第一图书网, tushu007.com

<<网络操作系统及配置管理>>

图书基本信息

书名：<<网络操作系统及配置管理>>

13位ISBN编号：9787302283744

10位ISBN编号：7302283745

出版时间：2012-7

出版时间：清华大学出版社

作者：苗凤君　等主编

页数：313

字数：512000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

内容概要

《网络操作系统及配置管理：Windows Server 2008与RHEL 6.0》由两部分内容组成，第1部分为Windows Server 2008，介绍了Windows Server 2008操作系统的安装，Windows Server 2008中的文件系统、磁盘管理以及在该平台下各种网络服务的安装、配置和使用；第二部分为RHEL6.0，介绍了RHEL6.0的安装，RHEL6.0中的文件系统、磁盘管理及其在该平台下常用网络服务的安装、配置和使用。

本书内容全面，注重实用性和可操作性。本书所有服务器的配置都经过了实际验证，因此，读者在使用本书时可以节约大量的调试时间。

本书适合作为本科及大中专院校计算机应用、计算机科学与技术、网络工程、网络系统管理等计算机相关专业的教材，也可作为网络管理员和系统管理员的服务器搭建手册。

书籍目录

第1章　网络操作系统简介
1.1 网络操作系统
1.1.1 网络操作系统的功能
1.1.2 网络操作系统的特征
1.1.3 网络操作系统的分类
1.2 Windows网络操作系统
1.2.1 WindowsServer2008的版本
1.2.2 WindowsServer2008的新特性
1.3 Linux网络操作系统
1.3.1 RHEL的版本
1.3.2 RHEL的新特性
本章小结
习题
第2章　WindowsServer2008的安装和基本配置
2.1 WindowsServer2008的安装
2.1.1 系统需求
2.1.2 安装过程
2.1.3 安装后的基本配置
2.2 NTFS文件系统
2.2.1 WindowsServer2008支持的文件系统
2.2.2 NTFS文件系统的访问和许可权
2.3 磁盘管理
2.3.1 基本磁盘
2.3.2 动态磁盘管理
2.3.3 NTFS文件系统的管理
本章小结
实验一 安装WindowsServer2008
实验二 磁盘管理和文件系统管理
习题
第3章　WindowsServer2008的基本网络服务
3.1 DHCP服务器的配置与管理
3.1.1 DHCP基本概念
3.1.2 DHCP服务器的安装和启动
3.1.3 DHCP服务器的配置
3.1.4 管理DHCP数据库
3.1.5 DHCP客户端的配置和测试
3.1.6 配置DHCP中继代理
3.2 DNS服务器的配置与管理
3.2.1 DNS服务基础
3.2.2 DNS服务器的安装
3.2.3 配置DNS区域
3.2.4 配置DNS转发器
3.2.5 DNS客户端的配置和测试
3.3 Web服务器的配置与管理
3.3.1 IIS基础

3.3.2 Web服务器的安装、测试、停止和启动
3.3.3 设置Web站点
3.3.4 管理Web站点
3.3.5 网站的安全性
3.4 FTP服务器的配置与管理
3.4.1 FTP的基本概念
3.4.2 安装FTP服务器
3.4.3 配置FTP服务器
3.4.4 测试FTP服务器
本章小结
实验三 DHCP和DNS服务器的安装与配置
实验四 WWW和FTP服务器的安装与配置
习题
第4章　活动目录的配置与管理
4.1 活动目录概述
4.1.1 活动目录的功能
4.1.2 活动目录对象
4.2 活动目录的安装
4.2.1 活动目录的安装
4.2.2 让域控制器向DNS服务器注册SRV记录
4.2.3 创建子域
……
第5章　证书服务器配置与管理
第6章　Windows Server 2008安全管理
第7章　RHEL6.0的安装和基本配置
第8章　RHEL6.0的基本网络服务
第9章　RHEL6.0的其他网络服务
第10章　RHEL6.0操作系统安全
习题答案
参考文献

章节摘录

版权页： 插图： 6.2.1 物理安全 为保护计算机和网络系统设备、设施免遭地震、水灾、火灾、有害气体和其他环境事故破坏，采取适当的物理保护措施实现物理安全防护。
（1）机房及终端计算机设备位置的选择。
应在具有防震、防风和防雨等能力的建筑内，还应当避开强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区。
（2）物理访问控制。
在对机房的管理上，管理员应鉴别进入的人员身份并记录在案，对来访人员限制和监控其活动范围，尤其重要区域配置监控系统，用于记录进入的人员身份并监控其活动。
（3）防盗窃和防破坏。
应将主要设备放置在物理受限的范围内，对设备或主要部件进行固定，并设置明显的无法除去的标记，应将通信线缆铺设在隐蔽处，如铺设在地下或管道中等，应对介质分类标识，存储在介质库或档案室中，设备或存储介质携带出工作环境时，应受到监控和内容加密，利用光、电等技术设置机房的防盗报警系统，以防进入机房的盗窃和破坏行为，应对机房设置监控报警系统。
（4）防雷击。
机房建筑设置避雷装置，要设置防雷保安器防止感应雷，还要设置交流电源地线。
（5）防火。
机房采取区域隔离防火措施，将重要设备与其他设备隔离开，其建筑材科应具有耐火等级，应设置自动灭火系统，加设灭火装置，必要时人工灭火。
（6）防水和防潮。
防止雨水渗透，水蒸气结露，地下积水的转移和渗透，以给予干燥的环境。
（7）防静电。
采用防静电地板，利用防静电消除器定期去除。
（8）温湿度控制。
定期检测机房内的温湿度，并做记录，查看趋向，以便及时采取措施，使机房温、湿度的变化在设备运行所允许的范围之内。
（9）电力供应。
装置稳压和过压防护设备，提供短期备用电力供应，设置冗余电力线缆电路，另加备用发电机，以备常用供电系统停电时使用。
（10）电磁防护。
采用接地方式防止外界电磁干扰和设备寄生耦合干扰，隔离电源线和通信线缆，避免互相干扰，开启电磁干扰器对重要设备和磁介质实施电磁屏蔽。
（11）散热。
应配备散热装置，防止温度过高烧坏设备。
6.2.2 防止外部远程入侵 网络层是网络入侵者进攻信息系统的渠道和通路。
保证网络安全的首要问题就是要合理划分网段，利用网络中间设备的安全机制控制各网络间的访问。同时由于网络系统内运行的TCP／IP协议并非专为安全通信而设计，所以存在着大量的安全隐患和威胁，故要设立防火墙策略控制进出系统的用户权限。

编辑推荐

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com