S10-L5 WINDOWS SERVER

Esercizio

Creazione di Gruppi in Windows Server 2022 Obiettivo Lo scopo di questo esercizio è di familiarizzare con la gestione dei gruppi di utenti in Windows Server 2022. Imparerai a creare gruppi, assegnare loro permessi specifici e comprendere l'importanza della gestione dei gruppi per la sicurezza e l'amministrazione del sistema.

INDICE

CREAZIONE GRUPPI

Una volta configurato il server di windows, passeremo alla creazione di 2 gruppi che identificheranno il reparto “amministrazione” ed il reparto “marcketing”.

Inseriremo all’interno di “**Amministrazione**”:

-Valerio Benedetti

-Carlo Benedetti

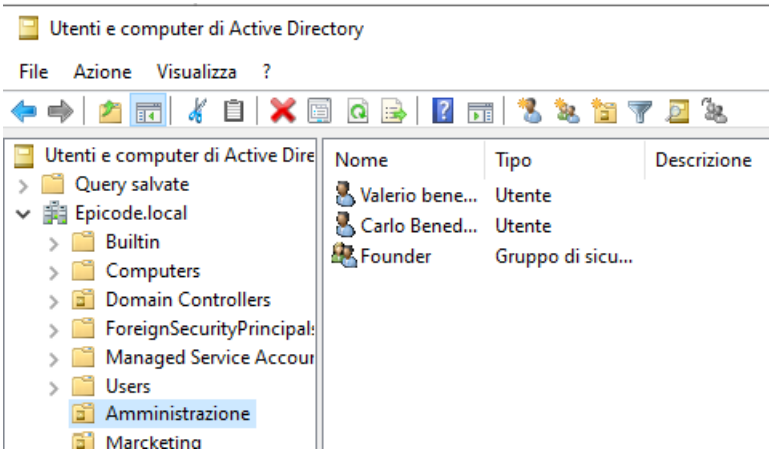
Inseriremo all’interno del “ **Marcketing**” :

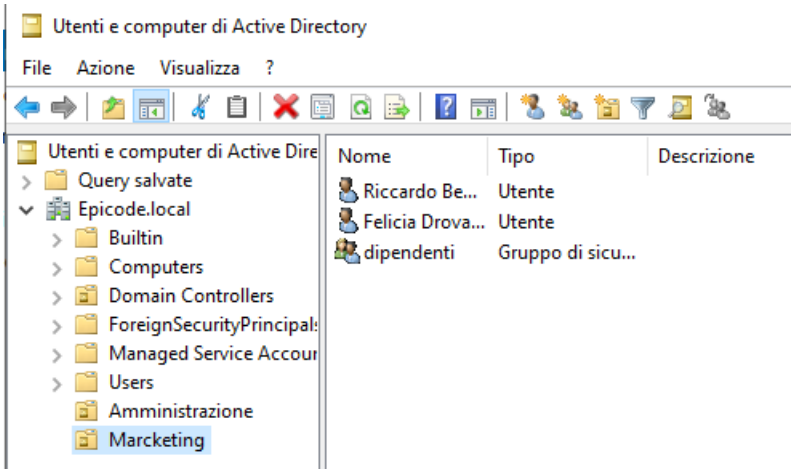
-Riccardo Benedetti

-Felicia drovandini

Dopo creeremo altri gruppi all’interno di amministrazione e di marcketing.

- Dentro amministrazione creeremo il gruppo “ **founder**”
- Dentro marcketing creeremo il gruppo “ **dipendenti**”

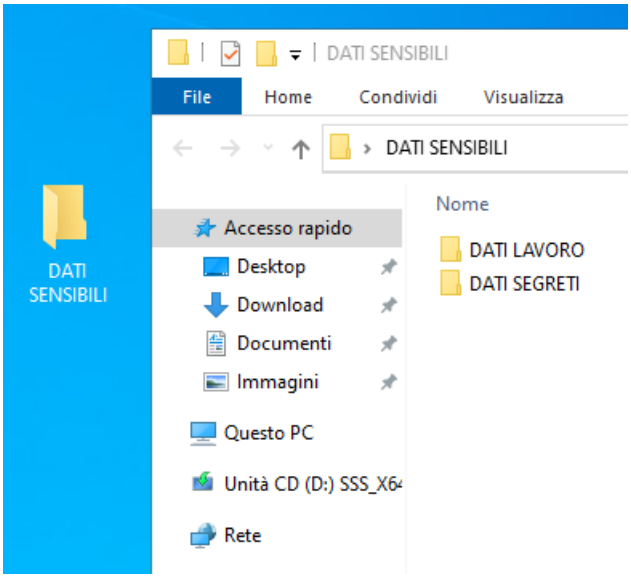




CREAZIONE CARTELLE

Creeremo nel server una cartella dal nome “ DATI SENSIBILI”, ed al suo interno inseriremo due cartelle:

- Dati lavoro
- Dati segreti



ASSEGNAZIONE PERMESSI

L'**assegnazione dei permessi sulle cartelle** è un processo che consente agli amministratori di sistema di definire chi può accedere, modificare o gestire specifiche cartelle (e i file al loro interno) su un sistema operativo, come **Windows Server 2022** o qualsiasi altra versione di Windows.

Questi permessi sono cruciali per garantire la **sicurezza dei dati**, limitando l'accesso solo alle persone o ai gruppi autorizzati.

Tipi di Permessi per Cartelle in Windows

Windows offre una gamma di permessi per gestire l'accesso alle cartelle. I permessi si dividono in:

1. Permessi Standard

Questi sono i permessi più comuni, facili da configurare:

- **Full Control (Controllo completo):** L'utente o il gruppo può eseguire tutte le operazioni sulla cartella, inclusa la modifica dei permessi e la cancellazione della cartella stessa.
- **Modify (Modifica):** Consente di modificare i file all'interno della cartella (inclusi aggiunta, eliminazione e modifica dei contenuti).
- **Read & Execute (Lettura ed esecuzione):** Consente di aprire file ed eseguire programmi nella cartella.
- **List Folder Contents (Visualizza contenuto della cartella):** Permette di visualizzare i nomi delle sottocartelle e dei file all'interno della cartella.
- **Read (Lettura):** Consente di aprire e leggere il contenuto della cartella e dei file, ma non di modificarli.
- **Write (Scrittura):** Consente di creare nuovi file o cartelle e di modificarli.

2. Permessi Avanzati

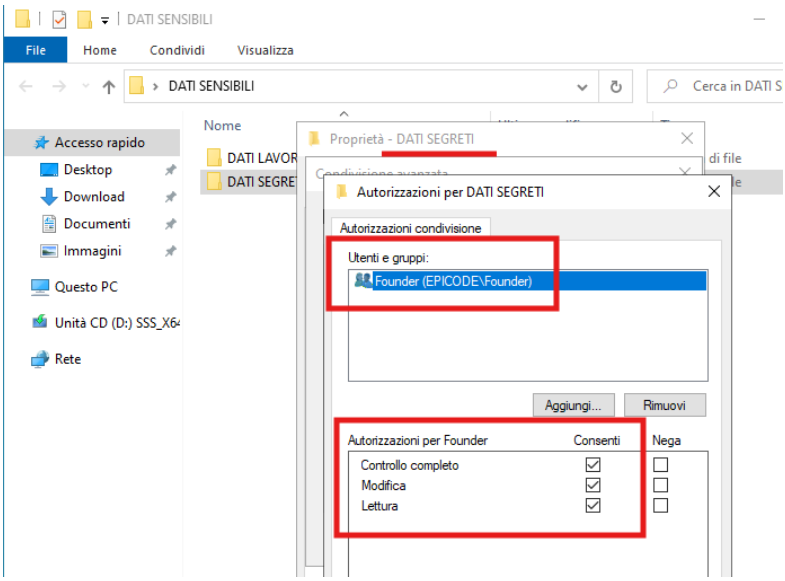
I permessi avanzati consentono un controllo più dettagliato. Questi includono:

- **Permessi su attributi specifici** (ad esempio, possibilità di cambiare proprietà di un file o una cartella).
- **Ereditarietà** (ad esempio, i permessi applicati alla cartella padre possono essere propagati alle sottocartelle).

DATI SEGRETI

Nella cartella “dati segreti “, una volta rimossa la funzione “everyone” (dove in automatico si assegnano a tutti il controllo completo) ed andremo a dare il permesso completo solo al gruppo FOUNDER (con al suo interno Valerio e Carlo).

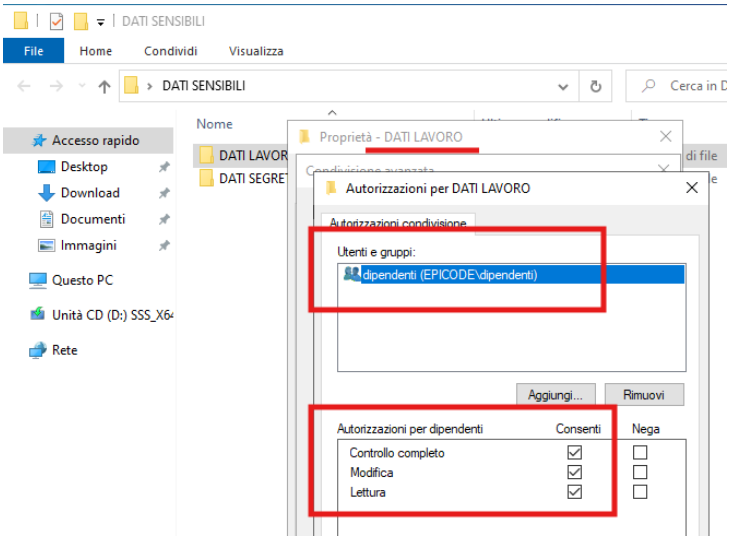
Cosi solo gli utenti Valerio e Carlo potranno avere accesso completo alla cartella dati segreti.



DATI LAVORO

Nella cartella “dati lavoro “, una volta rimossa la funzione “everyone” (dove in automatico si assegnano a tutti il controllo completo) ed andremo a dare il permesso completo solo al gruppo DIPENDENTI (con al suo interno Riccardo e Felicia).

Cosi solo gli utenti Ricacrdo e Felicia potranno avere accesso completo alla cartella dati lavoro.



CONTROLLO SU WINDOWS 10

Una volta assegnati i vari permessi andremo nell'host di windows ed entreremo (una volta accertati che siano sulla stessa rete tramite un ping) con l'account di Valerio e da qui potremo vedere che effettivamente noi abbiamo tutti i permessi per accedere alla cartella dei dati segreti, ma se volessimo entrare nella cartella dei dati lavoro non potremmo entrare.

FORESTA IN WINDOWS SERVER

Una **foresta** in **Windows Server** è un'unità logica di gestione all'interno di **Active Directory (AD)**. Rappresenta il livello più alto di una struttura Active Directory e contiene uno o più **domini**, che condividono una configurazione comune, uno schema, e una relazione di fiducia automatica.

Caratteristiche principali di una foresta

1. **Schema unificato:**
   Lo schema è l'insieme di regole che definiscono i tipi di oggetti (ad esempio, utenti, gruppi, computer) e i loro attributi. Tutti i domini all'interno di una foresta condividono lo stesso schema, il che garantisce uniformità nella gestione degli oggetti.
2. **Configurazione globale:**
   Le impostazioni generali, come le policy di sicurezza, possono essere configurate a livello di foresta e applicate a tutti i domini al suo interno.
3. **Relazione di fiducia automatica:**
   Tutti i domini nella stessa foresta hanno una relazione di fiducia automatica **bidirezionale e transitiva**, il che significa che gli utenti e i computer di un dominio possono autenticarsi in altri domini, a meno che non siano impostate restrizioni specifiche.
4. **Catalogo globale:**
   Ogni foresta ha un **global catalog (GC)**, che è un database parziale contenente informazioni su tutti gli oggetti in tutti i domini della foresta. Questo consente ricerche rapide in tutta la foresta.

Struttura di una foresta

Una foresta può essere composta da:

- **Domini:**
  Un dominio è l'unità principale che rappresenta una raccolta di oggetti (come utenti, gruppi, computer) all'interno di una rete. I domini condividono le policy di sicurezza e l'autenticazione.
- **Unità organizzative (OU):**
  All'interno dei domini, gli oggetti possono essere organizzati in **unità organizzative**, che aiutano a strutturare la gestione per gruppi specifici.
- **Trust (Fiducia):**
  La foresta può contenere più domini che sono collegati da relazioni di fiducia.

Tipologie di foresta

1. **Foresta singolo dominio:**
   Una foresta con un solo dominio. È la configurazione più semplice.

2. **Foresta multidominio:**
   Contiene più domini, utile in ambienti complessi o con organizzazioni che richiedono separazione amministrativa tra domini.

Perché utilizzare una foresta in Active Directory?

- **Gestione centralizzata:**
  Tutti i domini all'interno della foresta condividono configurazioni, policy e relazioni di fiducia.
- **Scalabilità:**
  Le foreste permettono di espandere l'infrastruttura includendo nuovi domini senza compromettere la gestione globale.
- **Sicurezza:**
  Grazie alle relazioni di fiducia e ai permessi ben definiti, è possibile controllare l'accesso agli oggetti in tutta la foresta.

DOMINIO IN WINDOWS SERVER

Un **dominio** in **Windows Server** è una struttura logica utilizzata per gestire e organizzare una rete di computer, utenti, gruppi e altre risorse in modo centralizzato. È una componente fondamentale di **Active Directory (AD)**, che consente agli amministratori di rete di controllare l'accesso e gestire la sicurezza e le configurazioni in modo uniforme.

Caratteristiche principali di un Dominio

1. **Autenticazione centralizzata:**
   Gli utenti e i dispositivi si autenticano tramite un **controller di dominio (DC)**, che gestisce le credenziali e autorizza l'accesso alle risorse.
2. **Struttura gerarchica:**
   Un dominio può contenere **oggetti**, come utenti, computer, gruppi e stampanti, organizzati in una gerarchia.
3. **Un unico nome DNS:**
   Un dominio è identificato da un nome univoco, come ad esempio azienda.local o example.com. Questo nome viene utilizzato per identificare e risolvere le risorse all'interno del dominio.
4. **Policy di gruppo (GPO):**
   I domini permettono di applicare **criteri di gruppo (Group Policy Objects)**, che consentono di configurare regole e impostazioni su tutti gli utenti e i computer membri del dominio.

5. **Relazione di fiducia:**
   I domini all'interno di una foresta possono avere relazioni di fiducia, consentendo l'accesso alle risorse tra domini diversi.

Componenti di un Dominio

1. **Controller di dominio (Domain Controller, DC):**
   Un server che gestisce Active Directory e fornisce servizi di autenticazione e autorizzazione per il dominio. È il cuore del dominio.
2. **Active Directory (AD):**
   Il servizio che contiene le informazioni su tutti gli oggetti nel dominio. È una sorta di "rubrica" centrale.
3. **Oggetti di Active Directory:**
   Include elementi come:
   - **Utenti:** Account delle persone che accedono alla rete.
   - **Computer:** Dispositivi registrati nel dominio.
   - **Gruppi:** Raccolte di utenti o computer per la gestione dei permessi.
   - **Unità organizzative (OU):** Contenitori logici per organizzare oggetti in modo gerarchico.
4. **Domain Name System (DNS):**
   Ogni dominio utilizza un sistema DNS per risolvere i nomi degli oggetti in indirizzi IP.

Vantaggi dell'utilizzo di un Dominio

1. **Gestione centralizzata:**
   Gli amministratori possono gestire utenti, computer e risorse da un unico punto centrale.
2. **Sicurezza migliorata:**
   Grazie a credenziali centralizzate e policy di gruppo, l'accesso alle risorse può essere controllato con precisione.
3. **Scalabilità:**
   I domini sono adatti sia per piccole reti che per reti aziendali complesse.
4. **Single Sign-On (SSO):**
   Gli utenti si autenticano una sola volta per accedere a tutte le risorse del dominio.
5. **Condivisione delle risorse:**
   File, stampanti e altre risorse possono essere facilmente condivise all'interno del dominio.

RIEPILOGO PASSAGGI

1. Configurazione iniziale

Creazione della foresta e dominio Active Directory

1. **Installazione di Active Directory (AD)**
    - Apri il Server Manager.
    - Vai su **Aggiungi ruoli e funzionalità**.
    - Seleziona il ruolo **Servizi di dominio Active Directory (AD DS)** e segui le istruzioni per completare l'installazione.
    - Al termine, configura AD DS promuovendo il server a controller di dominio.
        - Durante il setup, crea una nuova foresta con un dominio (ad esempio, example.local).
2. **Configurazione del DNS**
    - Durante la configurazione del dominio, il ruolo DNS verrà configurato automaticamente per supportare Active Directory.
3. **Riavvio del server**
    - Dopo aver completato la configurazione, riavvia il server per applicare le modifiche.

---

2. Creazione dei gruppi

1. Accedi al server con un account amministrativo.
2. Apri il pannello **Gestione utenti e computer di Active Directory** (digita dsa.msc nella barra di ricerca).
3. Naviga nella struttura di Active Directory:
    - Vai su **Users** o crea un'unità organizzativa (OU) personalizzata.
4. Crea due gruppi:
    - Fai clic destro sulla posizione desiderata (ad esempio, nella tua OU) e seleziona **Nuovo > Gruppo**.
    - Scegli un nome significativo per ciascun gruppo (ad esempio, amministrazione emarcketing).
    - Specifica il tipo di gruppo:
        - **Globale** (per utenti specifici del dominio).
        - **Distribuzione** o **Sicurezza** (scegli Sicurezza per assegnare permessi).
5. Completa la configurazione cliccando su **OK**.

---

3. Assegnazione dei permessi ai gruppi

1. **Accesso a file e cartelle**
    - Crea una cartella condivisa nel server (ad esempio, dati segreti e dati lavoro).

- Fai clic destro sulla cartella e seleziona **Proprietà > Sicurezza > Modifica**.
- Aggiungi il gruppo (ad esempio, founder) e specifica i permessi:
  - **Lettura** per visualizzare i file.
  - **Modifica** per aggiungere, modificare o eliminare file.

2. **Esecuzione di programmi specifici**
   - Configura permessi su eseguibili o applicazioni specifiche tramite la scheda **Sicurezza** delle proprietà del file.
3. **Modifiche alle impostazioni di sistema**
   - Per assegnare questi permessi, aggiungi il gruppo a **Administrators** (cautela con i permessi avanzati).
4. **Accesso remoto**
   - Apri **Proprietà del Sistema** (Win + R > sysdm.cpl).
   - Vai su **Accesso remoto > Seleziona utenti**.
   - Aggiungi il gruppo che necessita di accesso remoto.

---

4. Verifica della configurazione

Creazione degli utenti di prova

1. Torna a **Gestione utenti e computer di Active Directory**.
2. Crea un utente:
   - Fai clic destro sulla posizione desiderata e seleziona **Nuovo > Utente**.
   - Completa il modulo con nome e password.
3. Assegna l'utente a un gruppo:
   - Apri le proprietà dell'utente, vai su **Membro di**, e aggiungi il gruppo desiderato.

Verifica su Windows 10

1. Unisci il computer Windows 10 al dominio:
   - Vai su **Impostazioni > Sistema > Informazioni su > Cambia impostazioni**.
   - Inserisci il nome del dominio (esempio: EPICODE) e riavvia.
2. Accedi al computer con un utente di prova:
   - Usa le credenziali: EPICODE e la password.
3. Verifica:
   - Controlla i permessi di accesso alle risorse condivise e l'esecuzione di programmi in base al gruppo dell'utente.