Active Directory Collection

Article • 11/19/2014 • 14 minutes to read

In this article

Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2

Active Directory Domain Services Collection

Active Directory Domain Services (AD DS) directory service is the distributed directory service that is included with Microsoft Windows Server operating systems. AD DS enables centralized, secure management of an entire network, which might span a building, a city, or multiple locations throughout the world.

AD DS includes the following:

- AD DS on a Windows Server Network

- Active Directory Lightweight Directory Services (AD LDS)
- Structure and Storage Technologies
- Domain Controller Roles
- Replication Technologies
- Search and Publication Technologies
- Installation, Upgrade, and Migration Technologies

In distributed computing environments, networked computers and other devices communicate over remote connections to accomplish tasks through client/server applications. Distributed environments require a central repository of information and integrated services that provide the means to manage network users, services, devices, and additional information that administrators want to store.

Organizations operating a distributed environment need to have a way to manage network resources and services. As the organization grows, the need for a secure and centralized management system becomes more critical.

A directory service provides a centralized location to store information in a distributed environment about networked devices and services and the people who use them. A directory service also implements the services that make this information available to users, computers, and applications. A directory service is both a database storage system (directory store) and a set of services that provide the means to securely add, modify, delete, and locate data in the directory store.

AD DS is typically used for one of three purposes:

- Internal directory. Used within the corporate network for publishing information about users and resources within the enterprise. A company's internal directory may be accessible to employees when they are outside the company network using a secure connection such as a virtual private network (VPN) connection, but it is not accessible to non-employees.
- External directory. These are directories typically located on servers in the perimeter network or demilitarized zone (DMZ) at the boundary between the corporate local area network (LAN) and the public Internet. External directories are

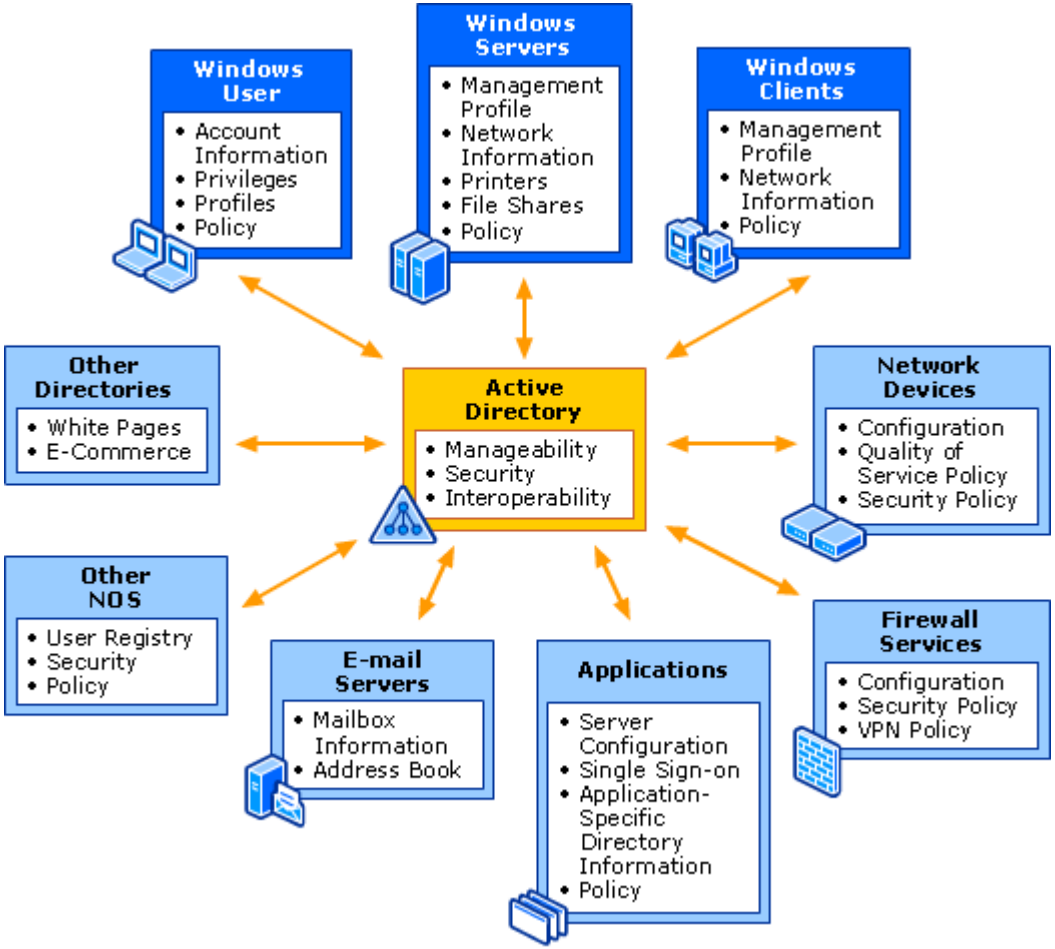
typically used to store information about customers, clients, and business partners who access external applications or services. They are also made available to customers, clients, and business partners to provide them with selected business information such as catalogs and so on.

- Application directory. Application directories store “private” directory data that is relevant only to the application in a local directory, perhaps on the same server as the application, without requiring any additional configuration to Active Directory. The personalization data, which is only interesting to the portal application and does not need to be widely replicated, can be stored solely in the directory associated with the application. This solution reduces replication traffic on the network between domain controllers.

AD DS on a Windows Server Network

AD DS is the information hub of the operating system. The following figure shows AD DS as the focal point of the Windows Server network used to manage identities and broker relationships between distributed resources so they can work together.

Active Directory on a Windows Server Network



Active Directory provides:

- A central location for network administration and delegation of administrative authority. You have access to objects representing all network users, devices, and resources and the ability to group objects for ease of management and application of security and Group Policy.
- Information security and single sign-on for user access to network resources. Tight integration with security eliminates costly tracking of accounts for authentication and authorization between systems. A single user name and password combination can identify each network user, and this identity follows the user throughout the network.

- Scalability. AD DS includes one or more domains, each with one or more domain controllers, enabling you to scale the directory to meet any network requirements.
- Flexible and global searching. Users and administrators can use desktop tools to search AD DS. By default, searches are directed to the global catalog, which provides forest-wide search capabilities.
- Storage for application data. AD DS provides a central location to store data that is shared between applications and with applications that need to distribute their data across entire Windows networks.
- Systematic synchronization of directory updates. Updates are distributed throughout the network through secure and cost-efficient replication between domain controllers.
- Remote administration. You can connect to any domain controller remotely from any Windows-based computer that has administrative tools installed.
- Single, modifiable, and extensible schema. The schema is a set of objects and rules that provide the structure requirements for AD DS objects. You can modify the schema to implement new types of objects or object properties.
- Integration of object names with Domain Name System (DNS), the Internet-standard computer location system. AD DS uses DNS to implement an IP-based naming system so that AD DS services and domain controllers are locatable over standard IP both on intranets and the Internet.
- Lightweight Directory Access Protocol (LDAP) support. LDAP is the industry standard directory access protocol, making AD DS widely accessible to management and query applications. AD DS supports LDAPv3 and LDAPv2.

Active Directory Lightweight Directory Services (AD LDS)

Active Directory Lightweight Directory Services (AD LDS) is a directory service designed to meet the needs of organizations that cannot rely solely on AD DS to provide directory services for directory-enabled applications. While AD DS offers many benefits for managing network infrastructure, organizations often need a more flexible directory service to support directory-

enabled applications. AD LDS is a Lightweight Directory Access Protocol (LDAP) directory service designed specifically for directory-enabled applications.

Structure and Storage Technologies

AD DS uses domains and forests to represent the logical structure of the directory hierarchy. Domains are used to manage the various populations of users, computers, and network resources in your enterprise. The forest represents the security boundary for AD DS. Within domains you can create organizational units to subdivide the various divisions of administration.

The logical structure of AD DS includes a two-dimensional definition that can be viewed as a hierarchy, even though the objects themselves are stored in a flat database file. In addition to its own name, each object stores the name of the container directly above it in the hierarchy. That container object stores the name of its superior container, and so on, up to the root container. In this way, a logical structure is imposed that can be viewed by using AD DS tools as a tree of containers. By virtue of a hierarchical naming system, the objects in the tree appear to be nested inside (contained by) other objects.

The AD DS schema defines the types of objects that are available to the directory service. The schema is stored in the schema partition, which is also defined as an object in the directory. The attributes and classes in AD DS are stored in the schema partition as directory objects called schema objects. It is possible for Administrators to add their own classes or attributes to an existing object type. However, the default schema provides all of the classes and attributes that AD DS needs to function.

AD DS uses objects to store and reference data in the directory. The AD DS database file (Ntds.dit) provides the physical storage of all AD DS objects for a single forest. Although there is a single directory, some directory data is stored within domains while other data is distributed throughout the forest, without regard for domain boundaries. Beginning with Windows Server 2003, data can also be distributed to domain controllers according to applications that use the data, where the scope of distribution can be set according to the needs of the application.

Any updates made to data in the directory are automatically distributed to the appropriate domain controllers by means of AD DS replication. By replicating data according to directory partitions, AD DS provides a data repository that is logically

centralized (maintains a single point of administration) but physically distributed (is synchronized on multiple domain controllers throughout the network).

Replication Technologies

Objects in the directory are distributed among the domain controllers in a forest, and all domain controllers can be updated directly. AD DS replication is the process by which the changes that are made on one domain controller are automatically synchronized with other domain controllers. Data integrity is maintained by tracking changes on each domain controller and updating other domain controllers in a systematic way. By default, AD DS replication uses a connection topology that is created automatically. This replication topology makes optimal use of physical network connections and frees administrators from having to determine which domain controllers replicate with one another. The replication topology can also be created manually. AD DS replication is designed to maximize directory consistency and minimize the impact to network traffic.

Domain Controller Roles

A domain controller is a server that has the AD DS server role installed.

Note

- Implementations of Microsoft Windows NT 3.51 and Microsoft Windows NT 4.0 operating systems also have domain controllers, but they do not support AD DS.

When you install Windows Server on a computer, you can choose to configure a 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 as a 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 can also store one or more application directory partitions.

Whereas every domain controller stores the objects for only one domain, a domain controller that is 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 a corresponding domain. The partial replicas on a global catalog server are not writable — you cannot update an object in a partial replica on a global catalog server, but only on a domain controller that stores a full replica. Thus 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 attributes that are replicated to the global catalog servers are the attributes that are most likely to be used to search for the object in AD DS. These attributes are identified by default in the schema as being included in the partial attribute set of 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 the domain controller that has the domain that stores 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.

All domain controllers can receive updates to any writable object that they store (with the exception of schema updates, which can be made only on the one domain controller in the forest that has the role of schema master). The day-to-day operations that are associated with managing users, groups, and computers are typically multimaster operations — that is, changes to these objects can be made on any domain controller. When a client application updates an object on a domain controller, the domain controller automatically replicates the change to all other domain controllers in the same domain if the change is a domain change or to all other domain controllers in the forest if the change is a configuration or schema change.

There are some operations, however, that are not performed as multimaster operations because they must occur at only one place and time. For these operations, there are specially designated domain controllers that manage the operations singly. Some master operations, required at the forest level, include the schema master and the domain naming master. Others, required at the domain level, include the PDC emulator, RID master and infrastructure master. Domain controllers that hold these special roles are called operations masters.

Search and Publication Technologies

Successful operation of an AD DS forest depends on clients and services being able to locate domain controllers. The success of domain controller location depends on the registration of information in DNS and the availability of that information. AD DS uses DNS to locate networked computers by resolving computer names to IP addresses. The Net Logon service on domain clients and domain controllers interacts with Windows server application programming interfaces (APIs) and DNS to provide a domain controller locator service (Locator). Locator finds requested service-specific and site-specific domain controllers.

After a domain controller has been located, LDAP is used to retrieve information from the directory. AD DS stores objects that provide information about the real objects that exist in an organization's network and that are associated with one or more domains, such as users, specific groups of users, computers, applications, services, files, and distribution lists. AD DS makes this information available to administrators, network users, and applications throughout the organization through LDAP. LDAP enables clients to query, create, update, and delete information stored in a directory service. The LDAP protocol is the AD DS core protocol, and is the preferred and most common way of interacting with AD DS.

The creation, storage, and maintenance of information in AD DS is called service publication. Directory-enabled services and applications can publish globally useful information, such as service availability and properties, in AD DS. This allows client processes to find and connect to any directory-enabled service as needed, and network clients and administrators to find, connect to, and manage services.

Installation, Upgrade, and Migration Technologies

The installation or removal of AD DS is performed by the Active Directory Installation Wizard. Before installing AD DS on a server, the wizard will verify that the server is eligible to run AD DS. After the prerequisites have been met, a user interface is used to gather information specific to the environment in which AD DS will be installed. Finally, the wizard configures the directory service, making the server a domain controller.

Part of the directory configuration process includes configuring the AD DS schema. The schema contains a master list of all classes (object types) and attributes that can be used in the directory. The Active Directory Preparation Tool (ADPrep) is used to prepare an AD DS forest and domain for a newer version of the directory service. One of several tasks accomplished by ADPrep is updating the AD DS schema. If you do not prepare your AD DS infrastructure, the upgrade will fail.

After installing or upgrading AD DS, you can enable the appropriate domain or forest functional level based on an assessment of your current environment. The functional level of a domain or forest defines the set of advanced AD DS features that are available in that domain or forest. The functional level of a domain or forest also defines the set of Windows operating systems that can run on the domain controllers in that domain or forest. Functional levels provide configuration support for the AD DS features and ensure compatibility with domain controllers running earlier operating systems.

Depending on the design of your environment, you might opt to restructure it instead of upgrading. For example, if your Windows NT 4.0 environment consists of multiple domains, rather than upgrading each domain it might be more productive to restructure the environment by consolidating some of those domains. Or if your Windows 2000 environment was poorly designed and you are upgrading your environment to Windows Server 2003, it might benefit you to restructure your existing environment before or after the upgrade takes place. You can perform either of these tasks by using the Active Directory Migration Tool (ADMT). ADMT includes wizards that automate migration tasks such as copying users, groups, and service accounts; moving computers; migrating trusts; and performing security translation. When you use ADMT to restructure Windows NT 4.0 domains, ADMT copies the accounts that are migrated, so that when the accounts are created in the target domain, they continue to exist in the source domain. The primary security identifiers (SIDs) for the accounts can be migrated to the SID history in the target domain. SID history maintains resource permissions when you migrate accounts, thus enabling access to resources in the source domain.

Another method for restructuring an AD DS environment is to rename a domain. You can use the domain rename process to change the names of your domains, and you can also use it to change the structure of the domain trees in your forest. This process involves updating the Domain Name System (DNS) and trust infrastructures as well as Group Policy and service principal names (SPNs).

The ability to rename domains provides you with the flexibility to make important name changes and forest structural changes as the needs of your organization change. Using domain rename, you can not only change the name of a domain,

but you can change the structure of the domain hierarchy and change the parent of a domain or move a domain located in one domain tree to another domain tree.