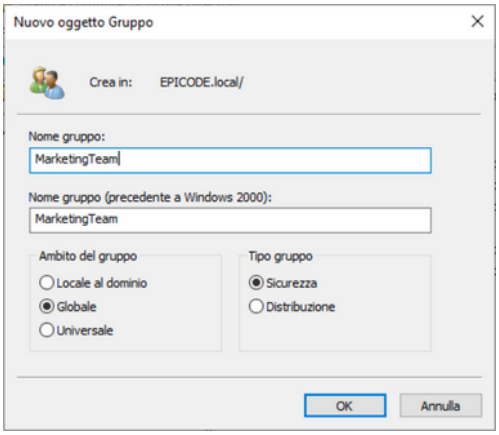
GRUPPI e PERMESSI / WINDOWS SERVER 22

Introduzione

In questo esercizio, ci siamo concentrati sulla gestione dei gruppi di utenti in un ambiente precedentemente configurato di Windows Server 2022, dove il dominio, le unità organizzative e i file condivisi già sono stati impostati. Il nostro obiettivo è stato quello di creare due gruppi di utenti con funzioni specifiche e assegnare loro i permessi necessari per svolgere le rispettive attività in modo efficiente e sicuro.
Questo approccio riflette un'implementazione pratica delle best practice per la gestione delle risorse e della sicurezza in un server aziendale.

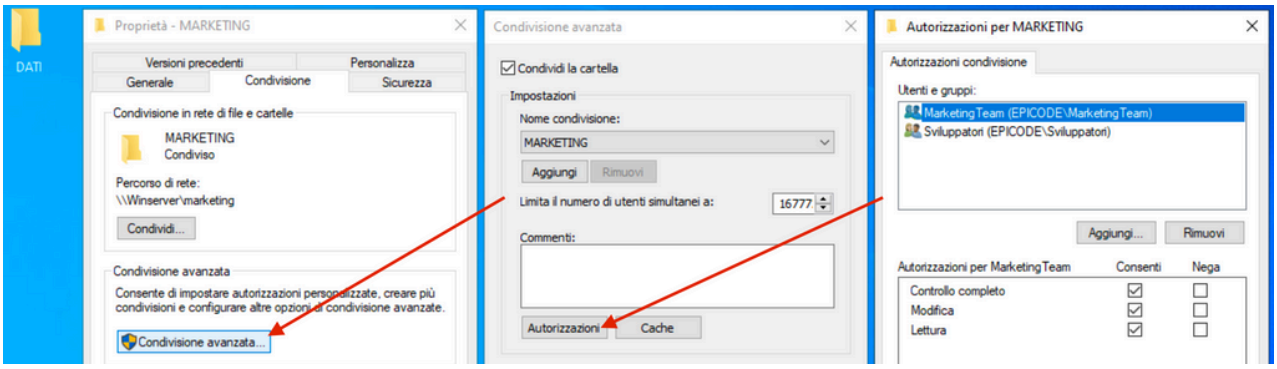


1. Creazione dei Gruppi

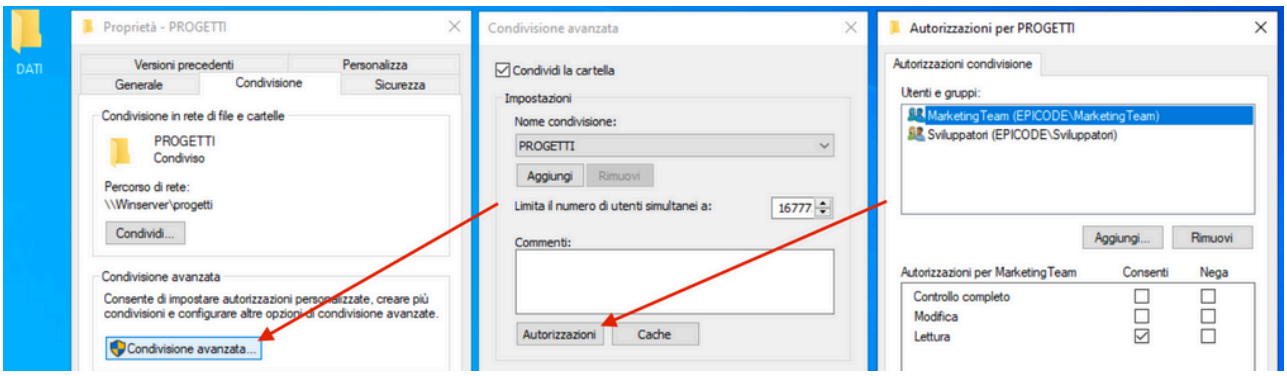
Attraverso **"Server Manager"** sono stati creati due gruppi Sviluppatori e MarketingTeam.
Sviluppatori: Responsabile della gestione e dello sviluppo delle applicazioni aziendali.
MarketingTeam: Accesso limitato per gestire file e cartelle specifici legati alle campagne pubblicitarie.

2. Assegnazione dei Permessi

Sono stati assegnati permessi distinti alle cartelle principali.
Alla directory principale DATI è stato assegnato il permesso di sola lettura al gruppo Everyone, così da consentire a tutti gli utenti di visualizzarne il contenuto senza apportare modifiche. Questo permette una facile navigazione, ma evita che i dati vengano alterati in modo accidentale o intenzionale.
Nella cartella MARKETING, il gruppo MarketingTeam ha ottenuto il controllo completo. Ciò significa che i membri di questo gruppo possono leggere, scrivere, modificare e gestire i file e le cartelle all'interno di questa directory. Invece, il gruppo Sviluppatori dispone del solo permesso di lettura, sufficiente per consultare i file, ma non per modificarli o crearne di nuovi.

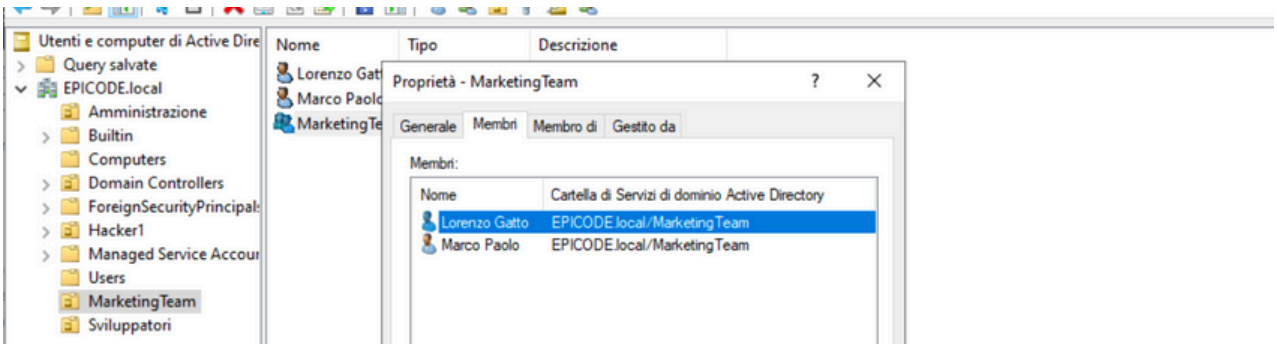


La situazione è stata invertita per la cartella PROGETTI. Qui, il gruppo Sviluppatori ha ricevuto il controllo completo, potendo così lavorare liberamente sui file relativi ai progetti aziendali. Il gruppo MarketingTeam, invece, dispone del solo permesso di lettura, così da poter consultare i dati senza però modificarli. Questo approccio riflette le esigenze operative del team di sviluppatori, che necessita di pieno controllo sui propri materiali, e garantisce che il team di marketing possa accedere alle informazioni senza rischi per l'integrità dei dati.



3. Creazione utenti di prova

Per verificare i permessi sono stati creati due utenti, che poi sono stati associati due per ogni gruppo, come possiamo vedere ad esempio nell'immagine sottostante.



Conclusioni

La gestione dei permessi è stata implementata con successo, rispettando i requisiti di sicurezza e operatività. Ogni gruppo ha accesso ai file necessari per le proprie attività, senza compromettere la sicurezza dei dati o l'integrità del sistema. Questo approccio bilancia flessibilità e protezione, contribuendo a un ambiente di lavoro organizzato e sicuro.