Microsoft Active Directory—Best Practice

Posted on May 28, 2011

In this article, I am writing an overview of Microsoft Active Directory. You might be thinking; well you know everything on Active Directory. I would recommend you to go through this article and revisit your own Active Directory infrastructure. You will improve Active Directory performance, enhance Active Directory infrastructure and rectify so many misconfiguration you have made over the years.

Lets start with basic question, What is Microsoft Active Directory? Active Directory is Microsoft's adoption of IEEE X.500. you can use Active Directory Domain Services (AD DS) as the central repository or database for user, group, and computer accounts as well as for application, shared folders and printers. With the adoption of Active Directory on Windows server 2000, Microsoft enhanced Active Directory on Windows Server 2003 and Windows Server 2008. Having the ability to manage these resources from any domain controller within your domain allows you to greatly reduce your administrative overhead.

Active Directory creates a secure boundary for an organization providing log on authentication. Active Directory creates a hierarchical containment structure includes the Active Directory forest, domains in the forest, DNS and organizational units (OUs) in each domain. Feature of Active Directory includes:

- A set of rules that is the schema, that defines the classes of objects and attributes
- A global catalog that contains information about every object in the directory.
- A query and index mechanism, so that objects and their properties can be published and found by network users or applications.
- A replication service that distributes directory data across a network and all domain controllers (writable and RODC)
- Operations master roles (flexible single master operations or FSMO roles).

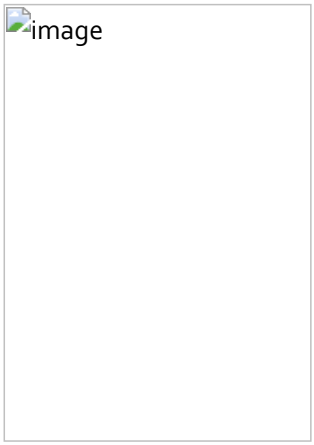
What's new in Windows Server 2008 R2 Active Directory? I reckon, since the adoption of Microsoft Active Directory in Windows Server 2000, the Active Directory has become the fundamental pillar of windows network infrastructure. AD has

grown and become a mature technology on windows server 2008 R2 release. There are new features in Windows Server 20008 R2. They are as follows

- Active Directory Application Mode (ADAM).
  Active Directory Federation Services (AD FS)
- Active Directory Rights Management Services (AD RMS)
- Active Directory Certificate Services (AD CS)
- Read -only domain controllers (RODCs)
- Active Directory on Windows Server Core installation

Active Directory has been partitioned in four important parts. Domain controllers in Active Directory typically contain the following directory partition replicas or naming context replicas:

- Configuration: The configuration partition or naming context (NC) contains objects that relate to the logical structure of the forest, structure of the domain, and replication topology. Each domain controller in the forest contains a read/write copy of the configuration partition. Any objects stored in the configuration partition are replicated to each domain controller in each domain, and in a forest.
- Domain: The domain partition or naming context (NC) contains all objects that are stored in a domain. Each domain controller in a domain has a read/write copy of the domain partition. Objects in the domain partition are replicated to only the domain controllers within a domain.
- Schema: The schema partition or naming context (NC) contains objects that can be created in the Active Directory directory, and the attributes which these objects can contain. Domain controllers in a forest have a read-only copy of the schema partition. Objects stored in the schema partition are replicated to each domain controller in domains/forests.
- Application: The application partition is a new feature introduced in Windows Server 2003. This partition contains application specific objects. The objects or data that applications and services store here can comprise of any object type excluding security principles. Security principles are Users, Groups, and Computers. The application partition typically contains DNS zone objects, and dynamic data from other network services such as Remote Access Service (RAS), and Dynamic Host Configuration Protocol (DHCP).



Flexible Single Master Operations (FSMO): The Active Directory extends the single-master model found in earlier versions of Windows to include multiple roles, and the ability to transfer roles to any domain controller (DC) in the enterprise. Because an Active Directory role is not bound to a single DC, it is referred to as a Flexible Single Master Operation (FSMO) role. Currently in Active Directory there are five FSMO roles:

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

Active Directory ISTG: For inter-site replication, one domain controller per site has the responsibility of evaluating the inter-site replication topology and creating Active Directory Replication Connection objects for appropriate bridgehead servers within its site. The domain controller in each site that owns this role is referred to as the Inter-Site Topology Generator (ISTG). Inter-site connection objects are created by the Inter Site Topology Generator (ISTG) and not the KCC. The first domain controller in a site has the role of Inter Site Topology Generator. There is only one ISTG within a particular site. It is the ISTG that is responsible for ensuring that the site has a replica of the configuration, domain and schema partitions.

KCC Replication: The Knowledge Consistency Checker (KCC) is an Active Directory component that is responsible for the generation of the replication topology between domain controllers. This article describes the role of one server per site, known as the Inter-Site Topology Generator, which is responsible for managing the inbound replication connection objects for all bridgehead servers in the site in which it is located.

The current ISTG notifies every other domain controller in the site that it is still present by writing the "inter-Site Topology Generator" attribute on "CN=NTDS Site Settings,CN=SiteName,CN=Sites,CN=Configuration,DC=Mydomain,DC=com" under its domain controller object in the Configuration naming context in Active Directory at a specified interval. You can modify this interval using the following registry value (which is not present by default, it must be added):

Key: HKEY_LOCAL_MACHINESystemCurrentControlSetServicesNTDSParameters
Value Name: KCC site generator renewal interval (minutes)
Value Data: 30 (in minutes)

As this attribute gets propagated to other domain controllers by Active Directory replication, the KCC on each of these computers monitors this attribute to verify that it has been written within a specified amount of time. If the amount of time elapses without a modification, a new ISTG takes over. You can modify this time interval using the following registry value:

Key: HKEY_LOCAL_MACHINESystemCurrentControlSetServicesNTDSParameters
Value Name: KCC site generator fail-over (minutes)
Value Data: 60 (in minutes)

Active Directory Replication Topology Options: Active Directory Sites and Services are the logical presentation of physical WAN connectivity and switching of your LAN and WAN. The Active Directory replication topologies typically are:

- Ring Topology: With intra-site replication, the KCC creates a ring topology that defines the replication paths within a site. In a ring topology, each domain controller in a site has two inbound and outbound replication partners. The KCC creates the ring so that there is no greater than three hops between domain controllers in a site.
- Full Mesh Topology: This topology is typically utilized in an organizations where redundancy is extremely important for all sites. You can configure full mesh if you have IPWAN or MPLS connections in all sites. A mix of MPLS and ADSL or other method of connectivity do not constitute full mesh. A full mesh topology is quite expensive to manage and is not

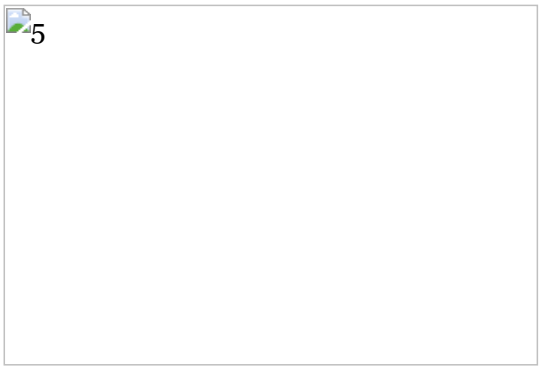
scalable.

- Hub And Spoke Topology: This topology is typically implemented in large organizations where scalability is important consideration. In this topology, one or multiple hub sites exist that have WAN connections to multiple spoke sites. The hub sites are usually connected to each other through high speed WAN connections.
- Hybrid Topology: The hybrid topology is combination of any of the above topologies. This is not a recommended topology even if you have high speed duct fibre or other WAN connectivity.

You can download Microsoft Active Directory Topology Diagrammer and find out your topology you have configured in Active Directory. I would recommend you not to configure configure full mesh topology in Active Directory. Mesh topology often lead you to a mess in active directory. It better to be simple as Hub and Spoke topology.

FRS and DFS replication: Windows Active Directory domain controllers use FRS to replicate system policy and login scripts for Windows servers and clients. However, because system policy and login script replication is performed by Active Directory replication, it is not affected by the following information. However, you can use DFS to replicate across domain controllers.

Domain and Forest Functional Level: Domain and forest functionality, which is available in Windows Server 2008 R2 AD DS, provides a way to enable domain-wide features or forest-wide Active Directory features in your network environment. Different levels of domain functionality and forest functionality are available, depending on your network environment. To check your domain functional, open dsa.msc>Right click on Domain Name>Click Raise Domain Functional Level>Select preferred functional level and click ok.

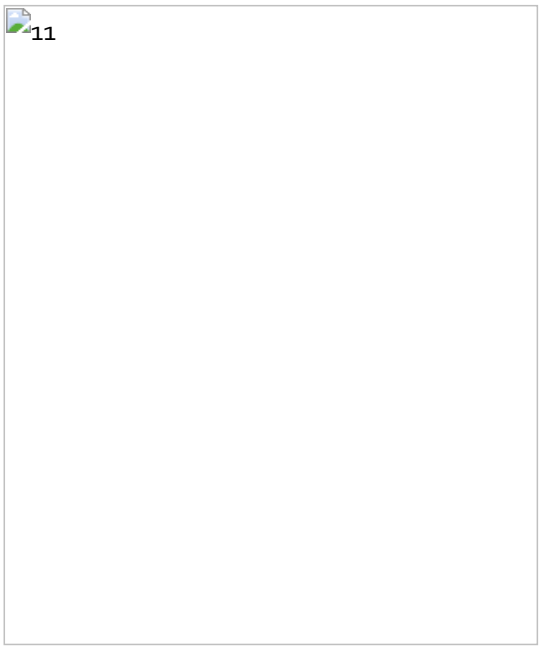


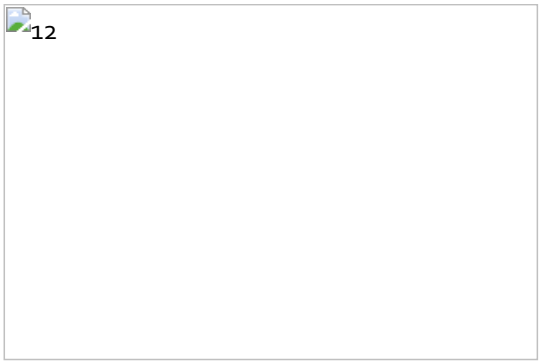
If all the domain controllers in your domain or forest are running Windows Server 2008 R2 and the domain and forest functional level is set to Windows Server 2008 R2, all domain-wide features and forest-wide features are available. When your domain or forest contains Windows 2000, Windows Server 2003 or Windows Server 2008 domain controllers, Active Directory features are limited. For more information about how to enable domain-wide features or forest-wide features,

Understanding Active Directory Domain Services (AD DS) Functional Levels and Raise the Domain Functional Level

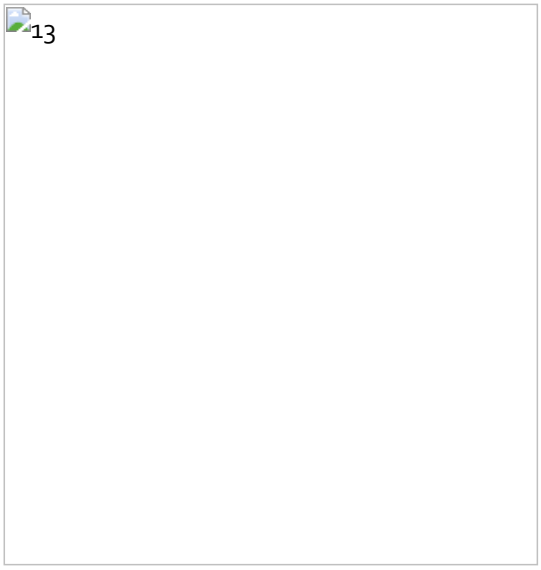
Domain Naming System (DNS): The Domain Name System (DNS) is a hierarchical, distributed database that contains mappings of DNS domain names to various types of data, such as Internet Protocol (IP) addresses. DNS allows you to use friendly names, such as http://www.microsoft.com, to easily locate computers and other resources on a TCP/IP-based network. When planning a secure DNS server deployment, first collect information about your environment. This information should include the structure and hierarchy of your internal and external domains, identification of DNS servers that will be authoritative for these domain names, and the DNS client requirements for host resolution on your network. After you collect this information, review the guidance in this topic to determine which tasks to perform so that you can deploy a secure DNS infrastructure.

To check DNS functional level, open DNS Manger>Expand Forward lookup zone>right click on domain name>Click property>Click Change on Replication: All DNS servers in this forest>Select to all DNS servers running in the domain controllers in this forest. Click OK.

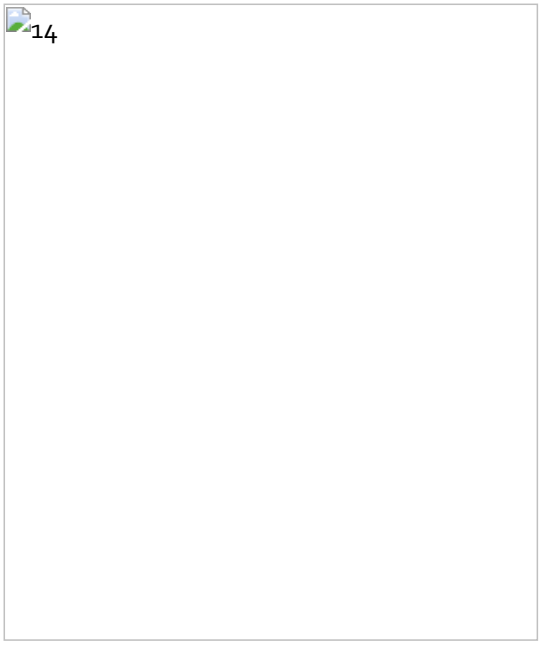


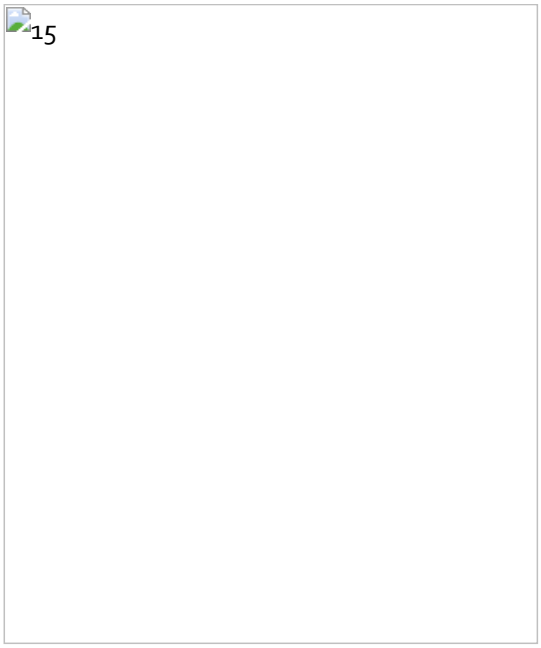


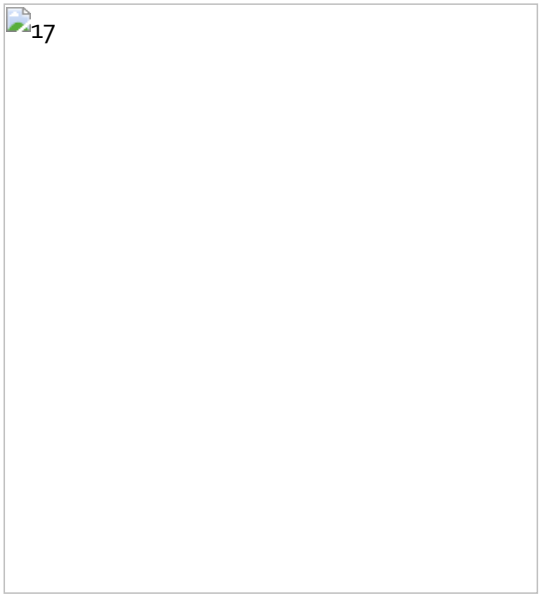
Select appropriate scavenging time to scavenge DNS records.



If you have more than one domain controllers, all domain controllers must be registered as authoritative Name Server (NS)





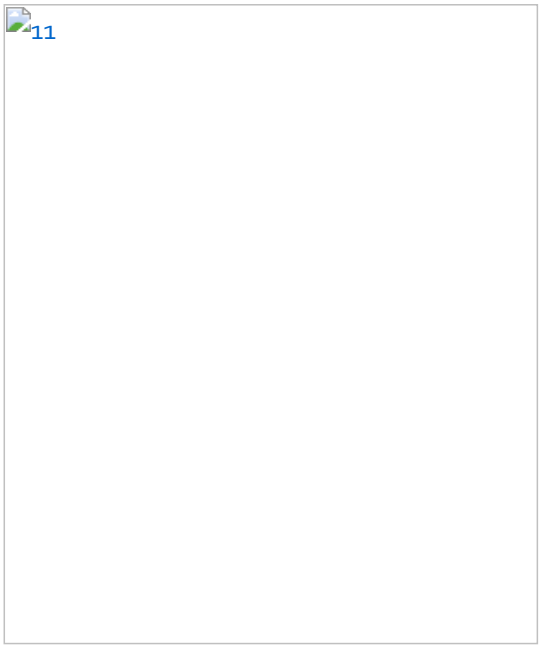


Consider the following when planning a secure DNS deployment: The following design choices can affect security of your DNS deployment

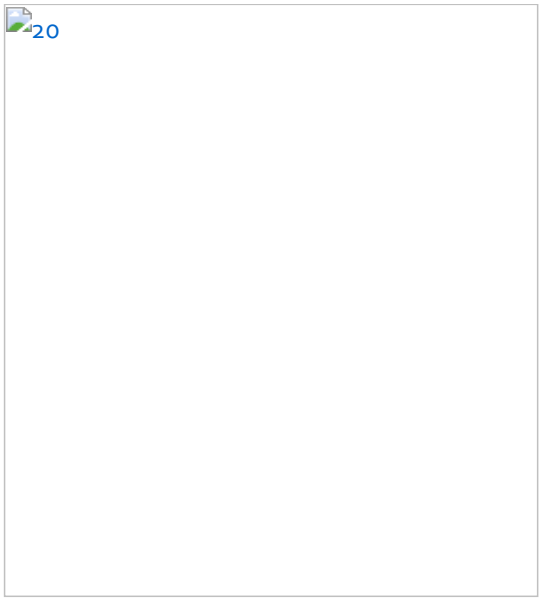
- **Communication with the Internet**. If your network hosts are not required to resolve names on the Internet, eliminate all communication between internal DNS servers and the Internet. In this DNS design, you can use a private DNS namespace that is hosted entirely in your network where internal DNS servers host zones for the root domain and top-level domains. In this configuration, your DNS servers will not use Internet root name servers. For more information about root hints, see Configure Internal Root Hints.
  If your network hosts are required to resolve names on the Internet, configure a group of DNS servers in the forest root domain (FRD) to forward queries for external names to an external DNS server. Configure DNS servers in a child domain to only forward queries to DNS servers in the FRD. Protect communications between internal and external DNS servers by configuring a packet-filtering firewall to only allow UDP and TCP port 53 communications. For more information about using forwarders, see Configure a DNS server to use forwarders
- **DNS namespace**. If your organization's DNS namespace is split into internal and external domains, host your internal

DNS namespace on DNS servers located on the internal network and the external DNS namespace on DNS servers located on a perimeter network. Protect internal DNS servers by placing them behind a firewall. If internal client computers are required to resolve hosts in the external namespace, your internal DNS namespace can be a subdomain of your external DNS namespace. For example, if the Internet DNS namespace for your organization is MicrosoftGURU.com.au, then the internal DNS namespace for your network might be corp.MicrosoftGURU.com.au. If internal network hosts do not need to resolve hosts in the external domain, then your internal DNS namespace can be distributed the same as the Internet DNS namespace. However, you should use a differing set of domain names for internal and external hosts so that the two domains do not overlap. For example, if your organization's parent domain name is MicrosoftGURU.com.au, you can use an internal DNS domain such as corp.MicrosoftGURU.com.au. By keeping your internal and external namespaces separate and distinct in this way, you enable simplified maintenance of configurations such as domain name filter or exclusion lists.

- **Restricting zone transfers**. For increased security, disable all zone transfers unless they are required. If required, configure this setting to allow zone transfers only to specified IP addresses. Allowing zone transfers to any server may expose your DNS data to an attacker attempting to footprint your network. By default, zone transfers are disabled for zones that are AD integrated. For non-AD integrated zones, default settings allow zone transfers only to servers that are listed in the name server (NS) resource records of the zone. For more information, see Restrict Zone Transfers.
- **Configuring AD integrated zones**. Security enhancements that are available when using directory-integrated zones include access control lists and secure dynamic updates. You cannot use directory-integrated zones unless the DNS server is also a domain controller. For more information, see Configure AD Integrated Zones.



- **Configuring the Discretionary Access Control List (DACL)**. You can use the DACL to secure a dnsZone object container in the directory tree. This feature provides granulated access to either the zone or a specified resource record in the zone. For example, the DACL for a zone resource record can be restricted so that dynamic updates are only allowed for a specified client computer or a secure group such as a domain administrators group. This security feature is not available with standard primary zones. For more information, see Configure the Discretionary Access Control List (DACL).
- **Allowing only secure dynamic updates**. Dynamic updates can be secure or non-secure. To help protect DNS servers from DNS spoofing attacks, you should only use secure dynamic updates. DNS update security is available only for zones that are Active Directory integrated. For more information, see Allow Only Secure Dynamic Updates.



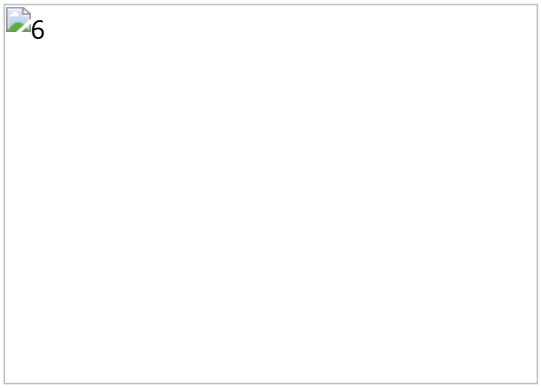
- **Configuring the Global Query Block List**. The global query block list is a new security feature introduced with the Windows Server® 2008 operating system. Use the global query block list to prevent malicious users from registering a host name that might have special significance for certain applications and allow them to divert network traffic. For more information, see Configure the Global Query Block List.
- **Configuring the socket pool**. The socket pool enables a DNS server to use source port randomization when issuing DNS queries. This provides enhanced security against cache poisoning attacks. You can also customize socket pool settings. For information, see Configure the Socket Pool.
- **Configuring cache locking**. When you enable cache locking, the DNS server will not allow cached records to be overwritten for the duration of the time to live (TTL). Cache locking also provides for enhanced security against cache poisoning attacks. Cache locking is available if your DNS server is running Windows Server 2008 R2. You can also customize the settings used for cache locking. For more information, see Configure Cache Locking.
- **Restricting DNS responses to selected interfaces**. By default, a DNS server that has multiple network interfaces, or is configured with multiple IP addresses on a single interface, will respond to DNS queries sent to all its IP addresses. To improve security of the DNS server, restrict the DNS service to listen only on IP addresses that are used by the server's DNS clients as their preferred DNS server. For more information, see Restrict DNS servers to listen only on selected interfaces.
- **Configuring internal Root Hints**. When the DNS Server service is running on a domain controller, root hints are read from Active Directory first. If the DNS Server service is not running on a domain controller or no root hints exist in Active Directory, root hints are implemented using a file, Cache.dns, stored in the %windir%System32Dns folder on the server computer. Root hints normally contain the name server (NS) and address (A, AAAA) resource records for the Internet root servers. If, however, you are using the DNS Server service on a private network, you can edit or replace Root hints with similar records that point to your own internal root DNS servers. This prevents your internal DNS servers from sending private information over the Internet when they resolve names. For more information, see Configure Internal Root Hints.
- **Disabling recursion**. To protect DNS servers, disable recursion on all servers that are not required to perform recursive queries. Recursion is a name-resolution technique in which a DNS server queries other DNS servers on behalf of the requesting client to fully resolve the name and then sends an answer back to the client. If enabled, an attacker can use the recursion process to cause domain names to resolve to the wrong IP address. By default, the DNS server performs recursive queries on behalf of its DNS clients and DNS servers that have forwarded DNS client queries to it. For more information, see Disable Recursion on the DNS Server.

- **Securing the DNS Cache**. By default, the DNS Server service is secured from cache pollution, which occurs when DNS query responses contain non-authoritative or malicious data. The Secure cache against pollution option prevents an attacker from successfully polluting the cache of a DNS server with resource records that were not requested by the DNS server. Changing this default setting will reduce the integrity of the responses that are provided by DNS Server service. You can restore the default setting if it was previously changed. For more information, see Secure the DNS Cache.

Active Directory Sites and Subnets: In Active Directory Sites and Subnets, you have to create various sites as per your real organization structure, add domain controller for authentication in that site and declare real network subnets assigned for sites. you have to create replication topology in active directory inter site links.

Sites: A site can be defined as a grouping or set of Internet Protocol (IP) subnets that are connected by a highly reliable, fast and inexpensive link. This is usually a local area network (LAN) or metropolitan area network (MAN). Domains can have domain controllers in multiple sites. A site can have domain controllers from multiple domains. In Active Directory, sites have the following main roles or purposes:

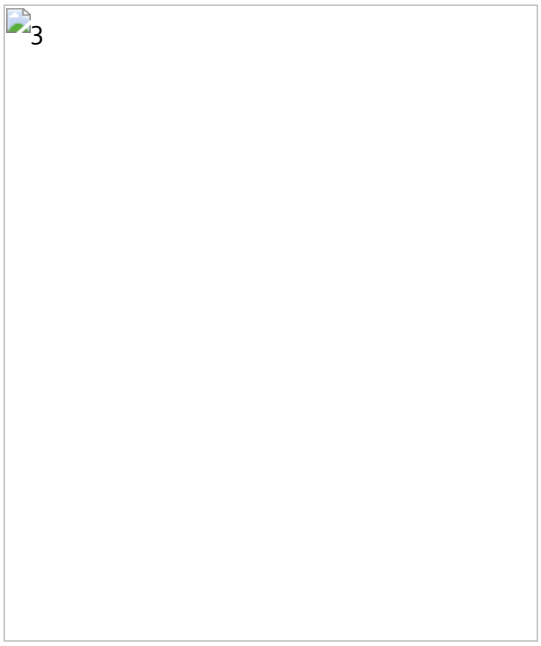
- A site determines the closest domain controller at workstation logon.
- A site operates as a replication boundary. As a replication boundary, a site optimizes replication between sites because it can be used to improve on and more efficiently manage Active Directory replication.
- A site also functions as a resource locator boundary. Clients are only able to access resources that are accessible in a particular site.



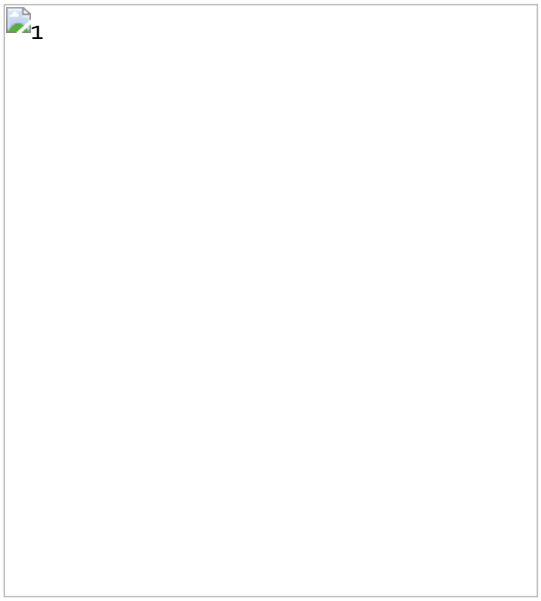
Site Links: Site links are logical connections that are established between sites is Active Directory that define a path between these sites. A site link defines the direction of Active Directory replication between sites. You can use either RPC over IP or SMTP as the transport protocol for moving replication data over a site link. Site links are assigned the following:

- Cost: With replication, the concept of cost indicates the cost of the physical link between two Active Directory sites and is utilized to detail optimal connection paths between one site and another site. When a site link is assigned a cost, the type of connection is taken into consideration. For replication, the lower costing links are used over higher costing links. A general method of calculating cost is Cost=1024/WAN Bandwidth. By default cost is 100.
- Interval: Replication over a site link takes place at predetermined time intervals. When assigning the replication interval, it is important not to set the value to too high or too low. An exceptionally high value means that changes take a longer time to be replicated, while an exceptionally lower value means that replication occurs too regularly.
- Schedule: A replication schedule and interval are basically used together. An interval is associated with a schedule. A schedule deals with when the replication of data is going to occur. I do not recommend to schedule and replication.

Keep it as default.

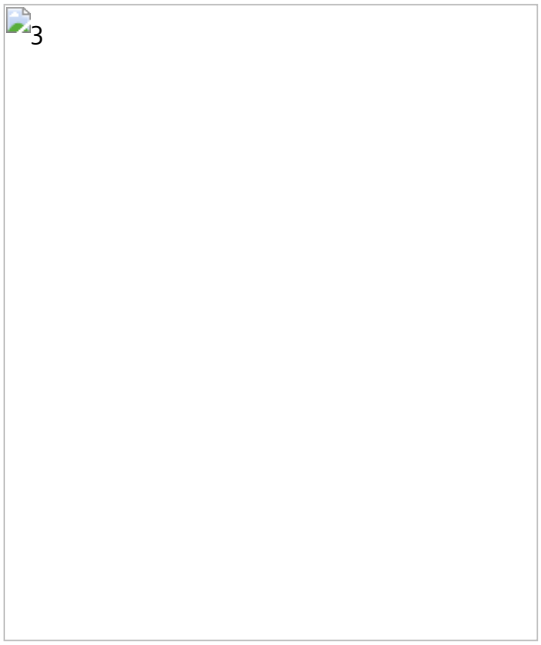


Site link bridge: In Active Directory, you can use a site link bridge to link sites that share common Active Directory data but who do not have a site link. The data typically shared by these sites is the Application directory partition.



Connection objects: In Active Directory, domain controllers replicate with specific replication partners. The partners that domain controllers replicate with are defined by connection objects. Connection object enable data to be replicated in Active Directory because they define inbound replication paths. Domain controllers and their associated connections are defined in a topology map. The Directory Replication Agent (DRA) handles replication between domain controllers. The Directory Replication Agent uses the connection objects in the topology map to find out those partners that are relevant when replicating changes to directory partitions. The DRA sends a replication request to the partners of a domain controller when the domain controller needs to update its copy of Active Directory. Administrators can manually create connection objects, or they can leave these objects to be created by the Knowledge Consistency Checker (KCC). When the KCC creates connection objects, it is an automatic process. The KCC runs on all domain controllers in Active Directory. As

an Administrator, you can create a manual connection object between any two domain controllers in a forest. If you want data to flow in two directions, you should create two connection objects. You can create manual connection objects between domain controllers in the same site or in different sites. The Knowledge Consistency Checker by default creates automatic connection objects. It references the site topology and then uses the information on sites and site links to automatically create connection objects. The KCC checks the site topology at regular intervals to determine whether the connection objects are still valid, and then changes connection objects based on its reviews. It is the KCC that is accountable for making certain that data in the directory partitions are replicated in sites. You can disable the automatic creation of connection objects on a per site and forest wide basis.



Planning AD SYSVOL: SYSVOL is a collection of folders that contain a copy of the domain's public files, including system policies, logon scripts, and important elements of Group Policy objects (GPOs). The SYSVOL directory must be present and the appropriate subdirectories must be shared on a server before the server can advertise itself on the network as a domain controller. Shared subdirectories in the SYSVOL tree are replicated to every domain controller in the domain. Sometimes systems administrator tent to utilize FRS functionality of Active Directory SYSVOL to keep software packages, application and files in SYSVOL. later on deploy these packages from SYSVOL. This is completely a wrong approach that lead to replication issues among domain controllers. the bigger the sysvol the greater possibility of replication failure. Remember that FRS has to replicate entire data of SYSVOL across domain controllers in a forest. If you have less bandwidth, your replication might goes into queue. Deploy packages from a different DFS share and keep un-related files and folder out of SYSVOL.

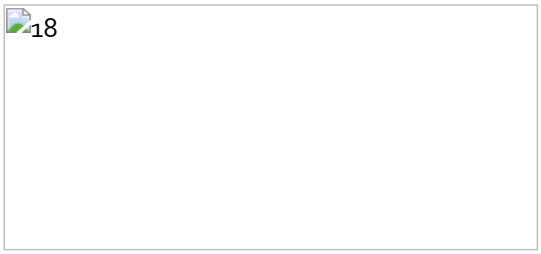
SYSVOL data and the File Replication Service (FRS): The system volume contains scripts and group policies. SYSVOL data is hosted on every domain controller. Changes to SYSVOL are replicated to domain controllers within the same domain via File Replication System (FRS) replication. With FRS replication, the full file is replicated and not just the actual changes that were made to the file. This differs to Active Directory replication. With Active Directory only the changes that were made to Active Directory objects are replicated.

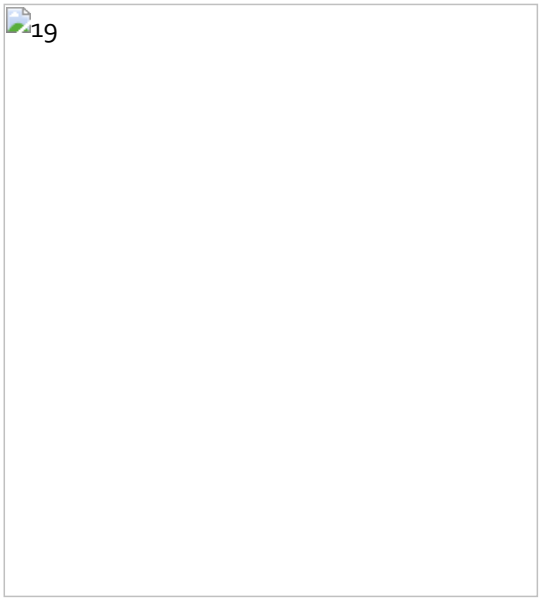
When you relocate folders, you use the first three levels of subdirectories to properly update the path locations that DFS Replication uses. These levels are affected by junction points and parameter settings. These folders include the following:

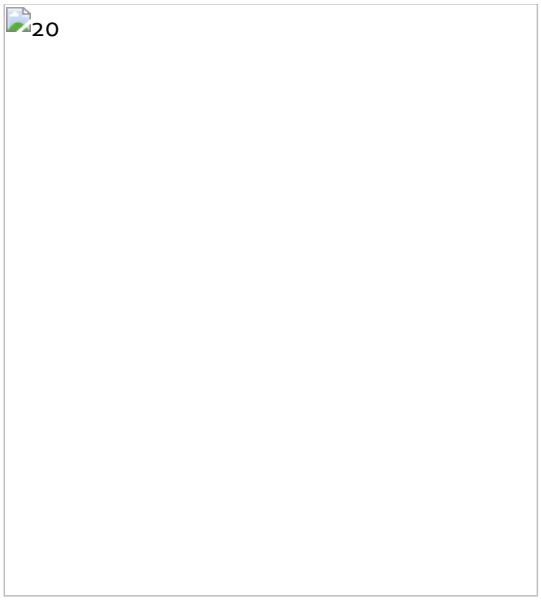
- %windir%SYSVOL
- %windir%SYSVOLdomain
- %windir%SYSVOLdomainDfsrPrivate
- %windir%SYSVOLdomainPolicies
- %windir%SYSVOLdomainscripts
- %windir%SYSVOLstaging
- %windir%SYSVOLstagingdomain
- %windir%SYSVOLstaging areas
- %windir%SYSVOLstaging areas<FQDN>, where FQDN is the fully qualified domain name of the domain that this domain controller hosts, for example, Microsoftguru.com.au.
- %windir%SYSVOLsysvol
- %windir%SYSVOLsysvol<FQDN>, where FQDN is the fully qualified domain name of the domain that this domain controller hosts, for example, Microsoftguru.com.au.

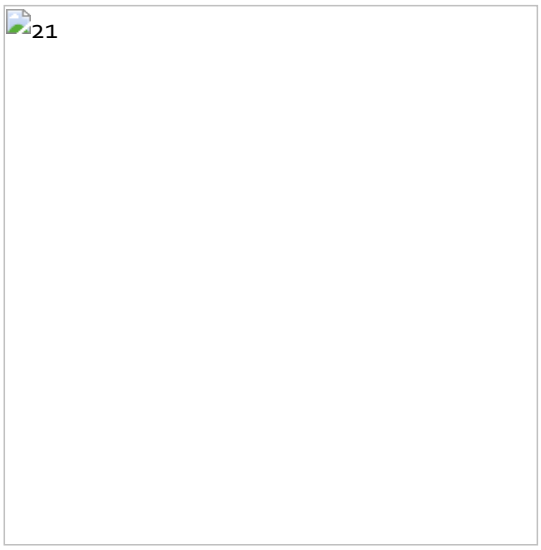
Dynamic Host Configuration Protocol and Active Directory: Windows Server 2008 provides integrated security support for networks that use Active Directory Domain Services (AD DS). This support adds and uses a class of objects that is part of the base directory schema, providing the following enhancements:

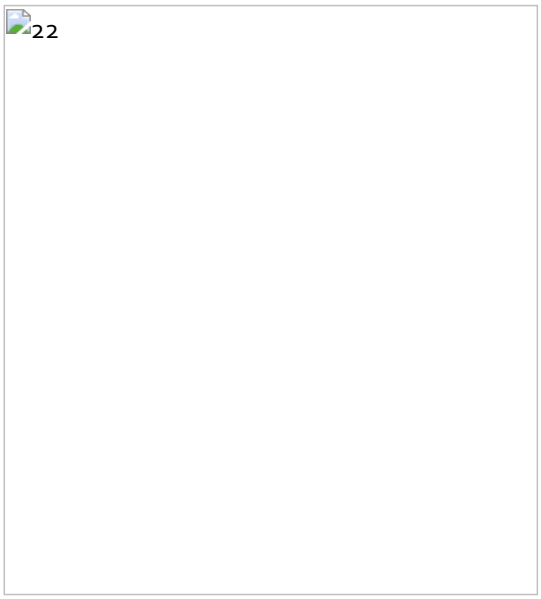
- A list of IP addresses available for the computers that you authorize to operate as DHCP servers on your network.
- Detection of unauthorized DHCP servers and prevention of their starting or running on your network.

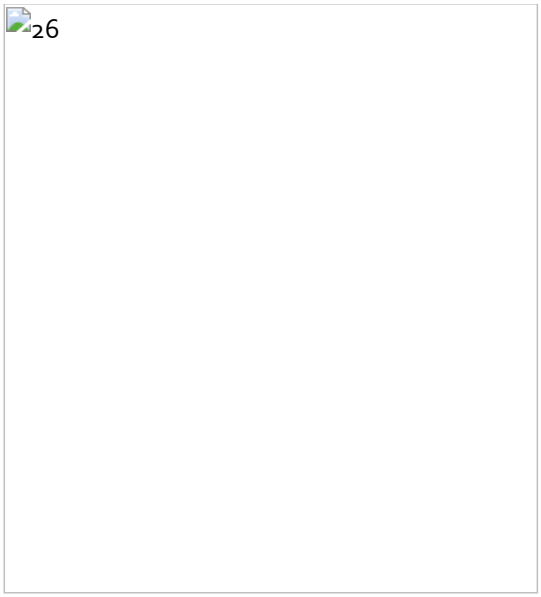


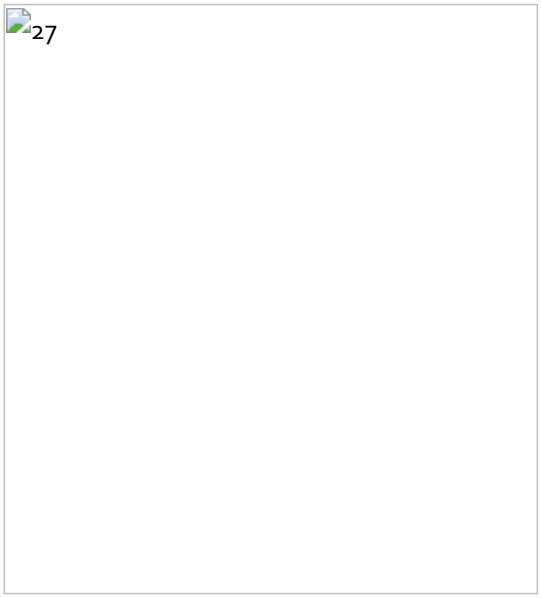



20


21


22





The authorization process for DHCP server computers depends on the installed role of the server on your network. A DHCP server can be installed on a domain controller, a member server or standalone. If you deploy AD DS, all computers operating as DHCP servers must be either domain controllers or domain member servers before they can be authorized and provide DHCP service to clients.

Although it is not recommended, you can use a stand-alone server as a DHCP server as long as it is not on a subnet with any authorized DHCP servers. When a stand-alone DHCP server detects an authorized server on the same subnet, it automatically stops leasing IP addresses to DHCP clients.

Do you need an WINS server anymore? Today, numerous Microsoft customers deploy WINS technology in their environment. WINS is an alternative name resolution protocol to DNS. It is an older service that uses NetBIOS over TCP/IP (NetBT). WINS and NetBT do not support IPv6 protocols and both are entering legacy mode. To help customers migrate to DNS for all name resolution the DNS Server role in Windows Server 2008 supports a special GlobalNames Zone (GNZ) feature. Some customers in particular require the ability to have the static, global records with single-label names that WINS currently provides. These single-label names typically refer to records for important, well-known and widely-used servers for the company, servers that are already assigned static IP addresses and are currently managed by IT-

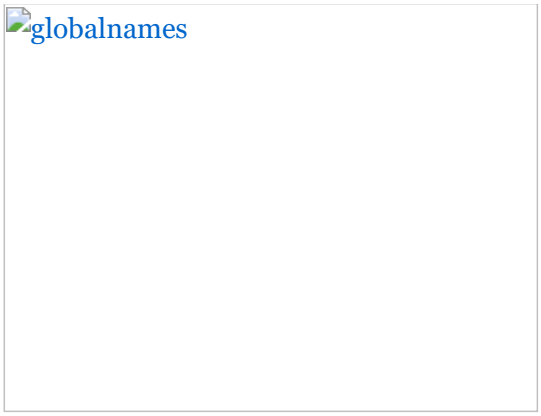
administrators using WINS. GNZ is designed to enable the resolution of these single-label, static, global names for servers using DNS.

GNZ is intended to aide retirement of WINS. It is not a replacement for WINS. GNZ is not intended to support the single-label name resolution of records that are dynamically registered in WINS, records which typically are not managed by IT administrators. Support for these dynamically registered records is not scalable, especially for larger customers with multiple domains and/or forests. This deployment guide is designed to help customers understand how to deploy the GlobalNames Zone in a variety of scenarios.

To Enable the GlobalNames Zone functionality, Open a command prompt, Click Start>right click Command Prompt>click Run as Administrator. Type the following, and then press Enter:

Dnscmd *ServerName* /config /Enableglobalnamessupport 1

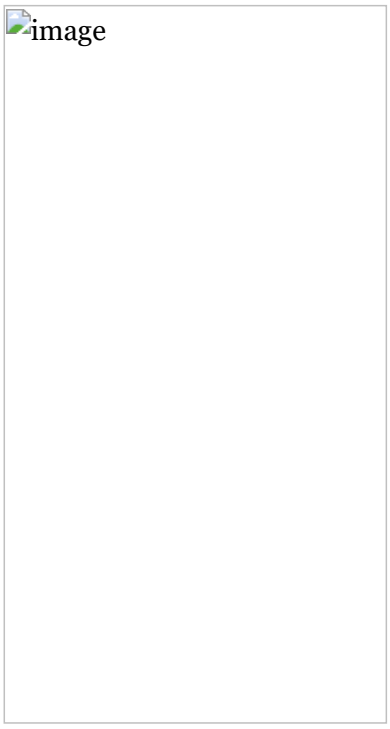
To Create the GlobalNames Zone using the Windows Interface, Open the DNS console. In the console tree, right-click a DNS server, and then click **New Zone** to open the New Zone Wizard> Create a new zone and give it the name GlobalNames. Choose Active Directory storage method and AD replication scope for the zone



Note: Microsoft recommend that you store the zone in AD DS and replicate it to all domain controllers that are DNS servers in the Forest. This will create a new AD DS-integrated zone called GlobalNames which is stored in the forest-wide DNS application partition.

For a customer with many domains, managing a suffix search list for all clients can be cumbersome, and client query performance is also somewhat lowered when querying a single-label name with the list of domains. For environments that require both many domains and single-label name resolution of corporate server resources, GNZ provides a more scalable solution.

Setting Organizational Unit: OUs organize resources like computers, users, servers and printers. The more you organize OU the better you can manage Active Directory. OU also help you to segregate control and permission through delegation. This requirement could be the result of management wishes for delegation, or to give control over OUs to specific administrators based on corporate policies or because of the acquisition of other companies.



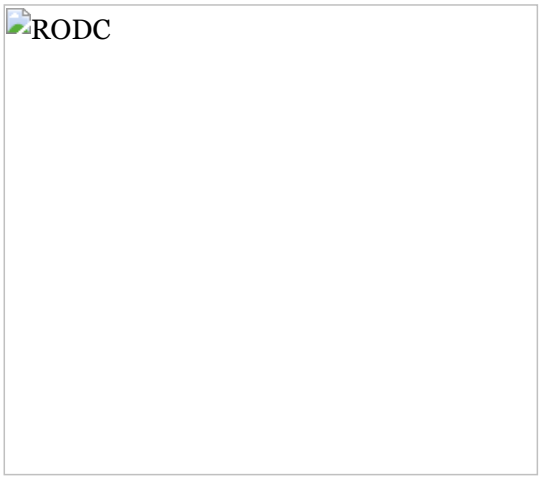
Active Directory Group Policy Object: Group Policy enables administrators to manage configurations for groups of computers and users, including options for registry-based policy settings, security settings, software deployment, scripts, folder redirection, Remote Installation Services, and Internet Explorer maintenance. By using Group Policy, you can deploy

software packages and secure computers and users . Because of factors such as the large number of policy settings available, the interaction between multiple policies, and inheritance options, Group Policy design can be complex. By carefully planning, designing, testing, staging and implementing a solution based on your organization's business requirements, you can provide the standardized functionality, security, and management control that your organization needs. Do not use Windows XP GPMC to deploy software and any security. Use Windows 7 or Windows Server 2008 GPMC to deploy group policy. Why is that? When you use Windows XP GPMC to create group policy it copies ADM folder to newly created GPO folder which resides in SYSVOL. ADM folder is just a template not real GPO. If you continuously create GPO using XP GPMC you will be copying 4MB extra files in SYSVOL which is un-necessary. However, using windows7 GPMC does not copy ADM template into new GPO folder. Its saves disk space and create less mess in GPO SYSVOL. If you are heavily dependent on GPO, you can utilize advanced group policy management to fulfill your requirements.

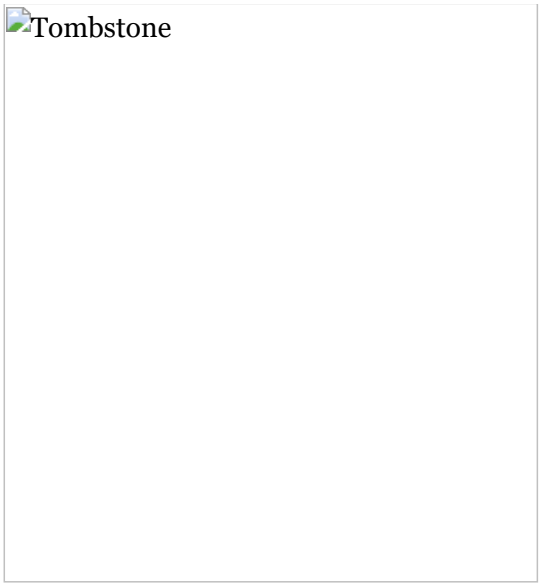
Read Only Domain Controller (RODC): RODC is highly advantageous for branch deployment where physical security isn't guaranteed and no system administrator is present to maintain domain controller whereas you want an reliable authentication provider. Microsoft has introduced the read-only domain controller (RODC) with the release of windows server 2008. The RODC contains a read-only copy of the Active Directory database that cannot be directly configured. This increases security, especially in areas where the physical security of the domain controller cannot be guaranteed.This functionality is gained by the RODC introducing technologies such as the following:

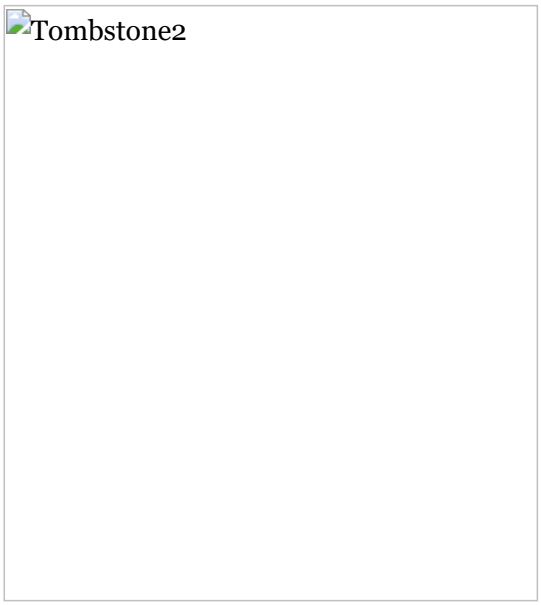
- Read-only AD DS database
- Unidirectional replication
- Credential caching
- Administrator role separation
- Read-only DNS

windows server 2008 domain controller installation wizard, simply select RODC to install RODC.

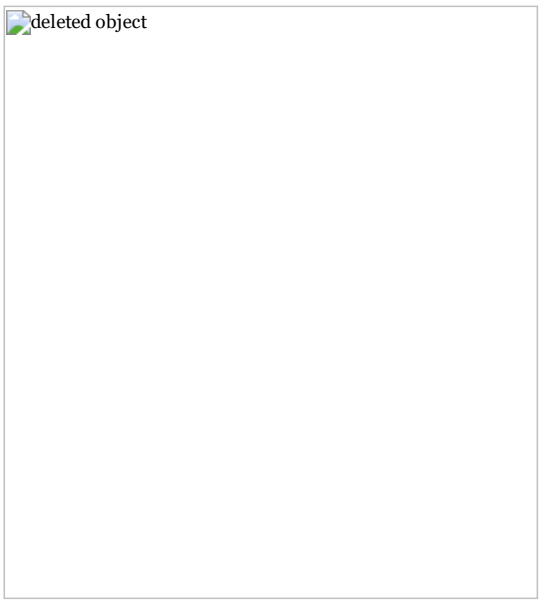


Tombstone Life Cycle: Depending on your system environment and business practices, you can increase or decrease the deleted object lifetime and the tombstone lifetime. If you want your deleted objects to be recoverable for longer than the default 180 days, you can increase the deleted object lifetime. If you want your recycled objects to be recoverable (through authoritative restore) for longer than the default 180 days, you can also increase the tombstone lifetime. I would not recommend to setup tombstone life is 3 days or a week though for weird reason I found systems administrator does this mistake. To modify Tombstone life using ADSIEDIT.msc follow the screenshot





To modify the deleted object lifetime by using the ADSIEDIT.msc



Active Directory Core Installation : In keeping with Microsoft's ongoing battle against all things security (whether implied or true), the company has introduced a new type of server for 2008. Windows 2008 Server Core is a Windows server that does not contain a GUI. All administration of Server Core is performed via the command line or via scripting. You may also administer some functions by connecting to Server Core from another server's Microsoft Management Console (MMC) utility. Server Core was introduced for many reasons:

- Reduced attack surface
- Reduced management
- Less disk space
- Reduced maintenance

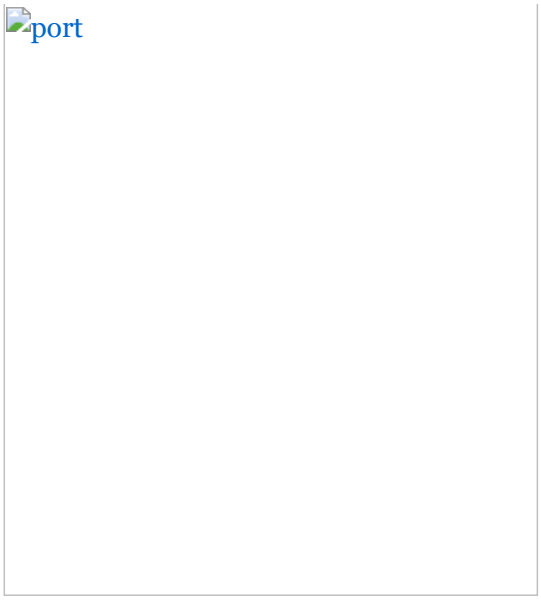
What you should do before implementing Active Directory: When working with any design, make sure you have a good framework from which to work. You need to plan, design, develop and deploy. Risk assessment vital for any project you do. For Microsoft Active Directory risk assessment is crucial stage. When you design Active Directory, you must keep in mind fault tolerance, highly available proportionate systems that meet your business needs.

Active Directory Post Consideration: Once you have deployed Active Directory, revisit your plan and follow what you have done practically. You must stick with your plan to minimize risk might have. The following would be a good best practice for post deployment consideration.

- Setup appropriate security in Active Directory and DNS
- Tighten up security for computers and users using GPO
- Delegate controls for OU
- Configure Sites and Subnets
- Setup correct replication policy
- Setup Audit policy in Active Directory
- Setup patching schedule

Patching Domain Controller using WSUS: Microsoft releases hotfixes, patch and service pack for Microsoft Windows operating system. Its necessary to keep yourself up to date with Microsoft products. Subscribe Microsoft security bulletins to get an updates from Microsoft Corp. Microsoft release updates in the third quarter of each month. A common patching involve asses, identify, evaluate and plan and than deploy. To follow a best practice, you must create a staging area separated from your production Active Directory infrastructure where you can stage an domain controller patching using WSUS. Staging will eliminate any unnecessary risk and avoid catastrophe. visit this URL to learn more about WSUS.

AD DS Port: AD DS port management is vital for AD administrator. By default ldap is configured with port 389. Its not a best practice to change port number to new port number. However if you do change port number for security reason, make sure you unblock that port in FF TMG and firewall and keep a record of the change. Occasionally, I found that systems administrator change ldap port in Active Directory DNS and security administrator block new ldap port in firewall. I would recommend you to get more information on AD DS port requirement from TechNet and deploy AD port as appropriate.



Microsoft Active Directory— DO and DONT:

KISS (Keep it simple & sweet) Policy: The first bit of advice is to keep things as simple as you can. Active Directory is designed to be flexible, and if offers numerous types of objects and components. But just because you can use something doesn't mean you should. Keeping your Active Directory as simple as possible will help improve overall efficiency, and it will make the troubleshooting process easier whenever problems arise.

Avoid mixing up server roles and app with domain controller: Avoid mixing up other server roles with Active Directory Domain Controller. For example, installing FF TMG , SQL server, exchange or IIS FTP on domain controller server is an worse idea. This will create a complete chaos among all these infrastructures. Domain controller will not perform at its best. Adding additional roles to a domain controller can affect the server's performance, reduce security, and complicate the process of backing up or restoring the server.

Use the appropriate site topology: Although there is definitely something to be said for simplicity, you shouldn't shy away from creating more complex structures when it is appropriate. Larger networks will almost always require multiple Active Directory sites. The site topology should mirror your network topology. Portions of the network that are highly connected should fall within a single site. Site links should mirror WAN connections, with each physical facility that is separated by a WAN link encompassing a separate Active Directory site. Keep adding all the new subnets in the appropriate sites.

Branch domain controllers: Having a read only domain controller in a branch is always good idea. However, if you want to setup a writable domain controller in branch than make sure you have tightened security and delegation in place.

DNS & GC Server: Microsoft recommend that you make all domain controller global catalog server. I found systems administrator install domain controller without integrating DNS with AD. you must integrate Active Directory with DNS. If you have a single DNS server and that DNS server fails, Active Directory will cease to function. Its better to have a more than one Active Directory, GC and DNS to obtain redundancy.

Virtualized Domain Controllers: : One of the main reasons organizations use multiple domain controllers is to provide a degree of fault tolerance in case one of the domain controllers fails. However, this redundancy is often circumvented by server virtualization. I often see organizations place all their virtualized domain controllers onto a single virtualization host server. So if that host server fails, all the domain controllers will go down with it. There is nothing wrong with virtualizing your domain controllers, but you should scatter the domain controllers across multiple host servers.

Maintain FSMO roles (backups): Although Windows 2000 and every subsequent version of Windows Server have supported the multi-master domain controller model, some domain controllers are more important than others. Domain controllers that are hosting Flexible Single Master Operations (FSMO) roles are critical to Active Directory health. Active Directory is designed so that if a domain controller that is hosting FSMO roles fails, AD can continue to function — for a while. Eventually though, a FSMO domain controller failure can be very disruptive.

I have seen sys admin say that you don't have to back up every domain controller on the network because of the way Active Directory information is replicated between domain controllers. While there is some degree of truth in that statement, backing up FSMO role holders is critical. I once had to assist with the recovery effort for an organization in which a domain controller had failed. Unfortunately, this domain controller held all of the FSMO roles and acted as the organization's only global catalog server and as the only DNS server. To make matters worse, there was no backup of the domain controller. We ended up having to rebuild Active Directory from scratch. This is an extreme example, but it shows how important domain controller backups can be. You can deploy Symantec live state backup for physical server or VCB backup for virtual DC.

Plan your domain structure and stick to it: Most organizations start out with a carefully orchestrated Active Directory architecture. As time goes on, however, Active Directory can evolve in a rather haphazard manner. To avoid this, I recommend planning in advance for eventual Active Directory growth. You may not be able to predict exactly how Active Directory will grow, but you can at least put some governance in place to dictate the structure that will be used when it does.

Have a management plan in place before you start setting up servers: Just as you need to plan your Active Directory structure up front, you also need to have a good management plan in place. Who will administrator Active Directory? Will one person or team take care of the entire thing or will management responsibilities be divided according to domain or organizational unit? These types of management decisions must be made before you actually begin setting up domain controllers.

Try to avoid making major logistical changes: Active Directory is designed to be extremely flexible, and it is possible to perform a major restructuring of it without downtime or data loss. Even so, I would recommend that you avoid restructuring your Active Directory if possible. I have seen more than one situation in which the restructuring process resulted in some Active Directory objects being corrupted, especially when moving objects between domain controllers running differing versions of Windows Server.

Domain controller & NTP: It's not bad to make domain controller a NTP. Its better to have a separate NTP server if you can. But you will be experience event log in domain controller. It would not be a good idea to make a virtualized domain controller having an NTP role.

Relevant Study:

Active Directory Domain Services Guide

Microsoft Active Directory Topology Diagrammer

Risk and Health Assessment Program for Active Directory (ADRAP) – Scoping Tool v1.6

Active Directory Domain Services in the Perimeter Network (Windows Server 2008)

Read-Only Domain Controller (RODC) Branch Office Guide

Windows Server 2008 Remote Server Administration Tools for Win 7

Installing or Removing the Remote Server Administration Tools Pack

Planning and Deploying Read-Only Domain Controllers

Infrastructure Planning and Design

About Raihan Al-Beruni

My Name is Raihan Al-Beruni. I am working as an Infrastructure Architect in Data Center Technologies in Perth, Western Australia. I have been working on Microsoft technologies for more than 15 years. Other than Microsoft technologies I also work on Citrix validated solution and VMware data center virtualization technologies. I have a Masters degree in E-Commerce. I am certified in Microsoft, VMware, ITIL and EMC. My core focus is on cloud technologies. In my blog I share my knowledge and experience to enrich information technology community as a whole. I hope my contribution through this blog will help someone who wants more information on data center technologies.

View all posts by Raihan Al-Beruni →