«[#list list as item]»

### «${item?index+1}». «${item.app\_ip}»

### 1.1 OS基础信息

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

### 1.2 Zookeeper基础信息

|  |  |
| --- | --- |
| 巡检项目 | 检查结果 |
| Zookeeper\_mode | «[#if (item.Zookeeper\_mode)??]${item.Zookeeper\_mode}[/#if]» |
| Zookeeper安装路径 | «[#if (item.Installation\_path)??]${item.Installation\_path}[/#if]» |
| 启动用户 | «[#if (item.Start\_User)??]${item.Start\_User}[/#if]» |
| JVM安装路径 | «[#if (item.JVM\_Instal\_path)??]${item.JVM\_Instal\_path}[/#if]» |
| JVM运行参数 | «[#if (item.JVM\_run\_parameters)??]${item.JVM\_run\_parameters}[/#if]» |
| Zookeeper\_Port | «[#if (item.Server\_Port)??]${item.Server\_Port}[/#if]» |
| zookeeper配置信息 | «[#if (item.Zookeeper\_config)??]${item.Zookeeper\_config}[/#if]» |

### 1.3 Zookeeper运行状态

|  |
| --- |
| «[#if (item.Zookeeper\_runtime\_status)??]${item.Zookeeper\_runtime\_status}[/#if]» |

### 1.4 Zookeeper安全基线信息

|  |  |  |  |
| --- | --- | --- | --- |
| 检查项 | 基线规则 | 检查结果 | 检查结论 |
| Zookeeper端口 | Pass:采用非默认2181端口  Failed:采用默认端口  建议:修改zookeeper默认监听端口2181为不易猜测的端口。 | «[#if (item.Security\_Baseline\_Port)??]${item.Security\_Baseline\_Port}[/#if]» | «[#if (item.Security\_Baseline\_Port1)??]${item.Security\_Baseline\_Port1}[/#if]» |
| Zookeeper客户端的最大连接数 | Pass:设置zk管理客户端最大连接数  Failed:不设置zk管理客户端最大连接数  建议:预防DOS攻击;建议限制zookeeper客户端的最大连接数。 | «[#if (item.Security\_Baseline\_MaxClientCnxns)??]${item.Security\_Baseline\_MaxClientCnxns}[/#if]» | «[#if (item.Security\_Baseline\_MaxClientCnxns1)??]${item.Security\_Baseline\_MaxClientCnxns1}[/#if]» |
| Zookeeper的管理控制台 | Pass:关闭zk管理控制台  Failed:开启zk管理控制台  建议:zookeeper的管理控制台，建议禁用。 | «[#if (item.Security\_Baseline\_Console)??]${item.Security\_Baseline\_Console}[/#if]» | «[#if (item.Security\_Baseline\_Console1)??]${item.Security\_Baseline\_Console1}[/#if]» |
| Zookeeper的授权访问 | Pass:非world:anyway的权限配置  Failed:world:anyway的权限配置  建议:zookeeper的授权访问。 | «[#if (item.Security\_Baseline\_Acl)??]${item.Security\_Baseline\_Acl}[/#if]» | «[#if (item.Security\_Baseline\_Acl1)??]${item.Security\_Baseline\_Acl1}[/#if]» |
| Zookeeper的日志审计 | Pass:开启zk日志审计功能  Failed:不开启zk日志审计功能  建议:zookeeper的日志审计，依据实际需求决定是否开启。 | «[#if (item.Security\_Baseline\_Audit)??]${item.Security\_Baseline\_Audit}[/#if]» | «[#if (item.Security\_Baseline\_Audit1)??]${item.Security\_Baseline\_Audit1}[/#if]» |
| Zookeeper的事务日志与快照日志分离 | Pass:配置zoo.cfg中的日志与快照日志分离  Failed:不配置zoo.cfg中的日志与快照日志分离  建议:zookeeper的事务日志与快照日志分离。 | «[#if (item.Security\_Baseline\_Log)??]${item.Security\_Baseline\_Log}[/#if]» | «[#if (item.Security\_Baseline\_Log1)??]${item.Security\_Baseline\_Log1}[/#if]» |
| Zookeeper的日志清理 | Pass:配置zoo.cfg中的日志自动清理策略  Failed:不配置zoo.cfg中的日志自动清理策略  建议:zookeeper的日志清理建议配置。 | «[#if (item.Security\_Baseline\_Clean)??]${item.Security\_Baseline\_Clean}[/#if]» | «[#if (item.Security\_Baseline\_Clean1)??]${item.Security\_Baseline\_Clean1}[/#if]» |
| Zookeeper的非特权用户运行 | Pass:采用特权用户启动zk进程  Failed:采用非特权用户启动zk进程  建议:建议修改zookeeper的非特权用户运行。 | «[#if (item.Security\_Baseline\_Root)??]${item.Security\_Baseline\_Root}[/#if]» | «[#if (item.Security\_Baseline\_Root1)??]${item.Security\_Baseline\_Root1}[/#if]» |
| Zookeeper的目录权限控制 | Pass:采用非特权用户设置zk目录权限  Failed:采用特权用户设置zk目录权限  建议:zookeeper的目录权限控制建议限制。 | «[#if (item.Security\_Baseline\_Dir)??]${item.Security\_Baseline\_Dir}[/#if]» | «[#if (item.Security\_Baseline\_Dir1)??]${item.Security\_Baseline\_Dir1}[/#if]» |
| Zookeeper限制监听地址 | Pass:设置固定监听地址  Failed:不设置固定监听地址  建议:修改zookeeper默认监听端口2181为不易猜测的端口。 | «[#if (item.Security\_Baseline\_ClientPortAddress)??]${item.Security\_Baseline\_ClientPortAddress}[/#if]» | «[#if (item.Security\_Baseline\_ClientPortAddress1)??]${item.Security\_Baseline\_ClientPortAddress1}[/#if]» |
| Zookeeper四字命令 | Pass:不配置四字命令  Failed:配置四字命令  建议:关闭zookeeper四字命令。 | «[#if (item.Security\_Baseline\_4lw)??]${item.Security\_Baseline\_4lw}[/#if]» | «[#if (item.Security\_Baseline\_4lw1)??]${item.Security\_Baseline\_4lw1}[/#if]» |

### 1.5 日志审查

|  |
| --- |
| «${item.Check\_log\_health}» |

### 1.6 总结

Zookeeper服务运行良好。

«[/#list]»