

网络服务器管理 教程

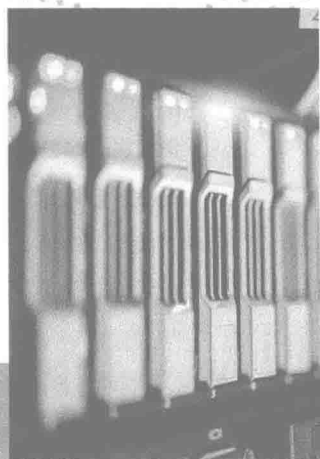
陈 波 主编



上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

网络服务器管理 教程

陈 波 主编



上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

内容提要

本书包括基础知识、网络配置和运维、系统配置、虚拟化配置等四篇，系统介绍了典型中小 IT 企业网络服务器管理中涉及的操作系统、网络架构及系统软件的安装与配置方法，以及小型服务器集群的构建等知识，侧重对备受关注的容器虚拟化技术进行了阐述。

本书从网络服务器管理岗位的实际需求角度出发，帮助读者理解、分析和解决服务器管理中的实际问题。

图书在版编目 (CIP) 数据

网络服务器管理教程/陈波主编. —上海: 上海交通大学出版社, 2018

ISBN 978-7-313-20780-7

I. ①网… II. ①陈… III. ①网络服务器—教材
IV. ①TP368.5

中国版本图书馆 CIP 数据核字 (2019) 第 001752 号

网络服务器管理教程

主 编: 陈 波

出版发行: 上海交通大学出版社

邮政编码: 200030

印 制: 虎彩印艺股份有限公司

开 本: 710×1000mm 1/16

字 数: 187 千字

版 次: 2019 年 4 月第 1 版

书 号: ISBN 978-7-313-20780-7/TP

定 价: 88.00 元

地 址: 上海市番禺路 951 号

电 话: 021-64071208

经 销: 全国新华书店

印 张: 17

印 次: 2019 年 4 月第 1 次印刷

版权所有 侵权必究

告读者: 如发现本书有印装质量问题请与印刷厂质量科联系

联系电话: 0769-85252189

前 言

当前，作为信息技术服务基础层的网络运维（运行及维护）管理市场迎来新的变革，尤其对网络服务器管理人才的需求非常紧迫。前些年，由于运维行业技术门槛相对较低，部分企业由开发人员兼职运维岗位，只对服务器做一些打打补丁之类的简单管理。随着云服务的发展，网络服务器的重要地位越来越突出，对维护人员的专业化程度要求越来越高，掌握专业服务器运维知识的人员也成为 IT 职场中备受青睐的紧缺人才。

然而，目前网络服务器管理的教学实践与人才培养之间还存在很大差距。很多学生虽然已经学习了操作系统、计算机网络、编程语言等相关课程，但没有服务器管理的全局观，也缺乏动手能力，难以将理论联系实践。网络服务器管理涉及的知识点散布在多门课程中，体系结构不够系统，或者知识不够全面，以至于学生难以掌握切实可行的技能。因此，我们在近几年讲授网络服务器管理的课程讲义的基础上，经过归纳和整理，推出了这本《网络服务器管理教程》。

本书以与企业中所用环境 Red Hat Enterprise Linux 较为接近的 Linux 版本——CentOS 7.3 为开发环境，而没有采用逐渐失去市场的 Windows NT Server 以及以个人学习目的为主的 Ubuntu 系统，与企业实际部署情况更为接近。Linux 的基本命令都是相通的，具备 Ubuntu 或其他 Linux 系统基础知识的读者可以很快地适应 CentOS 环境。出于同样的考虑，本书第一部分略过了 Linux 常用命令、Shell 编程基础、内核、网络服务原理等基础性的内容，而将重点突出在新型文件系统 ext4、大容量磁盘管理、



和服务启动过程的介绍上。

网络服务器是专指某些高性能计算机，能够通过网络，对外提供某类服务。本书的第二部分，重点对实际生产环境中经常接触到的网络接入配置、防火墙、运行级别、安全协议、域名服务、定时任务等进行介绍，涉及符合企业需求的常用工具搭建运维环境。

被安装到服务器上的软件，都是公司开展正常研发工作所必须的各类工具。本书的第三部分，重点介绍邮件、文件共享服务器软件的安装，对开发型公司，以目前最为流行的两套技术协议栈，LAMP 和 MEAN 为实例，介绍了相关软件的安装与配置。

虚拟化是云计算的关键技术之一，它可以获取更高的工作负载移动性、更优异的性能和资源可用性，同时大幅节约成本。随着云计算技术的迅速落地，很多读者都在尝试云服务商们提供的各类服务，对构建自己的云计算系统也很有兴趣。本书的第四部分重点介绍虚拟化技术的原理，并选择当前最热门的 docker 和 kubernetes 作为案例进行讲解。

本书共有 24 章，分为四个部分，各部分的大体内容如下。

第一部分是服务器运维管理的基础知识，首先陈述了运维的意义，介绍了运维管理的背景、挑战，运维体系的结构和运作方式，接着重点对 Linux 文件系统、磁盘和逻辑卷、服务器设备管理这三个问题，针对服务器特色进行了介绍。通过本部分的学习，读者可对网络服务器管理的背景有所了解，并能了解服务器与普通工作站机器的不同。

第二部分是服务器的网络配置与运维，讲解了 Linux 系统中常见网络服务的原理与安装配置，包括 DHCP 服务、DNS 服务、电子邮件服务以及 NFS 服务。接着讲解了与网络安全相关的配置，包括防火墙、IPSec 等，最后对 CentOS 系统中使用的防火墙工具——iptables、firewalld 的使用方式进行了介绍。

第三部分主要讲解了网络服务器上安装的邮件、文件共享等工具软



件，包括如何通过用户及组群管理实现访问控制。在技术协议栈软件上，选取了 LAMP（Linux+Apache+MySQL+PHP）和 MEAN（MongoDB+Express+Angular+NodeJS）进行了讲解。

第四部分主要讲解了与虚拟化技术相关的知识，包括虚拟化简介、虚拟化原理与架构、如何用 docker 搭建虚拟化环境、如何在单机上使用 minikube 搭建个人计算机集群和使用 Kubernetes 构建多机集群的知识。

读者若不能完全理解教材中所讲知识，可登录配套网站，配合平台中的教学资料进行学习。此外，在学习的过程中，务必要勤于练习，确保真正掌握所学知识。

目 录

第 1 部分 基础知识

1.1 运维基础知识	3
1.1.1 运维面临的挑战	3
1.1.2 建设运维体系的目标	4
1.1.3 运维体系的结构和运作方式	4
1.1.4 运维工程师职业规划	7
1.2 Linux 文件系统	10
1.2.1 ext4 的特性	10
1.2.2 创建一个 ext4 文件系统	13
1.2.3 转换到 ext4 文件系统	13
1.2.4 XFS 文件系统	14
1.2.5 添加交换空间	15
1.2.6 删除交换空间	19
1.3 磁盘与逻辑卷	21
1.3.1 LVM 是什么	21
1.3.2 磁盘存储区	22
1.3.3 查看分区表	24
1.3.4 创建分区	24



1.3.5	删除分区	27
1.3.6	重新划分分区大小	27
1.4	系统启动过程	29
1.4.1	概述	29
1.4.2	BIOS 安装	31
1.4.3	编写配置文件	32
1.4.4	GRUB2 镜像文件列表	33
1.4.5	GRUB 交互界面	35

第 2 部分 网络配置与运维

2.1	网络配置	41
2.1.1	基本配置	41
2.1.2	建立 IPsec 连接	45
2.2	基本防火墙配置	56
2.2.1	防火墙设置	56
2.2.2	激活 iptables 服务	64
2.3	控制对服务的访问	66
2.3.1	运行级别	66
2.3.2	TCP 回绕程序	68
2.3.3	ntsysv	69
2.3.4	chkconfig	70
2.4	OpenSSH	71
2.4.1	为什么使用 SSH	71
2.4.2	配置 OpenSSH 服务器	72



2.4.3	配置 OpenSSH 客户	73
2.5	动态主机配置协议	76
2.5.1	为什么使用 DHCP	76
2.5.2	配置 DHCP 服务器	77
2.5.3	配置 DHCP 客户	83
2.6	BIND 配置	86
2.6.1	安装 BIND	86
2.6.2	配置正确解析	88
2.6.3	添加逆向主区	90
2.6.4	DNS 以服务器设置	91

第 3 部分 系统配置

3.1	用户和组群配置	97
3.1.1	添加新用户	97
3.1.2	修改用户属性	99
3.1.3	添加新组群	100
3.1.4	修改组群属性	101
3.1.5	命令行配置	102
3.1.6	对进程的解释	105
3.2	自动化的任务	107
3.2.1	cron	107
3.2.2	anacron	110
3.2.3	at	112
3.2.4	batch	113



3.3 日志文件	116
3.3.1 定位日志文件	116
3.3.2 查看日志文件	117
3.4 内核模块	119
3.4.1 内核模块工具	119
3.5 邮件传输代理配置	123
3.5.1 安装 Postfix	123
3.5.2 测试 Postfix	133
3.5.3 创建测试域及用户	134
3.5.4 检查日志	135
3.5.5 测试邮箱客户端	136
3.6 Samba 文件共享	137
3.6.1 Samba 简介	137
3.6.2 Samba 功能和应用范围	138
3.6.3 复杂的用户共享模型	145
3.7 Web 服务器软件组合 LAMP	152
3.7.1 Apache 服务器	152
3.7.2 MySQL/Marie DB	153
3.7.3 PHP	156
3.7.4 Apache 的竞争者 Nginx	161
3.8 MEAN 全栈开发环境	165
3.8.1 源码编译安装 node.js	165
3.8.2 安装 MongoDB 数据库	168
3.8.3 安装 Express	169



3.8.4 安装 Vue.js	170
3.9 收集系统信息	173
3.9.1 系统进程	173
3.9.2 内存用量	177
3.9.3 文件系统	178
3.9.4 硬件	179
3.9.5 CentOS 7 新增管理工具	181

第 4 部分 虚拟化配置

4.1 Docker 容器技术	185
4.1.1 Docker 的历史与现状分析	185
4.1.2 Docker 的技术原理介绍	187
4.1.3 Docker 的基本概念	190
4.1.4 Docker 的部署与安装	191
4.2 Docker 基础命令	196
4.2.1 镜像有关的命令	196
4.2.2 将容器变成镜像	202
4.3 Kubernetes(k8s)基础	206
4.3.1 Kubernetes 是什么	206
4.3.2 使用 Kubernetes 能做什么	209
4.3.3 你好 minibike	211
4.4 Kubernetes 集群原理	219
4.4.1 Kubernetes 集群的组件	219
4.4.2 了解 Kubernetes 对象	221



4.4.3	labels	223
4.4.4	了解 Pod	227
4.4.5	master 和 node 之间的通信	229
4.5	Kubernetes 安装设置	231
4.5.1	搭建自定义集群	231
4.5.2	在节点上配置和安装基础软件	236
4.5.3	引导集群启动	240
4.5.4	故障排除	248
参考文献		256

第 1 部分 基础知识

1.1 运维基础知识

1.1.1 运维面临的挑战

假设你被一家 IT 公司录用为运维人员，这家公司的主要产品是一个线上游戏，说不定你也曾经玩过。以后可以抢先玩新关卡了，是不是很爽？且慢，老板首先跟你讲了几个需求：

第一个是游戏的需求。它表现为三个方面：一是游戏数量多，现在运营的游戏可能多达近百款。二是游戏架构复杂。游戏公司和一般的互联网公司有一个很大的区别，就是游戏的来源可能有很多，比如有国外的、国内的，有大厂商的、小厂商的；每个游戏的架构可能不一样，有的是分区制的，有的是集中制的，各种各样的需求。三是操作系统种类多，这与刚才的情况类似，游戏开发者的背景与编程喜好不一样，会有 Windows、Linux 等。

第二个是在硬件环境方面，主要表现为服务器数量多、服务器型号多。公司在发展过程中分批、分期采购的服务器几乎横跨 OEM 厂商的各大产品线，型号多而杂。

最后是人的因素。如果大家的技术能力都很强，很多时候一个人可以完成所有工作，可能也就不需要自动化运维体系了。正是因为每个人的能力不一样，技术水平参差不齐，甚至是习惯和工具也不一样，导致公司必须要创建一套规范的运维体系来提升工作效率。



1.1.2 建设运维体系的目标

接着，经理提出建设自动化运维体系的目标，总结为四个词。

第一个是“完备”，这个系统要能涵盖所有的运维需求。

第二个是“简洁”，简单好用。如果系统的操作流程、操作界面、设计思想都比较复杂，运维人员的学习成本就会很高，使用的效果不佳，系统的能力、发挥的效率也会因此打折扣。

第三个是“高效”，特别是在批量处理或者执行特定任务时，希望系统能够及时给用户反馈。

第四个是“安全”，如果一个系统不安全，可能很快就会被黑客接管，所以安全也是重要的因素。

1.1.3 运维体系的结构和运作方式

自动化运维体系往往分成几个子系统联合起来工作。首先，服务器会由自动化安装系统完成安装，然后被自动化运维平台接管。自动化运维平台会对自动化安检系统、自动化客户端更新系统和服务器端更新系统提供底层支撑。自动化数据分析系统与自动化客户端更新系统相关联，因此，自动化数据分析系统会对自动化客户端更新系统的结果给予反馈。

1. 自动化安装系统

自动化安装的整个流程采用通用的框架，首先由 PXE 启动，选择需要安装的操作系统类型（安装 Windows 或者 Linux），然后根据 Windows 系统自动识别出需要安装的驱动。服务器交付用户之前，会进行基本的安全设置，例如防火墙设置以及关闭 Windows 共享，这在一定程度上提高了安全性，也减少了一些人工操作。

2. 自动化运维平台

当服务器由自动化安装系统安装完成以后，就会被自动化运维平台接



管。自动化运维平台是运维人员的作业平台，它主要解决的就是因服务器、操作系统异构且数量多而带来的管理问题。操作系统五花八门，需要在设计系统过程中考虑以下几个因素：把整个系统的用户界面设计成基于浏览器的架构；统一管理异构服务器；充分利用现有协议和工具。

3. 自动化安检系统

下一个系统是自动化安检系统。由于子系统比较多，业务也比较多，怎样设计一套系统去保障它们的安全呢？这里主要是两个系统：自动化安检平台和服务器端。

先来看自动化安检平台。游戏公司和一般的互联网公司有一个区别，就是前者需要给玩家发送很多的客户端（特别是有的客户端比较大），或者补丁文件去更新、下载和安装。如果这些文件里面出现病毒和木马，将是一件很糟糕的事情，甚至会对业务和公司的声誉造成恶劣影响。在这些文件被发到玩家电脑上之前，必须经过病毒检测系统检测，确保它没有被注入相应的病毒代码。

再来看服务器端，主要是通过安全扫描架构来保障安全。安全并不是一蹴而就，一劳永逸的。如果不对系统进行持续地检查、检测、探测，那么你的一些错误操作会导致系统暴露在互联网上，或者是暴露在恶意攻击者的眼皮之下。通过一种主动、自发的安全扫描架构对所有服务器进行安全扫描，就能在很大程度上规避这样的问题。

4. 自动化客户端更新系统

游戏是有周期性的，特别是在游戏发布当天或者有版本更新的时候，此时玩家活跃度很高，下载行为也比较多，但是平时的更新和下载带宽可能并不大，这也是游戏的显著特点。这个特点对于我们构建一个分发系统提出了很大的挑战。第一个挑战就是在高峰时游戏产生的带宽可能达到数百 GB。第二是非法缓存的问题。很多小运营商或者中小规模的运营商会有一些缓存机制，这个缓存机制如果处理得不好，会对业务造成影响。第三是关于 DNS 调度的问题。DNS 调度是基于玩家本身的 Local DNS 的机制解析的，会有调度不准确的问题。第四是 DNS 污染，或者是 DNS TTL