ECS 云服务器

安全巡检

操

作

手

册

北京环宇数通科技有限公司

中国领先的云安全服务商

2024 年 3 月

前 言

云计算极大提升了企事业单位的信息化效能，国内外云计算厂商都提供了全面的弹性计算能力，提供了更高效率、更加安全以及更低运维成本的云平台。

面对功能如此强大的云计算平台，是否还有必要进行定期的人工巡检工作呢？回答是肯定的。

任何软件系统都会有不完善的地方，包括云平台本身也都在进行不断的软件版本升级，因此定期对云平台上的信息系统进行人工巡检是非常有必要的。巡检工作可以预防故障、保障安全、性能优化和规范管理，同时可以发现闲置资源或低使用率资源，进行调整而降低成本，还可以提前发现安全问题，提升服务质量，并满足等保合规要求，以及更好的应对未来突发的安全事件。

图：巡检维护的八大价值

本文将以阿里云 ECS 云服务器为例进行说明，其他云计算平台的安全巡检指标类似！更多的云产品和云安全产品的巡检操作手册，敬请期待！

目 录

一、ECS 巡检指标项 4
二、ECS 巡检操作 5
1. ECS 到期时间 5
2. 运行状态 7
3. CPU、内存和磁盘使用率 8
4. 安全组规则配置 9
5. 云盘快照备份策略 10
6. DDoS 基础防护状态 12
7. 云监控 agent 运行状态 12
8. 云监控告警规则配置 13
9. 云监控告警联系人配置 13
10. 云安全中心 agent 运行状态 15
三、ECS 巡检结论 16

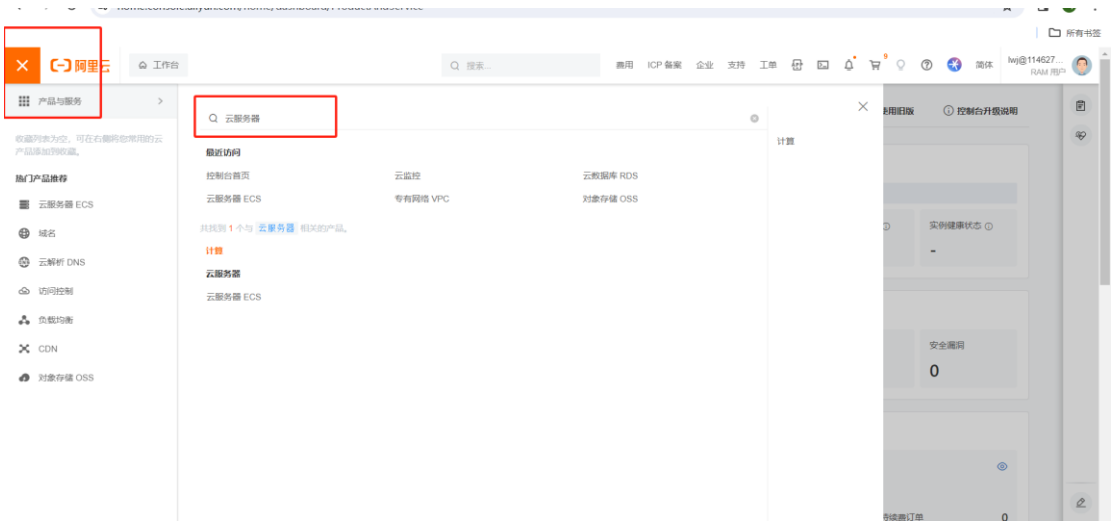
一、ECS 巡检指标项

序号	巡检指标	巡检描述
1	到期时间	查看实例到期，到期时间应大于一个巡检周期。
2	运行状态	查看服务器状态是否为正常“运行”状态。
3	CPU 使用率	查看服务器最近一个月 CPU 使用率平均值和峰值，是否属于合理区间（平均 30-50%，峰值不持续高于 85%）
4	内存使用率	查看服务器最近一个月内存使用率，是否属于合理区间（平均 30-50%，峰值不持续高于 85%）
5	磁盘空间使用量	查看服务器最近一个月磁盘占有率，是否低于 80%。
6	安全组规则配置	查看服务器安全组端口开放情况，以及 IP 地址授权，确认开放端口都是已经业务端口和授权 IP。
7	云盘快照备份策略	查看是否开启了云盘数据自动快照策略，以及自动快照策略配置合理，符合业务备份要求。
8	DDoS 基础防护状态	查看 DDOS 基础防护是否开启，可查看 DDOS 运行状态。
9	云监控 agent 运行状态	查看云监控 agent 是否正常运行，所有服务器的云监控 agent 都为运行状态。
10	云监控 告警规则	查看告警规则设置，配置了云服务器合理告警规则。
11	云监控 告警联系人配置	查看是否正确设置了告警联系人。
12	云安全中心 Agent 运行状态	查看云安全中心 agent 是否正常运行，所有服务器的云安全中心都为在线状态。

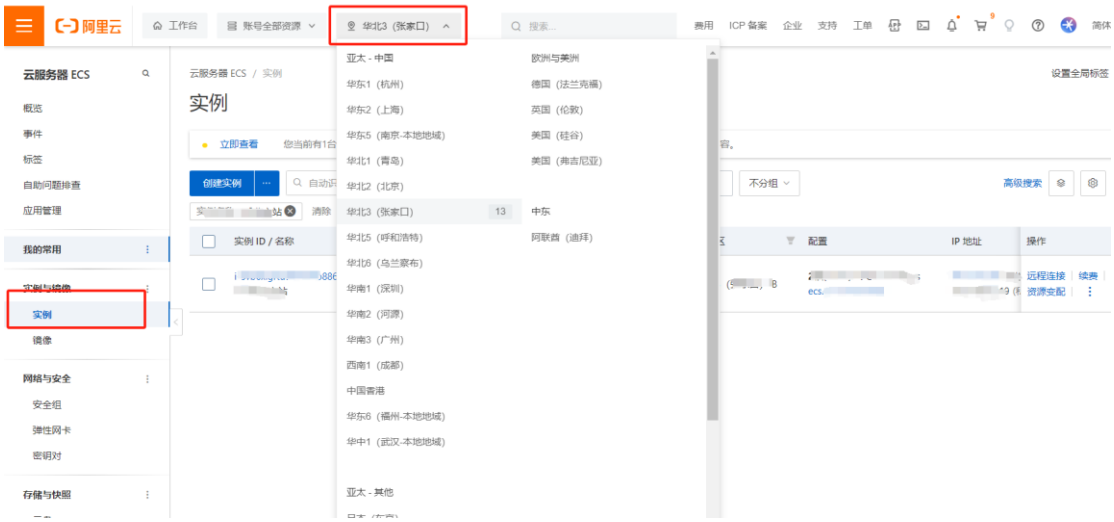
二、ECS 巡检操作

1. ECS 到期时间

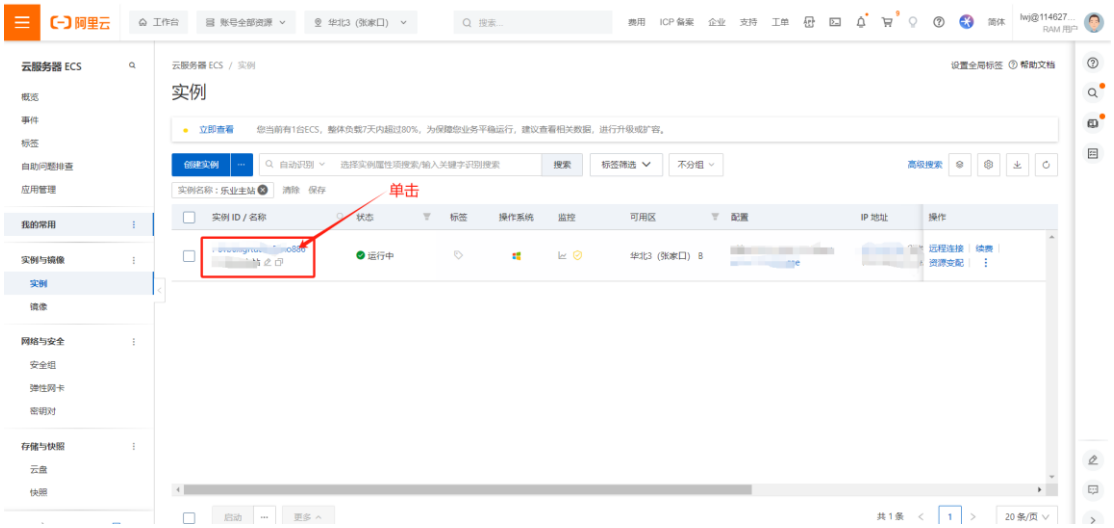
登录阿里云官网，点击右上角“控制台”，在控制台界面的搜索框中，输入“云服务器”：



实例➡地域➡点击实例服务器查看详情，查看到期时间：




阿里云
云服务器 ECS
实例
创建实例
搜索
运行中


阿里云
云服务器 ECS
实例
创建实例
搜索
单击
运行中


云服务器 ECS
运行中
远程连接
重启
实例详情
监控
安全组
云盘
快照一致性组
快照
弹性网卡
定时与自动化任务
操作记录
健康诊断
事件
基本信息
实例ID
实例名称
实例状态
运行中 停止 重启
所在可用区
张家口 可用区B
付费类型
包年包月
到期时间
2024年11月10日 23:59:59到期 续费
健康状态
正常 实例问题排查 实例问题排查历史
重要事件告警
暂无重要事件告警信息
安全防护
安全问题总数
1
Top 5 待处理任务

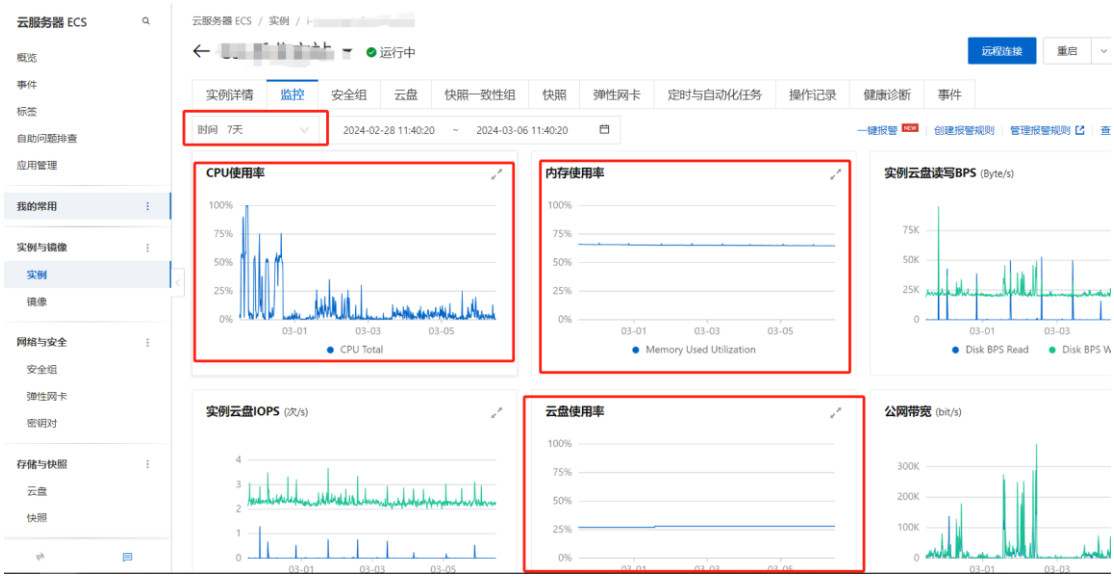
2. 运行状态

“实例状态”为绿色“运行中”：

3. CPU、内存和磁盘使用率

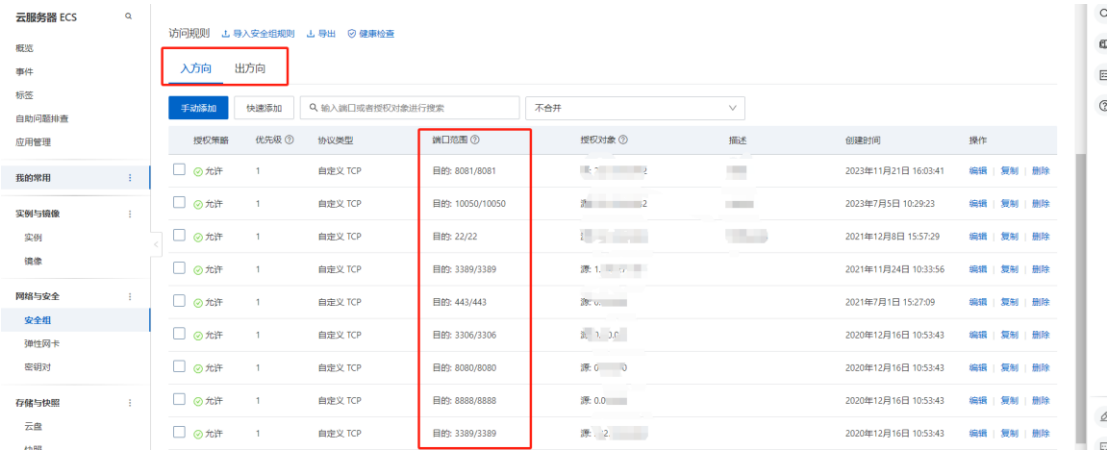
查看服务器第二个选项➡监控

备注：可点击查看更多指标（查看云监控）



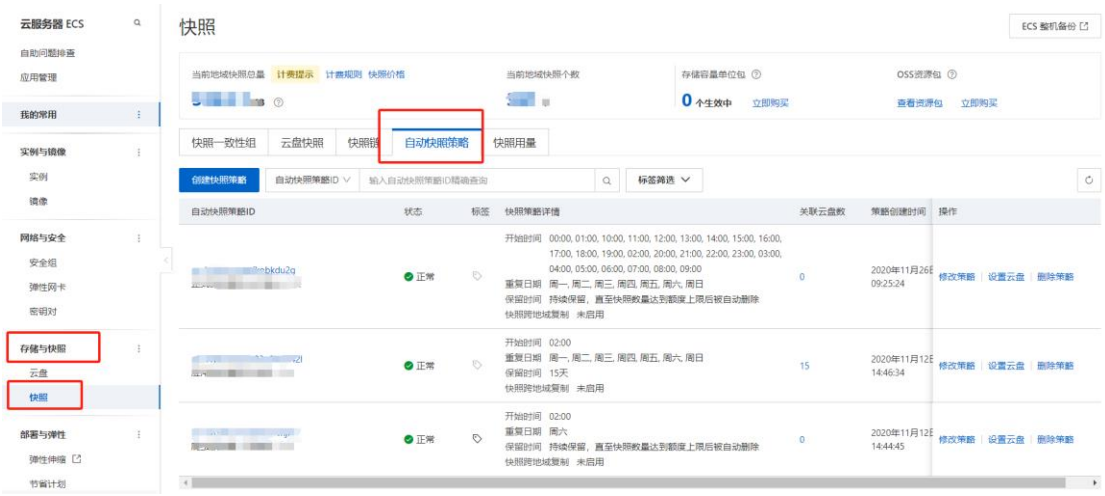
4. 安全组规则配置

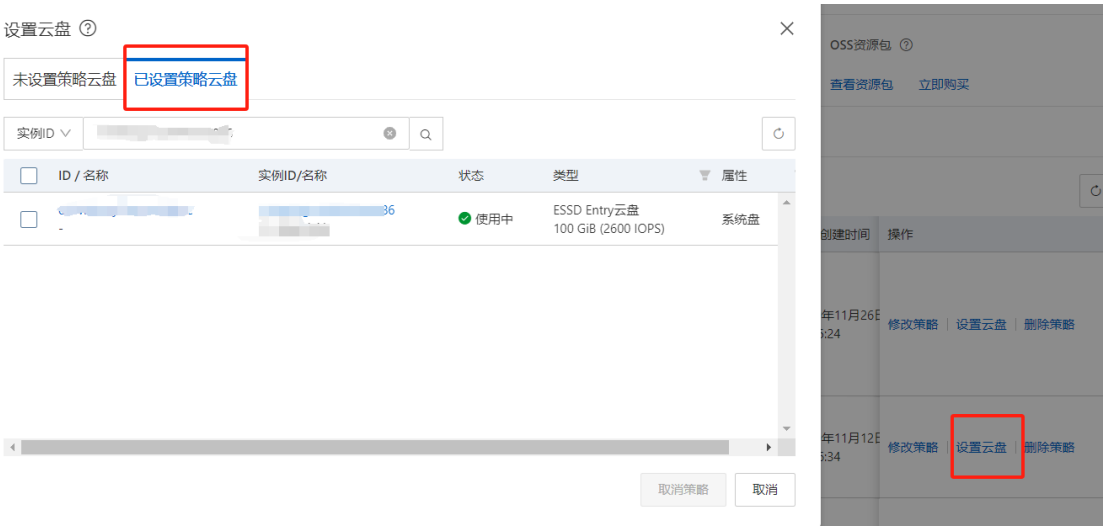
查看服务器第三个选项➡安全组



5. 云盘快照备份策略

选择云服务器左侧存储与快照➡快照➡自动快照策略





备注：按照自己的业务情况设置快照策略，添加云盘

6. DDoS 基础防护状态

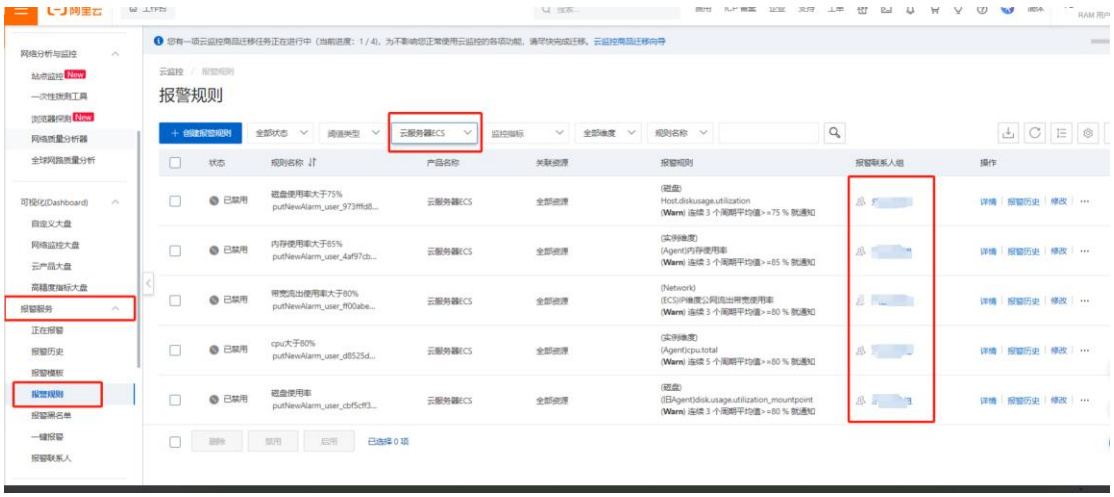
点击“实例”，右侧界面右下侧“DDoS 基础防护”：

7. 云监控 agent 运行状态

Agent 状态显示“运行中”为正常，否则就为非正常情况，将无法实现 7*24 云监控。

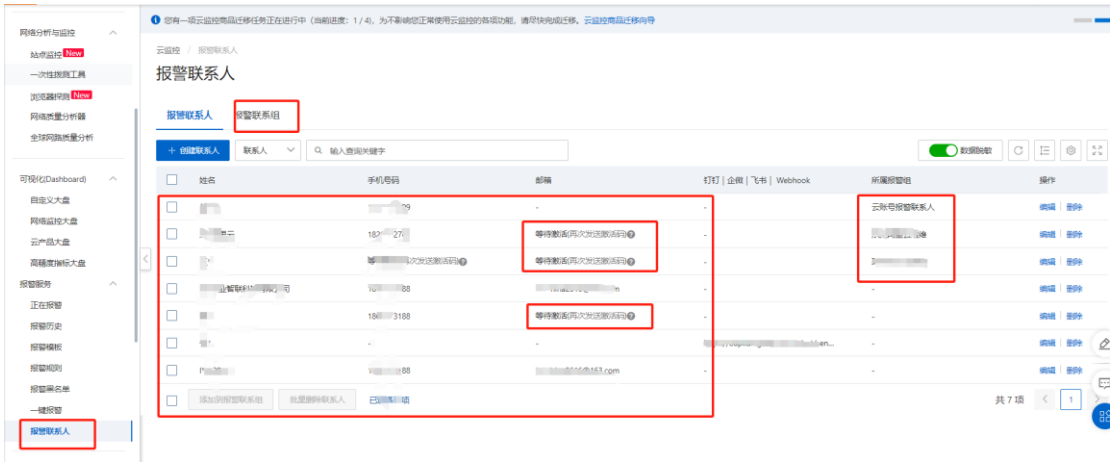
8. 云监控告警规则配置

云监控➡报警服务（左侧菜单）➡报警规则



9. 云监控告警联系人配置

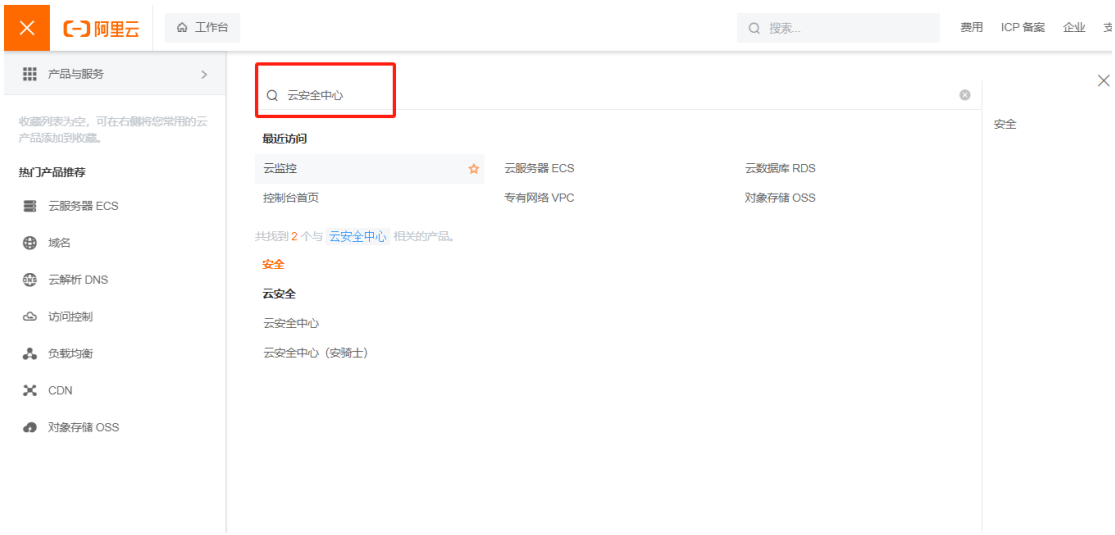
云监控➡报警联系人（左侧菜单）

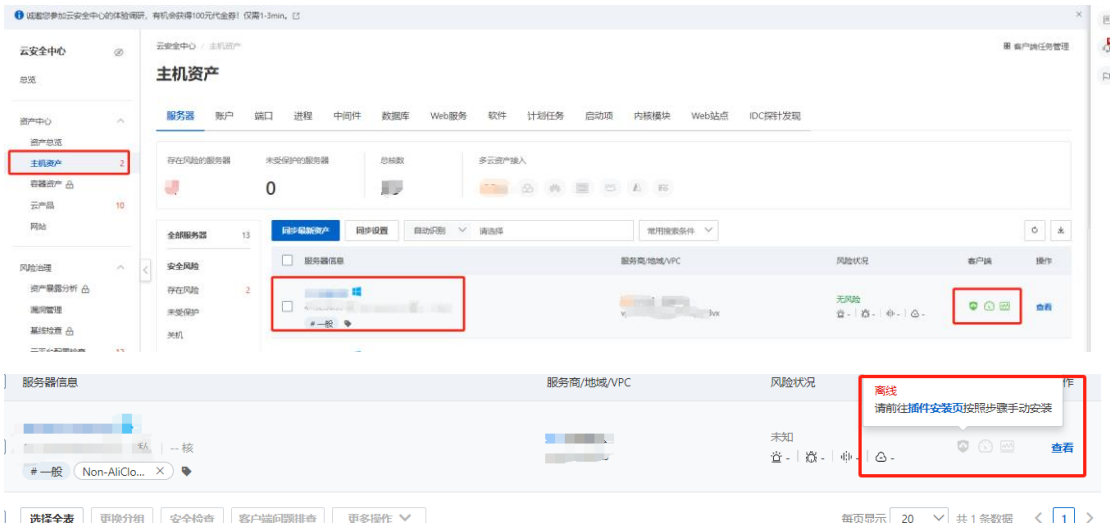


备注：查看手机号与邮箱是否激活，报警联系组是否添加。

10. 云安全中心 agent 运行状态

云安全中心➡主机资产（左侧菜单）





备注：如果没有安装活异常呈现上图所状

三、ECS 巡检结论

ECS 巡检时间： ECS 巡检人员：				
序号	巡检指标	巡检描述	正常	建议
1	到期时间	查看实例到期，到期时间应大于一个巡检周期。	正常/非正常	下一个巡检周期
2	运行状态	查看服务器状态是否为正常“运行”状态。		
3	CPU 使用率	查看服务器最近一个月 CPU 使用率平均值和峰值，是否属于合理区间（平均 30-50%，峰值不持续高于 85%）		
4	内存使用率	查看服务器最近一个月内存使用率，是否属于合理区间（平均 30-50%，峰值不持续高于 85%）		
5	磁盘空间使用量	查看服务器最近一个月磁盘占有率，是否低于 80%。		
6	安全组规则配置	查看服务器安全组端口开放情况，以及 IP 地址授权，确认开放端口都是已经业务端口和授权 IP。		
7	云盘快照备份策略	查看是否开启了云盘数据自动快照策略，以及自动快照策略配置合理，符合业务备份要求。		
8	DDoS 基础防护状态	查看 DDOS 基础防护是否开启，可查看 DDOS 运行状态。		
9	云监控 agent 运行状态	查看云监控 agent 是否正常运行，所有服务器的云监控 agent 都为运行状态。		
10	云监控告警规则	查看告警规则设置，配置了云服务器合理告警规则。		
11	云监控告警联系人配置	查看是否正确设置了告警联系人。		
12	云安全中心 Agent 运行状态	查看云安全中心 agent 是否正常运行，所有服务器的云安全中心都为在线状态。		