Server Security

Objective: To enhance Windows Server 2022 security by disabling guest and local administrator's accounts, restricting remote access, configuring account lockout policies, and disabling unnecessary services to protect against cyber threats and ensure secure operations

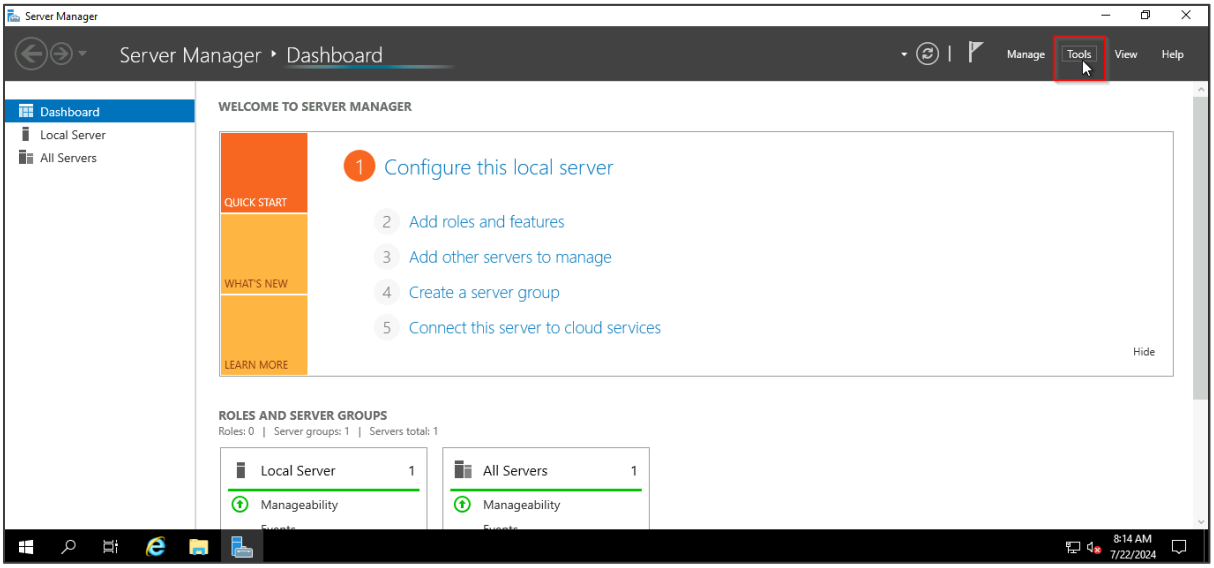
Steps to be followed:

1. Disable guest user accounts
2. Disable the local administrator account
3. Create a new, unique administrator account
4. Restrict remote access
5. Configure account lockout policy per best practices
6. Disable any unnecessary service

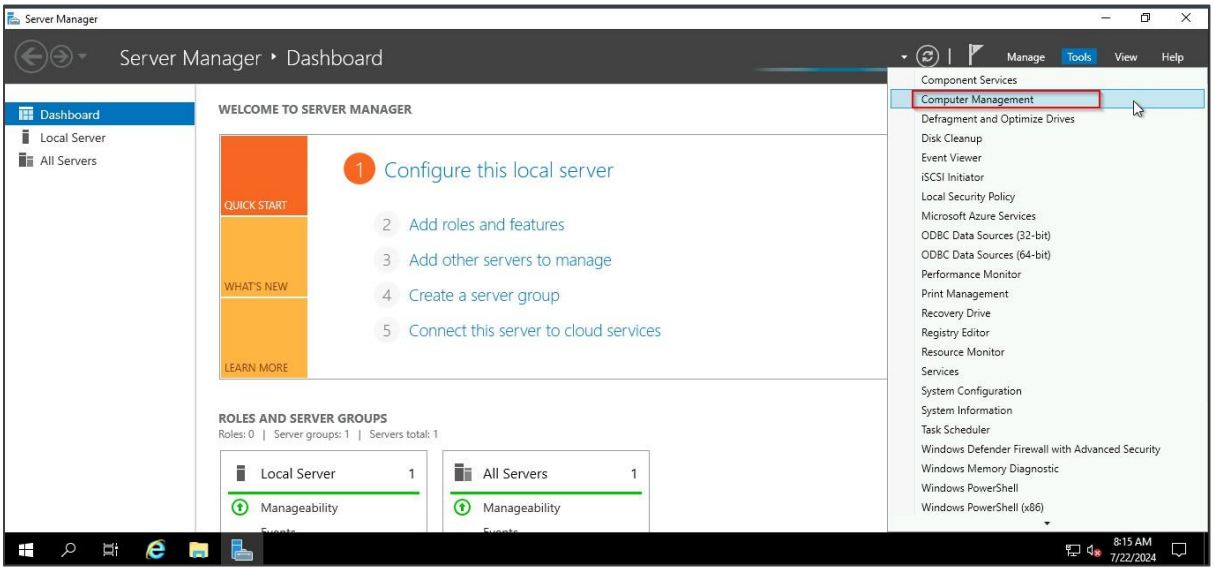
Step 1: Disable guest user accounts

1.1 Open the **Server Manager** by searching for it in the **Start** menu

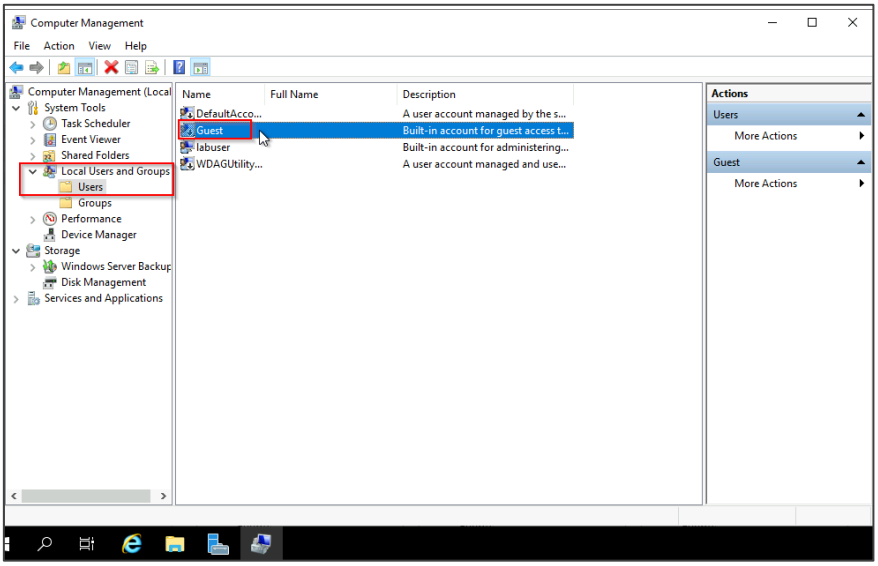
1.2 Click on the **Tools** option in the menu bar



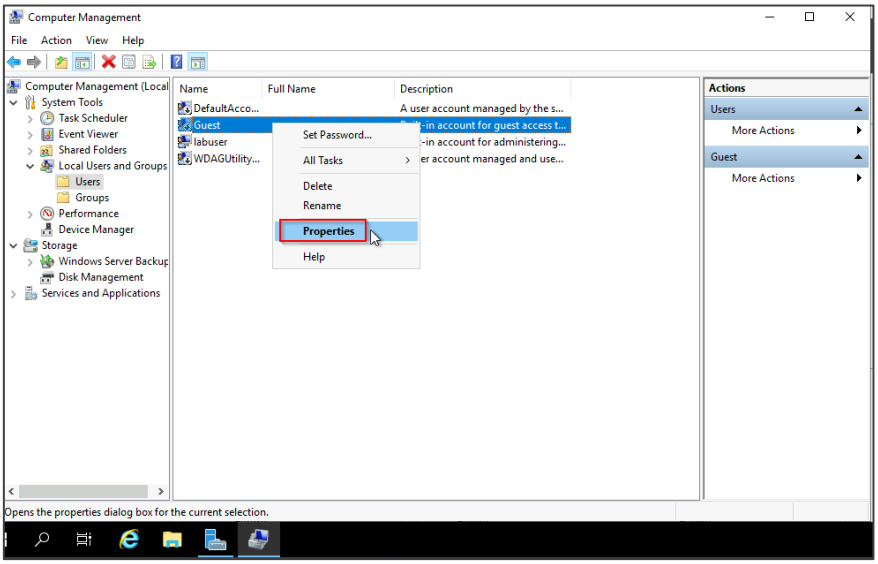
1.3 Click on **Computer Management** from the drop-down menu



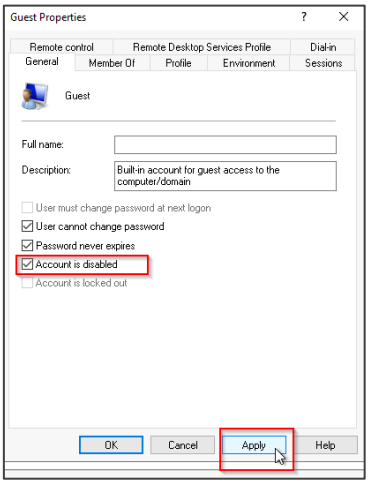
1.4 Click on **Local Users and Groups** and then select **Users**



1.5 Click on **Guest** and then select the **Properties** option

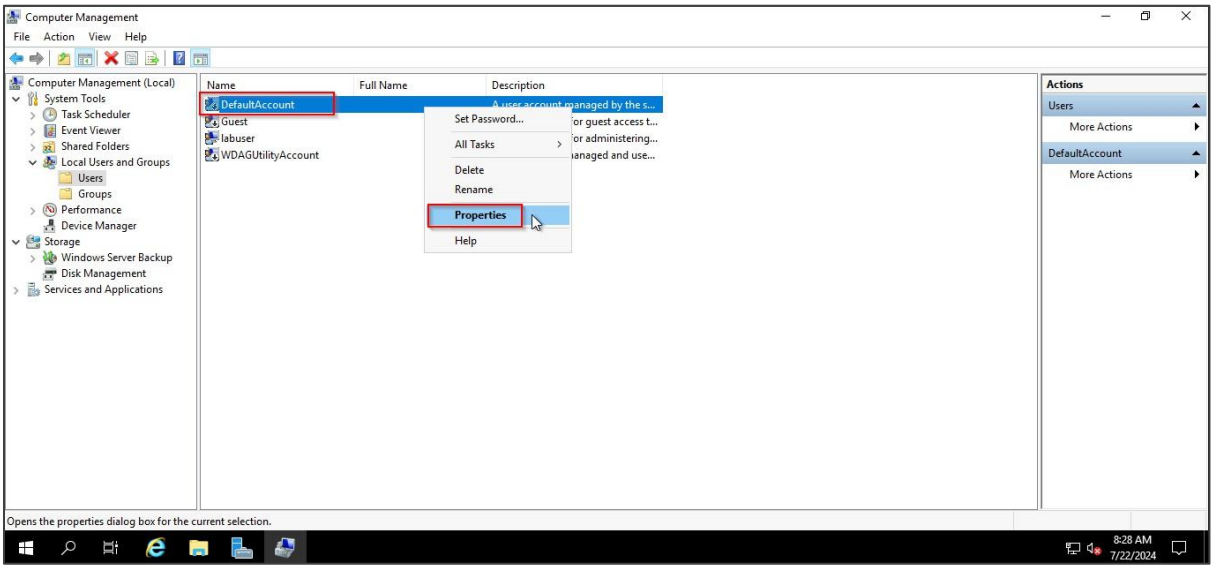


1.6 Disable the **Guest** user by selecting the **Account is disabled** option and save the changes by clicking **Apply** and **OK**

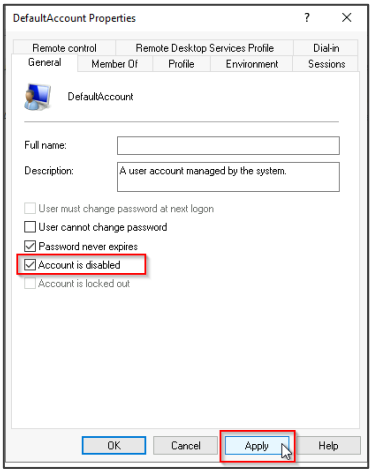


Step 2: Disable the local administrator account

2.1 Right-click on the **DefaultAccount** and select **Properties**

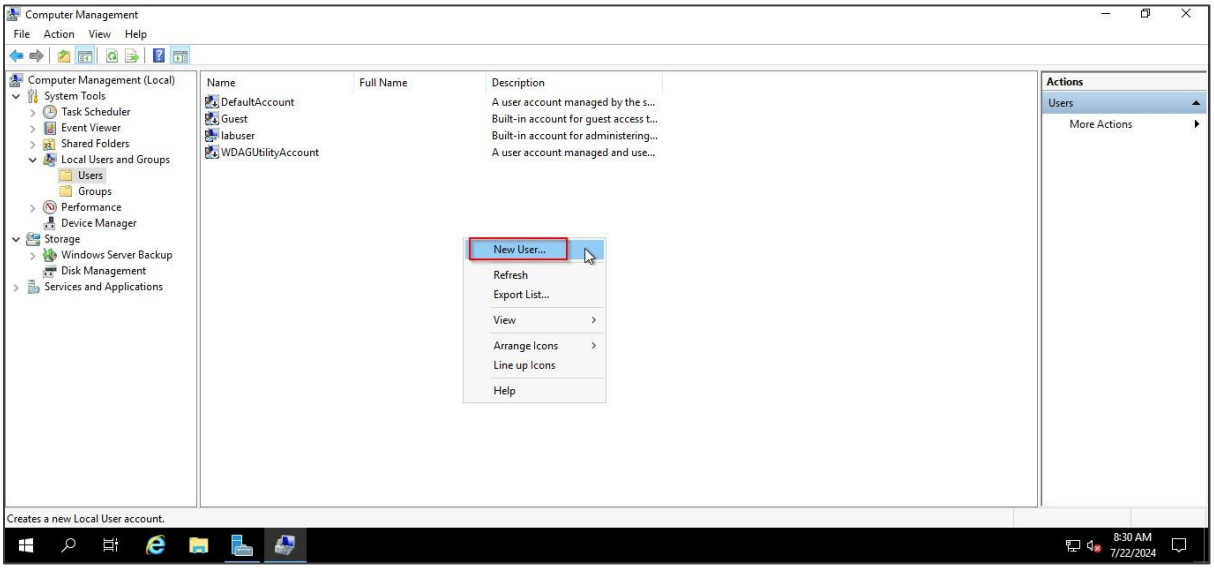


2.2 Select the **Account is disabled** option and save the changes by clicking on **Apply** and **OK**

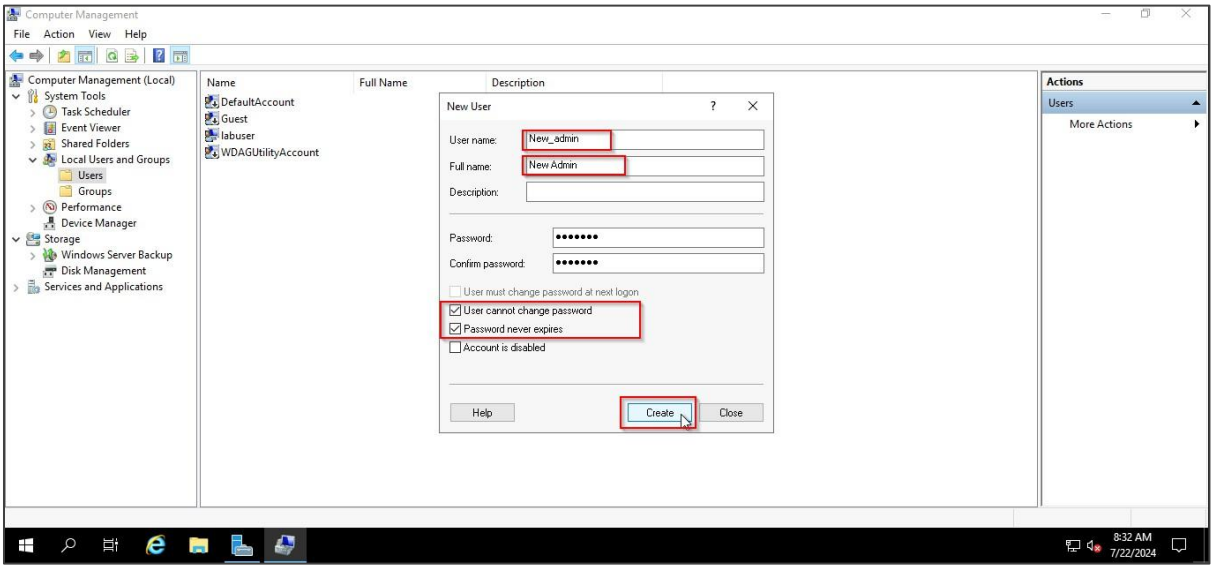


Step 3: Create a new, unique administrator account

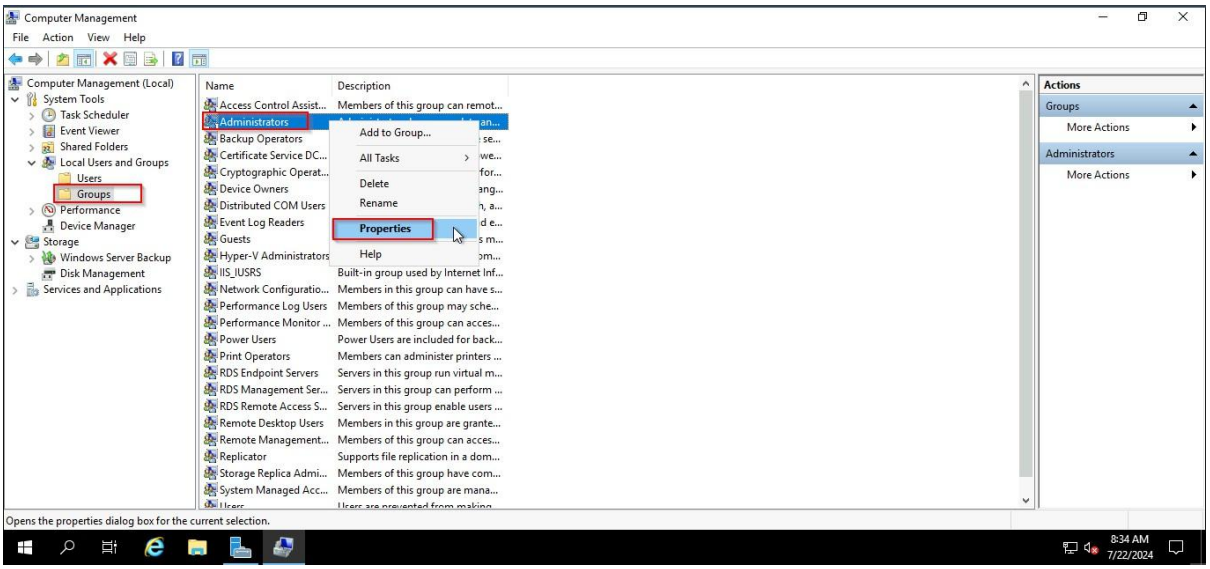
3.1 Right-click in the **Computer Management** window and select **New User** to create a new administrator user



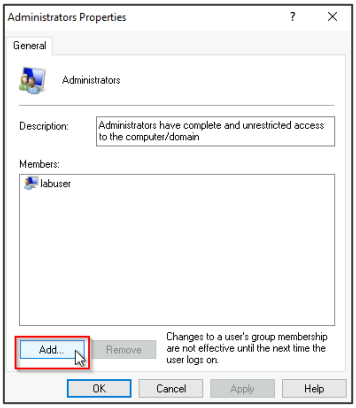
3.2 Enter the **User name** as **New_admin**, the **Full name** as **New Admin**, a password of your choice, and check the boxes as shown below and click on **Create**



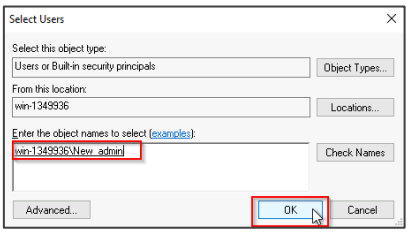
3.3 Click on **Groups**, right-click on **Administrators**, and then select **Properties**



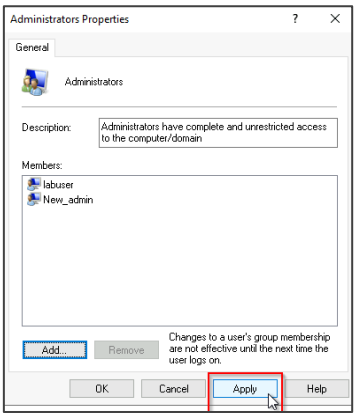
3.4 Click on **Add**



3.5 Enter the **New_admin** user to add it to the administrator's group and click **OK**

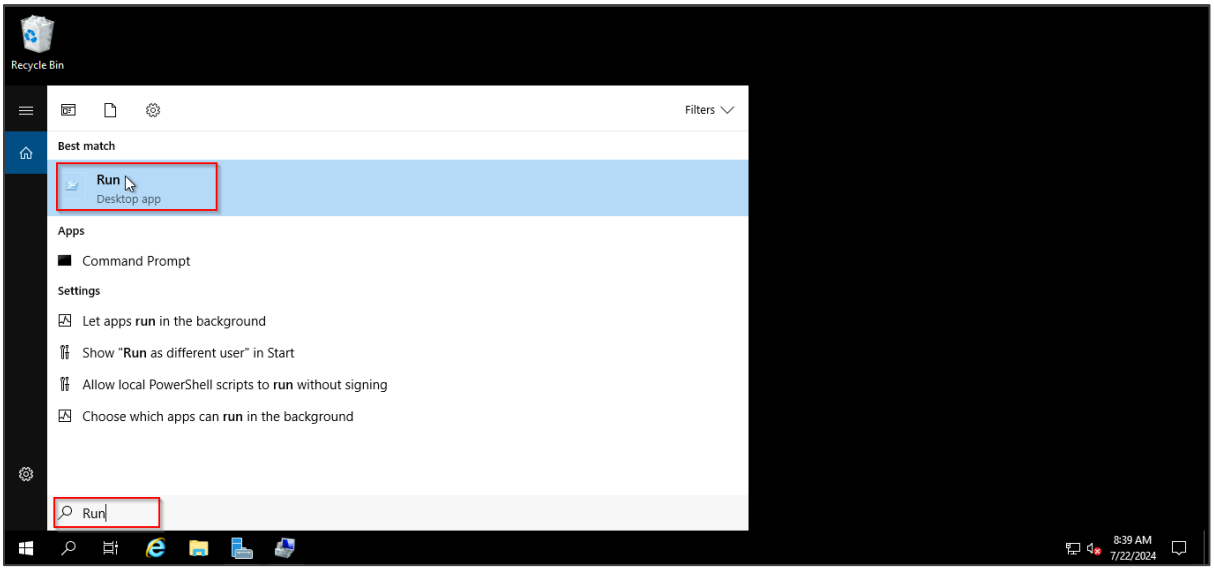


3.6 Further, click on **Apply** and **OK**

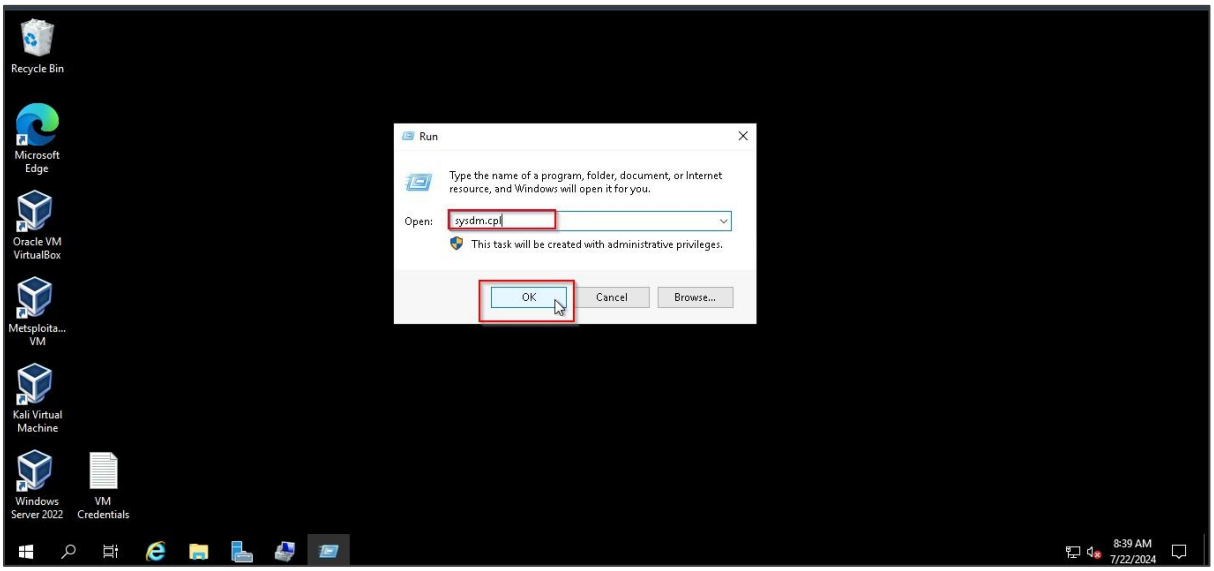


Step 4: Restrict remote access

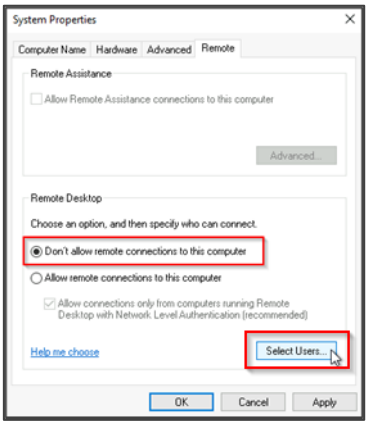
4.1 Type **Run** in the Windows search and open the **Run** app



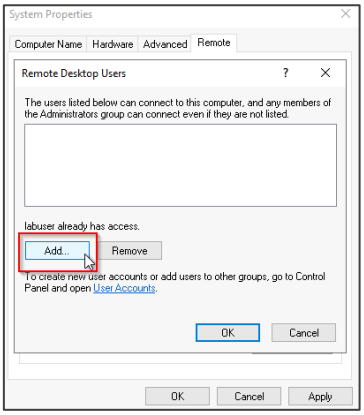
4.2 Enter **sysdm.cpl** in the **Open** field and click **OK**



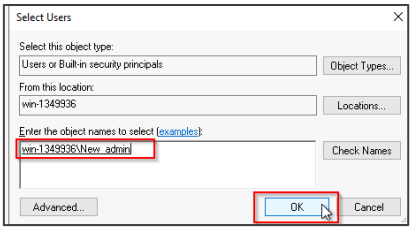
4.3 Select **Don’t allow remote connections to this computer**, and click on **Select Users**



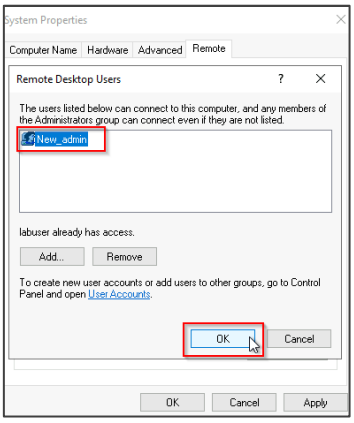
4.4 Click on the **Add** button to add the new administrator created earlier



4.5 Enter the object name as **New_admin** and click on **OK**

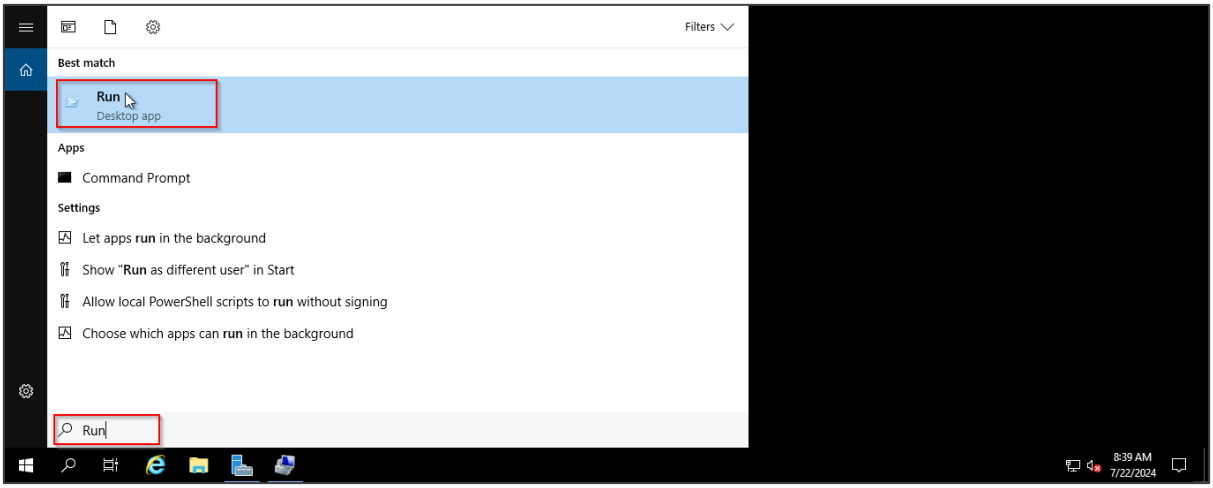


4.6 Click on **OK** to confirm the remote connection

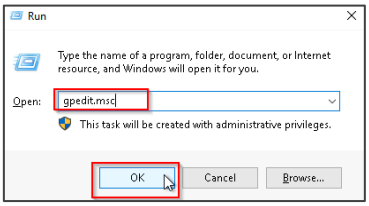


Step 5: Configure account lockout policy per best practices

5.1 Type **Run** in the Windows search and open the **Run** app

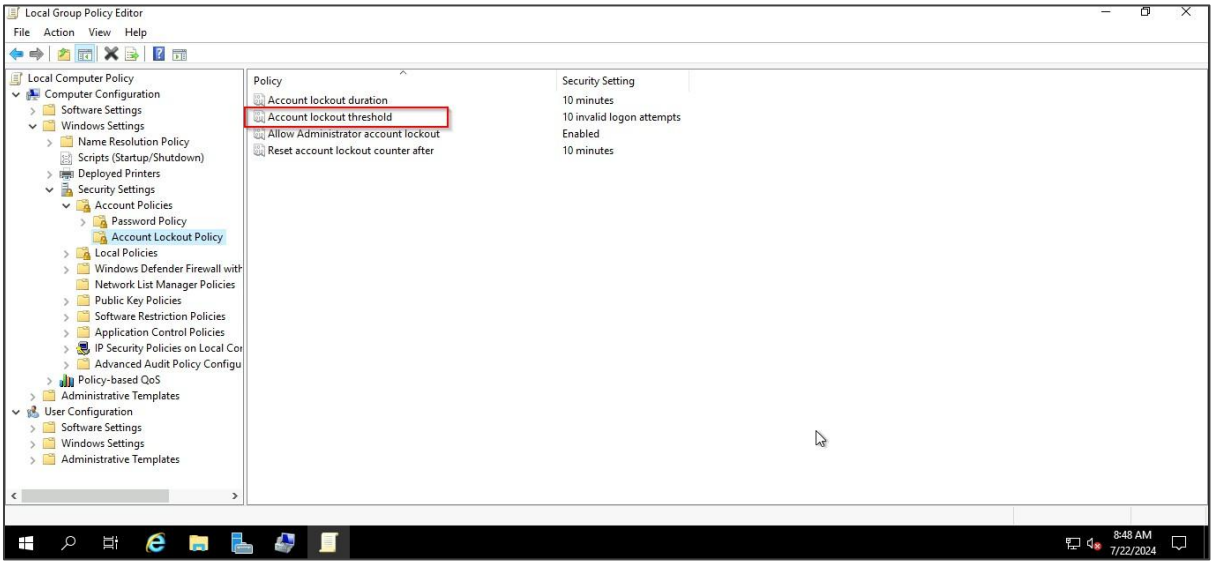


5.2 Type **gpedit.msc** in the **Open** Field and click **OK**

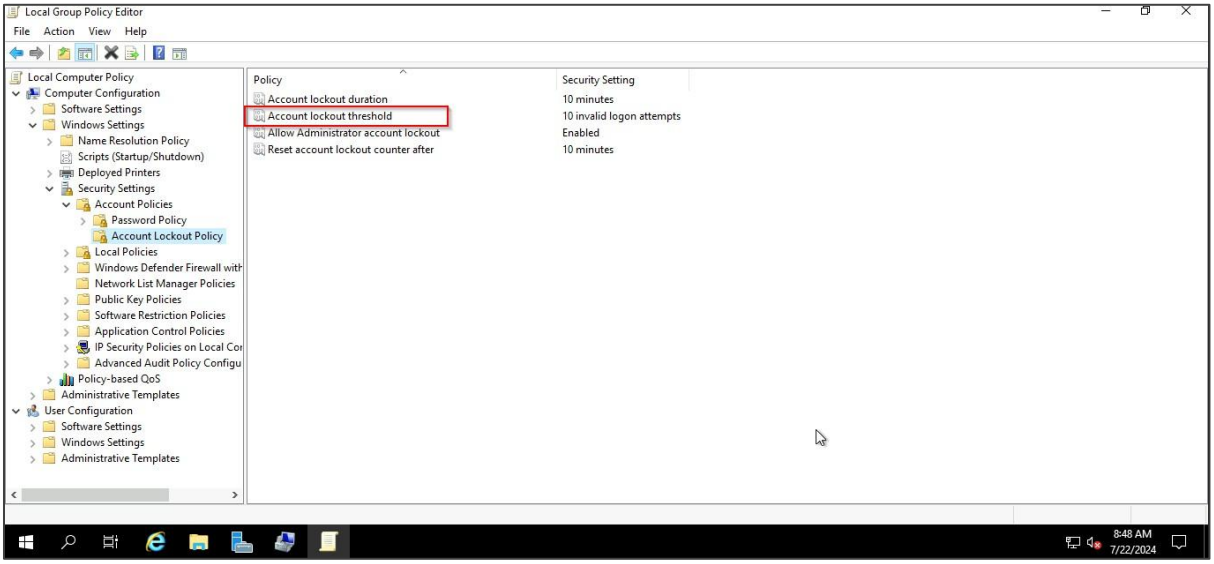


5.3 In the Local Group Policy Editor window, navigate to **Computer Configuration**

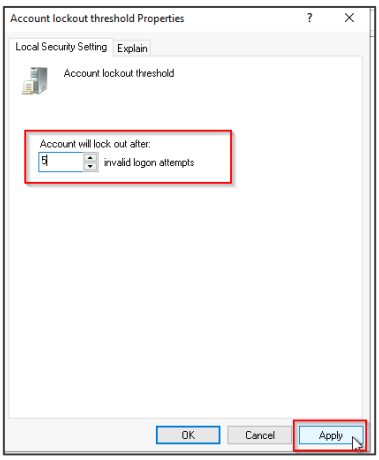
5.4 Navigate to **Computer Configuration**, then to **Windows Settings**, followed by **Security Settings**, then select **Account Policies**, and finally, **Account Lockout Policy**



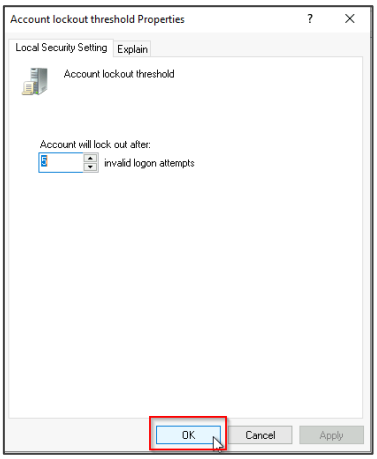
5.5 Under **Account Lockout Policy**, click on **Account lockout threshold**

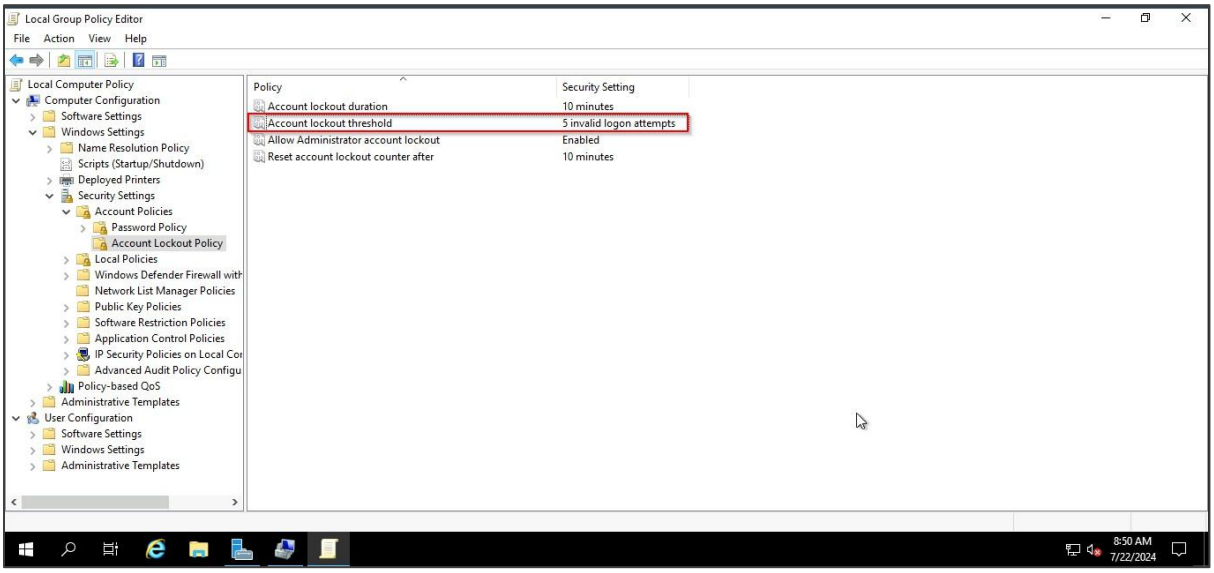


5.6 In the **Account lockout threshold**, change the login attempts to **5** and click on **Apply**



5.7 Further, click on **OK**

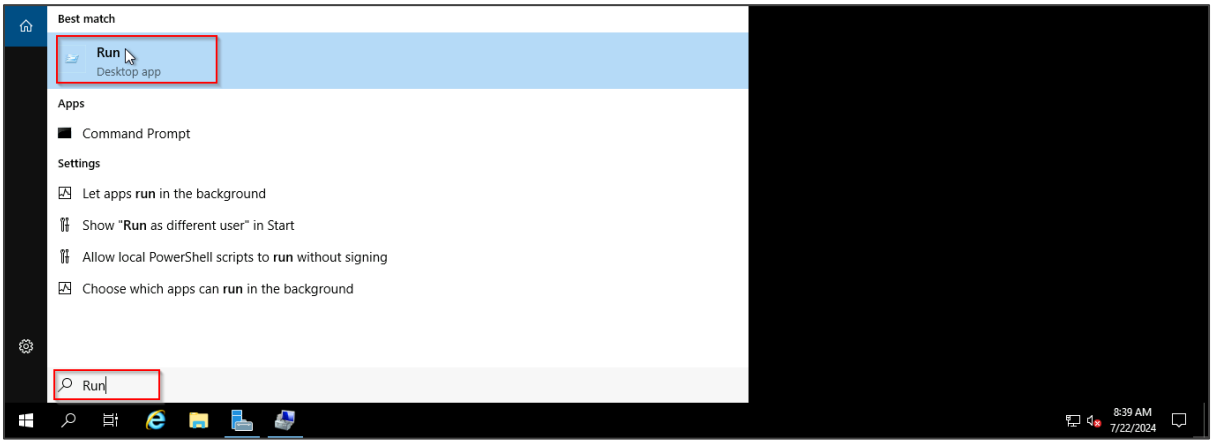




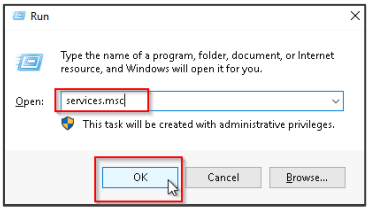
The login attempts are changed successfully.

Step 6: Disable any unnecessary service

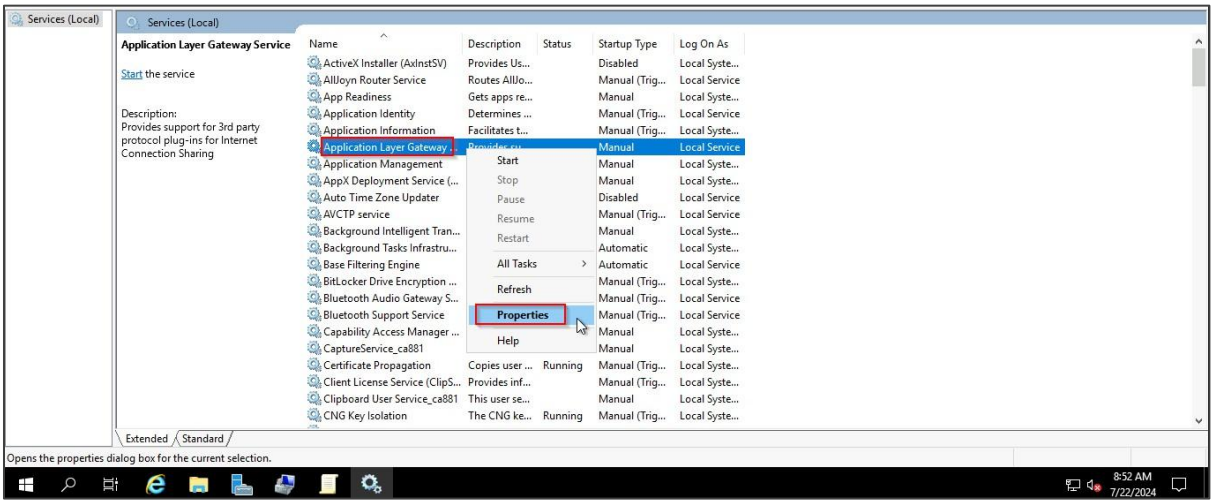
6.1 Type **Run** in the Windows search and open the **Run** app



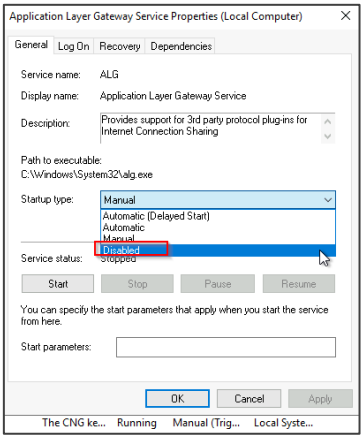
6.2 Type **services.msc** in the **Open** field and click **OK**

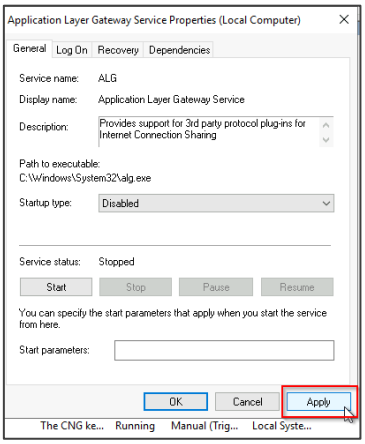


6.3 Right-click on the application you want to disable and then click on **Properties**

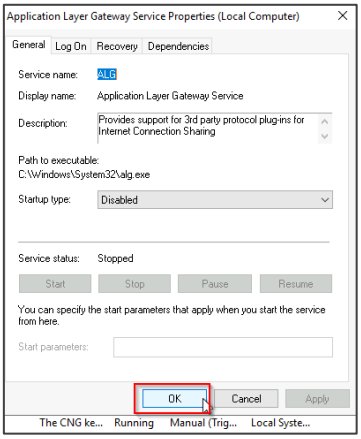


6.4 Select **Disabled** and click on **Apply**





6.5 Click on **OK** to confirm



Following the above steps, you have successfully enhanced Windows Server 2022 security by disabling guest and local administrator's accounts, restricting remote access, configuring account lockout policies, and disabling unnecessary services to protect against cyber threats and ensure secure operations.