第 4 章　活动目录

活动目录（Active Directory）是 Windows 2000 系统引入的新内容。它是 Windows 2000 以及后续 Windows 系统进行分布式联网的基础，同时也简化了包括组策略和远程安装在内的集中与分散管理技术的使用。活动目录在实施一个组织的网络，规划网络的安全中占有非常重要的地位。

4.1　活动目录基础

随着通过网络进行远程办公的人员数目越来越多，计算一直趋向于朝着更大的网络和更为分布式的方向发展。所以，现代的操作系统必须能够提供对分布式资源、实体和关系进行管理的机制。对于在地理位置上相互分离的网络，无论是外网（如 Internet）、企业内部网（Intranet）的用户还是在家办公的用户，这些系统都应该能够予以支持，并解决随之而来的安全性问题。

Windows 2000 通过实现一种目录服务解决方案，来达到了这一级别的功能。这种目录服务解决方案就是活动目录。换句话说，活动目录是 Windows 2000 用来满足分布式发展趋势，达到特定级别功能所实现的目录服务。活动目录提供了一个空间来存储关于用户、文件、应用程序、打印机等网络实体的信息，这样用户就能够找到他们所需要的信息。同时，活动目录还为管理和保护这些信息提供了一致的方法，这样就能确保只有适当的用户才可以访问某一网络资源。活动目录以中心授权机构的形式工作，管理实体，沟通这些分布式实体之间的关系，以使它们能够很好地协同工作。

对于目录服务而言，要提供网络操作系统的这些基本功能并保证网络的完整性和保密性，就必须紧密结合到操作系统的管理与安全机制中去。活动目录建立在 Internet 标准技术之上，是和 Windows 系统完全集成的，这样就为减少计算机所用目录的数量，并为网络资源的隔离、移植和集中管理提供了一种基础结构。

4.1.1　活动目录的作用

目录服务是为了满足网络分布式计算和远程办公的爆炸式需求应运而生的。目录服务的主要作用在于：

- 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，它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。这一功能允许 Windows 系统验证用户身份，并用访问控制列表（ACL）来控制用户对网络资源的访问。活动目录起到管理任务结合点的作用，并把系统合并为一个整体，让组织机构可以使用标准的业务规则来分配应用程序、网络资源和拥护，而不需要管理员维护不同的特殊目录。

4.1.1 活动目录的内容和工作方式

活动目录包括两个方面的内容：目录和与目录服务。

目录（又称数据存储区）是存储网络对象信息的分层结构。活动目录使用“对象”这个名词来表示如用户、组、计算机、硬件设备、应用和打印机等网络资源。而目录则是存储各种“对象”的一个物理上的容器，从静态的角度来理解与我们以前所认识的“目录”和“文件夹”没有本质区别，这里也仅仅是一个对象，是一个实体。活动目录把信息组织成由这些对象和容器所组成的一个树型结构，这就类似于 Windows 系统在计算机上用文件夹和文件来组织文件信息一样。例如，一般情况下，目录会存储用户账户的用户名、密码、电子邮件地址和电话号码等信息。

目录服务与目录的不同之处在于它既是目录信息源，又是使信息对管理员、用户、网络服务和应用程序有效并可用的服务。理想情况下，目录服务会使物理拓扑和协议（两个服务间传输数据所用的格式）透明化。这样，即使用户不知道资源的物理位置和连接方法，也能够访问该资源。我们继续上一个例子，正是目录服务使得同一网络中的其他授权用户能够访问针对用户对象所保存的目录信息，如电子邮件地址和电话号码等。目录服务可支持多种不同的功能：有些目录服务与操作系统集成，提供对用户、计算机和共享资源的管理；有些则是与一些应用程序（如 Microsoft Exchange 电子邮件目录）集成，使得用户能够查找其他用户的邮件地址信息并发送电子邮件。

活动目录在管理对象和容器之间关系的时候，还提供了一个单一集中化的视图，即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。这样就更容易在高度分布的网络中搜索、管理和使用资源。

总的来说，活动目录以面向对象的方式将对象信息保存在一个层次结构中，并为分布式网络环境提供多主复制（Multimaster Replication）的支持。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”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。

4.1.2 活动目录的优势

在 Windows 2000 系统中引入活动目录有以下一些优势。

1. 信息的安全性大大增强

在 Windows 2000 操作系统中，用户身份验证和访问控制的管理都已经完全与活动目录结合在一起，而它们都是系统的关键安全措施。活动目录将身份验证集中进行，不仅可以定义对目录中每个对象的访问控制，还可定义对每个对象的每个属性的访问控制，这一点是以前任何系统所不能达到的（包括 Windows NT 4.0）。除此之外，活动目录还可以提供存储和应用程序作用域的安全策略，提供安全策略的存储和应用范围。安全策略可以包含账户信息，如域范围内的密码限制或对特定域资源的访问权限等。

所以，从某种程度上可以这么说，Windows 2000 的安全性就是活动目录体现出来的安全性。

2. 基于策略的管理

活动目录服务存储着分配给特定环境的策略，称为组策略对象。组策略是在初始化时应用于计算机或用户的配置设置。所有的组策略设置都包含在应用到活动目录站点、域或组织单元的组策略对象（GPO）中。GPO 设置决定目录对象和域资源的访问权限，什么样的域

资源可以被用户使用，以及这些域资源怎样使用等。例如，组策略对象可以决定当用户登录时用户在他们的计算机上看到什么应用程序，当它在服务器上启动时有多少用户可连接至服务器，以及当用户转移到不同的组织单元或组时他们可访问什么文件或服务。

组策略对象使得我们只须管理少量的策略，而不是大量的用户和计算机。通过活动目录，就可以将组策略设置应用于适当的环境中，而不管它是整个组织单位还是单位中的某个特定的组织单元。

3. 很强的可扩展性

Windows 2000 的活动目录具有很强的可扩展性，管理员可以在架构中增加新的对象类别，或者给现有的对象类别增加新的属性。架构包括可以存储在目录中的每一个对象类别的定义和对象类别的属性。例如，在电子商务应用中，你可以给每一个用户对象增加一个购物授权属性，然后存储每一个用户的购买权限作为用户账户的一部分。

4. 很强的可伸缩性。

活动目录包含一个或多个域，每个域均有一个或多个域控制器，以便自由地调整目录规模以满足任何网络的需要。多个域可合并成为一颗域目录树，多颗域目录树又可合并成为目录林，活动目录也就随着域的伸缩而伸缩，较好地适应了单位网络的变化。目录将其架构和配置信息分发给目录中所有的域控制器，该信息存储在域的第一个域控制器中，并且复制到域中任何其他域控制器。当该目录配置为单个域时，添加域控制器将改变目录的规模，而不影响其他域的管理开销。将域添加到目录使得我们可以针对不同策略环境划分目录，并调整目录的规模以容纳大量的资源和对象。

5. 智能的信息复制能力

信息复制为目录提供了信息可用性、容错、负载平衡和性能优势。活动目录使用多主机复制，允许我们在任何域控制器上而不是单个主域控制器上同步更新目录。

多主机模式具有更大容错的优点，因为使用多域控制器的时候，即使任何单独的域控制器停止工作，也可以继续进行复制。由于进行了多主机复制，它们将更新目录的单个复本，在域控制器上创建或修改目录信息后，新创建或更改的信息将发送到域中的所有其他域控制器，所以保证其目录信息是最新的。域控制器需要最新的目录信息，但是要做到高效率，就必须把自身的更新限制在只有新建或更改目录信息的时候，以免在网络高峰期进行同步而影响网络速度。在域控制器之间不加选择地交换目录信息能够迅速搞垮任何网络。通过活动目录就能达到只复制更改的目录信息，而不至于大量增大域控制器的负荷。

6. 与 DNS 的紧密集成

活动目录使用域名系统（DNS）来为服务器目录命名。DNS 是一种 Internet 标准服务，用来将更容易理解的主机名（例如 eric.sjtu.edu.cn）转换成数字 IP 地址，利于在 TCP/IP 网络中计算机之间的相互识别和通信。关于活动目录与 DNS 的集成，我们将在下一节中予以详细论述。

7. 与其他目录服务具有互操作性

由于活动目录是基于标准的目录访问协议，许多应用程序界面（API）都允许开发者进入这些协议，例如活动目录服务接口（ADSI）、轻量型目录访问协议（LDAP）第三版和名称服务提供程序接口（NSPI），因此它可与使用这些协议的其他目录服务相互操作。LDAP 是用于在活动目录中查询和检索信息的目录访问协议。因为它是一种工业标准服务协议，所

以可使用 LDAP 开发程序，与同时支持 LDAP 的其他目录服务共享活动目录信息。活动目录支持 Microsoft Exchange 4.0 和 5.x 客户程序所用的 NSPI 协议，以提供与 Exchange 目录的兼容性。

8. 灵活的查询功能

用户和管理员若要通过对象属性快速查找网络中的对象，可使用“开始”菜单中的“查找”命令、桌面上的“网上邻居”图标或者是活动目录用户和计算机管理单元。例如，我们可以按照一个用户账户的姓名、电子邮件名、办公地点或其他属性查找该用户。而且，使用全局编录（GC）优化了查找信息的操作。

4.2 活动目录的体系结构

在详细阐述活动目录的体系结构之前，本节将先从两个区别很大的角度简单介绍活动目录。

- 第一个角度是从活动目录的最抽象意义上介绍：活动目录是一个与 Internet 域名系统（DNS）集成的名称空间。
- 第二个角度是从活动目录的最普通意义上介绍：活动目录是将服务器转换成域控制器的软件。

只要安装了活动目录域控制器，也就同时创建了初始的 Windows 2000 域，或已在原有域中添加了新的域控制器。那么域控制器和域是如何适应整个网络体系结构的呢？以下各小节将介绍基于活动目录的网络组件，以及这些组件的组织方式。此外，还阐述了如何将对组织单元（OU）、域或站点的管理责任委派给适当的个体，以及如何将配置设置分配给相同的三个活动目录容器。其中包括以下几个主题：

- 对象（包括架构）
- 对象命名规则（包括安全主管名称、SID、与 LDAP 相关的名称、对象 GUID 以及登录名）
- 对象发布
- 域（包括目录树、目录林、信任以及组织单元）
- 站点（包括复制）
- 如何将委派和组策略应用于 OU、域和站点

4.2.1 活动目录与域名服务（DNS）

活动目录和 DNS 都是名称空间。名称空间指的是任一有界区域，在其中对给定的名称进行解析。名称解析就是把名称转换成该名称代表的某一对象或信息的过程。例如，电话号码簿组成了一个名称空间，其中的电话用户名可解析成电话号码；Windows NTFS 文件系统组成了一个名称空间，其中的文件名可解析为文件本身。

1. DNS

要理解 Windows 2000 处理活动目录和 DNS 名称空间的方式，需要先了解有关 DNS 自身及其与 Internet 和 TCP/IP 之间关系的一些基本知识。

Internet 是一种采用 TCP/IP 协议的网络。TCP/IP 通信协议连接计算机，并使计算机可

以通过网络传输数据。Internet 或任何其他 TCP/IP 网络上的每台计算机都有一个 IP 地址。DNS 服务是一种名称解析服务，通过接收网络上的 DNS 请求并传入 DNS 数据库中，将用户能理解的计算机名称转换成 IP 地址。DNS 服务的核心——DNS 数据库既可以是分布在全球的 DNS 数据库，也可以是本地的 DNS 数据库。

DNS 组织成不同层次的域，使整个 Internet 成为一个名称空间。DNS 有几个顶级域，可进一步划分为二级域。Internet 域名空间的根由 Internet 职权部门（目前是 Internet 网络信息中心，简称 InterNIC）管理，该部门负责代理对 DNS 名称空间顶级域名的管理职责，并负责注册二级域名。顶级域名是一些大家熟悉的域类别，如商业组织（.com）、教育组织（.edu）、政府组织（.gov）等；而对于美国以外的国家和地区，则用两个字母的国家/地区代码来表示，如中国用.cn 表示，英国用.uk 表示。图 4-1 显示了组织单位通过网络连接到 Internet DNS 名称空间的方式。

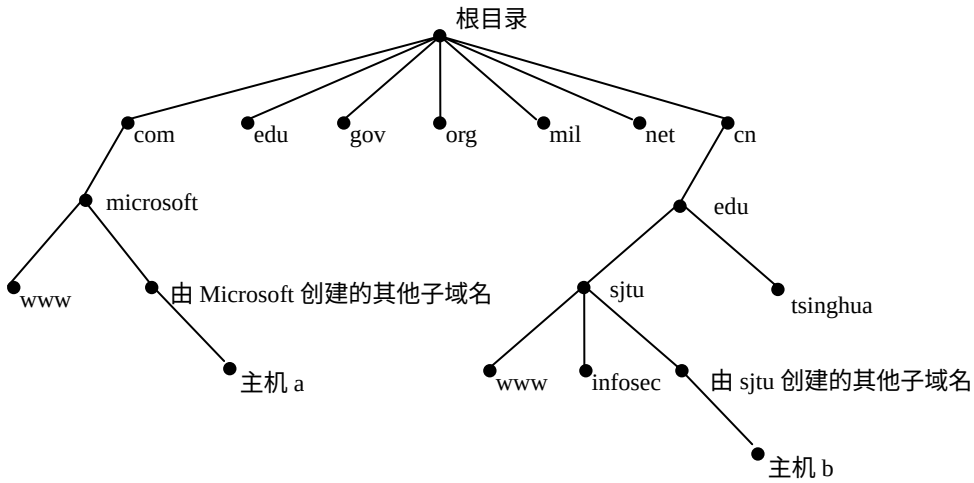

图 4-1　Internet 的 DNS 名称空间

2.　活动目录与 DNS 的集成

活动目录与 DNS 的集成是 Windows 2000 Server 操作系统的核心功能。DNS 域和活动目录域共享一个相同的域结构，使用相同的域名，但两者却是不同的名称空间，这是因为它们各自保存不同的数据，因而管理不同的对象。DNS 保存区域以及资源记录，而活动目录则保存域和域对象。

DNS 的域名以 DNS 分层命名结构为基础，这是一个反向树结构：最上方是一个根域，下面是父域和子域（枝和叶）。例如，有个域名为 child.parent.SjtuInfosec.net，这表明域名 child 是域名 parent 的子域，而 parent 本身也是域 SjtuInfosec.net 的一个子域。

DNS 域的每台计算机都可依据其完全合格的域名（FQDN）加以惟一识别，如位于域 child.parent.SjtuInfosec.net 的计算机的 FQDN 是 computername.child.parent.SjtuInfosec.net。

每个 Windows 2000 域都有一个 DNS 名称（如 SjtuInfosec.net），并且每台基于 Windows 2000 的计算机都有一个 DNS 名称（如 FileServer.SjtuInfosec.net）。因而，域和计算机都用活动目录对象和 DNS 节点来表示（DNS 分层结构中的一个节点代表一个域或一台计算机）。

DNS 和活动目录均用数据库来解析名称。

- DNS 是一种名称解析服务。 通过将 DNS 服务器接收的请求视为对 DNS 数据库的 DNS 查询，DNS 将域名和计算机名解析成 IP 地址。具体地说，DNS 客户机把 DNS 名称查询发送到已配置的 DNS 服务器。DNS 服务器先接收名称查询，然后通过本地保存的文件解析该名称查询，或咨询另一台 DNS 服务器进行解析。DNS 服务并不需要系统启动活动目录。

- 活动目录是一种目录服务。通过将域控制器接收的请求视为轻量型目录访问协议（LDAP）搜索，或改成对活动目录数据库的请求，活动目录将域对象名称解析成对象记录。具体而言，活动目录客户机使用 LDAP 向活动目录服务器发送查询。活动目录客户机通过查询 DNS 来定位活动目录服务器。即活动目录将 DNS 用作定位器服务，把活动目录域、站点及服务名称解析成 IP 地址。例如，要登录到活动目录域，活动目录客户机会查询已配置的 DNS 服务器，请求 LDAP 服务的 IP 地址（LDAP 服务在指定域的域控制器中运行）活动目录不需要系统启动 DNS。

实际上，可以这样理解 Windows 2000 环境中 DNS 与活动目录名称空间之间的差异：代表 DNS 区域中指定计算机的 DNS 主机记录，与活动目录域中代表“同一台计算机”的计算机账户对象处于不同的名称空间中。

总之，活动目录采用以下几种方式来与 DNS 集成：

- 活动目录域和 DNS 域有相同的分层结构。尽管由于目的不同，DNS 和活动目录域的组织名称空间各自独立，实施方法也有所不同，但它们却有相同的结构。例如，SjtuInfosec.net 既是一个 DNS 域又是一个活动目录域。
- DNS 区域可保存在活动目录中。如果使用 Windows 2000 DNS 服务，主区域就可以保存在活动目录中，以便复制到其他活动目录域控制器中，为 DNS 服务提供增强的安全性。
- 活动目录客户机使用 DNS 来定位域控制器。为了定位指定域的域控制器，活动目录客户机会查询已配置的 DNS 服务器，以查找指定的资源记录。

3. 活动目录与全局 DNS 名称空间

活动目录被设计成可处于 Internet 全局 DNS 名称空间的范围之内。如果某组织使用 Windows 2000 Server 作为其网络操作系统，则当该组织需要存在于 Internet 上时，活动目录名称空间会作为一个或多个分层的 Windows 2000 域，保留在已注册为 DNS 名称空间的根域名之下（组织也可选择不成为全局 Internet DNS 名称空间的一部分，但仍要求 DNS 服务定位于基于 Windows 2000 的计算机）。

根据 DNS 的命名规则，以英文句号（.）分隔的 DNS 名称的每部分都代表 DNS 分层树结构的一个节点，以及 Windows 2000 域分层树结构的一个可能的活动目录域名。如图 4-2 所示，DNS 分层结构的根是一个空标签（" "）的节点。活动目录名称空间的根（目录林根）无父根，它提供了指向活动目录的 LDAP 进入点。

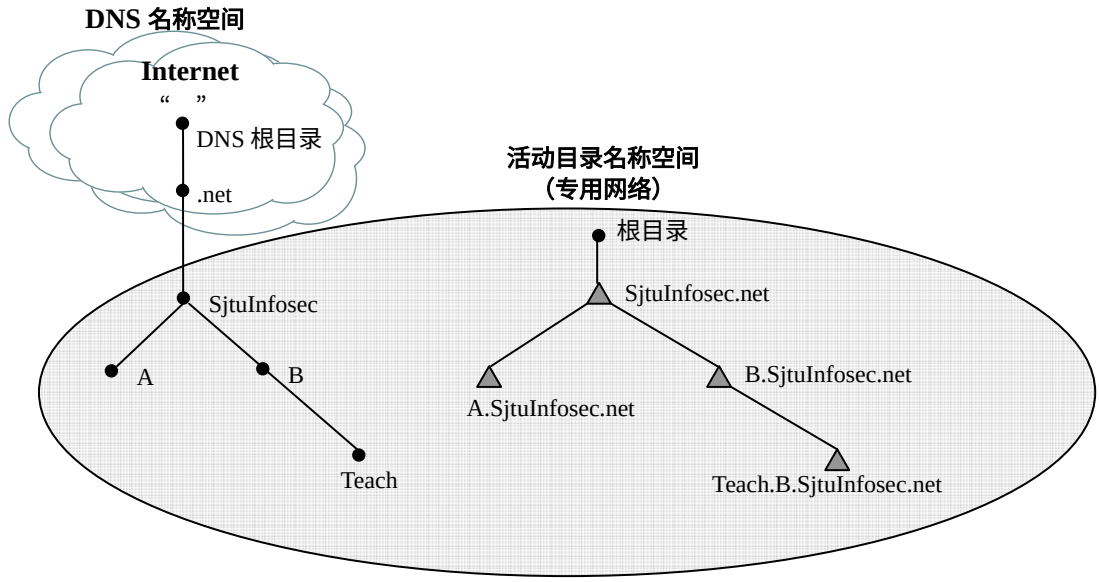

图 4-2　比较活动目录与 DNS 名称空间的根

4.　SRV 资源记录与动态更新

DNS 独立于活动目录，而活动目录却专门设计成与 DNS 协同工作。为了保证活动目录正常运行，DNS 服务器必须支持服务位置（SRV）资源记录。SRV 资源记录把服务名称映射成提供该服务的服务器名称。活动目录客户机和域控制器使用 SRV 资源记录来确定域控制器的 IP 地址。

除了要求 Windows 2000 网络的 DNS 服务器支持 SRV 资源记录外，DNS 服务器还需为 DNS 动态更新提供支持。DNS 动态更新定义了一种协议，以便使用新值或变更值动态更新 DNS 服务器。如果没有 DNS 动态更新协议，管理员必须手动配置由域控制器创建而由 DNS 服务器保存的记录。

新的 Windows 2000 DNS 服务既支持 SRV 资源记录，又支持动态更新。如果选用不是基于 Windows 2000 的 DNS 服务器，则必须保证该服务器支持 SRV 资源记录，否则应将其升级为支持这些记录的版本。有些旧的 DNS 服务器虽然支持 SRV 资源记录，但不支持动态更新，因此，在 Windows 2000 Server 提升为域控制器时，就必须手动更新这些服务器的资源记录。该过程可使用 Netlogon.dns 文件（位于 %systemroot%\System32\config 文件夹中）来完成，该文件由活动目录安装向导所创建。

4.2.2　活动目录与域控制器

在运行 Windows 2000 Server 系统的计算机上安装活动目录，实际上就是一种把服务器转换成域控制器的操作。虽然一个域可以有多个域控制器，但是一个域控制器只能控制一个域。

具体而言，域控制器就是一台运行 Windows 2000 Server 的计算机，它已使用活动目录安装向导进行了配置。该向导工具可安装并配置向网络用户和计算机提供活动目录服务的组件。域控制器会存储整个域的目录数据（如系统安全策略和用户身份验证数据），并管理用户和域的交互过程，包括用户登录进程、身份验证以及目录搜索。

使用活动目录安装向导将服务器提升为域控制器，可以是创建一个 Windows 2000 域，或者是在原有域中添加新的域控制器。

本小节将阐述活动目录域控制器的概念，以及它在网络中所扮演的某些重要角色。由于引入了活动目录，Windows 2000 域控制器的功能与“ 对等 ”类似。这与 Windows NT Server 主域控制器（PDC）和备份域控制器（BDC）扮演的主/从角色有所不同。对等域控制器支持“ 多主机复制 ”，可在所有域控制器之间复制活动目录信息。多主机复制的引入意味着管理员可以更新域中任何 Windows 2000 域控制器的活动目录。而在 Windows NT Server 系统中，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 上。

如果准备由原有域升级到 Windows 2000 操作系统，则可在方便时分阶段完成升级。如果正在为新的安装创建第一个域控制器，则会在加载活动目录的同时自动形成几个实体。接下来将解释在新的网络中安装活动目录域控制器的两个方面：

- 第一个域控制器是一个全局编录服务器
- 第一个域控制器扮演所有操作主机角色

9. 全局编录（GC）

Windows 2000 系统引入了全局编录概念，这是一个保存在一个或多个域控制器中的数据库。全局编录在登录用户和查询中扮演重要角色。

默认情况下，全局编录由 Windows 2000 目录林中的初始域控制器自动创建，并且每个目录林必须至少有一个全局编录。在目录林中安装了其他域控制器后，就可以用活动目录站点和服务工具将全局编录的默认位置更改为另一个域控制器。我们还可以根据组织对服务登录请求和搜索查询的要求，选择将任一域控制器设置成管理全局编录。全局编录服务器越多，对用户查询的响应就越快；但启用很多域控制器作为全局编录服务器会增加网络中的复制通信量，因而影响了响应速度。

全局编录执行两个关键的活动目录角色：登录和查询。

- 登录。在本机模式域中，全局编录通过为账户提供通用组成员身份信息（该账户将登录请求发送到域控制器），启用活动目录客户机的网络登录。实际上，不但对活动目录的用户验证，而且对每个对象的身份验证，甚至包括每台计算机的启动，都必须引用全局编录服务器。在多域安装中，为了完成用户登录过程，必须至少有一台包含全局编录的域控制器正在运行，并且有效。当用户以非默认的用户主要名称（UPN）登录时，全局编录服务器也必须存在而且有效。如果在用户启动网络登录进程时，全局编录是无效的，则用户将只能登录到本地计算机，而无法登录到网络中。惟一的例外是，如果用户是域管理员 (Domain Admin) 组的成员，就能够在全局编录无效的情况下登录到网络中。
- 查询。在包含多个域的目录林中，全局编录使得客户机能够方便快捷地执行跨所有域的搜索，而不必逐个搜索每个域。全局编录使目录林中的目录结构对查找信息的最终用户透明。绝大多数活动目录网络通信是与查询有关的：用户、管理员和程序都会请求有关目录对象的信息。查询过程要比目录更新过程的发生频度高得多。如果把不止一个域控制器指定为全局编录服务器，这样虽然会减少对查找目录信息的用户的响应时间，但同时也会导致网络的复制通信量增加。

10. 操作主机角色

对等域控制器间的多主复制对于某些类型的对活动目录的更改并不可行，因此，只有一个被称为“ 操作主机 ”的域控制器可以接受这种更改请求。由于多主机复制在基于活动目录的网络中占有重要地位，因此理解这些例外情况非常重要。在任一活动目录的目录林中，安装期间至少会将五个不同的操作主机角色分配给初始域控制器。

当在新目录林中创建第一个域时，全部五个独立的主机操作角色都会自动分配给该域中

的第一个域控制器。在只有一个域和一个域控制器的小规模活动目录的目录林中，这个惟一的域控制器仍担当起所有的操作主机角色。在一个较大的网络中，无论它有一个域还是多个域，我们都可以重新将这些角色分配给其他的一个或多个域控制器。有些角色必须在每个目录林中出现，而有些角色则必须在目录林的每个域中出现。

以下跨整个目录林的两种操作主机角色在目录林中必须是惟一的，即整个目录林中一种操作角色只能有一个。

- 架构主机。拥有架构主机角色的域控制器控制对架构的所有更新和修改。架构定义了可在目录中保存的每个对象（及其属性）。要更新目录林的架构，必须拥有架构主机的访问权。
- 域命名主机。拥有域命名主机角色的域控制器控制目录林中域的添加或删除。

以下整个域的三个操作主机角色在每个域内都必须是惟一的，即在目录林的每个域中都只能有一个。

- 相对标识符（RID）主机。RID 主机为域内的每个域控制器分配 RID 序列。只要域控制器创建了用户、组或计算机对象，该主机就会为对象指定一个惟一的安全 ID（SID）。安全 ID 由域安全 ID（对域中创建的所有安全 ID 都是相同的)和相对 ID（在域中创建的每个安全 ID 都是惟一的）组成。当域控制器用完自己的 RID 池后，会向 RID 主机请求另一个 RID 池。
- 主域控制器（PDC）模拟器。如果域包含未安装 Windows 2000 客户机软件的计算机，或者如果包含 Windows NT 备份域控制器（BDC），PDC 模拟器就会充当 Windows NT 主域控制器。它可以处理客户机的密码更改过程，并将更新情况复制到 BDC。对由域中其他域控制器执行的密码更改过程，PDC 模拟器可优先接收到对这些更改情况的复制。如果由于密码错误而导致在另一个域控制器的登录身份验证失败，域控制器会在拒绝登录尝试之前，将验证请求转发给 PDC 模拟器。
- 基础结构主机。当一个由其他对象引用的对象移动时，基础结构主机负责更新域间的所有引用。例如，只要组成员重新命名或有所更改，基础结构主机就会更新组与用户间的引用。当重新命名或移动组中的成员，并且成员与组不在同一域中，暂时看起来组中就像没有包含该成员。组所在域的基础结构主机负责更新组，使组能够了解成员的新名称或新位置。基础结构主机使用多主机复制来对更新情况进行分发。除非域中只有一个域控制器，否则不应把基础结构主机的角色分配给主持全局编录的域控制器。如果这样做，基础结构主机将无法行使其功能。如果域中的所有域控制器都主持全局编录（包括只有一个域控制器的情况），那么所有域控制器都会有当前的最新数据，因而就不需要基础结构主机这一角色了。

4.3 活动目录对象

活动目录对象是组成网络的实体。对象是代表用户、打印机或应用程序等一些具体事物的一组不同的、已命名的属性集。当创建一个活动目录对象时，活动目录会生成一些对象属性的值，其他属性值则须由我们输入。例如，当创建用户对象时，活动目录会指定全球惟一标识符（GUID），而我们则提供其他一些属性（如用户的姓、名、登录标识符等）的值。

4.3.1 架构

“ 架构 ”（Schema）是对“ 对象类别 ”（不同类型的对象）及这些对象类别的“ 属性 ”的说明。对于每个对象类别，架构定义了对象类别必须具有的属性，它可能具有的其他属性，以及可以成为其父对象的对象类别。活动目录对象都是一个对象类别的实例。每一属性只定义一次，但可用在多个类别中。例如，属性“ 描述 ”只定义了一次，却已用在许多不同类别中。

架构保存于活动目录中，而架构定义本身也作为对象保存——即类架构（Class Schema）对象和属性架构（Attribute Schema）对象。这使得活动目录可以用管理其他目录对象的同种方法来管理类别和属性对象。

创建或修改活动目录对象的应用程序采用架构来确定以下内容 :对象一定或可能有哪些属性，以及如何依据数据结构和语法限制来描述属性。

活动目录的对象不是容器对象就是叶对象（又称非容器对象）。容器对象存储其他对象，而叶对象却没有该功能。例如，文件夹是文件的容器对象，而文件则是叶对象。

活动目录架构中每一类别的对象都有这样一些属性，它们确保：

- 目录数据存储区中的每一对象都具有惟一的标识
- 对于安全主管（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
- 与目录对象名称的 LDAP 标准的兼容性

1. 架构属性与查询

使用活动目录架构工具能够将属性标记为有索引。这样做的结果是：将该属性的所有实例都添加至索引，而不仅仅是添加特定类别成员的实例。为属性建立索引有助于查询能够更加快速地找到具有该属性的对象。

也可以将一些属性加入全局编录。全局编录包含了目录林中每个对象的一组默认属性，而且可以将自己的选项添加进去。用户和应用程序都使用全局编录在整个目录林中定位对象。只有具有以下特征的属性才可包含在全局编录中。

- 全局通用。属性应是查找处于目录林任意位置的对象（即使仅用于读取访问）时需要的属性。
- 相对稳定。属性应是不变或极少改变的。某一全局编录中的属性会复制到目录林中所有其他全局编录中。如果属性经常变化，则会导致复制通信量骤增。
- 小型。全局编录中的属性会复制到目录林的每个全局编录中。属性越小，对复制过程的影响程度越低。

2. 架构对象名称

如上所述，类别和属性都是架构对象。任何架构对象都可以使用下列名称类型中的一种来进行引用，

- LDAP 显示名。对于每一架构对象来说，LDAP 显示名是全局惟一的。LDAP 显示名由一个或多个词组合而成，第一个词后面的词的词首字母大写。例如，mailAddress 和 machinePasswordChangeInterval 是两个架构属性的 LDAP 显示名。活动目录架构和其他 Windows 2000 管理工具都可以显示对象的 LDAP 显示名，程序员和管理员可使用该名称以编程方式来引用对象。
- 公用名。架构对象的公用名也是全局惟一的。可在架构中创建新对象类别或新属性时指定公用名。公用名是在架构中代表对象类别的、对象的相对专用的名称（RDN）。

- 对象标识符（OID）。 架构对象的标识符是由颁发机构，如国际标准化组织（ISO）和美国国家标准局（ANSI）颁发的数字。例如，SMTP 电子邮件地址属性的 OID 是 1.2.840.113556.1.4.786。OID 在整个全球网络中确保是惟一的。从颁发机构获得根 OID 后，即可用它来分配其他 OID。OID 是一种分层结构。例如，颁发给 Microsoft 的根 OID 是 1.2.840.113556。Microsoft 内部管理由这个根产生的进一步分支，其中一个分支用来为活动目录架构类别分配 OID，另一个用于活动目录属性。

4.3.2 对象命名规则

活动目录支持对象名称的几种不同格式，用以适应名称可能会采用的不同形式，采用何种形式取决于名称的使用环境（有些名称是数字形式）。下面分别说明活动目录对象命名规则的这些类型：

- 安全主体名称
- 安全标识符（又称安全 ID ，SID）
- 与 LDAP 相关的名称，包括专用的名称（DN）、相对专用的名称（RDN）、URL 以及规范名称
- 对象 GUID
- 登录名称，包括用户主体名（UPN）和 SAM 账户名

如果组织有多个域，就有可能会在不同域中使用相同的用户名或计算机名。由活动目录生成的安全标识符、GUID、LDAP 专用的名称以及规范名称都可惟一的标识目录中的每个用户或计算机。如果用户或计算机对象被重新命名或移至另一个域，虽然安全标识符、LDAP 的相对专用的名称、专用的名称和规范名称都会发生变化，但由活动目录生成的 GUID 却不会发生改变。

1. 安全主体名称

安全主体是由活动目录管理的 Windows 2000 对象，拥有自动分配的安全标识符（SID），用于登录身份验证和访问资源。安全主体可以是用户账户、计算机账户或组。因此，安全主体名称是用来惟一标识一个域内的用户、计算机或组的名称。安全主体对象必须由所在域的域控制器进行身份验证，并且可授予或剥夺其对网络资源的访问权。

安全主体名称在跨域时并不要求是惟一的。但是，为了实现后向兼容性，该名称在自己的域内必须是惟一的。安全主体对象的名称必须符合以下规则。

- 名称不得与同一域内的任何其他用户、计算机或组名称相同。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

2. 安全标识符

安全标识符（SID）是 Windows 2000 系统安全子系统创建的惟一数字，用来分配给安全主体对象，即分配给用户、组和计算机账户。网络上的每个账户都会在首次创建时获得惟一的一个 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。

每个活动目录对象都由访问控制列表（ACL）保护，每个访问控制列表包含一个或多个访问控制项（ACE）。访问控制项能够识别哪些用户或组可以访问该对象。每个 ACE 都包含有权访问该对象的每个用户或组的 SID，并定义了允许进行的访问的级别。例如，一个用户可能对某些文件有只读权限，对另一些文件有读写权限，而对其他的文件则没有访问权限。

假如我们先删除了一个原有的账户，然后又以相同用户名创建了一个账户，那么新账户并没有老账户以前所拥有的权限或许可，因为新老账户具有不同的 SID。

3. 与 LDAP 相关的名称

活动目录是一种服从轻量型目录访问协议（LDAP）的目录服务。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 定义了在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。

（1）LDAP 专用的名称（DN）与相对专用的名称（RDN）

LDAP 为对象提供了 DN 和 RDN，而活动目录在实现这些 LDAP 命名规则时会有所变化，如表 4-1 所示：

表 4-1 LDAP 命名规则及其活动目录对应规则

LDAP DN & RDN 命名规则	相应的活动目录命名规则
cn=公用名称	cn=公用名称
ou=组织单元	ou=组织单元
o=组织	dc=域组件
c=国家	（不支持）

每个活动目录对象均有一个 LDAP DN。可根据分层路径定位活动目录域内的对象，分层路径包括活动目录域名标签和容器对象每个级别的标签。DN 定义了到对象的完整路径，而对象自身的名称由 RDN 所定义。RDN 是对象 DN 的一部分（DN 则是对象自身的一个属性）。

通过使用到对象的完整路径（包括对象名称和到域根目录的所有父对象），DN 可惟一识别域分层结构中的对象。每个 RDN 都保存于活动目录数据库中，并包含到其父层的引用。在一次 LDAP 操作中，通过跟踪各级引用，最后达到根目录，从而建立了整个 DN 结构。在一个完整的 LDAP DN 中，待识别对象的 RDN 在左侧出现的是叶名称，在右侧出现的是根目录名称，如下例所示：

```
cn=Eric, ou=gongfang, ou=Teaching, dc=CNRegion, dc=OrgName, dc=com
```

Eric 用户对象的 RDN 是 cn=Eric，gongfang（Eric 的父对象）的 RDN 是 ou=gongfang，依此类推。

活动目录工具并不显示命名属性的 LDAP 缩写（dc=、ou=或 cn=）。上面显示这些缩写仅用于说明 LDAP 是怎样识别 DN 的各部分的。大多数活动目录工具以规范的格式（后面将作介绍）来显示对象名。Windows 2000 系统通过 DN 使 LDAP 客户机能够检索目录中的对象信息，但并没有 Windows 2000 的用户界面需要输入 DN。只有编写遵守 LDAP 的程序或脚本时，才需要明确区分 DN、RDN 和命名属性的用法。

（2）LDAP URL 名称

活动目录支持任何启用了 LDAP 的客户机使用 LDAP 协议来进行访问。RFC 1959 中说明了 LDAP 统一资源定位符（URL）的格式。URL 使得 Internet 客户机可以直接访问 LDAP 协议。LDAP URL 以前缀“ LDAP ”开头，接着为具有活动目录服务的服务器命名，然后是对象的属性名称（即专用的名称，DN）。例如：

```
LDAP://server1.CNRegion.OrgName.com/cn=Eric,ou=gongfang,ou=Teaching,dc=CNRegion,dc=OrgName,dc=com
```

（3）基于 LDAP 的活动目录规范名称

默认情况下，活动目录管理工具以“ 规范名称 ”的格式来显示对象名称，此格式列出了从根节点开始的 RDN，并且不包含 RFC 1779 命名属性描述符（即 dc=、ou= 或 cn=）。规范名称采用 DNS 域名格式，即名称的各段域标签是用英文句号（.）分隔的，如 CNRegion.OrgName.com。表 4-3 将 LDAP DN 与同名的规范名称格式做了一下比较：

表 4-3　LDAP DN 格式与规范名称格式的比较

LDAP DN 名称	cn=Eric, ou=gongfang, ou=Teaching, dc=CNRegion, dc=OrgName. dc=com
规范名称	CNRegion.OrgName.com/Teaching/gongfang/Eric

4. 对象 GUID

除了 LDAP DN，活动目录中的每个对象都有一个全局惟一标识符（GUID）。这是一个在对象创建时由目录系统代理分配的 128 位数字。GUID 不能被更改或删除，它保存在属性 objectGUID 中，该属性是每个对象的必有属性。与 DN 或 RDN 的可更改性有所不同，GUID 永不改变。

要在外部存储区（例如 Microsoft SQL Server 数据库）保存对活动目录对象的引用，就应该使用 objectGUID 值。

5. 登录名称

如前所述，安全主体是在登录身份验证和资源访问授权两方面均应用基于 Windows 安全措施的对象。用户即是一种类型的安全主体。在 Windows 2000 系统中，用户安全主体需要惟一的登录名，以获取对域及其资源的访问权。

（1）用户主体名称

在活动目录中，每个用户账户都有一个格式为<user>@<DNS-domain-name>的用户主体名（UPN）。UPN 是由管理员指定的友好名，它比系统使用的 LDAP 专用的名称要短，因此更易于记忆。UPN 独立于用户对象的 DN，所以移动或重新命名用户对象时不会影响用户登录名。使用 UPN 登录时，用户就不必再从登录对话框的列表中选择域了。

UPN 由三部分组成：UPN 前缀（用户登录名）、@字符以及 UPN 后缀（通常是一个域名）。用户账户的默认 UPN 后缀是活动目录域的 DNS 名，该域是用户账户所处的位置。例如，用户 Eric 在 OrgName.com 域（如果 OrgName.com 是目录树中惟一的域）中有一个用户账户，其 UPN 为 Eric@OrgName.com。UPN 是安全主体对象的一个属性(userPrincipalName)，如果一个用户对象的 userPrincipalName 属性没有值，那么该用户对象就会有一个默认的 UPN：userName@DnsDomainName。

如果所在的组织机构有很多域，形成了按部门和区域组织的大型域树，则默认的 UPN 名称可能会变得过于繁杂。例如用户的默认 UPN 可能是 teacher.SjtuInfosec.net。在该域中的用户登录名是 user@teacher.SjtuInfosec.net。如果不想把默认的 DNS 域名作为 UPN 后缀，则可为所有用户统一提供一个 UPN 后缀，以简化管理和用户登录进程。UPN 后缀只用于 Windows 2000 域，并且不必是有效的 DNS 域名。也可以选用自己的电子邮件域名作为 UPN 后缀，如 SjtuInfosec.net，那么前面用户的 UPN 名称就变成了 user@SjtuInfosec.net

对于基于 UPN 的登录，可能会需要全局编录，这要取决于用户登录以及用户计算机的域成员资格。如果用户以非默认的 UPN 登录，并且用户的计算机账户与其用户账户处于不同域中，则会需要全局编录。也就是说，如果未接受默认的 DNS 域名作为 UPN 后缀（如上例中的 user@teacher.SjtuInfosec.net），而是给所有用户提供了一个统一的 UPN 后缀（简化为 user@ SjtuInfosec.net），那么登录是就需要全局编录了。

使用活动目录域和信任工具来管理域的 UPN 后缀。在创建用户时分配 UPN，如果已为域创建其他后缀，创建用户或组账户时就可以从有效的后缀列表中进行选择。列表中的后缀按如下顺序显示：

- 备选后缀（如果有，最后创建的会显示在最前面）
- 根域
- 当前域

（2）SAM 账户名

考虑到与 Windows NT 3.x 和 Windows NT 4.0 域的兼容性，就需要引入 SAM（安全账户管理器）账户名。SAM 账户名有时也称为无层次名称。因为与 DNS 名称不同，SAM 账户名不使用分层的命名方式。由于 SAM 名称是无层次的，因此每个名称在域中都必须是惟一的。

4.3.3 对象发布

对象发布是在目录中创建特定对象的过程，这种对象或者包含希望使之生效的信息，或者对此类信息提供一个引用。例如，用户对象包括关于用户的有用信息，比如他们的电话号码和电子邮件地址，而卷对象包括对共享文件系统卷的一个引用。以下是对象发布的两个实例：在活动目录中发布文件和打印对象。

- 共享发布。可用活动目录用户和组管理单元，将共享文件夹发布为活动目录中的一个卷对象（又称共享文件夹对象）。这样，用户就可以方便快捷地在活动目录中查询该共享文件夹了。
- 打印机发布。在 Windows 2000 域中，管理、定位及连接打印机最简单的方式就是通过活动目录。默认情况下，当通过“ 添加打印机 ”向导添加了一台打印机，并选择共享这台打印机时，Windows 2000 Server 就会将其作为活动目录中的对象在域中发布。在活动目录中发布（列出）打印机就能使用户找到最方便的打印机。现在用户可按照类型（如 PostScript、颜色、纸张大小是否适合法律文件等）和位置等打印机属性进行搜索，轻而易举地查询活动目录中的任何一台打印机。而打印机从服务器中删除后，服务器将取消对该打印机的发布。

1. 发布时间

如果信息对用户群的大部分有用或者能够引起他们的兴趣，并且对这些信息的访问程序要求很高，就应该在活动目录中发布这些信息。在活动目录中发布的信息有下面两个主要特征。

- 相对静止。只发布不频繁更改的信息，如电话号码和电子邮件地址。
- 结构化。所发布的信息应是结构化的，并可以表示为一组离散的属性，如用户的商务地址。

2. 发布方法

发布信息的方式根据应用程序和服务的不同而变化。

- 远程过程调用（RPC）。RPC 应用程序应用 API 的 RpcNs*族在目录中发布它们的连接点，并查询已发布其连接点的服务的连接点。
- Windows 套接字。Windows 套接字应用程序使用 Winsock 2.0 中有效的 API 注册和解析族发布它们的连接点，并查询已经发布其连接点的服务的连接点。
- 分布式组件对象模型（DCOM）。DCOM 服务使用驻留于活动目录的 DCOM 类存储（DCOM Class Store）来发布它们的连接点。DCOM 是 Microsoft 组件对象模型（COM）的规范，用于定义组件在基于 Windows 的网络中的通信方式。使用 DCOM 配置工具集成跨多台计算机的客户/服务器应用程序。DCOM 也可以用于集成可靠的 Web 浏览器应用程序。

4.4 域

活动目录由一个或多个域组成，域是在 Windows 2000 网络中复制和安全性的基本单元。在网络中创建初始域控制器的同时也就创建了域，不可能创建没有一个域控制器的域。目录中的每个域都按 DNS 域名标识。可以使用活动目录域和信任工具来管理域。

使用域可以实现以下网络管理目标。

- 界定安全区域。Windows 2000 域可定义安全界限。安全策略和设置（如管理权和访问控制列表）不会从一个域跨至另一个域。活动目录可能包括一个或多个域，每个域都有其自己的安全策略。
- 复制信息。域是 Windows 2000 目录分区（又称命名环境)。这些目录分区就是复制的单元。每个域只存储位于该域中的对象的相关信息。域的所有域控制器均可接收对对象的更改情况，并可将这些更改复制到该域的其他所有域控制器中。
- 应用组策略。域为策略定义了一个可能的范围（组策略设置也可应用于各组织单元或站点)。针对域应用组策略对象（GPO）会建立配置和使用域资源所需的方法。例如，可以使用组策略控制桌面设置，如桌面锁闭和应用程序部署。这些策略只应用于该域，而不会跨域使用。
- 设计网络结构。既然一个活动目录域就可以横跨多个站点，且能够包含数百万个对象，大多数公司不需要再单独创建域来反映公司的分支机构和部门。但是，有些单位的确需要不止一个域才能满足要求，例如，那些独立的或完全自治的业务部门可能不希望让部门外的任何人对其对象拥有权限。这样的单位可以创建更多的域，并将这些域组织成一个活动目录的目录林。此外，如果网络的两部分由一个链路分开，且链接速度之慢使得根本没法通过该链路来完成复制通信，这时也可将网络分成独立的域。
- 委派管理权限。在运行 Windows 2000 的网络中，可将单个组织单元和独立域的管理权限彻底委派给别人，这样即可减少需要具有较高管理权限的管理员的数量。因为域是一个安全界限，所以默认情况下，对域的管理权限受域的限制。例如，虽然管理员在一个域中有权设置安全策略，但并未自动授予他在目录的任何其他域中设置安全策略的权限。

要理解域，就要理解目录树、目录林、信任和组织单元这些域组件，还要理解每个结构与域的关系如何。实际情况中，许多单位是由一个域组成结构，而域同时是只包含一个目录树的一个目录林。这种结构不仅是可能的，而且也许还是组织网络的最理想方式。

4.4.1 目录树

在 Windows 2000 系统中，目录树是指具有连续名称的一个或多个域的集合。如果存在多个域，则可将这多个域合并为分层的树结构。所创建的第一个域是第一个树的根域。同一域树中的其他域是子域。同一域树中，与一个域紧密相连的上面的域是该域的父域。

有同一颗域树的所有域组成了一个“ 连续名称空间 ”。在连续名称空间中的域有连续的 DNS 域名。这些名称以下列方式形成：子域的域名显示在左边，与其右侧的父域名用英文句号（.）分隔开。当有两个以上的域时，每个域的父域都在其域名的右侧，如图 4-3 所示。

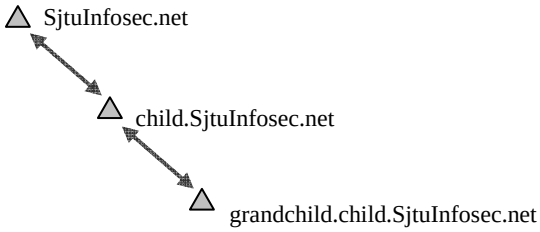

图 4-3　域树中的父域和子域

基于 Windows 2000 的域形成了一棵树，这些域通过双向、可传递的信任关系链接。信任关系将在后续章节中阐述。域树中域之间的父—子关系只是命名关系和信任关系。父域中的管理员不会自动成为子域的管理员，父域中的策略设置也不会自动应用于子域。

4.4.2　目录林

活动目录的目录林是一个分布式数据库，它是由跨多台计算机的许多局部数据库组成的数据库。目录林的数据库分区按域来定义，即一个目录林由一个或多个域组成。除域数据库外，目录林的所有域控制器还保管目录林配置和架构容器的一个副本。

一个目录林比较容易进行创建和维护，且在通常情况下完全能够满足组织的需要。因为所有的用户都通过全局编录来查看一个目录。在该目录林中添加新域时，无须进行额外的信任配置，因为目录林中的所有域都是用双向可传递的信任关系来连接的。在有多个域的目录林中，配置更改只需应用一次，即可影响所有域。只有确实需要时才创建其他目录林，因为所创建的每个目录林都会导致额外的管理开销。

一个目录林中的多个域树之间不会形成连续名称空间。也就是说，它们有非连续的 DNS 域名。尽管目录林中的目录树不共享同一名称空间，但目录林只有一个根域，称为“目录林根域”。按照定义，目录林根域为目录林中创建的第一个域。

如图 4-4 所示，SjtuInfosec.net、A.SjtuInfosec.net 和 B.SjtuInfosec.net 这三个域互不连续，其中 A.SjtuInfosec.net 和 B.SjtuInfosec.net 是 SjtuInfosec.net 的子域。虽然三个域的目录树中都有一个用于 Teach 的子域，但这些子域的 DNS 名却分别是 Teach.SjtuInfosec.net、Teach.A.SjtuInfosec.net 和 Teach.B.SjtuInfosec.net，它们之间没有共享名称空间。

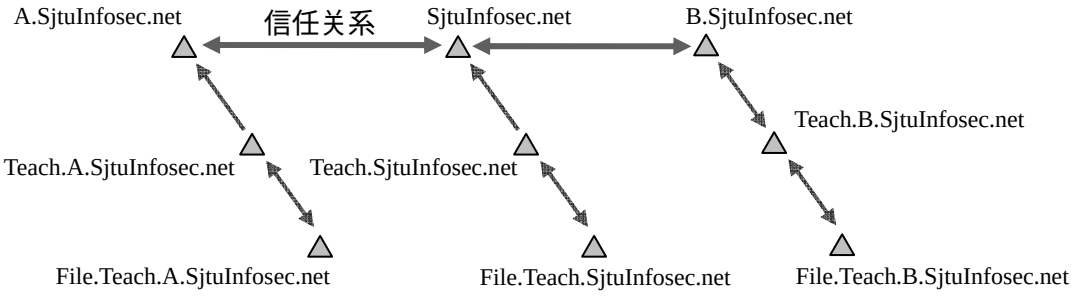

图 4-4　目录林中的目录树名称空间

目录林中每个域目录树的根域都会与目录林根域建立一种可传递的信任关系（将在下一小节中详细说明）。在图 4-4 中，SjtuInfosec.net 是目录林根域。其他域目录树（A.SjtuInfosec.net 和 B.SjtuInfosec.net）的根域均与 SjtuInfosec.net 有可传递的信任关系。这样就在目录林的所有域树之间建立了信任关系。

4.4.3 信任关系

信任关系是建立在两个域之间的关系，它使得一个域中的域控制器能够识别另一个域内的用户。信任允许用户访问另一个域中的资源，还允许管理员管理用户在其他域中的权限。对于运行 Windows 2000 的计算机来说，域之间的账户身份验证由双向的、可传递的信任关系所启动的。基于 Windows 2000 的目录林中的所有域信任关系都是双向可传递的，并以如下方式定义。

- 双向。创建新的子域时，子域会自动信任父域，反之亦然。实际上，就是说身份验证请求可在两个域之间进行两个方向的传递。
- 可传递。可传递的信任关系超出了最初信任关系中的两个域。以下是可传递信任的工作原理：如果域 A 和域 B（父域和子域）互相信任，而域 B 和域 C（也是父域和子域）也互相信任，那么域 A 和域 C 也是互相信任的（隐式），尽管它们之间没有直接的信任关系。在目录林一层，目录林根域和添至该目录林的每颗域树的根域之间都会自动建立信任关系，因此在活动目录的目录林所有域之间都存在完全的信任关系。实际上，因为信任关系是可传递的，所以一次登录过程会让系统在目录林中的所有域中验证某一用户（或计算机）。

我们来看一个例子。如图 4-5 所示：域 1 和域 2 有可传递的信任关系，而域 2 和域 3 有可传递的信任关系，所以域 3 中的用户（在获得相应权限时）可访问域 1 中的资源。同时又因为域 1 和域 A 具有可传递信任关系，并且域 A 的目录树中的其他域和域 A 具有可传递的信任关系，所以域 B 中的用户（当授与适当权限时）就可以访问域 3 中的资源。

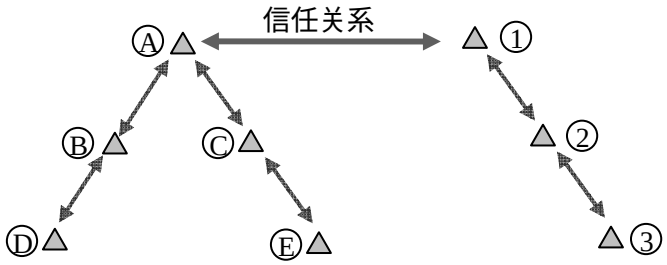

图 4-5　不同目录树的域之间信任关系

而两个处在不同目录林中的 Windows 2000 域之间的信任关系是不可传递的，即信任关系只存在这两个域之间，而不会传递到其他任何域上去。此外，在 Windows 2000 域和 Windows NT 域之间的所有信任关系也都是不可传递的。从 Windows NT 升级至 Windows 2000 时，现有的所有 Windows NT 信任关系都保持不动。在混合模式环境中，所有的 Windows NT 信任都是不可传递的。不可传递信任默认为单向信任关系。

4.4.4 组织单元

组织单元（OU，又称部门）是 Windows 2000 系统的新内容。组织单元是一种类型的目录对象，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。可在一个组织单元中放置用户、组、计算机、打印机、共享文件夹以及一个域内的其他组织单元。组织单元（在活动目录用户和计算机界面中用文件夹表示）允许按逻辑关系组织并存储域中的对象。如图 4-6 所示，组织单元中也可包含有其他组织单元。

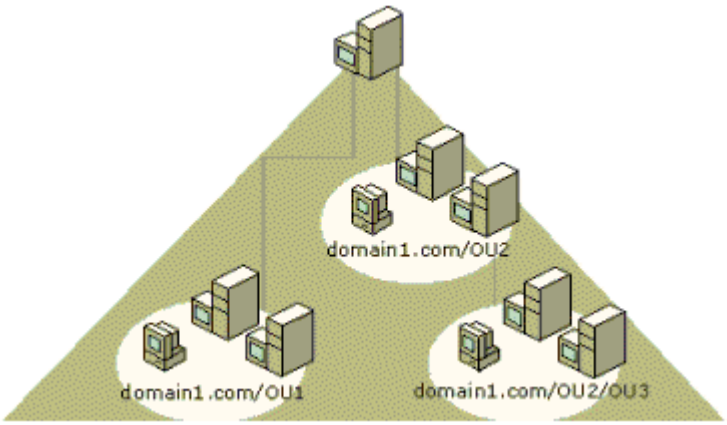

图 4-6　单域内的组织单元层次

组织单元主要用来委派对用户、组及资源集合的管理权限。组织单元是委派管理权限的最小分组。例如，可能会创建一个组织单元，其中包含整个公司的所有用户账户。创建了委派管理功能的组织单元之后，即可对组织单元应用组策略设置，来定义用户和计算机的桌面配置。因为组织单元是用来委派管理功能的，所以所创建的结构可能会反映管理模型，而不是反映业务组织。

4.4.5　混合模式域与本地模式域

Windows 2000 能够支持在 Windows 2000 域内给予 Windows NT 4.0 的工作站和服务器，因此就有下面两种可能情况。

- 混合模式域：既有 Windows NT 域控制器又有 Windows 2000 域控制器的域。
- 本地模式域：只有 Windows 2000 域控制器的域。

混合模式提供了与 Windows 操作系统早期版本之间最大的向下兼容性。一旦升级了域中所有的域控制器，那么就可以把域从混合模式切换到本地模式，但注意这个过程是不可逆的。

4.5　站点

所谓站点，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）。而站点之间一般是通过慢速连接来实现信息通信。可见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。我们可以使用活动目录站点和服务工具来配置站点内以及站点之间的连接。

4.5.1　站点提供的服务

在 Windows 2000 系统中，站点提供以下服务：

- 客户机可以向同一站点的域控制器请求服务
- 活动目录会尽量将站内复制的复制延迟降至最小
- 活动目录会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

用户和服务应该能够随时通过目录林的任何计算机访问目录信息。为此，必须把目录数据的添加、修改和删除等操作由起始域控制器复制到目录林的其他域控制器中。但是，必须保持广泛分发目录信息的需求与优化网络性能的需求之间的平衡。活动目录站点有助于保持这种平衡。

4.5.2 站点和域

站点是独立于域的，了解这一概念非常重要。站点映射网络的物理结构，而域一般映射组织的逻辑结构。逻辑结构和物理结构彼此独立，所以有：

- 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。但是在很多组织中，创建的域反映了物理网络结构。这是因为域是分区，而分区可以影响复制，通过将目录林分成多个更小的域，可以减少复制的通信量。
- 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。

4.5.3 站点信息的使用

可先用活动目录站点和服务工具指定站点信息，然后活动目录就可利用此信息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。当客户机向域控制器请求服务时，它会直接把请求发送给同一站点的域控制器（如有一个可用的域控制器）。选择与发出请求的客户机连接良好的域控制器，将会提高处理此类请求的效率。例如，当客户机使用域账户登录时，登录机制会首先查找与客户机在同一站点的域控制器。因为先使用了客户机所在站点的域控制器，使网络通信能在本地进行，从而提高了身份验证过程的效率。
- 复制目录数据。站点可启用站点内和站点间的目录数据复制。活动目录在站点内复制信息要比站点间复制频繁得多，这意味着：连接最好的域控制器（可能是最需要特定目录信息的域控制器）会最先收到复制；其他站点的域控制器接收目录更改的所有信息（但不频繁），这样就减少了网络带宽消耗。在域控制器之间复制活动目录数据，提供了数据的可用性、容错能力、负载平衡，并提高了性能。

4.5.4 站点内复制

如果网络是由一个局域网（LAN）或由通过主干网连接的一组 LAN 组成，整个网络就可以成为单个站点。最先安装的域控制器会自动创建第一个站点，称为“默认初始站点名称”（Default First Site Name）。安装完第一个域控制器后，其他所有域控制器就会被自动添至与初始控制器相同的统一站点之中（之后允许移动到其他站点）。惟一的例外情况是：安装一个域控制器时，如果其 IP 地址落在先前指定的另一个站点的子网上，那么该域控制器就会加到该站点上。

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。

图 4-7 描述了站点内的复制：三个域控制器（其中一个是全局编录）复制了目录林的架

构数据和配置数据，以及所有的目录对象（包括每个对象的一整套属性）。

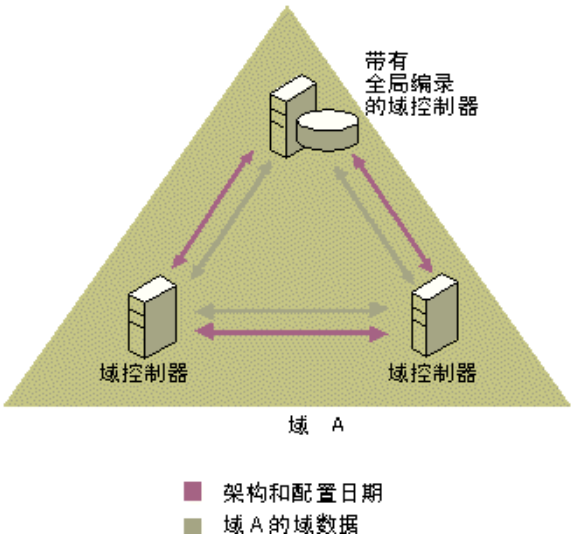

图 4-7　单域的站点内复制

4.5.5　站点间复制

在 Windows 2000 系统中可创建多个站点来优化 WAN 链接上的服务器到服务器、客户机到服务器的通信。站点间的复制可自动将站点间的带宽消耗降至最小。建立多个站点时，推荐的做法有。

- 将每个需要快速访问最新目录信息的地域建为一个单独的站点。这样，通过把需要直接访问最新活动目录信息的区域建成单独的站点，为用户提供了所需的资源。
- 每个站点至少有一个域控制器，且每个站点中至少有一个域控制器是全局编录（GC）。站点如果没有自己的域控制器，也没有全局编录，那么就只能依靠其他站点获取目录信息，这样效率会很低。

站点间的连接用“ 站点链接 ”表示。站点链接是两个或多个站点之间的低带宽或不可靠的网络连接。连接两个快速网络的 WAN 就是站点链接的一个例子。通常，对于任意两个网络，当其通过速度低于 LAN 的链接连接时，就认为这两个网络是通过站点链接连接的。另外，接近容量极限的快速链接带宽效率低，也视为站点链接。

在基于 Windows 2000 的网络中不能自动生成站点链接，必须使用活动目录站点和服务工具来创建。通过创建站点链接，并配置其复制可用性、相对成本和复制频率，就可以为活动目录提供一些信息，这些信息是关于需要创建哪些“ 连接对象 ”来复制目录数据的。活动目录用站点链接作为指示器，指示应该在什么位置创建“ 连接对象 ”，以及“ 连接对象 ”会在什么位置用实际的网络连接来交换目录信息。

默认情况下，站点链接是可传递的。这就意味着一个站点中的域控制器可以与任何其他站点的域控制器进行复制连接。也就是说，如果站点 A 与站点 B 相连，站点 B 与站点 C 相连，那么站点 A 的域控制器可以与站点 C 的域控制器进行通信。

图 4-8 显示了由一个站点链接连接的两个站点。在图中的六个域控制器中，其中有两个是桥头服务器。

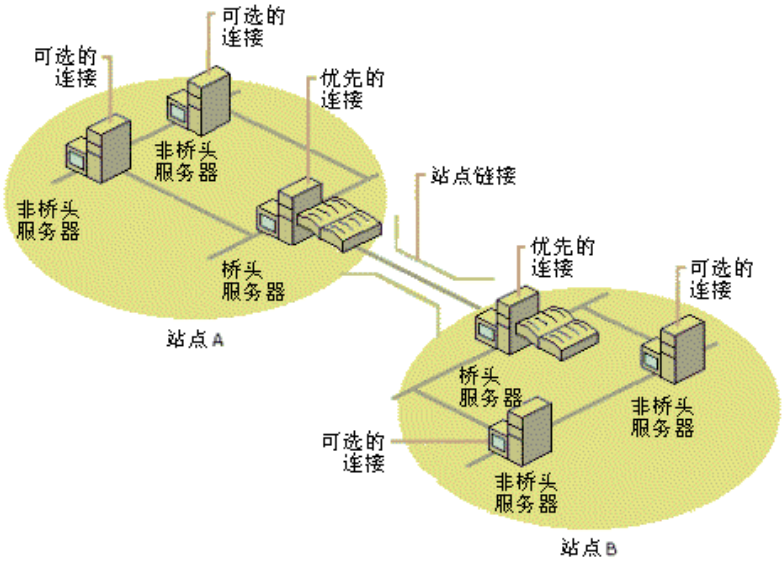

图 4-8　通过站点链路连接的两个站点

桥头服务器是站点间复制所使用的首选服务器，它是由系统自动指派的。我们也可以配置站点中的其他域控制器来复制站点间的目录更改。在更新由一个站点复制到另一个站点的桥头服务器后，就可以通过站点内复制把更新复制到站点内的其他域控制器了。

4.6　活动目录的管理

4.6.1　活动目录的规划

在安装活动目录之前，需要首先要对活动目录的结构进行细致的规划设计，让用户和管理员在使用时更为轻松。

1.　规划 DNS

如果准备使用活动目录，就需要先规划名称空间。当 DNS 域名称空间可在 Windows 2000 中正确执行之前，需要有可用的活动目录结构。所以从活动目录设计着手并用适当的 DNS 名称空间支持它。经过审阅，如果检测到任何规划中有不可预见的或不合要求的结果，则根据需要进行修改。

在 Windows 2000 中，用 DNS 名称命名活动目录域。选择 DNS 名称用于活动目录域时，以单位保留在 Internet 上使用的已注册 DNS 域名后缀开始（如“ SjtuInfosec.net ”），并将该名称和单位中使用的地理名称或部门名称结合起来，组成活动目录域的全名。

例如，可能命名 root 的教学组的域为“ teach.root.SjtuInfosec.net ”。这种命名方法确保每个活动目录域名是全球惟一的。而且，这种命名方法一旦被采用，使用现有名称作为创建其他子域的父名称以及进一步增大名称空间以供单位中的新部门使用的过程将变得非常简单。对于仅使用单个域或小型多域模式的小型企业，可以直接进行规划并按照与范例相似的方法进行操作。

2.　规划用户的域结构

最容易管理的域结构就是单域。规划时，用户应从单域开始，并且只有在单域模式不能满足用户的要求时，才增加其他的域。一个域可跨越多个站点并且包含数百万个对象。站点结构和域结构互相独立而且非常灵活。单域可跨越多个地理站点，并且单个站点可包含属于多个域的用户和计算机。如果只是反映用户公司的部门组织结构，则不必创建独立的域树。在一个域中，可以使用组织单位来实现这个目标。然后，可以指定组策略设置并将用户、组和计算机放在组织单位中。

可以在域中创建组织单位的层次结构。组织单位可包含用户、组、计算机、打印机、共享文件夹以及其他组织单位。组织单位是目录容器对象。它们表现为“活动目录 用户和计算机”中的文件夹。组织单位简化了域中目录对象的视图以及这些对象的管理。可将每个组织单位的管理控制权委派给特定的人。这样，用户就可以在管理员中分配域的管理工作，以更接近指派的单位职责的方式来管理这些管理性职责工作。

3. 何时创建域控制器

将 Windows 2000 Server 计算机升级为域控制器会创建一个新域或者向现有的域添加其他域控制器。创建域控制器可以：

- 创建网络中的第一个域
- 在树林中创建其他的域
- 提高网络可用性和可靠性
- 提高站点之间的网络性能

要创建 Windows 2000 域，必须在该域中至少创建一个域控制器。创建域控制器也将创建该域，不可能有没有域控制器的域。如果确定单位需要一个以上的域，则必须为每个附加的域至少创建一个域控制器。

4. 规划用户的委派模式

用户可以将权利下派给单位中最底层部门，方法是：在每个域中创建组织单位树，并将部分组织单位子树的权利委派给其他用户或组。通过委派管理权利，用户不再需要那些定期登录到特定账户的人员，这些账户具有对整个域的管理权。尽管用户还拥有带整个域的管理授权的管理员账户和域管理员器组，可以仍保留这些账户以备少数高度信任的管理员偶尔使用。

最后在规划活动目录结构时，除了需要认真考虑以上各项外，还要注意以下几点。

- 使用的域越少越好，因为 Windows 2000 已经大大扩展了单个域的容量。
- 限制组织单位的层次，在活动目录搜索事物的层次越深则运行效率越低。
- 限制组织单位中的对象个数，这样便于高效地查找特定资源。
- 用户可以将管理权限分配到组织单位级，这样将提高管理效率，降低管理员的负荷。

4.6.2 安装活动目录

安装活动目录前首先确定 DNS 服务正常工作。

1. 安装第一台域控制器

下面来安装根域为 nt2000.com 的域中第一台域控制器。

（1）利用配置服务器启动位于%Systemroot%\system32 中的活动目录安装向导程序 DCPromo.exe。如图 4-9 所示，单击“下一步”按钮继续。

图 4-9　活动目录安装向导

（2）由于建立的是域中的第一台域控制器，所以选择“ 新域的域控制器 ”，单击“ 下一步 ”按钮继续。

（3）选择“ 创建一个新域的域目录树 ”，单击“ 下一步 ”按钮继续。

（4）选择“ 创建一个新域的域目录林 ”，单击“ 下一步 ”按钮继续。

（5）在“ 新域的 DNS 全名 ”中输入要创建的域名（这里输入 SjtuInfoSec.net），如图 4-10 所示，单击“ 下一步 ”按钮继续。

图 4-10　为新域的 DNS 制定名称

（6）安装向导自动将域控制器的 NetBIOS 名称设置为“ SjtuInfoSec ”，单击“ 下一步 ”按钮继续。

（7）显示活动目录数据库、目录文件及 Sysvol 文件的保存位置，一般不必作修改。单击“ 下一步 ”按钮继续。

（8）配置 DNS 服务，单击“ 下一步 ” 按钮继续（如果在安装活动目录之前未配置 DNS 服务器可以在此让安装向导配置 DNS）。

（9）为用户和组选择默认权限，如果仍然需要使用 Windows 2000 的以前版本，就选择“ 与 Windows 2000 服务器之前版本相兼容的权限 ”，如图 4-11 所示，单击“ 下一步 ” 按钮继续。

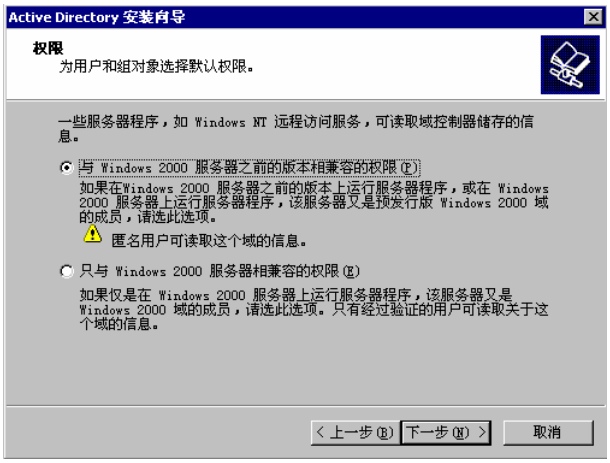

图 4-11　为用户和组选择默认权限

(10) 输入以目录恢复模式下的管理员密码，单击“下一步”按钮继续。

(11) 安装向导显示摘要信息，单击“下一步”开始安装，如图 4-12 所示。

图 4-12　正在安装和配置活动目录

(12) 安装完成之后，重新启动计算机。

2.　检验安装结果

（1）检查 DNS 文件的 SRV 记录

因为在安装过程中最重要的一项工作是在 DNS 数据库中添加服务记录（SRV 记录），所以可以用文本编辑器打开%systemroot%/system32/config/中的 Netlogon.dns 文件来察看 LDAP 服务记录，在本例中为

_ldap._tcp.SjtuInfoSec.net. 600 IN SRV 0 100 389 Server.SjtuInfoSec.net.

（2）验证 SRV 记录在 NSLOOKUP 命令工具中是否运行正常

① 在命令提示符下，输入 nslookup。

② 输入 set type=srv。

③ 输入_ldap._tcp.SjtuInfoSec.net，如果返回了服务器名称和 IP 地址，就说明 SRV 记录工作正常。

3.　安装第二台域控制器

在安装完第一台域控制器后，其域名为 SjtuInfoSec.net，在上例中该服务器用于总部，如果由于单位扩展的需要为其新建的部门建立自己的域名和域控制器，则将新部门的域名定义为 A.SjtuInfoSec.net。由于此域名与 SjtuInfoSec.net 是连续的域名，所以它们组成了一个目录树。今后随着单位的发展还可以在这个目录树下继续逐级添加子域（如 teach.A.

SjtuInfoSec.net）；如果需要添加的域名与该目录树不连续（如：TsingHuaInfoSec.net），那么就需要建立一个新的目录树，这样就由多个目录树组成了域目录林。

在安装第二台域控制器之前，首先检验它的 IP 设置和 DNS 设置，以保证可以访问域控制器（server.SjtuInfoSec.net）。

（1）利用配置服务器启动位于%Systemroot%\system32 中的活动目录安装向导程序 DCPromo.exe。

（2）由于用户所建立的是域中的一台域控制器，所以选择“ 新域的域控制器 ”，单击“ 下一步 ” 按钮继续。

（3）选择 “ 在现有域目录树中创建一个新的子域 ”，单击 “ 下一步 ” 按钮继续。

（4）在 “ 网络凭据 ” 对话框中输入上一级域的域名及具有管理员权限的用户名和密码，单击 “ 下一步 ” 按钮继续。

（5）在 “ 子域安装 ” 对话框中输入父域域名（SjtuInfoSec）和子域域名（A），在下方的子域完整域名中会自动显示 A.SjtuInfoSec.net，单击 “ 下一步 ” 按钮继续。

（6）安装向导自动将域控制器的 NetBIOS 名称设置为“ A ”，也可以手动对其进行修改，单击 “ 下一步 ” 按钮继续。

（7）显示数据库、目录文件以及 Sysvol 文件的保存位置，一般不必修改。单击 “ 下一步 ” 按钮继续

（8）为用户和组选择默认权限，单击 “ 下一步 ” 按钮继续。

（9）单击 “ 下一步 ” 按钮开始安装。在重新启动后，在 server.SjtuInfoSec.net 的“ Active Directory 域和信任关系 ” 中将显示新建的子域 A.SjtuInfoSec.net，如图 4-13 所示。

图 4-13　安装第二台域控制器之后的活动目录域和信任关系

4.6.3　活动目录工具

在活动目录顺利安装完毕后，Windows 2000 会在管理工具中提供了如下三个主要的工具。

- Active Directory 用户和计算机，如图 4-14 所示。

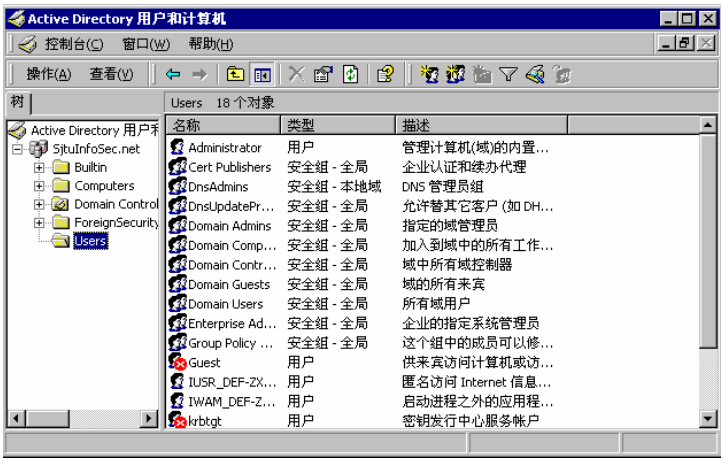

图 4-14　Active Directory 用户和计算机工具

- Active Directory 域和信任关系，如图 4-15 所示。

图 4-15　Active Directory 域和信任关系工具

- Active Directory 站点和服务，如图 4-16 所示。

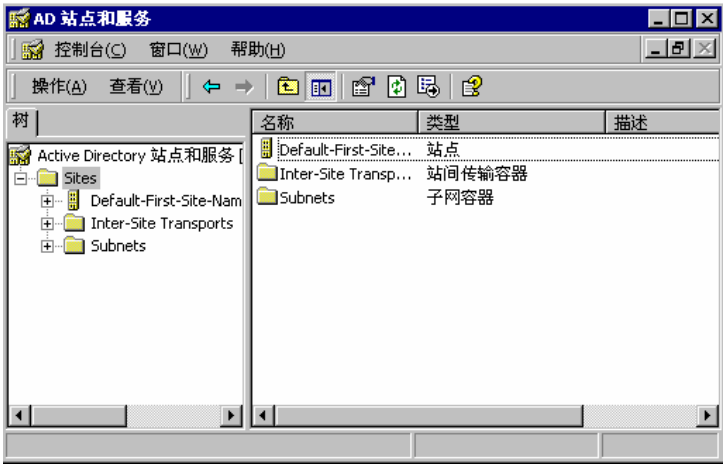

图 4-16　Active Directory 站点和服务工具

Active Directory 用户和计算机工具是配置活动目录最常用的工具，而 Active Directory 域和信任关系、Active Directory 站点和服务工具主要用于管理多个服务器或多个域之间的关系。