

**WINDOWS SERVER*****Indice:***

<i>Configurazione server</i>	<b>2</b>
<i>Creazione foresta</i>	<b>3</b>
<i>Creazione gruppi e utenti</i>	<b>4 - 8</b>
<i>Creazione permessi per ruoli e gruppi</i>	<b>9 - 11</b>
<i>Configurazione rete windows</i>	<b>10 - 12</b>
<i>Verifica permessi</i>	<b>13 - 16</b>
<i>Conclusioni</i>	<b>17</b>

## CONFIGURAZIONE WINDOWS SERVER 2022

Nella simulazione di oggi andremo a creare e gestire gruppi di utenti e permessi su Windows Server 2022.

Per prima cosa andiamo a configurare correttamente la rete e il dns, quindi ci rechiamo su Server Manager, Aggiungi ruoli e funzionalità e seguiamo i passaggi dell'installazione guidata fino alla fine, prestando attenzione ad inserire il Ruolo - SERVER DNS e Servizi di Dominio Active Directory.

```
C:\Users\vboxuser>ipconfig /all

Configurazione IP di Windows

Nome host . . . . . : win-server-22
Suffisso DNS primario . . . . . : epicode.local
Tipo nodo . . . . . : Ibrido
Routing IP abilitato. . . . . : No
Proxy WINS abilitato . . . . . : No
Elenco di ricerca suffissi DNS. . . . : epicode.local

Scheda Ethernet Ethernet:

Suffisso DNS specifico per connessione:
Descrizione . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Indirizzo fisico. . . . . : 08-00-27-28-A6-0A
DHCP abilitato. . . . . : No
Configurazione automatica abilitata . . : Sì
Indirizzo IPv6 locale rispetto al collegamento . : fe80::4591:d4cd:39cc:5a46%6(Preferenziale)
Indirizzo IPv4. . . . . : 192.168.1.191(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 101187623
DUID Client DHCPv6. . . . . : 00-01-00-01-2E-E4-70-61-08-00-27-28-A6-0A
Server DNS . . . . . : 192.168.1.191
NetBIOS su TCP/IP . . . . . : Attivato
```

### Selezione ruoli server

SERVER DI DESTINAZIONE  
win-server-22.epicode.local

Operazioni preliminari  
Tipo di installazione  
Selezione dei server  
**Ruoli server**  
Funzionalità  
Conferma  
Risultati

Selezionare uno o più ruoli da installare nel server selezionato.

#### Ruoli

- ☐ Accesso remoto
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ ADFS (Active Directory Federation Services)
- ☐ Attestazione dell'integrità del dispositivo
- ☐ Hyper-V
- ☐ Server DHCP
- ☒ Server DNS (Installato)
- ☐ Server fax
- ☐ Server Web (IIS)
- ☐ Servizi certificati Active Directory
- ☐ Servizi Desktop remoto
- ☐ Servizi di accesso e criteri di rete
- ☐ Servizi di attivazione contratti multilicenza
- ☒ Servizi di dominio Active Directory (Installato)
- ☐ Servizi di stampa e digitalizzazione
- ☒ Servizi file e archiviazione (2 di 12 installato/i)
- ☐ Servizio Sorveglianza host
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

#### Descrizione

Accesso remoto assicura una connettività semplice tramite DirectAccess, VPN e il proxy dell'applicazione Web. DirectAccess offre un'esperienza sempre attiva e gestita. RAS offre servizi VPN tradizionali tra cui connettività da sito a sito (a livello di filiale o basata sul cloud). Il proxy dell'applicazione Web consente la pubblicazione di applicazioni selezionate basate su HTTP e HTTPS nella rete aziendale nei dispositivi client all'esterno della rete aziendale. Il routing include funzionalità tradizionali tra cui NAT e altre opzioni di connettività. Accesso remoto e il routing possono essere distribuiti in un singolo tenant o in modalità multi-tenant.

< Precedente

Avanti >

Installa

Annulla

## CONFIGURAZIONE FORESTA

Ora che abbiamo installato i ruoli del server possiamo procedere a creare la foresta, ovvero il livello di organizzazione più alto in Active Directory che ci gestirà i domini, risorse di rete e utenti in modo centralizzato.

Clicchiamo sulla notifica per poter promuovere il server a controller di dominio e aggiungiamo una nuova foresta e procediamo con l'installazione guidata, in questo caso come nome dominio inseriremo **epicode.local**

Dopo aver configurato tutte le impostazioni di Active Directory in automatico verranno eseguite delle verifiche, al loro completamento se tutto è stato settato correttamente si avvierà la promozione del server e al suo termine si riavvierà.

Configurazione guidata Servizi di dominio Active Directory

SERVER DESTINAZIONE  
win-server-22

### Configurazione distribuzione

Configurazione distribuzi...

- Opzioni controller di dom...
- Opzioni aggiuntive
- Percorsi
- Verifica opzioni
- Controllo dei prerequisiti
- Installazione
- Risultati

Selezionare l'operazione di distribuzione

- ☐ Aggiungi un controller di dominio a un dominio esistente
- ☐ Aggiungi un nuovo dominio a una foresta esistente
- ☒ Aggiungi una nuova foresta

Specificare le informazioni di dominio per questa operazione

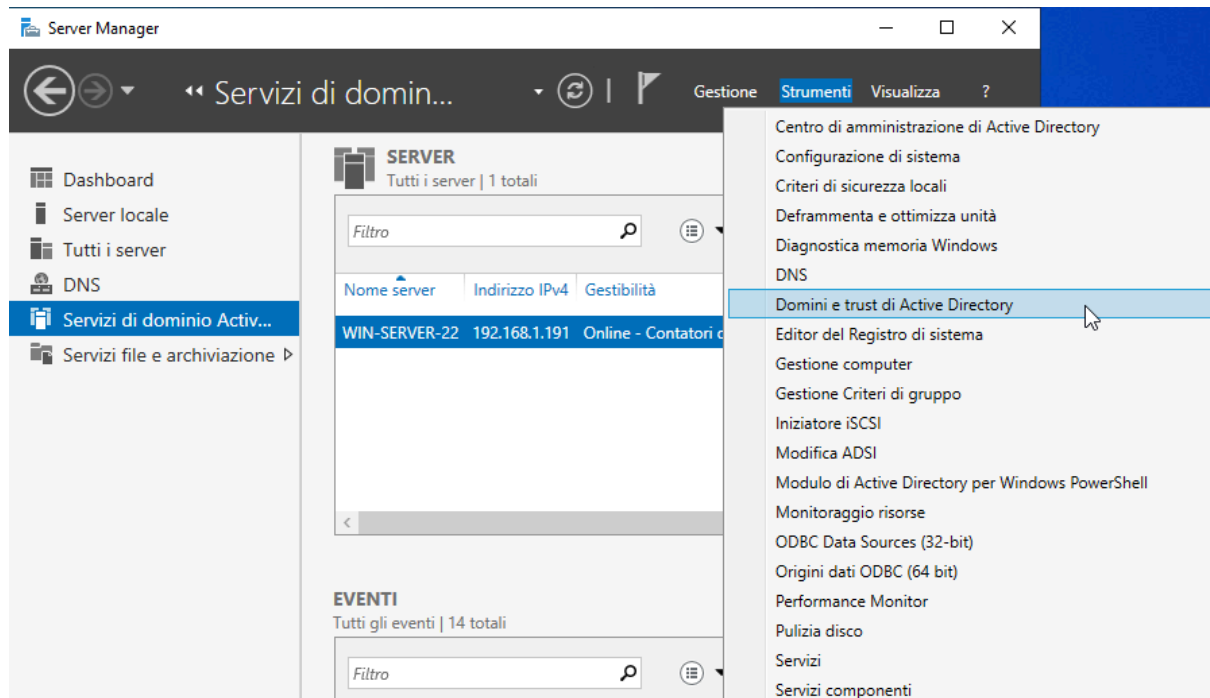
Nome dominio radice:

Informazioni sulle configurazioni di distribuzione

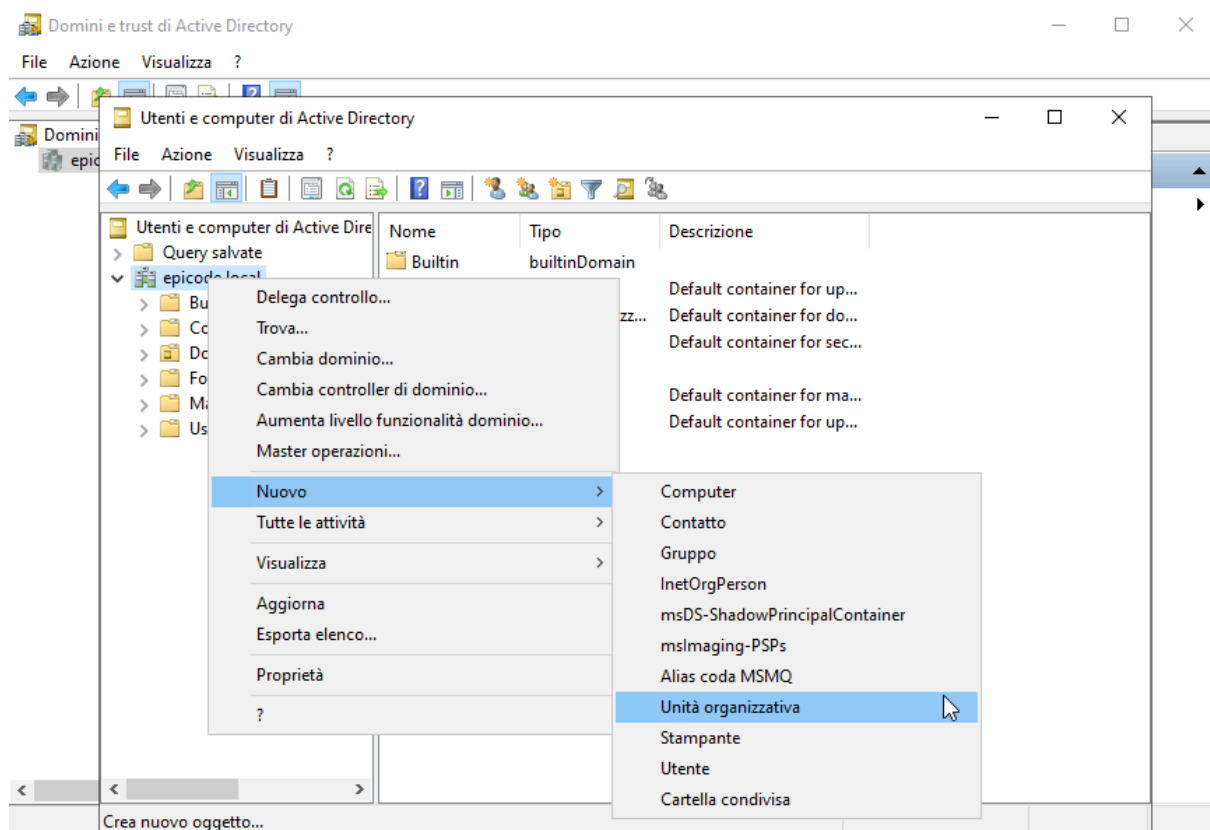
< Precedente Avanti > Installa Annulla

## CREAZIONE GRUPPI E UTENTI

Procediamo ora alla creazione di Unità Organizzative, Gruppi e Utenti, per farlo ci rechiamo nel menù in alto su strumenti, Domini e Trust di Active Directory.




Ci si aprirà la finestra Utenti e computer di Active Directory e possiamo procedere con la creazione delle **unità organizzative**, nel nostro caso **Amministrazione e IT**



Una volta create le unità organizzative possiamo procedere con la creazione degli utenti, ci rechiamo all'interno di **Amministrazione** e aggiungiamo i **nuovi utenti: Marco Lino, Paolo Veneto, Stefania Rossi**. Per ogni utente impostiamo la stessa password accertandosi che sia presente il flag su "Cambiamento obbligatorio password all'accesso successivo" permettendo così all'utente di poter impostare la propria password al suo primo accesso. Procediamo allo stesso modo anche per l'**unità organizzativa IT**.

Nuovo oggetto Utente ✕

 Crea in: epicode.local/Amministrazione

---

Nome:  Iniziali:

Cognome:


Nome completo:

Nome accesso utente:

Nome accesso utente (precedente a Windows 2000):

---

Nuovo oggetto Utente ✕

 Crea in: epicode.local/Amministrazione

---

Password:

Confirma password:

☒ Cambiamento obbligatorio password all'accesso successivo

☐ Cambiamento password non consentito

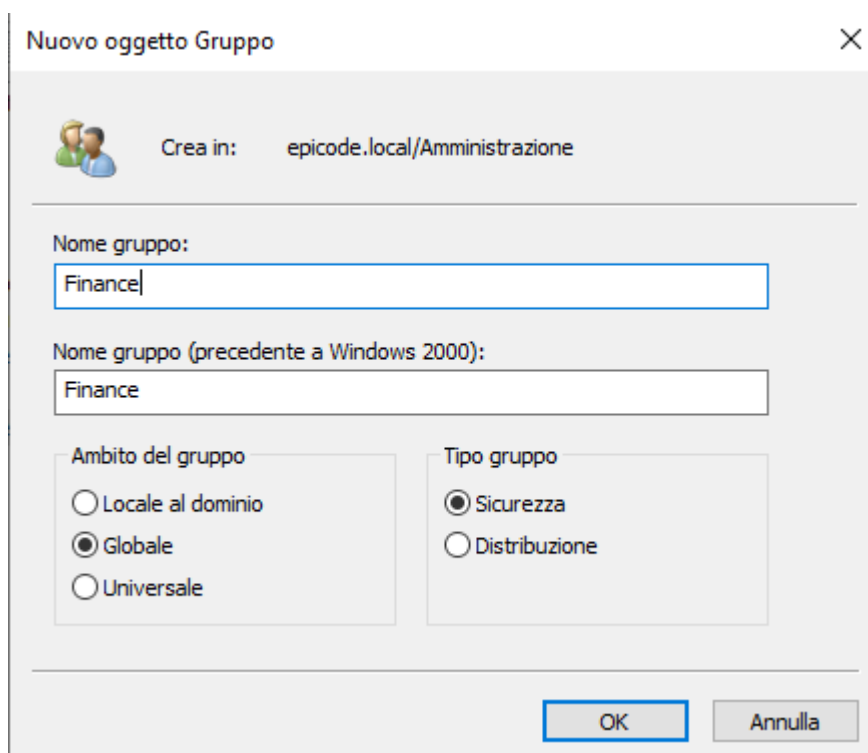
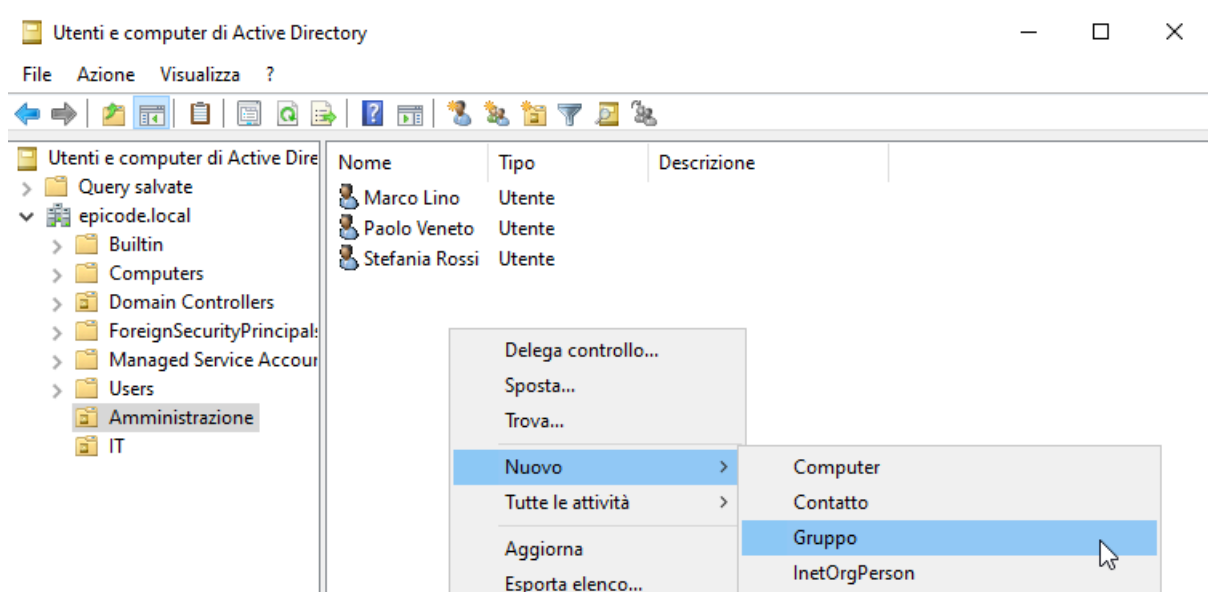
☐ Nessuna scadenza password

☐ Account disabilitato

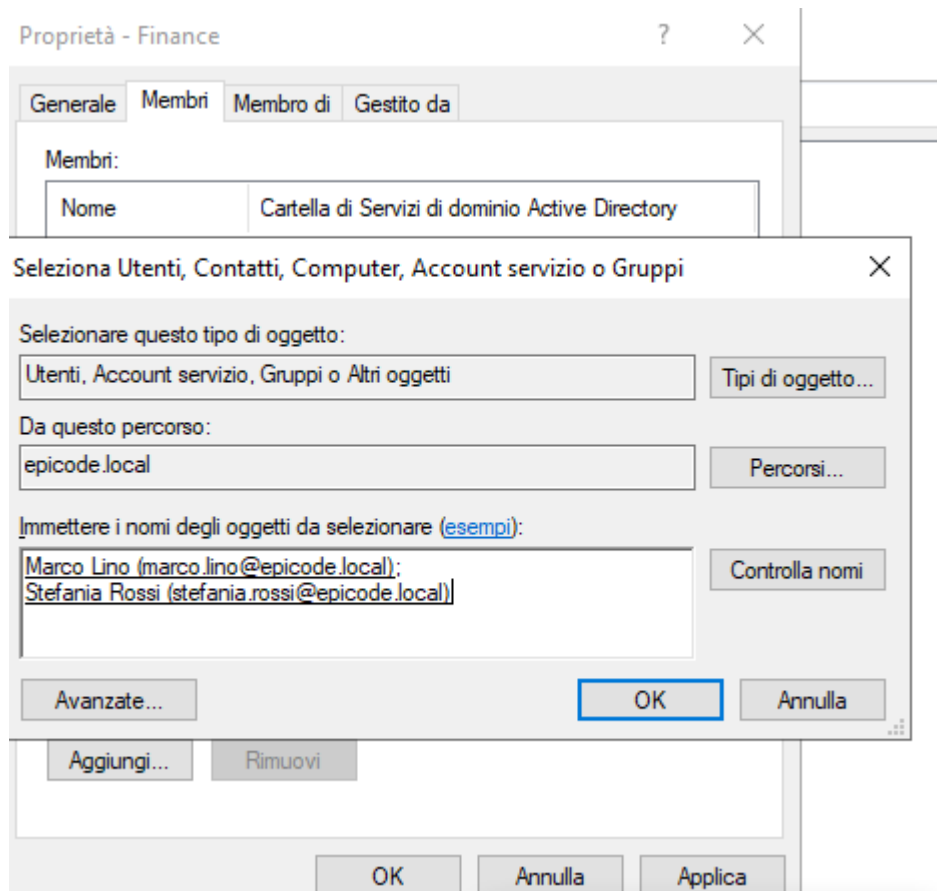
---

Ora che abbiamo inserito i nuovi utenti procediamo con la creazione dei gruppi, in questo caso abbiamo previsto due gruppi per unità organizzativa, ipotizzando che il Reparto **Amministrazione** abbiamo due uffici: **Finance e Tesoreria**, mentre **IT: Security e Support**, al loro interno assegneremo poi i relativi utenti.

Tasto destro su Amministrazione, nuovo e gruppo e seguiamo i passaggi come descritti dalle seguenti immagini, procediamo allo stesso modo per l'unità organizzativa IT.



Ora che abbiamo creato il gruppo possiamo procedere ad inserire i membri al suo interno.



Nel nostro caso abbiamo suddiviso come di seguito l'organizzazione:

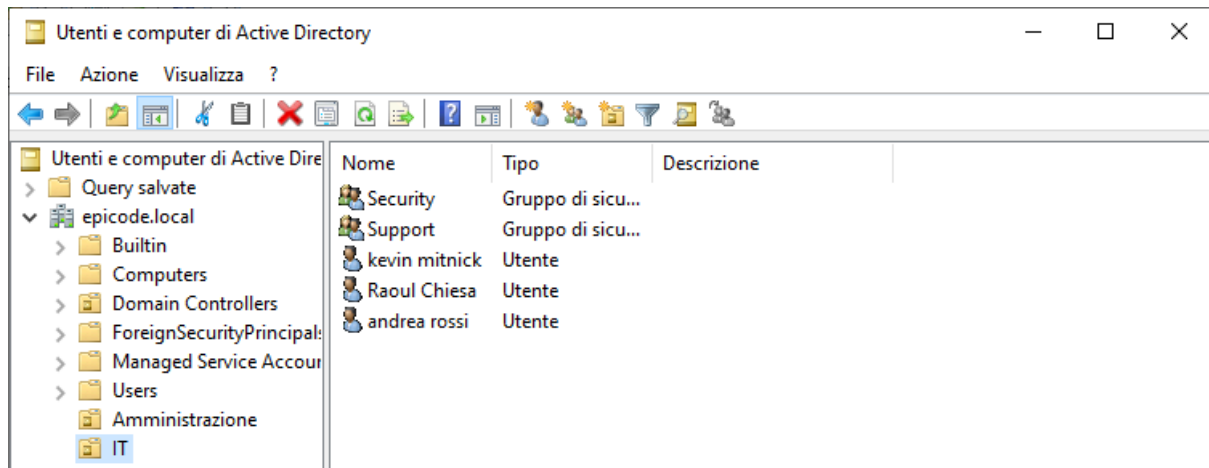
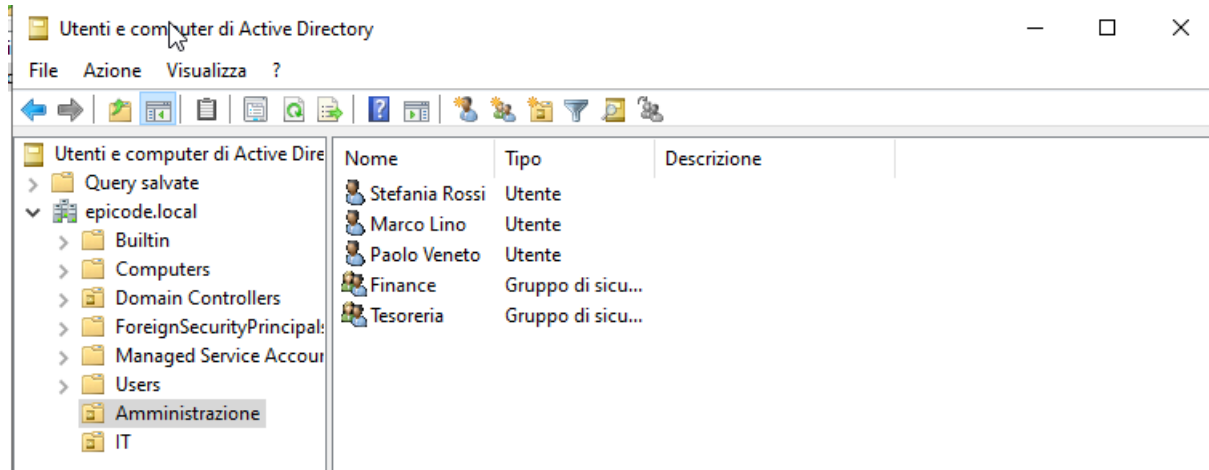
**Amministrazione:**

- Finance (gruppo):
  - Marco Lino (utente)
  - Stefania Rossi (utente)
- Tesoreria (gruppo):
  - Paolo Veneto (utente)

**IT:**

- Security (gruppo):
  - Kevin Mitnick (utente)
  - Raoul Chiesa (utente)
- Support (gruppo):
  - Andrea Rossi (utente)

Una volta impostato tutto correttamente avremo la situazione seguente:





## CREAZIONE PERMESSI PER RUOLI E GRUPPI

Ora andremo a impostare i permessi di accesso a file e risorse per i singoli utenti e gruppi.

All'interno della cartella Public abbiamo due directory: Procedure IT e Contabilità.

### Procedure IT contiene:

- Log di Sistema (directory)
  - LOG.txt
- Ticket Support (directory)
  - ticket1234.txt
- Formazione Phishing.txt
- Policy IT

### Contabilità contiene:

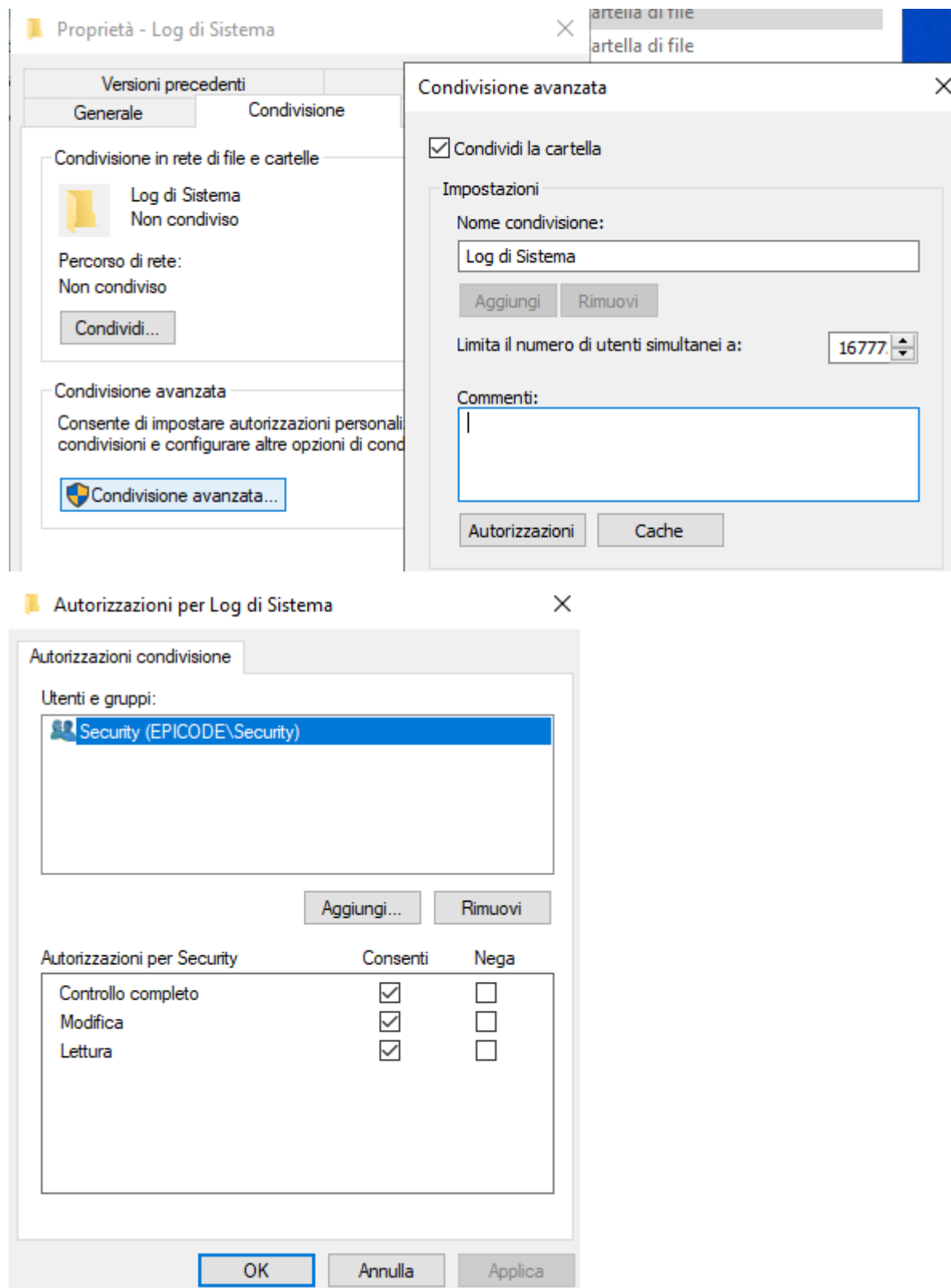
- Bilanci (directory)
- Generale (directory)
- Procedure inserimento fatture estere.txt

Di seguito una tabella riassuntiva dei permessi che verranno assegnati alle directory e file

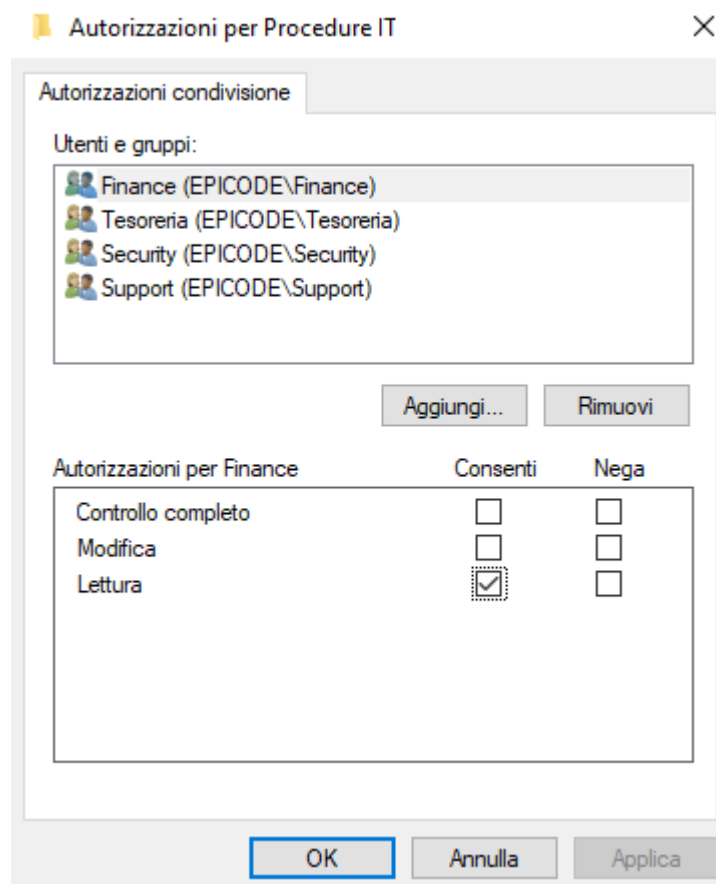
Directory/File	Gruppo	Permessi
Log di Sistema	Security	Controllo completo
Ticket Support	Support	Controllo completo
Formazione Phishing.txt	Finance Tesoreria	Sola lettura
	Security	Controllo completo
	Support	Sola lettura
Policy IT.txt	Security Support	Controllo completo Sola lettura
Bilanci	Finance	Controllo completo
Generale	Finance Tesoreria	Sola lettura Controllo completo
Procedure inserimento....txt	Finance Tesoreria	Controllo completo Sola lettura

Ora che abbiamo un quadro generale dei permessi da attribuire procediamo con la creazione degli stessi.

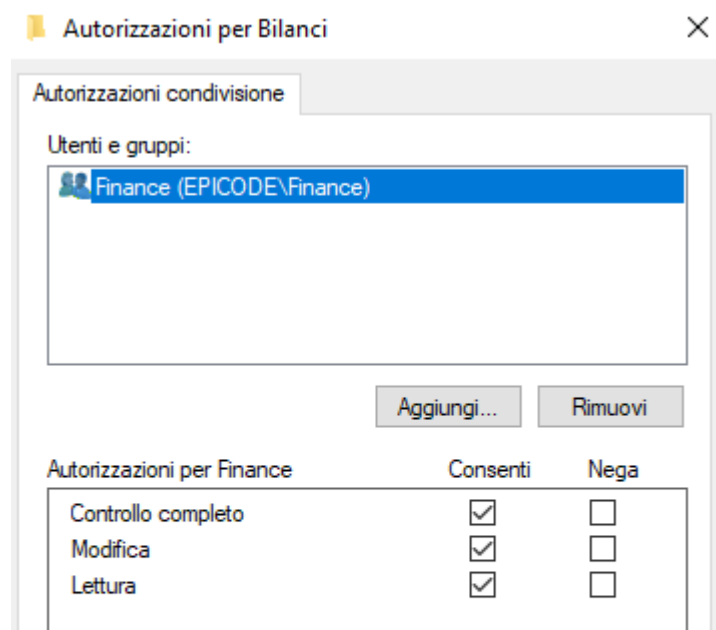
Ci rechiamo sulle cartelle, tasto destro, proprietà e configuriamo le schede Condivisione e Sicurezza come nelle immagini seguenti che ritraggono i permessi della cartella Log di Sistema.



Nel nostro caso dato che i gruppi Finance e Tesoreria devono poter leggere il file Formazione Phishing, dobbiamo dargli ovviamente i permessi per poter accedere alla cartella Procedure IT e di conseguenza leggere il file.



Di seguito invece l'esempio delle autorizzazioni della cartella Bilanci.



## CONFIGURAZIONE RETE WINDOWS 10

Ora che abbiamo correttamente configurato tutto, procediamo alla configurazione della macchina Windows 10.

Per prima cosa configuriamo anche qui l'indirizzo IP STATICO e impostiamo l'IP DNS uguale all'indirizzo IP del nostro server Windows (192.168.1.191).

Dopodichè ci rechiamo su DOMINI e configuriamo il dominio EPICODE.LOCAL inseriamo il nome utente kevin.mitnick e clicchiamo su ignora

Aggiungi un account



### Aggiungi un account

Immetti le info dell'account per la persona che userà questo PC. Se ignori questo passaggio, alla persona verranno assegnate le autorizzazioni predefinite per il dominio.

Account utente

kevin.mitnick

Tipo di account

Utente standard

Successivo

Ignora

## VERIFICA PERMESSI

A questo punto possiamo fare l'accesso alla nostra macchina sul dominio EPICODE.

Al primo accesso con l'utente kevin.mitnick ci verrà chiesto di reimpostare la password come da configurazione iniziale.

Una volta dentro ci rechiamo alle cartelle condivise per verificare che i permessi impostati siano corretti, faremo lo stesso test anche con l'utente Paolo Veneto.

Premiamo win+R e verifichiamo come detto precedentemente le impostazioni di rete

```
C:\Users\kevin.mitnick>ipconfig /all

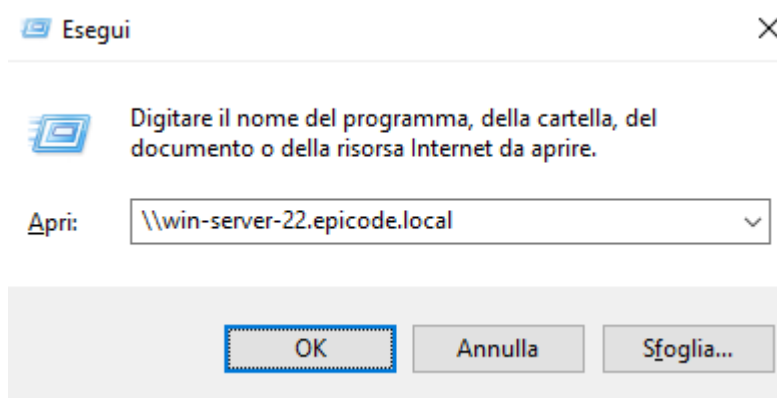
Configurazione IP di Windows

Nome host . . . . . : DESKTOP-BUDM672
Suffisso DNS primario . . . . . : epicode.local
Tipo nodo . . . . . : Ibrido
Routing IP abilitato. . . . . : No
Proxy WINS abilitato . . . . . : No
Elenco di ricerca suffissi DNS. . . . : epicode.local

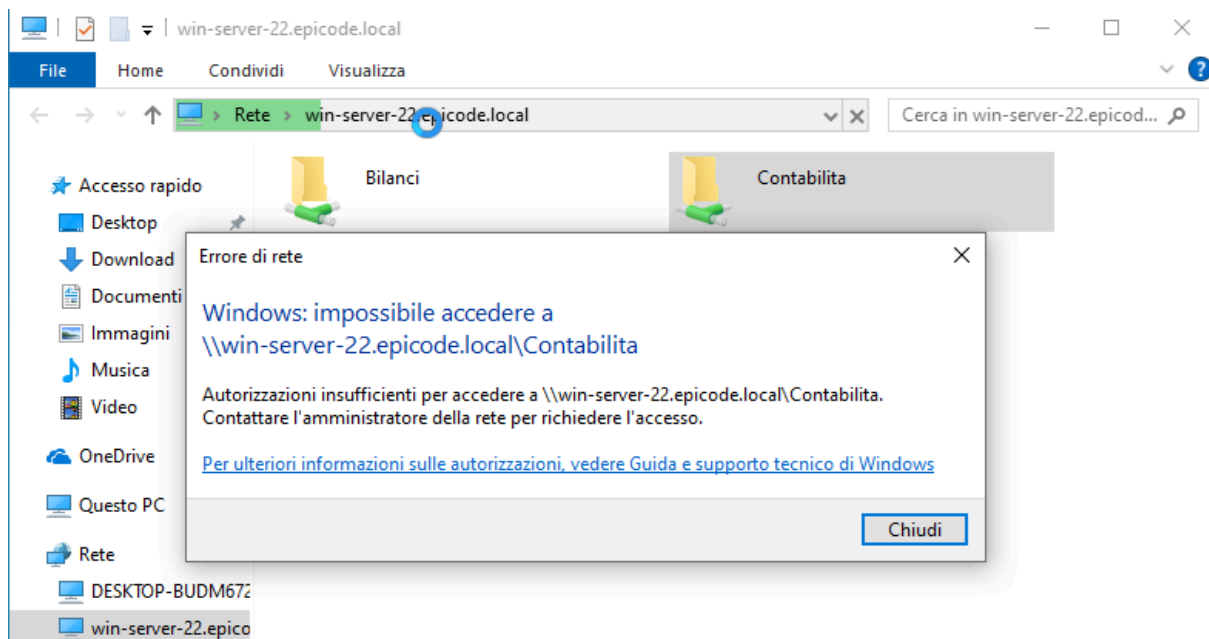
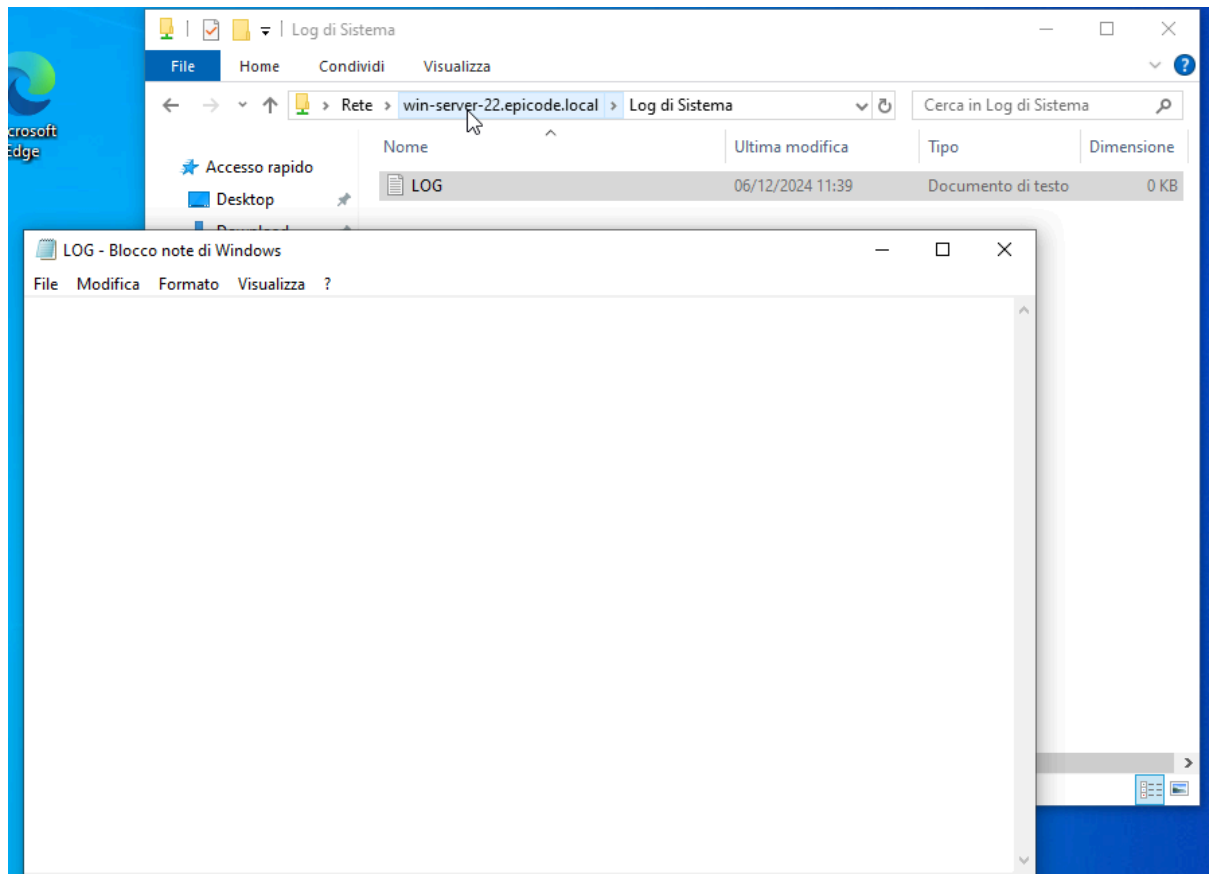
Scheda Ethernet Ethernet:

Suffisso DNS specifico per connessione:
Descrizione . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Indirizzo fisico. . . . . : 08-00-27-F4-F4-37
DHCP abilitato. . . . . : No
Configurazione automatica abilitata : Sì
Indirizzo IPv4. . . . . : 192.168.1.7(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1
Server DNS . . . . . : 192.168.1.191
NetBIOS su TCP/IP . . . . . : Attivato
```

ora premiamo nuovamente win+R e inseriamo il percorso del nostro server come da immagine seguente:



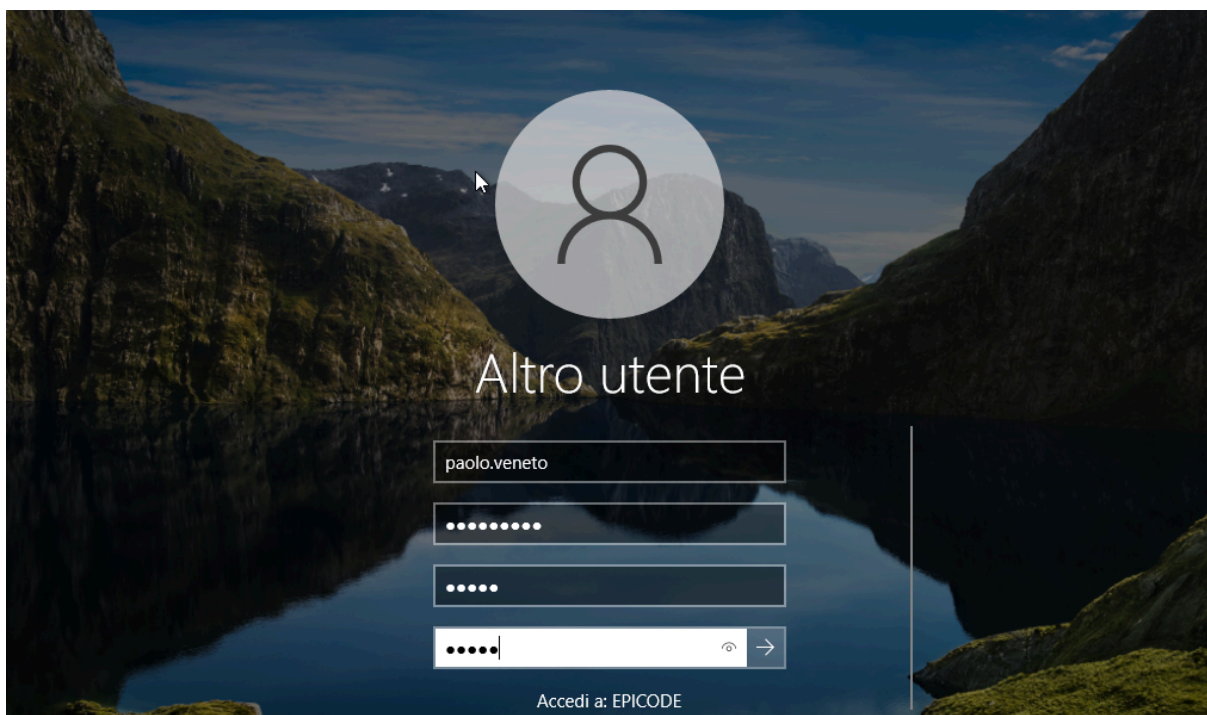
ci aprirà le directory presenti sul nostro server, per verificare bene che i permessi siano impostati correttamente proveremo ad entrare con l'utente Kevin nella cartella Contabilità e in Procedure IT- Log di Sistema e LOG.

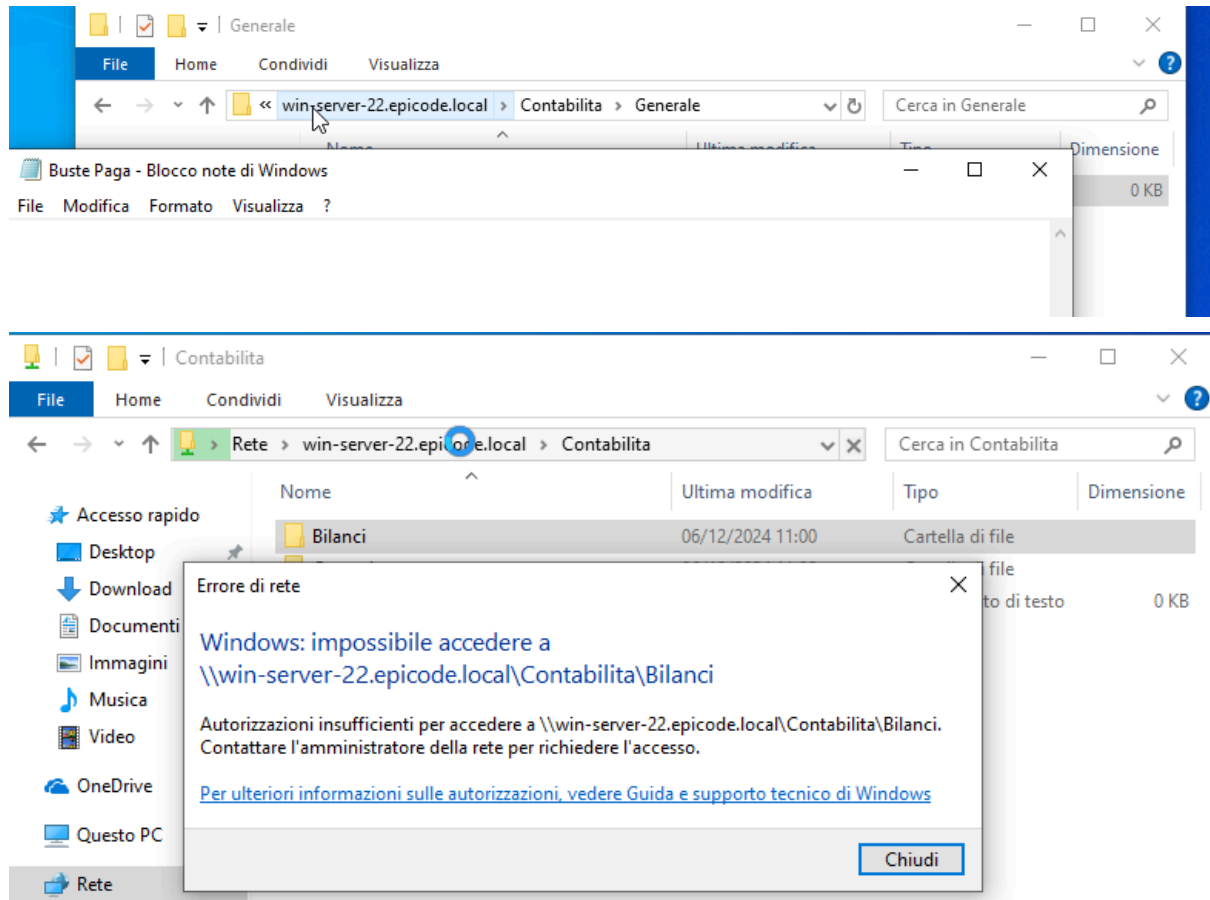


Come possiamo vedere l'accesso al file LOG.txt ci verrà consentito mentre l'accesso alla directory contabilità no.

Procediamo allo stesso modo con l'utente PAOLO VENETO appartenente al gruppo Tesoreria

Di seguito i passaggi:







## CONCLUSIONI

Possiamo affermare con estrema certezza che una corretta gestione degli utenti, gruppi e relativi permessi in Active Directory è di fondamentale importanza per un'azienda, questo ci assicura una gestione centralizzata che renderà le risorse sicure, accessibili e scalabili.

Organizzare gli utenti in gruppi ci semplifica l'assegnazione dei permessi e soprattutto ci riduce gli errori.

Nel nostro caso l'utilizzo delle Unità Organizzative ci ha aiutato a strutturare e configurare l'ambiente seguendo una logica dei dipartimenti aziendali.

Una gestione precisa e accurata ci garantisce il controllo degli accessi riducendo il rischio di violazioni di sicurezza e assicurando la conformità a normative europee come il GDPR.

Per concludere una configurazione e gestione corretta di AD, migliora l'efficienza e soprattutto è una vera e propria "garanzia" di sicurezza e integrità aziendale. L'investimento nella progettazione e implementazione di un Active Directory solida e ben fatta è la chiave per poter proteggere i dati, le risorse e l'intera infrastruttura aziendale da minacce esterne ed interne.