



# Windows安全原理与技术

## — 第四章：活动目录

王轶骏, Eric

*[Ericwyj@sjtu.edu.cn](mailto:Ericwyj@sjtu.edu.cn)*

SJTU.INFOSEC.A.D.T, 2008



# 活动目录基础



## ■ 背景

- 计算一直趋向于更大的网络和更为分布式的发展方向。
- 现代操作系统必须提供对分布式资源、实体和关系进行管理的机制。
- 现代操作系统应该能够支持在地理位置上相互分离的网络用户。
  - 外部网络
  - 企业内部网
  - 家庭办公



# 活动目录的作用



## ■ 目录服务的作用

- 允许用户使用对象的名称或者属性就可以搜索到相应的网络资源。
- 目录可以分布在网络中的多台计算机上，而无须考虑地理位置。
- 目录可以复制，更能防止访问失败。
- 目录可以分割保存，这就允许存储大量的对象。
- 目录的安全性可由管理员统一定义和实施。



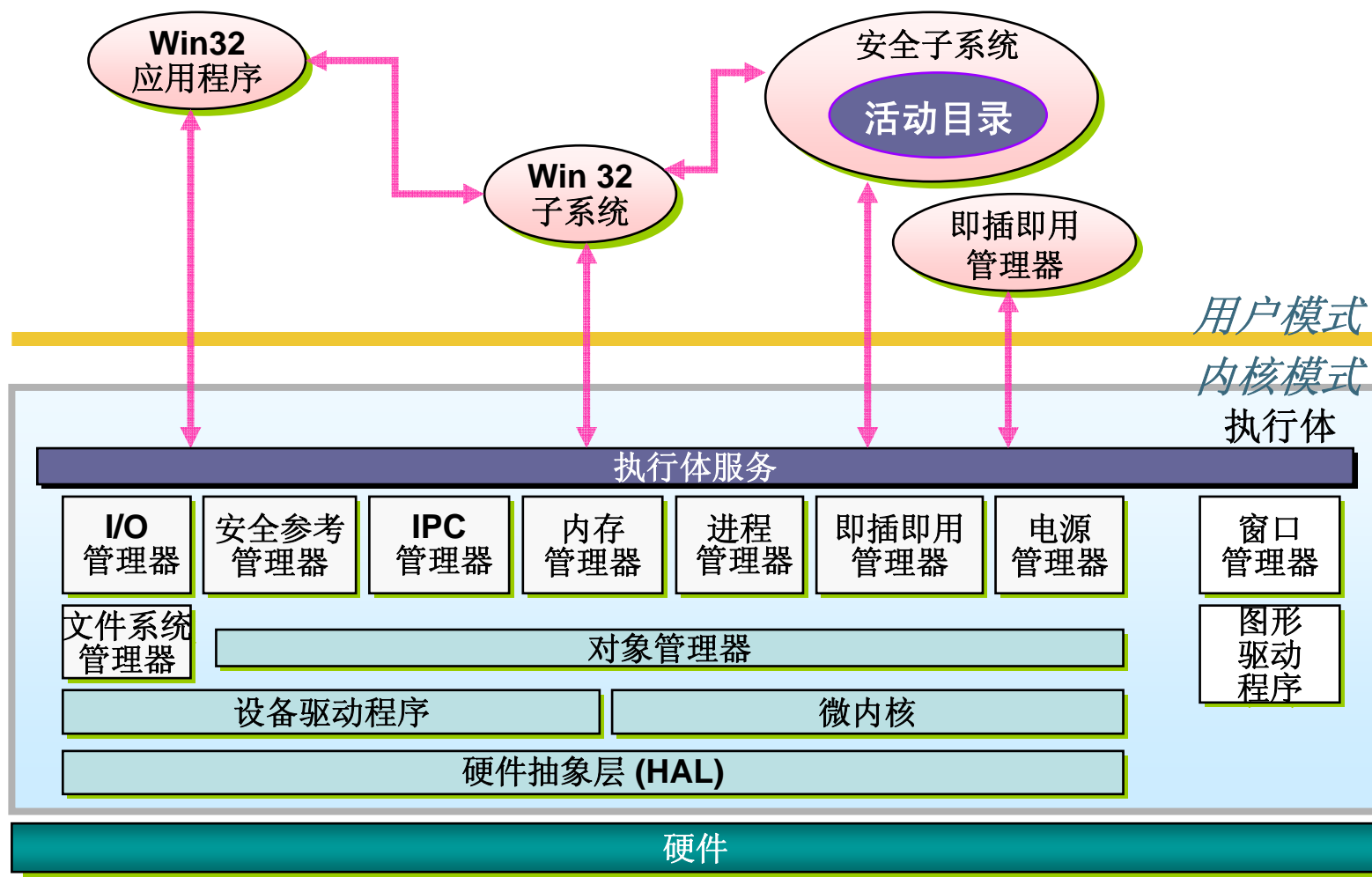


## ■ 活动目录作为Windows 2000所实现的一种目录服务

- 允许在网络资源与用户之间分配信息。
- 对网络安全起到中心授权机构的作用。



# 活动目录在Windows体系结构中的位置





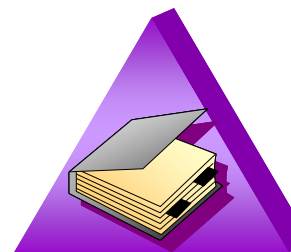
# 活动目录的内容

## ■ 目录

- 目录是一种存储网络对象信息的层次结构。
- 对象包括用户、计算机、共享资源等。

## ■ 目录服务

- 目录服务把目录和使目录信息对用户有效所需的服务组合起来。
- 通常向用户隐蔽了物理的网络拓扑和协议。
- 单一视图
- 多主复制



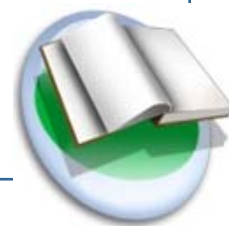
# 单一视图

- 不管用户从何处访问或者信息处在何处，都提供给用户统一的视图。
- 更容易在高度分布的网络中搜索、管理和使用资源。



## 多主复制

- 活动目录为了在分布式环境中提供很好的性能、可靠性和灵活性，采用了“多主复制”（Multimaster Replication）技术。
- 通过安装域控制器，就可以在整个网络环境中创建目录的多份复本。
- 网络中任何地方发生的变化都会在整个网络中自动复制。





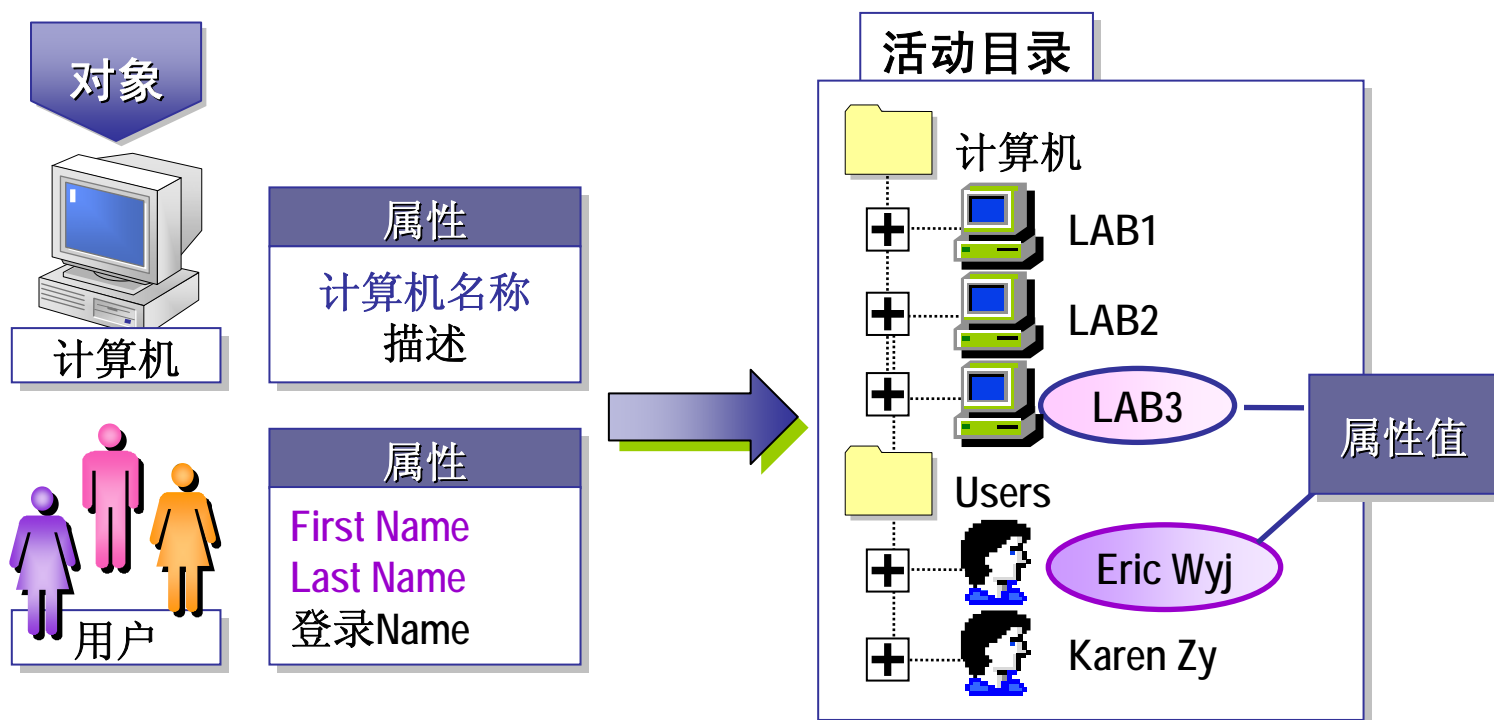
# 活动目录的优势

- 简化管理
- 增强安全性
- 扩展可操作性
- 基于策略的管理
- 很强的可伸缩性
- 智能的信息复制能力
- 灵活的查询能力



# 活动目录对象

- 活动目录对象是组成网络的实体。
- 一个对象是一些显式命名的属性集合。
- 对象的属性就是指在目录中对象的特征。



# 对象的分类



## ■ 容器对象

- 可存储其它对象。
- 如域、用户组、文件夹等。

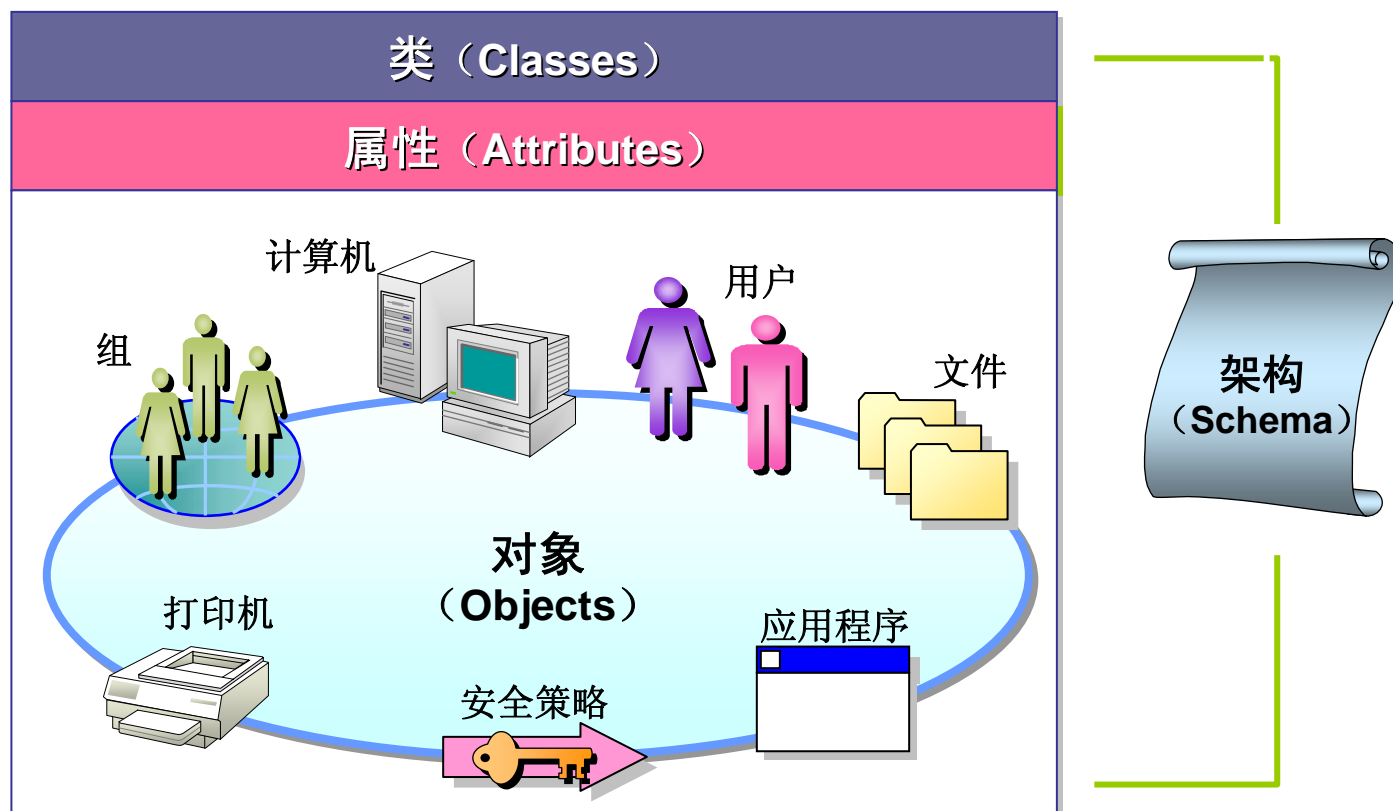
## ■ 叶对象（非容器对象）

- 不能存储其它对象。
- 如计算机、用户、文件等。



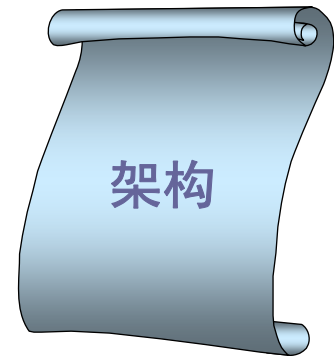
# 活动目录架构

- 在活动目录中，可以将对象组织成类。
- 架构描述了对象类和对象类的属性。





- 架构定义了每一种对象类的：
  - 必须具有的属性
  - 可以具有的额外属性
  - 可以成为其父类的对象类
- 每个活动目录对象都是某对象类的一个实例。
- 架构本身也是活动目录中的对象
  - 类架构对象
  - 属性架构对象



# 对象的标准属性



- 活动目录架构中每一类别的对象都可以保证下列标准的属性：
  - 目录数据存储区中的每一对象都具有唯一的标识，即全局唯一标识符（**GUID**）。
  - 对于安全主体（用户、计算机或组），与Windows NT 4.0操作系统和早期版本中所用的安全标识符（**SID**）的兼容性，即安全主体名称。
  - 目录对象名称与LDAP标准的兼容性，即**LDAP DN**和**RDN**。
- 活动目录将为以上这些属性生成具体的值，而其它属性值则必须由人输入。





# 对象的命名规则

- 安全主体名称
- 安全标识符
- 与LDAP相关的名称，包括专用名称DN和相对专用名称RDN
- 全局唯一标识符（**GUID**）



# 安全主体名称

- 安全主体名称是在单个域内用来唯一标识用户、计算机或组的名称。
- 安全主体名称在域内必须唯一，而在域间则无需唯一。
- 安全主体名称的命名规则
  - 名称最多可包含 20 个大写或小写字符，但以下字符除外： " / \ [ ] : ; | = , + \* ? < >
  - 用户名、计算机名和组名不可以只包含英文句号 (.) 或空格





# 安全标识符（Security Identifier, SID）



- **SID是Windows 2000系统安全子系统为安全主体对象（即用户、组和计算机账户）创建的唯一数字。**
- **网络上的每个账户都会在首次创建时获得唯一的一个SID。**
- **Windows 2000系统的内部进程引用的是账户的SID，而不是账户的用户或组名。**



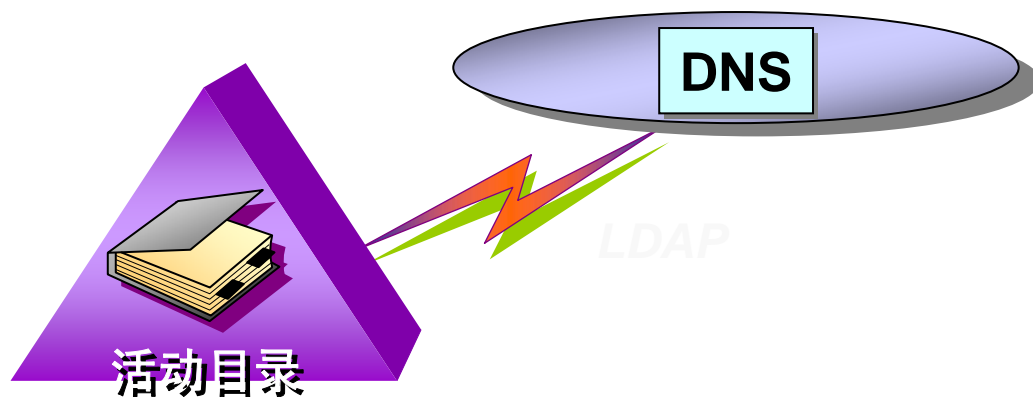
# LDAP专用的名称与相对专用的名称

(Distinguished Name, DN  
Relative Distinguished Name, RDN)



## ■ LDAP (Lightweight Directory Access Protocol)

- 在Windows 2000系统中，所有对活动目录对象的访问都是通过LDAP进行的。
- LDAP定义了目录中查询和修改信息时将执行的操作以及安全访问目录中信息的方式。



# DN和RDN



- **DN**定义了到对象的完整路径。
- **RDN**则是**DN**中属于对象自身属性并定义对象自己名称的那一部分。
- 通过使用对象的完整路径（包括对象名称以及域根节点的所有父对象名称），**DN**标识了域层次中的唯一对象。
- 每个**RDN**都保存在活动目录数据库中，并含有一个对其父对象的引用。
- 在**LDAP**操作期间，整个**DN**都是按照到根节点的引用来构造的。
- 在完整的**DN**中，所要标识对象的**RDN**在左边，并含有叶结点名，右边以根节点结尾。



一个LDAP DN示例:

cn=eric, ou=gongfang, ou=Teaching, dc=SjtuInfosec, dc=net

说明:

属性	说明
CN	公用名称
OU	组织单位名称
DC	域组件名称



DN, 专用的名称

Domain\_Name/Teaching/gongfang/Eric Wyj

RDN, 相对专用的名称

Domain\_Name

Teaching OU

Gongfang OU

Eric Wyj

Eric Wyj

Eric Wyj



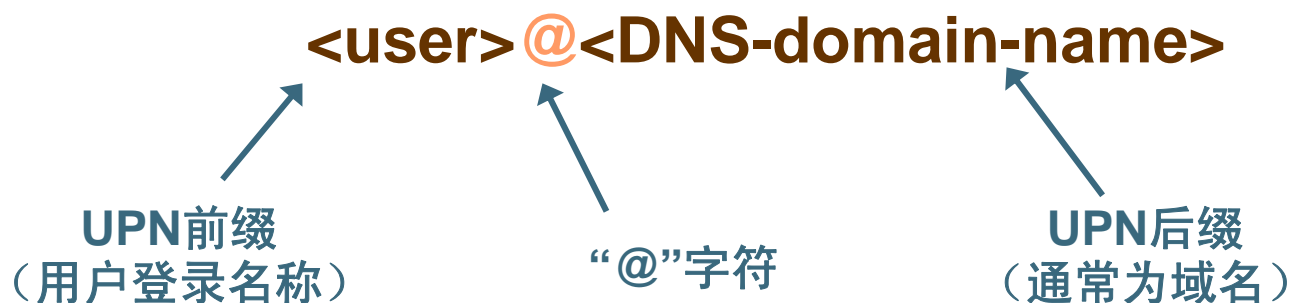
# 全局唯一标识符 (Global Unit Identifier, GUID)

- GUID是在对象创建时由活动目录分配的128位数字。
- GUID不能被修改和删除。



# 用户主体名称 (User Principal Name, UPN)

- 在活动目录中，每个用户账户都有一个格式如下的用户主体名称：





# 不同环境下的对象名称

## ■ 对象处于单一域内

- 由活动目录生成的安全标识符、**GUID**、**LDAP**专用的名称都可唯一的标识目录中的每个用户或计算机。

## ■ 对象被重新命名或移至另一个域内

- 由活动目录生成的安全标识符、**LDAP**专用的名称以及相对专用的名称都会发生变化。
- 由活动目录生成的 **GUID**不会发生改变。

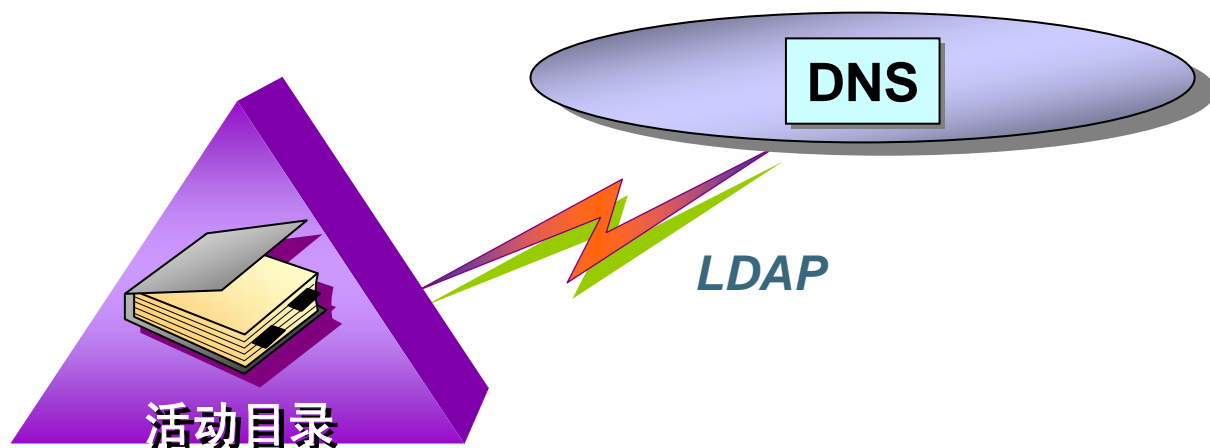




# 对象名称的解析

## ■ 活动目录和标准DNS协议在Windows 2000中的集成

- 共享相同的结构
- 不是相同的名称空间





## ■ 名称解析

- 是把名称转换成该名称代表的某一对象或信息的过程。

## ■ 名称空间

- 是任一有界的区域，在其中对给定的名称进行解析。

例如：电话号码簿、**Windows NTFS**文件系统



# DNS名称解析服务



## ■ DNS服务

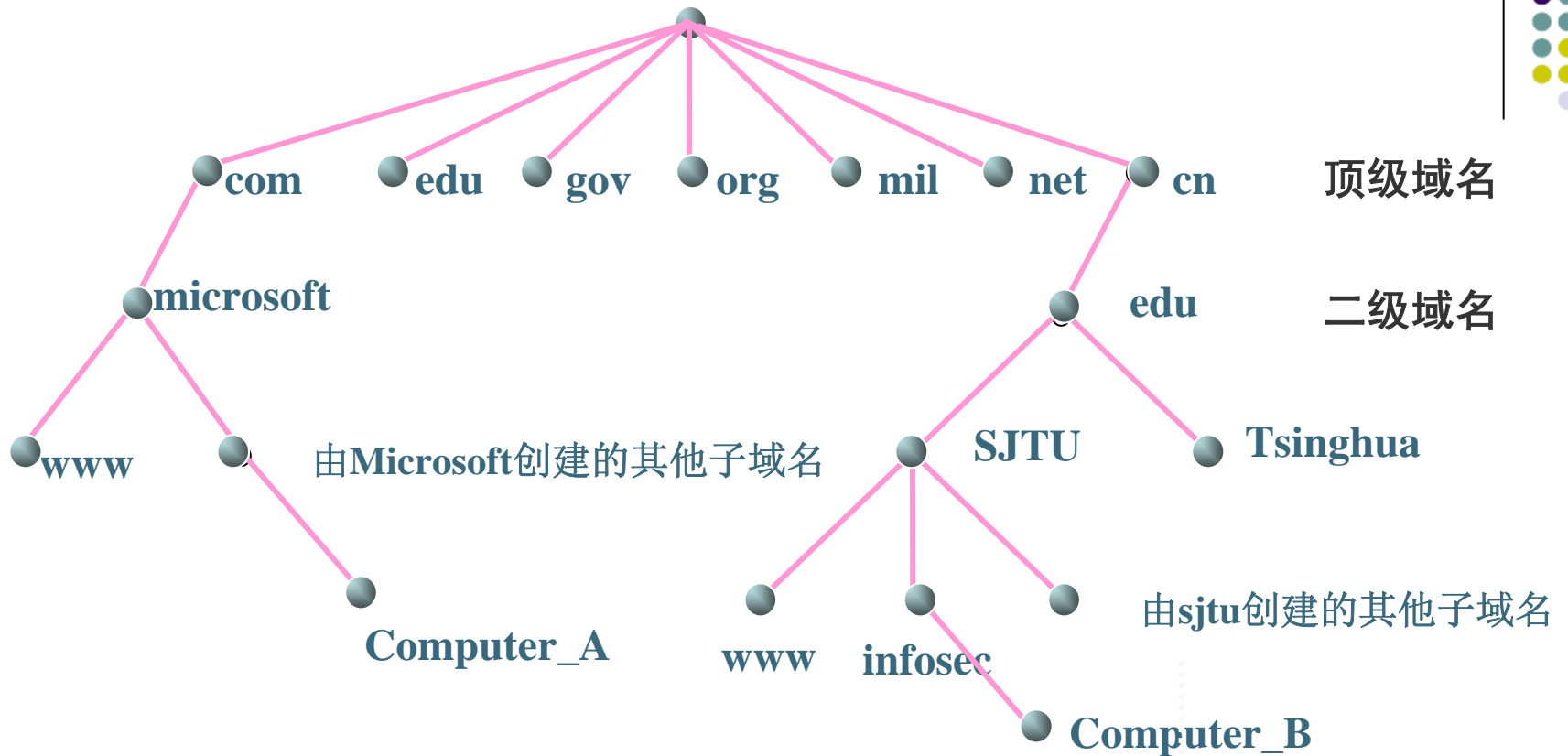
- 通过接受网络上的DNS请求并传入DNS数据库中，将用户能够理解的DNS名称或者计算机名称转换成IP地址。

## ■ DNS名称空间

- DNS组织成不同层次的域，使整个Internet成为一个名称空间。



## DNS名称空间的根目录



Computer\_B.infosec.sjtu.edu.cn

FQDN, Full Qualified Domain Name

# 活动目录与DNS的集成



- **DNS域和活动目录域的集成是Windows 2000的核心功能。**
- **两者共享一个相同的域结构，使用相同的域名。**
  - 如SjtulInfosec.net既是一个DNS域又是一个活动目录域。
- **两者是不同的名称空间，各自保存不同的数据，管理不同的对象。**
  - **DNS**保存区域以及资源记录（**SRV**）。
  - 活动目录保存域和域对象。
- **DNS区域可保存在活动目录中。**
- **活动目录客户机使用DNS来定位域控制器。**



## ■ DNS

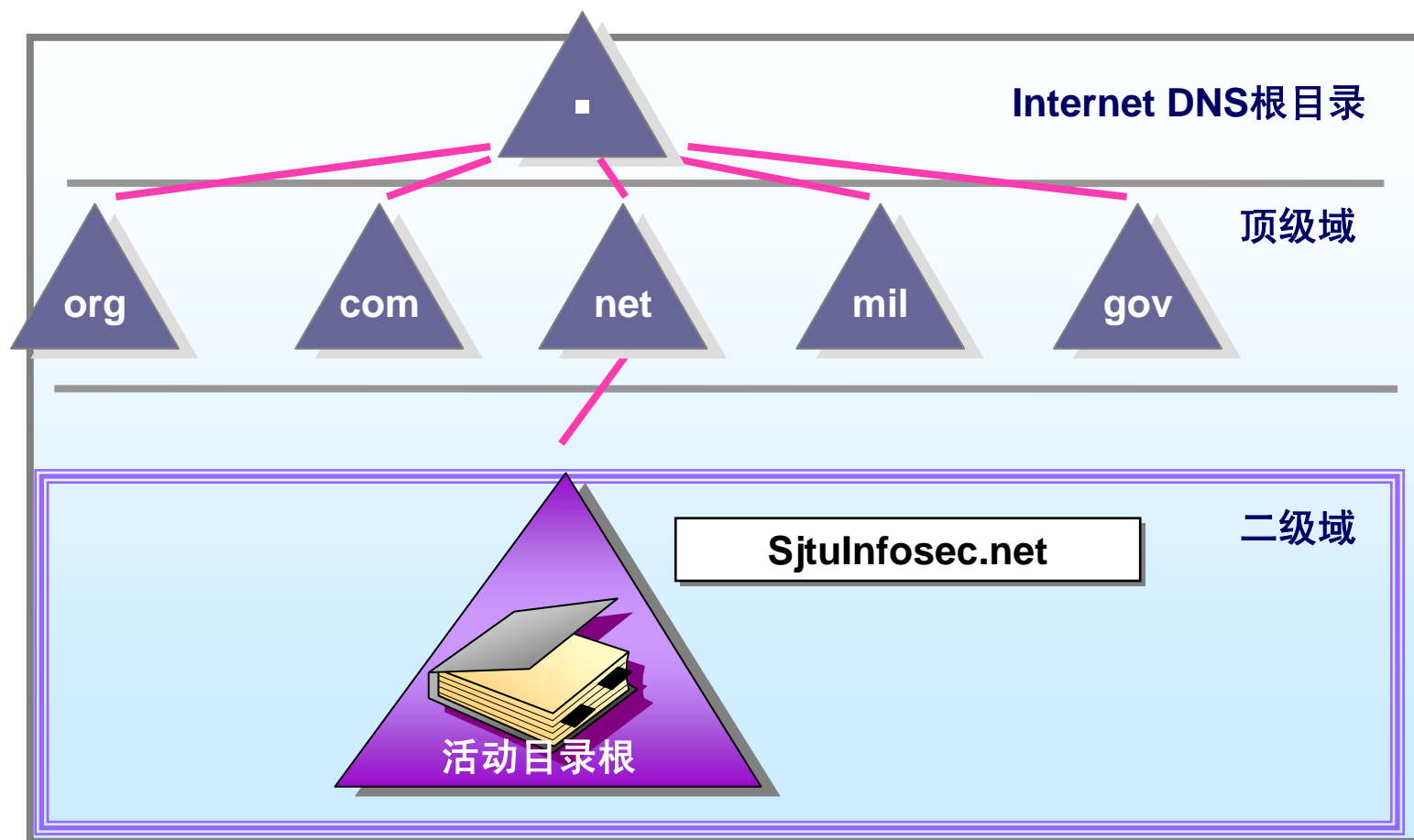
- 名称解析服务。
- 将DNS服务器接受的请求视为对DNS数据库的DNS查询。
- 将域名或计算机名解析成IP地址。
- 不需要系统启动活动目录。

## ■ 活动目录

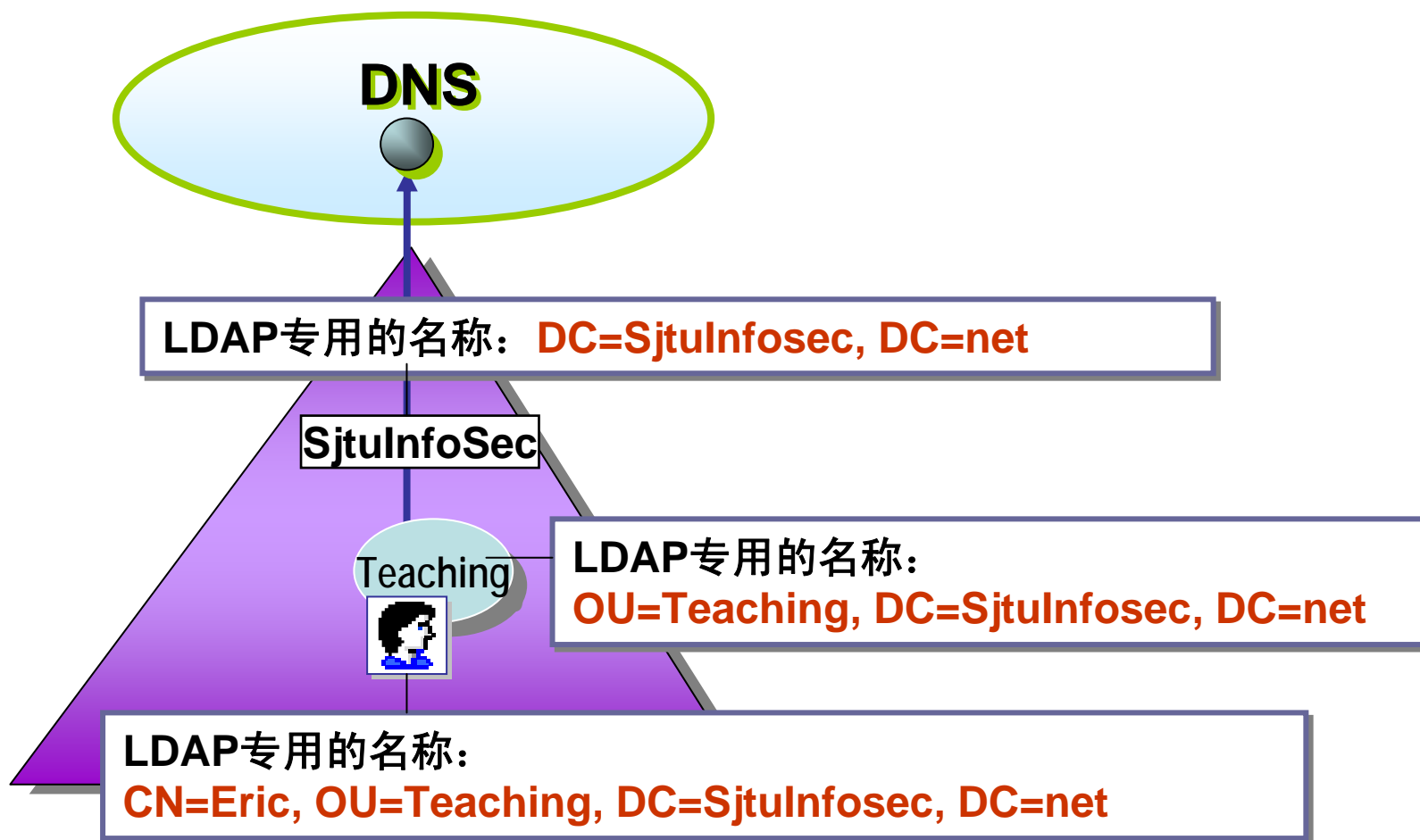
- 目录服务。
- 将域控制器接受的请求视为LDAP搜索或对活动目录数据库的搜索。
- 将域对象名称解析成对象记录。
- 需要系统启动DNS。



# 活动目录与全局DNS名称空间



## 解析唯一标识对象的LDAP名称





# 活动目录组件



## ■ 逻辑结构

- 域 (**Domain**)
- 组织单位 (**Organizational Unit, OU**)
- 域树 (**Tree**)
- 域森林 (**Forest**)

## ■ 物理结构

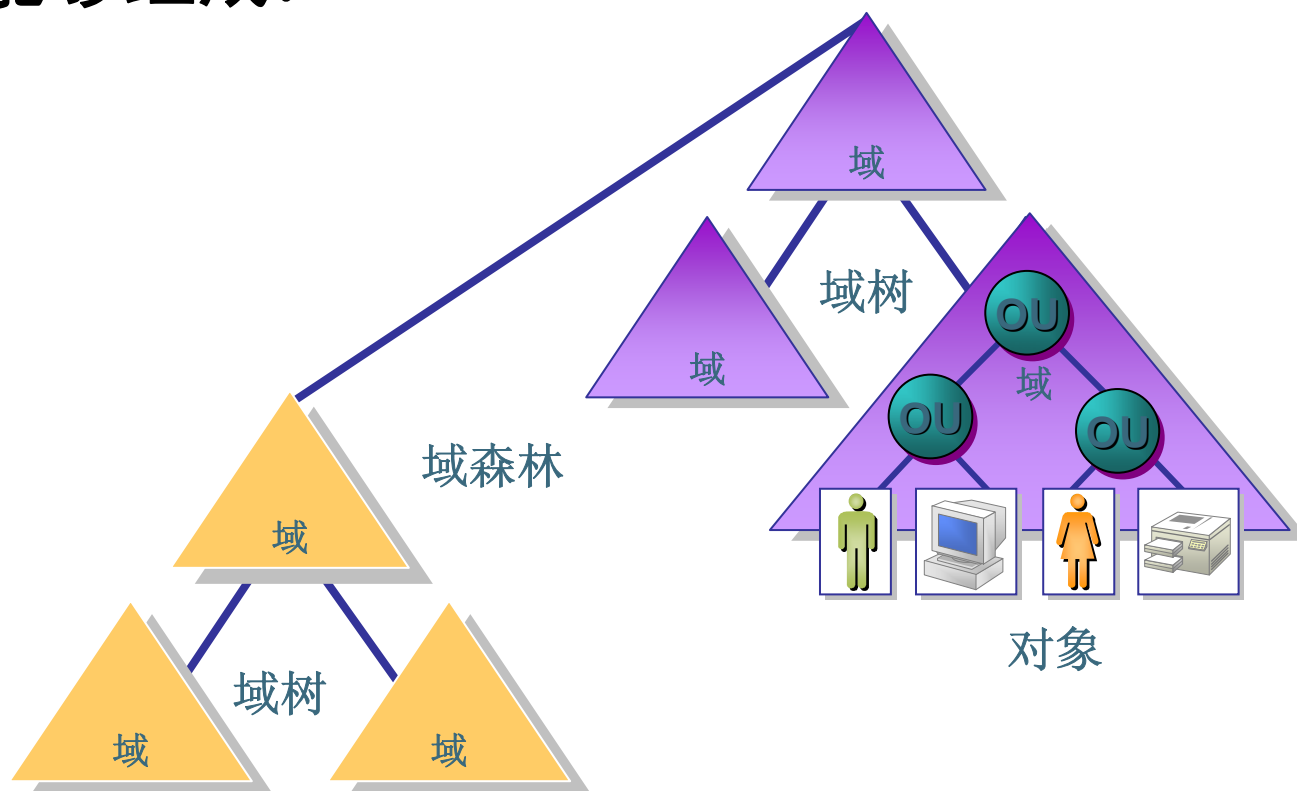
- 站点 (**Site**)
- 域控制器 (**Domain Controller**)



# 活动目录的逻辑结构组件

- 域和组织单位组成等级层次结构。
- 多重域能够组成：

- 树
- 森林

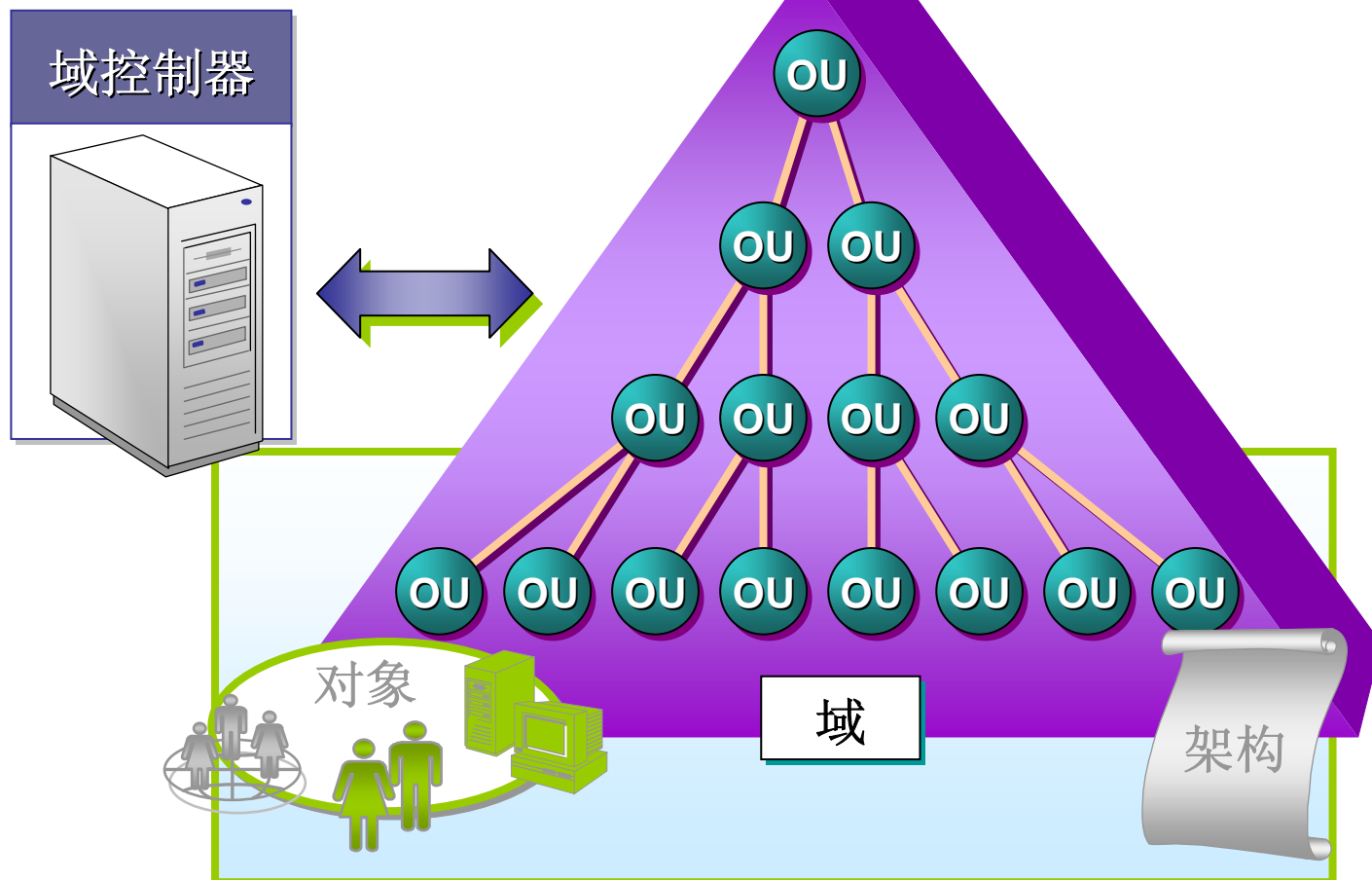


# 域 (Domain)

- 活动目录由一个或多个域组成。
- 域是网络中复制和安全性的基本单元。
- 创建初始域控制器的同时也就创建了域，不可能创建没有域控制器的域。



OU = 组织单位





## ■ 使用域可以实现的管理目标

- 界定安全区域
- 复制信息
- 应用组策略
- 设计网络结构
- 委派管理权限





## 组织单位（OU）

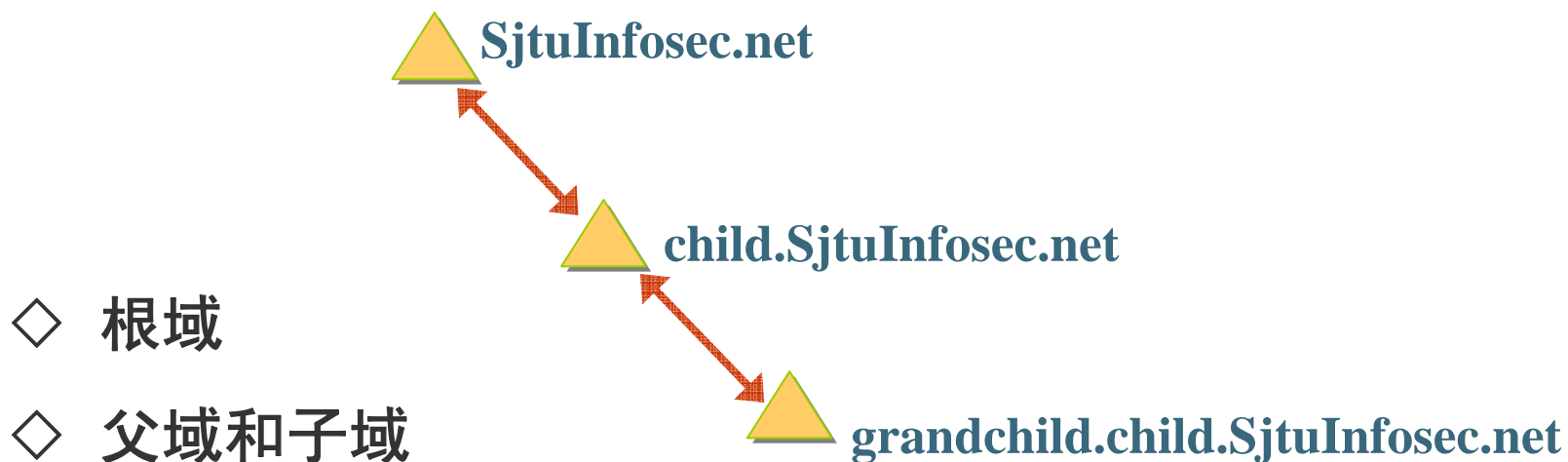
- 组织单位是一种目录对象，也是一个容器，它被用作把同在一个域中的对象组织到逻辑管理组中。
  - 可在一个组织单位中放置用户、组、计算机、打印机、共享文件夹以及一个域内的其他组织单位。
  - 组织单位主要用来委派对用户、组及资源集合的管理权限。组织单位是委派管理权限的最小分组。

组织单位（Organizational Unit, OU）又称部门，是Windows 2000系统新增的内容。

# 域树

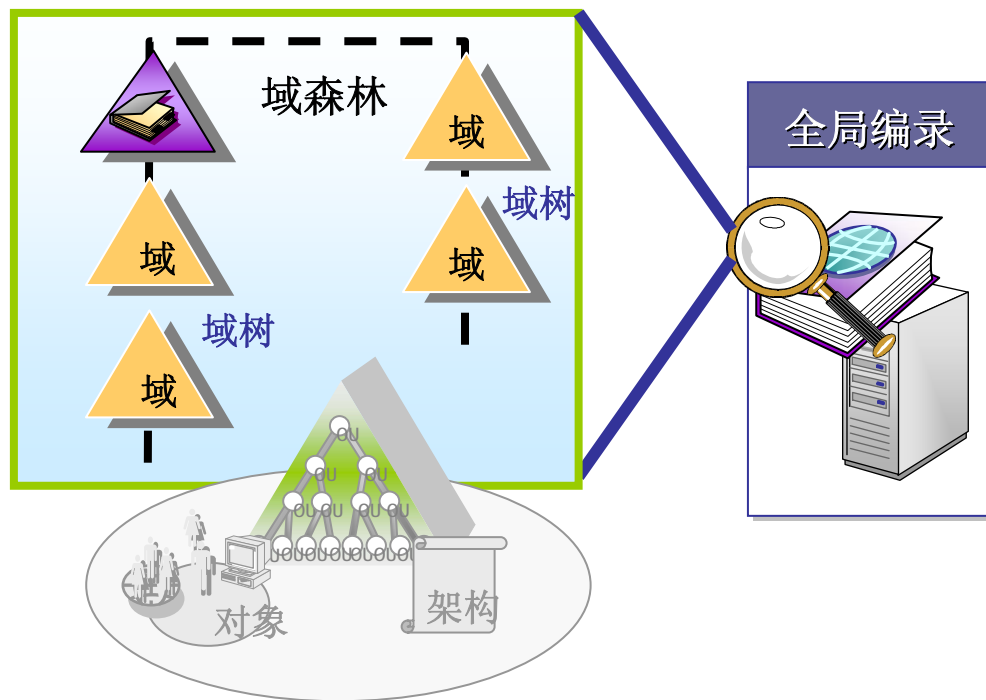


- 域树是对具有连续名称空间的一个或多个域的分组或分层排列的形式。



# 域森林

- 域森林是对一个或多个相互隔离、完全无关的域树进行分组或者分层次排列的形式。
- 域森林中
  - 所有的域树共享公共的架构。
  - 多个域树之间没有连续的名称空间。
  - 所有的域树共享一个公共的全局编录。
  - 所有的域树独立运作，但可以在整个组织内实现通讯。
  - 所有的域树之间默认存在双向可传递信任关系。







# 混合模式域和本地模式域

## ■ 混合模式域（Mixed Mode）

- 既有Windows NT域控制器又有Windows 2000域控制器的域。

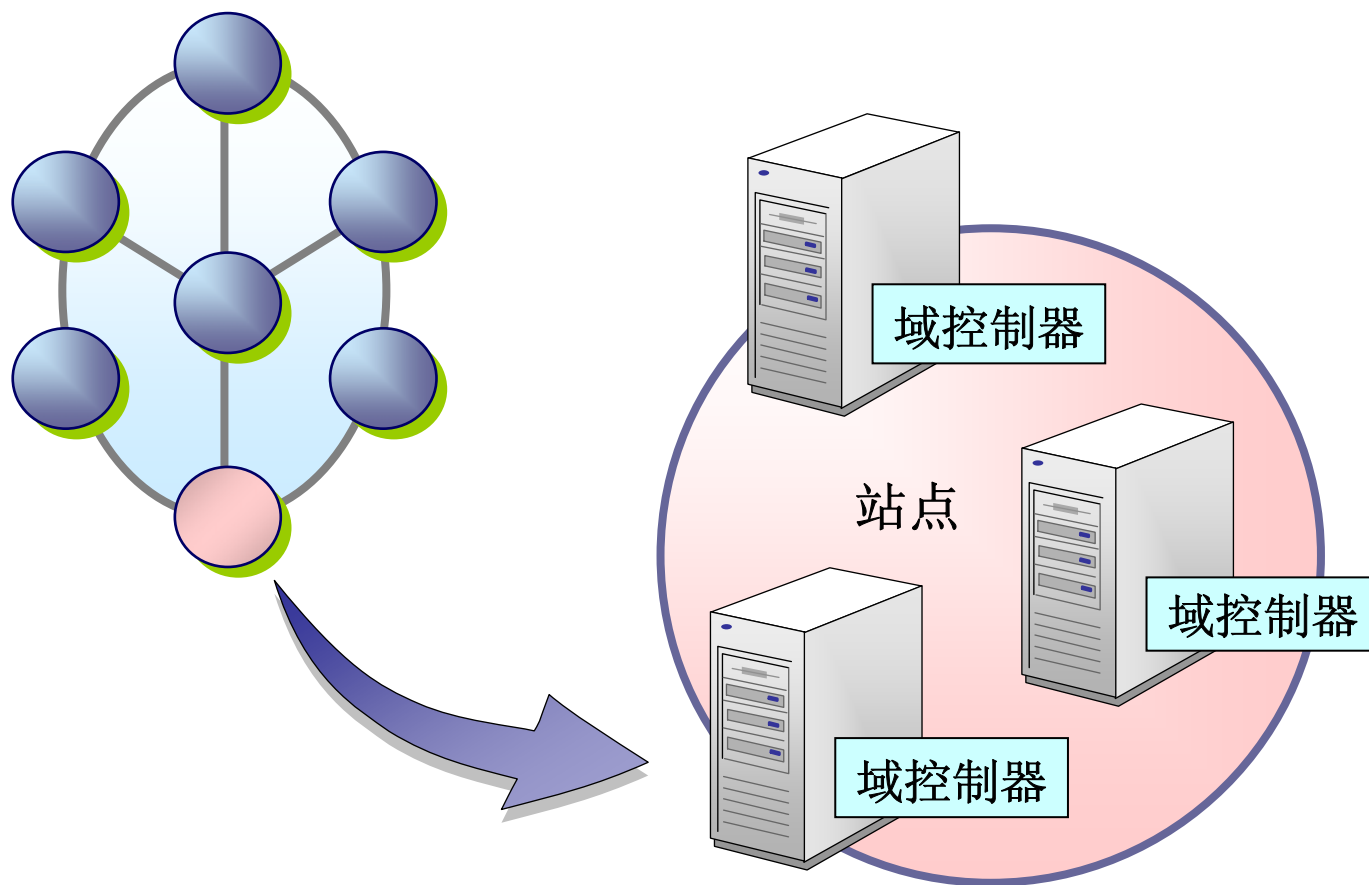
## ■ 本地模式域（Native Mode）

- 只有Windows 2000域控制器的域。

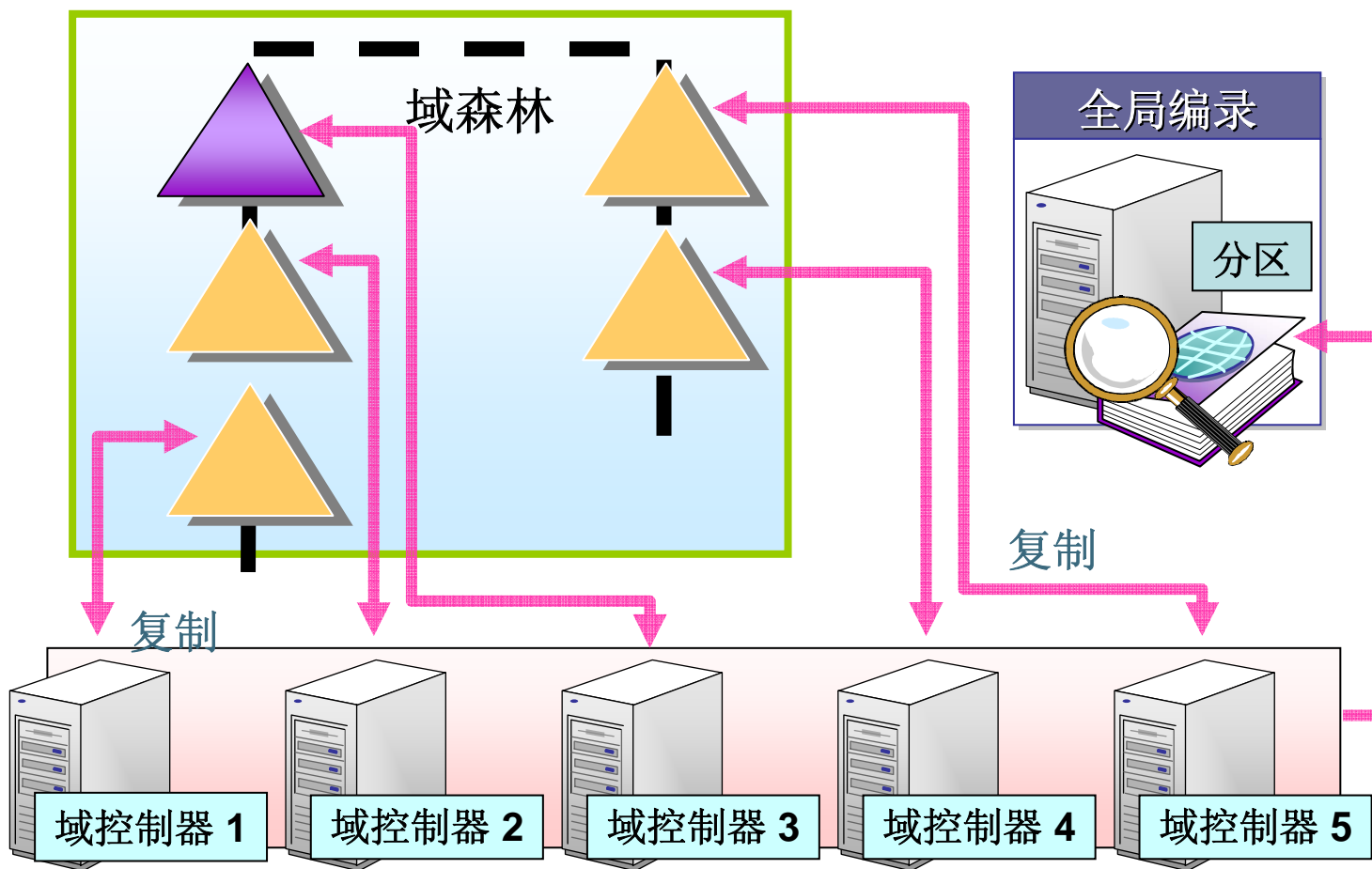
## ■ 混合模式域→本地模式域

- 升级所有的域控制器
- 切换过程不可逆

# 活动目录的物理结构组件



# 活动目录物理结构的操作



# 域控制器 (Domain Controller)



- 域控制器保存了整个域范围内的目录数据（如系统安全策略），并管理用户域交互（包括用户登录、验证和目录搜索）。

## ■ 域控制器的生成

- 安装活动目录就能把Windows 2000服务器变成域控制器。
- 安装时可以选择创建一个新域，也可以分配给一个现存的域。
  - 一个域可以有多个域控制器。
  - 一个域控制器只能控制一个域。





## 域控制器之间的角色

- **Windows 2000**域控制器之间扮演的是“对等”角色。
  - 支持“多主机复制”，可在所有域控制器之间复制活动目录信息。
- **Windows NT Server**主域控制器（**PDC**）和备份域控制器（**BDC**）之间扮演的是“主/从”角色。
  - 只有**PDC**有目录的可读写副本，**PDC**会把目录信息的只读副本复制到**BDC**中。



# 全局编录 (Global Catalog, GC)



- 全局编录是一个域树或者域森林中的所有对象信息的中心仓库。
- 全局编录服务器
  - 默认情况下，全局编录在域森林的初始域控制器上自动创建。该域控制器就称为全局编录服务器。
  - 可以随意配置任何域控制器为全局编录服务器。



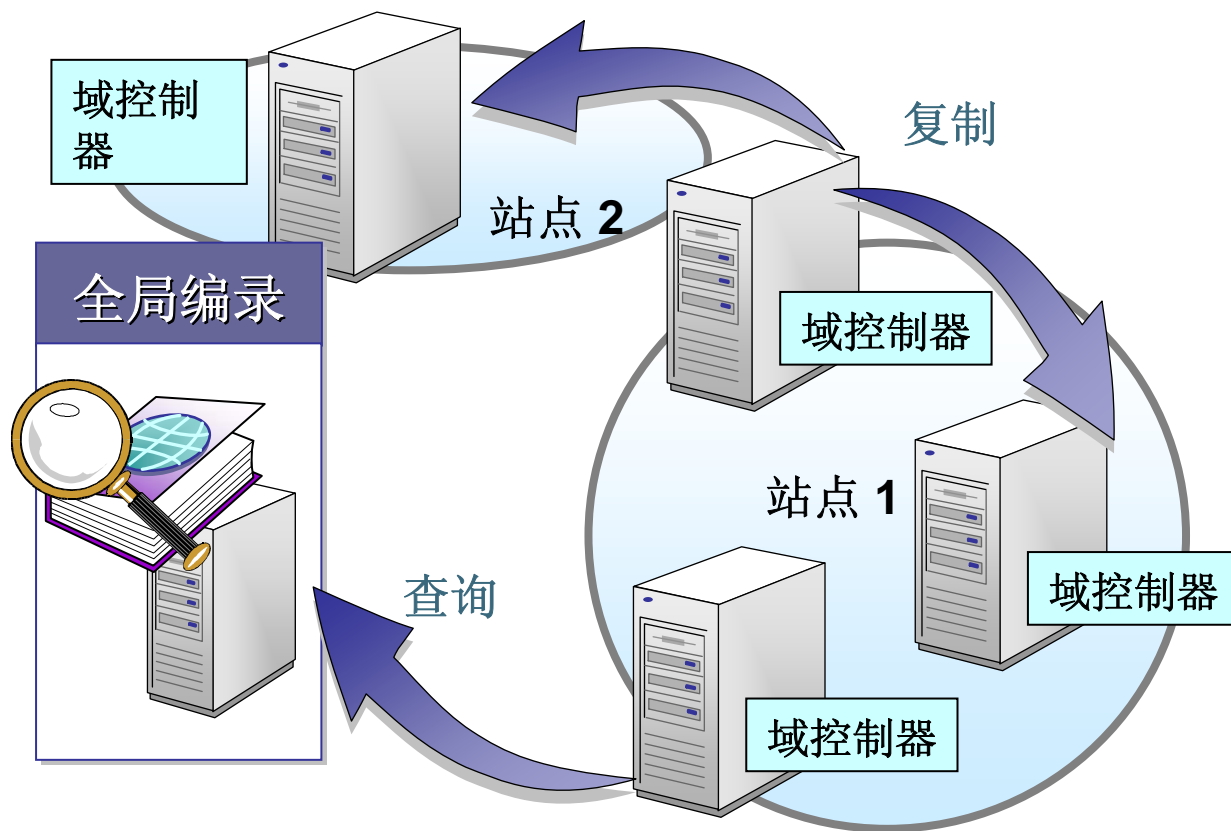
# 全局目录的任务



- 在客户登录时，向域控制器提供通用组成员信息。
  - 用户登录网络时，必须存在一台全局编录服务器，否则只能登录到本地。
  - 上述情况的例外是“域管理员组中的成员”。
- 在客户查询目录信息时，使其能够方便快捷的执行跨所有域的搜索，而不用具体考虑信息所在的域。
  - 多个全局编录服务器会减少客户查询的时间，但是会导致网络的复制通信量增加。
  - 推荐在每一个主要站点上设置一台全局编录服务器。



# 活动目录的信息数据流向





# 站点



- 站点是指在物理上有较好的线路连接的能实现较快通信速率的计算机的集合。
  - 一般是指一个局域网（LAN）。
- 站点之间一般是通过慢速连接来实现信息通信。
  - 一般是指广域网（WAN）。
- 站点是对网络上计算机的实际的物理分布的一种客观反映。



## 站点提供的服务

- 客户机可以向同一站点的域控制器请求服务。
- 活动目录尽量将站内复制的复制延迟降至最小。
- 活动目录尽量将站间复制的带宽消耗降至最小。
- 站点允许人为地安排站间复制的进程。



# 站点和域



## ■ 站点是独立于域的

- 站点映射网络的物理结构，域映射组织的逻辑结构。
- 站点和域名称空间之间没有必然的联系。
- 网络的物理结构和域结构之间也没有必然的关联。
- 活动目录允许在一个站点出现多个域，也允许一个域出现在多个站点中。





# 站点信息的使用

- 站点信息的指定：活动目录站点和服务工具
- 站点信息的用处：被活动目录利用来确定如何以最佳方式使用可用的网络资源。
- 利用站点可提高以下类型操作的效率：
  - 处理客户机请求
  - 复制目录数据





# 活动目录的复制

## ■ 域控制器中保存的信息包含以下三类：

- 域数据
  - 架构数据
  - 配置数据
- 每一类信息都位于单独的目录分区中

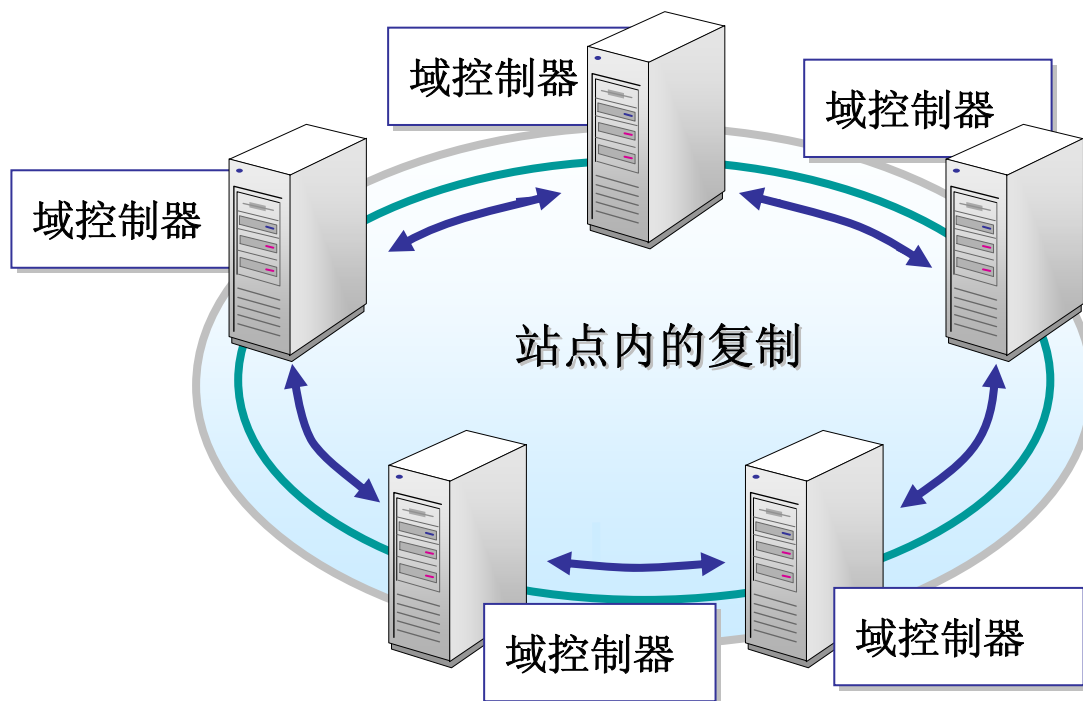
## ■ 作为全局编录服务器的域控制器中还保存第四种类型的信息：

- 为所有域保存域数据目录分区的部分副本



# 站点内复制 (Intra-Site Replication)

- 站点内目录信息的复制是频繁发生的，并且是自动进行的。
- 站点内复制被调节为复制延迟最小，也就是使数据尽可能地保持最新状态。



# 站点间复制（Inter-Site Replication）



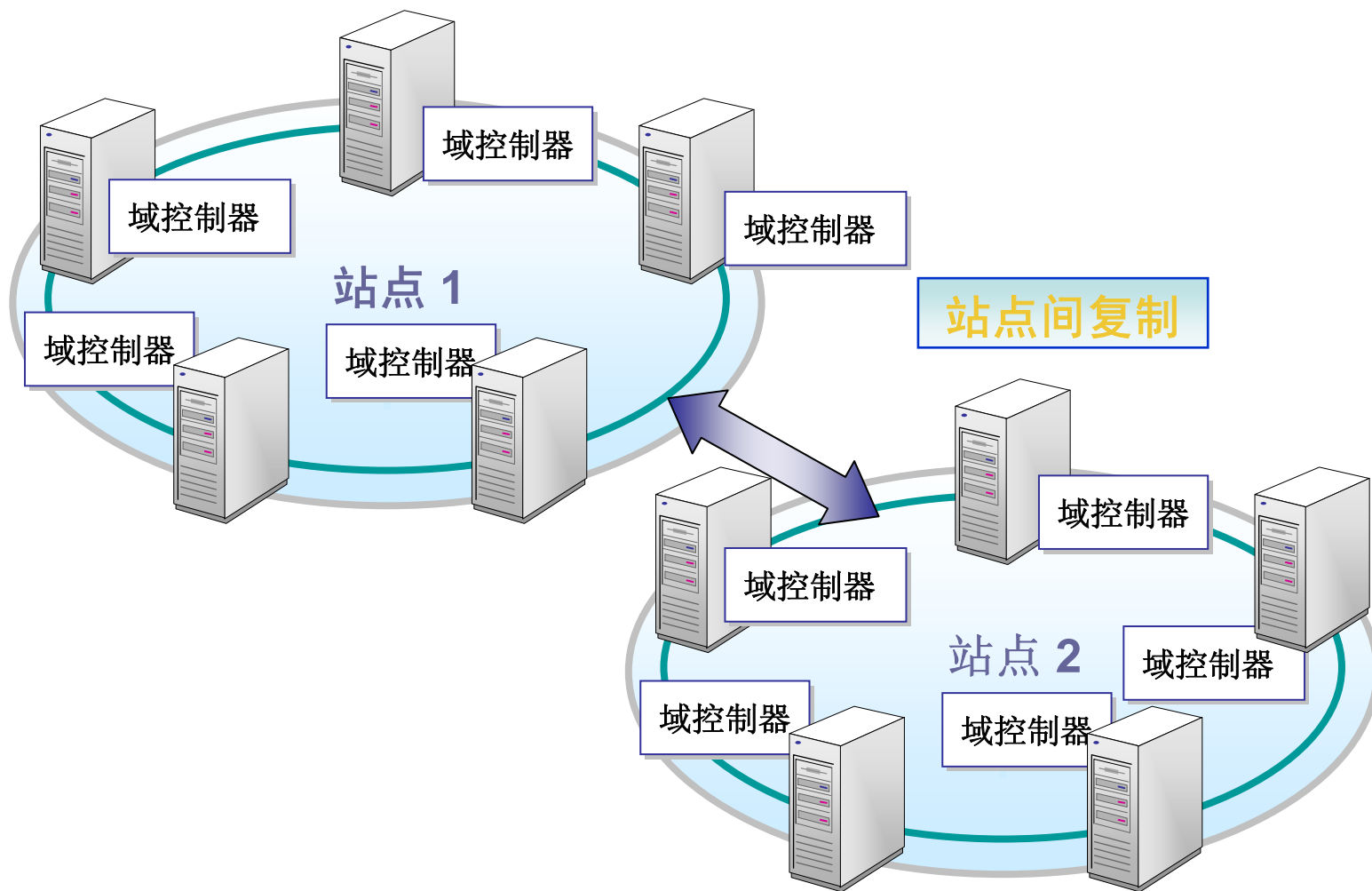
## ■ 多个站点的创建

- 优化WAN链接上的服务器到服务器的通信。
- 优化客户机到服务器的通信。

## ■ 站点间的复制

- 自动将站点的带宽消耗降至最小。







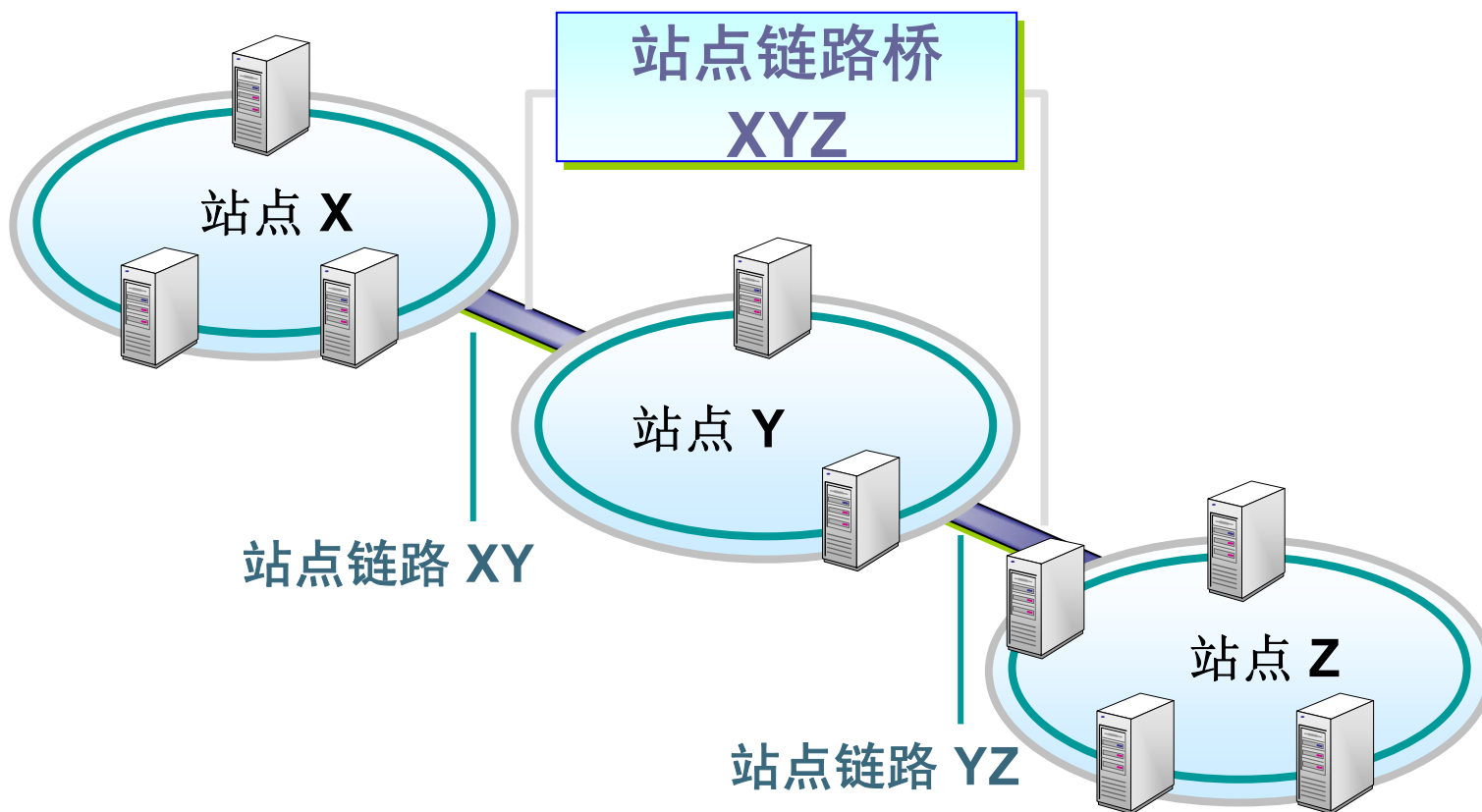
# 站点间的连接



## ■ 站点链接（Site-Link）

- 站点链接是指两个或多个站点之间的一个低带宽或不可靠的连接。
- 站点链接不是自动生成的，必须使用活动目录站点和服务工具来创建。
- 站点链接是可传递的。





# 活动目录的管理

## ■ 活动目录的安装

- 第一台域控制器的安装
- 第二台域控制器的安装

## ■ 实现组织单位的结构

## ■ 配置站点的设置

## ■ 管理任务的委派



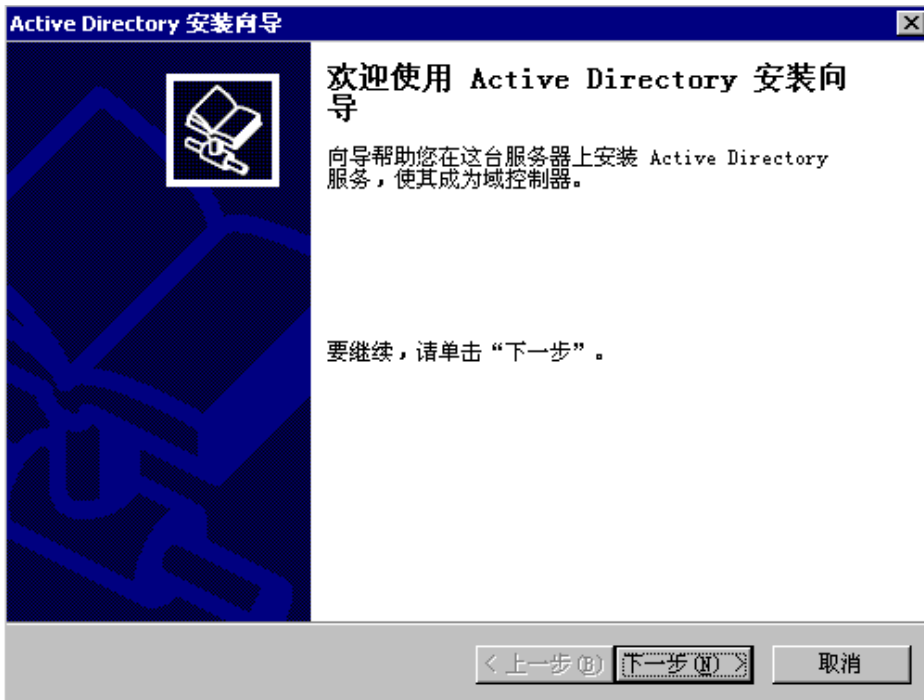


# 安装活动目录

## ■ 将一台独立的服务器提升为域控制器

- 确认安装了DNS服务器且正常运作（不过，在安装活动目录过程中也会提示安装DNS）
- “开始”→“运行”→`dcpromo.exe`



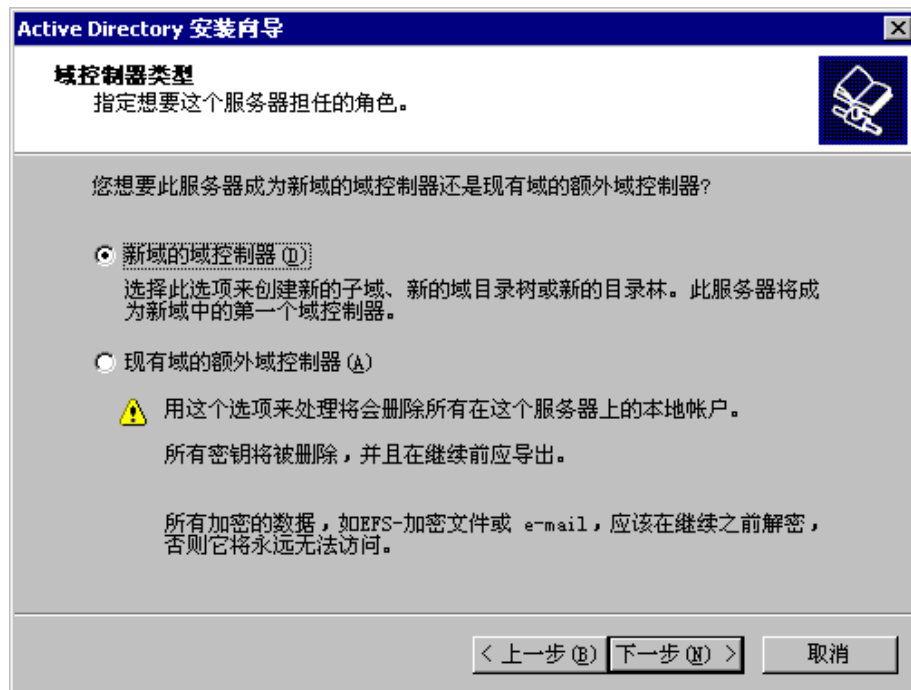


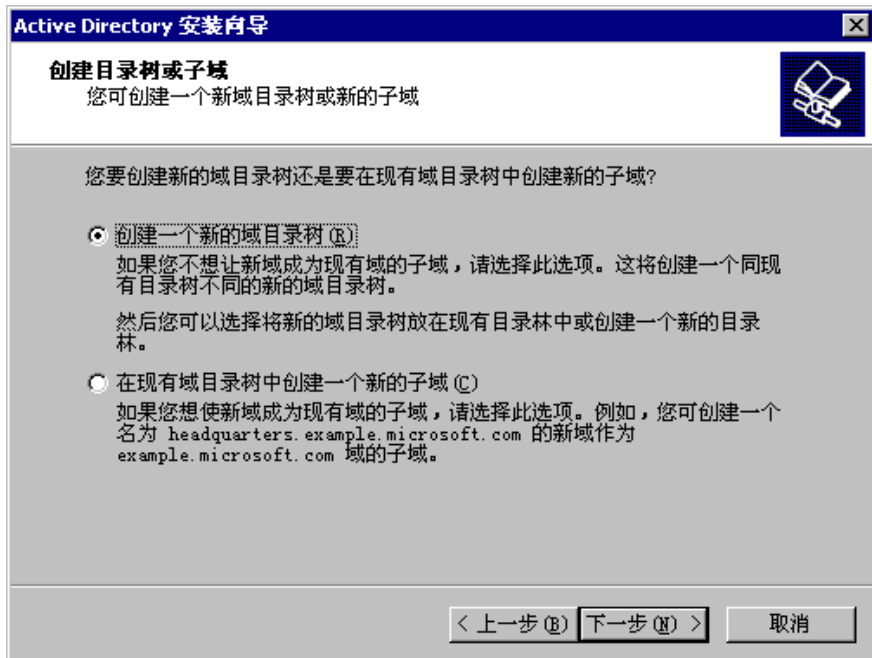
## ❖ 选择域控制器类型

❖ 新域的域控制器 ✓

❖ 现有域的额外域控制器

## ❖ 安装向导





## ❖ 创建目录树或子域

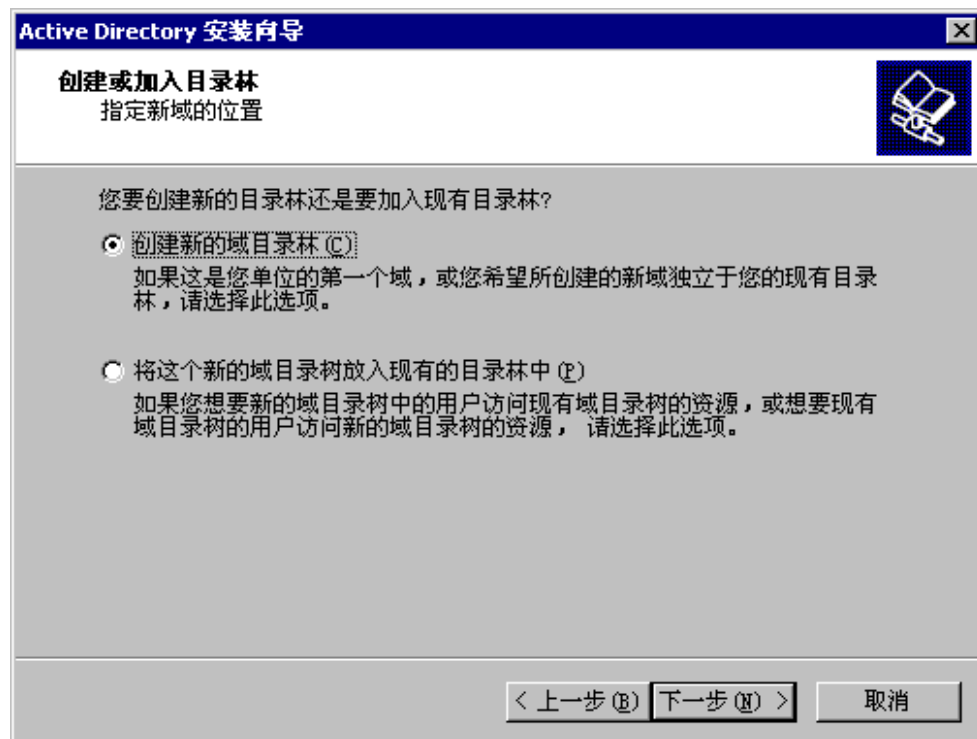
❖ 创建一个新的域目录树 ✓

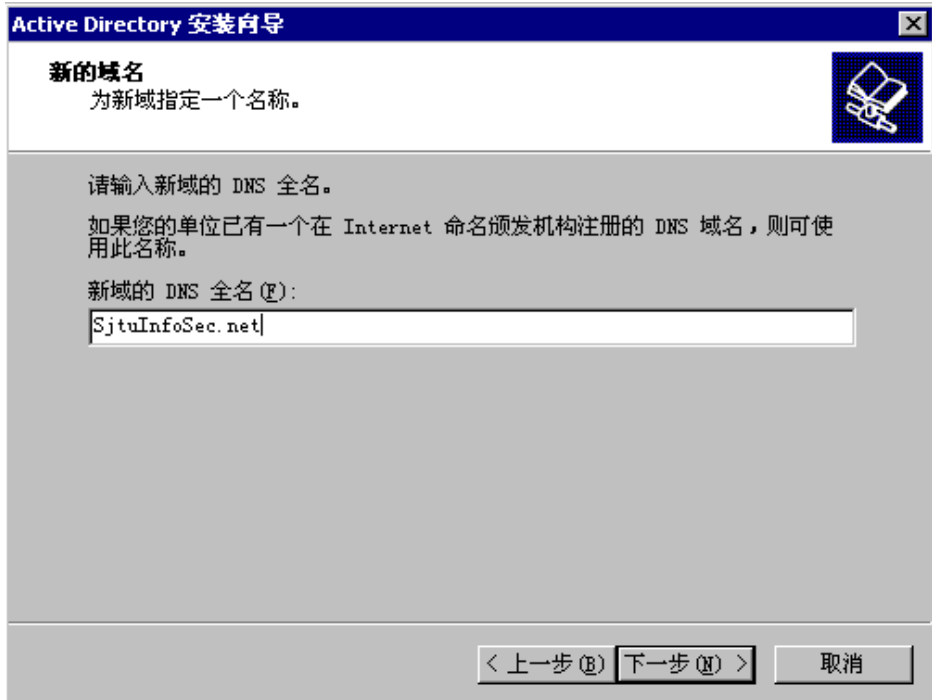
❖ 在现有域目录树中创建一个新的子域

## ❖ 创建或加入目录林

❖ 创建新的域目录林 ✓

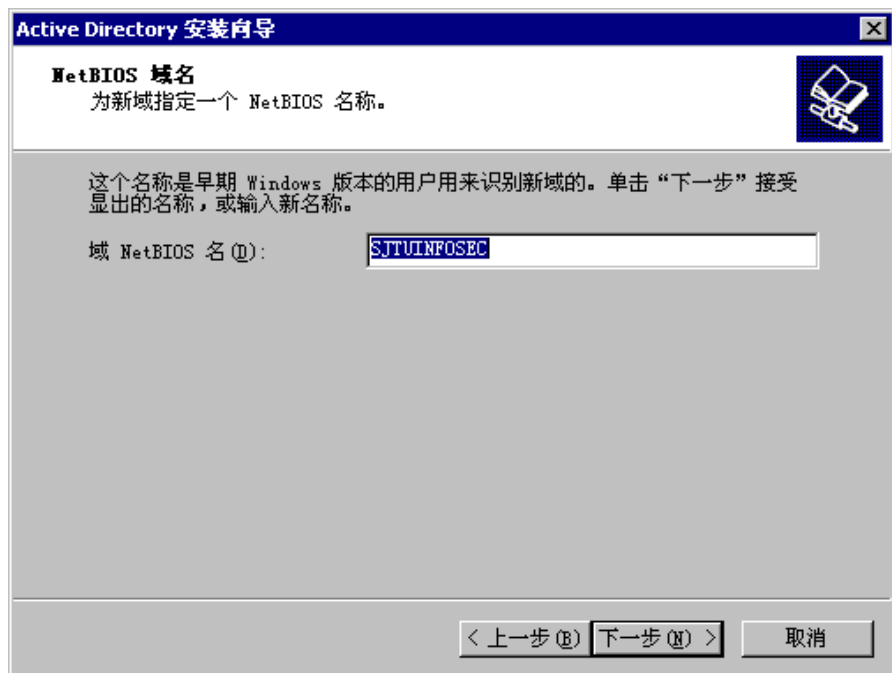
❖ 将这个新的域目录树放入现有的目录林中

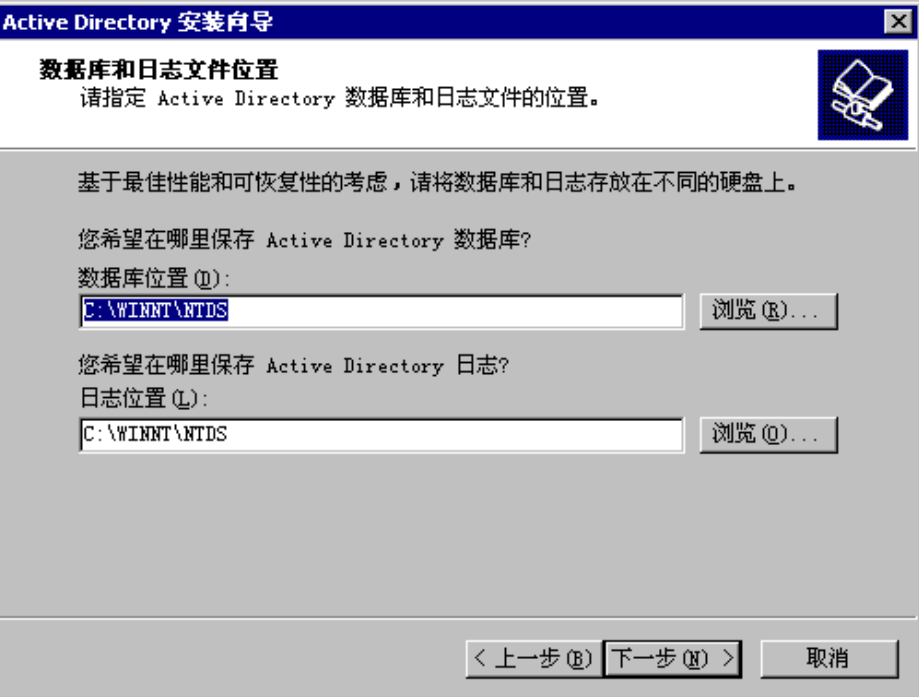




## ❖ 为新域指定名称

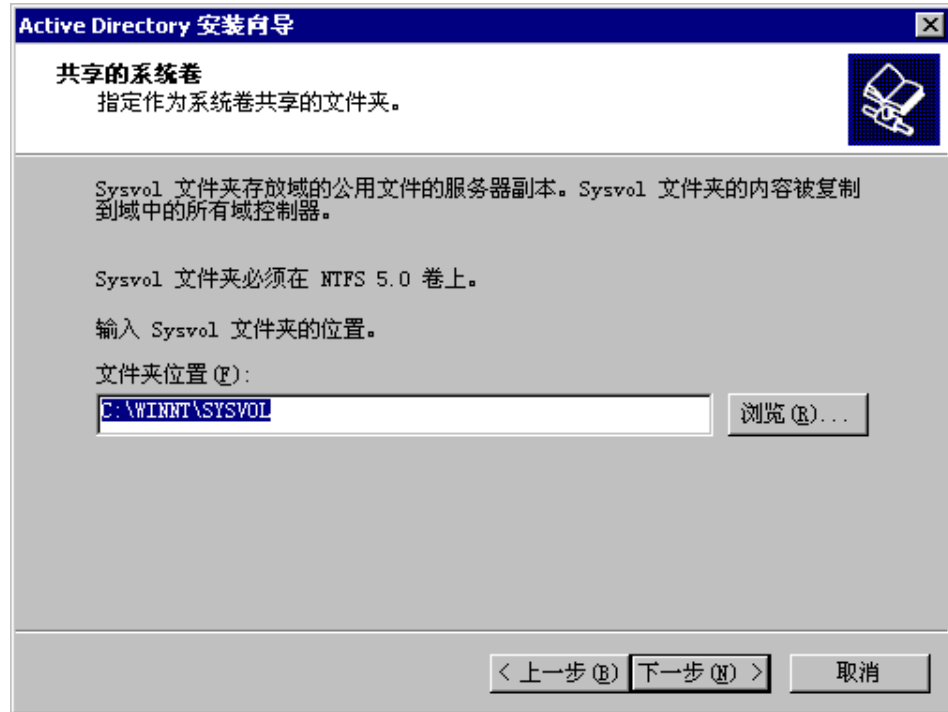
## ❖ 为新域指定Netbios名称



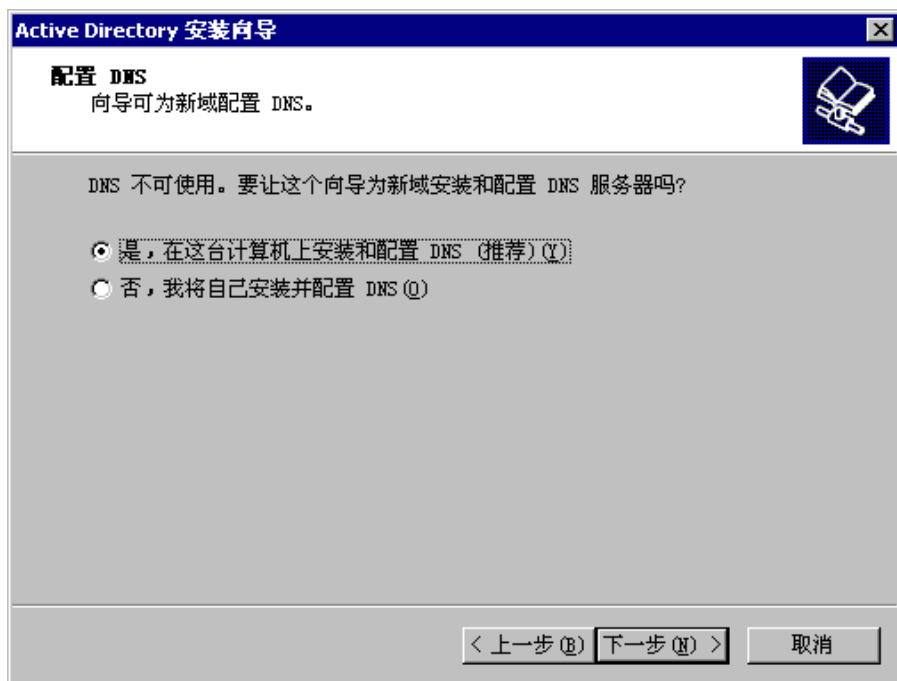
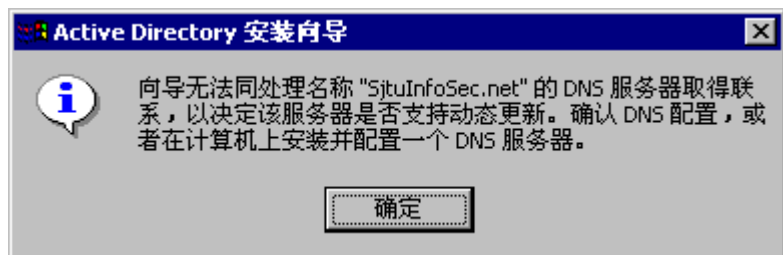


❖ 指定作为系统卷共享的文件夹

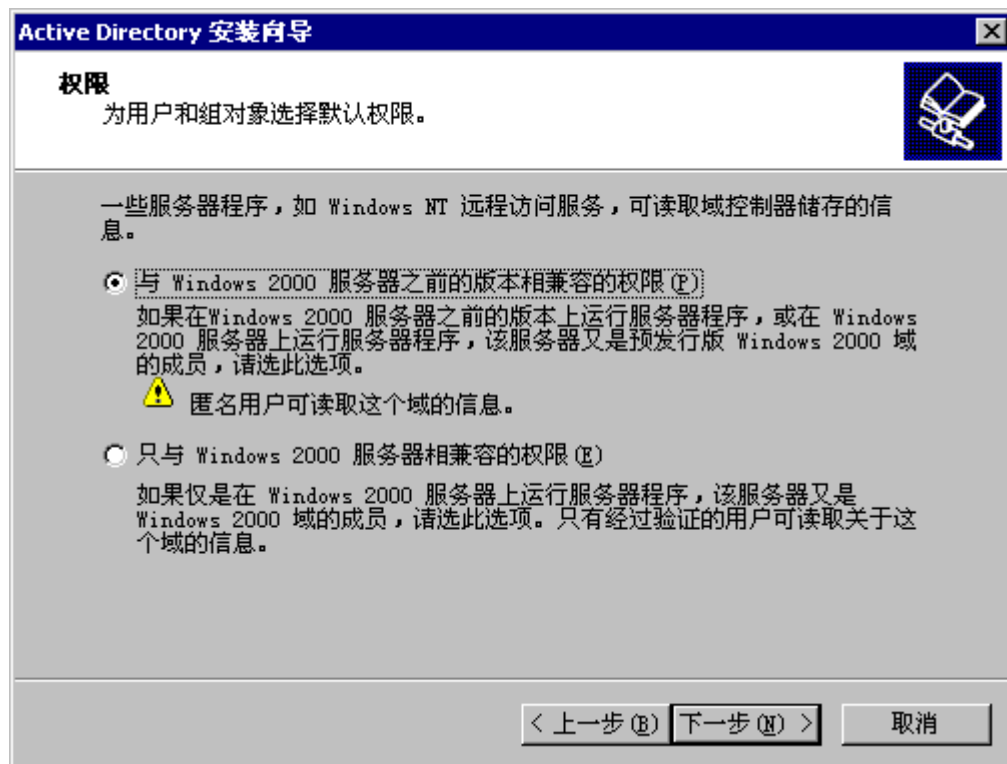
❖ 指定活动目录数据库和日志文件的位置







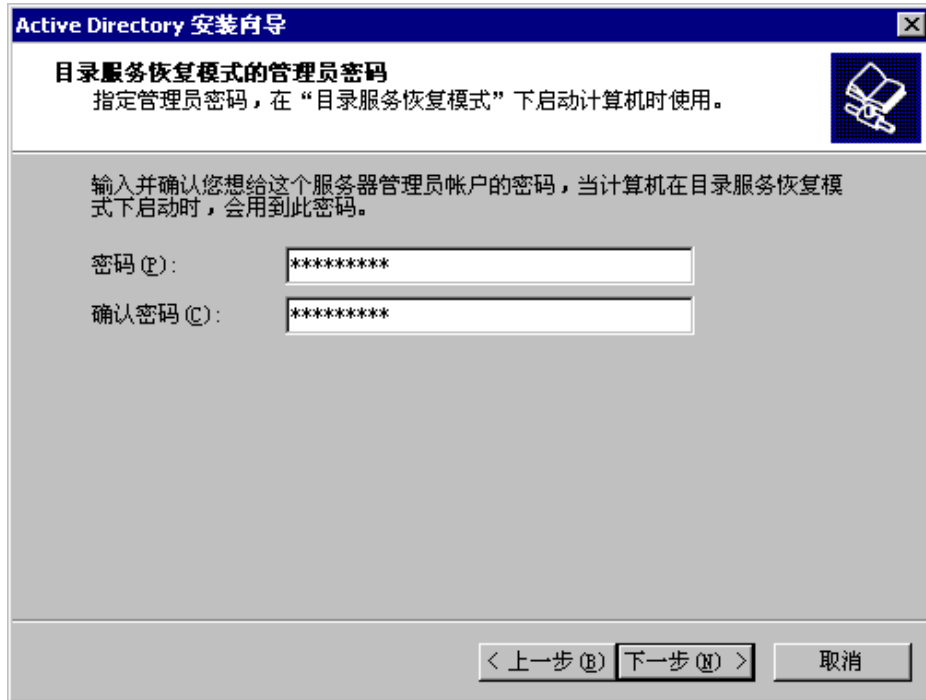
❖ 未安装DNS服务器时，为新域在这台机器上安装和配置DNS



## ❖ 为用户和组选择默认权限

❖ 与Windows 2000服务器之前的版本相兼容的权限

❖ 只与Windows 2000服务器相兼容的权限



## ❖ 输入目录恢复模式的管 理员密码

## ❖ 正在配置活动目录...





❖ 完成活动目录的安装



# 检验活动目录的安装

## ■ 检查DNS文件的SRV记录

- %systemroot%/system32/config/Netlogon.dns 文件中的 LDAP 服务记录

```
_ldap._tcp.SjtulInfoSec.net. 600 IN SRV 0 100 389 Server.SjtulInfoSec.net.
```

## ■ 验证SRV记录在nslookup工具中是否运行正常

- 在命令提示符下，输入nslookup
- 输入set type=srv
- 输入\_ldap.\_tcp.SjtulInfoSec.net，判断是否返回了服务器名称和IP 地址



# 活动目录的使用和管理

## ■ Active Directory域和信任关系

- 提供了域森林中所有域树的一个图形化视图。

## ■ Active Directory站点和服务

- 可以实现大型机构内部的管理功能。

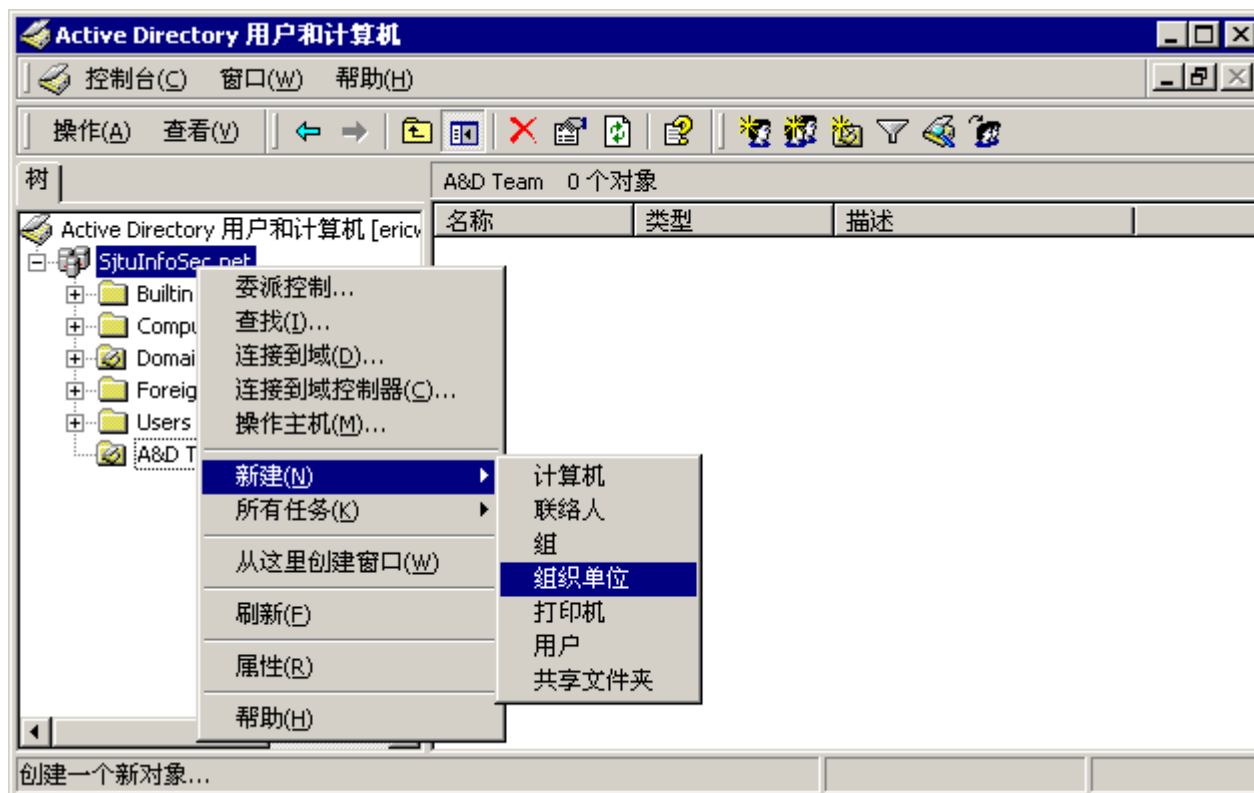
## ■ Active Directory用户和计算机

- 可以在活动目录内创建和管理用户、组、打印机、计算机对象和共享资源。

“开始”→ “程序”→ “管理工具”→ “Active Directory ...”

# 创建组织单位

“Active Directory用户和计算机”→ 右键点击对象（一个域或者另外一个OU）→ “新建”→ “组织单位”



# 使用“Active Directory用户和计算机工具”



- 创建组织单位，配置组织单位属性
- 创建、移动用户账户
- 创建组
- 把用户添加到组
- 发布共享文件夹
- 管理计算机
- 重命名、移动和删除对象
- 过滤一系列对象
- 设置ACL权限





# 设置组织单位属性



**A&D Team 属性** [?] [X]

常规 | 管理者 | 组策略

 A&D Team

描述 (D):

国家(地区) (C):

省/自治区 (V):

县市 (C):

街道 (S):

邮政编码 (Z):

确定 取消 应用 (A)

# 创建用户账户



新建对象 - 用户

创建在: SjtuInfoSec.net/A&D Team

姓 (L): steven

名 (F): sy 英文缩写 (I):

姓名 (A): stevensy

用户登录名 (U): steven @SjtuInfoSec.net

用户登录名 (Windows 2000 以前版本) (W): SJTUINFOSEC\ steven

< 上一步 (B) 下一步 (N) > 取消

新建对象 - 用户

创建在: SjtuInfoSec.net/A&D Team

密码 (P): \*\*\*\*\*

确认密码 (C): \*\*\*\*\*

☐ 用户下次登录时须更改密码 (M)

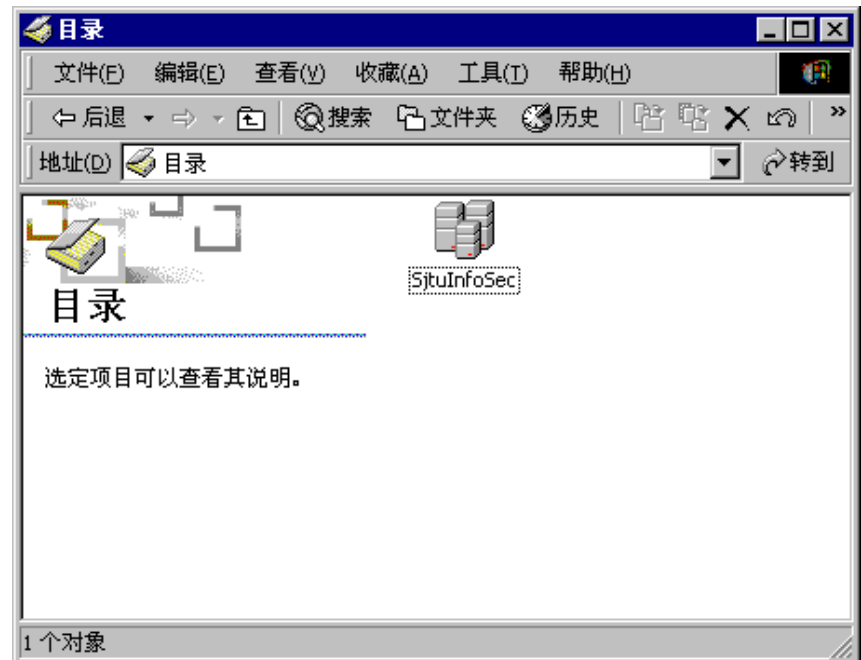
☐ 用户不能更改密码 (S)

☐ 密码永不过期 (U)

☐ 帐户已停用 (D)

< 上一步 (B) 下一步 (N) > 取消

现在就可以使用steven账户登录到Sjtuinfosec域中了，  
并且可以查看、搜索目录中的信息了



# 创建组



新建对象 - 组

创建在: SjtuInfoSec.net/A&D Team

组名 (A):  
develop

组名 (Windows 2000 以前版本) (W):  
develop

组作用域

☐ 本地域 (L)  
☒ 全局 (G)  
☐ 通用 (U)

组类型

☒ 安全式 (S)  
☐ 分布式 (D)

确定 取消

develop 属性

常规 成员 成员属于 管理者

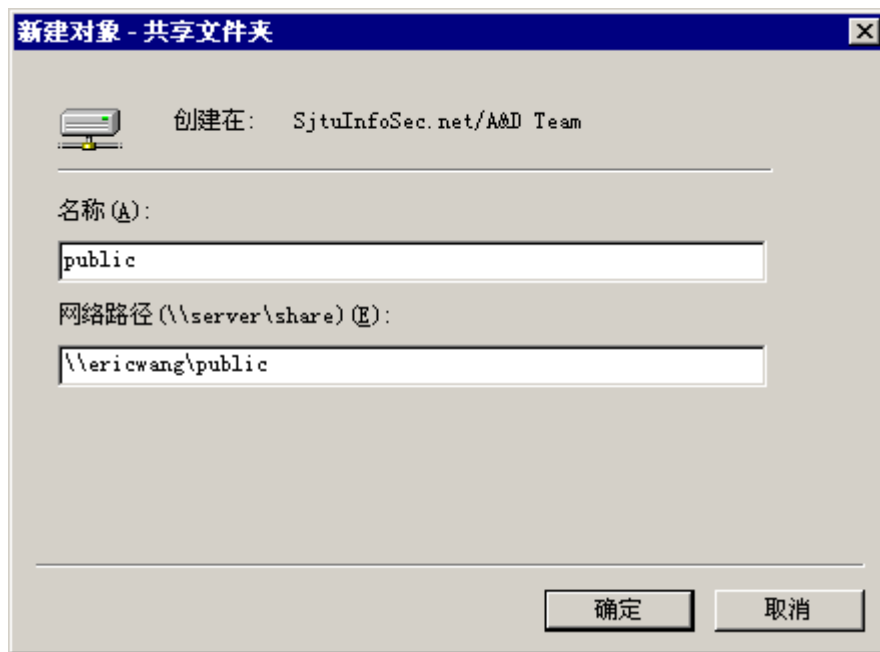
成员 (M):

名称	Active Directory 文件夹
ERICWANG2	SjtuInfoSec.net/Computers
stevensy	SjtuInfoSec.net/A&D Team

添加 (A) 删除 (R)

确定 取消 应用 (A)

# 发布共享文件夹



# 使用“Active Directory站点和服务工具”



- 显示有效的站点，创建、删除和重命名站点
- 显示参与到站点的服务器，删除或在站间移动服务器
- 显示使用站点知识的应用程序
- 显示站间的传输和链路
- 显示子网




# 添加新的站点

新建对象 - 站点

创建在: SjtuInfoSec.net/Configuration/Sites

名称 (A):


请为此站点选择一站点链接对象。站点链接对象可以在站点/站点间传输容器中定位 (S)。

链接名	传输
 DEFAULTIPSITELINK	IP

确定 取消

## ❖ 输入站点名称

Active Directory

 站点 Teaching 已创建。要完成配置 Teaching:

- 确认 Teaching 链接到有适当的站点链接的站点。
- 为 Teaching 添加子网到子网容器。
- 在 Teaching 安装一个或多个域控制器, 或将现存域控制器移入此站点。
- 为 Teaching 选择授权计算机。

确定 帮助



新建对象 - 子网

创建在: SjtuInfoSec.net/Configuration/Sites/Subnets

地址 (I):

192.168.33.0

掩码 (M):

255.255.255.0

名称 (N):

192.168.33.0/24

输入子网地址和掩码。它将被自动转换为格式为“网络/遮蔽字节”的子网名称。  
例如: 地址 10.14.209.14 掩码 255.255.240.0 将转换为子网 10.14.208.0/20。

为此子网选择站点对象 (S)。

站点名

Default-First-Site-Name

Teaching

确定

取消

AD 站点和服务

控制台 (C) 窗口 (W) 帮助 (H)

操作 (A) 查看 (V)

树

Active Directory 站点和服务

Sites

Default-First-Site-Name

Inter-Site Transports

Subnets

Teaching

名称	站点	类型
172.16.0.0/16	Default-First-Site-Name	子网
192.168.33.0/24	Teaching	子网



# 为子网关联站点



192.168.33.0/24 属性

子网 | 位置 | 对象 | 安全

192.168.33.0/24

描述 (D):

站点 (S): Teaching

网络: Default-First-Site-Name  
Teaching

掩码: 255 .255 .255 . 0

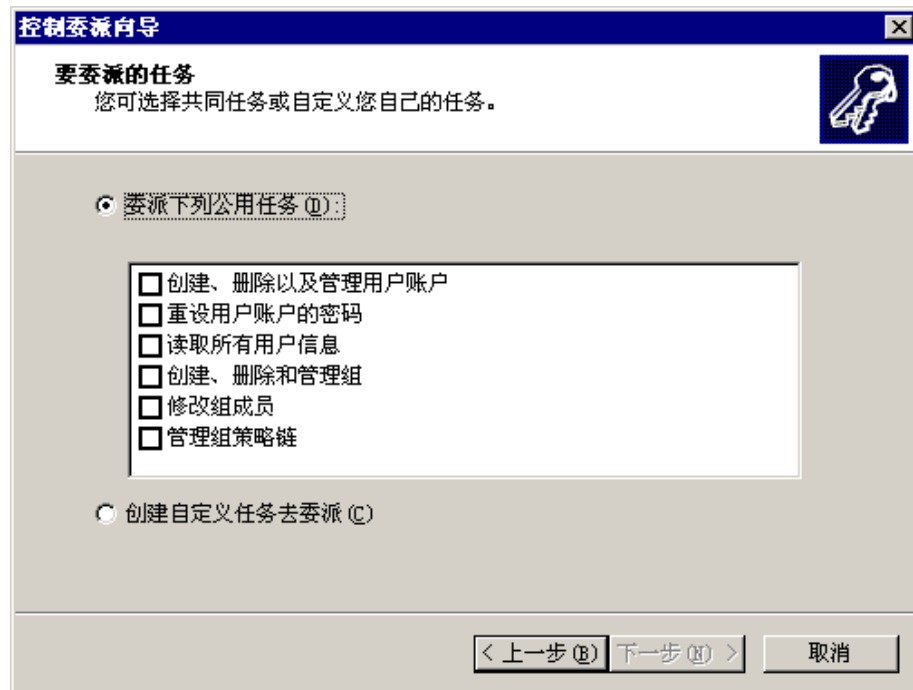
确定 取消 应用 (A)

# 委派域或组织单位的管理



## ❖ 添加授予控制权的用户或组

## ❖ 授予委派任务



# 委派站点的管理



**控制委派向导**

**要委派的任务**  
您可选择共同任务或自定义您自己的任务。

☐ 委派下列公用任务 (U):

☐ 管理组策略链

☒ 创建自定义任务去委派 (C):

< 上一步 (B)   下一步 (N) >   取消

**控制委派向导**

**Active Directory 对象类型选择**  
请指出要委派的任务范围。

委派以下对象的控制:

☐ 这个文件夹，这个文件夹中的对象，以及创建在这个文件夹中的新对象 (T)

☒ 只是在这个文件夹中的下列对象 (O):

☐ aCSResourceLimits 对象  
☐ certificationAuthority 对象  
☐ groupPolicyContainer 对象

< 上一步 (B)   下一步 (N) >   取消



SJTU Information Security Institute  
Network Attack & Defence Technology Research Studio

---

**Any Questions ?**

