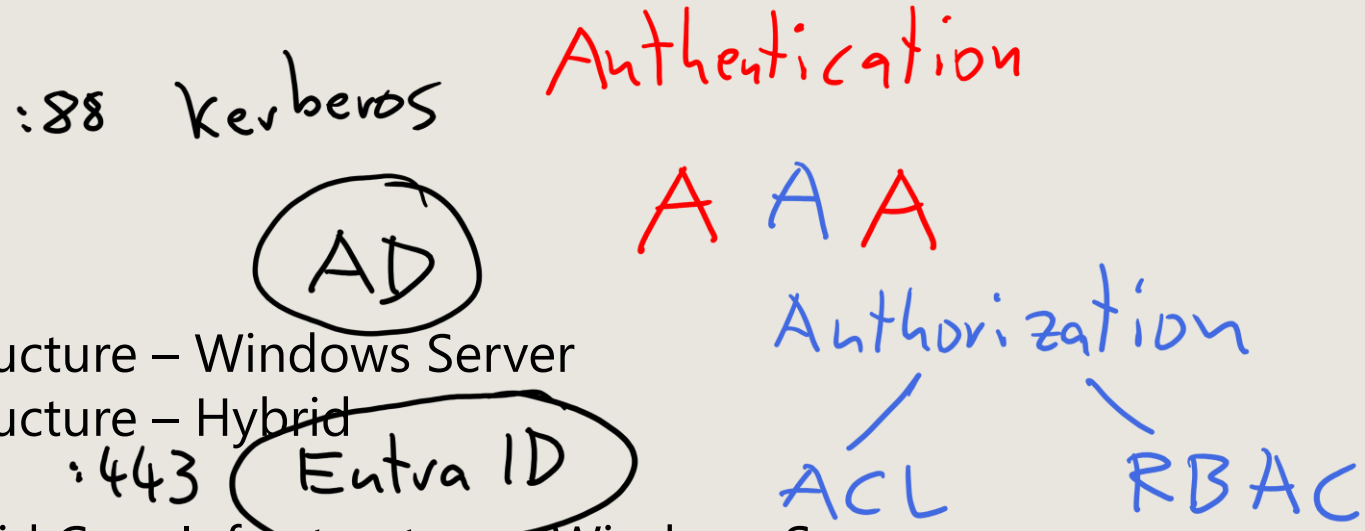
Microsoft

AZ-800 Administer Windows Server Hybrid Core Infrastructure

Agenda AZ-800



1 Deploy and manage identity infrastructure – Windows Server
2 Deploy and manage identity infrastructure – Hybrid

3 Administering Windows Server Hybrid Core Infrastructure – Windows Server
4 Administering Windows Server Hybrid Core Infrastructure – Hybrid

5 Manage virtualization and containers – Windows Server
6 Manage virtualization and containers – Hybrid

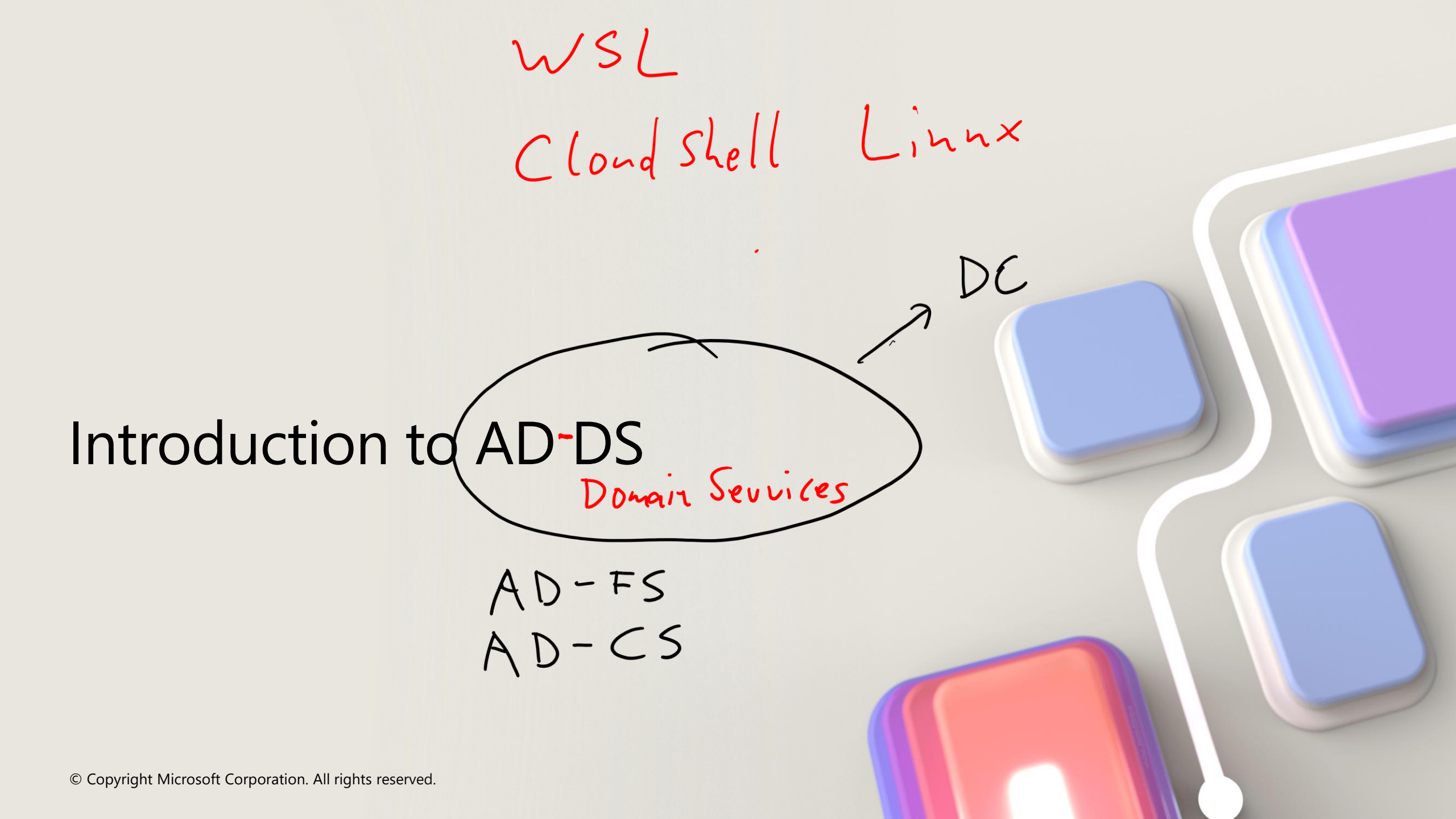
7 Implement and manage networking infrastructure – Windows Server
8 Implement and manage networking Infrastructure – Hybrid

9 Configure storage and file services – Windows Server
10 Configure storage and file services – Hybrid

Deploy and manage identity infrastructure (*Windows Server*)

- Introduction to AD DS
- Manage AD DS domain controllers and FSMO roles
- Implement Group Policy Objects
- Manage advanced features of AD DS
- Lab 01 – Implement identity services and Group Policy

Introduction to AD DS



Learning Objectives – Introduction to AD DS

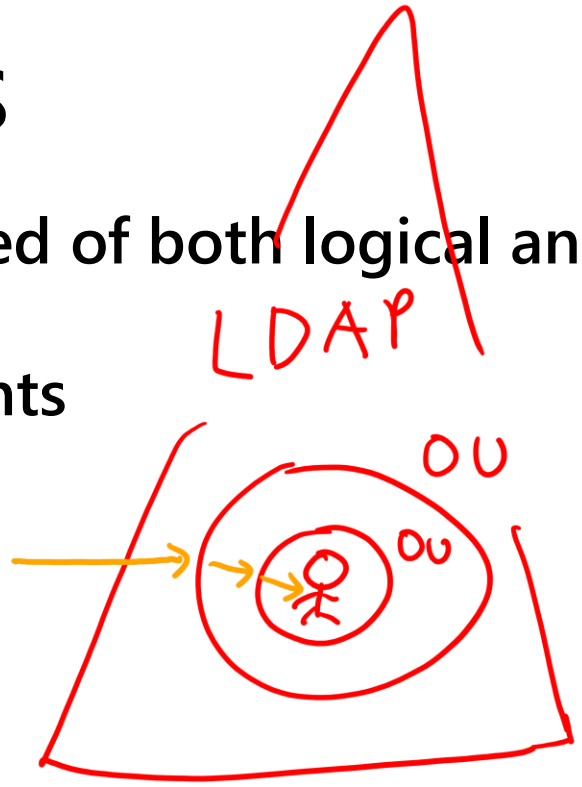
- Define AD DS
- Describe users, groups, and computers
- Identify and describe AD DS forests and domains
- Describe OUs
- Manage objects and their properties in AD DS
- Demonstration – Managing objects in AD DS
- Learning recap

Define AD DS

AD DS is composed of both logical and physical components

Logical components

- Partitions
- Schema
- Domains
- Domain trees
- Forests
- Sites
- OUs
- Containers



Physical components

- Domain controllers
- Data stores
- Global catalog servers
- RODCs

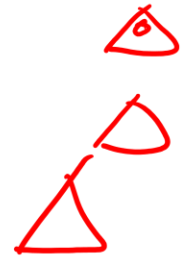
AD DS logical components

Logical component	Description
Partition	A partition, or naming context, is a portion of the AD DS database. Although the database consists of one file named Ntds.dit, different partitions contain different data.
Schema	A schema is the set of definitions of the object types and attributes that you use to define the objects created in AD DS.
Domain	A domain is a logical administrative container for objects such as users and computers. A domain maps to a specific partition, and you can organize the domain with parent-child relationships to other domains.
Domain tree	A domain tree is a hierarchical collection of domains that share a common root domain and a contiguous Domain Name System (DNS) namespace.
Forest	A forest is a collection of one or more domains that have a common AD DS root, a common schema, and a common global catalog.
OU	An OU is a container object for users, groups, and computers that provides a framework for delegating administrative rights and administration by linking Group Policy Objects (GPOs).
Container	A container is an object that provides an organizational framework for use in AD DS. You can use the default containers, or you can create custom containers. You can't link GPOs to containers.

What is an AD DS forest?

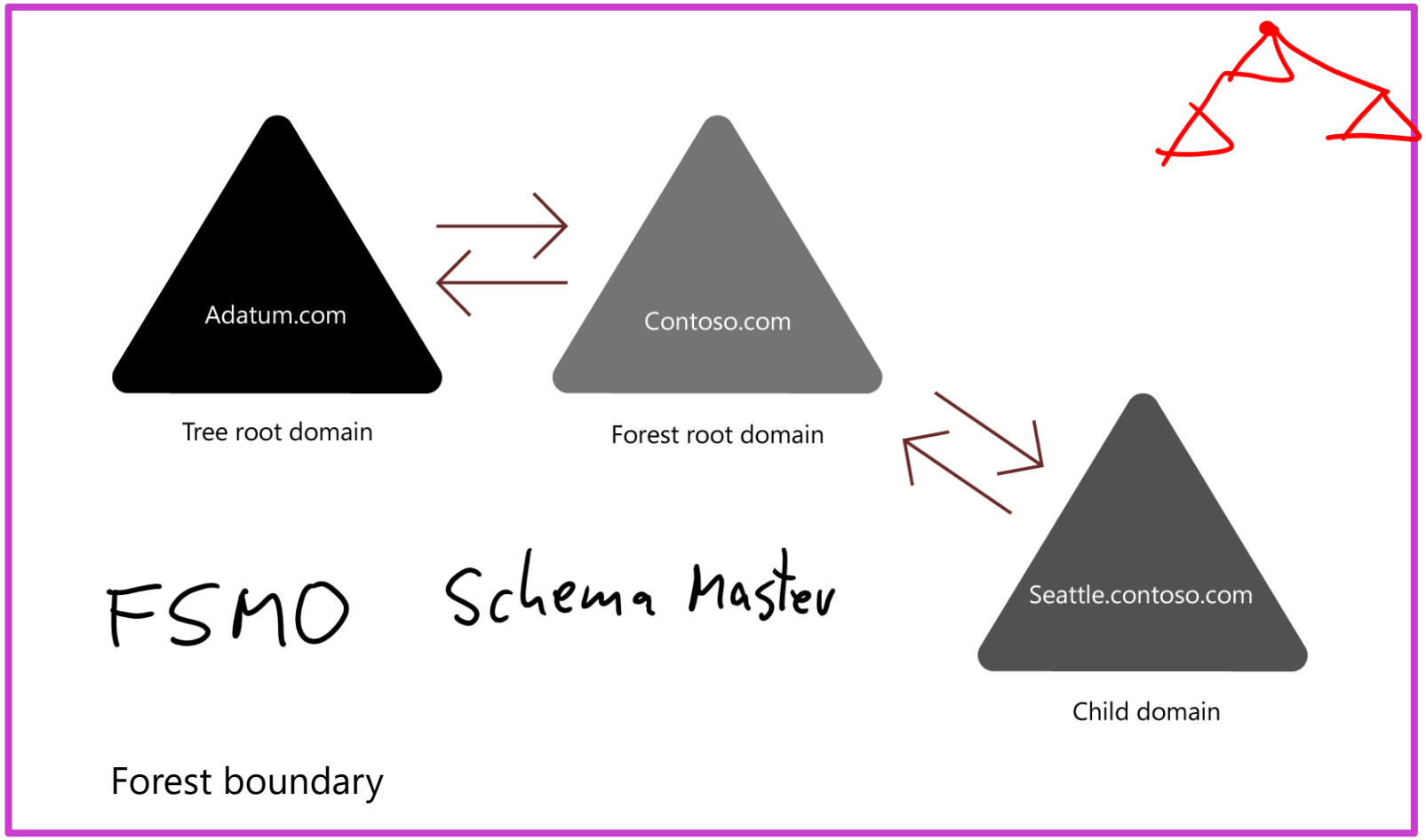
Domain
Tree
Forest

Domäne
Struktur
Gesamtstruktur



A Forest is a top-level container in AD DS

- A unique implementation of AD DS that has a 1:1 relationship with its schema.
- Made up of one or more trees, that themselves are made up of one or more domains
- Trust relationships
  - Provide access to resources in a complex AD DS environment



What is an AD DS domain?

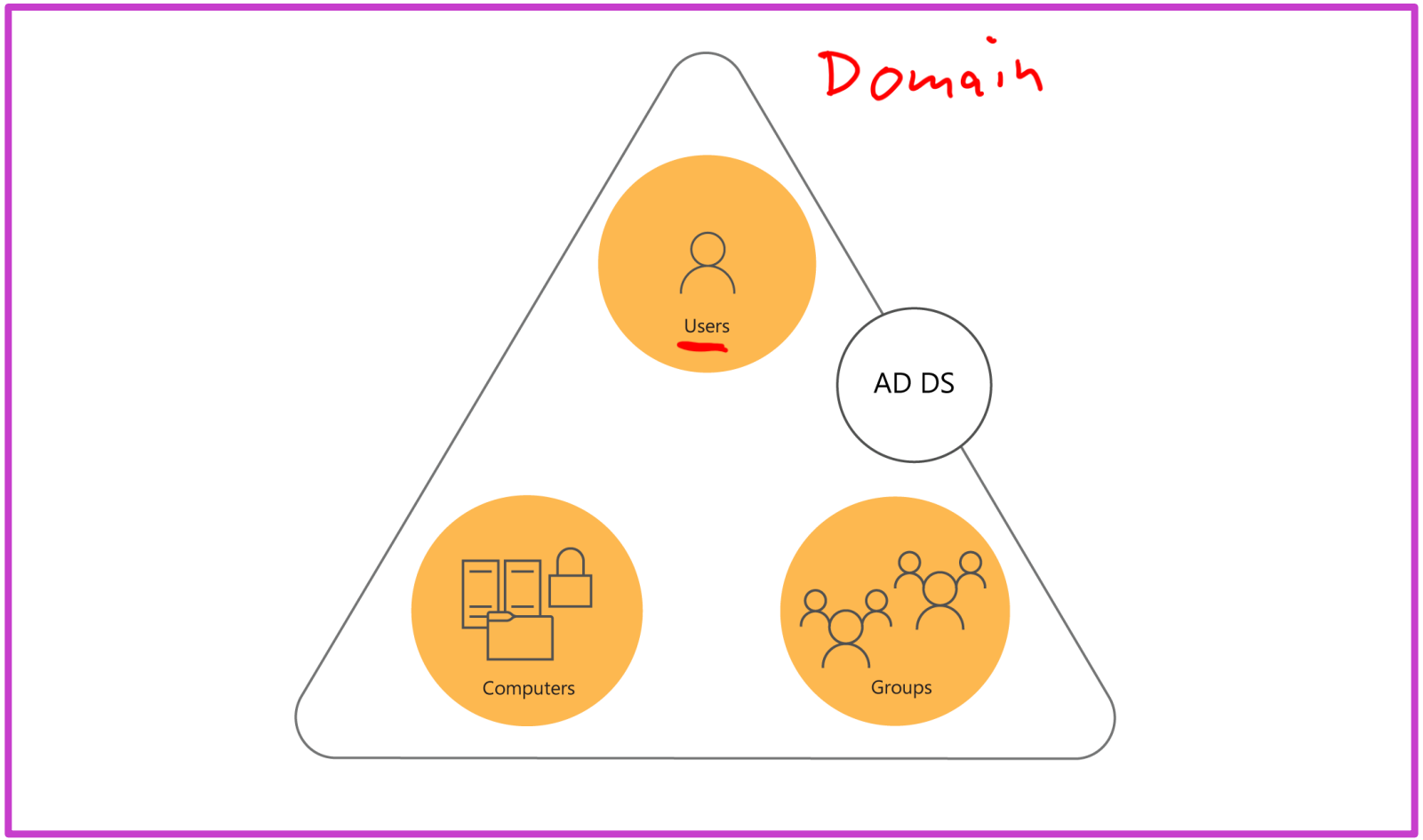
AD DS domains are logical containers for managing users, computers, groups, and other objects

AD DS domain is often described as:

- A replication boundary
- An administrative unit

An AD DS domain provides:

- Authentication
- Authorization



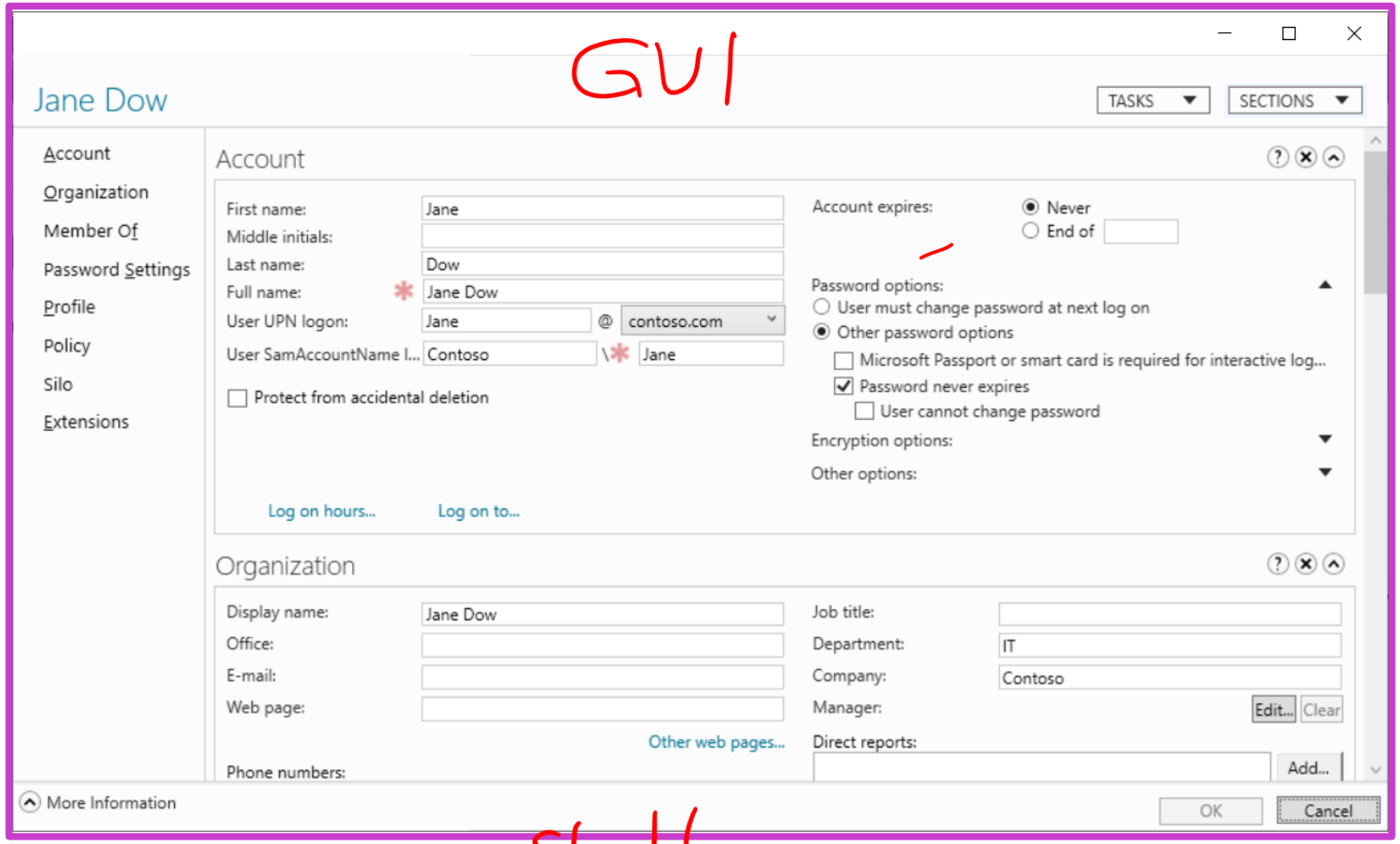
Define user objects

ADAC

Create user objects

A user account includes:

- The username
- A user password
- Group memberships



Define group objects

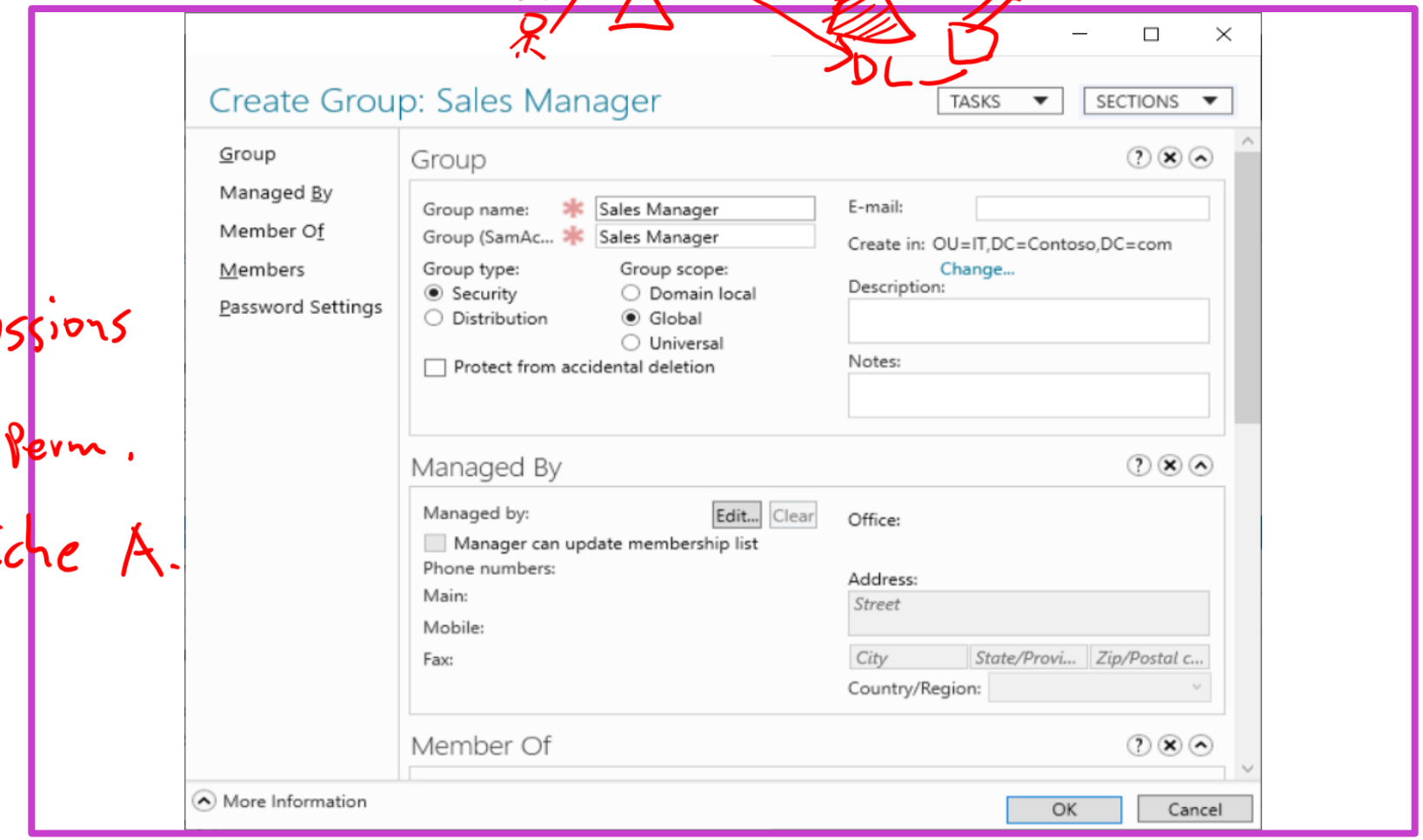
What are group objects?

Group types

- Security
- Distribution

Group scopes

- Local
- Domain-local
- Global
- Universal

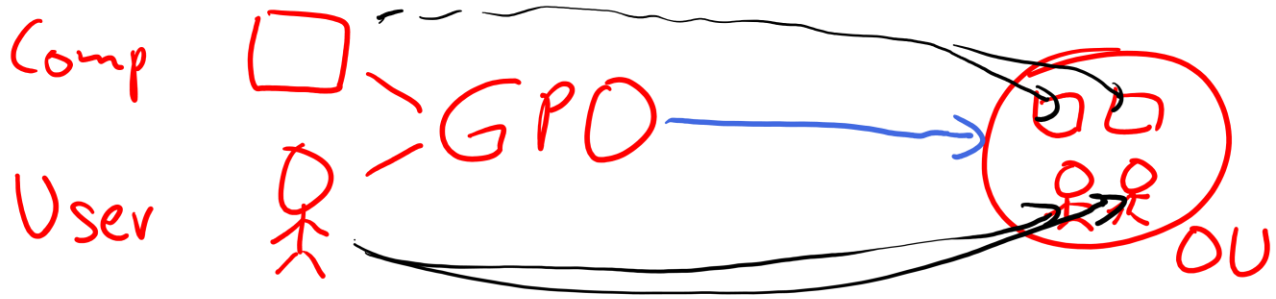


P
↑
DL
G
↑
A

Permissions für Perm. gleiche A.

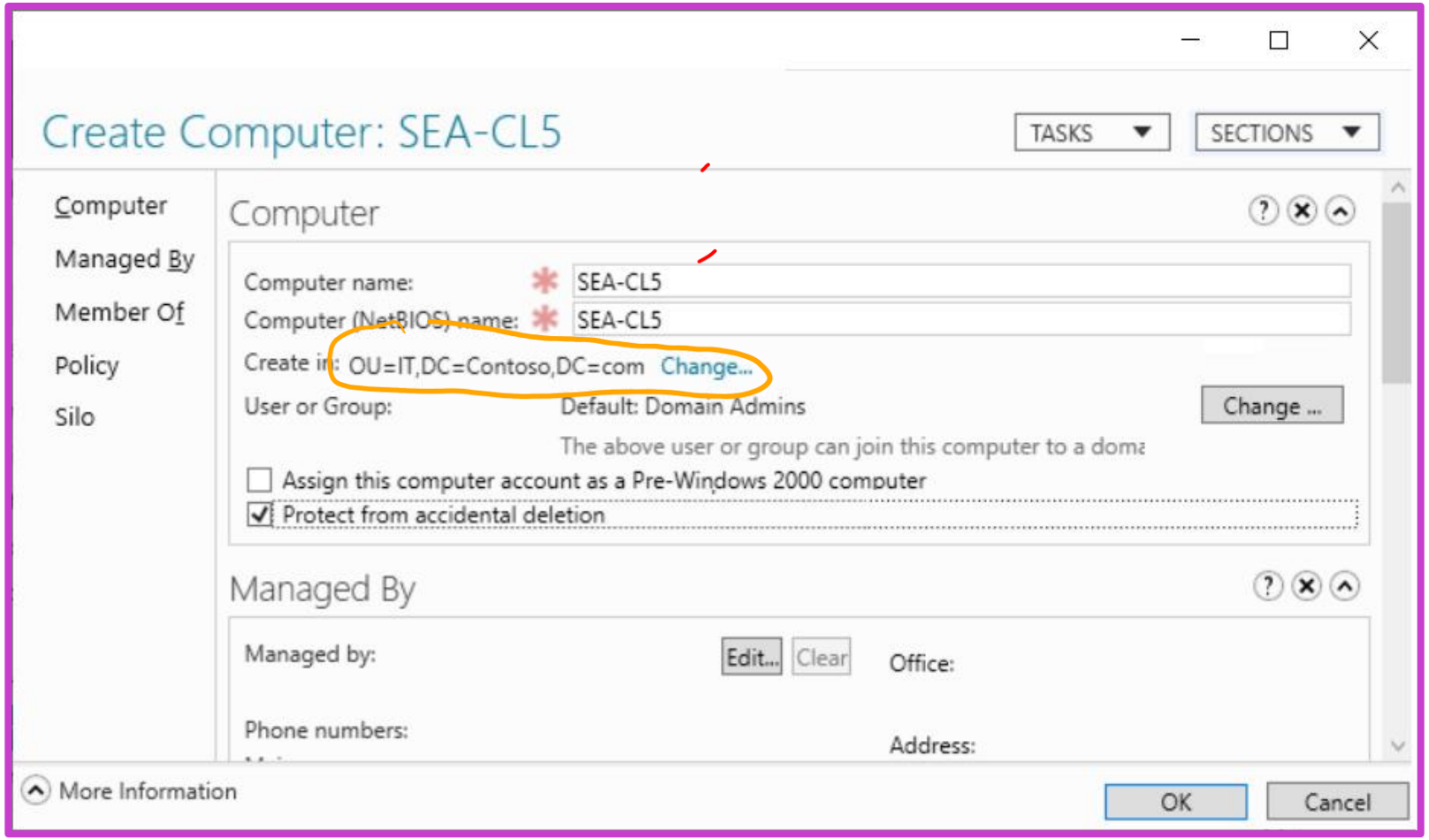
Account

Define computer objects



Computers are security principals:

- They have an account with a sign-in name and password.
- They authenticate with the domain.
- They can belong to groups and have access to resources



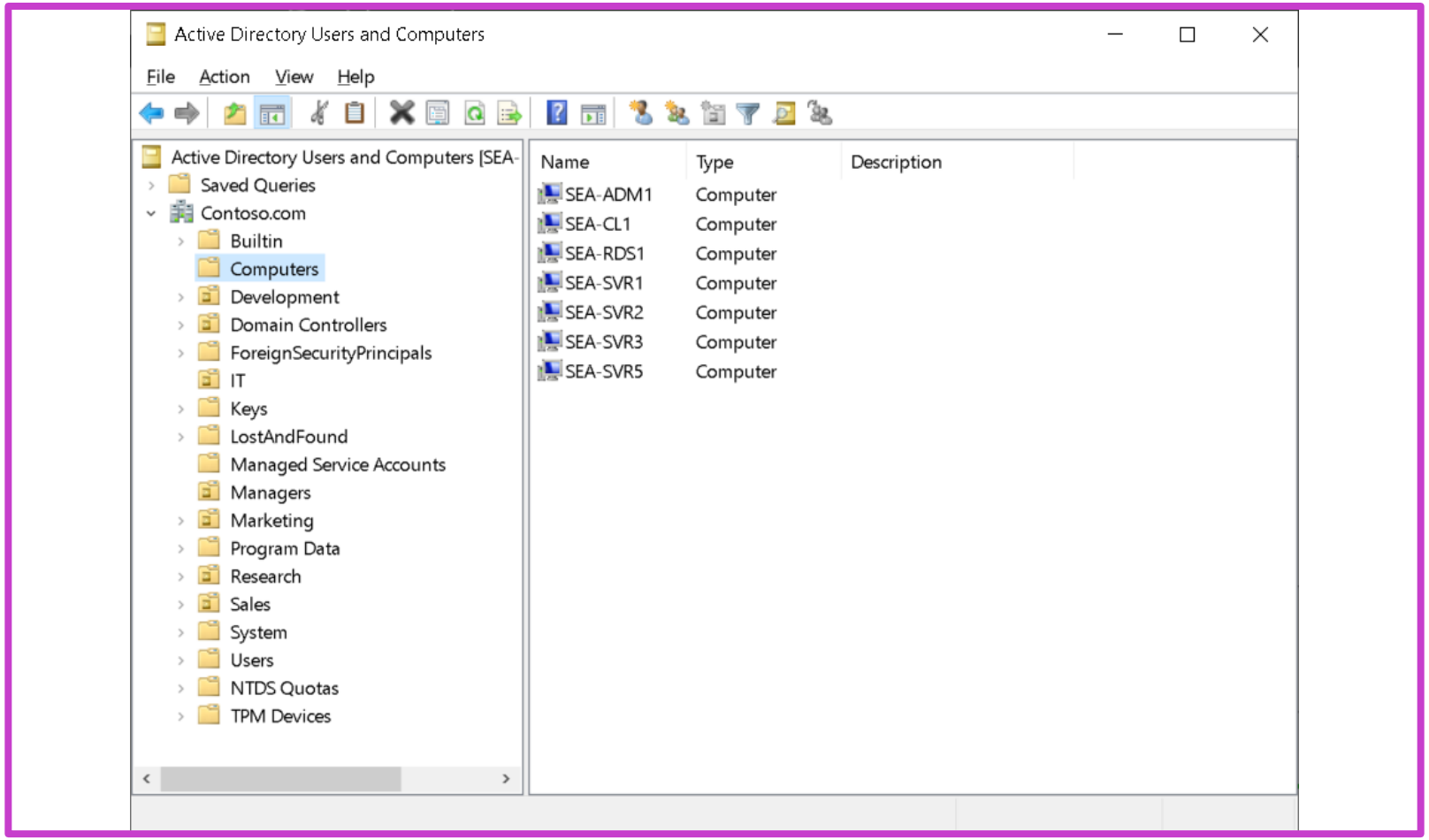
Define OUs

Use containers to group objects within a domain

- You cannot apply GPOs to containers
- Containers are used for system objects and as the default location for new objects

Create OUs to:

- Configure objects by assigning GPOs to them
- Delegate administrative permissions



Comparing service accounts

Standalone managed service accounts (sMSA)	Group managed service accounts (gMSA)	Delegated managed service accounts (dMSA)
Managed by Active Directory	Managed by Active Directory	Managed by administrators with device identity binding
Used for single server applications	Used for multiple server applications	Suitable for applications needing to run on specific serves with controlled access
Automatic password management	Automatic password management	Passwords are automatically updated and machine-bound
Simplified SPN management	Automatic SPN management	Enhanced security with Credential Guard
Requires Windows Server 2008 R2 or later	Active Directory domain and forest functional level must be Windows Server 2012 or later	Requires Windows Server 2025

AD DS management tools

Management Tools	Description
Windows Admin Center	Windows Admin Center is a web-based console that you can use to manage server computers and computers that are running Windows 11
Remote Server Administration Tools	RSAT is a collection of tools which enables you to manage Windows Server roles and features remotely.
Active Directory module for Windows PowerShell	The Active Directory module for Windows PowerShell supports AD DS administration, and it's one of the most important management components.
Active Directory Users and Computers	Active Directory Users and Computers is a Microsoft Management Console (MMC) snap-in that manages most common resources, including users, groups, and computers
Active Directory Sites and Services	The Active Directory Sites and Services MMC snap-in manages replication, network topology, and related services.
Active Directory Domains and Trusts	The Active Directory Domains and Trusts MMC snap-in configures and maintains trust relationships at the domain and forest functional levels.
Active Directory Schema snap-in	The Active Directory Schema MMC snap-in examines and modifies the definitions of AD DS attributes and object classes.

Demonstration – Managing objects in AD DS

Navigate within the Active Directory Administrative Center	Perform an administrative task within the Active Directory Administrative Center	Create objects and view all object attributes	Use the Windows PowerShell History viewer

Azure Powershell
CLI
Templates
(Bicep, Terraform)

Learning recap – Introduction to AD DS

Microsoft Learn Modules (docs.microsoft.com/Learn)

Introduction to AD DS

Module assessment

Manage AD DS domain controllers and FSMO roles

Learning Objectives – AD DS DCs and FSMO roles

- What is a DC?
- Deploy AD DS domain controllers
- Maintain AD DS domain controllers
- Manage the AD DS global catalog role
- Manage AD DS operations masters
- Manage AD DS schema
- Demonstration - Transfer FSMO roles
- Learning recap

What is a DC?

Domain controllers are servers that host the AD DS database (**Ntds.dit**) and **SYSVOL**

Host the Kerberos authentication service KDC services to perform authentication :88

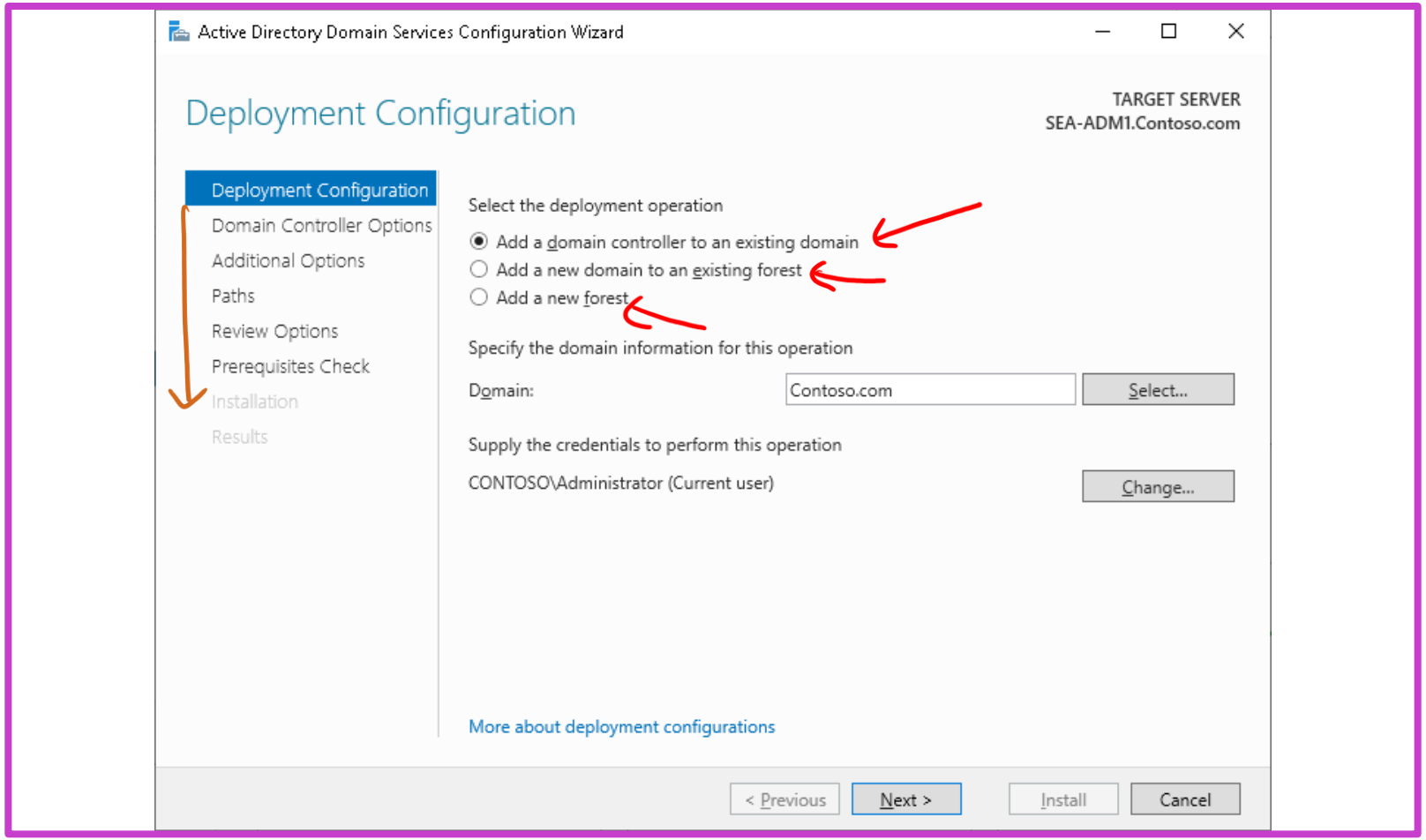
Have best practices for:

- **Availability** – Use at least two domain controllers in a domain
- **Security** – Use an RODC and BitLocker

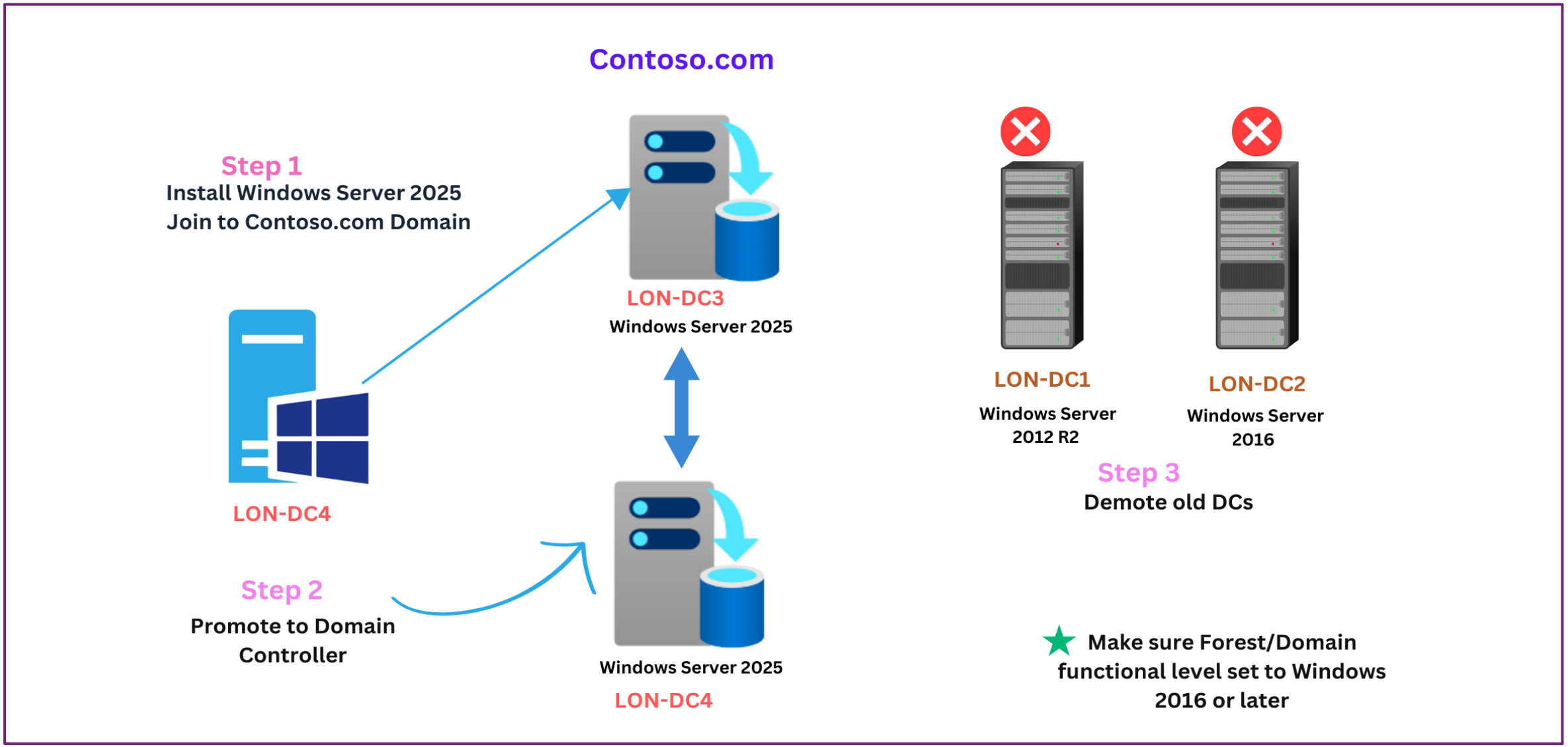
Deploy AD DS domain controllers

- Install a domain controller from Server Manager
- Install a domain controller on a Server Core installation of Windows Server

dcpromo



Upgrade from a previous version of AD DS



Domain and forest functional levels

Domain and forest functional levels:

- Determine the available AD DS capabilities within a domain or across a forest.
- Control which Windows Server operating systems can run on domain controllers in the domain or forest.

Operating system independence

- Functional levels do not dictate the operating systems that can run on workstations and member servers within the domain or forest.
- Operating systems and functional levels can be different.

Backward compatibility

- Functional levels can be raised to take advantage of new features. Rolling back requires using PowerShell or a forest recovery.

Deploy AD DS domain controllers in Azure VMs

When you implement AD DS in Azure, consider the following:

- **Network topology**. If you intend to join an existing on-premises AD DS infrastructure, you should extend network connectivity to your on-premises environment
- **Site topology**. Define and configure an AD DS site corresponds to the IP address space of your Azure Virtual Network.
- **IP addressing**. All Azure VMs receive Dynamic Host Configuration Protocol (DHCP) addresses by default, but you can configure static addresses.
- **DNS**. Azure's built-in DNS does not meet the requirements of AD DS, such as Dynamic DNS and service (SRV) resource records. Use Windows Server DNS server role.
- **Disks**. You have control of caching Azure VM disk configurations. When you install AD DS to an Azure VM, you should place the NTDS.DIT and SYSVOL files on one of its data disks

Maintain AD DS domain controllers

Plan for AD DS backup and restore

Restoring deleted AD DS objects by using Recycle Bin

Windows Server offers the **Active Directory Recycle Bin** feature.

AD DS backup and restore must explicitly include system state data

- **Nonauthoritative restore**
  By default, restoring a domain controller's information from backup only temporarily restores it as of the date of the backup. Once the recovered domain controller replicates with current domain controllers its stale information will be updated to reflect all changes since the backup.
- **Authoritative restore**
  An authoritative restore allows you to restore a known good copy of AD DS objects, which replaces the current version of these objects in the AD DS database.

Manage the AD DS global catalog role

Global catalog – Partial read-only, searchable copy of all the objects in a forest

- Helps speed up searches for objects that might be stored on domain controllers in a different domain in the forest Data store
- Doesn’t contain all the attributes for each object

Configure the environment for the global catalog

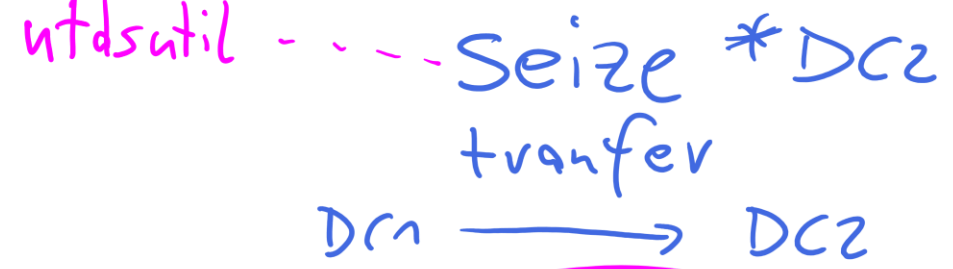
- **Single domain** – Configure all the domain controllers to hold a copy of the global catalog
- **Multiple-domain environment** – Infrastructure master should not be a global catalog server unless all the domain controllers in the domain are also global catalog servers
- **Multiple sites** – Make at least one domain controller at each site a global catalog server

Manage AD DS operations masters

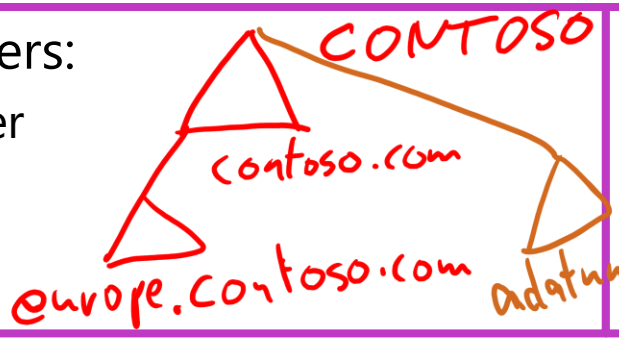
In the multimaster replication model, some operations must be single master operations

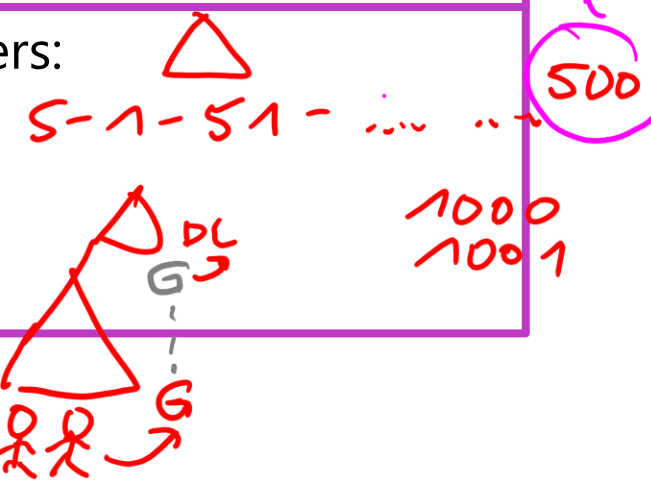
Many terms are used for single master operations in AD DS, including:

- Operations master (or operations master role)
- Single master role
- FSMO



The five FSMOs	
Forest operations masters: • Domain naming master • Schema master	Domain operations masters: • RID master • Infrastructure master • PDC emulator master





Demonstration – Transfer FSMO roles

Create a single domain AD DS forest containing two domain controllers

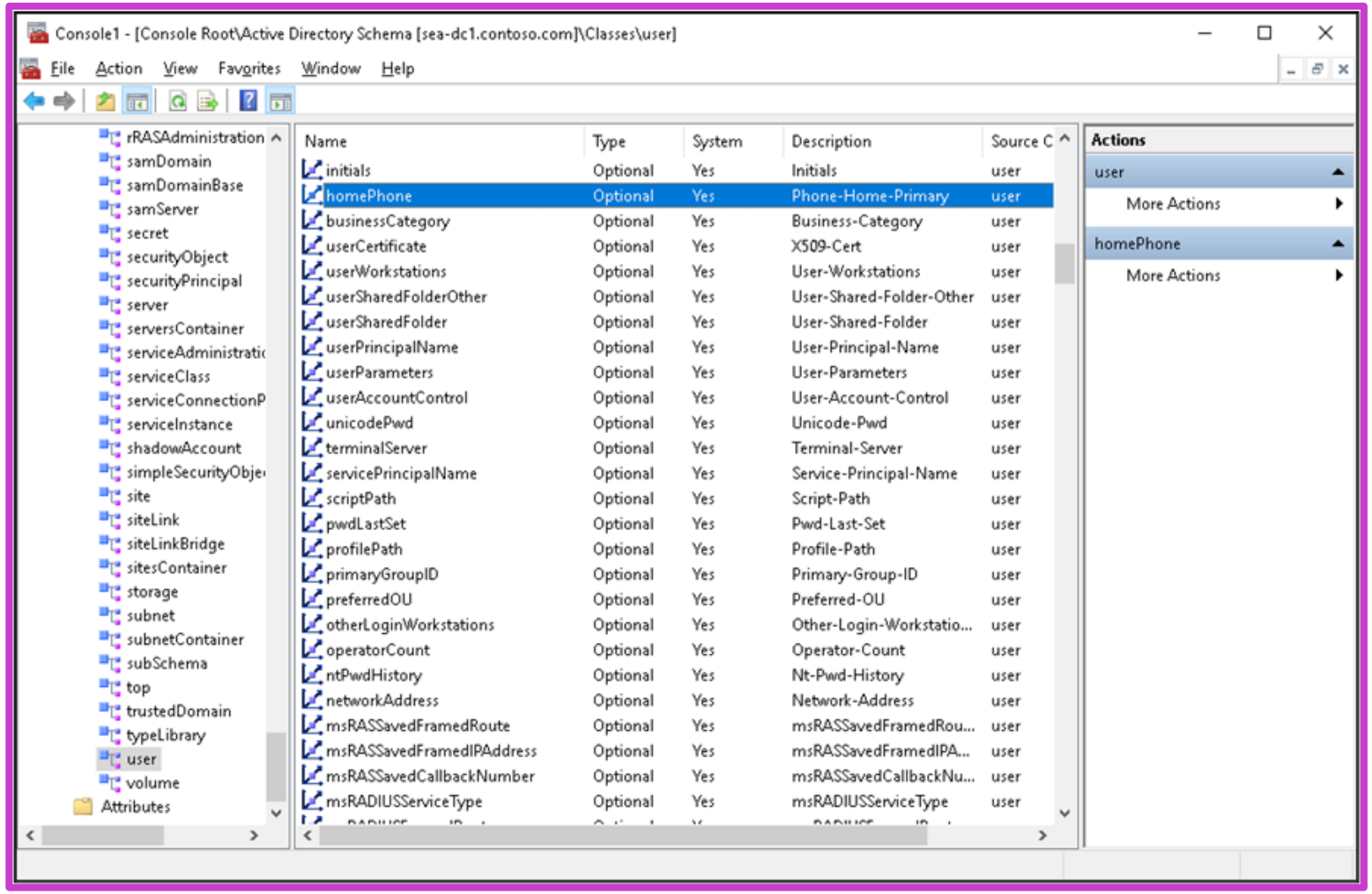
Check the placement of operations master roles

Transfer operations master roles between domain controllers by using the GUI tools

Transfer operations master roles between domain controllers by using command-line tools

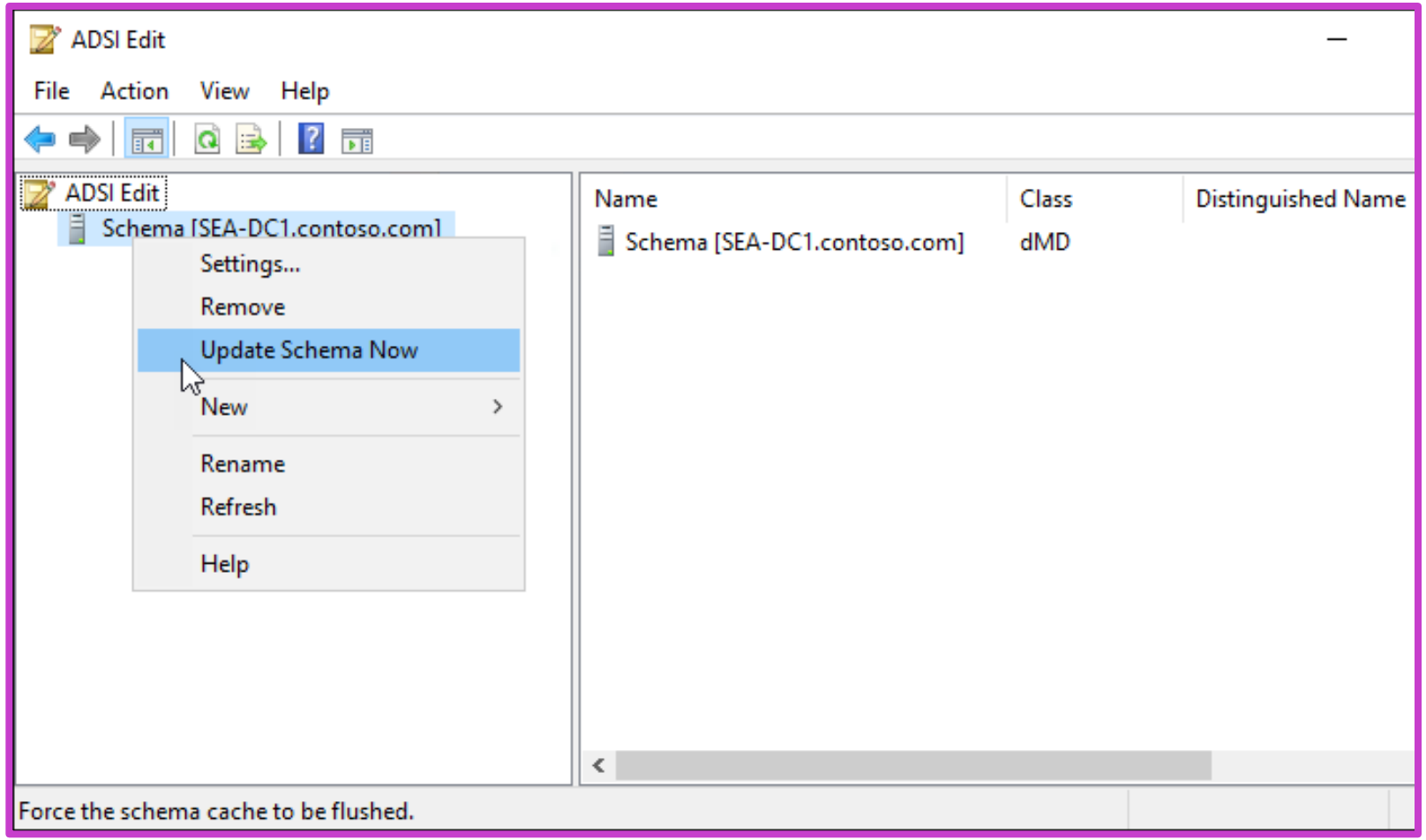
What is a schema?

- AD DS schema is the component that defines the rules and syntax of the AD DS database.
- AD DS uses objects as units of storage.
- Relationships among objects, rules, attributes, and classes



Manage AD DS schema

- Only members of the Schema Admins group in the root domain of the AD DS forest can modify the schema
- AD DS schema does not support deletions
- Change the schema only when necessary because the schema controls the storage of information



Learning recap – Manage AD DS domain controllers and FSMO roles

Microsoft Learn Modules (docs.microsoft.com/Learn)

Manage AD DS domain controllers and FSMO roles

Module assessment

AD — Authentication — Kerberos
AD — Config — GPO

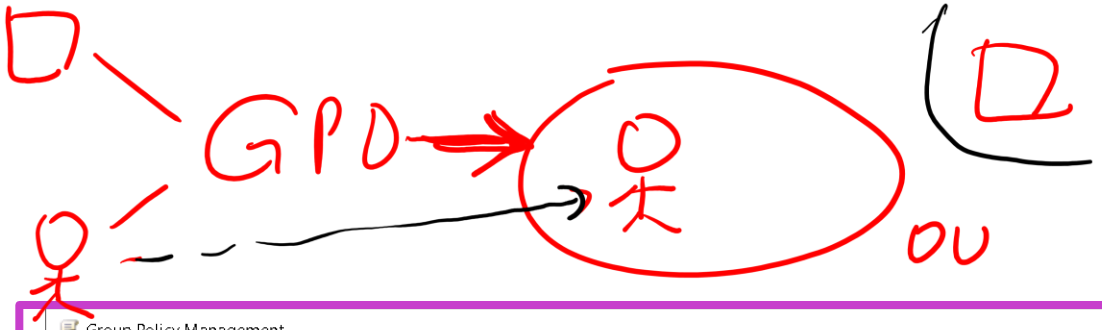
Implement Group Policy Objects

EntraID — Authentication — OAuth / OIDC
Intune — Config

Learning Objectives – Implement Group Policy Objects

- Define GPOs
- Implement GPO scope and inheritance
- Domain-based GPOs
- Demonstration - Create, configure, and apply GPOs
- Explain GPO storage
- Define administrative templates
- Learning recap

What is Group Policy?

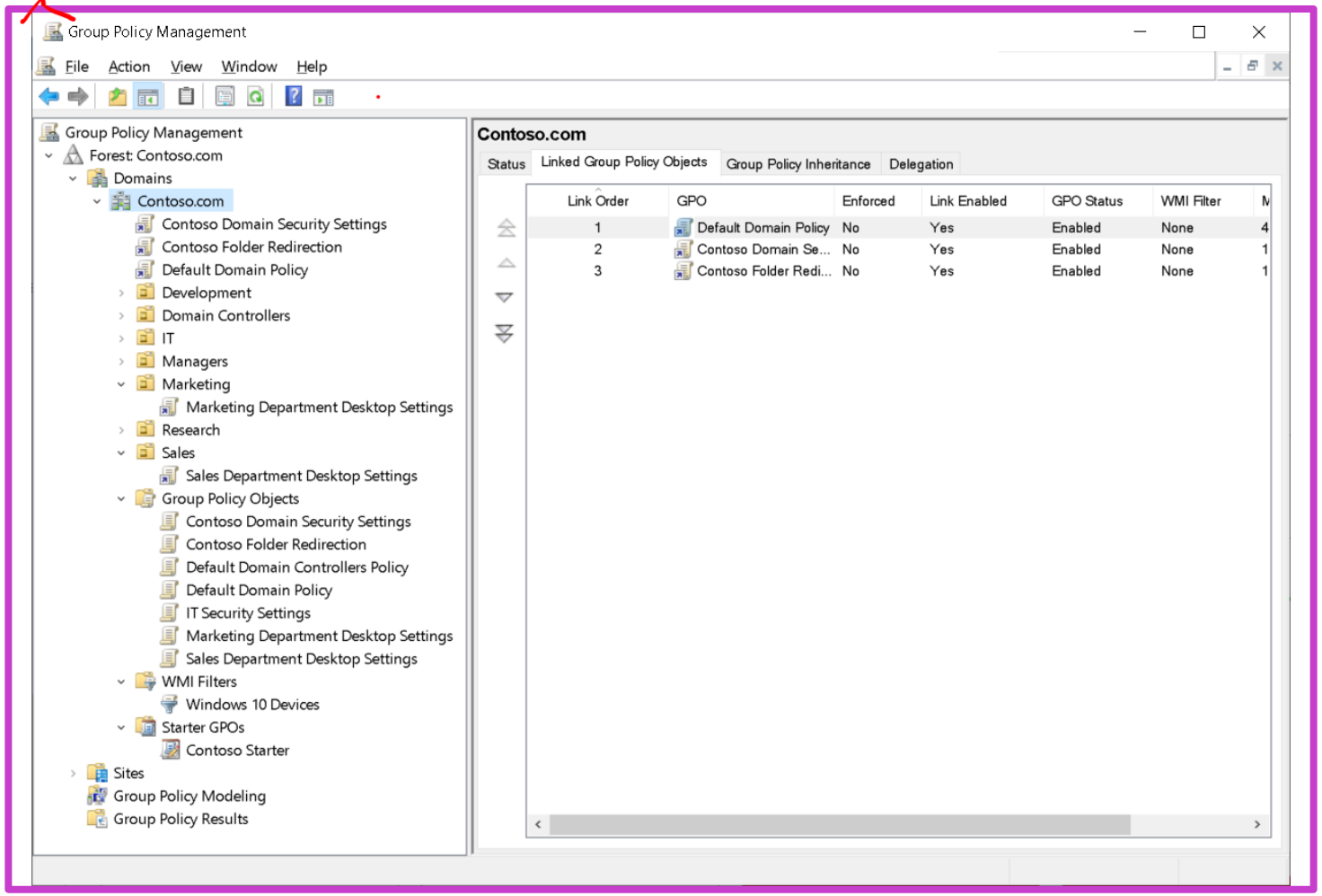


Group Policy is a powerful administrative tool

You can use it to enforce various types of settings to a large number of users and computers

Typically, you use GPOs to:

- Apply security settings
- Manage desktop application settings
- Deploy application software
- Manage Folder Redirection
- Configure network settings



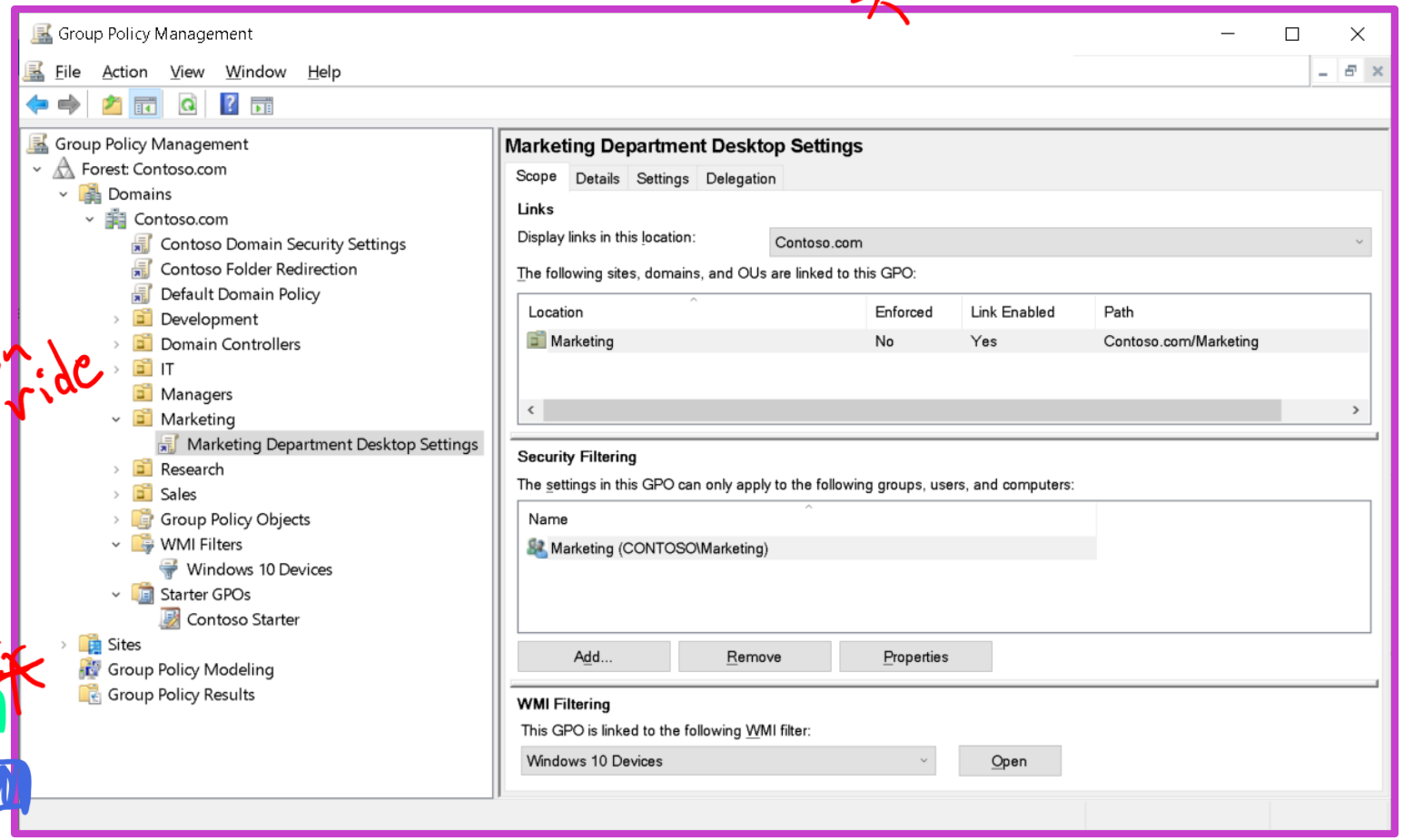
Implement GPO scope and processing order

Scope a GPO:

- Sites
- Domains
- OUs

Group Policy processing order:

1. Local GPOs.
2. Site-linked GPOs.
3. Domain-linked GPOs.
4. OU-linked GPOs.
5. Child OU-linked GPOs.



Applying GPOs

GPOs are applied:

1. Manually using the command line instruction **gpupdate /force**
2. Automatically
   a) at startup (computer configuration)
   b) at logon (user configuration)
   c) by default, after first application 90 minutes plus a randomized offset of up to 30 minutes
   d) by default, 90 minutes after the offset first re-application

Implement GPO inheritance

Block inheritance

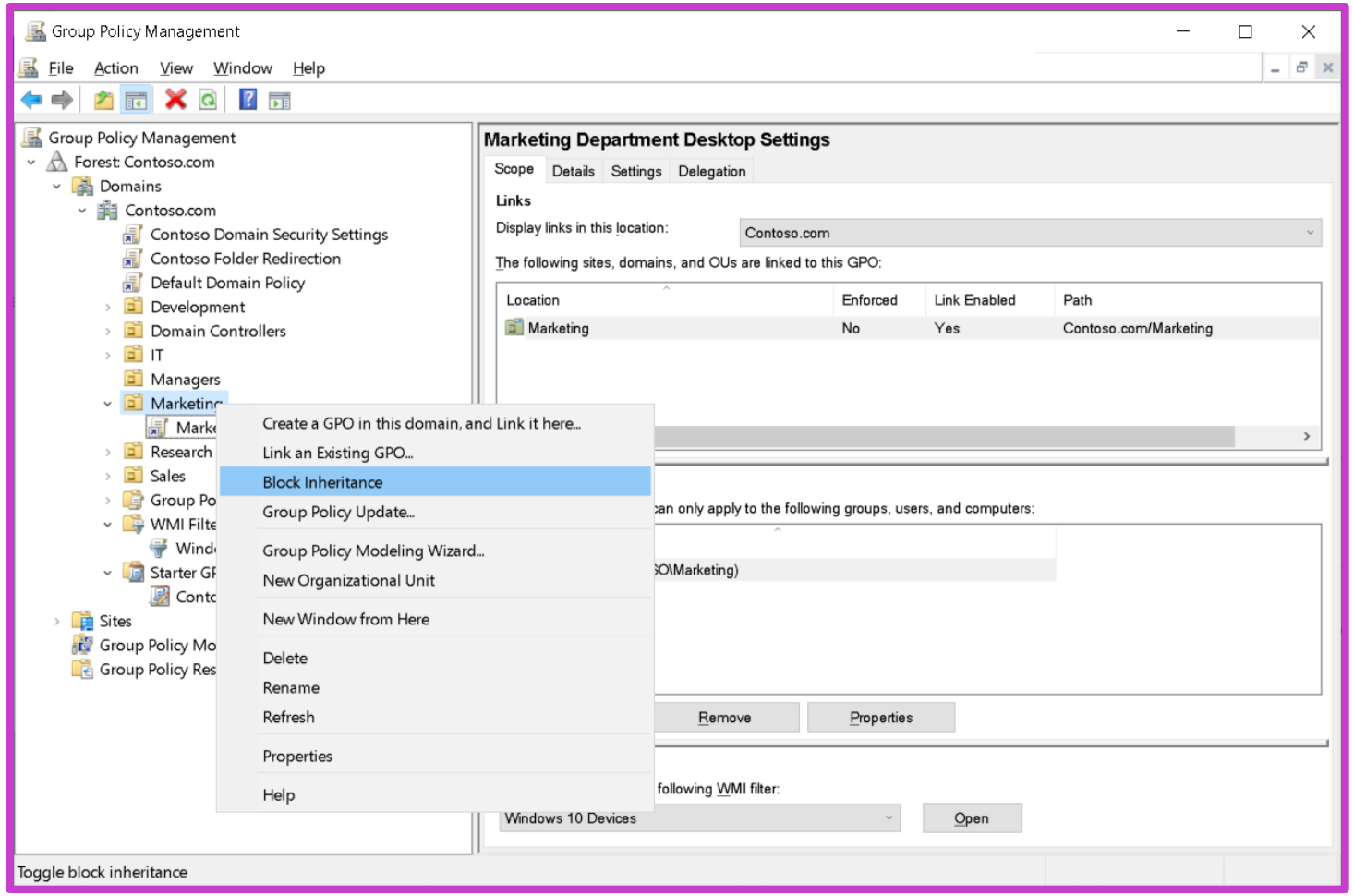
- Configure a domain or OU to prevent the inheritance of policy settings

Enforce a GPO link

- GPO takes the highest level of precedence
- Policy settings in that GPO prevail over any conflicting policy settings in other GPOs

Evaluating precedence

- Group Policy Inheritance tab displays the resulting precedence of GPOs

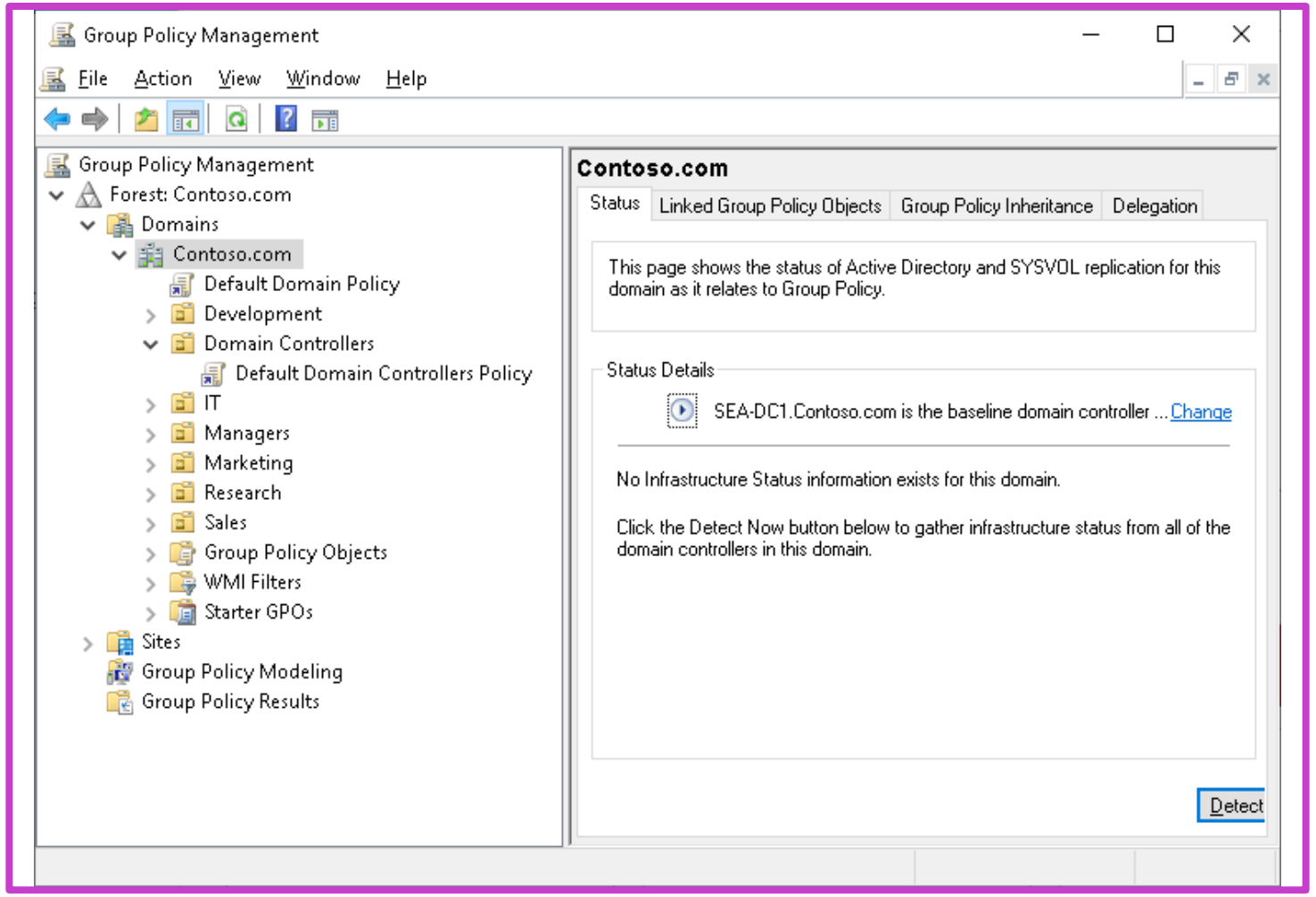


Domain-based GPOs

Create and store domain-based GPOs on domain controllers and use to manage configuration centrally for the domain's users and computers

A domain has two default GPOs

- **Default Domain Policy** linked to the domain, and it applies to Authenticated Users.
- **Default Domain Controllers Policy** links to the OU of the domain controllers.



What can you manage with GPOs?

Two major categories of policy settings:

- **Computer Configuration** node contains the settings that apply to computers, regardless of who logs on to them
- **User Configuration** node contains settings that apply when a user logs on to a computer, during background refreshes.

You can manage with GPOs:

- Apply security settings
- Manage desktop and application settings
- Deploy software
- Manage Folder Redirection
- Configuring network settings

Demonstration – Create, configure, and apply GPOs

From Group Policy Management console navigate to the Group Policy Objects container..	Create and link new GPO to the domain	Sign in to a client computer as an administrator and standard user to view the effects of the GPO's settings	Create and link additional GPOs to OUs	Examine order of precedence and verify application of settings

Define GPO storage

GPO includes two components:

- **Group Policy container** is in Active Directory, and it stores GPO metadata. It doesn't contain actual settings
- **Group Policy template** is a collection of files stored in the SYSVOL of each domain controller

GPO replication:

- The Group Policy container in AD DS replicates by the Directory Replication Agent
- The Group Policy template in the SYSVOL replicates by using the Distributed File System Replication

Define administrative templates

Two sets of administrative templates:

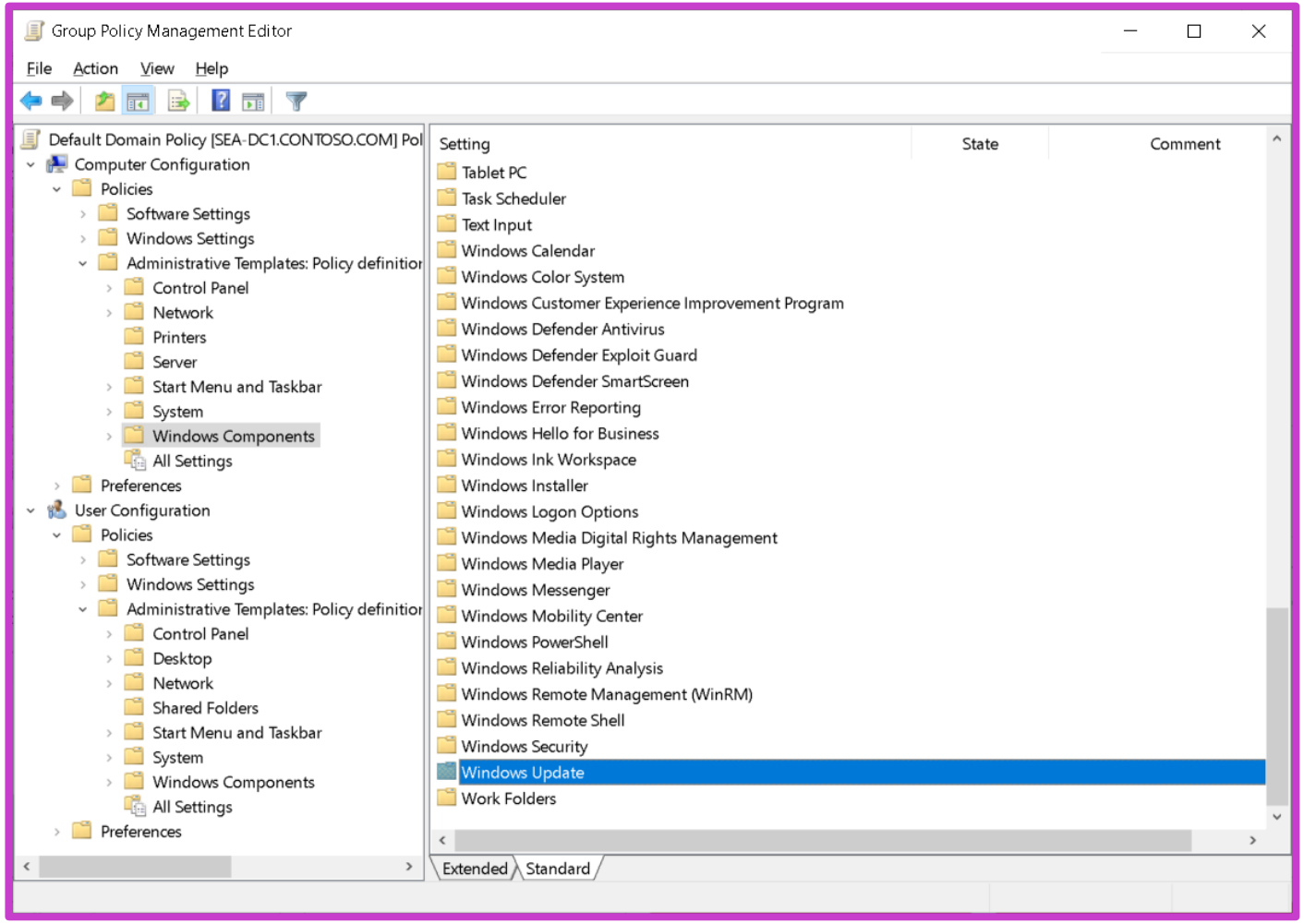
- Computer-related settings
- User-related settings

What are .admx and .adml files?

- All currently supported operating systems store the settings in .admx files.
- The PolicyDefinitions folder stores .adml files subfolders.

What is the Central Store?

- Central repository for .admx and .adml files
- Stored in SYSVOL and must be created manually



Learning recap – Implement Group Policy Objects

Module assessment

Microsoft Learn Modules (docs.microsoft.com/Learn)

Implement Group Policy Objects

Manage advanced features of AD DS

Learning Objectives – Manage advanced features of AD DS

- Create trust relationships
- Forest trust relationships
- Demonstration - Create a trust relationship
- Implement ESAE forests
- Monitor and troubleshoot AD DS
- Create custom AD DS partitions
- Demonstration - Create AD DS partitions
- Learning recap

What is trust relationship?

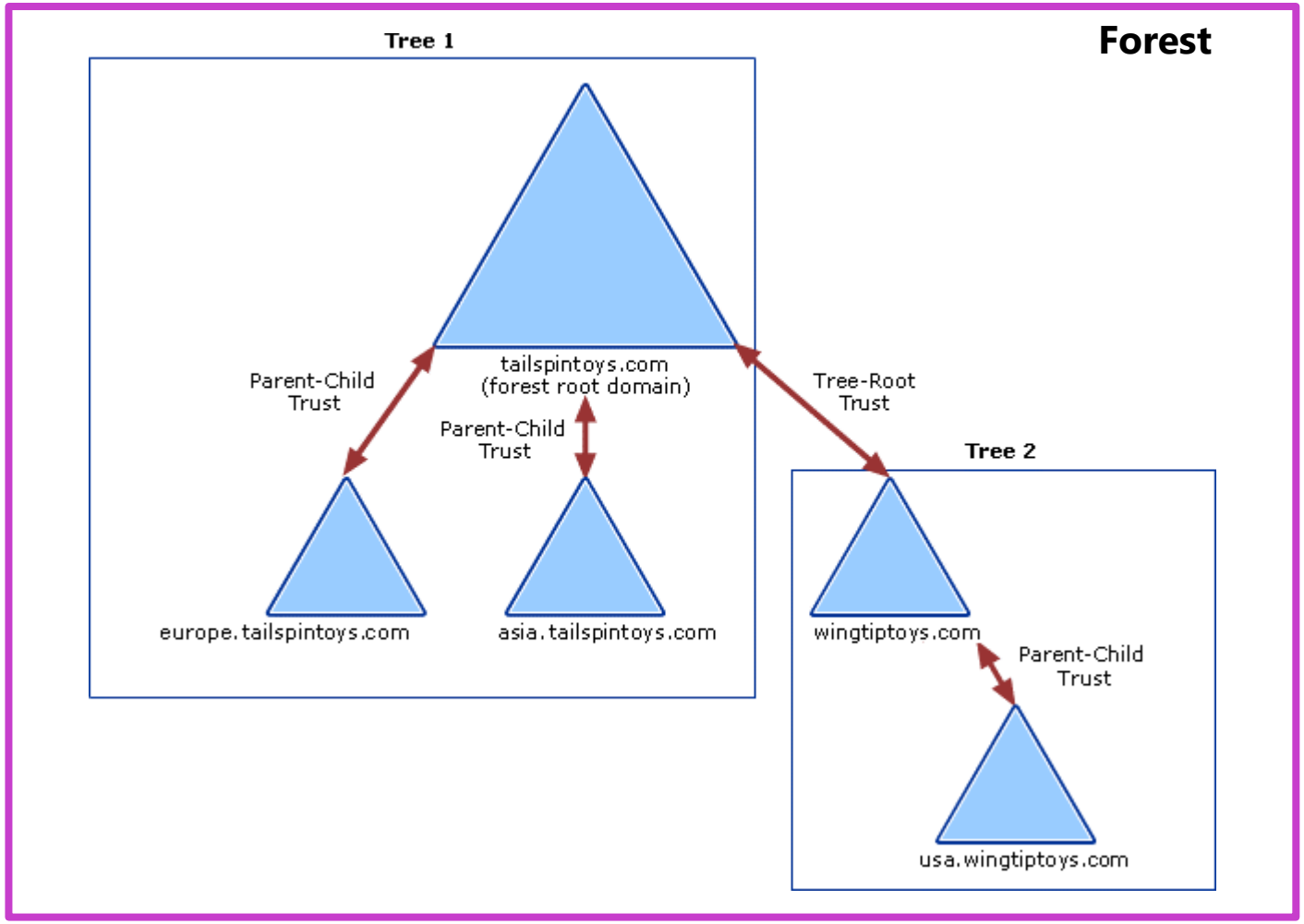
Trusts enables users to access the resources in a multiple-domain and multiple-forest AD DS environment

Parent-Child Trust

- Automatically established between the forest root and a child domain.
- Enables two-way transitive authentication and resource access.

Tree-Root Trust

- Created by default when a new tree root domain is added to a forest
- Facilitates two-way transitive trust for seamless domain integration

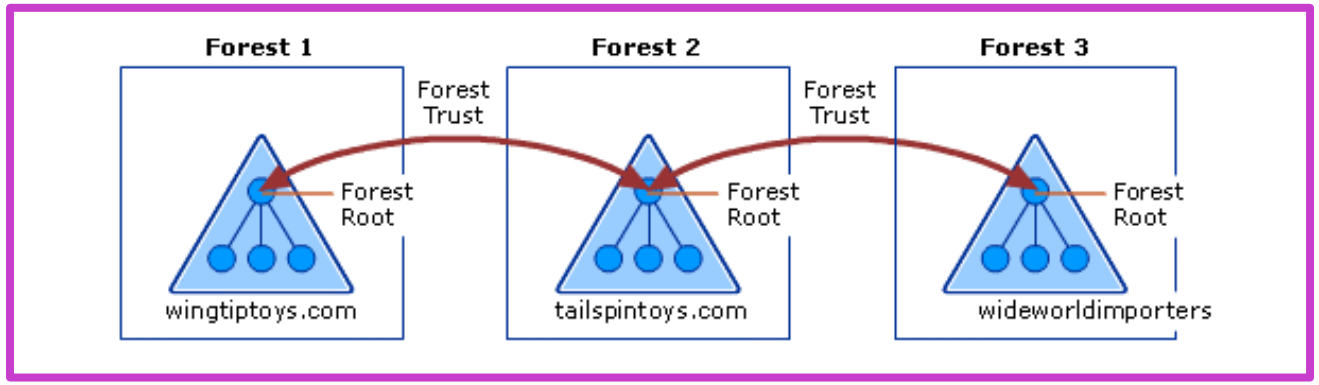


Types of trust relationship

Trust type	Description	Direction	Description
External	Nontransitive	One-way or two-way	Enable resource access with an individual AD DS domain in another forest.
Realm	Transitive or nontransitive	One-way or two-way	Establish an authentication path between a Windows Server AD DS domain and a Kerberos version 5 (v5) protocol realm that implements by using a directory service other than AD DS.
Forest (complete or selective)	Transitive	One-way or two-way	Allow two forests to share resources. The trust between two forests is transitive for all domains in the forest.
Shortcut	Nontransitive	One-way or two-way	Reduce the time taken to authenticate between two, not directly adjacent domains in the same multiple-domain AD DS forest.

Forest trusts provide most flexibility from the authentication standpoint

If you create a forest trust between Forest 1 and Forest 2 and you create a forest trust between Forest 2 and Forest 3, Forest 1 **doesn't** implicitly trust Forest 3



Demonstration – Create a trust relationship

Create two AD DS forests. Deploy two domain controllers

Configure DNS conditional forwarding.

Create a forest trust relationship **from the first forest to the second** one

Create a forest trust relationship **from the second forest to the first** one.

Monitor and troubleshoot AD DS

Monitor AD DS operational status

- The most commonly used tools are Task Manager, Resource Monitor, Event Viewer, and Performance Monitor

Tools for monitoring and troubleshooting replication

- **Repadmin.exe** – Command-line tool that report the status of replication on each domain controller
- **Dcdiag.exe** – Performs several tests and reports on the overall health of replication and operational status for AD DS

Monitoring replication with Microsoft System Center Operations Manager

- Includes replication monitoring functionality that collects AD DS replication alerts along with performance data representing replication latency, and the volume of both inbound and outbound replication traffic

Windows PowerShell AD DS replication cmdlets

- Windows Server supports Windows PowerShell cmdlets that facilitate monitoring AD DS replication and reviewing its configuration

Create custom AD DS partitions

What are default AD DS partitions?

- **Configuration partition** is created automatically when you create the first domain controller in a forest.
- **Schema partition** contains definitions of all the objects and attributes in the data store.
- **Domain partition** is created automatically when you create the first domain controller in a domain and is replicated on each DC in the same domain.
- **Application partition** stores nondomain, application-related information

How Create AD DS partitions?

- Creation and managing AD DS partitions performed by **NtdsUtil.exe** command-line tool

NtdsUtil.exe also allows you

- NTDS database maintenance, including snapshotting and offline defragmentation.
- Cleaning up domain-controller metadata following its unrecoverable failure.
- Resetting the password used to sign in to the DSRM.

Demonstration – Creating a custom AD DS partition

Create a single-domain AD DS forest containing two domain controllers.	Create a custom AD DS partition	Use command-line tools to create a custom application partition.	Verify that a custom AD DS partition exists.	Use command-line tools to delete a custom application partition.

Learning recap – Manage advanced features of AD DS Introduction

Module assessment

Microsoft Learn Modules (docs.microsoft.com/Learn)

Manage advanced features of AD DS

Lab 01 – Implement identity services and Group Policy

Lab 01: Implement identity services and Group Policy

Lab scenario

As part of the AD DS administration team at Contoso, you have been tasked with evaluating methods available in Windows Server for a non-interactive, remote domain controller deployment. You also need to automate certain AD DS administrative tasks and to establish configuration management based on Group Policy Objects (GPO.

Objectives

- Deploy a new domain controller on Server Core
- Configure Group Policy

End of presentation