Active Directory

By Contributors to Wikimedia projects

Published: 2001-12-05 · Archived: 2026-04-05 14:03:56 UTC

This article is about Microsoft's on-premises directory service. For their cloud-based system formerly known as Azure Active Directory, see Microsoft Entra ID.

Active Directory (**AD**) is a directory service developed by Microsoft for Windows domain networks. Windows Server operating systems include it as a set of processes and services.[1][2] Originally, only centralized domain management used Active Directory. However, it ultimately became an umbrella title for various directory-based identity-related services.[3]

A domain controller is a server running the **Active Directory Domain Services** (**AD DS**) role. It authenticates and authorizes all users and computers in a Windows domain-type network, assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer which is part of a Windows domain, Active Directory checks the submitted username and password and determines whether the user is a system administrator or a non-admin user.[4] Furthermore, it allows the management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services: Certificate Services, Active Directory Federation Services, Lightweight Directory Services, and Rights Management Services.[5]

Active Directory uses Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos,[6] and DNS.[7]

Robert R. King defined it in the following way:[8]

> "A domain represents a database. That database holds records about network services-things like computers, users, groups and other things that use, support, or exist on a network. The domain database is, in effect, Active Directory."

Like many information-technology efforts, Active Directory originated out of a democratization of design using Requests for Comments (RFCs). The Internet Engineering Task Force (IETF) oversees the RFC process and has accepted numerous RFCs initiated by widespread participants. For example, LDAP underpins Active Directory. Also, X.500 directories and the Organizational Unit preceded the Active Directory concept that uses those methods. The LDAP concept began to emerge even before the founding of Microsoft in April 1975, with RFCs as early as 1971. RFCs contributing to LDAP include RFC 1823 (on the LDAP API, August 1995),[9] RFC 2307, RFC 3062, and RFC 4533.[10][11][12]

Microsoft previewed Active Directory in 1999, released it first with Windows 2000 Server edition, and revised it to extend functionality and improve administration in Windows Server 2003. Active Directory support was also added to Windows 95, Windows 98, and Windows NT 4.0 via patch, with some unsupported features.[13][14]

Additional improvements came with subsequent versions of Windows Server. In Windows Server 2008, Microsoft added further services to Active Directory, such as Active Directory Federation Services.[15] The part of the directory in charge of managing domains, which was a core part of the operating system,[15] was renamed Active Directory Domain Services (ADDS) and became a server role like others.[3] "Active Directory" became the umbrella title of a broader range of directory-based services.[16] According to Byron Hynes, everything related to identity was brought under Active Directory's banner.[3]

Active Directory Services

[edit]

Active Directory Services consist of multiple directory services. The best known is Active Directory Domain Services, commonly abbreviated as AD DS or simply AD.

Active Directory Domain Services (AD DS) is the foundation of every Windows domain network. It stores information about domain members, including devices and users, verifies their credentials, and defines their access rights. The server running this service is called a domain controller. A domain controller is contacted when a user logs into a device, accesses another device across the network, or runs a line-of-business Metro-style app sideloaded into a machine.

Other Active Directory services (excluding LDS, as described below) and most Microsoft server technologies rely on or use Domain Services; examples include Group Policy, Encrypting File System, BitLocker, Domain Name Services, Remote Desktop Services, Exchange Server, and SharePoint Server.

The self-managed Active Directory DS must be distinct from managed Azure AD DS, a cloud product.[17]

Lightweight Directory Services

[edit]

Active Directory Lightweight Directory Services (AD LDS), previously called *Active Directory Application Mode* (ADAM),[18] implements the LDAP protocol for AD DS.[19] It runs as a service on Windows Server and offers the same functionality as AD DS, including an equal API. However, AD LDS does not require the creation of domains or domain controllers. It provides a Data Store for storing directory data and a *Directory Service* with an LDAP Directory Service Interface. Unlike AD DS, multiple AD LDS instances can operate on the same server.

Certificate Services

[edit]

Active Directory Certificate Services (AD CS) establishes an on-premises public key infrastructure. It can create, validate, revoke and perform other similar actions, public key certificates for internal uses of an organization. These certificates can be used to encrypt files (when used with Encrypting File System), emails (per S/MIME standard), and network traffic (when used by virtual private networks, Transport Layer Security protocol or IPSec protocol).

AD CS predates Windows Server 2008, but its name was simply Certificate Services.[20]

AD CS requires an AD DS infrastructure.[21]

Federation Services

[edit]

Active Directory Federation Services (AD FS) is a single sign-on service. With an AD FS infrastructure in place, users may use several web-based services (e.g. internet forum, blog, online shopping, webmail) or network resources using only one set of credentials stored at a central location, as opposed to having to be granted a dedicated set of credentials for each service. AD FS uses many popular open standards to pass token credentials such as SAML, OAuth or OpenID Connect.[22] AD FS supports encryption and signing of SAML assertions.[23] AD FS's purpose is an extension of that of AD DS: The latter enables users to authenticate with and use the devices that are part of the same network, using one set of credentials. The former enables them to use the same set of credentials in a different network.

As the name suggests, AD FS works based on the concept of federated identity.

AD FS requires an AD DS infrastructure, although its federation partner may not.[24]

Rights Management Services

[edit]

Active Directory Rights Management Services (**AD RMS**), previously known as Rights Management Services or RMS before Windows Server 2008, is server software that allows for information rights management, included with Windows Server. It uses encryption and selective denial to restrict access to various documents, such as corporate e-mails, Microsoft Word documents, and web pages. It also limits the operations authorized users can perform on them, such as viewing, editing, copying, saving, or printing. IT administrators can create pre-set templates for end users for convenience, but end users can still define who can access the content and what actions they can take.[25]

Active Directory is a service comprising a database and executable code. It is responsible for managing requests and maintaining the database. The Directory System Agent is the executable part, a set of Windows services and processes that run on Windows 2000 and later.[1] Accessing the objects in Active Directory databases is possible through various interfaces such as LDAP, ADSI, messaging API, and Security Accounts Manager services.[2]

A simplified example of a publishing company's internal network. The company has four groups with varying permissions to the three shared folders on the network.

Active Directory structures consist of information about objects classified into two categories: resources (such as printers) and security principals (which include user or computer accounts and groups). Each security principal is assigned a unique security identifier (SID). An object represents a single entity, such as a user, computer, printer, or group, along with its attributes. Some objects may even contain other objects within them. Each object has a unique name, and its definition is a set of characteristics and information by a schema, which determines the storage in the Active Directory.

Administrators can extend or modify the schema using the schema object when needed. However, because each schema object is integral to the definition of Active Directory objects, deactivating or changing them can fundamentally alter or disrupt a deployment. Modifying the schema affects the entire system automatically, and new objects cannot be deleted, only deactivated. Changing the schema usually requires planning.[26]

Forests, trees, and domains

[edit]

In an Active Directory network, the framework that holds objects has different levels: the forest, tree, and domain. Domains within a deployment contain objects stored in a single replicable database, and the DNS name structure identifies their domains, the namespace. A domain is a logical group of network objects such as computers, users, and devices that share the same Active Directory database.

On the other hand, a tree is a collection of domains and domain trees in a contiguous namespace linked in a transitive trust hierarchy. The forest is at the top of the structure, a collection of trees with a standard global catalog, directory schema, logical structure, and directory configuration. The forest is a secure boundary that limits access to users, computers, groups, and other objects.

Organizational units

[edit]

The objects held within a domain can be grouped into organizational units (OUs).[27] OUs can provide hierarchy to a domain, ease its administration, and can resemble the organization's structure in managerial or geographical terms. OUs can contain other OUs—domains are containers in this sense. Microsoft recommends using OUs

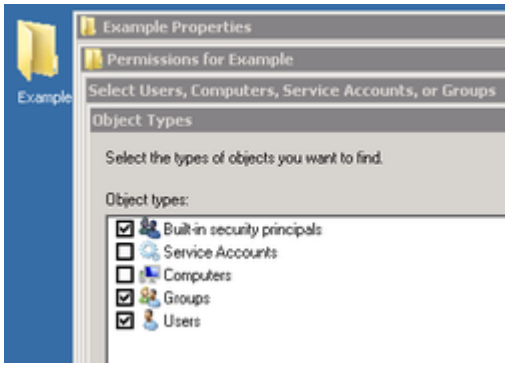
rather than domains for structure and simplifying the implementation of policies and administration. The OU is the recommended level at which to apply group policies, which are Active Directory objects formally named group policy objects (GPOs), although policies can also be applied to domains or sites (see below). The OU is the level at which administrative powers are commonly delegated, but delegation can be performed on individual objects or attributes as well.

Organizational units do not each have a separate namespace. As a consequence, for compatibility with Legacy NetBios implementations, user accounts with an identical SamAccountName are not allowed within the same domain even if the accounts objects are in separate OUs. This is because SamAccountName, a user object attribute, must be unique within the domain.[28] However, two users in different OUs can have the same common name (CN), the name under which they are stored in the directory itself such as "fred.staff-ou.domain" and "fred.student-ou.domain", where "staff-ou" and "student-ou" are the OUs.

In general, the reason for this lack of allowance for duplicate names through hierarchical directory placement is that Microsoft primarily relies on the principles of NetBIOS, which is a flat-namespace method of network object management that, for Microsoft software, goes all the way back to Windows NT 3.1 and MS-DOS LAN Manager. Allowing for duplication of object names in the directory, or completely removing the use of NetBIOS names, would prevent backward compatibility with legacy software and equipment. However, disallowing duplicate object names in this way is a violation of the LDAP RFCs on which Active Directory is supposedly based.

As the number of users in a domain increases, conventions such as "first initial, middle initial, last name" (Western order) or the reverse (Eastern order) fail for common family names like *Li* (李), *Smith* or *Garcia*. Workarounds include adding a digit to the end of the username. Alternatives include creating a separate ID system of unique employee/student ID numbers to use as account names in place of actual users' names and allowing users to nominate their preferred word sequence within an acceptable use policy.

Because duplicate usernames cannot exist within a domain, account name generation poses a significant challenge for large organizations that cannot be easily subdivided into separate domains, such as students in a public school system or university who must be able to use any computer across the network.



In Active Directory, organizational units (OUs) cannot be assigned as owners or trustees. Only groups are selectable, and members of OUs cannot be collectively assigned rights to directory objects.

In Microsoft's Active Directory, OUs do not confer access permissions, and objects placed within OUs are not automatically assigned access privileges based on their containing OU. It represents a design limitation specific to

Active Directory, and other competing directories, such as Novell NDS, can set access privileges through object placement within an OU.

Active Directory requires a separate step for an administrator to assign an object in an OU as a group member also within that OU. Using only the OU location to determine access permissions is unreliable since the entity might not have been assigned to the group object for that OU yet.

A common workaround for an Active Directory administrator is to write a custom PowerShell or Visual Basic script to automatically create and maintain a *user group* for each OU in their Directory. The scripts run periodically to update the group to match the OU's account membership. However, they cannot instantly update the security groups anytime the directory changes, as occurs in competing directories, as security is directly implemented into the Directory. Such groups are known as *shadow groups*. Once created, these shadow groups are selectable in place of the OU in the administrative tools. Microsoft's Server 2008 reference documentation mentions shadow groups but does not provide instructions on creating them. Additionally, there are no available server methods or console snap-ins for managing these groups.[29]

An organization must determine the structure of its information infrastructure by dividing it into one or more domains and top-level OUs. This decision is critical and can base on various models such as business units, geographical locations, IT service, object type, or a combination of these models. The immediate purpose of organizing OUs is to simplify administrative delegation and, secondarily, to apply group policies. While OUs serve as an administrative boundary, the forest itself is the only security boundary. All other domains must trust any administrator in the forest to maintain security.[30]

The Active Directory database is organized in *partitions*, each holding specific object types and following a particular replication pattern. Microsoft often refers to these partitions as 'naming contexts.[31] The 'Schema' partition defines object classes and attributes within the forest. The 'Configuration' partition contains information on the physical structure and configuration of the forest (such as the site topology). Both replicate all domains in the forest. The 'Domain' partition holds all objects created in that domain and replicates only within it.

Sites are physical (rather than logical) groupings defined by one or more IP subnets.[32] AD also defines connections, distinguishing low-speed (e.g., WAN, VPN) from high-speed (e.g., LAN) links. Site definitions are independent of the domain and OU structure and are shared across the forest. Sites play a crucial role in managing network traffic created by replication and directing clients to their nearest domain controllers (DCs). Microsoft Exchange Server 2007 uses the site topology for mail routing. Administrators can also define policies at the site level.

The Active Directory information is physically held on one or more peer domain controllers, replacing the NT PDC/BDC model. Each DC has a copy of the Active Directory. Member servers joined to Active Directory that are not domain controllers are called Member Servers.[33] In the domain partition, a group of objects acts as copies of domain controllers set up as global catalogs. These global catalog servers offer a comprehensive list of all objects in the forest.[34][35]

Global Catalog servers replicate all objects from all domains to themselves, providing an international listing of entities in the forest. However, to minimize replication traffic and keep the GC's database small, only selected

attributes of each object are replicated, called the *partial attribute set* (PAS). The PAS can be modified by modifying the schema and marking features for replication to the GC.[36] Earlier versions of Windows used NetBIOS to communicate. Active Directory is fully integrated with DNS and requires TCP/IP—DNS. To fully operate, the DNS server must support SRV resource records, also known as service records.

Active Directory uses multi-master replication to synchronize changes,[37] meaning replicas pull changes from the server where the change occurred rather than being pushed to them.[38] The Knowledge Consistency Checker (KCC) uses defined sites to manage traffic and create a replication topology of site links. Intra-site replication occurs frequently and automatically due to change notifications, which prompt peers to begin a pull replication cycle. Replication intervals between different sites are usually less consistent and don't usually use change notifications. However, it's possible to set it up to be the same as replication between locations on the same network if needed.

Each DS3, T1, and ISDN link can have a cost, and the KCC alters the site link topology accordingly. Replication may occur transitively through several site links on same-protocol *site link bridges* if the price is low. However, KCC automatically costs a direct site-to-site link lower than transitive connections. A bridgehead server in each zone can send updates to other DCs in the exact location to replicate changes between sites. To configure replication for Active Directory zones, activate DNS in the domain based on the site.

To replicate Active Directory, Remote Procedure Calls (RPC) over IP (RPC/IP) are used. SMTP is used to replicate between sites but only for modifications in the Schema, Configuration, or Partial Attribute Set (Global Catalog) GCs. It's not suitable for reproducing the default Domain partition.[39]

Generally, a network utilizing Active Directory has more than one licensed Windows server computer. Backup and restore of Active Directory are possible for a network with a single domain controller.[40] However, Microsoft recommends more than one domain controller to provide automatic failover protection of the directory.[41] Domain controllers are ideally single-purpose for directory operations only and should not run any other software or role.[42]

Since certain Microsoft products, like SQL Server[43][44] and Exchange,[45] can interfere with the operation of a domain controller, isolation of these products on additional Windows servers is advised. Combining them can complicate the configuration and troubleshooting of the domain controller or the other installed software more complex.[46] If planning to implement Active Directory, a business should purchase multiple Windows server licenses to have at least two separate domain controllers. Administrators should consider additional domain controllers for performance or redundancy and individual servers for tasks like file storage, Exchange, and SQL Server[47] since this will guarantee that all server roles are adequately supported.

One way to lower the physical hardware costs is by using virtualization. However, for proper failover protection, Microsoft recommends not running multiple virtualized domain controllers on the same physical hardware.[48]

The Active-Directory database, the *directory store*, in Windows 2000 Server uses the JET Blue-based Extensible Storage Engine (ESE98). Each domain controller's database is limited to 16 terabytes and 2 billion objects (but only 1 billion security principals). Microsoft has created NTDS databases with more than 2 billion objects.[49]

NT4's Security Account Manager could support up to 40,000 objects. It has two main tables: the *data table* and the *link table*. Windows Server 2003 added a third main table for security descriptor single instancing.[49]

Programs may access the features of Active Directory[50] via the COM interfaces provided by *Active Directory Service Interfaces*.[51]

To allow users in one domain to access resources in another, Active Directory uses trusts.[52]

Trusts inside a forest are automatically created when domains are created. The forest sets the default boundaries of trust, and implicit, transitive trust is automatic for all domains within a forest.

One-way trust
: One domain allows access to users on another domain, but the other domain does not allow access to users on the first domain.

Two-way trust
: Two domains allow access to users on both domains.

Trusted domain
: The domain that is trusted; whose users have access to the trusting domain.

Transitive trust
: A trust that can extend beyond two domains to other trusted domains in the forest.

Intransitive trust
: A one way trust that does not extend beyond two domains.

Explicit trust
: A trust that an admin creates. It is not transitive and is one way only.

Cross-link trust
: An explicit trust between domains in different trees or the same tree when a descendant/ancestor (child/parent) relationship does not exist between the two domains.

Shortcut
: Joins two domains in different trees, transitive, one- or two-way.

Forest trust
: Applies to the entire forest. Transitive, one- or two-way.

Realm
: Can be transitive or nontransitive (intransitive), one- or two-way.

External
: Connect to other forests or non-Active Directory domains. Nontransitive, one- or two-way.[53]

PAM trust
: A one-way trust used by Microsoft Identity Manager from a (possibly low-level) production forest to a (Windows Server 2016 functionality level) 'bastion' forest, which issues time-limited group memberships.[54][55]

Microsoft Active Directory management tools include:

- Active Directory Administrative Center (Introduced with Windows Server 2012 and above),
- Active Directory Users and Computers,

- Active Directory Domains and Trusts,
- Active Directory Sites and Services,
- ADSI Edit,
- Local Users and Groups,
- Active Directory Schema snap-ins for Microsoft Management Console (MMC),
- SysInternals ADExplorer.

These management tools may not provide enough functionality for efficient workflow in large environments. Some third-party tools extend the administration and management capabilities. They provide essential features for a more convenient administration process, such as automation, reports, integration with other services, etc.

Varying levels of interoperability with Active Directory can be achieved on most Unix-like operating systems (including Unix, Linux, Mac OS X or Java and Unix-based programs) through standards-compliant LDAP clients, but these systems usually do not interpret many attributes associated with Windows components, such as Group Policy and support for one-way trusts.

Third parties offer Active Directory integration for Unix-like platforms, including:

- *PowerBroker Identity Services*, formerly *Likewise* (BeyondTrust, formerly Likewise Software) – Allows a non-Windows client to join Active Directory[56]
- *ADmitMac* (Thursby Software Systems)[56]
- *Samba* (free software under GPLv3) – Can act as a fully functional Active Directory[57][58]

The schema additions shipped with Windows Server 2003 R2 include attributes that map closely enough to RFC 2307 to be generally usable. The reference implementation of RFC 2307, nss_ldap and pam_ldap provided by PADL.com, support these attributes directly. The default schema for group membership complies with RFC 2307bis (proposed).[59] Windows Server 2003 R2 includes a Microsoft Management Console snap-in that creates and edits the attributes.

An alternative option is to use another directory service as non-Windows clients authenticate to this while Windows Clients authenticate to Active Directory. Non-Windows clients include 389 Directory Server (formerly Fedora Directory Server, FDS), ViewDS v7.2 XML Enabled Directory, and Sun Microsystems Sun Java System Directory Server. The latter two are both able to perform two-way synchronization with Active Directory and thus provide a "deflected" integration.

Another option is to use OpenLDAP with its *translucent* overlay, which can extend entries in any remote LDAP server with additional attributes stored in a local database. Clients pointed at the local database see entries containing both the remote and local attributes, while the remote database remains completely untouched.[*citation needed*]

Administration (querying, modifying, and monitoring) of Active Directory can be achieved via many scripting languages, including PowerShell, VBScript, JScript/JavaScript, Perl, Python, and Ruby.[60][61][62][63] Free and non-free Active Directory administration tools can help to simplify and possibly automate Active Directory management tasks.

Since October 2017 Amazon AWS offers integration with Microsoft Active Directory.[64]

- AGDLP (implementing role based access controls using nested groups)
- Apple Open Directory
- Flexible single master operation
- FreeIPA
- List of LDAP software
- System Security Services Daemon (SSSD)
- Univention Corporate Server

1. ^ Jump up to: *a* *b* *"Directory System Agent"*. *MSDN Library*. *Microsoft*. *Retrieved 23 April 2014.*
2. ^ Jump up to: *a* *b* *Solomon, David A.; Russinovich, Mark (2005). "Chapter 13". Microsoft Windows Internals: Microsoft Windows Server 2003, Windows XP, and Windows 2000 (4th ed.). Redmond, Washington: Microsoft Press. p. 840. ISBN 0-7356-1917-4.*
3. ^ Jump up to: *a* *b* *c* *Hynes, Byron (November 2006). "The Future of Windows: Directory Services in Windows Server "Longhorn"". TechNet Magazine. Microsoft. Archived from the original on 30 April 2020. Retrieved 30 April 2020.*
4. ^ *"Active Directory on a Windows Server 2003 Network". Active Directory Collection. Microsoft. 13 March 2003. Archived from the original on 30 April 2020. Retrieved 25 December 2010.*
5. ^ *Rackspace Support (27 April 2016). "Install Active Directory Domain Services on Windows Server 2008 R2 Enterprise 64-bit". Rackspace. Rackspace US, Inc. Archived from the original on 30 April 2020. Retrieved 22 September 2016.*
6. ^ *"Microsoft Kerberos - Win32 apps". docs.microsoft.com. 7 January 2021.*
7. ^ *"Domain Name System (DNS)". docs.microsoft.com. 10 January 2022.*
8. ^ *King, Robert (2003). Mastering Active directory for Windows server 2003 (3rd ed.). Alameda, Calif.: Sybex. p. 159. ISBN 978-0-7821-5201-2. OCLC 62876800.*
9. ^ *Howes, T.; Smith, M. (August 1995). "The LDAP Application Program Interface". The Internet Engineering Task Force (IETF). Archived from the original on 30 April 2020. Retrieved 26 November 2013.*
10. ^ *Howard, L. (March 1998). "An Approach for Using LDAP as a Network Information Service". Internet Engineering Task Force (IETF). Archived from the original on 30 April 2020. Retrieved 26 November 2013.*
11. ^ *Zeilenga, K. (February 2001). "LDAP Password Modify Extended Operation". The Internet Engineering Task Force (IETF). Archived from the original on 30 April 2020. Retrieved 26 November 2013.*
12. ^ *Zeilenga, K.; Choi, J.H. (June 2006). "The Lightweight Directory Access Protocol (LDAP) Content Synchronization Operation". The Internet Engineering Task Force (IETF). Archived from the original on 30 April 2020. Retrieved 26 November 2013.*
13. ^ *Daniel Petri (8 January 2009). "Active Directory Client (dsclient) for Win98/NT".*
14. ^ *"Dsclient.exe connects Windows 9x/NT PCs to Active Directory". 5 June 2003.*
15. ^ Jump up to: *a* *b* *Thomas, Guy (29 November 2000). "Windows Server 2008 - New Features". ComputerPerformance.co.uk. Computer Performance Ltd. Archived from the original on 2 September 2019. Retrieved 30 April 2020.*

16. ^ *"What's New in Active Directory in Windows Server"*. *Windows Server 2012 R2 and Windows Server 2012 Tech Center. Microsoft. 31 August 2016.*
17. ^ *"Compare Active Directory-based services in Azure"*. *docs.microsoft.com. 3 April 2023.*
18. ^ *"AD LDS"*. *Microsoft. Retrieved 28 April 2009.*
19. ^ *"AD LDS versus AD DS"*. *Microsoft. 2 July 2012. Retrieved 25 February 2013.*
20. ^ *Zacker, Craig (2003). "11: Creating and Managing Digital Certificates". In Harding, Kathy; Jean, Trenary; Linda, Zacker (eds.). Planning and Maintaining a Microsoft Windows server 2003 Network Infrastructure. Redmond, WA: Microsoft Press. pp. 11–16. ISBN 0-7356-1893-3.*
21. ^ *"Active Directory Certificate Services Overview". Microsoft TechNet. Microsoft. Retrieved 24 November 2015.*
22. ^ *"Overview of authentication in Power Apps portals". Microsoft Docs. Microsoft. Retrieved 30 January 2022.*
23. ^ *"How to Replace the SSL, Service Communications, Token-Signing, and Token-Decrypting Certificates". TechNet. Microsoft. Retrieved 30 January 2022.*
24. ^ *"Step 1: Preinstallation Tasks". TechNet. Microsoft. Retrieved 21 October 2021.*
25. ^ *"Test Lab Guide: Deploying an AD RMS Cluster". Microsoft Docs. Microsoft. 31 August 2016. Retrieved 30 January 2022.*
26. ^ *Windows Server 2003: Active Directory Infrastructure. Microsoft Press. 2003. pp. 1–8–1–9.*
27. ^ *"Organizational Units". Distributed Systems Resource Kit (TechNet). Microsoft. 2011. "An organizational unit in* ***Active Directory*** *is analogous to a directory in the file system"*
28. ^ *"SamAccountName is always unique in a Windows domain... or is it?". Joeware. 4 January 2012. Retrieved 18 September 2013. "examples of how multiple AD objects can be created with the same SamAccountName"*
29. ^ Microsoft Server 2008 Reference, discussing shadow groups used for fine-grained password policies: https://technet.microsoft.com/en-us/library/cc770394%28WS.10%29.aspx
30. ^ *"Specifying Security and Administrative Boundaries". Microsoft Corporation. 23 January 2005. "However, service administrators have abilities that cross domain boundaries. For this reason, the forest is the ultimate security boundary, not the domain."*
31. ^ *Andreas Luther (9 December 2009). "Active Directory Replication Traffic". Microsoft Corporation. Retrieved 26 May 2010. "The Active Directory is made up of one or more naming contexts or partitions."*
32. ^ *"Sites overview". Microsoft Corporation. 21 January 2005. "A site is a set of well-connected subnets."*
33. ^ *"Planning for domain controllers and member servers". Microsoft Corporation. 21 January 2005. "[...] member servers, [...] belong to a domain but do not contain a copy of the Active Directory data."*
34. ^ *"What Is the Global Catalog?". Microsoft Corporation. 10 December 2009. "[...] a domain controller can locate only the objects in its domain. [...] The global catalog provides the ability to locate objects from any domain [...]"*
35. ^ *"Global Catalog". Microsoft Corporation.*
36. ^ *"Attributes Included in the Global Catalog". Microsoft Corporation. 26 August 2010. "The isMemberOfPartialAttributeSet attribute of an attributeSchema object is set to TRUE if the attribute is replicated to the global catalog. [...] When deciding whether or not to place an attribute in the global catalog remember that you are trading increased replication and increased disk storage on global catalog servers for, potentially, faster query performance."*

37. ^ *"Directory data store". Microsoft Corporation. 21 January 2005. "Active Directory uses four distinct directory partition types to store [...] data. Directory partitions contain domain, configuration, schema, and application data."*
38. ^ *"What Is the Active Directory Replication Model?". Microsoft Corporation. 28 March 2003. "Domain controllers request (pull) changes rather than send (push) changes that might not be needed."*
39. ^ *"What Is Active Directory Replication Topology?". Microsoft Corporation. 28 March 2003. "SMTP can be used to transport nondomain replication [...]"*
40. ^ *"Active Directory Backup and Restore". TechNet. Microsoft. 9 December 2009. Retrieved 5 February 2014.*
41. ^ *"AD DS: All domains should have at least two functioning domain controllers for redundancy". TechNet. Microsoft. Retrieved 5 February 2014.*
42. ^ *Posey, Brien (23 August 2010). "10 tips for effective Active Directory design". TechRepublic. CBS Interactive. Retrieved 5 February 2014. "Whenever possible, your domain controllers should run on dedicated servers (physical or virtual)."*
43. ^ *"You may encounter problems when installing SQL Server on a domain controller (Revision 3.0)". Support. Microsoft. 7 January 2013. Retrieved 5 February 2014.*
44. ^ *Degremont, Michel (30 June 2011). "Can I install SQL Server on a domain controller?". Microsoft SQL Server blog. Retrieved 5 February 2014. "For security and performance reasons, we recommend that you do not install a standalone SQL Server on a domain controller."*
45. ^ *"Installing Exchange on a domain controller is not recommended". TechNet. Microsoft. 22 March 2013. Retrieved 5 February 2014.*
46. ^ *"Security Considerations for a SQL Server Installation". TechNet. Microsoft. Retrieved 5 February 2014. "After SQL Server is installed on a computer, you cannot change the computer from a domain controller to a domain member. You must uninstall SQL Server before you change the host computer to a domain member."*
47. ^ *"Exchange Server Analyzer". TechNet. Microsoft. Retrieved 5 February 2014. "Running SQL Server on the same computer as a production Exchange mailbox server is not recommended."*
48. ^ *"Running Domain Controllers in Hyper-V". TechNet. Microsoft. Planning to Virtualize Domain Controllers. Retrieved 5 February 2014. "You should attempt to avoid creating potential single points of failure when you plan your virtual domain controller deployment.frank"*
49. ^ Jump up to: ***a*** ***b*** *efleis (8 June 2006). "Large AD database? Probably not this large". Blogs.technet.com. Archived from the original on 17 August 2009. Retrieved 20 November 2011.*
50. ^ *Berkouwer, Sander. "Active Directory basics". Veeam Software.*
51. ^ Active Directory Service Interfaces, Microsoft
52. ^ *"Domain and Forest Trusts Technical Reference". Microsoft Corporation. 28 March 2003. "Trusts enable [...] authentication and [...] sharing resources across domains or forests"*
53. ^ *"Domain and Forest Trusts Work". Microsoft Corporation. 11 December 2012. Retrieved 29 January 2013. "Defines several kinds of trusts. (automatic, shortcut, forest, realm, external)"*
54. ^ *"Privileged Access Management for Active Directory Domain Services". docs.microsoft.com. 8 February 2023.*
55. ^ *"TechNet Wiki". social.technet.microsoft.com. 17 January 2024.*

56. ^ Jump up to: *a b* *Edge, Charles S. Jr; Smith, Zack; Hunter, Beau (2009). "Chapter 3: Active Directory". Enterprise Mac Administrator's Guide. New York City: Apress. ISBN 978-1-4302-2443-3.*
57. ^ *"Samba 4.0.0 Available for Download". SambaPeople. SAMBA Project. Archived from the original on 15 November 2010. Retrieved 9 August 2016.*
58. ^ *"The great DRS success!". SambaPeople. SAMBA Project. 5 October 2009. Archived from the original on 13 October 2009. Retrieved 2 November 2009.*
59. ^ *"RFC 2307bis". Archived from the original on 27 September 2011. Retrieved 20 November 2011.*
60. ^ *"Active Directory Administration with Windows PowerShell". Microsoft. Retrieved 7 June 2011.*
61. ^ *"Using Scripts to Search Active Directory". Microsoft. 26 May 2010. Retrieved 22 May 2012.*
62. ^ *"ITAdminTools Perl Scripts Repository". ITAdminTools.com. Retrieved 22 May 2012.*
63. ^ *"Win32::OLE". Perl Open-Source Community. Retrieved 22 May 2012.*
64. ^ *"Introducing AWS Directory Service for Microsoft Active Directory (Standard Edition)". Amazon Web Services. 24 October 2017.*

- Microsoft Technet: White paper: Active Directory Architecture (Single technical document that gives an overview about Active Directory.)
- Microsoft Technet: Detailed description of Active Directory on Windows Server 2003
- Microsoft MSDN Library: [MS-ADTS]: Active Directory Technical Specification (part of the Microsoft Open Specification Promise)
- Active Directory Application Mode (ADAM)
- Microsoft MSDN: [AD-LDS]: Active Directory Lightweight Directory Services
- Microsoft TechNet: [AD-LDS]: Active Directory Lightweight Directory Services
- Microsoft MSDN: Active Directory Schema
- Microsoft TechNet: Understanding Schema
- Microsoft TechNet Magazine: Extending the Active Directory Schema
- Microsoft MSDN: Active Directory Certificate Services
- Microsoft TechNet: Active Directory Certificate Services
