# 什么是Active Directory

集中管理并存储所有资源，并使得用户或应用程序能进入到“所有”资源。

## 功能

1. 集中控制网络资源
2. 集中且分散（delegate）资源管理
3. 通过逻辑结构安全存储（hierarchical）
4. 通过物理结构优化流量

# AD的逻辑结构

逻辑结构使得用户可通过名称或属性来找到对象

* Objects
* Organization Units
* Domains
* Trees
* Forests

## Objects

对象是能够代表一种网络资源的一组独特的属性集合。

\*能够包含其他对象的对象，称为Container Objects

## Organization Units

Container Objects，在一个domain内使用

通过使用OU便捷管理公司期望的组织结构

### 何时需要使用OU

1. 在domain内显示公司结构，若无OU则所有资源显示在一个列表中
2. 便于更改组织结构。（Domains中用户重新组织繁琐）
3. Delegate网络资源管理，同时保持对他们的控制。
4. 便于对类似的网络资源定位并管理。
5. 限制网络资源可见性。

## Domains

AD逻辑结构中的核心单元，将objects组合为一个或多个domain则能在网络中反映公司组织结构。

Objects必须属于一个Domain，而每个Domain也仅存储所包含的Object信息。

所有的安全策略及设置，比如管理权限，安全策略和ACLs，不会跨Domain。Domain Administrator在其所属域内拥有绝对权力。

Domain提供以下功能：

1. Objects边界管理（ACLs，由ACEs）
2. 对贡献资源的安全性管理
3. A unit of replication for objects（？）

## Trees

树的组成方式：

1. 允许全局资源共享的域，以grouping或hierarchical方式组合
2. 可能由单个域或连续命名空间中的多个域组成。（？）

可以在层级结构中添加域来扩大树。

Kerberos传递信任。

## Forests

由一个或多个树组成。（？）

允许组织将不同命名规则的分部组合，这些分部可能独立运作但需要与整个组织进行沟通。共享same schema和configuration container，默认资源尽在林内共享。

## 在Active Directory中

树：

1. 使用连续命名空间的域，以层级形式组合。
2. 域之间使用Kerberos传递信任

林：

1. 一个或多个树
2. Common schema
3. Global catalog

# AD中的物理结构

通过决定when，where复制登录，进而优化网络流量。

* Domain Controllers
* Sites

## Domain controller

执行存储，复制，认证。

一个DC仅支持一个Domain，为确保稳定，每个domain应配置多个DC。

## Sites

站点是groups of well-connected computer/subnets，用以优化位于不同位置的DC间通信。

两个主要功能：

1. 优化网络内的复制流量  
   连接快的，放在同一个站点，更频繁地复制。  
   连接慢的，放在不同站点，控制复制频率。
2. 加快登录验证  
   用户会首先尝试通过相同站点（相同子网）的DC以验证。

## AD partitions

1. Domain partition  
   存储该域所有对象副本，且仅复制到该域其他DC
2. Configuration partition  
   forest topology（DC，connection）
3. Schema partition  
   forest-wide schema

Configuration和Schema在林中每个DC中复制。

# Operations Master Roles

为避免DC复制冲突，一些特定操作由特定角色来操作。只有拥有该类角色的DC才能做出对应修改。

## Forest-wide Roles

Schema Master

包含用于创建新对象所需的object classes和attributes。

Domain Naming Master

控制林中域的添加与删除

## Domain-wide Roles

Primary domain controller emulator(PDC)

新域中的第一个DC

Relative identifier master(RID)

创建新对象时分配一个唯一security identifier(SID)

=domain SID + RID

Infrastructure master

定期更新跨域对象的引用（GUID，DN，SID）

# Trust

受信任域的账户/组，可以访问信任域的资源。

## Transitive

默认在同一林的不同域中建立双向信任。

## Explicit

尽管默认同林中的域建立transitive trust。管理员仍可为下级域，或跨林域建立explicit single-way trust。

# How AD works

管理资源，极具扩展性。

## Directory Service

结构化“仓库”，用以存储对象及其属性，还有连接方式，用以定位及管理他们。

Capabilities:

1. 根据已知属性找到目标对象。
2. 用户无需知道物理位置或协议，即可找到目标。
3. 可存储极大量对象。

## AD Schema

树中通用，存储object classes和attributes。

属性仅定义一次可重复使用，可以通过新增属性来扩展类。

## Global Catalog

存储了所有对象的属性的DC，用以检索，管理员可以设置所需存储的属性。若无，则需去林中的每个域中进行搜索。

包含：

1. 常用检索属性
2. 确认独享位置的必备信息
3. 根据搜索人的权限来展示检索到的结果。

建议每个站点部署一台GC服务器

## Distinguished and Relative Distinguished Name

客户端使用Lightweight Directory Access Protocol（LDAP）来搜索和修改AD数据库中的对象。

LDAP是X.500的子集，X.500是为构建目录的行业标准。

DN

例子：shanghai.com域中sales组织单位中名为Suzan的用户。

CN = Suzan, OU = sales, DC = shanghai, DC = com

RDN

用于标识容器中的对象。

以上例子中为 Suzan

UPN

Suzan@shanghai.com

## AD如何启用单点登录

启用单点登录，方便用户。一次登录，全面应用。

单点登录：

1. 验证，验证链接尝试的凭据
2. 授权，连接尝试被允许

# AD与DNS

Query DNS查询SRV记录来找到DC。

# New Forest

创建林的第一个DC，将有以下情况：

1. Schema and Configuration Naming contexts  
   Dcpromo会创建，其他DC将一直从源DC复制
2. 林中首个DC变为GC  
   若需要其他GC则需管理员手动操作。
3. 承担5个角色  
   PDC emulator，RID，Infrastructure，Schema，Domain naming。  
   若被选为GC则Infrastructure Master不会启动。
4. 建立第一个站点及默认IP站点链接。

# Windows 2000 和Windows Server 2003

Windows Server 2003可以：

1. 支持应用程序分区
2. 可以使用Kerberos建立Transitive Trust
3. Reverse schema changes
4. 用户对象多选，同时修改多个
5. 保存查询
6. 使用命令行工具，dsadd，dsquery，dsmove