

Bangladesh University of Professionals (BUP)



Assignment – 06

Title - TryHackMe - Active Directory Basic

Course Name - Enterprise Security Architecture Design and Management

Course Code - MCS1103

Submitted To

Engr. Md. Mushfiquur Rahman

Submitted By

Jannatul Ferdous Katha

Masters in Cyber Security

Department of Computer Science and Engineering

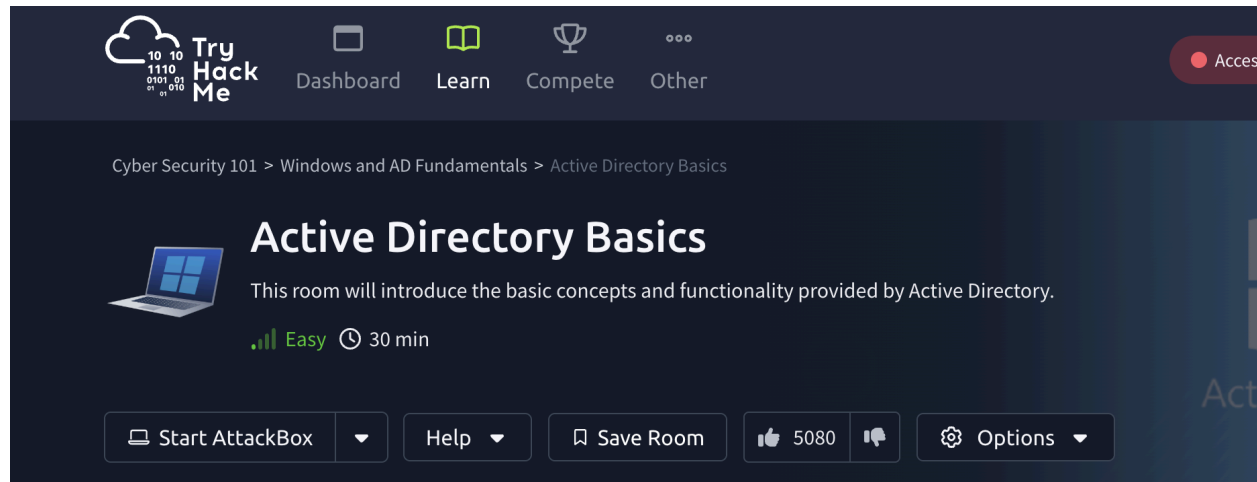
Submission Date: 28-04-2025

Table of Contents:

Active Directory Basics - TryHackMe

1. Task 1: Introduction
2. Task 2 - Windows Domain
3. Task 3 - Active Directory
4. Task - 4: Managing Users in AD
5. Task -5: Managing Computers in AD
6. Task -6: Group Policies
7. Task -7: Authentication Method
8. Task -8: Trees, Forest and Trusts
9. Task -9: Conclusion

Active Directory Basics - TryHackMe - Microsoft's Active Directory serves as a cornerstone for corporate IT infrastructure, streamlining the administration of users and devices in a business setting. In this room, we'll explore the core elements of Active Directory in detail.



Task 1: Introduction -

Define only the room objectives and prerequisites—no questions are needed for this task.

Answer the questions below

Click and continue learning!

No answer needed

✓ Correct Answer

Task 2 - Windows Domain:

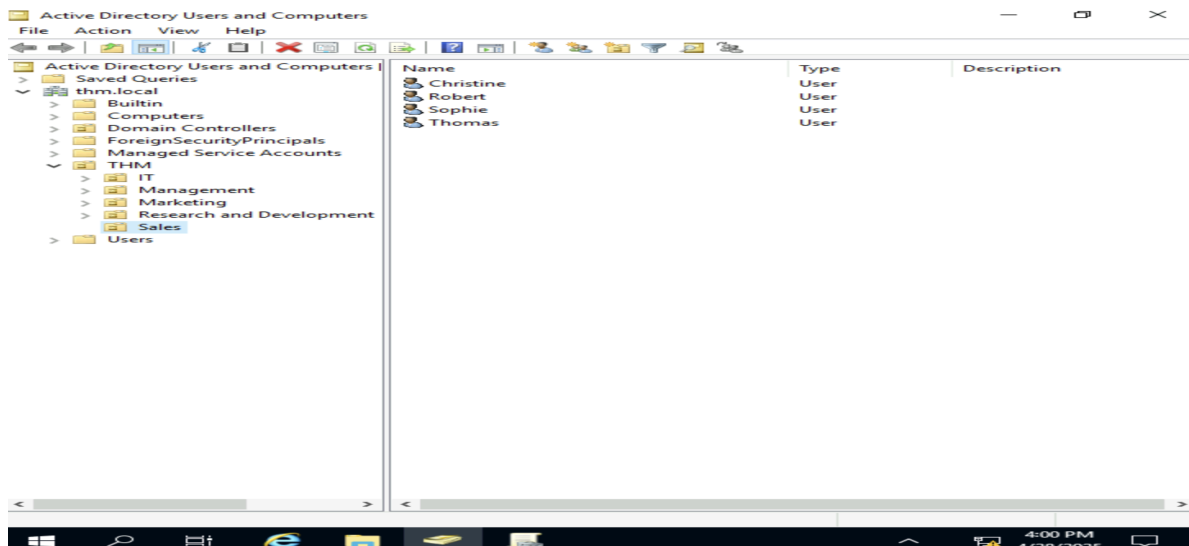
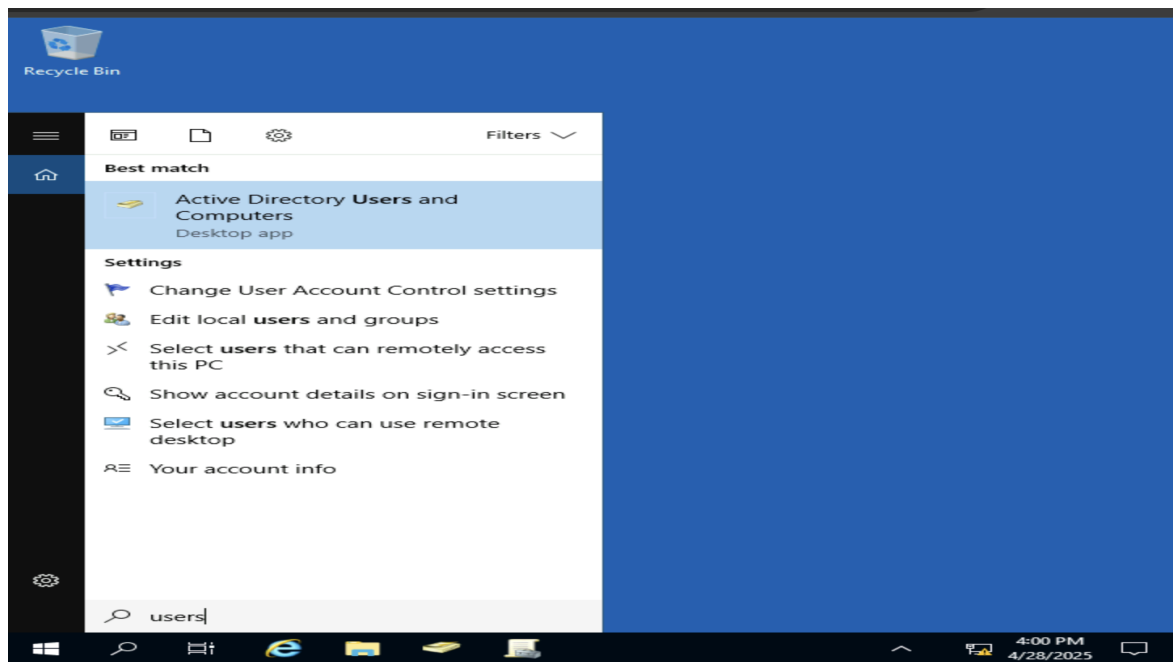
Question 01: In a Windows domain, credentials are stored in a centralised repository called -

Answer: Active Directory

Question 2: The server in charge of running the Active Directory services is called

Answer: Domain Controller

Task 3 - Active Directory :



Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

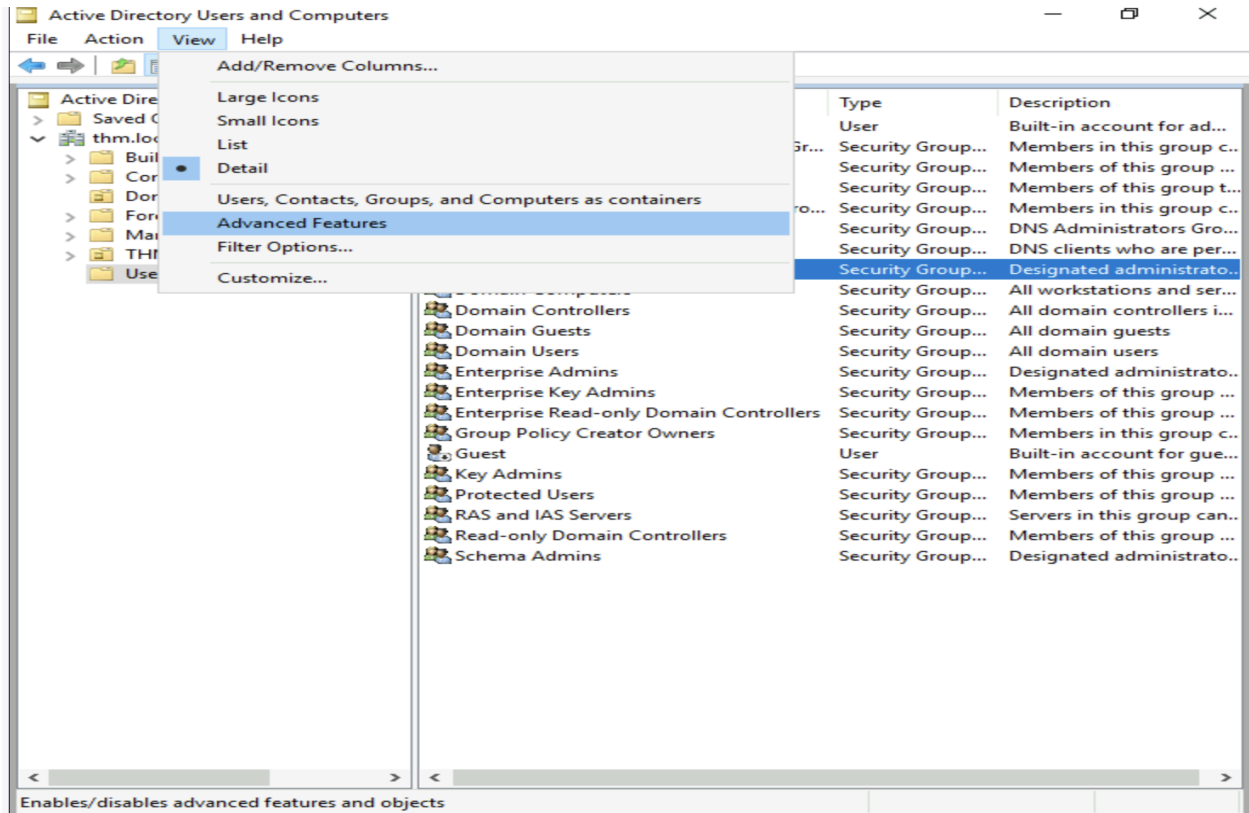
thm.local

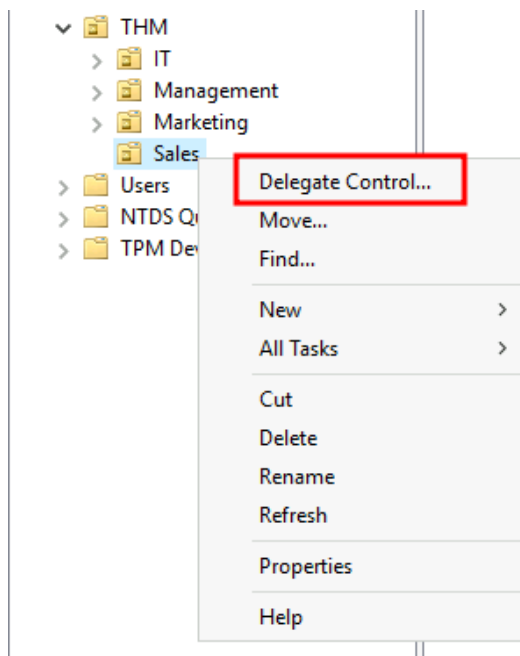
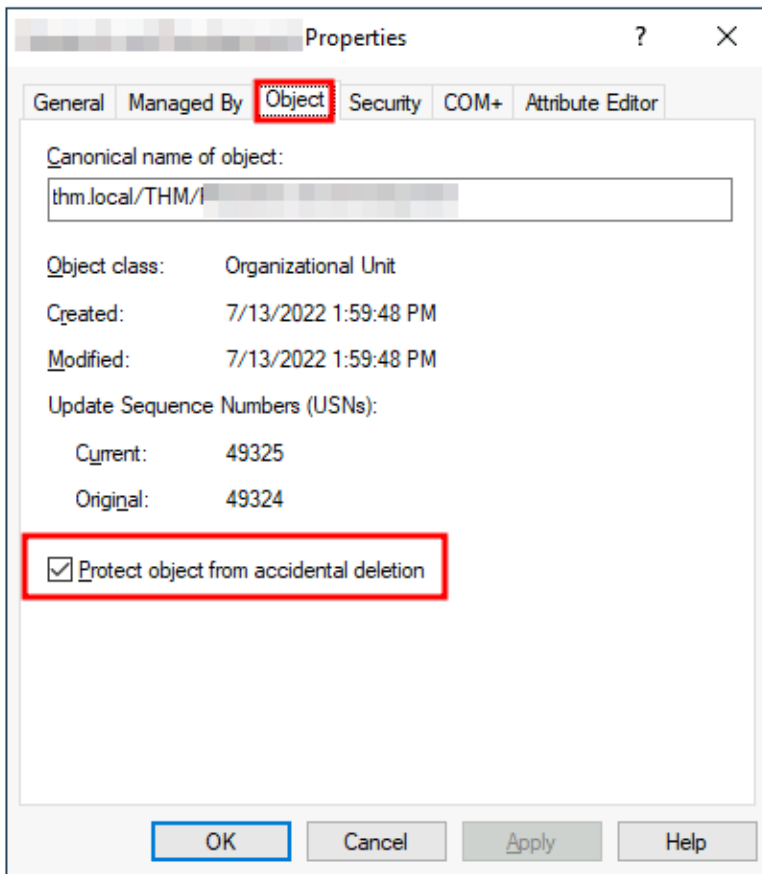
- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- Managed Service Accounts
- THM
- Users

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RODC Password Replication Gr...	Security Group...	Members in this group c...
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controllers	Security Group...	Members of this group t...
Denied RODC Password Replication Gro...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateProxy	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Key Admins	Security Group...	Members of this group ...
Enterprise Read-only Domain Controllers	Security Group...	Members of this group ...
Group Policy Creator Owners	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...
Read-only Domain Controllers	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...

4:03 PM 4/28/2025

Task - 4: Managing Users in AD





Delegation of Control Wizard

Users or Groups
Select one or more users or groups to whom you want to delegate control.

Selected users and groups:

Add... Remove

Select Users, Computers, or Groups

Select this object type:
Users, Groups, or Built-in security principals Object Types...

From this location:
thm.local Locations...

Enter the object names to select (examples):
Phillip (phillip@thm.local) Check Names

Advanced... OK Cancel

Answer the questions below

What was the flag found on Sophie's desktop?

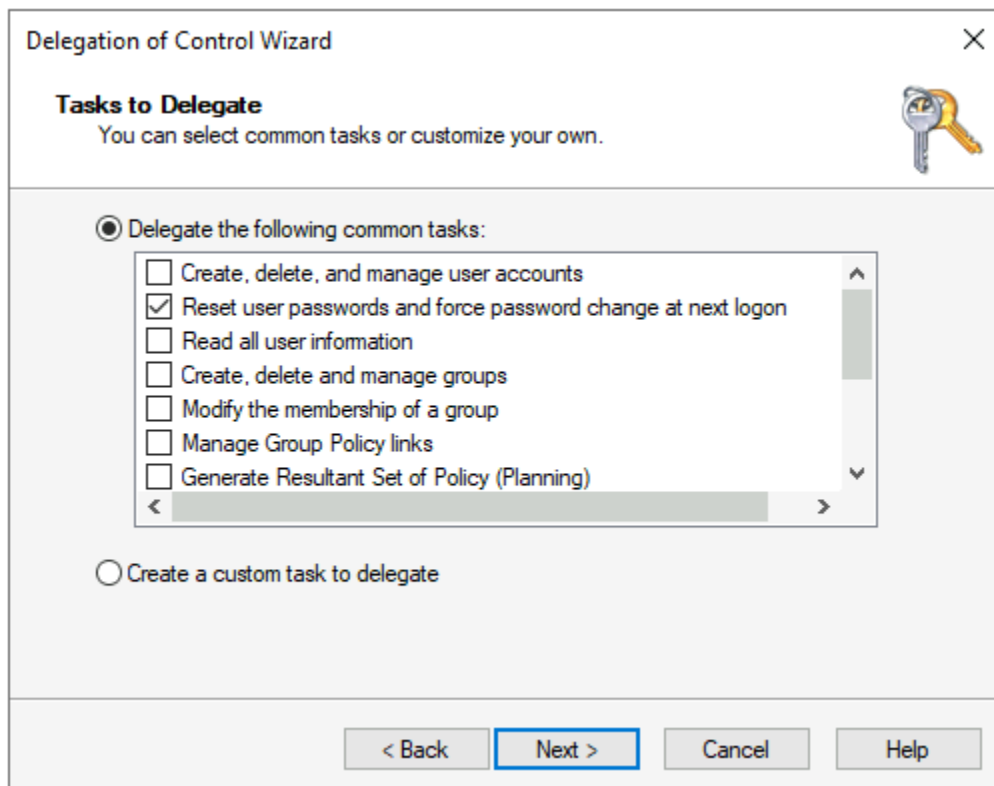
THM{thanks_for_contacting_support}

✓ Correct Answer

The process of granting privileges to a user over some OU or other AD Object is called...

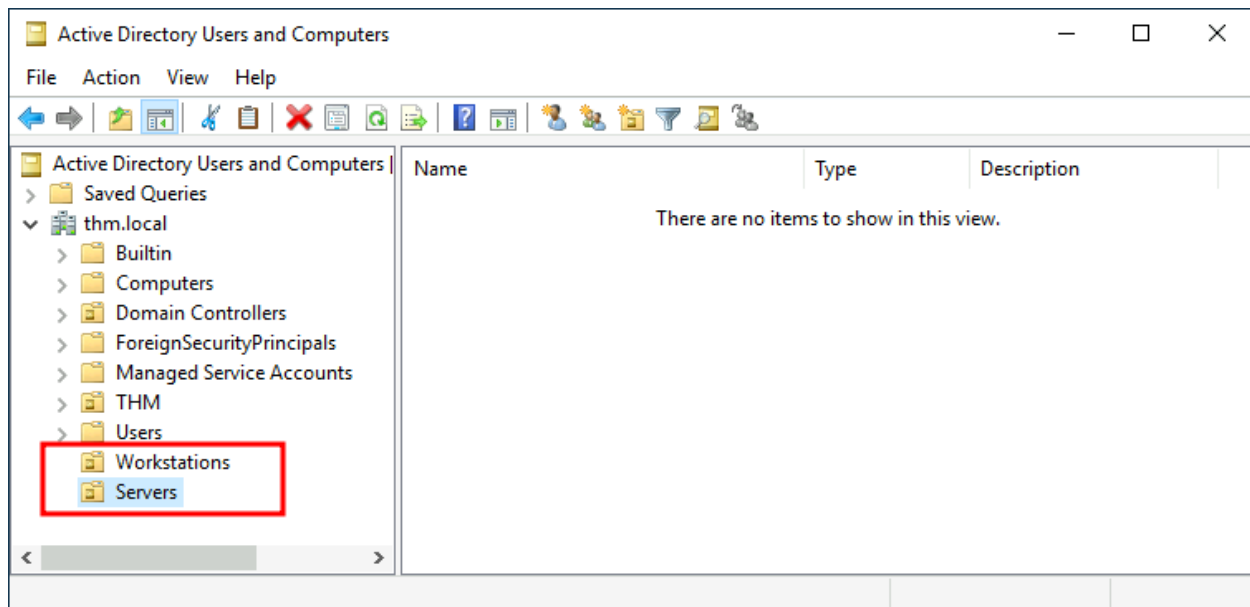
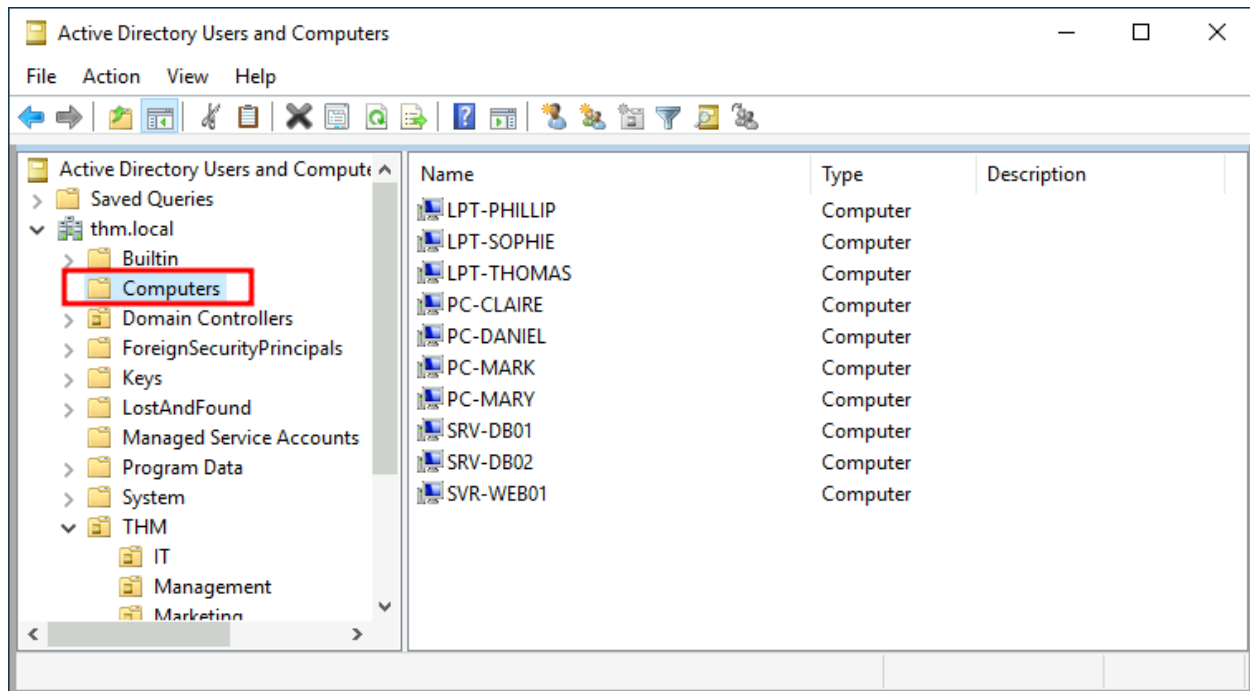
delegation

✓ Correct Answer



The screenshot shows the 'Delegation of Control Wizard' window. The title bar reads 'Delegation of Control Wizard' with a close button (X) on the right. Below the title bar, the section is titled 'Tasks to Delegate' with a subtitle 'You can select common tasks or customize your own.' and a key icon. There are two radio button options: 'Delegate the following common tasks:' (which is selected) and 'Create a custom task to delegate'. The first option is followed by a list box containing the following tasks with checkboxes: 'Create, delete, and manage user accounts', 'Reset user passwords and force password change at next logon' (checked), 'Read all user information', 'Create, delete and manage groups', 'Modify the membership of a group', 'Manage Group Policy links', and 'Generate Resultant Set of Policy (Planning)'. At the bottom of the window are four buttons: '< Back', 'Next >' (highlighted with a blue border), 'Cancel', and 'Help'.

Task -5: Managing Computers in AD:



Answer the questions below

After organising the available computers, how many ended up in the Workstations OU?

7

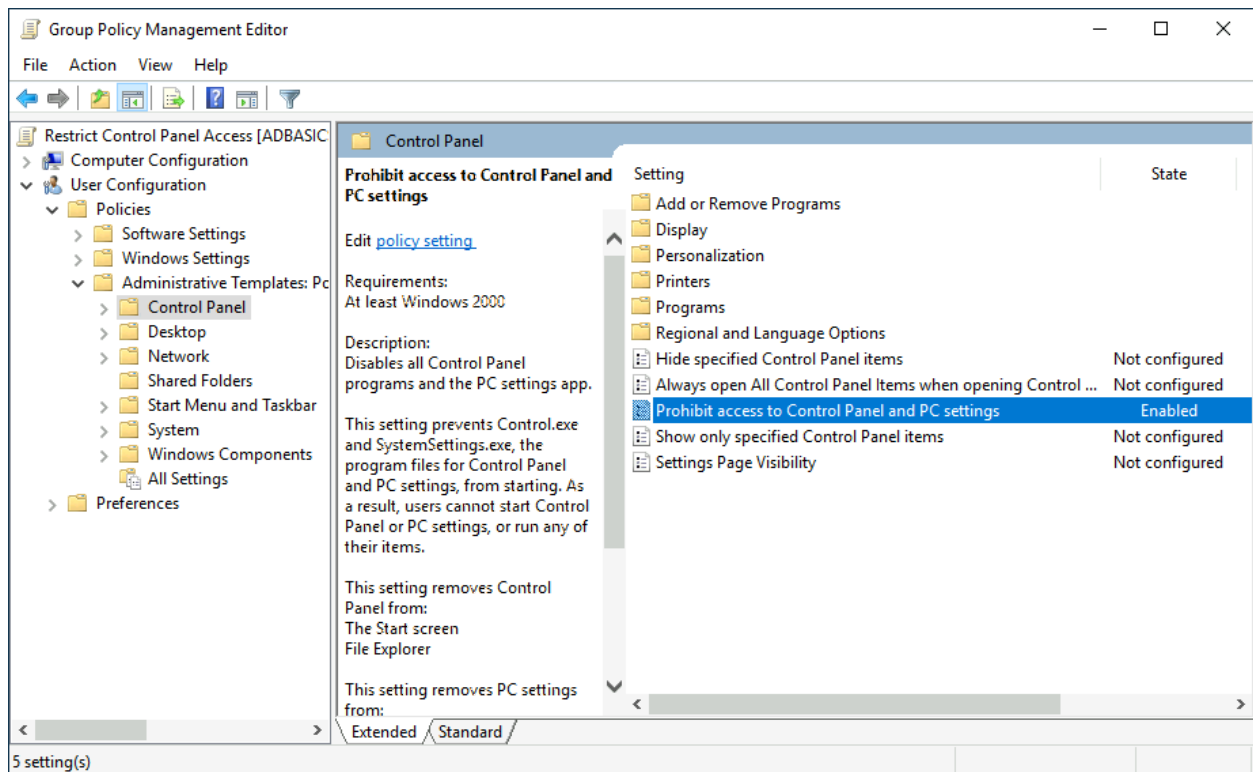
✓ Correct Answer

Is it recommendable to create separate OUs for Servers and Workstations? (yay/nay)

yay

✓ Correct Answer

Task -6: Group Policies



Group Policy Management

FileActionViewWindowHelp

Group Policy Management

Forest: thm.local

Domains

thm.local

Default Domain Policy

RDP policy

Domain Controllers

Default Domain Controllers Policy

THM

Group Policy Objects

Default Domain Controllers Policy

Default Domain Policy

RDP policy

WMI Filters

Starter GPOs

Sites

Group Policy Modeling

Group Policy Results

Default Domain Policy

ScopeDetailsSettingsDelegationStatus

Links

Display links in this location: thm.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled
thm.local	No	Yes

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers

Name
Authenticated Users

Add...RemoveProperties

WMI Filtering

This GPO is linked to the following WMI filter:

<none>

Open

Group Policy Management

FileActionViewWindowHelp

Group Policy Management

Forest: thm.local

Domains

thm.local

Default Domain Policy

RDP policy

Domain Controllers

Default Domain Controllers Policy

THM

Group Policy Objects

Default Domain Controllers Policy

Default Domain Policy

RDP policy

WMI Filters

Starter GPOs

Sites

Group Policy Modeling

Group Policy Results

Default Domain Policy

ScopeDetailsSettingsDelegationStatus

Links

Display links in this location: thm.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled
thm.local	No	Yes

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers

Name
Authenticated Users

Add...

Remove

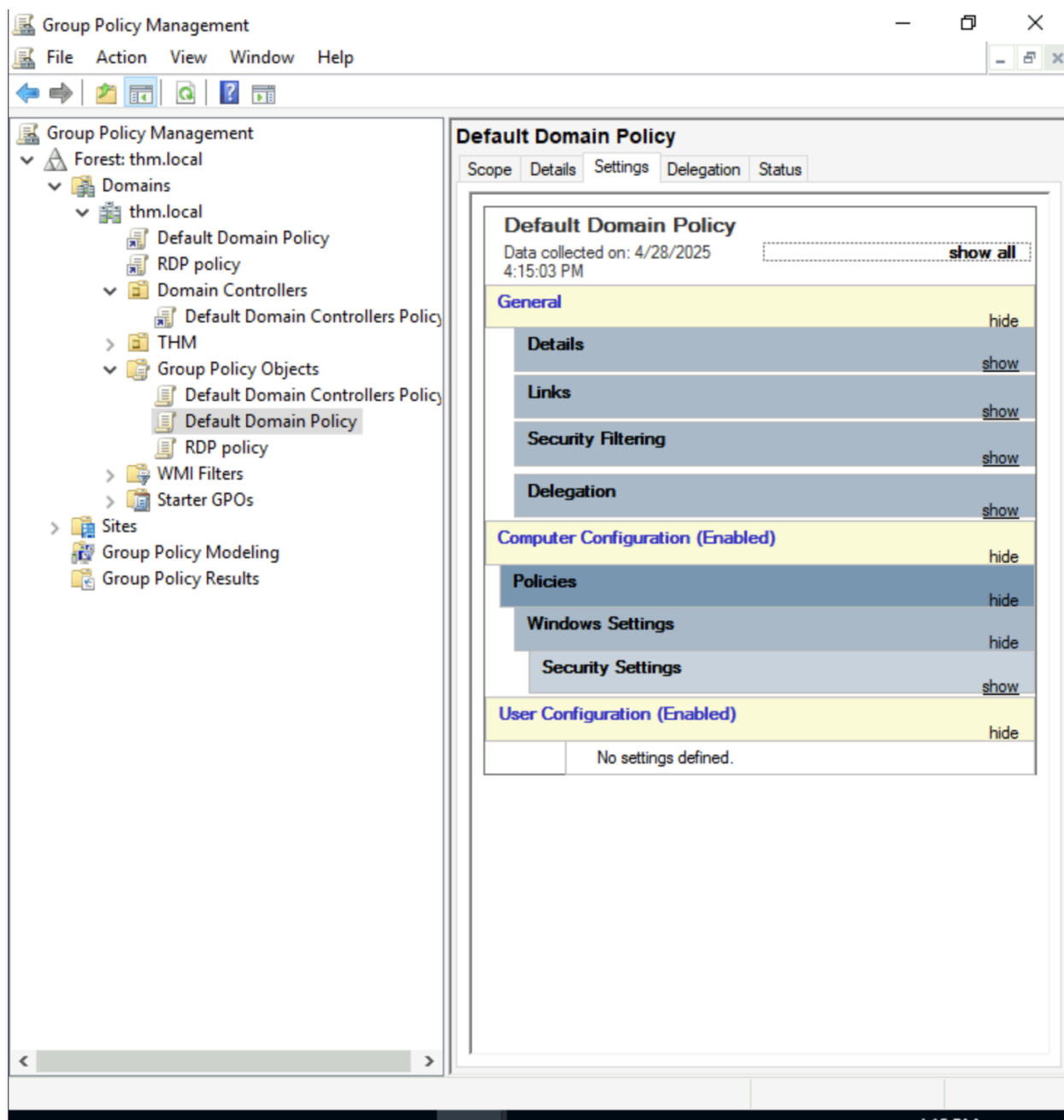
Properties

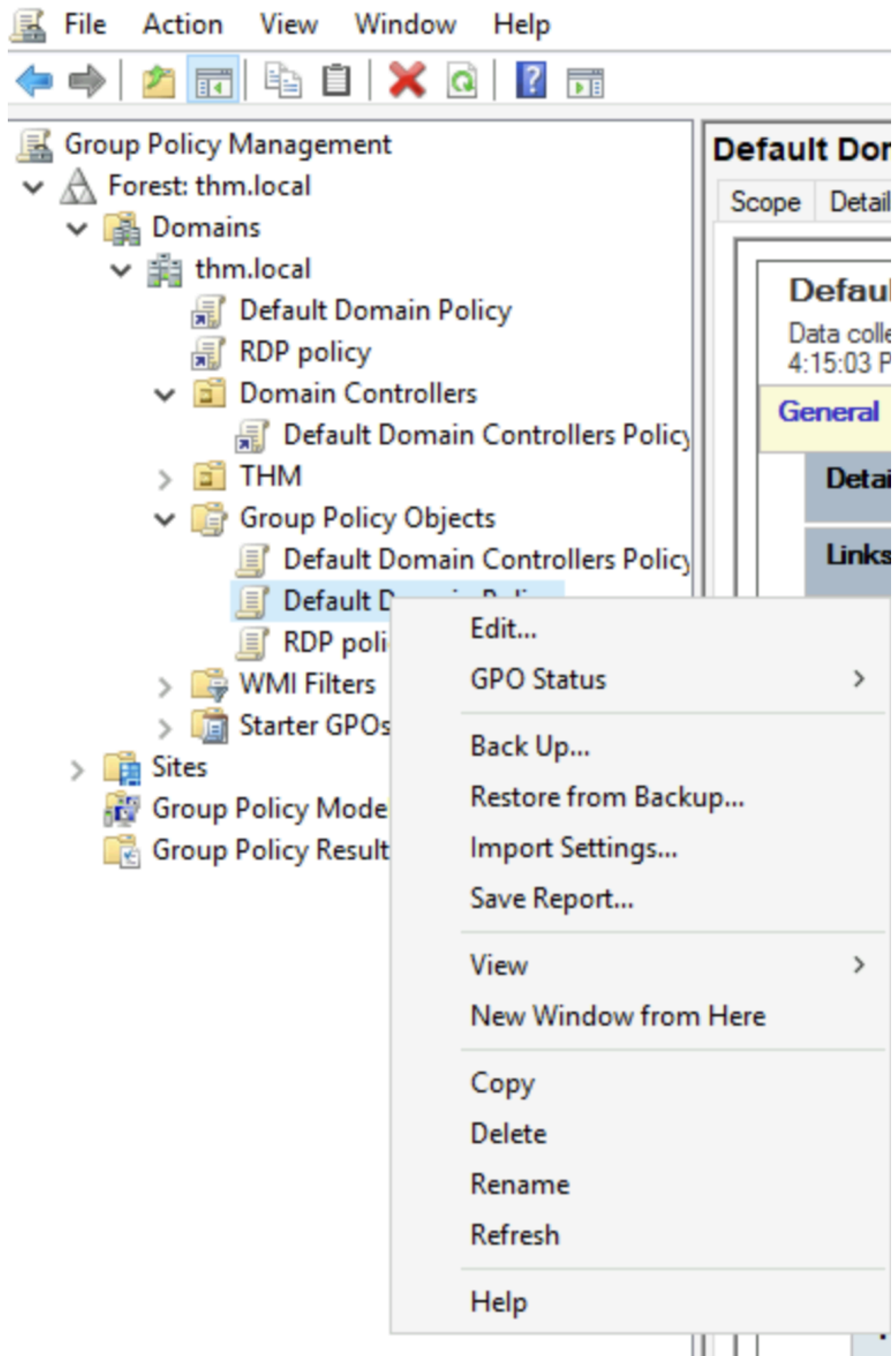
WMI Filtering

This GPO is linked to the following WMI filter:

<none>

Open





Ω

Group Policy Management

File Action View Window Help

Group Policy Management

- Forest: thm.local
 - Domains
 - thm.local
 - Default Domain Policy
 - RDP policy
 - Domain Controllers
 - Default Domain Controllers Policy
 - THM
 - Group Policy Objects
 - Default Domain Controllers Policy
 - Default Domain Policy
 - RDP policy
 - WMI Filters
 - Starter GPOs
 - Sites
 - Group Policy Modeling
 - Group Policy Results

Default Domain Policy

Scope Details Settings Delegation Status

Default Domain Policy

Data collected on: 4/28/2025 4:15:03 PM [show all](#)

General [hide](#)

Details [show](#)

Links [show](#)

Security Filtering [show](#)

Delegation [show](#)

Computer Configuration (Enabled) [hide](#)

Policies [hide](#)

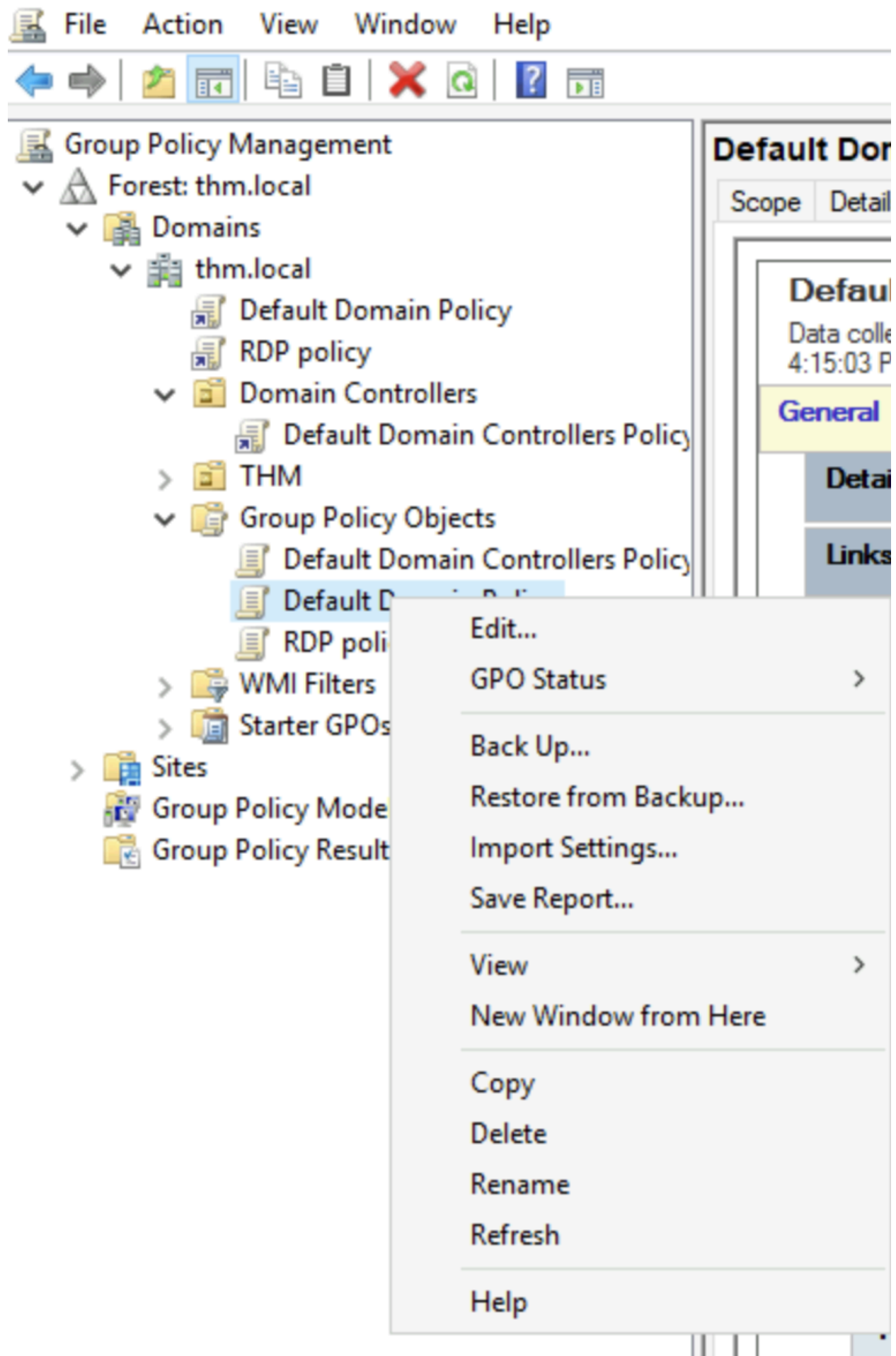
Windows Settings [hide](#)

Security Settings [hide](#)

- Account Policies/Password Policy** [show](#)
- Account Policies/Account Lockout Policy** [show](#)
- Account Policies/Kerberos Policy** [show](#)
- Local Policies/Security Options** [show](#)
- Public Key Policies/Encrypting File System** [show](#)

User Configuration (Enabled) [hide](#)

No settings defined.



Group Policy Management Editor

File Action View Help

Default Domain Policy [ADBASICS.THM.L

Computer Configuration

- 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
 - Event Log
 - Restricted Groups
 - System Services
 - Registry
 - File System
 - Wired Network (IEEE 802.3)
 - Windows Defender Firewall
 - Network List Manager Policies
 - Wireless Network (IEEE 802.11)
 - Public Key Policies
 - Software Restriction Policies
 - Application Control Policies
 - IP Security Policies on Internet
 - Advanced Audit Policy
 - Policy-based QoS
 - Administrative Templates: Policies
 - Preferences
- User Configuration
 - Policies
 - Preferences

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Minimum password length audit Properties



Security Policy Setting

Explain

Minimum password length audit

This security setting determines the minimum password length for which password length audit warning events are issued. This setting may be configured from 1 to 128.

You should only enable and configure this setting when trying to determine the potential impact of increasing the minimum password length setting in your environment.

If this setting is not defined, audit events will not be issued.

If this setting is defined and is less than or equal to the minimum password length setting, audit events will not be issued.

If this setting is defined and is greater than the minimum password length setting, and the length of a new account password is less than this setting, an audit event will be issued.

For more information see <https://go.microsoft.com/fwlink/?LinkId=2097191>.

For more information about security policy and related Windows features, [see the Microsoft website](#).

OK

Cancel

Apply

Answer the questions below

What is the name of the network share used to distribute GPOs to domain machines?

sysvol

✓ Correct Answer

Can a GPO be used to apply settings to users and computers? (yay/nay)

yay

✓ Correct Answer

Task -7: Authentication Method

Answer the questions below

Will a current version of Windows use NetNTLM as the preferred authentication protocol by default? (yay/nay)

nay

✓ Correct Answer

When referring to Kerberos, what type of ticket allows us to request further tickets known as TGS?

Ticket Granting Ticket

✓ Correct Answer

When using NetNTLM, is a user's password transmitted over the network at any point? (yay/nay)

nay

✓ Correct Answer

Task -8: Trees, Forest and Trusts

Answer the questions below

What is a group of Windows domains that share the same namespace called?

Tree

✓ Correct Answer

What should be configured between two domains for a user in Domain A to access a resource in Domain B?

A Trust Relationship

✓ Correct Answer

Task -9: Conclusion

No required tasks

Answer the questions below

Click and continue learning!

No answer needed

🚩 Complete

