OVERVIEW OF TYPICAL WINDOWS SERVER ROLES

Before you start

Objectives: learn about common server roles which can be used in Windows environment.

Prerequisites: no prerequisites.

Key terms: network, server, proxy, services, web, segment, firewall, internet, applications, gateway, router

---

What are Server Roles

Role is a set of features and services that are required to perform a specific function on the server and in that way in our environment. Software components in Windows Server system are separated, and that allows us to install only certain portions of the operating system. Those portions can be grouped into, what we call, roles. Different roles will then have different role services. Role services are specific programs that provide the function of the role. Together with roles we can also use different features of the operating system as an add-on to roles. Feature programs are not directly related to a role. They often add functionality to the whole server. Examples of roles include DNS server, DHCP server, File Server, and Print Server. Some roles, like DNS, have a single role service. Other roles, like Print Server, have multiple role services such as the LPD Service for Unix printing and Internet Printing. Features include management tools, communication protocols or clients, and clustering support.

Network Services

The first role that we will talk about is providing services. In this role our server provides services to clients on the network. These services include Active Directory, File, Print, DNS, DHCP and Web (IIS) services. If we can save a file to a server or if we can send a print job to a server, then that server is running some software that is enabling us to do those actions on the server. The same thing is if we have a web server. We request a web page and the server returns the requested web page. If we use Active Directory services, our computer will act as a Domain Controller (DC). All those scenarios are very common in server environments.

Active Directory (AD) is a database that stores information about network users, computers and printers. It helps administrators to mange all those resources, and it is required for Exchange Server implementation and Domain Group Policy. We should differentiate Active Directory Domain Services (ADDS) and Active Directory Certificate Services (ADCS). We can use ADCS to create manage public key certificates. Administrators can use ADCS to bind the identity of a person, device or service to a specific private key.

DNS is used to map IP addresses to logical names. With Server 2008 we also have support for IPv6 addresses. DHCP (Dynamic Host Configuration Protocol) service can be used to provide IP configuration information for hosts on our network including local IP address, default gateway, DNS server, etc. Print services allows us to manage printers on servers and to publish printers in Active Directory.

With File Services we can manage network file sharing. We can use Distributed File Service to store copies of shared folders on multiple servers. We can also manage quotas for users by using File Server Resource Manager (FSRM). We can also provide access to files by using NFS protocol which is often used on Linux machines.

Starting from Windows Server 2008 version, we also have Windows SharePoint services, Network Access Protection, improved Terminal Services, and Windows Deployment Services (WDS). Windows Sharepoint provides collaboration tools. Network Access Protection can be used to restrict access on our network for certain computers which are not compliant with our security policies. Terminal Services can be used to access server desktop over network or to run applications on terminal server. Windows Deployment Service can be used to deploy and install various Windows operating systems over network.

Active Directory (AD) Server Roles

There are several commonly used Active Driectory Server Roles:

- Active Directory Domain Services (AD DS) - AD DS is a distributed database that stores and manages information about network resources, such as users, computers, and printers. This helps administrators to securely manage information, resource sharing and collaboration between users.
- Active Directory Lightweight Directory Service (AD LDS) - AD LDS, formerly known as Active Directory Application Mode (ADAM), is an LDAP directory service that can be used to create a directory store (database) for use by directory-enabled applications. It is similar to Active Directory Domain Services (AD DS), but is customizable and can be much smaller than an AD DS database.
- Active Directory Federation Services (AD FS) - AD FS is a feature which enables secure access to web applications outside of a user's home domain or forest. It provides Web Single-Sign-On (SSO) technologies to authenticate a user to multiple Web applications using a single user account. It securely federates (shares) user identities and access rights in the form of digital claims between partner organizations.

- Active Directory Rights Management Service (AD RMS) - AD RMS is a feature which safeguards digital information from unauthorized use. It can define exactly how a recipient can use information, specifying who can open, modify, print, forward, and/or take other actions. It allows organizations to create custom usage rights templates (such as "Confidential - Read Only") that can be applied directly to information such as financial reports, e-mail messages, etc.
- Active Directory Certificate Services (AD CS) - AD CS is an identity and access control feature that creates and manages public key certificates used in software security systems. It provides customizable services for creating and managing public key certificates, and enhances security by binding the identity of a person, device, or service to a corresponding private key. It includes features that allow us to manage certificate enrollment and revocation in a variety of scalable environments. AD CS supports digital signatures, encrypting File System (EFS), Internet Protocol security (IPsec), Secure/Multipurpose Internet Mail Extensions (S/MIME), Secure Socket Layer/Transport Layer Security (SSL/TLS), Secure wireless networks, Smart card logon, and Virtual Private Networks (VPN).

Not all roles are supported on all versions of Windows Server OS. For example, when it comes to Windows Server 2008, AD FS is only supported in DataCenter or Enterprise editions of Windows Server 2008.

Applications Server

When the server is configured as application server, the server will provide certain network applications that can be accessed by users. For example, the server can have a database software installed that the users on the network can use to store or query data. When we talk about the client/server model, database servers can be programs that provide database services or they can be computers that are dedicated to running database programs.

Another example of applications on our server would be web-based applications. Web applications are not static web pages. Web application can be any web site that provides dynamic data or services to users. For example, web applications are web calendars, online spreadsheets, chat rooms, online CRM software, etc. There are different technologies which can be used to write web applications, but some of the most popular ones are PHP and ASP.NET.

Roles that we mentioned up to now are designed to provide services to users. However, there other roles which are related to network infrastructure. Those roles are the Gateway or Router, Bridge, Firewall or Proxy.

Gateway or Router

Technically, gateway and router are two different things. However, often the Gateway and Router are sometimes used interchangeably. That's because we often implement a Gateway when we implement a Router and vice versa. Gateways and Routers are similar in that they connect two distinct logical networks. To set the server to function as Gateway or Router, the server has to have two (or more) network interfaces installed. One network interface is connected to one network segment and the second interface is connected to another network segment. This alone will not make our server to route packets between those two network segments. We also have to have routing software installed. Operating systems like Windows, Linux and NetWare have this software. Hosts on different network segments will have different logical addresses (IPs) assigned. Our server (now router) will use IP addresses to route packets from one segment to another. If host on one network segment needs to send some data to a host on another network segment, it will first send data to a Default gateway. Default gateway will know on which network segment the destination host resides, so it will route data to that network segment. We can actually configure multiple routers to cover many different networks. That's how the Internet actually works.

Bridge

This role is not used often any more, but it was common in the old days. As we said, with Router we connect two different logical network segments. Now, with Bridge we connect to different physical network segments. With Bridge, those two physical networks are still one logical network segment. Bridge uses MAC (physical) addresses to isolate traffic from one physical network segment from another. So, the Bridge memorizes which host is on which physical network segment using the Mac address.

Firewall

Firewall role is often implemented on servers. The Firewall separates our internal computer network from the public network, which is usually the Internet. We want to allow some traffic from the Internet, but we also want to block some traffic from the Internet. Most operating systems have firewall software in them, like Linux and Windows. By using Firewall we can configure set of rules in which we define what and which type of network traffic is allowed to enter (or exit) our private network and which is not allowed. So, we can configure inbound and outbound rules. All traffic going between our local network inside and the public network outside has to go through the Firewall. The Firewall analyzes all that trafficking and based on the defined rules, decides to allow or deny specific traffic.

Proxy

Most operating systems also have a proxy feature which can be enabled. With proxy server we separate and hide our private network from the Internet, and we also have a degree of control which resources on the Internet are being accessed. A server running as a firewall can also run as a proxy or a separate proxy server can be set up. All hosts on the network are connected to our proxy server. If some host on our private network wants to go the Internet, it has to go trough our proxy server. The proxy server takes a look at all requests

and decides to allow or deny the request based on the configured rules. If the request is allowed, the servers send it out on the Internet and retrieve the resource requested (or its gets it from its cache). Then it forwards the results back to the original workstation. When we use a proxy server the address of the proxy server is the only address available to the public network.

Common Features

As we mentioned earlier, we can also use many features to improve services on our server machine. For example, we can use BitLocker. We can also set up Remote Assistance service, SMTP, Telnet server or Telnet client feature. We also have Failover Clustering, Network Load Balancing (NLB), WINS, Windows Backup and Powershell, Windows Backup and Powershell.

BitLocker is used to encrypt the entire hard disk on the server and in that way protect data on it. Remote Assistance is used to offer assistance to users on their computers and to correct problems over network. Simple Mail Transfer Protocol (SMTP) is used to transfer e-mail between systems and clients. For example, we can add SMTP feature to add e-mail support to IIS. With Telnet feature we can use a command line to manage remote servers. Telnet Server allows us to accept incoming connections, while Telnet Client allows us to initiate connections. Failover Clustering is used to increase the fault tolerance of network servers by sharing storage resources. In that way if one server fails, the available server will respond to the requests. Network Load Balancing feature is used to disperse workload between multiple servers to optimize performance and response time. This also provides fault tolerance. WINS server is used to map NetBIOS names and IP addresses. WINS database is used to resolve NetBIOS names. It is only used if we need to support legacy clients which can't use DNS for name resolution (DNS replaced WINS). Windows Server Backup can be used to backup and recover content from Windows Server machine.

Powershell is a command line scripting program which can be used to manage Windows Server.

Server 2003 vs Server 2008

To manage all those roles and features, in Windows Server 2003 OS we often used Computer Management MMC console. In Server 2008 we don't have Computer Management, and in place of that we have a new MMC console called Server Manager. Server Manager console allows us to add or remove roles, customize roles and work with additional features. Installation of roles in Server 2003 was similar to using Add/Remove Windows Components in Control Panel. In Windows Server 2008 the only way to add roles is trough Server Manager console.

Server Core Editions

Server core is a minimal server installation option available on Windows Server 2008 and newer Windows Server versions. It has limited GUI support, so most tasks are performed from a command prompt. The thing is, server core will only be able to run limited set of server roles, so be sure to check the documentation for the Windows Server version you are using or run **oclist** to see a list of roles, role services, and features that can be installed on server core. Run **start /w ocsetup** to add server roles to the server core system. Switches for the role or service must be typed exactly as they are listed, and role names are case-sensitive.

Source : http://www.utilizewindows.com/server/basics/354-overview-of-typical-windows-server-roles