Report S10/L5: Creazione e Gestione di Gruppi in Windows Server 2022

A cura di Iris Canole

1. Introduzione e Obiettivo della Lezione

Lo scopo primario di questa esercitazione è **familiarizzare l'utente con gli strumenti e le procedure di gestione dei gruppi di utenti all'interno dell'ambiente Windows Server 2022**.

La **gestione degli utenti e dei gruppi** è un aspetto fondamentale dell'amministrazione di qualsiasi sistema operativo, specialmente in ambienti aziendali che utilizzano **Windows Server 2022**. L'organizzazione efficiente degli account utente in gruppi logici non solo **semplifica l'amministrazione** quotidiana, ma è anche un pilastro essenziale per mantenere la **sicurezza** e l'integrità delle risorse di sistema.

2. Configurazione dell'Ambiente e Creazione Oggetti

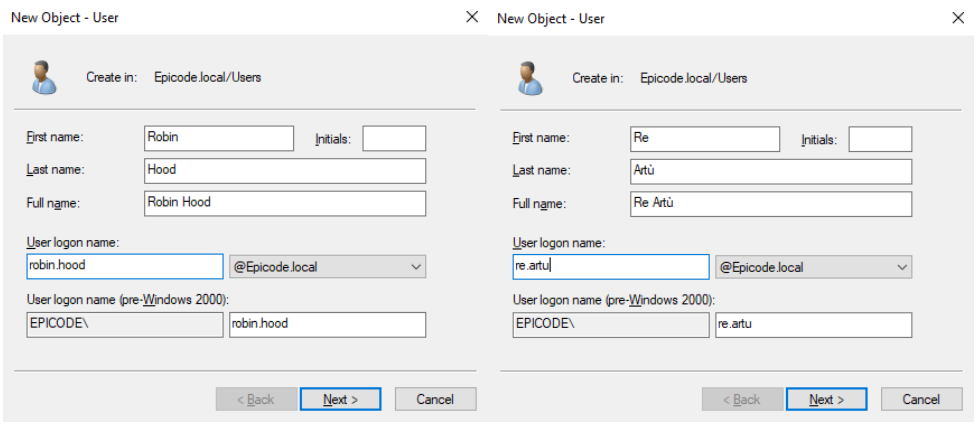
Prima di iniziare, è stato necessario accedere all'ambiente Windows Server 2022 con i **permessi amministrativi**.

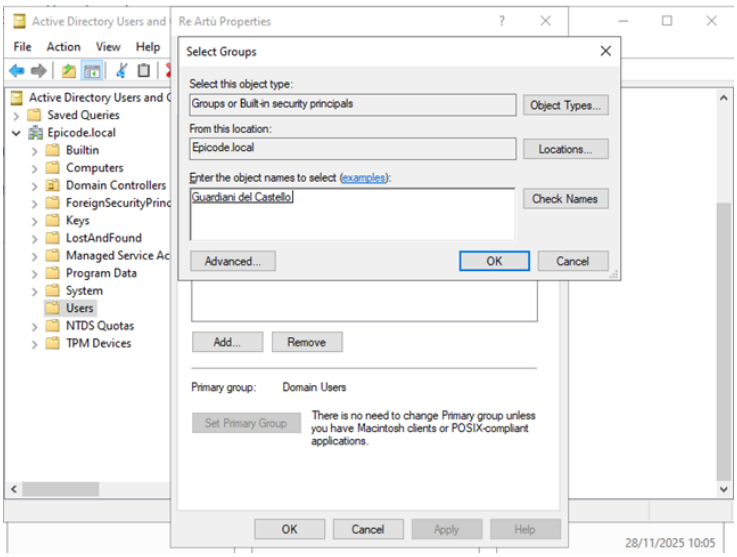
1. **Pulizia dell'Ambiente**
   Per garantire che i risultati del test fossero validi, ho eliminato tutti gli utenti, i gruppi e le Unità Organizzative (OU) creati nelle esercitazioni precedenti, riportando la console **Active Directory Users and Computers (ADUC)** a uno stato pulito.

2. **Creazione di Gruppi e Utenti**
   Sono stati creati due gruppi di sicurezza distinti, con nomi significativi per riflettere il loro ruolo nell'organizzazione, e sono stati assegnati loro i seguenti utenti:

Gruppo	Scopo (Ruolo)	Membri Assegnati	Privilegio
Guardiani del Castello	Amministrazione e Gestione Dati Sensibili	Re Artù, Mago Merlino	Elevato (Superiore)

Abitanti del Villaggio	Operazioni Quotidiane e Lavoro Standard	Robin Hood, Lady Marian	Standard (Minimo)

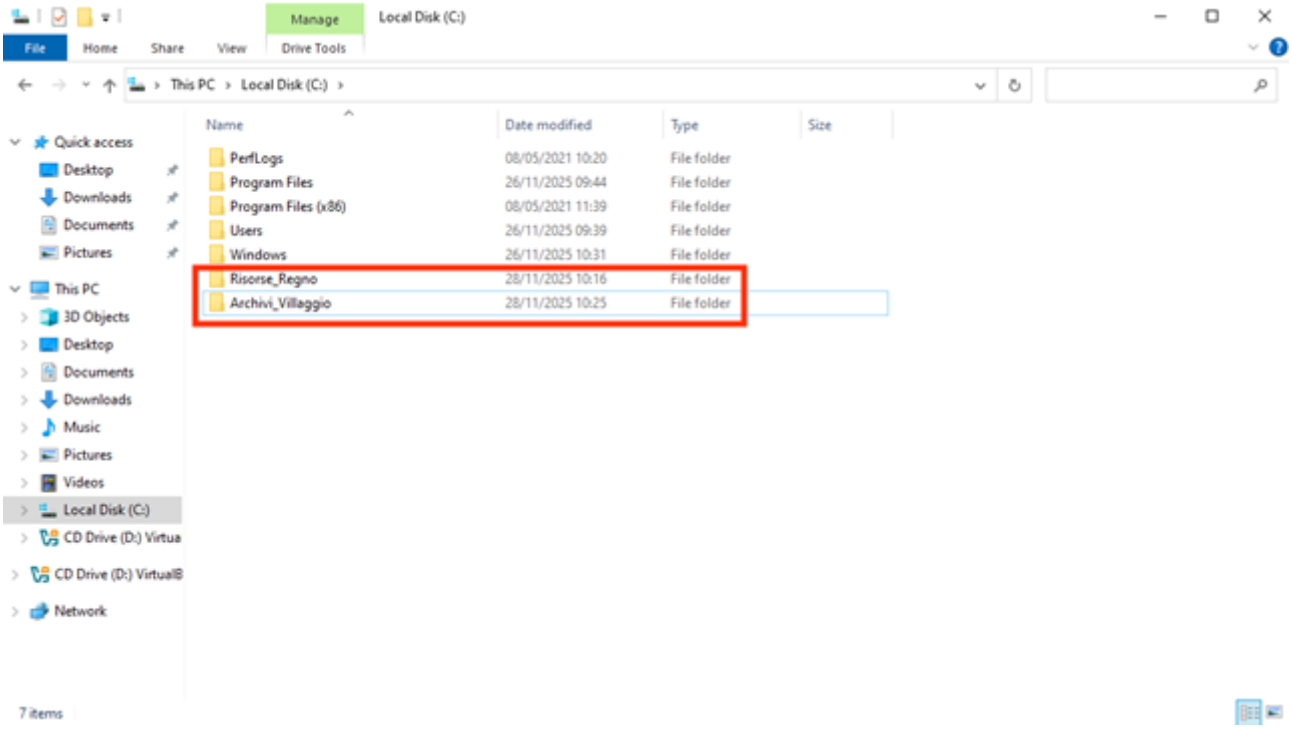




> **Nota**
>
> Le immagini di cui sopra rappresentano la creazione degli utenti Robin Hood e Re Artù, in più l'assegnazione del gruppo per l'utente Re Artù. Chiaramente tutti questi passaggi sono stati effettuati per tutti gli altri utenti creati e assegnati come mostrato in tabella. Gli screen sono omessi per evitare la rindondanza in questo report.

3. Assegnazione dei Permessi e Architettura dei Dati

Per testare l'efficacia della gestione dei gruppi, sono state create due cartelle sul server (`C:`) che rappresentano diversi livelli di sensibilità dei dati. I permessi sono stati configurati utilizzando le Autorizzazioni **NTFS** (New Technology File System).

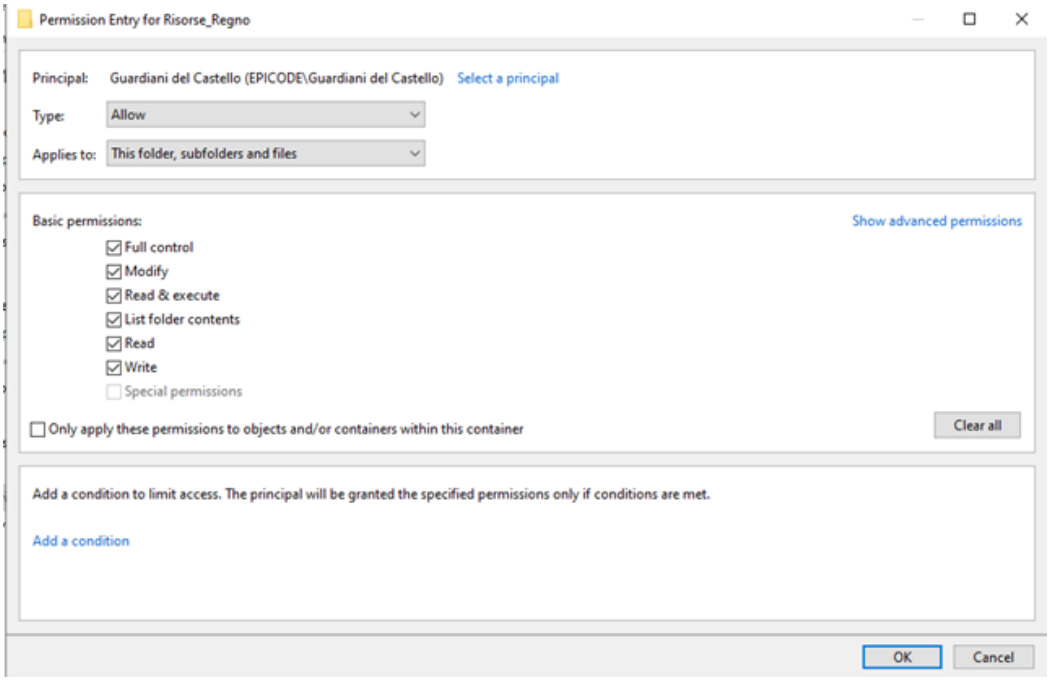


✨ NTFS

NTFS è il **file system proprietario con journaling** sviluppato da Microsoft. Fu introdotto con Windows NT 3.1 nel 1993 ed è da allora il file system predefinito per la famiglia di sistemi operativi Windows NT, inclusi tutti i sistemi operativi Windows moderni (come Windows 10 e 11), sostituendo il più datato File Allocation Table (FAT).

NTFS è stato progettato per garantire **robustezza, sicurezza e prestazioni** negli ambienti informatici moderni, soprattutto nella gestione di volumi e file di grandi dimensioni.

1. **Architettura dei Permessi**
    - **C:\Risorse_Regno** (Cartella Sensibile/Amministrativa)
        - **Funzione:** Contiene dati sensibili, accessibili solo agli amministratori.
        - **Gruppi Assegnati:** `Guardiani del Castello`.
        - **Permesso NTFS: Controllo Completo** (Full Control).

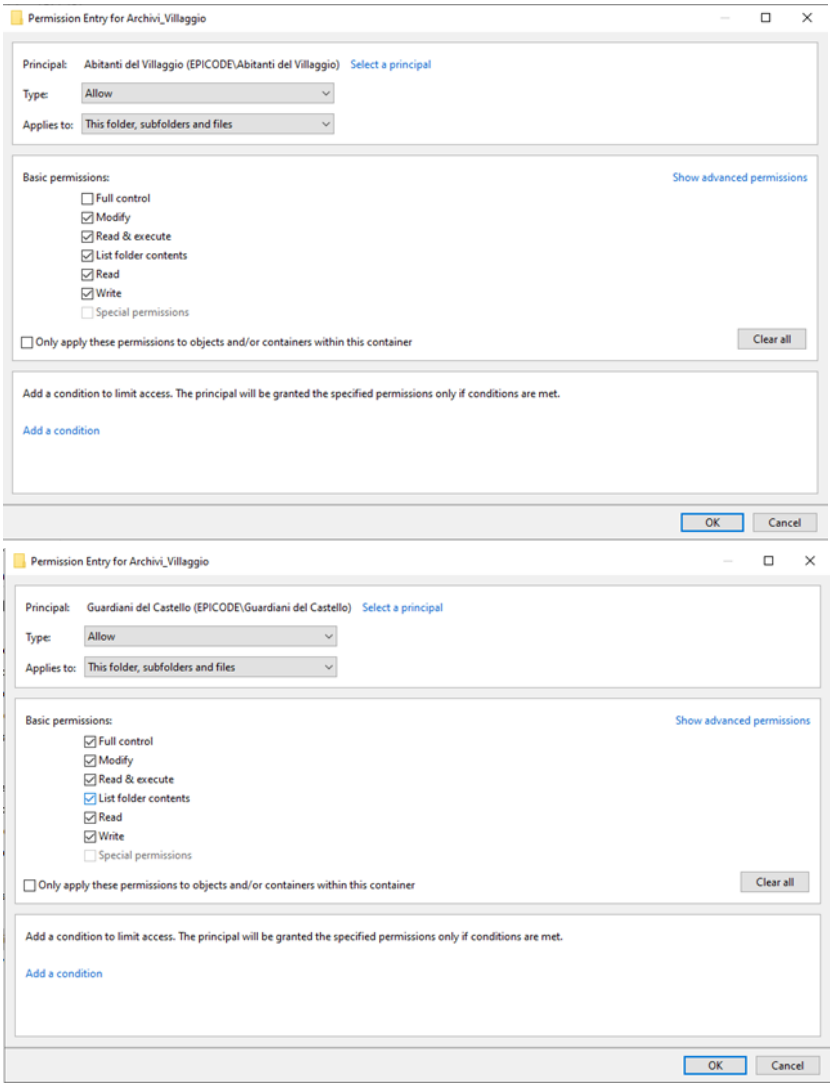


- **C:\Archivi_Villaggio** (Cartella di Lavoro Standard)
  - **Funzione:** Contiene dati operativi quotidiani, accessibili a tutti gli abitanti.
  - **Gruppi Assegnati:** `Guardiani del Castello` e `Abitanti del Villaggio`
  - Permesso NTFS:
    - `Guardiani del Castello`: **Controllo Completo** (Per l'amministrazione).
    - `Abitanti del Villaggio`: **Modifica** (Modify), **Lettura**, **Scrittura**, **Listing**, **Lettura** ed **Esecuzione**.

La scelta delle assegnazioni

L'assegnazione del **Controllo Completo** ai **Guardiani del Castello** (la Reggenza) sulla cartella `Archivi_Villaggio` è vitale per mantenere la **Catena di Comando**. Nonostante questa cartella sia il luogo di lavoro principale degli **Abitanti del Villaggio**, i Guardiani devono sempre conservare il diritto di **supervisione totale**. Questo assicura che possano intervenire in qualsiasi momento per compiti amministrativi essenziali, come:

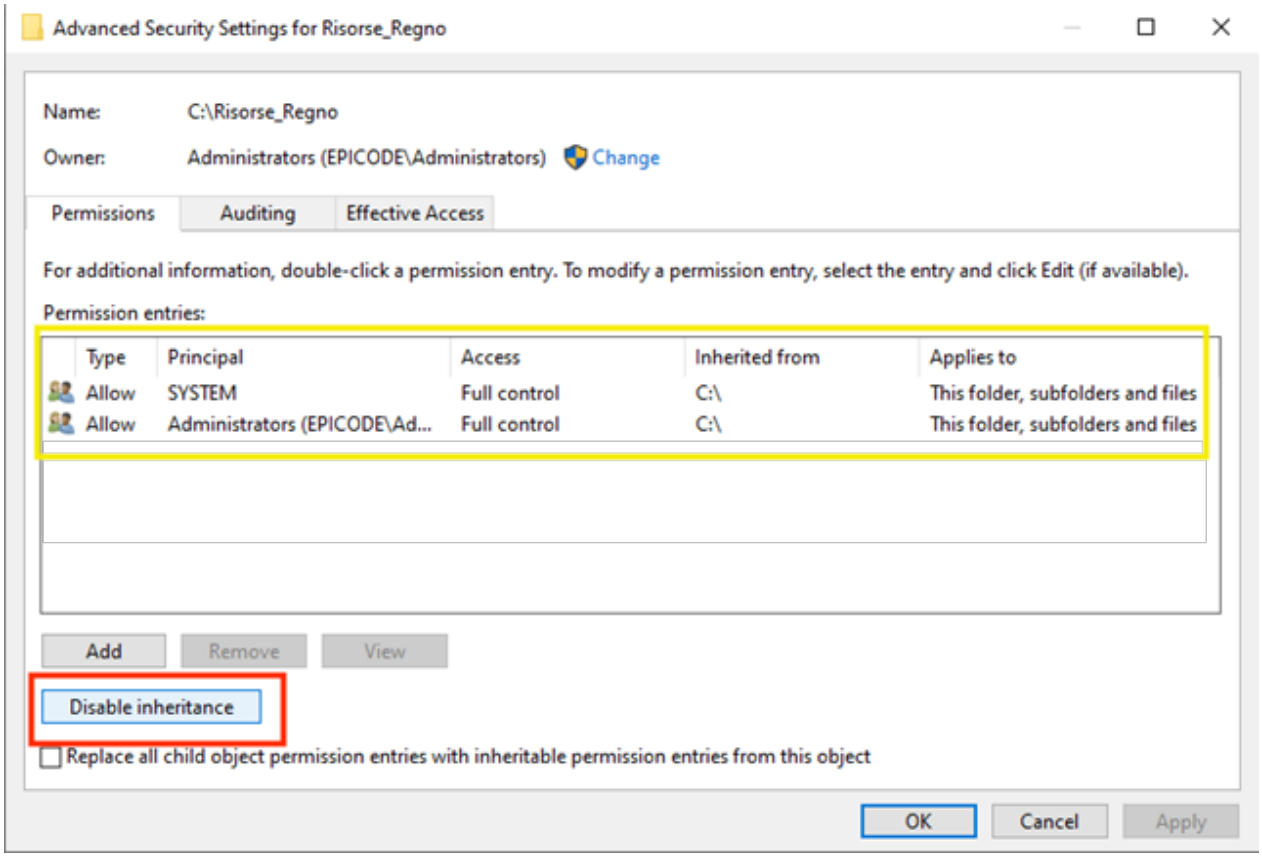
1. **Auditing e Revisione** dei registri.
2. **Risoluzione di Conflitti** (ad esempio, se un abitante blocca un file di un altro).
3. **Manutenzione d'Emergenza** (backup, ripristino o modifica diretta in caso di crisi). Senza questo Controllo Completo, l'amministrazione del Regno perderebbe la sua autorità sulla risorsa.



Nelle figure di sopra vediamo appunto che i `Guardiani del Castello` hanno `Full control` sulla cartella `Archivi_Villaggio`, mentre gli `Abitanti del Villaggio` hanno tutti gli altri accessi tranne `Full control`.

2. **Implementazione Tecnica**

   Dopo aver creato e condiviso le cartelle, per entrambe le risorse ho **disabilitato l'ereditarietà** e rimosso i permessi generici (`Users`, `CREATOR OWNER`). Questo passo è cruciale per la **sicurezza**, in quanto garantisce che solo i gruppi **esplicitamente definiti** controllino l'accesso.



---

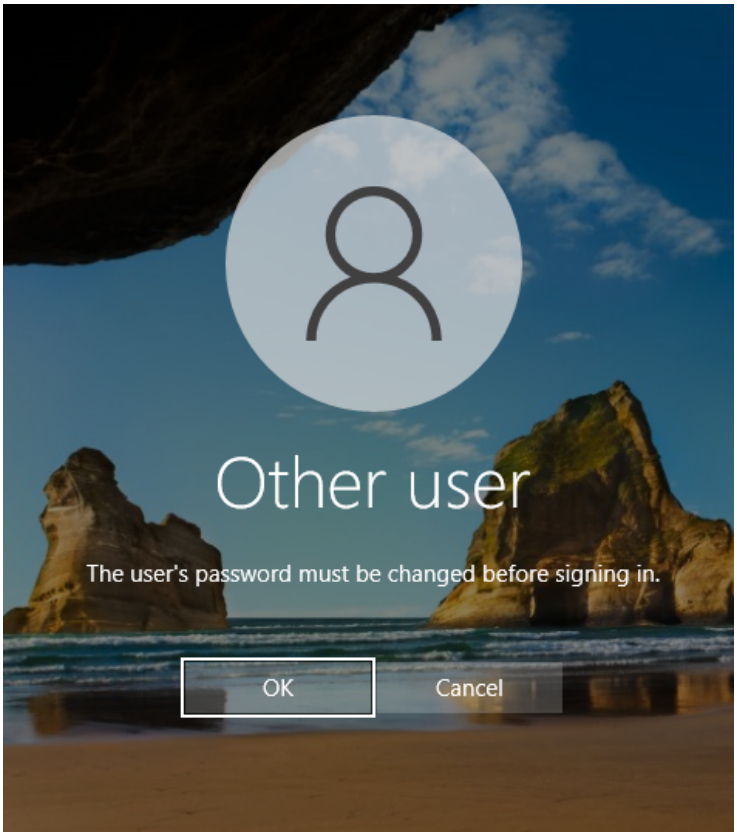
4. Verifica Remota e Risultati del Test

I test sono stati eseguiti accedendo da una **macchina client remota** e utilizzando i percorsi di rete (`\\EPICODESERVER\Nome_Cartella_Shared`), che è il metodo più realistico per **simulare** l'accesso di un utente di dominio alle risorse.

Login con Utenti creati con Administrator

Una volta implementata l'architettura degli utenti, gruppi e relativi permessi, iniziamo a loggarci con un utente alla volta, uno per ogni gruppo.

Prendendo il caso dell'utente **Robin Hood**, in fase di creazione dell'utente, è stato deciso di impostare una password **provvisoria**, da cambiare al primo **login**.
Di conseguenza, una volta immessa la password provvisoria, il sistema chiede di impostarne una **nuova**, proprio come volevamo:



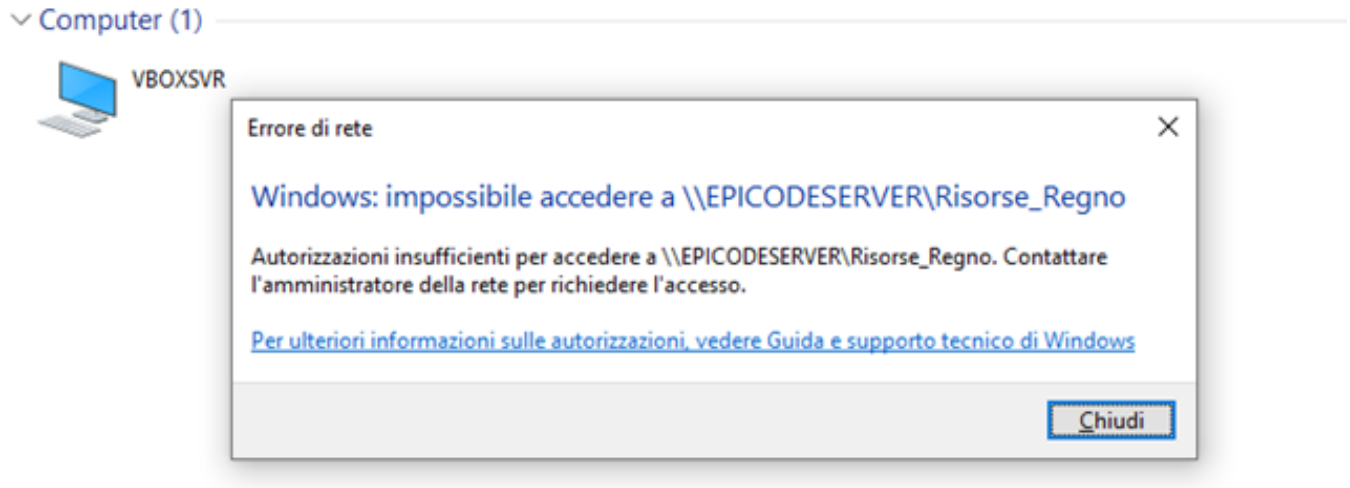
Immettiamo una password nuova e accediamo.

> **Nota Bene**
> Questa configurazione non è stata effettuata per tutti gli utenti, ma solo per alcuni. Quello che bisogna fare è semplicemente tentare di esegure il login con la password provvisoria in possesso e vedere se il sistema, in automatico, richieda l'immissione di una nuova password.

Test sulla Cartella Sensibile (`Risorse_Regno`)

Utente di Test	Accesso alla Cartella	Tentativo di Modifica	Risultato Verificato
Robin Hood (Abitante)	Accesso Negato	N/A	Corretto (Il Principio del Privilegio Minimo è applicato: non può accedere ai dati non necessari).

Re Artù (Guardiano)	Accesso Consentito	Consentito	Corretto (L'utente amministrativo ha il Controllo Completo sulla risorsa).

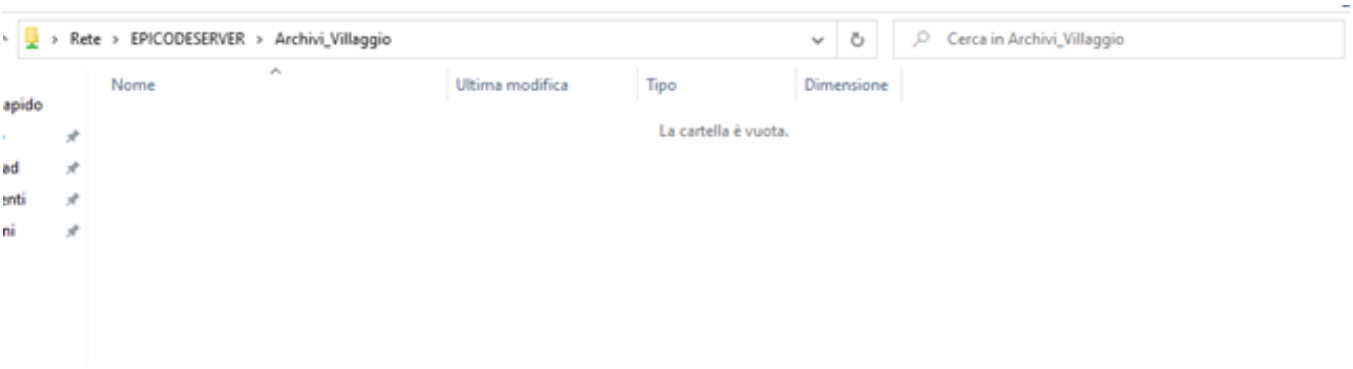


Nell'immagine soprastante, possiamo vedere il tentativo correttamente fallito di accesso alla cartella `Risorse_Regn`o per l'utente Robin Hood.

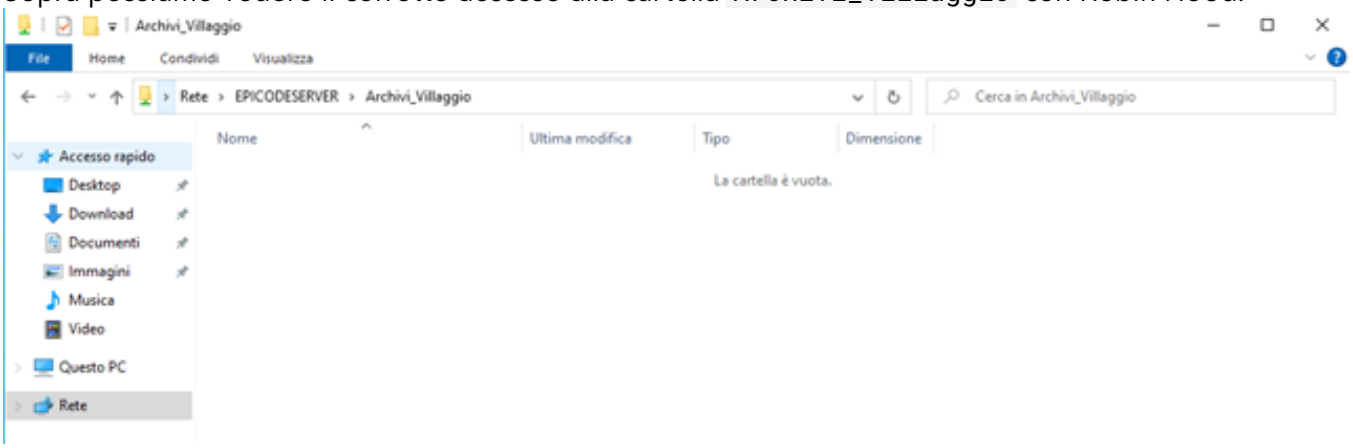
In ques'altra immagine possiamo vedere, invece, la corretta visualizzazione della cartella `Risorse_Regno` con l'utente Re Artù.

Test sulla Cartella Standard (`Archivi_Villaggio`)

Utente di Test	Accesso alla Cartella	Tentativo di Creazione/ Modifica	Tentativo di Amministrazione (Cambiare Permessi)
Robin Hood (Abitante)	Accesso Consentito	Consentito	Negato
Re Artù (Guardiano)	Accesso Consentito	Consentito	Consentito



Sopra possiamo vedere il corretto accesso alla cartella `Archivi_Villaggio` con Robin Hood.



Ques'ultima immagine, mostra l'accesso e la visualizzazione dei contenuti della cartella `Archivi_Villaggio` anche con Re Artù.

Conclusione

Questo progetto ha pienamente raggiunto l'obiettivo di applicare la gestione dei gruppi per definire i privilegi in un ambiente **Windows Server 2022**. La creazione di gruppi di sicurezza (Guardiani del Castello vs. Abitanti del Villaggio) e l'attenta configurazione delle autorizzazioni NTFS hanno dimostrato l'efficacia del **Controllo degli Accessi Basato sui Ruoli (RBAC - Role-Based Access**

Control).

In ottica di Cyber Security, la strategia adottata assicura che un utente compromesso o un attacco informatico che sfrutti le credenziali di un utente standard (Abitanti del Villaggio) non possa in alcun modo accedere o danneggiare i dati sensibili custoditi nella cartella `Risorse_Regno`. Questo limita il potenziale danno (o la "superficie d'attacco") e protegge l'integrità del sistema.

Prossimi Passi

La gestione dei gruppi non è un'attività una tantum, ma un processo continuo di governance. Per mantenere un ambiente sicuro ed efficiente nel tempo, è fondamentale istituire una policy formale di **Identity and Access Management** (IAM) che includa:

- **Revisioni Periodiche Programmate:** Stabilire un ciclo di revisione trimestrale o semestrale per riesaminare le appartenenze ai gruppi e la validità dei permessi assegnati, certificando che siano ancora allineati ai ruoli aziendali correnti.
- **Revisioni Attivate da Eventi (Event-Driven):** Eseguire una revisione ad-hoc dei permessi di un utente o di un gruppo in risposta a eventi specifici, quali:
  - Cambiamento di ruolo o mansione di un dipendente.
  - Implementazione di una nuova applicazione critica.
  - Rilevamento di un incidente di sicurezza.
  - Terminazione del rapporto di lavoro (offboarding).

Questo approccio proattivo assicura che le configurazioni rimangano costantemente allineate alle esigenze organizzative e ai principi di sicurezza più stringenti.