Active Directory Readiness Document

Prepared by: Identity Management - Premier Field Engineers

Date: February 2013

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

Table of Contents

Active Directory Replication

Active Directory replication has the following dependencies:

Domain Name System (DNS) that resolves DNS names to IP addresses. Active Directory requires that DNS is properly designed and deployed so that domain controllers can correctly resolve DNS names of replication partners.

Remote Procedure Call (RPC), Active Directory replication requires IP connectivity and the Remote Procedure Call (RPC) to transfer updates between replication partners.

Kerberos v5 authentication. The authentication protocol for both authentication and encryption that is required for all Active Directory RPC replication.

LDAP protocol. The primary access protocol for Active Directory. Replication of an entire replica of an Active Directory domain, as occurs when Active Directory is installed on an additional domain controller in an existing domain, uses LDAP communication rather than RPC.

NetLogon

Ports used by AD Replication

Service Name	UDP	TCP
RPC Endpoint Mapper	135	
AD Replicator Service		1024 and above (Dynamic Port)
LDAP	389	389
LDAP (SSL)		636 (Secure Sockets Layer [SSL])
LDAP (Global Catalog)		3268 (Global Catalog)
Kerberos	88	88
SMB over IP	445	445
DNS	53	53

How the Active Directory Replication Model Works

http://technet.microsoft.com/en-us/library/cc772726(WS.10).aspx

A Guide to Active Directory Replication

http://technet.microsoft.com/en-us/magazine/2007.10.replication.aspx

Inter-Site Topology Generator (ISTG)

http://support.microsoft.com/kb/224599

http://blogs.technet.com/b/janelewis/archive/2009/05/07/istg-what-happens-when-it-fails.aspx

DC GUIDs and Invocation IDs

http://blogs.dirteam.com/blogs/jorge/archive/2006/12/09/DSA_2D00_GUIDs-and-Invocation-IDs.aspx

USN Rollback and InvocationID reset

http://technet.microsoft.com/en-us/library/virtual_active_directory_domain_controller_virtualization_hyperv(WS.10).aspx

How to detect and recover from a USN rollback

http://support.microsoft.com/kb/875495/en-us

High-watermark

Active Directory domain controller maintains a value called the high watermark vector (HWMV) for other domain controllers that it is replicating with. Each DC will associate this high watermark vector with the Globally Unique Identifier (GUID) of the remote DC, to prevent any confusion if a remote domain controller is renamed or removed from the directory

Up-to-dateness vector

The UTDV is another piece of replication metadata that is used for propagation dampening; that is, its purpose is to prevent the same change from wasting bandwidth by being replicated across the network over and over again. Each DC maintains a UTDV table for every other DC that stores a replica of the naming context in question.

For the Domain NC, each DC in a domain maintains a UTDV for every DC in the domain;
for the Configuration and Schema NC, this is maintained for every DC in the forest.

The UTDV table keeps track, not only of the highest USN that each DC has received from its replication partners, but also the highest USN value that it has received from every DC that is replicating a given NC.

To allow for this, each replicated change also includes the following information:

- The GUID of the DC that is replicating the change. This can be a change that is being replicated as an originating write or as a replicated write.
- The USN from the DC that is replicating the change. Again, this can be from either an originating or a replicated write.
- The GUID of the DC that originated the change. If this GUID is the same as the GUID of the DC that is replicating the change, then this is an originating write. Otherwise, the UTDV table comes into play.

- The USN from the DC that originated the change. Again, if this USN is the same as the USN of the DC that is replicating the change, then this is an originating write. Otherwise, it's off the UTDV table.

http://technet.microsoft.com/en-us/magazine/2007.10.replication.aspx

Kerberos

http://blogs.technet.com/b/askds/archive/2008/03/06/kerberos-for-the-busy-admin.aspx

(Excellent Video)

http://technet.microsoft.com/en-us/ff606447.aspx

http://blogs.msdn.com/b/spatdsg/archive/2008/08/21/kerberos-domain-routing.aspx

http://blogs.technet.com/b/askds/archive/2009/04/10/name-suffix-routing.aspx

Troubleshooting Kerberos Errors

http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=21820

FSMO

Initial synchronization requirements for Windows 2000 Server and Windows Server 2003 operations master role holders

http://support.microsoft.com/kb/305476

Phantoms, tombstones and the infrastructure master

http://support.microsoft.com/kb/248047

The Infrastructure Master (IM) role should be held by a domain controller that is not a Global Catalog server (GC). If the Infrastructure Master runs on a Global Catalog server it will stop updating object information because it does not contain any references to objects that it does not hold. This is because a Global Catalog server holds a partial replica of every object in the forest. As a result, cross-domain object references in that domain will not be updated and a warning to that effect will be logged on that DC's event log. If all the domain controllers in a domain also host the global catalog, all the domain controllers have the current data, and it is not important which domain controller holds the infrastructure master role.

Global catalog and infrastructure master role conflict

If the IM Flexible Single Master Operation (FSMO) role holder is also a global catalog server, the phantom indexes are never created or updated on that domain controller. (The FSMO is also known as the operations master.) This behavior occurs because a global catalog server contains a partial replica of every object in Active Directory. The IM does not store phantom versions of the foreign objects because it already has a partial replica of the object in the local global catalog.

For this process to work correctly in a multidomain environment, the infrastructure FSMO role holder cannot be a global catalog server. Be aware that the first domain in the forest holds all five FSMO roles and is also a global catalog. Therefore, you must transfer either role to another computer as soon as another domain controller is installed in the domain if you plan to have multiple domains.

If the infrastructure FSMO role and global catalog role reside on the same domain controller, you continually receive event ID 1419 in the directory services event log. For more information, click the following article number to view the article in the Microsoft Knowledge Base:

251095 Event ID 1419 generated on a domain controller

Global catalog replication

http://technet.microsoft.com/en-us/library/cc759007(WS.10).aspx

Cross-domain references and the infrastructure master role

Certain types of groups in an active directory domain can contain accounts from trusted domains. To make sure that the names in the group's membership are accurate, the user object's GUID is referenced in the membership of the group. When Active Directory Tools displays these groups that have users from foreign domains, they must be able to display the accurate and current name of the foreign user without relying on immediate contact with a domain controller for the foreign domain or a global catalog.

Active Directory uses a phantom object for cross-domain group-to-user references. This phantom object is a special kind of object that cannot be viewed through any LDAP interface.

Phantom records contain a minimal amount of information to let a domain controller refer to the location in which the original object exists. The index of phantom objects contains the following information about the cross-referenced object:

- Distinguished name of the object
- Object GUID
- Object SID

During the addition of a member from a different domain to a local user group, the local domain controller that is performing the addition to the group creates the phantom object for the remote user.

If you change the foreign user's name or delete the foreign user, the phantoms must be updated or removed in the group's domain from every domain controller in the domain. The domain controller holding the infrastructure master (IM) role for the group's domain handles any updates to the phantom objects.

Lingering objects in Active Directory

http://technet.microsoft.com/en-us/edge/Video/hh672193

Sysvol, FRS and DFS-R Replication

FRS

The File Replication Service (FRS) is a technology that replicates files and folders stored in the SYSVOL shared folder on domain controllers and Distributed File System (DFS) shared folders. FRS is used in Windows Server 2000 and 2003. FRS is also used in Windows Server 2008 if the domain was upgraded, the domain functional level is not raised to 2008 and SYSVOL has not been migrated to DFS Replication. In the case of a new domain originally built on Windows Server 2008 domain functional level, DFS Replication will be used by default. When FRS detects that a change has been made to a file or folder within a replicated shared folder, FRS replicates the updated file or folder to other servers. Because FRS is a multi-master replication service, any server that participates in replication can generate changes. In addition, FRS can resolve file and folder conflicts to make data consistent among servers.
Microsoft recommends the following FRS replication limits:

Content and Data Limits

- Maximum file size of 20 GB
- Maximum of 64 GB of data
- No more than 500,000 files under the replica root
- Maximum 1,000,000 simultaneous change orders

Topology Limits

- 150 replica sets per computer
- 1,000 replica members

DFSR

The Distributed File System Replication Service (DFSR) was introduced in Windows 2003 R2 but could not be used with SYSVOL. In Windows Server 2008 DFSR can be used for replicating SYSVOL if the domain functional level is Windows 2008.

DFS Replication is a state-based, multi-master replication engine that supports replication scheduling and bandwidth throttling. DFS Replication uses a compression algorithm known as Remote Differential Compression (RDC). RDC detects insertions, removals, re-arrangements of data in files, enabling DFS Replication to replicate only the deltas (changes) when files are updated.

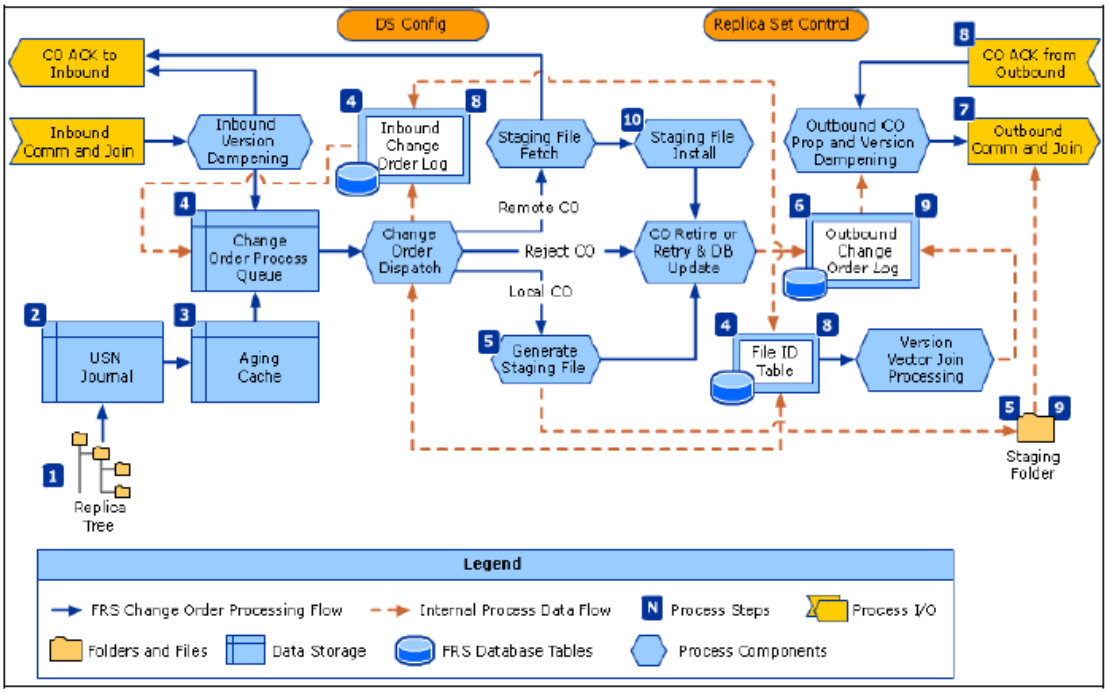
DFS Replication overcomes three common FRS issues:

- Journal wraps
- Excessive replication
- Morphed folders

How FRS Works

http://technet.microsoft.com/en-us/library/cc758169(WS.10).aspx

How Change Orders Are Processed



Step 1: NTFS creates a change journal entry

Step 2: FRS monitors the USN journal

Step 3: Aging cache is used

Step 4: FRS creates entries in the inbound log and file ID table

Step 5: FRS creates the staging file in the staging folder

Step 6: FRS creates the entry in the outbound log

Step 7: FRS sends a change notification

Step 8: FRS records and acknowledges the change notification

Step 9: FRS replicates the staging file

Step 10: FRS constructs the staging file (Pre - Install) and moves it into the replica tree

How to rebuild the SYSVOL tree and its content in a domain

http://support.microsoft.com/kb/315457

Using the BurFlags registry key to reinitialize File Replication Service

http://support.microsoft.com/kb/290762/en-us

Recovering missing FRS objects and FRS attributes in Active Directory

http://support.microsoft.com/kb/312862

DFS-R Recovery Sysvol

http://blogs.dirteam.com/blogs/jorge/archive/2010/08/13/restoring-the-sysvol-non-authoritatively-when-either-using-ntfrs-or-dfs-r-part-3.aspx

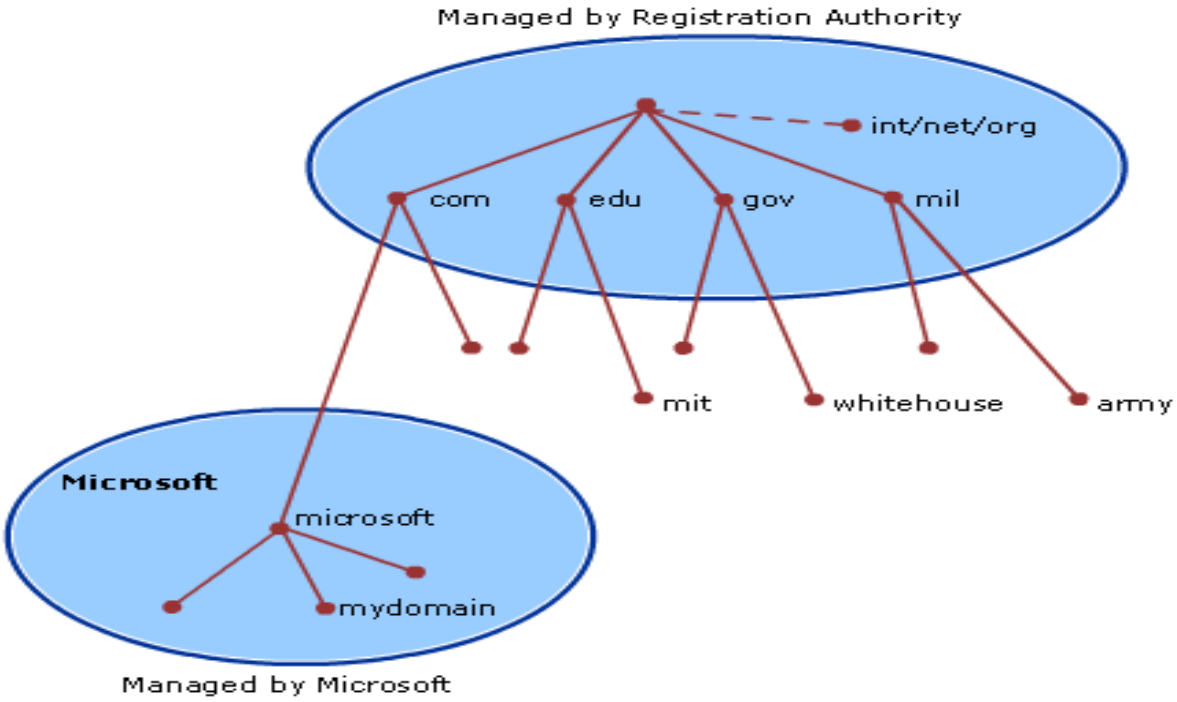
SYSVOL Migration

http://blogs.technet.com/b/filecab/archive/2008/02/08/sysvol-migration-series-part-1-introduction-to-the-sysvol-migration-process.aspx

http://technet.microsoft.com/en-us/library/dd641193(WS.10).aspx

Name Resolution

DNS is the primary name resolution service of Windows 2003 and 2008. DNS provides a reliable, hierarchical, distributed, and scalable database. Windows clients use DNS for name resolution and service location, including locating domain controllers for logging on. Domain controllers use DNS for replication and many other purposes. Without accurate name resolution, domain controllers will not replicate, clients will not log on, and service accounts will fail to start. This will cause problems with applications and users.



How DNS Works

http://technet.microsoft.com/en-us/library/dd197446(WS.10).aspx

DNS Support for Active Directory Tools and Settings

http://technet.microsoft.com/en-us/library/cc738266(WS.10).aspx

DNS Scavenging

http://blogs.technet.com/b/networking/archive/2008/03/19/don-t-be-afraid-of-dns-scavenging-just-be-patient.aspx

http://blogs.technet.com/b/askpfe/archive/2011/06/03/how-dns-scavenging-and-the-dhcp-lease-duration-relate.aspx

http://blogs.technet.com/b/networking/archive/2011/08/17/tracking-dns-record-deletion.aspx

Stub Zones and Conditional Forwarding

http://www.akomolafe.com/Portals/1/Docs/W2K3/DNS/Stub%20Zones%20and%20Conditional%20Forwarding.htm

Restrict the DNS resource records that are updated by Netlogon

http://technet.microsoft.com/en-us/library/cc778029(WS.10).aspx

Strict Name Checking

http://technet.microsoft.com/en-us/library/cc779394(WS.10).aspx

DNS Client Group Policy Settings

http://technet.microsoft.com/en-us/library/dd197486(WS.10).aspx

Network Ports Used by DNS

http://technet.microsoft.com/en-us/library/dd197515(WS.10).aspx

Deploy GlobalNames Zone

http://download.microsoft.com/download/e/2/0/e2090852-3b7f-40a3-9883-07a427af1560/DNS-GlobalNames-Zone-Deployment.doc

DNS Server Query Block List

http://download.microsoft.com/download/5/3/c/53cdc0bf-6609-4841-a7b9-cae98cc2e4a3/DNS_Server_Global_%20Query_Block%20List.doc

Secure DNS Deployment Guide

http://technet.microsoft.com/en-us/library/ee649266(WS.10).aspx

Single-Label name support

http://support.microsoft.com/kb/300684

Domain Controller Location Process

http://technet.microsoft.com/en-us/library/cc978011.aspx

DsGetDCName Function

http://msdn.microsoft.com/en-us/library/ms675983(VS.85).aspx

DNSLint utility

http://support.microsoft.com/kb/321045

How to verify that SRV DNS records have been created for a domain controller

http://support.microsoft.com/kb/816587

Restrict the DNS resource records that are updated by Netlogon

http://technet.microsoft.com/en-us/library/cc778029(WS.10).aspx

Troubleshooting Active Directory replication failures that occur because of DNS lookup failures, event ID 2087, or event ID 2088

http://support.microsoft.com/?id=824449

Using DNS Servers With DHCP -> Securing Records When Using the DnsUpdateProxy Group

http://technet.microsoft.com/en-us/library/cc787034(WS.10).aspx

How to Configure DNS Dynamic Updates in Windows Server 2003 -> Use the DnsUpdateProxy Security Group

http://support.microsoft.com/?id=816592

A DHCP Server Still Owns DNS Records When It Is a Member of the DnsUpdateProxy Group

http://support.microsoft.com/?id=314233

Reset Scavenging and Aging Properties for a Specified Resource Record

http://technet.microsoft.com/en-us/library/cc787627(WS.10).aspx

Understanding Aging and Scavenging

http://technet.microsoft.com/en-us/library/cc759204(WS.10).aspx

Enable Aging and Scavenging for DNS

http://technet.microsoft.com/en-us/library/cc755716(WS.10).aspx

Managing the Aging and Scavenging of Server Data

http://technet.microsoft.com/en-us/library/cc776907(WS.10).aspx

DNS Removes a Network Name Resource at the End of the Default Scavenging Interval in Windows Server 2003

http://support.microsoft.com/?id=838851

Setting Primary and secondary WINS server options

http://support.microsoft.com/?id=150737

How to Optimize the Location of a Domain Controller or Global Catalog That Resides Outside of a Client's Site

http://support.microsoft.com/?id=306602

Netlogon Incorrectly Registers SRV Records in DNS for Windows XP–based Clients

http://support.microsoft.com/?id=825675

Dynamic DNS Updates Do Not Work If the DHCP Client Service Stops

http://support.microsoft.com/?id=264539

Installing Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) on a Domain Controller

http://support.microsoft.com/?id=255134

How to Reconfigure an _msdcs Subdomain to a Forest-wide DNS Application Directory Partition When You Upgrade from Windows 2000 to Windows Server 2003 (817470)

http://support.microsoft.com/?id=817470

A Microsoft DNS container is created before full replication and causes a DNS conflict in Windows Server 2003

http://support.microsoft.com/?id=836534

Problems with Many Domain Controllers with Active Directory Integrated DNS Zones

http://support.microsoft.com/?id=267855

Common DNS Server Events Ids

http://technet.microsoft.com/en-us/library/cc735848(WS.10).aspx

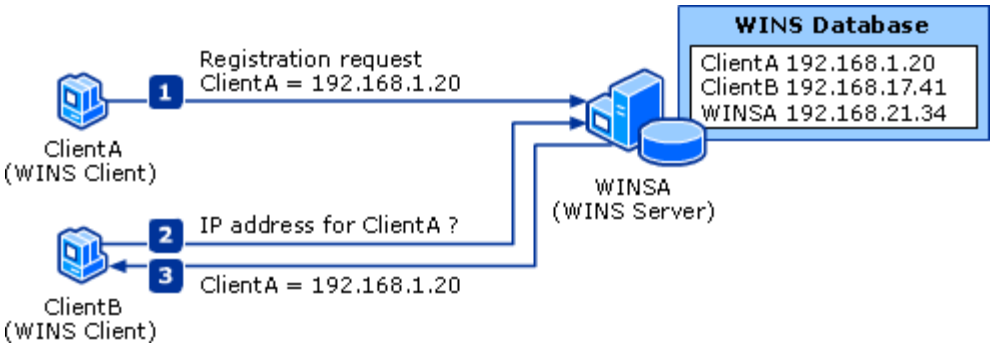
WINS

Role of WINS in the Network

Although NetBIOS and NetBIOS names can be used with network protocols other than TCP/IP, WINS was designed specifically to support NetBIOS over TCP/IP (NetBT). WINS is required for any environment in which user's access resources that have NetBIOS names. If you do not use WINS in such a network, you cannot connect to a remote network resource by using its NetBIOS name unless you use Lmhosts files, and you might be unable to establish file and print sharing connections.

The following figure illustrates the role of WINS for computers that use NetBIOS names. Typically, DHCP is used to assign IP addresses automatically.

WINS Name Registration and Resolution



In a typical scenario, the following occurs:

ClientA, which uses NetBIOS and is a WINS client, sends a name registration request to its configured primary WINS server (WINSA) when it starts up and joins the network. WINSA adds ClientA's NetBIOS name and IP address to the WINS database.

When ClientB needs to connect to ClientA by its name, it requests the IP address from the WINS server.

The WINS server locates the corresponding entry in its database and replies with ClientA's IP address.

Summary of WINS Benefits

WINS provides the following benefits over other NetBIOS name resolution methods:

- WINS name resolution reduces NetBIOS name query broadcast traffic because clients can query a WINS server directly instead of broadcasting queries.
- WINS enables the Computer Browser service to collect and distribute browse lists across IP routers.
- The WINS dynamic name-to-address database supports NetBIOS name registration and resolution in environments where DHCP-enabled clients are configured for dynamic TCP/IP address allocation.
- The WINS database also supports centralized management and replicates name-to-address mappings to other WINS servers.
- WINS and DNS can be used in the same environment to provide combined name searches in both namespaces.

WINS Overview

http://technet.microsoft.com/en-us/library/cc767878.aspx

Using WINS Lookup in DNS Zones

http://technet.microsoft.com/en-us/library/cc781381(WS.10).aspx

WINS Architecture and Capacity Planning White Paper Available

http://support.microsoft.com/?id=239950

Recommended Practices for WINS

http://support.microsoft.com/?id=185786

DHCP

Dynamic Host Configuration Protocol (DHCP) is a standard protocol defined by RFC 1541 (which is superseded by RFC 2131) that allows a server to dynamically distribute IP addressing and configuration information to clients. Normally the DHCP server provides the client with at least this basic information:

- IP Address
- Subnet Mask
- Default Gateway

Other information can be provided as well, such as Domain Name Service (DNS) server addresses and Windows Internet Name Service (WINS) server addresses. The system administrator configures the DHCP server with the options that are parsed out to the client.

DHCP (Dynamic Host Configuration Protocol) Basics

http://support.microsoft.com/kb/169289

How DHCP Technology Works

http://technet.microsoft.com/en-us/library/cc780760(WS.10).aspx

DHCP Lease Renewals

http://technet.microsoft.com/en-us/library/cc958919.aspx

Domain Controller Health

Summary of "piling on" scenarios in Active Directory domains

http://support.microsoft.com/kb/305027

w32Time

http://support.microsoft.com/kb/224799

Basic Operation

1. Client Boot No client boot-specific information.
2. Polling Loop
    1. The client contacts an authenticating domain controller.
        - Packets are exchanged to determine the latency of communication between the two computers.
        - W32Time determines what current time should be converged to locally, (the "target" time).
    2. The client adjusts the local time.
        - If the target time is ahead of local time, local time is immediately set to the target time.
        - If the target time is behind local time, the local clock is slowed (slewed) until the two times are aligned, unless local time is more than 3 minutes out of synchronization, in which case the time is immediately set.
    3. The time server client performs periodic checks.
        - The client connects to the authenticating domain controller once each "period."
        - The initial default period is 45 minutes.
    4. If the time synchronization attempt is successful three consecutive times, then the interval check period is increased to 8 hours. If it is not successful three consecutive times, then it is reset to 45 minutes.
3. Time Convergence Hierarchy
    1. All client desktops select an authenticating domain controller (the domain controller returned by DSGetDCName()) as their time source. If this domain controller becomes unavailable, the client re-issues its request for a domain controller.
    2. All member servers follow the same process.
    3. All domain controllers in a domain make 3 queries for a DC:
        - a reliable time service (preferred) in the parent domain,
        - a reliable time service (required) in the current domain,
        - the PDC of the current domain. It will select one of these returned DCs as a time source.
    4. The PDC FSMO at the root of the forest is authoritative, and can be manually set to synchronize with an outside time source (such as the United States Naval Observatory).

What is NT5DS and NTP

NTP – Synchronizes time via the manually designated NTP sources. Only the PDCE of the Forest root domain should use NTP.

NT5DS – Synchronizes time via the domain hierarchy. Default value. All DCs and member systems should use this value.

AllSync – May attempt to use both the domain hierarchy and designated NTP servers.

NoSync – Does not synchronize time. Will prevent a DC from advertising as a time source.

Windows Anti-Virus Exclusion List

http://social.technet.microsoft.com/wiki/contents/articles/953.aspx

http://support.microsoft.com/kb/943556

http://support.microsoft.com/kb/815263

Disaster Recovery

Active Directory is one of the most critical services in a Windows network. To avoid downtime and loss of productivity, it's essential that you have effective disaster recovery plans in place for problems related to Active Directory. This point may sound obvious, but it's amazing how many administrators don't have a plan for one of the most common Active Directory failure scenarios, accidental deletion of data.

Disaster Recovery, Active Directory Users and Groups

http://technet.microsoft.com/en-us/magazine/2007.04.adrecovery.aspx

Restoring Active Directory from Backup Media

http://technet.microsoft.com/en-us/library/cc961934.aspx

Performing Authoritative Restore of Active Directory Objects

http://technet.microsoft.com/en-us/library/cc816878(WS.10).aspx

How to perform a disaster recovery restoration of Active Directory on a computer with a different hardware configuration

http://support.microsoft.com/kb/263532

Active Directory Database

What is Active Directory?

http://msdn.microsoft.com/en-us/library/windows/desktop/aa746492(v=vs.85).aspx

Force Garbage Collection

http://blogs.technet.com/b/ad/archive/2009/03/24/taking-out-the-trash.aspx

Deactivate a Schema Object Class or Attribute

http://technet.microsoft.com/en-us/library/cc794738(WS.10).aspx

Disabling Existing Classes and Attributes

http://msdn.microsoft.com/en-us/library/ms675903(VS.85).aspx

Relocating Active Directory Database Files

http://technet.microsoft.com/en-us/library/cc782948(WS.10).aspx

Performing offline defragmentation of the Active Directory database

http://support.microsoft.com/kb/232122

Trusted Domain Object (TDO)

http://technet.microsoft.com/en-us/library/cc773178(WS.10).aspx

http://msdn.microsoft.com/en-us/library/cc234329(PROT.13).aspx

TDO Contents

Each domain or forest trust within an organization is represented by a Trusted Domain Object (TDO) stored in the System container within its domain.

The information contained in a TDO can vary depending on whether a TDO was created by a domain trust or by a forest trust. When a domain trust is created, attributes such as the DNS domain name, domain SID, trust type, trust transitivity, and the reciprocal domain name are represented in the TDO. Forest trust TDOs store additional attributes to identify all of the trusted namespaces from the partner forest. These attributes include domain tree names, user principal name (UPN) suffixes, service principal name (SPN) suffixes, and security ID (SID) namespaces.

Because trusts are stored in Active Directory as TDOs, all domains in a Windows Server 2003 forest have knowledge of the trust relationships that are in place throughout the forest. Similarly, when two or more forests are joined together through forest trusts, the forest root domains in each forest have knowledge of the trust relationships that are in place throughout all of the domains in trusted Windows Server 2003 forests. External trusts to a Windows NT 4.0 domain do not create TDOs in Active Directory.

Security Principle vs Security Descriptor

Security principals include the following:

- Any entity that can be authenticated by the system, such as a user account, a computer account, or a thread or process that runs in the security context of a user or computer account.
- Security groups of these accounts.

Every security principal is automatically assigned a security identifier (SID) when it is created.

Security principals that are created in an Active Directory domain are Active Directory objects, which can be used to manage access to domain resources. Local users and security groups are created on a local computer and can be used to manage access to resources on that computer. Local user accounts and groups are managed by the Security Accounts Manager (SAM) on the local computer.

All objects in the Active Directory directory service, and all securable objects on the network, have **security descriptors** to help control access to the objects.

Security descriptors contain access control lists (ACLs), and they include information about who owns an object, who can access it and in what way, and what types of access are audited.

You can use this access control model to individually secure objects such as files and folders, Active Directory objects, registry keys, and printers, as well as devices, ports, services, processes, and threads. Because of this individual control, you can adjust the security of objects to meet the needs of your organization, delegate authority over objects or attributes, and create custom objects or attributes that require unique security protections to be defined.

http://technet.microsoft.com/en-us/library/cc779144(WS.10).aspx

Difference of Security Descriptors (ACL's) between 2000 and 2003

Single Instance Store (SIS). SIS, an improved method for storing security descriptors, reduced the size of the global catalog database from 14 GB to 9 GB

Single instance of security descriptors is basically like having child objects use pointers back to the original ACL instead of holding a separate copy of it. Single instance of security descriptors can provide up to a 40% database size reduction when moving from 2000 to 2003.

Active Directory Services

Active Directory services include:

- Active Directory Certificate Services (AD CS)
- Active Directory Domain Services (AD DS)
- Active Directory Federation Services (AD FS)
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Rights Management Services (AD RMS)

http://technet.microsoft.com/en-us/library/dd578336(v=WS.10).aspx

Active Directory Certificate Services

Organizations can use AD CS to enhance security by binding the identity of a person, device, or service to a corresponding private key. AD CS gives organizations a cost-effective, efficient, and secure way to manage the distribution and use of certificates.

The features of AD CS in Windows Server 2008 R2 include:

- Certificate enrollment that uses the HTTPS protocol.
- Certificate enrollment across Active Directory Domain Services (AD DS) forest boundaries.
- Improved support for high-volume certificate issuance.
- Support for CAs on a Server Core installation of Windows Server 2008 R2.

http://technet.microsoft.com/en-us/windowsserver/dd448615

Active Directory Certificate Services Step-by-Step Guide

http://technet.microsoft.com/en-us/library/cc772393(v=WS.10).aspx

Active Directory Domain Services

Active Directory Domain Services (AD DS) stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches. An Active Directory domain controller is a server that is running AD DS.

http://technet.microsoft.com/en-us/library/cc770946(v=ws.10).aspx

Active Directory Federation Services

Active Directory Federation Services (AD FS) is a server role in Windows Server 2008 that provides Web single-sign-on (SSO) technologies to authenticate a user to multiple Web applications over the life of a single online session.

http://technet.microsoft.com/en-us/library/cc772128(v=ws.10).aspx

Active Directory Lightweight Directory Services

Active Directory Lightweight Directory Services (AD LDS) is a Lightweight Directory Access Protocol (LDAP) directory service that provides flexible support for directory-enabled applications, without the restrictions of Active Directory Domain Services (AD DS).

http://technet.microsoft.com/en-us/library/cc731868(v=ws.10).aspx

Active Directory Rights Management Services

Active Directory Rights Management Services (AD RMS) is an information protection technology that works with AD RMS-enabled applications to help safeguard digital information from unauthorized use. Content owners can define who can open, modify, print, forward, or take other actions with the information.

http://technet.microsoft.com/en-us/library/cc771234(v=ws.10).aspx

Virtualisation

Before you turn domain controllers into virtual machines, carefully consider the advantages and disadvantages of doing this. With Hyper-V, the difference between physical machines and virtual machines is decreasing. However, there are still important factors that can help you determine whether a domain controller should be virtualized.

To install and use the Hyper-V role, you must have the following:

- An x64 processor. Hyper-V is available in x64-based versions of Windows Server 2008—specifically, the x64-based versions of Windows Server 2008 Standard, Windows Server 2008 Enterprise, and Windows Server 2008 Datacenter.

- Hardware-assisted virtualization. This feature is available in processors that include a virtualization option, specifically, Intel Virtualization Technology (Intel VT) or AMD Virtualization (AMD-V).

- Hardware Data Execution Protection (DEP). Hardware DEP must be available and enabled. Specifically, you must enable Intel XD bit (execute disable bit) or AMD NX bit (no execute bit).

You should avoid creating potential single points of failure when you plan your virtual domain controller deployment. You can avoid introducing potential single points of failure by implementing system redundancy. For example, consider the following recommendations while keeping in mind the potential for increases in the cost of administration:

- Run at least two virtualized domain controllers per domain on different virtualization hosts, which reduces the risk of losing all domain controllers if a single virtualization host fails.
- As recommended for other technologies, diversify the hardware (using different CPUs, motherboards, network adapters, or other hardware) on which the domain controllers are running. Hardware diversification limits the damage that might be caused by a malfunction that is specific to a vendor configuration, a driver, or a single piece or type of hardware.
- If possible, domain controllers should be running on hardware that is located in different regions of the world. This helps to reduce the impact of a disaster or failure that affects a site at which the domain controllers are hosted.
- Maintain physical domain controllers in each of your domains. This mitigates the risk of a virtualization platform malfunction that affects all host systems that use that platform.

Running Domain Controllers in Hyper-V

http://technet.microsoft.com/en-us/library/virtual_active_directory_domain_controller_virtualization_hyperv(v=WS.10).aspx

Domain Controllers

When you install Windows Server on a computer, you can choose to configure a specific server role for that computer. When you want to create a new forest, a new domain, or an additional domain controller in an existing domain, you configure the server with the role of domain controller by installing AD DS.

By default, a domain controller stores one domain directory partition consisting of information about the domain in which it is located, plus the schema and configuration directory partitions for the entire forest. A domain controller that runs Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 can also store one or more application directory partitions. There are also specialized domain controller roles that perform specific functions in an AD DS environment. These specialized roles include global catalog servers and operations masters.

Global Catalog Servers

Every domain controller stores the objects for the domain in which it is installed. However, a domain controller designated as a global catalog server stores the objects from all domains in the forest. For each object that is not in the domain for which the global catalog server is authoritative as a domain controller, a limited set of attributes is stored in a partial replica of the domain. Therefore, a global catalog server stores its own full, writable domain replica (all objects and all attributes) plus a partial, read-only replica of every other domain in the forest. The global catalog is built and updated automatically by the AD DS replication system. The object attributes that are replicated to global catalog servers are the attributes that are most likely to be used to search for the object in AD DS. The attributes that are replicated to the global catalog are identified in the schema as the partial attribute set (PAS) and are defined by default by Microsoft. However, to optimize searching, you can edit the schema by adding or removing attributes that are stored in the global catalog.

The global catalog makes it possible for clients to search AD DS without having to be referred from server to server until a domain controller that has the domain directory partition storing the requested object is found. By default, AD DS searches are directed to global catalog servers.

The first domain controller in a forest is automatically created as a global catalog server. Thereafter, you can designate other domain controllers to be global catalog servers if they are needed.

Operations Masters

Domain controllers that hold operations master roles are designated to perform specific tasks to ensure consistency and to eliminate the potential for conflicting entries in the Active Directory database. AD DS defines five operations master roles: the schema master, domain naming master, relative identifier (RID) master, primary domain controller (PDC) emulator, and infrastructure master.

The following operations masters perform operations that must occur on only one domain controller in the forest:

- Schema master
- Domain naming master

The following operations masters perform operations that must occur on only one domain controller in a domain:

- Primary Domain Controller (PDC) emulator
- Infrastructure master
- Relative ID (RID) master

How Domain Controllers Are Located in Windows XP

http://support.microsoft.com/kb/314861

Enabling Clients to Locate the Next Closest Domain Controller

http://technet.microsoft.com/en-us/library/cc733142(WS.10).aspx

Distributed Link Tracking on Windows-based domain controllers

http://support.microsoft.com/kb/312403

Application Considerations When Upgrading to Windows Server 2008

http://technet.microsoft.com/en-us/library/cc771576(WS.10).aspx

Users who are members of more than 1,015 groups may fail logon authentication

http://support.microsoft.com/kb/328889

RODC

A read-only domain controller (RODC) is a new type of domain controller in the Windows Server® 2008 operating system. With an RODC, organizations can easily deploy a domain controller in locations where physical security cannot be guaranteed. An RODC hosts read-only partitions of the Active Directory® Domain Services (AD DS) database.

Before the release of Windows Server 2008, if users had to authenticate with a domain controller over a wide area network (WAN), there was no real alternative. In many cases, this was not an efficient solution. Branch offices often cannot provide the adequate physical security that is required for a writable domain controller. Furthermore, branch offices often have poor network bandwidth when they are connected to a hub site. This can increase the amount of time that is required to log on. It can also hamper access to network resources.

Beginning with Windows Server 2008, an organization can deploy an RODC to address these problems. As a result, users in this situation can receive the following benefits:

- Improved security
- Faster logon times
- More efficient access to resources on the network

For more information about RODCs, see the

Read-Only Domain Controller (RODC) Planning and Deployment Guide

http://go.microsoft.com/fwlink/?LinkID=135993

RODC Technical Reference

http://technet.microsoft.com/en-us/library/cc754218(WS.10).aspx

Windows Server 2008 read-only domain controller compatibility pack for Windows Server 2003 clients and for Windows XP

http://support.microsoft.com/kb/944043

Read-Only Domain Controller Planning and Deployment Guide

http://technet.microsoft.com/en-us/library/cc771744(WS.10).aspx

Group Policy

Here are some basic terms you need to be familiar with before drilling down into Group Policy:

Local policy - Refers to the policy that configures the local computer or server, and is not inherited from the domain. You can set local policy by running *gpedit.msc* from the Run command, or you can add "Group Policy Object Editor" snap-in to MMC. Local Policies also exist in the Active Directory environment, but have many fewer configuration options that the full-fledged Group Policy in AD.

GPO - Group Policy Object - Refers to the policy that is configured at the Active Directory level and is inherited by the domain member computers. You can configure a GPO – Group Policy Object - at the site level, domain level or OU level.

GPC – Group Policy Container - The GPC is the store of the GPOs; The GPC is where the GPO stores all the AD-related configuration. Any GPO that is created is not effective until it is linked to an OU, Domain or a Site. The GPOs are replicated among the Domain Controllers of the Domain through replication of the Active Directory.

GPT - Group Policy Templates - The GPT is where the GPO stores the actual settings. The GPT is located within the Netlogon share on the DCs.

Netlogon share - A share located only on Domain Controllers and contains GPOs, scripts and .POL files for policy of Windows NT/98. The Netlogon share replicates among all DCs in the Domain, and is accessible for read only for the Everyone group, and Full Control for the Domain Admins group. The Netlogon's real location is:

C:\WINDOWS\SYSVOL\sysvol\domain.com\SCRIPTS

When a domain member computer boots up, it finds the DC and looks for the Netlogon share in it.

To see what DC the computer used when it booted, you can go to the Run command and type *%logonserver%\Netlogon*. The content of the Netlogon share should be the same on all DCs in the domain.

GPO behavior

Group Policy is processed in the following order:

Local Policy > Site GPO > Domain GPO > OU GPO > Child OU GPO

WMI Filtering, and Item-level Targeting in Group Policy Preferences

http://blogs.technet.com/b/grouppolicy/archive/2009/07/30/security-filtering-wmi-filtering-and-item-level-targeting-in-group-policy-preferences.aspx

Loopback processing of Group Policy

http://support.microsoft.com/kb/231287

Group Policy processing and precedence

http://technet.microsoft.com/en-us/library/cc785665(WS.10).aspx

Windows Server 2012

What's New in Windows Server 2012

http://technet.microsoft.com/library/hh831769

Windows Server 2012 Jump Start

A series of online videos introducing the new features and concepts in Windows Server 2012

Windows Server 2012 Jump Start (01): Core Hyper-V
Windows Server 2012 Jump Start (02a): Virtualization Infrastructure, Part 1
Windows Server 2012 Jump Start (02b): Virtualization Infrastructure, Part 2
Windows Server 2012 Jump Start (03a): Storage Architecture, Part 1
Windows Server 2012 Jump Start (03b): Storage Architecture, Part 2
Windows Server 2012 Jump Start (04): Continuous Availability
Windows Server 2012 Jump Start (05a): Multi-Server Management, Part 1
Windows Server 2012 Jump Start (05b): Multi-Server Management, Part 2
Windows Server 2012 Jump Start (06a): Security and Access, Part 1
Windows Server 2012 Jump Start (06b): Security and Access, Part 2
Windows Server 2012 Jump Start (07): Remote Connectivity and Networking
Windows Server 2012 Jump Start (08): IIS, DHCP and IPAM

Windows Server 2012 Test Lab Guides

The Windows Server 2012 Test Lab Guides (TLGs) are a set of documents that describe how to configure and demonstrate the new features and functionality in Windows Server 2012 and Windows 8 in a simplified and standardized test lab environment.

http://social.technet.microsoft.com/wiki/contents/articles/7807.windows-server-2012-test-lab-guides.aspx

Active Directory Tools

Active Directory Utilities – Codeplex (Project Hosting for Open Source Software)

http://activedirectoryutils.codeplex.com/releases/view/13664

Troubleshooting replication with repadmin

http://www.microsoft.com/download/en/details.aspx?id=9028

http://technet.microsoft.com/en-us/library/cc736571(WS.10).aspx

Troubleshooting Active Directory with ntdsutil

http://technet.microsoft.com/en-us/library/cc753343(v=WS.10).aspx

Blogs

Ask the Directory Services Team Blog

http://blogs.technet.com/b/askds/

Active Directory Blog

http://blogs.technet.com/b/ad/

AD Troubleshooting blog

http://blogs.technet.com/b/instan/

Glenn LeCheminant's weblog

http://blogs.technet.com/b/glennl/

Post-Graduate AD Studies – Even More Reading!

The Ask the Directory Services Team Blog carried an article on Post-Graduate AD Studies with some suggested reading that new hires to Microsoft are encouraged to read to fill the cracks in their Directory Service knowledge.

The full reading list can be found here:

http://blogs.technet.com/b/askds/archive/2010/07/27/post-graduate-ad-studies.aspx

Active Directory Domain Services Ramp Up Guide

http://blogs.technet.com/b/mspremuk/archive/2012/02/15/active-directory-domain-services-ramp-up-guide.aspx