**北京沃丰时代数据科技有限公司**

**信息安全加密规范v1.2**

**文档信息：**

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** | 信息安全加密规范 | | |
| **文档编号** | WF-DM008 | | |
| **文档密级** | 内部 | **发布范围** | 公司内部 |
| **编制人** | 韦昭 | **编制日期** | 2021-01-20 |
| **评审人** | 周毅 | **评审日期** | 2023-03-23 |
| **批准人** | 张磊 | **批准日期** | 2023-04-23 |

**修订历史记录：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 状态 | 修订内容说明 | 编制人 | 日期 |
| V1.0 | 新建 | 新增 | 韦昭 | 2020-08-28 |
| V1.1 | 修订 | 添加范例 | 韦昭 | 2021-01-07 |
| V1.2 | 修订 | 格式调整 | 韦昭 | 2021-01-20 |
| V1.3 | 修订 | 修订文档信息 | 张帆 | 2023-04-23 |
|  |  |  |  |  |

目录

[第1章 概述 3](#_Toc93588269)

[第2章 术语 3](#_Toc93588270)

[第3章 密钥管理 4](#_Toc93588271)

[3.1 域名证书管理 4](#_Toc93588272)

[3.2 阿里密钥管理 5](#_Toc93588273)

[3.3 应用密钥管理 6](#_Toc93588274)

[第4章 数据加密 12](#_Toc93588275)

[4.1 数据传输层 12](#_Toc93588276)

[4.2 应用层文件存储 14](#_Toc93588277)

[4.3 数据库层磁盘加密 16](#_Toc93588278)

[4.4 数据库字段加密 17](#_Toc93588279)

# 第1章 概述

本文档编制目的，规范运维、开发过程中相关的加密解密活动。

**所有沃丰时代项目、配置都必须符合此规定。**

规定包括密钥管理、数据加密和安全算法要求。

密钥必须使用下面的管理系统和保存在：  
1.  阿里SSL证书服务  
2.  阿里密钥管理服务  
3.  KMS Vault服务

加密解密活动及对应密钥存储表

|  |  |  |
| --- | --- | --- |
| 活动 | 算法 | 密钥存储位置 |
| 数据传输 | RSA 2048  TLS1.2 | 阿里 SSL 证书服务 |
| 应用层文件存储 | AES256 | 阿里密钥管理服务 |
| 数据库层磁盘加密 | AES256 | 阿里密钥管理服务 |
| 应用层密码存储 | Bcrypt | 无 |
| 应用层敏感数据存储 | AES256 | KMS Vault 服务 |

# 第2章 术语

**阿里云“SSL 证书服务”:** 阿里云提供的证书管理服务，帮助文档见：[SSL证书服务](https://help.aliyun.com/product/28533.html)

**KMS:**密钥管理系统(Key Management Service)

**阿里云密钥管理服务**: 阿里云提供的密钥管理服务， 帮助文档见：[密钥管理服务](https://help.aliyun.com/product/28933.html)

**Vault:** HashiCorp 公司提供的开源密钥管理系统(KMS)，提供对密钥的加密存储和访问控制。帮助文档见：<https://www.vaultproject.io/docs/what-is-vault>

**阿里云OSS**：阿里云对象存储服务，类似AWS的S3 帮助文档见： [对象存储 OSS](https://help.aliyun.com/product/31815.html)

# 第3章 密钥管理

## 3.1 域名证书管理

1 域名证书管理使用阿里云 SSL证书服务。

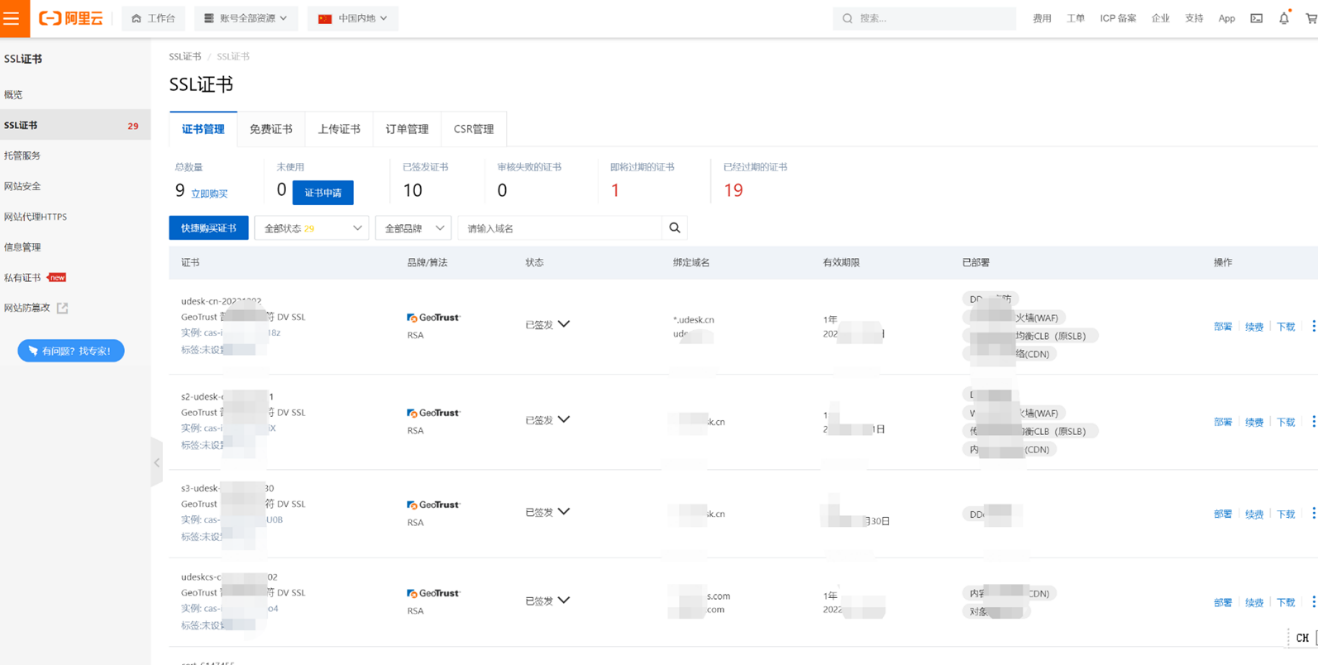
2 在进行域名证书购买或部署时，由CTO或技术总监受权，下发阿里MFA验证码或短信验证授权给运维主管，由运维主管进行，完成后回收权限，以禁止单独个人访问到明文证书。

3 对数字证书和实例进行管理，该服务提供了对数字证书的管理、有效性检查检查等功能；

4 普通账号无权下载证书明文；

5 证书为RSA2048证书，每年一签。

**阿里SSL证书服务**，详见文档：[SSL证书服务](https://help.aliyun.com/product/28533.html)



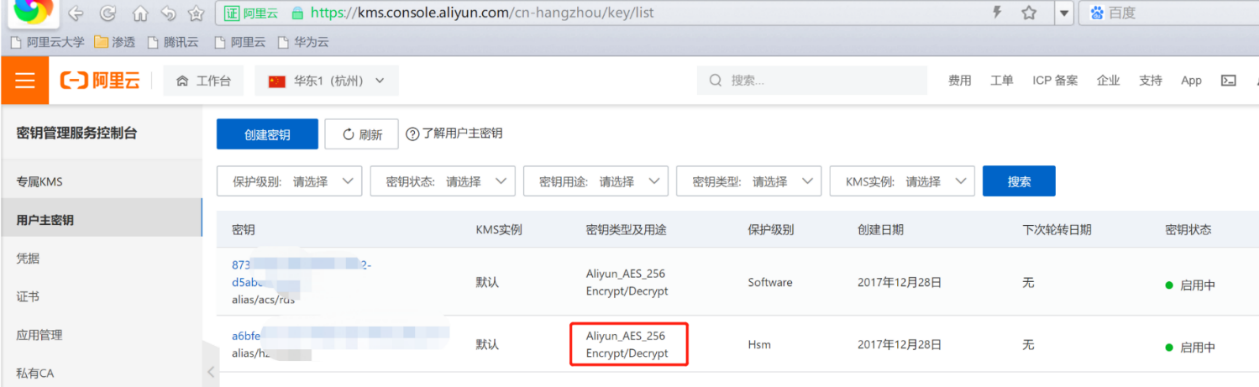
普通账号无权下载证书

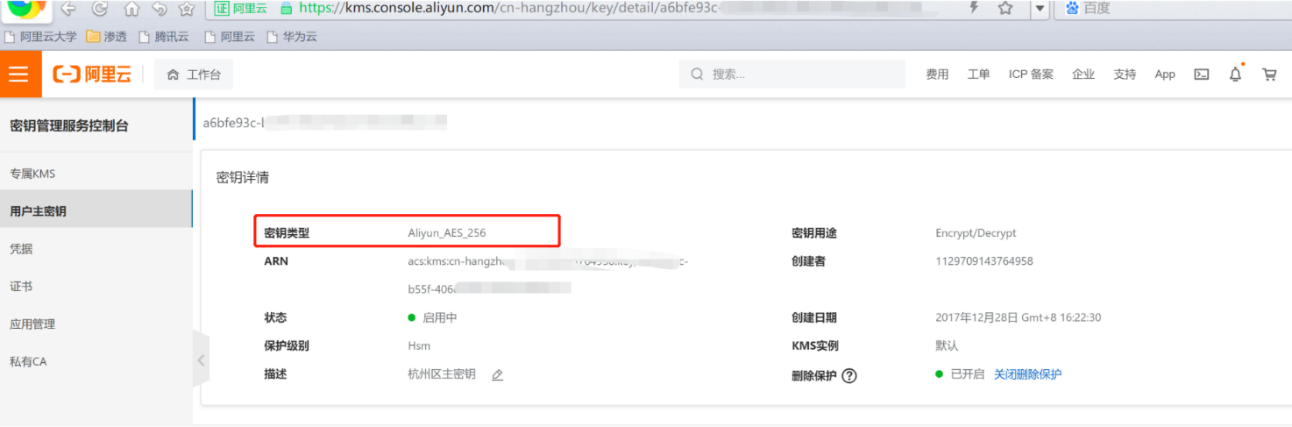


## 3.2 阿里密钥管理

阿里云基础设施，包括阿里云数据库和对象存储，必须使用阿里密钥管理服务进行存储和管理，密钥类型必须使用 AES 256。

**阿里密钥管理示例** 帮助文档见： <https://help.aliyun.com/product/28933.html>





## 3.3 应用密钥管理

应用程序使用的密钥，必须使用 HashiCorp Vault 进行存储和管理:

1 测试环境、生产环境使用的自己的Vault ，把不同环境隔离开来

2 Vault仅允许本区域或环境访问，禁止外部防问，使对应数据在离开指定环境后无法取到对应密钥

3 密钥由专门的高层管理人员产生并集中管理

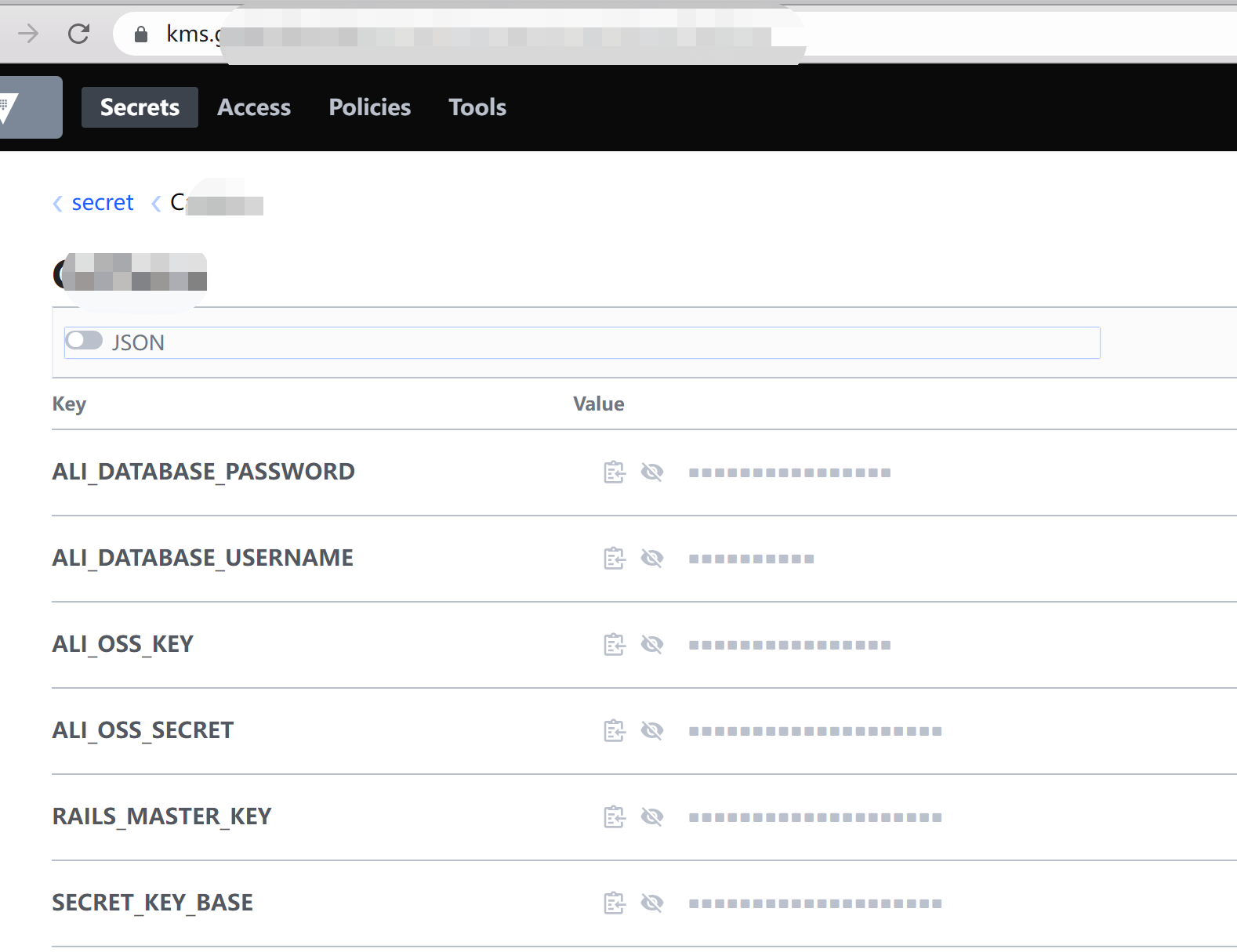
4 线上操作人员需要在企业微信进行权限申请，必须经过安全和高层经理的审批以获得

5 密钥必须加入GithubMonitor 进行数据泄露监控，当出现数据泄露时进行 应急响应处理

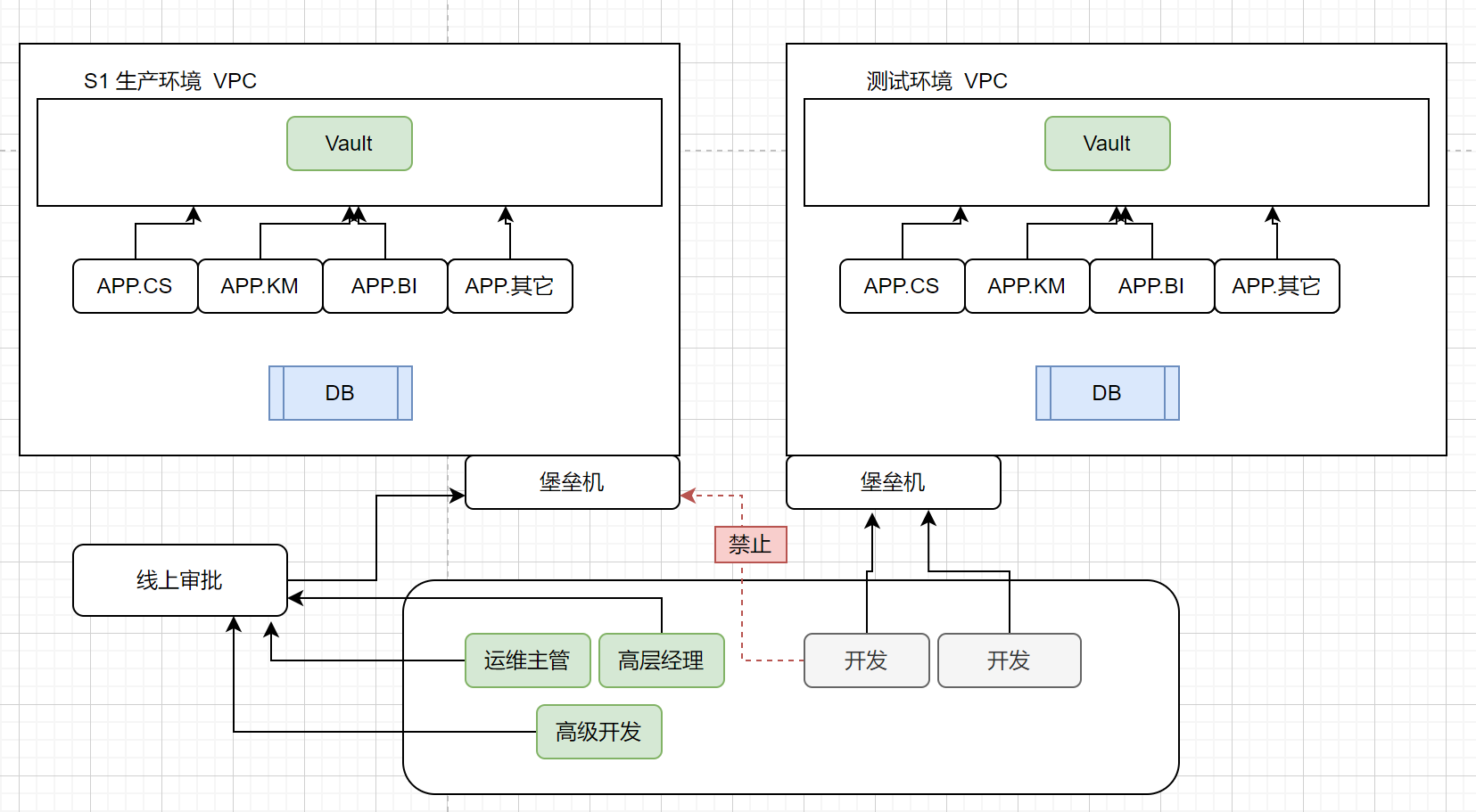
6 Vault 后端使用阿里RDS进行数据存储，并且必须高可用版本、开启数据备份和日志备份,以保证密钥服务的高可用和数据恢复能力

**Vault实例示例**， 帮助文档见：<https://www.vaultproject.io/docs/what-is-vault>

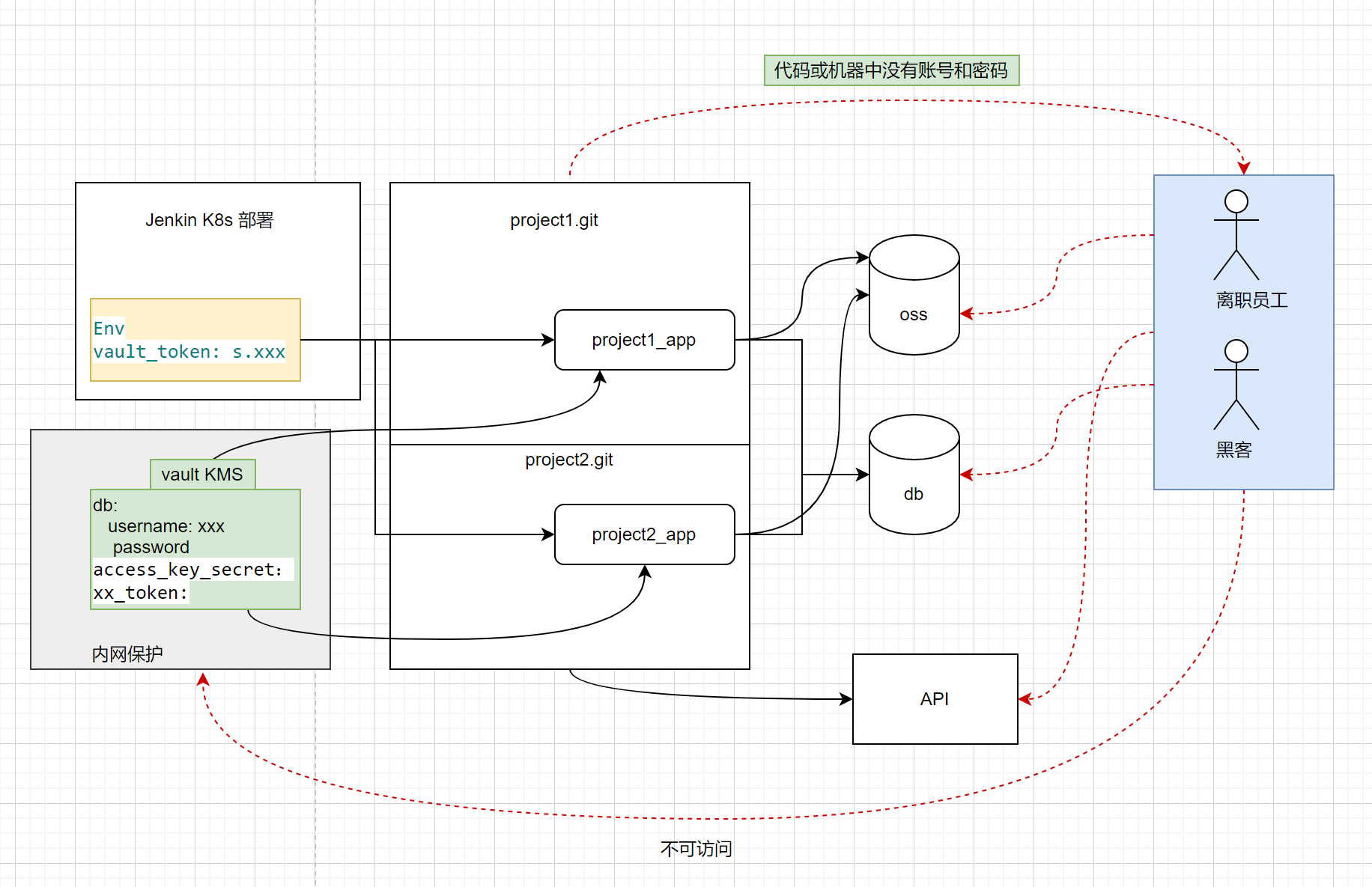




生产测试配置管理隔离，架构图



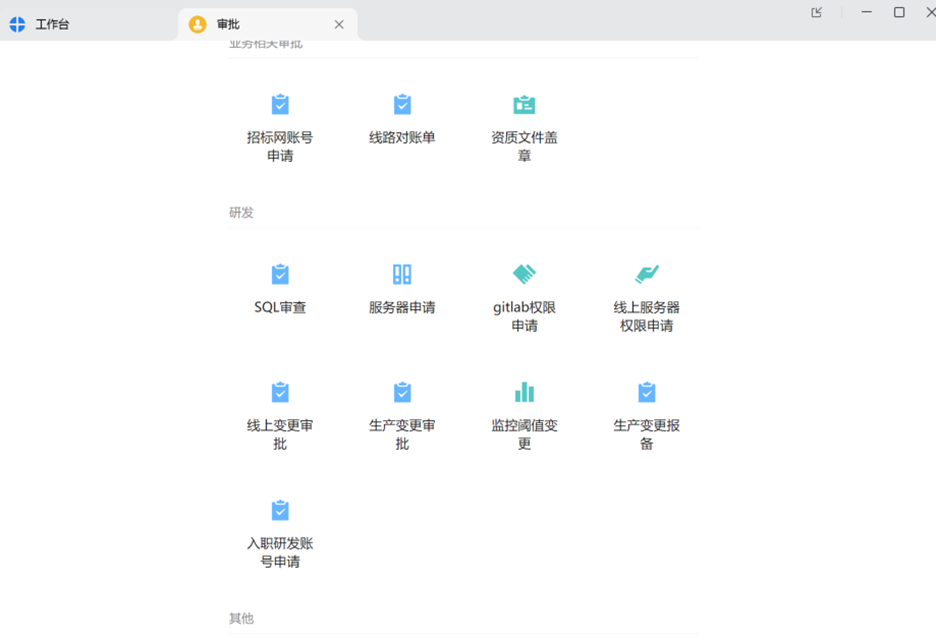
对应数据在离开指定环境后无法取到对应密钥



企业微信权限审批示例



入口：企业微信->应用→审批->研发



线上权限申请示例



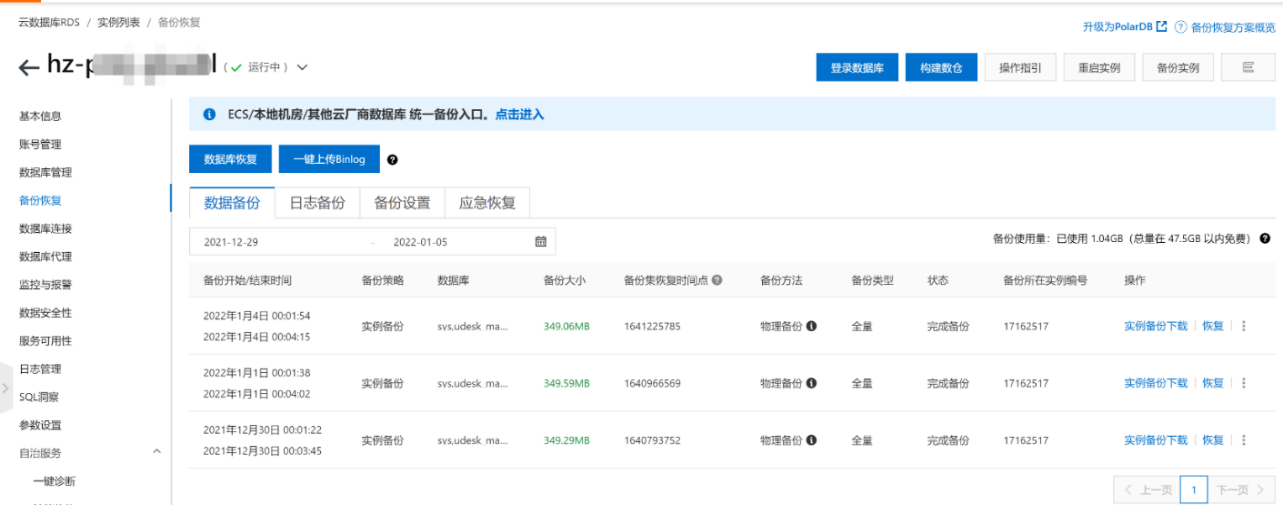
已处理疑似泄露数据

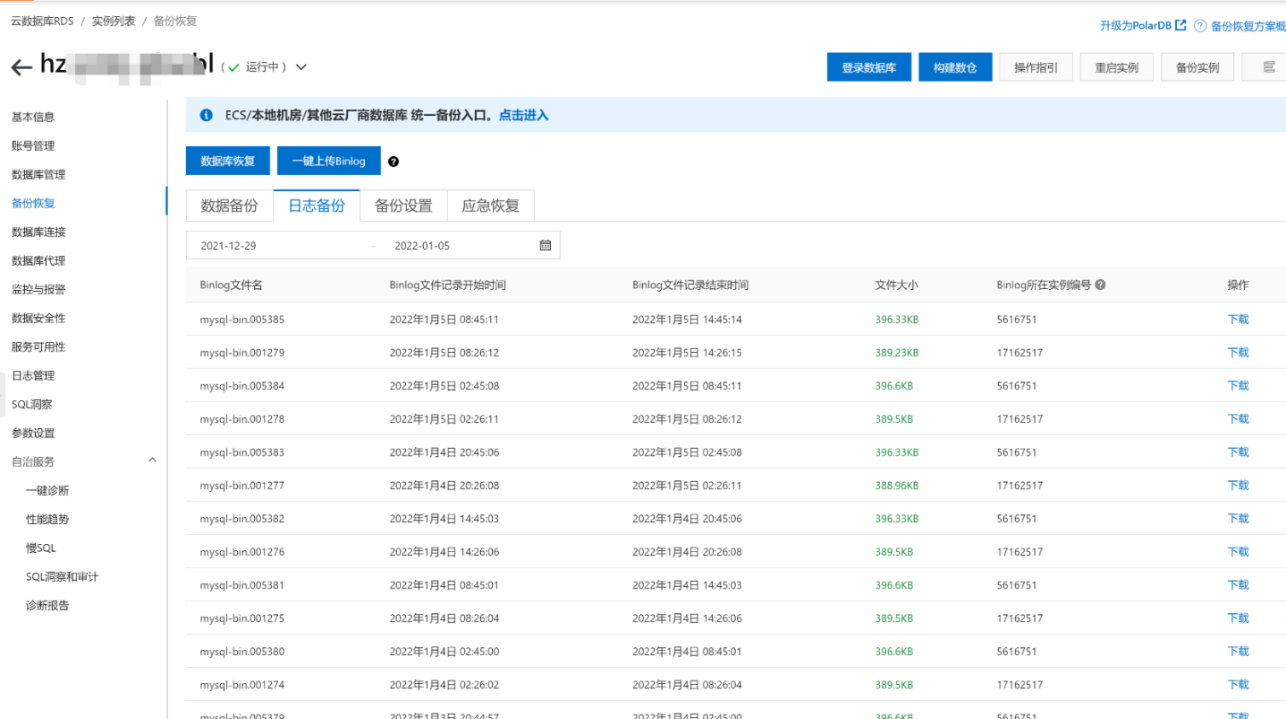
#### 

Vault 数据存储于RDS,并且必须是高可用版本、开启数据备份和日志备份。

阿里高可用版本定义为：采用一主一备的经典高可用架构。







# 第4章 数据加密

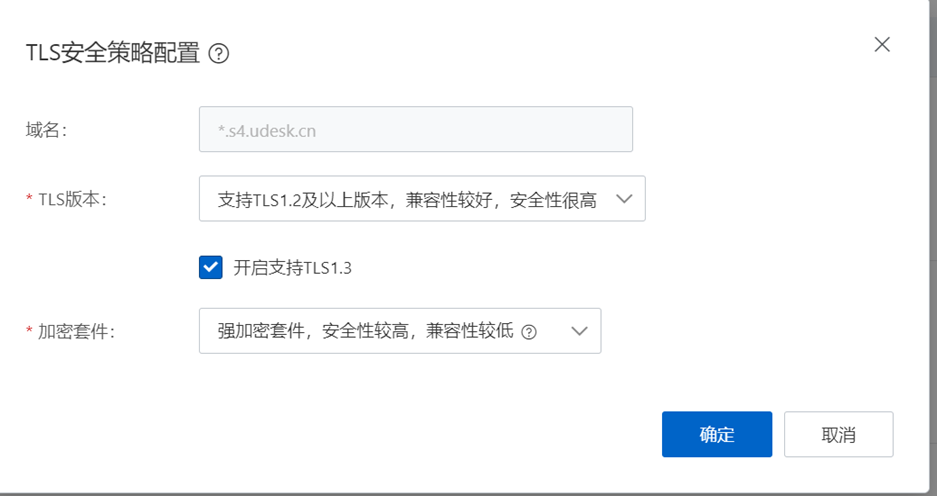
## 4.1 数据传输层

应用层的数据传输使用RSA2048位证书 和 TLS1.2算法加密，必须使用阿里SSL管理服务进行购买和管理  
       范围：  
        1 阿里高防：域名接入TLS安全政策配置为 TLS版本：支持TLS1.2及以上版本  
        2 阿里WAF：网站接入TLS配置

**证书RSA 2048 位**



高防配置示例：

  
WAF配置示例  


## 4.2 应用层文件存储

应用层生成和上传必须存放在阿里对象存储中，对象存储Bucket必须启动**服务器端加密**功能，并使用 AES256 算法加密，并使用阿里云密钥管理

在创建阿里云对象存储时，必须选择 服务端加密方式为 KMS，加密算法为 AES256，选择 3.2 中配置的AES256密钥

阿里OSS服务端加密文档详见： <https://help.aliyun.com/document_detail/31871.html>



配置后，bucket的基础设置，显示服务端加密，并且使用KMS加密方式和AES256加密算法



## 4.3 数据库层磁盘加密

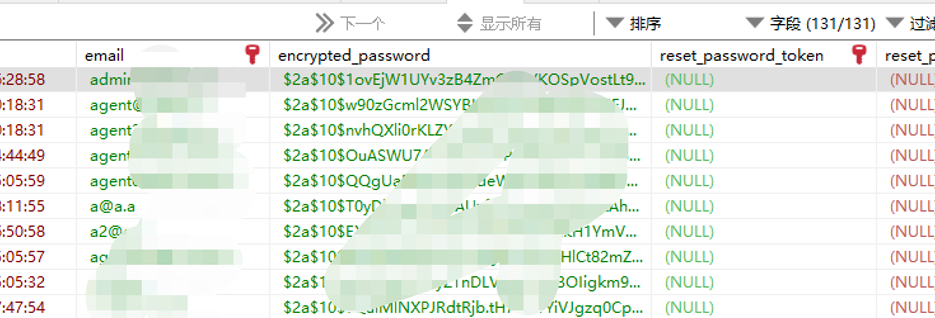
在创建RDS数据库时，必须选择 ESSD 云盘，并选择"云盘加密"功能,密钥选择阿里KMS中的 AES256 密钥

阿里RDS云盘加密帮助文档详见: [云盘加密](https://help.aliyun.com/document_detail/135361.htm?spm=5176.rdsbuy.0.0.6c8a752fSOL3mr)  
  
   
配置后，RDS实例显示使用   


## 4.4 数据库字段加密

密码类相关数据散列加密算法bcrypt加密，用户邮件等敏感数据，使用AES256双向加密算法, 并将密钥存储于Vault中。

**bcrypt加密示例**

  
邮件加密示例/AES256：

  
加密代码示例：

