

服务器日常巡检表

巡检日期： 年 月 日
巡检人：
服务器标识/名称：
IP 地址：
物理位置/机房：
巡检周期： ☐ 每日 ☐ 每周 ☐ 每月

一、 硬件状态检查

检查项目	正常范围/状态	检查结果	备注
电源状态	所有电源单元 (PSU) 状态正常 (绿灯)	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	双电是否都正常?
风扇状态	所有风扇运转正常, 无告警	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	注意转速和噪音
CPU 温度	< 75°C (具体参考服务器手册)	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	通过iDRAC/iLO/BIOS查看
内存状态	无ECC错误或告警	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	
磁盘指示灯	无橙色/红色告警灯 (通常蓝色/绿色)	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	物理查看硬盘柜
RAID 状态	所有虚拟磁盘状态为“Optimal”	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	进入RAID卡管理界面查看
物理磁盘	所有物理磁盘状态“Online”, 无预测性故障	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	检查是否有坏块警告
网络链路	网卡链路灯正常, 端口无错误包	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	ethoo1 <接口名>
外设状态	无异常报警或错误日志	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	

(对于品牌服务器, 如Dell的DRAC, HP的iLO, IBM的MM, 是检查以上硬件状态的最佳工具)

二、 操作系统状态检查 (以Linux为例, Windows附后)

检查项目	命令/方法 (Linux)	正常范围/状态	检查结果	备注
系统运行时间	<code>uptime</code>	无意外重启	<div><div></div></div>	确认运行时长
CPU 使用率	<code>top</code> 或 <code>vmstat 1 5</code>	平均 < 80%	<div><div><div>□ 正常</div><div>□ 偏高</div><div>□ 异常</div></div></div>	关注 %idle 和 %wa
内存使用率	<code>free -h</code>	剩余可用 > 20%	<div><div><div>□ 正常</div><div>□ 偏高</div><div>□ 异常</div></div></div>	关注 available 列
Swap 使用	<code>free -h</code> 或 <code>swapon -s</code>	使用率 ≈ 0%	<div><div><div>□ 正常</div><div>□ 异常</div></div></div>	若使用较多需关注
磁盘空间使用	<code>df -h</code>	根分区/ 使用率 < 90%	<div><div><div>□ 正常</div><div>□ 警告</div><div>□ 危险</div></div></div>	重点检查常用分区
磁盘 I/O 状态	<code>iostat -x 1 3</code>	%util < 90%, await 较低	<div><div><div>□ 正常</div><div>□ 偏高</div><div>□ 异常</div></div></div>	
网络连接数	<code>ss -s</code> 或 <code>netstat -an</code>	无骤增, ESTAB 数在正常范围	<div><div><div>□ 正常</div><div>□ 异常</div></div></div>	
关键进程状态	<code>systemctl status <服务名></code> 或 <code>ps -ef grep <进程名></code>	所有关键服务状态为 active (running)	<div><div><div>□ 正常</div><div>□ 异常</div></div></div>	如nginx, mysql, tomcat等
系统日志	<code>tail -100 /var/log/messages</code> 或 <code>journalctl -xe --since "2 hours ago"</code>	无 Error, Critical, Fail 等关键字	<div><div><div>□ 正常</div><div>□ 警告</div><div>□ 异常</div></div></div>	
root 邮件	<code>mail</code>	无关键告警邮件	<div><div><div>□ 正常</div><div>□ 异常</div></div></div>	

Windows服务器补充检查：

- **事件查看器：**检查 windows日志 -> 系统 和 应用程序，筛选 错误 和 警告。
- **任务管理器：**直观查看CPU、内存、磁盘、网络性能。
- **服务控制台 (services.msc)：**确认关键服务是否运行。
- **资源监视器：**深入分析磁盘I/O、网络活动。

三、应用与服务状态检查

检查项目	检查方法	正常状态	检查结果	备注
Web 服务	浏览器访问/ <code>curl -I http://localhost</code>	返回 200 OK	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	
数据库 服务	<code>mysql -uxx -pxx -e "status;"</code> 或 <code>SELECT 1;</code>	连接成功, 查询正常	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	如MySQL, PostgreSQL
中间件 服务	通过管理端口或控制台连接	状态为 "Running"	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	如Tomcat, Weblogic
备份任务	检查备份日志或备份文件日期	最近备份成功完成	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	确认文件大小和日期
定时任务	<code>crontab -l</code> 并检查 <code>/var/log/cron</code> 日志	无失败或长期运行任务	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	
应用业务日志	<code>tail -f /path/to/your/app.log</code>	无错误、异常堆栈信息	<input type="checkbox"/> 正常 <input type="checkbox"/> 警告 <input type="checkbox"/> 异常	

四、 安全性与网络检查

检查项目	检查方法	正常状态	检查结果	备注
防火墙 状态	<code>systemctl status firewalld</code> 或 <code>ufw status</code>	运行中, 策略正确	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	
SSH 登录日志	<code>last</code> 和 <code>grep "Failed password" /var/log/secure</code>	无未知IP的失败登录尝试	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	防暴力破解
开放端口	<code>ss -tulnp</code> 或 <code>netstat -tulnp</code>	无未知、非授权端口开放	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	
病毒扫描	(如有) 检查病毒库日期和扫描日志	病毒库最新, 无感染	<input type="checkbox"/> 正常 <input type="checkbox"/> 异常	

五、 巡检总结与处理意见

本次巡检总体评估:	<input type="checkbox"/> 一切正常 <input type="checkbox"/> 存在隐患 <input type="checkbox"/> 发现故障 <input type="checkbox"/> 需紧急处理
发现的问题及处理记录:	
1. 问题描述:	
原因分析:	
处理过程与结果:	
2. 问题描述:	
原因分析:	
处理过程与结果:	
后续优化建议:	(如: 扩容磁盘、调整内核参数、清理日志等)

使用建议:

- 1. **自动化:** 尽量使用脚本 (Shell/Python) 自动化收集大部分信息 (如CPU、内存、磁盘空间), 人工主要负责分析和判断。
- 2. **监控系统:** 对于大型或重要业务, 应使用Zabbix, Prometheus, Nagios等专业监控系统进行7x24小时监控, 巡检表作为补充和深度检查。
- 3. **定期评审:** 定期回顾巡检表中发现的问题, 优化巡检项和频率。
- 4. **文档化:** 妥善保存每次的巡检记录, 便于追溯和分析系统长期运行状态。