«[#list list as item]»

# . «${item.app\_ip}»

## OS基础信息

|  |  |
| --- | --- |
| 巡检项目 | 检查结果 |
| ip | «[#if (item.osinfo.IP\_Address)??]${item.o» |
| 主机名 | «[#if (item.osinfo.Hostname)??]${item.osi» |
| 操作系统位数 | «[#if (item.osinfo.Architecture)??]${item» |
| 操作系统内核版本 | «[#if (item.osinfo.Kernel\_Release)??]${it» |
| 物理内存 | «[#if (item.osinfo.Physical\_Memory)??]${i» |
| CPU核数 | «[#if (item.osinfo.Cpu\_Cores)??]${item.os» |
| 逻辑CPU个数 | «[#if (item.osinfo.Cpu\_Proc\_Num)??]${item» |
| 运行时间 | «[#if (item.osinfo.Uptime)??]${item.osinf» |
| 平均系统负载 | «[#if (item.osinfo.Load)??]${item.osinfo.» |
| 内存总量 | «[#if (item.osinfo.MemTotal)??]${item.osi» |
| 空闲内存 | «[#if (item.osinfo.MemUsed)??]${item.osin» |
| 内存占用率 | «[#if (item.osinfo.Mem\_Rate)??]${item.osi» |
| Openfile | «[#if (item.osinfo.Openfile)??]${item.osi» |
| Swap\_Method | «[#if (item.osinfo.Swap\_Method)??]${item.» |
| 磁盘总量 | «[#if (item.osinfo.Totalsum)??]${item.osi» |
| 磁盘已使用总量 | «[#if (item.osinfo.Usesum)??]${item.osinf» |
| 磁盘占用率 | «[#if (item.osinfo.Diskutil)??]${item.osi» |
| IO\_Idle | «[#if (item.osinfo.IO\_Idle)??]${item.osin» |
| TCP配置 | «Tcp\_Tw\_Recycle: ${item.osinfo.Tcp\_Tw\_Rec»  «Tcp\_Tw\_Reuse: ${item.osinfo.Tcp\_Tw\_Reuse»  «Tcp\_Fin\_Timeout: ${item.osinfo.Tcp\_Fin\_T»  «Tcp\_Fin\_Timeout: ${item.osinfo.Tcp\_Keepa»  «Tcp\_Fin\_Timeout: ${item.osinfo.Tcp\_Keepa» |

## ActiveMQ基础信息

|  |  |
| --- | --- |
| 巡检项目 | 检查结果 |
| AMQ安装目录 | «[#if (amqinfo.activemqHome)??]${amqinfo.» |
| AMQ运行目录 | «[#if (amqinfo.activemqBase)??]${amqinfo.» |
| AMQ 版本信息 | «[#if (amqinfo.amqversion)??]${amqinfo.am» |
| AMQ数据目录 | «[#if (amqinfo.activemqData)??]${amqinfo.» |
| AMQ配置文件 | «[#if (amqinfo.activemqConfigfile)??]${am» |
| AMQ JVM参数 | «[#if (amqinfo.server\_jvm)??]${amqinfo.se» |
| AMQ运行用户 | «[#if (amqinfo.runUser)??]${amqinfo.runUs» |
| AMQ配置信息 | «[#if (amqinfo.amqconfiginfo)??]${amqinfo» |

## ActiveMQ运行分析

|  |  |
| --- | --- |
| 巡检项目 | 检查结果 |
| AMQ 队列运行 | «[#if (amqinfo.queuestatus)??]${amqinfo.q» |
| AMQ topic运行 | «[#if (amqinfo.topicstatus)??]${amqinfo.t» |

## ActiveMQ安全基线检查

|  |  |  |  |
| --- | --- | --- | --- |
| 检查项目 | 基线规则 | 检查结果 | 检查结论 |
| ActiveMQ版本 | ActiveMQ应用服务器各版本都存在安全漏洞，需要及时安装厂商提供的安全补丁 | «[#if (amqinfo.amqversion)??]${amqinfo.am» |  |
| 禁止特权身份运行 | Pass：使用非root用户运行Activemq  Failed:特权用户身份运行ActiveMQ | «[#if (amqinfo.runUser)??]${amqinfo.runUs» | «[#if (amqinfo.runUserResult)??]${amqinfo» |
| 默认账号密码身份鉴别 | activemq管理控制台默认的账号和密码为admin，建议修改默认账号和密码 | «[#if (amqinfo.securityauth)??]${amqinfo.» | «[#if (amqinfo.securityauthresult)??]${am» |
| 设置启用activemq的消息后台认证机 | 若不设置启用activemq的消息后台认证机制，任何知道activemq服务的IP、端口和消息地址的人，都可以接受和发送消息，存在严重的安全隐患 | «[#if (amqinfo.securityplugin)??]${amqinf» | «[#if (amqinfo.securitypluginresult)??]${» |
| fileserver服务接口服务配置 | fileserver是一个存储文件的restful api接口，支持GET、PUT、DELETE等HTTP请求，存在文件上传，文件移动，信息泄露等高危漏洞。5.14.0以后的版本已经删除该接口，5.14.0以前版本修复建议：修改配置文件<activemq\_path>/conf/jetty.xml，找到id=securityHandler项：将配置的value值修改为/fileserver的项删除。修改完成后保存并重启activemq服务 | «[#if (amqinfo.fileserverbug)??]${amqinfo» | «[#if (amqinfo.fileserverbugResult)??]${a» |

## ActiveMQ日志分析

## 总结

ActiveMQ服务运行状态良好。