 理解了活动目录的原理之后，现在我们就可以进行活动目录的安装与配置了，活动目录的安装配置过程并不是很复杂，因为WIN2K中提供了安装向导，只需按照提示一步步按系统要求设定即可。但安装前的准备工作显得比较复杂，只有充分理解了活动目录的前提下才能正确地安装配置活动目录。下面我就详细地介绍一下活动目录的安装与配置及其准备了。 一、活动目录的安装前的准备 在前面我们知道“ 活动目录 ”是整个WIN2K系统中的一个关键服务，它不是孤立的，它与许多协议和服务有着非常紧密和关系，还涉及到整个WIN2K系统的系统结构和安全。安装“ 活动目录 ”不是安装一般Windows组件那么简单，在安装前要进行一系列的策划和准备。否则轻则根本无法享受到活动目录所带来的优越性，重则不能正确安装“ 活动目录 ”这项服务。 1、首先在 安装活动目录之前，必须保证已经有一台机器安装了WIN2K Server 或者Advanced Server，且至少有一个NTFS分区， 而且已经为TCP/IP 配置了DNS协议，并且DNS服务支持SRV记录和动态更新协议。 2、其次是要规划好整个系统的域结构，活动目录它可包含一个或多个域，如果整个系统的目录结构规划得不好，层次不清就不能很好地发挥活动目录的优越性。在这里选择根域（就是一个系统的基本域）是一个关键， 根域名字的选择可以有以下几种方案：1）可以使用一个已经注册的DNS 域名作为活动目的根域名，这样的好处在于企业的公共网络和私有网络使用同样

的DNS名字。 2）我们还可使用一个已经注册的DNS域名的子域名作为活动目录的根域名。 3）为活动目录选择一个与已经注册的DNS域名完全不同 的域名。这样可以使企业网络在内部和互联网上呈现出两种完全不同的命名结构。 4）把企业网络的公共部分用一个已经注册的DNS域名进行命名，而私有网络用另一个内部域名，从名字空间上把两部分分开，这样做就使得每一部分要访问另部时必须使用对方的名字空间来标识对象。 3、再一个就是要进行域和帐户命名策划，因为使用活动目录的意义之一就在于使内、外部网络使用统一的目录服务，采用统一的命名方案，以方便网络管理和商务往来。活动目录域名通常是该域的完整DNS名称，但是为确保向下兼容，每个域最好还有一个WIN2K以前版本的名称，以便在运行WIN2K以前版本的操作系统的计算机上使用。用户帐户在活动目录中，每个用户帐户都有一个用户登录名、一个WIN2K以前版本的用户登录名（安全帐户管理器的帐户名）和一个用户主要名称后缀。在创建用户帐户时，管理员输入其登录名并选择用户主要名称，活动目录建议 WIN2K 以前版本的用户登录名使用此用户登录名的前 20 个字节。活动目录命名策略是企业规划网络系统的第一个步骤，命名策略直接影 响到网络的基本结构，甚至影响网络的性能和可扩展性。活动目录为现代企业提供了很好的参考模型，既考虑到了企业的多层次结构，也考虑到了企业的分布式特性，甚至为直接接入Internet提供完全一致的命名模型。 所谓用户主要名称是指由用户账户名称和表示用户账户所在的域的域名组成。这是登录到 WIN2K 域的标准用法。标准格式为：user@domain.com (象个人的电子邮件地址)。但不要在用户

登录名或用户主要名称中加入 @ 号。活动目录 在创建用户主要名称时自动添加此符号。包含多个 @ 号的用户主要名称是无效的。 在活动目录中，默认的用户主要名称后缀是域树中根域的 DNS名。如果用户的单位使用由部门和区域组成的多层域树，则对于底层用户的域名可能很长。对于该域中的用户，默认的用户主要名称可能是 grandchild.child.root.com。该域中用户默认的登录名可能是 user@grandchild.child.root.com 。这要一来用户登录时就要输入的用户名可能太长，输入起来就非常不方便，WIN2K为了解决这一问题，规定在创建主要名称后用户只要在根域后加上相应的用户名， 使同一用户使用更简单的登录名 user@root.com 就可以登录，而不是前面所提到的那一长串。 4、最后就是要注意设置规划好域间的信任关系，对于WIN2K计算机，通过基于 Kerberos V5 安全协议的双向、可传递信任关系启用域之间的帐户验证。在域树中创建域时，相邻域（父域和子域）之间自动建立信任关系。在域林中，在树林根域和添加到树林的每个域树的根域之间自动建立信任关系。如果这些信任关系是可传递的，则可以在域树或域林中的任何域之间进行用户和计算机的身份验证。 如果将 WIN2K 以前版本的 Windows域升级为WIN2K域时，WIN2K域将自动保留域和任何其他域之间现有的单向信任关系。包括WIN2K以前版本的Windows域的所有信任关系。如果用户要安装新的WIN2K域并且希望与任何WIN2K以前版本的域建立信任关系，则必须创建与那些域的外部信任关系。 二、活动目录的安装 所有的新安装都是安装成为Member Server，如果您在新安装WIN2K SERVER时选择安装了“ 活动目录 ”选项，则系统就会出现类似于“ 如果您此

时安装活动目录则系统中的所有域名就不能再次改变…… ”之类的提示。一般情况下我们在新安装系统时不选择安装活动目录，以便我们有时间来具体规划与活动目录有关的协议和系统结构。目录服务都需要事后用 Dcprom o的命令特别安装。目录服务还可以卸载，而不用象在安装Windows NT 4.0那样，一开始就要定终身，系统会区分域控制器还是Member Server，两者之间不可转换。 Dcpromo是一个图形化的向导程序，引导用户一步一步地建立域控制器，可以新建一 个域森林，一棵域树，或者仅仅是域控制器的另一个备份，非常方便。很多其他的网络服 务，比如DNS Server、DHCP Server和Certificate Server等，都可以在以后与活动目录 集成安装，便于实施策略管理等。 这个图形化界面向导程序也没有什么特别之处，只要我们在前面理解好了活动目录的含义，并进行了安装前的一系列规划，则可以很容易完成所有的安装任务。 在活动目录安装之后，主要有三个活动目录的微软管理界面（MMC），一个是活动目 录用户和计算机管理，主要用于实施对域的管理；一个是活动目录的域和域信任关系的管理，主要用于管理多域的关系；还有一个是活动目录的站点管理，可以把域控制器置于不 同的站点。一般局域网的范围内，为一个站点，站点内的域控制器之间的复制是自动进行的；站点间的域控制器之间的复制，需要管理员设定，以优化复制流量，提高可伸缩性。 从活动目录管理界面，还可以在站点、域和组织单元中用鼠标右键点击，启动组策略（Group Policy）的管理界面，实施对对象的细致管理。 对于站点、域和组织单元，管理员还可以方便地进行管理授权。右键点击它们就可以启动"管理授权 向导"，一步一步地设定

哪些管理员对于哪些对象有什么样的管理权限。比如说企业内部 技术支持中心的管理员，只有复位用户口令的权限，没有创建和删除用户账号的权限。这 种更细致的管理方法，成为"颗粒化"。 另外，活动目录还充分地考虑到了备份和恢复目录服务的需要，WIN2K备份工具中有专门备份活动目录的选项，在出现意外事故的时候，可以在机器启动时按F8进入安全恢复 模式，保证减少灾难的恶性影响。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com