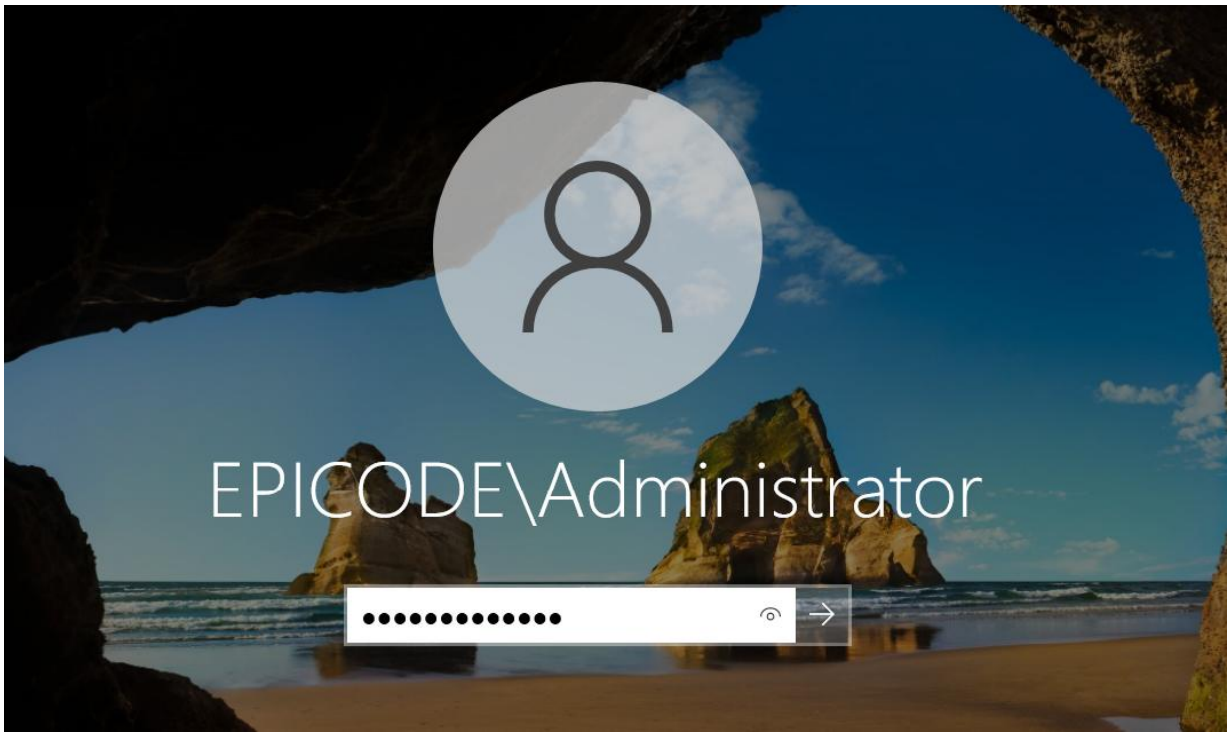
PROGETTO S10

Lo scopo dell' 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.

1. ***Preparazione***:
    a. Accedi al tuo ambiente Windows Server 2022.
    b. Assicurati di avere i permessi amministrativi necessari per creare e gestire gruppi.
2. ***Creazione dei gruppi***:
    a. Crea due gruppi distinti. Puoi scegliere i nomi che preferisci per questi gruppi, ma assicurati che i nomi siano significativi per riflettere la loro funzione o ruolo all'interno dell'organizzazione (ad esempio, "Amministratori", "UtentiStandard", "MarketingTeam", "Sviluppatori", ecc.).
3. ***Assegnazione dei permessi***:
    a. Accesso ai file e alle cartelle.
    b. Esecuzione di programmi specifici.
    c. Modifiche alle impostazioni di sistema.
    d. Accesso remoto al server.
4. ***Verifica***:
    a. Una volta creati i gruppi e assegnati i permessi verifica che le impostazioni siano corrette.
5. ***Documentazione, scrivi un breve report, che includa***:
    a. I nomi dei gruppi creati.
    b. I permessi assegnati a ciascun gruppo.
    c. I passaggi seguiti per creare e configurare i gruppi.
    d. Eventuali problemi riscontrati.

SVOLGIMENTO

Procedo effettuando l' accesso alla mia macchina ***Windows Server 2022*** come amministratore, e vado a creare due gruppi, il primo gruppo "***Amministratori***" e il secondo "***TeamSviluppo***".



Una volta effettuato l' accesso mi trovo nella console di gestione ***Server Manager***, procedo quindi facendo click in alto a destra su ***Tools → Active directory Users and Computers***. ***Figura 1***

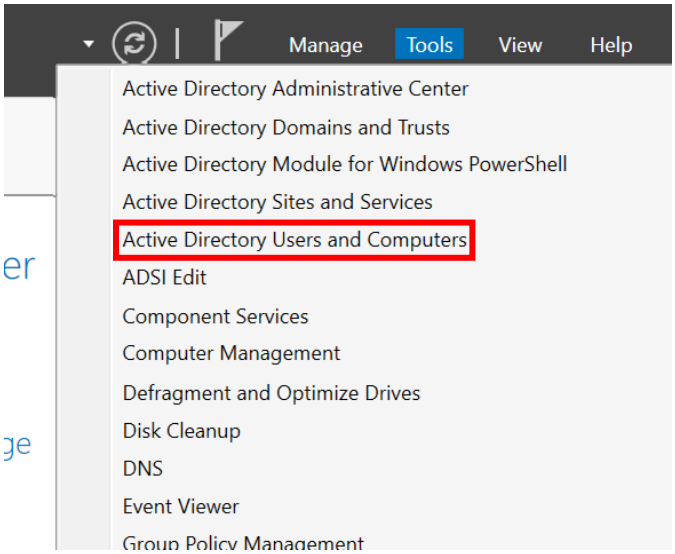


Figura 1.

Prima di iniziare con la creazione dei gruppi andrò a creare una nuova ***Organizational Unit*** chiamata ***Progetto***, all' interno della quale andrò a creare e gestire i due gruppi.

A questo punto facendo click destro su "***Progetto***" seguo con ***New → Group***. ***Figura 2***

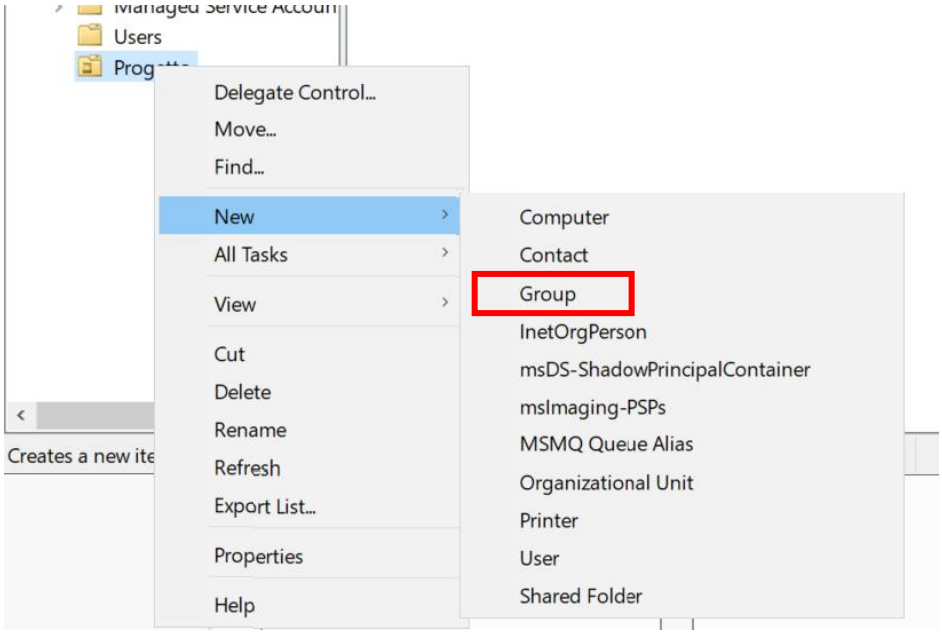


Figura 2, passi per la creazione di un gruppo.

Creo quindi il gruppo "Amministrazione" e do Ok.

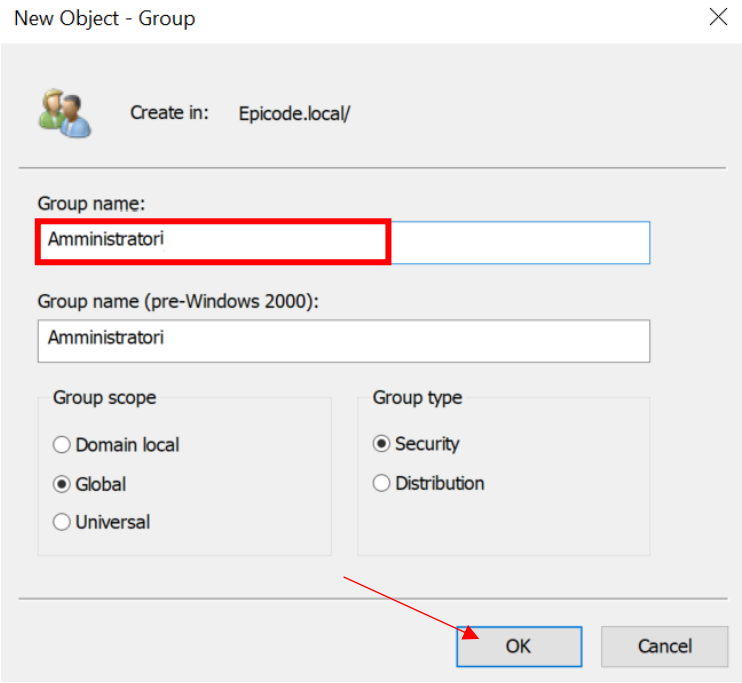


Figura 3, creazione del gruppo Amminstrazione.

Procedo in maniera analoga per la creazione di un secondo gruppo al quale questa volta assegnerò il nome "TeamSviluppo".

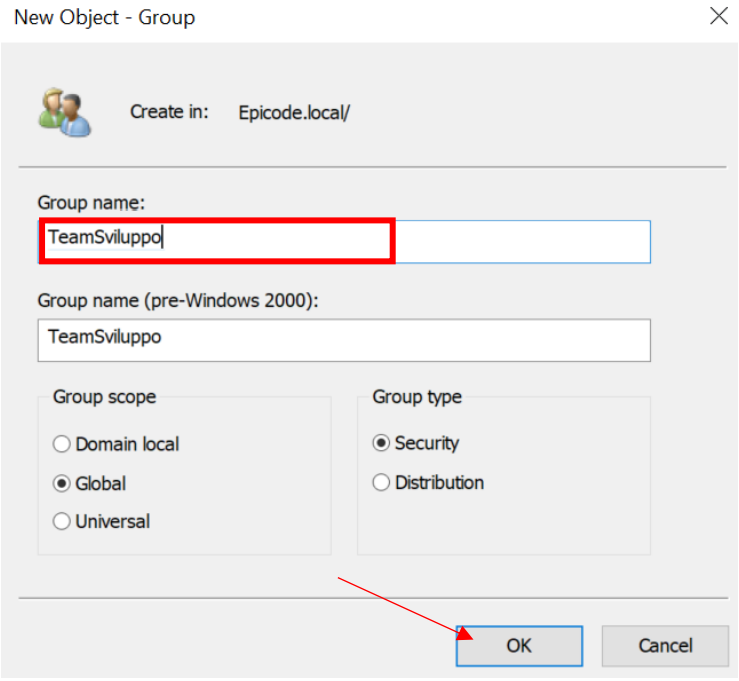
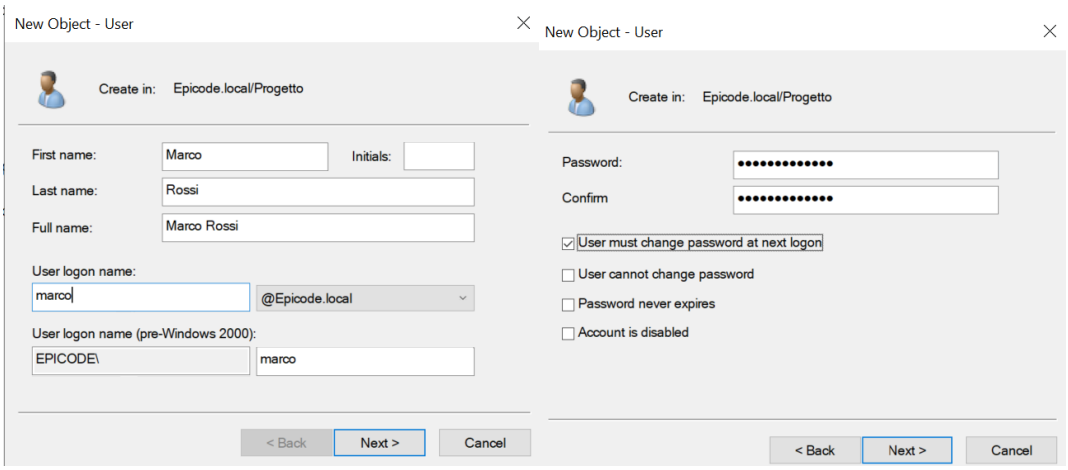
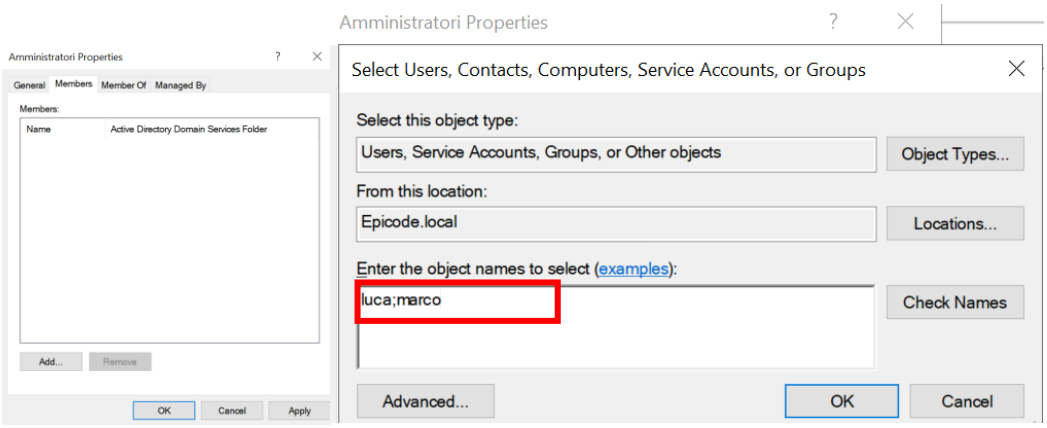


Figura 4, creazione del gruppo TeamSviluppo

A questo punto andrò ad aggiungere ai due gruppi degli utenti, al primo gruppo aggiungo le utenze Marco Rossi e Luca Bianchi e al secondo Martina Verdi e Luigi Neri (molta fantasia). Devo prima creare gli utenti per farlo farò click destro ***New → User***



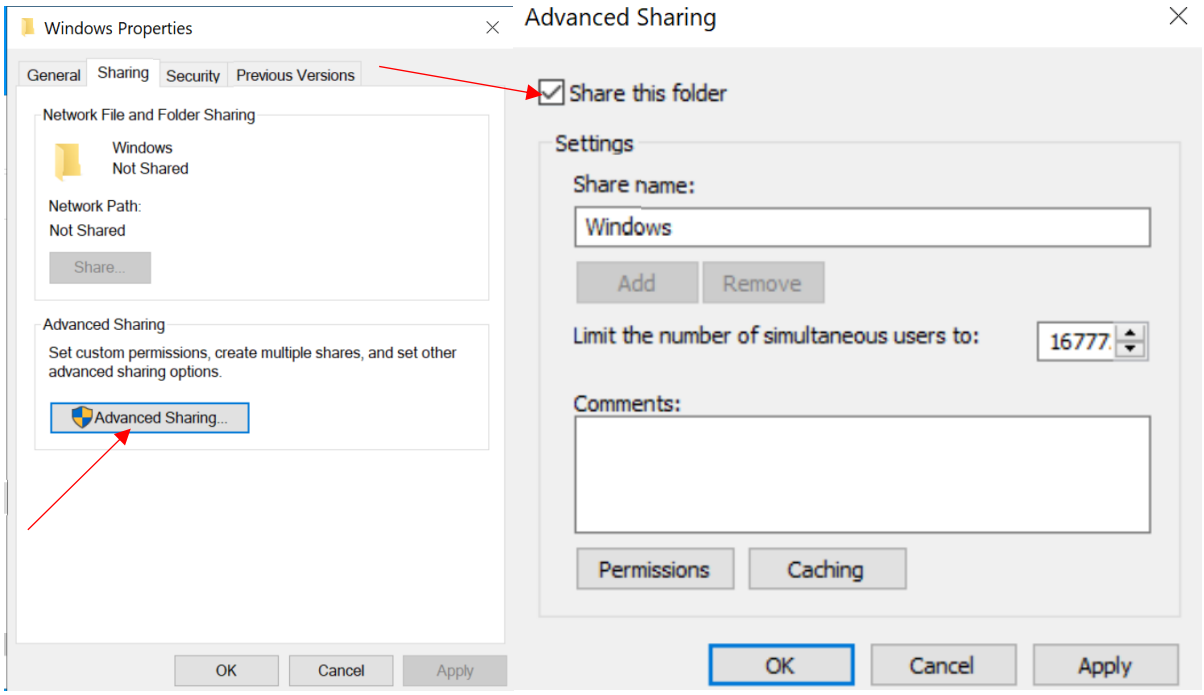
E assegnerò una password provvisiora ***flaggando*** la spunta per consentire all' utente di cambiarla al primo login. Ripeterò questi passaggi per tutte le utenze. Posso quindi aggiungere gli utenti creati ai gruppi, faccio doppio click sul gruppo amministratori e accedendo alla sezione Members vado su add e inserendone i nomi separati da ";".



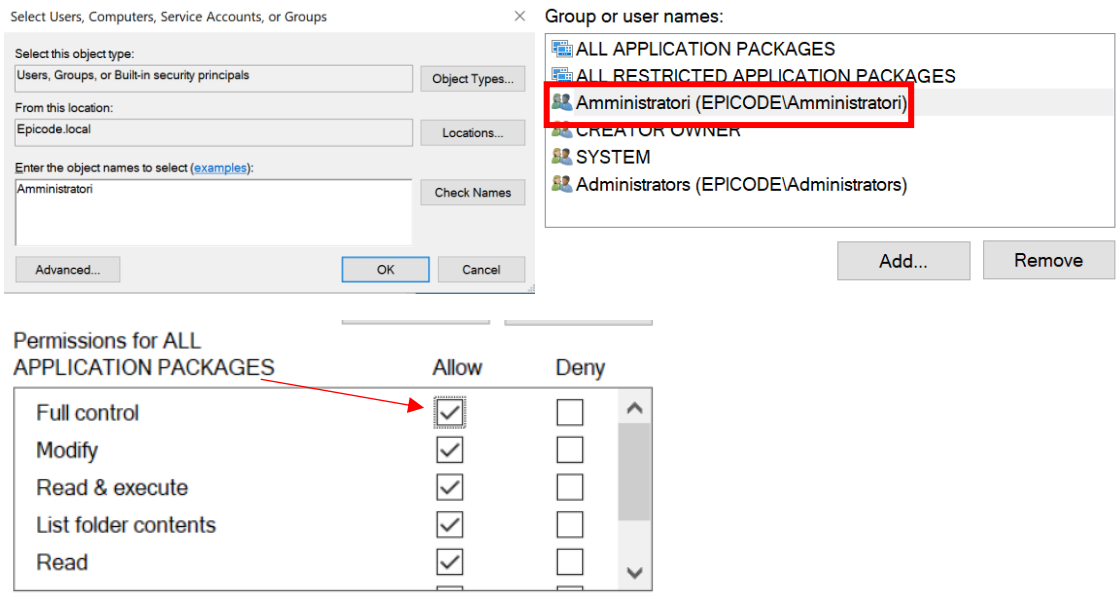
Farò analogamente anche per il gruppo "TeamSviluppo" nel quale aggiungerò le utenze Martina e Luigi.

A questo punto posso procedere andando ad assegnare i permessi ai rispettivi gruppi andando a definirne i ruoli.

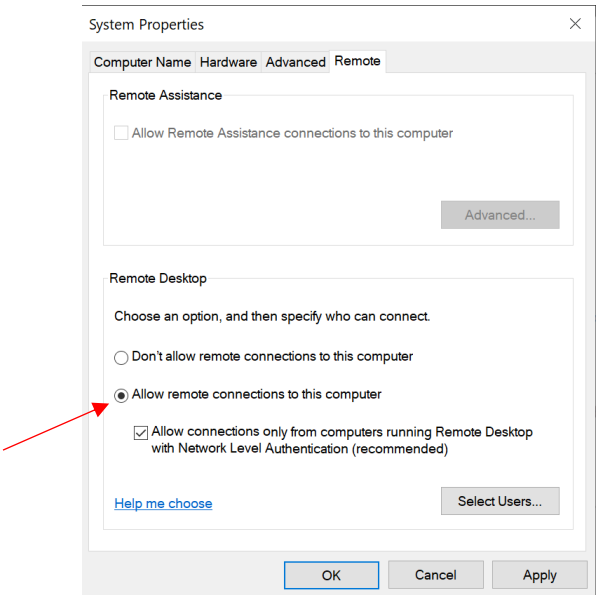
Al gruppo ***Amministratori*** assegnerò completo controllo sulla macchina, con accesso a tutti i file, possibilità di modifica dei file di sistema e accesso remoto al server. Dal server quindi accedo al Disco Locale C e facendo click destro vado su "***Condivisione***" e "***Condivisione Avanzata***".

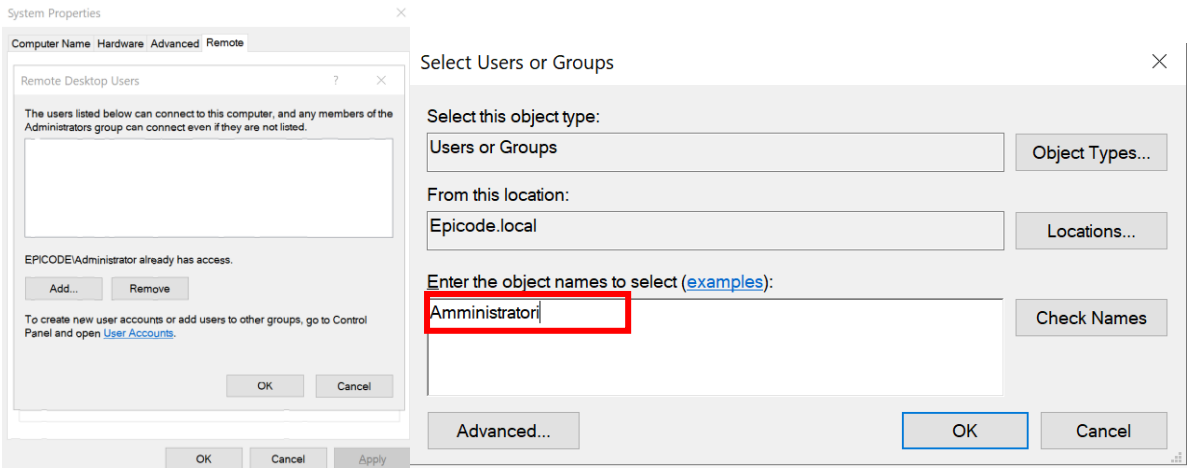


Quindi nella sezione “Sicurezza” procedo con “Edit” e “Aggiungi” e inserisco il nome del gruppo al quale voglio consentire l’ acceso ai file di sistema, in questo caso “Amministratori”, a questo punto flaggo “Controllo completo”.

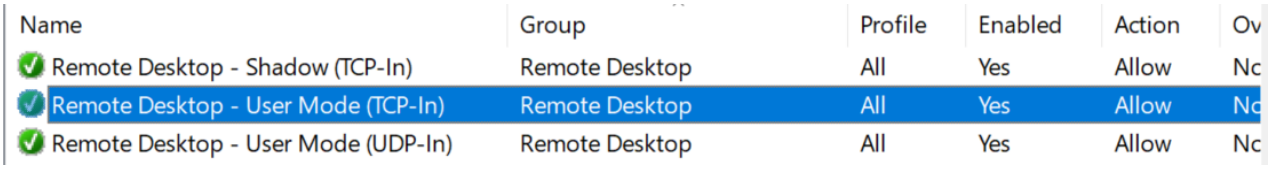


A questo punto voglio abilitare la possibilità di accedere al server remoto al gruppo ***Amministratori***. Dal server manager vado su “Local Server” e abilito le connessioni al server remoto. Posso quindi poi andare a selezionare gli utenti al quale consentire l’ accesso nello specifico solo quelli appartenenti al gruppo amminstratori.

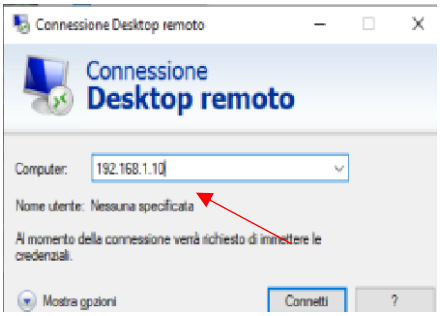




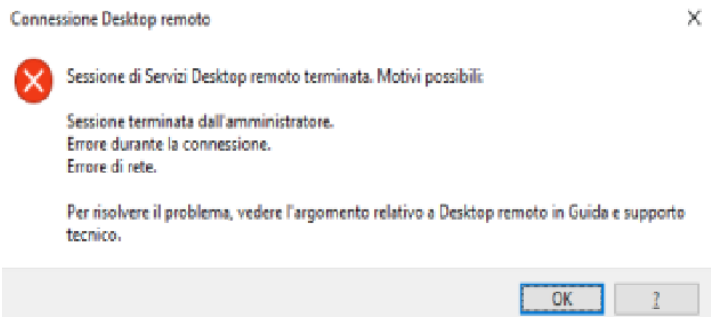
Coime ultimo passaggio devo poi aprire nel firewall la porta RDP. Abilitando la regola per le connessioni da desktop remoto.



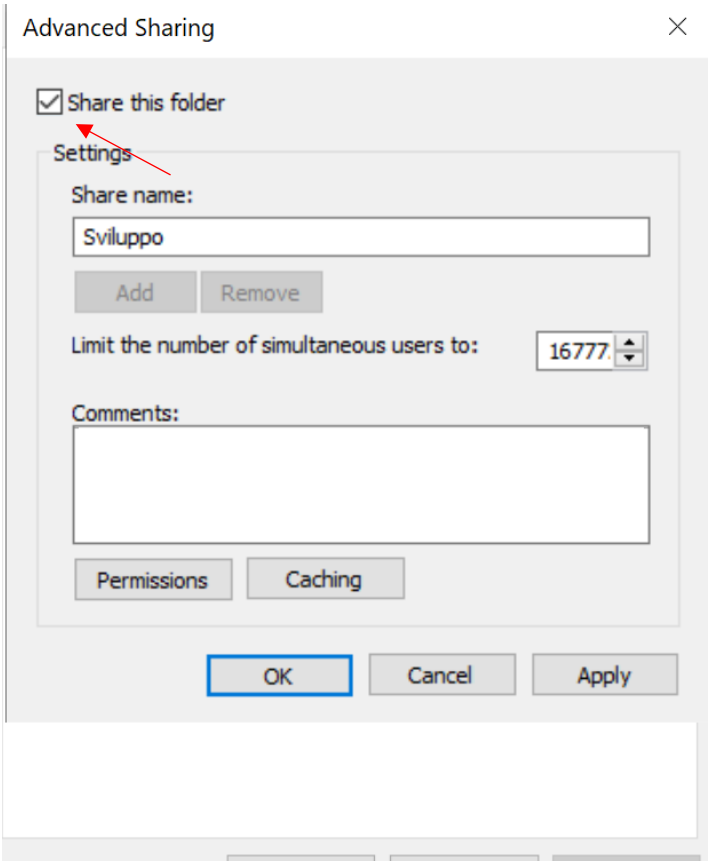
Vado quindi a testare la connessione dal client procedendo inserendo l' ip del server.

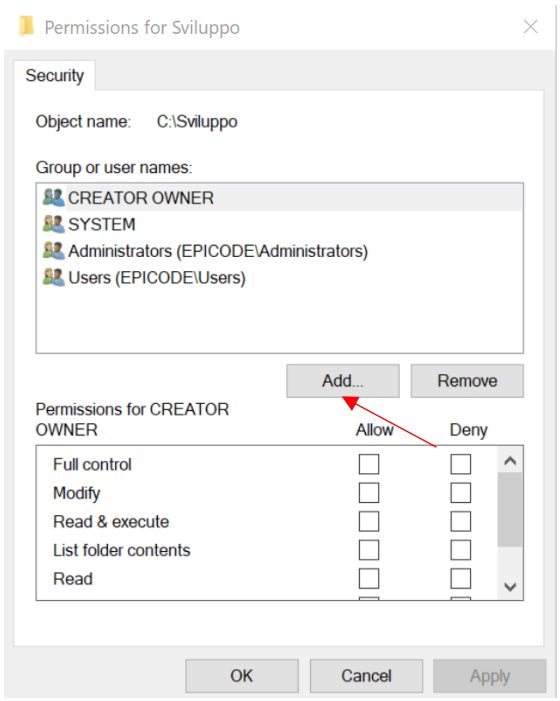


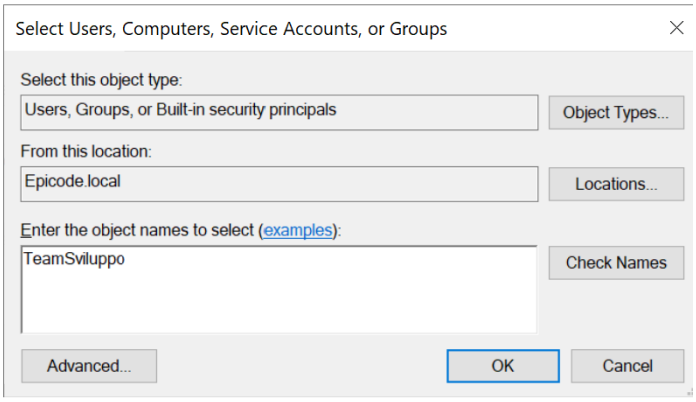
La connessione riesce con successo ma ricevo dopo breve tempo un messaggio di erore di rete, tuttavia l' accesso resta comunque possibile.



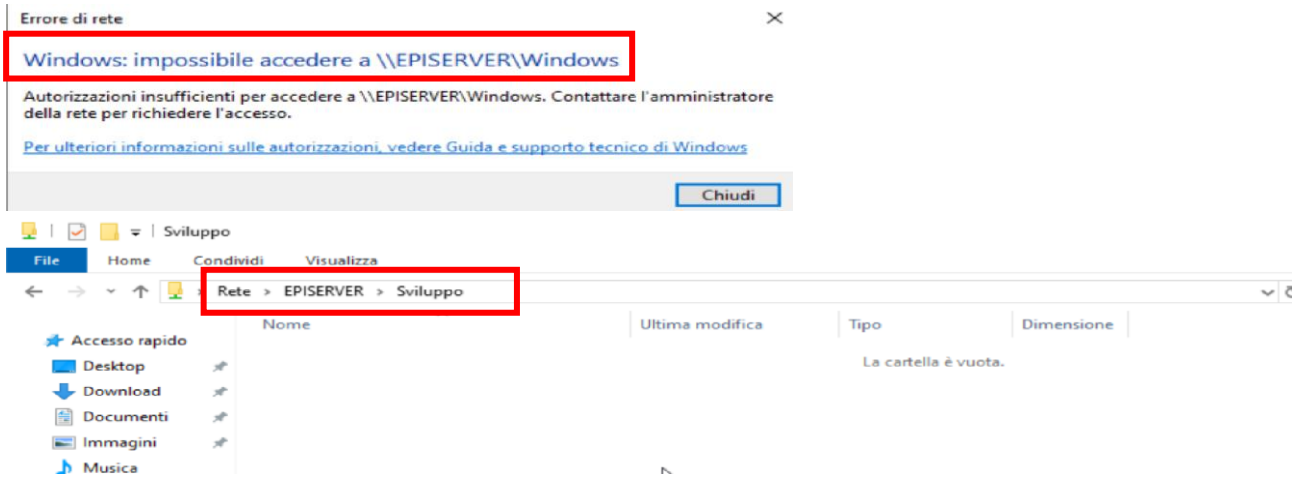
A questo punto vado invece a limitare i permessi dell' altro gruppo, in primo luogo a questi permetterò l' accesso alla sola cartella Sviluppo seguemdo il procedimento analogo a quello visto prima per "Amministratori".







Vado quindi a verificare da una delle utenze di questo gruppo che appunto non mi sia possibile accedere ai file di sistema e che invece ciò sia possibile sulla cartella Sviluppo. Eseguo la verifica dall' utente Martina.

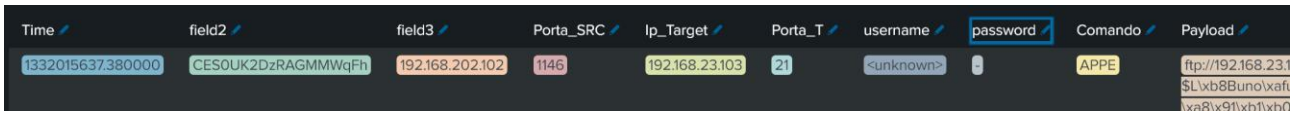


In sostanza quindi quello che ho fatto è stato andare a creare due gruppi distinti, Amminstratori e TeamSviluppo. Al primo gruppo ho assegnato controllo completo consentendo accesso remoto a tutti i file compresi i file di sistema e abilitando l' accesso remoto al server, al secondo gruppo invece ho limitato i ruoli consentendone il solo accesso alla cartella "Sviluppo".

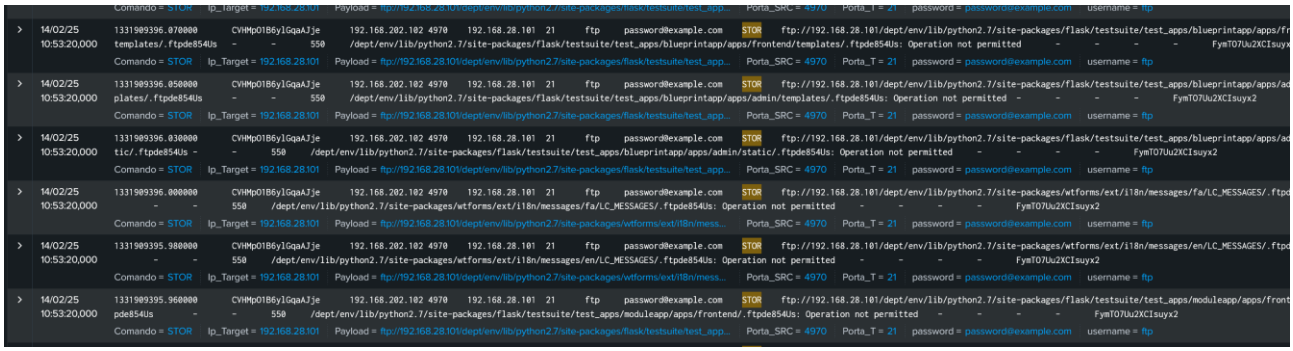
BONUS

Da una prima occhiata, notando anche la porta sulla quale va ad agire l' attaccante posso immaginare che si tratti del log di una serie di azioni di trasferimento di file mediante protocollo FTP.

Vado in primo luogo ad estrarre e rinominare i campi che possono essere di mio interesse, quindi aggiungerò, Time, Porta_SRC, Ip_Target, Porta_T, username, password, comando e Payload.



Posso notare come vi sia un traffico anomalo dall' IP: ***192.168.202.102*** nello specifico questo va ad eseguire un elevata quantità di comandi ***PASV***, ***STOR***, ***DEL*** sul bersaglio.



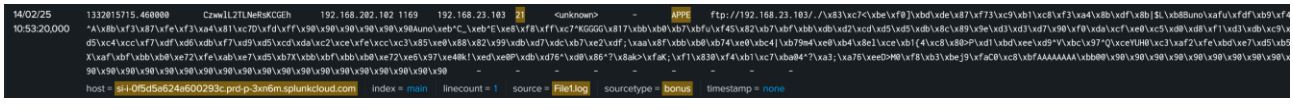
Il comando ***PASV*** fa riferimento ad una connessione ***FTP Passiva*** che puo far sospettare il tentativo di oltreppassare un firewall, a questa poi vado a sommare i comandi ***store*** e ***delete*** che mi fanno generare ulteriori sospetti è possibile infatti che vi sia il tentativo di uploadere dei file ed eliminarne altri sul server mediante protocollo ***FTP***.

Vi è inoltre un elevata presenza di comandi "***APPE***" questo sta per ***Append***, e si utilizza quando vengono aggiunti ***payload*** a dei file già esistenti o quando vi è tentativo di caricare ***exploit*** , con la query:

source="File1.log" host="si-i-0f5d5a624a600293c.prd-p-3xn6m.splunkcloud.com" sourcetype="bonus" "appe"

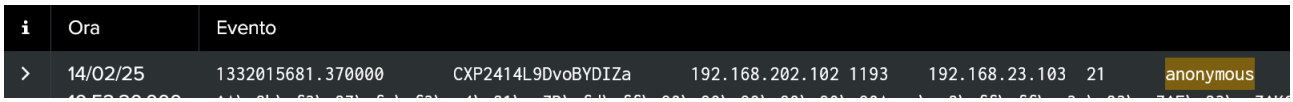
si evidenzia come nello specifico siano presenti 72 eventi di questo tipo.

Tutti provenienti dall stesso ***IP: 192.168.202.102***,da utente ***unknow***, la cosa che inoltre noto è che tutti gli eventi avvengono in un intervallo di tempo particolarmente breve.



I payload sono offuscati è possibile che stiano venendo caricati dei file sospetti (***malware***) o ***exploit***.

Un altra cosa che noto è che l' accesso a ***FTP*** stia avvenendo mediante l' utente "Anonymous", nel caso specifico gli eventi di accesso mediante quest ultimo sono 329, un unmero sicuramente anomalo, si evince inoltre che le password siano sempre in chiaro, anche questo costituisce un ulteriore problema.



i	Ora	Evento					
>	14/02/25	1332015681.370000	CXP2414L9DvoBYDIZa	192.168.202.102	1193	192.168.23.103	21	anonymous

Un attaccante in questo caso ha la possibilità di sfruttare il servizio ***FTP*** esposto e andare ad agire sul server per esempio per cancellare dei file oppure per caricare file malevoli o magari andare ad "appendere" file dannosi come malware a file già esistenti.

REMEDIATION

Disabilitare utente Anonymous:

- Su ***Vsftpd***, il server FTP su Linux) si va a modificare il file ***/etc/vsftpd.conf***, impostando ***anonymous_enable=no***
- Riavviare il servizio con ***systemctl restart vsftpd***.

Poichè le password in chiaro rendono vulnerabili agli attacchi MITM sarà necessario:

- Diabiiatare l' ***ftp*** non cifrato.
- Impostare un ***firewall*** che consenta solo ***FTPS (FTP over SSL/TLS)***

Controllare l' upload dei file:

- ***Antivirus*** sui file caricati con scansione auto.
- Limitare i permessi di scrittura ad un numero ristretti di utenti "noti".

Limitare gli ip malevoli:

- Impostare un limite di accessi per ip specifici per esempio con ***iptables***.

Ulteriormente si puo procedere con update di FTP:

apt update && apt upgrade

REPORT.

Nel log analizzato si evidenzia un attacco dall' IP: 192.168.202.102 ai danni del server, nello specifico ciò che avviene è un tentativo di connessione con protocollo FTP. Vi sono da parte dell' attaccante ripetuti tentativi, in intervalli brevissimi, di caricare file sul target e di aggiungere dei payload offuscati potenzialmente malevoli. La connessione FTP avviene con successo mediante utente Anonymous.

Le password risultano essere in chiaro, evidenziando un ulteriore vulnerabilità.

- Bloccare l' indirizzo IP dell' attaccante, 192.168.202.102.
- Il primo passo è quello di procedere andando a Disabilitare l' accesso "Anonymous" al protocollo FTP.
- Utilizzare FTPS
- Scansione file caricati automatica.
- Crittografia delle password.