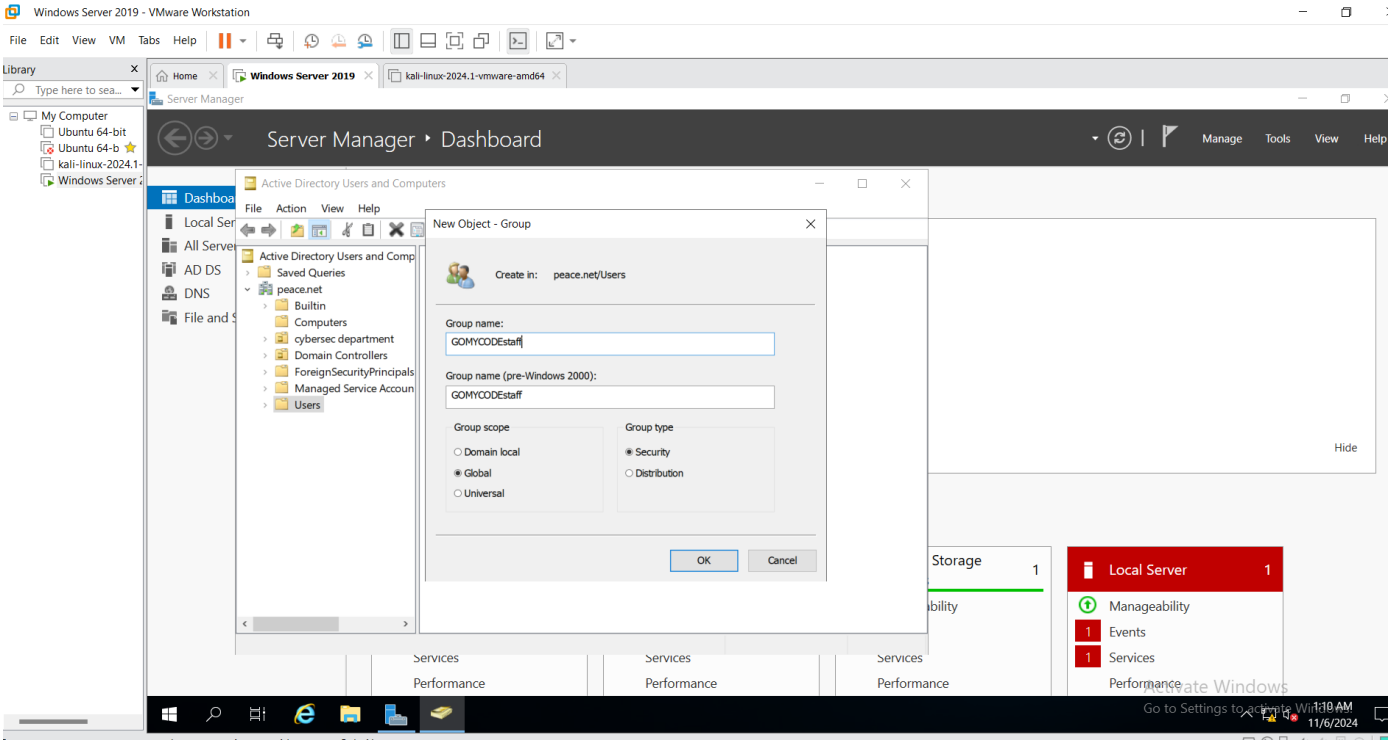
Checkpoint Architecture and Design II

Question

Instructions

first login to the windows server on the server manager goes to : tools → Active Directory Users and Computers Right click on the user folder and choose the new group : https://i.imgur.com/hBBrhUc.png Create a group named GOMYCODEstaff: https://i.imgur.com/qzdFvgZ.png now leave the User and Group Management and go to : tools → Active Directory Administrative Center On the left side choose: gomycode (local) → system → Password settings https://i.imgur.com/Li9iMpb.png Now on the white space right click and choose new password settings : https://i.imgur.com/NyUgLE2.png We want to configure the following policies: All IT staff privileged accounts must contain a minimum of 20 characters and be complex. Passwords must be changed every 30 days. Passwords may not be changed more than once per day and the 24 most recent passwords cannot be repeated. IT staff-privileged accounts are subject to an account lockout policy, with a maximum of three failed login attempts allowed. Accounts will be locked out for a duration of 20 minutes. Reset failed attempts after 10 minutes. Follow the following screen-shot: https://i.imgur.com/6qJJQzN.png click on add type GOMYCODEstaff in the enter the object names to select : https://i.imgur.com/XIoTBU0.png hit OK confirm with okay we can see that the policy was added to the gomycode (local) Now let's try to add a group Policy go to tools → group policy management : https://i.imgur.com/zyma8tX.png Name the GPO : SecureAdminWorkstation : https://i.imgur.com/S74LI6q.png Edit the GPO : (right click + edit): https://i.imgur.com/Lr5onct.png Select Computer Configuration → Policies → Windows Settings → security settings → Local Policies →Security Options : https://i.imgur.com/3kpqzme.png Now you can disable Guest Accounts change the Administrator account choose to not display the last user name in an interactive log-on

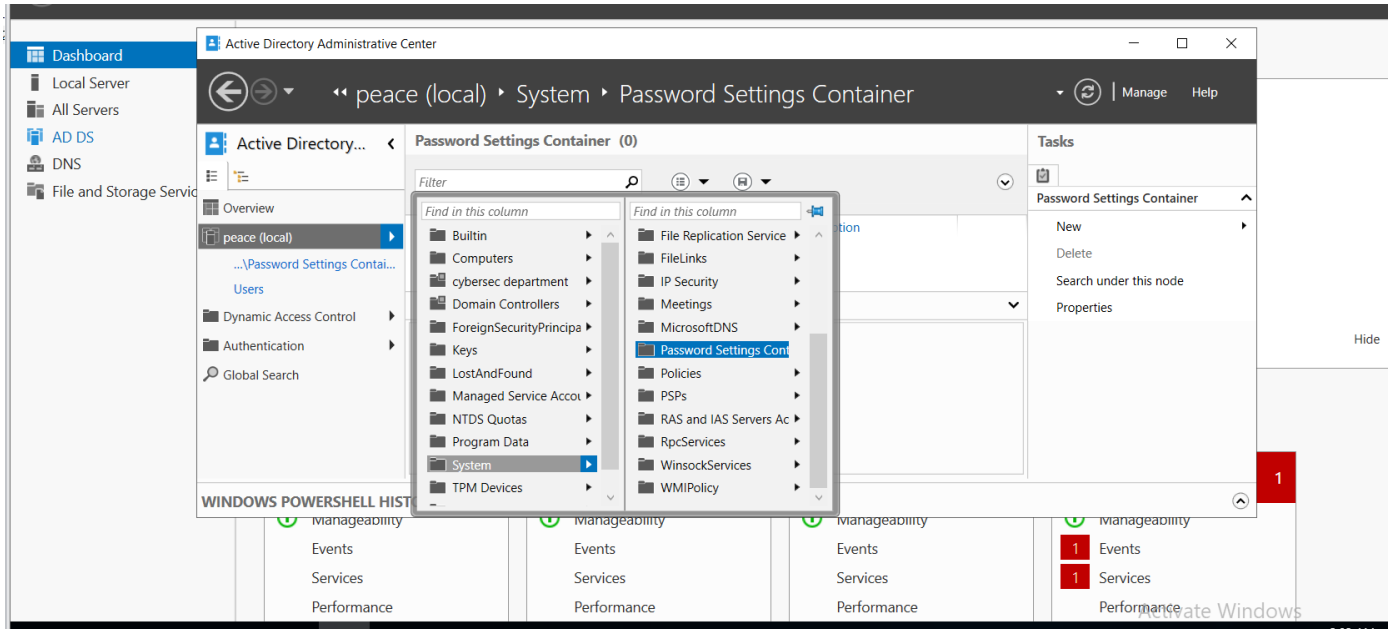
1.



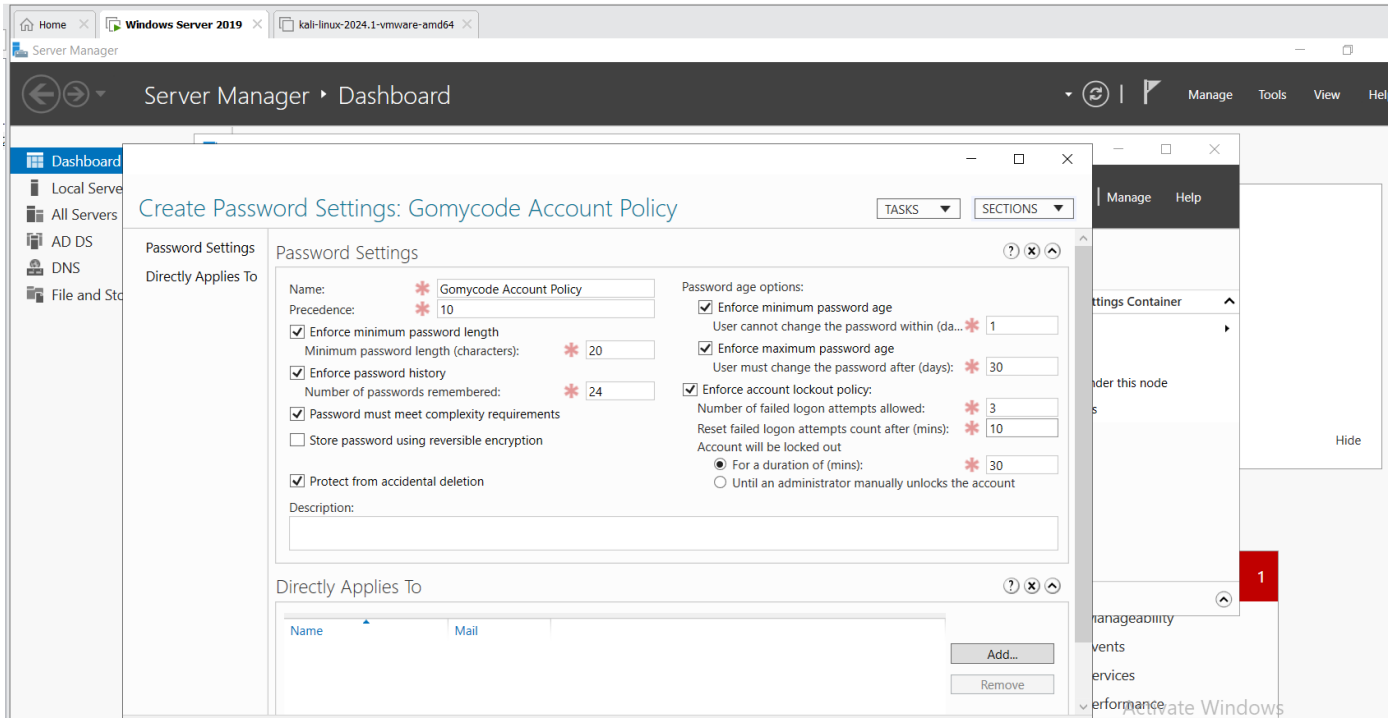
2.

Managed Service Accoun
Users
Domain Con... Security Group ... All domain controllers in ...
Domain Gue... Security Group ... All domain guests
Domain Users Security Group ... All domain users
Enterprise A... Security Group ... Designated administrato...
Enterprise Ke... Security Group ... Members of this group c...
Enterprise Re... Security Group ... Members of this group a...
GOMYCODE... Security Group ...
Group Policy... Security Group ... Members in this group c...
Guest User Built-in account for gues...
Key Admins Security Group ... Members of this group c...

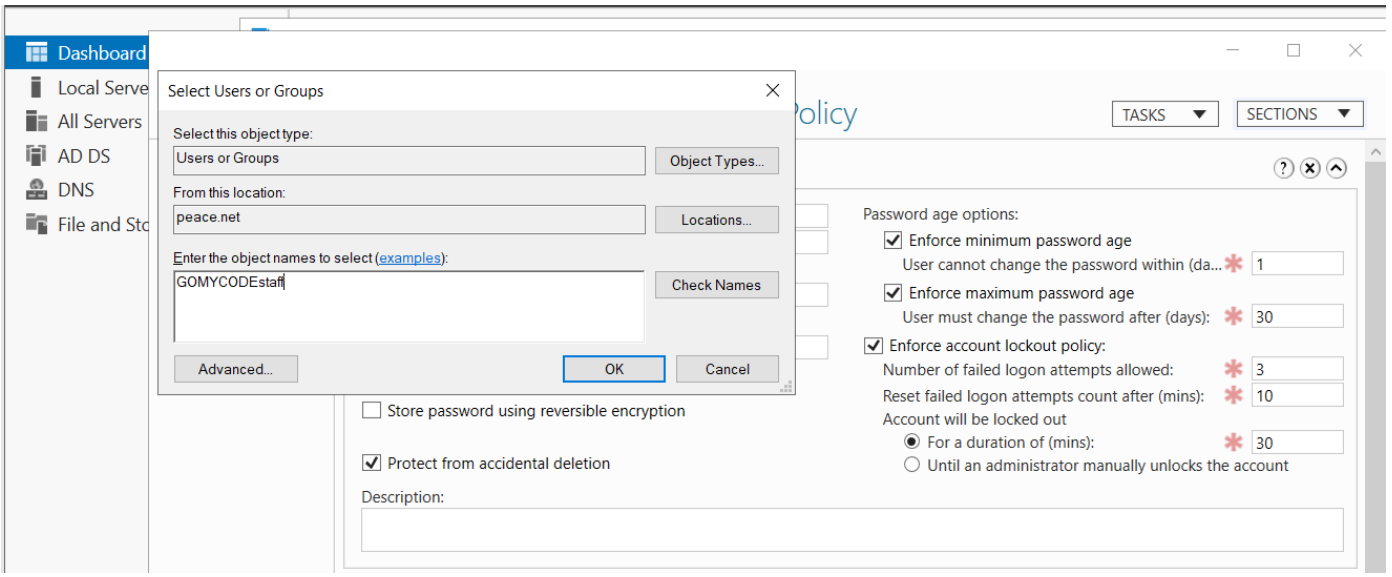
3.


Active Directory Administrative Center
peace (local) ‣ System ‣ Password Settings Container
Manage Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Servic
Active Directory...
Overview
peace (local)
...\Password Settings Contai...
Users
Dynamic Access Control
Authentication
Global Search
Password Settings Container (0)
Filter
Find in this column
Builtin
Computers
cybersec department
Domain Controllers
ForeignSecurityPrincipa
Keys
LostAndFound
Managed Service Accou
NTDS Quotas
Program Data
System
TPM Devices
File Replication Service
FileLinks
IP Security
Meetings
MicrosoftDNS
Password Settings Cont
Policies
PSPs
RAS and IAS Servers Ac
RpcServices
WinsockServices
WMIPolicy
Tasks
Password Settings Container
New
Delete
Search under this node
Properties
Hide
WINDOWS POWERSHELL HIST
Manageability
Events
Services
Performance
1
Activate Windows

4.


Home
Windows Server 2019
kali-linux-2024.1-vmware-amd64
Server Manager
Server Manager ‣ Dashboard
Manage Tools View
Dashboard
Local Serve
All Servers
AD DS
DNS
File and Sto
Create Password Settings: Gomycode Account Policy
TASKS
SECTIONS
Password Settings
Directly Applies To
Password Settings
Name: Gomycode Account Policy
Precedence: 10
Enforce minimum password length
Minimum password length (characters): 20
Enforce password history
Number of passwords remembered: 24
Password must meet complexity requirements
Store password using reversible encryption
Protect from accidental deletion
Description:
Password age options:
Enforce minimum password age
User cannot change the password within (da... 1
Enforce maximum password age
User must change the password after (days): 30
Enforce account lockout policy:
Number of failed logon attempts allowed: 3
Reset failed logon attempts count after (mins): 10
Account will be locked out
For a duration of (mins): 30
Until an administrator manually unlocks the account
Directly Applies To
Name
Mail
Add...
Remove
Manage Help
Hide
1
Activate Windows

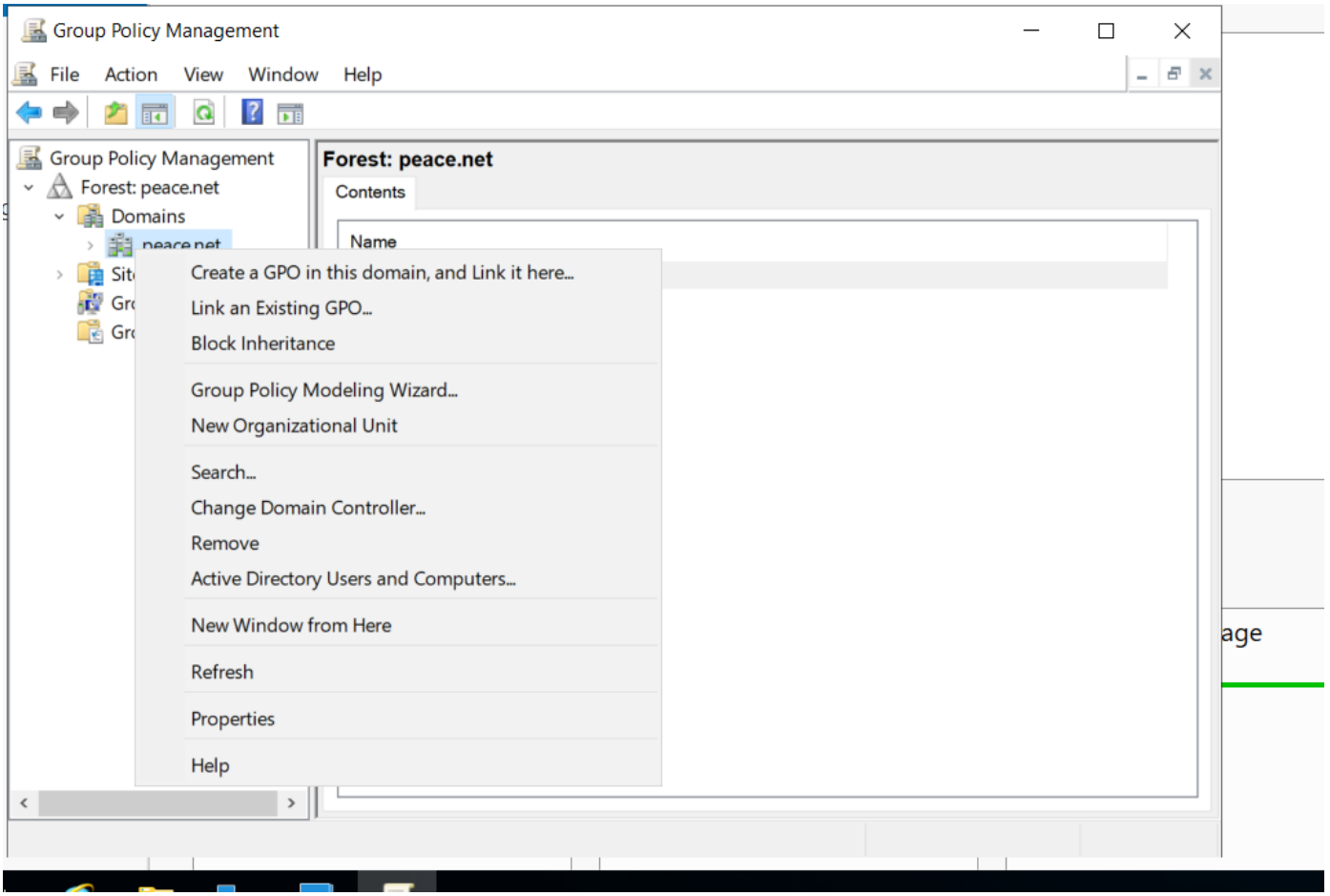
5.


Dashboard
Local Serve
All Servers
AD DS
DNS
File and Sto
Select Users or Groups
Select this object type:
Users or Groups
Object Types...
From this location:
peace.net
Locations...
Enter the object names to select (examples):
GOMYCODEstaff
Check Names
Advanced...
OK
Cancel
Policy
TASKS
SECTIONS
Password age options:
Enforce minimum password age
User cannot change the password within (da...
1
Enforce maximum password age
User must change the password after (days):
30
Enforce account lockout policy:
Number of failed logon attempts allowed:
3
Reset failed logon attempts count after (mins):
10
Account will be locked out
For a duration of (mins):
30
Until an administrator manually unlocks the account
Store password using reversible encryption
Protect from accidental deletion
Description:

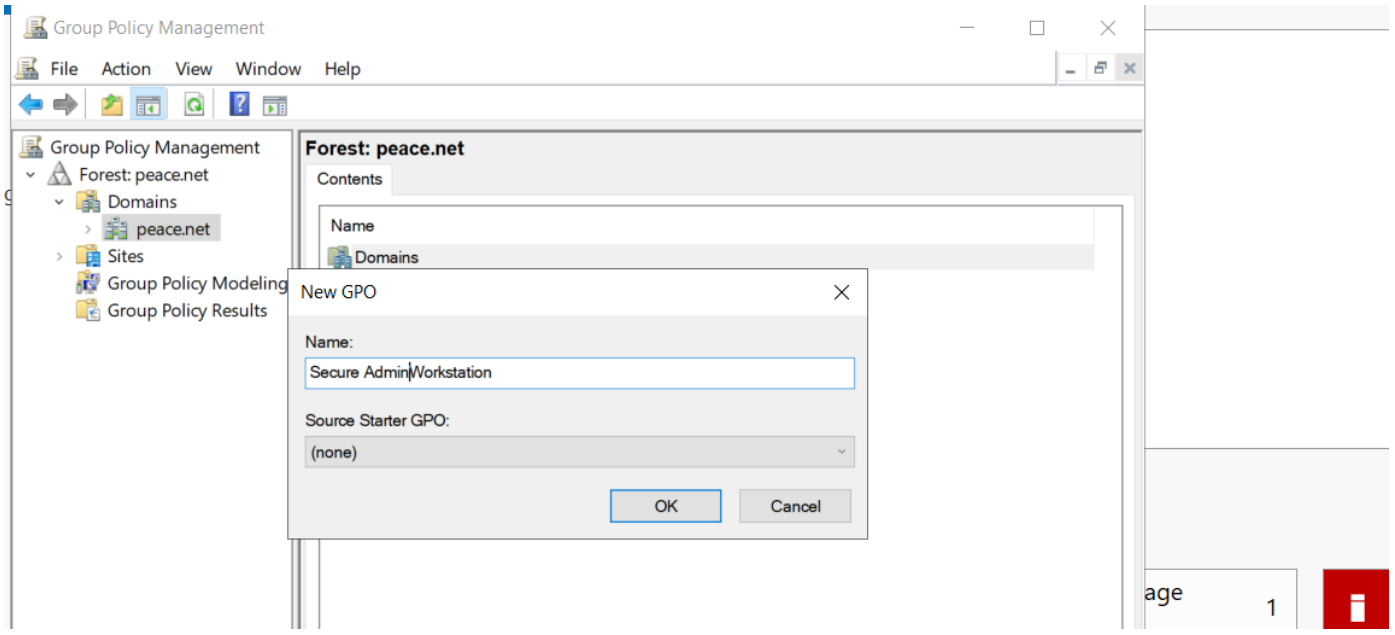
6.

Directly Applies To
Name
Mail
GOMYCODEstaff
Add...
Remove

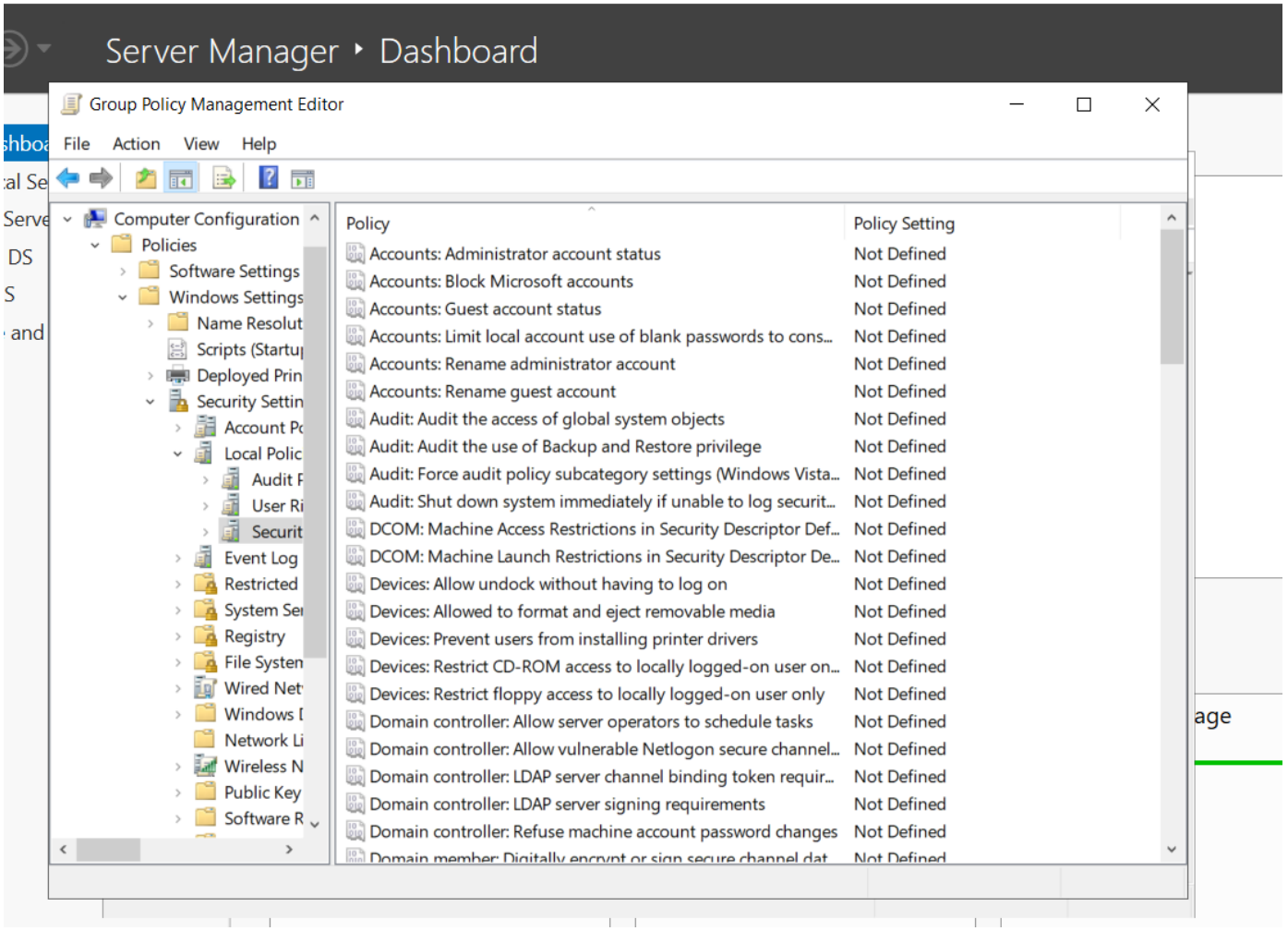
7.


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: peace.net
Domains
peace.net
Forest: peace.net
Contents
Name
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Active Directory Users and Computers...
New Window from Here
Refresh
Properties
Help

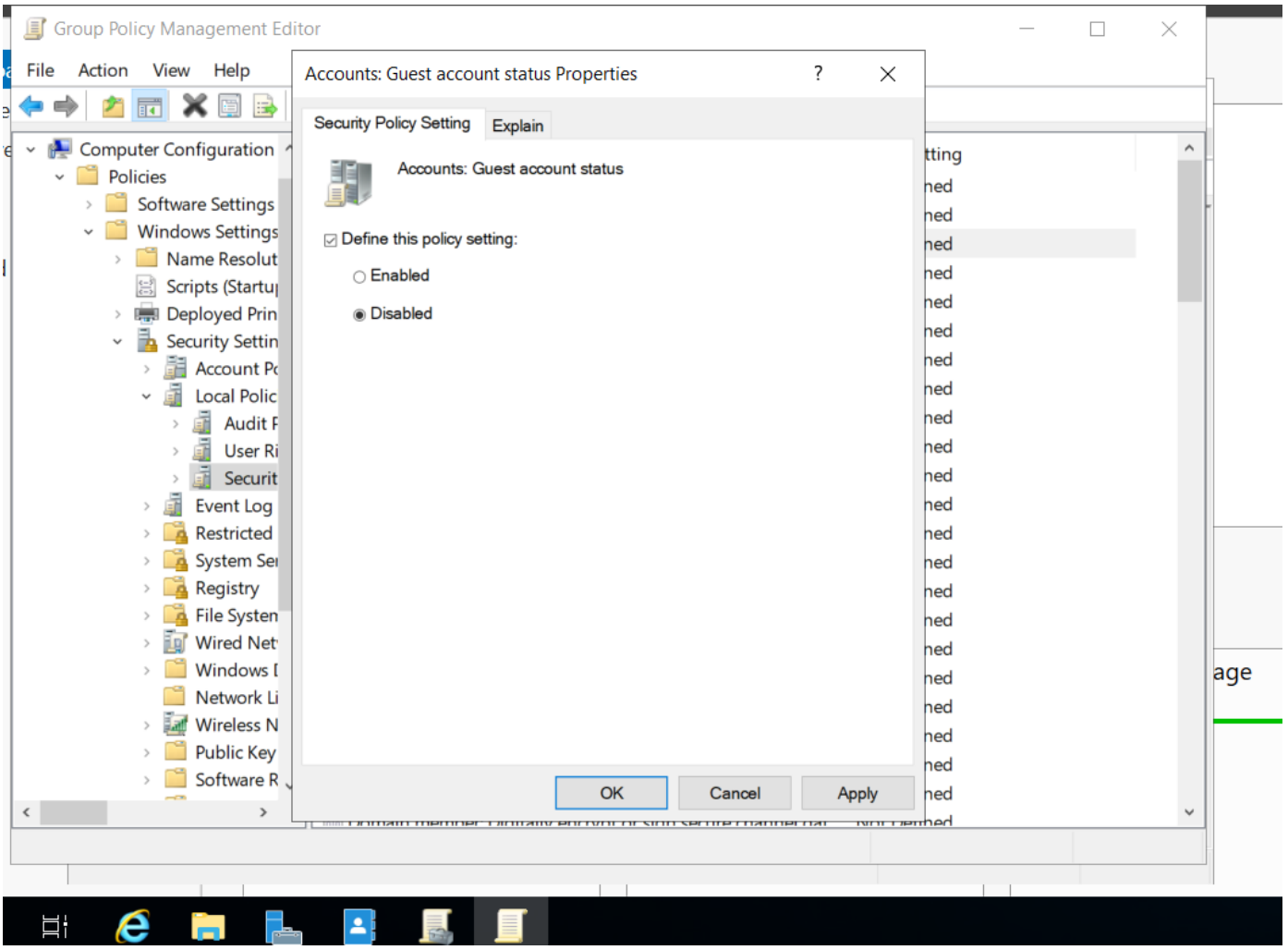
8.


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: peace.net
Domains
peace.net
Sites
Group Policy Modeling
Group Policy Results
Forest: peace.net
Contents
Name
Domains
New GPO
Name:
Secure AdminWorkstation
Source Starter GPO:
(none)
OK
Cancel

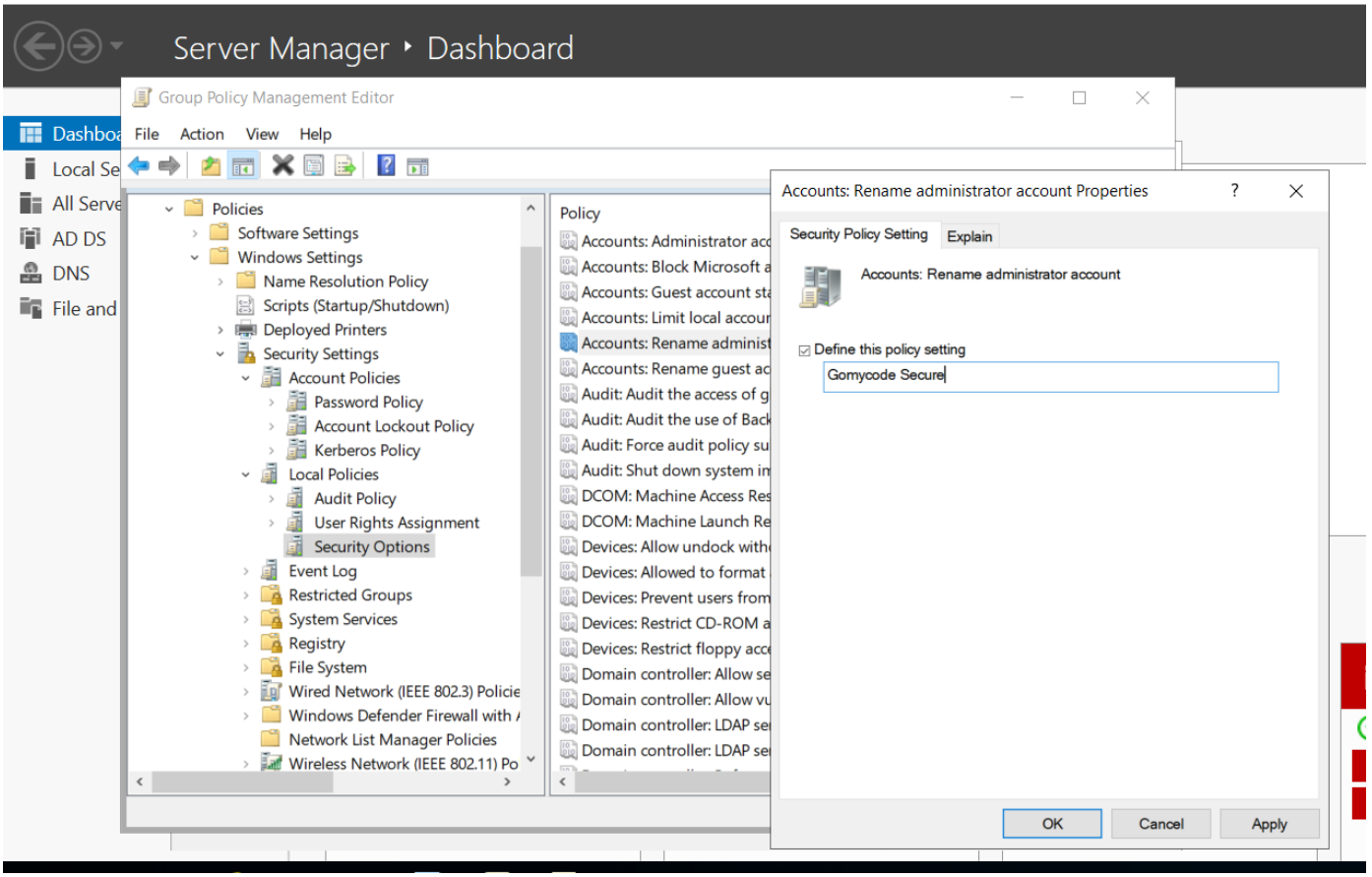
9.


Server Manager ‣ Dashboard
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Deployed Prin
Security Settin
Account Po
Local Polic
Audit P
User Ri
Securit
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows F
Network Li
Wireless N
Public Key
Software R
Policy
Policy Setting
Accounts: Administrator account status Not Defined
Accounts: Block Microsoft accounts Not Defined
Accounts: Guest account status Not Defined
Accounts: Limit local account use of blank passwords to cons... Not Defined
Accounts: Rename administrator account Not Defined
Accounts: Rename guest account Not Defined
Audit: Audit the access of global system objects Not Defined
Audit: Audit the use of Backup and Restore privilege Not Defined
Audit: Force audit policy subcategory settings (Windows Vista... Not Defined
Audit: Shut down system immediately if unable to log securit... Not Defined
DCOM: Machine Access Restrictions in Security Descriptor Def... Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor De... Not Defined
Devices: Allow undock without having to log on Not Defined
Devices: Allowed to format and eject removable media Not Defined
Devices: Prevent users from installing printer drivers Not Defined
Devices: Restrict CD-ROM access to locally logged-on user on... Not Defined
Devices: Restrict floppy access to locally logged-on user only Not Defined
Domain controller: Allow server operators to schedule tasks Not Defined
Domain controller: Allow vulnerable Netlogon secure channel... Not Defined
Domain controller: LDAP server channel binding token requir... Not Defined
Domain controller: LDAP server signing requirements Not Defined
Domain controller: Refuse machine account password changes Not Defined

10.


Group Policy Management Editor
File Action View Help
Accounts: Guest account status Properties
Security Policy Setting
Explain
Accounts: Guest account status
Define this policy setting:
Enabled
Disabled
OK
Cancel
Apply
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Deployed Prin
Security Settin
Account Po
Local Polic
Audit P
User Ri
Securit
Event Log
Restricted
System Ser
Registry
File Systen
Wired Net
Windows F
Network Li
Wireless N
Public Key
Software R

11.


Server Manager ‣ Dashboard
Group Policy Management Editor
File Action View Help
Accounts: Rename administrator account Properties
Security Policy Setting
Explain
Accounts: Rename administrator account
Define this policy setting
Gomycode Secure
OK
Cancel
Apply
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policie
Windows Defender Firewall with
Network List Manager Policies
Wireless Network (IEEE 802.11) Po
Policy
Accounts: Administrator acc
Accounts: Block Microsoft a
Accounts: Guest account sta
Accounts: Limit local accour
Accounts: Rename administ
Accounts: Rename guest ac
Audit: Audit the access of g
Audit: Audit the use of Back
Audit: Force audit policy su
Audit: Shut down system in
DCOM: Machine Access Res
DCOM: Machine Launch Re
Devices: Allow undock with
Devices: Allowed to format
Devices: Prevent users from
Devices: Restrict CD-ROM a
Devices: Restrict floppy acc
Domain controller: Allow se
Domain controller: Allow vu
Domain controller: LDAP se
Domain controller: LDAP se

12.