**等保测评之上云篇**

# 一、阿里云

===============================================================================

**根据等保安全点进行分析**

（一）、针对web网站系统

1、网站防篡改、web应用攻击防护、CC恶意攻击安全防护、网站一键https、SQL注入等。

2、推荐使用：云WAF

3、安全等级：高

（二）恶意代码防范方面

1、linux主机：安装clamav开源杀毒软件 windows主机：安装360、瑞星等

2、推荐使用：态势感知、安骑士（态势感知包含安骑士基本上所有功能）

3、安全等级：中

（三）入侵防范方面和抗ddos攻击（针对游戏行业）

1、推荐使用：态势感知、安骑士（是否合理？）、抗D高防IP

2、安全等级：高

（四）安全审计和日志方面（应用日志，操作系统日志，网络日志，安全事件日志）

1、linux主机：rsyslog、auditd进程开启 windows主机：安全策略勾选 数据库：c2等安全策略勾选或者my.cnf文件中配置log命令

2、推荐使用：云堡垒机、数据库审计、态势感知（有日志分析平台功能，但是否符合？）、云WAF（有日志管理功能，是否符合？）、

或者自己搭建日志服务器（对于开源的jumpserver（开源堡垒机，基本符合收费堡垒机功能）、zabbix（除监控外，也有审计和日志功能）是否满足？）

3、安全等级：高

（五）操作审计、账号管理权限分配、双因子认证、远程安全管理

1、推荐使用：云堡垒机

2、安全等级：中

**阿里云中一些细节问题：**

1、凡是租用或购买阿里云服务器的，阿里云免费提供5G抗DDOS高防

2、购买安骑士或态势感知，会以账号绑定总的ECS服务器数量进行购买

**四川抽查工作重点：**

1. 系统所包含的服务器、数据库、网络及安全产品等重要资产是否齐全，不能出现虚报资产

我要等保：针对那些将系统分类进行等保测评的项目，需要统计所有的资产（比如迈齐科技）；对于那种由一套系统组成（比如：3个服务器、2套数据库），当新增加客户业务时就clone一份同样的系统配置，这种情况统计资产的时候，需要把所有的业务资产统计（比如：3个客户资源，这个系统的资产就应该是9个服务器、6套数据库）

1. 网络安全职责是否明确，是否有明确的主管领导、分管领导、责任部门且同一人员不得兼任

我要等保：制度中的系统应急预案和单位网络安全管理机构设置情况说明

1. 是否用明确的信息发布审核、登记制度，违法有害信息审核、清除制度、病毒检测和漏洞检测等管理制度

我要等保：管理制度测评报告中重点关注这几点进行判断扣分

1. 日志保存时间是否达到六个月，日志包括：主机、网络、数据库、应用，日志包含的内容：ip地址、访问时间、源端口号等关键类型。日志记录是否异机实时备份。

我要等保：日志包括系统所关联的日志，要满足日志的完整性和可追踪溯源，强烈建议日志审计系统

1. 数据传输是否加密保护，登录是否有二次验证机制，数据存储是否加密保护

我要等保：登录是否有二次验证机制就是针对测评中的双因子认证

1. 是否用web应用防护、入侵防范、病毒木马查杀等安全措施

我要等保：这一点就是对安全设备或安全服务明确指出

1. 是否存在操作系统、中间件、数据库及其他容易导致黑客攻击入侵非法获取服务器权限的高危漏洞

我要等保：这点覆盖测评中漏扫和渗透部分

===============================================================================

## 1 现场测评内容

物理安全和网络安全没有进行测评，但是物理机房的信息需要记录；网络安全中的安全产品需要记录，并且要获取销售许可证，如果需要对网络架构测评，那么需要询问阿里云提供网络结构的截图；剩下的按照非云系统进行测评。

## 2 阿里云和云租户责任划分

### 2.1 合规责任共担

阿里云平台与云上租户系统分别定级和测评

阿里云平台测评结论可供租户系统测评时复用



### 2.2 阿里云提供资料

阿里云平台等保备案证明 阿里云测评报告关键页

阿里云云盾销售许可证 阿里云部分测评项说明

我要等保：阿里云的云盾产品都只用一个销售许可证

### 2.3 责任分担详解

阿里云的公共云、电子政务云通过等级保护三级备案和测评；金融云通过等级保护四级的备案和测评。

根据监管部门明确的结论复用原则，阿里云上的租户系统通过等级保护测评时，物理安全、部分网络安全和安全管理的结论可以复用，阿里云可提供说明。

## 3 《网络安全等级保护基本要求》重点解读（按照2.0标准）

### 3.1 网络与通信安全

#### 3.1.1 测评指标

网络架构：应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

访问控制：应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；

通信传输：应采用校验码技术或加解密技术保证通信过程中数据的完整性；

边界防护：应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；

入侵防范：应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警；

安全审计：应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

#### 3.1.2 条款解读

* 根据服务器角色和重要性，对网络进行安全域划分；
* 在内外网的安全域边界设置访问控制策略，并要求配置到具体的端口；
* 在网络边界处应当部署入侵防范手段，防御并记录入侵行为；
* 对网络中的用户行为日志和安全事件信息进行记录和审计；

#### 3.1.3 应对策略

* 推荐使用阿里云的VPC和安全组对网络进行安全域划分并进行合理的访问控制；
* Web应用防火墙防范网络入侵；态势感知的日志功能对用户行为日志和安全事件进行记录分析和审计；
* 对于经常面临DDoS威胁系统，还可使用DDoS高防进行异常流量过滤和清洗。

**问题：目前这一部分我理解的是和网络安全相类似，但是我是没有进行测评的，是否不规范？如果需要测评怎么开展这部分？**

### 3.2 设备和计算机

#### 3.2.1 测评指标

身份鉴别：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性；

访问控制：应根据管理用户的角色建立不同账户并分配权限，仅授予管理用户所需的最小权限，实现管理用户的权限分离；

安全审计：应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

入侵防范：应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

恶意代码防范：应采用免受恶意代码攻击的技术措施或采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性检测，并在检测到破坏后进行恢复。

#### 3.2.2 条款解读

* 避免账号共享、记录和审计运维操作行为是最基本的安全要求；
* 必要的安全手段保证系统层安全，防范服务器入侵行为；

#### 3.2.3 应对策略

* 推荐使用阿里云的堡垒机、数据库审计对服务器和数据的操作行为进行审计，同时为每个运维人员建立独立的堡垒机账号，避免账号共享；
* 使用安骑士对服务器进行完整的漏洞管理、基线检查和入侵防御；

**问题：这部分应该是对应的主机安全，入侵防范使用安骑士？安全审计使用态势感知和数据库审计？对账号管理，权限分配和运维审计这块用堡垒机？但在测评过程中遇见很多使用jumpserver和zabbix作为运维审计、日志管理，这个怎么去判定是否符合？**

### 3.3 应用和数据安全

#### 3.3.1 测评指标

身份鉴别：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求；

访问控制：应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；

安全审计：应提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

数据完整性：应采用校验码技术或加解密技术保证重要数据在传输过程中的完整性和保密性；

数据备份恢复：应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；

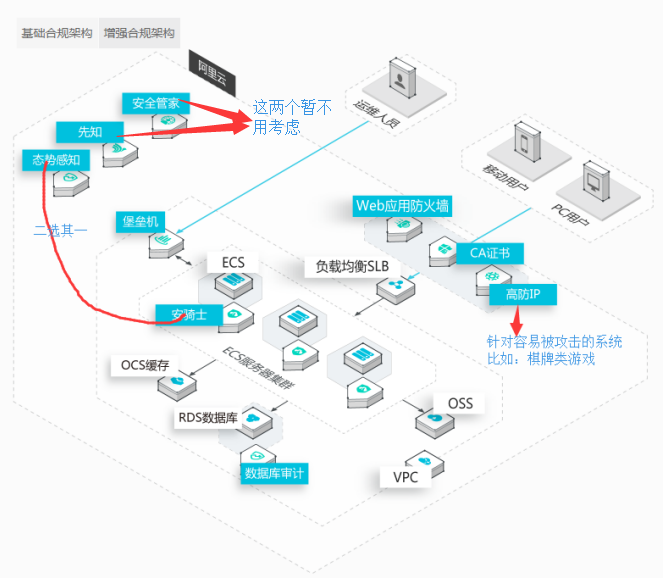
#### 3.3.2 条款解读

* 应用是具体业务的直接实现，不具有网络和系统相对标准化的特点。大部分应用本身的身份鉴别、访问控制和操作审计等功能，都难以用第三方产品来替代实现；
* 数据的完整性和保密性，除了在其他层面进行安全防护以外，加密是最为有效的方法；
* 数据的异地备份是等保三级区别于二级最重要的要求之一，是实现业务连续最基础的技术保障措施。

#### 3.3.3 应对策略

* 在应用开发之初，就应当考虑应用本身的身份鉴别、访问控制和安全审计等功能；对已经上线的系统，通过增加账号认证、用户权限区分和日志审计等功能设计满足等保要求；
* 数据的安全，推荐使用成熟的云盾CA证书服务实现HTTPS，确保数据在传输的过程中保持处于加密状态；数据备份，推荐使用RDS的异地容灾实例自动实现数据备份，亦可以将数据库备份文件手工同步到阿里云其他地区的服务器。

## 4 安全合规架构



堡垒机参考文献

<https://help.aliyun.com/document_detail/52922.html?spm=a2c4g.11174283.6.539.jHs2cX>

态势感知参考文献

<https://help.aliyun.com/knowledge_detail/42302.html?spm=a2c4g.11174283.6.539.Str9ef>

WEB防火墙参考文献

<https://help.aliyun.com/document_detail/28517.html?spm=a2c4g.11186623.6.539.hblWOt>

数据库审计参考文献

<https://help.aliyun.com/document_detail/52480.html?spm=5176.139959.721467.1.6b6536aaZbGtfC>

证书参考文献

<https://help.aliyun.com/document_detail/28535.html?spm=a2c4g.11186623.6.539.BX77uQ>

高防IP参考文献

<https://help.aliyun.com/document_detail/28464.html?spm=5176.7946143.1090659.1.4ace6d63DieV1O>

## 5、云计算基础服务

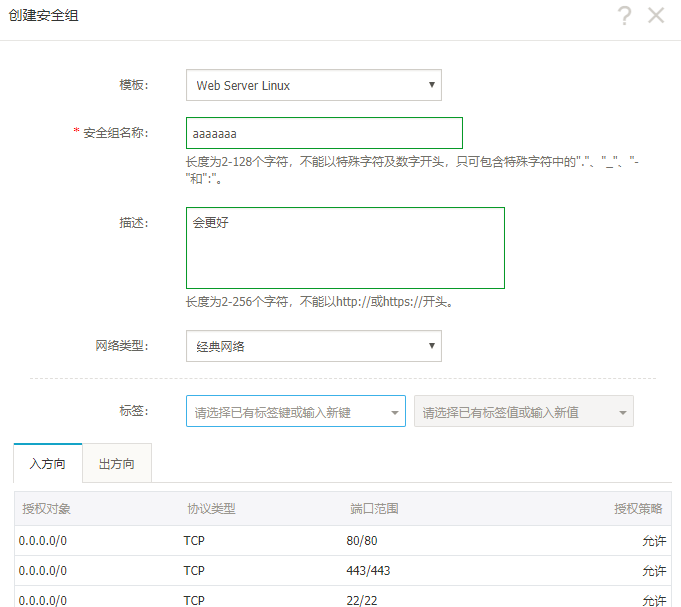
### 5.1 云服务器ECS

#### 5.1.1 安全组

安全组是一种虚拟防火墙，具备状态检测包过滤功能。安全组用于设置单台或多台云服务器的网络访问控制，它是重要的网络安全隔离手段，用于在云端划分安全域。

参考文献：

<https://help.aliyun.com/document_detail/25387.html?spm=5176.2020520101.200.2.aee34df57kOjOd>



我要等保：这个功能就可以认为是传统上面的防火墙

#### 5.1.2 密钥对

用于加强远程登录加强口令安全

参考文献：

<https://help.aliyun.com/document_detail/51792.html?spm=5176.2020520101.300.1.aee34df57kOjOd>

#### 5.1.3 问题诊断

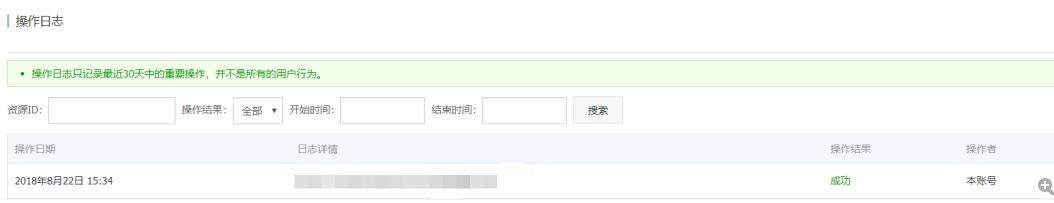
这个可以作为日志问题记录吗？



#### 5.1.4 快照和镜像

快照已经商业化，镜像还在公测中，这个就是阿里云提供的服务器备份功能

#### 5.1.5 操作日志



### 5.2 云数据库RDS版

#### 5.2.1 快捷登录

阿里云数据库登录方式，这个符合远程登录数据库安全

参考文献：

<https://help.aliyun.com/document_detail/26453.html?spm=5176.2020520169.118.16.2ae375bdZICOZg>



#### 5.2.2 我的操作日志

记录操作日志信息



高级版和免费版功能区分：

<https://common-buy.aliyun.com/?commodityCode=dmspre#/buy>



#### 5.2.3 审计日志



#### 5.2.4 审计分析



#### 5.2.5 选中数据库进入

1、日志管理





2、数据安全性：白名单设置、SQL审计（需要付费）



3、备份恢复



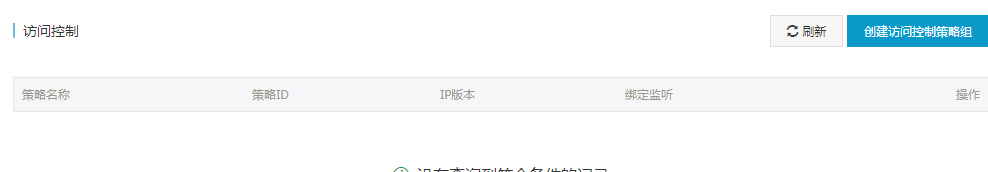


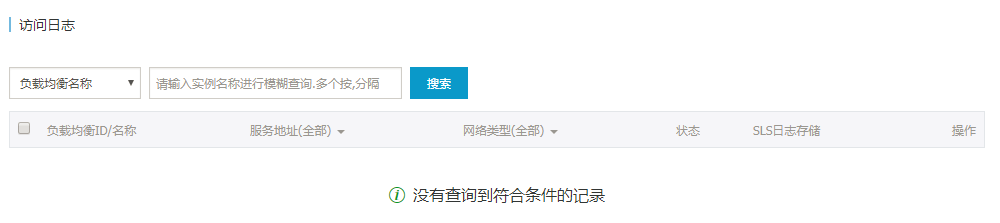


### 5.3 负载均衡

#### 5.3.1 访问控制

这个是控制什么的？

5.3.2 访问日志



#### 5.3.3 健康检查日志

记录的什么日志信息？



### 5.4 操作审计



### 5.5 云监控

该监控免费版是否满足等保要求？

#### 5.5.1 主机监控



1. 操作系统监控

Cpu使用率（保持在10%一下）、内存使用量（保持在40%左右）、系统平均负载（保持在0.4左右）、磁盘使用量（总量40G、目前使用20G）

网络监控指标：网络流入流出使用率、网络流入流出数据包、tcp连接数

1. 基础监控

cpu使用率、网络流入、流出带宽、公网流出带宽使用率、系统磁盘BPS、系统盘IOPS

1. 进程监控

主要监控游戏业务重要进程

监控对象：进程名称、pid、用户、cpu使用率、内存使用、打开文件数、时间

1. 报警机制

事件报警、阙值报警

#### 5.5.2 事件监控



#### 5.5.3 自定义监控



#### 5.5.4 日志监控



#### 5.5.5 云服务监控---云数据库RDS版

1、磁盘使用率（目前使用73%）、IOPS使用率（目前0.2）、连接数使用率（目前3%）、cpu使用率（1%）、内存使用率（31%）、MySQL网络入/出流量

2、报警机制



## 6、安全服务产品

### 6.1 分类

攻击防护：高防IP、Web应用防火墙、安骑士

安全审计：态势感知、堡垒机、数据库审计

数据加密与安全管理：证书服务、安全管家、先知

### 6.2 各个安全服务产品功能

#### 6.2.1 WAF

##### 6.2.1.1 产品介绍

对网站或者APP的业务流量进行恶意特征识别及防护，将正常、安全的流量回源到服务器。避免网站服务器被恶意入侵，保障业务的核心数据安全，解决因恶意攻击导致的服务器性能异常问题。

云盾Web应用防火墙(Web Application Firewall, 简称 WAF)基于云安全大数据能力实现，通过防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、木马上传、非授权核心资源访问等OWASP常见攻击，过滤海量恶意CC攻击，避免您的网站资产数据泄露，保障网站的安全与可用性。

##### 6.2.1.2 功能介绍

**常见Web应用攻击防护**

防御OWASP常见威胁，包括：SQL注入、XSS跨站、Webshell上传、后门隔离保护、命令注入、非法HTTP协议请求、常见Web服务器漏洞攻击、核心文件非授权访问、路径穿越、扫描防护等。

网站隐身：不对攻击者暴露站点地址、避免其绕过Web应用防火墙直接攻击。

0day补丁定期及时更新：防护规则与淘宝同步，及时更新最新漏洞补丁，第一时间全球同步下发最新补丁，对网站进行安全防护。

友好的观察模式：针对网站新上线的业务开启观察模式，对于匹配中防护规则的疑似攻击只告警不阻断，方便统计业务误报状况。

**CC恶意攻击防护**

对单一源IP的访问频率进行控制，基于重定向跳转验证，人机识别等。

针对海量慢速请求攻击，根据统计响应码及URL请求分布、异常Referer及User-Agent特征识别，结合网站精准防护规则进行综合防护。

充分利用阿里云大数据安全优势，建立威胁情报与可信访问分析模型，快速识别恶意流量。

**精准访问控制**

提供友好的配置控制台界面，支持IP、URL、Referer、User-Agent等HTTP常见字段的条件组合，配置强大的精准访问控制策略；支持盗链防护、网站后台保护等防护场景。

与Web常见攻击防护、CC防护等安全模块结和，搭建多层综合保护机制；依据需求，轻松识别可信与恶意流量。

**虚拟补丁**

在Web应用漏洞补丁发布和修复之前，通过调整Web防护策略实现快速防护。

[Web应用攻击防护](https://help.aliyun.com/document_detail/43440.html)

[恶意IP惩罚](https://help.aliyun.com/document_detail/58035.html)

[CC安全防护](https://help.aliyun.com/document_detail/43443.html)

[精准访问控制](https://help.aliyun.com/document_detail/42780.html)

[封禁地区](https://help.aliyun.com/document_detail/49020.html)

[新智能防护引擎](https://help.aliyun.com/document_detail/49018.html)

[网站防篡改](https://help.aliyun.com/document_detail/50348.html)

[数据风控](https://help.aliyun.com/document_detail/44822.html)

[防敏感信息泄漏](https://help.aliyun.com/document_detail/53966.html)

支持网站一键HTTPS

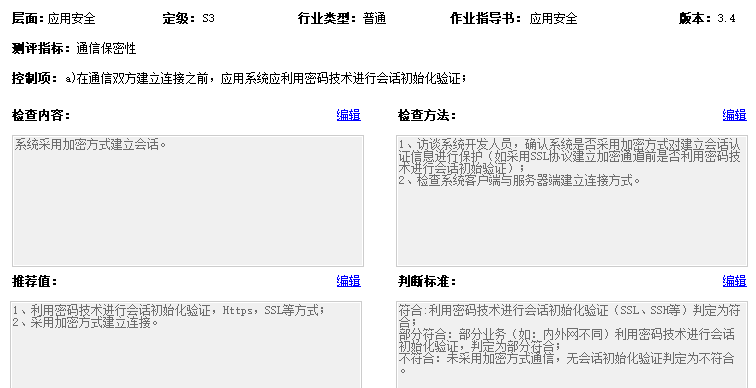
源站如果为HTTP网站，上传证书私钥后，可一键改造为HTTPS，无需服务器改造

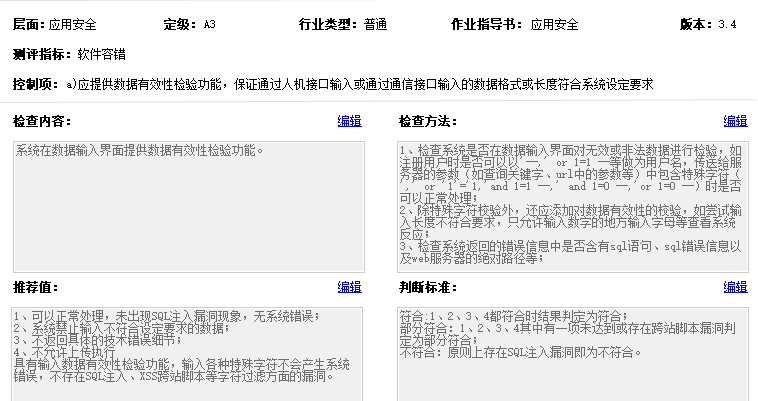
支持HTTP回源

支持HTTPS业务流量以HTTP回源，降低源站的负载消耗，优化业务性能

我要等保：WAF一般针对网站系统，主要功能：常见web应用攻击防护、CC恶意攻击防护、网站一键https、[网站防篡改](https://help.aliyun.com/document_detail/50348.html)。

等保测评中依据：





#### 6.2.2 堡垒机

##### 6.2.2.1 产品介绍

堡垒机是云盾提供的一个核心系统运维和安全审计管控平台。

云盾堡垒机集中了运维身份鉴别、账号管控、系统操作审计等多种功能。基于协议正向代理实现，通过正向代理的方式实现对 SSH 、Windows 远程桌面、及 SFTP 等常见运维协议的数据流进行全程记录，并通过协议数据流重组的方式进行录像回放，达到运维审计的目的。

##### 6.2.2.2 功能介绍

**操作审计**

多面记录运维人员的操作行为，作为事件追溯的保障和事故分析的依据。

运维操作记录： 操作失误、恶意操作、越权操作详细记录。

Linux命令审计： 可提取命令符审计，支持命令定点回放。

Windows操作录像： 远程桌面的操作，支持全程录像，包括键盘操作、鼠标操作、窗口打开等。

文件传输审计： 支持远程桌面文件传输、FTP/SFTP的原文件审计。

**职权管控**

通过账号管控和权限组管理，实现分职权进行人员和资产的管理。

账号管控： 运维账号唯一，解决共享账号、临时账号、滥用权限等问题。

权组管理： 按照人员、部门组织、资源组，建立人员职责与资源分配的授权管理。

**安全认证**

引入双因子认证机制，通过短信认证、动态令牌等技术，控制账号密码泄露风险，防止运维人员身份冒用和复用。

**高效运维**

从架构、工具、ECS接入等多方面提升运维效率。

C/S架构运维接入： 支持SSH、RDP、SFTP协议。

多运维工具： 支持PuTTY、SecureCRT、Xshell、WinSCP、mstsc等工具。

ECS高效接入： 支持一键同步并导入ECS云服务器。

我要等保：堡垒机主要功能：操作审计、职权管控、安全认证。

等保测评中的依据：

