



Active Directory Technical Overview

Microsoft Corporation

Published: July 2002

Abstract

Building on the foundation of the Microsoft® Windows® 2000 operating system, the Active Directory® service in the Windows Server 2003 family introduces key features ensuring that it is one of the most flexible directory structures in the marketplace today. As directory-enabled applications become more prevalent, organizations can use Active Directory to manage even the most complicated enterprise network environments. In addition, the Windows Server 2003 family includes many new features that make it the ideal platform for developing and deploying directory-enabled applications. This article provides an introduction to basic concepts in Active Directory and summarizes new features and improvements.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

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.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2002. Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, IntelliMirror, Visual Basic, Visual C++, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

| | |
|---|-----------|
| Introduction | 1 |
| Active Directory Basics | 2 |
| Directory Data Store | 2 |
| Active Directory and Security..... | 3 |
| Active Directory Schema..... | 3 |
| Classes..... | 3 |
| Extending the Schema | 3 |
| Attributes | 4 |
| Multi-Valued Attributes | 4 |
| Indexing Attributes..... | 4 |
| The Role of the Global Catalog..... | 5 |
| Finding Directory Information..... | 6 |
| Efficient Search Tools | 6 |
| Active Directory Replication | 6 |
| The Role of Sites in Replication | 7 |
| Active Directory Clients..... | 7 |
| New Features and Improvements for Active Directory | 9 |
| Active Directory Integration and Productivity | 10 |
| Making Active Directory Easier to Use and Manage | 10 |
| Additional Integration and Productivity Features and Improvements..... | 10 |
| Active Directory Performance and Scalability | 12 |
| Improving Performance for Branch Offices..... | 12 |
| Additional Performance Features and Improvements..... | 12 |
| Active Directory Administration and Configuration Management | 14 |
| Configuring Active Directory with New Setup Wizards | 14 |
| Additional Administrative Features and Improvements..... | 14 |
| Active Directory Group Policy Features | 18 |
| Group Policy Management | 18 |
| Purpose of GPMC | 18 |

| | |
|---|-----------|
| Managing Windows 2000 and Windows Server 2003 Domains | 18 |
| Additional Group Policy Features and Improvements..... | 19 |
| Active Directory Security Enhancements | 22 |
| Managing Security with Forest Trusts | 22 |
| Forest Trust | 22 |
| Trust Management | 22 |
| Trusted Namespaces | 22 |
| Additional Security Features and Improvements | 22 |
| Summary | 25 |
| Related Links | 26 |

Introduction

The Microsoft® Active Directory® service is a central component of the Windows® platform, providing the means to manage the identities and relationships that make up network environments.

Expanding on the foundation of the Windows 2000 operating system, the Windows Server 2003 family improves the manageability of Active Directory as well as eases migration and deployment. Application developers and independent software vendors (ISVs), in particular, will also find Active Directory in Windows Server 2003 is their best choice for developing directory-enabled applications.

Active Directory has been enhanced to reduce total cost of ownership (TCO) and operation within the enterprise. New features and enhancements have been provided at all levels of the product to extend versatility, simplify management, and increase dependability. With Windows Server 2003, organizations can benefit from further reductions in cost while increasing the efficiency in which they share and manage the various elements of the enterprise.

This article is intended for IT administrators, network system architects, or anyone desiring to understand the major improvements and new features of Active Directory in Windows Server 2003. This article begins with an overview of basic concepts in Active Directory and then addresses new features and improvements for Active Directory in the Windows Server 2003 family:

- Integration and productivity.
- Performance and scalability.
- Administration and configuration management.
- Group Policy features.
- Security enhancements.

Active Directory Basics

Active Directory is the directory service for Windows Standard Server, Windows Enterprise Server, and Windows Datacenter Server. (Active Directory cannot be run on Windows Web Server but it can manage any computer running Windows Web Server.) Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information.

Directory Data Store

This data store is often simply referred to as the directory. The directory contains information about objects such as users, groups, computers, domains, organizational units (OUs), and security policies. This information can be published for use by users and administrators.

The directory is stored on servers known as domain controllers and can be accessed by network applications or services. A domain can have one or more domain controllers. Each domain controller has a writeable copy of the directory for the domain in which it is located. Changes made to the directory are replicated from the originating domain controller to other domain controllers in the domain, domain tree, or forest. Because the directory is replicated, and because each domain controller has a writeable copy of the directory, the directory is highly available to users and administrators throughout the domain.

Directory data is stored in the Ntds.dit file on the domain controller. It is recommended that this file is stored on an NTFS partition. Some data is stored in the directory database file, and some data is stored in a replicated file system, like logon scripts and Group Policies.

There are three categories of directory data replicated between domain controllers:

- **Domain data.** The domain data contains information about objects within a domain. This is the information typically thought of as directory information such as e-mail contacts, user and computer account attributes, and published resources that are of interest to administrators and users. For example, when a user account is added to your network, a user account object and attribute data are stored in the domain data. When changes to your organization's directory objects occur, such as object creation, deletion, or attribute modification, this data is stored in the domain data.
- **Configuration data.** The configuration data describes the topology of the directory. This configuration data includes a list of all domains, trees, and forests, and the locations of the domain controllers and global catalogs.
- **Schema data.** The schema is the formal definition of all object and attribute data that can be stored in the directory. Windows Server 2003 includes a default schema that defines many object types, such as user and computer accounts, groups, domains, organizational units, and security policies. Administrators and programmers can extend the schema by defining new object types and attributes, or by adding new attributes for existing objects. Schema objects are protected by access control lists (ACLs), ensuring that only authorized users can alter the schema.

Active Directory and Security

Security is integrated with Active Directory through logon authentication and access control to objects in the directory. With a single network logon, administrators can manage directory data and organization throughout their network, and authorized network users can access resources anywhere on the network. Policy-based administration eases the management of even the most complex network.

Active Directory provides protected storage of user account and group information by using access control on objects and user credentials. Because Active Directory stores not only user credentials but also access control information, users who log on to the network obtain both authentication and authorization to access system resources. For example, when a user logs on to the network, the security system authenticates the user with information stored in Active Directory. Then, when the user attempts to access a service on the network, the system checks the properties defined in the discretionary access control list (DACL) for that service.

Because Active Directory allows administrators to create group accounts, administrators can manage system security more efficiently. For example, by adjusting a file's properties, an administrator can permit all users in a group to read that file. In this way, access to objects in Active Directory is based on group membership.

Active Directory Schema

The Active Directory Schema is the set of definitions that defines the kinds of objects—and the types of information about those objects—that can be stored in Active Directory. Because the definitions are themselves stored as objects, Active Directory can manage the schema objects with the same object management operations used for managing the rest of the objects in the directory. There are two types of definitions in the schema: attributes and classes. Attributes and classes are also referred to as schema objects or metadata.

Classes

Classes, also referred to as object classes, describe the possible directory objects that can be created. Each class is a collection of attributes. When you create an object, the attributes store the information that describes the object. The User class, for example, is composed of many attributes, including Network Address, Home Directory, and so on. Every object in Active Directory is an instance of an object class.

Extending the Schema

Experienced developers and network administrators can dynamically extend the schema by defining new classes and new attributes for existing classes.

The content of the schema is controlled by the domain controller that holds the schema operations master role. A copy of the schema is replicated to all domain controllers in the forest. The use of this common schema ensures data integrity and consistency throughout the forest.

You can also extend the schema by using the Active Directory Schema snap-in. In order to modify the schema, you must satisfy the following three requirements:

- Be a member of the Schema Administrators group.
- Install the Active Directory Schema snap-in on the computer holding the schema operations master role.
- Have administrator permission to modify the schema master.

When considering changes to the schema, there are three key points to remember:

- **Schema extensions are global.** When you extend the schema, you extend the schema for the entire forest because any changes to the schema are replicated to every domain controller in every domain in the forest.
- **Schema classes related to the system cannot be modified.** You cannot modify default system classes within the Active Directory schema; however, applications that are used to modify the schema may add optional system classes that you can change.
- **Schema extensions can be reversible.** Some properties of attributes or classes may be modified after creation. Once a new class or attribute has been added to the schema, it can be deactivated, but it cannot be removed. However, you can defunct definitions and re-use object identifiers (OIDs) or display names, which allows you to reverse a schema definition.

For more information about modifying the schema, see the [Microsoft Windows Resource Kits](http://www.microsoft.com/reskit) at <http://www.microsoft.com/reskit>.

Active Directory does not support deletion of schema objects; however, objects can be marked as deactivated, providing many of the benefits of deletion.

Attributes

Attributes are defined separately from classes. Each attribute is defined only once and can be used in multiple classes. For example, the Description attribute is used in many classes, but is defined once in the schema, ensuring consistency.

Attributes describe objects. Each attribute has its own definition that describes the type of information that can be specified for that attribute. Each attribute in the schema is specified in the Attribute-Schema class, which determines the information that each attribute definition must contain.

The list of attributes that can be applied to a particular object are determined by the class of which the object is an instance and by any superclasses of that object's class. Attributes are defined only once and potentially used many times. This ensures consistency across all classes that share a particular attribute.

Multi-Valued Attributes

Attributes can be single-valued or multi-valued. The schema definition of an attribute specifies whether an instance of the attribute can have multiple values. An instance of a single-valued attribute can be empty or it can contain a single value. An instance of a multi-valued attribute can be empty, or it can contain a single value or multiple values. Each value of a multi-valued attribute must be unique.

Indexing Attributes

Indexes apply to attributes, not to classes. Indexing an attribute can help queries more quickly find objects having that attribute. When you mark an attribute as indexed, all instances of the attribute are added to the index, not just the instances that are members of a particular class.

Adding indexed attributes can affect Active Directory replication time, available memory, and database size. Because the database is larger, it takes longer to replicate.

Multi-valued attributes can also be indexed. Indexing multi-valued attributes increases the size of Active Directory and object creation time more than indexing single-valued properties. When choosing attributes to be indexed, make sure that they will be commonly used and balance the cost versus performance.

An indexed schema attribute can also be searched by the container in which the attribute is stored rather than searching the entire Active Directory database. This will improve search time and cut down on the amount of resources used during the search.

The Role of the Global Catalog

A global catalog is a domain controller that stores a copy of all Active Directory objects in a forest. In addition, the global catalog stores each object's most common searchable attributes. The global catalog stores a full copy of all objects in the directory for its host domain and a partial copy of all objects for all other domains in the forest, which provides efficient searches without unnecessary referrals to domain controllers.

A global catalog is created automatically on the initial domain controller in the forest. You can add global catalog functionality to other domain controllers or change the default location of the global catalog to another domain controller.

A global catalog performs the following directory roles:

- **Finds objects.** A global catalog enables user searches for directory information throughout all domains in a forest, regardless of where the data is stored. Searches within a forest are performed with maximum speed and minimum network traffic.
When you search for people or printers from the Start menu or choose the Entire Directory option within a query, you are searching a global catalog. Once you enter your search request, it is routed to the default global catalog port 3268 and sent to a global catalog for resolution.
- **Supplies user principal name authentication.** A global catalog resolves user principal names when the authenticating domain controller does not have knowledge of the account. For example, if a user's account is located in example1.microsoft.com and the user decides to log on with a user principal name of user1@example1.microsoft.com from a computer located in example2.microsoft.com, the domain controller in example2.microsoft.com will be unable to find the user's account and will then contact a global catalog server to complete the logon process.
- **Supplies universal group membership information in a multiple domain environment.** Unlike global group memberships, which are stored in each domain, universal group memberships are only stored in a global catalog. For example, when a user who belongs to a universal group logs on to a domain that is set to the Windows 2000 native domain functional level or higher, the global catalog provides universal group membership information for the user's account.
If a global catalog is not available when a user logs on to a domain running in Windows 2000 native or higher, the computer will use cached credentials to log on the user if the user has logged on to the domain previously. If the user has not logged on to the domain previously, the user can only log on to the local computer.

Note: Members of the Domain Administrators group are able to log on to the network even when a global catalog is not available.

Finding Directory Information

As explained earlier, Active Directory is designed to provide information to queries about directory objects from both users and programs. Administrators and users can easily search for and find information in the directory by using the Search command on the Start menu. Client programs can access information in Active Directory by using Active Directory Service Interfaces (ADSI).

One of the principal benefits of Active Directory is its rich store of information about network objects. Information published in Active Directory about users, computers, files, and printers is available to network users. This availability is controlled by security permissions to view information.

Everyday tasks on a network involve communication with other users and connection to published resources. These tasks require finding names and addresses to send mail or connect to shared resources. In this respect, Active Directory functions as a shared address book for the enterprise. For example, you can find a user by first name, last name, e-mail name, office location, or other properties of that person's user account. Finding information is optimized by use of the global catalog, as explained earlier in this paper.

Efficient Search Tools

Administrators can use the advanced Find dialogs in the Active Directory Users and Computers snap-in to perform management tasks with greater efficiency and to easily customize and filter data retrieved from the directory. In addition, administrators can add objects to groups quickly and with minimal network impact by utilizing browse-less queries to help find likely members.

Active Directory Replication

Replication provides information availability, fault tolerance, load balancing, and performance benefits for the directory. Active Directory uses multimaster replication, enabling you to update the directory at any domain controller, rather than at a single, primary domain controller. The multimaster model has the benefit of greater fault tolerance, since, with multiple domain controllers, replication continues, even if any single domain controller stops working.

A domain controller stores and replicates:

- **Schema information.** This defines the objects that can be created in the directory and what attributes those objects can have. This information is common to all domains in the forest. Schema data is replicated to all domain controllers in the forest.
- **Configuration information.** This describes the logical structure of your deployment, containing information such as domain structure or replication topology. This information is common to all domains in the forest. Configuration data is replicated to all domain controllers in the forest.
- **Domain information.** This describes all of the objects in a domain. This data is domain-specific and is not distributed to any other domains. For the purpose of finding information throughout the domain tree or forest, a subset of the properties for all objects in all domains is stored in the global catalog. Domain data is replicated to all domain controllers in the domain.
- **Application information.** Information stored in the application directory partition is intended to satisfy cases where information needs to be replicated, but not necessarily on a global scale. Application data can be explicitly rerouted to administrator-specified domain controllers within a forest to prevent unnecessary replication traffic, or it can be set to replicate to all domain controllers in the domain.

The Role of Sites in Replication

Sites streamline replication of directory information. Directory schema and configuration information is replicated throughout the forest and domain data is replicated among all domain controllers in the domain and partially replicated to global catalogs. By strategically reducing replication, the strain on your network can be similarly reduced.

Domain controllers use sites and replication change control to optimize replication in the following ways:

- By occasionally re-evaluating which connections are used, Active Directory uses the most efficient network connections.
- Active Directory uses multiple routes to replicate changes, providing fault tolerance.
- Replication costs are minimized by only replicating changed information.

If a deployment is not organized into sites, information exchange among domain controllers and clients can be chaotic. Sites improve the efficiency of network usage.

Active Directory replicates directory information within a site more frequently than among sites. This way, the best-connected domain controllers—those most likely to need particular directory information—receive replications first. The domain controllers in other sites receive all changes to the directory, but less frequently, reducing network bandwidth consumption. And because data is compressed when replicating between sites, bandwidth consumption is further reduced. To be efficient, updates are limited only to times when new directory information has been added or current directory information has been changed.

If directory updates are constantly distributed to all other domain controllers in the domain, they will consume network resources. Although you can manually add or configure connections or force replication over a particular connection, replication is automatically optimized by the Active Directory Knowledge Consistency Checker (KCC) based on information that you provide in the Active Directory Sites and Services administration tool. The KCC is responsible for constructing and maintaining the replication topology for Active Directory. In particular, the KCC decides when replication will occur, and the set of servers that each server must replicate with.

Active Directory Clients

With the Active Directory client, many of the Active Directory features available on Windows 2000 Professional or Windows XP Professional are available to computers running Windows 95, Windows 98, and Windows NT® 4.0 operating systems:

- **Site awareness.** You can log on to the domain controller that is closest to the client in the network.
- **Active Directory Service Interfaces (ADSI).** You can use scripting to Active Directory. ADSI also provides a common programming API to Active Directory programmers.
- **Distributed File System (DFS) fault tolerance client.** You can access Windows 2000 and servers running Windows DFS fault tolerant and fail over file shares specified in Active Directory.
- **NTLM version 2 authentication.** You can use the improved authentication features in NT LanMan (NTLM) version 2. For more information about enabling NTML version 2, see article Q239869, "[How to Enable NTLM 2 Authentication](http://support.microsoft.com/)," in the Microsoft Knowledge Base at <http://support.microsoft.com/>.
- **Active Directory Windows Address Book (WAB) property pages.** You can change properties, such as phone number and address, on user object pages.
- **Active Directory search capability.** From the **Start** button, you can locate printers and people in a

Windows 2000 Server or Windows domain. For information about publishing printers in Active Directory, see article Q234619, "[Publishing a Printer in Windows 2000 Active Directory](#)," in the Microsoft Knowledge Base at <http://support.microsoft.com>.

Windows 2000 Professional and Windows XP Professional provide functionality not included in the Active Directory client on Windows 95, Windows 98, and Windows NT 4.0, including Kerberos version 5 support; Group Policy or IntelliMirror® management technologies support; and service principal name or mutual authentication. You can take advantage of these additional features by upgrading to Windows 2000 Professional or Windows XP Professional. For more information see:

- [Upgrading to Windows 2000](#) at <http://www.microsoft.com/windows2000/professional/howtobuy/upgrading/default.asp>.
- [Windows XP Professional Upgrade Center](#) at <http://www.microsoft.com/windowsxp/pro/howtobuy/upgrading/default.asp>.

To install the Active Directory client, see the [Active Directory client page](#) at <http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/adextension.asp>

New Features and Improvements for Active Directory

The remainder of this paper summarizes new features and improvements for Active Directory in the Windows Server 2003 family in the following areas:

- [Integration and productivity.](#)
- [Performance and scalability.](#)
- [Administration and configuration management.](#)
- [Group Policy features.](#)
- [Security enhancements.](#)

Active Directory Integration and Productivity

As the principal means to manage enterprise identities, objects, and relationships, the interfaces in Active Directory (both programmatic and user interfaces) have been improved to increase administration efficiency and integration capabilities.

Making Active Directory Easier to Use and Manage

Active Directory contains many enhancements that make it easier to use such as improvements to MMC snap-ins and the object picker component. MMC plug-ins will be able to facilitate management of multiple objects. Administrators can:

- **Edit multiple user objects.** Select and edit multiple object properties at once.
- **Save queries.** Save queries against the Active Directory service for future use. Results are exportable in XML.
- **Quickly select objects using the improved object picker component.** The component has been redesigned and enhanced to improve workflow, increase efficiency in finding objects in a large directory, and provide a more flexible query capability. It is used by numerous user interfaces and is available for use by third-party developers.

Additional Integration and Productivity Features and Improvements

| Feature | Description |
|---|---|
| ACL List User Interface Changes | The ACL user interface has been enhanced to improve usability as well as improving inherited versus specific object permissions. |
| Extensibility Enhancements | An administrator who has an independent software vendor (ISV) or original equipment manufacturer (OEM) device that utilizes Active Directory has enhanced management capabilities and can add any class of object to be a member of a group. |
| User Objects from other LDAP Directories | User objects defined in LDAP directories that use the inetOrgPerson class as defined in RFC 2798, (such as Novell and Netscape), can be defined using the Active Directory User Interfaces. The user interface that works with Active Directory user objects will work with inetOrgPerson objects. Now, any application or customer that needs to use the inetOrgPerson class may do so easily. |
| Passport Integration (via IIS) | Passport authentication is now available for Internet Information Services (IIS) 6.0 and enables Active Directory user objects to be mapped to their corresponding Passport identification (if it exists). A token is created by the Local Security Authority (LSA) for the user and is set by IIS 6.0 for the HTTP request. Internet users who have a corresponding Passport identification may now use their Passport to access resources as if they were using their Active Directory credentials. |
| Terminal Server Usage with ADSI | Terminal server user-specific properties can be scripted using the Active Directory Services Interface (ADSI). User properties can be scripted with ADSI in addition to being set manually through the directory, a benefit that makes it easy to implement bulk or programmatic changes through ADSI. |
| Replication and Trust Monitoring WMI Providers | Windows Management Instrumentation (WMI) classes can monitor whether domain controllers are successfully replicating Active Directory information |

| | |
|--------------------------------|---|
| | among themselves. Because many Windows 2000 components, such as Active Directory replication, rely on inter-domain trust, this feature also provides a method to monitor that trusts are functioning correctly. Administrators or operations staff can be easily alerted to replication problems through WMI now. |
| MSMQ Distribution Lists | Message Queuing (MSMQ) adds support for sending messages to Distribution Lists that are hosted in Active Directory. MSMQ users can easily manage Distribution Lists from within Active Directory. |

Active Directory Performance and Scalability

Major changes have been made in the way Windows Server 2003 manages the replication and synchronization of Active Directory information. New features have also been added for installation, migration, and maintenance to make Active Directory more flexible, robust, and efficient.

Improving Performance for Branch Offices

A branch office deployment usually consists of numerous remote offices each with their own domain controllers—but with slow links to a corporate hub or data center. Windows Server 2003 improves the logon process for branch offices by no longer requiring access to the central global catalog server each time a user wishes to log on. Now organizations do not have to deploy a global catalog server in branch offices where the network is unreliable.

Instead of contacting a global catalog each time a user logs on to a domain controller, the domain controller caches the universal group membership of users who have previously logged on from this site or from off-site global catalog servers when the network was available. Users are then allowed to log on without the need for the domain controller to contact a global catalog server at logon time, which reduces the demand on slow or unreliable networks. This improvement also provides added reliability if a global catalog is unavailable to process logon requests for users.

Additional Performance Features and Improvements

| Feature | Description |
|--|--|
| Disabling Compression of Inter-Site Replication Traffic | Replication-traffic compression between domain controllers residing in different sites can be disabled. This can reduce the CPU demand on the domain controllers, thereby increasing performance if needed. |
| Clustered Virtual Server Support | A computer object is now defined for clustered servers. Cluster-aware and Active Directory-aware applications can associate their own configuration information with a well-defined object. |
| Concurrent LDAP Binds | Multiple Lightweight Directory Access Protocol (LDAP) binds can be performed on the same connection for the purposes of authenticating users. This feature, when utilized by the application developer, vastly improves the performance of LDAP binds and authentication requests against Active Directory. |
| Domain Controller Overload Prevention | <p>This feature prevents overloading a first Active Directory domain controller introduced in a domain that already contains a large number of upgraded Windows 2000 and Windows Server 2003 domain members.</p> <p>A Windows NT® Server 4.0 domain contains Windows 2000 and Windows Server 2003 domain members including both clients and servers. When a Primary domain controller (PDC) is upgraded to Windows 2000 Service Pack 2 (SP2) or upgraded to Windows Server 2003, it can be configured to emulate the Windows NT 4.0 domain controller behavior. The Windows 2000 and Windows Server 2003 domain members will not distinguish between upgraded domain controllers and Windows NT 4.0 domain controllers.</p> <p>To accommodate special needs of administrators, domain members running either Windows 2000 SP2 or Windows Server 2003 can be configured to inform domain controllers running Windows 2000 SP2 or Windows Server 2003 to not emulate Windows NT 4 domain controller behavior when responding to such</p> |

| Feature | Description |
|--|---|
| | domain members. |
| Global Catalog Replication Tuning | In Windows Server 2003 domains with global catalog replication, tuning the global catalog synchronization state is preserved rather than reset, minimizing the work generated as a result of a Partial Attribute Set (PAS) extension by only transmitting attributes that were added. The overall benefit is a reduction in replication traffic and more efficient PAS updates. |
| Group Membership Replication Improvements | When a forest is advanced to Windows Server 2003 Forest Native Mode, group membership is changed to store and replicate values for individual members instead of treating the entire membership as a single unit. This results in lower network bandwidth and processor usage during replication and virtually eliminates the possibility of lost updates during simultaneous updates. |
| LDAP Extended to Support Time to Live (TTL) for Dynamic Entries | Active Directory can store dynamic entries. These entries specify a Time to Live (TTL) value. The user can modify the TTL value causing the entry to remain longer than its current remaining life. The LDAP C language API was extended to support this new capability. This provides application developers with the ability to store information in the directory that does not need to persist for long periods of time and will automatically be deleted by Active Directory once the TTL expires. |
| Support for 64-bit Deployment | Group Policy settings are now provided to help manage 64-bit software deployment. Options in the Application Deployment Editor (ADE) aid in determining if 32-bit applications should be deployed to 64-bit clients. Group Policy can be used to ensure that only the appropriate applications are deployed to 64-bit clients. |

Active Directory Administration and Configuration Management

Windows Server 2003 enhances the administrator's ability to efficiently configure and manage Active Directory even in very large enterprises with multiple forests, domains, and sites.

Configuring Active Directory with New Setup Wizards

The new Configure your Server wizard eases the process of setting up Active Directory and provides pre-defined settings for specific server roles, a benefit that helps administrators standardize the way servers are initially deployed.

Administrators are assisted during server setup to make the process easier by helping users finish installing optional components that they choose during the Windows setup. They can use it to perform the following:

- Set up the first server on a network by automatically configuring DHCP, DNS, and Active Directory using basic default settings.
- Help users configure member servers on a network by pointing to the features they need to set up a file server, print server, Web and media server, application server, RAS and routing, or IP address management server.

An administrator can use this feature for disaster recovery, replicating a server configuration to multiple computers, finishing setup, configuring server roles, or setting up the configuration of first or primary server on a network.

Additional Administrative Features and Improvements

| Feature | Description |
|--|---|
| Automatic Creation of DNS Zone | Domain Name System (DNS) Zones and servers can be automatically created and configured when running one of the Windows Server 2003 family operating systems. They are created through the enterprise to host the new zone. This can significantly reduce the time it would take to manually configure every DNS server. |
| Improved Inter-Site Replication Topology Generation | The Inter-Site Topology Generator (ISTG) has been updated to use improved algorithms and will scale to support forests with a greater number of sites than in Windows 2000. Because all domain controllers in the forest running the ISTG role must agree on the inter-site replication topology, the new algorithms are not activated until the forest has advanced to Windows Server 2003 Forest Native Mode. The new ISTG algorithms provided improved replication performance across forests. |
| DNS Configuration Enhancements | This feature simplifies debugging and reporting of an incorrect DNS configuration and helps to properly configure the DNS infrastructure required for Active Directory deployment. This includes the situation if a domain controller is promoted in an existing forest, the Active Directory Installation Wizard contacts an existing domain controller to update the directory and replicate the required portions of the directory from the domain controller. If the Wizard fails to locate a domain controller due to an incorrect configuration of DNS or if the domain controller is not available, it performs debugging and reports the cause of the failure and indicates how to fix |

| Feature | Description |
|------------------------------------|---|
| | <p>the problem.</p> <p>In order to be located on a network, every domain controller must register domain controller locator DNS records. The Active Directory Installation Wizard verifies that the DNS infrastructure is properly configured to allow the new domain controller to perform a dynamic update of its domain controller locator DNS records. If this check discovers the incorrectly configured DNS infrastructure, it is reported with an explanation on how to fix the problem.</p> |
| Install Replica from Media | <p>Instead of replicating a complete copy of the Active Directory database over the network, this feature allows an administrator to source initial replication from files created when backing up an existing domain controller or global catalog server. The backup files, generated by any Active Directory-aware backup utility, can be transported to the candidate domain controller using media such as tape, CD, DVD, or file copy over a network.</p> |
| Migration Tool Enhancements | <p>The Active Directory Migration Tool (ADMT) is enhanced in Windows Server 2003 to provide:</p> <ul style="list-style-type: none"> ▪ Password migration. ADMT version 2 will allow migrating passwords from Windows NT 4.0 to Windows 2000 or Windows Server 2003 domains as well as migrating passwords from Windows 2000 to Windows Server 2003 domains. ▪ New scripting interface. For the most commonly used migration tasks, such as migration of users, groups, and computers, a new scripting interface is provided. ADMT can now be driven from any language and supports COM interfaces, such as Visual Basic® Script, Visual Basic, and Visual C++® development systems. ▪ Command-line support. The scripting interface has also been extended to provide command-line support. All scriptable tasks can be executed directly from a command line or through batch files. ▪ Security translation improvements. The security translation, such as redoing resources within ACLs, is extended in a way that the source domain can be decommissioned at the time when security translation runs. ADMT will now also allow specifying a mapping file that can be used as input for security translations. <p>ADMT version 2 makes it easier to migrate to Active Directory and provides more options to automate migration.</p> |

| Feature | Description |
|--|---|
| Application Directory Partitions | <p>Active Directory services will allow the creation of a new type of naming context , or partition, referred to as Application Partition. This naming context can contain a hierarchy of any type of object except security principals (users, groups and computers), and can be configured to replicate to any set of domain controllers in the forest, not necessarily all in the same domain.</p> <p>This feature provides the capability of hosting dynamic data in Active Directory without significantly impacting network performance by providing the ability to control the scope of replication and placement of replicas.</p> |
| Integrated DNS Zones Stored in Application Partitions | <p>DNS zones in Active Directory can be stored and replicated in the application partition. Using application partitions to store the DNS data results in a reduced number of objects stored in the global catalog. In addition, when DNS zone data is stored in an application partition, it is replicated to only that subset of domain controllers in the domain that is specified in the application partition. By default, DNS-specific application partitions contain only those domain controllers that run the DNS server. In addition, storing the DNS zone in an application partition enables replication of the DNS zone to the DNS servers running on the domain controllers in different domains of an Active Directory forest. By integrating DNS zones in an application partition it is possible to limit the replication of this information and decrease overall replication bandwidth requirements.</p> |
| DirSync Control Improvements | <p>This feature improves Active Directory support for LDAP control, called DirSync control, to retrieve changed information from the directory. The DirSync control can access checks similar to those performed on normal LDAP searches.</p> |
| Functionality Levels | <p>Similar to native mode in Windows 2000, this feature provides a versioning mechanism that can be used by Active Directory core components to determine what features are available on each domain controller in a domain and in a forest. It is also used to prevent pre-Windows Server 2003 domain controllers from joining a forest that has the Windows Server 2003-only Active Directory feature activated.</p> |
| Deactivation of Schema Attributes and Classes | <p>Active Directory has been enhanced to allow the deactivation of attributes and class definitions in the Active Directory schema. Attributes and classes can be redefined if an error was made in the original definition.</p> <p>Deactivation provides the ability to supercede the definition of an attribute or class after it has been added to the schema if an error was made in setting an immutable property. It is a reversible operation, allowing administrators to undo an accidental deactivation without side-affects. Administrators now have greater flexibility with respect to their Active Directory schema management.</p> |
| Domain Rename | <p>This feature supports changing the DNS and/or NetBIOS names of existing domains in a forest while ensuring that the resulting forest is still "well formed". The identify of a renamed domain represented by its domain Globally Unique ID (GUID) and its domain Security ID (SID) will not change. In addition, a computer's domain membership does not change as a result of the holding domain being renamed.</p> <p>This feature does not include changing which domain is the forest root domain. Although a forest root domain can be renamed, a different domain cannot be designated to become the new forest root.</p> <p>Domain rename will cause a service interruption requiring every domain controller to be rebooted. Domain rename will also require that every member computer of the renamed domain must be rebooted twice. Although this feature provides a</p> |

| | |
|---|---|
| | supported means to rename a domain, it is not viewed nor is intended to be a routine IT operation. |
| Upgrading Forest and Domains | Active Directory has added improvements in security and application support. Before the first domain controller running the Windows Server 2003 operating system can be upgraded in an existing forest or domain, the forest and domains have to be prepared for these new features. Adprep is a new tool to aid forest and domain upgrades. The adprep tool is not needed when upgrading from Windows NT 4.0 or when Active Directory is clean-installed on servers running Windows Server 2003. |
| Replication and Trust Monitoring | This allows administrators to monitor whether domain controllers are successfully replicating Active Directory information among themselves. Because many Windows components, such as Active Directory replication, rely on inter-domain trust, this feature also provides a method to monitor that trusts are functioning correctly. |

Active Directory Group Policy Features

Group Policy Management

The Microsoft Group Policy Management Console (GPMC) is the new solution for Group Policy management that helps you manage your enterprise more cost-effectively. It consists of a new Microsoft Management Console (MMC) snap-in and a set of scriptable interfaces for managing Group Policy. GPMC is planned to be available as a separate component by the time Windows Server 2003 is launched.

Purpose of GPMC

GPMC is designed to:

- Simplify the management of Group Policy by providing a single place for managing core aspects of Group Policy. You can think of GPMC as a "one-stop shopping location" for managing Group Policy.
- Address top Group Policy deployment requirements, as requested by customers, by providing:
 - A user interface (UI) that makes Group Policy much easier to use.
 - Backup/restore of Group Policy objects (GPOs).
 - Import/export and copy/paste of GPOs and Windows Management Instrumentation (WMI) filters.
 - Simplified management of Group Policy–related security.
 - HTML reporting for GPO settings
 - HTML reporting for Group Policy Results and Group Policy Modeling data (formerly known as Resultant Set of Policy).
 - Scripting of GPO operations that are exposed within this tool—but not scripting of settings with a GPO.

Prior to GPMC, administrators were required to use several Microsoft tools to manage Group Policy. GPMC integrates the existing Group Policy functionality exposed in these tools into a single, unified console, along with the new capabilities listed above.

Managing Windows 2000 and Windows Server 2003 Domains

GPMC will be able to manage both Windows 2000 and Windows Server 2003–based domains with the Active Directory® service. In either case, the administrative computer on which the tool itself runs must be running one of the following:

- Windows Server 2003.
- Windows XP Professional with Service Pack 1 (SP1), plus an additional post-SP1 hotfix, and the Microsoft .NET Framework.

For more information, see [Enterprise Management with the Group Policy Management Console](#).

Additional Group Policy Features and Improvements

| Feature | Description |
|---|--|
| Redirecting Default User and Computer Containers | <p>Windows Server 2003 includes tools to automatically redirect new user and computer objects into specified organizational units where Group Policy can be applied.</p> <p>This helps administrators avoid a situation where new user and computer objects are left in default containers at the domain root level. Such containers were not designed to hold Group Policy links, and clients were not designed to read and apply Group Policy from these containers. This forced many customers who used these containers to introduce domain-level policy, which can be unwieldy in many cases.</p> <p>Instead, Microsoft recommends creating a logical hierarchy of organizational units to hold newly created user and computer objects. Administrators can use two new Resource Kit tools— RedirUsr and ReDirComp—to specify an alternative default for the three legacy APIs: NetUserAdd(), NetGroupAdd(), NetJoinDomain(). This will allow administrators to redirect the default locations to suitable organizational units and then apply Group Policy directly to these new organizational units.</p> |
| Group Policy Results | <p>Group Policy Results enables administrators to determine and analyze the current set of policies applied to a particular target. With Group Policy Results, administrators can review existing policy settings on targeted computers. Group Policy Results was formerly known as Resultant Set of Policy – logging mode.</p> |
| Group Policy Modeling | <p>Group Policy Modeling is designed to help administrators plan for growth and reorganization. It allows administrators to poll standing policy settings, applications, and security for a "What If" scenario. Once an administrator decides that a change is necessary or inevitable, a series of tests can be run to see what would happen to a user or group of users if they are moved to another location, security group or even another computer. This includes which policy settings will be applied and which files will be automatically loaded after the change has taken effect.</p> <p>Group Policy Modeling greatly benefits administrators by providing the means to fully test policy changes before implementing them throughout their network.</p> |
| New Policy Settings | <p>Windows Server 2003 includes over 150 new policy settings. These policy settings provide the capability to customize and control the behavior of the operating system for groups of users. These new policy settings affect functionality such as error reporting, Terminal Server, networking and dial-up connections, DNS, network logon requests, Group Policy, and roaming profiles.</p> |
| Web View Administrative Templates | <p>This feature enhances the Group Policy Administrative Template extension snap-in making it possible to view detailed information about the different available policy settings. When a policy setting is selected, information detailing the settings behavior and additional information on where the setting may be used is displayed in a Web view within the Administrative templates user interface. This information is also available from the Explain tab on the Property page of each setting.</p> |

| Feature | Description |
|---|--|
| Manage DNS Client | Administrators can configure the DNS client settings on Windows Server 2003 using Group Policy. This simplifies the steps to configure domain members when adjusting DNS client settings such as enabling and disabling dynamic registration of the DNS records by the clients, using devolution of the primary DNS suffix during name resolution, and populating DNS suffix search lists. |
| “My Documents” Folder Redirection | An administrator can use this feature to transition users from a legacy deployment of home directories to the My Documents model while maintaining compatibility with the existing home directory environment. |
| Full Install of User Assigned Applications at Logon Time | The Application Deployment Editor contains a new option that allows a user-assigned application to be installed completely at logon time, instead of on demand. Administrators can ensure that users have the appropriate software automatically installed on their computers. |
| Netlogon | This feature provides the capability to configure the Netlogon settings on Windows Server 2003-based computers using Group Policy. This simplifies the steps required to configure domain members when adjusting Netlogon settings such as enabling and disabling dynamic registration of the specific domain controller locator DNS records by the domain controllers, periodicity of refreshing such records, enabling and disabling auto-site-coverage, and many other popular Netlogon parameters. |
| Network and Dial-up Connections | Windows Server 2003 networking configuration user interfaces can be made available for (or limited to) specific users via a Group Policy. |
| Distributed Eventing Policies | WMI eventing infrastructure is expanded to operate in a distributed environment. The enhancements consist of components that will enable configuring subscription, filtering, correlation, aggregation, and transport of WMI events. An ISV can enable health monitoring, event logging, notification, auto recovery, and billing with the addition of a user interface and definition of a policy type. |
| Disable Credential Manager | A new feature in Windows Server 2003, Credential Manager eases managing user credentials. Group Policy allows you to disable Credential Manager. |
| Support URL for Software Deployment | This feature provides a capability to edit and add a support URL for the package. When the application appears in the Add/Remove Programs on target computers, the user can then select the Support Information URL and will be directed to a support Web page. This feature can assist in reducing calls to a helpdesk or support team. |
| WMI Filtering | <p>Windows Management Instrumentation (WMI) makes a large amount of data, such as hardware and software inventory, settings, and configuration information, available for a target computer. WMI surfaces data from the registry, drivers, file system, Active Directory, Simple Network Management Protocol (SNMP), the Windows Installer service, structured query language (SQL), networking, and Exchange Server. WMI Filtering in Windows Server 2003 allows you to dynamically determine whether to apply a GPO based on a query of WMI data. These queries (also called WMI filters) determine which users and computers receive the policy settings configured in the GPO where you create the filter. This functionality lets you dynamically target Group Policy based on the properties of the local machine.</p> <p>For example, a GPO might exist that assigns Office XP to users in a certain organizational unit. However, administrators are uncertain if all of the older desktops in that organizational unit have enough hard disk space to</p> |

| Feature | Description |
|------------------------|---|
| | accommodate the software. In this case, a WMI filter could be used with the GPO to assign Office XP only to users who have desktops with more than 400 megabytes (MB) of available hard disk space. |
| Terminal Server | An administrator can use Group Policy to manage how a Terminal Server can be used, such as enforcing redirection capabilities, password access, and wallpaper settings. |

Active Directory Security Enhancements

In the Windows Server 2003 family, Active Directory has been enhanced with some additional security features that make it easier to manage multiple forests and cross-domain trusts. In addition, the new credential manager provides a secure store of user credentials and X.509 certificates.

Managing Security with Forest Trusts

Forest trust is a new type of Windows trust for managing the security relationship between two forests. This feature vastly simplifies cross-forest security administration and enables the trusting forest to enforce constraints on which security principal names it trusts other forests to authenticate. This feature includes:

Forest Trust

- A new trust type that allows all domains in one forest to (transitively) trust all domains in another forest, via a single trust link between the two forest root domains.
- Forest trust is not transitive at the forest level across three or more forests. If Forest A trusts Forest B, and Forest B trusts Forest C, this does not create any trust relationship between Forest A and Forest C.
- Forest trusts can be one-way or two-way.

Trust Management

- A new wizard simplifies creating all types of trust links, especially forest trust.
- A new property page lets you manage the trusted namespaces associated with forest trusts.

Trusted Namespaces

- Trusted namespaces are used to route authentication and authorization requests for security principals whose accounts are maintained in a trusted forest.
- The domain, user principal name (UPN), service principal name (SPN) and security identifier (SID) namespaces that a forest publishes are automatically collected when a forest trust is created, and refreshed by the Active Directory Domains and Trust user interface.
- A forest is trusted to be authoritative for the namespaces it publishes, on a first-come, first-served basis, as long as they do not collide with trusted namespaces from existing forest trust relationships.

Overlapping trusted namespaces are automatically prevented. Administrators can also manually disable individual trusted namespaces.

Additional Security Features and Improvements

| Feature | Description |
|------------------------------------|---|
| Cross-Forest Authentication | Cross-forest authentication enables secure access to resources when the user account is in one forest and the computer account is in another forest. This feature allows users to securely access resources in other forests, using either Kerberos or NTLM, without sacrificing the single sign-on and administrative benefits of having only one user ID and password maintained in the user's home forest. Cross-forest authentication includes: Name Resolution |

| Feature | Description |
|-----------------------------------|--|
| | <ul style="list-style-type: none"> ▪ When Kerberos and NTLM cannot resolve a principal name on the local domain controller, they call a global catalog. ▪ When the global catalog cannot resolve the name, it calls a new cross-forest name matching function. ▪ The name matching function compares the security principal name with trusted namespaces from all trusted forests. If a match is found, it returns the trusted forest name as a routing hint. <p>Request Routing</p> <ul style="list-style-type: none"> ▪ Kerberos and NTLM use routing hints to route authentication requests along the trust path from the originating domain to the probable target domain. ▪ For Kerberos, Key Distribution Centers (KDCs) generate referrals that follow the trust path, and the client chases them in standard Kerberos fashion. ▪ For NTLM, domain controllers chain the request across secure channels that follow the trust path, using pass-through authentication. <p>Authentication Supported</p> <ul style="list-style-type: none"> ▪ Kerberos and NTLM network logon for remote access to a server in another forest. ▪ Kerberos and NTLM interactive logon for physical logon outside the user's home forest. ▪ Kerberos delegation to N-tier application in another forest. ▪ User Principal Name (UPN) credentials are fully supported. |
| Cross Forest Authorization | <p>Cross-forest authorization makes it easy for administrators to select users and groups from trusted forests for inclusion in local groups or ACLs. This feature maintains the integrity of the forest security boundary while allowing trust between forests. It enables the trusting forest to enforce constraints on what Security Identifiers (SIDs) it will accept when users from trusted forests attempt to access protected resources.</p> <p>Group membership and ACL Management</p> <ul style="list-style-type: none"> ▪ The object picker has been enhanced to support selection of user or group names from a trusted forest. ▪ Names must be typed in completely. Enumeration and wild card searches are not supported. <p>Name-SID Translation</p> <ul style="list-style-type: none"> ▪ The object picker and ACL editor use system APIs to store SIDs in group member and ACL entries and to translate them back to friendly names for display purposes. ▪ Name-SID translation APIs are enhanced to use cross-forest routing hints, and leverage NTLM's secure channels between domain controllers along the trust path, to resolve security principal names or SIDs from trusted forests. <p>SID filtering</p> <ul style="list-style-type: none"> ▪ SIDs are filtered when authorization data passes from the root domain of the trusted forest to the root domain of the trusting forest. The trusting forest will only accept SIDs that are relative to domains it trusts the other forest to |

| Feature | Description |
|---|--|
| | <p>manage. Any other SIDs are automatically discarded. SID filtering is automatically enforced for Kerberos and NTLM authentication, as well as name-SID translation.</p> |
| <p>Cross Certification Enhancements</p> | <p>The Windows Server 2003 client cross-certification feature is enhanced by enabling the capability for department-level and global-level cross certifications. For example, WinLogon will now be able to query for cross certificates and download these into the “enterprise trust/enterprise store.” As a chain is built, all cross certificates will be downloaded.</p> |
| <p>IAS and Cross-Forest Authentication</p> | <p>If Active Directory forests are in cross-forest mode with two-way trusts, then the Internet Authentication Service/Remote Authentication Dial-In User Server (IAS/RADIUS) server can authenticate the user account in the other forest with this feature. This gives administrators the capability to easily integrate new forests with already existing IAS/RADIUS services in their forest.</p> |
| <p>Credential Manager</p> | <p>The Credential Management feature provides a secure store of user credentials, including passwords and X.509 certificates. This will provide a consistent single-sign on experience for users, including roaming users. For example, when a user accesses a line-of-business application within their company’s network, the first attempt to access this application requires authentication and the user is prompted to supply a credential. After the user provides this credential, it will be associated with the requesting application. In future access to this application, the saved credential will be re-used without prompting the user.</p> |

Summary

Building on the foundation established in Windows 2000, Active Directory in Windows Server 2003 emphasizes simplified management, versatility, and unmatched dependability. More than ever, Active Directory has become a solid foundation for building enterprise networks unsurpassed in its ability to:

- Take advantage of existing investments and consolidation management of directories.
- Extend administrative control and reduce redundant management tasks.
- Simplify remote integration and use network resources more efficiently.
- Provide a robust development and deployment environment for directory-enabled applications.
- Reduce TCO and improve the leverage of IT resources.

Related Links

See the following resources for further information:

- [Microsoft Windows 2000 Active Directory Home Page](http://www.microsoft.com/ad) at <http://www.microsoft.com/ad>.
- [Enterprise Management with the Group Policy Management Console](http://www.microsoft.com/windowsserver2003/gpmc) at <http://www.microsoft.com/windowsserver2003/gpmc>.
- [Windows DNS Overview](http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadrmgmt/dnsover.asp) at <http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadrmgmt/dnsover.asp>.
- [Microsoft Windows Resource Kits](http://www.microsoft.com/reskit) at <http://www.microsoft.com/reskit>.
- [Upgrading to Windows 2000](http://www.microsoft.com/windows2000/professional/howtobuy/upgrading/default.asp) at <http://www.microsoft.com/windows2000/professional/howtobuy/upgrading/default.asp>.
- [Windows XP Professional Upgrade Center](http://www.microsoft.com/windowsxp/pro/howtobuy/upgrading/default.asp) at <http://www.microsoft.com/windowsxp/pro/howtobuy/upgrading/default.asp>.

For the latest information about Windows Server 2003, see the [Windows Server 2003 Web site](http://www.microsoft.com/windowsserver2003) at <http://www.microsoft.com/windowsserver2003>.