VIET NAM NATIONAL UNIVERSITY – HO CHI MINH CITY
UNIVERSITY OF SCIENCE

AUTHOR’S NAME: VU HIEU HOANG

STUDENT’S ID: 21200092

TIME OF TRANING: 2021-2025

LEVEL OF TRAINING: UNDERGRADUATE

FORM OF TRAINING: FULL-TIME

REPORT
ADVANCED COMPUTER NETWORKS

FACULTY: ELECTRONICS AND TELECOMUNICATIONS

REPORTS ON RESEARCH ABOUT THE RELATIONSHIPS IN MULTI DOMAIN SYSTEM

2024

VIET NAM NATIONAL UNIVERSITY – HO CHI MINH CITY
UNIVERSITY OF SCIENCE

AUTHOR’S NAME: VU HIEU HOANG

STUDENT’S ID: 21200092

TIME OF TRANING: 2021-2025

LEVEL OF TRAINING: UNDERGRADUATE

FORM OF TRAINING: FULL-TIME

REPORT
ADVANCED COMPUTER NETWORKS

DEPARTMENT: COMPUTER AND EMBEDDED SYSTEMS

TECHNICAL REPORT

LECTURER: M.S. NGUYEN QUANG ANH

2024

Abstract

In the evolving landscape of enterprise IT infrastructure, the implementation of multiple domain systems within Active Directory Domain Services (AD DS) stands as a cornerstone for robust, scalable, and secure network architecture. This report delves into the intricacies of deploying and managing a multi-domain environment, addressing the challenges and benefits that come with it.

AD DS, a directory service developed by Microsoft, provides a framework for centralized domain management, facilitating resource sharing and security across a network. The advent of multiple domain models has further enhanced administrative flexibility and security isolation, catering to the diverse needs of large organizations with varied operational requirements.

This report will explore the strategic planning necessary for successful AD DS deployment across multiple domains, the technical considerations for ensuring seamless inter-domain interactions, and the best practices for maintaining system integrity and security. Through a comprehensive analysis, we aim to provide valuable insights for IT professionals tasked with overseeing complex domain infrastructures within their organizations

Table of contents

PART 1. INTRODUCTION TO AD DS

Chapter 1 Active Directory Domain Services

1.1 AD DS

AD DS is Active Directory Domain Services

AD DS and its related services form the foundation for enterprise networks that run Windows operating systems. The AD DS database is the central store of all the domain objects, such as user accounts, computer accounts, and groups. AD DS provides a searchable, hierarchical directory and a method for applying configuration and security settings for objects in an enterprise.

AD DS includes both logical and physical components. You should understand how AD DS components work together so that you can manage your infrastructure efficiently. In addition, you can use AD DS options to perform actions such as:

- Installing, configuring, and updating apps.
- Managing the security infrastructure.
- Enabling Remote Access Service and DirectAccess.
- Issuing and managing digital certificates.

1.2 What are the logical components?

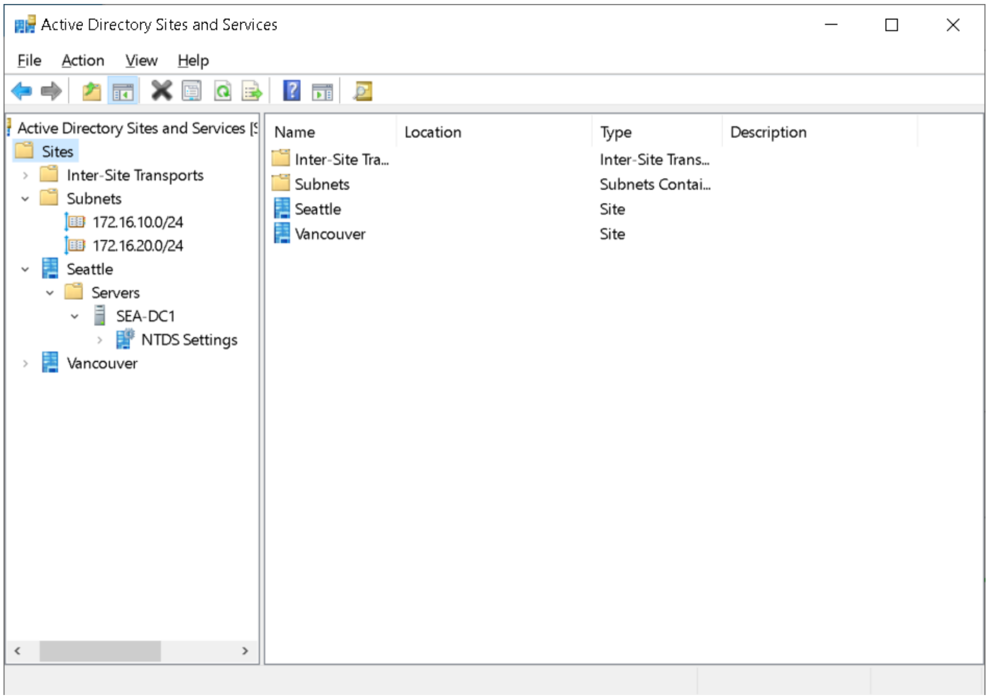
AD DS logical components are structures that you use to implement an AD DS design that is appropriate for an organization. The following table describes the types of logical components that an AD DS database contains.

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. For example, the schema partition contains a copy of the Active Directory schema. The configuration partition contains the configuration objects for the forest, and the domain partition contains the users, computers, groups, and other objects specific to the domain. Active Directory stores copies of partitions on multiple domain controllers and updates them through directory replication.
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.

1.3 What are the physical components?

Physical components in AD DS are those objects that are tangible, or that are described as tangible components in the real world.



Name	Location	Type	Description
Inter-Site Tra...		Inter-Site Trans...	
Subnets		Subnets Contai...	
Seattle		Site	
Vancouver		Site	

Physical component	Description
Domain controller	A domain controller contains a copy of the AD DS database. For most operations, each domain

	controller can process changes and replicate the changes to all the other domain controllers in the domain.
Datastore	A copy of the data store exists on each domain controller. The AD DS database uses Microsoft Jet database technology and stores the directory information in the Ntds. dit file and associated log files. The C:\Windows\NTDS folder stores these files by default.
Global catalog server	A global catalog server is a domain controller that hosts the global catalog, which is a partial, read-only copy of all the objects in a multiple-domain forest. A global catalog speeds up searches for objects that might be stored on domain controllers in a different domain in the forest.
Read-only domain controller (RODC)	An RODC is a special, read-only installation of AD DS. RODCs are common in branch offices where physical security is not optimal, IT support is less advanced than in the main corporate centers, or line-of-business applications need to run on a domain controller.
Site	A site is a container for AD DS objects, such as computers and services that are specific to a physical location. This is in comparison to a domain, which represents the logical structure of objects, such as users and groups, in addition to computers.
Subnet	A subnet is a portion of the network IP addresses of an organization assigned to computers in a site. A site can have more than one subnet.

Chapter 2 Define users, groups, and computers

In addition to the high-level components and objects, AD DS contains other objects such as users, groups, and computers.

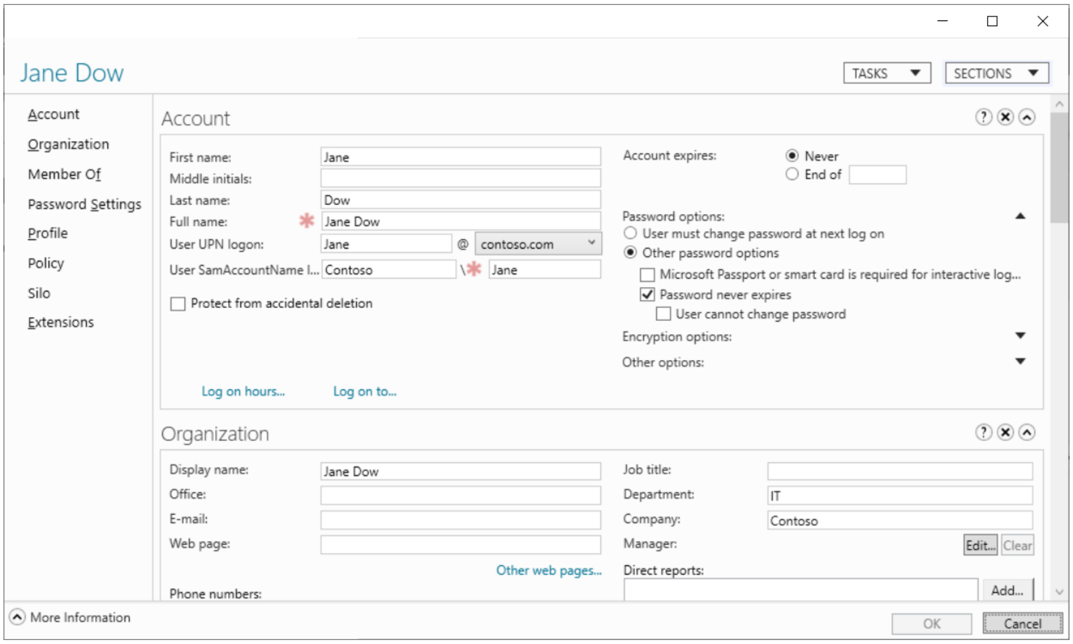
2.1 Create user objects

In AD DS, you must provide all users who require access to network resources with a user account. With this user account, users can authenticate to the AD DS domain and access network resources.

In Windows Server, a user account is an object that contains all the information that defines a user. A user account includes:

- The username.
- A user password.
- Group memberships.

A user account also contains settings that you can configure based on your organizational requirements.



Jane Dow

Account

First name: Jane
Middle initials:
Last name: Dow
Full name: * Jane Dow
User UPN logon: Jane @ contoso.com
User SamAccountName l...: Contoso * Jane
□ Protect from accidental deletion

Account expires: ● Never ○ End of

Password options:
○ User must change password at next log on
● Other password options
□ Microsoft Passport or smart card is required for interactive log...
☑ Password never expires
□ User cannot change password
Encryption options:
Other options:

Organization

Display name: Jane Dow
Office:
E-mail:
Web page:
Phone numbers:
Job title:
Department: IT
Company: Contoso
Manager:
Direct reports:

The username and password of a user account serve as the user's sign-in credentials. A user object also includes several other attributes that describe and manage the user. You can use the following to create and manage user objects in AD DS:

- Active Directory Administrative Center.
- Active Directory Users and Computers.
- Windows Admin Center.
- Windows PowerShell.
- The dsadd command-line tool.

2.2 What are managed service accounts?

Many apps contain services that you install on the server that hosts the program. These services typically run at server startup or are triggered by other events. Services often run in the background and don't require any user interaction. For a service to start up and authenticate, you use a service account. A service account might be an account that is local to the computer, such as the built-in Local Service, Network Service, or Local System account. You also can configure a service account to use a domain-based account located in AD DS.

To help centralize administration and meet program requirements, many organizations choose to use a domain-based account to run program services. While this does provide some benefits over using a local account, there are a number of associated challenges, such as the following:

- Extra administration effort might be necessary to manage the service account password securely.
- It can be difficult to determine where a domain-based account is being used as a service account.
- Extra administration effort might be necessary to manage the service principal name (SPN).

Windows Server supports an AD DS object, named a managed service account, which you use to facilitate service-account management. A managed service account is an AD DS object class that enables:

- Simplified password management.
- Simplified SPN management.

2.3 What are group-managed service accounts?

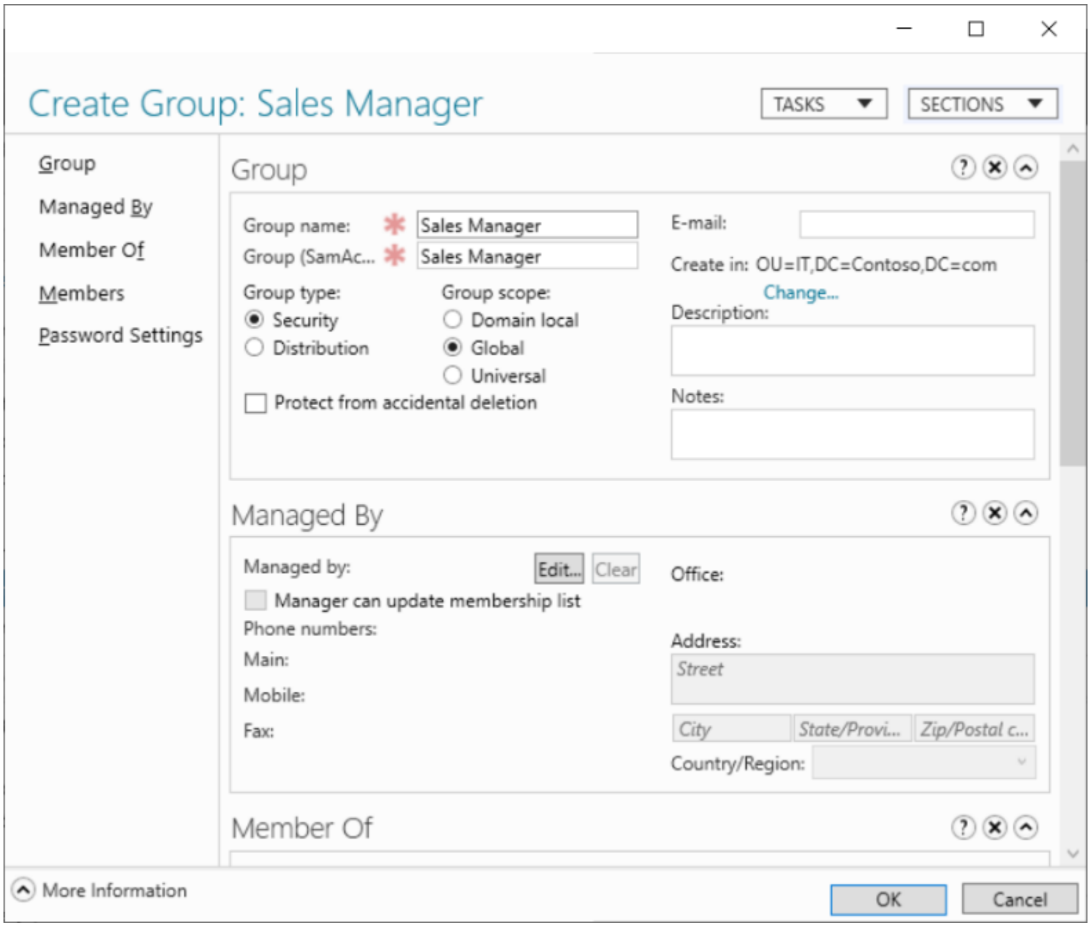
Group-managed service accounts enable you to extend the capabilities of standard managed service accounts to more than one server in your domain. In server farm scenarios with Network Load Balancing (NLB) clusters or IIS servers, there often is a need to run system or program services under the same service account. Standard managed service accounts can't provide managed service account functionality to services that are running on more than one server. By using group-managed service accounts, you can configure multiple servers to use the same managed service account and still retain the benefits that managed service accounts provide, like automatic password maintenance and simplified SPN management.

2.4 What are group objects?

Although it might be practical to assign permissions and rights to individual user accounts in small networks, this becomes impractical and inefficient in large enterprise networks.

For example, if several users need the same level of access to a folder, it's more efficient to create a group that contains the required user accounts, and then assign the required permissions to the group.

Before you implement groups in your organization, you must understand the scope of various AD DS group types. In addition, you must understand how to use group types to manage access to resources or to assign management rights and responsibilities.



Create Group: Sales Manager

Group name: * Sales Manager

Group (SamAc... * Sales Manager

Group type: ● Security ○ Distribution

Group scope: ○ Domain local ● Global ○ Universal

□ Protect from accidental deletion

Create in: OU=IT,DC=Contoso,DC=com

□ Manager can update membership list

2.5 Group types

In a Windows Server enterprise network, there are two types of groups, described in the following table.

Group type	**Description**
Security	Security groups are security-enabled, and you use them to assign permissions to various resources. You can use security groups in permission entries in access control lists (ACLs) to help control security for resource access. If you want to use a group to manage security, it must be a security group.
Distribution	Email applications typically use distribution groups, which are not security-enabled. You also can use security groups as a means of distribution for email applications.

2.6 Group scopes

Windows Server supports group scoping. The scope of a group determines both the range of a group's abilities or permissions and the group membership. There are four group scopes.

- **Local**. You use this type of group for standalone servers or workstations, on domain-member servers that are not domain controllers, or on domain-member workstations. Local groups are available only on the computer where they exist. The important characteristics of a local group are:
  - You can assign abilities and permissions on local resources only, meaning on the local computer.
  - Members can be from anywhere in the AD DS forest.
- **Domain-local**. You use this type of group primarily to manage access to resources or to assign management rights and responsibilities. Domain-local groups exist on domain controllers in an AD DS domain, and so, the group's scope is local to the domain in which it resides. The important characteristics of domain-local groups are:
  - You can assign abilities and permissions on domain-local resources only, which means on all computers in the local domain.
  - Members can be from anywhere in the AD DS forest.
- **Global**. You use this type of group primarily to consolidate users who have similar characteristics. For example, you might use global groups to join users who are part of a department or a geographic location. The important characteristics of global groups are:
  - You can assign abilities and permissions anywhere in the forest.
  - Members can be from the local domain only and can include users, computers, and global groups from the local domain.

- **Universal**. You use this type of group most often in multidomain networks because it combines the characteristics of both domain-local groups and global groups. Specifically, the important characteristics of universal groups are:
    - You can assign abilities and permissions anywhere in the forest similar to how you assign them for global groups.
    - Members can be from anywhere in the AD DS forest.

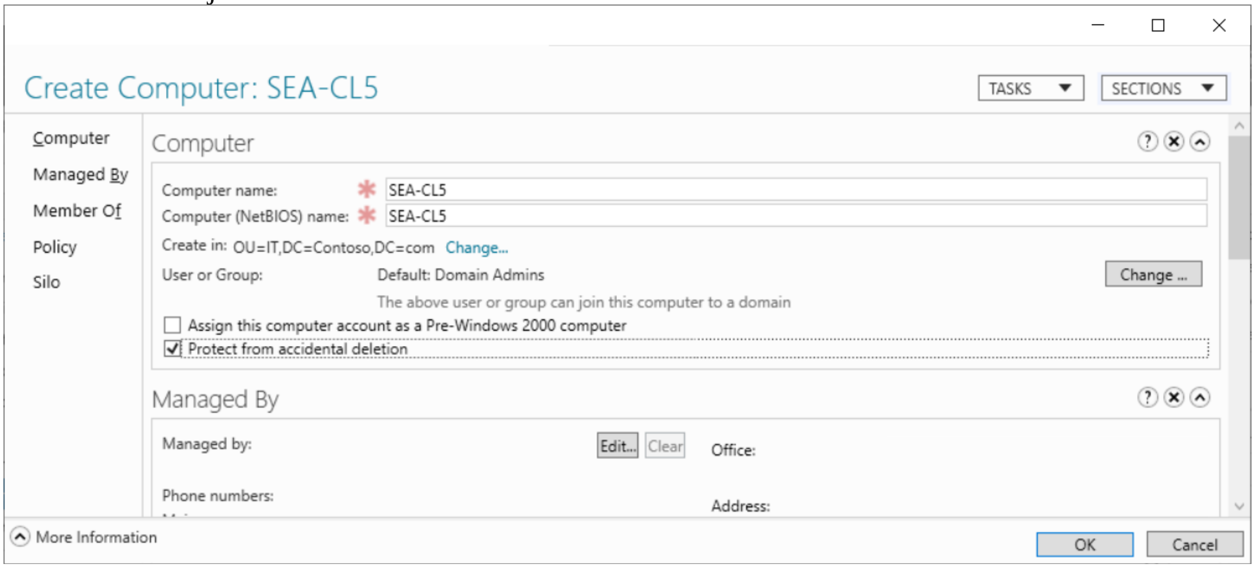
2.7 What are computer objects?

Computers, like users, are security principals, in that:

- They have an account with a sign-in name and password that Windows changes automatically on a periodic basis.
- They authenticate with the domain.
- They can belong to groups and have access to resources, and you can configure them by using Group Policy.

A computer account begins its lifecycle when you create the computer object and join it to your domain. After you join the computer account to your domain, day-to-day administrative tasks include:

- Configuring computer properties.
- Moving the computer between OUs.
- Managing the computer itself.
- Renaming, resetting, disabling, enabling, and eventually deleting the computer object.



Create Computer: SEA-CL5

Computer

Computer name: * SEA-CL5

Computer (NetBIOS) name: * SEA-CL5

Create in: OU=IT,DC=Contoso,DC=com Change...

User or Group: Default: Domain Admins

The above user or group can join this computer to a domain

□ Assign this computer account as a Pre-Windows 2000 computer

☑ Protect from accidental deletion

Managed By

Managed by:

Office:

Phone numbers:

Address:

2.8 Computers container

Before you create a computer object in AD DS, you must have a place to put it. The computer container is a built-in container in an AD DS domain. This container is the default location for the computer accounts when a computer joins the domain.

This container is not an OU. Instead, it is an object of the Container class. Its common name is CN=Computers. There are subtle but important differences between a container and an OU. You cannot create an OU within a container, so you cannot subdivide the Computers container. You also cannot link a Group Policy Object to a container. Therefore, we recommend that you create custom OUs to host computer objects, instead of using the Computers container.

Chapter 3 Define AD DS forests and domains

An AD DS forest is a collection of one or more AD DS trees that contain one or more AD DS domains. Domains in a forest share:

- A common root.
- A common schema.
- A global catalog.

An AD DS domain is a logical administrative container for objects such as:

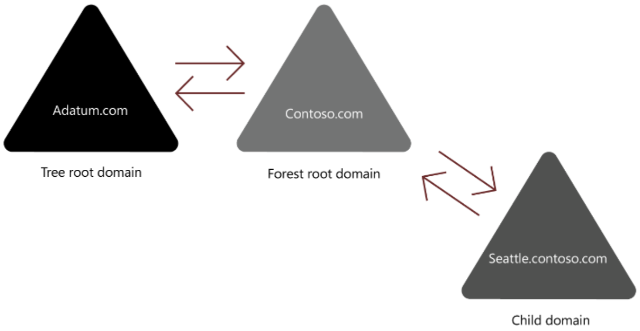
- Users
- Groups
- Computers

3.1 What is an AD DS forest?

A forest is a top-level container in AD DS. Each forest is a collection of one or more domain trees that share a common directory schema and a global catalog. A domain tree is a collection of one or more domains that share a contiguous namespace. The forest root domain is the first domain that you create in the forest.

The forest root domain contains objects that don't exist in other domains in the forest. Because you always create these objects on the first domain controller, a forest can consist of as few as one domain with a single domain controller, or it can consist of several domains across multiple domain trees.

The following graphic displays Contoso.com as the forest root domain. Beneath are two domains, Adatum.com in a separate tree, and Seattle.Contoso.com as a child of Contoso.com.



The following objects exist in the forest root domain:

- The schema master role.
- The domain naming master role.
- The Enterprise Admins group.
- The Schema Admins group.

An AD DS forest is often described as:

- A security boundary. By default, no users from outside the forest can access any resources inside the forest. In addition, all the domains in a forest automatically trust the other domains in the forest. This makes it easy to enable access to resources for all the users in a forest, regardless of the domain to which they belong.
- A replication boundary. An AD DS forest is the replication boundary for the configuration and schema partitions in the AD DS database. Therefore, organizations that want to deploy applications with incompatible schemas must deploy additional forests. The forest is also the replication boundary for the global catalog. The global catalog makes it possible to find objects from any domain in the forest.

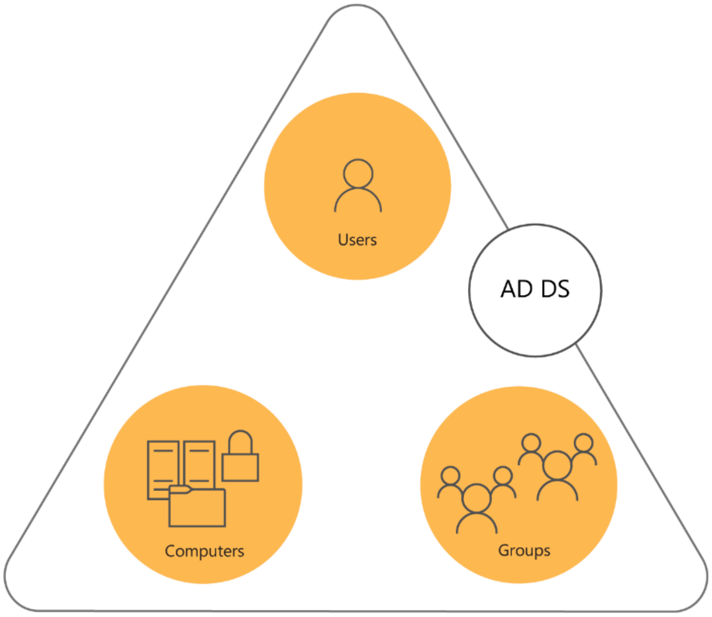
The following objects exist in each domain (including the forest root):

- The RID master role.
- The Infrastructure master role.
- The PDC emulator master role.
- The Domain Admins group.

3.2 What is an AD DS domain?

An AD DS domain is a logical container for managing users, computers, groups, and other objects. The AD DS database stores all domain objects, and each domain controller stores a copy of the database.

The following graphic displays an AD DS domain. It contains users, computers, and groups.



The most commonly used objects are described in the following table:

Object	**Description**
User accounts	User accounts contain information about users, including the information required to authenticate a user during the sign-in process and build the user's access token.
Computer accounts	Each domain-joined computer has an account in AD DS. You can use computer accounts for domain-joined computers in the same way that you use user accounts for users.
Groups	Groups organize users or computers to simplify the management of permissions and Group Policy Objects in the domain.

An AD DS domain is often described as:

- A replication boundary. When you make changes to any object in the domain, the domain controller where the change occurred replicates that change to all other domain controllers in the domain. If multiple domains exist in the forest, only subsets of the changes replicate to other domains. AD DS uses a multi-master replication model that allows every domain controller to make changes to objects in the domain.
- An administrative unit. The AD DS domain contains an Administrator account and a Domain Admins group. By default, the Administrator account is a member of the Domain Admins group, and the Domain Admins group is a member of every local

Administrators group of domain-joined computers. Also, by default, the Domain Admins group members have full control over every object in the domain.

An AD DS domain provides:

- Authentication. Whenever a domain-joined computer starts or a user signs in to a domain-joined computer, AD DS authenticates it. Authentication verifies that the computer or user has the proper identity in AD DS by verifying its credentials.
- Authorization. Windows uses authorization and access control technologies to determine whether to allow authenticated users to access resources.
-

3.3 What are trust relationships?

AD DS trusts enable access to resources in a complex AD DS environment. When you deploy a single domain, you can easily grant access to resources within the domain to users and groups from the domain. When you implement multiple domains or forests, you should ensure that the appropriate trusts are in place to enable the same access to resources.

In a multiple-domain AD DS forest, two-way transitive trust relationships generate automatically between AD DS domains so that a path of trust exists between all the AD DS domains.

You can deploy other types of trusts. The following table describes the main trust types.

Trust type	**Description**	**Direction**	**Description**
Parent and child	Transitive	Two-way	When you add a new AD DS domain to an existing AD DS tree, you create new parent and child trusts.
Tree-root	Transitive	Two-way	When you create a new AD DS tree in an existing AD DS forest, you automatically create a new tree-root trust.
External	Nontransitive	One-way or two-way	External trusts enable resource access with a Windows NT 4.0 domain or an AD DS domain in another forest. You also can set these up to provide a framework for a migration.
Realm	Transitive or nontransitive	One-way or two-way	Realm trusts establish an authentication path between a Windows

			Server AD DS domain and a Kerberos version 5 (v5) protocol realm that is implemented by using a directory service other than AD DS.
Forest (complete or selective)	Transitive	One-way or two-way	Trusts between AD DS forests allow two forests to share resources.
Shortcut	Nontransitive	One-way or two-way	Configure shortcut trusts to reduce the time taken to authenticate between AD DS domains that are in different parts of an AD DS forest. No shortcut trusts exist by default, and an administrator must create them if they are required.

When you set up trusts between domains within the same forest, across forests, or with an external realm, Windows Server creates a trusted domain object to store the trusts' information, such as transitivity and type, in AD DS. Windows Server stores this trusted domain object in the System container in AD DS.

Chapter 4 Define OUs

An OU is a container object within a domain that you can use to consolidate users, computers, groups, and other objects. You can link Group Policy Objects (GPOs) directly to an OU to manage the users and computers contained in the OU. You can also assign an OU manager and associate a COM+ partition with an OU.

You can create new OUs in AD DS by using:

- Active Directory Administrative Center.
- Active Directory Users and Computers.
- Windows Admin Center.
- Windows PowerShell with the Active Directory PowerShell module.

Chapter 5 Why create OUs?

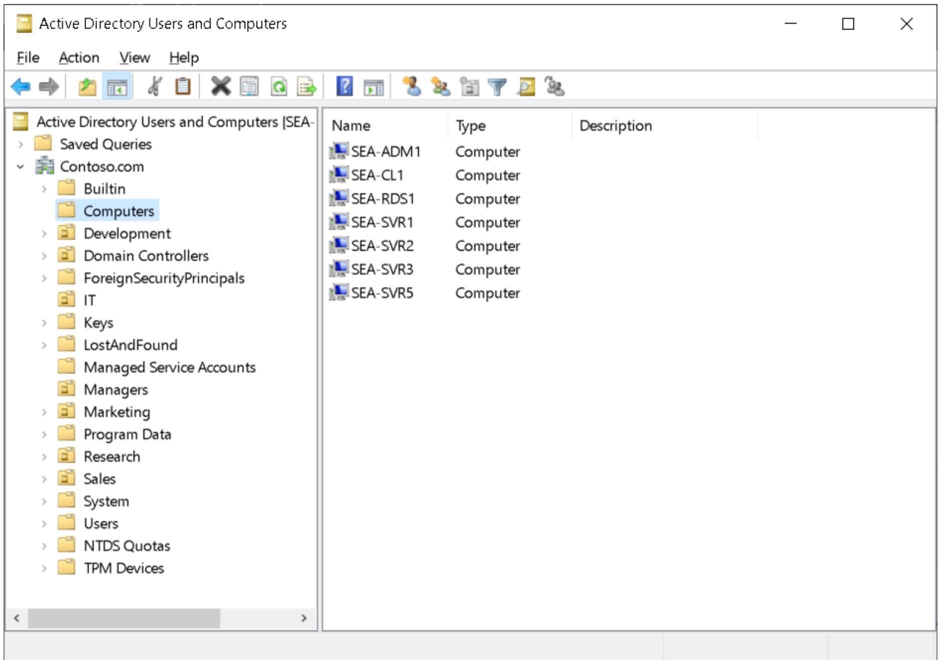
There are two reasons to create an OU:

- To consolidate objects to make it easier to manage them by applying GPOs to the collective. When you assign GPOs to an OU, the settings apply to all the objects within the OU. GPOs are policies that administrators create to manage and configure settings for computers or users. You deploy the GPOs by linking them to OUs, domains, or sites.
- To delegate administrative control of objects within the OU. You can assign management permissions on an OU, thereby delegating control of that OU to a user or a group within AD DS, in addition to the Domain Admins group.

You can use OUs to represent the hierarchical, logical structures within your organization. For example, you can create OUs that represent the departments within your organization, the geographic regions within your organization, or a combination of both departmental and geographic regions. You can use OUs to manage the configuration and use of user, group, and computer accounts based on your organizational model.

5.1 What are the generic containers?

AD DS has several built-in containers, or generic containers, such as Users and Computers. These containers store system objects or function as the default parent objects to new objects that you create. Don't confuse these generic container objects with OUs. The primary difference between OUs and containers is the management capabilities. Containers have limited management capabilities. For example, you can't apply a GPO directly to a container.



Name	Type	Description
SEA-ADM1	Computer	
SEA-CL1	Computer	
SEA-RDS1	Computer	
SEA-SVR1	Computer	
SEA-SVR2	Computer	
SEA-SVR3	Computer	
SEA-SVR5	Computer	

Installing AD DS creates the Domain Controllers OU and several generic container objects by default. AD DS primarily uses some of these default objects, which are also hidden by default. The following objects are displayed by default:

Domain. The top level of the domain organizational hierarchy.

Builtin container. A container that stores several default groups.

Computers container. The default location for new computer accounts that you create in the domain.

Foreign Security Principals container. The default location for trusted objects from domains outside the local AD DS domain that you add to a group in the local AD DS domain.

Managed Service Accounts container. The default location for managed service accounts. AD DS provides automatic password management in managed service accounts.

Users container. The default location for new user accounts and groups that you create in the domain. The Users container also holds the administrator, the guest accounts for the domain, and some default groups.

Domain Controllers OU. The default location for domain controllers' computer accounts. This is the only OU that is present in a new installation of AD DS.

There are several containers that you can review when you select Advanced Features. The following table describes the objects that are hidden by default.

Object	**Description**
LostAndFound	This container holds orphaned objects.
Program Data	This container holds Active Directory data for Microsoft applications, such as Active Directory Federation Services (AD FS).
System	This container holds the built-in system settings.
NTDS Quotas	This container holds directory service quota data.
TPM Devices	This container stores the recovery information for Trusted Platform Module (TPM) devices.

5.2 Use a hierarchical design

The administrative needs of the organization dictate the design of an OU hierarchy. Geographic, functional, resource, or user classifications could all influence the design. Whatever the order, the hierarchy should make it possible to administer AD DS resources as effectively and flexibly as possible. For example, if you need to configure all IT administrators’ computers in a certain way, you can group all the computers in an OU and then assign a GPO to manage those computers.

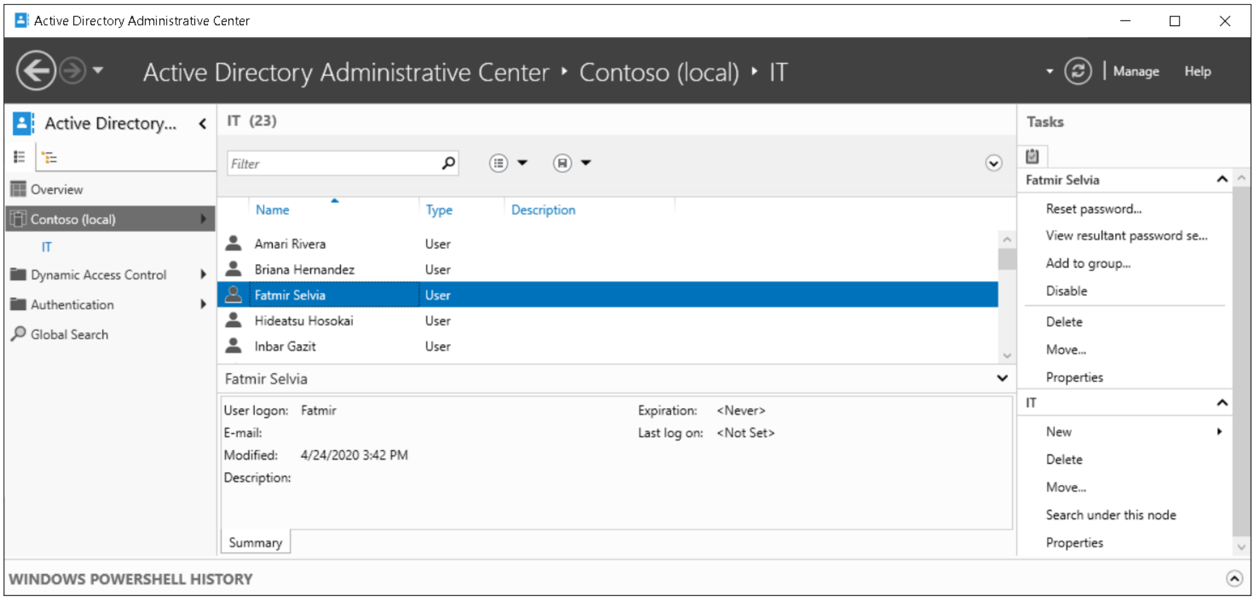
You also can create OUs within other OUs. For example, your organization might have multiple offices, each with its own IT administrator who is responsible for managing user and computer accounts. In addition, each office might have different departments with different computer-configuration requirements. In this situation, you can create an OU for each office, and then within each of those OUs, create an OU for the IT administrators and an OU for each of the other departments.

Although there is no limit to the number of levels in your OU structure, limit your OU structure to a depth of no more than 10 levels to ensure manageability. Most organizations use five levels or fewer to simplify administration. Note that applications that work with AD DS can impose restrictions on the OU depth within the hierarchy for the parts of the hierarchy that they use.

Chapter 6 Manage objects and their properties in AD DS

6.1 Active Directory Administrative Center

The Active Directory Administrative Center provides a GUI that is based on Windows PowerShell. This enhanced interface allows you to perform AD DS object management by using task-oriented navigation, and it replaces the functionality of Active Directory Users and Computers.



Name	Type	Description
Amari Rivera	User	
Briana Hernandez	User	
Fatmir Selvia	User	
Hideatsu Hosokai	User	
Inbar Gazit	User	

Fatmir Selvia

User logon: Fatmir
E-mail:
Modified: 4/24/2020 3:42 PM
Description:
Expiration: <Never>
Last log on: <Not Set>

Tasks that you can perform by using the Active Directory Administrative Center include:

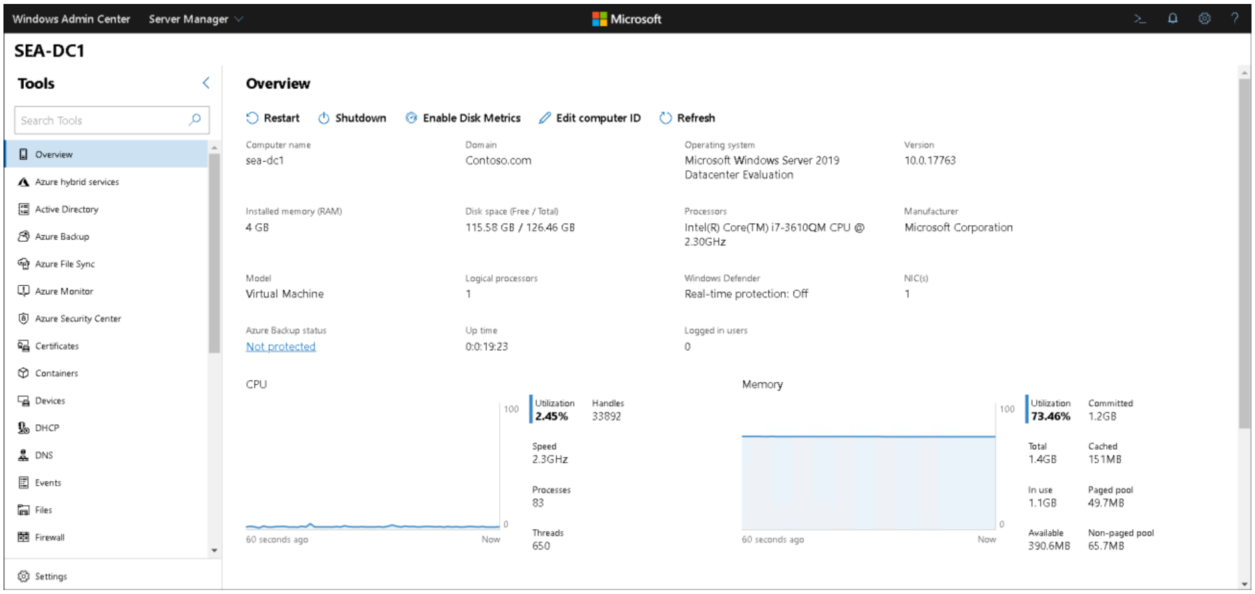
- Creating and managing user, computer, and group accounts.
- Creating and managing OUs.
- Connecting to and managing multiple domains within a single instance of the Active Directory Administrative Center.
- Searching and filtering AD DS data by building queries.
- Creating and managing fine-grained password policies.
- Recovering objects from the Active Directory Recycle Bin.
- Managing objects that the Dynamic Access Control feature requires.

6.2 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 10. Typically, you use Windows Admin Center to manage servers instead of using Remote Server Administration Tools (RSAT).

Windows Admin Center works with any browser that is compliant with modern standards, and you can install it on computers that run Windows 10 and Windows Server with Desktop Experience.

With a decreasing number of exceptions, Windows Admin Center supports most current Windows Server and Windows 10 administrative functionality. However, Microsoft intends that Windows Admin Center will eventually support all the administrative functionality that is presently available through RSAT.



Computer name: sea-dc1
Domain: Contoso.com
Operating system: Microsoft Windows Server 2019 Datacenter Evaluation
Version: 10.0.17763
Installed memory (RAM): 4 GB
Disk space (Free / Total): 115.58 GB / 126.46 GB
Processors: Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz
Manufacturer: Microsoft Corporation
Model: Virtual Machine
Logical processors: 1
Windows Defender: Real-time protection: Off
NIC(s): 1
Azure Backup status: Not protected
Up time: 0:0:19:23
Logged in users: 0

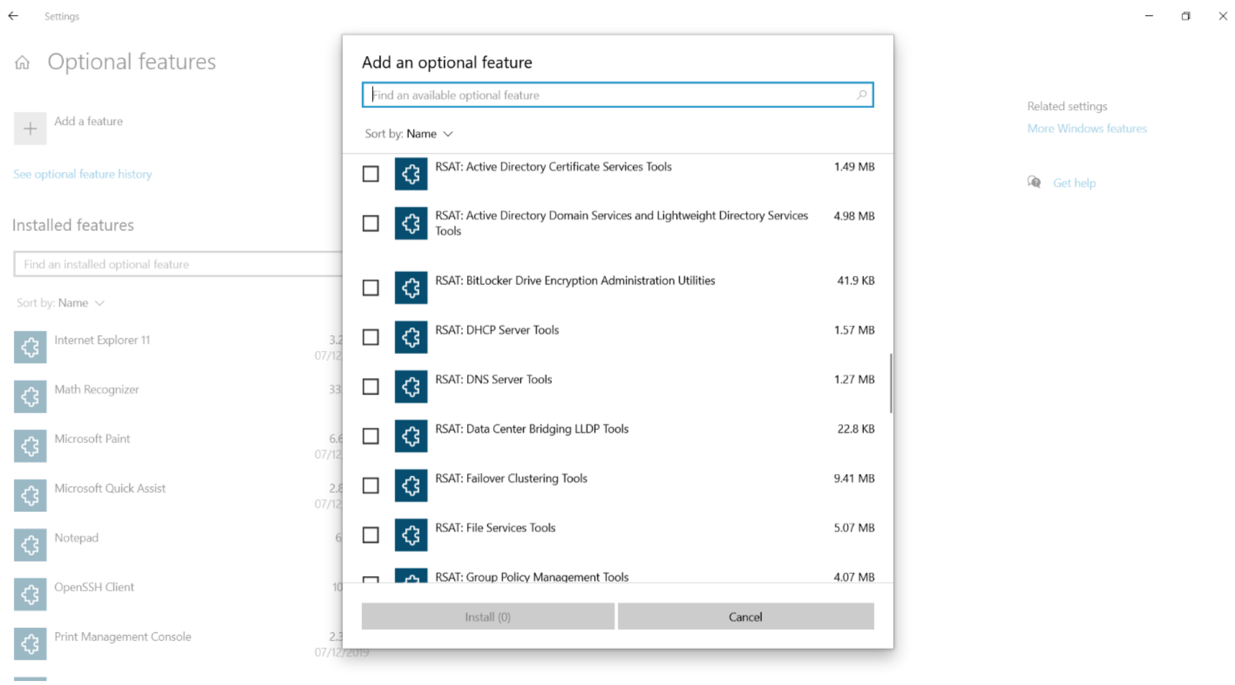
CPU — Utilization 2.45%; Handles 33892; Speed 2.3GHz; Processes 83; Threads 650

Memory — Utilization 73.46%; Committed 1.2GB; Total 1.4GB; Cached 151MB; In use 1.1GB; Paged pool 49.7MB; Available 390.6MB; Non-paged pool 65.7MB

To use Windows Admin Center, you must first download and install it. You can download Windows Admin Center from the Microsoft download website. After downloading and installing Windows Admin Center, you must enable the appropriate TCP port on the local firewall. On a Windows 10 computer (in standalone mode), this defaults to 6516. On Windows Server (in gateway mode), this defaults to TCP 443. In both cases, you can change it during setup.

6.3 Remote Server Administration Tools

RSAT is a collection of tools that enables you to manage Windows Server roles and features remotely.



Settings

Optional features

Add a feature

See optional feature history

Installed features

Find an installed optional feature

Sort by: Name

- Internet Explorer 11
- Math Recognizer
- Microsoft Paint
- Microsoft Quick Assist
- Notepad
- OpenSSH Client
- Print Management Console

Add an optional feature

Find an available optional feature

Sort by: Name

□	RSAT: Active Directory Certificate Services Tools	1.49 MB
□	RSAT: Active Directory Domain Services and Lightweight Directory Services Tools	4.98 MB
□	RSAT: BitLocker Drive Encryption Administration Utilities	41.9 KB
□	RSAT: DHCP Server Tools	1.57 MB
□	RSAT: DNS Server Tools	1.27 MB
□	RSAT: Data Center Bridging LLDP Tools	22.8 KB
□	RSAT: Failover Clustering Tools	9.41 MB
□	RSAT: File Services Tools	5.07 MB
□	RSAT: Group Policy Management Tools	4.07 MB

You can install the consoles available within RSAT on computers running Windows 10 or on server computers that are running the Server with Desktop Experience option of a Windows Server installation. Until the introduction of Windows Admin Center, RSAT consoles were the primary graphical tools for administering the Windows Server operating system.

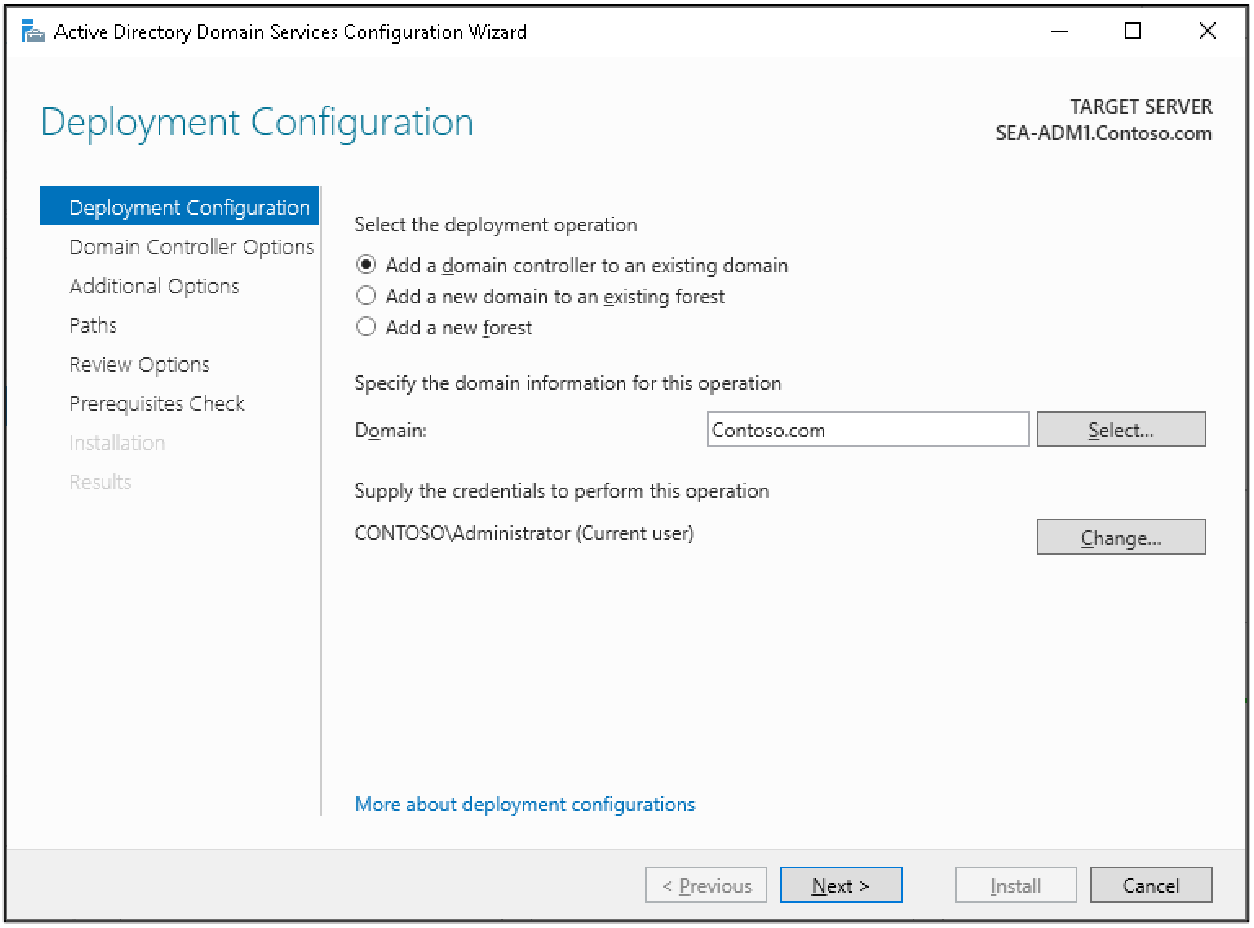
PART 2. Manage AD DS domain controllers and FSMO roles

Chapter 7 Deploy AD DS domain controllers

Domain controllers authenticate all users and computers in a domain. Therefore, it's critical to ensure the optimal number and placement of domain controllers in any AD DS environment, especially in larger, distributed environments such as the one that Contoso is transitioning to.

7.1 Deploy AD DS domain controllers in an on-premises environment

The domain controller deployment process has two steps. First, you install the binaries necessary to implement the domain controller role. For this purpose, you can use Windows Admin Center or Server Manager. At the end of the initial installation process, you have installed the AD DS files, but not yet configured AD DS on the server. The second step is to configure the AD DS role. The simplest way to perform this configuration is by using the **Active Directory Domain Services Configuration Wizard**. You start the wizard by selecting the AD DS link in Server Manager.



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
SEA-ADM1.Contoso.com

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: Contoso.com

Supply the credentials to perform this operation

CONTOSO\Administrator (Current user)

More about deployment configurations

7.1.1 Install a domain controller on a Server Core installation of Windows Server

A Windows Server computer that is running a Server Core installation doesn't have the Server Manager graphical user interface (GUI). Therefore, you must use alternative methods to install the files for the domain controller role and to install the domain controller role itself. You can use Windows Admin Center, Server Manager, Windows PowerShell, or Remote Server Administration Tools (RSAT) installed on any supported version of Windows Server that has the **Desktop Experience** feature, or any supported Windows client such as Windows 10.

7.1.2 Install a domain controller from the media

If you have a network connection between sites that is slow, unreliable, or costly, you might find it beneficial to add another domain controller at a remote location or branch office. In this scenario, to significantly reduce the amount of traffic moving over the wide area network (WAN) link, you can create an AD DS backup (perhaps to a USB drive) and take this backup to the remote location. When you're at the remote location and run Server Manager to install AD DS, you can select the **Install from Media** option. Most of the copying occurs locally. In this scenario, the WAN link transfers only security-related traffic and AD DS changes following the backup. The WAN link also helps ensure that the new domain controller receives any changes made to the central AD DS after you create the Install from media backup.

7.1.3 Branch Office Considerations

When you deploy a domain controller in a branch office that can't guarantee physical security, you can use additional measures to reduce the impact of a security breach. One option is to deploy an RODC. The RODC contains a read-only copy of the AD DS database, and by default, it doesn't cache any user passwords. However, you can configure the RODC to cache the passwords for users in the branch office. If an RODC is compromised, the potential loss of information risk is much lower than with a full read/write domain controller.

7.2 Upgrade domain controllers from the previous version

The process for upgrading a domain controller is the same for any version of Windows Server starting with Windows Server 2012 R2 through Windows Server 2022. You can upgrade to a Windows Server 2022 domain using either of the following methods:

- Upgrade the OS on existing domain controllers that are running Windows Server 2012 R2 or later.
- Add servers running Windows Server 2022 as domain controllers in a domain that already has domain controllers running earlier Windows Server versions.

We recommend the latter method because when you finish you'll have a clean installation of both the Windows Server 2022 OS and the AD DS database. Whenever you add a new domain controller, Windows Server automatically updates the domain DNS records so clients will be able to locate and use this domain controller.

7.3 Deploy AD DS domain controllers in Azure virtual machines (VMs)

Azure provides infrastructure as a service (IaaS), which is a cloud-based virtualization platform. When deploying AD DS on Azure IaaS, you're installing the domain controller on a VM, so all the rules that apply to virtualizing a domain controller apply to deploying AD DS in Azure.

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

- Network topology. To meet AD DS requirements, you must create an Azure Virtual Network and attach your VMs to it. If you intend to join an existing on-premises AD DS infrastructure, you can extend network connectivity to your on-premises environment. You can achieve this through hybrid connectivity methods such as a virtual private network (VPN) connection or an Azure ExpressRoute circuit, depending on the speed, reliability, and security that your organization requires.
- Site topology. As with a physical site, you should define and configure an AD DS site that 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 that will persist across restarts and shutdowns.
- DNS. Azure's built-in DNS does not meet the requirements of AD DS, such as Dynamic DNS and service (SRV) resource records. To provide DNS functionality for an AD DS environment in Azure, you can use the Windows Server DNS server role or other DNS solutions available in Azure, such as Azure private DNS zones.
- 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, and set the **Host Cache Preference** setting of that disk to **NONE**.

Chapter 8 Maintain AD DS, domain controllers

There are operational aspects applicable to every AD DS environment that focus on maintaining the business continuity of the authentication services. This includes backup and recovery of domain controllers, and the AD DS objects they host.

8.1 Maintain AD DS domain controller availability

Domain controllers use a multi-master replication process to copy data from one domain controller to another. As a best practice, an AD DS domain should have at least two domain controllers per AD DS site. This makes the AD DS database more available and spreads the authentication load during peak sign-in times.

8.2 Plan for AD DS backup and restore

Maintaining the reliability of the Active Directory data is important. Performing regular backups can play a part in this process but knowing how to restore or recover data after a failure is vital.

8.2.1 Restoring deleted AD DS objects by using the Recycle Bin

Because restoring objects deleted from AD DS by using traditional backup methods involves temporary OS downtime, Windows Server offers the **Active Directory Recycle Bin** feature, which provides a straightforward method to restore deleted objects with no AD DS downtime. After you enable the **Active Directory Recycle Bin**, the Deleted Objects container displays in the Active Directory Administrative Center. Deleted objects persist in this container until their deleted object lifetime expires. For new AD DS deployments, that lifetime is set to 180 days, but you have the option to change it. You can choose to restore the objects either to their original location or to an alternate location within AD DS.

8.2.2 AD DS backup and restore

To restore AD DS, a backup must explicitly include system state data. *The system state* is a collection of critical OS and server role files that include the AD DS database and the registry.

To perform an AD DS restore, you must have full access to the files on the domain controller. This requires restarting the domain controller in DSRM. If you're restarting a domain controller locally, open the advanced startup options and choose the DSRM from the menu.

When you start a domain controller in DSRM, you will sign in as an Administrator with the DSRM password. You then can use Windows Server Backup to restore the directory database. After completing the restore process, you must restart the server you are recovering. The domain controller will ensure that its database is consistent with the rest of the domain by pulling from its replication partners the changes to the directory that have occurred since the date of the backup.

8.3 Nonauthoritative restore

By default, you restore an AD DS backup as of a known good date. Essentially, you roll the domain controller back in time. When AD DS restarts on the domain controller, the domain controller contacts its replication partners and requests all subsequent updates. In other words, the domain controller catches up with the rest of the domain by using standard replication mechanisms.

This type of restore is useful when the directory on a domain controller has been damaged or corrupted, but the problem has not spread to other domain controllers. However, in some scenarios, this approach is not suitable. For example, this will not enable you to recover an object you deleted after the backup took place if that deletion has replicated to other domain controllers. If you restore a known good version of AD DS and restart the domain controller, the deletion that happened after the backup took place will simply replicate back to the domain controller.

8.4 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. In an authoritative restore, you start with the same sequence of steps as the nonauthoritative restore. However, before you restart the domain controller, you mark the restored objects that you want to persist as authoritative, so they will replicate from the restored domain controller outbound to its replication partners.

Chapter 9 Manage the AD DS Global Catalog role

As part of planning for domain controller deployments, it's important to identify the optimal number and placement of the global catalog role. This becomes relevant when expanding the AD DS environment to other locations, as is the case with Contoso's planned expansion.

9.1 Manage the AD DS global catalog role

The *global catalog* is a partial, read-only, searchable copy of all the objects in a forest. The global catalog can help speed up searches for objects that might be stored on domain controllers in a different domain in the forest.

Within a single domain, the AD DS database on each domain controller contains all the information about every object in that domain. However, only a subset of this information replicates to the global catalog servers in other domains in the forest. Within a domain, a query for an object is directed to one of the domain controllers in that domain. However, that query does not return results about objects in other domains within the forest. For a query to include results from other forest domains, you must query a domain controller that is also a global catalog server.

The global catalog doesn't contain all the attributes for each object. Instead, it maintains the subset of attributes that are most likely to be useful in cross-domain searches. These attributes include, for example, **givenName**, **displayName**, and **mail**. You can change the set of attributes replicated to the global catalog by modifying the AD DS schema.

In a multiple-domain forest, searching the global catalog can be useful in many situations. For example, when a server that's running Microsoft Exchange Server receives an incoming email, it must search for the recipient’s account so it can decide how to route the message. By automatically querying the global catalog, the server can find the recipient in a multiple-domain environment. Additionally, when users sign in to their Active Directory accounts, the domain controller that performs the authentication must contact the global catalog to check for universal group memberships before authenticating the users.

In a single domain, you should configure all the domain controllers to have a copy of the global catalog. In multiple-domain and multiple-site forests, it might sometimes make sense to limit the number of domain controllers hosting the global catalog role to reduce the volume of replication traffic, although this is an uncommon scenario. Note, however, that this will introduce a dependency on connectivity to other sites when performing global catalog queries.

Chapter 10 Manage AD DS operations masters

AD DS uses a multiple-master process to copy data between domain controllers and automatically implements a conflict resolution algorithm that remediates simultaneous, conflicting updates. These provisions allow for a distributed management model, where multiple users and applications can concurrently apply changes to AD DS objects on different domain controllers. Such a model is necessary to support any AD DS environment with two or more domain controllers. However, it's particularly critical for larger, distributed environments such as Contoso's. It's important to remember though, that certain operations can be performed only by a specific role, on a specific domain controller.

10.1 What are AD DS operations masters?

AD DS operation master roles are responsible for performing operations that are not suitable for a multiple-master model. A domain controller that has one of these roles is an operations master. An operations master role is also known as a *Flexible Single Master Operation (FSMO)* role. There are five operations master roles:

- Schema master
- Domain-naming master
- Infrastructure master
- RID master
- PDC emulator master

By default, the first domain controller installed in a forest hosts all five roles. However, you can transfer these roles after deploying additional domain controllers. When performing operations master-specific changes, you must connect to the domain controller with the role. The five operations master roles have the following distribution:

- Each forest has one schema master and one domain naming master.
- Each AD DS domain has one relative ID (RID) master, one infrastructure master, and one primary domain controller (PDC) emulator.

You can place all five on a single domain controller, or distribute them across several domain controllers.

10.2 Forest operations masters

A forest has the following operations master roles:

- Domain naming master. This is the domain controller that you must contact when you add or remove a domain or make domain name changes.

10.3 Domain operations masters

A domain has the following operations master roles:

- RID master. Whenever you create a security principal such as a user, computer, or group in AD DS, the domain controller where you created the object assigns the object a unique identifying number known as a *security ID (SID)*. To ensure that no two domain controllers assign the same SID to two different objects, the RID master allocates blocks of RIDs to each domain controller within the domain to use when building SIDs.
- Infrastructure master. This role maintains interdomain object references, such as when a group in one domain has a member from another domain. In this situation, the infrastructure master manages to maintain the integrity of this reference. For example, when you review an object's **Security** tab, the system references the listed SIDs and translates them into names. In a multiple-domain forest, the infrastructure master updates references to SIDs from other domains with the corresponding security principal names.
- PDC emulator master. The domain controller which is the PDC emulator master serves as the time source for the domain. The PDC emulator master in each domain in a forest synchronizes their time with the PDC emulator master in the forest root domain. You set the PDC emulator master in the forest root domain to synchronize with a reliable external time source. Additionally, by default, changes to Group Policy Objects (GPOs) are by default written to the PDC Emulator master. The PDC emulator master is also the domain controller that receives urgent password changes. If a user's password changes, the domain controller with the PDC emulator master role receives this information immediately. This means that if the user tries to sign in, the domain controller in the user's current location will contact the domain controller with the PDC emulator master role to check for recent changes. This will occur even if a domain controller in a different location that had not yet received the new password information authenticated the user.

10.4 Manage AD DS operations masters

In an AD DS environment where you distribute operations master roles among domain controllers, you might need to move a role from one domain controller to another. When you perform a move in a planned manner between two online domain controllers, the move is known as *transferring the role*. In emergencies, if the current role holder is not available, the move is known as *seizing the role*. When you transfer a role, the latest data from the domain controller in that role replicates to the target server.

Role	**Snap-in**
Schema master	Active Directory Schema
Domain-naming master	Active Directory Domains and Trusts
Infrastructure master	Active Directory Users and Computers
RID master	Active Directory Users and Computers
PDC emulator master	Active Directory Users and Computers

Chapter 11 Manage AD DS schema

Many applications and services utilize data that are stored in an AD DS database. Some of them, such as Contoso's newly developed in-house application that you need to implement, require that data be in a specific format. This, in turn, might require extending the AD DS schema.

11.1 What is a schema?

AD DS stores and retrieves information from a wide variety of applications and services. It does this, in part, by standardizing how the AD DS directory stores data. By standardizing data storage, AD DS can retrieve, update, and replicate data while helping to maintain data integrity.

An *AD DS schema* is the component that defines all the object classes and attributes that AD DS uses to store data. All domains in a forest contain a copy of the schema that applies to that forest. Any change in the schema replicates to every domain controller in the forest via their replication partners. However, changes originate at the schema master.

11.2 Objects

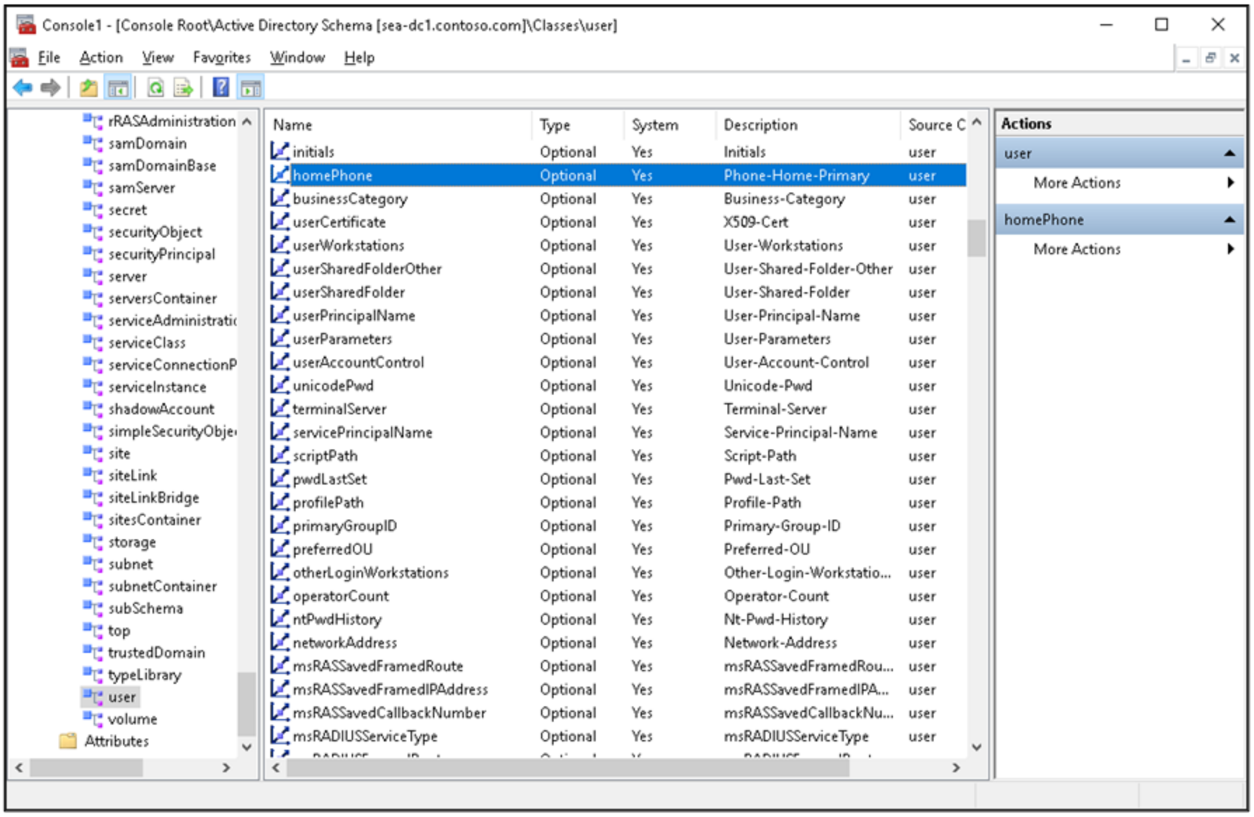
AD DS uses objects as units of storage. The schema defines all object types. Each time the directory manages data, the directory queries the schema for an appropriate object definition. Based on the object definition in the schema, the directory creates the object and stores the data.

Object definitions specify both the types of data that the objects can store and the data syntax. You can only create objects that the schema defines. Because objects store data in a rigidly defined format, AD DS can store, retrieve, and validate the data that it manages, regardless of which application supplies it.

11.2.1Relationships among objects, rules, attributes, and classes

AD DS schema objects consist of attributes, which are grouped together into classes. Each class has rules that define which attributes are mandatory and which are optional. For example, the user class consists of more than 400 possible attributes, including **cn** (the common name attribute), **givenName**, **displayName**, **objectSID**, and **manager**. Of these attributes, the **cn** and **objectSID** attributes are mandatory.

The user class is an example of a structural class. A structural class is the only type of class that can have objects in an AD DS database. To modify the schema, you can create an auxiliary class with its own attributes, and then reference it in the definition of a structural class.

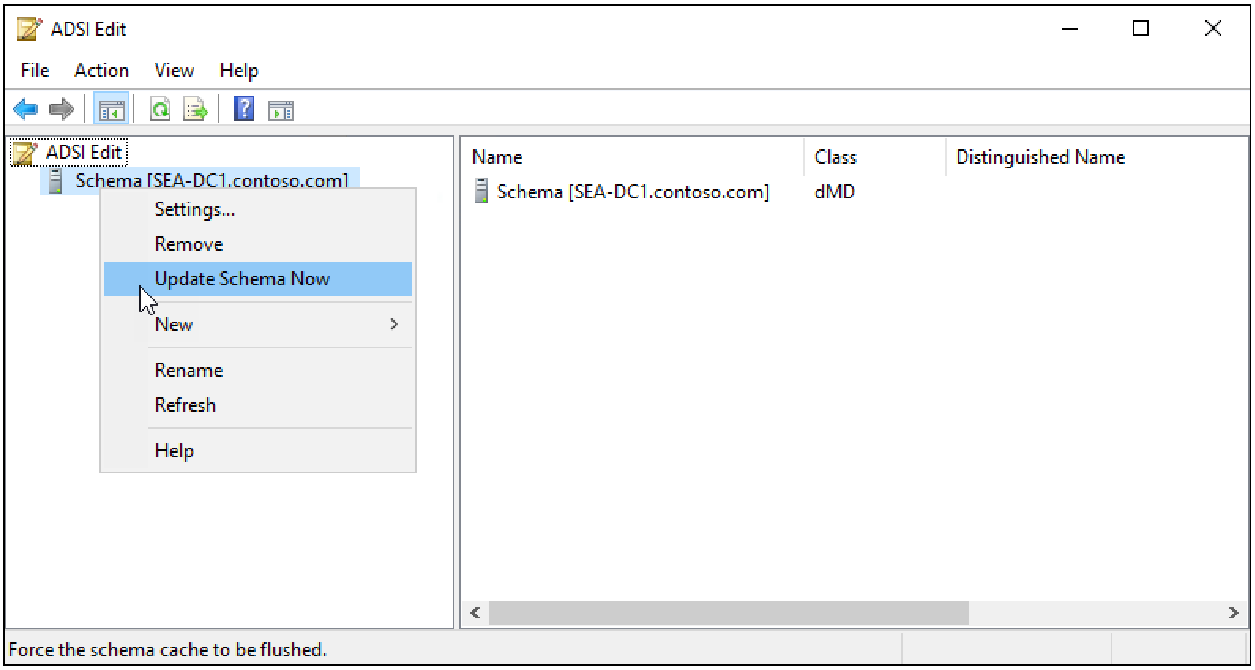


Name	Type	System	Description	Source C
initials	Optional	Yes	Initials	user
homePhone	Optional	Yes	Phone-Home-Primary	user
businessCategory	Optional	Yes	Business-Category	user
userCertificate	Optional	Yes	X509-Cert	user
userWorkstations	Optional	Yes	User-Workstations	user
userSharedFolderOther	Optional	Yes	User-Shared-Folder-Other	user
userSharedFolder	Optional	Yes	User-Shared-Folder	user
userPrincipalName	Optional	Yes	User-Principal-Name	user
userParameters	Optional	Yes	User-Parameters	user
userAccountControl	Optional	Yes	User-Account-Control	user
unicodePwd	Optional	Yes	Unicode-Pwd	user
terminalServer	Optional	Yes	Terminal-Server	user
servicePrincipalName	Optional	Yes	Service-Principal-Name	user
scriptPath	Optional	Yes	Script-Path	user
pwdLastSet	Optional	Yes	Pwd-Last-Set	user
profilePath	Optional	Yes	Profile-Path	user
primaryGroupID	Optional	Yes	Primary-Group-ID	user
preferredOU	Optional	Yes	Preferred-OU	user
otherLoginWorkstations	Optional	Yes	Other-Login-Workstatio...	user
operatorCount	Optional	Yes	Operator-Count	user
ntPwdHistory	Optional	Yes	Nt-Pwd-History	user
networkAddress	Optional	Yes	Network-Address	user
msRASSavedFramedRoute	Optional	Yes	msRASSavedFramedRou...	user
msRASSavedFramedIPAddress	Optional	Yes	msRASSavedFramedIPA...	user
msRASSavedCallbackNumber	Optional	Yes	msRASSavedCallbackNu...	user
msRADIUSServiceType	Optional	Yes	msRADIUSServiceType	user

11.3 Manage AD DS schema

When managing the AD DS schema, you can modify the schema only if you are a member of the Schema Admins group in the root domain of the AD DS forest. For this purpose, you can use the Active Directory Schema snap-in.

You should change the schema only when necessary because the schema controls the storage of information. Additionally, any changes made to the schema affect every domain controller. Before you change the schema, you should review the changes and implement them only after you've performed testing. This will help ensure that the changes Won't adversely affect the rest of the forest or any applications that use AD DS.



Name	Class	Distinguished Name
Schema [SEA-DC1.contoso.com]	dMD	

Force the schema cache to be flushed.

Summary

With all the above content, we have learned about relationships in an Active Direction Domain system and how to manage domains in the system.

However, because it is the first time reporting, as well as limited vocabulary and knowledge, errors cannot be avoided. Therefore, we hope to receive comments and corrections from specialized lecturers. Thanks so much!