Active Directory Services

Scope of Work & Deliverables

09-July-2018

Ver:1.0

Contents

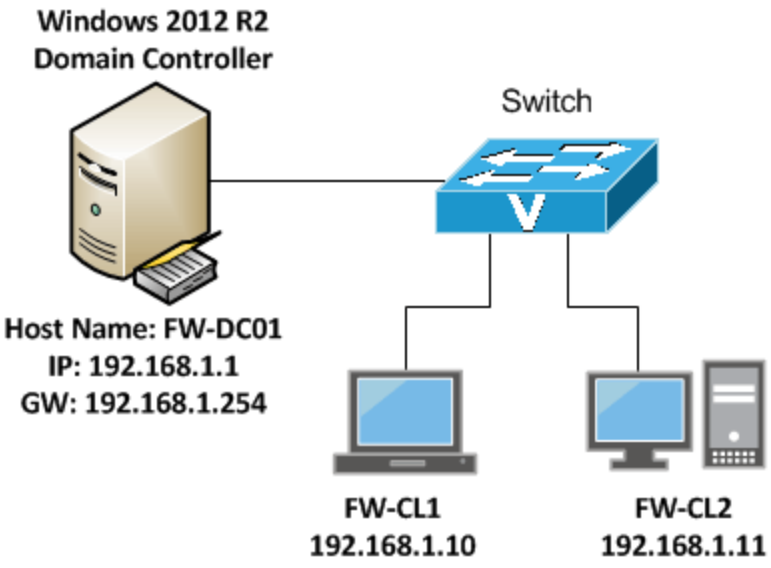
Overview

A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators. For example, AD DS stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information.

Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information.

This data store, also known as the directory, contains information about Active Directory objects. These objects typically include shared resources such as servers, volumes, printers, and the network user and computer accounts.

Communication Design



BENEFITS OF ACTIVE DIRECTORY

1. Centralizing Resource and Security Administration

This is the main benefits of Active Directory. Active Directory provides a single point from which administrators can manage network resources and their associated security objects. An organization can administer Active Directory based on an organizational model, a business model, or the types of functions being administered.

For example, an organization could choose to administer Active Directory by logically dividing the users according to the departments in which they work, their geographical location, or a combination of these characteristics.

Active Directory can simplify the security management of all network resources and extend interoperability with a wide range of applications and devices.

Management is simplified through centralized access to the administrative tools and to the Active Directory database of network resources. Interoperability with prior versions of Microsoft Windows is available in Windows Server 2008 through the use of functional levels.

When Active Directory is installed and configured, it includes a number of GUI and command-lines tools that can be used to administer network services, resources, and security at a detailed level.

These administrative tools can be accessed from any domain controller in the network or an administrative workstation that has these tools installed. When you configure a Windows 2008 Server as an Active Directory domain controller, you will see the following tools added to the Administrative Tools folder:

a. Active Directory Users and Computers
b. Active Directory Domains and Trusts
c. ADSI Edit
d. Active Directory Sites and Services

2. Providing a Single Point of Access to Resources

Active Directory provides a single point of management for network resources. Active Directory uses a single sign-on to allow access to network resources located on any server within the domain.

The user is identified and authenticated by Active Directory once. After this process is complete, the user signs on once to access the network resources that are authorized for the according to his or her assigned roles and privileges within Active Directory.

Prior to the introduction of directory services into corporate networks, all users were required to log on too many different servers in order to access a variety of different resources.
This required users to enter their authentication information multiple times, and an administrator had to maintain duplicate user account on every server in the organization.

Imagine how enormous the task of managing a separate username and password on each server would be if your organization contained 10 servers and 10 users per server.

Now imagine how much more difficult that would become with 10 servers and 500 users per servers. You would have to create and maintain 5000 user accounts, with all of the associated security assignments, if you were maintaining separate authentication for each individual server.

3. Benefiting from Fault Tolerance and Redundancy

Fault Tolerance and Redundancy is the second benefits of Active Directory Domain Services. Active Directory builds in fault tolerance through its multitasker domain controller design.

This fault tolerance is created due to the fact that all domain controllers in an Active Directory domain share a common database file called “ntds.dit;” any change that is made on one domain controller is replicated to all other domain controllers in the environment. This ensures that all domain controllers have consistent information about the domain.

A system is said to be fault tolerance if it is capable of responding to a software or hardware failure. For example, a server is fault tolerance if it can continue to function when a power supply or a hard drive suffers a mechanical failure. An authentication system such as Active Directory is considered fault tolerant when it has the ability to continue providing authentication services even if one or more servers that provide authentication services experience hardware failure or a loss of network connectivity.

In this way, Active Directory can offer a redundant solution which can continue to provide authentication services without any adverse effects noticed by users, workstations, or other services.

Windows Server 2008 introduces the Read-Only Domain Controller (RODC), a domain controller that contains a copy of the “ntds.dit” file that cannot be modified and that does not replicate its changes to other domain controllers within Active Directory.

Microsoft introduced this type of domain controller as a way to increase security in branch-office deployment because many companies find it necessary to deploy domain controllers in far-removed locations that are not secured as well as a centralized data centre.

The Read-Only Domain Controller protects Active Directory against unauthorized changes made from these remote locations.

Because the entire Active Directory database is duplicated on all domain controllers, it is possible for authentication and resource access to take place via another domain controller if one domain controller fails.

Because a single domain controller environment does not offer the fault tolerance described here, configuring at least two domain controllers in every environment is recommended.

4. Simplifying Resource Location

Active Directory simplifies this process by allowing files and print resources to be published on the network. Publishing an object allows users to access network resources by searching the Active Directory database for the desired resource.

This search can be based on the resource's name, description, or location. For example, a shared folder can be found by clicking the appropriate search button using My Network Places in Windows XP or Microsoft Windows Server 2003 or the Network and Sharing Centre in Windows Vista.

A user can configure the search scope. The shared folder name and keyword do not need to be search criteria. Providing more search information creates more specific results.

For example, if you have configured the word "accounting" as a keyword for 100 folders, a search for the keyword will return 100 results that a user would need to sort through to find the desired folder.

Imagine you are a user in a 10 server environment, where every server has a different set of resources that you need to do your job.

If you were in this situation, identifying which server provides each resource would not be an easy task. This is even more complicated when you have mobile users, such as an employee visiting from another site who needs to locate printers and other devices to become productive at the new site.

PREREQUISITE

DC SERVER REQUIREMENT

1.1.1 Hardware Requirement

CPU	Minimum X64 Intel Xeon or x64 AMD Opteron Quad-Core Processor, 2 Dual Processor is Recommended
RAM	DDR3/DDR4 ECC 16GB, 64GB or more recommended for 100+ Users/Workstations
HDD	HDD must be minimum 300GB with at least RAID 1 Configured, RAID 5 Recommended Our Recommended Storage space must be 500+ GB for 100+ Users/Workstations
No. of Users	All the recommended hardware requirements can support 300+ Users/Workstations, AD-DNS, DHCP, WSUS, File Services

1.1.2 Software Requirement

Operating System	Windows Server 2008/2008 R2 with Service Pack 2/2012/2012 R2/2016, all 64-bit Standard/Enterprise/Datacenter Editions
No. of Users	For 10-100 Users Standard Edition, for 100-3000 Users Enterprise Edition

	and for 3000+ Users Datacenter Edition is recommended
.Net Framework	Framework 4.5.2 or Above

1.1.3 Network Requirement

Local Area Network IP Address	**Static**

Client workstation requirement

1.1.4 Hardware Requirement

CPU	Intel Core i3 or Higher
RAM	4 GB or above
Monitor	SVGA color monitor (1366x768)
Hard Disk Space required for Application	500 GB

1.1.5 Software Requirement

Operating System	Microsoft Windows 7 / Windows 10 Professional 32 or 64 Bit with themes other than Basic and Classic
.Net Framework	Framework 4.5.2 or Above
Packages / Patch	• Microsoft Office Excel 2007 or above • XPS Services (Add from Windows Feature) • XPS Viewer (Add from Windows Feature) • Install 'Windows6.1-KB2496898-v3-x86' patch available on Microsoft website (Only for Windows 7)

1.1.6 Network Requirement

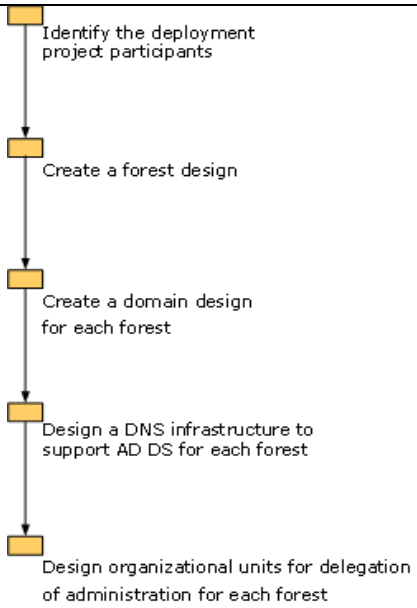
Local Area Network IP Address	DHCP, Static
Both the server & Client Machine should be on same Local Area Network & Primary DNS IP Should be same of Server	

DESIGNING & PLANNING OF ACTIVE DIRECTORY

Designing the Active Directory Logical Structure

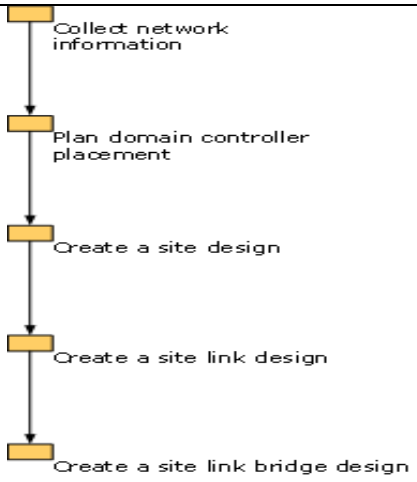
Before you deploy Windows Server 2008 Active Directory Domain Services (AD DS), you must plan for and design the AD DS logical structure for your environment. The AD DS logical structure determines how your directory objects are organized, and it provides an effective method for managing your network accounts and shared resources. When you design your AD DS logical structure, you define a significant part of the network infrastructure of your organization.

To design the AD DS logical structure, determine the number of forests that your organization requires, and then create designs for domains, Domain Name System (DNS) infrastructure, and organizational units (OUs). The following illustration shows the process for designing the logical structure.



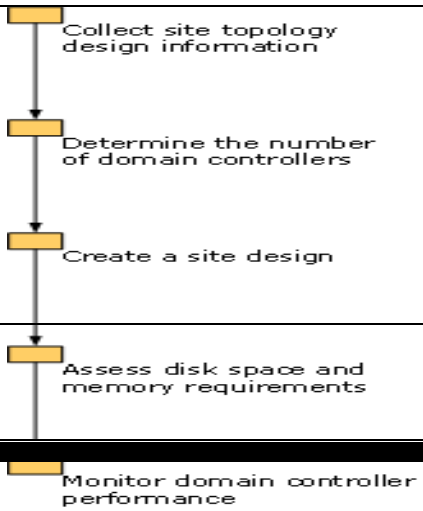
Designing the Site Topology

After you design the logical structure for your AD DS infrastructure, you must design the site topology for your network. The site topology is a logical representation of your physical network. It contains information about the location of AD DS sites, the AD DS domain controllers within each site, and the site links and site link bridges that support AD DS replication between sites. The following illustration shows the site topology design process.



Planning domain controller capacity

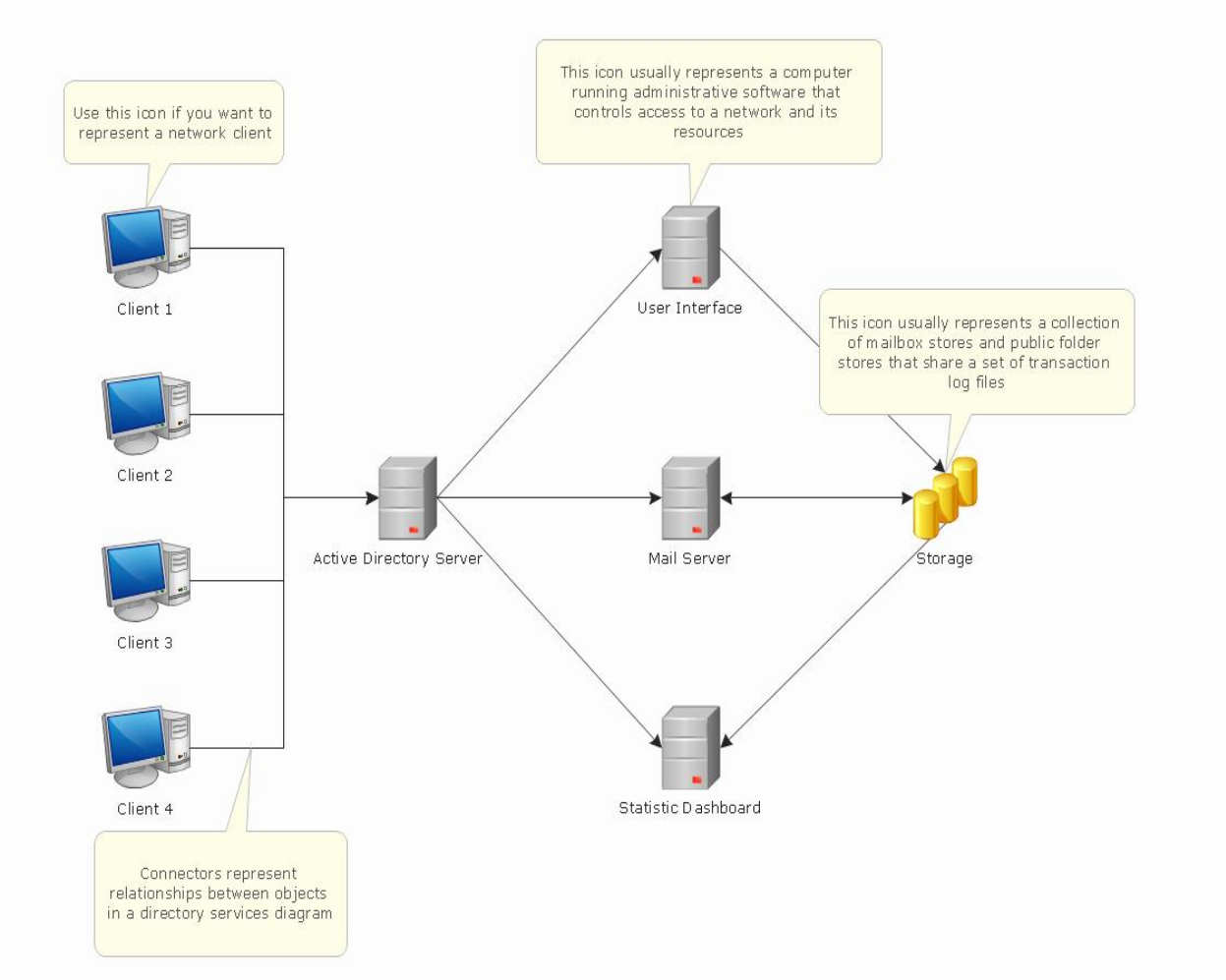
To ensure efficient AD DS performance, you must determine the appropriate number of domain controllers for each site and verify that they meet the hardware requirements for Windows Server 2008. Careful capacity planning for your domain controllers ensures that you do not underestimate hardware



requirements, which can cause poor domain controller performance and application response time. The following illustration shows the process of domain controller capacity planning.	
Enabling Windows Server AD DS features	
Install the required Roles and Features	

SCOPE OF WORK – INSTALLATION / CREATION OF ACTIVE DIRECTORY

- Install Domain Services Roles and Promote the Server to serve as Active Directory Domain Controller
- Install the Domain Naming services
- Configure the Active Directory Services
- Configure the Domain Naming Services
- Organizational Unit's to be created as per the requirement
- User Accounts to be created
- Group to be Created if any
- Configuration of Group policies
- User Account policies to be set as per requirement
- Segregation of Group Policies as per requirement
- Workstations or Client system to be joined domain
- Domain Profiles to be created on each PC
- Profile Data to be Managed if any
- Validating the Site replication if more than one DC
- Validating the DNS Lookup
- Configuring the DC IP address as Primary DNS for all the machines



SCOPE OF WORK – MIGRATION OF ACTIVE DIRECTORY

Migration of AD DS	**Scope of Action**
Backup	Before proceeding with role transfers will take system state backup
Preparation	Prepare all information before proceeding
Installation of services	Install the Windows Server OS and install AD DS services on new Box
Promote to Domain Controller	Now promote the server as additional Domain Controller for the current Domain
Testing	Check for the successful promotion and replication of directory database
Transfer of Roles	Next will step-by-step transfer the FSMO roles hold by old server to new server gracefully

Testing	Now check if the newly promoted FSMO role holder server is promoting itself as FSMO role holder
Assigning as Primary DNS	Now will set newly installed server IP as Primary DNS server for hosts
Removal of old DC	When everything is working as it should will demote the old server and keep it as member server

SCOPE OF WORK – ANNUAL MAINTENANCE OF ACTIVE DIRECTORY

Service Maintenance of AD DS Infrastructure	**Scope of Action**
Backup	To maintain scheduled backup and verification of Server backup as per customer requirement
Group Policy	To manage & configure GP as per customer, monitor if working properly
Performance Monitor	To monitor and troubleshoot performance related issues with AD DS Server
Single sign on setup	To help customer to configure SSO
User Management	To manage & Train customer for user creation, deletion, unlock & other basic daily transactions.
User Rights Management	To manage which user has what rights to access domain resources
Printer Management	To manage & configure the Printers & other network resources which need to be shared as per customer.
File Server	To configure and manage File & Folder sharing permissions.
Scheduled Monitoring	To conduct daily or weekly or monthly monitoring depending on the customer user base
Schedule Auditing	To perform quarterly audit of Security Logs, Performance Log, System Logs, Application Logs

--- End of Document --