网络工程师

运 维 实 战 手 册

从入门到日常维护 · 一套搞定服务器/网络/虚拟化运维

一线运维工程师实操经验总结

Linux · 网络 · PVE虚拟化 · 安全加固 · 故障排查

2026年5月

前 言

很多想入行运维的朋友，面对浩瀚的技术栈不知道从哪下手。也有很多已经在做运维的朋友，遇到问题时东查西查效率太低。这本手册把运维工程师日常工作中使用频率最高的技能提炼出来，按实战场景分类，遇到问题直接翻，平时有空翻一翻也能涨功力。

适用人群：

- 想转行做运维的IT新人
- 刚入职的初级运维工程师
- 自己管理服务器的个人开发者
- 中小企业IT管理员

前置要求：基本的电脑操作能力，了解IP地址、浏览器等基础概念。

典型运维架构示意图：

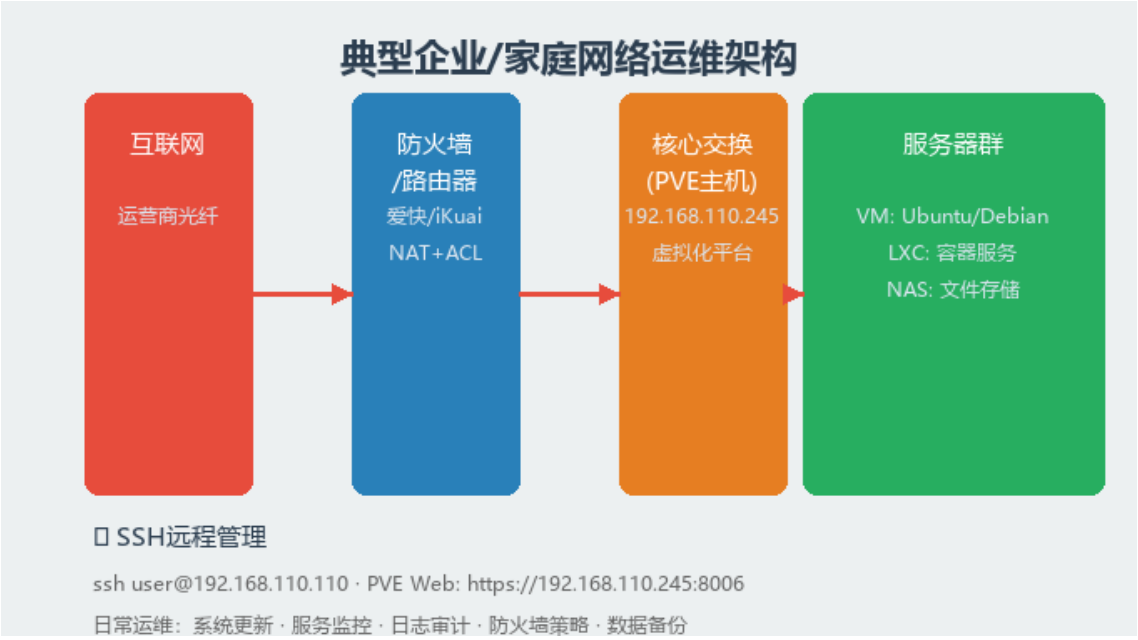

图0-1：从互联网到服务器群的典型运维架构

第一章 • Linux服务器基础运维

Linux是运维工程师的必修课。本章精选最常用的操作命令，按场景分类，即查即用。

1.1 系统信息与资源监控

```
uname -a 查看系统内核版本信息
cat /etc/os-release 查看发行版信息
free -h 查看内存使用情况（-h 友好显示）
df -h 查看磁盘分区与使用率
du -sh * 查看当前目录下各文件/文件夹大小
uptime 查看服务器运行时间与负载
htop / top 实时监控进程与资源占用
```

> 提示："df -h" 是运维检查磁盘的第一命令。如果使用率超过80%，就该考虑清理或扩容了。

1.2 服务管理（systemctl）

```
systemctl status nginx 查看服务运行状态
systemctl start/stop/restart nginx 启动/停止/重启服务
systemctl enable nginx 设置开机自启
systemctl daemon-reload 重新加载服务配置
journalctl -u nginx -n 50 查看最近50条服务日志
journalctl -xe 查看系统最近错误日志
```

1.3 用户与权限管理

```
useradd -m username 创建用户并创建家目录
passwd username 设置/修改用户密码
usermod -aG sudo username 将用户添加到sudo组
chmod 755 file 设置文件权限（rwxr-xr-x）
chown user:group file 修改文件所有者
ls -la 查看文件详细列表（含权限信息）
```

1.4 日志与故障排查

```
tail -f /var/log/syslog 实时跟踪系统日志
grep "error" /var/log/nginx/error.log 搜索错误关键信息
dmesg | tail -20 查看内核最后20条消息
last 查看最近登录记录
lastb 查看登录失败记录（发现大量失败=有人在暴力破解）
```

> 如果发现lastb有大量来自陌生IP的登录失败记录，说明服务器正在被暴力破解。立即启用fail2ban。

1.5 软件包管理

```
apt update && apt upgrade -y 更新系统（Ubuntu/Debian）
apt install nginx -y 安装软件包
apt remove nginx 卸载软件包
apt autoremove 清理不再需要的依赖包
dpkg -i package.deb 安装本地deb包
```

> 提示：养成好习惯：每周执行一次 apt update && apt upgrade -y，保持系统安全更新。

第二章 • 网络基础与设备运维

网络是运维的核心技能。不懂网络，服务器配得再好也是白搭。本章从最基础的概念到实战配置。

2.1 必备网络概念

概念	说明	举例
IP地址	设备在网络中的唯一标识	192.168.1.100
子网掩码	区分网络位和主机位	255.255.255.0 (/24)
网关	出网的必经之路	192.168.1.1
DNS	域名解析为IP	114.114.114.114
VLAN	虚拟局域网，隔离广播域	VLAN 10/20/30
NAT	内网地址转公网地址	路由器/防火墙功能
DHCP	自动分配IP地址	路由器开启
端口	服务在设备上的入口	80(HTTP)/443(HTTPS)/22(SSH)

2.2 Linux网络配置命令

```
ip a 查看所有网卡IP配置
ip route show 查看路由表（默认网关在哪）
ss -tlnp 查看当前监听的所有TCP端口
ping 114.114.114.114 测试外网连通性
traceroute 目标IP 追踪数据包路径
nslookup baidu.com 测试DNS解析
curl -I https://example.com 测试HTTP响应头
tcpdump -i eth0 port 80 抓取80端口数据包
```

> 提示：排查网络故障的标准流程：ping网关 → ping DNS → ping外网 → curl网站，一步一步定位。

2.3 防火墙配置

UFW（推荐新手使用）：

```
ufw enable 启用防火墙
ufw allow 22/tcp 放行SSH端口
ufw allow 80,443/tcp 放行Web端口
ufw deny 3306 禁止外部访问MySQL端口
ufw status verbose 查看详细规则
```

iptables（进阶）：

```
iptables -L -n --line-numbers 查看规则（带行号）
```

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT 放行SSH
iptables -P INPUT DROP 默认拒绝所有入站
iptables-save > /etc/iptables.rules 保存规则
```

> 配置防火墙一定要先放行SSH端口再改默认策略，否则会把自己锁在外面！

2.4 SSH远程连接与安全

```
ssh user@192.168.1.100 -p 22 SSH远程登录
ssh-keygen -t ed25519 生成密钥对（更安全）
ssh-copy-id user@192.168.1.100 复制公钥到服务器
```

SSH安全加固要点（修改 /etc/ssh/sshd_config）：

- Port 2222 —— 改掉默认22端口，减少90%的暴力破解
- PermitRootLogin prohibit-password —— 禁止root密码登录
- PasswordAuthentication no —— 关闭密码登录，只用密钥
- MaxAuthTries 3 —— 最大认证尝试次数

第三章 • PVE虚拟化运维

Proxmox VE（PVE）是目前中小企业最流行的开源虚拟化平台之一，融合了KVM和LXC。本章基于实战环境（PVE 8.x）讲解日常运维操作。

3.1 PVE基础管理

- 访问地址：https://192.168.x.x:8006
- 默认账号：root，密码是安装时设置的
- 数据中心 → 节点 → 虚拟机/容器，三级管理结构

3.2 虚拟机（VM）管理

操作	说明	等效命令行
创建VM	Web界面：创建虚拟机	qm create 100 ...
启动/停止	右键 → 启动/关机	qm start/stop 100
备份VM	节点 → 备份 → 现在备份	vzdump 100 --mode snapshot
恢复VM	存储 → 备份 → 选择恢复	qmrestore backup.vma 100
迁移VM	右键 → 在线迁移	qm migrate 100 node2
控制台	硬件 → 显示器 → 打开	qm terminal 100
快照	右键 → 快照	qm snapshot 100 snap1

3.3 容器（LXC）管理

- 比VM更轻量，适合跑单一服务（Nginx、MySQL等）
- 权限管理严格，默认无法使用特权命令
- 创建：Web界面 → 创建CT → 选择模板（提前下载模板）
- 命令行：pct list/pct start 101/pct enter 101

3.4 存储管理

- PVE支持：local（本地）、NFS、Ceph、ZFS
- 定期检查存储使用率：数据中心 → 存储 → 查看使用量
- 建议：系统盘放local，数据盘单独挂载或NFS

3.5 备份策略（重要！）

- 设置定时备份：节点 → 备份 → 添加定时备份任务
- 推荐策略：每日增量 + 每周全量，保留最近7天
- 备份存储建议：异地/NFS远程存储，本地备份和服务器一起挂了就完了
- 每月至少手动恢复一次验证备份是否可用

> 不做备份的运维等于裸奔。硬盘挂了、误删了、被黑了，没有备份神仙都救不了。

3.6 PVE网络配置

- PVE默认创建一个Linux Bridge（vmbr0），虚拟机通过桥接上网
- 网卡绑定（Bond）：将多张物理网卡聚合提高带宽和冗余
- VLAN：在网桥上设置VLAN Tag，实现网络隔离

第四章 • 安全加固与监控

安全不是可选项，是运维的基本功。不做安全的服务器，在互联网上活不过24小时。

4.1 服务器安全基线

- 修改SSH默认端口，禁用root密码登录
- 安装fail2ban：自动封禁暴力破解IP
- 开启UFW防火墙，只放行必要的端口
- 禁止密码登录，只使用密钥认证
- 定期更新系统：apt update && apt upgrade -y
- 更换所有默认密码（包括PVE root密码）

4.2 fail2ban配置

```
apt install fail2ban -y 安装
systemctl enable fail2ban && systemctl start fail2ban 启动
fail2ban-client status 查看状态
fail2ban-client status sshd 查看SSH被封的IP列表
```

> 提示：fail2ban安装后会自动监控SSH登录日志，同一IP尝试5次失败自动封禁24小时。

4.3 系统监控方案

以下工具任选一个，不用全部装：

工具	监控能力	推荐场景
htop	进程/CPU/内存实时	日常排查必备
nmon	CPU/内存/网络/磁盘	性能分析
netdata	Web可视化全面监控	个人/小团队
Prometheus+Grafana	企业级全面监控+告警	企业运维
Zabbix	传统企业监控	大型环境
哪吒监控	轻量主机监控+告警	个人多台服务器

4.4 日志审计

- /var/log/syslog —— 系统日志
- /var/log/auth.log —— 认证日志（SSH登录等）

- /var/log/nginx/access.log —— Web访问日志
- /var/log/nginx/error.log —— Web错误日志
- 建议日志保留至少90天，用logrotate自动轮转

第五章 • 故障排查流程

遇到问题不要慌，按流程排查，80%的问题能在5分钟内定位。

5.1 网络不通排查流程

步骤1：检查物理连接——光猫灯正常吗？网线插紧了吗？

步骤2：ping网关——通=局域网正常，不通=内网问题

步骤3：ping DNS（114.114.114.114）——通=网络层正常

步骤4：ping 外网域名（baidu.com）——通=DNS解析正常

步骤5：curl 目标网站——看HTTP状态码

> 提示：排查口诀：先物理后逻辑，先内网后外网，先网络后应用。

5.2 服务启动失败排查

1. systemctl status 服务名 —— 看服务和错误信息
2. journalctl -xe —— 查看详细日志
3. 检查配置文件语法——nginx -t / nginx.conf语法检查
4. 检查端口是否被占用——ss -tlnp | grep 端口号
5. 检查磁盘空间——df -h（磁盘满了服务起不来）

5.3 服务器响应慢排查

1. top/htop —— 看CPU和内存谁在吃
2. df -h —— 看磁盘是否满了
3. free -h —— 看内存是否耗尽
4. dmesg | tail —— 看内核有没有报OOM（内存溢出）
5. iostat -x 1 5 —— 看磁盘IO是否成为瓶颈

5.4 运维新人常见错误

- 防火墙忘记放行端口——配置完服务发现连不上，先看防火墙
- SSH改配置把自己锁外面——改sshd_config时留一个窗口别关
- rm -rf 删错文件——删之前确认三遍，使用完整路径

- chmod 777 图省事——这是安全隐患，755够用
- 不备份就上生产——改配置前先备份原文件

> 不要在生产环境跑不熟悉的命令。先在测试环境验证，再上生产。

附 录

附录1：Linux运维常用命令速查图

附录图：Linux运维常用命令分类速查

附录2：常用端口速查表

端口	服务	协议	用途
22	SSH	TCP	远程管理（建议改端口）
80	HTTP	TCP	Web服务
443	HTTPS	TCP	加密Web服务
3306	MySQL/MariaDB	TCP	数据库（禁止外网开放）
5432	PostgreSQL	TCP	数据库
6379	Redis	TCP	缓存数据库
8006	PVE Web	HTTPS	PVE管理界面
9090	Prometheus	TCP	监控系统
27017	MongoDB	TCP	数据库

附录3：运维远程协助服务

自己搞不定的，我帮你远程处理：

服务项目	价格	说明
Linux服务器维护	50元起	系统更新/安全加固/故障排查
PVE虚拟化运维	80元起	PVE安装配置/VM管理/备份恢复
网络安全加固	60元/次	防火墙配置/SSH安全/fail2ban
网站/应用部署	80元起	Nginx/MySQL/Web应用部署

联系方式请查看闲鱼主页。不解决不收费！

感谢阅读本手册！如果对你有帮助，欢迎给个好评支持原创。