06/12/2024

Report di Implementazione e Configurazione: Windows Server 2022 e Windows 10 Pro

Indice

1. Introduzione

Questa relazione illustra il processo di creazione e gestione di gruppi in un ambiente Windows Server 2022 e l'assegnazione dei relativi permessi su file, cartelle e risorse condivise, oltre ad includere i passi necessari per abilitare e gestire il controllo remoto del server. L'obiettivo è fornire una guida chiara e al tempo stesso professionale, spiegando il contesto teorico, le motivazioni, i passi pratici e le considerazioni finali. Il dominio utilizzato come esempio è EPICODE.local, un dominio interno utilizzato in contesto aziendale o didattico.

2. Contesto: Foreste, Domini e la Struttura EPICODE.local

In un’infrastruttura Active Directory, la suddivisione gerarchica base comprende:

Foresta: l’entità logica più ampia, costituita da uno o più domini che condividono una configurazione e uno schema.

Dominio: una parte della foresta, con il proprio repository di utenti, gruppi e computer.

Il dominio EPICODE.local viene utilizzato per distinguere l’infrastruttura interna da internet. L’estensione “.local” è comune per gli ambienti interni, consentendo gestione autonoma di servizi, utenti e gruppi senza conflitto con i domini pubblici.

3. Creazione di Gruppi in Windows Server 2022

3.1 Concetti chiave sui gruppi e i loro benefici

I gruppi di Active Directory permettono di semplificare la gestione dei permessi. Anziché assegnare autorizzazioni a singoli utenti, si definiscono gruppi con ruoli e privilegi specifici. All’occorrenza, gli utenti vengono aggiunti o rimossi dai gruppi, con un notevole risparmio di tempo e una riduzione del rischio di errori.

3.2 Tipologie di gruppi

Gruppi Globali: Contengono tipicamente utenti dello stesso dominio e possono essere utilizzati per assegnare permessi anche in altri domini della stessa foresta.

Gruppi Locali di Dominio: Permettono di assegnare permessi alle risorse del dominio in cui sono definiti.

Gruppi Universali: Possono includere utenti e gruppi di più domini della stessa foresta, facilitando l’amministrazione su larga scala.

La scelta del tipo di gruppo dipende dalla complessità dell’ambiente. In uno scenario semplice, i Gruppi Locali di Dominio offrono flessibilità nella gestione delle risorse condivise nel medesimo dominio.

4. Assegnazione dei Permessi

4.1 Criteri di scelta dei permessi

Prima di assegnare i permessi è importante definire il principio del “minimo privilegio”: concedere solo ciò che è strettamente necessario. Alcune domande da porsi:

Gli utenti devono solo leggere o anche modificare i file?

Possono eseguire programmi specifici sul server?

Devono poter accedere in remoto al server per attività di gestione o manutenzione?

4.2 Esempio pratico di assegnazione permessi a gruppi

Supponiamo di aver creato due gruppi:

Gruppo “Amministrazione”:

Permessi: Controllo completo sulle cartelle critiche, possibilità di modificare impostazioni di sistema, esecuzione di programmi amministrativi e accesso remoto al server tramite Remote Desktop.

Gruppo “Operativo”:

Permessi: Lettura e modifica ai file presenti in una cartella condivisa (“num utenti”, “ricevute” ecc.), ma senza controllo completo e senza poteri amministrativi.

Non avrà permessi di modifica a livello di sistema né di accesso remoto al server.

4.3 Controllo Remoto del Server (Remote Desktop Services)

Per consentire a determinati gruppi o utenti l’accesso remoto al server, occorre configurare i servizi di Remote Desktop. Su Windows Server 2022, i passi principali sono:

Abilitare il Remote Desktop:

Aprire Server Manager.

Andare su Local Server.

Cliccare su “Remote Desktop” (disabilitato di default) e selezionare “Allow remote connections to this computer”.

Eventualmente abilitare l’opzione di Network Level Authentication (NLA) per una maggiore sicurezza.

Definire chi può accedere in remoto:

Cliccare su “Select Users…” e aggiungere il gruppo di sicurezza creato per questo scopo. Ad esempio, “Amministrazione”. Gli utenti inseriti in “Amministrazione” avranno dunque accesso al Desktop Remoto del server senza doverli configurare singolarmente.

Nota: L’accesso remoto è un punto delicato, va gestito con attenzione, assegnando il permesso solo agli amministratori o al personale tecnico di fiducia, in modo da mantenere il server sicuro.

5. Verifica delle Impostazioni

5.1 Creazione di utenti di prova

Creiamo due utenti di test, “Paolo” (paolo@EPICODE.local) e “Giovanna” (giovanna@EPICODE.local). Supponiamo:

Paolo viene inserito nel gruppo “Operativo”.

Giovanna viene inserita nel gruppo “Amministrazione”.

5.2 Test dei permessi assegnati e del controllo remoto

Paolo (gruppo Operativo) accede alla cartella condivisa “ricevute” dalla propria workstation:

Deve poter leggere e modificare i file, ma non eliminare la cartella, cambiare permessi o accedere da remoto al server.

Giovanna (gruppo Amministrazione) effettua un tentativo di connessione tramite Remote Desktop:

Dovrà potersi collegare al server EPICODE.local, accedere a tutte le cartelle con controllo completo e, se necessario, modificare le impostazioni di sistema.

La verifica avviene provando ad aprire il Remote Desktop Connection (mstsc), inserire l'indirizzo del server (ad es. "servername.EPICODE.local") e autenticarsi con le credenziali di Giovanna. Se la configurazione è corretta, l'accesso avviene con i privilegi previsti.

6. Esempio di Documentazione Finale

Gruppi Creati:

Amministrazione

Operativo

Permessi Assegnati:

Amministrazione:

Controllo completo su cartelle critiche.

Esecuzione di programmi di amministrazione.

Modifica alle impostazioni di sistema.

Accesso remoto al server tramite Remote Desktop.

Operativo:

Lettura e modifica dei documenti aziendali condivisi.

Nessun privilegio di sistema.

Nessun accesso remoto.

Passaggi Seguiti:

Creazione dei gruppi in Active Directory (da Active Directory Users and Computers).

Configurazione delle cartelle condivise con le autorizzazioni per i gruppi creati.

Abilitazione del Remote Desktop sul server e assegnazione del gruppo “Amministrazione” ai Remote Desktop Users (o utenti autorizzati), garantendo ai membri accesso remoto.

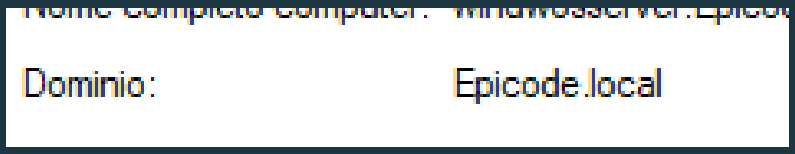
Creazione di utenti di prova, assegnazione ai gruppi pertinenti e test delle impostazioni.

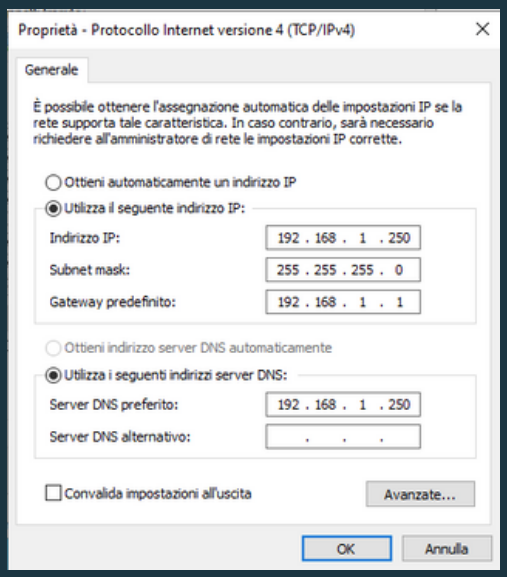
7. Conclusioni e Considerazioni Finali

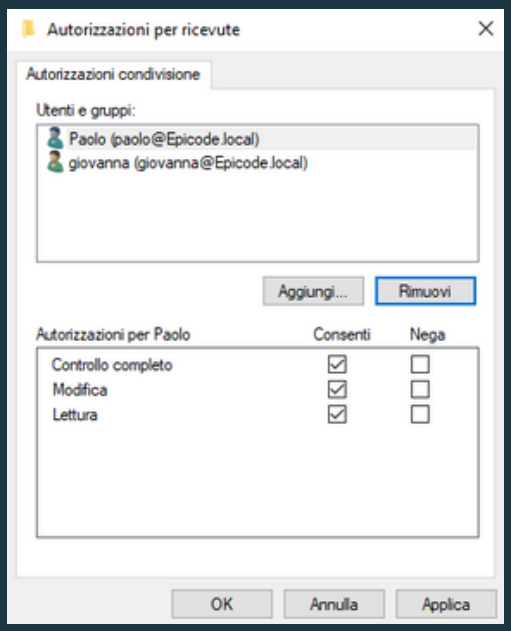
La gestione centralizzata di utenti, gruppi e permessi in un dominio interno come EPICODE.local su Windows Server 2022 migliora notevolmente l’efficienza, la sicurezza e la flessibilità dell’infrastruttura IT. L’assegnazione di permessi basata sui gruppi riduce errori e tempi di configurazione, garantendo che ciascun utente abbia esattamente i privilegi necessari al proprio ruolo.

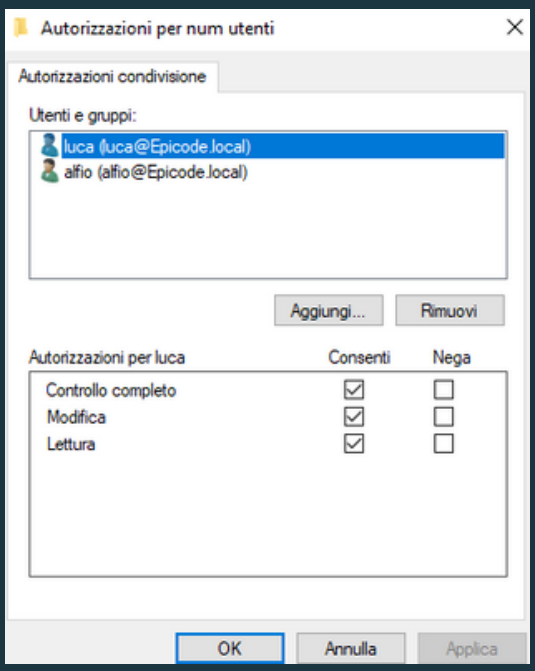
L’introduzione del controllo remoto (Remote Desktop) per il gruppo “Amministrazione” consente un intervento rapido su configurazioni di sistema e manutenzione senza accedere fisicamente al server. Questo si traduce in maggiore operatività, affidabilità e controllo, specialmente in contesti distribuiti.

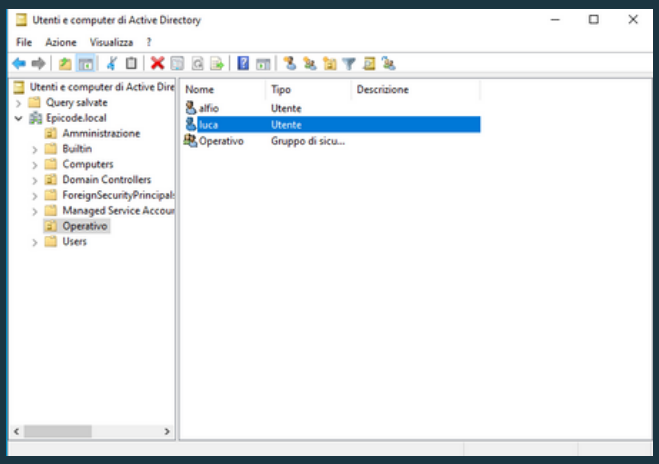
In sintesi, grazie a questa struttura gerarchica (foresta, dominio, OU, gruppi, utenti) e alla corretta assegnazione dei permessi, l’organizzazione può beneficiare di un ambiente stabile, sicuro e facile da amministrare, sia a livello di risorse interne (cartelle, file) sia in termini di gestione remota del server, garantendo una pronta risposta alle esigenze di manutenzione, monitoraggio e interventi emergenziali.

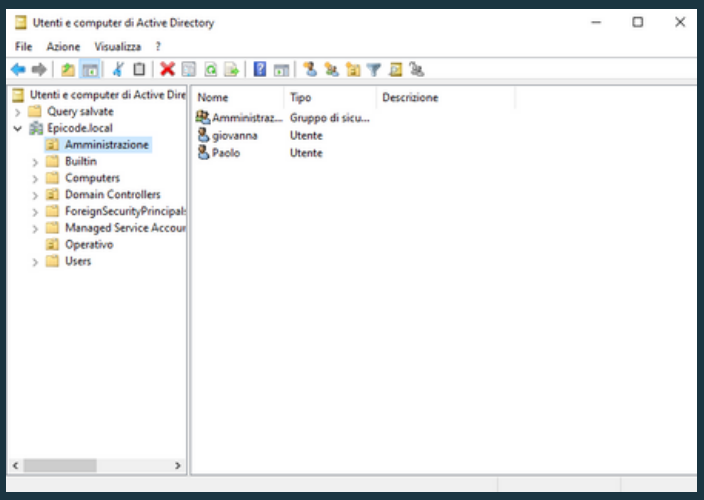

Dominio:
Epicode.local

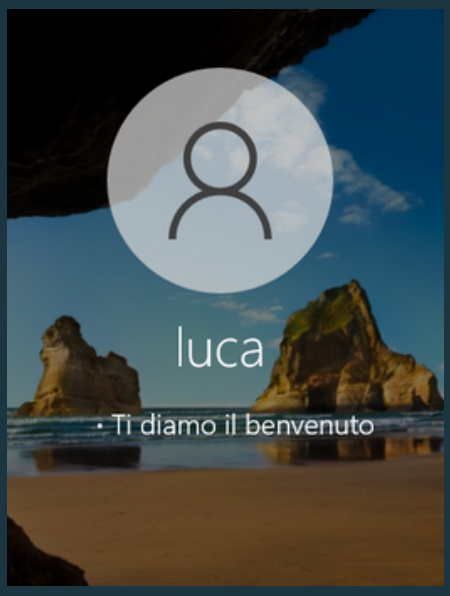

Proprietà - Protocollo Internet versione 4 (TCP/IPv4)
Generale
È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.
Ottieni automaticamente un indirizzo IP
Utilizza il seguente indirizzo IP:
Indirizzo IP: 192 . 168 . 1 . 250
Subnet mask: 255 . 255 . 255 . 0
Gateway predefinito: 192 . 168 . 1 . 1
Ottieni indirizzo server DNS automaticamente
Utilizza i seguenti indirizzi server DNS:
Server DNS preferito: 192 . 168 . 1 . 250
Server DNS alternativo:
Convalida impostazioni all'uscita
Avanzate...
OK
Annulla

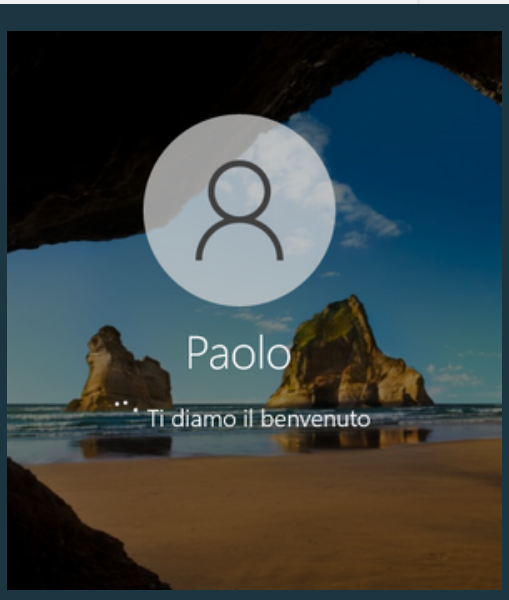

Autorizzazioni per ricevute
Autorizzazioni condivisione
Utenti e gruppi:
Paolo (paolo@Epicode.local)
giovanna (giovanna@Epicode.local)
Aggiungi...
Rimuovi
Autorizzazioni per Paolo
Consenti
Nega
Controllo completo
Modifica
Lettura
OK
Annulla
Applica

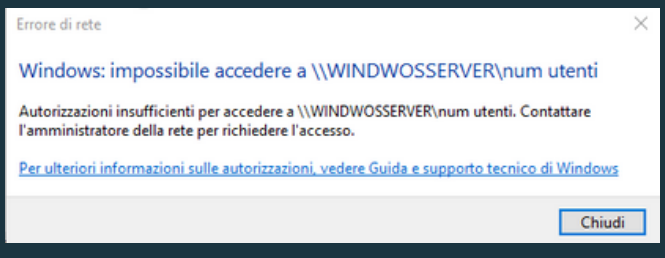

Autorizzazioni per num utenti
Autorizzazioni condivisione
Utenti e gruppi:
luca (luca@Epicode.local)
alfio (alfio@Epicode.local)
Aggiungi...
Rimuovi
Autorizzazioni per luca
Consenti
Nega
Controllo completo
Modifica
Lettura
OK
Annulla
Applica


Utenti e computer di Active Directory
File Azione Visualizza ?
Utenti e computer di Active Dire
Query salvate
Epicode.local
Amministrazione
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Operativo
Users
Nome
Tipo
Descrizione
alfio Utente
luca Utente
Operativo Gruppo di sicu...


Utenti e computer di Active Directory
File Azione Visualizza ?
Utenti e computer di Active Dire
Query salvate
Epicode.local
Amministrazione
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Operativo
Users
Nome
Tipo
Descrizione
Amministraz... Gruppo di sicu...
giovanna Utente
Paolo Utente


luca
Ti diamo il benvenuto


Paolo
Ti diamo il benvenuto


Errore di rete
Windows: impossibile accedere a \\WINDWOSSERVER\num utenti
Autorizzazioni insufficienti per accedere a \\WINDWOSSERVER\num utenti. Contattare l'amministratore della rete per richiedere l'accesso.
Per ulteriori informazioni sulle autorizzazioni, vedere Guida e supporto tecnico di Windows
Chiudi