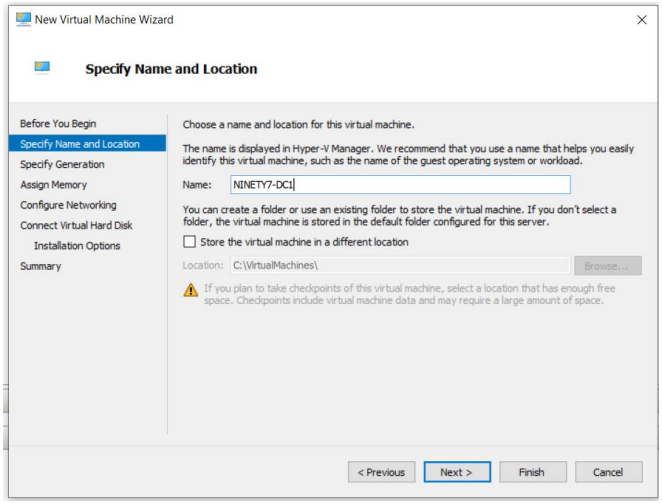
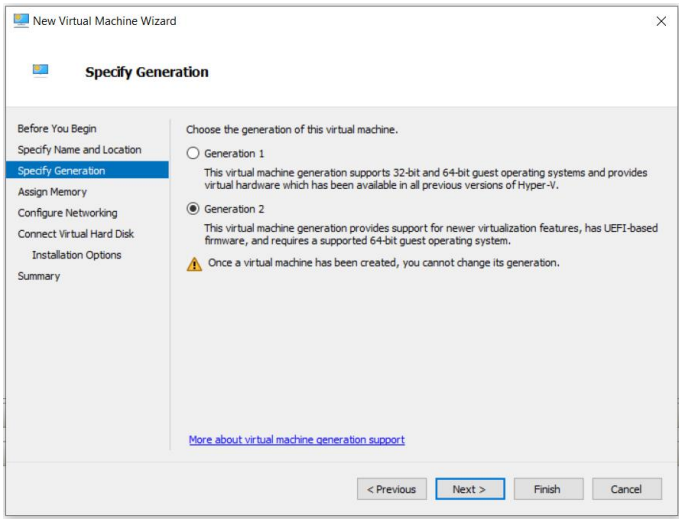
If you are going to be doing this with Hyper V like me. Make sure your host machine is capable of virtualization and has Hyper V setup

Also make sure you have NAT network setup. You can check my GitHub for scripts.

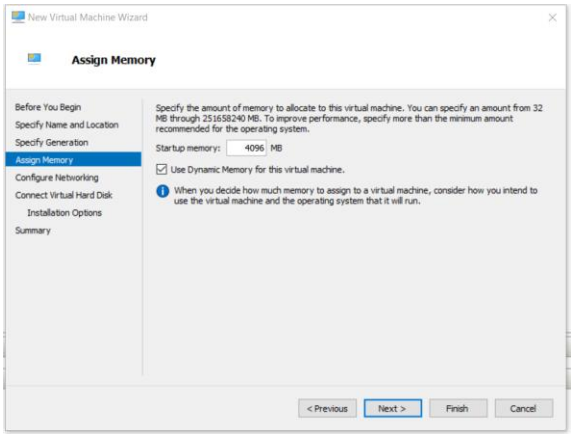
I created my first VM for this project NINETY7-DC1



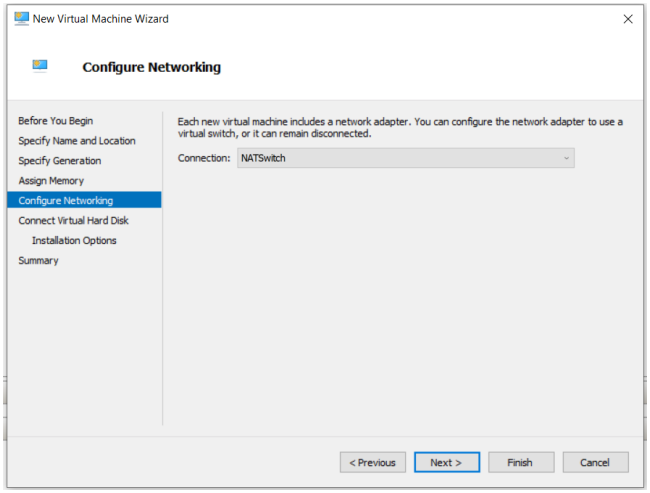
I used Generation 2 VM. Generation 2 VMs are better for security, performance, and modern hardware support.



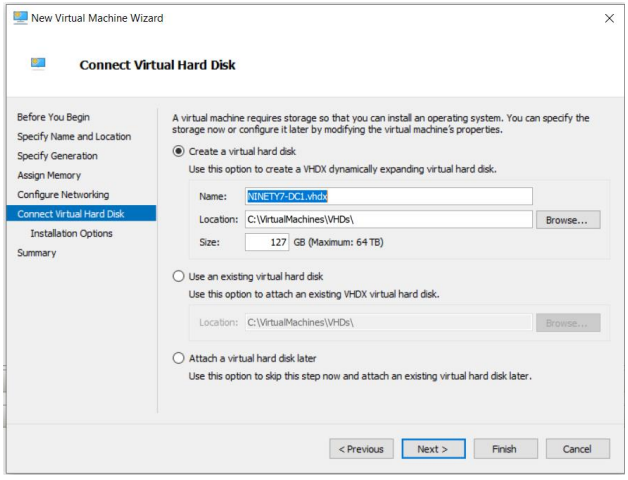
Assign memory



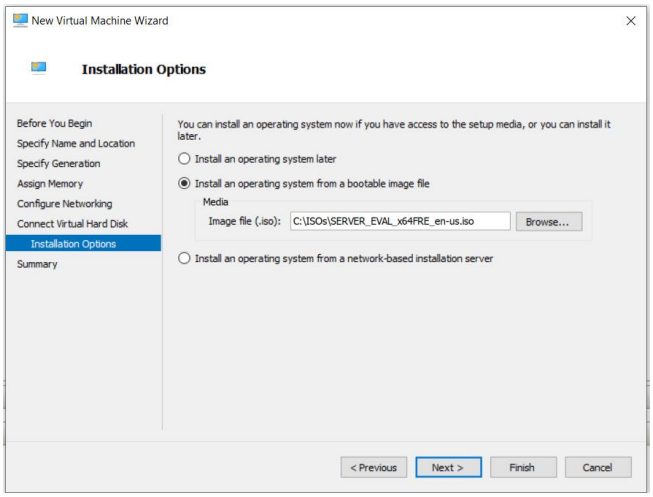
Select NATSwitch you created (Check GitHub for more info)



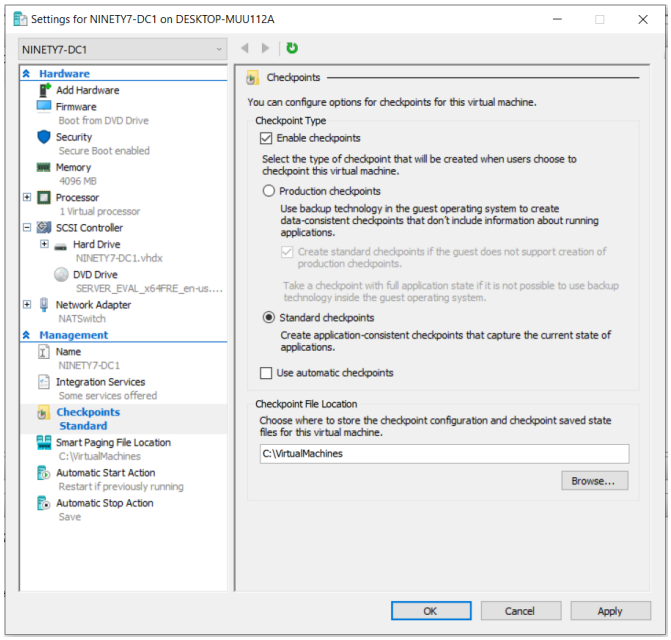
Configure VHD and specify location



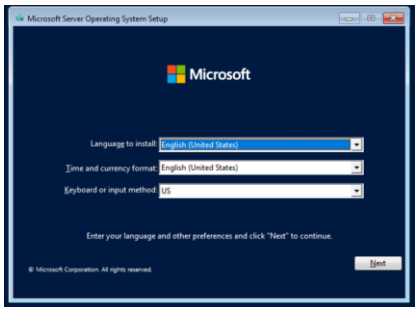
Specify Server image path. I used the Windows Server 2022 Evaluation Edition.



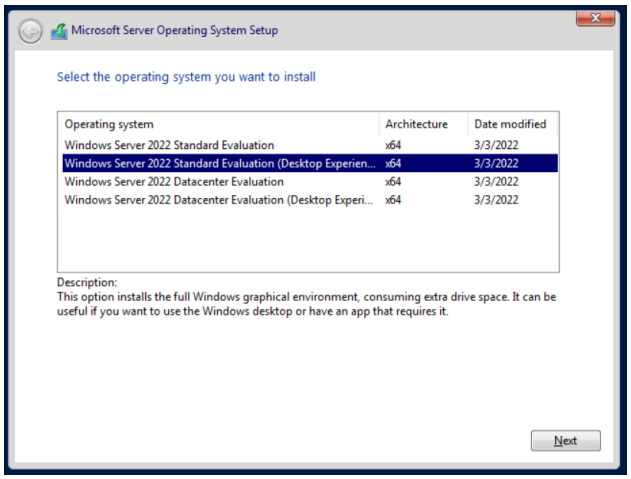
Make sure “Use automatic checkpoints is unchecked”. It’s highly recommended to uncheck automatic checkpoints to avoid performance issues and ensure reliable backups.



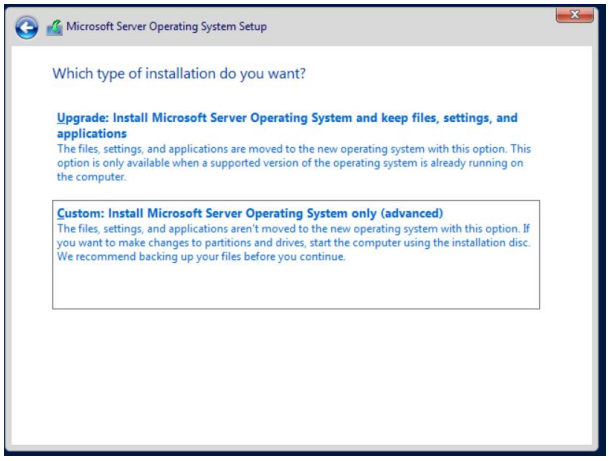
Begin installation



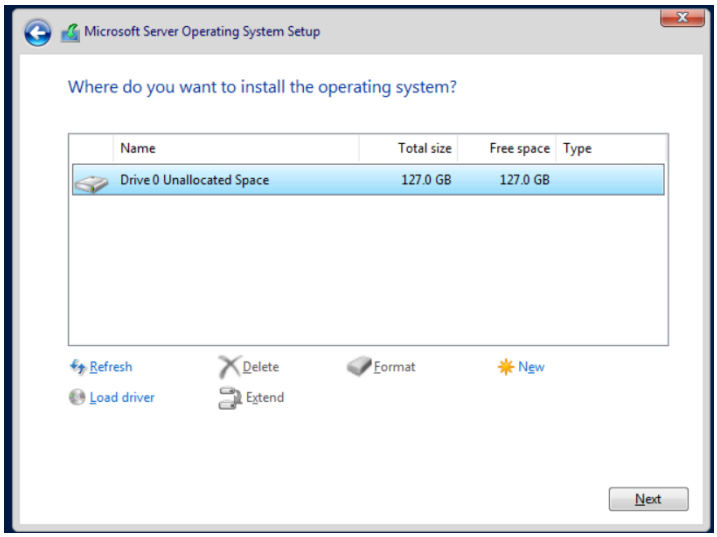
Select Desktop experience version with GUI.

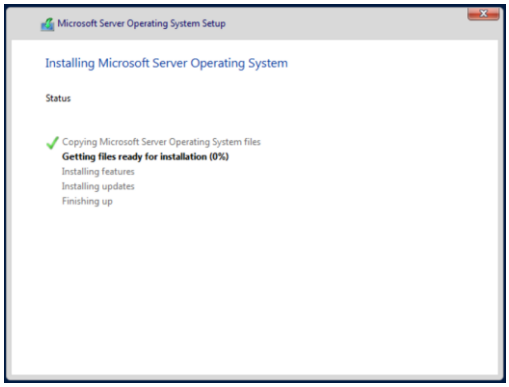


We will select custom installation as this is first time install.

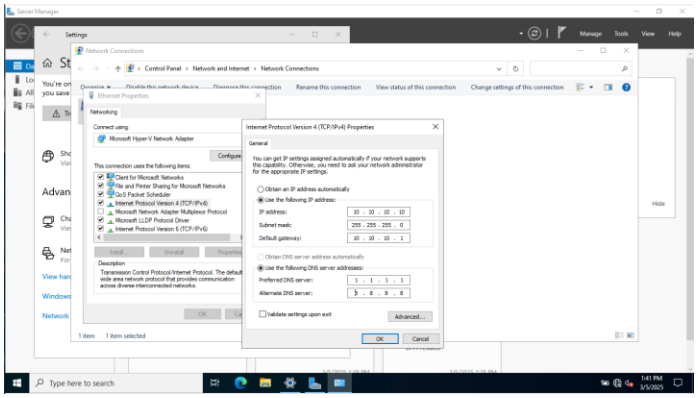


Select drive and/or partitions. I used defaults.

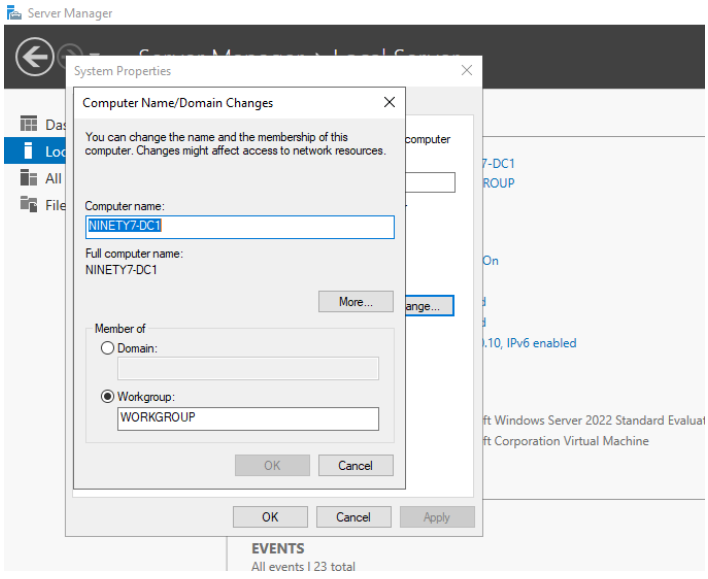




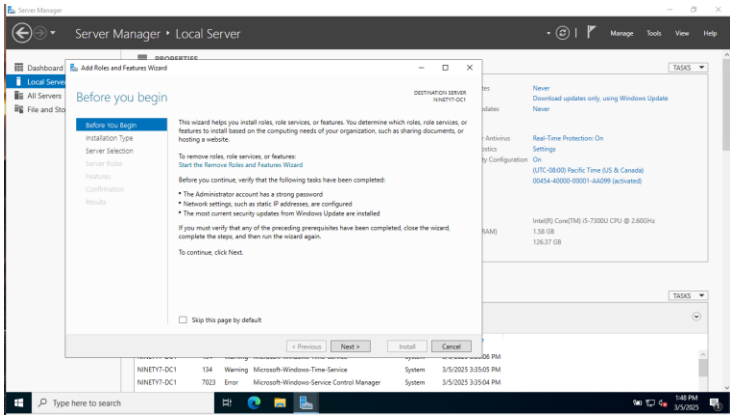
Configure IPV4/DNS properties to enable Internet access.

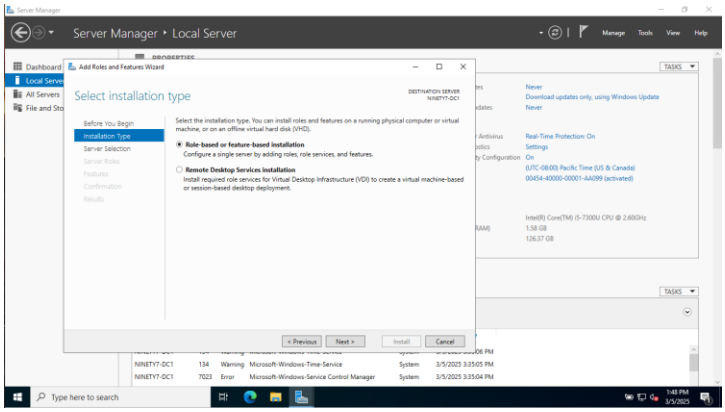


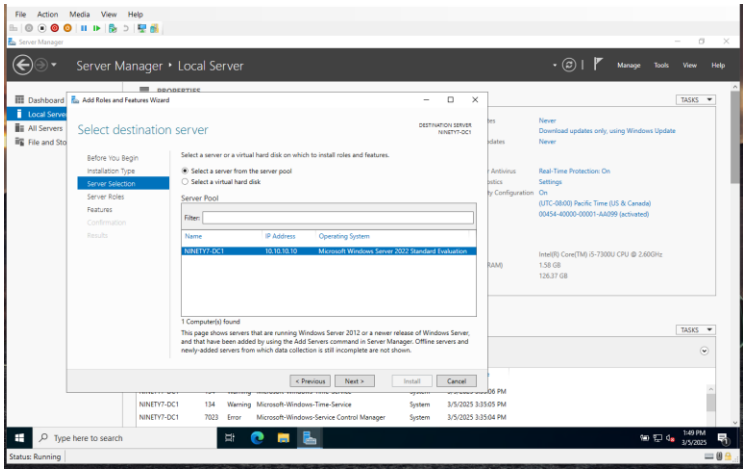
Change computer name for proper management purposes.



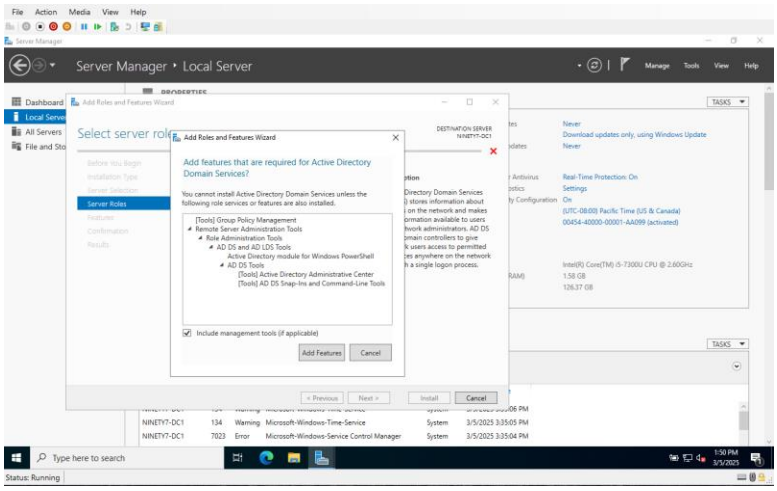
Install AD DS and promote the server to a DC

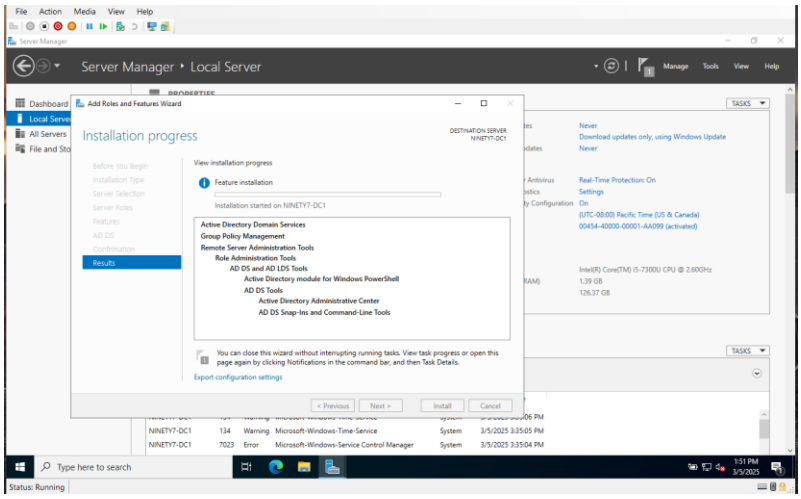


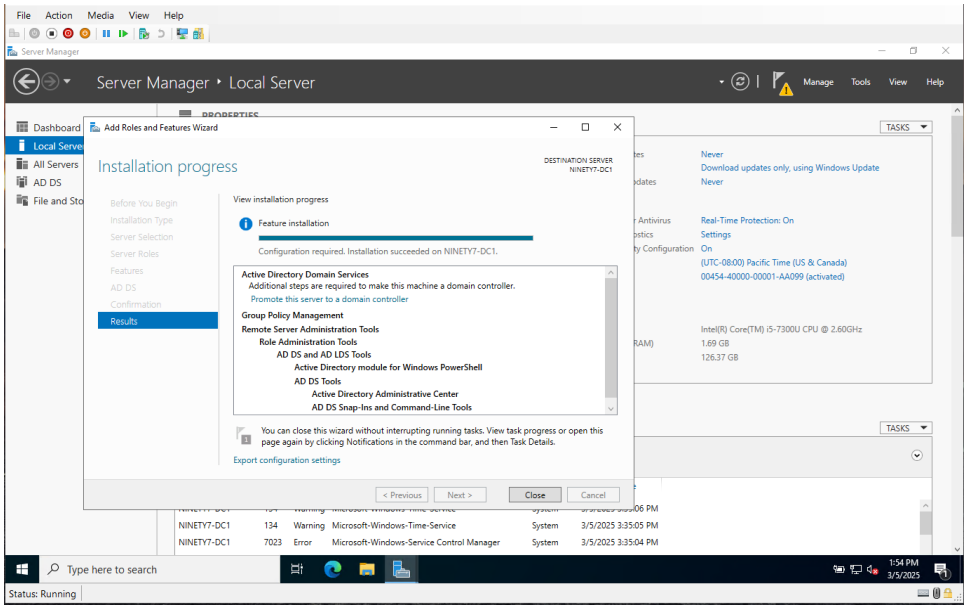




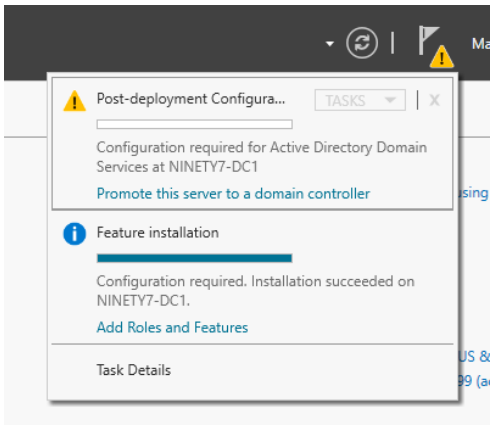
Select defaults.



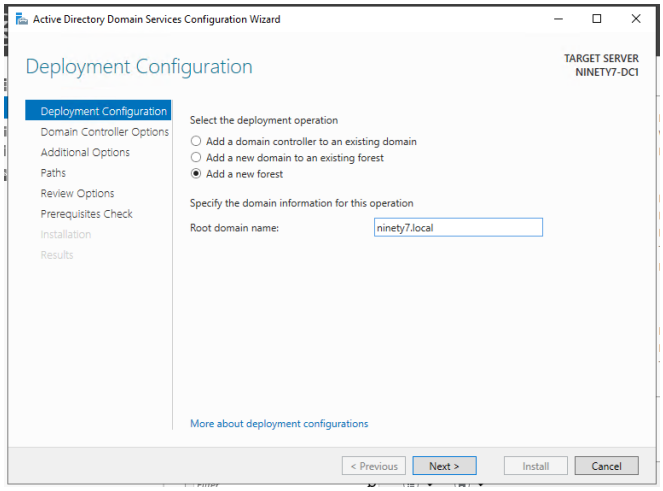




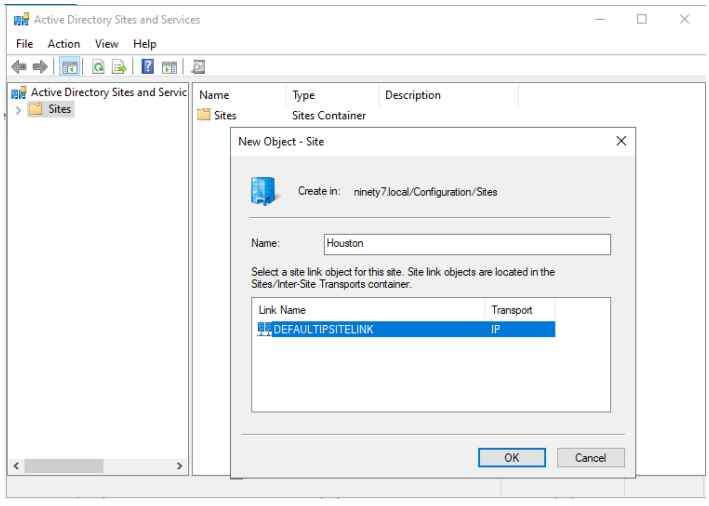
After AD DS installation is complete. Promote your server to a DC.



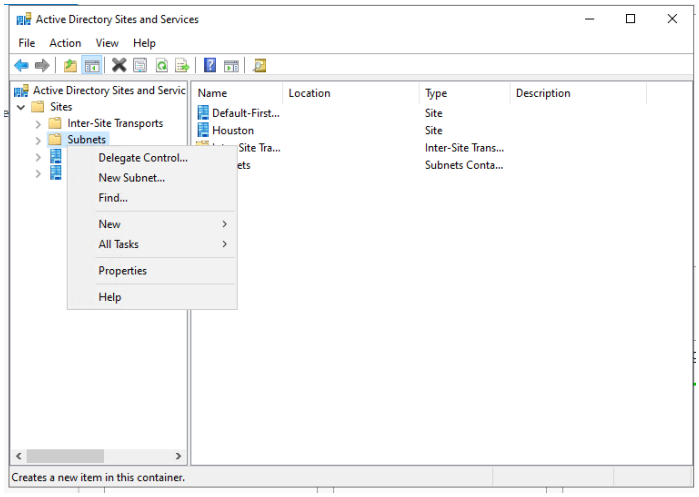
Create a new forest. In my case ninety7.local is my first and only internal domain name in this project.

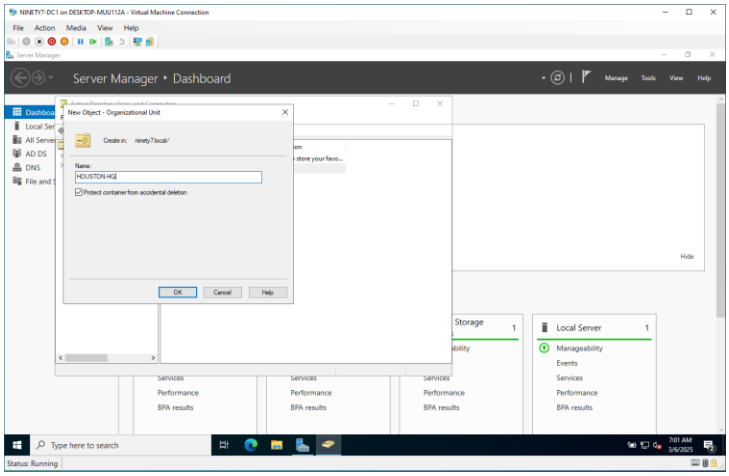


Create new site.

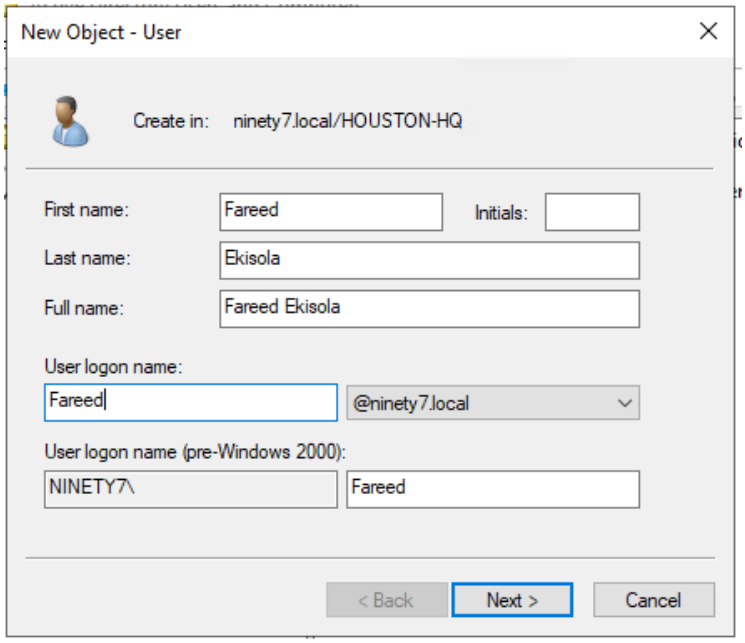


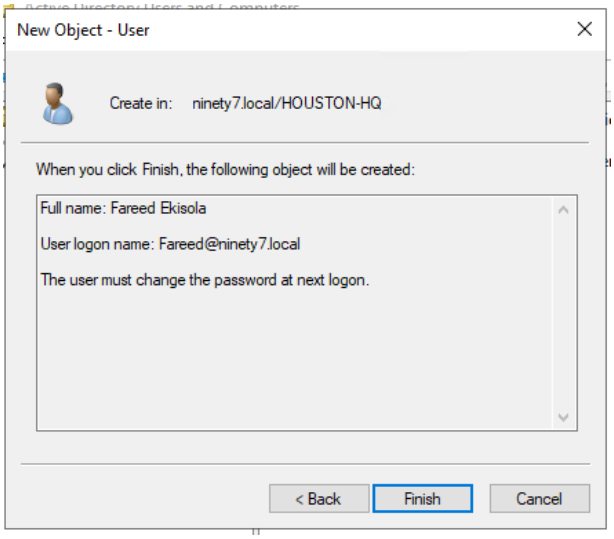
Create new subnet.



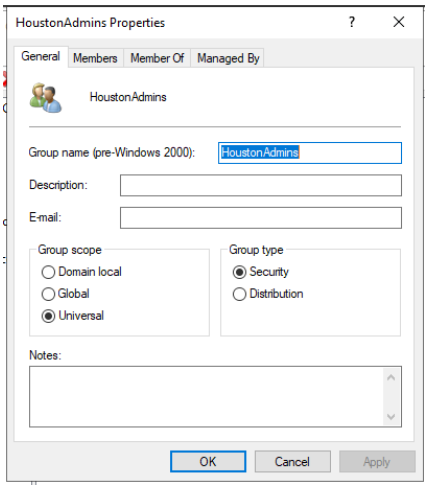


After initial configuration of NINETY7-DC1 was complete I created a user with my name.

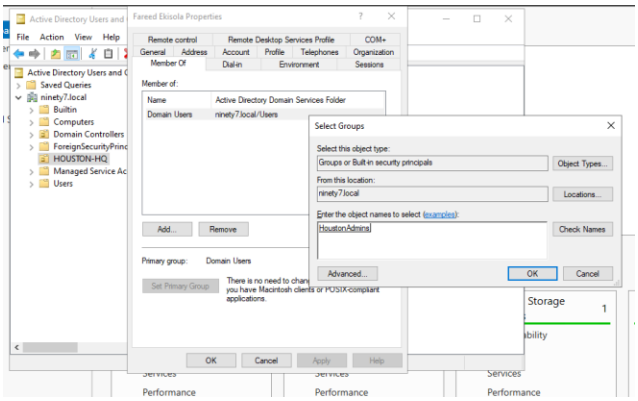




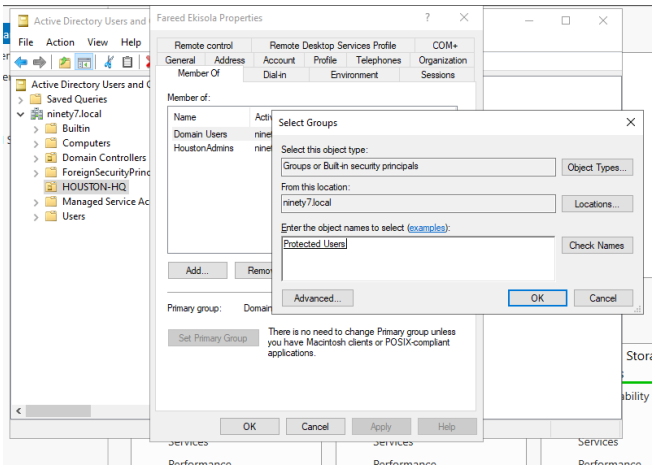
Created a new security group to delegate admin rights and permissions to certain users.



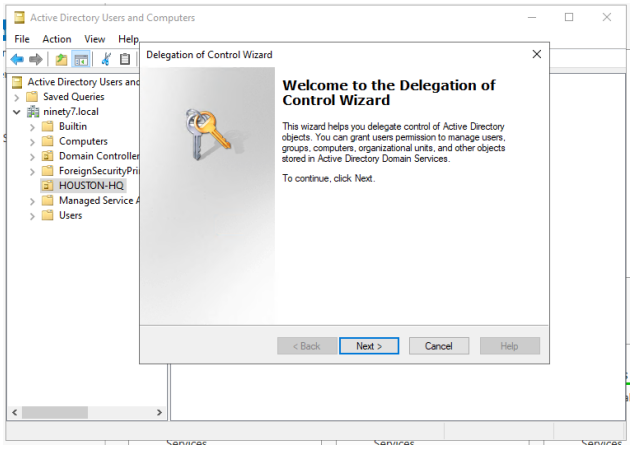
Added myself (Fareed Ekisola) to HoustonAdmins group



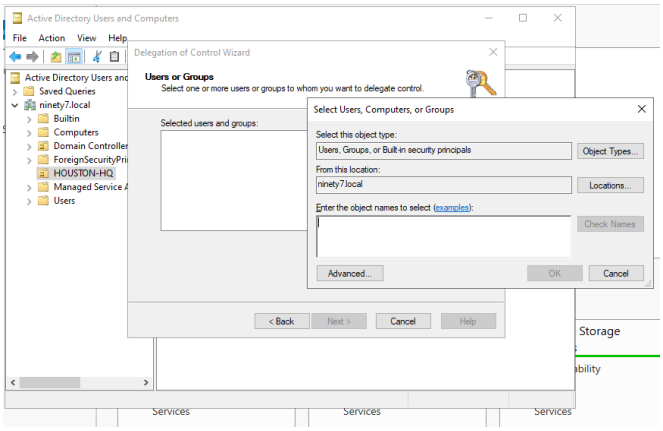
Added to Protected Users group (The Protected Users group is a powerful security feature in Active Directory that helps protect privileged accounts against credential theft attacks.)

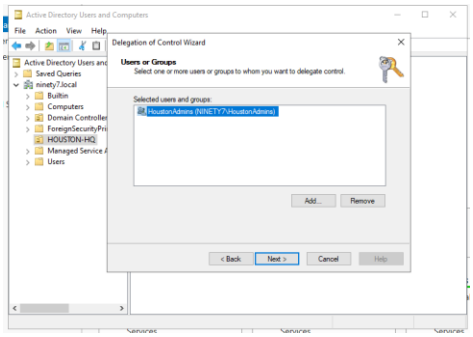


Delegate control to HoustonAdmins group

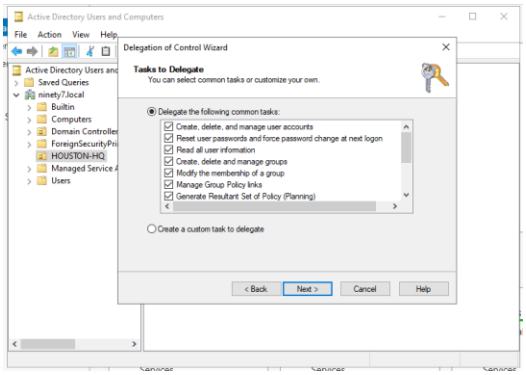


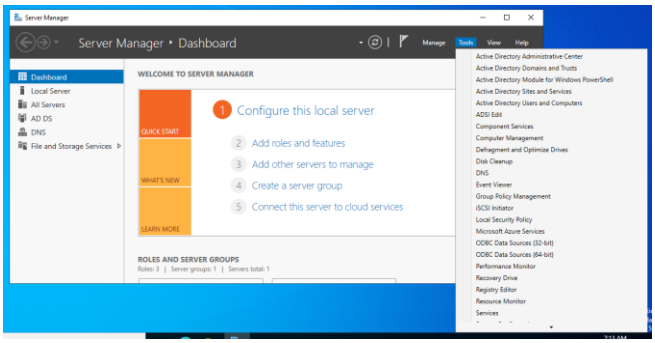
Specify group.





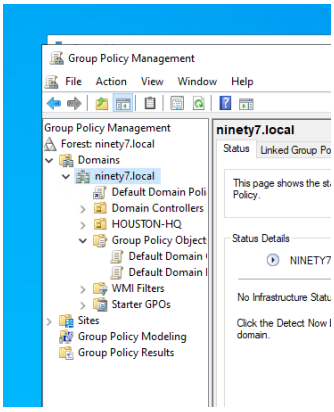
Select tasks you want to delegate.

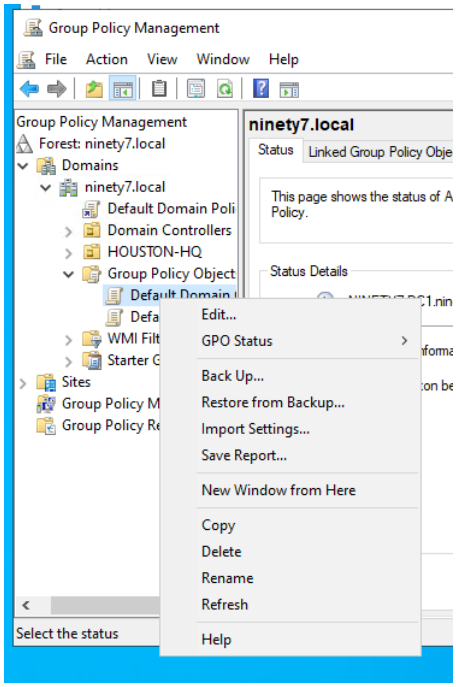


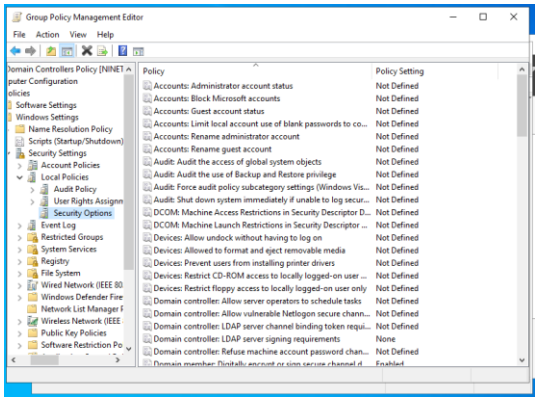


SECURITY MEASURES

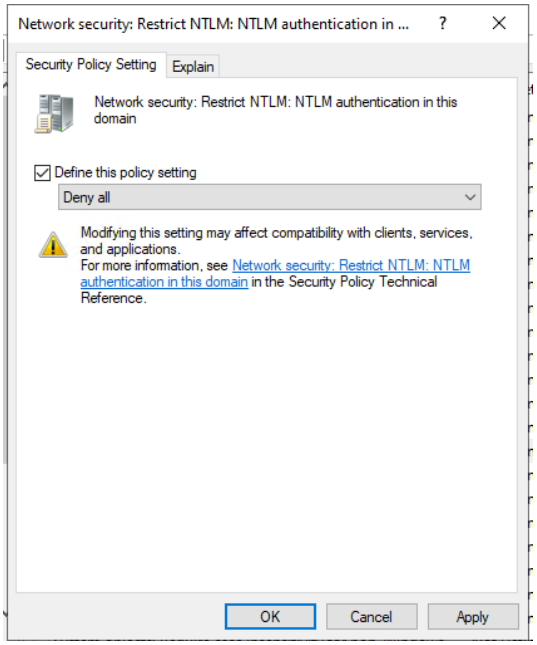
Modify GPOs, security policies to make my server more secure.



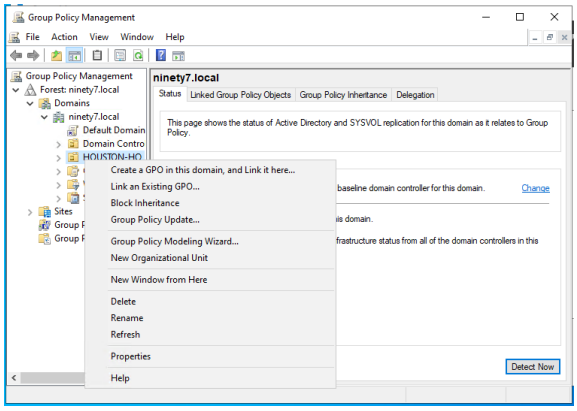


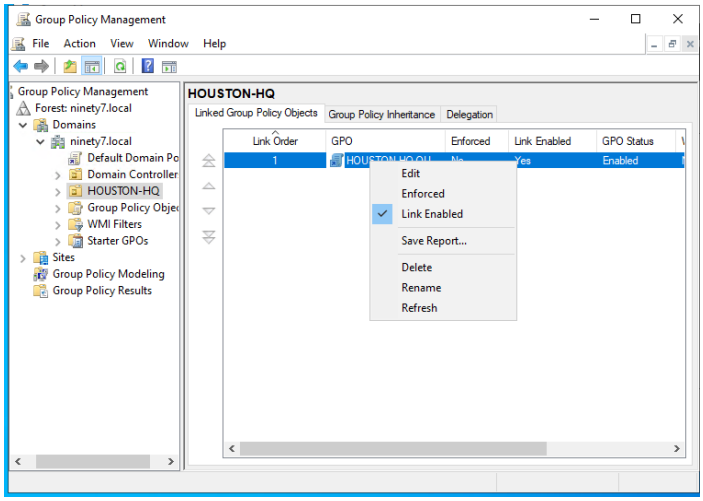


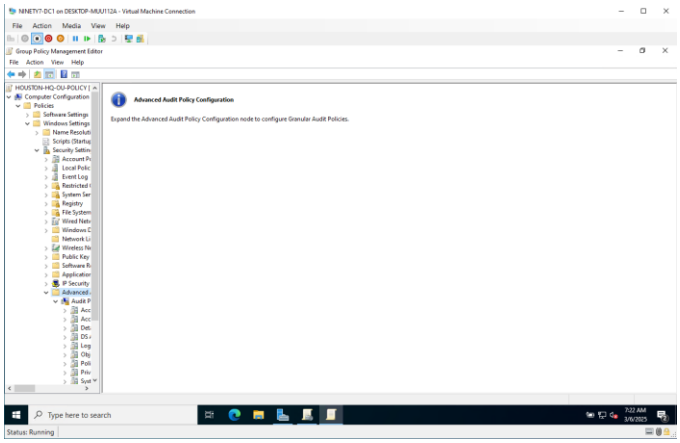
Restrict NTLM auth. NTLM is outdated, insecure, and should be restricted wherever possible. Before disabling NTLM, audit its usage to avoid breaking critical applications.


Network security: Restrict NTLM: NTLM authentication in ...
Security Policy Setting
Explain
Network security: Restrict NTLM: NTLM authentication in this domain
Define this policy setting
Deny all
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: Restrict NTLM: NTLM authentication in this domain in the Security Policy Technical Reference.
OK
Cancel
Apply

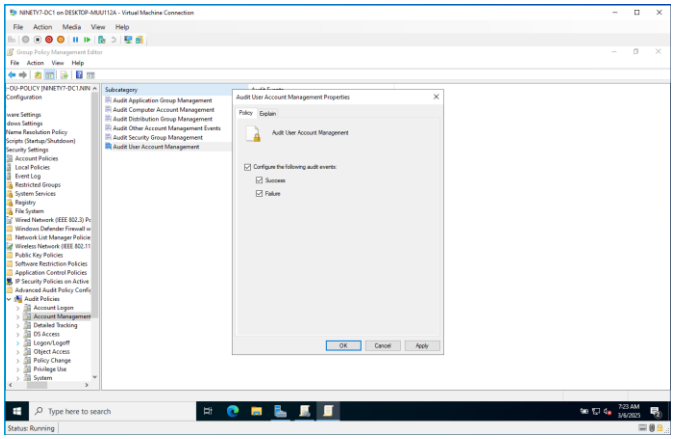
Link GPO.


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: ninety7.local
Domains
ninety7.local
Default Domain
Domain Contro
HOUSTON-HQ
Sites
ninety7.local
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
This page shows the status of Active Directory and SYSVOL replication for this domain as it relates to Group Policy.
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Update...
Group Policy Modeling Wizard...
New Organizational Unit
New Window from Here
Delete
Rename
Refresh
Properties
Help
baseline domain controller for this domain.
Change
Detect Now

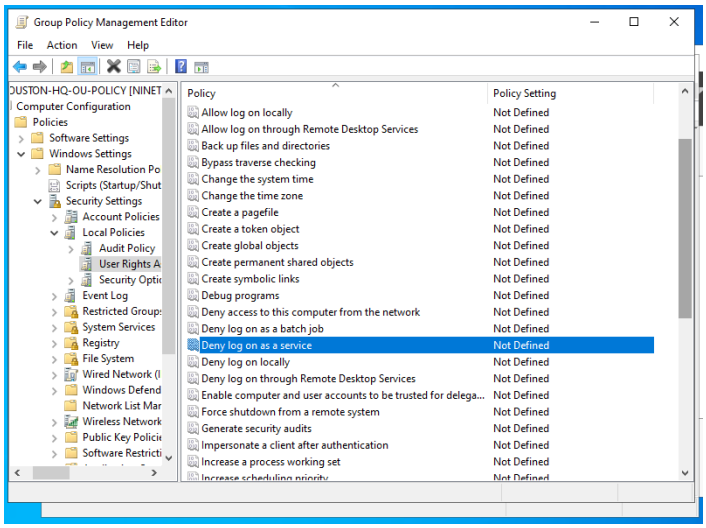

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: ninety7.local
Domains
ninety7.local
Default Domain Po
Domain Controller
HOUSTON-HQ
Group Policy Objec
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
HOUSTON-HQ
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
1
Yes
Enabled
Edit
Enforced
Link Enabled
Save Report...
Delete
Rename
Refresh



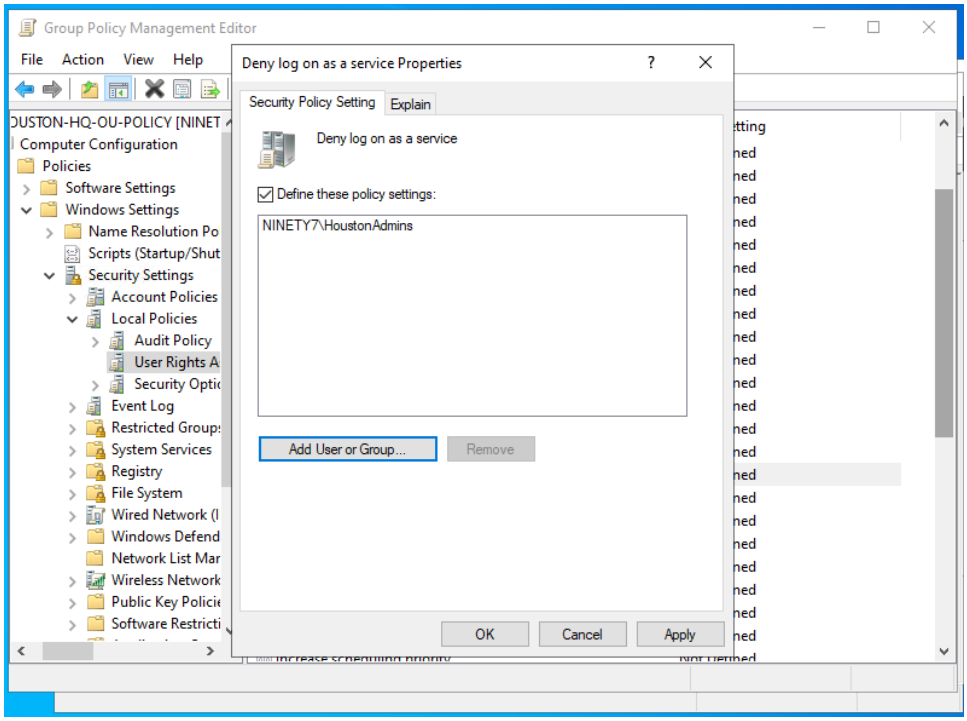
Enable Audit User Account Management.



Deny Log On as a service for Admin users. Restricting "Log on as a Service" is a proactive security measure that helps prevent malware execution, privilege escalation, and unauthorized service installations.



Specify group.



KEY TAKEAWAYS

Create VM & Install OS: Set up Windows Server with a static IP.

Install AD DS & Promote to DC: Use Server Manager or PowerShell.

Disable NTLM: Set NTLM traffic to Deny all in Group Policy.

Enforce Strong Passwords: Set complex password policies.

Enable Auditing: Monitor logon and group changes via Group Policy.

Scripts and more info on my GitHub