举例介绍活动目录的优势 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/454/2021_2022__E4_B8_BE_E4_BE_8B_E4_BB_8B_E7_c100_454469.htm Active Directory服务提供了单一登入的能力和一个所有基础设施相关信息的集中储存机制，大幅度的简化了使用者和计算机的管理，同时提供优越的网络资源存取能力。我在本文中主要讲述一下Microsoft Windows Server 2003 中的 Active Directory 相关优点、新功能和改进部份的概观说明。 微软在Windows Server 2000中首次引入了AD技术，经过几年的发展，AD技术已经成为了微软网络架构的核心，几乎所有的产品和技术都是围绕这AD这个核心运转的。可以这么说，在网络中不实现AD，就无法基于微软产品和技术实现基本的网络管理，也无法适应将来的技术发展！ 那么到底安装活动目录有什么意义呢？这是所有初学Windows Server 2003的人首要要问的一个问题。因为活动目录并不是Windows系统必需安装的一种服务，要全面理解它又是非常的不容易，那么安装活动目录的意义在哪里呢？它主要体现在以下几个方面： 1、信息的安全性大大增强 安装活动目录后信息的安全性完全与活动目录集成，用户授权管理和目录进入控制已经整合在活动目录当中了（包括用户的访问和登录权限等），而它们都是WIN2K33系统的关键安全措施。活动目录集中控制用户授权，进行控制不仅仅在每一个目录中的对象上定义，而且还能在每一个对象的每个属性上定义，这一点是以前任何系统所不能达到的，包括WINNT 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

。安全策略可以包含帐户信息，如域范围内的密码限制或对特定域资源的访问权限等。所以从一定程序上可以这么说WIN2K3的安全性就是活动目录所体现的安全性，由此可见对于网管来说如何配置好活动目录中对象及属性的安全性是一个网管配置好WIN2K3系统的关键。 具体应用：比如在工作组下面有3台计算机，分别是A、B、C，各有一个帐号a、b、c，如果B上有一个文档要给a用户访问，b就要在B计算机上创建一个帐号a‘给a，让a用a’去访问，或者b把自己的帐号密码告诉a，让a来访问，同理，其他资源也是一样处理。结果就是每一个用户要记好几个帐号密码来访问不同的资源，或者就是网络里有很多额外的帐号密码存在，或者很多人的密码告诉给其他人，最终网络安全变成一句空话。 但是如果实现了域就不一样了，b只要在资源上设置a的访问权限就可以了，不用额外创建帐号，也不用把自己的帐号密码告诉别人，a来访问的时候，如果权限合适就可以直接进行操作。用户a也不需要记录额外的帐号密码。 再比如，经理m有一台计算机M，为了保证安全性，M计算机只能由m来登录，在AD中只要简单的设置一下就可以了。再有一台打印机，如果有这这样的安全要求，上班时间大家都可以使用，下了班就不能打印了。当有大文档打印时，如果经理m要打印文档，可以中间插入打印，m打印完了，原来的那个大文档继续打印下去。诸如此类的设置，在AD中都可以非常方便的设置。 2、引入基于策略的管理，使系统的管理更加明朗 活动目录服务包括目录对象数据存储和逻辑分层结构（上次在杭州我讲过的目录、目录树、域、域树、域林等所组成的层次结构），作为目录，它存储着分配给特定环境的策略，称为组策略

对象。作为逻辑结构，它为策略应用程序提供分层的环境。组策略对象表示了一套商务规则，它包括与要应用的环境有关的设置，组策略是用户或计算机初始化时用到的配置设置。所有的组策略设置都包含在应用到活动目录，域，或组织单元的组策略对象（GPOs）中。GPOs设置决定目录对象和域资源的进入权限，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 Server，以及当用户转移到不同的部门或组时他们可访问什么文件或服务。组策略对象使您可以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，您可将组策略设置应用于适当的环境中，不管它是您的整个单位还是您单位中的特定部门。 具体应用：比如单位里面为了放置病毒感染和信息安全，要求所有的计算机只能使用USB的鼠标和键盘，U盘和移用硬盘不能使用。为了控制USB接口的使用类型，工作组下面就只有一台一台计算机去设置组策略了，而AD下仅仅一条组策略就可以完成，花费不到10秒钟！ 在比如，为了防止员工修改系统配置导致系统崩溃，或为了禁止员工上班时间玩游戏，需要禁止某些组件的使用，用AD自带的组策略功能也非常方便。至于给所有员工发送一个信息或安装一个软件之类的常规性管理任务，AD的组策略也很容易就实现。而且这些策略的设置可以依据单位的部门或职称架构来实现。非常方便！ 3、具有很强的可扩展性 WIN2K3的活动目录具有很强的可扩展性，管理员可以在计划中增加新的对象类，或者给现有的对象类增加新的属性。计划包括可以存储在目录中的每一个对象类的定

义和对象类的属性。例如，在电子商务上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购买权限作为用户帐号的一部分。 具体应用：比如单位将来用实现邮件系统和企业内部通讯系统，实现依据网络来完成企业内部的文件，信息，语音等等的通讯，这样可以大大节省企业运行成本。利用活动目录的可扩展性，只不过是在用户帐号上多了邮箱属性或MSN属性而已，用户甚至可以使用IE来安全的收发邮件，连Outlook都不需要！ 4、具有很强的可伸缩性 活动目录可包含在一个或多个域，每个域具有一个或多个域控制器，以便您可以调整目录的规模以满足任何网络的需要。多个域可组成为域树，多个域树又可组成为树林，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。将域添加到目录使您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，允许您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，即使任何单独的域控制器停止工作，也可继续复制。由于进行了多主机复制，它们将更新目录的单个副本，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，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，而不至于大量增加域控制器的负荷。 6、与 DNS 集成紧密 活动目录使用域名系统 （DNS）来为服务器目录命名，DNS 是将更容易理解的主机名（如 Mike.Mycompany.com）转换为数字 IP 地址的 Internet 标准服务，利于在TCP/IP网络中计算机之间的相互识别和通讯。DNS 的域名基于 DNS 分层命名结构，这是一种倒置的树状结构，单个根域，在它下面可以是父域和子域（分支和叶子）。 具体应用：任何一台计算机加入到域之后，就获得了一个唯一限定名（FQDN），由于域名称是层次结构的，所以该名称在整个企业中也是唯一的，这样当我们需要查找任何计算机都可以使用该名称。 而且由于该名称是由AD注册在DNS中，完全符合当前网络的状态（所有计算机都在AD中注册），这一点在动态地址分配的情况下非常有利。而且由于DNS是不受地域和网络基础结构影响的，任何地点的任何用户都可以方便的访问到需要的资源。 另外，在AD中，每一个用户都有唯一的用户主名（UPN），类似于邮件地址的用户主名不仅有利于用户记忆（在多域环境下特别有用），而且和邮件系统挂钩，进一步简化了终端用户的使用。 7、与其他目录服务具有互连性 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，例如活动目录服务界面（ADSI）、轻型目录访问协议 （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*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 2003客户程序所用的 NSPI 协议，以提供与 Exchange 目录的兼容性。 8、具有灵活的查询 任何用户可使用“ 开始 ”菜单、“ 网上邻居 ”或“ 活动目录用户和计算机 ”上的“ 搜索 ”命令，通过对象属性快速查找网络上的对象。如您可通过名字、姓氏、电子邮件名、办公室位置或用户帐户的其他属性来查找用户，反之亦然。 具体应用：比如在A地的一个员工要给B地的员工发送一份文档，他不需要将文档打印出来再快递过去，他完全可以在AD中搜索B地员工办公室（或附近办公地点）的某台打印机就可以了，然后直接将文档发送到那台打印机上，B的用户就可以直接拿到文档了。而A的用户不知道B地的打印机没有关系，他可以根据地名，楼层，办公室等等信息，很快定位到正确的打印机！ 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