深圳竹云科技有限公司

竹云权限管理平台技术白皮书

Bamboocloud Identity Management Products White Paper

编号：BBC-WP-2018001

深圳竹云科技有限公司

2018 年 4

目录

1 背景

在当今极具挑战的世界，企业、政府机构和组织团体（以下简称企业）都要依赖于来自各种信息源的信息，尤期在业务决策中需要依赖于这些信息的准确性和可靠性。企业的关键业务均大量地采用计算机系统和网络技术，因此企业基于 IT 环境的业务系统越来越多、越来越庞大，除了传统的服务中断、黑客攻击，也带来了新的威胁和风险，如未经授权的访问、访问权限混乱、授权管理复杂等，进一步突出了信息安全的重要性，这就要求采取适当的管理措施和技术手段确保权限授予的合理性和合规性，企业面临的具体存在的问题与风险如下：

- 高危安全风险：黑心员工非法获取特权账号，修改系统配置和权限，导致信息安全风险加大；
- 数据泄露：存在众多信息孤岛，无法对所有用户的访问权限、访问行为进行集中有效
- 管控，造成大量数据泄密。
- 无法支持合规审计：缺乏实时有效的事前、事中审计，事后责任难以追溯到人；
- IT 建设成本高：各应用系统的权限体系独立建设，造成 IT 重复建设和企业成本增加。

2 产品介绍

2.1 概念和术语

BCM：竹云权限管理产品，即 Bamboocloud Compliance Manager，以下简称“平台”。

2.2 产品描述

竹云权限管理平台 BCM 为企业提供集中的授权管理，实现用户与应用系统权限管理和合规审计，基于角色、应用、群组、数据等多层次细粒度授权，实现权限自动化分配、及时回收和权限互斥。

2.3 特点和优势

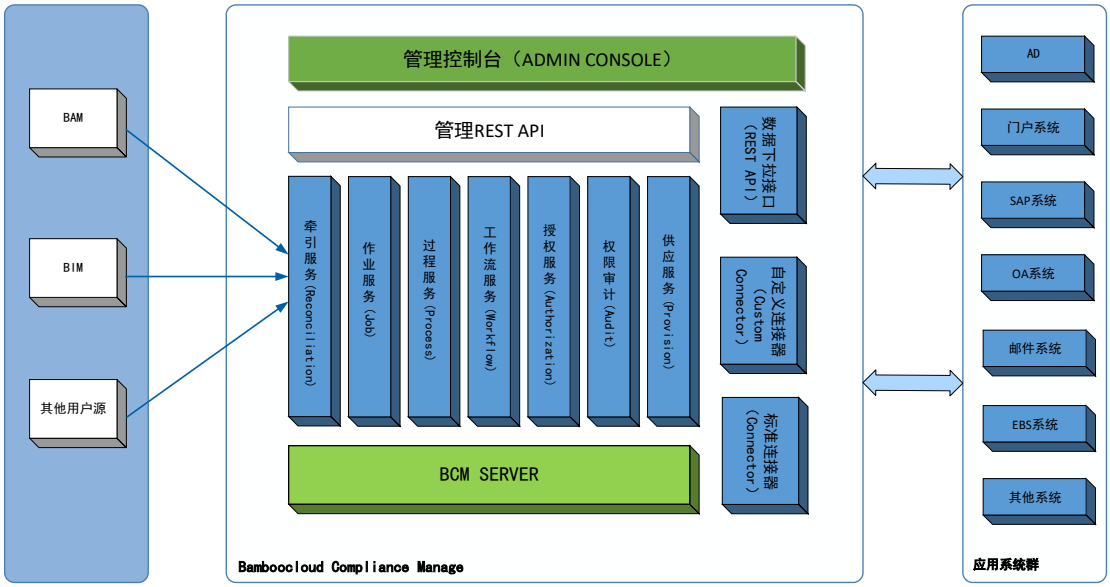
竹云权限管理产品除了支撑企业自身业务发展的形势和信息化建设的要求外，还可以帮助企业业务及信息系统提供强有力的支撑，其产品应用价值主要体现在以下方面：

- 健全的应用权限集中管理，可减少信息泄露和加强隐私保护；
- 统一权限管理建设，可提升整体信息化安全水平；
- 统一权限管理建设，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。
- 产品特点如下：

- 业务贴合紧密：具备很强的灵活性、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，支持标准化的集成场景。
- 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：提供灵活的多认证方法支持配置，轻松配置，开发简单。
- 业务适应性：不仅支持标准的 RBAC 和 XRBAC 权限模型，同时支持复杂场景的权限模型。

2.4 系统架构

2.4.1 体系结构



平台可解决各应用系统的集中授权，其平台结构包括三个层面，即数据层、服务层和目标应用层，分别说明如下：

数据层：通常为企业的权威数据源如 HR 系统以及竹云身份管理平台和竹云访问控制平台，通过连接器提供用户信息至平台，主要为业务系统实现授权管理。

服务层：平台的核心层面，是用户授权的中央枢纽，包括授权服务和集成服务。

目标应用层：指各应用系统，如财务系统、OA 系统、邮件系统等，平台可根据应用系统提供集中的业务授权。

2.4.2 兼容性

平台适应多类型基础资源，可部署于物理机也可部署于虚拟机，具体运行环境适配性如下：

- 操作系统：支持 Windows，Linux、AIX 等。
- 数据库：支持 Maria DB、Oracle 、MySQL、SQL Server、DB2 等主流数据库。
- JDK 版本：支持 Java 1.7 以上版本。
- 中间件：支持 Tomcat、Jboss、Weblogic、WebSphere 等。

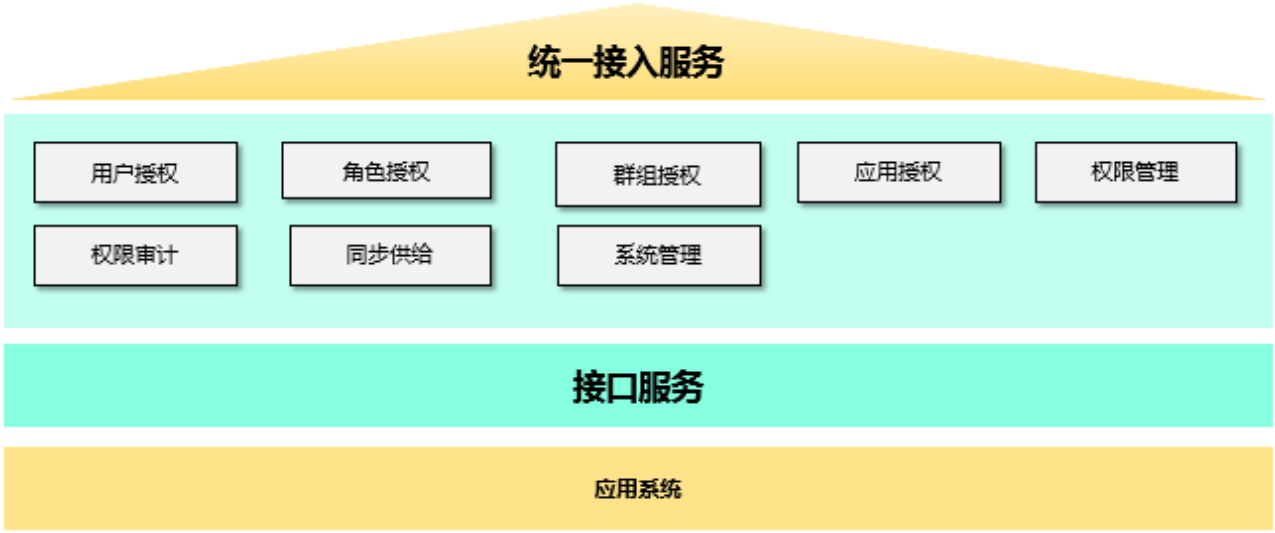
- 浏览器：支持 IE10 以上版本及 Chrome 等浏览器。

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

2.5 主要功能介绍

平台主要包括用户授权、角色授权、群组授权、应用授权、权限管理、权限审计、同步供给和系统管理等模块。



- 用户授权：提供基于用户个人的权限分配和设置。
- 角色授权：提供基于业务角色的权限分配和设置。
- 群组授权：提供基于群组的权限分配和设置。
- 应用授权：提供基于应用业务功能、菜单、按钮、页面等细粒度权限分配和设置。
- 授权管理：提供全局权限的定义、设置和策略等管理。
- 权限审计：提供权限的查看、审阅、合规检查及权限互斥等功能。
- 同步供给：提供下游应用系统权限信息的自动供给和自动回收。
- 系统管理：提供权限导入、流程集成、安全设置等系统管理功能。

2.5.1 用户授权

平台提供基于用户个人的权限分配和设置，包括用户权限分配、临时授权、

委托授权及权限回收等。

➢ 用户权限分配： 平台管理员针对用户提供权限的分配操作。

➢ 临时授权：管理员可以针对临时人员在特定的时间段内给该人员的账户授予相应权限。

➢ 委托授权：管理员将账户（委托人）拥有的全部/部分权限在特定的时间段委托给其它的账户（被委托人），并根据需要可以同时自动冻结委托人账户，且不违反现有的业务策略。

➢ 用户权限回收：用户离职、部门调动及临时权限可集中进行统一权限回收。

➢ 多账户授权：提供单用户多账户的支持，并支持主/从账户定义，允许一个用户的多个账户授予不同的权限。

2.5.2 2.5.2 角色授权

平台提供集中统一的业务角色授权功能，实现应用系统的业务角色统一进行创建、变更和分配。

➢ 角色创建：针对平台管理员或业务管理员提供业务角色的创建操作。

➢ 角色变更：针对平台管理员或业务管理员提供业务角色的变更操作。

➢ 角色启用：针对平台管理员或业务管理员提供角色启用功能。

➢ 角色禁用：针对平台管理员或业务管理员提供角色禁用功能。

➢ 角色授权：平台管理员或业务管理员针对用户提供角色分配和授权功能。

➢ 角色导入：支持角色信息导入功能，支持多种常用文件格式。

➢ 角色导出：支持角色信息导出功能，支持多种常用文件格式。

2.5.3 2.5.3 群组授权

平台提供集中统一的业务群组授权功能，实现应用系统的业务群组统一进行创建、变更和分配。

➢ 群组创建：针对平台管理员或业务管理员提供业务群组的创建操作。

➢ 群组变更：针对平台管理员或业务管理员提供业务群组的变更操作。

➢ 群组启用：针对平台管理员或业务管理员提供业务群组启用功能。

➢ 群组禁用：针对平台管理员或业务管理员提供业务群禁用功能。

➢ 群组删除：针对平台管理员或业务管理员提供业务群删除功能。

➢ 群组合并：支持不同业务群组的合并迁移功能。

➢ 群组挂靠：实现嵌套和动态群组的挂靠功能。

➢ 群组授权：平台管理员或业务管理员对用户或用户组提供业务群组的分配和授权。

➢ 群组导入：支持群组授权信息导入功能，支持多种常用文件格式。

➢ 群组导出：支持群组授权信息导出功能，支持多种常用文件格式。

2.5.4 应用授权

平台提供基于应用系统的业务细粒度授权，包含菜单、页面和按钮等级别，方便应用系统业务权限集中管理。

➢ 菜单授权：提供细化至应用系统菜单级别的授权，业务管理员可统一管理菜单权限。

➢ 功能授权：提供细化至应用系统功能模块级别的授权，业务管理员可统一管理业务功能权限。

➢ 按钮授权：提供细化至应用系统按钮级别的授权，业务管理员可统一管理按钮权限。

➢ 页面授权：提供细化至应用系统页面级别的授权，业务管理员可统一管理页面权限。

➢ 组合授权：提供应用系统各细粒度权限的组合授权，包括菜单、功能模块、页面等多种组合授权模式。

2.5.5 权限管理

➢ 权限定义： 平台管理员对全局权限进行定义和配置，包括具备的权限、权限规则和权限对象等。

➢ 权限模板设置： 支持权限模板的设置并作为模板可应用于各应用系统中作为通用权限使用。

➢ 权限策略： 基于用户属性进行权限策略的定义和管理，包括岗位权限的界定、部门权限的界定等。

➢ 权限继承：基于组织架构、群组实现下属部门、嵌套群组的权限继承，通过权限继承，下属部门和群组具备一级部门和一级群组的权限。

2.5.6 权限审计

平台提供集中统一的权限审计功能，包括权限的查看、审阅、合规检查及权

限互斥等功能。

- 权限查看：用户或业务管理员可查看个人、群组、部门等不同维度的权限列表。
- 权限审阅：平台管理员或业务管理员针对特定资源的权限进行分析和合规检查。
- 权限互斥： 针对具备不同业务权限的对象包括用户、群组、角色、岗位、组织机构等实现权限最小化分析和管理，实现权限的细化管控。
- 权限日志存储： 提供权限信息的日志集中存储，包括权限名称、容器、使用对象等。
- 权限日志输出： 针对第三方平台提供权限信息的供给和输出，基于接口的形式实现。

2.5.7 系统管理

平台提供权限导入，权限导出、权限流程对接等功能，方便平台管理员进行统一管理和维护。

- 权限导入：提供权限信息的集中和批量导入，支持多种常用文件格式。
- 权限导出：提供权限信息的集中和批量导出，支持多种常用文件格式。
- 权限流程对接：可实现与竹云身份管理平台的权限流程或第三方流程平台对接，实现权限申请流程的申请、审批。
- 安全管理：提供平台及应用系统的数据安全、接口安全、交互安全等管理方式和技术手段。

3 产品部署

BCM 产品需要与 BIM 集成部署（包含自服务平台、业务控制台）：满足大部分身份管理、认证与访问控制需求和场景，提供企业内部权限管理的解决方案。

4 产品集成

平台作为权限主数据平台，同时也作为上游数据源对应用系统提供权限信息的同步供给服务。

- 规则定义：平台提供配置化规则，包括权限创建、变更、合并、分配等各种场景的匹配关联，实现业务规则的预先定义。
- 属性映射：提供应用系统同步信息的属性关联、分配、合并、扩展等映射管理和配置。
- 供给策略：提供应用系统同步供给的策略，包括同步供给内容、同步供给权限控制、同步供给对象控制、同步供给频率、同步供给异常处理等。
- 任务设置：提供应用系统同步供给的任务设置，包括同步供给时间、同步供给设置等。
- 自定义供应：提供扩展化的同步供给设置，包括同步供给内容定义、过程处理、事件触发等自定义设置。
- 接口服务：提供多类型接口服务，包括 Connector、WebService、协议、RESTful 等多种方式，并支持 Pull 和 Push 连接集成。