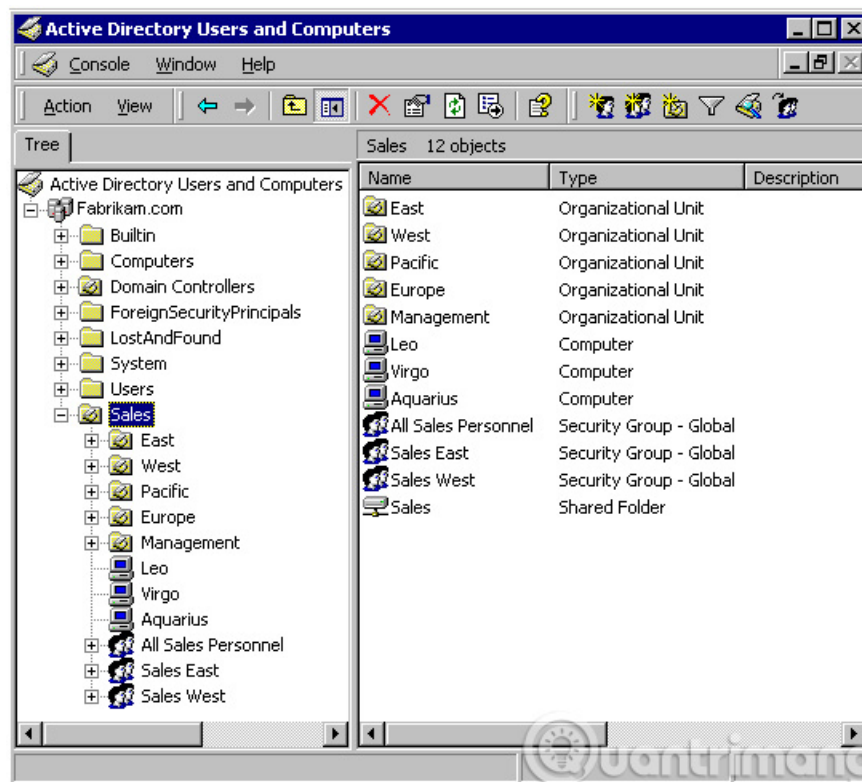


Theory - What is Active Directory?

What is Active Directory? Active Directory is a copyrighted directory service by Microsoft, which is an integral part of Windows architecture.

In this article, I will show you some basic knowledge about Active Directory and the benefits of implementing **Active Directory** . Information about **forests, domains, organizational units** and **sites** as well as basic knowledge about **LDAP (Lightweight Directory Access Protocol)** and **Group Policy** .



1. What is Active Directory?

First of all, let's find out what **Active Directory** is. **Active Directory** is a copyrighted directory service by Microsoft, which is an integral part of Windows architecture. Like other directory services, such as **Novell Directory Services (NDS)** , **Active Directory** is a standard and centralized system, which automates the management of user data, security, and resources. It is distributed, allowing interaction with other directories. In addition, Active Directory is specifically designed for networked environments that are allocated in a certain way.

Active Directory can be considered a new development point compared to **Windows 2000 Server** and is improved and improved better in **Windows Server 2003** , becoming an important part of the operating system. **Windows Server 2003 Active Directory** provides a reference, called a **directory service** , to all objects in a network, including **users, groups, computers, printers, policies and permissions** .

In short and in general, Active Directory is a form of database that is clear and specific, but it is not a complete replacement for the Windows Registry. Please imagine this, a large network of clients has hundreds, thousands of employees, and each employee has different names (surname), different jobs, different departments . And each of those client "server" management servers must have Active Directory to best sort and handle the work. Data sections in Active Directory are inherited, replicated, rank . clear and flexible.

2. Why is Active Directory necessary?

There are several reasons to explain the above question. **Microsoft Active Directory** is considered a significant step forward compared to **Windows NT Server 4.0 domains** or even **standalone** server networks . **Active Directory** has a centralized administration mechanism across the entire network. It also provides redundancy and automatic failover when two or more **domain controllers** are deployed in a domain.

Active Directory will automatically manage communication between **domain controllers** to ensure the network is maintained. Users can access all resources on the network through a single sign-on mechanism. All resources in the network are protected by a strong security mechanism, this security mechanism can check user identity and the authority of each access to resources.

Active Directory allows for easy leveling up and downgrade of domain controllers and member servers. Systems can be managed and protected through Group Policies policies. This is a flexible hierarchical organizational model, allowing for easy management and delegating administrative responsibilities. Most importantly, though, the Active Directory is capable of managing millions of objects within a domain.

3. Basic units of Active Directory?

Active Directory networks are organized using four types of units or item structures. These four units are divided into **forest, domain, organizational unit and site** .

Picture 2 of Theory - What is Active Directory?

1. **Forests** : Group objects, attributes, and attribute syntax in **Active Directory** .
1. **Domain** : A group of computers that share a common policy set, a name, and a database of their members.
1. **Organizational unit (OU)** : Groups of items in certain domains. They create a hierarchical architecture for the domain and create the corporate structure of Active Directory according to organizational and geographical conditions.
1. **Sites** : A physical group of components independent of the domain and OU structure. Sites distinguish between locations connected by high-speed connections and low-speed connections, and are defined by one or more IP subnets.

Forests are not restricted by geography or network topology. A forest can consist of multiple domains, each sharing a common schema. Domain members of the same forest do not even need to have a LAN or WAN connection between them. Each private network can also be a family of multiple independent forests. In general, a forest should be used for each entity. However, additional forests are required for performing tests and research purposes outside the production forest.

Domains - Domains serve as entries in security policies and administrative tasks. All objects within a domain are subject to wide domain Group Policies. Similarly, any domain administrator can manage all objects within a domain. In addition, each domain also has its unique account database. Therefore authentication is one of the basics of the domain. When a user account is completely authenticated to a certain domain, this user account can access resources within the domain.

Active Directory requires one or more domains to operate. As mentioned earlier, an Active Directory domain is a set of computers that share a common set of policies, names and databases of their members. A domain must have one or more domain controller (DC) machines and save the database, maintain policies and provide authentication for domain logins.

Previously in Windows NT, the **primary domain controller - primary domain controller (PDC)** and the **backup domain controller - backup domain controller (BDC)** were roles that could be assigned to a server in a network of used computers. Windows operating system. Windows used the domain idea to manage access to network resources (applications, printers, and .) for a group of users. Users who only need to log in to the domain are able to access resources, which can be on a number of different servers in the network.

The server is known as the PDC, which manages the Master user database for the domain. One or more other servers are designed as BDC. PDC periodically sends database copies to BDCs. A BDC may be able to act as a PDC if the PDC server fails and can also help balance the workflow if it is too busy.

With Windows 2000 Server, when domain controllers are maintained, the PDC and BDC server roles are basically replaced by Active Directory. Users also do not create distinguished domains to divide administrative privileges. Within Active Directory, users can delegate administrative privileges based on OUs. Domains are not restricted by a number of 40,000 users. **Active Directory** domains can manage millions of objects. Because PDC and BDC are no longer available, Active Directory uses **multi-master replication** and all domain controllers are equal.

Organizational units are more flexible and allow for easier management than domains. OU allows you to have almost infinite flexibility, you can move, delete and create new OUs if needed. Although regions also have flexible properties. They can be newly created, but this process can easily lead to environmental disruption compared to OUs and should be avoided if possible.

By definition, *sites* are containing IP subnets that have fast and reliable communication links between hosts. By using the site, you can control and reduce the amount of traffic on slow WAN links.

4. Infrastructure Master and Global Catalog:

Another major component within **Active Directory** is the **Infrastructure Master** . **Infrastructure Master (IM)** is a **domain-wide FSMO (Flexible Single Master of Operations)** that plays a role in responding to automated processes to correct errors in the **Active Directory** database.

Phantom is created on DCs, it requires a cross-database reference between an object inside a separate database and an object from the domain within the forest. An example might be encountered when you add a user from a domain to a group within another domain with the same forest. Phantom will be invalidated when they do not contain updated data, which occurs because changes are made to the external object that Phantom represents, such as when the target object is renamed, move somewhere between domains, or delete. **The Infrastructure Master** has the ability to locate and fix some phantom. Any changes that occur due to error correction are replicated to all the remaining DCs within the domain.

The Infrastructure Master is sometimes confused with **Global Catalog (GC)** , which maintains a copy that allows read only for domains within a forest, used for universal group storage and login process, . Because GC stores incomplete copies of all objects within the forest, they can create cross references between domains that do not need phantom.

5. Active Directory and LDAP:

LDAP (Lightweight Directory Access Protocol) is part of Active Directory, it is a software protocol that allows organizations, individuals or other resources such as files and devices in the network, even if your network is a network. Public Internet or intranet in the company.

In a network, a directory will tell you where to store certain data. In TCP / IP networks (including the Internet), domain name system (DNS) is a directory system used to associate a domain name with a specific network address (the only location in the network). However, you may not know the domain name, but LDAP allows you to search for specifics without knowing where they are located.

The LDAP directory is organized in a simple tree architecture consisting of the following levels:

1. **The root directory** has sub-branches
 1. **Country** , every Country has its branches
 1. **Organizations** , each organization has sub-branches
 1. **Organizational units** (units, departments, .), OU has branches
 1. **Individuals** (individuals, including people, files and shared resources, such as printer)

An LDAP directory can be distributed among multiple servers. Each server can have a replica version of the master directory and is synchronized periodically.

Administrators need to understand LDAP when searching for information in Active Directory, creating useful LDAP queries when searching for information stored in the Active Directory database.

6. Managing Group Policy and Active Directory:

When it comes to Active Directory, we definitely have to mention Group Policy. Administrators can use Group Policy in Active Directory to define user and computer settings throughout the network. This setting is configured and stored in Group Policy Objects (GPOs), which are then combined with Active Directory objects, including domains and sites. This is the main mechanism for applying changes to computers and users in the

Windows environment.

Through Group Policy management, administrators can globally configure desktop settings on user computers, restrict or allow access to certain files or folders within the network.

In addition, we also have to understand how GPOs are used. The Group Policy Object is applied in the following order: Internal machine policies are used first, then site policies, domain policies, and policies used for individual OUs. At some point, a user object or computer can only belong to one site or domain, so they will only receive GPOs associated with that site or domain.

GPOs are divided into two separate parts: **Group Policy Template (GPT)** and **Group Policy Container (GPC)**. The Group Policy Template is responsible for saving the settings created within the GPO. It stores settings in a folder structure and large files. To successfully apply these settings to all user and computer objects, the GPT must be replicated to all DCs within the domain.

Group Policy Containers are part of a GPO and are stored in Active Directory on DCs in the domain. The GPC is responsible for keeping references to **Client Side Extensions (CSEs)**, paths to GPT, links to installation packages and other reference aspects of the GPO. GPC does not contain much information related to its GPO, but it is an essential component of Group Policy. When software installation policies are configured, GPC will help keep the links within the GPO. It also keeps other relational links and paths stored in object properties. Knowing the structure of GPC and how to access the hidden information stored in attributes will be necessary when you need to check for a problem related to GP.

With Windows Server 2003, Microsoft released a **Group Policy** management solution that is the **Group Policy Management Console (GPMC)**. GPMC provides administrators with a management interface that simplifies tasks related to GPOs. *Good luck!*

You finished reading the article "**Theory - What is Active Directory?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.