深圳竹云科技有限公司

竹云身份管理平台白皮书

Bamboocloud Identity Manager Products White Paper

编号：BBC-WP-BIM-2018001

深圳竹云科技有限公司

2018 年 4 月

目录

1 背景

随着信息化的发展，企业应用系统规模日渐庞大，信息安全威胁也逐渐增多，据统计，约有 80%的信息安全威胁来自于企业内部，其中绝大多数是由于对应用系统账号及权限的管理不当造成的。员工账号与权限的传统管理方式主要为系统管理员在业务系统中逐个手动创建，这样既增加了工作量，同时失误也不可避免，造成某些员工权限不够必须重复申请，而某些员工拥有超过其工作所需的权限，对企业造成信息安全威胁，尤其在企业员工集中入职或企业组织机构发生调整时更为明显。员工对于某些应用系统使用权限的申请尽管大多数企业都拥有完整的流程，但缺乏有效监控，同样也造成员工权限未被回收的安全隐患，具体存在的问题与风险如下：

- 数据泄密风险高：用户账号的手工创建和回收，导致应用系统存在孤儿账号、违建账号的可能，导致数据泄密风险及经营损失风险增加。
- 流程效率低：大量用户电话要求重置密码、入职、离职等手工操作，IT 服务部门需要投入大量资源处理用户账号及体验问题，造成资源浪费和服务乏力。
- 用户体验差：用户需记忆众多不同账号和密码，一旦用户忘记密码，频繁联系管理员处理，用户满意度不高体验差。
- IT 建设成本高：各应用系统的用户体系独立建设，造成 IT 重复建设和企业成本增加。
- 为了有效的应对这些问题，身份管理产品提供用户的生命周期管理，统一管理用户在各个应用系统中的账号，提供统一的用户自服务，能够有效的降低风险，提升用户体验，优化现有的流程。

2 产品介绍

2.1概念和术语

- BIM：竹云面向企业的统一用户身份管理产品，即 Bamboocloud Identity Manager
- BAM：竹云面向企业的统一访问控制系统，即 Bamboocloud Access manager
- AppHub：竹云面向企业的统一导航平台
- e 账通：竹云面向企业的生物特征认证平台
- 回收: 将外部系统中的信息同步到 BIM 中的过程
- 供应: 将 BIM 中的信息同步到应用系统中的过程
- 连接服务器：在 BIM 中主动发起供应和回收的时候，需要通过连接服务器来统一与应用系统交换信息
- 用户：所有自然人在 BIM 中都对应一个用户。BIM 中也允许虚拟用户存在。所有用户都有唯一的用户名。
- 组织机构：用户的基本属性之一，标识用户的隶属关系
- 组织机构树：组织机构以树形形式组成一棵树就是组织机构树，可以有多棵机构树
- 应用系统：与 BIM 集成的应用系统，比如 HR 系统，OA 系统等
- 账号：每个接入 BIM 平台的应用系统,都对应一个应用账号。 可以一个用户对应多个账号,也可以多个用户对应一个账号。
- 应用机构：应用系统中的组织机构，可以与系统的机构对应，也可以单独的维护
- 平台权限：用户在 BIM 系统中的权限，包含菜单权限，数据权限

2.2产品描述

BIM 为企业提供统一用户管理，实现用户信息与账号的集中存储、全生命周期闭环管理。

BIM 平台包含 4 个部分分别为身份管理引擎，开发平台，业务控制台以及自服务平台。这 4 个部分自成一体。

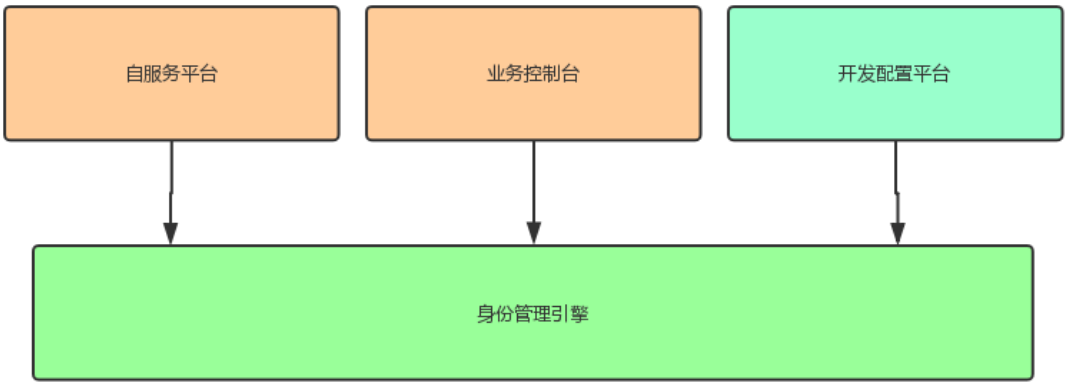

图 1 产品描述示意图

身份管理引擎主要提供供应和回收等核心功能，并负责调度作业运行，工作流执行，过程任务运行等。提供面向产品的 api，供开发平台，业务控制台以及自服务平台使用。同时提供面向外部的 api，供应用系统接入以及与其它系统集成

开发平台主要是开发集成时使用，可以完成身份管理系统本身的初始配置以及应用系统的接入配置。

业务控制台主要是业务人员使用，通过分级授权，管理 BIM 平台的用户以及机构，管理各应用系统中的账号，应用机构以及应用资源。同时提供报表、合规、审计、平台运维等功能。

自服务平台所有用户都使用。用户可以自注册，找回账号，忘记密码，自助维护密保工具，管理自己的密码等。同时可以申请应用权限和办理审批事项。

2.3特点和优势

- 业务贴合紧密：具备很强的灵活性、适应性、可扩展性，紧密贴合业务需求。
- 组件化配置：核心代码 Core JAVA， 完全组件化模式，轻松部署。
- 标准化接口：提供完整的管理 REST API 接口，可轻松进行业务流程再造，并提供主动供应和主动下拉模式，支持供标准化的集成场景。
- 多类型接口提供：提供丰富的标准产品连接器，轻松配置，即插即用。
- 可配置化管理：提供灵活的自定义连接器配置，轻松配置，开发简单。
- 安全数据管理：一应用一通道，数据单独管理，数据安全且有保障

BIM 除了支撑企业自身业务发展的形势和信息化建设的要求外，还可以帮助企业业务及信息系统提供强有力的支撑，其产品应用价值主要体现在以下方面：

- 用户的集中管理，可快速促进信息化资源整合；
- 电子身份的自动化流程管理，可有效的提升流程效率；
- 统一身份管理建设，可提升整体信息化安全水平；
- 统一身份管理建设，可控制经营成本与投入；
- 可快速帮助企业有效执行合规要求；
- 大幅改善应用系统用户体验，提升企业用户满意度。

2.4 系统架构

2.4.1 整体架构

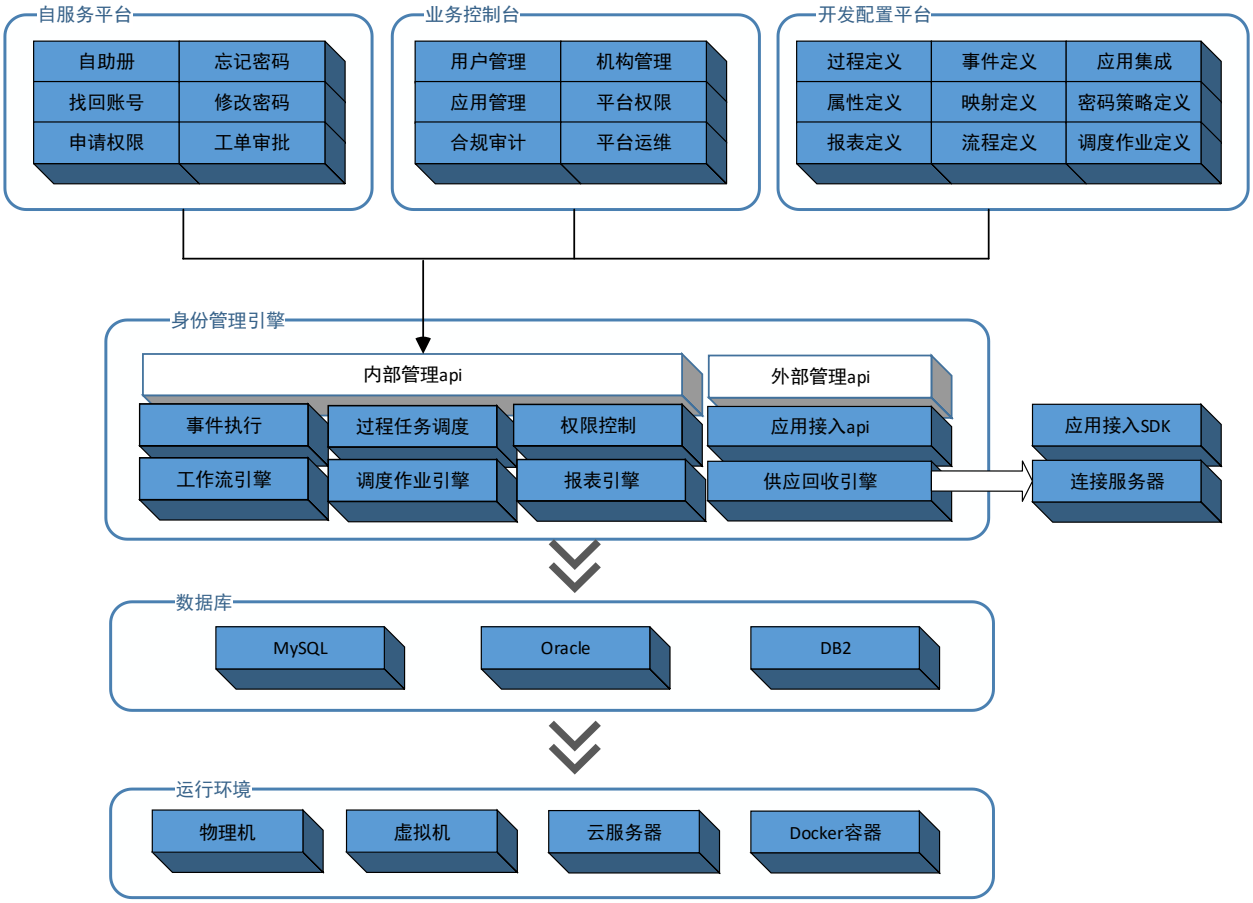

图 2 整体架构示意图

BIM 的整体架构如上图所示，身份管理引擎是核心，包含供应回收引擎，调度作业引擎，工作流引擎，报表引擎，并提供多样性的 API，供内部使用以及外部使用。

自服务平台、业务控制台是客户最终使用的平台，开发配置平台在集成配置的时候使用，三个不同的入口为不同的用户所使用。

2.4.2 兼容性

BIM 采用标准的 J2EE 体系统的结构构建，可部署并运行于标准的 Java Web 应用环境。支持的环境说明如下：

- 操作系统：支持 Windows、Linux 和 Unix 等各种 64 位的系统平台。
- Java 虚拟机：支持 JDK 1.6 x64 及以上版本。
- 数据库：支持 Mysql、Oracle、DB2 等数据库。
- 应用服务器：支持 Tomcat、WebLogic、WebSphere 等应用服务器，也可以不使用应用服务器，直接启动。
- 浏览器：支持 IE8 以上版本，以及 Chrome、Firefox 等浏览器。

2.4.3 运行环境

- 系统由 JAVA 开发，可兼容 X86 架构的各种硬件
- 支持虚拟机部署
- 支持云平台部署
- 支持 docker 容器部署

2.5主要功能介绍

2.5.1 用户管理

BIM 提供用户管理功能，主要功能包含：

- **用户属性自定义：**在开发平台中自定义用户属性，不同类型的用户可以有不同的属性。支持单值，多值属性，支持基本数据类型以及关联属性类型。
- **用户基本信息维护：** 平台存储用户基本信息、机构信息、岗位信息等，可以自动从其它系统同步，或者管理员通过平台进行维护和管理，提供基本的用户的新建、变更、启用、禁用，调动、删除等操作。用户属性的变化自动的同步到用户的所有主账号中。
- **用户应用权限管理：**维护用户的应用权限，包含权限分配，权限撤销等。支持按照策略的自动分配和撤销，也支持管理员手动的创建、变更、启用、禁用、删除，并支持批量操作。
- **注销用户管理：**对于已经注销的用户提供查询，导出等功能，也提供物理删除功能。

2.5.2 用户密码管理

BIM 集中管理用户的密码信息，密码信息的安全性关系到接入了 BIM 的应用安全性。

通过自服务的功能，用户可以自己维护自己密码。

- 密码策略：平台支持定义多套密码策略，密码策略作用在用户或者应用账号上，通过匹配规则来确定用户或者账号使用的什么密码策略。密码策略包含密码本身的复杂度，也包含密码的使用策略。
- 密码策略的应用：无论是用户通过自服务来修改密码或者重置密码，还是管理员通过业务控制台来修改密码或者重置密码，都会应用密码策略。用户在登录的时候会检查用户密码是否过期，如果快过期将提醒用户，如果已经过期，将强制用户修改密码。
- 密保工具维护：用户自己维护手机、邮箱、密保问题这些密码工具。初次登陆的时候根据配置强制初始化密保工具，维护密保工具的时候需要选择一种密保工具来验证。所有的密保工具是对等的。
- 忘记密码：支持通过手机、邮箱、密保问题重置密码。
- 密码安全存储：密码等敏感信息自动加密存储在数据库中，支持 AES 加密，SM4 加密

2.5.3 机构管理

BIM 提供组织机构管理功能，并支持多组织机构树，主要包含如下功能：

- 机构属性自定义：自定义机构属性，不同机构树上的机构可以有不同的属性。支持单值，多值属性，支持基本数据类型以及关联属性类型。
- 多维组织机构：为了适应企业有多套机构的情况，BIM 提供多机构树的管理。可以对不同的机构树分别维护。机构可以自动从其它系统同步，也可以由管理员手动在 BIM 上维护。
- 组织机构信息维护： 平台存储机构基本信息，自动从其它系统同步，或者管理员通过平台进行维护和管理，提供基本的机构的新建、修改、删除等操作。机构属性的变化自动的同步到应用系统中。机构在系统中以树形展示。
- 组织机构转移合并：组织机构的隶属或从属关系通过划转的方式进行迁移和合并。转移合并过程中自动处理用户的变化。
- 撤销机构管理：对于已经撤销的机构提供查询，导出等功能，提供物理删除功能。

2.5.4 应用管理

BIM 通过开发平台对应用管理提供如下的功能：

- 应用属性自定义：自定义应用属性，支持单值，多值属性，支持基本数据类型。

- 应用信息维护： 平台存储应用的基本信息。提供基本的应用的新建、修改、删除等操作。
- 应用对象自定义：一个应用系统中可能有比如账号，应用机构，应用角色等对象，还可能有比如菜单，菜单权限等对象。为了管理这些对象，BIM 平台需要先定义这些对象。BIM 平台支持自定义各种应用对象，通用的对象包含账号，应用机构，应用组，应用角色，对于非通用的对象，都使用应用资源来表示。
- 应用对象属性自定义：不同的应用对象有不同的属性，可以对不同的应用中的不同对象分别自定义属性，支持单值，多值属性，支持基本数据类型以及关联属性类型。

2.5.5 应用账号管理

应用系统中账号分为三类：普通账号，公共账号和孤儿账号。普通账号是和人关联的账号，一个人在一个应用系统中可以有多个普通账号，其中一个账号是主账号，其它为从账号。主帐号的属性会主动的和用户属性同步，从账号一般只自动同步密码。普通账号的生命周期一般小于对应的用户的生命周期。公共账号不与具体的人绑定，只设置使用者和责任人。公共账号的生命周期与其使用者和责任人没有直接关系。孤儿账号是因为特殊原因出现的账号，可以作为普通账号和公共账号转换的桥梁。

应用账号管理主要包含如下功能：

- 普通账号管理： 提供普通账号的新建、修改、删除、解绑、启用、禁用、修改密码等操作。
- 孤儿账号管理：支持孤儿账号绑定到用户成为普通账号，也支持孤儿账号转成公共账号。可以创建孤儿账号。
- 公共账号管理：公共账号可以标记为系统账号，公共账号可以转换成孤儿账号。对于公共账号可以设置责任人和使用者，责任人负责管理公共账号的密码，使用者通过 apphub 在不知道账号密码的情况下可以使用此公共账号。
- 账号所属应用角色：如果应用系统中有应用角色对象，并且应用角色是多值属性，可以通过账号管理单独管理账号所属应用角色。
- 账号所属应用组：如果应用系统中有应用组对象，并且应用组是多值属性，可以通过账号管理中单独管理账号所属的应用组。

2.5.6 应用机构管理

在 BIM 中通过树形管理应用机构：

- **应用机构管理：** 提供应用机构的新建、修改、删除等操作。

2.5.7 应用对象管理

应用中除了常见的应用账号和应用机构外，还有应用角色，应用组等常见对象以及应用资源对象，比如应用菜单，应用菜单权限等。

- **应用角色管理：**提供应用角色的新建、修改、删除等操作。
- **应用角色成员管理：**通过 BIM 管理应用角色成员，管理应用角色与应用账号的关系。
- **应用组管理：**提供应用组的新建、修改、删除等操作。
- **应用组成员管理：**通过 BIM 管理应用组成员，管理应用组与应用账号的关系。
- **应用资源管理：**提供应用资源的新建、修改、删除等操作。

2.5.8 平台权限管理

平台权限分为菜单权限和数据权限，菜单权限通过菜单角色与人关联，数据权限直接与人关联。数据权限分为机构权限、应用权限、应用机构权限和报表权限。主要包含如下功能：

- **平台菜单角色管理：**系统内置了一批菜单角色，可以根据需要创建、修改、删除菜单角色，可以给菜单角色赋予不同的菜单权限。
- **给用户分配权限：**选定管理访问内的用户之后，可以给用户分配菜单权限，机构权限、应用权限、应用机构权限和报表权限。
- **将权限分配给用户：**选定权限（包含菜单权限，机构权限、应用权限、应用机构权限和报表权限）之后，可以看到拥有此权限的用户，可以将权限分配给其他的用户 。
- **分级授权：**管理员可以将自己的权限子集分配给自己管理范围内的用户，实现分级管理功能。对于任何权限都可以控制是否可以再分配。

2.5.9 供应

满足一定条件的用户可以自动的分配账号，满足一定条件的机构也可以自动的供应到应用系统中。对于已经供应或者已经回收的对象，平台可以自动将对象在平台中的变化同步到应用系统中，也提供应用系统主动下拉的接口。

- **供应策略：**平台通过全局角色实现账号的自动分配，提供全局角色的新建、修改、删除等操作。全局角色成员可以是静态成员，也可以通过匹配规则定义动态成员。
- **匹配规则：**匹配规则确定了满足一定条件的对象。支持 AND 和 OR 逻辑运算，支持子规则。匹配规则不仅仅用在自动供应中，还可以应用到密码策略，映射定义中。

- **撤销策略：**对于自动供应的账号，当用户不满足条件或者不是全局角色成员的时候提供撤销策略。撤销策略可以立即撤销权限，或者禁用权限，或者保留权限。
- **事件：**通过内置的事件实现机构的自动供应，将满足条件的机构自动同步到应用系统中。平台支持自定义事件，在任何操作之前或者操作之后做特定的处理。
- **过程任务：**通过过程任务的异步执行，将应用系统对象在平台中的变化主动的推送到应用系统。也支持过程任务的被动执行，也就是应用主动下列。过程任务支持串行执行，并行执行，也支持串行忽略执行。过程任务支持自动重试。
- **映射规则：**提供对象属性之间的转换规则，分别作用在预填充、供应、应用对象回收和系统对象回收上。映射定义对于每个不同的属性，使用匹配规则来确定映射规则。可以使用复制，脚本，自定义处理等来实现映射规则。

2.5.10 回收

对于应用中已有的对象，可以通过回收功能将对象纳入平台来管理。平台提供两种类型的回收。

- **应用对象回收：**应用对象从应用系统回收到 BIM。回收可以是 BIM 主动发起，也可以是应用系统主动发起。提供增量回收，全量回收，支持基于查询的回收，也支持基于变更日志的回收。
- **系统对象回收：**将应用对象回收成 BIM 的系统对象，比如用户回收，机构回收，数据字典回收等。提供增量回收，全量回收功能。
- **数据字典：**数据字典就是一个键值对的集合。提供数据字典定义，数据字典内容维护功能。数据字典支持空值，支持加密存储，支持树形结构。支持数据字典的回收。
- **回收事件：**对于每一个对象的回收，都会创建回收事件，并根据操作类型做不同处理。通过回收事件跟踪回收处理，可以自定义回收事件处理器。

2.5.11 定时任务

系统内置定时任务引擎，执行批量作业，比如回收等。定时任务包含如下功能:

- **定时任务定义：**系统内置一批定时任务模板，可以根据需要创建，修改，删除定时任务。也可以自开发定时任务来运行。支持灵活多样的执行时间参数配置，支持运行参数配置。
- **定时任务运行：**根据定时任务配置的时间参数执行任务。支持单次执行，循环执行，定时执行。

- **定时任务历史：**系统维护定时任务的历史记录。对于失败的定时任务，详细记录出错点的堆栈信息供运维分析原因。

2.5.12 通知

通知在平台中广泛使用，比如工作流任务通知，重置密码通知，修改密码通知等。平台内置通知引擎，内置 3 种通知方式

- **邮件通知：**提供发送邮件功能。
- **短信通知：**提供发送短信功能
- **钉钉通知：**提供发送钉钉消息功能。

2.5.13 合规

合规需要从两个维度来描述，一是什么岗位的用户可以有什么样的应用系统权限，二是什么权限是互斥的。对于需要合规检查的系统，可以配置开启合规检查。合规包含如下的一些功能:

- **合规规则：**每条规则定义了岗位与应用以及应用角色的关系。可以按照应用来定义合规规则，也可以按照岗位来定义合规规则。
- **互斥规则：**互斥规则分为应用系统内规则和跨应用系统的规则。应用系统内的互斥一般是应用角色的互斥，通过账号来体现。跨应用系统的互斥通过用户来体现。
- **岗位维护：**岗位一般从 HR 或其它数据源同步回来，也支持管理员手动的维护岗位信息，支持岗位的创建、修改、删除等操作。
- **合规检测：**无论是创建账号还是修改账号或者岗位调动，都会进行合规检测。对于不满足合规定义的给出提示，对于满足互斥定义的直接拒绝操作。
- **合规报表：**对于不合规的账号以及通过回收发现的互斥账号提供报表功能，提供按用户来询，以及按应用查询的功能。报表支持导出成 excel，pdf，word，html 等格式。
- **报表定时发送：**有些报表需要按照固定的周期生成，通过定时任务，周期性的或者在某些时间点生成报表并发送报表文件到个人邮箱。

2.5.14 审计

审计主要通过操作日志来体现，任何用户做的任何操作以及操作的内容都被记录下来。主要包含如下的一些功能:

- **操作日志：**管理员通过业务控制台做的所有操作都被详细记录，包括操作的内容，被操作的对象，时间等。提供查询一个用户在一段时间内做的所有操作的功能，如果是修

改操作还好汉修改的新旧值。业务对象被删除之后，操作记录仍然可查询。

- **变更溯源：**平台对于管理员通过业务控制台的操作，用户通过自服务的操作以及后台服务通过定时任务的操作都会记录操作日志。无论是用户、机构还是应用系统中对象，任何变化都可以追溯到是谁在什么时间的什么操作引起的。
- **对象轨迹：**对于用户、机构以及应用系统中对象，通过每个对象的历史变更记录以及变更源头，完整的反应这个对象在整个生命周期中轨迹。

2.5.15 报表

报表分为两类，一类是查询报表，另外一类是统计报表。统计报表不仅支持静态的统计还支持动态的参数。

- **报表定义：**系统内置 15 张报表，可以根据需要重新定义报表（调整参数），也支持自开发报表，然后再定义报表。支持报表本身的创建、修改、删除，参数调整等操作。
- **报表查看：**无论是查询报表还是统计报表，都支持在线实时查看。对于查询类报表支持输入参数查询。
- **报表导出：**在线报表查看时支持将报表导出成 excel，pdf，word，html 等格式。
- **报表定时发送：**有些报表需要按照固定的周期生成，支持通过定时任务，周期性的或者在某些时间点生成报表并发送报表文件到个人邮箱。

2.5.16 工作流

基于 Activiti 工作流引擎构建了工作流平台，主要功能包含：

- **工作流模型：**在线创建，修改工作流模型并发布成流程。
- **工作流流程：**工作流流程的激活与挂起，支持工作流流程的导入与导出。工作流流程支持直接转换成模型来编辑。
- **工作流任务分配：**配置工作流流程中任务的审批人，支持指定固定的人，指定用户组以及自定义处理器来动态指定。系统内置一批工作流任务分配处理器。
- **工作流策略：**配置不同的请求类型对应的工作流。支持通过脚本或者 java handler 来确定请求对应的流程。
- **工单的拆分与合并：**应用账号申请这类复杂请求拆分成多阶段，实现工单的智能审批以及并行审批。
- **申请与审批：**通过自服务，用户自助申请应用系统权限。审批人在自服务中审批请求。审批通过之后用户将自动的被授予或者撤销对应的应用系统权限。

- **工单跟踪：**申请人或者管理员都可跟踪工单的审批情况，审批人可查看工单的审批历史
- **工单通知：**审批人有任务待办，或者工单审批结束之后自动通知用户，支持内置的所有通知方式。
- **审批代理设置：**用户将自己的工单审批权限代理给其它用户 。对于已经生效的代理可以提前结束，没有生效的代理可以直接撤销。代理用户可以帮助审批工单。

2.5.17 导入导出

系统提供了丰富导入导出功能，主要分为如下 3 个部分：

- **业务数据的导入与导出：**用户、机构、应用账号、应用角色、应用组、应用机构、应用资源等对象导入与导出。导出的数据范围受当前用户的数据权限限制。导入功能是运维功能，一般在上线时执行，不校验具体的数据权限。系统提供导入模板下载，按照模板填写即可直接导入。导入导出都支持 csv 和 Excel 格式。
- **配置信息的导入导出：**配置从一个环境迁移到另外一个环境使用配置信息的导入导出。支持导出的对象包含属性定义，应用系统，应用对象定义，java Handler，过程定义，事件定义，映射定义，定时任务，报表定义，工作流配置等。导出的格式为 json 格式。
- **平台权限的导入导出：**批量的初始化平台管理员，以方便支持分级授权模型。平台权限的导入支持菜单权限，机构权限，应用权限，应用机构权限，报表权限。

2.5.18 自服务

自服务是所有用户都可以使用的，主要包含如下功能：

- **自注册：**用户自己在 BIM 注册用户。对于注册过程可以配置审批流程。如果自注册有审批流程，用户在不登陆 BIM 的情况下能够跟踪审批流程的执行情况。
- **忘记账号：**支持通过邮箱，手机号，员工号找回账号。
- **信息维护：**自己维护特定的信息。支持用户查看自身的历史记录，看谁在什么时间对自身用户做了什么操作。
- **应用权限：**查看自身的应用系统账号以及账号的历史，支持申请账号。可以查看自己使用的公共账号。自己管理的公共账号，可以修改密码并维护使用者。
- **OTP 绑定：**为了实现 OTP 登陆，支持用户自助绑定 OTP。
- **安全测评：**根据用户的密码，OTP 绑定以及手机，邮箱等信息，评估用户账号的安全性。

2.5.19 运维

为了方便上线后的系统运维管理，提供了如下的功能

- **平台监控：**系统内置数据库监控，系统资源监控等。并提供健康检查接口，方便与监控平台对接。
- **系统运行监控：**无论是过程任务，定时任务，还是回收事件，提供查询界面供运维人员及时了解系统运行情况。出现错误之后都完整的保存堆栈信息供运维分析。
- **集群维护：**提供集群成员自动维护功能。比如身份管理引擎集群有 4 台机器，其中 1 台停机维护时，集群自动将其移除。服务启动之后会自动的加入集群。
- **功能自动转移：**对于过程任务，定时任务，回收事件处理等需要大量计算资源的处理，可以指定单独的服务器来执行。当指定的服务器宕机时，这些任务的执行自动的转移到集群中其它机器执行。
- **自动归档：**无论是过程任务还是操作日志，数据可能非常多，提供自动按照月份归档功能。

2.5.20 开发平台

开发平台提供了丰富的功能可以扩展 BIM 的功能，并提供完善的开发文档指导开发。开发平台主要是方便用户自定义各种处理器，主要包含如下一些内容：

- **事件处理器：**在每个操作之前或者操作之后执行。比如创建用户之前校验用户属性。
- **过程任务处理器：**在操作完成之后，异步的执行，比如创建账号之后通知用户。
- **定时任务处理器：**定时执行任务，比如定时的执行回收任务。
- **回收事件处理器：**回收事件的处理。
- **映射转换器：**映射时根据自定义的代码来做属性转换。
- **通知接口：**自定义通知方式。
- **密码策略校验器：**自定义密码策略校验方法。
- **工作流任务分配：**动态的根据请求内容确定审批人
- **工作流策略处理器：**动态的确定请求对应的工作流。
- **工单拆分处理器：**拆分工单，实现工单的智能审批。
- **表单字段依赖转换：**动态表单中如果字段之间有依赖，可以自定义依赖处理器。
- **脚本引擎：**在映射定义，匹配规则，审批策略等中都支持脚本，内置 JavaScript，Groovy，Freemarker，Velocity 脚本引擎。

3 产品部署

3.1 简介

BIM 分为 4 个组件，每个组件均可以单独部署。4 个组件都可以在应用服务器上运行，也可以直接启动。任何一个组件都支持集群部署。

在任何一个完整的环境中，至少要有一个身份管理引擎。开发配置平台最多需要一个，在上线开发配置完成之后可以关闭。自服务平台和业务控制台根据需要来部署。

3.2 部署示例

简单部署中各个组件都只部署 1 份，不需要配置集群。一般在开发环境可以使用这种部署。开发环境实际上还可以简化，比如只有身份管理引擎和开发配置平台。

常规部署中无论是自服务，业务控制台或者身份管理引擎都需要使用集群部署，保证系统的高可用性。可以根据需要增加或者减少身份管理引擎，比如自服务使用两台单独的身份管理引擎，业务控制使用另外两台单独的身份管理引擎，这四台身份管理引擎组成一个集群。

在复杂部署中，由于有回收任务或者调度作业以及过程任务等需要消耗大量的 CPU 资源，这时候可以在常规部署的基础上再增加一些身份管理引擎来单独的做调度作业执行以及过程任务执行。

在集群部署时，还可以通过负载均衡设备提供更高的可用性。

3 种不同的部署方式如下图所示：

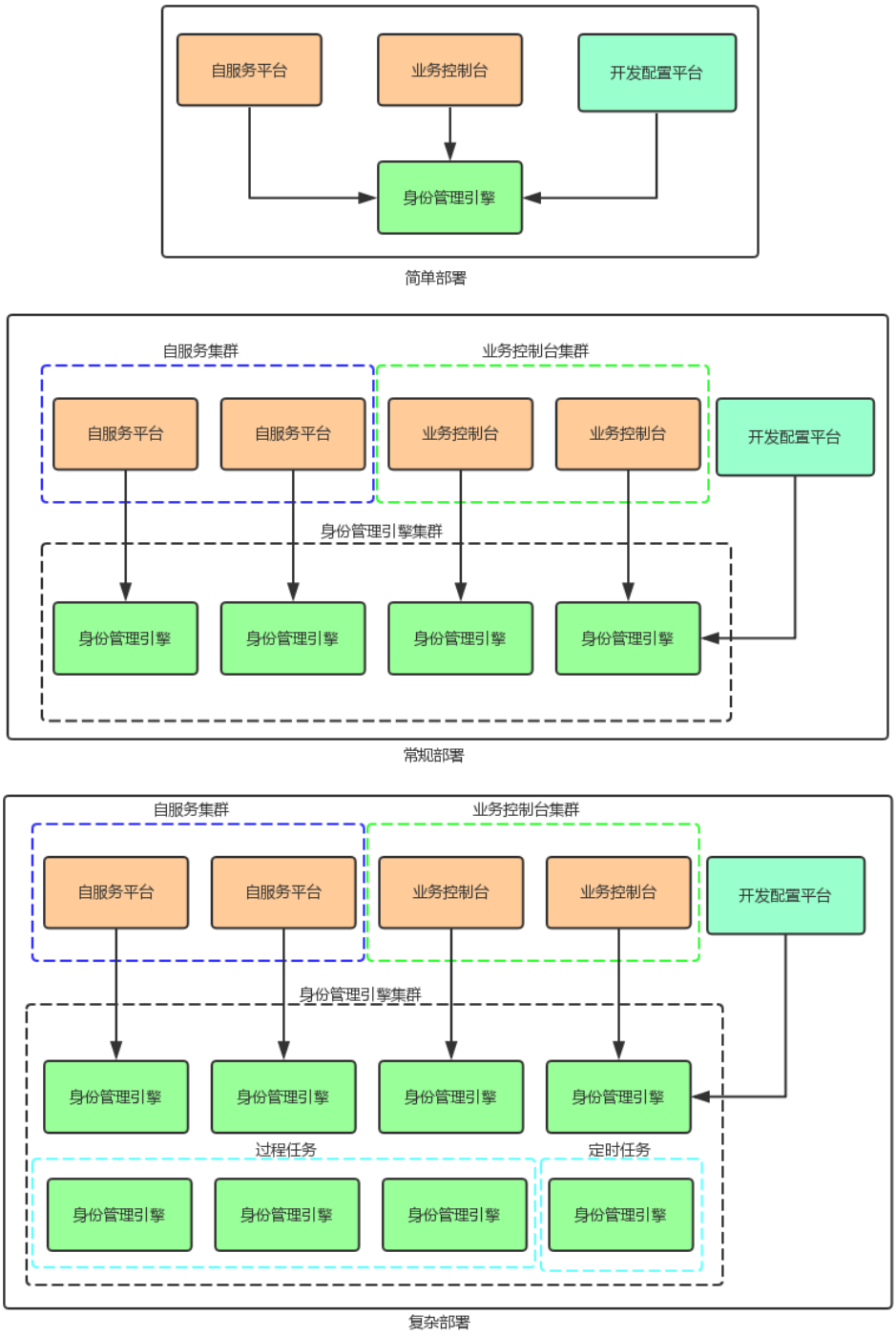
自服务平台
业务控制台
开发配置平台
身份管理引擎
简单部署
自服务集群
业务控制台集群
自服务平台
自服务平台
业务控制台
业务控制台
开发配置平台
身份管理引擎集群
身份管理引擎
身份管理引擎
身份管理引擎
身份管理引擎
常规部署
自服务集群
业务控制台集群
自服务平台
自服务平台
业务控制台
业务控制台
开发配置平台
身份管理引擎集群
身份管理引擎
身份管理引擎
身份管理引擎
身份管理引擎
过程任务
定时任务
身份管理引擎
身份管理引擎
身份管理引擎
身份管理引擎
复杂部署

图 3 部署示例

4 产品集成

4.1内部产品集成

BIM 与竹云的其它主要产品都实现了集成。

自服务和业务控制台与竹云的 BAM 实现了单点登录的集成，可以使用统一的账号访问 BIM 以及其它与 BAM 集成了的应用。并且通过 BAM 以及 e 账通，支持 OTP，短信等多因素认证，也支持指纹，人脸等生物特征认证。

自服务和业务控制台与竹云的 AppHub 实现了融合集成，无论是管理员还是普通用户都可以通过 Apphub 来访问自服务以及业务控制台。

APPHub、BAM、e 账通也也 BIM 做了集成，在身份管理系统中创建的用户将自动的供应到 AppHub、BAM 以及 e 账通中。无论是在自服务中还是在业务控制台中对用户信息的变更包含密码都自动的同步的 APPHub、BAM、e 账通。

为了支持 AppHub 中的应用代填以及用户多账号的情况，BIM 中的应用信息以及应用账号信息也会自动的同步到 AppHub 中。

4.2常见商业应用集成

常见的商业应用一般都提供了对外的接口，BIM 通过这些接口可以管理对应的应用中的账号等信息。BIM 平台提供了标准的连接器与常见的商业产品集成。

4.2.1 通用连接器

通用连接器使用通用的标准接口，与具体的产品无关：

- **DB 连接器：**直接通过 JDBC 接口访问应用系统中表实现对应用系统中对象的管理。
- **LDAP 连接器：**通过 LDAP 协议访问应用系统后台的 LDAP，实现对应用系统中对象的管理。
- **CSV 连接器：**通过文件与应用系统交换信息，使用文件读写接口来实现。

4.2.2 数据库用户管理

- **Mysql 用户连接器：**实现对 Mysql 中的用户管理。
- **SQL Server 用户连接器：**实现对 SQL Server 中的用户管理。

- **Oracle DB 用户连接器：**实现对 Oracle DB 中的用户管理。

4.2.3 商业套件集成

- **AD 连接器：**实现对 AD 中的用户，机构，组的管理。
- **AD 密码反向同步：**用户通过 AD 修改密码之后，密码可以自动同步到 BIM，并通过 BIM 同步到其它应用系统。
- **Exchange 连接器：**通过 remote power shell 实现对 Exchange 邮箱中的用户管理。
- **Lync 连接器：**通过 remote power shell 实现对 Lync 中的用户管理。
- **SAP ABAP 连接器：**通过 ABAP 接口实现对 SAP 中的用户管理。
- **SAP UME 连接器：**通过 Java 接口实现对 SAP 中的用户管理。
- **Lotus Notes 连接器：**通过 DIIOP 接口实现对 Domino 中的用户管理。
- **Oracle EBS 连接器：**通过存储过程实现 EBS 中的用户管理。
- **钉钉连接器：**实现钉钉中的中的用户，机构管理。
- **致远 OA 连接器:**实现致远 OA 中的中的用户、机构管理。
- **seafile 连接器：**实现 seafile 中的中的用户管理。

4.3自定义集成

如果不是常见的商业应用，可以通过 BIM 提供的应用集成接口与应用系统集成，实现对应用系统中的用户等对象的管理。应用系统通过接口集成分为 3 种方式：连接器模式，SDK 模式以及 REST 接口方式。

连接器集成： 连接器定义了标准的创建，修改，删除应用系统中对象的接口，实现连接器的时候需要实现这些接口，完成对应用系统中对象的操作。连接器方式集成的时候 BIM 中的变化可以实时的同步到应用系统中，这些同步可以通过标准的过程任务来完成。如果应用系统中的对象变更之后需要同步到 BIM，使用标准的回收定时任务来完成。

REST 接口集成:BIM 中的应用数据变化之后不立即同步到应用系统,应用系统通过 REST API 来获取应用系统中对应的数据的变化来完成同步。应用系统也可以主动的通过接口将应用系统中的变化数据推送到 BIM。

SDK 集成：为了方便应用系统使用 REST 接口集成，产品封装了 Java 版本的 SDK，应用可以直接使用 SDK 的方式来集成。

4.4外部接口

除了应用集成接口之外，BIM 还提供外部接口。通过外部接口可以方便的将 BIM 与其它系统连接起来。比如与已有的工作流平台对接的时候，工作流审批结束之后，可以使用外部接口自动完成操作。也可以通过外部接口来自定义控制台等。

外部接口分为三类，一类是管理接口，提供 BIM 中所有对象的管理功能。第二类是通用类，比如常见的加解密服务，国密算法被封装在通用类接口中。第三类是自定义类，可以自己定制服务，增强 BIM 的功能。