

秉承作者一贯理论兼实践的写作风格，深获读者信赖

Windows Server 2016 Active Directory配置指南

十几年磨一剑 畅销书第8次升级

系统配置、微软认证考试，一次搞定

本套书的宗旨是希望能够让读者通过实际应用操作来充分理解Windows Server 2016，进而轻松管理Windows Server 2016的网络环境。书中不但理论阐述清晰，且范例丰富。对需要参加微软认证考试的读者来说，本书更是不可或缺的实用参考手册。

循序渐进地介绍Active Directory域服务（AD DS）的基本概念：从域基本概念、域树状目录、域树、站点、域与林功能等级到目录分区，使读者有基本的认识。

独家讲述实用的Active Directory域服务（AD DS）配置专题。

按部就班地介绍如何配置“Server Core服务器”与“Nano服务器”，让您很容易建立一个更安全的、管理负担更低的运行环境。

深入探讨组策略的关键问题，包括组策略的运行、账户策略、自动报告指令码、首选项设置、文件夹重定向、WMI筛选器、组策略模型、组策略结果、入门GPO等。

涵盖经典且实用的专题，包括限制用户运行软件、限制访问可移动存储设备、管理用户工作环境、管理客户端计算机环境、一次同时添加多个用户账户等。

身为IT人员必备的知识与技能，包括：操作主机的管理、AD DS的备份与恢复、Active Directory资源回收站、AD DS数据库的维护与优化、通过AD DS公布资源、AD DS数据库的复制、站点的配置与管理、AD DS与防火墙等。

- 完整详细地说明域环境的配置，包括域树、域树状目录、域、子域、域控制器、只读域控制器（RODC）、RODC阶段式安装、域升级、自动安装域控制器、加入域、脱机加入域与脱离域等。

- 软件部署的完整介绍，包含软件发布、软件分配、软件升级、自动修复部署的软件、Adobe Acrobat的部署、软件重新包装等，让系统管理员更容易管理客户端所需的软件。

- 介绍如何建立信任关系，包含快捷方式信任、林信任、外部信任等，让大型网络之间沟通更加容易和有效。

- 采用Windows Server 2016 Hyper-V的虚拟环境，因此只要一台电脑就可以建立完整的学习环境。

- 作者以多年的实践经验，详细列举实际操作时的心得和技巧，引导您部署稳定的AD DS运行环境。

清华社官方微信号



扫 我 有 惊 喜

ISBN 978-7-302-51796-2



9 787302 517962 >

定价：89.00元

[General Information]

书名=Windows Server 2016 Active Directory配置指南

页数=398

SS号=14567602

封面
书名
版权
前言
目录

第1章 Active Directory域服务 (AD DS)

- 1.1 Active Directory域服务概述
 - 1.1.1 Active Directory域服务的适用范围 (Scope)
 - 1.1.2 名称空间 (Namespace)
 - 1.1.3 对象 (Object) 与属性 (Attribute)
 - 1.1.4 容器 (Container) 与组织单位 (Organization Units ,

OU)

- 1.1.5 域树 (Domain Tree)
 - 1.1.6 信任 (Trust)
 - 1.1.7 林 (Forest)
 - 1.1.8 架构 (Schema)
 - 1.1.9 域控制器 (Domain Controller)
 - 1.1.10 只读域控制器 (RODC)
 - 1.1.11 可重启的AD DS (Restartable AD DS)
 - 1.1.12 Active Directory回收站
 - 1.1.13 ADDS的复制模式
 - 1.1.14 域中的其他成员计算机
 - 1.1.15 DNS服务器
 - 1.1.16 轻型目录访问协议 (LDAP)
 - 1.1.17 全局编录 (Global Catalog)
 - 1.1.18 站点 (Site)
 - 1.1.19 目录分区 (Directory Partition)
- 1.2 域功能级别与林功能级别
 - 1.2.1 域功能级别 (Domain Functionality Level)
 - 1.2.2 林功能级别 (Forest Functionality Level)
- 1.3 Active Directory轻型目录服务

第2章 建立AD DS域

- 2.1 建立AD DS域前的准备工作
 - 2.1.1 选择适当的DNS域名
 - 2.1.2 准备好一台支持AD DS的DNS服务器
 - 2.1.3 选择AD DS数据库的存储位置
- 2.2 建立AD DS域
- 2.3 确认AD DS域是否正常
 - 2.3.1 检查DNS服务器内的记录是否完备
 - 2.3.2 排除注册失败的问题
 - 2.3.3 检查AD DS数据库文件与SYSVOL文件夹

- 2.3.4 新增的管理工具
 - 2.3.5 查看事件日志文件
 - 2.4 提升域与林功能级别
 - 2.5 新建额外域控制器与RODC
 - 2.5.1 安装额外域控制器
 - 2.5.2 利用安装媒体来安装额外域控制器
 - 2.5.3 更改RODC的委派与密码复制策略设置
 - 2.6 RODC阶段式安装
 - 2.6.1 建立RODC账户
 - 2.6.2 将服务器附加到RODC账户
 - 2.7 将Windows计算机加入或脱离域
 - 2.7.1 将Windows计算机加入域
 - 2.7.2 利用已加入域的计算机登录
 - 2.7.3 脱机加入域
 - 2.7.4 脱离域
 - 2.8 在域成员计算机内安装AD DS管理工具
 - 2.9 删除域控制器与域
- 第3章 域用户与组账户的管理
- 3.1 管理域用户账户
 - 3.1.1 创建组织单位与域用户账户
 - 3.1.2 用户登录账户
 - 3.1.3 创建UPN后缀
 - 3.1.4 账户的常规管理工作
 - 3.1.5 域用户账户的属性设置
 - 3.1.6 搜索用户账户
 - 3.1.7 域控制器之间数据的复制
 - 3.2 一次同时新建多个用户账户
 - 3.2.1 利用csvde.exe来新建用户账户
 - 3.2.2 利用ldifde.exe来新建、修改与删除用户账户
 - 3.2.3 利用dsadd.exe等程序添加、修改与删除用户账户
 - 3.3 域组账户
 - 3.3.1 域内的组类型
 - 3.3.2 组的作用域
 - 3.3.3 域组的创建与管理
 - 3.3.4 AD DS内置的组
 - 3.3.5 特殊组账户
 - 3.4 组的使用原则
 - 3.4.1 A、G、DL、P原则
 - 3.4.2 A、G、G、DL、P原则
 - 3.4.3 A、G、U、DL、P原则
 - 3.4.4 A、G、G、U、DL、P原则

第4章 利用组策略管理用户工作环境

4.1 组策略概述

4.1.1 组策略的功能

4.1.2 组策略对象

4.1.3 策略设置与首选项设置

4.1.4 组策略的应用时机

4.2 策略设置实例演练

4.2.1 策略设置实例演练一：计算机配置

4.2.2 策略设置实例演练二：用户配置

4.3 首选项设置实例演练

4.3.1 首选项设置实例演练一

4.3.2 首选项设置实例演练二

4.4 组策略的处理规则

4.4.1 一般的继承与处理规则

4.4.2 例外的继承设置

4.4.3 特殊的处理设置

4.4.4 更改管理GPO的域控制器

4.4.5 更改组策略的应用间隔时间

4.5 利用组策略来管理计算机与用户环境

4.5.1 计算机配置的管理模板策略

4.5.2 用户配置的管理模板策略

4.5.3 账户策略

4.5.4 用户权限分配策略

4.5.5 安全选项策略

4.5.6 登录/注销、启动/关机脚本

4.5.7 文件夹重定向

4.6 利用组策略限制访问可移动存储设备

4.7 WMI筛选器

4.8 组策略建模与组策略结果

4.9 组策略的委派管理

4.9.1 站点、域或组织单位的GPO链接委派

4.9.2 编辑GPO的委派

4.9.3 新建GPO的委派

4.10 StarterGPO的设置与使用

第5章 利用组策略部署软件

5.1 软件部署概述

5.1.1 将软件分配给用户

5.1.2 将软件分配给计算机

5.1.3 将软件发布给用户

5.1.4 自动修复软件

5.1.5 删除软件

- 5.2 将软件发布给用户
 - 5.2.1 发布软件
 - 5.2.2 客户端安装被发布的软件
 - 5.2.3 测试自动修复软件的功能
 - 5.2.4 取消已发布的软件
- 5.3 将软件分配给用户或计算机
 - 5.3.1 分配给用户
 - 5.3.2 分配给计算机
- 5.4 将软件升级
- 5.5 部署Adobe Acrobat
 - 5.5.1 部署基础版
 - 5.5.2 部署更新程序
- 第6章 限制软件的运行
 - 6.1 软件限制策略概述
 - 6.1.1 哈希规则
 - 6.1.2 证书规则
 - 6.1.3 路径规则
 - 6.1.4 网络区域规则
 - 6.1.5 规则的优先级
 - 6.2 启用软件限制策略
 - 6.2.1 建立哈希规则
 - 6.2.2 建立路径规则
 - 6.2.3 建立证书规则
 - 6.2.4 建立网络区域规则
 - 6.2.5 不要将软件限制策略应用到本地系统管理员
- 第7章 建立域树与林
 - 7.1 建立第一个域
 - 7.2 建立子域
 - 7.3 建立林中的第二个域树
 - 7.3.1 选择适当的DNS架构
 - 7.3.2 建立第二个域树
 - 7.4 删除子域与域树
 - 7.5 更改域控制器的计算机名称
- 第8章 管理域与林信任
 - 8.1 域与林信任概述
 - 8.1.1 信任域与受信任域
 - 8.1.2 跨域访问资源的流程
 - 8.1.3 信任的种类
 - 8.1.4 建立信任前的注意事项
 - 8.2 建立快捷方式信任
 - 8.3 建立林信任

- 8.3.1 建立林信任前的注意事项
 - 8.3.2 开始建立林信任
 - 8.3.3 选择性身份验证设置
- 8.4 建立外部信任
- 8.5 管理与删除信任
 - 8.5.1 信任的管理
 - 8.5.2 信任的删除
- 第9章 AD DS数据库的复制
 - 9.1 站点与AD DS数据库的复制
 - 9.1.1 同一个站点之间的复制
 - 9.1.2 不同站点之间的复制
 - 9.1.3 目录分区与复制拓扑
 - 9.1.4 复制通信协议
 - 9.2 默认站点的管理
 - 9.2.1 默认的站点
 - 9.2.2 Servers文件夹与复制设置
 - 9.3 利用站点来管理AD DS复制
 - 9.3.1 建立站点与子网
 - 9.3.2 建立站点链接
 - 9.3.3 将域控制器移动到所属的站点
 - 9.3.4 指定首选的bridgehead服务器
 - 9.3.5 站点链接与AD DS数据库的复制设置
 - 9.3.6 站点链接桥
 - 9.3.7 站点链接桥的两个范例讨论
 - 9.4 管理全局编录服务器
 - 9.4.1 向全局编录内添加属性
 - 9.4.2 全局编录的功能
 - 9.4.3 通用组成员缓存
 - 9.5 解决AD DS复制冲突的问题
 - 9.5.1 属性标记
 - 9.5.2 冲突的种类
- 第10章 操作主机的管理
 - 10.1 操作主机概述
 - 10.1.1 架构操作主机
 - 10.1.2 域命名操作主机
 - 10.1.3 RID操作主机
 - 10.1.4 PDC模拟器操作主机
 - 10.1.5 基础结构操作主机
 - 10.2 操作主机的放置优化
 - 10.2.1 基础结构操作主机的放置
 - 10.2.2 PDC模拟器操作主机的放置

- 10.2.3 林级别操作主机的放置
 - 10.2.4 域级别操作主机的放置
- 10.3 找出扮演操作主机角色的域控制器
 - 10.3.1 利用管理控制台找出扮演操作主机的域控制器
 - 10.3.2 利用命令找出扮演操作主机的域控制器
- 10.4 转移操作主机角色
 - 10.4.1 利用管理控制台
 - 10.4.2 利用Windows PowerShell命令
- 10.5 夺取操作主机角色
 - 10.5.1 操作主机停摆所造成的影响
 - 10.5.2 夺取操作主机角色实例演练
- 第11章 AD DS的维护
 - 11.1 系统状态概述
 - 11.1.1 ADDS数据库
 - 11.1.2 SYSVOL文件夹
 - 11.2 备份AD DS
 - 11.2.1 安装Windows Server Backup功能
 - 11.2.2 备份系统状态
 - 11.3 还原AD DS
 - 11.3.1 进入目录服务修复模式的方法
 - 11.3.2 执行AD DS的非授权还原
 - 11.3.3 针对被删除的AD DS对象执行授权还原
 - 11.4 AD DS数据库的移动与整理
 - 11.4.1 可重新启动的ADDS (Restartable ADDS)
 - 11.4.2 移动AD DS数据库文件
 - 11.4.3 重整AD DS数据库
 - 11.5 重置“目录服务修复模式”的系统管理员密码
 - 11.6 更改可重新启动的AD DS的登录设置
 - 11.7 Active Directory回收站
- 第12章 将资源发布到AD DS
 - 12.1 将共享文件夹发布到AD DS
 - 12.1.1 利用Active Directory用户和计算机控制台
 - 12.1.2 利用计算机管理控制台
 - 12.2 查找AD DS内的资源
 - 12.2.1 通过网络
 - 12.2.2 通过Active Directory用户和计算机控制台
 - 12.3 将共享打印机发布到AD DS
 - 12.3.1 发布打印机
 - 12.3.2 通过AD DS查找共享打印机
 - 12.3.3 利用打印机位置来查找打印机
- 第13章 自动信任根CA

13.1 自动信任CA的设置准则

13.2 自动信任内部的独立CA

13.2.1 下载独立根CA的证书并保存

13.2.2 将CA证书导入到受信任的根证书颁发机构

13.3 自动信任外部的CA

13.3.1 下载独立根CA的证书并保存

13.3.2 建立证书信任列表（CTL）

附录A ADDS与防火墙

A.1 AD DS相关的端口

A.1.1 将客户端计算机加入域、用户登录时会用到的端口

A.1.2 计算机登录时会用到的端口

A.1.3 建立域信任时会用到的端口

A.1.4 验证域信任时会用到的端口

A.1.5 访问文件资源时会用到的端口

A.1.6 执行DNS查询时会用到的端口

A.1.7 执行AD DS数据库复制时会用到的端口

A.1.8 文件复制服务（FRS）会用到的端口

A.1.9 分布式文件系统（DFS）会用到的端口

A.1.10 其他可能需要开放的端口

A.2 限制动态RPC端口的使用范围

A.2.1 限制所有服务的动态RPC端口范围

A.2.2 限制AD DS数据库复制使用指定的静态端口

A.2.3 限制FRS使用指定的静态端口

A.2.4 限制DFS使用指定的静态端口

A.3 IPSec与VPN端口

A.3.1 IPSec所使用的通信协议与端口

A.3.2 PPTP VPN所使用的通信协议与端口

A.3.3 L2TP/IPSec所使用的通信协议与端口

附录B Server Core与Nano服务器

B.1 Server Core服务器概述

B.2 Server Core服务器的基本设置

B.2.1 更改计算机名称

B.2.2 更改IP地址

B.2.3 启用Server Core服务器

B.2.4 加入域

B.2.5 将域用户加入本地Administrators组

B.2.6 更改日期与时间

B.3 在Server Core服务器内安装角色与功能

B.3.1 查看所有角色与功能的状态

B.3.2 DNS服务器角色

B.3.3 DHCP服务器角色

- B.3.4 文件服务角色
- B.3.5 Hyper-V角色
- B.3.6 打印服务角色
- B.3.7 Active Directory证书服务 (AD CS) 角色
- B.3.8 Active Directory域服务 (AD DS) 角色
- B.3.9 Web服务器 (IIS) 角色
- B.4 远程管理Server Core服务器
 - B.4.1 通过服务器管理器来管理Server Core服务器
 - B.4.2 通过MMC管理控制台来管理Server Core服务器
 - B.4.3 通过远程桌面来管理Server Core服务器
 - B.4.4 硬件设备的安装
- B.5 在虚拟机内运行的Nano服务器
 - B.5.1 建立供虚拟机使用的Nano服务器映像文件
 - B.5.2 建立与启动Nano服务器的虚拟机
 - B.5.3 将Nano服务器加入域
- B.6 在物理机内运行的Nano服务器
 - B.6.1 建立供物理机使用的Nano服务器映像文件
 - B.6.2 利用WinPE启动计算机与安装Nano服务器

封底