



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCC5003 Network Operating Systems and Security

Alexandru Balasa

1814696

Lecture:

Terry Walcott

**Assignment 1: Administering the Network Infrastructures by
Using the services of Core Intrinsic Network**

Table of Contents

Work sheet 1: The Use of the Active Directory for the Building of NOS infrastructure	3
Work sheet 2: Resource Management in Active Directory: Users, Groups, and Computers..	10
Work sheet 3: Resource Management in case of Active Directory: Management of the access to folder as well as files and controlling the domain of the environment of the user.	14
Work sheet 4: Deployment and Planning of the DNS in the network infrastructure.	15
Work sheet 5: Network Administration with the usage of DHCP.....	17

Work sheet 1: The Use of the Active Directory for the Building of NOS infrastructure

Producing Active Directory forest and domain styles, we need to style a website Name System infrastructure (DNS) to assist the Active Directory logical structure. DNS permits users to use amicable names that square measure straightforward to recollect to attach to computers and different resources on the IP networks.

The process for planning DNS to assist AD DS varies in keeping with whether or not your organization has an associated current DNS Server service already, otherwise you square measure deploying a brand-new DNS Server service:

If DNS infrastructure is already there then, just by integrating the Active Directory namespace into that setting by using AD DS into associate Existing DNS Infrastructure setup can be done.

If DNS infrastructure in situ is done, you want to style and post a brand-new DNS infrastructure to assist AD DS. the method is termed Deploying name System (DNS).

So, before DNS infrastructure to assist AD DS, it will be useful to examine the DNS hierarchy, the DNS name resolution method, and the way DNS assist AD DS.

Reviewing DNS Concepts

Applies To: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

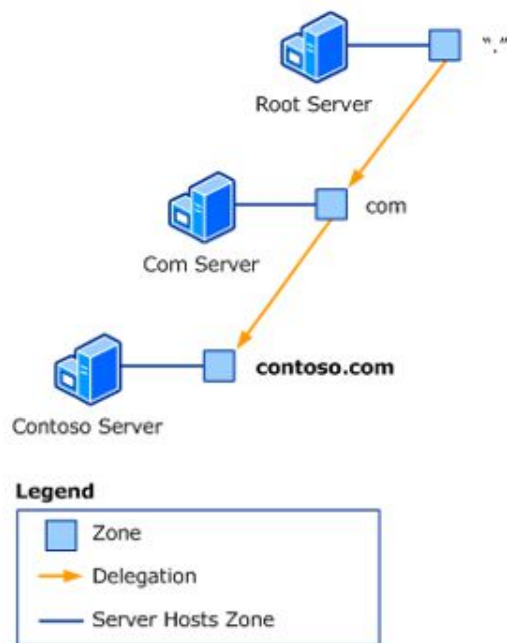
Domain Name System (DNS) is a distributed database that represents a namespace. The namespace contains all of the information needed for any client to look up any name. Any DNS server can answer queries about any name within its namespace. A DNS server answers query in one of the following ways:

- If the answer is in its cache, it answers the query from the cache.
- If the answer is in a zone hosted by the DNS server, it answers the query from its zone. A zone is a portion of the DNS tree stored on a DNS server. When a DNS server hosts a zone, it is authoritative for the names in that zone (that is, the DNS server can answer queries for any name in the zone). For example, a server hosting the zone contoso.com can answer queries for any name in contoso.com.
- If the server cannot answer the query from its cache or zones, it queries other servers for the answer.

It is important to understand the core features of DNS, such as delegation, recursive name resolution, and Active Directory-integrated DNS zones because they have a direct impact on your Active Directory logical structure design.

Delegation

For a DNS server to answer queries about any name, it must have a direct or indirect path to every zone in the namespace. These paths are created through delegation. A delegation is a record in a parent zone that lists a name server that is authoritative for the zone in the next level of the hierarchy. Delegations make it possible for servers in one zone to refer clients to servers in other zones. The following illustration shows one example of delegation.



The DNS root server hosts the root zone represented as a dot (.). The root zone contains a delegation to a zone in the next level of the hierarchy, the com zone. The delegation in the root zone tells the DNS root server that, to find the com zone, it must contact the Com server. Likewise, the delegation in the com zone tells the Com server that, to find the contoso.com zone, it must contact the Contoso server.

Note

A delegation uses two types of records. The name server (NS) resource record provides the name of an authoritative server. Host (A) and host (AAAA) resource records provide IP version 4 (IPv4) and IP version 6 (IPv6) addresses of an authoritative server.

This system of zones and delegations creates a hierarchical tree that represents the DNS namespace. Each zone represents a layer in the hierarchy, and each delegation represents a branch of the tree.

By using the hierarchy of zones and delegations, a DNS root server can find any name in the DNS namespace. The root zone includes delegations that lead directly or indirectly to all other zones in the hierarchy. Any server that can query the DNS root server can use the information in the delegations to find any name in the namespace.

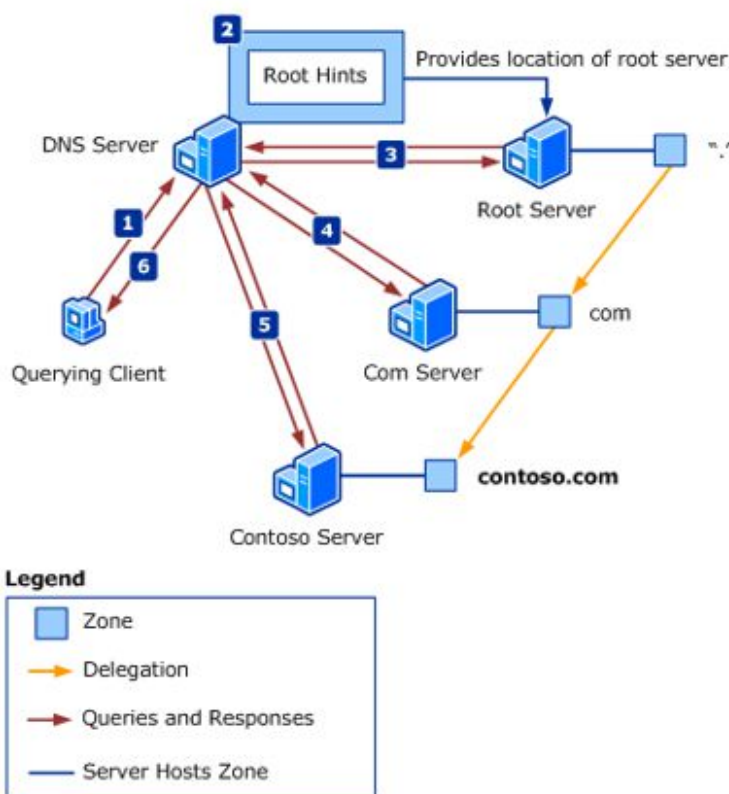
Recursive name resolution

Recursive name resolution is the process by which a DNS server uses the hierarchy of zones and delegations to respond to queries for which it is not authoritative.

In some configurations, DNS servers include root hints (that is, a list of names and IP addresses) that enable them to query the DNS root servers. In other configurations, servers forward all queries that they cannot answer to another server. Forwarding and root hints are both methods that DNS servers can use to resolve queries for which they are not authoritative.

Resolving names by using root hints

Root hints enable any DNS server to locate the DNS root servers. After a DNS server locates the DNS root server, it can resolve any query for that namespace. The following illustration describes how DNS resolves a name by using root hints.

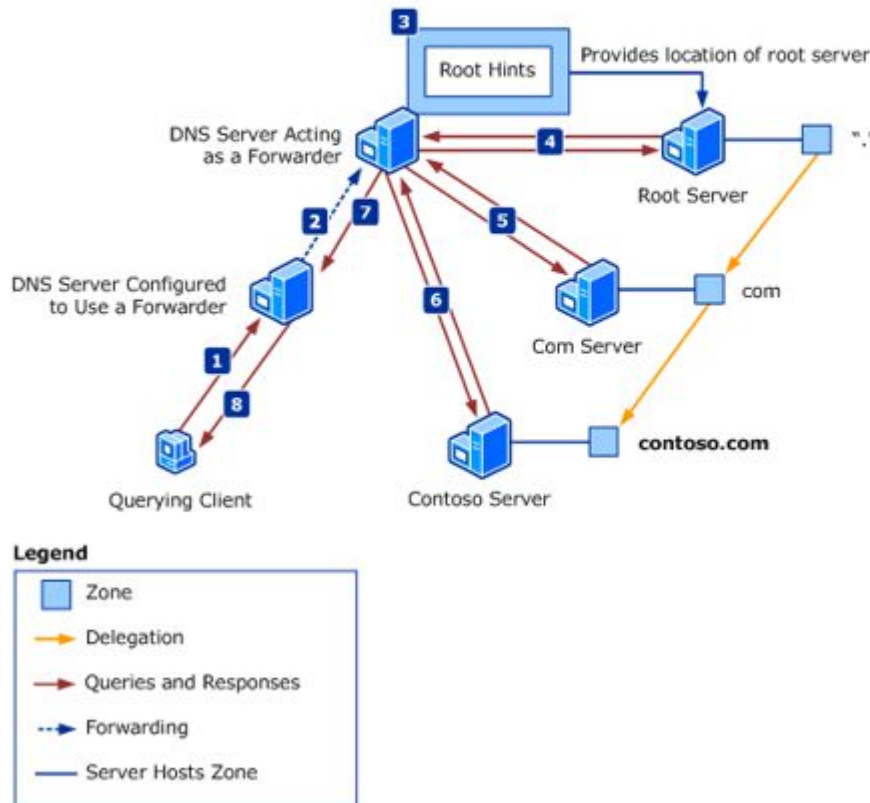


In this example, the following events occur:

1. A client sends a recursive query to a DNS server to request the IP address that corresponds to the name ftp.contoso.com. A recursive query indicates that the client wants a definitive answer to its query. The response to the recursive query must be a valid address or a message indicating that the address cannot be found.
2. Because the DNS server is not authoritative for the name and does not have the answer in its cache, the DNS server uses root hints to find the IP address of the DNS root server.
3. The DNS server uses an iterative query to ask the DNS root server to resolve the name ftp.contoso.com. An iterative query indicates that the server will accept a referral to another server in place of a definitive answer to the query. Because the name ftp.contoso.com ends with the label com, the DNS root server returns a referral to the Com server that hosts the com zone.
4. The DNS server uses an iterative query to ask the Com server to resolve the name ftp.contoso.com. Because the name ftp.contoso.com ends with the name contoso.com, the Com server returns a referral to the Contoso server that hosts the contoso.com zone.
5. The DNS server uses an iterative query to ask the Contoso server to resolve the name ftp.contoso.com. The Contoso server finds the answer in its zone data and then returns the answer to the server.
6. The server then returns the result to the client.

Resolving names by using the forwarding

Forwarding enables you to route name resolution through specific servers instead of using root hints. The following illustration describes how DNS resolves a name by using forwarding.



In this example, the following events occur:

1. A client queries a DNS server for the name ftp.contoso.com.
2. The DNS server forwards the query to another DNS server, known as a forwarder.
3. Because the forwarder is not authoritative for the name and does not have the answer in its cache, it uses root hints to find the IP address of the DNS root server.
4. The forwarder uses an iterative query to ask the DNS root server to resolve the name ftp.contoso.com. Because the name ftp.contoso.com ends with the name com, the DNS root server returns a referral to the Com server that hosts the com zone.
5. The forwarder uses an iterative query to ask the Com server to resolve the name ftp.contoso.com. Because the name ftp.contoso.com ends with the name contoso.com, the Com server returns a referral to the Contoso server that hosts the contoso.com zone.
6. The forwarder uses an iterative query to ask the Contoso server to resolve the name ftp.contoso.com. The Contoso server finds the answer in its zone files and then returns the answer to the server.
7. The forwarder then returns the result to the original DNS server.
8. The original DNS server then returns the result to the client.

Work sheet 2: Resource Management in Active Directory: Users, Groups, and Computers

This segment covers the subsequent Microsoft-specified target for the "Managing Users, Computers, and Groups" portion of the Managing and keeping a MS Windows Server. Develop and manage the accounts of the user.

A most important duty of a network administrator is to make and manage the accounts of user, simply due to the fact that the accounts of the users are required for them to verify the network and to see what inputs the user can get. For a little network, developing and changing the accounts of the user one by one with the help of a management tool isn't too much time taking. However, on a network with many users, it is smart to utilize the tools that automate the method. If the info in relation to the users is there in another form, like a new-hire database, you'll develop the accounts of the user by bringing them from an appropriate file. New tools of command line and directory management like dsquery, dsmod, dsadd, and dsget. So, be confirmed that you recognize what everything is for still as a way to use it. Also, take care to grasp directing the output from a command because of the input to a different. Understand what is the relevance of them, and find to get the command structure.

This segment covers making and managing accounts of the user, cluster accounts, as well as laptop accounts, and fixing the roaming profiles. A massive part of the task could be Trouble shooting. It entails serving the users and perceiving why they are unable to connect with the network—whether it's attributable to locked-out accounts of the user, defunct laptop accounts, or alternative reasons.

Active Directory Users and Computers (ADUC) is a Microsoft Management Console snap-in that you use to administer Active Directory (AD). You can manage objects (users, computers), Organizational Units (OU), and attributes of each.

ADUC is one of the many tools that you can use to administer AD, but since it has been around since Windows 2000, it is one of the most popular. Read on to see how to run and use ADUC to manage AD.

How to Add Active Directory Users and Computers?

Some of you might have already looked for ADUC on your laptop to discover that it's not there. It's not part of the default installation, and how you get it installed depends on your version of Windows.

In current versions of Windows, ADUC is part of an administrative suite of tools called Remote Server Administration Tools (RSAT).

Remote Server Administration Tools (RSAT)

In an October 2018 update, Microsoft moved all of the Active Directory administration tools to a 'feature on-demand' called RSAT. Attackers use whatever they can for privilege escalations and exfiltration. They don't need RSAT to do major damage to your network, but it sure makes it easier! If an attacker got hold of a computer with ADUC installed, they could just change passwords and access rights at will. That would be very bad.

Anyway, if you want to access ADUC on your computer, you need to install RSAT. ADUC is not part of the default installation for any Windows version. Follow the instructions below to install:

Installing ADUC for Windows 10 Version 1809 and Above

1. From the Start menu, select *Settings > Apps*.
2. Click the hyperlink on the right side labeled *Manage Optional Features* and then click the button to *Add feature*.
3. Select *RSAT: Active Directory Domain Services and Lightweight Directory Tools*.
4. Click *Install*.
5. When the installation completes, you will have a new menu item in the start menu called *Windows Administrative Tools*.

Installing ADUC for Windows 8 and Windows 10 Version 1803 and Below

- Download and install *Remote Server Administrator Tools* depending on your version of Windows. The link is for Windows 10, other versions are available in the Microsoft Download Center.
- Click the Start button and select *Control Panel > Programs > Programs and Features > Turn Windows features on or off*.
- Scroll down the list and expand *Remote Server Administration Tools*.
- Expand *Role Administration Tools*.
- Expand *AD DS and AD LDS Tools*.
- Check *AD DS Tools*, then select "OK."
- When the install completes you will have a folder for *Administrative Tools* on the Start menu. ADUC should be on this list.

Troubleshooting RSAT Installation

There are two common installation issues to check if something goes sideways and you can't get RSAT installed. First, check that you have enabled Windows Firewall. RSAT uses the Windows Update backend and thus needs Windows Firewall enabled.

Sometimes after the install, you might be missing tabs and such. Uninstall and reinstall. You might have had an older version and the update didn't work 100%. You can also right click on ADUC in the Start menu and verify the shortcut is pointing to %SystemRoot%\system32\dsa.msc. If it doesn't point there then you need to uninstall and reinstall for sure.

- **Active Directory Administrative Center:** Allows management for the AD Trash Can (accidental deletes), password policies, and displays the PowerShell history.
- **Active Directory Domains and Trusts:** Lets you administer multiple domains to manage functional level, manage forest functional level, manage User Principle Names (UPN), and manage trusts between domains and forests.
- **Active Directory Module for Windows PowerShell:** Enables the PowerShell cmdlets to administer AD.
- **Active Directory Sites and Services:** Allows you to view and manage Sites and Services. You can define the topology of AD and schedule replication.
- **ADSI Edit:** ADSI Edit is a low-end tool to manage AD objects. AD experts don't recommend that you use ADSI Edit, use ADUC instead.

ADUC for Delegating Control

Scenario: You are looking to limit the sysadmin team's responsibility to manage specific domains in your network. You would like to assign two sysadmins per domain, a primary and a backup. Here is how you would do this:

1. Open ADUC as Admin.
2. Right click the domain and select Delegate Control.

Work sheet 3: Resource Management in case of Active Directory: Management of the access to folder as well as files and controlling the domain of the environment of the user.

Resource record management summary

By deploying IPAM in the Windows Server 2016, you may do server discovery to feature DNS and DHCP servers to the console of IPAM server management. The IPAM server then actively musters the DNS knowledge after each six hours from the DNS servers that it's designed to control. IPAM is responsible for maintaining section info wherever it keeps this DNS knowledge. IPAM also provides a notification of the day and time to the user that the server knowledge was collected, it's going to tell the following day and time once knowledge assortment from DNS servers will occur.

The knowledge of DNS that is mustered includes the DNS zone along with the resource record info. you will be ready to put together IPAM to assemble zone info from your most popular DNS server. IPAM musters all the file-based as well as the Active Directory zones. IPAM mechanically logs all DNS configuration changes that you {simply that you just} simply build exploitation of the IPAM console.

To add a DNS resource record

1. In Server Manager, click **IPAM**. The IPAM client console appears.
2. In the navigation pane, in **MONITOR AND MANAGE**, click **DNS Zones**. The navigation pane divides into an upper navigation pane and a lower navigation pane.
3. In the lower navigation pane, click **Forward Lookup**. All IPAM-managed DNS Forward Lookup zones are displayed in the display pane search results. Right-click the zone where you want to add a resource record, and then click **Add DNS resource record**.

Work sheet 4: Deployment and Planning of the DNS in the network infrastructure.

If a company has an associate degree already in the existing name System i.e., the (DNS) Server service, the DNS for the (AD DS) i.e., Active Directory Domain Services owner should work with the owner of the DNS for a company to combine AD DS into the present infrastructure.

Making a configuration of DNS server

When desegregating AD DS with associate degree existing DNS namespace, steps have to be compelled to be followed:

Install the DNS Server service on each domain controller within the forest. This gives tolerance of the fault if one in every of the DNS servers is inaccessible. during this method, domain controllers don't have to be compelled to place confidence in different DNS servers for name resolution. This additionally makes the management atmosphere easy as a result of all domain controllers have the same configuration.

A pc may need a unique DNS name, already existing, if the organization antecedently, statically registered the pc in DNS or in other cases if the organization antecedently deployed associate degree combined Dynamic Host Configuration Protocol (DHCP) resolution. consumer computers had a registered DNS name, once the domain to that they're joined is upgraded to the Windows Server 2008 (the AD DS), they'll have 2 different names:

- The already existing DNS names
- The latest qualified name (FQDN)

Clients will remain to be the beset by either name. Any existing DNS, or the existing DHCP, or even the combined DNS/DHCP resolution is left intact. The new major names are developed mechanically and up dated through active updates. they're clean up mechanically using scavenging.

Creating the DNS client configuration

To configure DNS on client computers, the DNS for AD DS owner must specify the computer naming scheme and how the clients will locate DNS servers. The following table lists our recommended configurations for these design elements.

Design element	Configuration
Computer naming	Use default naming. When a Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008 , or Windows Vista-based computer joins a domain, the computer assigns itself a fully qualified domain name (FQDN) that comprises the host name of the computer and the name of the Active Directory domain.
Client resolver configuration	Configure client computers to point to any DNS server on the network.

Work sheet 5: Network Administration with the usage of DHCP

Work sheet 5: Network Administration mistreatment DHCP Dynamic Host Configuration Protocol (DHCP) mechanically configures the IP address for all host on a network, therefore reassuring that every host encompasses a sound, distinctive IP address. DHCP even mechanically reconfigures IP addresses just as the hosts arrives back and go. Just as you may think, DHCP will protect a network administrator several hours of tiring configuration work. Though the main work of DHCP is to distributed IP addresses and subnet masks, DHCP provides a lot of configuration info than merely the IP address to its purchasers. The following can be a listing of some familiar DHCP choices which could be designed by the server:

- The router address, additionally observed because the Default entree address
- The hour for the expiry of the configuration info name
- Name Server (DNS) server address
- Windows net Name Service i.e, the WINS server address

DHCP servers

A DHCP server could also be a server laptop settled on the TCP/IP network. All trendy server operative systems have an integral DHCP server. to line up DHCP on a network server, all you have to undertake and do is modify the server's DHCP to operate and set up its settings. A server laptop running DHCP shouldn't be devoted entirely to DHCP unless the network is extraordinarily giant. for several networks, an electronic computer will share duty as a DHCP server. This will be a reality if you give big leases for your IP addresses. A lot of multi functioning routers even have integral DHCP servers. To decrease the burden on network servers with the DHCP operate, modify the router's integral DHCP server. An advantage of permitting the router to be your network's DHCP server is just simply seldom have to be compelled to power down a router. In distinction, you sometimes have to be compelled to start again or power down an electronic computer to do maintenance of the system, apply up grades, or do trouble shooting. If you erroneously based 2 DHCP servers for the identical scope, you will be left with the twin address assignments if the servers tries to give the identical IP address to the hosts which are different.