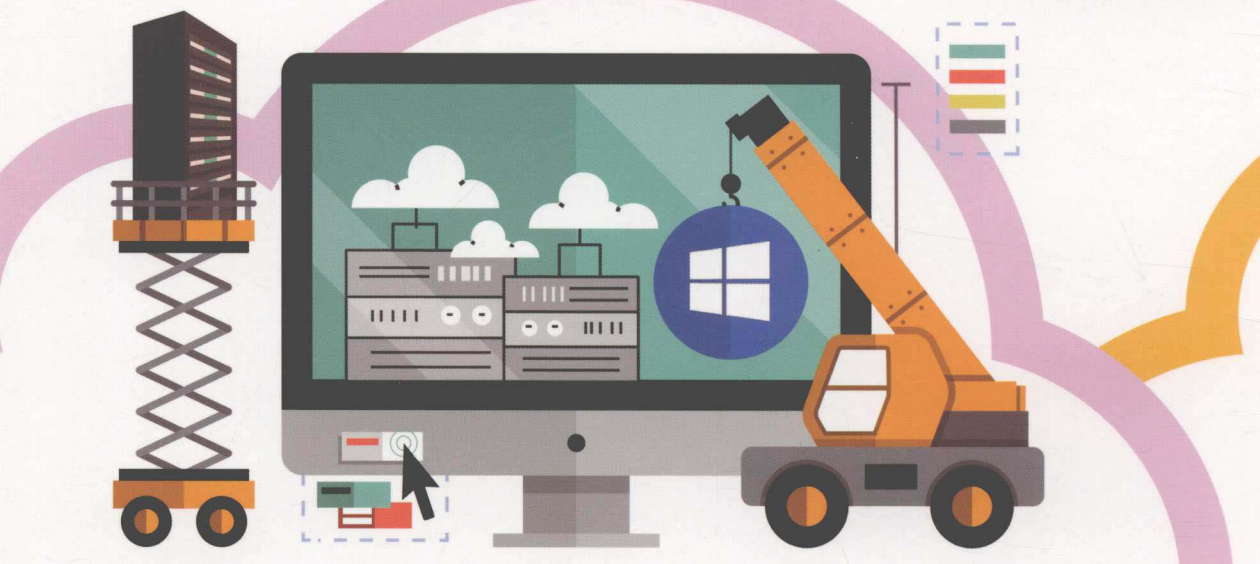
GOTOP

2016 Windows Server

Active Directory配置指南

戴有炜 编著



- 独家讲述实用的Active Directory域服务（AD DS）配置专题
- 导入虚拟技术，一台电脑便可以拥有完整的虚拟网络环境
- 充分掌握Active Directory域服务的完整知识
- Server Core与Nano Server配置全攻略
- 微软MCSM、MCSE、MCSA与MTA等认证考试的实用参考书

清華大學出版社

2016 Windows Server

Active Directory配置指南

戴有炜 编著

清華大學出版社
北京

内 容 简 介

本书由台湾知名的微软技术专家戴有炜先生倾力编著，是他最新推出的 Windows Server 2016 三卷力作中的 Active Directory 配置指南篇。

本书延续了作者的一贯写作风格：大量的实例演示兼具理论，以及完整清晰的操作过程，以简单易懂的文字进行描述，内容丰富，图文并茂。本书共分 13 章，内容包括 Active Directory 域服务、建立 AD DS 域、域用户与组账户的管理、利用组策略管理用户工作环境、利用组策略部署软件、限制软件的运行、建立域树和林、管理域和林信任、AD DS 数据库的复制、操作主机的管理、AD DS 的维护、将资源发布到 AD DS 以及自动信任根 CA。

本书面向广大初、中级网络技术人员、网络管理和维护人员，也可作为高等院校相关专业和技术培训班的教学用书，同时可以作为微软认证考试的参考用书。

图书在版编目（CIP）数据

Windows Server 2016 Active Directory 配置指南 / 戴有炜编著.—北京：清华大学出版社，2019
ISBN 978-7-302-51796-2

Ⅰ. ①W… Ⅱ. ①戴… Ⅲ. ①Windows 操作系统－网络服务器 Ⅳ. ①TP316.86

中国版本图书馆 CIP 数据核字（2018）第 269762 号

责任编辑：夏毓彦
封面设计：王　翔
责任校对：闫秀华
责任印制：杨　艳
出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：190mm×260mm　　**印　张：**25.75　　**字　数：**659 千字
版　　次：2019 年 2 月第 1 版　　**印　次：**2019 年 2 月第 1 次印刷
定　　价：89.00 元

产品编号：079763-01

序

首先要感谢读者长期以来的支持与爱护！这一系列书籍仍然采用我一贯秉承的编写风格，也就是完全站在读者立场思考，并且以务实的观点来改编升级这三本Windows Server 2016书籍。我花费了相当多的时间在不断地测试与验证书中所述内容，并融合多年的教学经验，以最容易让你理解的方式将其写到书中，希望能够帮助你快速地学会Windows Server 2016。

本套书的宗旨是希望能够让读者通过书中丰富的示例与详尽的实用操作来充分了解Windows Server 2016，进而能够轻松地管理Windows Server 2016的网络环境，因此书中不但理论解说清晰，而且范例充足。对需要参加微软认证考试的读者来说，这套书更是不可或缺的实用参考手册。

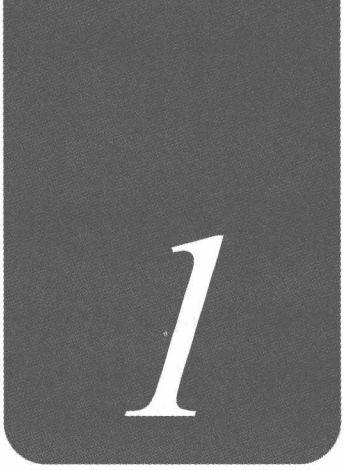
学习网络操作系统，首当其冲注重动手实践，唯有实际演练书中所介绍的各项技术，才能充分了解与掌握它，因此建议使用Windows Server 2016 Hyper-V等提供虚拟技术的软件来搭建书中的网络测试环境。

本套书分为《Windows Server 2016 Active Directory配置指南》《Windows Server 2016系统配置指南》《Windows Server 2016网络管理与架站》三本，内容丰富翔实，相信这几本书仍然不会辜负你的期望，在学习Windows Server 2016时给予你最大的帮助。

感谢所有让这套书能够顺利出版的朋友们，他们给予宝贵的意见、帮助版面编排、支持技术审校、出借测试设备或提供软件资源等方面的协助。

戴有炜

目 录



第 1 章　Active Directory 域服务（AD DS）

在Windows Server 2016的网络环境中，Active Directory域服务（Active Directory Domain Services，AD DS）提供了用来组织、管理与控制网络资源的各种强大功能。

- Active Directory域服务概述
- 域功能级别与林功能级别
- Active Directory轻型目录服务

1.1 Active Directory域服务概述

什么是**directory**呢？日常生活中的电话簿内记录着亲朋好友的姓名和电话等数据，它就是**telephone directory**（电话目录）；计算机中的文件系统（file system）内记录着文件的文件名、大小与日期等数据，它就是**file directory**（文件目录）。

如果这些directory内的数据能够系统地加以整理的话，用户就能够很容易与快速地找到所需要的数据，而directory service（目录服务）所提供的服务，就是要让用户很容易与快速地在directory内查找所需要的数据。在现实生活中，查号台也是一种目录服务；在Internet上，Google网站所提供的搜索功能也是一种目录服务。

Active Directory域内的directorydatabase（目录数据库）被用来存储用户账户、计算机账户、打印机与共享文件夹等对象，而提供目录服务的组件就是**Active Directory域服务**（Active Directory Domain Services，AD DS），它负责目录数据库的存储、添加、删除、修改与查询等工作。

1.1.1 Active Directory域服务的适用范围（Scope）

AD DS的适用范围非常广泛，它可以用在一台计算机、一个小型局域网（LAN）或多个广域网（WAN）结合的环境中。它包含此范围中的所有对象，例如文件、打印机、应用程序、服务器、域控制器与用户账户等。

1.1.2 名称空间（Namespace）

名称空间是一个界定好的区域（bounded area），在此区域内，我们可以利用某个名称来找到与此名称有关的信息。例如一本电话簿就是一个**名称空间**，在这本电话簿内（界定好的区域内），我们可以利用姓名来找到此人的电话、地址与生日等信息。又如Windows操作系统的NTFS文件系统也是一个**名称空间**，在这个文件系统内，我们可以利用文件名来找到此文件的大小、修改日期与文件内容等信息。

Active Directory域服务（AD DS）也是一个**名称空间**。利用AD DS，我们可以通过对象名称来找到与此对象有关的所有信息。

在TCP/IP网络环境内利用Domain Name System （DNS）来解析主机名与IP地址的映射关系，例如利用DNS来得知主机的IP地址。AD DS也与DNS紧密地集成在一起，它的域名**空间**也是采用DNS架构，因此域名是采用DNS格式来命名的，例如可以将AD DS的域名命名为

sayms.local。

1.1.3 对象（Object）与属性（Attribute）

AD DS内的资源是以对象的形式存在，例如用户、计算机等都是对象，而对象是通过**属性**来描述其特征的，也就是对象本身是一些**属性**的集合。例如如果要为用户**王乔治**建立一个账户，则需要新建一个对象类型（object class）为**用户**的对象（也就是用户账户），然后在此对象内输入**王乔治**的姓、名、登录名与地址等，这其中的用户账户就是对象，而姓、名与登录名等就是该对象的属性（参见表1-1-1）。另外，图1-1-1中的**王乔治**就是对象类型为**用户**（user）的对象。

表1-1-1

对象（object）	属性（attributes）
用户（user）	姓 名 登录名 地址 …

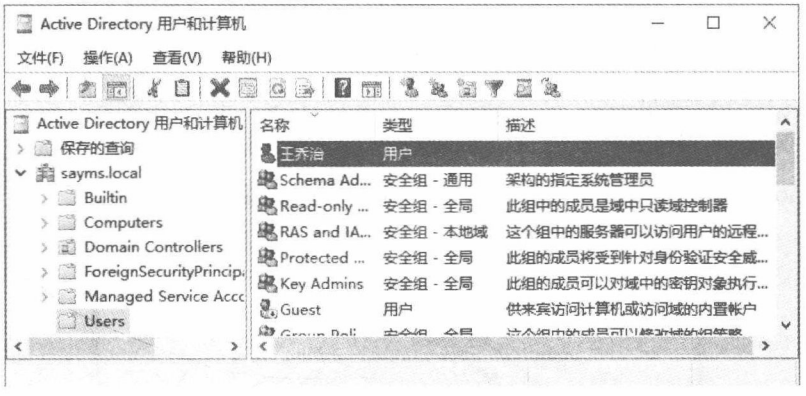


图 1-1-1

1.1.4 容器（Container）与组织单位（Organization Units，OU）

容器与对象相似，它也有自己的名称，也是一些属性的集合，不过容器内可以包含其他对象（例如**用户**、**计算机**等），也可以包含其他容器。而组织单位是一个比较特殊的容器，除了可以包含其他对象与组织单位之外，还有**组策略**（group policy）的功能。图1-1-2所示就是一个名称为**业务部**的组织单位，其中包含着多个对象，其中两个为**用户**对象、两个为**计算机**对象与两个本身也是组织单位的对象。