Creazione di Gruppi in Windows Server 2022

Introduzione

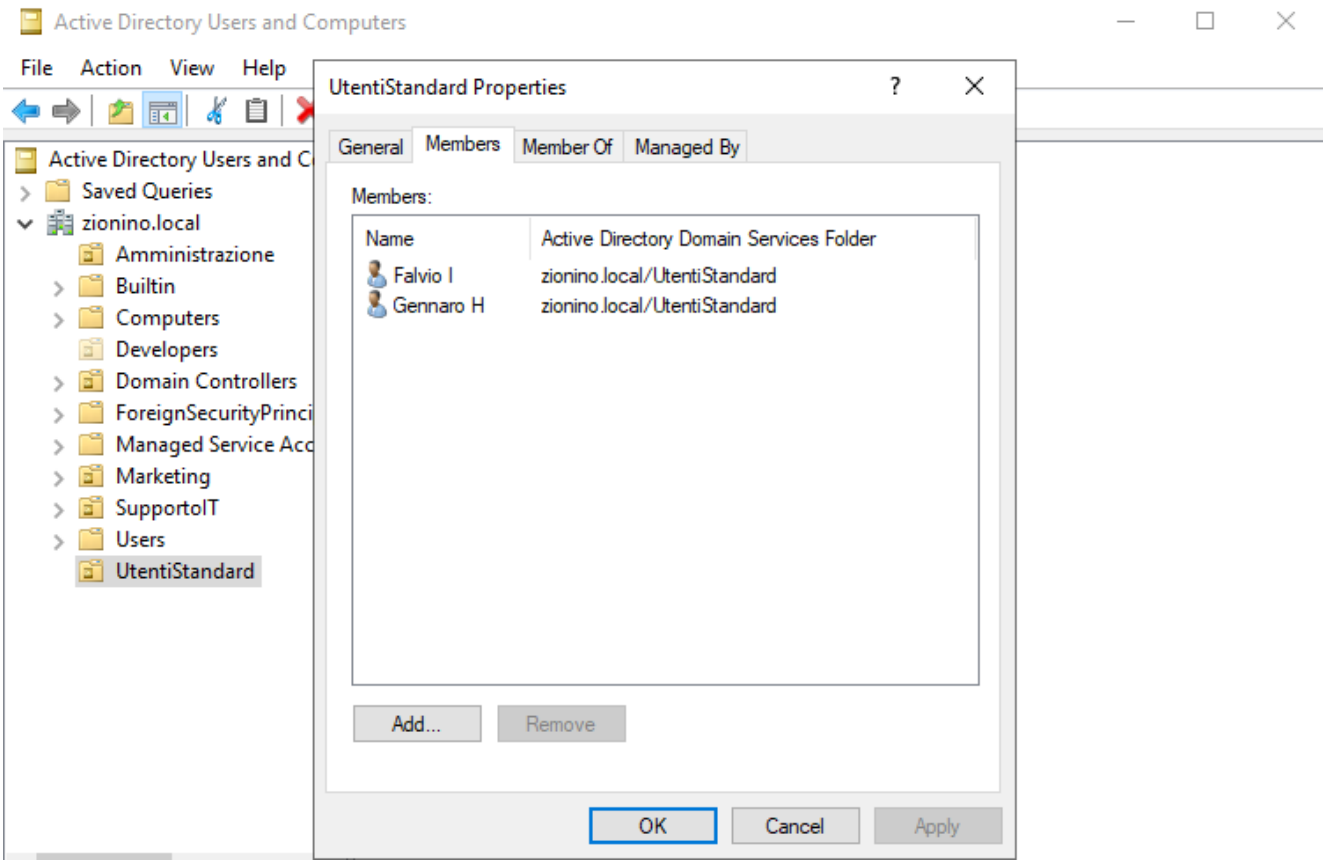
In questo esercizio sono stati creati due gruppi in Windows Server 2022: Amministrazione e Utenti Standard. Sono state assegnate autorizzazioni specifiche per ciascun gruppo, considerando aspetti come l'accesso ai file e alle cartelle, l'esecuzione di programmi specifici, la possibilità di modificare le impostazioni di sistema e l'accesso remoto al server. Di seguito vengono descritti i dettagli dei gruppi, i permessi assegnati, il motivo delle scelte effettuate e i risultati della verifica.

Creazione delle Organizational Units e dei Gruppi

La prima fase del processo riguarda la creazione di due Organizational Units (OU) all'interno di Active Directory Users and Computers. Le OU sono state progettate per separare gli utenti in base alle loro funzioni operative. La prima OU, denominata Amministrazione, è stata dedicata al gruppo di amministrazione, mentre la seconda, chiamata UtentiStandard, è stata riservata agli utenti standard.

All'interno dell'OU Amministrazione è stato creato un gruppo concepito per includere gli utenti che necessitano di accesso completo alle risorse del server, inclusi la gestione delle cartelle condivise, l'installazione di software e la configurazione dei servizi. L'utente Nino è stato aggiunto come membro di questo gruppo, rappresentando un amministratore del sistema.

Successivamente, all'interno dell'OU Utenti Standard, è stato creato un secondo gruppo di sicurezza globale, progettato per gli utenti che richiedono solo un accesso limitato alle risorse di base del server, come la lettura di file condivisi. Gli utenti Falvio e Gennaro sono stati aggiunti a questo gruppo, rappresentando gli utenti standard che utilizzano il server per attività quotidiane.



Dettagli delle cartelle e permessi assegnati:

Amministrazione

Il gruppo "Amministrazione" è stato creato per gestire completamente le risorse del server. I permessi assegnati sono i seguenti:

- 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.
- 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.

L'unico membro del gruppo è Nino, che è stato aggiunto come utente di prova per verificare i permessi.

Utenti Standard

Il gruppo "Utenti Standard" è stato creato per fornire un accesso limitato alle risorse di base del server. I permessi assegnati sono i seguenti:

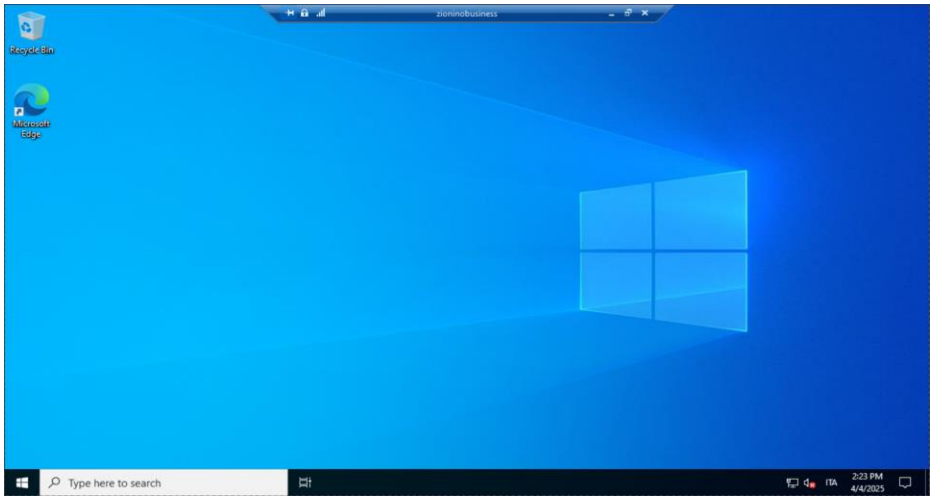
- Accesso ai file e alle cartelle: Permesso di lettura sulla cartella Common. Questa scelta è stata fatta per garantire che gli utenti possano visualizzare i file condivisi senza modificarli accidentalmente.
- Modifiche alle impostazioni di sistema: Nessun permesso. Gli utenti standard non devono avere 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

Per verificare che i permessi fossero corretti, sono stati creati utenti di prova e aggiunti ai gruppi. Ecco i risultati:

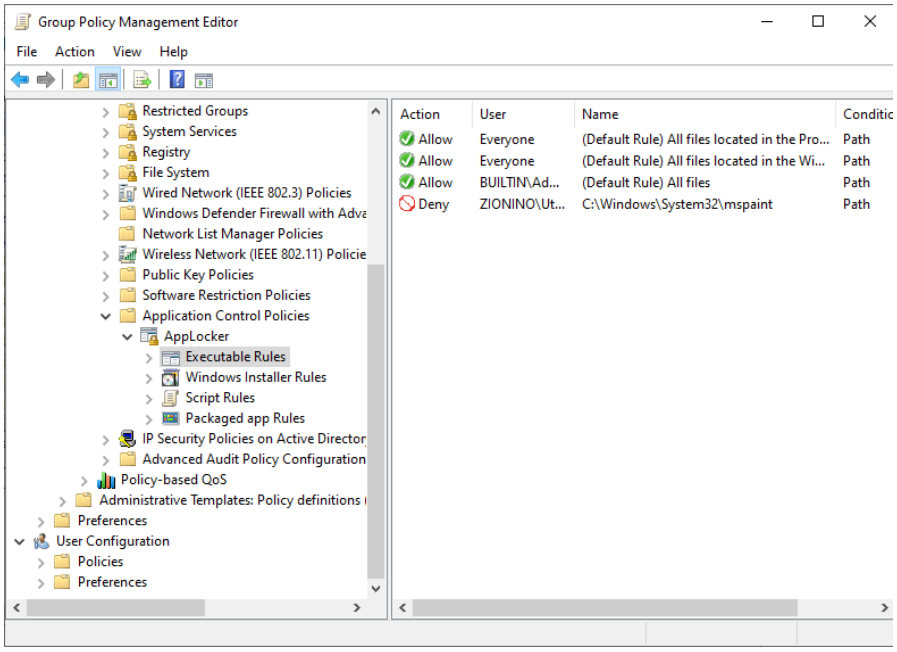
Nino (Amministrazione):

- Ha accesso completo a tutte le cartelle condivise, con permesso di Full Control
- Può connettersi al server tramite RDP.

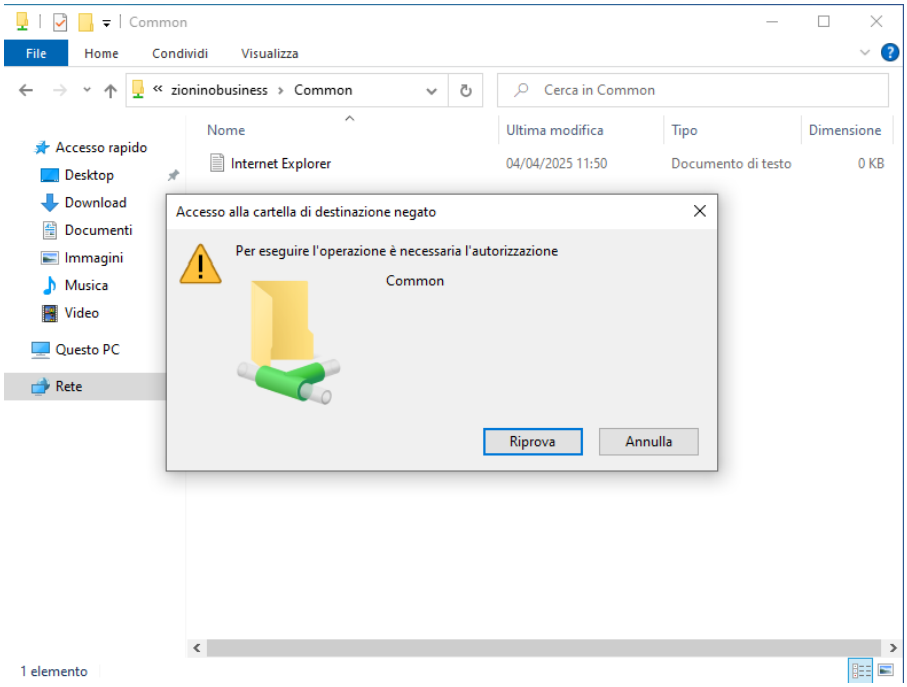


Flavio e Gennaro (Utenti Standard):

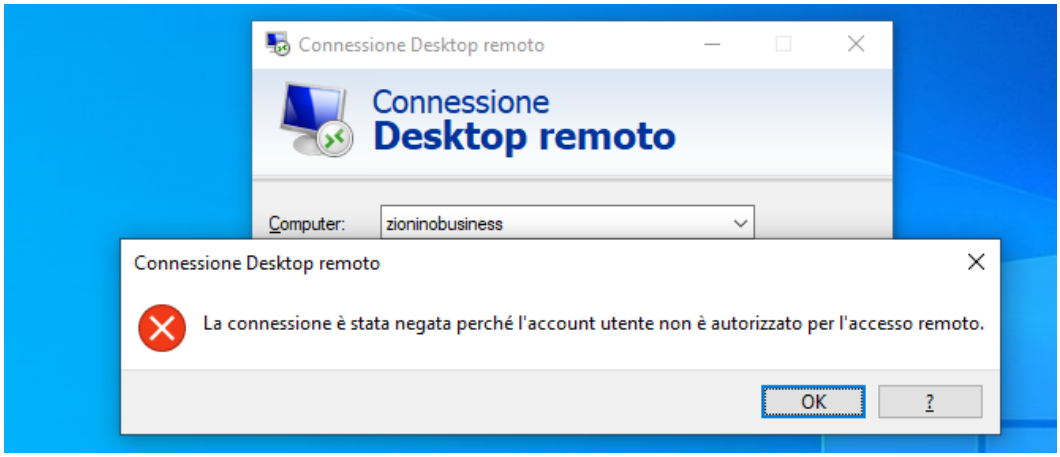
- Tramite Applocker è possibile bloccare applicazioni per renderle non eseguibili da un gruppo di utenti.



- Hanno accesso alla cartella Common con permessi di sola lettura.



- Non possono connettersi al server tramite RDP.



Conclusione

La creazione dei gruppi "Amministrazione" e "Utenti Standard" è stata completata con successo. I permessi assegnati sono stati attentamente documentati e verificati, garantendo che ogni gruppo abbia accesso solo alle risorse necessarie per svolgere il proprio ruolo. La gestione centralizzata dei gruppi semplifica l'amministrazione del sistema e migliora la sicurezza, riducendo il rischio di errori umani.