

Windows Server

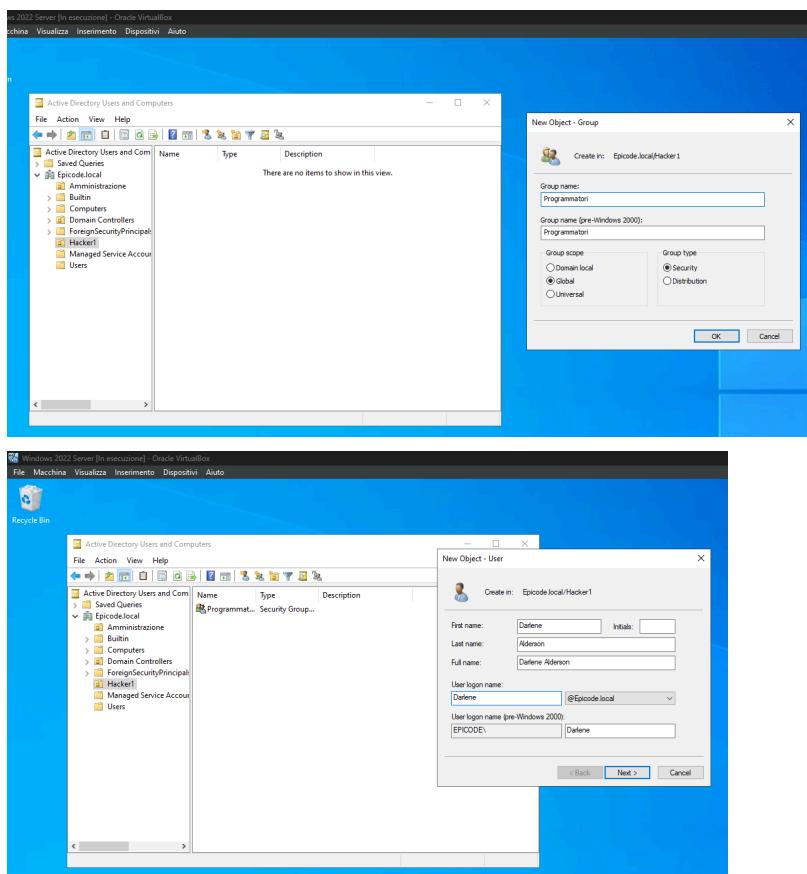
Per prima cosa ho creato i gruppi e utenti andando su Tools poi Active Directory Users and Computer poi negli OU creati(Amministrazione Hacker1) ho inserito in Amministrazione Elliot con il suo gruppo Amministratore e Darlene in Hacker1 con il gruppo programmatori

The image consists of three vertically stacked screenshots of the Windows Server Active Directory Users and Computers management console.

Screenshot 1: New Object - Group
This screenshot shows the "New Object - Group" dialog box. The "Create in:" dropdown is set to "Epicode.local/Amministrazione". The "Group name:" field contains "Amministratori". The "Group type" section has "Security" selected. The "Group scope" section has "Global" selected. Buttons for "OK" and "Cancel" are at the bottom.

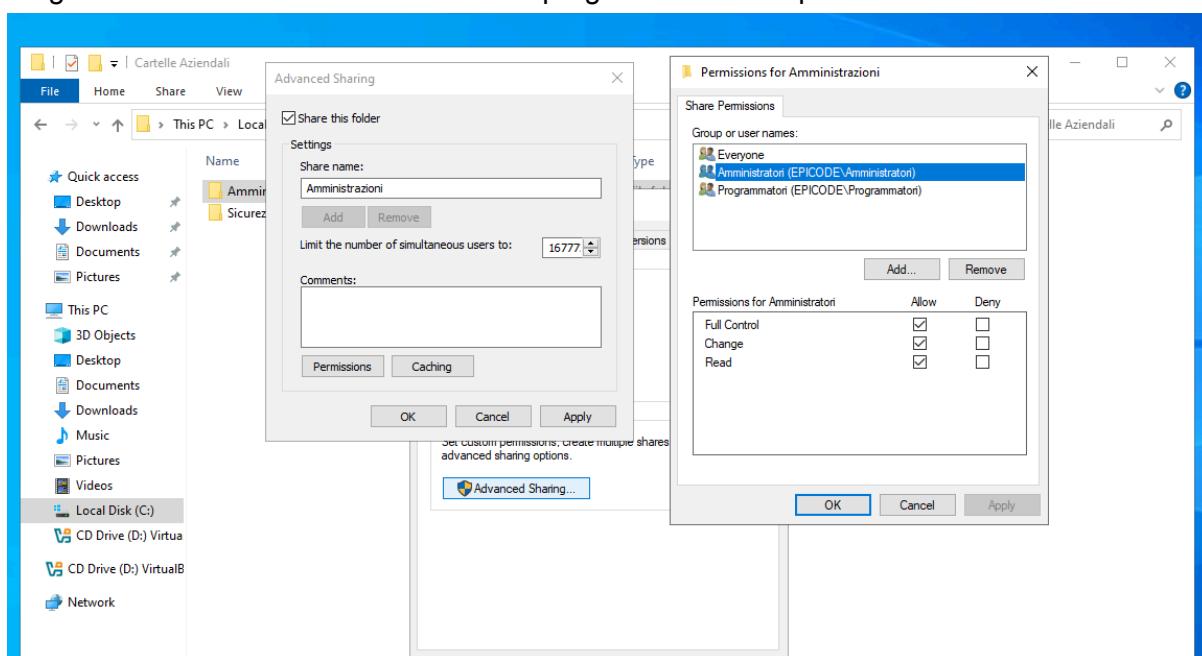
Screenshot 2: New Object - User
This screenshot shows the "New Object - User" dialog box. The "Create in:" dropdown is set to "Epicode.local/Amministrazione". The "First name:" field is "Elliot", "Last name:" is "Alderson", and "Full name:" is "Elliot Alderson". The "User logon name:" field is "Elliot" with a dropdown showing "@Epicode.local". The "User logon name (pre-Windows 2000):" fields show "EPICODE\" and "Elliot". Buttons for "< Back", "Next >", and "Cancel" are at the bottom.

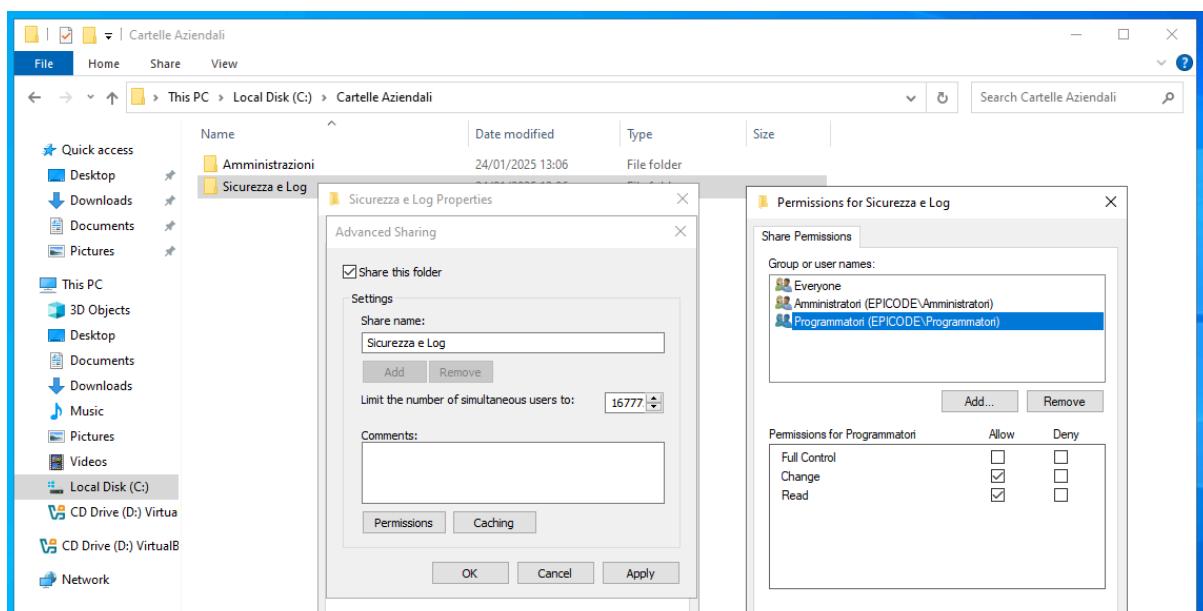
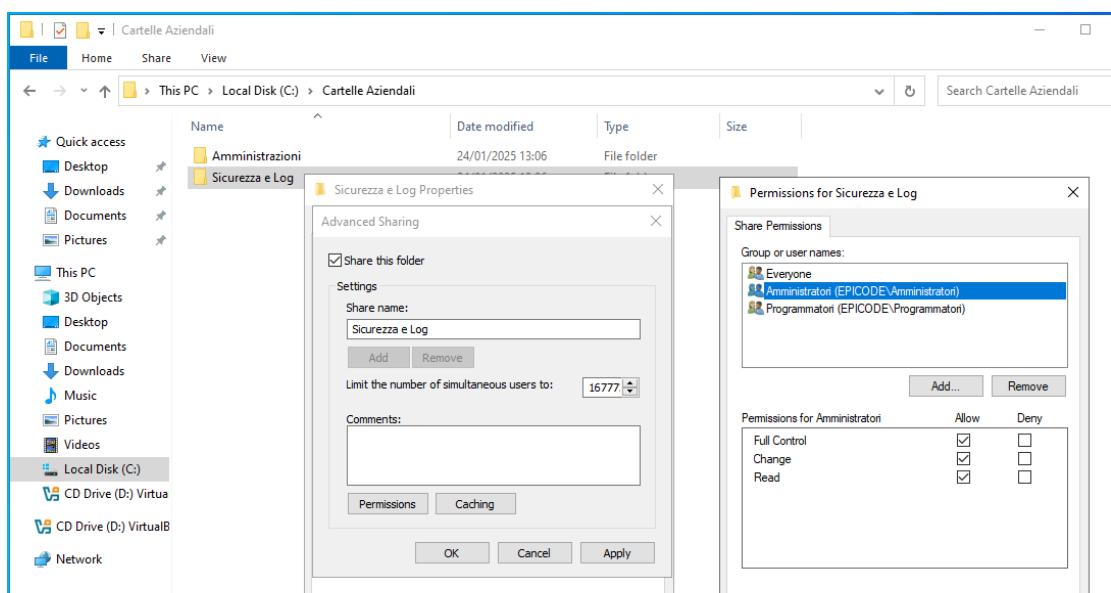
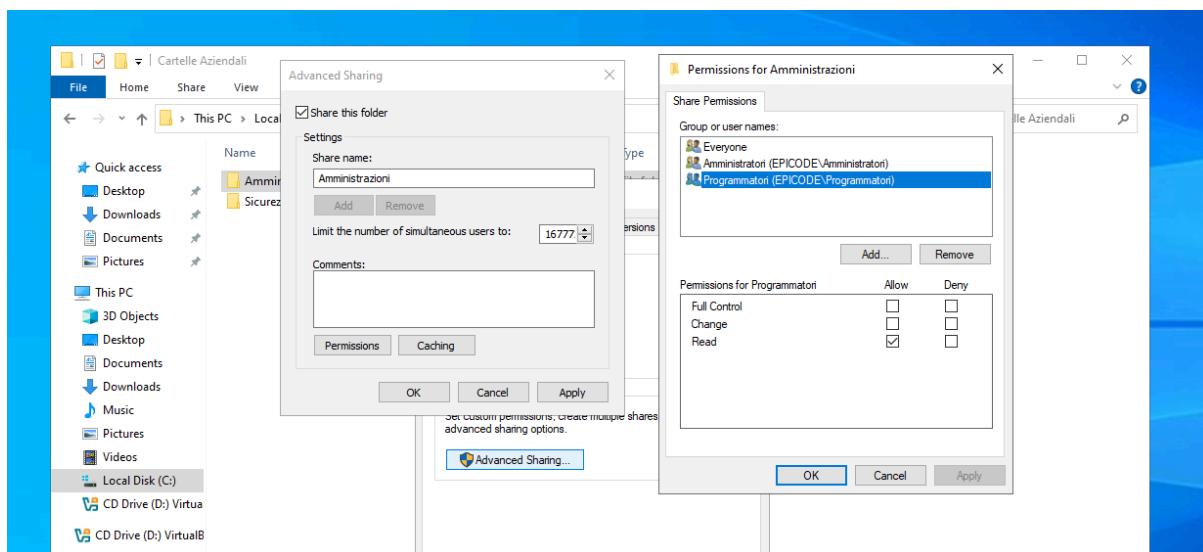
Screenshot 3: Active Directory Users and Computers
This screenshot shows the "Active Directory Users and Computers" main window. The left navigation pane shows an "Administrators" folder under "Epicode.local/Amministrazione". A "Members" tab is selected, showing the "Active Directory Domain Services Folder". A "Select Users, Contacts, Computers, Service Accounts, or Groups" dialog box is open over the main window, listing "Elliot" as a selected item. Buttons for "OK" and "Cancel" are at the bottom of the dialog.



Accesso ai file e alle cartelle:

Successivamente ho creato una cartella (Cartella aziendale) dove all'interno ho messo due sotto cartelle (Amministrazioni, Sicurezza e Log) successivamente premendo il tasto destro andando Proprietà poi su Sharing e Advanced Sharing ho inserito i permessi nella quale in amministrazioni il gruppo Amministratori hanno il Full Control mentre il gruppo Programmatori il Read in modo tale che i programmatori non possano modificare nulla





Esecuzione di programmi specifici:

Premendo Win+R e inserendo gpmc.msc

Crea un nuovo GPO:

- In Group Policy Management, crea un nuovo GPO chiamato "Limitazioni Programmatori".

Imposta la lista di programmi consentiti:

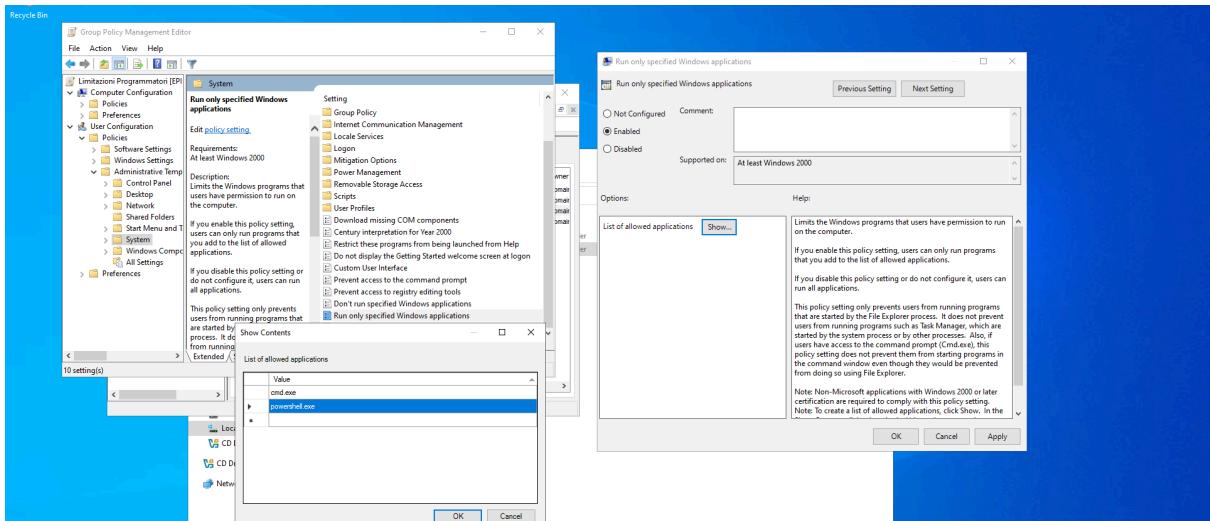
- Vai su:Configurazione Utente > Criteri > Modelli Amministrativi > Sistema.
- Abilita Esegui solo applicazioni Windows specifiche e aggiungi:
 - cmd.exe
 - powershell.exe.

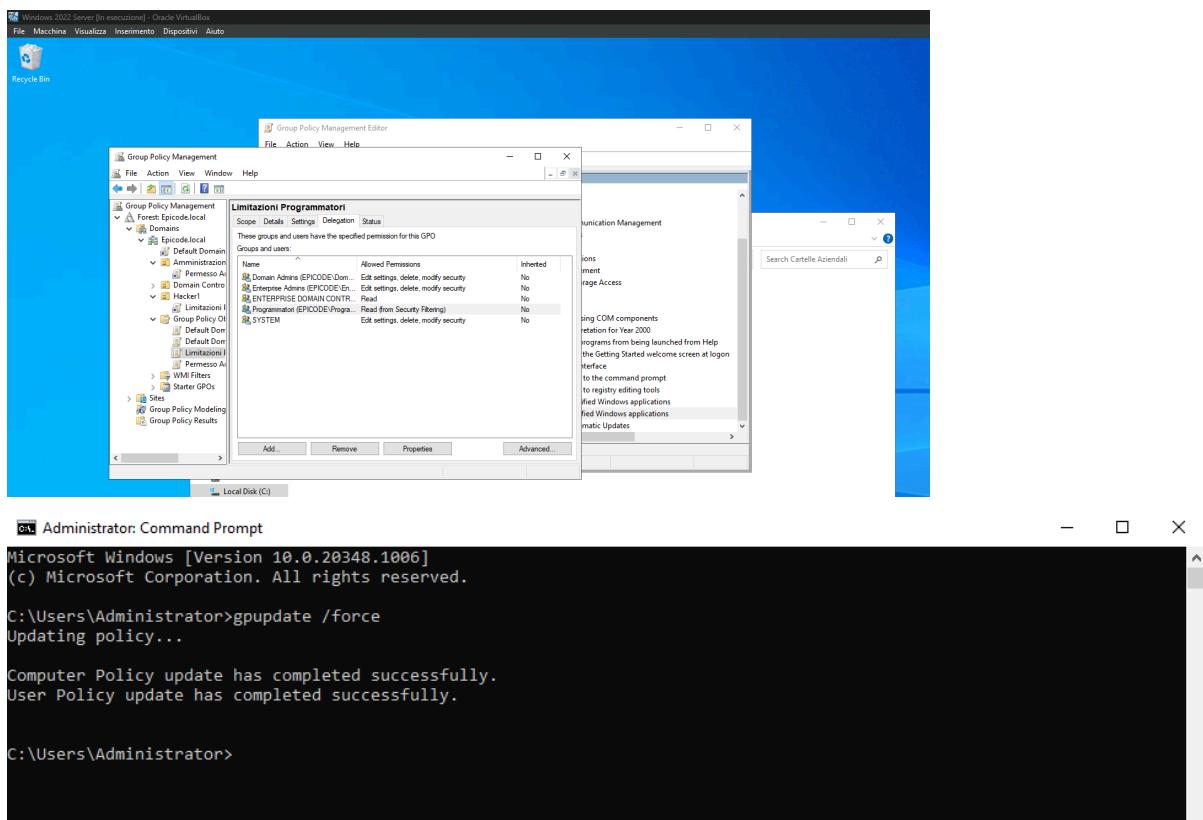
Applica il GPO:

- Collega il GPO alla OU o gruppo "Programmatori".

Aggiorna i criteri:

- Esegui il comando sul cmd `gpupdate /force` per applicare immediatamente le modifiche.





Modifiche alle impostazioni di sistema:

Sempre nella stessa scheda di prima con ma con un GPO diverso
GPO:

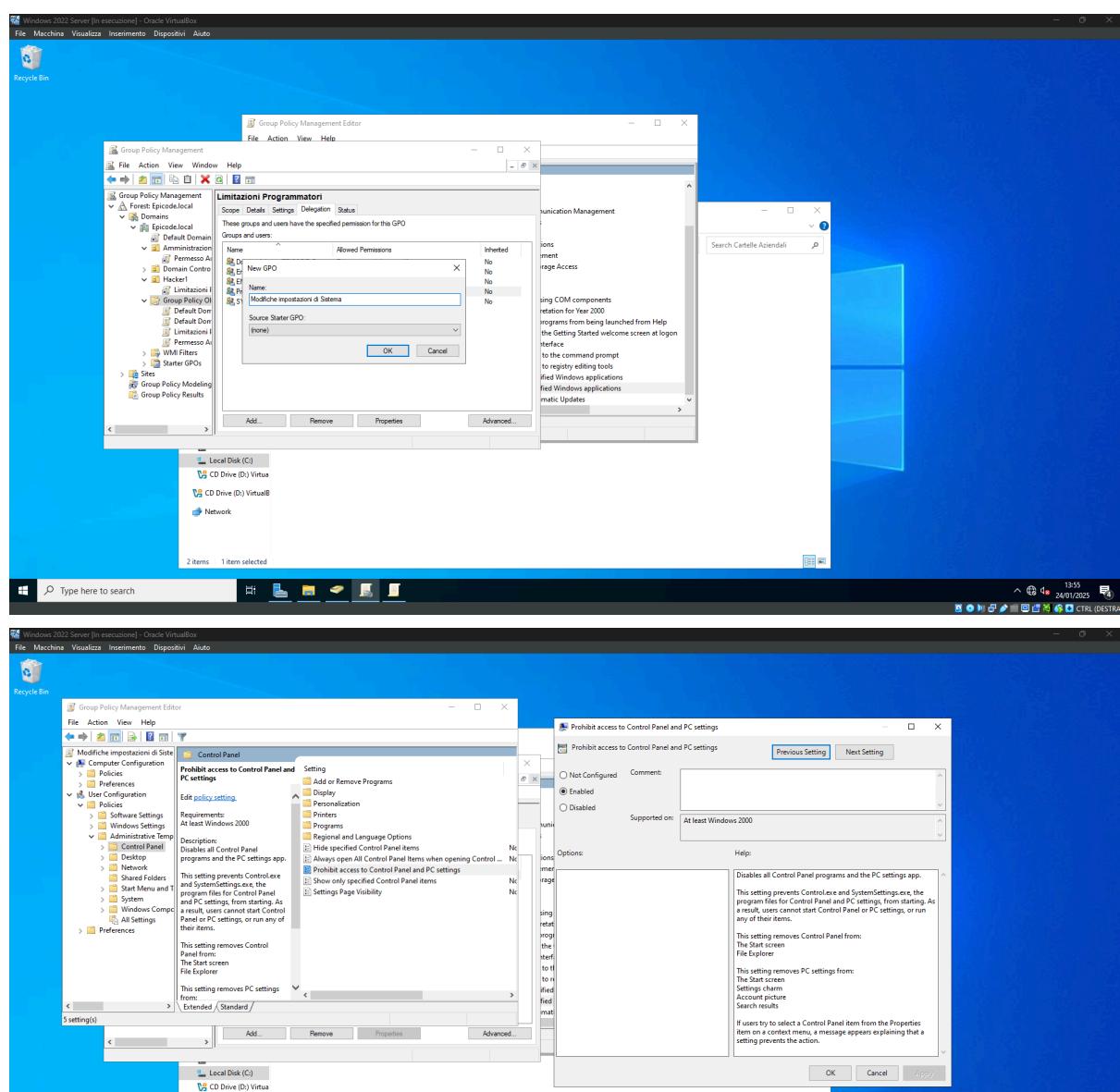
- Vai:
User Configuration > Policies > Administrative Templates > System.

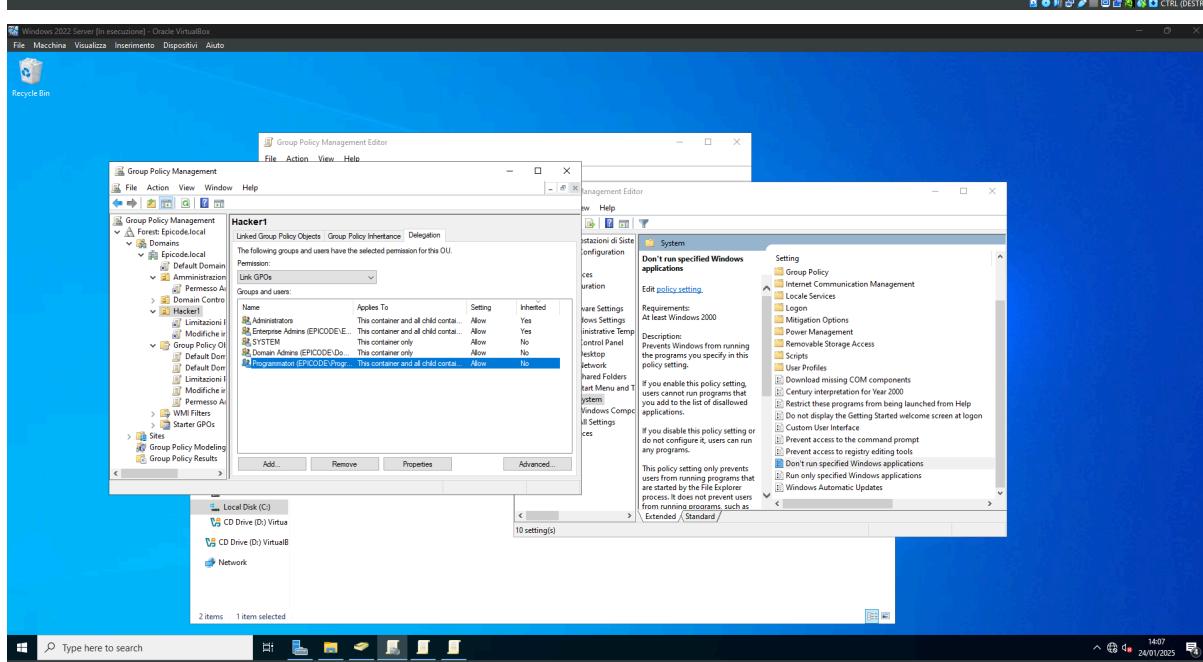
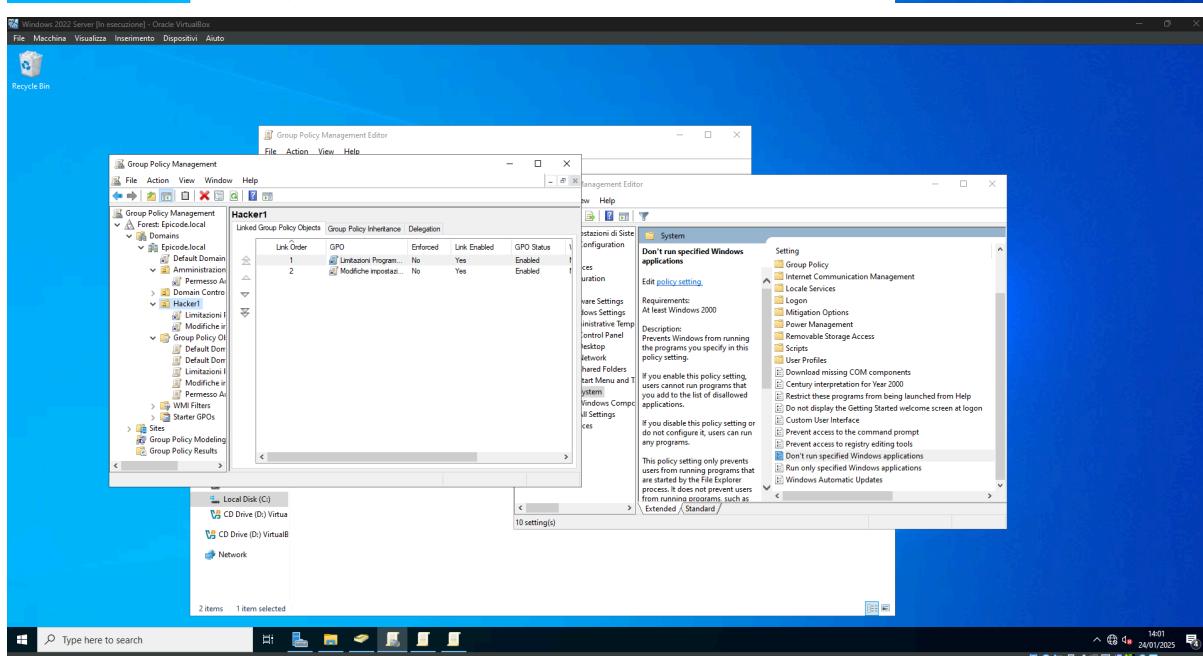
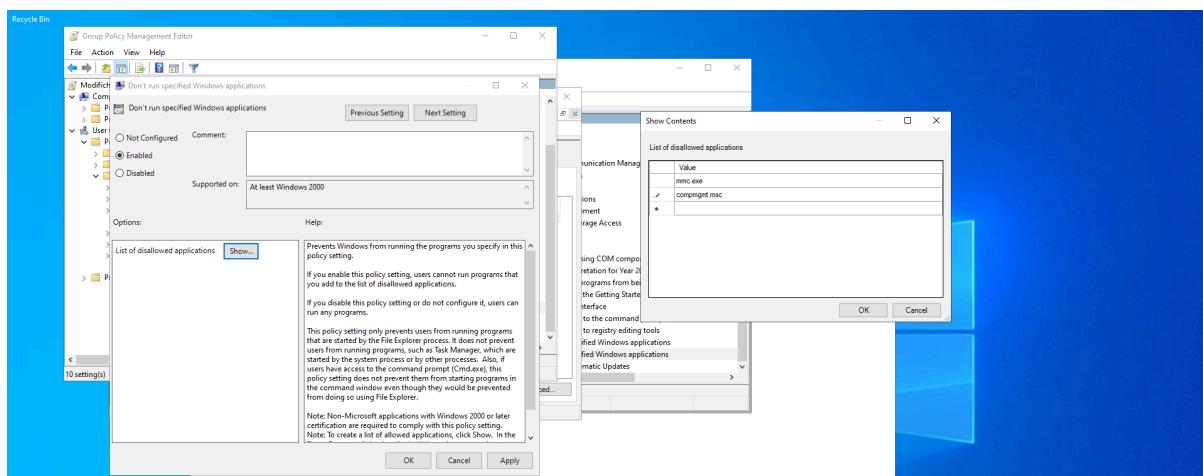
Enable e configura:

- Don't run specified Windows applications.

Blocco di applicazioni di Windows::

- mmc.exe (Microsoft Management Console)
- compmgmt.msc (Computer Management)





Accesso remoto al server:

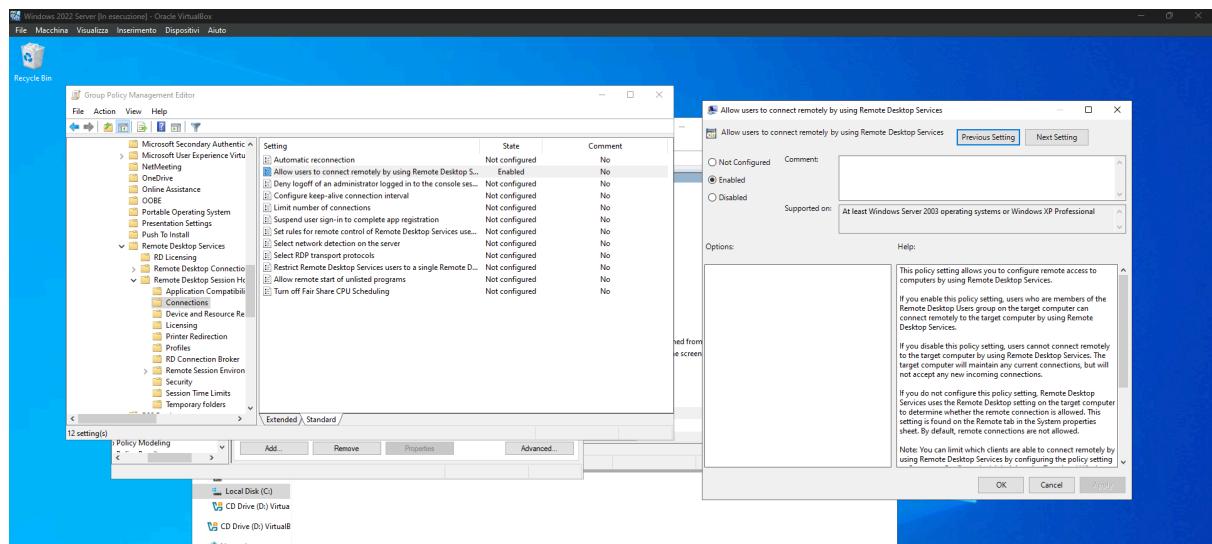
Sempre nella stessa scheda ho aggiunto un GPO e

Imposta la policy per l'accesso remoto:

- Vai su:
Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections.
- Abilita l'opzione Allow users to connect remotely using Remote Desktop Services.

Limitare l'accesso remoto agli Amministratori:

- Vai su:
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment.
- Trova l'opzione Allow log on through Remote Desktop Services.
- Aggiungi il gruppo Amministratori dalla OU Amministrazione.
- Fai clic su Add User or Group, digita il nome del gruppo Amministratori e premi OK.
- Poi andando nelle impostazioni ho abilitato il Remote Desktop aggiungendo il gruppo Amministratori



Windows 2022 Server [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimenti Dispositivi Auto

Recycle Bin

Group Policy Management Editor

File Action View Window Help

Accesso Remoto per Amministratori

Scope Details Settings Delegation

These groups and users have the specified permission for this GPO

Groups and users	Mapped Permissions	Inherited
Authenticated Users	Edit settings, delete, modify security	No
Domain Admins (EPICODE\Dom...)	Edit settings, delete, modify security	No
Enterprise Admins (EPICODE\En...)	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTRO... (SYSTEM)	Read	No
	Edit settings, delete, modify security	No

Add Remove Properties Advanced...

Local Disk (C) CD Drive (D) Virtus

Group Policy Management Editor

File Action View Help

Accesso Remoto per Amministratori [EPICODE\Dom...]

Policy Policy Setting

- Computer Configuration
 - Policies
 - Windows Settings
 - Security Settings
 - Local Policies
 - User Rights Assignment
 - Audit Policy
 - Change password time
 - Create a file
 - Create a logon script
 - Create a token object
 - Create a global object
 - Create permanent shared objects
 - Create symbolic links
 - Debug programs
 - Deny access to this computer from the network
 - Network List Manager Policies
 - Wireless Network (IEEE 802.11) I
 - Public Key Policies
 - Software Restriction Policies
 - Security Options
 - Event Log
 - Restricted Groups
 - System Services
 - Registry
 - File Systems
 - Network
 - Windows Defender Firewall with
 - Windows Update

Verifiche effettuate:

Le prime due verifiche effettuate sono state effettuate con l'account Darlene ovvero il gruppo Programmatori e da come si può vedere ha accesso alla modifica della cartella Amministrazione e neanche al Remote Desktop, per quanto riguarda l'ultima verifica è stata effettuata dall'utente Elliot nel gruppo Amministratori è da come si può vedere ha effettuato il Remote Desktop

