第 8 章
应用程序服务器

应用程序服务器提供的集成环境可用于部署和运行使用 Microsoft. NET Framework 3.0 构建的自定义业务应用程序。安装应用程序服务器角色时，可选择支持特定应用程序的服务，这些应用程序是专为使用 COM＋、消息队列、Web 服务和分布式事务而构建的。

本章将介绍一些常用的应用程序服务器，以供读者掌握应用程序服务器的基本概念。

8.1 了解应用服务器

应用程序服务器为信息技术(IT)专业人员和开发人员提供了以下好处：支持有效部署和管理高性能业务应用程序的核心运行时为基于服务器的应用程序提供简化编程模型以及高性能执行模型的 .NET Framework 开发环境。.NET Framework 启用 Web 服务，并将新的应用程序与现有应用程序和基础结构相集成；为在组织中运行应用程序所需的各种角色服务和功能提供选择的用户友好安装向导；自动安装特定角色服务所需功能的安装功能。

8.1.1 邮件服务器

邮件服务器是一个常用的而且大多数公司必不可少的应用服务器。邮件服务器被用来存储和管理用户之间的电子邮件。如果用户使用微软的电子邮件产品的话，将会使用 Microsoft Exchange 作为邮件服务器并且使用 Microsoft Outlook 或者 Web 浏览器来存取邮件。

Microsoft Exchange Server 是个消息与协作系统。Exchange Server 可以被用来构架应用于企业、学校的邮件系统或免费邮件系统。它还是一个协作平台。可以在此基础上开发工作流、知识管理系统、Web 系统或者是其他消息系统。Microsoft Exchange Server 是一个 Intranet 协作应用服务器，适合有各种协作需求的用户使用。Exchange Server 协作应用的出发点是业界领先的消息交换基础，Exchange Server 提供了包括从电子邮件、会议安排、团体日程管理、任务管理、文档管理、实时会议和工作流等丰富的协作应用，而所有应用都可以通过 Internet 浏览器来访问。除了常规的 SMTP/POP 协议服

务之外，它还支持 IMAP4、LDAP 和 NNTP 协议。Exchange Server 服务器有两种版本，标准版包括 Active Server、网络新闻服务和一系列与其他邮件系统的接口；企业版除了包括标准版的功能外，还包括与 IBM Office Vision、X.400、VM 和 SNADS 通信的电子邮件网关。

Microsoft Exchange 同活动目录高密度的集成在一起，当 Microsoft Exchange 安装在一个运行着的活动的服务器上时，默认会将所有用户和账户信息存储在活动目录的数据存储中。采取这样的方法可以保证所有数据和信息的复制能够保持同步。

8.1.2 数据库服务器

数据库(Database)是按照数据结构来组织、存储和管理数据的仓库，它产生于五十年前，随着信息技术和市场的发展，特别是二十世纪九十年代以后，数据管理不再仅仅是存储和管理数据，而转变成用户所需要的各种数据管理的方式。数据库有很多种类型，从最简单的存储有各种数据的表格到能够进行海量数据存储的大型数据库系统都在各个方面得到了广泛的应用。

运行在局域网中的一台或多台计算机和数据库管理系统软件共同构成了数据库服务器，数据库服务器为用户应用提供服务，这些服务是查询、更新、事务管理、索引、高速缓存、查询优化和安全及多用户存取控制等。

SQL Server 是 Microsoft 大型数据库管理系统，它建立在成熟而强大的关系模型基础上，可以很好的支持客户机和服务器网络模式，能够满足各种类型的企业对构建网络数据库的需求，并且在易用性、可扩展性、可靠性以及数据仓库等方面确立了世界领先的地位。

SQL Server 作为数据存储机制、活动目录在很大程度上使用 SQL Server。然而，这一环节上缺少了访问控制。如果需要访问控制只有 SQL Server 具有的性能，那么，推荐使用活动目录和 SQL Server。

8.1.3 监视服务器与故障排除

当管理公司的复杂系统时，可能需要计划、设计、实施与监督和替换服务器、服务和应用程序，这一过程良好的管理可以节省时间和金钱，并且使组织得到满足。

信息技术基础架构库(ITIL)是一组管理信息技术系统的概念和做法，例如：IT 服务管理、IT 开发和 IT 作业。ITIL 根据自己单位的需要，给出一些重要 IT 做法详细的描述，提供详细完整的检验清单、任务和程序。

当要开始使用一个服务器、服务或者应用程序的时候，应该遵循一定的步骤来执行。这些步骤包括：

(1)收集需求；

(2)设计和规划；

(3)实施；

(4)管理和监控。

收集需求，是在定义的服务器、服务、应用程序时应该做的，包括其工作量。如果没有

适当的收集需求，可能会根据所需求的目标选择错误的硬件或软件。然后，用户必须规划和设计服务器、服务或者应用程序，以确保所做的事情是应该做的而不会干扰其他服务器、服务或者应用程序。接下来将实际操作服务器、服务或者应用程序，其中包括对其进行的安装和配置。最后需要管理和监控服务器、服务或者应用程序以确保所执行工作的目的是让用户和服务可以存取它。当监控系统时应该看看系统效能，以了解何时更换服务器、服务或者应用程序。用户需要找出潜在的问题，在影响服务器、服务或者应用程序之前将其修正。

当管理服务器时，可以选择以下两种方法：主动或者被动。主动的含义是在服务器、服务或者应用程序效能降低或者无法使用前，提前计划或者预见问题，意味着用户正在等待问题发生之前解决这些问题。从长远看，最好的办法是要主动。当然必须分配一些时间和精力在硬件和软件上，来有效的监视服务器、服务或者应用程序。

使用有效方法排除故障减少解决问题的时间。微软产品支持用户使用“检测方法”，其中包括六个步骤：

(1)发现问题：确定并记录问题的症状和搜索技术信息资料，以确定问题是否为一个已知的情况。

(2)评估系统配置：询问客户端并且检查系统的文件，确定是否有任何硬件、软件或网络已经作了修改。包括任何新增加的事物。同时检查所有日志，包括寻找事件监视器。

(3)列出或追踪可能的方案，并尝试利用删除或停用的硬件或软件组件找出问题，可以考虑开启额外的日志记录或运行诊断程序，收集更多资讯和试验某些组件。

(4)执行计划：测试潜在的解决方案，如果这些解决方案无法解决或者对计算机造成负面影响，这时应该有应变的计划。当然，不能使问题变得更糟，可能的话需要备份所有重要的系统或者应用程序文件。

(5)检查结果：如果问题并未解决，回去追溯可能的其他解决方案。

(6)采取主动式的做法：记录沿途解决这个问题所做的更改。同时通知客户与记录问题的症状，以防止发生解决了这个问题后影响到其他领域。

解决问题时需要用到几个工具，可以帮助隔离和解决问题，具体如下：

- 系统消息；
- 事件监视器；
- Windows 任务管理器；
- 资源管理器；
- 效能监视器；
- 系统设定；
- 内存检测工具；
- 故障排除指南；
- 启动选项包括安全模式；
- Windows 修复。

8.2 了解 Web 服务

Web Service 技术，能使得运行在不同机器上的不同应用无须借助附加的、专门的第三方软件或硬件，就可相互交换数据或集成。依据 Web Service 规范实施的应用之间，无论它们所使用的语言、平台或内部协议是什么都可以相互交换数据。Web Service 是自描述、自包含的可用网络模块，可以执行具体的业务功能。Web Service 也很容易部署，因为它们基于一些常规的产业标准以及已有的一些技术，诸如标准通用标记语言下的子集 XML、HTTP 等。Web Service 减少了应用接口的花费，Web Service 为整个企业甚至多个组织之间的业务流程的集成提供了一个通用机制。

8.2.1 IIS、WWW 和 FTP

IIS 是 Internet Information Services 的缩写，是一个 World Wide Web Server。Gopher Server 和 FTP Server 全部包容在里面。IIS 意味着用户能发布网页，并且由 ASP (Active Server Pages)、JAVA、VB Script 产生页面，有着一些扩展功能。IIS 支持有编辑环境的界面(FrontPage)、有全文检索功能的(Index Server)、有多媒体功能的(Net Show)。其次，IIS 是随 Windows NT Server 4.0 一起提供的文件和应用程序服务器，是在 Windows NT Server 上建立 Internet 服务器的基本组件。它与 Windows NT Server 完全集成，允许使用 Windows NT Server 内置的安全性以及 NTFS 文件系统建立强大灵活的 Internet/Intranet 站点。IIS(Internet Information Server，互联网信息服务)是一种 Web(网页)服务组件，其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面，它使得在网络(包括互联网和局域网)上发布信息成了一件很容易的事。Windows Server 2008 R2 包含 IIS 7.5、Windows Server 2008 包含 IIS 7.0、Windows Server 2003 包含 IIS 6.0。IIS 7.0 和 IIS 7.5 支持 FTP、FTPS、SMTP 和 HTTP/HTTPS 协议，而 IIS 6.0 支持 FTP、SMTP 和 HTTP/HTTPS。

WWW 是环球信息网的缩写，(亦作“Web”、“WWW”、“W3”，英文全称为“World Wide Web”)，中文名字为“万维网”，“环球网”等，常简称为 Web。分为 Web 客户端和 Web 服务器程序。WWW 可以让 Web 客户端(常用浏览器)访问浏览 Web 服务器上的页面。WWW 是一个由许多互相链接的超文本组成的系统，通过互联网访问。在这个系统中，每个有用的事物，称为一样“资源”；并且由一个全局“统一资源标识符”(URI)标识；这些资源通过超文本传输协议(Hypertext Transfer Protocol)传送给用户，而后者通过点击链接来获得资源。

FTP 是 TCP/IP 网络上两台计算机传送文件的协议，FTP 是在 TCP/IP 网络和 Internet 上最早使用的协议之一。尽管 World Wide Web(WWW)已经替代了 FTP 的大多数功能，FTP 仍然是通过 Internet 把文件从客户机复制到服务器上的一种途径。FTP 客户机可以给服务器发出命令来下载文件、上传文件、创建或改变服务器上的目录。原来

的 FTP 软件多是命令行操作，有了像 CUTEFTP 这样的图形界面软件，使用 FTP 传输变得方便易学。主要使用它进行“上载”，即向服务器传输文件，由于 FTP 协议的传输速度比较快。FTP 是应用层的协议，它基于传输层，为用户服务，它们负责进行文件的传输。FTP 是一个 8 位的客户端/服务器协议，能操作任何类型的文件而不需要进一步处理，就像 MIME 或 Unicode 一样。但是 FTP 有着极高的延时，这意味着，从开始请求到第一次接收需求数据之间的时间会非常长，并且不时的必须执行一些登录进程。FTP 服务一般运行在 20 和 21 两个端口。端口 20 用于在客户端和服务器之间传输数据流，而端口 21 用于传输控制流，并且是命令通向 FTP 服务器的进口。当数据通过数据流传输时，控制流处于空闲状态。而当控制流空闲很长时间后，客户端的防火墙会将其会话置为超时，这样当大量数据通过防火墙时，会产生一些问题。此时，虽然文件可以成功的传输，但因为控制会话会被防火墙断开，传输会产生一些错误。

8.2.2　添加组件

IIS 的添加：请进入“控制面板”，依次单击“添加/删除程序”→“添加/删除 Windows 组件”，将“Internet 信息服务(IIS)”前的小钩去掉，重新单击提示操作即可完成 IIS 组件的添加。用这种方法添加的 IIS 组件中将包括 Web、FTP、NNTP 和 SMTP 等全部四项服务。

IIS 的运行当 IIS 添加成功之后，再进入“开始”|“设置”|“控制面板”|“管理工具”|“Internet 服务管理器(Internet 信息服务)”以打开 IIS 管理器，对于有“已停止”字样的服务，均在其上单击右键，选“启动”来开启。

8.2.3　站点

站点内容管理平台主要管理的是逻辑单元，站点管理是对一个 Internet 的站点进行组织、维护和管理的功能集合。站点可分父子站点(站点和虚拟目录)，通过站点管理，用户可以根据自己的需要设计出自己网站结构。

若要建立新站点，可以执行如下操作步骤：

(1)打开 IIS 管理界面。

(2)在界面中鼠标右键单击网站树中的网站节点，然后单击新增网站。

(3)在新增网站对话框中，在网站名称框中输入一个网站的友好名称。

(4)如果想选择一个不同于框中所列的应用程序群集，需要单击选取。在选择应用程序群集对话框中，选择一个应用程序群集列表，然后单击确定。

(5)输入 Web 站点的文件夹的所在路径或者单击浏览按钮(…)转移到文件系统来寻找所用文件夹。

(6)如果输入的文件夹路径为远程共用，需要单击连接身份按钮来指定有权限的存取路径的特定用户。如果不使用特定使用者，则选择应用程序的使用者选项。

(7)从类型列表选择站点协议。

(8)预设值在 IP 地址栏中为全部未指派。如果用户必须指派一个网站的静态 IP 地址就需要输入在 IP 地址栏中输入 IP 地址。

(9)在连接文字方框中输入端口号。

(10)在主机名称方框中输入一个主机名称。

(11)如果不进行对站点的任何修改,并且希望站点立即使用,则选择立即启用站点。

(12)单击“确定”按钮。

预设定的 Web 站点应对所有 IP 地址分配给服务器的端口号为 80 和 443。此外,任何一个 Web 服务器将名称对应于一个 IP 地址。为了支援多个站点,用户可以指定额外的 IP 地址和分配给每一个站点一个 IP 地址。还可以定义不同的端口号而不是 80 或者 443 端口。

可以共享同一个 IP 和端口号的方法是使用主机名,这是用来指定该网站将回应的一个名称,而不是指向所有名称的位置。

要设定 IP 地址、端口号并且命名回应名称,用户需要设定站点连接。要改变站点的连接,在 IIS 管理界面中鼠标右键单击该站点,然后选择连接,单击站点中要更改的项目,然后单击编辑按钮。如果需要新增的话,可以单击新增按钮。

虚拟目录是用于一个网站的一个目录,对应于服务器其他位置上的一个真实文件夹或者另一台服务器的一个网站。这允许用户在对各网站重复使用相同的文件夹而不需要移动位置。

8.2.4 端口

端口可以认为是计算机与外界通讯交流的出入口。逻辑意义上的端口一般是指 TCP/IP 协议中的端口,端口号的范围为 0～65535,比如用于浏览网页服务的 80 端口,用于 FTP 服务的 21 端口等。

本地操作系统会给那些有需求的进程分配协议端口(Protocol Port,即端口),每个协议端口由一个正整数标识,例如:80、139、445 等。当目的主机接收到数据包后,将根据报文首部的目的端口号,把数据发送到相应端口,而与此端口相对应的那个进程将会领取数据并等待下一组数据的到来。端口其实就是队列,操作系统为各个进程分配了不同的队,数据包按照目的端口被推入相应的队中,等待进程取用,在极特殊的情况下,这个队也是有可能溢出的,不过操作系统允许进程指定和调整自己的队的大小。不光接受数据包的进程需要开启它自己的端口,发送数据包的进程也需要开启端口,这样数据包中将会标识有源端口,以便接受方能顺利地回传数据包到这个端口。

根据提供服务类型的不同,端口分为两种,一种是 TCP 端口,另一种是 UDP 端口。计算机之间相互通信时,分为两种方式:一种是发送信息以后,可以确认信息是否到达,也就是有应答的方式,这种方式大多采用 TCP 协议;另一种是发送以后就不管了,不去确认信息是否到达,这种方式大多采用 UDP 协议。对应这两种协议的服务提供的端口,也就分为 TCP 端口和 UDP 端口。

8.2.5 SSL

SSL(Secure Sockets Layer,即安全套接层)用于保障在 Internet 上数据传输的安全,利用数据加密(Encryption)技术,可确保数据在网络上的传输过程中不会被截取及窃听。

SSL 协议位于 TCP/IP 协议与各种应用层协议之间，为数据通讯提供安全支持。SSL 协议可分为两层：SSL 记录协议(SSL Record Protocol)：它建立在可靠的传输协议(例如 TCP)之上，为高层协议提供数据封装、压缩、加密等基本功能的支持；SSL 握手协议(SSL Handshake Protocol)：它建立在 SSL 记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法和交换加密密钥等。

当用户使用 SSL 加密网络流量时，使用非对称加密技术，它设计了一个公开密钥和私有密钥。公开密钥使用两个密钥，一个是公开的，另一个是私有的。两种密钥都能进行数据加密，但是只有私有密钥可以进行数据加密。为了方便于应用，需要依赖于公开密钥基础结构(PKI)来实现。这两个密钥由一个数学过程生成，两个密钥之间通过数学过程相关联。所以用其中一个密钥加密的信息只可以被另一个密钥解密。私有密钥加密技术也称为对称密钥加密技术，或者常规加密技术。这种加密技术使用同一个密钥对数据进行加密和解密。也就是说，锁门和开门所使用的是同一把钥匙。信息的发送者和接收者使用的是相同的密码或者密钥。发送者用这个密钥给信息编码，接收者用同一个密钥给信息解码。这种加密的形式在公共领域中不是最安全的。因为对于广泛发布的信息，无数的团体都可以拥有对应的密钥。在密钥不太可能泄露的网络身份验证中，可以使用这种加密方式。

8.2.6　数字证书

数字证书为实现双方安全通信提供了电子认证。在因特网、公司内部网或外部网中，使用数字证书实现身份识别和电子信息加密。数字证书中含有密钥(公开密钥和私有密钥)对所有者的识别信息，通过验证识别信息的真伪实现对证书持有者身份的认证。

数字证书在用户公开密钥后附加了用户信息及 CA 的签名。公开密钥是密钥对的一部分，另一部分是私有密钥。公开密钥公之于众，谁都可以使用。私有密钥只有自己知道。由公开密钥加密的信息只能由与之相对应的私有密钥解密。为确保只有某个人才能阅读信件，发送者要用收件人的公有密钥加密信件；收件人便可用自己的私有密钥解密信件。同样，为证实发件人的身份，发送者要用自己的私有密钥对信件进行签名；收件人可使用发送者的公开密钥对签名进行验证，以确认发件人的身份。在线交易中可使用数字证书验证对方身份。用数字证书加密信息，可以确保只有接收者才能解密、阅读原文，确保信息在传递过程中的保密性和完整性。有了数字证书网上安全才得以实现，电子邮件、在线交易和信用卡购物的安全才能得到保证。所以数字证书具有以下功能：

- 保密性：只有收件人才能阅读信息。
- 认证性：确认信息发送者的身份。
- 完整性：信息在传递过程中不会被篡改。
- 不可抵赖性：发送者不能否认已发送的信息。
- 保证请求者与服务者的数据交换的安全性。

CA 是证书的签发机构。CA 是负责签发证书、认证证书、管理已颁发证书的机关。它要制定政策和具体步骤来验证、识别用户身份，并对用户证书进行签名，以确保证书持有者的身份和公开密钥的拥有权。

CA 也拥有一个证书(内含公开密钥和私有密钥)。网上的公众用户通过验证 CA 的签字从而信任 CA,任何人都可以得到 CA 的证书(含公开密钥),用以验证它所签发的证书。

如果用户想得到一份属于自己的证书,他应先向 CA 提出申请。在 CA 判明申请者的身份后,便为他分配一个公开密钥,并且 CA 将该公开密钥与申请者的身份信息绑在一起,并为之签字后,便形成证书发给申请者。如果一个用户想鉴别另一个证书的真伪,就用 CA 的公开密钥对那个证书上的签字进行验证,一旦验证通过,该证书就被认为是有效的。证书实际是由证书签证机关(CA)签发的对用户的公开密钥的认证。

证书的内容包括:电子签证机关的信息、公开密钥用户信息、公开密钥、权威机构的签字和有效期等。目前,证书的格式和验证方法普遍遵循 X.509 国际标准。

8.3 了解远程访问

远程访问是集成的"路由和远程访问"服务的一部分,用来为远程办公人员、外出人员,以及监视和管理多个部门办公室服务器的系统管理员提供远程网络。

通常需要进行远程访问的人有两类,一类是系统管理员,另一类是普通的用户。

系统管理员通常需要远程访问企业内网的网络设备或服务器,进行远程配置管理操作。以目前的产品发展来看,大部分企业级的网络设备或服务器,通常都提供远程配置管理的接口或功能,管理员可以通过 Telnet、SSH、Web GUI 乃至远程管理软件终端等方式,从企业网络的 WAN 侧进入内网进行管理维护。

普通用户的远程访问需求,通常是远程办公人员、外出人员,尤其是企业高管等需要经常出差又经常需要操作 ERP、CRM、HR 等信息化系统,进行查看、审批和提单等操作。在企业信息化不断发展进步的今天,越来越多的此类远程访问需求逐渐成为企业 IT 管理员关注的焦点。

8.3.1 远程管理

对于早期网络,用户使用简易的终端(系统包括一个显示器或键盘,不包含中央处理器)连接到一个主机。后来计算机可以使用 Telnet 连接到服务器并在命令提示界面执行命令。远程桌面前身为终端服务,是 Microsoft Windows 其中的一个组件,允许使用者通过网络存取远程计算机的应用程序和资料。

根据设定,Windows 服务器被设定为可以使用远程桌面的用户授权的模式,最多支持两个远程连接,主要是用于连接到服务器来执行管理工作。但是,如果用户执行的应用程序需要超过标准的两个远程对话时,用户需要首先进入和设定一个名为远程桌面会话主机的服务器角色,还需要服务器授权。

要对远程计算机进行操作,用户会通过远程桌面连接到远程计算机,包括桌面、程序,就好像坐在远端的计算机前面一样。有两种方法可以实现远程管理,一种是存取远程计算机的桌面,另一种是通过 TCP 端口 1389 来实现远程协助。

要实现远程管理计算机需要具备以下条件：

- 被连接的计算机必须是开机状态。
- 需要网络连接。
- 被连接的计算机必须启用远程桌面服务。
- 必须具有连接权限。(管理员组成员或者远程桌面使用者组成员)

启用远程桌面的方法：

- 鼠标右键单击“计算机”,单击“属性”后选择“远程设置”。
- 选择允许哪些方式远程连接计算机。第一种方式是允许来自任何版本的计算机进行连接(较不安全),第二种是仅允许通过网络验证的计算机进行连接(较安全)。
- 系统提示用户输入管理员的账号和密码。
- 单击“选择用户”,设置哪些用户可以进行访问。

远程连接桌面的方法：

- 单击“开始”中的“运行”,在“运行”中输入 mstsc.exe 打开远程桌面窗口。
- 输入远程计算机的计算机名或者 IP 地址,单击“显示选项”设置详细的连接信息,然后单击“连接”。

远程连接桌面软件是一种特殊模式的远程桌面服务,是可以在用户自己的计算机桌面上执行的应用程序。这个应用程序可以对远程计算机控制进行设置,然后将设置信息打包成一个.rdp 文件或者分散式的.msi 的 Windows 安装程序,这样就可以根据需要正确连接到远程计算机的桌面了。

8.3.2　VPN

VPN(虚拟专用网络)可以在公用网络上建立专用网络,进行加密通讯。在企业网络中有广泛应用。VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN 有多种分类方式,主要是按协议进行分类。VPN 可通过服务器、硬件、软件等多种方式实现。VPN 具有成本低,易于使用的特点。

VPN 属于远程访问技术,简单地说就是利用公用网络架设专用网络。例如某公司员工出差到外地,想访问企业内网的服务器资源,这种访问就属于远程访问。在传统的企业网络配置中,要进行远程访问,传统的方法是租用 DDN(数字数据网)专线或帧中继,这样的通讯方案必然导致高昂的网络通讯和维护费用。对于移动用户(移动办公人员)与远端个人用户而言,一般会通过拨号线路(Internet)进入企业的局域网,但这样必然带来安全上的隐患。

让外地员工访问到内网资源,利用 VPN 的解决方法就是在内网中架设一台 VPN 服务器。外地员工在当地连上互联网后,通过互联网连接 VPN 服务器,然后通过 VPN 服务器进入企业内网。为了保证数据安全,VPN 服务器和客户机之间的通讯数据都进行了加密处理。有了数据加密,就可以认为数据是在一条专用的数据链路上进行安全传输,就如同专门架设了一个专用网络一样,但实际上 VPN 使用的是互联网上的公用链路,因此 VPN 称为虚拟专用网络,其实质上就是利用加密技术在公网上封装出一个数据通讯隧道。有了 VPN 技术,用户无论是在外地出差还是在家中办公,只要能上互联网就能利用

VPN 访问内网资源，这就是 VPN 在企业中应用得如此广泛的原因。

Windows Server 2008 的 VPN 服务器使用的三种通道类型如下：

(1)点对点通道通讯协议(Point-to-Point Tunneling Protocol，PPTP)：点对点通信只能实现网络内任意两个用户之间的信息交换。点对点的通信时，只有一个用户可收到信息。作为一种计算机网络的通信模式，点对点通信中的两台计算机处在同等地位，有时也称对等网络(Peer to Peer Network)。它们共享网络资源，每台机器都以同样的方式作用于对方。在对等网络中，所有计算机既是服务器又是客户机。PPTP 是容易建立的，但加密技术相对薄弱。

(2)第二层通道通讯协议(Layer 2 Tunneling Protocol，L2TP)：用来整合多协议拨号服务至现有的因特网服务提供商。PPP 定义了多协议跨越第二层点对点链接的一个封装机制。用户通过使用众多技术之一(如：拨号 POTS、ISDN、ADSL 等)获得第二层连接到网络访问服务器(NAS)，然后在此连接上运行 PPP。在这样的配置中，第二层终端点和 PPP 会话终点处于相同的物理设备中(如：NAS)。L2TP 扩展了 PPP 模型，允许第二层和 PPP 终点处于不同的由包交换网络互相连接的设备。通过 L2TP，用户在第二层连接到一个访问集中器(如：调制解调器池、ADSL DSLAM 等)，然后这个集中器将单独的 PPP 帧隧道到 NAS。这样，可以把 PPP 包的实际处理过程与 L2 连接的终点分离开来。对于这样的分离，其明显的一个好处是：L2 连接可以在一个(本地)电路集中器上终止，然后通过共享网络帧中继电路或广域网扩展逻辑 PPP 会话，而不用在 NAS 上终止。从用户角度看，直接在 NAS 上终止 L2 连接与使用 L2TP 没有什么功能上的区别。L2TP 协议也用来解决“多链接联选组分离”问题。多链接 PPP，一般用来集中 ISDN 通道，需要构成多链接捆绑的所有通道在一个单独网络访问服务器(NAS)上组合。因为 L2TP 使得 PPP 会话可以出现在接收会话的物理点之外的位置，它用来使所有的通道出现在单个的 NAS 上，并允许多链接操作，即使是在物理呼叫分散在不同物理位置的 NAS 上的情况下。用 IPSec 来提供安全保护，L2TP 是建立安全通道的业界标准。

(3)安全通讯端通道通讯协议(Secure Socket Tunneling Protocol，SSTP)：由 Windows Server 2008 首先引入，用户运用 HTTPS 通讯协议通过 TCP 端口 443 传输流量和用过封锁 PPTP 与 L2TP/IPSec 连接防火墙与 Web 代理服务器。

使用 VPN 时有以下几种形式的身份验证：

(1)密码验证通讯协议(Password Authentication Protocol，PAP)：使用纯文字(未进行加密的密码)。PAP 是最低的安全身份验证，不建议使用。

(2) Challenge Handshake 验证通讯协议(Challenge Handshake Authentication Protocol，CHAP)：是一种挑战响应(Challenge-Response)身份验证，使用业界标准的 MD5 拼凑方法来加密回应。

(3)微软的 CHAP 版本 2(MS-CHAP v2)：提供双向认证(相互认证)。MS-CHAP v2 提供比第一版本更强的安全性。

(4)可延伸认证通讯协议(EAP-MS-CHAP v2)：通过认证架构允许开发定义的身份认证方案，包括扫描、声音识别、指纹识别、智慧卡、Kerberos 和数位认证。还提供一个相互认证的方法，支持基于密码的用户或者计算机身份验证。

8.3.3　应用程序虚拟化

应用虚拟化将应用程序与操作系统整合，为应用程序提供了一个虚拟的运行环境。在这个环境中，不仅包括应用程序的可执行文件，还包括它所需要的运行时环境。从本质上说，应用虚拟化是把应用对低层的系统和硬件的依赖抽象出来，可以解决版本不兼容的问题。

所谓应用虚拟化，技术原理是基于应用/服务器计算 A/S 架构，采用类似虚拟终端的技术，把应用程序的人机交互逻辑（应用程序界面、键盘及鼠标的操作、音频输入输出、读卡器和打印输出等）与计算逻辑隔离开来。在用户访问一个服务器虚拟化后的应用时，用户计算机只需要把人机交互逻辑传送到服务器端，服务器端为用户开设独立的会话空间，应用程序的计算逻辑在这个会话空间中运行，把变化后的人机交互逻辑传送给客户端，并且在客户端的相应设备上展示出来，从而使用户获得如同运行本地应用程序一样的访问感受。

App-V（Application Virtualization）应用程序虚拟化。是 MDOP 中提供了一套用于优化客户端桌面环境的组件，MDOP 是桌面优化套件（Microsoft Desktop Optimization Pack）。App-V 允许用户通过网络获得一个软件的虚拟运行环境，然后无需安装软件，直接可以在虚拟环境中运行软件。

8.4　了解文件和打印服务

打印和文件服务允许用户集中执行打印服务器和网络打印机任务。使用此角色，用户还可以从网络扫描仪中接收扫描的文档，并将这些文档路由到共享网络资源、Windows SharePoint Services 站点或电子邮件地址。

用户还可以使用传真服务器发送和接收传真，并允许用户管理传真服务器，例如任务、设置、报告和传真设备之类的传真资源。

打印服务器可以帮助用户监视打印队列，并在打印队列停止处理打印作业时接收通知。此外，使用该服务，还可以使用组策略迁移打印服务器并部署打印机连接。分布式扫描服务器提供了从网络扫描仪中接收扫描的文档并将其路由到正确目标的服务。它还包括“扫描管理”管理单元，用户可以使用该单元管理网络扫描仪和配置扫描进程。传真服务器服务器角色可以为传真管理员节省大量的时间。无需在客户端计算机上安装传真计算机并管理和监视传真计算机，用户可以用 2 个或 3 个步骤同时在多台计算机上远程完成那些步骤。通过使用传真服务管理器，用户可以自动使传真连接对用户的组织中的用户和计算机可用。

8.4.1　本地打印机

通过相关驱动程序和配置程序，在计算机上直接设置的打印机配置工具，称本地打印机。本地打印机可供本机使用，也可供远程使用。

访问本地打印机有两种方式:自动的打印机重定向和手动的打印机重定向。当在远程计算机上运行的 Windows 版本中没有本地打印机所需要的驱动程序时,使用手动重定向。

当本地打印机使用安装在服务器上的驱动程序时,打印机自动重定向。当登录到终端服务器上的会话,或运行 Windows Professional 或 Server 和"远程桌面"的计算机时,将自动检测网络打印机以及客户端(本地)计算机上安装的所有打印机,并在服务器上创建本地队列。该服务器可以使用默认打印机的客户端打印机设置和一些属性(例如双面打印)。当用户断开连接或结束会话时,打印机队列将被删除,且不完整或待打印作业将丢失。有关客户端的本地打印机和设置的信息都保存在客户端的计算机上。在以后登录时,使用存储在客户端计算机上的信息创建打印机队列。

如果在该服务器上找不到打印机驱动程序,则在日志中记录事件,而且不创建客户端打印机。为使打印机可用,驱动程序必须是手动安装在服务器上的。

虽然不支持手动重定向通过 USB 端口连接的打印机,但可手动重定向连接到客户端(本地)计算机上的 LPT 和 COM 端口的打印机。要手动重定向客户端打印机,请与管理员联系并提供计算机的名称(或对基于 Windows 的终端则提供 IP 地址)。客户端必须在手动重定向期间连接到远程计算机。在初次进行手动重定向之后,打印机将在以后的登录过程中自动重定向。

8.4.2 网络打印机

网络打印机是指通过打印服务器(内置或者外置)将打印机作为独立的设备接入局域网或者 Internet,从而使打印机摆脱一直以来作为电脑外设的附属地位,使之成为网络中的独立成员,成为一个网络节点、信息管理与输出终端,其他成员可以直接访问使用该打印机。

从表面上看,网络打印与共享打印的区别是一根线和几根线。网络打印只需要一根网线,而共享打印则是有几个终端就需要几根导线。而从技术上看,网络打印机通过 EIO 插槽直接连接网络适配卡,能够以网络的速度实现高速打印输出。而共享打印是通过计算机服务器或者共享实现简单的网络连接,数据传输仍然必须通过打印机的并口来进行,因此速度很低。

网络打印机要接入网络,一定要有网络接口,目前有两种接入的方式,一种是打印机自带打印服务器,打印服务器上有网络接口,只需插入网线分配 IP 地址就可以了;另一种是打印机使用外置的打印服务器,打印机通过并口或 USB 口与打印服务器连接,打印服务器再与网络连接。

网络打印机一般有管理和监视软件,通过管理软件可以从远程查看和干预打印任务,对打印机的配置参数进行设定,绝大部分的网络打印管理软件都是基于 Web 方式的、简单快捷。通过监视软件,用户可以查看打印任务,打印机的工作状态等信息。一般管理软件是给网管或者高级用户使用的,普通用户都只有打印机监视功能。

网络打印机对于工作组和部门级打印机来说是一个必备功能,因为网络连接的易管理性和高的传输速率对于工作组和部门级用户都有非常明显的优势,影响打印机的网络

打印功能和性能的两个重要方面是网络打印服务器和网络管理软件。一个完善的网络打印机的网络打印服务器不仅仅是一个网络适配器，它必须根据打印需求对网络连接性能进行优化，同时还需要与打印机内部控制器很好地匹配，同时还要有一定的网络流量管理和打印队列管理的能力，可以适应多种网络环境。一个好的网络管理软件，可以在多种平台下使用，用户可以通过它实现打印机的全方位管理和控制，同时还可以通过网络及时进行升级。

8.4.3　打印机池

打印池是由一组打印机组成的一个逻辑打印机，它通过打印服务器的多个端口连接到多台打印机。处于空闲状态的打印机便可以接收发送到逻辑打印机的下一份文档。

这对于打印量很大的网络非常有帮助，因为它可以减少用户等待文档的时间。使用打印池还可以简化管理，因为可以从服务器上的同一台逻辑打印机来管理多台打印机。使用创建的打印池，用户打印文档时不再需要查找目前哪一台打印机可用。逻辑打印机将检查可用的端口，并按端口的添加顺序将文档发送到各个端口。应首先添加连接到快速打印机上的端口，这样可以保证发送到打印机的文档在分配给打印池中的慢速打印机前以最快的速度打印。

在设置打印池之前，应考虑以下几点：池中的所有打印机必须使用相同的驱动程序。由于用户不知道指定的文档由池中的哪一台打印机打印，因此确保池中的所有打印机位于同一位置。

8.4.4　Web 打印

随着 IIS 与 Windows Server 操作系统完全集成，如果安装并启用了 IIS 服务，客户端就能够通过 Https 协议连接打印服务器的打印机。在连接服务器的逻辑打印机共享时，服务器自动将所需的打印机驱动程序更新到客户端。

Web 打印使用简单、灵活，能满足绝大多数页面打印的需要，它内含一个在 vc7.0 上开发的 ATL 小控件(只有 74 K)，这个小控件主要实现对 IE 浏览器中文档打印格式的控制，可以定制打印纸型、纸张来源、打印方向、设置表头、表尾、表格、表格列宽、打印预览、分页、缩放等用户经常关心的属性。Web 打印使用户通过脚本可以控制自定义纸张、打印方向和页边距等属性达到定制打印的目的，这些定制属性的设置不会改变 IE 浏览器的默认打印机属性。也可以通过服务器端的页面从而调用 Web 打印生成用户端的页面从而达到设置打印参数的目的。

8.4.5　文件、文件夹和共享权限和权力

权限是控制被访问对象的一种手段，是保护数据和网络资源的屏障。文件和文件夹权限由 NTFS 控制，一旦对 NTFS 格式化卷权限就没有了。就像文件夹和文件一样，卷用 NTFS 权限保护，一旦按照 NTFS 5.0 格式化一个卷，在 Windows 资源管理器上鼠标右键单击这个卷，然后在弹出的菜单中选择属性选项。单击属性对话框的安全选项卡，就会注意到默认情况下很多组都有访问文件夹的权限。最可疑的组是“Everyone”。

虽然 Everyone 组添加到了安全设置中，但是默认情况下是没有权利的。但是，仍然建议修改这种默认的行为，并且在赋予了对新建文件夹访问权限的默认组中，将 Everyone 组删除。

若要删除组，可以执行如下操作步骤：

(1)在 Windows 资源管理器中选择磁盘卷，然后鼠标右键单击，继而选择属性选项，这个动作将加载该卷的属性对话框。之后在对话框中选择安全选项卡。

(2)在属性对话框上单击高级按钮。将打开高级安全设置对话框。如果组列表中包含 Everyone 组，就删除这个组或者禁止该组拥有任何权利。最好的办法是删除这个组，因为一开始列表中就没有 Everyone 组比拒绝使用任何权利要安全得多。而且选择拒绝选项将关闭整个共享，因为这样做可以拒绝任何人访问，使文件或者文件夹更安全。

(3)选中“替换所有子对象的权限”，这时有关更改的内容将被警告；在警告对话框中单击“确定”按钮继续。现在，就对驱动器上所有对象拥有访问权的组的列表中删除掉了 Everyone 组。

文件夹的权限类型如下：

- 完全控制：这个权限允许用户获得所有权以及执行所有动作。
- 修改：这个权限允许用户修改或删除其所辖的文件夹以及该文件夹所有权限。
- 读和执行：这个权限允许移动文件夹，也可以让用户在管理和所有子文件夹下的这个文件夹中读文件和执行应用程序。
- 读：这个权限是对文件夹内容提供访问的第一个权限，没有这个权限不能访问该文件夹中的内容。“读”权限允许用户看所有权、权限和文件属性。
- 写：这个权限允许用户创建文件和这个文件夹管理下的文件夹也能改变文件属性以及查看所有权和权限。
- 列出文件内容：这个权限允许用户查看这个文件夹管理下的文件和子文件夹。
- 特殊权限：只有启用了特殊权限或者高级权限，才可以选中该权限的复选框。只有通过高级按钮才能访问高级权限。

文件的权限类型如下：

- 完全控制：这个权限允许用户获得所有权以及执行所有动作。
- 修改：这个权限允许用户删除和执行文件的所有动作。
- 读和执行：这个权限允许用户运行应用程序，也可以对文件应用读的权限。
- 读：这个权限允许用户读文件、查看文件属性、所有者和权限。
- 写：这个权限允许用户修改文件的内容和属性，并且能查看所有权和权限。
- 特殊权限：只有启用了特殊权限或者高级权限，才可以选中该权限的复选框。只有通过高级按钮才能访问高级权限。

共享文件夹的权限类型如下：

(1)读：用户能够看见整个共享文件夹树(根共享文件夹和子共享文件夹)。用户也能在文件夹树里看见所有文件并且打开文件进行阅读。用户可以按照共享文件夹层次执行应用程序。

(2)修改：该特殊权限继承读的权限并且允许用户在共享文件夹的名字空间以内修改

文件夹和文件中的数据。用户也可以修改文件的属性,以及能够复制、移动和删除文件和文件夹。但是用户不能改变实际的共享。

(3)完全控制:该特权允许用户在共享文件夹的名字空间里获得文件和文件夹的所有权,它继承了读和修改的权限。在 NTFS 下,只有完全控制允许用户修改权限和获得文件和文件夹的所有权。

8.4.6　审核

每当用户执行了指定的某些操作,审核日志就会记录一个审核项。例如,修改文件或策略可以触发一个审核项。审核项显示了所执行的操作、相关的用户账户以及该操作的日期和时间。用户可以审核操作中的成功尝试和失败尝试。

计算机上的操作系统和应用程序的状态是动态变化的。例如,有时可能需要临时更改安全级别,以便立即解决管理问题或网络问题。这些更改经常会被忘记,并且永远不会撤销。这说明计算机可能不再满足企业安全的要求。作为企业风险管理项目的一部分,定期分析可以使管理员跟踪并确保每个计算机有足够的安全级别。分析的重点是专门指定的、与安全有关的所有系统方面的信息。这使用户可以调整安全级别,而且最重要的是,可以检测到系统中随着时间的推移而有可能产生的所有安全缺陷。

安全审核对于任何企业系统来说都极其重要,因为只能使用审核日志来说明是否发生了违反安全的事件。如果通过其他某种方式检测到入侵,正确的审核设置所生成的审核日志将包含有关此次入侵的重要信息。通常,失败日志比成功日志更有意义,因为失败通常说明有错误发生。例如,如果用户成功登录到系统,一般认为这是正常的。然而,如果用户多次尝试都未能成功登录到系统,则可能说明有人正试图使用他人的用户 ID 侵入系统。事件日志记录了系统上发生的事件。安全日志记录了审核事件。组策略的“事件日志”容器用于定义与应用程序、安全性和系统事件日志相关的属性,例如日志大小的最大值、每个日志的访问权限以及保留设置和方法。

8.4.7　打印作业管理

Windows Server 在一个组织单元对组织单元的基础上委托作业管理功能。从快捷键、打印菜单和各自打印队列对话框的菜单里访问作业管理选项。

- 暂停作业:双击打印机,打开队列或者打印作业管理器,然后选择一个打印文档,鼠标右键单击或者单击文档菜单,选择暂停选项。靠近这个文档会出现复选标记显示作业暂停。
- 暂停所有作业:鼠标右键单击打印机队列,选择脱机,所有作业被挂起。
- 恢复作业:恢复作业有两种方法。一种是从文档下拉式菜单选择恢复选项,另一种是鼠标右键单击这个作业,重新单击暂停选项,清除复选标记。
- 取消所有作业:在任何作业上鼠标右键单击队列窗口,选择“取消所有文档”选项。
- 删除单一作业:选择这个文档并且单击“删除”。

将停止的作业重定向到另一个物理打印机要比删除它们并重新提交它们要好。逻辑打印机保持不变,所做的只是更改端口和物理打印机。

打开逻辑打印机的属性,选择端口选项卡,然后选择一个新的端口,只需知道新的端

口与重定向的端口一样,使用相同的驱动程序,文档就会被打印。

8.5 了解服务器虚拟化

将服务器物理资源抽象成逻辑资源,让一台服务器变成几台甚至上百台相互隔离的虚拟服务器,我们将不再受限于物理上的界限,而是让 CPU、内存、磁盘、I/O 等硬件变成可以动态管理的"资源池",从而提高资源的利用率,简化系统管理,实现服务器整合,让 IT 对业务的变化更具适应力——这就是服务器的虚拟化。

本节将介绍服务器虚拟化的一些底层概念,通过掌握这些概念,用户将更容易地学习更高级的虚拟化技术。

8.5.1 虚拟化模式

虚拟化,是指通过虚拟化技术将一台计算机虚拟为多台逻辑计算机。在一台计算机上同时运行多个逻辑计算机,每个逻辑计算机可运行不同的操作系统,并且应用程序都可以在相互独立的空间内运行而互不影响,从而显著提高计算机的工作效率。

虚拟化是一个广义的术语。是指计算元件在虚拟的基础上而不是在真实的基础上运行,是一个为了简化管理,优化资源的解决方案。如同空旷、通透的写字楼,整个楼层没有固定的墙壁,用户可以用同样的成本构建出更加自主适用的办公空间,进而节省成本,发挥空间最大利用率。这种把有限的固定的资源根据不同需求进行重新规划以达到最大利用率的思路,在 IT 领域就叫做虚拟化技术。

虚拟化技术可以扩大硬件的容量,简化软件的重新配置过程。CPU 的虚拟化技术可以单 CPU 模拟多 CPU 并行,允许一个平台同时运行多个操作系统,并且应用程序都可以在相互独立的空间内运行而互不影响,从而显著提高计算机的工作效率。

虚拟化技术与多任务以及超线程技术是完全不同的。多任务是指在一个操作系统中多个程序同时并行运行,而在虚拟化技术中,则可以同时运行多个操作系统,而且每一个操作系统中都有多个程序运行,每一个操作系统都运行在一个虚拟的 CPU 或者是虚拟的主机上;而多线程技术只是单 CPU 模拟双 CPU 来平衡程序运行性能,这两个模拟出来的 CPU 是不能分离的,只能协同工作。

虚拟化可以通过很多方法来证实。它不是一个单独的实体,而是一组模式和技术的集合,这些技术提供了支持资源的逻辑表示所需的功能,以及通过标准接口将其呈现给这些资源的消费者所需的功能。这些模式本身都是前面介绍过的各种不同虚拟形式的重复出现。

下面是在实现虚拟化时常常使用的一些模式和技术:

(1)单一资源多个逻辑表示:这种模式是虚拟化最广泛使用的模式之一。它只包含一个物理资源,但是它向用户呈现的逻辑表示却仿佛它包含多个资源一样。用户与这个虚拟资源进行交互时就仿佛自己是唯一的用户一样,而不会考虑他正在与其他用户一起共享资源。

(2)多个资源单一逻辑表示:这种模式包含了多个组合资源,以便将这些资源表示为提供单一接口的单个逻辑表示形式。在利用多个功能不太强大的资源来创建功能强大且丰富的虚拟资源时,这是一种非常有用的模式。存储虚拟化就是这种模式的一个例子。在服务器方面,集群技术可以提供用户只与一个系统(头节点)进行交互,而集群事实上可以包含很多的处理器或节点。实际上,这就是从 IT 技术设施的角度看到的网格可以实现的功能。

(3)在多个资源之间提供单一逻辑表示:这种模式包括一个以 N 分之一的形式表示的虚拟资源。虚拟资源会根据指定的条件来选择一个物理资源实现,例如资源的利用、响应时间或临近程度。尽管这种模式与上一种模式非常类似,但是它们之间有一些细微的差别。首先,每个物理资源都是一个完整的副本,它们不会在逻辑表示层上聚集在一起。其次,每个物理资源都可以提供逻辑表示所需要的所有功能,而不是像前一种模式那样只能提供部分功能。这种模式的一个常见例子是使用应用程序容器来均衡任务负载。在将请求或事务提交给应用程序或服务时,用户并不关心到底是几个容器中执行的哪一个应用程序的副本为请求或事务提供服务。用户只是希望请求或事务得到处理。

(4)单个资源单一逻辑表示:这是用来表示单个资源的一种简单模式,就仿佛它是别的什么资源一样。启用 Web 的企业后台应用程序就是一个常见的例子。在这种情况下,用户不是修改后台的应用程序,而是创建一个前端来表示 Web 界面,它会映射到应用程序接口中。这种模式允许通过对后台对应用程序进行最少的修改(或根本不加任何修改)来重用一些基本的功能。也可以根据无法修改的组件,使用相同的模式构建服务。

(5)复合或分层虚拟:这种模式是刚才介绍的一种或多种模式的组合,它使用物理资源来提供丰富的功能集。信息虚拟化是这种模式一个很好的例子。它提供了底层所需要的功能,这些功能用于管理对资源、包含有关如何处理和使用信息的元数据以及对信息进行处理的操作的全局命名和引用。例如 Open Grid Services Architecture(OGSA)或者 Grid Computing Components,实际上都是虚拟化的组合或虚拟化的不同层次。

通过使用虚拟机技术,用户可以同时在一台计算机上执行多个操作系统,它允许分隔的服务,同时使成本降至最低。

8.5.2　VHD

微软的 VHD 文件格式是一种虚拟机硬盘(Virtual Machine Hard Disk),并可以被压缩成单个文件存放在宿主机器的文件系统上,主要包括虚拟机启动所需的系统文件。

关于 VHD 的应用,Virtual PC 是一种 Windows 虚拟机,它可以虚拟各种版本的 Windows,一个 Windows 应该装在一个硬盘分区上,而它是虚拟的 Windows,不可能单独划出一个硬盘分区给它安装,所以它启动所需的系统文件都被压缩成一个 VHD 格式的文件放在硬盘上。

VHD 格式还用于 Microsoft Windows Server 2008 R2,包括 Hypervisor 为基础的虚拟化技术(Hyper-V)。Hyper-V 可以离线操作 VHD ,使得管理员可以通过一个 VHD 文件安全进入系统,管理员可以对虚拟文件(VHD)访问和执行一些离线的管理任务。

VHD 虚拟硬盘有固定 VHD、动态 VHD、差异 VHD 和链接硬盘四种类型,用户可以

根据自己的实际需求去选择相应的格式。

• 固定 VHD:对已分配的大小不会更改。

• 动态 VHD:大小与写入的数据大小相同,并随着数据的写入而相应增加成减少直到达到大小上限。

• 差异 VHD :与动态 VHD 类似,但只包含所关联的父 VHD 修改后的磁盘块。

• 链接硬盘 VHD:文件本身指向一个磁盘或者一个分区。

VHD 具有如下优点:

• 维护简单:VHD 磁盘操作时就跟物理磁盘一样,维护起来较为简单,我们可以对它进行分区、格式化、压缩和删除等操作,这些操作并不影响物理分区。这种操作更有利于初学者反复试验分区和格式等功能。

• 像 U 盘般加载自如:当用户对 VHD 分区写入一些重要数据后,并不想他人修改其中的内容时,我们可以随时将此 VHD 进行脱机或分离操作;在需要的时候再将它附加进来进行修改。同样可以向 U 盘一样从“安全删除硬件并弹出媒体”中弹出某个 VHD。

• 轻松备份:备份时用户需要将创建的 VHD 文件进行备份,它所包含的分区中的内容便被统一备份,当然用户也可以用备份工具将 VHD 文件所在的整个物理分区进行备份。(Windows 7 和 Windows Server 2008 的 Backup 工具备份产生的主文件也是 VHD 格式)

• 迁移方便:当用户有一个 VHD 文件需要在多台计算机上使用时,用户只要先将此 VHD 分离开来,将其复制到目的计算机上,再进行附加即可。同时可以通过服务器进行分发,使用脚本附加到目的机。当然在物理机与虚拟机之间迁移也是没问题的。

• 与虚拟机互相通用:Windows Server 2008 R2 的 VHD 文件与 VPC、Hyper-V 的虚拟硬盘是互通的,用户可以将虚拟机中的 VHD 文件附加到 Windows Server 2008 R2 中。

• 可直接用于系统部署:我们可以使用 Imagex 工具将已经捕获的映像释放,或通过 WDS 服务器部署系统到 VHD。

• 双重的安全保护:由于 VHD 创建时产生的是一个存储文件,在这里可以对此文件和 VHD 的分区进行不同的权限限制,这样即可以对分区读写权限进行设置以保证部分用户有往 VHD 分区中存储数据的权限,也可以对此 VHD 文件设置读写权限以保证此文件在分离后不被他人给删除。

8.5.3 虚拟内存

虚拟内存是计算机系统内存管理的一种技术。它使得应用程序认为它拥有连续的可用的内存(一个连续完整的地址空间),而实际上,它通常是被分隔成多个物理内存碎片,还有部分暂时存储在外部磁盘存储器上,在需要时进行数据交换。

电脑中所运行的程序均需要经过内存执行,若执行的程序占用内存很大或很多,则会导致内存消耗殆尽。为解决该问题,Windows 中运用了虚拟内存技术,匀出一部分硬盘空间来充当内存使用。当内存耗尽时,电脑就会自动调用硬盘来充当内存,以缓解内存的紧张。若计算机运行程序或操作所需的随机存储器(RAM)不足时,则 Windows 会用虚

拟存储器进行补偿。它将计算机的 RAM 和硬盘上的临时空间组合。当 RAM 运行速率缓慢时，它便将数据从 RAM 移动到称为“分页文件”的空间中。将数据移入分页文件可释放 RAM，以便完成工作。一般而言，计算机的 RAM 容量越大，程序运行得越快。若计算机的速率由于 RAM 可用空间匮乏而减缓，则可尝试通过增加虚拟内存来进行补偿。但是，计算机从 RAM 读取数据的速率要比从硬盘读取数据的速率快，因而扩增 RAM 容量(可加内存条)是最佳选择。

虚拟内存是 Windows 为作为内存使用的一部分硬盘空间。即便物理内存很大，虚拟内存也是必不可少的。虚拟内存在硬盘上其实就是为一个大的文件，文件名是 PageFile.Sys，通常状态下是看不到的。必须关闭资源管理器对系统文件的保护功能才能看到这个文件。虚拟内存有时候也被称为是“页面文件”就是从这个文件的文件名中来的。

8.5.4　虚拟网络

虚拟网络是一种包含至少部分是虚拟网络链接的计算机网络。虚拟网络链接是在两个计算设备间不包含物理连接，而是通过网络虚拟化来实现。

VLAN(Virtual Local Area Network)建立在交换技术的基础上，将网络结点按工作性质与需要划分成若干个“逻辑工作组”，一个“逻辑工作组”即一个虚拟网络。VLAN 的实现技术有四种：用交换机端口(Port)号定义虚拟网络、用 MAC 地址定义虚拟网络、IP 广播组定义虚拟网络、用网络层地址定义虚拟网络。“逻辑工作组”的划分与管理由软件来实现。通过划分虚拟网，可以把广播限制在各个虚拟网的范围内，从而减少整个网络范围内广播包的传输，提高了网络的传输效率；同时各虚拟网之间不能直接进行通讯，而必须通过路由器转发，为高级的安全控制提供了可能，增强了网络的安全性。

VPN(Virtual Private Network，VPN)是指在公用网络上建立专用网络的技术。之所以称为虚拟网主要是因为整个 VPN 网络的任意两个结点之间的连接并没有传统专用网络建设所需的点到点的物理链路，而是架构在公用网络服务商 ISP 所提供的网络平台之上的逻辑网络。用户的数据是通过 ISP 在公共网络(Internet)中建立的逻辑隧道(Tunnel)，即点到点的虚拟专线进行传输的。通过相应的加密和认证技术来保证用户内部网络数据在公网上安全传输，从而真正实现网络数据的专有性。

8.5.5　快照

磁盘“快照”是虚拟机磁盘文件(VMDK)在某个时间点上即时生成的复本。系统崩溃或系统异常时，用户可以通过使用恢复到快照来保持磁盘文件系统和系统存储。当升级应用和服务器及给它们打补丁的时候，运用快照是是一个很好的方法。

如果用户创建了多于一个的虚拟机快照，那么将有多个还原点可以用于恢复。当用户创建了一个快照，那些现在可写的在那个点上就变成了只读的。使用 in-file delta 技术就能创建新文件记录所有的关于原始磁盘文件的变更(delta)。

快照文件的大小不能超过原始磁盘文件的大小。任何时候，一个磁盘块改变了，就将在 delta 文件里创建快照并能随着改变而更新。如果进行一次快照后，用户改变了每个单独的磁盘存储块，这个快照将仍然像原始磁盘文件那么大。快照文件最初很小(16

MB),不过,随着对虚拟磁盘文件的写入将增大。

16 MB 的快照空间用于降低 SCSI 预留冲突。当收到改变原始磁盘上存储块的请求时,它代替在 delta 文件里的改变。如果先前在 delta 文件里更改了的磁盘存储块再次被更改,由于它简单地更新在 delta 文件里现有的存储块,不会增加 delta 文件的大小。

虚拟机一旦创建完毕即可创建快照。通常,快照创建过程只需几秒钟,而且虚拟机不需暂停、停止或关闭。快照是由 Hyper-V 创建、执行的,它完全独立于运行在子分区的子操作系统的类型和性能。快照相关文件会自动储存到 Hyper-V 服务器设置的默认路径下。在 Hyper-V 管理控制台用户可以轻松地创建快照,只需右击虚拟机,选择“创建快照”即可。任何时刻用户都可以创建快照,它会自动嵌入该虚拟机的即时状态浏览树结构中。在快照属性中,可以查看快照的详细信息。快照中储存的设置是只读的,除非将它们应用到现有虚拟机。Hyper-V 快照与文件系统快照不是一回事,例如:微软的 VSS 功能的快照。这两项技术使用了同样的术语,但是 Hyper-V 快照并不依赖于文件系统快照功能。Hyper-V 模式的主要好处是它可以让管理员快速简易地创建改变关系结构、可以返回到任何时刻。而且,它解决了与虚拟机配置相关的潜在问题(例如,如果虚拟网络或内存设置改变),以及 VHD 较多的虚拟机可能存在的问题。

当用户应用快照时,当前的虚拟机配置会被完全覆盖。记住,这包括所有附属 VHD 的内容。因为这个操作是永久性的,所以,最好在应用原来的快照之前先创建一个新快照。以便今后还可以再返回到当前状态。另外,如果虚拟机原来的状态是关闭的,那么虚拟机返回后也会是处于关闭状态。当返回到某一快照时,任何依赖于次快照的其他快照都会被移除,因为它们已经失效。

通常,用户应该在做任何可能有风险的更改之前,为虚拟机创建快照。例如,如果用户要应用 OS 更新或补丁,但又希望可以轻松地撤销它们,那么就在应用之前创建一个快照。同样,当用户想更改虚拟机配置设置或关键的子操作系统服务时,先为虚拟机创建快照。快照并不是在任何情况下都适用。首先,快照不能取代备份。用户仍应该遵循虚拟机备份的最佳做法。只要恰当,一定要利用子操作系统的功能。例如,如果用户要做一个关键的数据库更改,那么从虚拟机内做一个标准的数据库备份。记住,有些类型的应用和服务可能不太适合返回过去状态。当使用微软的 Active Directory 时,需要注意,这个复制的数据库依赖于时间戳(time stamps)和连续变更日志文件,以便保持一致。

8.5.6 物理到虚拟

物理到虚拟,即 Physical to virtual,简称 P2V。它是指将操作系统、应用程序或者数据从计算机的物理硬盘中迁移到一个虚拟环境中或是磁盘分区中。

P2V 可以手工创建或定义一个虚拟环境,并在此环境中安装操作系统、应用程序或者数据。这可能会是一个冗长或不确定的过程,尤其是在一个包含大量旧的硬件条件的新环境中。为了简化操作,会有一些支持全部或者部分虚拟化的自动软件工具,也就是我们所熟识的迁移工具,通常 P2V 就是创建虚拟的应用服务器环境。

物理到虚拟的具体步骤:

(1)制作镜像:通过镜像制作工具将物理机的系统整体制作成物理机的镜像。

(2)选择驱动:替换掉镜像中与特定硬件设备相关的驱动程序或者磁盘驱动器,并且保证镜像中新的驱动程序和其他驱动程序在系统初始化时有序启动,已使镜像能够在虚拟环境中运行。

(3)定制配置:用户手动输入必要的参数,例如虚拟机的 CPU、内存、MAC 地址等。

8.5.7　虚拟到物理

虚拟机到物理机的迁移是指把一个操作系统、应用程序和数据从一个虚拟机中迁移到物理机的主硬盘上,它可以同时迁移虚拟机系统到一台或多台物理机上。尽管虚拟化的基本需求是整合物理机到虚拟机中,但这并不是虚拟化的唯一的应用。比如有时虚拟机上的应用程序的问题需要在物理机上验证,以排除虚拟环境带来的影响。另外,配置新的工作站是件令 IT 管理者头痛的事情,但虚拟化的应用可以帮助他解决这个难题。先配置好虚拟机,然后运用硬盘克隆工具复制数据至工作站硬件,不过这种克隆方法有两个局限:一个镜像只能运用在同种硬件配置的机器上;要想保存配置的修改,只能重做新的镜像。

8.5.8　了解 Active Directory

活动目录(Active Directory)是面向 Windows Standard Server、Windows Enterprise Server 以及 Windows Datacenter Server 的目录服务。活动目录服务是 Windows Server 操作系统平台的中心组件之一。理解活动目录对于理解 Windows Server 的整体价值是非常重要的。活动目录服务在一个目录内提供存储、组织和获取信息。目录服务是用于定位、管理和组织共同项目和网络资源,例如:存储区、文件夹、资料、打印机、使用者、群组、设备和电话号码等。

Active Directory 一个微软创建的技术,它提供了各种网络服务,包括以下内容:

(1)LDAP;

(2)基于 Kerberos 的单一登录认证;

(3)基于 DNS 的命名和其他网络资源;

(4)一个提供网络管理和权限下放的中央位置。

轻量级目录存取协议(LDAP),是一种应用程序协议,使用在 TCP/IP 上执行的目录服务协议以提供资料查询和修改。在目录内,项目集合是一个合乎逻辑的分层方式的组织,以便用户可以轻松地查询和管理。该结构能反应地域与组织的界限,倾向于使用 DNS 名称的层次结构。在更深层的目录内,项目有人员名称、组织单位、群组或者其他任何一个指定的树状目录。LDAP 使用 TCP 389 端口。

Kerberos 是计算机网络认证协议,它允许主机在不安全的网络中以一种安全的方式证明自己的身份。它也可以提供相互验证,使服务器与用户互相验证对方的身份。处于安全原因,Kerberos 协议的信息是被安全的保护的,以防止窃听和攻击。

单一登录允许登录一次去存取多个相关但独立的软件系统,而无需再次登录。当用户登录使用 Active Directory 的 Windows,用户将被分配一个存取权限,然后可以用于自动登录到其他系统。

Active Directory 允许用户组织所有的网络资源，包括使用者、群组、打印机和计算机等，以便在网络上将指定密码、权限和授权给使用者。用户也可以指定某个人可以管理一组项目。

8.6 了解账户和组

本节将全面讲解 Windows 系统中所使用的用户账户和用户组的相关概念，用户和用户组是 Windows 用户管理中的基本概念。

8.6.1 本地账户与域账户

使用者账户使得使用者能够登录到计算机和 AD 域中。因此，它可以用来证明身份，这个身份信息可以被用于确定哪些使用者可以存取以及拥有什么样的权限。它也可以用于审核，因此如果发生任何安全问题，其中一些文件被存取或者删除，执行存取或者删除的人可以被确认。

在今天的 Windows 网络中，有两种类型的使用账户：

(1)本地账户；

(2)域账户。

使用者账户允许使用者登录并存取计算机上的资源。本地使用者账户存储在本地计算机上的安全账户管理器(SAM)资料库中。唯一没有 SAM 资料库的 Windows 计算机是域控制器。Administrator 是本地使用者账户，同时建立和预设在 Windows 中。虽然这个账户不能被删除，但是可以被重新命名。

在预设情况下的另一个账户是 Guest 账号，这个账号默认情况下是不启用，是专门为低安全网络下需要偶尔存取网络资源的使用者。

域用户账户的访问权掌管于域控制器内，假设用户已经被授予来存取项目，就会允许用户存取域中的资源。域管理员账户是唯一的账户，当用户第一次建立一个域时，在 Windows 默认情况下会被建立并且启用。虽然域管理员使用者账户不能被删除，但是可以被重命名。

当建立一个域管理员使用者账户时，必须提供一个名字、姓氏和登录名。用户登录名在域中必须是唯一的。用户账户建立后，可以打开账户属性和设定名称、登录时间、电话号码和地址等。用户还可以指定密码是否过期，是否可以更改密码，该账户是否被停用。最后，在设定选项卡中，用户可以定义账户的主目录、登录脚本和设定文件路径等与账户有关系的账户设定。

8.6.2 用户配置文件

用户配置文件是一个文件夹和文件的集合，用来存储账户当前桌面环境和应用程序设定。账户设定还记录了网络连接，所以当账户登录到计算机时，它会将记录映射到公用文件夹。因此当账户登录到特定的计算机时会获取与以前登录过的计算机上相同的桌面

环境。

账户配置文件包括三种：

(1)本地账户配置文件：这种类型的配置文件是存储在账户登录的计算机的本地磁盘驱动器内。如果用户登录到另一台计算机将会得到该计算机的设置。

(2)漫游账户配置文件：这种类型的配置文件是建立并存储在网络中的服务器上的公共文件夹中。不管任何种类的计算机账户登录到网络域中都会获得相同的设置。

(3)强制账户配置文件：这种类型的配置文件被用作漫游账户配置文件，因为它的设置可以改变。当账户再次登录时，所有设置会被重置回预设定的值。

8.6.3　组类型

一个群组是一个用户账户或者计算机账户的集合或者列表。与容器不同，群组只是个列表不存储账户或者计算机信息，利用群组可以在分配权力和权限时简化管理。群组用于将账户和计算机连接到一起，这样当用户分配权力和权限时可以将它们分配给整个组而不是单独分配给一个账户。账户和计算机可以是多个群组的成员，而且在某些情况下，一个群组可以被指定分配到另一个群组。

在 Windows Active Directory 中设有两种类型的群组：安全组和通讯组。一个安全组用于分配存取网络资源的权力和权限，它可以被用来作为一个通讯组。通讯组仅用于非安全性功能，例如：电子邮件。但不能用于分配权力和权限。

8.6.4　组范围

任何群组无论是安全组还是通讯组均具有范围的特性，此范围用来确定群组在网络域树状目录中使用的程度。

组作用域组(无论是安全组还是通讯组)都有一个作用域，用来确定在域树或林中该组的应用范围。有三类不同的组作用域：

(1)通用组：包括域树或林中任何域中的其他组和账户，而且可在该域树或林中的任何域中指派权限。

(2)全局组：包括只在其中定义该组的域中的其他组和账户，而且可在林中的任何域中指派权限。

(3)本地域组：包括来自多个网络域的通用组，其中有通用组、其他本地域组和计算机账户。由于通用类别目录复制本地域组中的成员，用户应该限制通用组的成员身份。这样，如果用户在通用组内更改成员，通用类别和目录将不必复制更改。

具有本地域的组将帮助用户定义和管理对单个域内资源的访问，例如：要使五个用户访问特定的打印机，可在打印机权限列表中添加全部五个用户。如果以后希望这五个用户都能访问新的打印机，则需要再次在新打印机的权限列表中指定全部五个账户。如果采用简单的规划，可通过创建具有本地域作用域的组并指派给其访问打印机的权限来简化常规的管理任务。将五个用户账户放在具有全局作用域的组中，并且将该组添加到有本地域作用的组。当希望使五个用户访问新打印机时，可将访问新打印机的权限指派给有本地域作用的组。具有全局作用域的组的成员自动接受对新打印机的访问。

使用具有全局作用域的组管理那些需要每天维护的目录对象，如用户和计算机账户。因为有全局作用域的组不在自身的域之外复制，所以具有全局作用域的组中的账户可以频繁更改，而不需要对全局编录进行复制以免增加额外通信量。虽然权利和权限指派只在指派它们的域内有效，但是通过在相应的域中统一应用具有全局作用域的组，可以合并对具有类似用途的账户的引用。这将简化不同域之间的管理，并使之更加合理化。

使用具有通用作用域的组来合并跨越不同域的组。为此，请将账户添加到具有全局作用域的组并且将这些组嵌套在具有通用作用域的组内。使用该策略，对具有全局作用域的组中的任何成员身份的更改都不影响具有通用作用域的组。具有通用作用域的组成员身份不应频繁更改，因为对这些组成员身份的任何更改都将引起整个组的成员身份复制到树林中的每个全局编录中。

8.6.5 组嵌套

组嵌套是授权组成员资格管理的一种有效途径。在本地模式下，可以创建一个通用组，然后把成员资格控制权授权给企业或者从事全局组成员资格管理工作的高级管理员。通用组管理成员有职责管理组成员资格，以及授权用户或者本地组的成员资格。

域必须在原始模式下嵌套安全组。在混合模式下通用组是不可用的。

8.6.6 AGDLP

A 表示用户账号，G 表示全局组，U 表示通用组，DL 表示域本地组，P 表示资源权限。A-G-DL-P 策略是将用户账号添加到全局组中，将全局组添加到域本地组中，然后为域本地组分配资源权限。

AGDLP 是基于角色的访问控制（RBAC），它能简化常规账户管理操作，并促进安全审计。系统管理员不需要直接向个人用户账户分配权限。相反，个人获得通过其角色内一个组织，消除了需要编辑可能很大的资源权限和用户权限分配时创建、修改或删除用户账户的访问权限。与传统的访问控制列表不同，RBAC 权限描述在一个特定的应用程序或系统而不是基础的低级数据对象的访问方法的范围内有意义的操作。确定和控制角色成员资格和角色的权限的过程简化了存储的集中式的数据库或目录服务中的角色和权限。审计可以无需一种特定的访问控制资源特定的实现细节，从而分析单个位置的分配权限。

假设，有两个域，A 和 B，A 中的 5 个财务人员和 B 中的 3 个财务人员都需要访问 B 中的“FINA”文件夹，这时，用户可以在 B 中建一个 DL，因为 DL 的成员可以来自所有的域，然后把这 8 个人都加入这个 DL，并把 FINA 的访问权赋给 DL。因为 DL 是在 B 域中，所以管理权也在 B 域，如果 A 域中的 5 个人变成 6 个人，那只能 A 域管理员通知 B 域管理员，将 DL 的成员做一下修改，B 域的管理员的工作量会很大。

所以如果需要减少管理员的工作量，需要改变一下，在 A 和 B 域中都各建立一个全局组(G)，然后在 B 域中建立一个 DL，把这两个 G 都加入 B 域中的 DL 中，然后把 FINA 的访问权赋给 DL。这下两个 G 组都有权访问 FINA 文件夹了，原因是组嵌套造成权限继承。这时候，两个 G 分布在 A 和 B 域中，也就是 A 和 B 的管理员都可以自己管理自己

的 G，只要把那 5 个人和 3 个人加入 G 中，就可以了。以后有任何修改，都可以自己做了，这样 B 域的管理员工作量就减少了。

对于多个拥有相同权限的用户，只需将其添加到组中并给组授权就行了。或许每个网络管理员都有自己独特的方法达到该目的，但微软推荐的 AGDLP 方案已经被无数成功的实践证明了它是一种最有效率的途径。不论单域还是多域，充分的运用 G 组和 DL 组进行合理的用户添加、嵌套与权限的分配，就能解决日常的 IT 管理工作。具体方法是：先将用户（Acounts-A）加入全局组 G；再将 G 加入域本地组 DL；最后给 DL 授权（Permissions-P）。

DC 安装时默认 U 组不可用，其选项为灰色，这时该 DC 的域处于混合模式（MIX），表示当前域内可能还有基于 WIN-NT 操作系统的域控制器在使用，如果域内已没有基于 WIN-NT 操作系统的域，并且森林内有多域共存时就可将 DC 转换到本机模式，U 组才能使用。这样做是为了保持操作系统版本的兼容性，即使是在有了 WINDOWS 2008 的今天，全世界还有很多大中型企业的网络平稳地运行在 WIN-NT 的平台上。当 U 组可用时，已建的 G 组和 DL 组可以有条件的转换为 U 组，根据上述规则，G 组转换为 U 组的前提是该 G 组不是另一个 G 组的成员；与此相反，把 DL 组转换成 U 组的前提是该 DL 组内没有另一个 DL 组作为它的成员。U 组既然通用，可以把用户都加入到 U 组。多域环境称为森林，为保持各个域之间的用户信息共享，U 组和它的全部成员都被写入了一个名为全局目录（Global Caltalog，GC）的数据库中，保存于森林内第一台域控制器之中，该 GC 会在森林内各个域的 DC 之间进行复制，虽然 G 组和 DL 组也被写入了 GC，但只有组名，没有成员。由此可见，如果把所有成员都加入到 U 组的话，会使得 GC 在森林内进行域间复制时的网络流量剧增，造成网速下降；而通过建立适当的 G 组和 DL 组，并且在 U 组内避免直接添加用户，就能够显著减小 GC 容量的大小，从而降低 GC 复制时带来的网络流量。U 组的策略称为 AGUDLP 策略。通过 U 组可以使 AGDLP 的应用能力升级到可以适合大型跨国公司的域用户权限的管理，解决任意复杂的多域环境中域内用户和资源的分配、管理问题。虽然可以对每个用户 A 单独授权，但通常是将用户 A 添加到 G 组，必要时才将 G 组添加到 U 组，再将 G 组或 U 组添加到 DL 组，最后对 DL 组授权（P）。这就是 AGDLP 策略。表面上，它只是一种技术，在将网络权限分配的机动性、灵活性最大化的同时，使其复杂性最小化，但实质上，它除了是 ALP 策略的扩展以外，更是微软的管理思想的体现，DL 本身不能加入到任何组，只能用来分配资源权限，称为资源组；G 组和 U 组用来添加那些有相同资源需求的用户账户组，称为账户组。早在 NT 域模式下要分别建立账户域和资源域的时候，这种管理思想就已经初见端倪了。

8.7　了解组织单位和容器

组织单位和容器是 Active Directory 中管理用户的单元，很多组织机构都采用 Active Directory 来管理本组织内的用户，因此，组织单位和容器是组织和管理用户的重要手段。

8.7.1 组织单位

组织单位(Organizational Unit,OU),是可以将用户、组、计算机和其他组织单位放入其中的 AD(Active Directory,活动目录)容器,是可以指派组策略设置或委派管理权限的最小作用域或单元。

一个组织可能有成千上万的使用者和数以千计的计算机。如果使用 Windows NT,在遇到一些性能问题时,一个域只能处理有限数量的单位。后来版本的 Windows 中,域的大小增加了很多。虽然使用 Windows NT 用户有可能需要多个域来定义组织,但是用户现在可以使一个域代表一个大的组织。然而,用户仍然需要一种方法来组织和管理网域内的单位。

为了帮助在一个域中组织对象,和减少用户需要的域数目,用户可以使用组织单位,俗称 OU。组织单位可用于保存账户、群组、电脑和其他组织单位。组织单位只能包含位域内的对象。虽然没有限制用户能拥有多少 OU,但是用户要设计一个层次结构来获得更好的效能。

包含在域中特别有用的目录对象类型就是组织单元。组织单元是将用户、组、计算机和其他单元放入活动目录的容器中,组织单元不能包括来自其他域的对象。组织单元是可以指派组策略设置或委派管理权限的最小作用单位。使用组织单元,用户可在组织单元中代表逻辑层次结构的域中创建容器,这样用户就可以根据用户的组织模型管理账户、资源的配置和使用,可使用组织单元创建可缩放到任意规模的管理模型。可授予用户对域中所有组织单元或对单个组织单元的管理权限,组织单元的管理员不需要具有域中任何其他组织单元的管理权。

当首次安装 Active Directory 时,有几个组织单元已经内建。它们包括计算机、使用者、域控制器和内建的 OU,这些组织单元不允许用户委派权限或分配群组原则。

假设用户有实体位置的域名。用户可以指定网络管理员的权限来管理 OU,以便用户管理控制 OU 内的单位。用户还可以按功能和管理区域构建 OU。例如:可以建立一个销售 OU 容纳所有的销售部的员工。可以建立一个打印类型 OU 来容纳所有的打印机单位,并指定打印机管理员。

如果把 AD 比作一个公司的话,那么每个 OU 就是一个相对独立的部门。创建组织单位 OU 的创建需要在域控制器中进行,创建步骤如下:

(1)以系统管理员身份登录域控制器。然后依次单击“开始”|“管理工具”|“Active Directory 用户和计算机”菜单,打开“Active Directory 用户和计算机”控制台窗口。

(2)在左窗格中鼠标右键单击域名,并在弹出的快捷菜单中单击“新建”|“Organizational Unit”命令。

(3)打开“Organizational Unit”对话框,在“名称”编辑框中输入新的 OU 的名称,单击“确定”按钮,组织单位的设计是为了有效的组织活动目录对象,OU 根据公司业务模式的不同来创建不同的 OU 层次结构。

若要删除组织单位,可以执行如下操作步骤:

(1)使用 Windows 界面打开“Active Directory 用户和计算机”。

(2)在控制台树中,鼠标右键单击要删除的组织单位。

(3)单击“删除”。

要执行此过程,必须是 Active Directory 中 Domain Admins 组或 Enterprise Admins 组的成员,或者用户必须被委派了适当的权限。作为最安全的操作,请考虑使用“运行方式”执行此过程。

如果选定的组织单位包含其他对象,“Active Directory 用户和计算机”将提示继续或取消删除。如果继续删除,则该组织单位中的所有单元也会被删除。

使用命令行删除组织单位:

(1)打开“命令提示符”。

(2)键入:dsrmOrganizationalUnitDN,OrganizationalUnitDN 用于指定要删除的组织单位的可分辨名称。

若要打开命令提示符,请单击“开始”,依次指向“所有程序”、“附件”,然后单击“命令提示符”。

试图删除包含其他对象的组织单位将导致出错,除非使用-subtree 选项。使用-subtree 选项时,dsrm 将同时删除选定的组织单位和它所包含的任何对象。

要查看该命令的完整语法,请在命令提示符下键入:dsrm /?

以下是几种常见的设计方法:

(1)基于部门的组织单位为了和公司的组织结构相同。OU 可以基于公司内部的各种各样的业务功能部门创建,例如:行政部、人事部、工程部和财务部等。

(2)基于地理位置的组织单位可以为每一个地理位置创建 OU,例如:北京、上海和广州等。

(3)基于对象类型的组织单位在活动目录中可以将各种对象分类,为每一类对象建立 OU,例如:根据用户、计算机、打印机和共享文件夹等。同时在单域结构里一个 OU 下还可以创建子 OU,权限也继承于其父项 OU。例如:在父 OU 下设置屏蔽“搜索”,子 OU 下设置屏蔽“运行”,则子 OU 的用户“运行”和“搜索”都被屏蔽了。

8.7.2　容器

容器是一个可以储存或持有其他单位的单位。它们包括树系、树状目录、域和组织单位。为了帮助管理用户的单位,可以把权力下放到一个容器,特别是域或组织单位。

每个 Active Directory 域包含一组标准的容器和组织单位 (OU),是在安装 Active Directory 域服务(AD DS)期间创建的。包括以下内容:

- 域控制器:它作为层次结构的根容器。
- 内置容器:它包含默认服务管理员账户。
- 用户容器:它是在域中创建的新用户账户和组的默认位置。
- 计算机容器:它是在域中创建的新计算机账户的默认位置。
- 域控制器容器:它是域控制器计算机账户的计算机账户的默认位置。

容器也是活动目录名字空间的一部分,与目录对象一样,它也有属性,但与目录对象不同的是,它不代表有形的实体,而是代表存放对象的空间,因为它仅代表存放一个对象

的空间,所以它比名字空间小。例如:用户和对象。但这个对象的容器就仅限于从这个对象本身所能提供的信息空间,它只能提供用户名、用户密码。其他的信息有工作单位、联系电话、家庭住址等就不属于这个对象的容器范围了。

AD 中 users 容器下的各个组介绍:

- cert publishers:成员获准为用户和计算机发行证书。
- DnsAdmin:成员具有对 dns server 服务的管理访问权。
- DnsUpdateProxy:成员是可以代表其他客户端执行动态更新的 dns 客户端。
- Domain Admins:成员具有对该域的完全控制权。
- Domain computers:包含加入到此域的所有工作站和服务器。
- Domain controllers:包含此域中的所有域控制器。
- Domain Guest :包含所有域来宾。
- Domain users:包含所有域用户。
- Enterprise Admins:成员具有对林中所有的域的完全控制作用。
- Group Policy Creator Owners:成员可以修改此域中的组策略。
- ras 和 ias servers:该组中的服务器可以访问用户的远程访问信息。
- schema admins:成员可以修改 AD 中的架构。

8.7.3 委派

通过委派管理,用户可以指定一个范围的管理任务给适当的用户和群组。例如:用户可以分配基本的管理任务给普通使用者或者群组,并留下域范围和树系范围的管理任务给 domain admins 和 enterprise admins 群组的成员。通过委派管理,用户可以允许在组织内的群组控制更多在本地网络的资源。用户还可以通过限制管理员组的成员以帮助保护网络避免遭受意外或者恶意的破坏。

用户可以通过建立域组织来委托管理控制到任何等级的域树状目录和委派特定的使用者或群组去管理控制特定的组织单位。

执行委派控制需要执行以下操作:

(1)打开 Active Directory 账户和计算机。

(2)在控制台树状结构目录中,鼠标右键单击需要委派控制的组织单位。

(3)单击“委派控制来启动委派控制功能”,然后按照说明操作。

执行从 Windows Server 2003 到 Windows Server 2008 的正确域升级时,会自动将现有用户和计算机放置到用户和计算机容器中。如果创建的是新的 Active Directory 域,则用户和计算机容器是该域中所有新用户账户和非域控制器计算机账户的默认位置。

如果需要委派对用户或计算机的控制权限,则不要修改用户和计算机容器上的默认设置,而是创建新的 OU 并将用户和计算机对象从其默认容器移动到新的 OU 中。根据需要委派对新 OU 的控制权限。建议不要修改控制默认容器。

对默认的用户和计算机容器应用组策略设置。若要对用户和计算机应用组策略,请创建新的 OU 并将用户和计算机对象移动到这些 OU 中。对新的 OU 应用组策略设置。或者,也可以重定向放置在默认容器中的对象的创建以放置在用户选择的容器中。

可以使用组织单位将对象的管理委派给指定的个人或组。若要使用 OU 委派管理，请将要委派管理权限的个人或组放置到某个组中，将要控制的对象集放置在 OU 中，然后将 OU 的管理任务委派给该组。

使用 Active Directory 域服务，可以以非常详细的级别控制可以委派的管理任务。例如：可以将一个组指定为具有对 OU 中所有对象的完全控制权限；将另一组指定为仅具有在 OU 中创建、删除和管理用户账户的权限；然后将第三个组指定为仅具有重置用户账户密码的权限。可以使这些权限成为可继承的权限，以便它们应用于放置在原始 OU 的子树中的任何 OU。

在安装 ADDS 期间创建的默认 OU 和容器由服务管理员控制。最理想的情况是服务管理员继续控制这些容器。如果需要委派对目录中对象的控制，可创建其他 OU 并将对象放置在这些 OU 中。将对这些 OU 的控制委派给适当的数据管理员。这样便可以委派对目录中对象的控制，而无需更改指定给服务管理员的默认控制。

林所有者确定委派给 OU 所有者的授权级别。范围从在 OU 中创建和操纵对象的能力到只获准控制 OU 中一种类型对象的一个属性的能力。授予用户在 OU 中创建对象的能力即隐式授予该用户操纵该用户创建的任何对象的任何属性的能力。此外，如果创建的对象是容器，则该用户隐式具有创建和操纵放置在该容器中的任何对象的能力。

用于在 OU 结构中委派控制的组类型基于账户所在的与要管理的 OU 结构相对的位置。如果管理用户账户和 OU 结构全都位于一个域中，则创建用来委派的组必须是全局组。如果组织拥有一个管理其自己的用户账户的部门并且多个地区存在该部门，则用户可能拥有一个负责管理位于多个域中的账户 OU 的数据管理员组。如果数据管理员的账户全都位于一个域中并且在多个域中拥有要向其委派控制的 OU 结构，则可使这些管理账户成为全局组的成员，并且将对每个域中的 OU 结构的控制委派给这些全局组。如果要向其委派对 OU 结构的控制的数据管理员账户来自多个域，则必须使用通用组。通用组可以包含来自不同域的用户，因此可以用来在多个域中委派控制。

使用 Windows 界面移动组织单位步骤如下：

(1)若要打开 Active Directory 用户和计算机，请依次单击“开始”和“控制面板”，然后依次双击“管理工具”和“Active Directory 用户和计算机”。要在 Windows Server 2012 中打开“Active Directory 用户和计算机”，请单击“开始”，键入“dsa.msc”。

(2)在控制台树中，右键单击要移动的组织单位 (OU)。位置：Active Directory 用户和计算机\domain node\organizational unit。

(3)单击“移动”，然后单击要将 OU 移动到的文件夹。

还可以通过使用 Windows PowerShell 的 Active Directory 模块执行此过程中的任务。若要打开 Active Directory 模块，请依次单击“开始”、“管理工具”和 Windows PowerShell 的 Active Directory 模块。

要在 Windows Server 2012 中打开 Active Directory 模块，请打开“服务器管理器”，依次单击“工具”和 Windows PowerShell 的 Active Directory 模块。

8.7.4 默认设置

向域中添加域控制器时,它们的计算机对象会自动添加到域控制器 OU 中。此 OU 具有一组默认策略。若要确保将这些策略统一应用于所有域控制器,建议用户不要将域控制器的计算机对象移出此 OU。应用默认策略失败可能会导致域控制器无法正常工作。

默认情况下,服务管理员控制此 OU。不要将对此 OU 的控制委派给除了服务管理员之外的个人。

默认组例如 Domain Admins 组,是创建 Active Directory 域时自动创建的安全组。使用这些预定义的组可以帮助控制对共享资源的访问,并委派特定域范围的管理角色。

许多默认组被自动指派一组用户权限,授权组中的成员执行域中的特定操作,如登录到本地系统或备份文件和文件夹。例如:Backup Operators 组的成员有权对域中的所有域控制器执行备份操作。

当将用户添加到组中时,用户将接受指派给该组的所有用户权限以及指派给该组的有关任何共享资源的所有权限。

可以通过使用 Active Directory 用户和计算机来管理组。默认组位于“Builtin”容器和“Users”容器中。“Builtin”容器包含用本地域作用域定义的组。“Users”容器包含通过全局作用域定义的组和通过本地域作用域定义的组。可将这些容器中的组移到域中的其他组或组织单位,但不能将它们移到其他域。

8.8 了解 Active Directory 基础结构

Active Directory 是微软 Windows Server 中负责架构大中型网络环境的集成式目录管理服务(Directory Services),自 Windows 2000 Server 以来,就已内置于 Windows Server 产品,主要负责处理组织中的各种网络对象,例如用户、组、计算机、域控制器、邮件、组织单位和域等,只要是在 Active Directory 结构架构中定义的对象,就可以储存在 Active Directory 数据库中,并利用 Active Directory Service Interface 来访问。

本节将介绍 Active Directory 的一些构成要素,通过掌握这些基本构成要素,用户将具备坚实的相关知识。

8.8.1 域控制器

“域”的真正含义指的是服务器控制网络上的计算机能否加入的计算机组合。组合需要严格的控制,所以实行严格的管理对网络安全是非常必要的。

虽然域、树状目录和树系是组织的逻辑表示法,网站和域控制器则代表网络的实体结构。

一个网站(Site)包含一个高速连接一个或多个 IP 子网,通常由地理位置来定义。例如,假设有一座四层办公楼,虽然包括若干子网,但是所有建筑物内的电脑均使用第二层

和三层交换机来相互通信。如果有多个网站，每个网站连接到其他网站，均利用一个很慢的 WAN 连接，至少慢于区域网的速度。然后，可以依据网站定义的方式来定义各种不同的网络通信模式。

当用户登录时，Active Directory 客户端会找到一个 Active Directory 服务器，被称为在同一网站的域控制器。每个域都自己的一套域控制器来提供域资源的存取，例如：账户和计算机。

对于容错而言，一个网站应该有两个或多个域控制器。这样，如果一个网域控制站出现故障，其他网域控制站仍然可以服务客户。

注意：每当一个对象的用户名或密码被修改，会自动被复制到其他网域控制站中。

域控制站是 Windows 服务器，用来存储账户和安全资讯的副本，并定义域边界。为了使计算机执行 Windows Server 2008 域控制器，必须安装 Active Directory 域服务和执行 DC promotion 指令。

当用户提升计算机到域控制器，可以使用多种 MMC 管理单元的控制台来管理 Active Directory。这些控制台如下：

• Active Directory 用户和计算机：用于管理账户、群组、计算机和组织单位。

• Active Directory 域和新用户关系：用于管理域信任关系，域和树系功能级别，用户主要名称(UPN)尾码。

• Active Directory 网站和服务：用户管理 Active Directory Domain Services(AD DS)树系中所有网站目录资料的副本。

• Active Directory 管理中心：用于管理和发布目录的咨询，包括管理账户、群组、计算机、域、域控制器和组织单位。在 Windows Server 2008 R2 中 Active Directory 管理中心是属于新的功能。

• 群组原则管理控制台(GPMC)：在整个企业中提供一个单一的管理群组原则的执行手段。GPMC 是自动安装在 Windows Server 2008 域控制器和随后的控制器，但必须下载并安装在 Windows Server 2003 域控制器。

尽管这些工具被安装在域控制器，它们也可以安装在客户端计算机，让用户可以管理 Active Directory，即使没有登录到域控制器。

一个服务器没有执行作为域控制器被称为成员服务器。域控制器降级为成员服务器，用户会重新执行 Dcpromo 程序。

在对等网模式下，任何一台计算机只要接入网络，其他机器就都可以访问共享资源，例如：共享上网等。尽管对等网络上的共享文件可以加访问密码，但是非常容易被破解。在由 Windows 9x 构成的对等网中，数据的传输是非常不安全的。

在“域”模式下，至少有一台服务器负责每一台连入网络的计算机和用户的验证工作，相当于一个单位的门卫一样，称为域控制器(Domain Controller，DC)。

域控制器中包含了由这个域的账户、密码、属于这个域的计算机等信息构成的数据库。当计算机连入网络时，域控制器首先要鉴别这台计算机是否是属于这个域的，用户使用的登录账号是否存在、密码是否正确。如果以上信息有一样不正确，那么域控制器就会拒绝这个用户从这台电脑登录。不能登录，用户就不能访问服务器上有权限保护的资源，

只能以对等网用户的方式访问 Windows 共享出来的资源，这样就在一定程度上保护了网络上的资源。

要把一台计算机加入域，使它和服务器在网上邻居中能够相互可见是不够的，必须要由网络管理员进行相应的设置，把这台计算机加入到域中，这样才能实现文件的共享。

在服务器端以系统管理员身份在已经设置好 Active Directory（活动目录）的 Windows Server 上登录，选择“开始”菜单中“程序”选项中的“管理工具”，然后再选择“Active Directory 用户和计算机”，之后在程序界面中鼠标右键单击“Computers”，在弹出的菜单中单击“新建”，然后选择“计算机”，之后填入想要加入域的计算机名即可。要加入域的计算机名最好为英文。

在客户端首先要确认计算机名称是否正确，然后在桌面“网上邻居”上鼠标右键单击“属性”出现网络属性设置窗口，确认“主网络登录”为“Microsoft 网络用户”。选中窗口上方的“Microsoft 网络用户”，如果没有此项，说明没有安装，单击“添加”安装“Microsoft 网络用户”选项。单击“属性”按钮，出现“Microsoft 网络用户属性”对话框，选中“登录到 Windows NT 域”复选框，在“Windows NT 域”中输入要登录的域名。这里的域用户账号和密码，必须是网络管理员为用户建的那个账号和密码，而不是由本机用户自己创建的账号和密码。如果没有将计算机加入到域中，或者登录的域名、用户名、密码有一项不正确，都会出现错误信息。

只读域控制器是一种新型的用于 Windows Server 2008 操作系统的域控制器，它的安全性得到了提高，同时能够更加快速的登录访问网络资源。在 Windows Server 2008 操作系统中，为了能够支持只读域控制器，在域名解析系统中添加了新的活动目录域密码复制策略。而为了部署只读域控制器，在 Windows Server 2008 操作系统中必须至少运行一个可写域控制器。域的功能及和森林应该是 Windows Server 2003 系统中或其他更高系统中的单向复制，只读 AD DS 数据库，凭据缓存，管理员角色分隔等只读域控制器的功能。

8.8.2 林与树

域林是指由一个或多个没有形成连续名字空间的域树组成，它与域树最明显的区别就在于域林之间没有形成连续的名字空间，而域树则是由一些具有连续名字空间的域组成的。但域林中的所有域树仍共享同一个表结构、配置和全局目录。域林中的所有域树通过 Kerberos 信任关系建立起来，所以每个域树都知道 Kerberos 信任关系，不同域树可以交叉引用其他域树中的对象。域林都有根域，域林的根域是域林中创建的第一个域，域林中所有域树的根域与域林的根域建立可传递的信任关系。例如：benet. com. cn 可以创建同属于一个林的 accp. com. cn，这两个域之间就在同一个域林里。

当创建第一个域控制器的时候，创建的第一个域，也称林根域或第一个林。林，是一个或多个共享公共架构和全局编录的域组成，每个域都有单独的安全策略和与其他域的信任关系。一个单位可以有多个林。

域树由多个域组成，这些域共享同一个表结构和配置，形成一个连续的名字空间。树中的域通过信任关系连接起来，“活动目录”包含一个或多个域树。域树中的域层次越深

级别越低，一个“.”代表一个层次。如域“child. Microsoft. com”就比“Microsoft. com”这个域级别低，因为前者有两个层次关系，而后者只有一个层次。域树中的域是通过双向可传递信任关系连接在一起的，因此在域树或树林中新创建的域可以立即与域树或树林中每个其他的域建立信任关系。这些信任关系允许单一的登录过程，在域树或树林中的所有域上对用户进行身份验证，但这不一定意味着经过身份验证的用户在域树的所有域中都拥有相同的权利和权限。因为域是安全界限，所以必须在每个域的基础上为用户指派相应的权利和权限。

目录林是活动目录的主要组件之一。它是活动目录域的集合。目录林有两个主要作用：简化用户对目录的管理和简化用户与目录的交互过程。活动目录还具有以下主要特征：单一配置容器(Single Configuration Container)、架构(Scheme)、信任(Trust)、全局编录(Global Catalog)配置容器提供目录林的所有域控制器的复制，配置容器中存储属于目录林的与目录相关的应用程序的信息。活动目录架构定义对象类别和这些对象的属性。对象类别定义可以在目录中创建的对象的类型。架构可复制到目录林中的每个域控制器。活动目录自动在目录林和域之间创建双向的可传递信任关系。来自任何其他信任域的组或用户都能看到这种信任关系。全局编录包含目录林中每个域的每个对象，但只包含每个对象的一个属性子集，为了在整个目录林内进行快速、高效的搜索。全局编录把目录林中的目录结构完全展现给最终用户。

开始规划目录林模式时，建议首先配置单一目录林。在很多情况下，单一目录林就足够了。如果决定要创建其他的目录林，必须具备合理的原因。如果只建立了单一目录林，则所有的用户都通过全局编录看到单一的目录，这样的目录结构是很清楚的。信任关系是自动建立的，配置更改只需应用一次，然后可以被传播到所有的目录林。

如果网络管理分布在多个自治部分之间，则有必要创建多个目录林。不过要切记，每增加一个目录林，就要增加相应的成本，每个目录林必须有至少一个域，增加域同样会增加成本。

目录林用户可以通过目录林全局编录查找到所要访问的位于目录林资源，由于它们之间具有单向信任关系，可以进行直接访问。

在确定目录林数目时，请记住用户的需求永远是位于第一位的，而不要考虑对管理员的影响。不要因为解决管理问题而采取建立多个目录林的方法，这样从用户的角度来看，可能会破坏单一的目录视图。当然在有些情况下，这种单一目录视图对用户并不重要，这时建立多个目录林是可以接受的。

所建的每个目录林都应当有相应的目录林更改控制策略(Forest Change Control Policy)。它是目录林规划文档的一部分，将用其指导会对整个目录林产生影响的更改。用户无需在执行之前确定各个过程，但了解其所属关系是重要的。目录林更改控制策略应包括目录林中每个共享元素的相关信息。

建立或监控架构更改策略(Schema Change Policy)同样很重要。架构更改策略应包括：控制架构管理的小组名称、小组的成员数和架构更改的规则，最后还要设计配置更改策略。除了包括与架构更改策略相同的策略外，还增加了在目录林中建立新域或更改域、修改拓扑结构的规则。

8.8.3 操作主机角色

Active Directory 支持域中所有域控制器之间的目录数据存储的多主机复制，因此域中的所有域控制器实质上都是对等的。但是，某些更改不适合使用多主机复制执行，因此对于每一个此类更改，都有一个称为“操作主机”的域控制器接收此类更改的请求。

在每个林中，可为一台或多台域控制器指派操作主机角色。在每个林中，林范围的操作主机角色必须只出现一次。在林中的每个域中，域范围的操作主机角色必须在每个域中出现一次。操作主机角色有时称为灵活的单主机操作（FSMO）角色。

每个林必须具有以下角色：

• 架构主机：架构主域控制器控制对架构的全部更新和修改。要更新林的架构，用户必须具备访问架构主机的权限。在整个林中，只能有一个架构主机。

• 域命名主机：担当域命名主机角色的域控制器控制树林中域的添加或删除。在整个林中只能有一个域命名主机。在林中这些角色必须是唯一的。这意味着在整个林中，只能有一个架构主机和一个域命名主机。

• 架构主机：任何运行 Windows Server 2003 的域控制器都可以担当域命名主机这一角色。担当域命名主机角色而且运行 Windows 2000 Server 的域控制器还必须启用为全局编录服务器。

林中的每个域都必须有下列角色：

• 相对 ID（RID）主机。

• 主域控制器（PDC）仿真主机。

• 基础结构主机。

在每个域中这些角色都必须是唯一的。即林中的每个域都只能有一个 RID 主机、PDC 仿真主机以及基础结构主机。

RID 主机：RID 主机将相对 ID（RID）序列分配给域中每个不同的域控制器。在任何时候，林中的每个域中只能有一个域控制器作为 RID 主机。

每次当域控制器创建用户、组或计算机对象时，它就给该对象指派一个唯一的安全 ID（SID）。SID 包含一个“域”SID（它与域中创建的所有 SID 相同）和一个 RID（它对域中创建的每个 SID 是唯的）。

要在域之间移动对象（使用 Movetree.exe），必须由启动在域控制器上的移动操作，而此域控制器必须是目前包含该对象的域的 RID 主机。

PDC 仿真主机：如果此域包含在没有 Windows 2000 或 Windows XP Professional 客户端软件情况下运行的计算机，或者包含 Windows NT 备份域控制器（BDC），则由 PDC 仿真主机担当 Windows NT 的主域控制器。它处理来自客户端的密码更改并将更新复制到 BDC。在任何时候，林中的每个域中只能有一个域控制器作为 PDC 仿真主机。

在默认情况下，PDC 仿真主机还负责同步整个域内所有域控制器上的时间。域的 PDC 模拟器将其时钟设置为父域中任意域控制器上的时钟。父域中的 PDC 模拟器应配置为与外部时间源同步。用户可以使用下列语法执行“net time”命令，同步 PDC 模拟器和外部服务器上的时间：

```
net time \\ ServerName /setsntp :TimeSource
```

最终结果是整个林内所有运行 Windows Server 2003 或 Windows 2000 的计算机的时间相差都在几秒钟以内。

PDC 模拟器接受域中其他域控制器执行的密码更改的首选复制。如果密码最近被更改,则需要花费一定时间将此次更改复制到域中的每个域控制器。如果登录身份验证由于密码错误而在另一个域控制器中执行失败,则该域控制器将在拒绝登录尝试前将身份验证请求转发给 PDC 模拟器。

配置了 PDC 模拟器角色的域控制器支持两种身份验证协议:

(1)Kerberos V5 协议;

(2)NTLM 协议。

基础结构主机在任何时候,每个域中只能有一个域控制器作为基础结构主机。基础结构主机负责更新从它所在的域中的对象到其他域中对象的引用。基础结构主机将其数据与全局编录的数据进行比较。全局编录通过复制操作接收所有域中对象的定期更新,从而使全局编录的数据始终保持最新。如果基础结构主机发现数据已过时,则它会从全局编录请求更新的数据。然后,基础结构主机再将这些更新的数据复制到域中的其他域控制器。

除非域中只有一个域控制器,否则不应将基础结构主机角色指派给全局编录所在的域控制器。如果基础结构主机和全局编录处于相同的域控制器中,则基础结构主机不会运行。基础结构主机从不查看过时的数据,也从不将任何更改复制到域中的其他域控制器。

如果域中的所有域控制器都存有全局编录,则所有域控制器都将拥有最新数据,因而无论哪个域控制器承担基础结构主机角色均不重要。

基础结构主机还负责在重命名或更改组成员时更新“组到用户”的引用。当用户重命名或移动组成员(并且该成员驻留在组中不同的域中)时,组中可能暂时不显示该成员。组所属的域的基础结构主机负责组的更新工作,所以它知道成员的新名称或位置。这样当重命名或删除用户账户时,就可防止与该用户账户关联的组成员身份丢失。基础结构主机通过多主机复制的方法分发更新的内容。

在成员重命名和组更新期间,对安全性无危害。只有查看那个特定组成员身份的管理员才会注意到暂时的不一致性现象。

8.8.4　域与工作组的对比

工作组是最常用最简单最普遍的资源管理模式。简单是因为默认情况下计算机都是采用工作组方式进行资源管理的。默认情况下所有计算机都处在名为 workgroup 的工作组中,工作组资源管理模式适合于网络中计算机不多,对管理要求不严格的情况。它的建立步骤简单,使用起来也很好上手。大部分中小公司都采取工作组的方式对资源进行权限分配和目录共享。

例如计算机希望加入公司的工作组步骤如下:

(1)在系统桌面上鼠标右键单击“我的电脑”,选择属性。

(2)在弹出的窗口中选择“网络标识”标签。

(3)单击属性按钮进入工作组设置窗口,在隶属于工作组处输入希望加入的工作组名。

(4)设置完毕后需要重新启动计算机才能将新设置生效。

在一个网络内,可能有上百台计算机,如果对这些计算机不进行分组,都列在“网上邻居”中,电脑无规则的排列为访问资源带来不便。为了解决这一问题,Windows 操作系统引用了“工作组”这个概念,将不同的计算机按功能分别列入不同的组中,要访问某个部门的资源,就在“网上邻居”里找到那个部门的工作组名,双击就可以看到那个部门的计算机了。计算机通过工作组进行分类,使得用户访问资源更加具有层次化。在工作组情况下资源可以相当随机和灵活的分布,更方便资源共享,管理员只需要实施相当低级的维护。

使用工作组的缺点是缺乏集中管理与控制的机制,没有集中的统一账户管理,没有对资源实施更加高效率的集中管理,没有实施工作站的有效配置和安全性严密控制,只适合小规模用户的使用。

但是并不是说不在同一个工作组中的计算机就不能互相访问,当两台计算机所在工作组是同一个时,进入网上邻居选“工作组计算机”就可以看到对方,而不在一个工作组的话则需要进入网上邻居选择“整个网络”,才可以看到局域网中其他工作组,进入相应的工作组后通过双击实现访问的目的。

域与工作组的平等性有所不同,“域”是一个相对严格的管理模式。“域”指的是服务器控制网络上的计算机能否加入。实行严格的管理对网络安全是非常必要的。在工作组模式下,任何一台电脑只要接入网络,就可以访问共享资源,尽管工作组中计算机的共享文件可以加上访问密码,但这样的防范措施非常容易被破解。

而在“域”模式下,至少有一台服务器负责每一台连入网络的电脑和用户的验证工作。域的优点就是集中的管理和集中的安全控制,当然由域服务器承担集中式的管理和安全职能。缺点是采用域的方式管理资源配置起来相对麻烦,需要专门人员进行管理维护。

本机访问其他的计算机必须提供该计算机的账户和密码,假如公司的计算机有 100 台,现在让每台计算机都访问一下,需要记住 100 个账户和 100 个密码,而如果登录到域的计算机,而公司其他的计算机也都加入了域,那么访问域中计算机的共享目录都不需要账户和密码。

域与工作组的具体区别是,域是集中化管理,一台计算机如果加入了域中,那么所有本地的资源都会受到域管理员的控制,也就是说域管理员集中管理着整个网络的运作。工作组是分散式管理,一台机器可以随便的加入到任意一个工作组中,工作组中的每一台机器都有自己自主权,本地的管理员控制了资源的所有权以及资源的分配和共享。

域主要是为了方便管理,方便使用网络中的资源,提高网络的集中度和安全度。用于网络规模比较大网络使用量比较大,资源共享度比较大的场合,最为重要的是网络中的资源属于个人私自的不太多的场合。

一个企业组建的内部网,公司员工使用的机器都是企业的机器,机器里存放的资源也是与企业有关的,员工之间要经常的进行数据交流和资源共享,这样就有必要使用域模式的网络了。

相反，如果网络中的主机都是个人私有的，并且主机与主机之间的关系并不是那么的集中。内部网络利用率并不是那么的高，这时比较适合使用工作组模式。

比如一个内部局域网，网络内部的主机与主机之间的交流比较少，交流的范围也比较小，最重要的是网络中的主机都是个人私有的，所以使用工作组模式是最好不过的.

8.8.5　子域

子域是相对父域来说的，是指域名中的每一个段。各子域之间用小数点分隔开。放在域名最后的子域称为最高级子域，或称为一级域，在它前面的子域称为二级域。

如果所在的机构比较小，很可能只有一个单域。然而，大的机构常常是将服务分离开，并且机构名字空间中的不同部分的职责和管理也是分离的。或者说，可能只是为其他机构保存 DNS 记录，要完成这些任务可以通过子域和委托。

一个子域是一个现存域的孩子。例如，west. latinaccents. biz 是 latinaccents. biz 的一个子域。域 west. west. latinaccents. biz 又是 latinaccents. biz 的一个子域。域 latinaccents. biz 就是所有这些域的主语。域 latinaccents. biz 中的名字服务器能够保存它所有子域的资源记录，提供该域名字空间的集中管理。子域中主机的查询会被 latinaccents. biz 的名字服务器处理。然而，latinaccents. biz 域可以将其子域委派给其他名字服务器，比如存在于子域位置的名字服务器。例如，latinaccents. biz 位于佛罗里达，可以将 west. latinaccents. biz 域委托给位于西海岸的支持组的名字服务器。既然这样，一个查询到达 latinaccents. biz 的名字服务器后，该服务器会被查询提交给 support. latinaccents. biz 子域。两个例子的区别是，前者是所有的区域和数据否存在于 latinaccents. biz 的服务器上，而后者却依据域结构的需要将区域和数据分成较小的部分保存于其他的服务器上。

无论是将子域的数据保存到机构的主要名字服务器还是将数据委托给其他服务器，第一步都是创建子域。通过 DNS 控制台可以完成这个任务。在控制台中，打开要创建子域的服务器，然后再打开其父域。例如，要创建子域 west. latinaccents. biz，就应该打开 latinaccents. biz 区域。在其父域上鼠标右击，然后选择新域名。Windows Server 2003 会提示输入子域的名字。输入单一的名字并单击“确定”按钮，该子域就会作为一个分支出现在父域下方。创建了子域后，就可以给其增加记录了。只需要在子域上鼠标右击并选择要创建的记录类型。因为在创建父域的记录时，只能指定主机的单一名字。例如：如果要为 jane. west. latinaccents. biz 创建一个主机记录，将为 jane 在 west. latinaccents. biz 子域中创建一条主机记录。

无论是将子域的数据保存到机构的主要名字服务器还是将数据委托给其他服务器，第一步都是创建子域。通过 DNS 控制台可以完成这个任务。在控制台中，打开要创建子域的服务器，然后再打开其父域。例如，要创建子域 west. latinaccents. biz，就应该打开 latinaccents. biz 区域。在父域上鼠标右击，然后选择新域名。Windows Server 2003 会提示输入子域的名字。输入单一的名字并单击“确定”按钮，该子域就会作为一个分支出现在父域下方。创建了子域后，就可以给其增加记录了。只需要在子域上鼠标右击并选择要创建的记录类型。因为在创建父域的记录时，只能指定主机的单一名字。例如：如果要

为 jane. west. latinaccents. biz 创建一个主机记录，将为 jane 在 west. latinaccents. biz 子域中创建一条主机记录。

用户将某个子域委托给其他服务器，而不将子域中的记录保存于父域的名字服务器中。例如：假设 Support 组将其自己的 DNS 记录保存于它自己的服务器，需要执行以下步骤来委托 west. latinaccents. biz：

(1)在 Support 组的名字服务器上，创建区域 west. latinaccents. biz 并且使其支持反向查找区域，然后将 west. latinaccents. biz 中主机的适当资源记录添加到该区域。

(2)在上级即 latinaccents. biz 的名字服务器上，打开 DNS 控制台，然后打开 latinaccents. biz 区域。在该区域上鼠标右击并选择 New Delegation 来启动 New Delegation Wizard。

(3)在向导中，指定被委托域的名字。该向导自动使用父域名做后缀将全限定域名装配到被委托域，再单击“下一步”按钮。

(4)在服务名页，单击“添加”按钮来添加服务器的全限定域名和 IP 地址，该服务器保存有子域的记录。

(5)添加管理子域记录的其他名字服务器，单击“确定”按钮，然后再单击“完成”按钮来结束该过程。

若要新建子域，可以执行如下操作步骤：

(1)单击“开始”，单击“运行”，然后键入 depromo 以启动“Active Directory 安装向导”。

(2)在“操作系统兼容性”页上，阅读相关信息，然后单击“下一步”。

(3)如果这是第一次在运行 Windows Server 的服务器上安装 Active Directory，请单击“兼容性帮助”获得更多信息。

(4)单击“域控制器类型”页面上的“新域的域控制器”，然后单击“下一步”。

(5)在“创建一个新域”页面上，单击“在现有域树中的子域”，然后单击“下一步”。

(6)在“网络凭据”页面上，键入要用于该操作的用户账户的用户名、密码及用户域，然后单击“下一步”。此用户账户必须是 Enterprise Admins 组的成员。

(7)在“子域安装”页面上，验证父域并键入新子域名称，然后单击“下一步”。

(8)在“NetBIOS 域名”页上，验证 NetBIOS 名称，然后单击“下一步”。

(9)在“数据库和日志文件文件夹”页面上，键入要安装数据库和日志文件夹的位置，或单击“浏览”选择位置，然后单击“下一步”。

(10)在“共享的系统卷”页面上，键入要安装 Sysvol 文件夹的位置，或单击“浏览”选择位置，然后单击“下一步”。

(11)在“DNS 注册诊断”页面上，验证 DNS 配置设置是否正确，然后单击“下一步”。

(12)在“权限”页面上，选择以下选项之一“与 Windows 2000 Server 之前的服务器操作系统兼容的权限”或者“只与 Windows 2000 或 Windows Server 2003 操作系统兼容的权限”。

(13)在“目录服务还原模式管理员密码”页面上，键入并确认要指派给该服务器管理员账户的密码，然后单击“下一步”。在“目录服务还原模式”下启动计算机时会使用此密

码。

(14)检查“摘要”页面,然后单击“下一步”开始安装。

(15)重新启动计算机。

要执行此过程,用户必须是 Active Directory 中 Domain Admins 组或 Enterprise Admins 组的成员,或者用户必须被委派了适当的权限。使用该过程安装 Active Directory 的服务器将是新子域中的第一个域控制器。

在安装 Active Directory 之前,需要考虑与 Windows 2000 以前版本兼容的安全级别,并标识域的 DNS 名称。

当子域被添加到现有的树域中时,默认情况下将建立一个双向的可传递的父子信任关系。“权限”页上的向导选项会影响与运行 Windows 2000 和 Windows Server 2003 操作系统以前版本的计算机的兼容性,而与域功能无关。还可以使用智能卡来验证管理凭据。

“Active Directory 安装向导”允许 Active Directory 域名最多包含 64 个字符或 155 个字节。虽然 64 个字符限制通常在 155 个字节限制之前达到,但如果名称中包含采用三个字节的 Unicode 字符,则会发生相反的情况。这些限制不适用于计算机名。

不能在运行 Windows Server 2003,Web Edition 的计算机上安装 Active Directory,但可以将该计算机作为成员服务器加入到 Active Directory 域中。

8.8.6　信任

域是安全边界,若无信任关系,域用户账户只能在本域内使用。信任关系在两个域之间架起了一座桥梁,使得域用户账户可以跨域使用。确切地说就是信任关系使一个域的域控制器可以验证其他域的用户,这种身份验证需要信任路径。例如:A 域与 B 域没有信任关系,A 域上的员工使用自己在 A 域的账户,将不能访问 B 域上的资源。

两个域之间只有建立适当的信任关系后才可以实现互相访问,这就像两个国家之间要进行友好往来需要建立外交关系一样。

信任是有方向的,信任的方向决定了资源访问的方向。例如,如果 A 域信任 B 域,那么 B 域中的用户就可以访问 A 域中的资源。在 Window Server 2003 中默认建立的信任关系都是双向的,手工建立的则可以根据访问需要建立单项或双向的信任关系。

Windows Server 2008 域依照信任关系相互关联或相互操作。依照两个域之间的信任关系,一个域的安全主体被另一个域的安全服务信任。

信任根据它的传递性可以分为可传递的和不可传递的。如果 A 域和 B 域之间的信任是可传递的,B 域和 C 域之间的信任也是可传递的,那么 A 域和 C 域之间就自动创建信任关系。如果 A 域和 B 域之间的信任是不可传递的,或者 B 域和 C 域之间的信任是不可传递的,那么 A 域和 C 域之间不会自动创建信任关系。

信任的工作方式是目录林中的两棵树之间及每棵树的父域之间都存在双向的信任关系。如果 B 域中的用户要访问 Y 域中的资源,用户所在的客户端计算机会先联系 B 域的 DC 进行资源访问验证,因为要访问的资源不在本域,所以验证的请求会沿着信任的路径传递到资源所在的 Y 域,并最终进行资源的访问。

默认信任是系统自动建立的信任关系，不需要通过配置建立信任。默认信任有以下几种：

• 父子信任：在森林中，父子域之间存在的信任关系，称为父子信任。在默认情况下，当现有域树中添加新的子域时，将自动建立父子信任关系。这种信任是双向的可传递的信任关系。

• 域间（树根）信任关系：在森林中两棵树之间存在的信任关系，称为域间信任关系，在一个森林中建立第二棵树的时候将自动创建一个新的树根信任关系。这个信任是双向的可传递的。

其他信任关系不是系统自动创建的，需要手动创建，把手动创建的归为“其他信任”。

• 快捷信任：在同一个森林里的两棵树中的两个子树，默认的信任关系是通过信任关系的传递完成的信任。

• 外部信任：构建在两个不同的森林或者两个不同的域之间的信任关系。这种信任是双向或单向的、不可传递的信任关系。

• 森林信任：如果在 Windows Server 2008 功能级别，可以在两个森林之间创建一个森林信任关系。这个信任是单向或双向的、可传递的信任关系。森林信任只能在两个森林的根域上建立。

• 领域信任：不同系统之间创建和使用信任。

Microsoft Windows 采用了安全标准 Kerberos。Kerberos 和活动目录为 Windows Server 带来了票据授权服务，创立了一个分布式安全网络。如同单一登录，由一个域发布的 Kerberos 票据可以在另一个域中使用。Kerberos 票据就像信用卡护照一样允许持有人在任何接受这个票据的地方使用它。

一个域中的资源经常需要访问另一个域中的资源，为了实现这种情况，如果域和域不是同源的，它们就必须建立信任关系。默认情况下，同一棵域树中的域彼此信任，而其他目录林中的其他域树的域、非 Windows 2008 域和其他环境中的域都没有信任关系，因而必须明确的建立信任关系。被另一个域所信任的域称为被信任域，信任其他域的域称为信任域。

Windows Server 2008 域容器和安全技术是与众不同的。这是由于具有强健的目录服务、热门的安全技术和强大的管辖能力的支持。同一名字空间，同一家族甚至同一目录林的域隐含彼此的信任。这种信任关系不仅是隐含的存在，而且是可传递的。

建立信任是很麻烦的，只要两个域出现不信任，两个域的管理员就要建立信任。但是管理员必须知道如何在操作系统之间建立信任关系。两个系统共存的唯一方法，是一切转换的关键。一旦登录验证成功用户或应用程序便获得了到网络和资源的某些默认权利。

在 Windows Server 2008 域中，域之间的相互信任能力是很明显的，其中确实存在着巨大差异。NT 域之前的互操作是单调乏味的。小型和中型公司在 NT4.0 中分开创建域根本没有特别的意义，即使是跨越广域网，也同样如此。如果拥有 10 人的公司要创建 10 万多个域对象是不合理的。小公司创建多个域就没有任何其他的理由，只是为了组织他们的想法。

因为域是处于不断的变化状态，所以很少有人能遵守 Windows NT 域的 10 万个对象的限制规则。经常监视 SAM 的大小非常有意义，因为它在增长到大于 35 MB 或 40 MB 时就会变得不稳定。

只有在出现特殊情况下，才有必要在一个公司中管理多个域，最高纪录是一个公司有 70 个以上的域。因为这时要从不同的接管企业继承域。管理员每天都可能在分配资源和吸收用户时遇到问题。尽管如此，许多大型公司都用光可注册表空间，或是因为它们创建各自的资源域，用来容纳设备和其他网络服务，与“用户”或“账号”域分开。

Windows Server 2008 域是以 Internet 域为模版，具有层次性和透明性，而且几乎可以无限划分。它们是相互信任的，就像同一个屋檐下的家人互相信任一样，虽然每个家庭成员都在各自的房间里干自己的事情。

在 Windows Server 2008 域上创建多个域很有意义。出于不同的原因，最重要的一点是权利下放和管理委派的原因。正如接下来将看到的，可以创建的域来自包括子网、站点、部门、位置和其他同样的事物。只要是源于同一个根的域，它们之间的信任关系就是双向的。尽管“传递”一词总是与存在于多个域之间的双向信任关系有关，但却不是意味着两个域组就能够像两棵植物一样彼此嫁接在一起。但在目录林中迁移、移动域和最终消除孤立域却是比较容易的。

建立信任规划的第一步是确定何时需要在目录林中建立信任关系。如果在 Windows Server 2008 的两个目录林之间建立了信任关系，则目录林中的每个域都自动建立传递的信任关系。目录林信任关系只能在两个目录林的根之间建立。

在建立目录林信任关系之前，需要确认所有的域控制器都安装了 Windows Server 2008，因为必须有 Windows Server 2008 支持这个功能。同时还需验证 DNS 结构是否正确。两个目录林 DNS 服务器可以权威解析 DNS 结构，或者可以在两个 DNS 服务器上建立 DNS 转发。下面为目录林信任规划的步骤；

(1)掌握各种信任关系的知识。

(2)正确设定目录林的 DNS 结构。

(3)功能级设在 Windows Server 2003 上。

建立信任关系时，必须要有两个目录林的企业管理员的权限，每个新建立的信任都有对应的密码，两个目录林的管理员都需要知道这个密码。

8.8.7　功能级别

从 Windows NT 到 Windows 2000、Windows 2003、Windows 2008 都提供活动目录功能，然而不同操作系统运行的域提供不同功能的服务，在域内由不同类型的操作系统组合而成的域，支持不同的功能和服务，这就称之为域的功能级别。同理在林中也存在林的功能级，这个概念在 Windows 2003 的 Active Directory 中提供了比 Windows 2000 Active Directory 更高的功能级别，称为 Windows 2003 临时模式和 Windows 2003 模式。只有把所有的域控制器升级到 Windows 2003 模式，整个森林才能被提升到 Windows 2003 模式。森林功能级别的提升需要手动完成。

域功能级别上的域功能激活只影响这个域和该域的功能。Windows Server 2008 功

能级别支持五功能级别，以下分别介绍五功能级别及其功能级别所支持的域控制器：

• Windows 2000 混合模式(默认)其网络配置使用 Windows 2000 和 Windows NT 的任意组合系统。Windows 2000 域控制器和 Windows NT 4.0 备份域控制器可以在同一个域中无缝共存而不会出现任何问题。当然，Windows 2003 域控制器也支持此模式。激活的功能包括本地与全局组并支持全局编录。

• Windows 2000 本机模式。域中所有域控制器都可以运行 Windows 2000 或 Windows 2003。激活的功能包括组嵌套、通用组、Sidhistory、安全组与通讯组之间的转换。

• Windows Server 2003 临时模式。允许 Windows 2004 域控制和 Windows NT 4 域控制器的混合使用，但不能与 Windows 2000 域控制器混合使用。显见支持的域控为 Windows 2003 和 Windows NT，此级别内没有域范围的激活功能。该模式只在将 NT 4 的域控升级到 Windows 2003 域控时使用。

• Windows Server 2003 模式。域中所有域控制器只能是 Windows 2003 和 Windows 2008。支持的功能包括：Netdom.exe 提供的域控制器重命名功能、更新登录时间。将使用用户或计算机的上次登录时间来更新 Last Logon Times 属性。可以在域内复制该属性。在 inetOrgPerson 和用户对象上将 user Password 属性设置为有效密码的功能，重定向用户和计算机容器的功能。默认情况下，已提供了两个已知的容器，用于容纳计算机和用户/组账户：即“cn＝Computers，域根”和“cn＝Users，域根”。该功能可用于定义这些账户新的已知位置。授权管理器能够将其授权策略存储在 Active Directory 域范围(AD DS)中。包含受限制的委派，以便使应用程序可通过 Kerberos 身份验证协议充分利用用户凭据的安全委派。可以将委派配置为仅允许特定的包服务，支持选择性的身份验证，通过它可以从受信任林指定允许对信任林中资源服务进行身份验证的用户和组。

• Windows Server 2008 模式。目前为止所有域功能级别中最高级别，支持所有 Windows 2003 域功能级别，之外还支持一下功能 SYSVOL 的分布式文件系统复制支持，可提供 SYSVOL 内容的更稳健更详细的复制。Kerberos 协议的高级加密服务(AES 128 和 256)支持。上次交互式登录信息，将显示用户上次成功交互式登录的时间、来自什么工作站，以及自上次登录失败的登录尝试次数。严格的密码策略，这可以为域中的用户和全局安全组指定密码和账户锁定策略。注：Windows Server 2008 支持目前所有 5 种域的功能级别。

域功能级别的评估：

• Windows 2000 混合级别对于没有完全淘汰 Windows NT 域控制器的企业最为合适，但现在 NT 应该很难寻觅。

• Windows 2000 本机域级别如果已经部署了从 Windows NT 到 Windows 2000 的 AD 迁移，那么这个功能级别显然最合适，而且这种模式也仅仅从 NT 域环境升级到 Windows 2000。

• Windows Server 2003 过度级别为那些直接从 Windows NT 域控制升级到 Windows 2003 的用户准备。但是此种模式不支持 Windows 2000。

• Windows Server 2003 域级别：如果打算在转换林之前将域级别提升到 Windows 2003 功能级别，此种模式为最好的选择。要求域中所有控制为 Windwos 2003 或 Windows 2008。

• Windows Server 2008 域级别是目前最高级别，要求所有域控都是 Windows Server 2008。

林的功能级别主要分为三种：

(1)Windows 2000 支持所有默认的 Active Directry 功能。

(2)Windows Server 2003 所有默认的 Active Directory 功能及以下功能：林信任和域重命名。对于链接值复制而言，组成员身份将被更改为各个成员存储并复制值，而不是作为单个单位复制整个成员身份。在不同域控制器中同时添加或删除不同成员时，这种更改可在复制期间占用更少的网络带宽并降低处理器使用率，同时消除丢失更新的可能性。部署运行 Windows Server 2008 的只读域控制器(RODC)的功能。改进的知识一致性检查器(KCC)的算法和可伸缩性。站点间拓扑生成器(ISTG)使用改进的算法，可缩放支持具有远远大于在 Windows 2000 林功能级别上所支持站点的数量的林。改进的 ISTG 选择算法是一种在 Windows 2000 林功能级别选择 ISTG 的入侵性较小的机制。改进的 TSTG 算法更好的缩放 ISTG 用于连接林中所有站点的算法。在域目录分区中创建动态辅助类的实例的功能。将 inetOrgPerson 对象实例转换为 User 对象实例的功能，反之亦然。创建新组类型的实例以支持基于角色的身份验证的功能。在架构中停用并重新定义属性和类别。

(3)Windows 2008 该功能级别提供 Windows Server 2003 林功能级别上可用的所有功能，但不提供任何其他功能。但在默认情况下，随后添加到林的所有域，将在 Windows Server 20 域功能级别进行操作。

提升域功能级别：大家比较熟悉的是由 Windows 2000 混合模式升级到 Windows 2003 模式。注意，当域功能级别提升后，运行较老的域控制器将不能被加入到域中。例如，如果将域的功能级别提升到 Windows 2003，则原来的 Windows 2000 的域控制将不能被添加到域中。

8.8.8　命名

活动目录采用了几种命名模式，允许应用程序和用户使用常用的格式访问活动目录。这些名字格式如下：

(1)RFC822：是使用电子邮件和 WWW 冲浪时最广为人知的命名约定。这些名称也称为用户主体名称(UPN)，格式为 somename@somedomain，比如 thepresident@thewhitehouse.gov。活动目录对所有用户都提供 RFC822 名字空间。如果需要寻找某人在公司中的分机号码，假设此号码是公开的，只需在目录中查找 someone@somedomain.com，软件会将此名称翻译成正确的 LDAP 查询，UPN 同样可以进入 Windows Server 域的登录名或用户 ID。Windows 用户现在可以使用下列格式输入他们的 ID 和密码，便可登录到 Windows Server 2003 网络。可以对某个域指定用任何 UPN 来登录。也就是说，可以创建一个成为 MCITY 的域，但指定用户以 someone@

acmesales.com 登录，这样用户只需要记住电子邮件地址就可以登录了。

(2)LDAP 和 X.500 名称：LDAP 和 X.500 命名约定也称为属性命名。它由带有目录的服务器名称、用户名称、组织单位等组成，例如可以表示为：LDAP://anldapserver.bigbrother.com/cn=jsmithers,ou=trucksales,dc=bigbrother,dc=com。

其中，LDAP 名称可用来查询活动目录。

DN 的每个部分都是对象的一个属性，用 attribute_type=value 表示。当提到对象名称本身或 RDN 时，所指的是对象的规范名(canonical)或通用名(common)。在 LDAP 术语中以 cn=表示。如果讨论用户时，通用名采用 cn=jchang 的格式。

每个对象的 RDN 都存储在活动目录中，每个都包含到它的父类的引用。当沿着路径链向上引用时，同时也得到了 DN。这就是 LDAP 执行目录查询的方式。这种命名模式与 Internet 的 DNS 机制很相似。

现在已经讨论了活动目录的命名机制，应该明白 Windows 不需要用户每次访问对象时都进行这项工作。用户接口隐藏了具体的细节完成所有的工作。但是在下列情况中仍需要进行这项工作：利用活动目录 API(ADSI)或 LDAP 直接编写代码，或使用脚本语言或工具进行查询，执行比其他标准工具能提供的更高级的操作。

活动目录支持 LDAPv2 和 LDAPv3 命名规范，它们符合 Internet 的 RFC1779 和 RFC2247。这种规范采用如下形式：

cn=common name

ou=organizational unit

o=organization

c=country

但活动目录去掉了 c=country，并用 dc=domain component 代替 o=organization。例如表示为：cn=jchang,ou=marketing,dc=mcity,dc=org 在 DN 中逗号是分隔符的作用。LDAP 函数解析 DN，利用分隔符将 DN 解析为不同的部分。

在点分隔表示法中，将表示为 jchang.marketing.mcity.org。LDAP 算法将 LDAP 名称转换为 DNS 格式，反之亦然。只要遵从 LDAP 命名约定，任何 LDAP 客户端都能够通过下列的 LDAP URL 查询活动目录：

LDAP://ldapserver.mcity.org/cn=jchang,ou=marketing,dc=mcity,dc=org

活动目录中的对象根据它的全局唯一标识符(GUID)的属性来存储和追踪，这个属性称为 objectGUID。对象可以被移动、更改甚至重命名，但它的 objectGUID 始终是不变的。GUID 是在对象创建时分配，是一个 128 位的数字。在活动目录中，不存在没有 GUID 的对象，GUID 是对象创建时被自动分配的必要属性之一。GUID 可以被外部处理过程和编程函数引用。换句话说，外部程序可以通过 GUID 引用活动目录对象。这种机制确保了对象只要存在就可以访问，且不论对象移动到什么地方都是可以访问的。

活动目录通过 SAM 访问控制机制为对象提供保护，通过存取控制表(ACL)保证对象的安全性。换句话说，如果希望更改或删除某个对象，必须能够证明对该对象具有所有权和相应权限。

8.8.9　站点

站点(Site)是表示在一个或多个 TCP/IP 网段上的一个或一组网络位置,抽象为一个活动目录对象。在 Windows Server 域控制器矩阵中,站点是作为一个逻辑单元来管理的。

在活动目录中,站点是由其所在的 TCP/IP 子网来识别或者定位的,是通过 DNS 来解析对应的子网。就站点内或者站点间的复制来说,站点直接与域相关。站点也间接同目录林中的其他部分相关,这是由于其他的命名环境比如全局编录和架构等导致的。站点也是一个完全独立于域名空间的逻辑容器。

活动目录要求站点连接良好,这个术语相对有点模糊。根据 Microsoft 所下的定义,站点应该通过可靠的连接访问。排除这一术语是指同 28.8 KB/s 调制解调器连接。可在现实中,需要设有大量带宽的 56 KB/s 或者 64 KB/s 的站点。

Windows Server 要求站点以及时和可靠的方式快速获取域复制。通过 TCP/IP 子网定义站点,可以快速构建活动目录网络,并将其映射到对应的物理结构网络。

但是,最重要的是利用站点来决定包含域控制器的网络间的复制需求,并与此相关的所有其他的复制服务,例如:WINS、DNS、Exchange、NDS 等。所有连接和编址在同一 IP 子网的计算机和网络实际上都是这个站点的一部分。

站点控制完成下列几个功能:

- 身份验证:站点用来协助客户定位最近的 DC 和 GC。DC 有一个站点的列表,并根据手中的 IP 地址信息判断哪一个 DC 离用户最近。
- 复制:当目录发生更改时,站点配置将决定何时对其他的 DC 和 GC 进行相应的更改。
- 间接的活动目录服务与应用:像 DFS 这样的服务可以被配置为能感知站点,可以用从活动目录获取的站点信息来自动进行配置。将来,应用程序也可以获得指定的站点信息。

KCC 用来完成站点内域控制器之间的复制服务。KCC 依照下列规则在 DC 之间建立复制路径:

- 从一个 DC 到另一个 DC 至少要有两条以上的复制路径。
- 同时,DC 和复制源 DC 不能相距多于三个跳跃点。

这样的拓扑可以保证,即使有一个域控制器停机,复制仍然可以继续传播到其他域控制器。

KCC 也为域控制器建立附加路径,但是这种情况下不会有任何域控制器有连接。只有在站点内域控制器的数量达到七个时,附加路径才会起作用,以此来保证“三跳”复制的规则。

活动目录允许用户定义连接对象(Connection Object)。连接对象是域控制器间复制的手动配置点。KCC 自动建立连接对象,但是可以对这些对象进行访问配置。如果需要,就可以建立符合自身需要的复制拓扑。在大多数情况下,用户不需要手动配置连接对象,KCC 会处理好建立连接与复制环境的任务。

站点链接(Site Link)将两个或多个连接在一起。站点链接同 Exchange 连接器相似,在配置上也类似。同 Exchange 和 WINS 类似,链接是单向的,用来建立复制拓扑。

建立站点链接时,并不需要做什么工作,因为在创建站点和添加域控制器时,活动目录已经自动创建用来站点链接。当然,用户也可以手动配置站点链接。在涉及特殊的环境和冗余等情况时,手动配置站点链接就变得很有必要。

由于站点链接是单向的,所以有时可能需要建立双向站点链接。由于站点链接是依据现有广域网的基础结构进行管理的,所以有多个配置选项。配置选项如下:

• 传输协议:这一选项决定采用何种技术在 DC 间传递实际数据。活动目录提供了两种选择:RPC 或 SMTP。SMTP 是一种邮件传输协议,是不可靠的登录验证数据传输协议,但是它不要求很多的 CPU 资源。另一方面,RPC 对数据进行压缩,因此也更有效,尤其是在介质带宽很小时。可以利用 SMTP 进行 GC 复制、架构和文件复制服务(FRS)主要原因是这些技术并不支持压缩。

• 链接成本:可以为站点确定一个成本值,以判断到这个站点使用哪个路径成本最低,大家当然不希望链接上的路径的成本与每月或每年的服务相反。在可能的情况下应当为站点链路配置成本低的路径,这样活动目录才能使用最小成本路径。

• 频率:频率值是用来决定间隔多少分钟检测站点链接复制。频率的默认值是 100 分钟,时间表默认值是三小时(180 分钟)。

• 时间表:时间表控制何时进行复制。如果站点在白天很忙,网络需要把所有的可用资源用在关键应用任务上,这时应该停止复制。

站点链接是一种简单工具。它保证复制从一个域传播到另一个域,反之亦然。但是对于复杂结构的站点,复制过程就会变得有点冗长。站点链接是不可传递的。这就是说,信息从站点 A 复制到站点 B,站点 B 复制到站点 C;如果站点 B 出现问题,则站点 A 和站点 C 之间不会发生复制。这种情况的解决引出站点的又一特性,称为站点链接桥(Site Link Bridge)。

把活动目录划分成站点可以减少与复制相关的网络流量,但是仅仅把活动目录划分成站点是不够的。为了在站点之间交换信息,必须在站点之间建立链接。通过站点链接提供信息,Windows Server 知道哪个站点需要复制,多长时间复制一次。当使用同样的链接传输把两个以上的站点链接起来时,它们就被桥接起来。IP 站点链接起来,组成一个站点链接桥,通过这个链接桥它们任何二者都可以直接通信。

站点链接桥是可传递的,这就意味着当创建一个站点链接时,这个链接中的任何站点都是自动桥接。只要所有的站点都在路由器的 IP 网络上,甚至不用创建新的站点。

站点链接桥成本是包括桥中所有链接成本的总和。用户可以和服务提供商协调链接成本。

为了设计复制拓扑,可以手动创建和管理连接对象。这里将是从工具的角度来讨论连接对象,这些工具用来管理同一站点内不同 DC 间的复制拓扑,也可以使用它们手动配置不同站点中 DC 间的复制。

活动目录的复制拓扑具有很大的灵活性,这也是为什么建议用户探究其他用法的原因,例如 DNS 复制。可以手动管理复制,这意味着可以自己创建所有的连接对象;也可以

让活动目录安全自动进行复制，并将全部站点都连接到站点链接桥中；当然也可以自动配置一部分，手动配置一部分。

如果有特殊需要或者有特殊的链接，只能手动配置，使用手动选项；否则，都选择自动配置。

8.8.10　复制

在一个网站内的复制的路径或网站的拓扑结构，是由一个服务自动来管理的，称为知识一致性检查器（KCC）。通常情况下，网站内发生的复制速度比在网站之间的复制还快。Active Directory 网站和服务 MMC 管理单元允许用户控制网站间的复制。用户可以使用它来建立网站连接桥接的对象和设定复制模式。

在 Active Directory 中，用户需要定义每个子网。Active Directory 可以找出最佳的方式复制本地和网站之间的资讯。

为了减少跨越广域网络连接的流量，桥接服务器可在两个网站之间执行目录复制，而只有两个指定的域控制器可相互交流。如果有来自多个域的域控制器，每个网域将有一个桥接的服务器。

8.9　组策略

组策略（Group Policy）是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。通过使用组策略可以设置各种软件、计算机和用户策略。

8.9.1　理解组策略

Windows Server 2008 上的更改控制工具是组策略对象编辑器（GPDE 或简写为 GPE）。应用程序是一个 MMC 管理单元，从这里策略可以应用于 Windows Server 2008 网络的安全主体，包括：计算机、用户和组。组策略也可以应用于诸如安全管理和硬件配置等项目。

组策略用于创建一个对象，该对象包含来扩展计算机控制和用户对网络和机器资源访问的属性，这一对象被称为组策略对象即 GPO。该策略是由存储在工作站或服务器上的各种各样的模板而创建的。

当安全主体是同 GPO 相联系的容器的成员时，安全主体就处于那个 GPO 的影响下了。当一个容器同多重 GPO 相连接时，结果是连接到容器上的所有 GPO 的效应合并在一起。

组策略并不直接应用于一个单个的安全主体，尽管可以通过建立特定的 OU 来达到粒度化而是应用于安全主体集合。Windows Server 2008 网络中的安全主体汇聚在三个位置：站点、域和组织单元。由于 GP 适用于所有三类容器，所以也可以称之为 GP 层次。

Windows Server 2008 的组策略是庞大的，而且其功能非常强大。需要花费一些时间来适应，而且要花费大量时间来尝试各种不同的应用方法。在大型公司里，管理 GP 的

任务应该分配给个人，他们可能是更改管理委员会的成员。对于一个管理员来说，管理GP很容易就会成为一个专职职业。GP将成为主要技术，应用这一技术可以管理更改、用户配置、桌面设置、工作站锁定安全和软件安全等。

组策略对象(GPO)拥有100多项与安全相关的设置，700多项基于注册表的设置，应用某些API和用户模板还可以扩展和加强GP技术。具体地说，GP技术提供下列功能：

• GPO被设定并且存储在活动目录中。GP也可以定义为一个本地策略对象，即定义在工作站上。单独的计算机使用本地GPO就可以保证安全或者锁定(本章后面的“组策略如何工作”部分会提供更多相关信息)。然而GP却依赖于活动目录。

• 在AD容器(站点、域和OU)中将GPO应用于用户和计算机。

• GPO是安全的。可以像锁定Windows Server 2003操作系统中的其他任何对象一样锁定一个GPO。

• GPO能够被安全组中的成员过滤或控制。实际上，这可以加速策略在安全组成员上的应用。

• 在Windows网络中，GPO就是安全力量集中的位置。

• 利用GPO维护Internet Explorer。

• 利用GPO登录、注销和启动脚本。

• 利用GPO维护、限制软件和进行软件安装。

• 利用GPO重定向文件夹(例如My Documents)。

• 与Windows NT4.0中的情况相似，当策略更改时，GPO不会暴露用户的配置文件，使其遭到篡改。

• 计算机上的GP设置并不是永远不变的。换句话说，与以前的管理或锁定工作站的技术不同，注册表并不是一次完成并且不能更改的。用户可以在任何时候很容易地更改参数与配置信息。

8.9.2 组策略的类型

组策略只对Windows网络上的全部过程、应用程序或者服务有影响。因为服务器和工作站都要受到GP的影响，所以只有配置Windows 2000 Professional或者Windows XP时，GP才能应用于整个企业。Windows和NT4.0工作站受到的影响程度与Windows 2000/XP客户端不同。因为客户端分机的这种卸载和读取策略的扩展性能在这些原有的台式计算机操作系统中并未出现。

这意味着一个由多种Windows版本所组成的网络也将是比较安全的，但是不易于管理。很明显，一个难以管理控制的网络的长期维护是非常昂贵的。所以最初把整个企业升级到Windows Server 2008的成本从长远来看是合算的。在安全性方面，比如通过加密技术可以预防黑客或者通过文件夹重定向挽救关键数据，不仅可以挽救一台机器，甚至可以挽救整个公司。消除的版本越多，网络就越安全、越易于管理。

有许多不同类型的组策略集，下面描述来这些策略集的“意图”：

• 应用程序配置：这些策略用来管理用户对应用程序的访问。可以采用下列方法控制管理应用程序的配置或者安装：

• 分配：GP 在客户端计算机上安装或者升级应用程序和软件。分配也可以用来发布应用程序的图标或者快捷方式并保证用户无法删除图标。

• 应用程序发布：应用程序可以在活动目录上发布。用户在控制面板中单击 Add/Remove 图标时，应用程序将出现在组件列表中。

• 文件配置：这些策略使得可以在用户的计算机上的某个文件夹中放置文件。例如，可以将用户的 My Documents 文件夹作为目标文件夹，提供给他完成一个项目所需的文件。

• 脚本：这些策略允许按预定的次数选择脚本运行。在启动和关闭计算机时，或者当一个用户从一台机器注销而另一个用户又从这台机器上登录时，这对于保证脚本被处理尤其有效。Windows Server 2008 可以处理 VB 脚本、Jscript 和为 Windows 脚本主机所编写的脚本。

• 软件：这些策略允许在用户的工作站的整个或者局部范围上配置软件。这可以通过用户配置文件中的配置设置实现，例如：桌面设置、Start 菜单结构和其他应用程序菜单。

• 安全性：就目前来说，在 Windows Server 2008 中可能没有其他的策略集能比安全策略集更加重要。

除了能够最终减少所有权的总成本以外（通过降低管理成本），还有一条要考虑关于组策略的建议。它不是为了给用户和管理员制造麻烦而是为了保护、改善工作环境和用户环境。因此应当确保有足够的资金来平衡双方的需要。

在努力保证环境安全的过程中，毫无疑问会遇到与维护“用户友好”环境宗旨相违背的冲突。在密码长度上的使用就是一个好例子。设置过长的密码既不会增加安全性，还会使用户感到麻烦，由于密码太长根本记不住，用户还可能把密码粘贴在显示器上，这是不安全的。如果必须加强安全性，这种情况下的选择可能是把安全需求提到管理日程上或者建议使用智能卡或者生物测定方法。在锁定环境的同时不应该把用户锁在外面。

环境可以通过多种方法改善。当用户需要获取一个新软件的时候，从用户的观点来看，存在下列三种传输方法：

(1)在桌子前等待几个小时或者几天直到管理员来安装新的软件。

(2)被要求登录到网络分配点，自己安装软件。

(3)在软件好像没有受到人为干涉而神秘地自动安装到机器上时，休息一下。

改善用户环境同时意味着帮助他们更加容易地定位应用软件，更加聪明地改变文件夹路径或者将其文件夹映射到资源，在工作站不活跃的时期使登录或者注销过程自动化。

8.9.3　组策略成分

在管理员看来 GP 由以下几个成分组成，它们包括：

• 组策略对象；

• 活动目录容器；

• 组策略链接；

• 组策略的政策（如组策略对中断点的刷新）；

- 详细描述策略对象的说明性文本；
- 组策略编辑器；
- 计算机配置和用户配置节点；
- GP 容器和 GP 模板；
- gpt.ini 文件。

组策略对象或者 GPO 是容纳组策略属性的对象。在最高级别上 GPO 实际上是一个存储属性和性质的容器，策略是通过同 GPO 的连接传送的，也就是说，这些属性删除了包含在一个 GP 容器内的用户或者计算机对象。在使用 GPO 策略以前，必须将它们创建和命名。

活动目录容器是 GPO 的默认对象。换句话说，容器默认通过与 GPO 的链接来接收组策略的配置。容器通过与 GPO 建立链接而处于 GPO 及其策略的影响之下。当创建一个 GP 时，上述这些会自动发生。可以与 GPO 相链接的容器包括站点、域和组织单元。但是 GP 也能够与一个单独计算机相关联，所有计算机都可以链接到本地 GPO。

容器通过 GP 链接从而同 GPO 关联。用户可以搜索特定域的链接。通过“发展”这些链接，可以建立影响特定容器及其成员的 GPO。

策略是 GPO 的属性，策略就是链接中应用的实际设置。所有 GPO 都有相同的策略，不必从 GPO 增加或者删除某个策略，策略可以通过几种方式激活。策略必须首先被定义，然后才能被激活或者使其失效，或者在某个特定的 GPO 中具有活性以及在一个安全组中被应用。一旦它被激活或者定义，就可以操作包含这些策略的设置了。

若要在使用之前定义的策略，可以选择为 DNS 服务器定义。一旦定义了策略，就可以设置启动标准。已经定义了 DNS 服务器的策略并将其启动参数设为自动(Automatic)，其中一些策略要求用户简单地激活或者使其失效，而另一些则需要定义、激活然后进一步地配置或者安装。

说明性文本通过策略的 Explain 选项卡访问。并非所有的策略都有 Explain 选项卡。说明性文本从本质上描述策略实现什么和一些关于如何应用策略的指导，还描述来自哪种环境中不应当应用策略。

组策略编辑器(GPOE)就是提供 GPO 设置访问的 MMC 插件。为了给 GPO 建立一个容器，必须首先在 GPE 中载入一个已有的或者新的 GPO。

一个 GPO 被分为两个节点。这两个节点就是 Computer Configuration 和 User Configuration。每个节点包含来各自安全主体的策略。可以把策略应用到任一个 GPO 中的两个节点之一。

8.9.4 GPO 的位置

所有的 GPO 把信息存储在两个位置：组策略容器(GPC)和组策略模板(GPT)。这些对象通过全局惟一的标识符(GUTD)来辨别，它保证了两个位置的对象同步。当产生一个 GPO 时，同它相关联的信息就传送到了这两个位置。

操作系统在 systemroot 中 sysvol 、结构中为 GPT 建立了一个文件夹供其使用。这个文件夹的实际名称就是该 GPT 的标识符(GUID)。一个典型的 GPT 文件夹如下所

示：

%systemroot%\SYSVOL\sysvol\genesis.mcity.org\policies\{31B2F304-016D-11D2-945F-00C04FB984F9}

GPC 位于活动目录中。在目录给定的空间中，它给自己建立了一个容器层，其中存储的是计算机和用户配置信息。

GPC 处理版本、状态和设置以及由扩展名定义的所有策略设置。GPO 的 SYSVOL 端包含有客户端扩展名、用户配置参数、计算机配置参数（registry.pol）和来源于管理模板的注册表中设置的列表。

作为一般原则，数量很少并且更改很少的策略数据存储在 GPC 中，而数量很大而且很频繁更改的策略数据通常存储在 GPT 中。

GPT 结构的默认内容是同安全相关的内容，但是在配置用户和机器环境时，GPT 结构会填满文件夹和与大范围 GP 相关联的信息和更改管理信息。

以下是可以进入 GPT 结构中的文件夹和信息：

- \ADM：包含同 GPT 相关联的 ADM 文件。
- \MACHINE：包含同机器注册表设置相关的 REGISTRY.POL 文件。
- \MACHINE\APPLICATIONS：包含 Microsoft Windows Installer 所使用的 AAS 文件。
- \MACHINE\DOCUMENTS&SETTINGS：包含在用户登录到计算机时用来配置用户桌面的文件。
- \MACHINE\MICROSOFT\WINDOWSNT\SECEDIT：包含 CPTTMPI.INI 安全性编辑器文件。
- \MACHINE\SCRIPTS：包含启动和关闭文件夹。
- \MACHINE\SCRIPTS\STARTUP：包含启动脚本及其相关的其他文件。
- \MACHINE\SCRIPTS\SHUTDOWN：包含关闭脚本及其相关的其他文件。
- \USER：包含同用户注册设置相关的 REGISTRY.POL 文件。
- \USER\APPLICATIONS：包含 Microsoft Windows Installer 所使用的 AAS 文件。
- \USER\DOCUMENTS&SETTINGS：包含用来配置用户桌面的文件。
- \USER\SCRIPTS：包含登录和注销脚本。
- \USER\SCRIPTS\LOGON：包含登录脚本及其相关的其他文件。
- \USER\ SCRIPTS\LOGOFF：包含注销脚本及其相关的其他文件。

在每个 GPT 的根文件夹里，可以找到一个 gpt.ini 文件。这个文件中有两个同本地 GPO 相关的重要项目：

- version＝x：这一项是 GPO 的版本号，X 是一个由版本计数器函数设置的数字的占位符。通常版本号的基数是 0，每次修改 GPO 时计数器都会增加 1。然而，版本号是由十进制显示的 8 位十六进制数字，占用一个双字节，该类型数据可以被组策略进程所识别。其中，低四位数字标识计算机设置的版本号，高四位数字表示用户设置的版本号。换句话说，如果看到版本号为 65539，其存储在计算机中相应的十六进制数字为 0X00010003。从数字中可知，计算机设置版本号为 3，用户设置版本号为 1。

• Disabled=y:这一项指的是本地 GPO,并且通知其从属函数本地 GPO 是否有效。如果 GPO 失败,此处的变量为 0;当被激活时,变量值变为 1。

8.9.5 组策略如何工作

Windows Server 2008 组策略应用程序层次通常为:首先是站点,其实是域,再次是 OU。换句话说,如果 GP 是为站点设置的,那么这个站点中的所有对象都会受到该 GP 的影响,包括域及其所有成员。如果接着将 GP 应用于域,那么域中所有对象的 GP 就是从站点和域继承合并来的。如果 GP 是为站点和域设置的,将其进一步应用于 OU,那么 OU 中任何对象的 GP 就是这三者的结合。

OU 中的组合控制可能来源于域策略,也可能来源于站点策略,除非继承的策略很明显被内在的覆盖机制阻碍,这个覆盖机制可以被激活或者被禁用,或者被组和用户的访问控制机制阻碍。也可以通过在一个对象上链接 GPO 来强行执行策略,然后设置链接禁止覆盖。

GPO 也存在这两种情况:本地 GPO 和域范围 GPO。因为本地 GPO 早于非域范围 GPO 应用于计算机,计算机的实际继承层次结构首先是本地 GPO,其次是非本地站点,再次是域,最后是 OU。同样,本地 GPO 首先应用于计算机,然后在用户登录以后来自 DC 的任何策略才能被应用。

组策略应用程序被成功运行。换句话说,机器设置的最近一次激活的策略将被应用。因此,如果定义了一个本地策略,而没有定义站点策略,那么站点策略配置就会生效。如果继续定义域配置策略而没有定义 OU 策略,则最后的结果是这些配置不会对该 GPO 内的任何对象产生影响。

对于本地 GP,如果其高层策略没有定义,则本地策略生效。如果没有域策略,而为了在确保网络安全性的同时保证用户在一定范围内持续工作,应该建立本地策略。

然而,GP 经常在一定程度上取代本地策略,并且取代来源于域的安全策略。即使本地安全策略很强大,但是安全策略也会经常将其覆盖。如果不定义域级别的安全策略,则本地级安全策略也会保持无效,可通过运行合成策略集的报告来验证这点。每一台 Windows 计算机都有一个管理的本地 GPO。在任何一台 Windows 计算机上,可以通过在命令行上运行 gpedit.msc 来打开本地 GPO,或者从安装的菜单项中拉出 MMC 管理单元打开本地 GPO。但是有一点一定要注意,就是非本地 GPO 可以覆盖本地 GPO。

活动目录的体系结构规定,后应用于对象的策略覆盖先应用的策略。换句话说,如果在本地 GPO 中删除来允许用户登录本地计算机的权利,稍后又在一个站点或者域 GPO 中恢复了这一权利,因为这一恢复设置是后应用的,所以这一设置是有效的。例外的情况是未定义的东西不能改变现存控制,所以早先明确激活或禁用的控制都可允许继续存在。

在早期的容器中,任何一个激活的或者禁用的 GPO 控制状态都是持续的。但是如果上级某些控制被定义,则在本地级这些控制都是有效的。这对于个人计算机的控制访问和一定的安全机制十分有用,其中明确禁用的选项防止了管理员无意中激活它或者在非本地域层次中故意激活它。

另一个需要重点注意到是:可以为一个容器建立多重 GPO。控制应用程序的次序是

后应用的策略覆盖先应用的策略。也就是说，如果一个 OU 中有两个 GPO，列表中第一个 GPO 里表达“是”的任何设置将被后来表达“不”的 GPO 覆盖，这被称为管理次序，这一次序可以通过 OU 属性窗口上 Group Policy(组策略)选项卡上的 Up 和 Down 按钮重新排列。

通过选中 No Override on a GPO 选项，可以在 GPO 上设置 No Override，链接在较低级别上的 GPO 不能覆盖较高级别 GPO。使用 No Override 还可以防止链接在同一级别上的 GPO 的互相覆盖。当在 AD 中存在的多个同一级别的链接都被设置为 No Override 时，需要根据用户决定的优先权排列它们，列表中级别较高的链接具有较高的优先权。

当对域或者是站点应用 GP 时，理解这一点很重要。可能想保持许多有效的设置，而本地管理员则可能试图覆盖这些设置。只要用户在较高级别的 GPO 上设置来 No Override，那么激活的设置将在较低级别的目录下强制执行。

No Override 设置应用于链接，而不是应用于实际的 GPO。块策略继承设置应用于域或者 OU，因而它适用于链接到这一级别或者更高级别的所有 GPO。站点没有更高的权限。

可以阻止从更高级别的 GPO 处继承 GP。这一点可以通过选中域或者 OU 属性窗口的 GP 选项卡上的 Block Policy Inheritance 复选框实现。这一选项不适用于站点，因为 GP 在层次中是最高的。这是一个安全难题，当用户认为发现了安全漏洞时，如果 No Override(严禁覆盖)被激活，它将处于优先状态。

为了调查 GPO 所支持的链接，按照下面步骤执行：

(1)按照前面介绍的方法打开 OU 属性窗口并选择 Group Policy 选项卡。

(2)选择 GPO，然后单击 Properties (属性)按钮。选择 Links (链接)选项卡，单击 Find Now 按钮。

编辑 GPO 时，所改变的设置并未立即应用于容器，但是策略上的更改却是即时的。GPO 设置在默认情况下每 90 分钟应用于对象一次。但是这个刷新时间是可以改变的。

由于应用 GP，可能会造成冲突，设置登录密码的可尝试次数低而导致账户锁定，如果用户连续几次输入错误的密码，这种情况很容易发生，因为用户可能打开来 Caps Lock 键功能，就需要重新设定锁定功能。

账户锁定可能是个别策略执行其规定操作的结果，而这些结果却不是最初的意图。为了在这种情况下开启账户，可以打开 Active Directory Users and Computers 插件进入用户账户。右击账户，在弹出菜单中选择 Properties 选项，在系统弹出属性窗口中选择 Account 选项卡，可以看到 Account Lock Out 复选框已经被选中。这是操作系统按照 GP 的指令选上的，取消选定，用户就可以登录了。

虽然父域 GP 可以覆盖子域 GP，但是如果子域 GP 同父域 GP 相抵触，子域 GP 优先。与其在覆盖、继承、访问控制联结方面制造恶战，不如尽力保持简单并完整记录所有 GP、组成员资格和任何特殊连结。

8.9.6 过滤策略

GP 也能够从居于安全组中的安全主体范围中过滤出来。换句话说,可以精确地定义出哪一个用户或者计算机的安全组受 GP 影响,其他无关组受 OU 控制。可以通过设置组上的任意访问控制列表许可来实现。这样一来,GPO 不仅可以更快地作用于安全主体,而且也可以限制特定的安全策略与 GPO 建立 AD 链接。

DACL 是一个对象的许可列表。根据组的成员资格使用 DACL 允许或者拒绝 GPO 访问。有两种方式应用过滤:

(1)右键单击 GPOE 中 GPO 的根节点,在弹出菜单中选择“Properties(属性)选项”,系统打开属性窗口。选择“Security(安全)选项卡”,该选项卡显示组和用户及其相关的许可权限。

(2)另外一种方法是打开进入活动目录站点、域或者 OU 中的容器,单击右键,在弹出菜单中选择“属性选项”。在系统弹出的属性窗口中,选择“Group Policy 选项卡”。然后在这个选项卡中的 GPO 列表中选择“GPO”。单击右键,在弹出菜单中选择“属性选项”,然后在新弹出的窗口中选择“Security”选项卡,直接单击属性按钮也可完成同样的操作。

现在就可以通过选中或者不选中容器中的 Apply Group Policy access control entry (ACE)来指定哪些组受到影响,而哪些组不受影响。同时应该知道的是,默认的已验证用户选中的是 Apply Group Policy 和 Red permissions 两个复选框,而不是 Write Control 或者 Full Control 复选框。这就意味着用户不能修改 GPO。这样就可以更严格地控制 GPO 访问。

这些技术允许用户使用 GPO 上的 Security 选项卡来决定哪一个管理组可以修改 GP。应用这些技术可以加强域的安全性。

组策略进行如下委托:

(1)为站点、域或 OU 委托组策略链接分配。

(2)委托建立 GPO。

(3)委托管理 GPO。

委托是通过对使用 MMC 控制台和执行与 GP 相关插件的特定管理权利的委托来实现,它们通过 GPO 来自我控制。为了授权 GPO 访问的任务,必须控制谁可以访问组策略 MMC 插件。路径如下:进入 AD 中的容器,右键单击项目。在弹出菜单中选择 Propertion Group Policy 选择一个 GPO,如果还未建立 GPO,则先要建立一个。单击 Edit 按钮,系统将载入 Group Policy 控制台。进入 User Configuration,Administrative Templates,Windows Components,Microsoft Management Console,最后进入 Group Policy。在 Group Policy 节点上,可以看到 12 条同组策略插件相关的文件夹和策略。

管理员可以通过称为域管理员组或者内置管理组的成员来管理组策略。非管理员必须经过本地登录许可方能管理,执行路径如下:Computer Configuration, Windows Settings,Security Settings,Local Policies,User Rights Assignment,最后进入 Allow Log on Locally。允许许多用户登录 DC 是不安全的,同时也是不明智的。因此,最好将诸如活动目录、用户和计算机工具等活动目录工具的使用分配给网络系统管理员或台式机咨

询顾问的工作站。得到了适合的权限,这些系统管理员无需要进入服务器机房就可以登录 DC 了。

Windows Server 2008 机器上的本地 GPO 只配置安全设置,通常绝大对数是禁用的。本地 GPO 存储在%SYSTEMROOT%SYSTEM32\GROUPPOLICY 目录下,通过 DACL 可以设定下列许可:

(1)系统管理员(安全)。

(2)操作系统(安全)。

(3)鉴别用户(只读和执行)。

组策略几乎是完全在客户端进行处理的。惟一完全在服务器端进行的 GP 服务是远程安装服务。这是因为客户端不存在处理这一策略的操作系统。

一组称为客户端组策略扩展名的 DLL 首先向 GPO 列表的 DC 提出要求,然后执行客户端处理,处理次序从 GPO 列表中获得。处理中的优先规则是,计算机配置优先于用户配置。将所有的用户放入一个小型的 OU 集,然后将他们的计算机放在其他的能与关键管理实体(KME)相连接的 OU 中。

组策略行为的发生是为了检查事件的健全性。一种被称为组策略回送的特性允许用户设置基于所使用的计算机的组策略。回送特性允许用户从两种模式中进行选择来控制用户配置或者计算机配置。

当用户登录到计算机上,并且回送特性处于合并模式时,首先根据用户配置读入 GP 对象,然后根据计算机配置再次读入 GP 对象。因为最后是在计算机配置中读入的,所以计算机配置具有优先权。这就是说与计算机相关的 GP 比用户 GP 具有更高的优先级别。如果用户的 GP 不受计算机配置的影响,用户配置的策略才会被应用。

这一模式强制 GP 忽略用户的 GP 配置。也就是说,只有计算机配置中 GP 才起作用。同所有 GP 过程选项一样,一个 GPO 的合并模式与替换模式也可以通过 Computer Configuration\Administrative Templates\System\Group Plicy 来设置。

GP 处理可以同步处理也可以异步处理。异步处理可以在其他线程上进行,因而处理更快发生。而同步处理线程在一项处理完成之后才能开始。可以使 GP 处理的处理行为用户化,但是只能在专门的应用程序中使用,在这些程序中用户需要尽快地应用 GP。规则如下:为了加快速度,使用异步处理;为了安全可靠则使用同步处理。

虽然规则在 Windows Server 2008 操作系统中工作的很好,但是在 Windows XP 操作系统中给 GP Pool 带来了一点麻烦。如果 GP 被异步应用,Windows XP 会快速启动,因此它启动的速度是非常快的。用户可能在所有策略没有完全执行的情况下对计算机进行操作。上述情况的发生并不意味着用户在打开文档编辑器进行工作的同时,一些诸如文件夹重定向的策略会在用户操作的十分钟后才执行。一些策略并不是同步执行的。

Windows XP 和异步处理带来的问题只会对软件分配造成影响。如果向工作站分发应用程序,这可能需要用户在软件策略执行和软件安装完成前进行多次登录与注销的操作。这样就会出现这种情况:一个被分发的软件正在安装,而用户为了运行计算机上的另一个软件,需要不停地进行登录和注销操作,甚至于这些操作会耗费一上午的时间。

默认的刷新频率是每 90 分钟一次。因而对于应用于特定用户或者计算机的任何 GP

变更只在这一默认时间内有效，用户可以通过使用管理模板中的 GP 设置来更改这一默认值。设置为零将强制每 7 秒进行一次刷新操作。可以在安全需求较高的应用程序中或者特定的处理情况下设置更短的刷新间隔。默认的刷新频率看起来确实很长，可以至少将其缩短到每 60 分钟一次。

设置较短的刷新间隔会导致网络通信量的增加，用户计算机上非常小的间隔可能会干扰工作环境。而较长的刷新间隔在网络中就比较容易应用，但是却降低了网络的安全性。最长的间隔时间是 45 天，但是如果需要改变安全策略，这样长的时间是无益的。

为了改变设置，需要编辑默认城控制器的 FPO，它同 DC 的 OU 链接，打开 GPO 进入“Computer Configuration”→“Administrative Templates”→“System”→“Group Policy”→“Group Policy Refresh Interval for Computers”节点。

用户需要编辑默认域控制器(Default Domain Controller)的 GPO 来更改设置，该 GPO 与 DG 的 OU 相连接。打开 GPO，进入其计算机配置节点。选择管理模板(Administrative Template)并依次进入 System，Group Policy，直到达到计算机节点的 Group Policy Refresh Interval。

在域控制器中，刷新策略都是禁用的。用户可能需要检查一下自己的 DC 上是不是这种情况，文档记载的 DC 刷新频率是每 5 分钟一次。

管理 GP 设置，如文件夹重定向和软件安装，只发生在计算机启动期间或者之后，或者当用户登录时，而不是在前面所讲的周期性刷新期间。这样做的原因是显而易见的，用户不希望正在使用软件的同时，该软件执行自我删除的操作。

每一个客户端扩展名都有一个控制 GP 处理的策略参数。默认情况下，客户端扩展名在刷新间隔判断出 GP 已经改变时，才会刷新 GP。这样做是为了使性能最优化。但是为了安全起见，可以保证在每个刷新间隔，即使策略不曾改变，也可以刷新 GP。

用户应当非常有选择性的应用这一操作，因为执行了该操作后，用户将会发现尽管增加了带宽，但 GP 的刷新速度反而减慢了。

如果 GP 探测到的是低带宽网络，它将在客户端扩展名上设置标记。标记一旦出现，将发生下列 GP 处理：

(1)总是执行安全策略。

(2)总是处理管理模板中的策略。

(3)跳过软件安装。

(4)脚本关闭。

(5)跳过文件夹重定向。

(6)Internet Explorer 维护关闭。

GP 使用内置的算法计算出基于数据和时间参数的反应频率以及所使用的链接。如果计算结果与默认的 500 KB/s 相等，则 GP 认为这是一个低速链接并在 GP 处理中做出必要的调整。但也可以在 GPO 的 Group Policy 节点上将默认值更改为用户认为合适的数值。这个策略就是“组策略低速链接探测”。记住在用户配置节点中也要为用户设置成这一数值。用户配置中的目标策略的一样的。

用户配置文件对于低速链接也有超时策略。它位于 Computer Configuration 节点

处，目标策略是 GPE 的 Logon 节点。如果扩展名不能探测到服务器，它默认为测量文件系统性能，这就是 NT 测量性能的方式。这一策略被设置成 Kb/s 为单位的链接速度极限和以毫米为单位的传输时间极限。

在一个域中同时管理数百台 Windows 工作站。它们的接收策略设置为每天的链接超过 32 Kh/s。迄今为止，这样的速度是可以接受的。

当设置用户的活动目录基础结构时，需要保证在整个企业内适当地宣传和传播 CP 设置，还要确保复制模糊 GP 信息的传播过程。

用户有以下几种考虑：如果所支持的是一个小型企业，通常只有一台处于同其他人一样的网络上的 DC，那么不需要关心在哪里编辑 GP。但是对于大型公司，用户可能为 GP 更改面非常谨慎地控制目标 DC，以及非常谨慎地确定哪些人有权利做出这些更改。

若接受 GP 编辑的 DC 或者实施改变的管理员超过一个，问题就会出现。用户的 GP 编辑在复制过程中可能被重写，因此产生 GP 编辑冲突。因为依靠 DC 的位置，不一定总能对 GPO 进行创建和编辑。

有两种方法设置 GP 域控制台选项。一种是通过 GPO 编辑插件，另一种方法就是通过 GP 设置，即通过编辑 Administrative Templates 节点中的策略来使用户有权设置 DC 选项。

为了进入上诉选项中的设置，需要打开 Default Domain Policy 进入 GPOE，选择根。在 View 菜单中，可以看到一个 DC Options 菜单项。

对话框包括下面三个选项，从中选择与网络环境最适用的一个选项：

(1)The one With the Operations Master token for the PDC emulator(PDC 仿真程序的 Operations Master 令牌)：这是微软文件的默认选项，但是在相同网络部分拥有多个 DC 时，也存在一个例外的情况。然而，这个选项保证只有一个 DC 是 GPO 创建和编辑的目标，其余的 DC 从同一资源中接受 GP 更改。这个选项使控制台强迫用户或其他人员每次都只用同一个 DC。这就是此项只是控制台的一部分而不是处于首位的插件原因。此外，应当限制能够在某个域中使用 GP 的人数或者把规划 GP 任务作为更改管理的一部分(拥有 Operations Master 令牌的 DC 通常是为树林创建的第一个 DC，但是如果迫不得已也可以放弃这个特权)。

(2)The one used by the Active Directory Snapins(活动目录管理单元使用的选项)：管理单元包含一个选项，允许更改作为其核心的一个 DC(所有 MMC 控制台允许选择一台计算机)。只要确定所选的 DC 正确，那么此选项就能够工作。但是如果不注意细节，这可能造成运行中的问题。

(3)Use any available domain controller(使用任何可用的域控制器)：这个选项是最不理想的，但是也能满足某些情况的需要，比如网络上的组连接非常紧密或 DC 簇运行在高高速网络上。

可通过在 GP 中设置自己喜欢的选项而覆盖上面的三个选项。GPO 能够保证编辑 GPO 时，所有的插件都选择主域控制器仿真程序。

用户也可以使用策略指定 GP 如何选择域控制器。换句话说，通过把选项设定为策略，用户可以准确地指定用哪一个 DC。

8.9.7 使组策略工作

GP 和更改管理的两个关键问题是软件更改控制和安全，它们代表了更改控制和更改管理的两个关键领域，是由 Windows Server 2008 的 GP 技术支持的。

软件策略包括用来管理应用程序、Windows Server 2008 及其各个组件的策略。在下面的例子中，将演示如何使用 GPE 插件来修改、处理设置和环境设置。

按照下列步骤编辑软件 GPO：

(1)打开 Active Directory Users and Computers 管理单元，进入想要放置 GPO 的站点、域或者 OU 中，通常称为 SDOU 容器，SDOU 代表 Site Domain and Organization Unit。

(2)右击容器，在弹出菜单上选择 Properties 选项，然后在新弹出的窗口中选择 Group Policy 选项卡。

(3)选择 GPO 链接，编辑或创建一个新的 GPO，单机 Edit 按钮。

(4)按照路径，通过 Administrative Templates/Control Panel，进入 User Configuration 节点。通过禁用 Background 选项卡，设置一个禁止用户更改桌面模式和墙纸的策略。

(5)鼠标右键单击策略进行修改，从弹出菜单中选择 Properties 选项。

(6)首先检查策略是否被执行、定义或者激活，如果没有，通过选中复选框定义或者激活策略，然后选择策略设置。单击 Apply 按钮和 OK 按钮返回控制台。

以上就是一个简单的策略更改的全过程，会发现当浏览软件相关的策略时。有些策略会要求增加更多细节，如路径名或其他类似信息等。

策略管理着 Windows Server 2008 网络安全配置。安全 GP 对每一个可能造成系统整体安全隐患的端口配置都是适用的，例如：登录/注销、通信、文件系统、硬件和媒体等。

以下是与安全领域相关的组策略：

- 账户策略：这些策略设定密码、账户锁定、验证和 Kerberos 等。
- 本地策略：这些策略设定审计和用户权力定义等。
- 受限制组：这些策略聚合安全敏感性组的组员资格。内置管理员组就是一个受限组的实例。
- 系统服务：这些策略设定计算机上运行的服务的安全和默认启动行为。
- 注册表：这些策略设定注册密钥的安全性。
- 文件系统：这些策略设定文件系统的安全性。
- 活动目录：这些策略设定每个域中目录对象的安全性。
- 公共密钥：这些策略设定加密数据恢复的代理、可信证书权限和其他与公共密钥基础结构或 PKI 相关的参数。
- IP 安全：这些策略设定与 IP 安全相关的策略。

更改控制策略结合的第一准则是：更改控制策略通过计算机实施于用户。也就是说，更改控制的对象是用户的计算机。

如果能够把更改策略用于计算机，那么就能把这些策略用于用户。如果用户没有计算机的控制权，用户就没有能力避开策略。虽然 GPO 分为两个配置区：用户和计算机，

但是计算机配置享有优先权。

通过 GP 所拥有的能力和 Windows 的所有组件，访问控制、GP 继承、GP 覆盖锁定、GP 刷新、GPO 链接、OU 嵌套和域嵌套等，用户很有可能建立起难以理解的 GP 系统，因此在计算阶段应谨慎行事。

但是，把用户限定在一台特定的计算机上的做法越来越不实际。终端服务会话将无法处理，而且也很难为移动用户和定向任务人员管理计算机。所以在网络上用户的身份验证即 ID 登录和网络上工作站的身份验证合并或组合在一起，给用户和他们的计算机提供一个更改控制，可以为客户提供过滤权限和优先权限，从而达到控制的目的。

这种权利让用户桌面跟随到任何一台本地或远程计算机上。既然已确定需要更改管理和控制，就需要实施。也就是说，需要创建更改控制实体，提出实施更改控制委员会构想的策略，并通过 GP 以及所发现和定制的适合自身环境的其他机构，在企业各个层次上执行更改控制。

在处理组策略过程中，认为无论微软安装什么作为默认的组策略都是足够的这种想法很危险。首先，各个企业的实际情况不同，GP 中的设置可能适用于一个公司，而并不适合用于另一个公司。其次，微软设置默认 GP 的标准并未被用户广泛知晓，而且不适于大部分用户。最后，在大多数情况下，在安装和测试服务及其组件时会发现微软所注明的默认策略与实际并不相符。

处理 Windows 网络的最好办法就是安装它，装好所有的接线端口、引导项目、测试和实验用品；或者可采取更为保守的方法、测试和确认。可以专门在网络中为某种特殊类型的设备进行配置。如果需要让一个服务器启动并运行起来，那就应该尽可能地使用某项特定的服务，这样可以去掉安装运行步骤。

目录顶部打开新的域控制器的 GPE。从这里开始，往下沿着 SDOU 等级中的每一个容器，调查相应位置的 GPO 链接。打开容器的 Properties 窗口，选择 Group Policy 选项卡。接着编辑每个容器中的链接，然后把用户配置和计算机配置中的每一个对象里定义或激活的设置都查看一遍。

几乎不可能在创建新域的同时以任何方式锁定或覆盖任何设置。所以可以放心地认为已经建好了站点策略，正是把跟 DC 过滤器放入了这个站点的目录底部。换句话说，现在创建任何的 OU 都可以从上一级继承。当然域处于这个等级的中部，所以需要查看一下应用在域层次的 GP，以观察它会对处于 OU 层次的用户理想的控制产生什么影响，每一个创建的域都有一个默认的域 GPO。对这个信息进行研究并把它记载在帮助台或变更管理系统中。如果没有更改的系统，用数据库或文字处理文件也能达到目的，但这可能不大好使用，不过现在还可以用。

在应用之前，应首先坐下来研究一下更改管理和安全策略，把一个树林的末端到另一端需要的策略与从一个域的末端到另一端所需要的策略分别开来。如果树林中只有一个域，就不需要太长时间。因为此目录将会发生更改并且会变得很长。

借助于全局策略指令列表，可以首先为放置根 DC 的站点编辑 GPO，这个站点位于活动目录域或 Internet 域或名字空间之间的最顶部。在这个站点中，建立用户希望整个企业默认的策略，比如密码长度。如果没有 GPO 链接于站点，那么创建一个，然后打开

进行编辑。

在这一层上创建的任何策略都会过滤到用户建立的各种域和 OU 中，注意，当首次进入策略时，密码长度还未进行设置。所以当打开域 GPO 时，会发现默认长度是 0 个字符，这种安全的程度很低。

在大多数的时候，把计算机账户集中到代表用户 KME 的 OU 中都是切实可行的。能沿着 KME 线路或功能创建 OU，并把为 KME 服务的计算机收集到各自的 OU 中，也可以将计算机或者工作站 OU 中的计算机账户分组，这种方法经常使用，例如：所有的用户都设置在一个大的用户 OU 中。

也可以把一组计算机添加到一个安全组中，然后把安全组设置到各自的 OU 中，现在，无论计算机组添加到那里，该组通过关联就出现在其他 OU 中也是可行的。计算机将按照它们接受策略的顺序受到影响。对于一组计算机来说，顺序为：首先是它们单独或在组中存在的 OU，然后是受组认可的 GP 作用的任何其他结构。应注意，最后应用的 GP 将覆盖先前的 GP，除非明确地禁止覆盖或阻止继承。

用户的更改控制和管理或配置技术属于称为 IntelliMirror 的体统范畴。这种体系始于几年前的零管理 Windows(ZAW)。

可以在企业中的任何时候开始应用 IntelliMirror 技术，可以从操作系统的安装、软件安装和配置，或者用户设置等多处着手。更改管理矩阵的每一部分都是相当复杂。

下面的建议为使用 GP 和 IntelliMirror 相关的技术进行更改配置提供了出发点。本教材选择配置登录/注销脚本、锁定桌面、自定义和锁定 Start 菜单，重定向文件夹和管理模板中各种配置等为出发点，这些领域代表了多年从事商业活动，并且深入其业务和资源的客户的紧急需要。因为仅组策略就需要考虑 700 多项设定。使用它们支持已经开始实施或仍在计划中的更改管理。

在计算机启动和登录桌面出现之前，(需按【Ctrl＋Alt＋Del】键)有一段闲置时间(用户看着荧屏)，在用户注销后也有一段闲置时间。

这段闲置时间里，可以使用策略运行各种选项，例如：运行反病毒检查，向网络中添加或删除信息，同步脱机文件和文件夹，运行诊断程序，或者登录机器时把信息集中到代表用户活动的数据文件中。借助于应用软件程序，可以有充足的理由在登录或注销的闲置时间内运行某些选项。

锁定桌面的更改控制的一个重要组成部分可通过执行下载和浏览策略，也可以为 IntelliMirror Explorer 创建客户配置等，其他及其重要的策略可以达到以下目的：

• 防止用户更改访问“My Documents”文件夹的路径。如果需要保证用户文档和其他工作相关文件被转移到一定能够进行备份的服务文件夹中，这一点将会经常使用。

• 禁止控制面版：以防止用户胡乱更改管理显示、网络连接、通信等设置。如果需要访问某个项目，也可以隐藏特定的控制面版程序。

• 隐藏对 CD-ROM 和软盘驱动器的访问：通过去除这些端口，可以防止用户使用不明软件给网络带入病毒，还可以保证企业能够控制软件盗版。还可以对用户隐藏硬盘驱动器。

• 禁用命令控制台：使用户不能从命令行中执行命令。对于黑客来说，计算机的命令

行就如进门的第一步。

• 可以设定禁止对注册表编辑工具进行访问，例如：Regedt32 和 Regeit。

GP 允许禁用部分 Start(开始)菜单，使用户无法看见他们。还可以自定义 Start 菜单反应更改管理的需要。例如：

• 可以从 Start 菜单中删除 Run 菜单。这个选项页也可锁定开启 Run 菜单的快捷键。

• 还可以将 Logoff 项添加到 Start 菜单中，这是为终端会话用户服务的。

• 还可以禁止拖拉 Start 菜单中的快捷菜单，这样会使得用户不能在 Start 菜单中记录、删除和排列项目。

每位用户都被授予了能够访问域或工作站上的大量个人文件夹的权限，这些文件夹包括 My Documents，My Pictures 和 Application Data。为了保护用户文件、企业的知识产权和应用软件数据，组策略的一个宝贵特点就是允许把每位用户的个人文件夹和应用软件数据的集合重定向到网络服务器上。

文件夹重定向将使企业从以下三个方面受益。首先，由于数据被强制存储在网络服务器上，所以无论个人数据还是应用数据都可以得到定期备份。

其次，数据和文件可以进行定期的病毒检测。存储在企业本地机器上的数据通常不能备份，而在每个工作站施加的反病毒措施也并不能保证机器百分之百不受病毒的威胁。尽管在每一个工作站上都安装了病毒检测程序，但是不可能保证每一台机器都拥有每个月发布的数千种新病毒的最新数据文件。所以保护一台服务器要比设置保护每一台机器不受侵犯的程序简单得多。

再次，可以保证无论用户在何地登录，即使在应用服务器的终端，都能够访问他们的文件夹，而他们的应用软件数据也都保存在同一个地点，以便于访问。

重定向文件夹很容易，从用户放入服务的任何一个指定文件夹都可以完成。可以重新设定文件夹到共享处，也可以通过组成员资格激活文件夹重定向。

要激活文件夹重定向，进入到 User Configuration 节点/Windows Settings/Folder Redirection 重新定向。

重要定向文件夹，按照下列步骤进行：

(1)右键单击文件夹，例如 My Documents，从弹出菜单中选择“Properties 选项”，出现文件夹加载对话框(在本例中是 My Document 属性对话框)。

(2)在下拉列表中选择“Basic-Redirect Everyones Folder to the Same Location 选项”，或者根据组成员资格重新定向，可以选择“Advanced-Specific Locations for various user groups 选项”。

(3)然后在 Target 文件夹地址栏中输入目标文件夹。需要在这里键入 UNC 名称，必要时使用%username%变量。也可以通过 Browse 选项来选择路径。如果在上一步选择 Advanced 选项，则需要单击对话框中的 Add 按钮来选择此选项所应用的组。

(4)单击对话框上的 Settings 选项卡，进一步设置重定向的标准。例如：权限和转移策略(当策略被转移时使用)等。完成单击 Apply 按钮，再单击 OK 按钮。

现在完成上述工作后，需要保证对新定向的资源进行备份和病毒检测。

Windows Server 2008 中更改控制管理的首要技术是能够使用自身的更改管理。GP 的应用与管理的继续发展的最大问题是该项技术非常复杂,难于管理。为了使 GP 管理更加容易,Microsoft 承诺将提供更好的工具。但这项工作至今仍然进展比较缓慢。

在讨论这项技术的困难性之前,深入思考一下,该技术是如何经常地被应用于严格的质量控制和确认过程的。首先,在实验室中发现和证明这些概念之前,系统是通过纸张、Vision 或 Rational Rose 设计出来的。然后将实验室环境中的设计和测试应用与实践,系统从实验中移植出来并根据规格重新建立。这个步骤完成后,完成正规的确认工作,这个确认工作包括确保系统的安装和操作的正确性,以及系统的工作符合标准。

系统被应用后,将根据维护过程、灾难恢复操作和更改控制对其进行维护。组策略的实现在设计和外置阶段都应该遵循相同的步骤,这对于整个企业的运转具有深远的影响。然而,由于 GP 创建和应用程序结构本身具有一些缺陷,因此这样的做法是不切实际的。

GP 不仅必须逐渐创建,而且对象一旦被保存,它将马上开始工作。因此,任何验证和测试都是没有意义的,GP 立刻与其内部创建的容器相链接。如果在主 OU 中创建一个与所有计算机向冲突的 GPO,难么其所带来的损害将很难被修复。

8.9.8 GP 的发展与建立

为了减轻 GP 应用的复杂性,应该在所有 GP 创建的域中创建一个 Staging OU。这个 OU 必须是所有 OU 树的最低层。这样做使得用户可在创建 GPO 时,无需与任何产品 OU 相链接,这些 OU 下存在许多不可知的用户和计算机并作用于它们。GPO 在创建后可以与 Staging OU 断开链接,而与其他任何 OU 建立链接。GPO 也可以应用于域中的一个组。

这种 GP 隔离的方式可以为 GP 的阶段实现提供测量方法。GPO 创建后,即将一个测试 OU 上的所有测试计算机和用户集合起来,并且将 GP 移走。如果 GPO 依照设计工作,则可通过更改控制将其放入最后产品。通过将 GPO 与另一容器进行链接或将其反应用于一组用户或计算机即可实现。

组策略的维护和更改控制不可能在不影响用户的情况下将 GPO 扩展或测试,甚至将其取回到实验室进行修复。因此通常的做法是,为新特性创建一个新的 GPO,扩展或缩减原来的版本。

破坏或中断 GPO 当然是可能的。应用一个与理想状况有偏差的设置也是有可能的。因此,必须为 GP 实行严格的更改控制。但是在大多数情况下,GP 结构的更改管理是非常困难的。

扩展一个现存的 GP 有两个缺点。首先,GPO 的新定义和设置增加了对象的复杂性,GPO 中的设置越多就越难维护,并且使其在域中移动也变得更加困难了。一个拥有好的登录脚本设置的 GPO 是非常难于扩展的。如果在 GPO 中增加访问 XP 的管理设置,那么受登录脚本设置控制的用户在登录 XP 时会受到同样的限制。因此在不影响登录脚本设置的前提下,不可能将所有用户的访问权限进行分级。

如果接触过 Windows 的 GP 管理,将会发现 GPO 故障检测以及预测或测试一个 GPO 是否按照设计工作是非常麻烦的,在 Windows 中引入合成策略集(RSOP)的概念,

它对于 GP 计划的制定以及发生在实施 GP 工作站上的故障检测都是非常有帮助的。Windows Server 2008 也使用了相同的技术。

RSOP 可以获得包含实施于用户和设备的所有组策略设置的报告。该报告可以帮助我们进行 GP 的故障检测，以及决定 RSOP 如何更改用户计算机的桌面与工作环境。

Windows 的 RSOP 功能可以从用户所应用的计算机或域中任意一台计算机上提取出 RSOP。也可以使用命令(GPRESULT)来获得实施于一个用户及其使用的计算机上的所有 GP 设置。

使用 RSOP 来定制 GP 应用程序的方法是打开用户和计算机的活动目录，选择树表上任意一个 OU；鼠标右键单击 All Tasks 菜单选项，然后从上下文菜单中选择“Resultant Set of Policy”。

规划(Planning)选项。这些操作会装入合成策略集向导(Resultant Set of Policy Wizard)，使用合成策略集向导可以通过各种设置在目标 OU、用户、计算机或组上模拟实现 GP 应用程序，如回溯模式、低速网络连接和 WMI 过滤器。

RSOP 工具对于故障检测来说是非常重要的。打开服务器上的 Resultant Set of Policy 控制台(RSOP . mmc)建立目标用户和计算机的 RSOP 报告。在打开控制台前，RSOP 会将当前设备和登录的用户的 GP 信息集中起来。控制台会根据这些信息进行启动。用户可通过同样操作获得其他设备(主要是工作站)和计算机 RSOP 报告。

然而，作为目标设备的本地管理员(默认包括域 Admins 组成员)去创建一个 RSOP 报告，其在 Windows 上使用 RSOP 控制台是有权限限制的。但是，为了合成 GP 的故障检测和模拟而创建报告是 RSOP 最大的用处，GPO 中出现漏洞的几率是非常大的。由于一些用户模板对 GP 造成过度损坏而使得一个功能完善的 GPO 遭到破坏，这样的情况不会发生。撤销更改，从实验室中取得 GP 备份，或者恢复 GP 备份。操作系统本身提供的标准工具是不能实现这些操作的。想要解决这些困难，需要第三方软件的支持。

目前，备份、修复 GPO 的唯一方法就是通过全备份/修复过程来完成的，该过程备份和修复整个活动目录。如果一个 GPO 中的某一件事被中断或者不小心被删除，用户无法在活动目录中将该 GPO 单独进行备份和修复。

FAZAM 2000 提供 GPO 的备份与修复功能。设计与建造 GP 代价是非常大的，即使不持续几周，也要花费好几天的时间。而且一旦做错某项操作，如在删除对话框中选错了一个单选按钮，前面所做的工作就有可能前功尽弃。

如果 GPO 遭到中段或者破坏，甚至于不知道什么原因而丢失，除了从作为操作系统一部分的备份磁带中进行恢复外没有其他本法。当然，可以使用 DCGPOFIX 命令行命令恢复默认的 GPO，但是这个意味着原来在这些 GP 中的设置都丢失了。然而，使用 FAZAM 2000 来备份和修复 GPO 是非常容易的。

FAZAM 工具可以在测试域中创建和测试 GPO，并且将策略定义保存在数据仓库中，这是该工具最有用的特点。通过 FAZAM，可以在桌面版、本地版 SQL Server 和完全版中创建和存储对象。

为了使用户可以将 GPO 从其在 SQL Server 存储仓库中的存储位置装载到域中，仓库结构为 GPO 提供了一个全恢复系统。这样 GPO 将是完全可恢复的。如果用户终端

要删除一个对象，只需要连接上 SQL Server，这根本用不了几天或几周，就可以将丢失的 GPO 重建并恢复工作的正常运行。

对于活动目录中，GP 的更改控制或更改管理的实现，仓库机构也是非常理想的。FAZAM 可以在实验域中创建测试组策略。无论何时通过更改控制，均可以将该 GPO 移植到正式域中。

尽管 Windows 为提升 GP 管理功能而增加了一个系列的新特性，但是如果没有诸如 FAZAM 等管理软件的保护，GP 管理依然是一个沉重的管理负担并具有相当风险。

8.10 组策略中的最新功能

在 Windows Server 2008 R2 和带有远程服务器管理工具(RSAT)的 Windows 7 中提供以下更改：

- 组策略的 Windows PowerShell Cmdlet：能够从 Windows PowerShell 命令行管理组策略并且能够在登录和启动过程中运行 PowerShell 脚本；
- 组策略首选项：其他类型的首选项；
- Starter 组策略对象：改进了 Starter GPO；
- 管理模板设置：改进了用户界面和其他策略设置。

组策略为操作系统以及操作系统上运行的应用程序的集中配置管理提供了基础结构。

各组人士可能会对下列这些更改感兴趣：

- 必须管理域环境中的用户和计算机的 IT 专业人员；
- 专门的组策略管理员；
- IT 多面手；
- 支持人员。

在接下来的各个小节中，将分别介绍组策略的 Windows PowerShell Cmdlet、组策略首选项、Starter 组策略对象以及管理模板设置。

8.10.1 组策略的 Windows PowerShell Cmdlet

Windows PowerShell 是一种 Windows 命令行界面和脚本语言，可用于自动化许多相同的任务(使用组策略管理控制台(GPMC)在用户界面中执行这些任务)。为了帮助用户执行这些任务，Windows Server 2008 R2 中的组策略提供了 25 多个 cmdlet。每个 cmdlet 都是一个简单的单一功能命令行工具。

可以使用组策略 cmdlet 为基于域的组策略对象(GPO)执行以下任务：

- 维护 GPO：创建、删除、备份和导入 GPO。
- 将 GPO 与 Active Directory(R)容器相关联：创建、更新和删除组策略链接。
- 在 Active Directory 组织单位(OU)和域中设置继承标志和权限。
- 配置基于注册表的策略设置和组策略首选项注册表设置：更新、检索和删除。
- 创建和编辑 Starter GPO。

若要使用 Windows PowerShell 组策略 cmdlet，用户必须在安装了 GPMC 的域控制器或成员服务器上运行 Windows Server 2008 R2，或运行安装了远程服务器管理工具(RSAT)的 Windows 7。RSAT 包含 GPMC 及其 cmdlet。

还必须先使用 Import-Module grouppolicy 命令导入组策略模块，然后在每个使用 cmdlet 的脚本的开头和每个 Windows PowerShell 会话的开始处使用 cmdlet。

可以使用 GPRegistryValue cmdlet 来更改基于注册表的策略设置，并且可以使用 GPPrefRegistryValue cmdlet 来更改注册表首选项。

现在，新增的策略设置能够指定：在用户计算机启动和关机以及用户登录和注销过程中是否在运行非 Windows PowerShell 脚本之前运行 Windows PowerShell 脚本。默认情况下，在运行非 Windows PowerShell 脚本之后运行 Windows PowerShell 脚本。

8.10.2　组策略首选项

可以使用 Windows Server 2008 R2 和带有远程服务器管理工具(RSAT)的 Windows 7 管理以下新类型首选项。针对这些新类型首选项的客户端扩展包含在 Windows Server 2008 R2 和 Windows 7 中：

(1)“电源计划(Windows Vista 和更高版本)”首选项。

(2)“计划任务(Windows Vista 和更高版本)”首选项。

(3)“即时任务(Windows Vista 和更高版本)”首选项。

(4)“Internet Explorer 8”首选项。

使用组策略首选项，可以在无需学习脚本语言的情况下，管理驱动器映射、注册表设置、本地用户和组、服务、文件和文件夹。用户可以使用首选项来减少脚本编辑和所需的自定义系统映像数，实现标准化管理，以及帮助保护网络的安全。使用首选项级别的目标，可以通过减少所需的组策略对象数量来简化桌面管理。

借助添加的新类型首选项，Windows Server 2008 R2 和带有 RSAT 的 Windows 7 改进了多个首选项扩展，从而提供了对电源计划的支持；提供对 Windows 7、Windows Server 2008 和 Windows Vista 的计划任务和即时任务的支持；以及提供对 Windows Internet Explorer 8 的支持。

1.“电源计划(Windows Vista 和更高版本)”首选项

借助添加的“电源计划(Windows Vista 和更高版本)”首选项，Windows Server 2008 R2 和带有 RSAT 的 Windows 7 改进了“电源选项”首选项扩展。

可以使用“电源计划”首选项来配置默认睡眠和显示选项，以便管理计算机的电源消耗、降低电源消耗同时有益于环境。借助“电源计划”首选项，可以让用户对那些默认选项进行更改。尽管也可以使用强制的策略设置来管理电源选项，但是某些用户角色(如移动用户)可能需要拥有自己更改这些设置的灵活性的权力。

“电源计划”首选项的用户界面与“控制面板”的“电源选项”中的高级电源设置的用户界面类似，此相似性使得该功能更易于学习。对于任何其他类型的首选项，可以使用首选项级的目标来限制要将“电源计划”首选项应用到的计算机和用户。

“电源计划”首选项只能用于管理运行 Windows 7、Windows Server 2008 和 Windows

Vista 的计算机的电源消耗。对于运行 Windows XP 或 Windows Server 2003 的计算机，请改用“电源选项(Windows XP)”首选项和“电源方案(Windows XP)”首选项。

2.“计划任务(Windows Vista 和更高版本)”首选项

借助添加的“计划任务(Windows Vista 和更高版本)”首选项，Windows Server 2008 R2 和带有 RSAT 的 Windows 7 改进了“计划任务”首选项扩展。

可以使用“计划任务(Windows Vista 和更高版本)”首选项创建、替换、更新和删除任务及其关联属性。尽管仍可使用“计划任务”首选项为 Windows 7、Windows Server 2008 和 Windows Vista 管理任务，但是“计划任务(Windows Vista 和更高版本)”首选项提供与 Windows 7、Windows Server 2008 和 Windows Vista 中的任务计划程序类似的用户界面，以及它所独有的选项。对于任何其他类型的首选项，可以使用首选项级的目标来限制要将“计划任务”首选项应用到的计算机和用户。

“计划任务(Windows Vista 和更高版本)”首选项只能用于为运行 Windows 7、Windows Server 2008 和 Windows Vista 的计算机管理任务。对于运行 Windows XP 或 Windows Server 2003 的计算机，请更改“计划任务”首选项。

3.“即时任务(Windows Vista 和更高版本)”首选项

借助添加的“即时任务(Windows Vista 和更高版本)”首选项，Windows Server 2008 R2 和带有 RSAT 的 Windows 7 改进了“计划任务”首选项扩展。

可以使用“即时任务(Windows Vista 和更高版本)”首选项创建在刷新组策略之后立即运行(然后将其删除)的任务。以前，Windows Server 2008 和 Windows Vista 并不支持“即时任务”首选项。“即时任务(Windows Vista 和更高版本)”首选项提供与 Windows 7、Windows Server 2008 和 Windows Vista 中的任务计划程序相似的直观用户界面，以及它所独有的选项。对于任何其他类型的首选项，可以使用首选项级的目标来限制要将“即时任务”首选项应用到的计算机和用户。

“即时任务(Windows Vista 和更高版本)”首选项只能用于为运行 Windows 7、Windows Server 2008 和 Windows Vista 的计算机管理任务。对于运行 Windows XP 或 Windows Server 2003 的计算机，请更改“即时任务(Windows XP)”首选项。

4.“Internet Explorer 8”首选项

借助添加的“Internet Explorer 8”首选项，Windows Server 2008 R2 和带有 RSAT 的 Windows 7 改进了“Internet 设置”首选项扩展。

可以使用“Internet Explorer 8”首选项为 Internet Explorer 8 更新 Internet 选项。对于任何其他类型的首选项，可以使用首选项级的目标来限制要将“即时任务”首选项应用到的计算机和用户。

Internet Explorer 8 和 Internet Explorer 7 具有不同的默认设置，因此相应类型的首选项也具有不同的默认设置。

Internet Explorer 8 首选项只能用于为 Internet Explorer 8 管理 Internet 选项。若要为早期版本的 Internet Explorer 管理 Internet 选项，请使用“Internet Explorer 7”首选项或“Internet Explorer 5”和“Internet Explorer 6”首选项。

8.10.3　Starter 组策略对象

在 Windows Server 2008 R2 和带有远程服务器管理工具(RSAT)的 Windows 7 中，提供以下方案的系统 Starter 组策略对象(GPO)：

(1)Windows Vista 企业客户端(EC)；

(2)Windows Vista 专用安全限制功能(SSLF)客户端；

(3)Windows XP Service Pack 2(SP2)EC；

(4)Windows XP SP2 SSLF 客户端。

系统 Starter GPO 为只读 Starter GPO，用于为特定方案提供设置基线。与 Starter GPO 相似，系统 Starter GPO 派生自 GPO，允许用户将一系列管理模板策略设置存储到单个对象中，并且可以进行导入。

系统 Starter GPO 是作为 Windows Server 2008 R2 和带有 RSAT 的 Windows 7 的一部分附带的，不必单独下载和安装。

Windows Server 2008 R2 和带有 RSAT 的 Windows 7 附带的系统 Starter GPO 为 Windows Vista 安全指南或 Windows XP 安全指南中所述的以下方案提供推荐的组策略设置：

(1)为 Windows Vista EC 客户端环境推荐的计算机和用户组策略设置包含在 Windows Vista EC 计算机和 Windows Vista EC 用户系统 Starter GPO 中。

(2)为 Windows Vista SSLF 客户端环境推荐的计算机和用户组策略设置包含在 Windows Vista SSLF 计算机和 Windows Vista SSLF 用户系统 Starter GPO 中。

(3)为 Windows XP SP2 EC 环境推荐的计算机和用户组策略设置包含在 Windows XP SP2 EC 计算机和 Windows XP SP2 EC 用户系统 Starter GPO 中。

(4)为 Windows XP SP2 SSLF 客户端环境推荐的计算机和用户组策略设置包含在 Windows XP SP2 SSLF 计算机和 Windows XP SP2 SSLF 用户系统 Starter GPO 中。

用户不再需要下载系统 Starter GPO，因为它们包含在带有 RSAT 的 Windows Server 2008 R2 和 Windows 7 中。

8.10.4　管理模板设置

在 Windows Server 2008 R2 和带有远程服务器管理工具(RSAT)的 Windows 7 中提供以下更改：

(1)改进的用户界面。

(2)对多字符串注册表和 QWORD 值类型的支持。

管理模板(.ADMX files)是基于注册表的策略设置，显示在“计算机配置”和“用户配置”节点的“管理模板”节点下。当组策略管理控制台读取基于 XML 的管理模板文件时，便会创建此层次结构。

管理模板现在提供一个改进的用户界面，并提供对多字符串(REG_MULTI_SZ)值和 QWORD 注册表类型的支持。

1. 改进的用户界面

在以前版本的 Windows 中，管理模板策略设置的属性对话框包含三个单独的选项卡："设置"(用于启用或禁用策略设置并设置其他选项)、"说明"(用于了解有关策略设置的详细信息)和"注释"(用于输入有关策略设置的可选信息)。在 Windows Server 2008 R2 中，将在属性对话框中的单个位置，而不是在三个单独的选项卡中提供这些选项。此对话框现在可调整大小。

另外，"说明"字段(提供有关策略设置的附加信息)现在称为"帮助"。

通过在单个位置提供配置策略设置所需的所有选项，改进的管理模板用户界面减少了配置策略设置和了解其详细信息所需的管理时间。

2. 对多字符串注册表和 QWORD 值类型的支持

管理模板现在提供对多字符串(REG_MULTI_SZ)值和 QWORD 注册表值类型的支持。

通过使组织能够使用管理模板策略设置管理使用 REG_MULTI_SZ 和 QWORD 注册表值类型的应用程序，以此更改扩展了组策略管理选项。

如果提供对 REG_MULTI_SZ 注册表值类型的支持，便可以在配置管理模板策略设置时执行以下任务：

(1)启用策略设置，输入多行文本以及对条目排序。

(2)编辑现有的已配置设置，以及添加新的行项。

(3)编辑现有的已配置设置，以及编辑各个行项。

(4)编辑现有的已配置设置，选择一个或多个条目以及删除选定条目。这些条目不必连续。

(5)如果提供对 QWORD 注册表值类型的支持，便可以使用管理模板策略设置来管理 64 位应用程序。

8.11 Windows 安全审核功能

在 Windows Server 2008 R2 和 Windows 7 中有许多审核增强功能，这些增强功能可提高安全审核日志中的详细级别并简化审核策略的部署和管理。这些增强功能包括：

(1)全局对象访问审核。在 Windows Server 2008 R2 和 Windows 7 中，管理员可以为文件系统或注册表定义计算机范围系统访问控制列表(SACL)。然后将指定的 SACL 自动应用于该类型的每个对象。这对于验证计算机上的所有关键文件、文件夹以及注册表设置是否受保护以及确定系统资源发生问题的时间，可能非常有用。

(2)"访问原因"报告。此访问控制项(ACE)列表提供的权限用于决定允许还是拒绝访问对象。这对于描述允许或阻止出现特殊可审核事件的权限(如组成员身份)，可能非常有用。

(3)高级审核策略设置。可以使用这 53 个新设置代替"本地策略\审核策略"下的九个基本审核设置，以允许管理员更加明确地以他们要审核的活动类型为目标，去掉了可能使审核日志难于管理和解密的不必要的审核活动。

下面更加详细地介绍这些增强功能。

8.11.1　新增的审核功能有哪些用途

在 Windows XP 中，管理员具有九种类别的安全审核事件，他们可以用于监视成功、失败或者成功和失败。这些事件范围非常广泛并且可以由各种类似操作触发，其中一些可以生成大量事件日志项。

在 Windows Vista(R)和 Windows Server 2008 中，可审核事件的数量从 9 增加到 53，这使得管理员在可审核的事件数量和类型方面更具选择性。但是，与九个基本的 Windows XP 事件不同，这些新的审核事件未与组策略集成，并且只能使用 Auditpol.exe 命令行工具生成的登录脚本进行部署。

在 Windows Server 2008 R2 和 Windows 7 中，所有审核功能都已经与组策略集成。这允许管理员在组策略管理控制台(GPMC)或本地安全策略管理单元中为域、站点或组织单位(OU)配置、部署和管理这些设置。Windows Server 2008 R2 和 Windows 7 更便于 IT 专业人士跟踪网络上进行精确定义的重要活动的时间。

Windows Server 2008 R2 和 Windows 7 中的审核策略增强功能允许管理员连接业务规则和审核策略。例如，在域和 OU 的基础上应用审核策略设置将允许管理员描述规则的遵从性，例如：

- 跟踪服务器上具有财务信息的所有组管理员活动。
- 跟踪已定义的员工组访问的所有文件。
- 确认在访问时将正确的 SACL 应用于每个文件、文件夹和注册表项。

Windows Server 2008 R2 和 Windows 7 中的审核增强功能支持对负责实现、维护和监视组织的物理和信息资产的现行安全的 IT 专业人士的需要。

这些设置可以帮助管理员回答诸如以下内容的问题：

- 谁正在访问我们的资产？
- 他们正在访问哪些资产？
- 他们在何时何地访问这些资产？
- 如何获得访问权限？

安全意识和取证跟踪的期望是这些问题之后的重要动力。越来越多的组织审核员要求并评估该信息的质量。

8.11.2　使用新增审核功能时的注意事项

很多特殊注意事项适用于与 Windows Server 2008 R2 和 Windows 7 中与审核增强功能关联的各种任务：

- 创建审核策略。若要创建高级 Windows 安全审核策略，必须在运行 Windows Server 2008 R2 或 Windows 7 的计算机上使用 GPMC 或本地安全策略管理单元。(安装远程服务器管理工具之后，可以在运行 Windows 7 的计算机上使用 GPMC。)
- 应用审核策略设置。如果使用组策略应用高级审核策略设置和全局对象访问设置，则客户端计算机必须运行 Windows Server 2008 R2 或 Windows 7。此外，只有运行

Windows Server 2008 R2 或 Windows 7 的计算机才能提供“访问原因”报告数据。

• 开发审核策略模型。若要计划高级安全审核设置和全局对象访问设置，必须使用以运行 Windows Server 2008 R2 的域控制器为目标的 GPMC。

• 分发审核策略。开发包含高级安全审核设置的组策略对象(GPO)之后，可以使用运行任何 Windows 服务器操作系统的域控制器对其进行分发。但是，如果无法将运行 Windows 7 的客户端计算机放在单独的 OU 中，则应该使用 Windows Management Instrumentation(WMI)筛选以确保仅将高级策略设置应用于运行 Windows 7 的客户端计算机。

提示：还可以将高级审核策略设置应用于运行 Windows Vista 的客户端计算机。但是，必须使用 Auditpol.exe 登录脚本单独为这些客户端计算机创建和应用审核策略。

注意：将“本地策略/审核策略”下的基本审核策略设置与高级审核策略配置下的高级设置一起使用可能会造成意外的结果。因此，不应该将两组审核策略设置组合使用。如果使用高级审核策略配置设置，则应该启用“本地策略/安全选项”下的“审核：强制审核策略子类别设置(Windows Vista 或更高版本)替代审核策略类别设置”策略设置。这将通过强制忽略基本安全审核来防止类似设置之间的冲突。

此外，若要计划和部署安全事件审核策略，管理员需要解决很多操作和战略问题，包括：

• 为什么需要审核策略？

• 哪些活动和事件对于组织最重要？

• 可以从审核策略中忽略哪些类型的审核事件？

• 希望占用管理员多少时间和网络资源来生成、收集和存储事件以及分析数据？

8.11.3 详解新增的审核功能

可以处理组策略的所有版本的 Windows Server 2008 R2 和 Windows 7 都可以配置使用这些安全审核增强功能。无法加入域的 Windows Server 2008 R2 和 Windows 7 版本无法访问这些功能。32 位和 64 位版本的 Windows 7 之间的安全审核支持没有任何差别。

Windows Server 2008 R2 和 Windows 7 提供了以下新功能：全局对象访问审核、“访问原因”设置以及高级审核策略设置，下面讲解一下。

1. 全局对象访问审核

使用全局对象访问审核，管理员可以为文件系统或注册表定义每种对象类型的计算机 SACL。然后将指定的 SACL 自动应用于该类型的每个对象。

审核员将能够通过只查看全局对象访问审核策略设置的内容来证实系统中的每个资源受审核策略的保护。例如，策略设置“跟踪组管理员所进行的所有更改”将足以表明该策略有效。

资源 SACL 对于诊断方案也非常有用。例如，将全局对象访问审核策略设置为记录特定用户的所有活动以及在资源(文件系统或注册表)中启用“访问失败”审核策略将帮助管理员快速确定系统中的哪些对象拒绝用户访问。

注意：如果在计算机上配置了文件或文件夹 SACL 和全局对象访问审核策略(或者

单个注册表设置 SACL 和全局对象访问审核策略),则有效的 SACL 源于将文件或文件夹 SACL 和全局对象访问审核策略组合。这意味着如果活动与文件或文件夹 SACL 或者全局对象访问审核策略匹配,则会生成一个审核事件。

2.“访问原因”设置

Windows 中有多个事件,无论操作成功还是失败都会进行审核。这些事件通常包括用户、对象和操作,但它们缺少允许或拒绝该操作的原因。通过记录原因、基于的特定权限以及某个人访问企业资源的原因,在 Windows Server 2008 R2 和 Windows 7 中改进了取证分析和支持方案。

3. 高级审核策略设置

在 Windows Server 2008 R2 和 Windows 7 中,可以使用域组策略配置和部署增强的审核策略,这样将降低管理成本和开销,并极大地提高了安全审核的灵活性和效率。

以下部分介绍组策略的高级审核策略配置节点中可用的新事件及事件类别。

(1)账户登录事件

此类别中的事件帮助文档域尝试对账户数据、域控制器或本地安全账户管理器(SAM)进行身份验证。与登录和注销事件(它们跟踪访问特殊计算机的尝试)不同,此类别中的事件报告正在使用的账户数据库,见表 8-1。

表 8-1　　账户登录事件的设置选项

设置	描述
凭据验证	审核由对用户账户登录凭据的验证测试生成的事件
Kerberos 服务票证操作	审核 Kerberos 服务票证请求生成的事件
其他账户登录事件	审核由响应为用户账户登录提交的凭据请求(非凭据验证或 Kerberos 票证)生成的事件
Kerberos 身份验证服务	审核由 Kerberos 身份验证票证授予票证(TGT)请求生成的事件

(2)账户管理事件

可以使用此类别中的设置监视对用户和计算机账户和组的更改,见表 8-2。

表 8-2　　账户管理事件的设置选项

设置	描述
用户账户管理	审核对用户账户的更改
计算机账户管理	审核由对计算机账户的更改(如当创建、更改或删除计算机账户时)生成的事件
安全组管理	审核由对安全组的更改生成的事件
分发组管理	审核由对分发组的更改生成的事件
应用程序组管理	审核由对应用程序组的更改生成的事件
其他账户管理事件	审核由此类别中不涉及的其他用户账户更改生成的事件

(3)详细跟踪事件

可以使用详细跟踪的事件监视各个应用程序的活动,以了解计算机的使用方式以及该计算机上用户的活动,见表 8-3。

表 8-3 详细跟踪事件的设置选项

设置	描述
进程创建	审核当创建或启动进程时生成的事件。还要审核创建该进程的应用程序或用户的名称
进程终止	审核当进程结束时生成的事件
DPAPI 活动	审核当对数据保护应用程序接口(DPAPI)进行加密或解密请求时生成的事件。DPAPI 用来保护机密信息,如存储的密码和密钥信息
RPC 事件	审核入站远程过程调用(RPC)连接

(4)DS 访问事件

DS 访问事件提供对访问和修改 Active Directory(R)域服务(AD DS)中对象的尝试进行较低级别的审核跟踪。仅在域控制器上记录这些事件,见表 8-4。

表 8-4 DS 访问事件的设置选项

设置	描述
目录服务访问	审核当访问 AD DS 对象时生成的事件,但仅记录具有匹配的 SACL 的 AD DS 对象。此子类别中的事件与以前版本的 Windows 中可用的目录服务访问事件类似
目录服务更改	审核由对 AD DS 对象的更改生成的事件。当创建、删除、修改、移动或恢复对象时记录事件
目录服务复制	审核两个 AD DS 域控制器之间的复制
详细的目录服务复制	审核由域控制器之间详细的 AD DS 复制生成的事件

(5)登录/注销事件

使用登录和注销事件可以跟踪以交互方式登录计算机或通过网络登录计算机的尝试。这些事件对于跟踪用户活动以及标识网络资源上的潜在攻击尤其有用,见表 8-5。

表 8-5 登录/注销事件的设置选项

设置	描述
登录	审核由用户账户在计算机上的登录尝试生成的事件
注销	审核由关闭登录会话生成的事件。这些事件发生在所访问的计算机上。对于交互登录,在用户账户登录的计算机上生成安全审核事件
账户锁定	审核由登录锁定账户的失败尝试生成的事件
IPSec 主模式	审核在主模式协商期间由 Internet 密钥交换协议(IKE)和已验证 Internet 协议(AuthIP)生成的事件
IPSec 快速模式	审核在快速模式协商期间由 Internet 密钥交换协议(IKE)和已验证 Internet 协议(AuthIP)生成的事件
IPSec 扩展模式	审核在扩展模式协商期间由 Internet 密钥交换协议(IKE)和已验证 Internet 协议(AuthIP)生成的事件
特殊登录	审核由特殊登录生成的事件
其他登录/注销事件	审核与“登录/注销”类别中不包含的登录和注销有关的其他事件
网络策略服务器	审核由 RADIUS(IAS)和网络访问保护(NAP)用户访问请求生成的事件。这些请求可以是授予、拒绝、放弃、隔离、锁定和解锁

(6)对象访问事件

使用对象访问事件可以跟踪网络或计算机上访问特定对象或对象类型的尝试,见表 8-6。若要审核文件、目录、注册表项或任何其他对象,必须为成功和失败事件启用“对象访问”类别。例如,审核文件操作需要启用“文件系统”子类别,审核注册表访问需要启用“注册表”子类别。

证明该策略对于外部审核员有效非常困难。没有简单的方法验证在所有继承的对象上是否设置了正确的 SACL。

表 8-6　　对象访问事件的设置选项

设置	描述
文件系统	审核用户访问文件系统对象的尝试。仅对于具有 SACL 的对象,并且仅当请求的访问类型(如写入、读取或修改)以及进行请求的账户与 SACL 中的设置匹配时才生成安全审核事件
注册表	审核访问注册表对象的尝试。仅对于具有 SACL 的对象,并且仅当请求的访问类型(如读取、写入或修改)以及进行请求的账户与 SACL 中的设置匹配时才生成安全审核事件
内核对象	审核访问系统内核(包括 Mutexes 和 Semaphores)的尝试。只有具有匹配的 SACL 的内核对象才生成安全审核事件。审核:对全局系统对象的访问进行审核策略设置控制内核对象的默认 SACL
SAM	审核由访问安全账户管理器(SAM)对象的尝试生成的事件
证书服务	审核 Active Directory 证书服务(AD CS)操作
生成的应用程序	审核通过使用 Windows 审核应用程序编程接口(API)生成事件的应用程序。设计为使用 Windows 审核 API 的应用程序使用此子类别记录与其功能有关的审核事件
句柄操作	审核当打开或关闭对象句柄时生成的事件。只有具有匹配的 SACL 的对象才生成安全审核事件
文件共享	审核访问共享文件夹的尝试。但是,当创建、删除文件夹或更改其共享权限时不生成任何安全审核事件
详细的文件共享	审核访问共享文件夹上文件和文件夹的尝试。“详细的文件共享”设置在每次访问文件或文件夹时记录一个事件,而“文件共享”设置仅为客户端和文件共享之间建立的任何连接记录一个事件。“详细的文件共享”审核事件包括有关用来授予或拒绝访问的权限或其他条件的详细信息的事件
筛选平台数据包丢弃	审核由 Windows 筛选平台(WFP)丢弃的数据包
筛选平台连接	审核 WFP 允许或阻止的连接
其他对象访问事件	审核由管理任务计划程序作业或 COM+对象生成的事件

(7)策略更改事件

使用策略更改事件可以跟踪对本地系统或网络上重要安全策略的更改,见表 8-7。由于策略通常是由管理员建立的,用于确保网络资源的安全,因此任何更改或更改这些策略的尝试都可能是网络安全管理的重要方面。

表 8-7 策略更改事件的设置选项

设置	描述
审核策略更改	审核安全审核策略设置的更改
身份验证策略更改	审核由对身份验证策略的更改生成的事件
授权策略更改	审核由对授权策略的更改生成的事件
MPSSVC 规则级别策略更改	审核由 Windows 防火墙使用的策略规则的更改生成的事件
筛选平台策略更改	审核由对 WFP 的更改生成的事件
其他策略更改事件	审核由策略更改类别中不审核的其他安全策略更改生成的事件

(8)权限使用事件

为用户或计算机授予对网络的权限以完成定义的任务,见表 8-8。有了权限使用事件可以跟踪一台或多台计算机上某些权限的使用。

表 8-8 权限使用事件

设置	描述
敏感权限使用	审核由使用敏感权限(用户权限)生成的事件,如充当操作系统的一部分、备份文件和目录、模拟客户端计算机或生成安全审核
非敏感权限使用	审核由使用非敏感权限(用户权限)生成的事件,如本地登录或使用远程桌面连接登录、更改系统时间或从扩展坞删除计算机
其他权限使用事件	未使用

(9)系统事件

使用系统事件可以跟踪对其他类别中不包含且有潜在安全隐患的计算机的高级更改,见表 8-9。

表 8-9 系统事件的设置选项

设置	描述
安全状态更改	审核由计算机安全状态更改生成的事件
安全系统扩展	审核与安全系统扩展或服务有关的事件
系统完整性	审核违反安全子系统的完整性的事件
IPSec 驱动程序	审核由 IPsec 筛选器驱动程序生成的事件
其他系统事件	审核以下任何事件: ①启动和关闭 Windows 防火墙 ②由 Windows 防火墙处理的安全策略 ③加密密钥文件和迁移操作