

S10L5

Obiettivo

Lo scopo di questo esercizio è familiarizzare con la gestione dei gruppi di utenti in Windows Server 2022. Imparerai a:

- Creare gruppi.
 - Assegnare loro permessi specifici.
 - Comprendere l'importanza della gestione dei gruppi per la sicurezza e l'amministrazione del sistema.
-

Istruzioni

1. Preparazione

- Accedi al tuo ambiente Windows Server 2022.
- Assicurati di avere i permessi amministrativi necessari per creare e gestire gruppi.

2. Creazione dei Gruppi

- Crea due gruppi distinti.
- Puoi scegliere i nomi che preferisci, ma assicurati che siano significativi e riflettano la loro funzione o ruolo all'interno dell'organizzazione (es. "Amministratori", "UtentiStandard", "MarketingTeam", "Sviluppatori", ecc.).

3. Assegnazione dei Permessi

Per ogni gruppo, assegna permessi specifici. Considera i seguenti aspetti:

- Accesso ai file e alle cartelle.
- Esecuzione di programmi specifici.
- Modifiche alle impostazioni di sistema.
- Accesso remoto al server.

 Nota: Documenta i permessi assegnati a ciascun gruppo, spiegando le motivazioni delle scelte effettuate.

4. Verifica

Dopo aver creato i gruppi e assegnato i permessi, verifica che le impostazioni siano corrette attraverso i seguenti passaggi:

- Crea utenti di prova e aggiungili ai gruppi.
- Controlla che gli utenti abbiano i permessi assegnati in base al gruppo di appartenenza.
- Verifica che altri utenti non possano accedere a risorse non autorizzate.

5. Documentazione

Scrivi un breve report che includa:

- I nomi dei gruppi creati.
- I permessi assegnati a ciascun gruppo.
- I passaggi seguiti per creare e configurare i gruppi.
- Eventuali problemi riscontrati e le soluzioni adottate.

1. Nomi dei Gruppi Creati:

- **AmministratoriT**: Responsabili della gestione del sistema e delle configurazioni avanzate.
- **UtentiStandard**: Utenti con accesso limitato per l'uso quotidiano delle risorse aziendali.
- **Guests**: Utenti temporanei con accesso minimo alle risorse aziendali.

2. Permessi Assegnati a Ciascun Gruppo:

- **AmministratoriT**:
 - Accesso completo a tutte le cartelle e i file del sistema.
 - Possibilità di installare ed eseguire qualsiasi programma.
 - Modifica delle impostazioni di sistema, inclusi servizi, criteri di gruppo e gestione utenti.

- Accesso remoto al server tramite RDP.
 - **UtentiStandard:**
 - Accesso in sola lettura ai file e cartelle condivise, scrittura per specifiche cartelle.
 - Possibilità di eseguire solo applicazioni approvate, tra cui:
 - Microsoft Office (Word, Excel, PowerPoint)
 - Browser web (Microsoft Edge, Google Chrome, Mozilla Firefox)
 - Client di posta elettronica (Outlook, Thunderbird)
 - Software di gestione documentale (Adobe Acrobat Reader, Foxit Reader)
 - Strumenti di comunicazione aziendale (Microsoft Teams, Zoom, Skype for Business)
 - Nessun permesso per modificare le impostazioni di sistema.
 - Accesso remoto al server solo per alcuni utenti.
 - **Guests:**
 - Accesso limitato a cartelle pubbliche con permesso di sola lettura.
 - Possibilità di eseguire solo programmi di base, come:
 - Browser web (Microsoft Edge, Google Chrome)
 - Visualizzatore PDF (Adobe Acrobat Reader)
 - Strumenti di base (Blocco note, Calcolatrice)
 - Nessuna possibilità di installare software o modificare impostazioni di sistema.
 - Nessun accesso remoto al server.
-

Server Manager

Server Manager • Dashboard

SERVER MANAGER

AVVIO RAPIDO

1 Configura il server locale

2 Aggiungi ruoli e funzionalità

3 Aggiungi altri server da gestire

4 Crea un gruppo di server

5 Connetti il server ai servizi cloud

NOVITÀ

ULTERIORI INFORMAZIONI

RUOLI E GRUPPI DI SERVER

Ruoli: 3 | Gruppi di server: 1 | Totale server: 1

| | | |
|--|--|--|
| DNS 1 | Servizi di dominio Active Directory 1 | Servizi file e archiviazione |
| Gestibilità Eventi Servizi Prestazioni Risultati BPA | Gestibilità Eventi Servizi Prestazioni Risultati BPA | Gestibilità Eventi Servizi Prestazioni Risultati BPA |

| | |
|--|--|
| Server locale 1 | Tutti i server 1 |
| Gestibilità Eventi 5 Servizi Prestazioni Risultati BPA | Gestibilità Eventi 5 Servizi Prestazioni Risultati BPA |

Centro di amministrazione di Active Directory

Configurazione di sistema

Criteri di sicurezza locali

Deframmenta e ottimizza unità

Diagnostica memoria Windows

DNS

Domini e trust di Active Directory

Editor del Registro di sistema

Gestione computer

Gestione Criteri di gruppo

Iniziatore iSCSI

Modifica ADSI

Modulo di Active Directory per Windows PowerShell

Monitoraggio risorse

ODBC Data Sources (32-bit)

Origini dati ODBC (64 bit)

Performance Monitor

Pulizia disco

Servizi

Servizi componenti

Servizi Microsoft Azure

Siti e servizi di Active Directory

System Information

Unità di ripristino

Utenti e computer di Active Directory

Utilità di pianificazione

Visualizzatore eventi

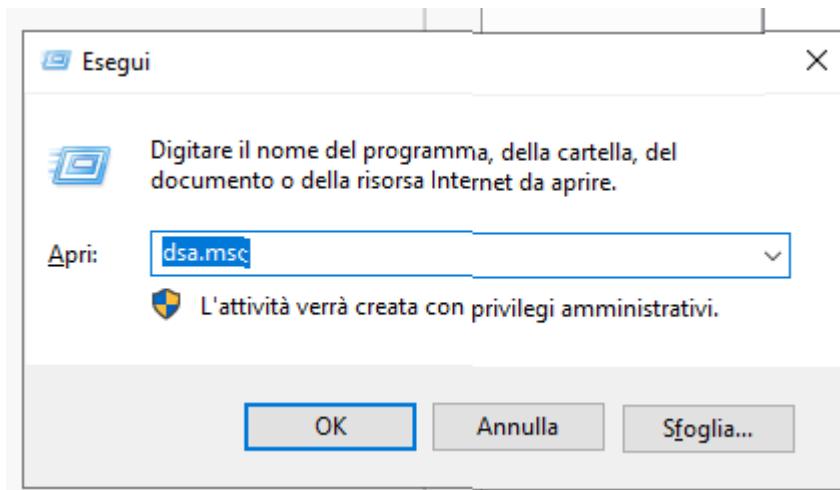
Windows Defender Firewall con sicurezza avanzata

Windows PowerShell

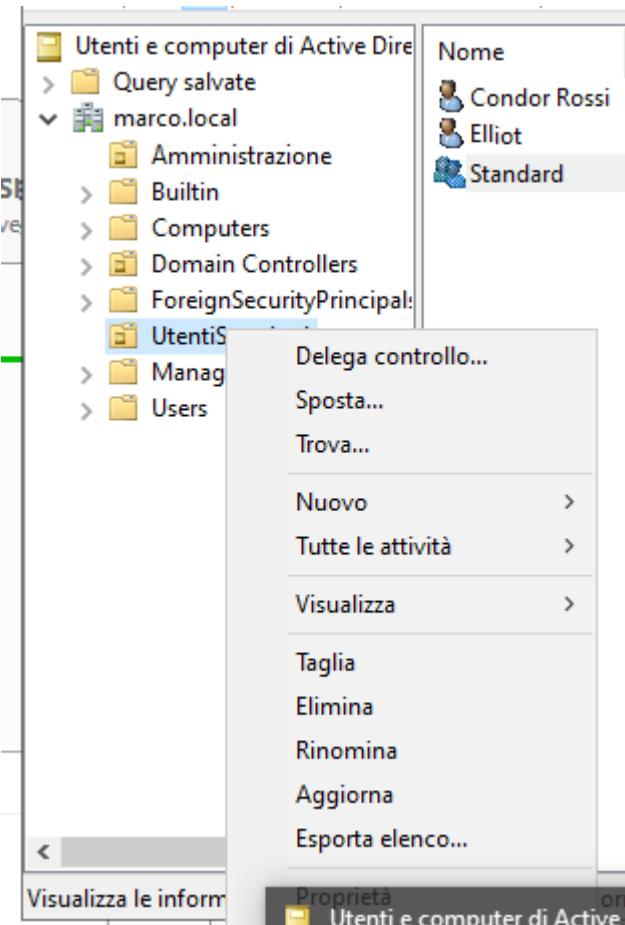
Windows PowerShell (x86)

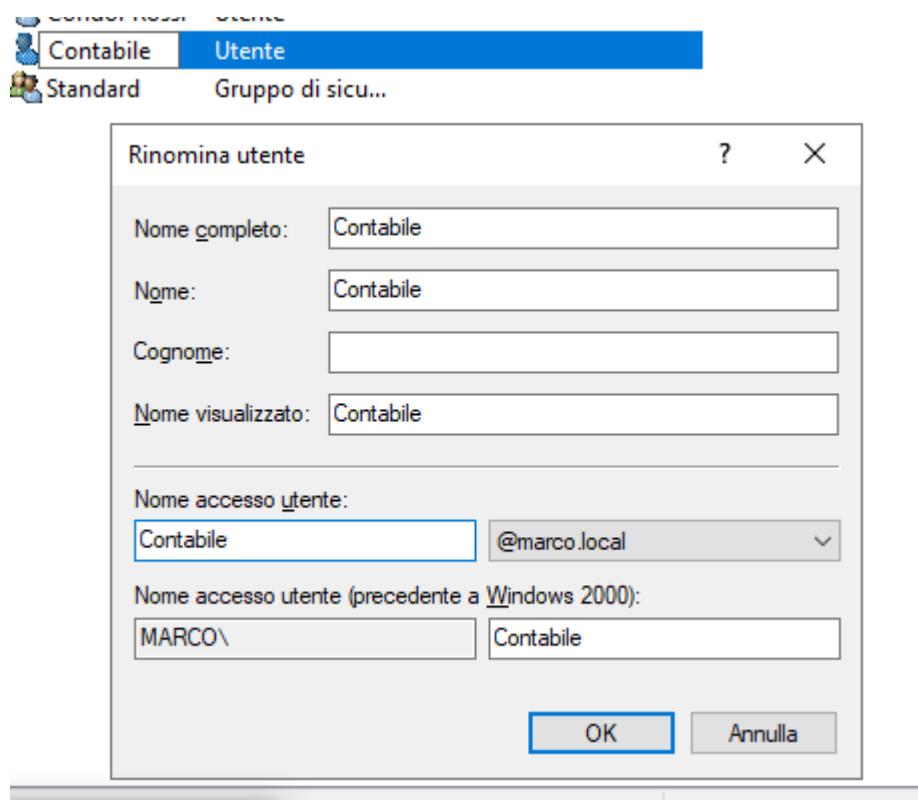
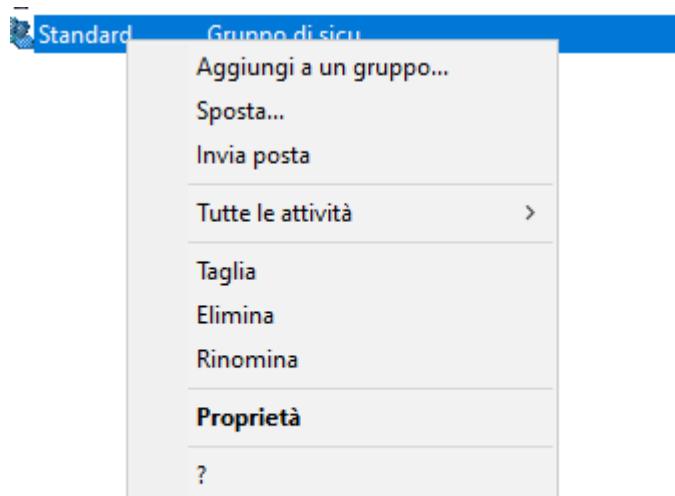
Windows Server Backup

Uso Win+R per aprire “esegui” e con dsa.msc apro la gestione degli utenti active sync



È presente una configurazione precedente, andremo a rinominare i gruppi, gli utenti e a sistemare la struttura di gruppi e utenti, aggiungendo il gruppo Guest, che ha permessi molto limitati per i visitatori. A seguire alcuni screenshot da cui si capisce la procedura seguita.





| Nome | Tipo | De |
|------------|-------------------|----|
| Segretario | Utente | |
| Contabile | Utente | |
| Standard | Gruppo di sicu... | |

Direttiva Nome Tipo Descrizione

Rinomina utente ? X

| | |
|--|--------------|
| Nome completo: | Segretario |
| Nome: | Pinco |
| Cognome: | Pallo |
| Nome visualizzato: | Segretario |
| Nome accesso utente: | |
| Segretario | @marco.local |
| Nome accesso utente (precedente a Windows 2000): | |
| MARCO\ | Segretario |
| <input type="button" value="OK"/> <input type="button" value="Annulla"/> | |

Una volta creato un utente, ricordiamoci di aggiungerlo al gruppo di pertinenza per fargli ereditare i permessi del gruppo

ire Nome Tipo Descrizione

| | | |
|------------|-------------------|--|
| CEO | Utente | |
| Contabile | Utente | |
| Segretario | Utente | |
| Standard | Gruppo di sicu... | |

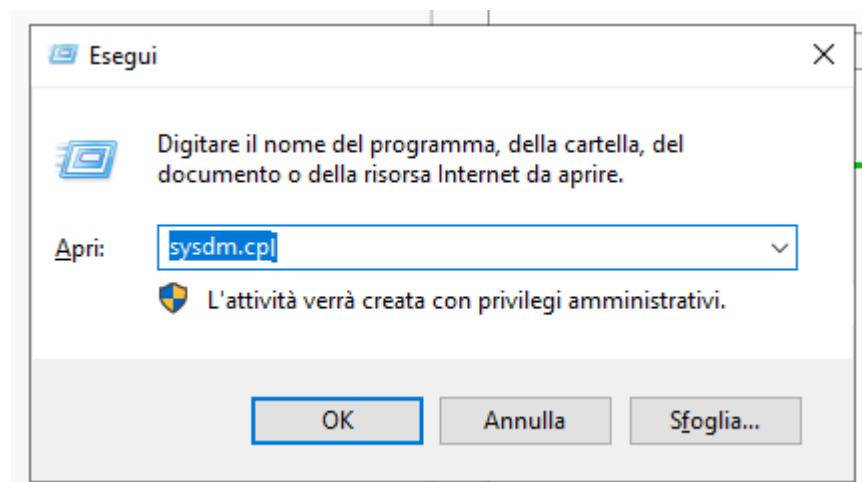
ale

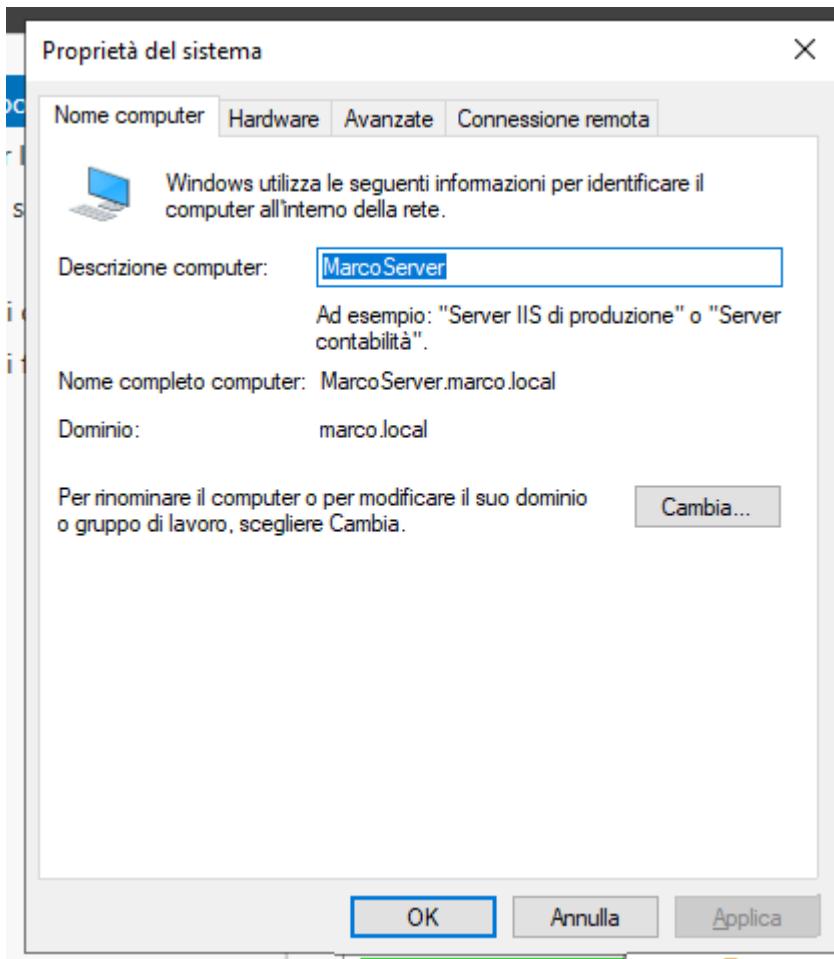
The screenshot shows the Windows Server 2022 Active Directory Users and Computers snap-in. A group named "AdminUsers" is selected. The "Membri" tab is active, listing the following members:

| Nome | Carta di Servizi di dominio Active Directory |
|---------------|--|
| AdminBackup | marco.local/AmministrazioneIT |
| CyberSecurity | marco.local/AmministrazioneIT |
| MarcoAdmin | marco.local/AmministrazioneIT |
| AdminBackup | marco.local/AmministrazioneIT |

Buttons at the bottom of the member list include "Aggiungi..." and "Rimuovi".

Una volta rinominati gli utenti, andremo ad aprire le proprietà di sistema per modificare il nome della macchina
win server 2022





Andiamo a creare una cartella chiamata “Condivisa” in C:\ e assegniamo i permessi adeguati ai nostri utenti come discusso precedentemente.

La cartella Condivisa avrà all’interno le seguenti cartelle

| Questo PC > Disco locale (C:) > Condivisa > | |
|---|-------|
| Nome | Ultim |
| Amministrazione | 14/02 |
| Guest | 14/02 |
| Standard | 14/02 |

I permessi sono così assegnati.

Gruppo AmministratoreIT avrà accesso completo su tutto

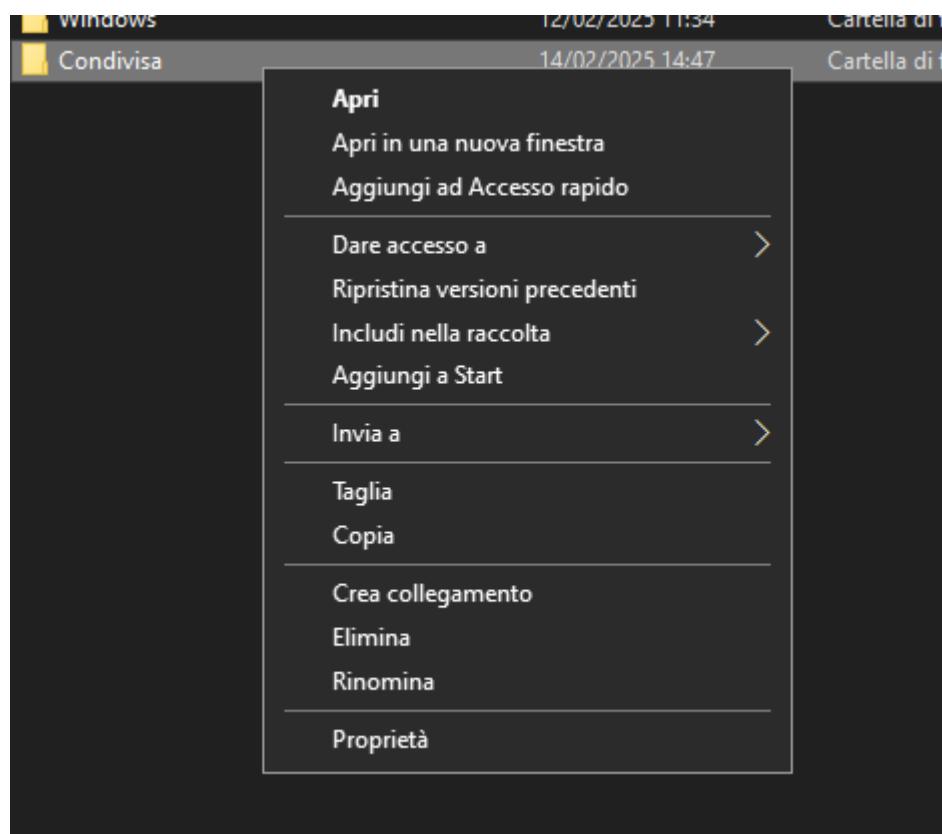
Gruppo Standard avrà scrittura e lettura sulla cartella Standard e sola lettura su Guest

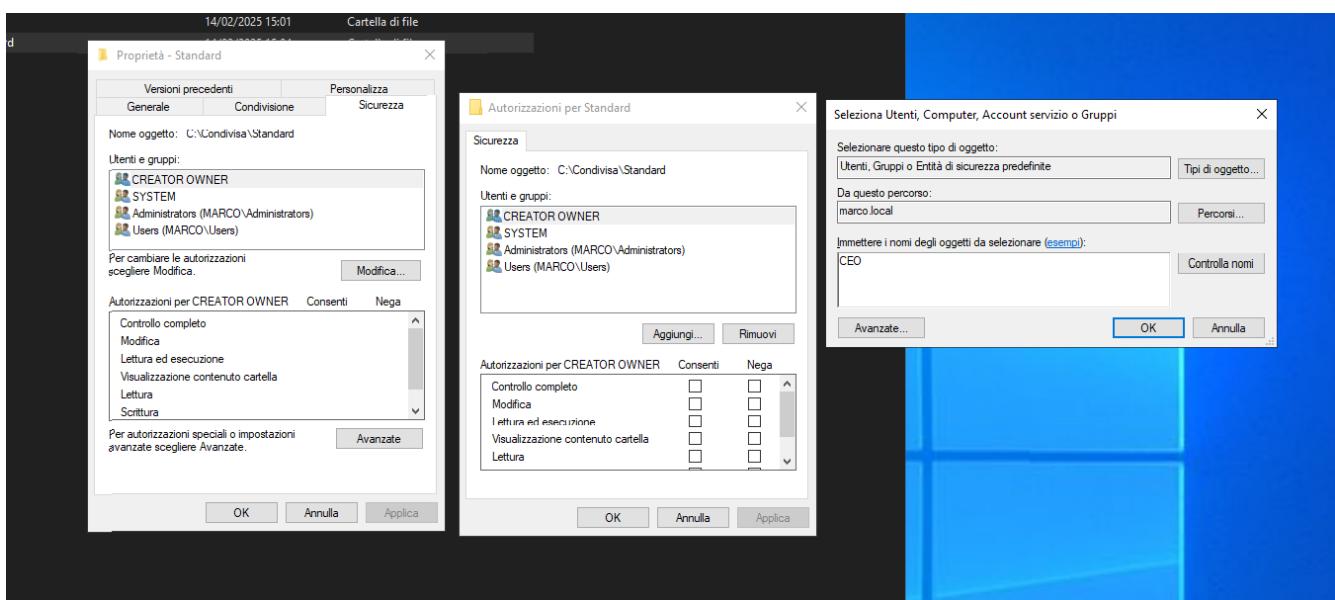
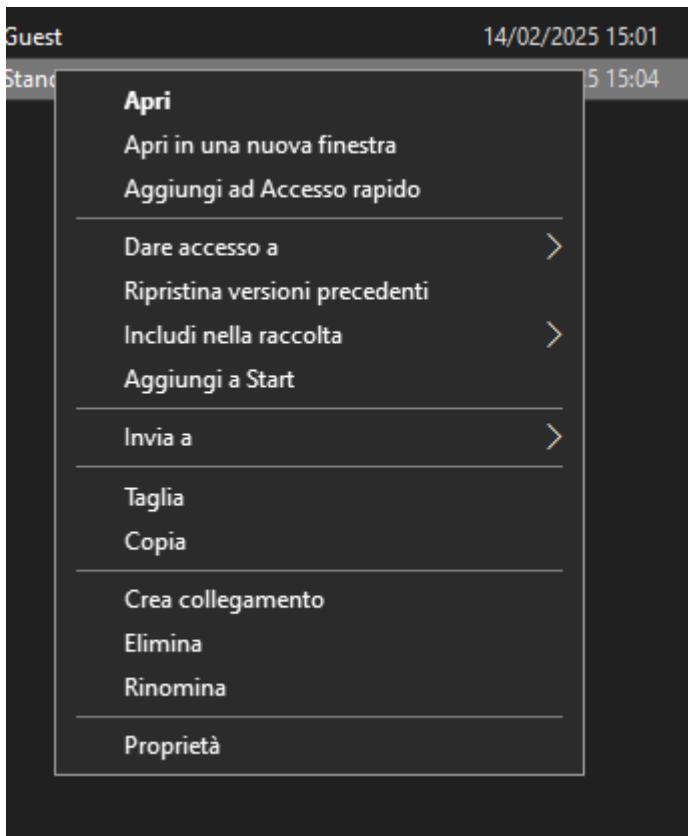
| Visualizza | |
|--|------------------|
| Questo PC > Disco locale (C:) > Condivisa > Standard | |
| | |
| Nome | Ultima modifica |
| Amministrazione | 14/02/2025 15:34 |
| Contabilità | 14/02/2025 15:34 |
| Segreteria | 14/02/2025 15:34 |

All'interno del gruppo Standard l'utente CEO avrà controllo completo su tutto, l'utente contabile avrà RW (read write) su Contabilità e su Segreteria

Segreteria avrà RW su Segreteria e basta

Mostriamo ora un esempio di assegnazione dei permessi





The screenshot shows the context menu for a file or folder in Windows File Explorer. The 'Condividi' (Share) option is highlighted. Below it, the 'Condividi con...' (Share with...) option is selected, showing a list of users and groups: 'Administrator (MARCO\Administrators)', 'CEO (CEO@marco.local)', and 'Users (MARCO\Users)'. At the bottom of the list are 'Aggiungi...' (Add) and 'Rimuovi' (Remove) buttons.

Administrator (MARCO\Administrators)
CEO (CEO@marco.local)
Users (MARCO\Users)

Aggiungi... Rimuovi

Autorizzazioni per CEO

| | Consenti | Nega |
|------------------------------------|-------------------------------------|--------------------------|
| Controllo completo | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Modifica | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Lettura ed esecuzione | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Visualizzazione contenuto cartella | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Lettura | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

OK Annulla Annulla

Per condividerla in rete, facciamo così

← Accesso alla rete

Scegliere gli utenti della rete a cui consentire l'accesso alla condivisione

Digitare un nome, quindi fare clic su Aggiungi oppure fare clic sulla freccia per trovare un utente.

The screenshot shows the 'Accesso alla rete' (Network sharing) dialog. It lists users and their sharing levels:

| Nome | Livello di autorizzazione |
|----------------|---------------------------|
| Administrator | Lettura/Scrittura ▼ |
| Administrators | Proprietario |
| CEO | Lettura/Scrittura ▼ |

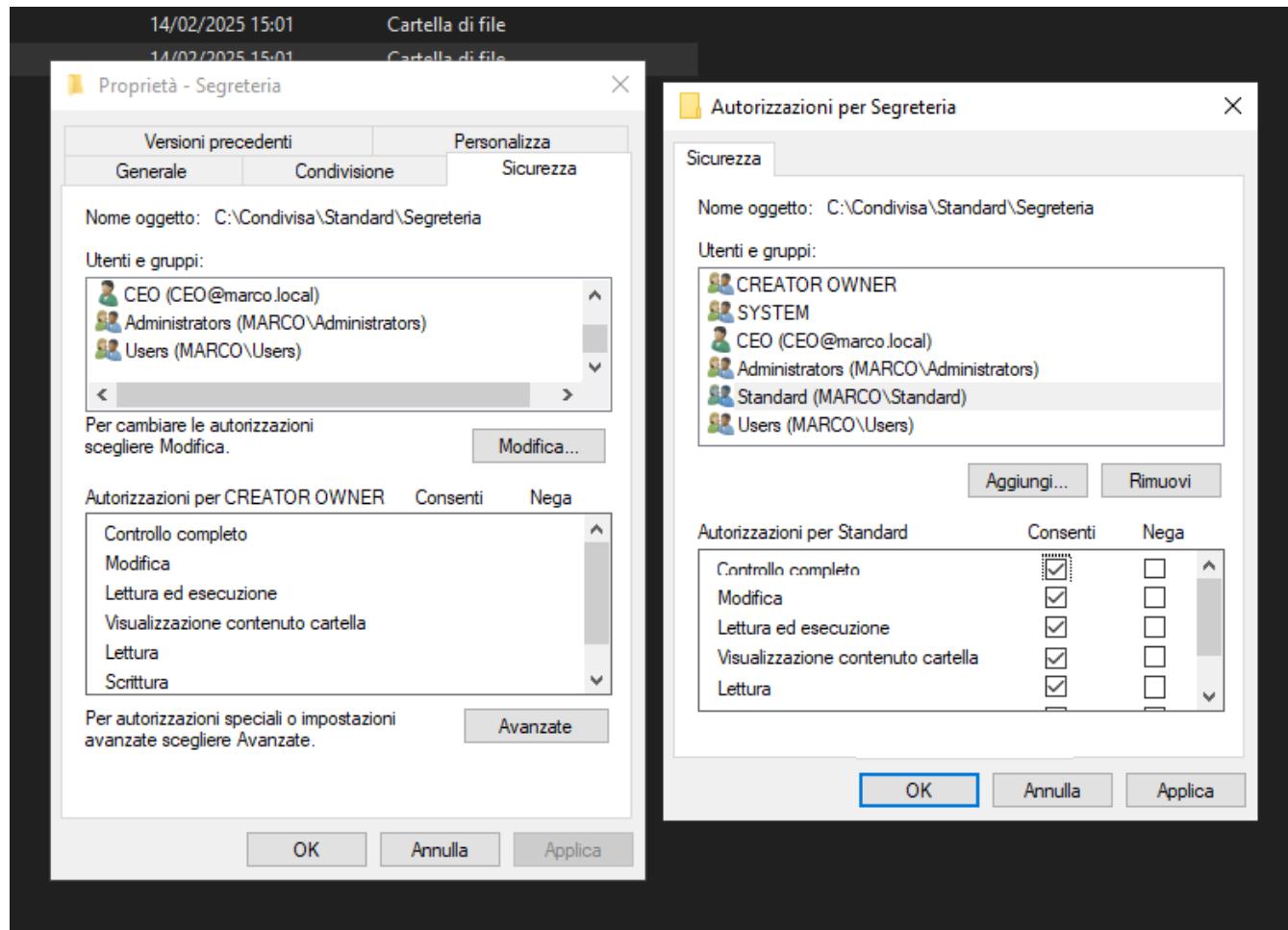
Aggiungi

Problemi di condivisione

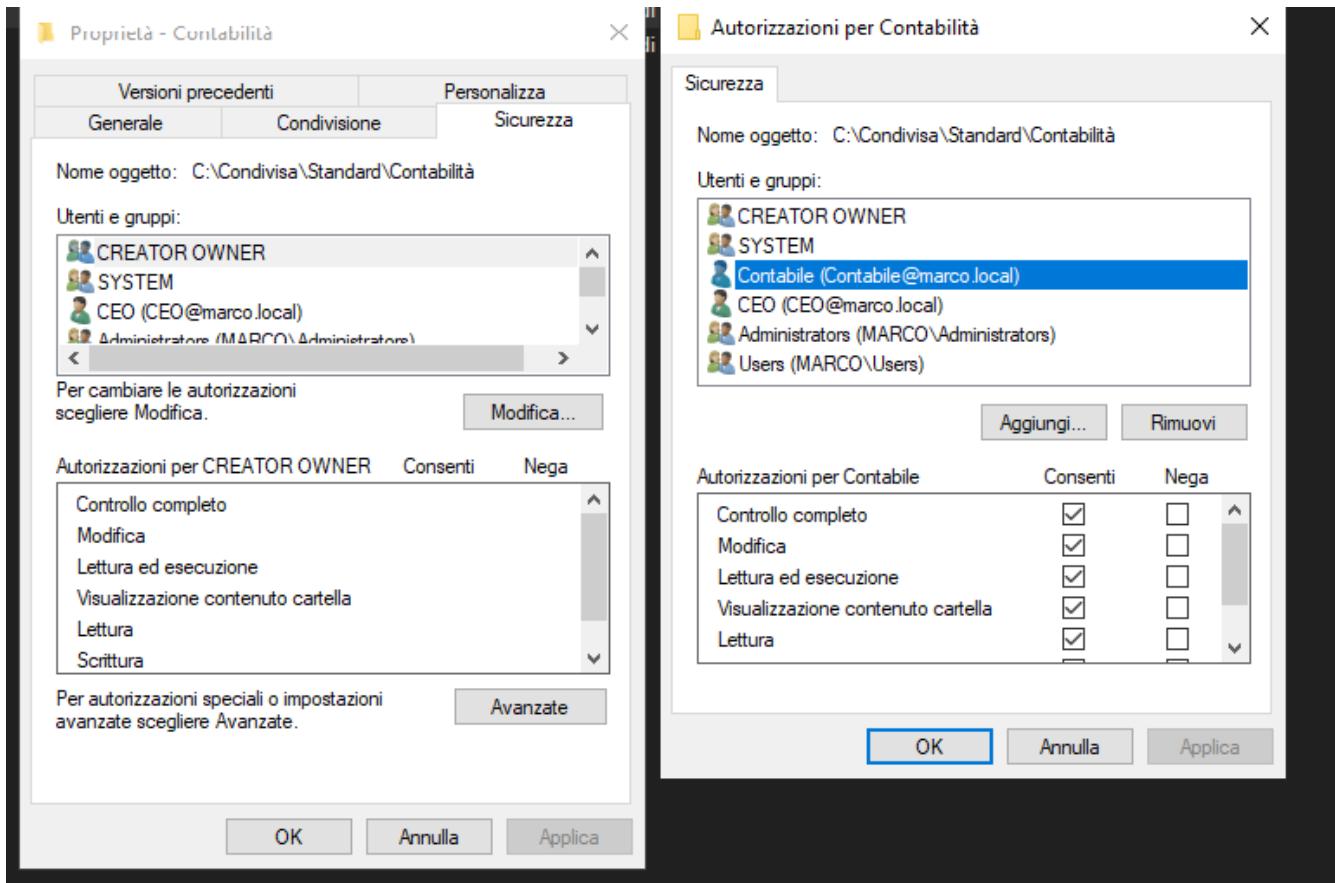
Condividi

Annulla

Ora passiamo alla cartella Segreteria, a cui tutti nel gruppo hanno accesso



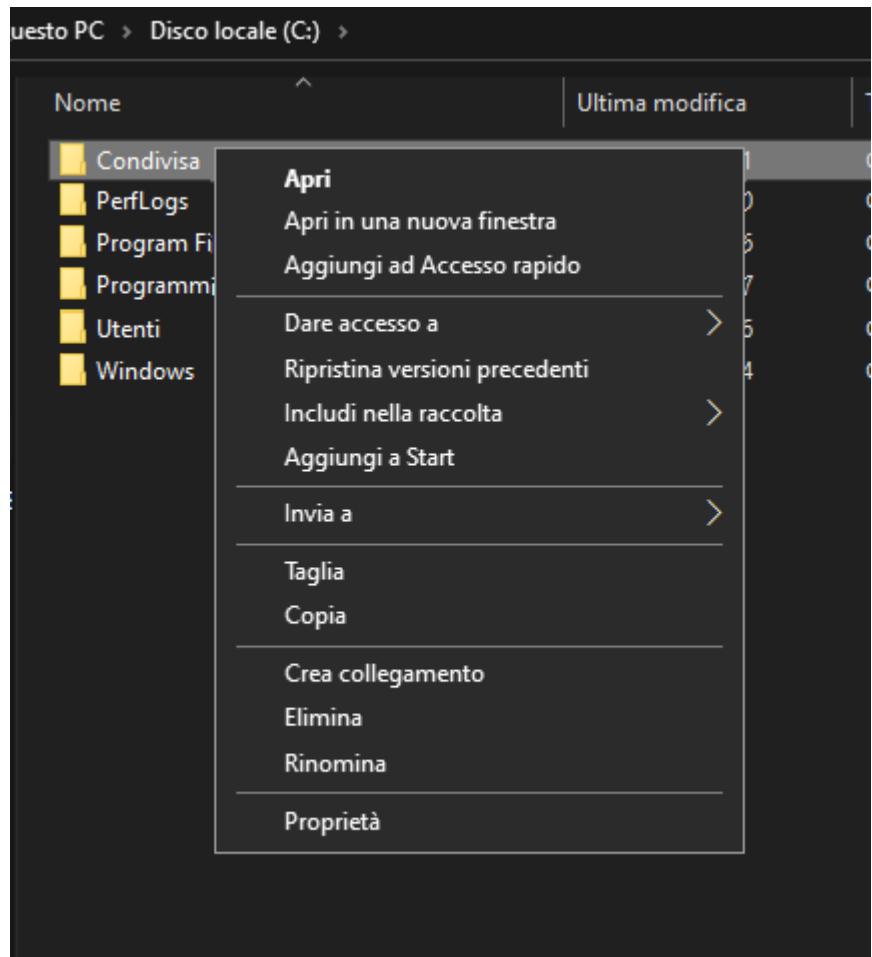
L'utente contabile invece avrà RW sulla sua cartella

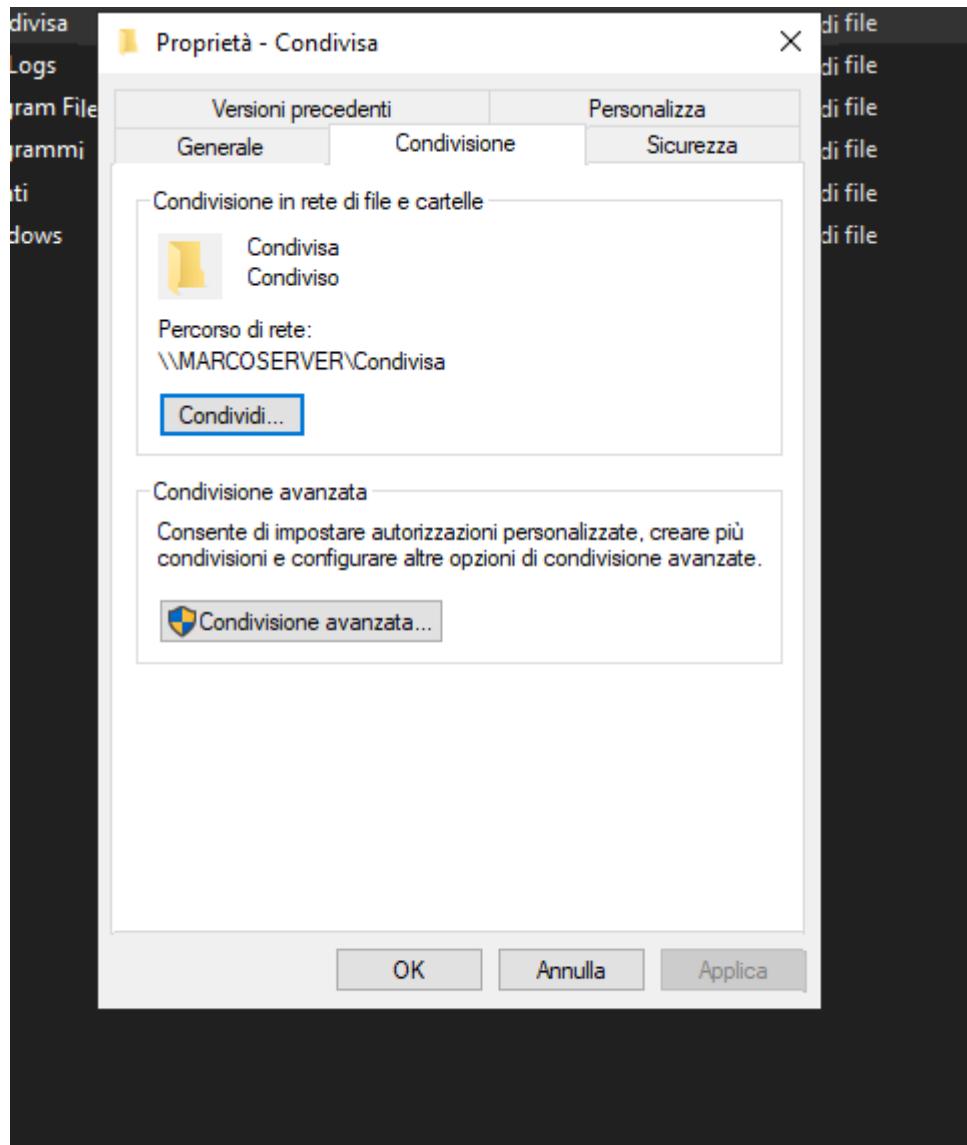


AmministrazioneIT avrà permessi su tutto, i permessi vengono assegnati analogamente a prima.

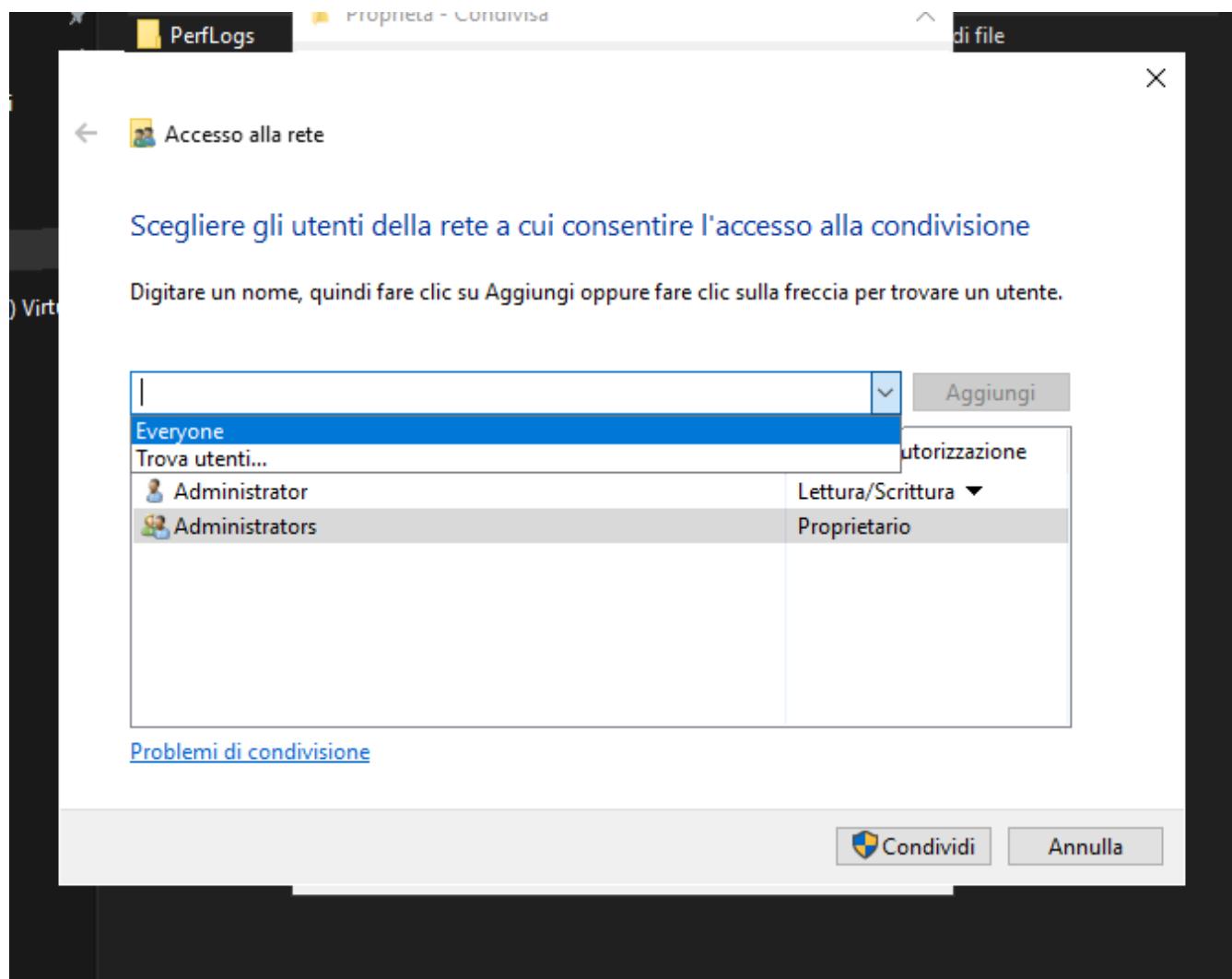
Ora provvedo a condividere la cartella “Condivisa”, i permessi sono già impostati ma per essere sicuri si può andare ad assegnare a mano i permessi di lettura e scrittura

Proprietà

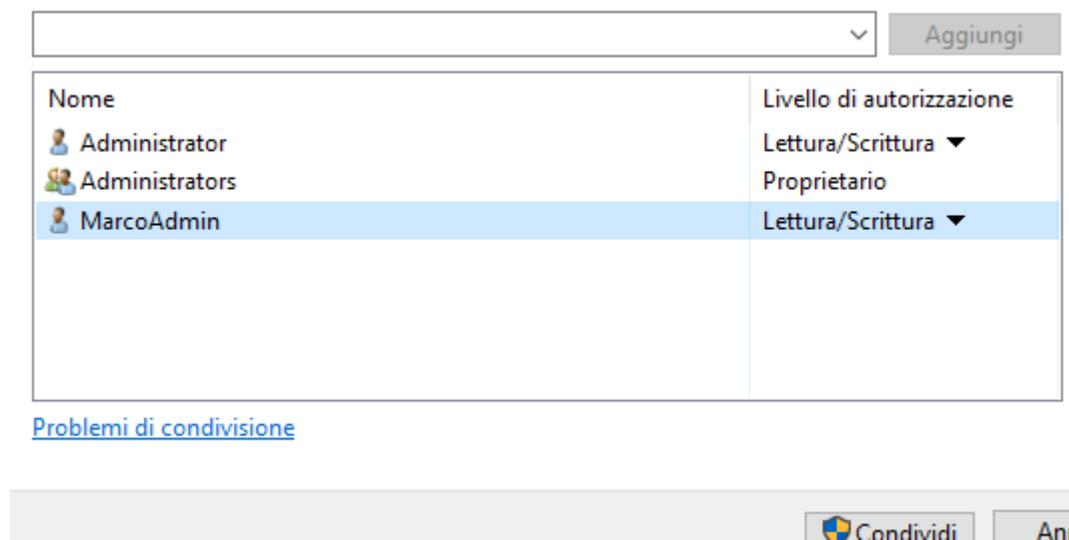




Condividi



Qui sceglio un utente ad esempio MarcoAdmin. In caso di configurazione perfetta dei permessi si può selezionare il gruppo o anche Everyone, noi ci limitiamo a selezionarli manualmente

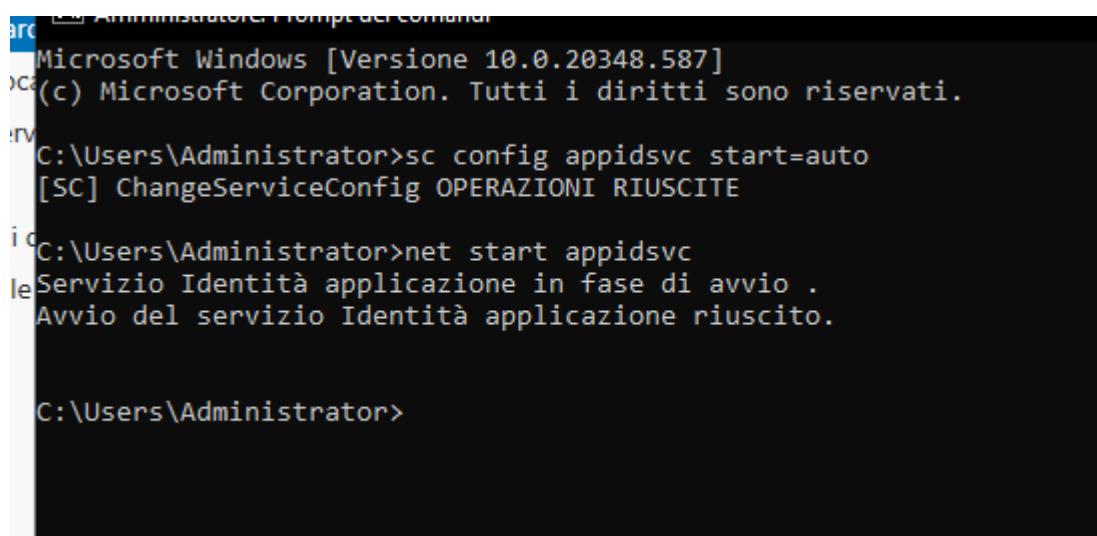


Ora procediamo a dare gli accessi di esecuzione di programmi specifici

Per limitare l'accesso a programmi specifici usiamo AppLocker, per abilitarlo apro il prompt dei comandi come amministratore ed eseguo i seguenti comandi:

```
sc config appidsvc start=auto
```

```
net start appidsvc
```



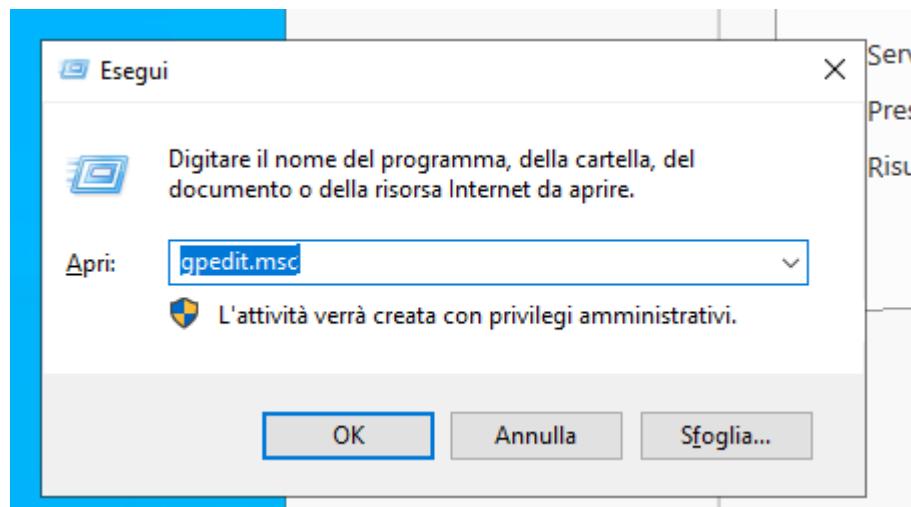
```
Administrator: Prompt dei comandi
Microsoft Windows [Versione 10.0.20348.587]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

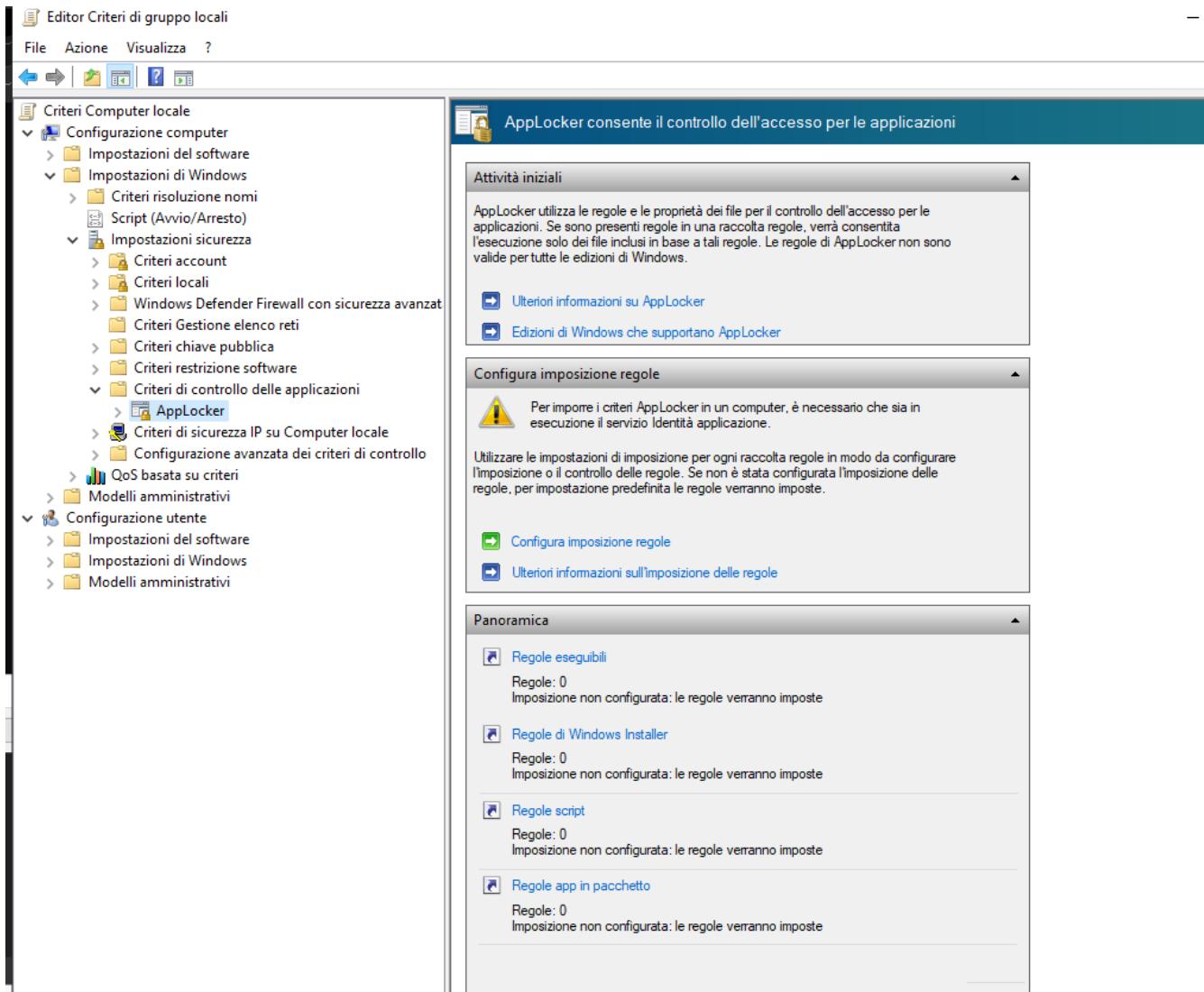
C:\Users\Administrator>sc config appidsvc start=auto
[SC] ChangeServiceConfig OPERAZIONI RIUSCITE

C:\Users\Administrator>net start appidsvc
Servizio Identità applicazione in fase di avvio .
Avvio del servizio Identità applicazione riuscito.

C:\Users\Administrator>
```

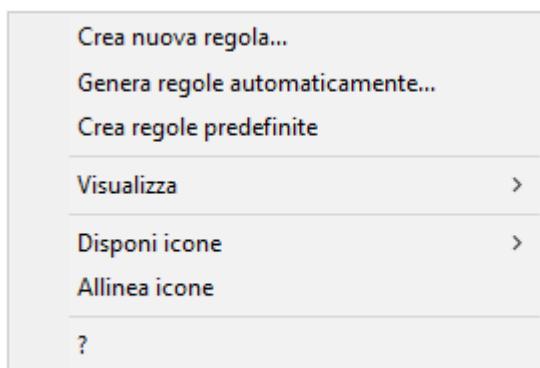
```
gpedit.msc
```





Regole eseguibili

Click destro



Autorizzazioni

Prima di iniziare

Autorizzazioni

Condizioni

Autore

Eccezioni

Nome

Selezionare l'azione da utilizzare e l'utente o il gruppo a cui applicare la regola. Un'azione di assenso consente l'esecuzione dei file interessati, mentre un'azione di negazione ne impedisce l'esecuzione.

Azione:

Consenti

Nega

Utente o gruppo:

MARCO\Segretario

Seleziona...

Condizioni

Prima di iniziare

Autorizzazioni

Condizioni

Percorso

Eccezioni

Nome

Selezionare il tipo di condizione primaria da creare.

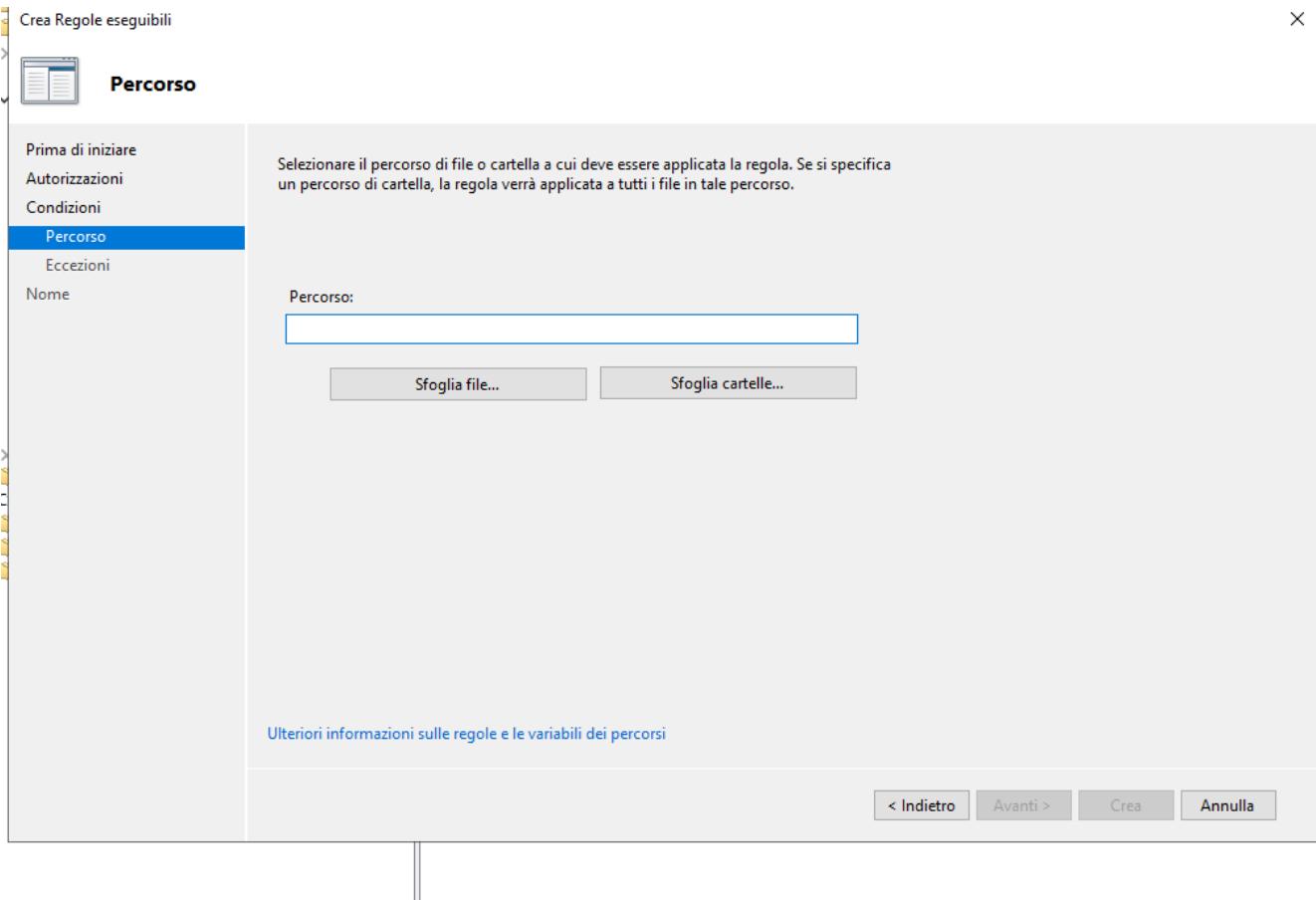
Autore
Selezionare questa opzione se l'applicazione per la quale si desidera creare la regola è firmata dall'autore del software.

Percorso
Crea una regola per un percorso di cartella o file specifico. Se si seleziona una cartella, tutti i file contenuti nella cartella saranno sottoposti alla regola.

Hash file
Selezionare questa opzione per creare una regola per un'applicazione non firmata.

[Ulteriori informazioni sulle condizioni per la regole](#)

< Indietro Avanti > Crea Annulla



Qui inserisco il percorso dei software che voglio abilitare, come outlook (gestione mail e calendario), word, excel e edge browser.

Per bloccare tutti gli altri percorsi, non inserisco come percorso da bloccare per impedire l'esecuzione di qualsiasi altra applicazione.

Una volta eseguite tutte le modifiche, apro il terminale come amministratore, digito

```
gpupdate /force
```

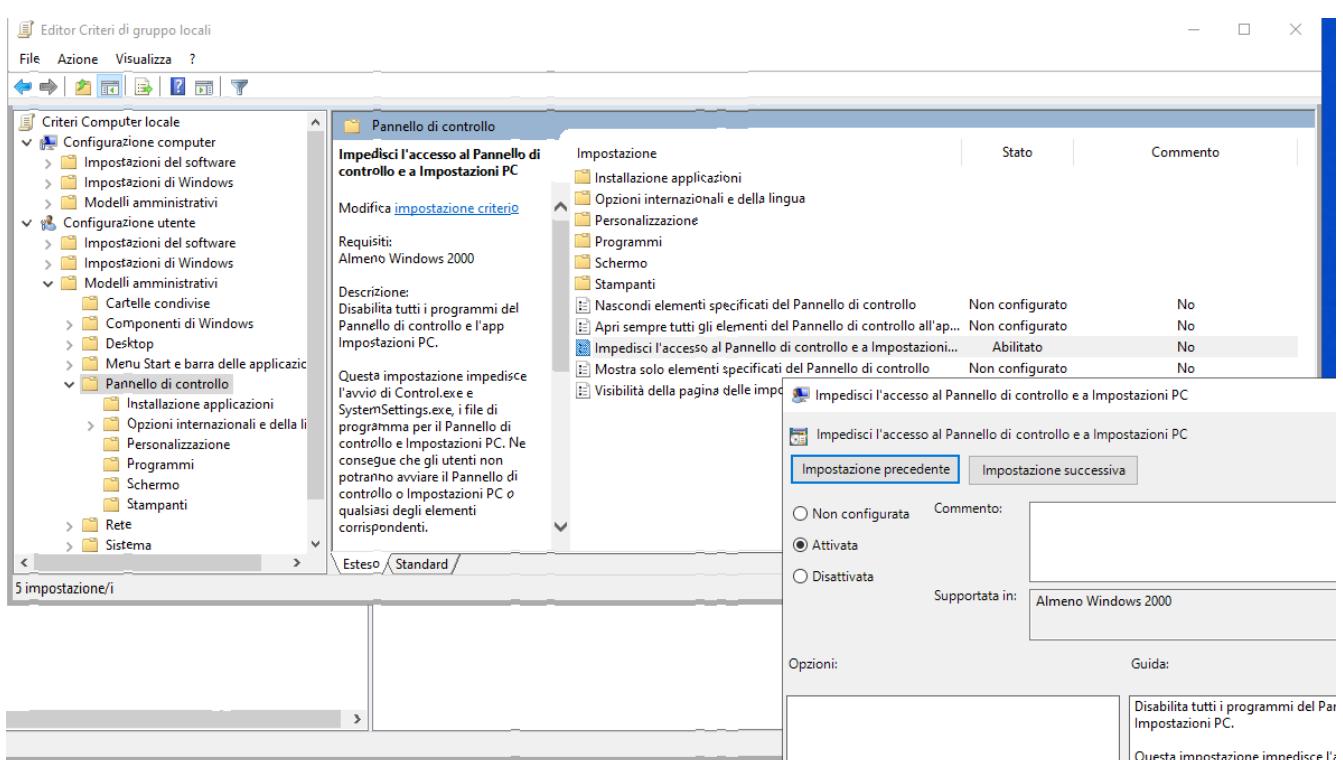
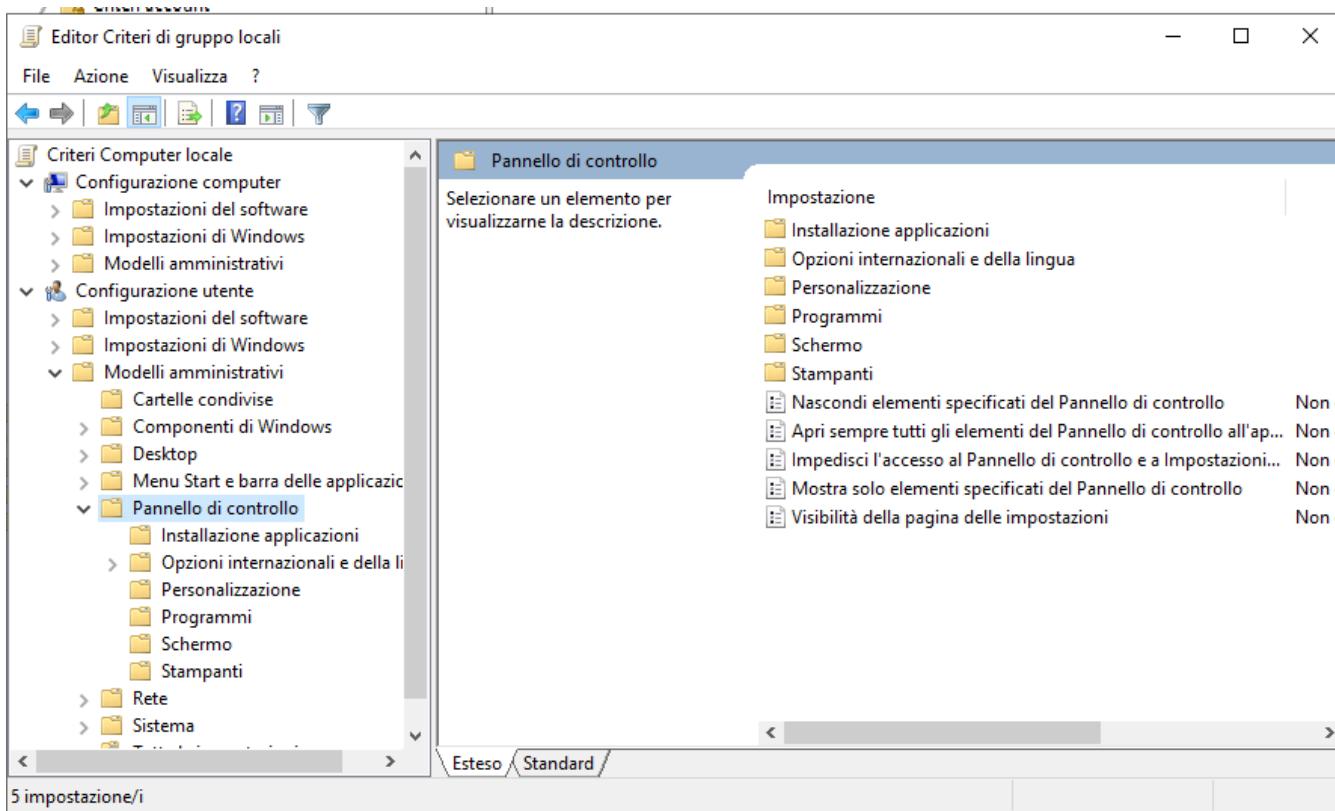
E riavvio il server per applicare i nuovi criteri

In alternativa è possibile usare **SRP (software restriction policies)** che permette di impostare il livello di sicurezza sulle applicazioni, come ad esempio “non limitato”, “non consentito” o “imparziale”. Quest’ultimo permette l’esecuzione senza privilegi di amministratore.

Per bloccare le modifiche, uso GPO e modifco i criteri di gruppo

Win + R, digito gpedit.msc

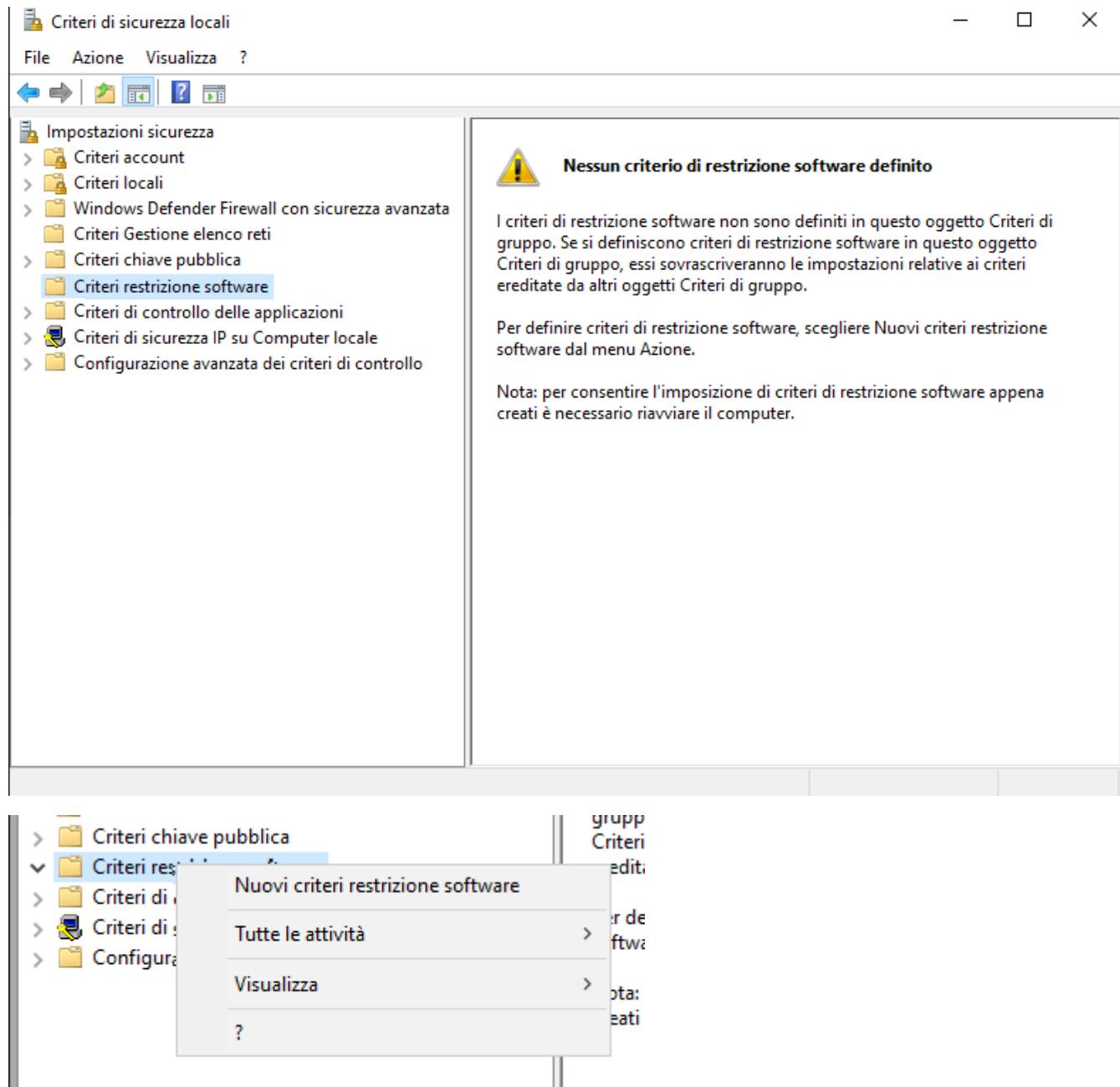
Per esempio, per l’utente CEO, vogliamo evitare che faccia danni alla sua macchina senza limitare quindi possiamo bloccare l’accesso al pannello di controllo e alle impostazioni di sistema



Possiamo anche impedire l'accesso ad altre risorse sensibili, come regedit, cmd, gestione dispositivi e altri.

Queste impostazioni si applicano a tutti gli utenti, esclusi gli amministratori

In alternativa, per una gestione più capillare dei permessi, possiamo usare secpol.msc



Criteri di sicurezza locali

File Azione Visualizza ?



- Impostazioni sicurezza
 - > Criteri account
 - > Criteri locali
 - > Windows Defender Firewall con sicurezza avanzata
 - Criteri Gestione elenco reti
 - Criteri chiave pubblica
 - > Criteri restrizione software
 - Livelli di sicurezza
 - Regole aggiuntive
 - > Criteri di controllo delle applicazioni
 - > Criteri di sicurezza IP su Computer locale
 - > Configurazione avanzata dei criteri di controllo

| Nome | Tipo | Livello di sicurezza |
|--------------|----------|----------------------|
| %HKEY_LOC... | Percorso | Senza restrizio... |
| %HKEY_LOC... | Percorso | Senza restrizio... |

Nuova regola certificato...

Nuova regola hash...

Nuova regola area rete...

Nuova regola percorso...

Tutte le attività >

Aggiorna

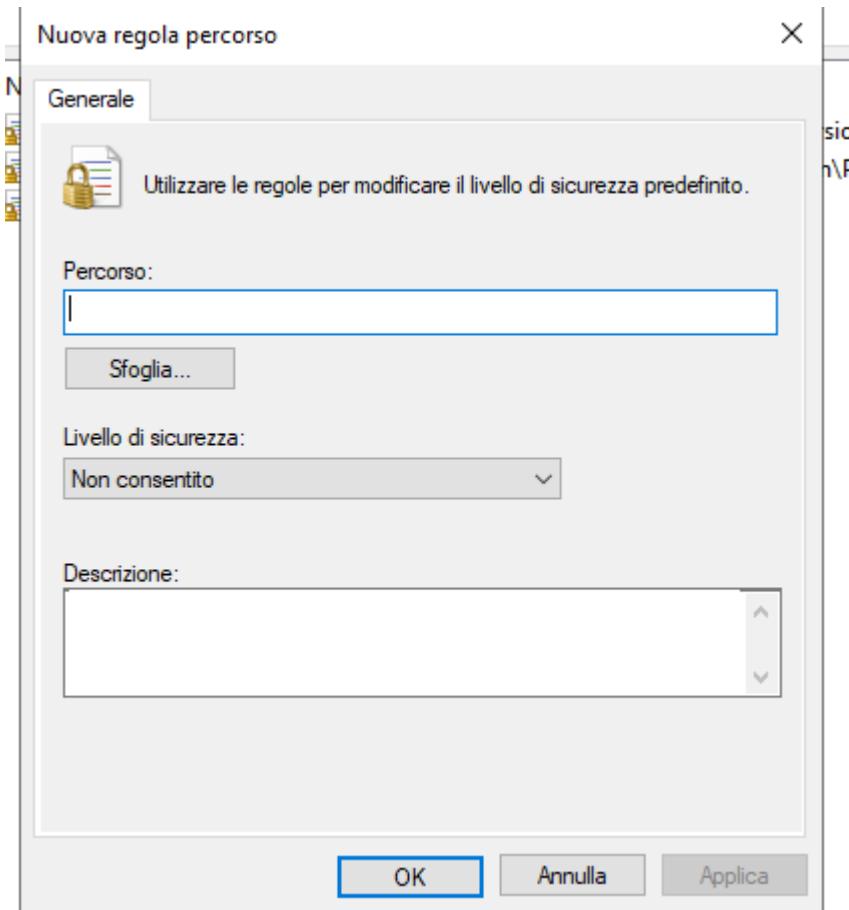
Esporta elenco...

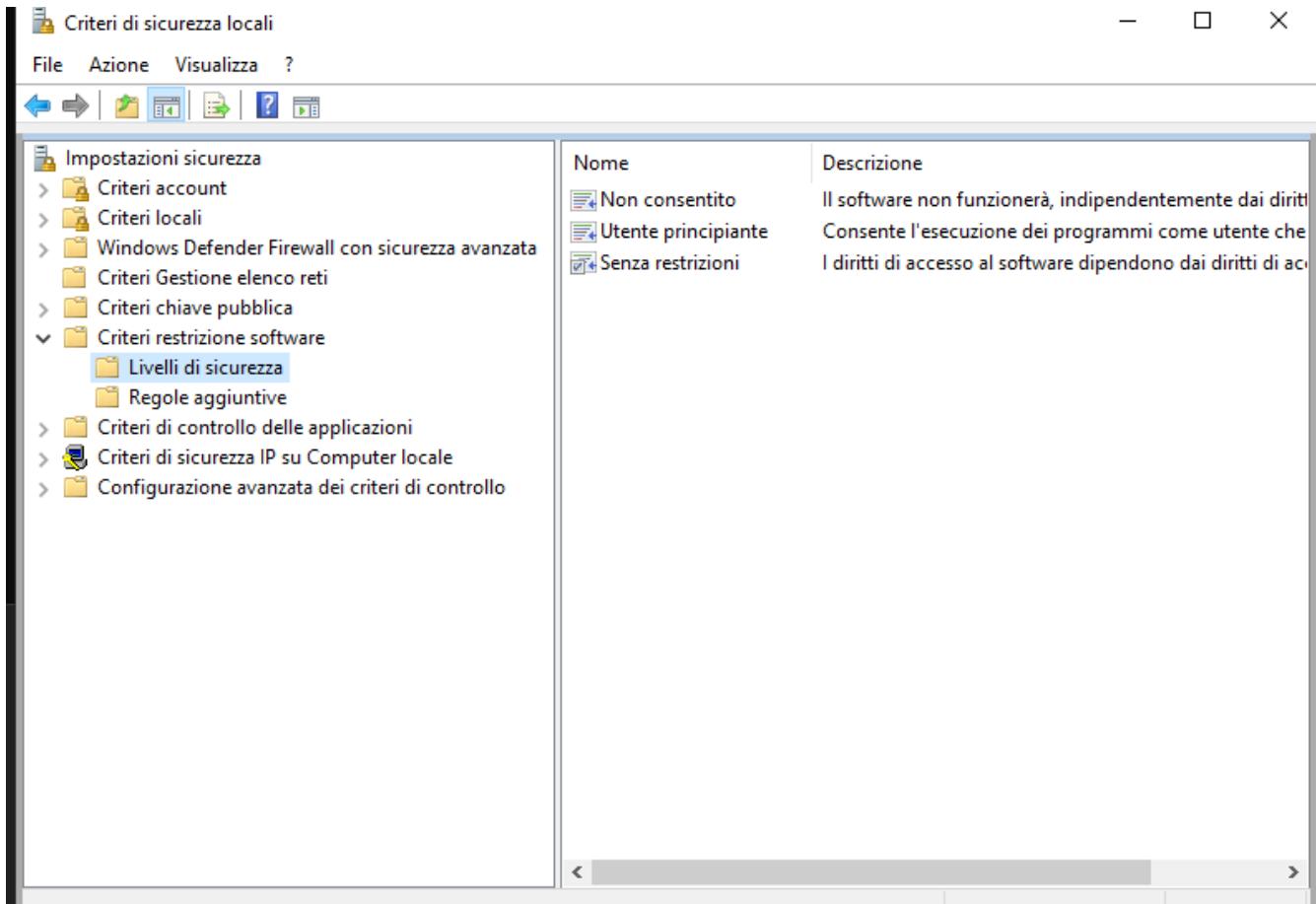
Visualizza >

Disponi icone >

Allinea icone

?





Nel caso di problemi, per riattivare l'accesso alle risorse di pannello di controllo all'utente administrator, possiamo fare così:

```
C:\Users\Administrator>reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v NoControlPanel /t REG_DWORD /d 0 /f
Operazione completata.

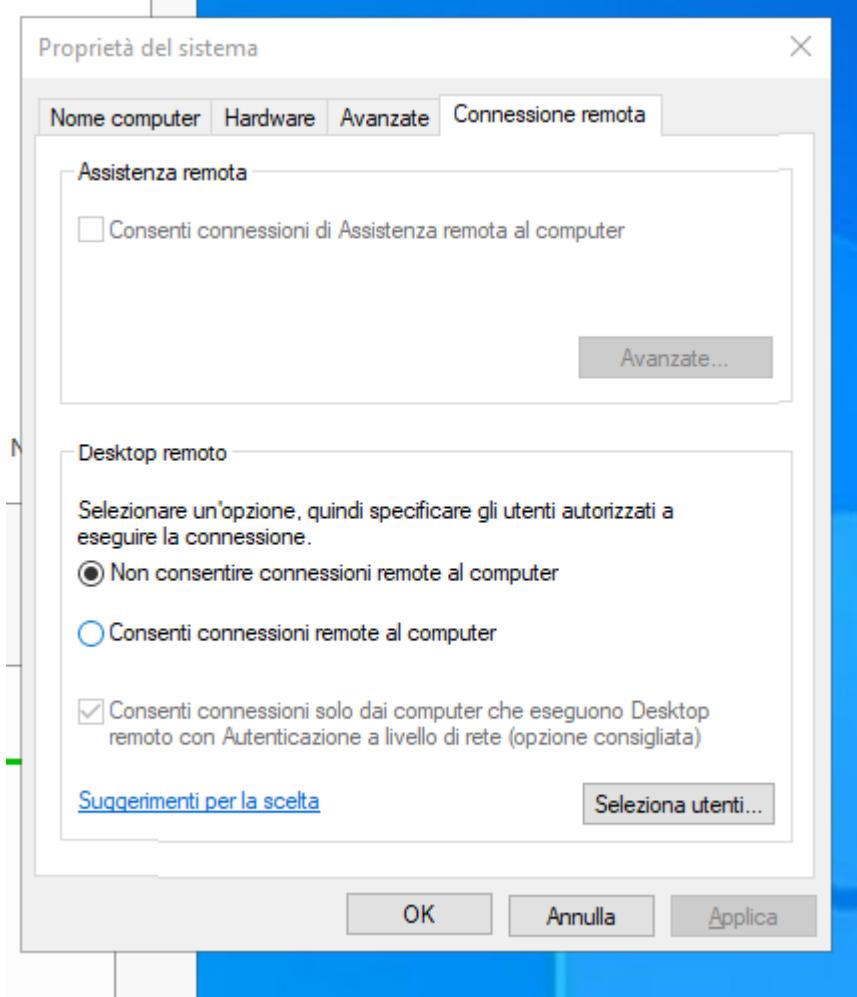
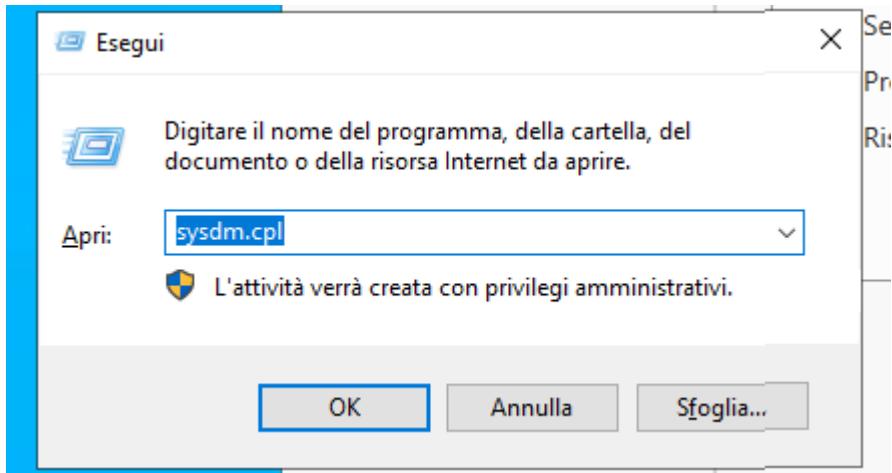
C:\Users\Administrator>reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v NoControlPanel /t REG_DWORD /d 0 /f
Operazione completata.

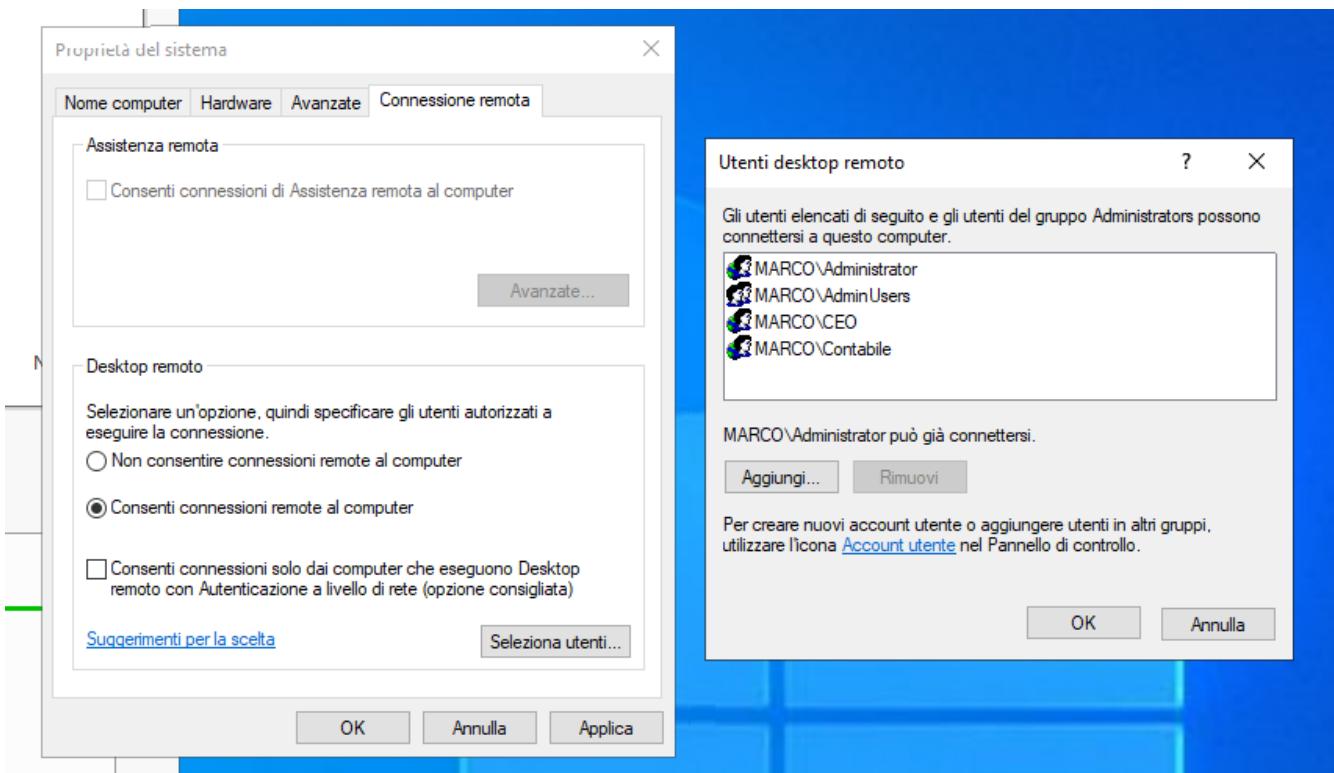
C:\Users\Administrator>gpupdate /force
Aggiornamento criteri in corso...

Aggiornamento dei criteri computer completato.
Aggiornamento dei criteri utente completato.

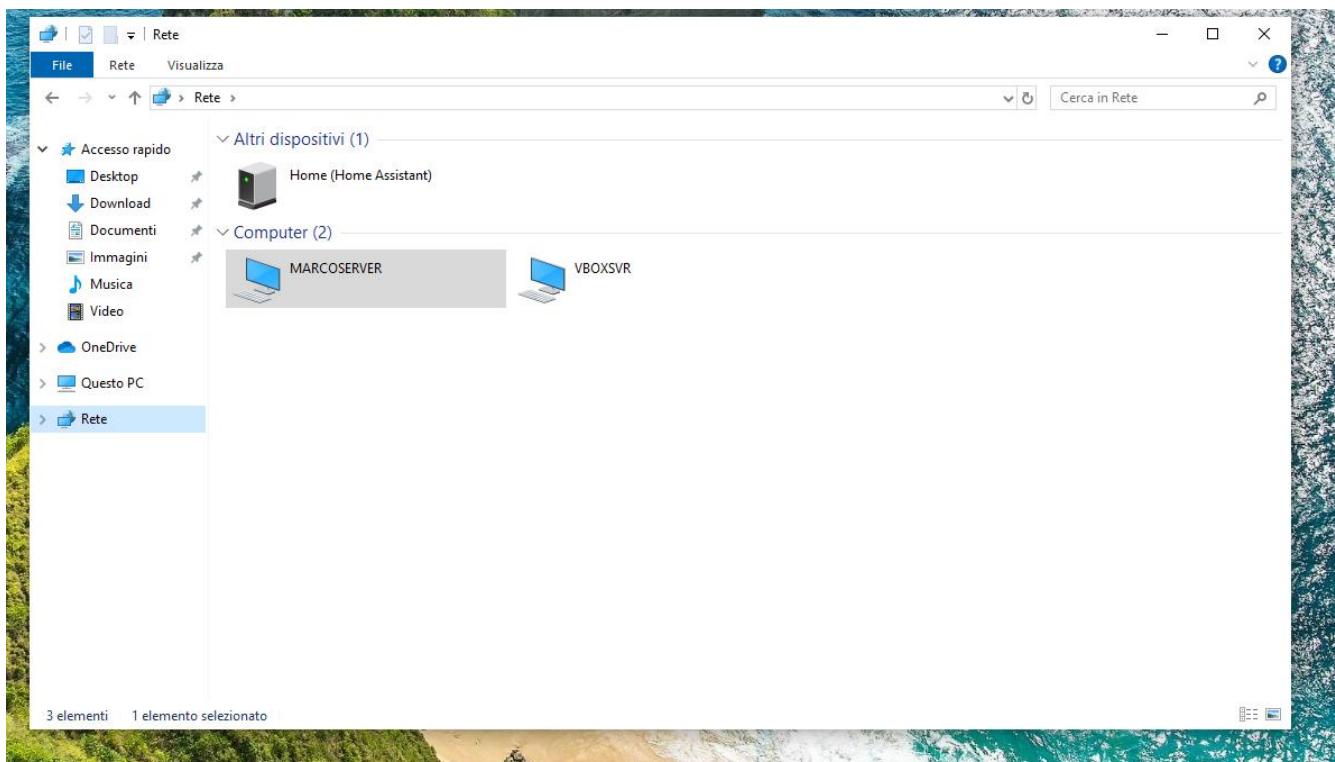
C:\Users\Administrator>shutdown -r -t 0
```

Per abilitare l'accesso remoto, usiamo sysdm.cpl





Entriamo ora nell'utente Segretario



Condividi Visualizza

Rete > MARCOSERVER

Condivisa

Condividi Visualizza

Rete > MARCOSERVER > Condivisa > Standard > Segreteria

| Nome | Ultima modifica | Tipo | Dimensione |
|--------------------------------|------------------|--------------------|------------|
| Nuovo documento di testo prova | 14/02/2025 16:23 | Documento di testo | 0 KB |

Sono riuscito a creare questo file

Faccio lo stesso per CEO

Vedo tutte le cartelle create per Standard:

| Nome | Ultima modifica |
|-----------------|------------------|
| Amministrazione | 14/02/2025 16:28 |
| Contabilità | 14/02/2025 15:01 |
| Segreteria | 14/02/2025 16:23 |

| C:\ > Rete > MARCOSERVER > Condivisa > Standard > Amministrazione | | | | |
|---|------|------------------|--------------------|------------|
| | Nome | Ultima modifica | Tipo | Dimensione |
| rapido | test | 14/02/2025 16:28 | Documento di testo | 0 KB |
| ad | | | | |
| enti | | | | |

Riusciamo a creare un file nella cartella Amministrazione, i permessi sono correttamente settati

Per testare se le regole di applocker funzionano correttamente torniamo sull'utente Segretario e proviamo ad aprire l'applicazione whitelistata

L'applicazione si apre correttamente. Proviamo ora ad aprire una che non è in whitelist

L'applicazione non si apre.

Lo stesso per il pannello di controllo

Verifichiamo ora che per un utente di amministrazione funzioni tutto correttamente

Il comportamento è come ci aspettavamo

Per collegarci in remoto possiamo usare pfsense e mettere le due macchine su reti diverse. Per mancanza di tempo, questa parte non verrà svolta