**北京沃丰时代数据科技有限公司**

**服务账号管理**

**文档信息：**

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** | 服务账号管理 | | |
| **文档编号** | WF-DM014 | | |
| **文档密级** | 内部 | **发布范围** | 公司内部 |
| **编制人** | 张帆 | **编制日期** | 2022-01-15 |
| **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** | **修订日期** | **编制人** |
| V1.0 | 新建 | 新增 | 2022-01-15 | 张帆 |
| V1.1 | 修订 | 修订文档信息 | 2023-04-23 | 张帆 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目录

1. 概述 3

1.1. 目的 3

1.2. 范围 3

2. 服务账号管理细则 3

2.1. 申请 3

2.2. 权限设计 4

2.3. 记录 5

2.4. 审查 5

# 概述

本公司使用内部自建的 Confluence 系统完成服务账号的管理。

## 目的

本文档目的是为了保证本司研发部服务账号的统一控制，包括权限设计及供应和解除供应的控制，使其不能用于损害数据和应用程序的机密性、完整性、可用性和不可抵赖性，确保遵守最小特权原则，保证用户所有权、数据所有权和过程所有权。

## 范围

本文档适用范围是本公司研发部门所有团队

# 服务账号管理细则

## 申请

服务账号申请，由研发业务线技术负责人发起，由安全负责人和技术总监审批，由运维人员执行，申请表如下。



* 申请人需要填写服务名称、所在实例、类型、账号、所属项目、权限、使用期限、申请人、用途字段。
* 申请人填写好后，由审批人对申请人填写的各个字段完成检查、评估、审批。如果有问题，会与申请人进行沟通和协调，确定最终的服务账号申请信息。
* 审批人在审批阶段重点关注。
  + 权限设置是否符合最小特权原则。
  + 用途是否合理，用途和权限设置是否匹配。
  + 服务账号供应或者解除供应后，是否可以保证应用和数据的机密性、完整性、可用性和不可抵赖性。
  + 服务账号供应或者解除供应后，是否可以保证用户所有权、数据所有权和过程所有权。
  + 服务账号供应或者解除供应后，对应用和数据的影响范围和风险。
  + 是否符合安全要求。
* 审核通过后，由运维人员生成至少16位且高安全等级的服务账号密码，完成服务账号的新增或者修改，并且记录账号密码和把密码以文件的形式发送给申请人。
* 如果供应或者解除供应后有问题，需要进行增加、修改、删除，则重新提交服务账号申请。
* 如果需要修改或者删除服务账号，申请人和执行人需要确定账号快速恢复方案，需要把信息同步给审批人。

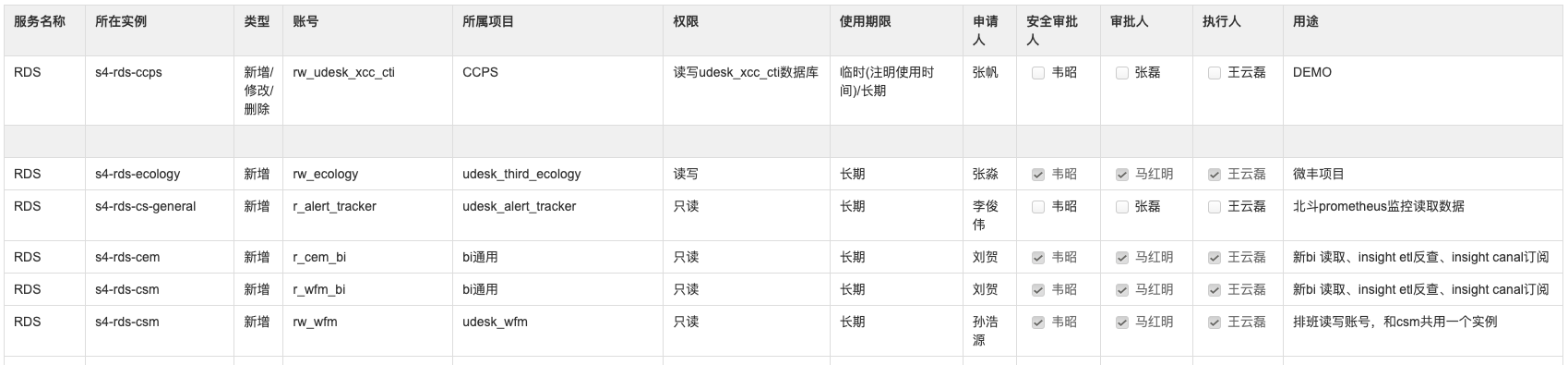
## 权限设计

服务账号权限设计，由研发业务线技术负责人设计权限，填写到服务账号申请表中，由安全负责人和技术总监检查、评估、审批，由运维人员配置。权限设计具体规则如下。

* 服务账号不可以拥有服务的根权限或者管理员权限。
* 服务高权限、根权限、管理员权限的账号不可以作为服务账号使用。
* 一个服务账号只可以一个项目使用，不可以跨项目使用。
* 多项目共用的服务，多个项目不可以共用同一个服务账号，每个项目的服务账号只可以拥有该项目在该服务中的权限，不可以拥有用其他项目在该服务中的权限，要符合最小特权原则。
* 根据账号用途精准评估权限，要符合最小特权原则。
* 服务账号的供应和解除供应操作后，要保证服务、应用、数据的机密性、完整性、可用性和不可抵赖性。
* 服务账号的供应和解除供应操作后，要保证用户所有权、数据所有权和过程所有权。
* 保证服务账号的供应和解除供应操作后应用和服务的影响范围最小化。
* 评估服务账号的供应和解除供应操作后的风险和应对风险的解决方案。

## 记录

服务账号申请记录，可以查询到所有的服务账号申请记录，保证服务账号供应和解除供应的可追溯性和不可抵赖性。服务账号申请记录如下。



## 审查

服务账号审查，运维人员和安全人员每半年会对服务账号进行一次审查，主要审查内容如下。

* 服务账号是否还在使用，是否需要清理。
* 服务账号是否符合当前的权限设计规则。
* 服务账号是否符合安全要求。
* 服务账号是否存在使用和安全风险。

审查完成后，运维人员将审查的结果和问题发送给技术总监，运维人员负责协调整改审查出现的问题。

* 如果服务账号不再使用，和研发业务线技术负责人确认是否需要清理。
* 如果服务账号不符合当前的权限设计规则和安全要求，则通知相关负责人，并且推进整改，直到整改完成。
* 如果服务账号存在使用和安全风险，则通知相关负责人，并且推进整改，直到整改完成。
* 整改以上问题，如果需要进行服务账号变更，则需要发起服务账号申请流程。