Module 2

Introduction to Active Directory Domain Services

Module Overview

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 provides a method for applying configuration and security settings for objects in the enterprise. This module covers the structure of AD DS and its various components, such as forest, domain, and organizational units (OUs).

Overview of AD DS

AD DS is composed of both logical and physical components. You need to understand the way the components of AD DS work together so that you can manage your infrastructure efficiently. In addition, you can use many other AD DS options to perform actions such as installing, configuring, and updating apps, managing the security infrastructure, enabling Remote Access and DirectAccess, and issuing and managing digital certificates.

Active Directory Domain Services (AD DS) is composed of both logical and physical components

Logical components	Physical components
• Partitions • Schema • Domains • Domain trees • Forests • Sites • Organizational units (OUs) • Containers	• Domain controllers • Data stores • Global catalog servers • Read-only domain controllers (RODC)

One of the most used AD DS features is Group Policy, which enables you to configure centralized policies that you can use to manage most objects in AD DS. Understanding the various AD DS components is important to successfully using Group Policy.

Logical Components

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

Logical component	Description
Partition	A section of the AD DS database. Although the database is one file named Ndts.dit, it is viewed, managed, and replicated as if it consisted of distinct sections or instances. These are called *partitions*, which are also referred to as *naming contexts*.
Schema	The set of definitions of the object types and attributes that are used to create objects in AD DS.
Domain	A logical, administrative container for users and computers.
Domain tree	A collection of domains that share a common root domain and a contiguous Domain Name System (DNS) namespace.
Forest	A collection of domains that share a common AD DS.
Site	A collection of users, groups, and computers as defined by their physical location. Sites are useful in planning administrative tasks such as replication of changes to the AD DS database.
Organizational unit (OU)	An organizational unit is a container object that provides a framework for delegating administrative rights and for linking Group Policy Objects (GPOs).
Container	A container is an object that provides an organizational framework for use in AD DS. Containers cannot have GPOs linked to them.

Physical Components

The following table lists some of the physical components of AD DS and gives a brief description of each.

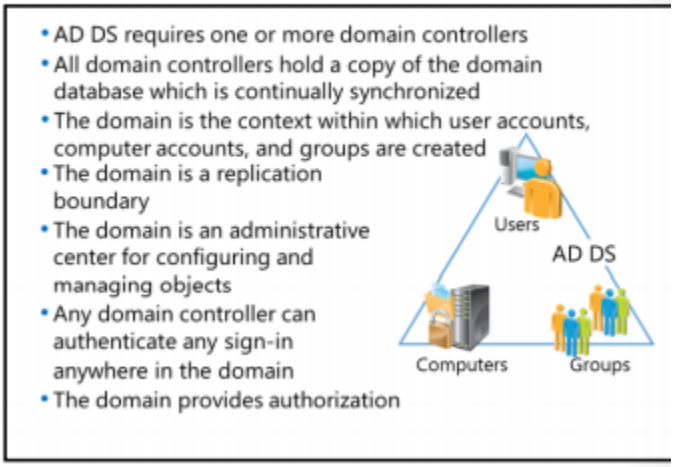
Physical component	Description
Domain controller	Contains a copy of the AD DS database. For most operations, each domain controller can process changes and replicate the changes to all the other domain controllers in the domain.
Data store	The files on each domain controller that holds the AD DS database. The Ntds.dit file, and associated log files, is a Microsoft JET database, which is stored in the C:\Windows\NTDS folder by default.

Global catalog server	A domain controller that hosts the *global catalog*, which is a partial, read-only copy of all the objects in the 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)	A special read-only installation of AD DS. These are often used in branch offices where security and IT support are less advanced than in the main corporate centers.

What Are AD DS Domains?

The AD DS Domain Contains User, Computers, Groups

An AD DS domain is a logical container used to manage user, computer, group, and other objects. All of the domain objects are stored in the AD DS database, a copy of which is stored on each domain controller.



There are many types of objects in the AD DS database, including user accounts, computer accounts, and groups. The following list gives a brief description of these three object types:

- User accounts. User accounts contain the required information to authenticate a user during the sign-in process and to build the users access token.
- Computer accounts. Each domain-joined computer has an account in AD DS. Computer accounts are used in the same matter as user accounts, only for the domain-joined computers.
- Groups. Groups are used to organize users or computers to make it easier to manage permissions and group policy in the domain.

The AD DS Domain is a Replication Boundary

When changes are made to any object in the domain, the domain controller where the change occurred replicates that change to all the other domain controllers in the domain. If there are multiple domains in the forest, only subsets of the changes are replicated to other domains. AD DS uses a multi-master replication model that allows every domain controller to make changes to objects in the domain. Changes to relative ID (RID) management in the Windows Server 2012 version of Active Directory Domain Services (Windows Server 2012 Active Directory now allow a single domain to contain nearly 2 billion objects. With this capacity, most organizations could deploy only a single domain although organizations that have decentralized administrative structures, or that are distributed across multiple locations, might consider implementing multiple domains in the same forest.

The AD DS Domain is an Administrative Center

It 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 members of the Domain Admins group have full control over every object in the domain. The Administrator account in the forest root domain has additional rights as detailed in the "What Is an AD DS Forest?" topic.

The AD DS Domain Provides Authentication

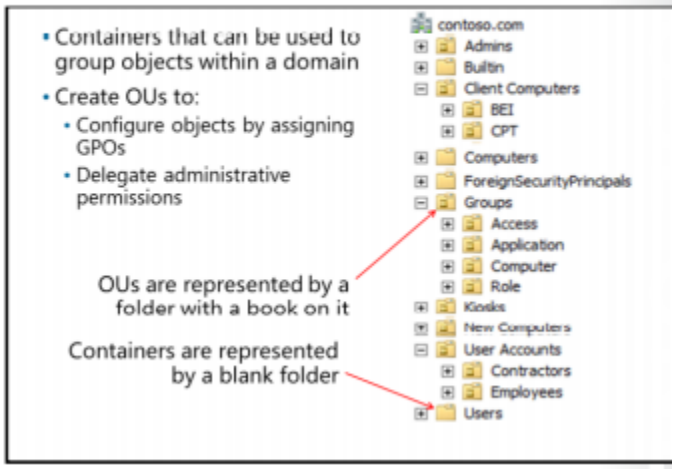
Whenever a domain-joined computer starts up, or a user signs in to a domain-joined computer, AD DS authenticates them. Authentication verifies the computer or user has the proper credentials for an AD DS account.

The AD DS Domain Provides Authorization

Windows operating systems use authorization and access control technologies to allow authenticated users to access resources. Typically the authorization process is performed locally at the resource. Windows Server 2012 introduced domain based Dynamic Access Control to allow for central access rules to control access to resources. Central access rules do not replace the current access control technology; it just provides an additional level of control.

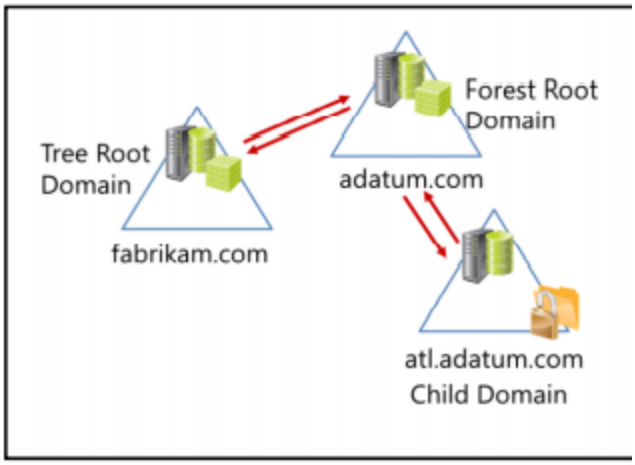
What Are OUs?

An *organizational unit* (OU) is a container object within a domain that you can use to consolidate users, computers, groups, and other objects. These should not be confused with the generic container objects in AD DS. The primary difference between OUs and containers are the management capabilities. Containers have limited management capabilities, for instance you cannot directly apply a GPO to a container. Typically containers are used for system objects and as the default locations for new objects. With OUs you have more management options; you can directly link GPOs, assign an OU manager



What Is an AD DS Forest?

A domain *tree* is a collection of one or more domains that share a contiguous name space. A *forest* is a collection of one or more domain trees that share a common directory schema and global catalog. The first domain that is created in the forest is called the *forest root domain.* The *forest root domain* contains a few objects that do not exist in other domains in the forest. Since these objects are always created on the very first domain controller created, a forest can consist of as little as one domain with a single domain controller, or

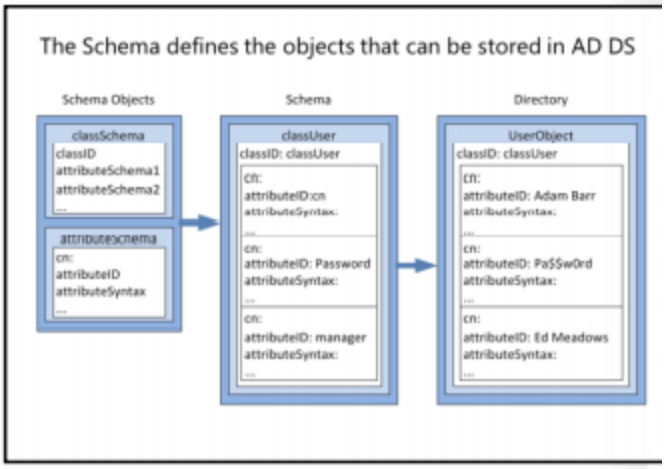


it can consist of hundreds of domains across multiple trees. These objects that only exist in the forest root domain are as follows:

- The schema master role. This is a special forest-wide domain controller role. There is only one schema master in any forest. The schema can be changed only on the domain controller which holds the schema master.
- The domain naming master role. This is also special forest-wide domain controller role. There is only one domain naming master in any forest. New domain names can be added to the directory only by the domain naming master.
- The Enterprise Admins group. By default, the Enterprise Admins group has the Administrator account for the forest root domain as a member. The Enterprise Admins group is a member of the local administrators group in every domain in the forest. This allows members of the Enterprise Admins group to have full control administrative rights to every domain throughout the forest.
- The Schema Admins group. By default, the Schema Admins group has no members. Only members of the Enterprise Admins group can add members to the Schema Admins group. Members of the Schema Admins group are the only administrators that can make changes to the Schema.

What Is the AD DS Schema?

The *AD DS schema* is the component that defines all object classes and attributes that AD DS uses to store data. It is sometimes referred to as the blueprint for AD DS. The schema is replicated among all domain controllers in the forest. Any change that is made to the schema is replicated to every domain controller in the forest from the schema master holder, typically the first domain controller in the forest.



AD DS stores and retrieves information from a wide variety of applications and services; it does this, in part, by standardizing how data is stored in the AD DS directory. By standardizing how data is stored, AD DS can retrieve, update, and replicate data, while ensuring that the integrity of the data is maintained.

Objects

AD DS uses objects as units of storage. All object types are defined in the schema. Each time that the directory handles 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 syntax of the data. You can only create objects in AD DS that are defined by the schema. Because the data is stored in a rigidly defined format, AD DS can store, retrieve, and validate the data that it manages, regardless of which application the data came from.

What Is a Domain Controller?

A *domain controller* is a server that is configured to store a copy of the AD DS directory database (Ntds.dit) and a copy of the SYSVOL folder. All domain controllers except RODCs store a read/write copy of both Ntds.dit and the SYSVOL folder. Ntds.dit is the database itself, and the SYSVOL folder contains all the template settings and files for GPOs.

Domain Controllers

Servers that host the AD DS database (Ntds.dit) and SYSVOL

Kerberos authentication service and Key Distribution Center (KDC) services perform authentication

Best practices:

- Availability:

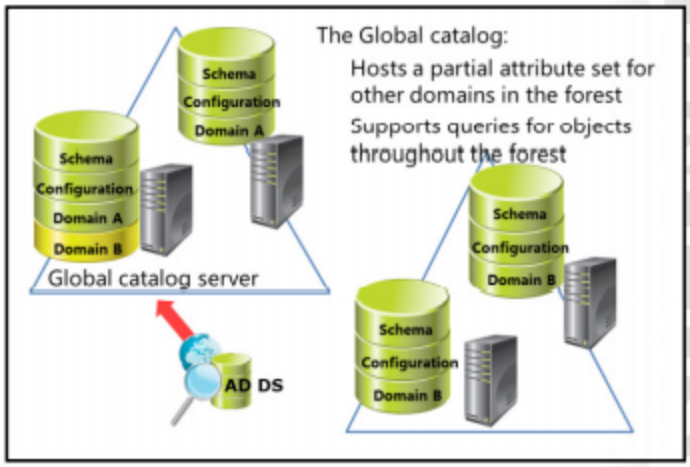
  At least two domain controllers in a domain
- Security:

  RODC and BitLocker

Domain controllers use a multi-master replication process; for most operations, data can be modified on any domain controller, except on RODCs. The AD DS replication service then synchronizes the changes that have been made to the AD DS database to all other domain controllers in the domain. The SYSVOL folders are replicated either by the File Replication Service (FRS), or by the newer Distributed File System (DFS) Replication.

What Is the Global Catalog?

The *global catalog* is a partial, read-only, searchable copy of all the objects in the forest. It speeds 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, but only a subset of this information is replicated to global catalog servers in other domains in the forest. Within a given domain, a query for an object is directed to one of the domain controllers in that domain, but that query cannot provide any results for objects in other domains in the forest. For a query to include results from other domains in the forest you must query a domain controller that is a global catalog server. By default, the only global catalog server that is hosted is the first domain controller in the forest root domain. To enhance searching across domains in a forest, you should configure additional domain controllers to store a copy of the global catalog.

Module 2

Module 2: Introduction to Active Directory Domain Services

Lab: Installing Domain Controllers

Exercise 1: Installing a Domain Controller

▶ Task 1: Add an Active Directory Domain Services (AD DS) role to a member server

1. On LON-DC1, in Server Manager, in the left column, click **All Servers**.
2. Right-click **All Servers**, and then click **Add Servers**.
3. In the **Add Servers** dialog box, in the **Name (CN)** box, type **LON-SVR1**, and then click **Find Now**.
4. Under Name, click **LON-SVR1**, and then click the arrow to add the server to the Selected column.
5. Click **OK** to close the **Add Servers** dialog box.
6. In Server Manager, in the Servers pane, right-click **LON-SVR1**, and then select **Add Roles and Features**.
7. In the Add Roles and Features Wizard, click **Next**.
8. On the **Select installation type** page, ensure that **Role-based or feature-based installation** is selected, and then click **Next**.
9. On the **Select destination server** page, ensure that **Select a server from the server pool** is selected.
10. Under **Server Pool**, verify that **LON-SVR1.Adatum.com** is highlighted, and then click **Next**.
11. On the **Select server roles** page, select the **Active Directory Domain Services** check box, click **Add Features**, and then click **Next**.
12. On the **Select features** page, click **Next**.
13. On the **Active Directory Domain Services** page, click **Next**.
14. On the **Confirm installation selections** page, select the **Restart the destination server automatically if required** check box, and then click **Install**.

    Installation will take several minutes.
15. When the installation completes, click **Close** to close the Add Roles and Features Wizard.

▶ Task 2: Configure a server as a domain controller

1. On LON-DC1, in Server Manager, on the command bar, click the **Notifications** icon—it looks like a flag.
2. Under Post-deployment Configuration, click **Promote this server to a domain controller**.

   The Active Directory Domain Services Configuration Wizard will open.
3. In the Active Directory Domain Services Configuration Wizard, on the **Deployment Configuration** page, ensure that **Add a domain controller to an existing domain** is selected, and then, beside the Domain line, click **Select**.
4. In the **Windows Security** dialog box, in the **Username** box type **Administrator**, in the **Password** box type **Pa$$w0rd** and then click **OK**.
5. In the **Select a domain from the forest** dialog box, click **adatum.com**, and then click **OK**.
6. Beside the **Supply the credentials to perform this operation** line, click **Change**.
7. In the **Windows Security** dialog box, in the **Username** box, type **Adatum\Administrator**, in the **Password** box, type **Pa$$w0rd**, and then click **OK**.
8. On the **Deployment Configuration** page, click **Next**.
9. On the **Domain Controller Options** page, ensure that **Domain Name System (DNS) server** is selected, and then deselect **Global Catalog (GC)**.

Note: You would usually also want to enable the global catalog, but for the purpose of this lab, this is done in the next lab task.

10. In the **Type the Directory Services Restore Mode (DSRM) password** section, type **Pa$$w0rd** in both text boxes, and then click **Next**.
11. On the **DNS Options** page, click **Next**.
12. On the **Additional Options** page, Click **Next**.
13. On the **Paths** page, accept the default folders, and then click **Next**.
14. On the **Review Options** page, click **View Script**, examine the Windows PowerShell script that the wizard generates.
15. Close the Notepad window.
16. On the **Review Options** page, click **Next**.
17. On the **Prerequisites Check** page, read any warning messages, and then click **Install**.
18. When the task completes successfully, click **Close**.
19. Wait for LON-SVR1 to restart.

▶ Task 3: Configure a server as a global catalog server

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. In Server Manager, click **Tools**, and then click **Active Directory Sites and Services**.
3. When Active Directory Sites and Services opens, expand **Sites**, expand **Default-First-Site-Name**, expand **Servers**, and then expand **LON-SVR1**.
4. In the left column, right-click **NTDS Settings**, and then click **Properties**.
5. In the **NTDS Settings Properties** dialog box, select **Global Catalog (GC)**, and then click **OK**.
6. Close Active Directory Sites and Services.

Results: After completing this exercise, you will have explored Server Manager and promoted a member server to be a domain controller.

IF YOU RUN INTO PROBLEMS IN EXERCISE 2 TASK 2 CHECK LOGIN TO SVR2 AS ADATUM ADMINISTRATOR AND CHECK ALL THREE SERVERS DC1, SVR2, RTR RUNNING. ALSO MAKE SURE FOLDER IFM SUCCESSFULLY CREATED ON LON-DC1.

IF COMMAND FAILS FOR SOME REASON THIS PC ON SVR2 AND MAP

Exercise 2: Installing a Domain Controller by Using IFM

▶ Task 1: Use the Ntdsutil tool to generate IFM

1. On LON-DC1, in the lower-left corner of the screen, click the **Start** button.
2. On the Start screen, type **CMD**, right click **Command Prompt** and then click **Run as administrator**.
3. At a command prompt, type the following, pressing Enter after each line:

```
Ntdsutil
Activate instance ntds
Ifm
Create sysvol full c:\ifm
```

4. Wait for the IFM command to complete and then close the command prompt.

▶ Task 2: Add the AD DS role to the member server

1. Switch to **LON-SVR2**, and, if required, sign in as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. In the lower-left corner of the screen, click the **Start** button.
3. On the Start screen, type **CMD**, and then press Enter.
4. Type the following command, and then press Enter:

```
Net use k: \\LON-DC1\c$\IFM
```

5. Switch to **Server Manager**.
6. From the list on the left, click **Local Server**.
7. In the toolbar, click **Manage**, and then click **Add Roles and Features**.
8. On the **Before you begin** page, click **Next**.
9. On the **Select installation type** page, ensure that **Role-based or feature-based installation** is selected, and then click **Next**.
10. On the **Select destination server** page, verify that **LON-SVR2.Adatum.com** is highlighted, and then click **Next**.
11. On the **Select server roles** page, click **Active Directory Domain Services**.
12. In the Add Roles and Features Wizard, click **Add Features**, and then click **Next**.
13. On the **Select Features** page, click **Next**.
14. On the **Active Directory Domain Services** page, click **Next**.
15. On the **Confirm installation selections** page, click **Restart the destination server automatically if required**. Click **Yes** at the message box.
16. Click **Install**.
17. After the installation completes, click **Close**.

Note: If you see a message stating that a delegation for the DNS server cannot be created, click **OK**.

IF PROBLEMS OCCURRED IN TASK 2 TRY REVERTING SVR2 OR RESTART

▶ Task 3: Use IFM to configure a member server as a new domain controller

1. On LON-SVR2, At the command prompt, type the following command, and then press Enter:

```
Robocopy k: c:\ifm /copyall /s
```

2. Close the Command Prompt window.
3. In Server Manager, on the command bar, click the **Notifications** icon.
4. Under Post-deployment Configuration, click **Promote this server to a domain controller**.

   The Active Directory Domain Services Configuration Wizard will open.
5. On the **Deployment Configuration** page, ensure that **Add a domain controller to an existing domain** is selected, and confirm that **adatum.com** is the target domain. Click **Next**.
6. On the **Domain Controller Options** page, ensure that both **Domain Name System (DNS) server** and **Global Catalog (GC)** are selected. For the **DSRM** password, type **Pa$$w0rd** in both boxes, and then click **Next**.
7. On the **DNS Options** page, click **Next**.
8. On the **Additional Options** page, select **Install from media**, in the **Install from media path** box, type **C:\ifm**, and then click **verify**.
9. When the path has been verified, click **Next**.
10. On the **Paths** page, click **Next**.
11. On the **Review Options** page, click **Next**, and then observe the Active Directory Domain Services Configuration Wizard as it performs a check for prerequisites.
12. Click **Install**, and wait while AD DS is configured.

    While this task is running, read the information messages that display on the screen.
13. Wait for the server to restart.

Results: After completing this exercise, you will have installed an additional domain controller for the branch office by using IFM.

▶ Prepare for the next module

When you have completed the lab, revert the virtual machines back to their initial state.

To do this, complete the following steps:

1. On the host computer, start Hyper-V® Manager.
2. In the **Virtual Machines** list, right-click **20410C-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for 20410C-LON-SVR1, 20410C-LON-RTR, and 20410C-LON-SVR2.