Linux 运维知识体系与自动化笔记系统

可落地的巡检清单、故障排查模板、标准化笔记规范，以及 Ansible/Zabbix 自动化集成方案

巡检清单 故障排查 笔记规范 自动化

一、通用 Linux 运维检查清单

系统层 | 存储与 FS | 账号与权限 | 服务与任务 | 应用中间件 | 监控与备份

版本与内核

```
uname -a; cat /etc/os-release
```

资源使用

```
top/htop; free -m; df -h; iostat -x 1 3; sar -u -r -d 1 3
```

负载与进程

```
uptime; w; ps aux --sort=-%cpu | head; pkill -9 僵尸进程名
```

网络

```
ip a; ss -tulnp; netstat -s; ifconfig; ping/traceroute
```

时钟与时区

```
timedatectl; ntpq -p
```

安全审计

```
last -n 20; faillock; auditctl -l; firewall-cmd --list-all
```

二、故障排查记录模板与范例

通用模板结构

1. 基本信息

发生时间/持续时长/影响范围/优先级/负责人/环境

2. 现象与告警

症状描述、告警原文、错误码/比例/峰值

3. 初步假设

按可能性排序，列出最可疑原因

4. 排查步骤与证据

命令/脚本/查询及输出摘要

5. 根因与处理

技术根因、具体操作、回滚点

6. 验证与改进

修复后指标、预防措施、责任人

范例 A：Nginx 502 Bad Gateway

PHP-FPM 进程耗尽引发的连锁故障

P1 故障

时间信息

2025-12-03 09:12–09:40（28分钟）

影响范围

华东生产站 20% 请求失败

现象与告警

5xx 比例升至 18%，error.log 出现 `upstream prematurely closed connection`，PHP-FPM slow log 超时增多

关键排查证据

```
# pm.status_path 显示队列积压
active=0, idle=0, waiting=大量
pm.max_children=200 实际仅 60
slow log: 95% 请求 >3s
```

根因结论

PHP-FPM 子进程配置过小且队列积压；上游 Java 服务因内存不足导致响应变慢，连锁引发 Nginx 502

处理方案

- 临时：调大 pm.max_children=120，pm.start_servers=40
- Java 服务 JVM 参数调整，增加内存 headroom
- 验证：5xx 降至 <1%，响应延迟恢复

范例 B：MySQL 连接超时

连接池配置不匹配引发的服务中断

P1 故障

时间信息

2025-12-02 14:20–14:50（30分钟）

影响范围

订单写入失败

现象与告警
ProxySQL/业务报错 "Lost connection to MySQL server during query"；Show processlist 显示大量 Sleep 线程超过 wait_timeout

关键排查证据

```
# Prometheus 指标
Aborted_clients/Threads_running 飙升
slow log: 缺失索引的更新语句持锁
事务隔离: REPEATABLE READ，长事务阻塞
```

根因结论
应用侧连接池配置与 MySQL wait_timeout 不匹配；热点行更新缺索引，造成锁等待与连接堆积

时间信息

2025-12-01 10:00–10:25（25分钟）

影响范围

日志无法写入，业务只读

现象与告警
df -h 显示 / 100%；Inodes 亦 100%；IO 卡顿；logrotate 失败

关键排查证据

```
du -sh /* 发现:
/var/log/audit/audit.log 巨大
docker/overlay2 占用高
未清理 core/crashdump
```

后续改进

- 为 /var/log/audit 设独立分区
- logrotate 日更；接入 eBPF/OpenObserve
- 为 Docker 设数据保留策略

三、运维笔记标准化规范

元信息头（YAML Front Matter）

```yaml
---
Title: "[简短准确]"
Created: "2025-12-03T10:00+08:00"
Updated: "2025-12-03T14:30+08:00"
Environment: "prod"
Region: "cn-east-1"
Version: "nginx/1.24.0"
Owner: "@ops-team"
Tags: ["nginx", "502", "php-fpm", "incident"]
Source: "ansible-playbook"
---
```

内容结构

1. **Objective/背景**
   目标与边界说明
2. **References**
   RF/设计文档、Dashboard、Runbook 链接
3. **Prerequisites/前置条件**
   权限、证书、白名单、变更窗口
4. **Step-by-step**
   编号命令/配置/脚本，附带预期输出
5. **Verification + Rollback**
   验收标准与回滚方案

Markdown | Confluence | Notion

```markdown
# Nginx 502 故障处理 | 2025-12-03

**环境**: prod | **所有者**: @ops-team | **标签**: nginx, 502, incident

---

## 背景/目标
解决 PHP-FPM 进程耗尽导致的 502 错误

## 前置条件
```

```
- [x] 已申请变更窗口
- [x] 已备份配置文件

## 步骤
1. `systemctl status php-fpm`
   - 期望：active (running)
2. `pm.status_path` 检查队列状态
   - 预期：waiting < max_children * 0.2

## 验证
- `curl -I http://health-check | grep 200`
- Dashboard: [Grafana Link]

## 回滚
```bash
cp /etc/php-fpm.d/www.conf.bak /etc/php-fpm.d/www.conf
systemctl restart php-fpm
```
```

四、自动化生成可检索笔记

Ansible 日志 → 笔记

1. 结构化输出

```
ansible-playbook -i inventory site.yml -vvv \
--output=/var/log/ansible/run-{{YYYYMMDD}}.json
```

2. 关键字段

timestamp host task result changed failed duration

3. 推送方式

- **Markdown**：脚本渲染 → Git commit/PR
- **Confluence**：REST API 创建"变更记录"页面
- **Notion**：API 插入结果到 Database

Zabbix 告警 → 笔记

触发器动作 → Webhook

PROBLEM 状态时自动生成"事件快照"页面

预填字段：时间、主机、问题名称、
严重性、原始值、图形链接、建议步骤

RESOLVE 时追加

- 处置结果 / 根因分析
- 规避措施 / 后续改进
- 自动打标签 `resolved`

数据源字段映射

```
event.id → 笔记标题
trigger.name → 问题分类
item.value → 指标快照
graph.url → 可视化嵌入
```

检索增强体系

统一标签体系

service/component/env/incident-id/change-id 五维标签

全文索引方案

- Obsidian/Logseq: ripgrep + fzf
- Notion: 高级搜索语法
- Confluence: CQL 查询

别名/同义词

502 / BadGateway / upstream error → 统一标签 nginx-502

落地建议

1

最小可用模板

先建 Runbook/Incident/Change 各一个，强制包含"步骤/验证/回滚"

2

存量迁移

批量转换既有笔记，统一命名：YYYY-MM-DD-主题-简述.md

3

自动化流水线

CI/CD 定时拉取 Ansible/Zabbix 数据，渲染推送，人工校对发布

4

持续改进

定期回顾 Top N 高频故障，补齐监控/告警/自动化