重庆银行

运维账户及操作风险管理系统建设技术方案

修 订 记 录

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 版本 | 修改者 | 描 述 |
| 2019/9/2 | 1.0 | 徐荣凯 | 建立 |
| 2019/9/16 | 2.0 | 徐荣凯 | 修改项目规划、新增网络拓扑图 |
| 2019/9/24 | 3.0 | 徐荣凯 | 修改网络架构、增加应急场景及账号自动改密要求 |
|  |  |  |  |
|  |  |  |  |

# 概述

## 项目背景

随着我行业务快速发展、信息化建设不断推进，IT设备已超过3000台、系统帐号数量已超过6000个，运维规模扩张明显；设备类型越来越多、操作环境越来越复杂，运维难度越来越高。随着2019年《信息安全技术 网络安全等级保护基本要求》简称“等保2.0”的出台，对信息系统安全运维管理提出了更高要求。

当前在用的运维审计系统是2012年5月上线的系统，在设备兼容性、系统集成、帐号自动化管理、权限细粒度控制等方面，已不能满足监管和运维安全管理的需要。同时也不能适应运维一体化的发展。具体表现如下：

* 不支持大多数网络设备纳管
* 不支持IPV6协议资产纳管
* 不支持数据库、中间件、应用帐号密码登陆代填
* 操作命令黑白名单控制功能不完善
* 帐号自动改密功能不完善
* 不支持帐号密码状态自动检测并集中展示
* 不支持与第三方系统对接

建设运维账户及操作风险管理系统，对我行的数量众多的生产设备、帐号、运维操作权限进行自动化和细粒度的管理，已迫在眉睫。

现有运维审计系统在产品框架上不支持直接进行升级来满足监管及行内功能要求，因此本次运维账户及操作风险管理系统采用新建系统方式建设。

## 项目建设目标

## 1.2.1可行性

经过前期同业调研及与齐治科技、江南科友、安恒信息、上讯信息等多家国内一线运维安全厂商现场会议交流，新运维风险管理平台在帐号自动改密、帐号密码状态自动检测、操作命令黑白名单控制，及数据库、中间件、应用帐号密码登陆代填等方面技术已经成熟，主流厂商已有在多家大中型全国性股份制商业银行总行、城市商业银行总行、农村商业银行总行、农信社总行成功实施案例，其产品性能安全稳定。 同时在设备兼容性、系统集成方面有了长足的进步，新平台已成功兼容市面上大多数网络设备纳管，保留了底层API接口，一线厂商已有多家大中型银行总行级网络设备成功纳管案例及和ITSM系统、CMDB平台成功对接案例。

综上所述，新运维风险管理平台在技术上已具备实施的可行性。

## 1.2.2建设目标

基于我行运维安全现状及运维一体化发展需要，兼顾监管要求，本次运维账户及操作风险管理系统的建设目标为：

* 完善系统功能：须涵盖我行现有运维审计系统的全部功能，进一步满足我行对运维安全风险管理的新增功能需求。包括但不限于帐号管理（支持帐号自动改密及帐号密码状态自动检测展示），权限管理（支持操作命令黑白名单控制）等功能。
* 符合监管要求：运维账户及操作风险管理系统的功能实现须满足当前银监会、等保2.0、上市审计及内控对银行安全管理的规范要求。包括 “帐号定期自动改密”等要求。
* 提升用户体验：运维账户及操作风险管理系统须提供更稳定的系统性能、更快的系统响应速度、更便捷的操作方式，给用户良好的运维操作体验。包括“帐号密码登陆代填”、“双中心双活”、 “电子工单”等新功能。
* 增强系统兼容性：运维账户及操作风险管理系统须兼容不同的网络设备及应用帐号密码纳管，满足不同的网络设备及应用帐号密码登陆代填等安全管理要求。
* 符合运维一体化发展：运维账户及操作风险管理系统须提供安全的底层API接口，支持与ITSM、CMDB等第三方系统对接，适应运维一体化发展要求。

综上所述，运维账户及操作风险管理系统的建设，须解决当前运维审计系统的痛点，进一步完善功能，优化结构，兼顾监管要求，给用户更便捷、良好的操作体验。

## 项目建设规划

## 1.3.1总体规划

针对当前我行运维安全风险管理现状，兼顾科技部运维一体化发展规划，我中心将按照“保障安全，稳步推进”的原则，分三步完成整个项目建设。第一步：原运维审计系统管理资产平滑迁移到运维风险管理平台；第二步：纳管所有生产网络设备及其它设备和数据库；第三步：与ITSM、CMDB对接。

## 1.3.2实施步骤

运维账户及操作风险管理系统建设过程具体步骤如下：

1. 完成系统平台搭建后，迅速接管现有运维审计系统管理的资产，将运维审计系统中管理的资产平滑迁移到运维风险管理平台上。开始使用“电子工单“。完成全面纳管所有生产系统主机，达到保障生产运维工作正常开展的基础目标，提升用户体验。
2. 逐步将生产网络设备及其它设备纳管到运维风险管理平台上； 开始使用数据库中间件及应用帐号“帐号密码登陆代填”； “操作命令黑白名单控制”及“帐号自动改密”等新功能。达到完善系统功能，符合监管要求，增强系统兼容性的目标。
3. 最后完成与ITSM系统、CMDB平台对接，通过与ITSM系统对接，获取生产运维资源申请数据和事件变更单数据；通过与CMDB对接，同步生产资产更新数据。达到符合运维一体化发展的目标。

## 1.3.3将纳管的生产服务器及网络设备情况

经与网络设备同事交流和从现用运维审计系统统计估算，拟接入系统的生产服务器和网络设备情况如表1所示：

|  |  |
| --- | --- |
| 系统名称 | 服务器数量 |
| 生产系统主机 | 约1400台 |
| 网络设备 | 约1200台 |
| 数据库 | 约300个 |

表1 拟纳管生产服务器和网络设备情况表

# 总体架构

## 总体应用架构

运维账户及操作风险管理系统应用架构如图1所示：

**接口**



**数据中心**

**Computer**

**Network**

**Database**

**Middle**

**ITSM**

**运维风险管理平台**

**资产管理**

**用户管理**

**权限管理**

**帐号管理**

**电子工单**

**审计管理**

**报表管理**

B/S

C/S

**用户UI**

PLSQL

Chrome

“”…..



**发布服务器**

**CMDB**

**外接系统**

图1 运维账户及操作风险管理系统应用架构图

经过调研及多次与市场上主流厂商交流，我行运维风险管理平台采用市面上主流产品架构---B/S架构。

运维人员主要通过浏览器登录运维风险管理平台到达目标服务器，系统也支持通过客户端工具如Xshell、SecureCRT、Putty登陆运维风险管理平台访问目标服务器。运维风险管理平台通过系统内置接口调用SSH/Telnet/RDP协议，完成登陆生产主机进行运维操作；通过系统内置接口调用SSH/Telnet协议，完成登陆网络设备进行运维操作；通过系统内置接口调用JDBC完成登陆数据库进行运维操作；通过系统内置接口调用WEBService，完成登陆中间件进行运维操作；通过调用发布服务器上安装的应用，完成登陆应用系统进行运维操作。待ITSM、CMDB建成后，通过接口与ITSM、CMDB对接，实现数据交互。

系统主要功能模块由七部分组成,包括：用户管理、资产管理、帐号管理、权限管理、审计管理、电子工单、报表管理。具体功能描述如下：

* 用户管理

用户管理是对用户角色分权、用户认证及身份识别的集中统一管理。即在用户角色分权管理的同时考虑认证多样化，不同的角色可以使用不同的认证方式，或多种认证方式组合。加强用户认证安全，满足用户身份识别安全管理规范。系统支持自定义用户角色和根据功能来新建角色，并可依据角色灵活配置相应系统模块的管理权限，支持用户按组划分。提供主从帐号管理，让用户的身份和具体的操作对应起来，从而实现用户实名制管理。

* 资产管理

资产管理是系统分模块对主机、网络设备、数据库、应用系统资产的集中统一管理。包括资产的添加、修改、删除及批量导入，资产可按组分类。支持动态全景视图管理，管理员在配置好资产的层级属性后，系统可自动生成动态全景视图。支持网络设备资产纳管，支持IPV6协议资产纳管，支持数据库、中间件、应用帐号密码登陆代填，具备资产发现功能，支持按网段扫描发现资产。支持等价资产功能，使资产实现归一化管理，当其中一个资产属性发生变更时，等价资产属性随之自动调整；

* 帐号管理

帐号管理是对帐号密码的全生命周期管理，包括帐号及密码的添加、修改、删除、锁定等管理。支持帐号密码自动检测，以及帐号密码自动检测结果智能化分析，帐号密码状态异常集中展示，比如密码失效、弱密码、空密码等。支持AD域账号的自动化同步。支持帐号自动改密，帐号类型包括Unix/linux/Windows操作系统账号，Oracle、MysqL等数据库账号，Weblogic、Tomcat等中间件帐号及应用帐号。支持ORACLE、DB2、Mysql数据库，Weblogic、WAS 、Tomcat中间件的联动改密。支持各类系统的密码策略，支持历史帐号密码留存功能，管理员可在运维安全管理平台上查阅历次密码变更记录及变更前的帐号密码信息，便于管理员进行密码恢复操作。支持密码加密导出及备份。

* 权限管理

权限管理是系统对用户通过运维风险管理平台访问生产系统、网络设备、数据库中间件的操作权限进行管理。资产帐号权限进行管控的功能。包括分别针对资产组、资产，用户组、用户的操作权限添加、修改、删除。支持通过用户属性、资产属性、帐号属性来创建动态权限规则，以达到细粒度的最小化权限授权。支持操作命令黑白名单控制。支持基于A/B角管理模式的双人复核，当用户登录到目标资产时，必须经过复核人的复核确认后才能正常操作；当会话复核人发现操作存在风险，可实时暂停；支持变更单管理功能，管理员可以基于使用人、资产、系统账号、到期时间，上传、创建值班表模式的权限变更单，变更单无需审批，但可以自动生成时效性的访问权限。

* 审计管理

审计管理包括操作监控、操作会话审计、字符会话审计、图形会话审计、数据库会话审计、文件传输审计功能模块。系统能对在线操作会话进行监控并实时切断，对字符会话、图形会话、数据库会话、文件传输进行审计，提供按资产、用户、会话操作及日期、时间段检索会话记录，支持多关键字检索，检索结果直接定位到相关操作片段。支持文件传输审计，可以完整记录用户通过系统进行的SFTP、剪切板、磁盘映射、rz/sz四大类文件传输操作，可对传输的文件信息进行留存。支持字符会话审计日志syslog外发。支持数据库审计SQL语句文本提取。支持以2M会话流量或者15分钟操作时长为标准的会话缩略图切片展示功能，管理员点击任意切片，即可直接定位到对应操作片段。

* 电子工单

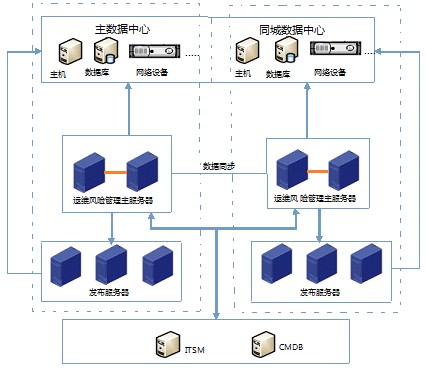
电子工单是用来管理用户对资产、帐号、密码的申请、审批权限自动下发的流程。用户申请时可以选择：服务器IP、账户、运维有效期、备注事由等。可实现按时间段授予资产帐号权限，“一事一密”，到期自动失效。

* 报表

报表是对资产、用户、帐号、运维操作访问等数据的多维度分析统计。包括从用户、资产、帐号、运维时长、运维命令、文件传输、访问源、运维时间特性等角度进行细粒度分析；支持报表一键导出。

## 系统部署架构

运维账户及操作风险管理系统部署架构如图2所示：

 图2 运维账户及操作风险管理系统部署架构图

运维风险管理平台是生产系统运维操作的入口，影响全行生产系统运维开展，间接影响业务故障恢复时间。考虑到其重要性，拟采用双中心独立部署并可相互接管业务，单中心双机高可用方式建设。运维风险管理平台服务器包括主服务器和发布服务器两部分，生产服务器操作系统登陆通过主服务器可以实现直接登陆运维，而应用系统登陆需要主服务器调用发布服务器上的应用端实现登陆应用服务器运维。

数据库和应用部署在同一台服务器上，使用数据同步机制实现数据自动同步。

外联系统有ITSM和CMDB。连接ITSM系统，完成运维风险管理平台的权限申请审批流程管理；连接CMDB系统，实现CMDB资产数据的同步更新，保障CMDB数据的准确性。

## 网络拓扑图

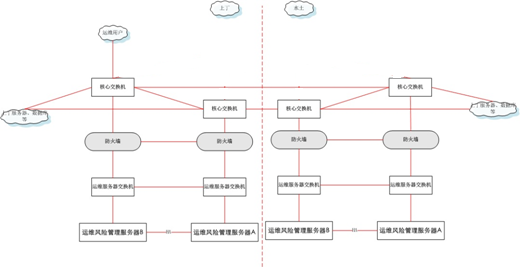


图3 运维账户及操作风险管理系统网络拓扑图

运维账户及操作风险管理系统采用双中心独立部署并可相互接管业务、单中心高可用架构。通过双中心任意一台运维风险管理服务器均可实现登陆双中心生产系统服务器进行运维的目标。双中心运维账户及操作风险管理系统分别独自对外提供服务。上丁中心运维账户及操作风险管理系统两台服务器A和B，通过双机HA管理服务器A和B的高可用，并对用户提供访问服务；水土中心也是同样配置。用户可以输入上丁中心运维账户及操作风险管理系统地址登陆上丁运维账户及操作风险管理系统进行上丁和水土两个中心生产运维，也可以输入水土中心运维账户及操作风险管理系统地址登陆水土运维账户及操作风险管理系统进行上丁和水土双中心服务器生产运维。

运维风险管理服务器内部包括应用和数据库两部分。双中心中，一个中心数据库为“W/R”，另一个中心数据库为“R”，双中心数据库同步通过系统自身程序实现，从“W/R”库 往“R”库同步，网络只需3层IP可达即可。

## 应急场景

运维账户及操作风险管理系统应急场景分为四种情况：单中心两台服务器中任意一台服务器应用或数据库出现故障；单中心两台服务器应用均同时出现故障；单中心两台服务器数据库均同时出现故障；双中心应用或数据库均同时出现故障。

应急场景一（单台服务器停止服务，服务包括应用和数据库）：单中心两台运维风险管理服务器A和B（双机HA高可用，A提供服务），当A服务器因硬件、软件或网络等原因，导致应用或数据库或两个都停止服务时，通过HA机制，B服务器会自动接管，对外提供服务。

应急场景二（单中心服务器停止应用服务）：双中心甲中心和乙中心，当甲中心两台运维风险管理服务器A和B同时因硬件、软件等原因，停止应用服务时，乙中心运维账户及操作风险管理系统可以接管，对外提供服务。

应急场景三（单中心服务器停止数据库服务）：双中心甲中心和乙中心，当甲中心两台运维风险管理服务器A和B同时因硬件、软件等原因，停止数据库服务时，如果甲中心数据库配置为“W/R”，则需要手动将乙中心数据库配置改为“W/R”，乙中心两台运维风险管理服务器A和B数据库才可以接管服务，如果甲中心数据库配置为“R”，则乙中心运维风险管理服务器数据库可以直接提供服务。

应急场景四（双中心服务器停止服务，服务包括应用和数据库）：双中心甲中心和乙中心，当双中心4台运维风险管理服务器同时因硬件、软件或网络原因，停止应用或数据库服务时。开放备份保存的生产服务器密码，通过双中心各最后一台容灾跳板机（开通访问双中心生产服务器网络策略，跳板机及密码由内控组管控）登陆生产服务器进行运维。

## 第三方系统对接

* ITSM系统

通过与ITSM系统对接，获取生产运维资源申请数据和事件变更单数据，实现ITSM统一的权限申请审批流程管理。

* CMDB平台

通过与CMDB平台对接，同步生产资产更新数据。保障CMDB资产数据的准确性。

## 软硬件配置

运维账户及操作风险管理系统服务器配置如表2所示

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 服务器种类 | CPU  要求 | 内存  要求 | 存储  要求 | 数量 | 硬件  平台 | 操作系统及版本 | 备注 |
| 主服务器 | 8C | 32G | 2T | 4 |  | 厂商提供操作系统及数据库 | 虚拟机 |
| 发布服务器 | 4C | 16G | 500G | 6 |  | Windows server2012及以上 | 虚拟机 |

表2运维账户及操作风险管理系统服务器配置

# 技术需求

## 系统要求

### 软件架构及客户端要求

运维账户及操作风险管理系统采用B/S软件体系结构开发，同时支持C/S模式运维，用户访问支持Windows10环境及IE浏览器11版本。

### 系统功能设计要求

运维账户及操作风险管理系统作为管理运维安全的产品，其系统功能设计满足“4A”安全管理要求，即集中认证(Authentication) 、集中帐号(Account)、集中授权 (Authorization) 、集中审计(Audit)。

### 账号自动改密要求

账号自动改密须提供安全、可靠的改密机制，确保改密过程中风险可控，改密后能正常登陆，并保存改密前后的新旧密码。其安全改密机制应不低于如下改密机制：

1. 改密前按自定义的密码策略生成期望密码，并将期望密码存储在运维风险管理数据库中
2. 根据期望密码生成改密模板，调用系统服务进行登录比对改密。
3. 改密完成后，使用期望密码进行账号密码登陆测试
4. 账号密码登陆测试成功，则将运维风险管理数据库中原密码存储为旧密码，期望密码更新替换原密码。登陆测试失败则改密失败。
5. 改密成功后，通过邮件或其它方式加密导出保存变更后的密码。账号密码文件和解密密钥分开保管。

### 系统其他要求

* 为适应行内服务器虚拟化发展，方便统一化管理，系统须能同时支持虚拟化部署及云化部署。

## 数据库要求

系统须支持国内外主流商用数据库产品，并且实施厂商能在一定时期，根据行内基础设施及系统软件规划要求提供相应解决方案，负责平滑迁移数据库。

## 性能要求

### 响应时间要求

* 为提升用户体验，通过运维账户及操作风险管理系统登陆目标服务器的等待时间应控制在：文本协议连接1秒以内，图形化远程桌面连接在5秒以内。
* 审计数据查询及报表统计查询应在5 秒以内；

### 总体处理能力及并发处理能力要求

* 从系统网络中心提供的数据，我行现有生产主机（包括虚拟机）、数据库及网络设备约3000台，考虑到业务的发展、双中心的建设、设备的增长，故系统的资产管理能力应不低于6000台。
* 现有科技部运维人员106人，按同时在线运维人员最多60人（参照新核心上线时数量），每人平均字符会话5个，图形会话3个计算，系统联机交易字符会话并发数应不低于300，图形会话并发数应不低于200。

### 可靠性要求

系统应支持7×24的连续运行。为了支持系统的不间断服务要求，系统应支持单中心高可用，双中心双活架构，以提升系统稳定性及容灾能力。

### 安全性要求

1. 在本系统投产前和日常运行中，对行内通过专业工具不定期对本系统进行安全扫描发现的漏洞及时进行修复。
2. 网络传输采用SSL协议，提高数据传输的安全性，并对SSL证书有效性进行校验。URL参数使用数据国密算法加密，保护数据的安全性。
3. 在身份认证、数字签名、数据加密等方面要求具备安全保密功能，确保系统数据、用户数据的保密性、完整性、可用性。
4. 系统须对用户选择的密码进行检查，避免用户采用过于简单的密码，支持用户密码定期改密及密码连续输错多次自动锁定等密码安全保护机制。
5. 满足除以上要求外，还需满足《信息安全技术 网络安全等级保护基本要求》的相关要求。

## 运维要求

### 日志查看要求

用户在运维风险管理平台查看日志时，系统须提供机制，保障不管在哪个服务器上都可以查看到完整的日志记录，而不需要再登陆到发生交易的服务器上去查看。

### 监控要求

按照当前监控要求，对系统硬件资源使用情况及数据容量等指标进行监控。

### 数据库备份要求

定期备份数据库数据，制定数据库备份清理策略，数据库审计数据可保留近6个月内数据，超过6个月线下离线保存。后期可根据业务具体情况进行调整。

### 日志备份要求

生产日志可实时查询6个月内日志，生产日志保留1年的日志备份。

### 离线数据查看要求

数据离线备份保存后，遇需要查看离线数据的情况，须提供离线数据查看方式。

### 日常运维要求

系统应提供便捷的方式，方便运维人员查看系统状态，迅速对系统服务进行重启，恢复系统正常运行。对于运行在linux操作系统上的应用系统，用户登录后应自动展现运维菜单，包括：应用启动、应用停止、状态察看等操作内容。运维人员可输入数字选项进行相应的运维操作。其具体内容如下：

* 应用启动

指启动应用进程操作，如果该系统有多个进程，并且之间相互独立且有启动先后顺序，则可以将该操作分成多个启动选项；

* 应用停止

指停止应用进程操作，如果该系统有多个进程，并且之间相互独立且有停止先后顺序，则可以将该操作分成多个停止选项；

* 状态察看

指察看各个进程状态和数目的操作，方便运维人员检查应用系统健康状态；

## 质量管理要求

本项目质量控制目标必须完全实现新建项目所规定的所有内容，各个环节的质量控制贯穿于项目全过程，项目建设过程须遵循重庆银行相关管理办法的要求。

# 其他需求

## 版本要求

提供给我行的版本必须是供应商开发的最新稳定版本。

## 培训

实施周期内通过阶段性培训、项目交付物等方式完成培训

1）系统操作培训需求

系统操作培训指对本系统各类操作使用知识的培训。整个培训应基于实施厂商提供的操作手册，采用集中分批培训的方式对所有使用该系统的人员进行培训。该部分工作由实施厂商配合行内技术人员进行。通过培训要求使用人员熟练掌握运维账户及操作风险管理系统的操作使用方法，提升系统使用人员对系统功能的理解和运用。

2）系统管理培训需求

系统管理培训主要是指对应用软件的管理和维护。经过培训要求系统管理人员熟练掌握应用系统业务方面常用的维护、配置内容，包括：用户的添加、修改、删除，资产账号的添加、修改、删除，权限的配置及高危命令的配置等。

3）运维知识转移需求

通过培训重庆银行运维人员，使运维人员熟练掌握系统工作模式，数据结构和数据处理、流转原理，查看系统日志能初步判断出系统运行状况，进行系统服务启停及系统常见问题处理，培训我行系统和数据库维护人员操作系统和数据库的安装、启停，数据库切换及常见问题处理，并提供可执行的操作手册。

## 实施人员要求

运维账户及操作风险管理系统提供商中标本项目前，应在表述中对项目人员作出安排，所有人员入场、撤场、更换均需得到行方项目经理认可。本项目要求配备项目经理，同时要求项目组成员具有扎实的理论知识和丰富的项目实施经验。项目经理须带领团队成功实施过三家及以上银行运维风险管理项目，其他项目组成员必须有2年或以上银行系统项目建设经验。

## 售后要求

系统项目验收后，实施公司需提供一年及以上免费维护服务。在免费服务期内，凡遇系统出现重大故障（如系统无法正常使用），需立即派遣维护人员到现场支持解决问题，如维护人员不在现场，需在接到行方电话咨询后2小时以内给出正式的解决方案并以公司邮件方式发出，4小时内到达现场，8小时内解决故障。

行方在此期间发现的生产产品缺陷，实施公司需在接到行方正式问题邮件提出之日起，最长3日内给出解决方案，最长1月内下发升级包并完成缺陷修复。