

# NOS 01

Installing and configuring domain controllers

# Module Overview

- Overview of AD DS
- Overview of AD DS domain controllers
- Deploying a domain controller

# Lesson 1: AD DS components

AD DS is composed of both logical and physical components

<b>Logical components</b>	<b>Physical components</b>
<ul style="list-style-type: none"><li>• Partitions</li><li>• Schema</li><li>• Domains</li><li>• Domain trees</li><li>• Forests</li><li>• Sites</li><li>• OUs</li><li>• Containers</li></ul>	<ul style="list-style-type: none"><li>• Domain controllers</li><li>• Data stores</li><li>• Global catalog servers</li><li>• RODCs</li></ul>

# What is the AD DS schema?

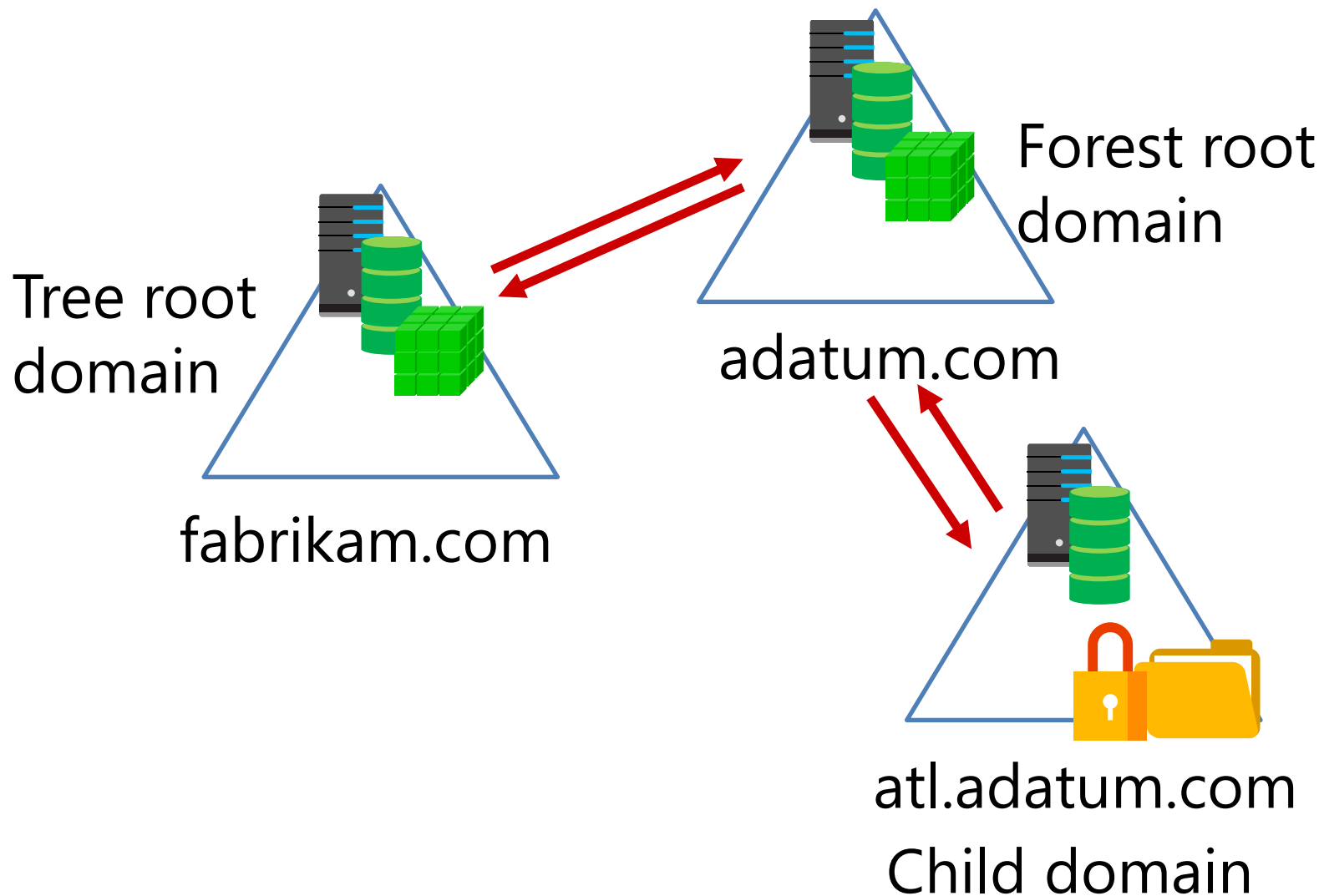
Console1 - [Console Root\Active Directory Schema [LON-DC1.Adatum.com]\Classes\user]

File Action View Favorites Window Help

← → ↶ ↷ ↸ ↹ ↺ ↻

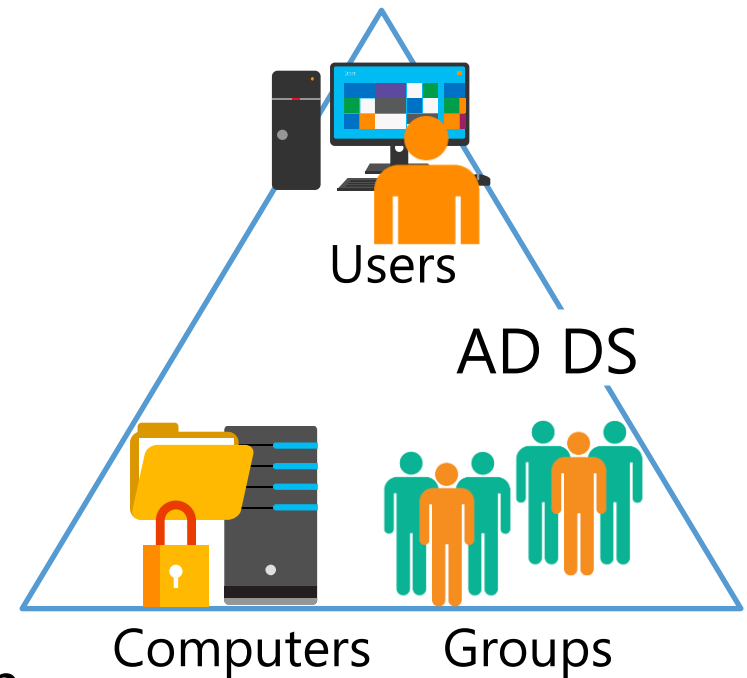
Name	Type	System	Description	Source Class
userPassword	Optional	No	User-Password	posixAccount
homeDirectory	Optional	No	Home-Directory	posixAccount
unixHomeDirectory	Optional	No	The absolute path to the...	posixAccount
gidNumber	Optional	No	An integer uniquely ide...	posixAccount
uidNumber	Optional	No	An integer uniquely ide...	posixAccount
cn	Optional	No	Common-Name	posixAccount
uid	Optional	No	A user ID.	posixAccount
userPassword	Optional	Yes	User-Password	person
telephoneNumber	Optional	Yes	Telephone-Number	person
sn	Optional	Yes	Surname	person
serialNumber	Optional	Yes	Serial-Number	person
seeAlso	Optional	Yes	See-Also	person
attributeCertificateAtt...	Optional	No	A digitally signed or cert...	person
cn	Mandatory	Yes	Common-Name	person
msDS-AllowedToAct...	Optional	Yes	This attribute is used for...	organizationalPerson
x121Address	Optional	Yes	X121-Address	organizationalPerson
comment	Optional	Yes	User-Comment	organizationalPerson
title	Optional	Yes	Title	organizationalPerson
co	Optional	Yes	Text-Country	organizationalPerson
primaryTelexNumber	Optional	Yes	Telex-Primary	organizationalPerson
telexNumber	Optional	Yes	Telex-Number	organizationalPerson
teletexTerminalIdentif...	Optional	Yes	Teletex-Terminal-Identifi...	organizationalPerson
street	Optional	Yes	Street-Address	organizationalPerson
st	Optional	Yes	State-Or-Province-Name	organizationalPerson
registeredAddress	Optional	Yes	Registered-Address	organizationalPerson
preferredDeliveryMet...	Optional	Yes	Preferred-Delivery-Meth...	organizationalPerson
postalCode	Optional	Yes	Postal-Code	organizationalPerson
postalAddress	Optional	Yes	Postal-Address	organizationalPerson
postOfficeBox	Optional	Yes	Post-Office-Box	organizationalPerson
thumbnailPhoto	Optional	Yes	Picture	organizationalPerson
physicalDeliveryOffic...	Optional	Yes	Physical-Delivery-Office...	organizationalPerson

# What is an AD DS forest?

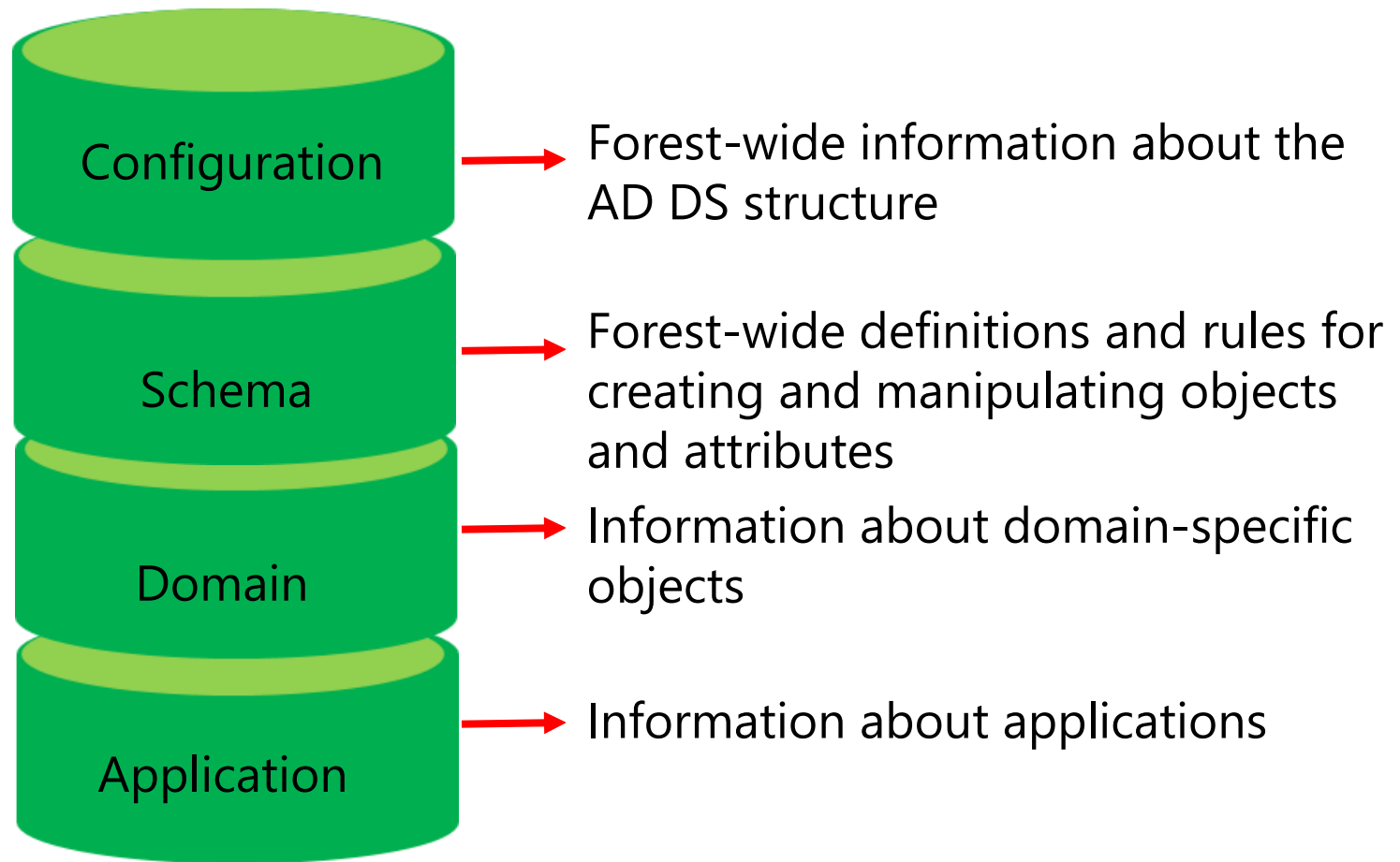


# What is an AD DS domain?

- AD DS requires one or more domain controllers
- All domain controllers hold a copy of the domain database, which is continually synchronized
- The domain is the context within which user accounts, computer accounts, and groups are created
- The domain is a replication boundary
- The domain is an administrative center for configuring and managing objects
- Any domain controller can authenticate any sign-in anywhere in the domain
- The domain provides authorization



# What are AD DS partitions?



AD DS database

# What are 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



# Overview of AD DS administration tools

You typically perform AD DS management by using the following tools:

- Active Directory Administrative Center
- Active Directory Users and Computers
- Active Directory Sites and Services
- Active Directory Domains and Trusts
- Active Directory Schema snap-in
- Active Directory module for Windows PowerShell

## Lesson 2: Overview of AD DS domain controllers

- What is a domain controller?
- What is a global catalog?
- Overview of domain controller SRV records
- Demonstration: Viewing the SRV records in DNS
- AD DS sign-in process
- What are operations masters?
- Transferring and seizing roles

# What is a domain controller?

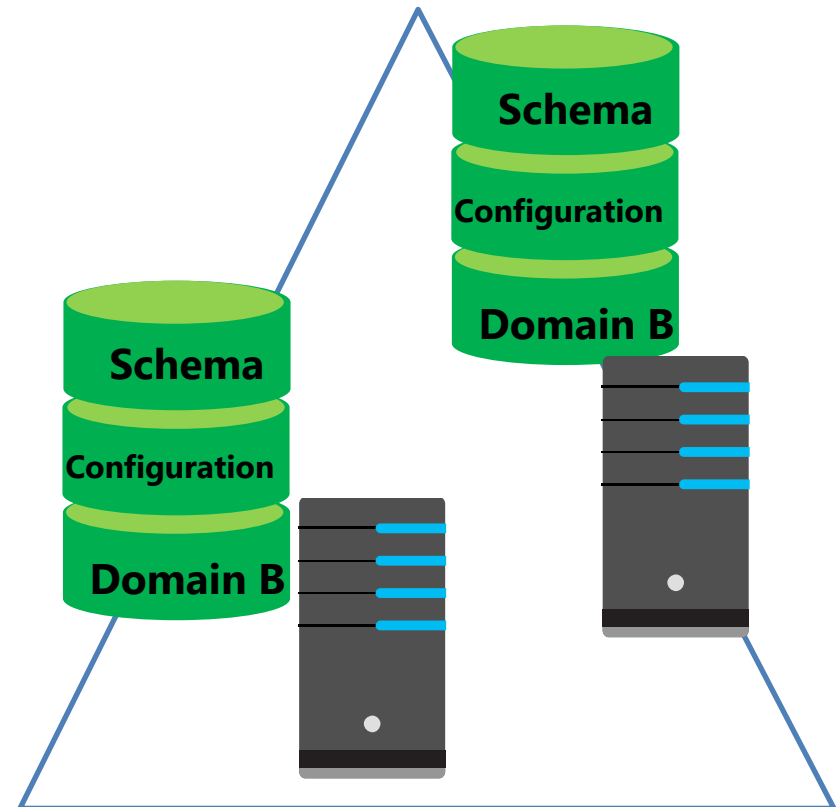
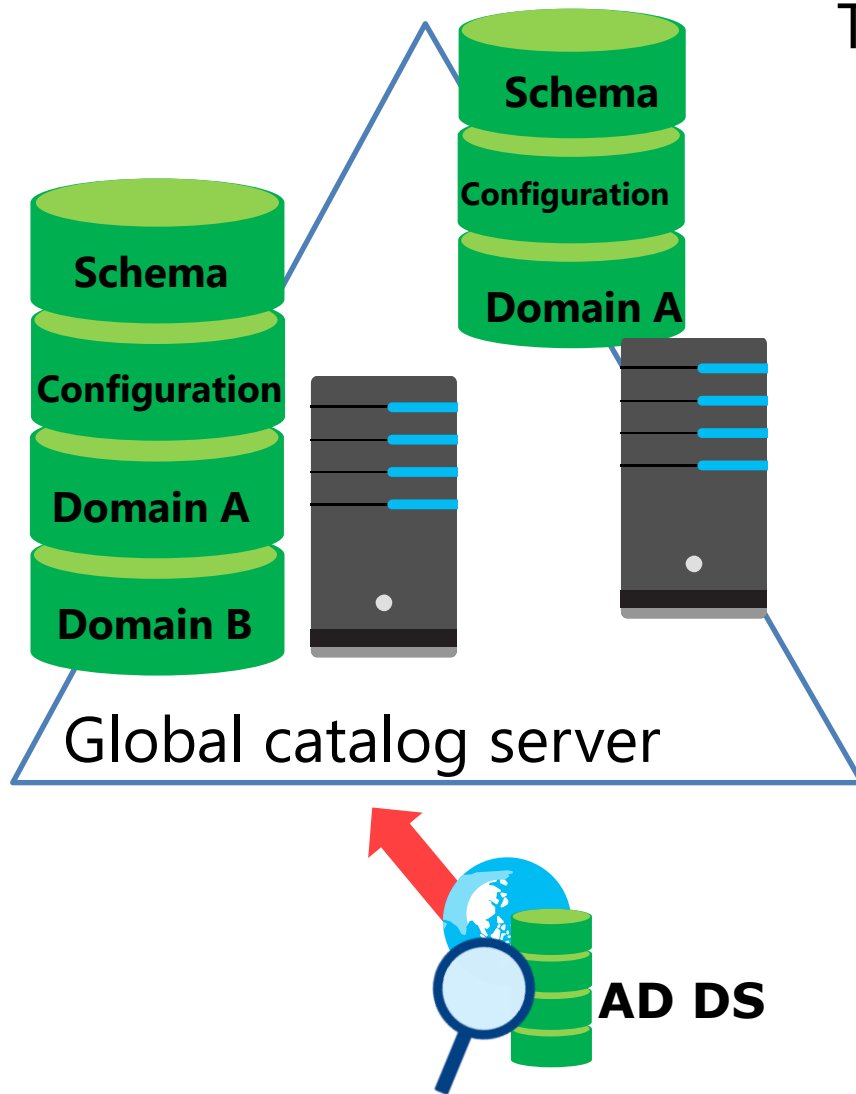
## Domain controllers:

- Are servers that host the AD DS database (**Ntds.dit**) and **SYSVOL**
- Host the Kerberos authentication service and KDC services to perform authentication
- Have best practices for:
  - Availability:
    - Use at least two domain controllers in a domain
  - Security:
    - Use an RODC or BitLocker

# What is a global catalog?

## The global catalog:

- Hosts a partial attribute set for other domains in the forest
- Supports queries for objects throughout the forest

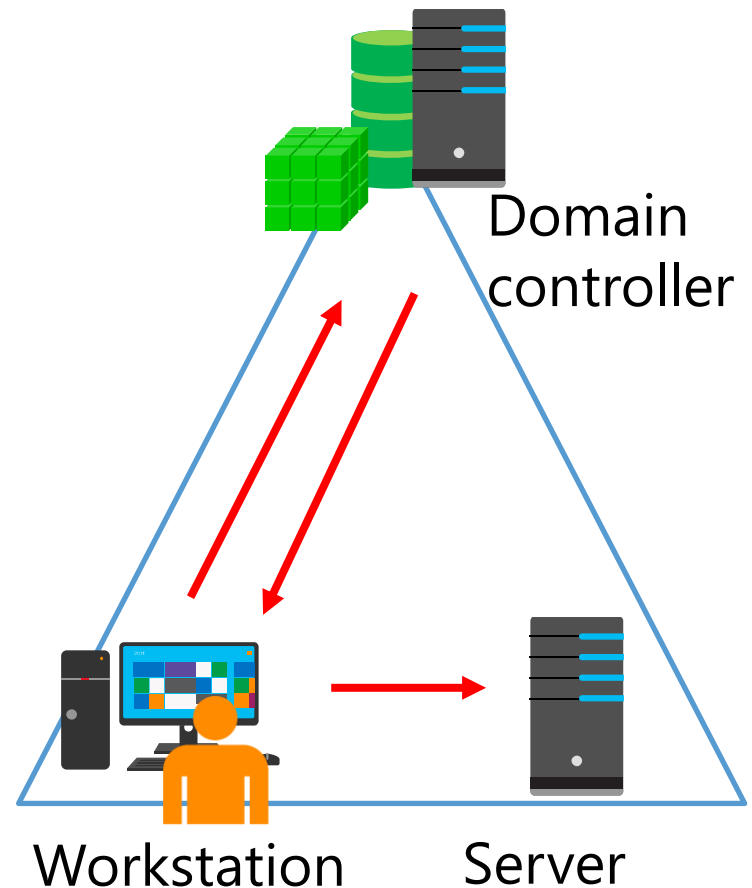


# Overview of domain controller SRV records

- Clients find domain controllers through DNS lookup
- Domain controllers dynamically register their addresses with DNS
- The results of DNS queries for domain controllers are returned in this order:
  1. A list of domain controllers in the same site as the client
  2. A list of domain controllers in the next closest site, if none are available in the same site
  3. A random list of domain controllers in other sites, if no domain controller is available in the next closest site

# AD DS sign-in process

1. The user account is authenticated to the domain controller
2. The domain controller returns a TGT back to client
3. The client uses the TGT to apply for access to the workstation
4. The domain controller grants access to the workstation
5. The client uses the TGT to apply for access to the server
6. The domain controller returns access to the server



# What are 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
  - Flexible single master operations (FSMO)

## The five FSMOs

### Forest:

- Domain naming master
- Schema master

### Domain:

- RID master
- Infrastructure master
- PDC emulator master

# Transferring and seizing roles

- Transferring is:
  - Planned
  - Done with the latest data
  - Done through snap-ins, Windows PowerShell, or ntdsutil.exe
- Seizing is:
  - Unplanned and a last resort
  - Done with incomplete or out-of-date data
  - Done through Windows PowerShell or ntdsutil.exe



## Lesson 3: Deploying a domain controller

- Installing a domain controller from Server Manager

# Installing a domain controller from Server Manager

## The **Deployment Configuration** section of the **Active Directory Domain Services Configuration Wizard**

Select the deployment operation

☒ Add a domain controller to an existing domain

☐ Add a new domain to an existing forest

☐ Add a new forest

Specify the domain information for this operation

Domain:

Supply the credentials to perform this operation

<No credentials provided>

# Overview of domain and forest boundaries in an AD DS structure

AD DS object	Boundary type
Domain	Domain partition replication
	Administrative permissions
	Group Policy application
	Auditing
	Password and account policies
	Domain DNS zone replication
Forest	Security
	Schema partition replication
	Configuration partition replication
	Global catalog replication
	Forest DNS zone replication

# AD DS domain functional levels

New functionality requires that domain controllers are running a particular version of the Windows operating system:

- Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
- 
- You cannot raise the functional level while domain controllers are running previous Windows Server versions
  - You cannot add domain controllers that are running previous Windows Server versions after raising the functional level

# Deploying new AD DS domains

- Forest root domain:
  - Is automatically created with a new forest
  - Is the base of an AD DS infrastructure
  - Can be the only domain in an AD DS deployment
- Child domain:
  - Is a child of a parent domain
  - Shares the same namespace with the parent domain
- Tree domain:
  - Creates a new domain tree and a new namespace
  - Are commonly used in merger and acquisition scenarios