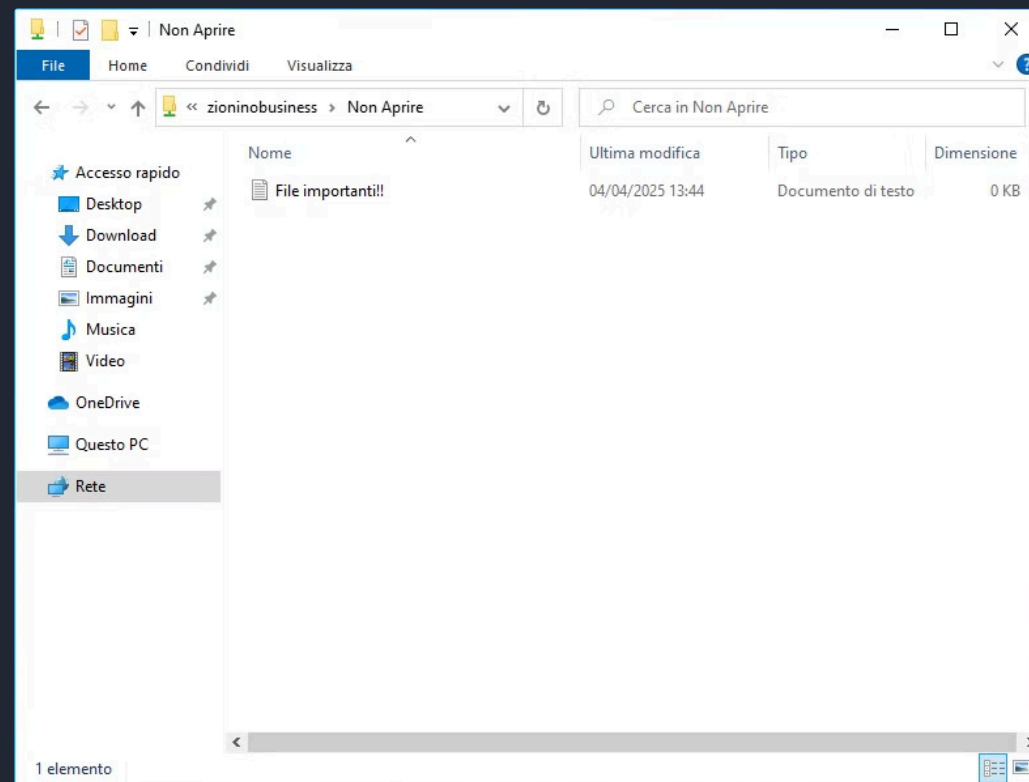
Accesso remoto al server

Permesso di connessione tramite Remote Desktop Protocol (RDP). Gli amministratori devono poter accedere al server da remoto per risolvere problemi urgenti o eseguire manutenzione.

Verifica dei permessi Amministrazione

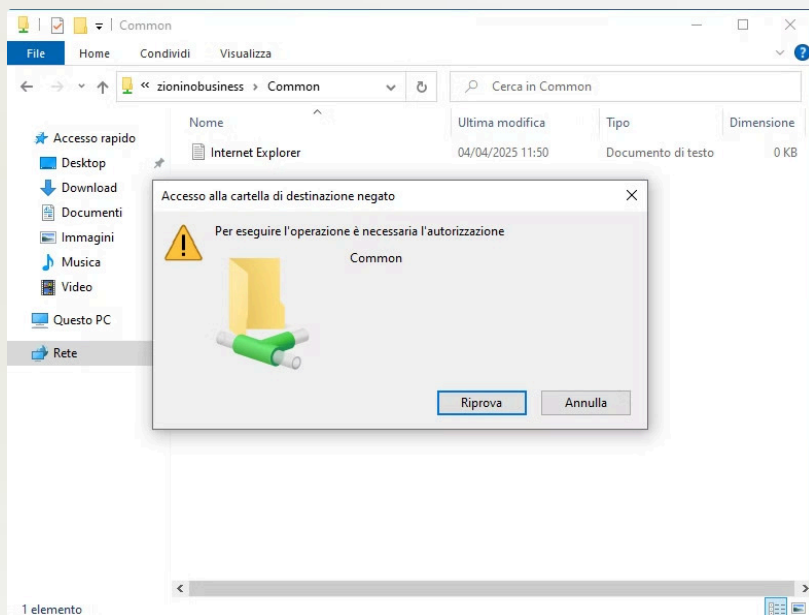


Remote Desktop



Cartelle condivise

Permessi del Gruppo Utenti Standard



Accesso ai file e alle cartelle

Permesso di lettura sulla cartella Common. Questa scelta è stata fatta per garantire che gli utenti possano visualizzare i file condivisi senza modificarli accidentalmente.



Esecuzione di programmi specifici

Accesso solo alle applicazioni standard, come browser web e suite office. Questo è sufficiente per le attività quotidiane degli utenti standard.



Modifiche alle impostazioni di sistema

Nessun permesso. Gli utenti standard non devono avere la possibilità di modificare le impostazioni del sistema per evitare errori o compromettere la sicurezza.



Accesso remoto al server

Nessun permesso. L'accesso remoto è riservato solo agli amministratori per motivi di sicurezza.

Verifica dei Permessi: Gruppo Utenti Standard

Accesso alla cartella Common

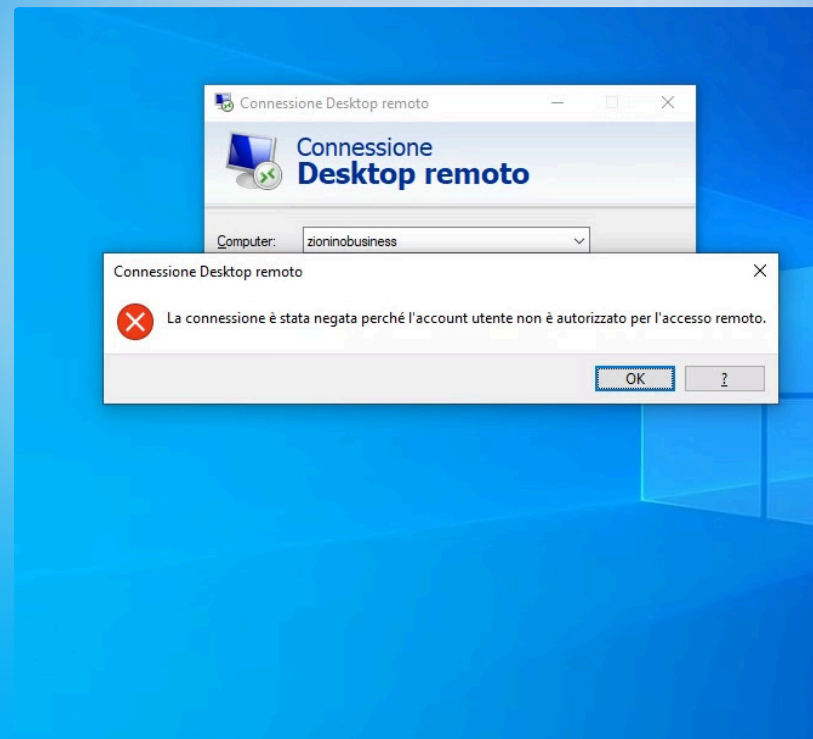
Falvio e Gennaro hanno accesso alla cartella Common con permessi di sola lettura. Possono visualizzare i file ma non possono modificarli o crearne di nuovi.

Esecuzione di applicazioni standard

Possono eseguire solo le applicazioni standard, come browser web e suite office, sufficienti per le loro attività quotidiane.

Limitazioni confermate

È stato verificato che non possono modificare le impostazioni di sistema né connettersi al server tramite RDP, confermando la corretta implementazione delle restrizioni di sicurezza.



Confronto dei Permessi tra Gruppi

Gruppo Amministrazione

- Full Control su tutte le cartelle
- Accesso completo a tutti i programmi
- Modifiche alle impostazioni di sistema
- Connessione remota tramite RDP

Questi permessi garantiscono il controllo completo del sistema per gli amministratori, consentendo loro di gestire efficacemente l'infrastruttura IT.

Gruppo Utenti Standard

- Sola lettura sulla cartella Common
- Accesso limitato alle applicazioni base
- Nessuna modifica alle impostazioni
- Nessun accesso remoto

Questi permessi limitati proteggono il sistema da modifiche accidentali, garantendo al contempo che gli utenti possano svolgere le loro attività quotidiane.

Motivazioni delle Scelte di Permessi



La struttura dei permessi è stata progettata per bilanciare la sicurezza con la funzionalità. Gli amministratori hanno accesso completo per gestire efficacemente il sistema, mentre gli utenti standard hanno limitazioni per prevenire modifiche accidentali o non autorizzate.

Vantaggi della Gestione Centralizzata dei Gruppi

Sicurezza migliorata
Riduzione dei rischi di accessi non autorizzati

Scalabilità
Facile adattamento a nuovi utenti

Efficienza amministrativa
Gestione semplificata degli utenti

Coerenza dei permessi
Applicazione uniforme delle politiche



La gestione centralizzata dei gruppi in Windows Server 2022 offre numerosi vantaggi organizzativi. Permette di applicare politiche di sicurezza coerenti, semplifica l'onboarding di nuovi utenti e riduce il carico amministrativo quando si devono apportare modifiche ai permessi.

Conclusione e Considerazioni Finali



Implementazione completata

La creazione dei gruppi "Amministrazione" e "Utenti Standard" è stata completata con successo, con permessi correttamente configurati e verificati.



Sicurezza garantita

Ogni gruppo ha accesso solo alle risorse necessarie per svolgere il proprio ruolo, migliorando la sicurezza complessiva del sistema.



Documentazione di riferimento

Questo report può essere utilizzato come riferimento per future configurazioni o revisioni della gestione dei gruppi nel server.

La configurazione implementata rappresenta una solida base per la gestione dei permessi in Windows Server 2022. In futuro, potrebbe essere utile considerare l'implementazione di gruppi aggiuntivi per ruoli più specifici, migliorando ulteriormente la granularità del controllo degli accessi.

