

*i***ITCO**

Windows 2000 AD
Benefits

White Paper

Active Directory Defined

Active Directory is the central management structure for Windows 2000 based networks. Windows 2000 uses Active Directory to organize security principals such as users and computers, as well as to manage administrative objects such as shared folders and printers, into manageable collections called "Organizational Units" and "domains". Domains are related to other domains in a parent/child hierarchical relationship within a DNS namespace called a "tree". Trees can be linked together into a "forest"; the forest is the Active Directory. These structures together form the hierarchical structure of the Active Directory.

Active directory is composed of a hierarchical database that stores information about the objects that make up your network; computer, users, security policies, and technically anything someone writes an application to support.

Active Directory Functions

Windows 2000 uses Active directory to:

- Organize security domains into parent/child relationships.
- Automatically create trust relationships between related domains.
- Manage security accounts in a domain.
- Manage authentication between machines and users.
- Organize users, computers, printers, and other objects into policy collections called Organizational Units.
- Enforce policies based on the organizational structure.
- Delegate network administration in a hierarchy.
- Distribute software automatically.

Active Directory Features

Manageability

Feature	Description
Centralized Management	Active Directory centrally manages Windows users, clients, and servers through a single consistent management interface, reducing redundancy and maintenance costs.
Group Policy	Group Policy allows administrators to define and control the policies governing groups of computers and users within their organization. Administrators can set group policy for any of the sites, domains, or organizational units in Active Directory. They can also filter its effect by using membership in security groups. Once set, the system maintains group policy without need for further intervention.
Global Catalog	The Global Catalog holds all objects from all domains in the Windows 2000 Server directory, together with a subset of each object's properties. Designed for high performance, the Global Catalog lets users search by selected attributes to find an object easily, regardless of where it is in the tree.
IntelliMirror Desktop Management	IntelliMirror® management technologies provide administrators with automatic software distribution and maintenance, centralized desktop-configuration management, and remote operating system installation. For end users, IntelliMirror provides location independence by making user-specific desktop settings, application data and documents available from any machine on the network.
Automated Software Distribution	Active Directory lets administrators automatically distribute applications to users based on their role in the company. For example, all accountants can automatically receive spreadsheet software.
Active Directory Service Interfaces (ADSI)	ADSI greatly simplifies the development of directory-enabled applications, as well as the administration of distributed systems. Developers and administrators use this single set of interfaces to manage the resources in a directory service, no matter which network environment contains the resource. ADSI supports interfaces for ActiveX/COM, Lightweight Directory Access Protocol (LDAP), MAPI and

	Java (JADSI).
Backward	Windows 2000 Server supports a mixed environment of Active Directory
Compatibility	domain controllers. Connected computers running software designed prior to Windows 2000 will respond as if they are accessing the domain controllers of the Windows NT@Server 4.0 operating system.
Delegated Administration	Windows 2000 lets administrators delegate a selected set of administrative privileges to appropriate individuals within the company and specify the specific rights they have over different containers (collections of objects) and objects in the directory.
Multi-Master Replication	With multi-master replication, the changes made to any one domain controller will also be made to all the other domain controllers in the same domain. Even if individual domain controllers are unavailable, multi-master replication assures that the directory is available for changes 100 percent of the time. In addition, by providing multiple copies of the directory across multiple servers, the Windows 2000 Server directory automatically optimizes the use of replication bandwidth across WAN links.

Security

Feature	Description
Kerberos Authentication	Full support for Kerberos 5 protocol provides fast, single sign-on to Windows 2000-based resources, as well as to other environments that support this protocol.
Smart Card Support	Supports logon via smart cards for strong authentication to sensitive resources.
Transitive Trust Domain	Transitive trust agreements greatly reduce the number of trust relationships to manage between Windows domains.
PKI/x.509	Support for x.509 certificates and public key infrastructure (PKI) ensures interoperability with and deployment of extranet and e-commerce applications.
LDAP over SSL	Support for LDAP over secure sockets layer (SSL) for secure directory transactions for extranet and e-commerce applications.
Required Authentication	Allows administrators to require the specific type of logon needed including Kerberos, x.509 certificate, or NTLM.
Mechanism	
Attribute-Level Security	The Global Catalog enforces object and attribute-level security for detailed control of access to information stored in the directory.
Spanning Security Groups	In Windows 2000, there are no restrictions on security groups that span domain partitions. This means that groups can be managed centrally.

LDAP ACL Support	Consistent interpretation of access control lists (ACLs) through LDAP ensures interoperability for secure extranets and e-commerce applications.
-------------------------	--

Interoperability

Feature	Description
DirSync Support	DirSync, a proposed Internet Engineering Task Force (IETF) standard, is a synchronization mechanism for exchanging update information between multiple directories.
Active Directory Connectors (ADC)	ADC provides directory synchronization and import/export tools. It lets administrators replicate a hierarchy of directory objects between a Microsoft Exchange Server 5.5 directory and Active Directory. It also lets Active Directory connect to Novell Directory Services.
Open APIs	All Active Directory functions are available through LDAP, ADSI and MAPI for extending and integrating with other applications, directories, and devices.
Native LDAP	Active Directory is implemented as a native LDAP server that doesn't require request translation to ensure interoperability in extranet environments and e-commerce applications.
DNS Naming	The native Internet-standard DNS naming service uses protocols to simplify the Internet naming and placement of objects.
Open Change History	Active Directory provides built-in, LDAP-based change history interfaces to facilitate its use as a metadirectory and management focal point within organizations.
DEA Platform	Active Directory provides a directory-enabled application (DEA) platform which enables applications to make use of the directory for automating aspects of their installation, distribution, and maintenance.
DEN Platform	Active Directory, combined with hardware and software support from Cisco Systems, introduces a directory-enabled networking (DEN) platform that allows administrators to allocate network bandwidth and quality of service to users based on their role in the company.
Extensible Schema	Active Directory lets developers and administrators extend the directory schema and create new properties and objects. Using the directory as a data store, developers can use this feature to create their own data structures for applications. In addition, users on the network can publish important information in the directory so other users can easily find it.

Active Directory Design

Good design, be it for automobiles or Active Directory structure, is always improved by the principle of “keeping it simple”. In terms of the Active Directory Structure this means the best answer to the following questions is always “one”:

- How many Forests should I have?
- How many Trees do I need?
- How many Domains should I have?

There are exceptions to all of these items, but the vast majority of businesses today will function best with one Forest, one Tree, and one Domain.

Domain Centralization

The effect of these decisions is to centralize the administration of your domains. For organizations that have created several domains under NT 4.0, the effect is a great reduction in administrative cost.

Another benefit of this type of consolidation is the “unification” of computing resources within the NT network. Suddenly the organization can:

Access computing resources without the barrier of crossing from one domain to another.

- Login anywhere using the same account.
- Define and enforce security policies upon a corporation.

Gain the economies of scale through purchasing decisions that can be made for the corporation, not just a single domain.

Simplify IT
iTCO
your eBusiness Partner
www.itcosolutions.com

iTCO Solutions Corporation
P.O. Box 610090
Redwood City, CA 94061
United States

<http://www.itcosolutions.com/>

Enterprise Sales Team Contact
Ryan Edwards
National Accounts Manger
Tel: 650-367-0514
E-Mail: redwards@itcosolutions.com