Microsoft®

Windows Server 2008 活动目录服务的实现与管理

微软公司 著

人民邮电出版社
POSTS & TELECOM PRESS

CD-ROM

Windows Server 2008 活动目录服务的实现与管理

微软公司 著

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

Windows Server 2008活动目录服务的实现与管理 /
微软公司著. -- 北京 : 人民邮电出版社, 2011.2 (2014.6重印)
ISBN 978-7-115-22567-2

Ⅰ. ①W… Ⅱ. ①微… Ⅲ. ①服务器－操作系统（软
件）, Windows Server 2008 Ⅳ. ①TP316.86

中国版本图书馆CIP数据核字(2010)第049634号

版 权 声 明

内 容 提 要

本教材主要讲解 Windows Server 2008 Active Directory 域服务与身份和访问解决方案的配置、故障排除等相关内容。

教材共 20 章，内容覆盖了 Active Directoy 域服务、Active Directory 证书服务、Active Directory 轻型目录服务、Active Directory 联合身份验证服务、Active Directory Rights Management Services 服务的实现与管理。读者按照项目次序循序渐进地学习，并配合实战训练，可以掌握相关知识和技能。

本教材主要面向掌握 Windows Server 2008 网络基础结构、活动目录服务基础知识，希望对 Active Directory 相关服务深入了解和提高的读者。

Windows Server 2008 活动目录服务的实现与管理

◆ 著　　微软公司
责任编辑　刘　浩
◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京铭成印刷有限公司印刷
◆ 开本：787×1092　1/16
印张：29　　2011 年 2 月第 1 版
字数：693 千字　　2014 年 6 月北京第 2 次印刷

ISBN 978-7-115-22567-2

定价：85.00 元（附光盘）

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

编审委员和组织策划 林元宏　王　林　田本和　蒋　斌
李朝晖

技术编审 蒋　斌　张　宪　李家存　望正茂　宫　丽
张博成

前　言

Active Directory 是微软的目录服务产品。在 Windows Server 2008 中，Active Directory 服务的功能得到了增强，包括 Active Directory 域服务、Active Directory 轻型目录服务、Active Directory 证书服务、Active Directory Rights Management Services、Active Directory 联合身份验证服务。这些服务都是基于活动目录实现的。本书将着重介绍这 5 个服务及其应用，帮助读者系统学习这些服务并加以实践。

通过本课程的学习，读者能够：

- 实施 AD DS；
- 为 AD DS 配置 DNS；
- 配置 Active Directory 对象和信任；
- 配置 Active Directory 站点和复制；
- 创建和配置组策略；
- 使用组策略配置用户环境；
- 使用组策略实施安全性；
- 实施 AD DS 监视计划；
- 实施 AD DS 维护计划；
- 排除 Active Directory 域服务、域名服务和复制问题的故障；
- 排除组策略问题的故障；
- 实施 AD DS 基础结构；
- 探究 IDA 解决方案；
- 配置 Active Directory 证书服务（AD CS）；
- 部署和管理证书；
- 配置 Active Directory 轻型目录服务（AD LDS）；
- 配置 Active Directory 联合身份验证服务（AD FS）；
- 配置 Active Directory Rights Management Services（AD RMS）；
- 维护访问管理解决方案；
- IDA 解决方案故障排除。

本书适用对象

本书主要面向希望了解以下内容的读者：如何在分布式环境中实施 Active Directory、如何使用组策略保护域的安全、如何执行备份和还原，如何监视和排查 Active Directory 配置故障以确保其无故障运转，以及如何在 Windows Server 2008 中配置身份认证和访问（IDA）管理解决方案。

在学习本教材前，读者需要具备下列知识和技能。

- 对网络有基本了解。例如，TCP/IP 的工作方式、编址、DNS、WINS 和连接方法（有线、无线、VPN）。
- 对操作系统有一定了解。例如，Windows 2000、Windows XP、Windows Server 2003 等，以及 Windows Vista 操作系统客户端（建议具备）。
- 了解安全的最佳做法。例如，文件系统权限、身份验证方法、工作站和服务器加固方法等。
- 对服务器硬件的基本知识有所了解。
- 具备在 Active Directory 中创建和管理对象及权限的经验。
- 对 Windows Server 环境中备份和恢复的基本概念有所了解。例如，备份类型、备份方法、备份拓扑等。

本书结构

本书共分为 20 章，内容分为两大部分。

第一部分内容为 Windows Server 2008 Active Directory 域服务的配置与故障排除。章节内容包含第 1 章到第 12 章。

第 1 章　“实施 Active Directory 域服务”讨论实施 AD DS 所需的必备硬件和软件，并介绍了 AD DS 的安装过程和只读域控制器（RODC）及其安装过程。

第 2 章　“为 Active Directory 域服务配置域名服务”介绍特定于 AD DS 的 DNS 配置。

第 3 章　“配置 Active Directory 对象和信任”讨论如何实施和配置 AD DS 对象和信任。

第 4 章　“配置 Active Directory 域服务站点和复制”介绍如何创建和配置站点来管理复制。

第 5 章　“创建和配置组策略”介绍组策略对象（GPO）的工作方式以及如何创建和应用 GPO。

第 6 章　“使用组策略配置用户环境”讨论如何使用组策略配置用户桌面设置。

第 7 章　“使用组策略实施安全性”描述如何配置安全设置并使用 GPO 应用安全设置。

第 8 章　“实施 Active Directory 域服务监视计划”描述如何监视 AD DS 基础结构和服务。

第 9 章　“实施 Active Directory 域服务维护计划”讨论如何执行 Active Directory 服务器和对象的维护、备份和恢复。

第 10 章　“Active Directory 域服务、域名服务和复制问题的故障排除”介绍如何排查并解决与 AD DS、DNS 和复制相关的问题。

第 11 章　“组策略问题的故障排除”描述如何排查并解决与组策略相关的问题。

第 12 章　“实施 Active Directory 域服务基础结构”为实验，此章提供的场景可以帮助读者了解如何创建解决方案。

第二部分内容为 Windows Server 2008 Active Directory 身份和访问解决方案的配置与故障排除。章节内容包含第 13 章到第 20 章。

第 13 章　“探究 IDA 解决方案”介绍身份认证和访问管理（IDA 管理）解决方案。读者将学会识别 IDA 管理中的 Active Directory 服务器角色。这一章还将描述 Identity Lifecycle

Manager（ILM）的概念。

第 14 章　“配置 AD CS”说明公钥基础结构（PKI）的概念。读者还将学习部署证书颁发机构（CA）层次结构，以及安装 AD CS。最后，这一章描述如何配置 AD CS。

第 15 章　“部署和管理证书”描述了如何使用 AD CS 部署证书。此外，这一章详细描述了使用自动注册部署证书、证书吊销以及证书模板和证书恢复的配置。

第 16 章　“配置 AD LDS”详细说明如何安装 AD LDS，以及如何配置 AD LDS、AD LDS 实例、AD LDS 复制以及 AD LDS 与 AD DS 的集成。

第 17 章　“配置 AD FS”提供 AD FS 的概念及其部署方案。该章还描述了如何部署 AD FS 和实施 AD FS 声明。

第 18 章　“配置 AD RMS”说明 AD RMS 的概念。该章描述如何安装和配置 AD RMS 服务器组件。该章还说明了 AD RMS 的管理以及 AD RMS 信任策略的实施。

第 19 章　“维护访问管理解决方案”说明了 AD CS、AD LDS、AD FS 和 AD RMS 的维护。

第 20 章　“IDA 解决方案故障排除”描述如何排查 AD CS、AD LDS、AD FS 和 AD RMS 的故障。

教学参考资料

获得微软授权使用该教材进行教学的教师，除了可以获得上述材料外，还可以从微软公司获得如下教学资料。

教参	章节教参与教学大纲
实验答案	实验的具体操作步骤
虚拟机	配置好的虚拟机实验环境，用于进行实验和课堂演示
实验室安装指南	包括在实验室部署虚拟机的指南
PowerPoint	用于进行课堂演示

虚拟机

本书案例提供的虚拟机实验均采用微软的 Lab Launcher 进行操作，它是一种虚拟机操作界面，能让用户用一种更简易的操作界面进行虚拟机操作。该工具基于 Virtual Server R2 SP1 实现。虚拟机安装完毕后，用户即可在此界面进行操作。操作界面参见图 0-1。

虚拟机的运行环境要求如下。

- 操作系统为 Windows XP 简体中文版或 Windows Vista 简体中文版。
- 系统中安装.NET Framework 2.0 简体中文版。
- 系统中安装 Microsoft Virtual Server 2005 R2 简体中文版。
- 2GB 物理内存。

本课程一共包含两套虚拟机，分别对应不同的内容。

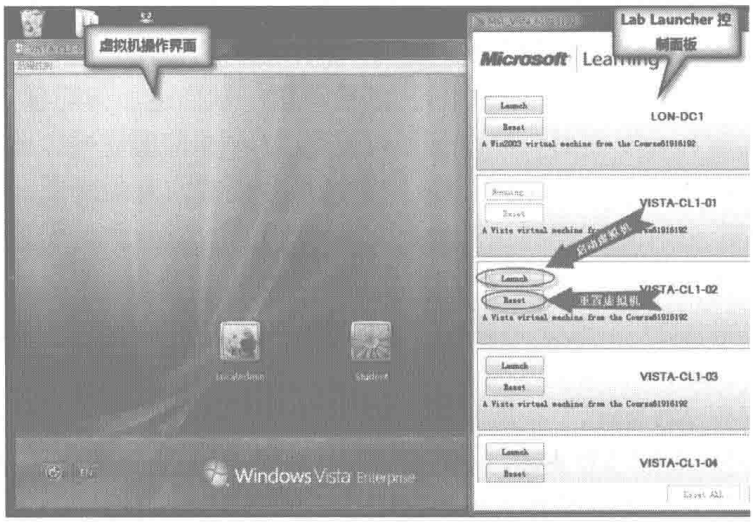

图 0-1　虚拟机操作界面

课程第一部分第 1～12 章，讲述的是 Windows Server 2008 Active Directory 域服务的配置与故障排除，所用的虚拟机如表 0-1 所示。

表 0-1　　第 1～12 章虚拟机

虚　拟　机	角　　色
10078A-NYC-DC1	WoodgroveBank.com 域中的域控制器
10078A-NYC-DC2	WoodgroveBank.com 域中的域控制器
10078A-MIA-RODC	在 Windows Server 2008 服务器核心上运行的只读域控制器
10078A-NYC-SVR1	独立服务器
10078A-NYC-SVR2	Windows Server 2008 服务器核心计算机
10078A-NYC-CL1	WoodgroveBank.com 域中的 Windows Vista 计算机
10078A-NYC-RAS	WoodgroveBank.com 域中的成员服务器
10078A-LON-DC1	EMEA.WoodgroveBank.com 域中的域控制器
10078A-VAN-DC1	Fabrikam.com 域中的 Windows Server 2003 域控制器

课程第二部分第 13～20 章，讲述的是 Windows Server 2008 Active Directory 身份和访问解决方案的配置与故障排除，所用的虚拟机如表 0-2 所示。

表 0-2　　第 13～20 章虚拟机

虚　拟　机	角　　色
10079A-CHI-DC1	Northwind Traders 域的域控制器
10079A-NYC-CL1	Woodgrove Bank 客户端
10079A-NYC-DC1 10079A-NYC-DC1-B	Woodgrove Bank 域控制器
10079A-NYC-SVR1	Woodgrove Bank 成员服务器

两套虚拟机的安装参见相关虚拟机安装文档。

目　录