银行运维作业自动化系统平台
权限及安全说明

一、 自动化系统平台的权限控制：

平台具有强大用户管理功能，能实现基于角色的用户管理，让不同用户管理不同作业网，满足银行各种用户权限管理需求。

平台有自己的用户管理，主要目的是建立用户对作业网的权限以及同操作系统用户之间的映射。整个用户管理由用户，角色，映射关系三个方面组成。详细的用户管理增强了业务管理的安全性，可靠性。

（1）用户

在认证服务器（JP1/AJS2 管理端）建立 JP1 用户，提供登录 JP1/AJS2 管理端的用户名和密码。

（2）角色

在用户基础上分配该用户角色，不同角色拥有不同的权限。

权限	说明
JP1_AJS_Admin	管理员权限。具有对单元所有者、资源组操作权限、以及作业网等的定义・执行・编辑权限
JP1_AJS_Manager	作业网的定义・执行・编辑权限
JP1_AJS_Editor	作业网定义・编辑权限
JP1_AJS_Operator	作业网的执行・浏览权限
JP1_AJS_Guest	作业网的浏览权限
JP1_JPQ_Admin	管理员权限。具有作业执行环境的设定权限、队列和作业执行代理器的操作权限、以及对其他用户的队列作业的操作权限等
JP1_JPQ_Operator	队列和作业执行代理器的操作权限、对其他用户的队列作业的操作权限
JP1_JPQ_User	作业的提交、以及本机队列作业的操作权限

也可以把几个角色合并在一起组成资源组，在作业网定义的时候就可以一次性指定某个用户对作业网所拥有的几个角色。并且角色可以基于作业网来定义，不同角色拥有不同作业网的权限。

（3）映射关系

JP1 用户和操作系统用户之间有对应关系，即从管理端向业务主机调度作业时，JP1 用户要作为执行程序主机的 OS 用户来对待。并且新建，修改，删除用户等操作都可以由 GUI 方式实现。

通过这种映射关系的设置，可以使 JP1 进行作业调度时只拥有特定的 OS 用户权限，避免可能带来的安全隐患。

二、 Agent 方式部署的权限管理：

Agent 方式部署即在业务主机上安装 Agent 组件及相关模块。安装时需要使用管理员权限，并在安装完成后进行一个或多个 OS 用户映射。在设计作业网（即作业流程时，需指定作业单元执行所使用的用户），通过分离设计作业网与执行作业网的权限即可实现简单的安全管理。

Linux、Unix 系列的主机，映射完成之后修改 OS 用户密码，不需要再次设定映射关系。

Windows 系列主机，当修改了 OS 用户密码时，需通过 GUI 界面，完成映射关系中的密码修改。通过部署 ID 插件，可以实现自动修改密码，但需二次开发。

三、 Agentless 方式部署的权限管理：

Agentless 方式部署即无需在业务主机上安装 Agent 及相关组件，但需在 Linux/UNIX 主机上开放 SSH 协议端口；在 Windows 主机上安装 SSH 协议并开放相应端口，或者开放系统自带的远程管理接口；

该方式下无法进行 OS 用户映射，远程调度执行自动化管理时需要用到 OS 的用户名及密码，OS 用户名密码需要保存在平台管理端数据库中。目前采用密文保存，使用时通过特定脚本读取数据库后进行连接自动化操作。

该方式下无论 Windows 系统还是 Linux/UNIX 系统，当修改了 OS 用户密码时，需通过 GUI 界面，或者 BS 系统界面进行修改。也可通过部署 ID 插件，实现自动修改密码，即密码同步，但需二次开发。