深圳竹云科技有限公司

互联网用户管理产品白皮书

Bamboocloud Internet Users Identity Management Products

White Paper

编号：BBC-WP-IUIM-2018001

深圳竹云科技有限公司

2018 年 4 月

目录

1 背景

当前随着互联网建设的发展，越来越多的企业已经建设了基于消费者的信息化服务，这些服务在开始发展期间，为了满足业务快速上线，用户层面往往没有打通，形成孤岛，在管理和运营面向互联网用户的应用时将会面临以下问题：

- **IT 建设成本高：**各应用建立各自的账号管理体系，包括网站、桌面应用、移动 APP 等各类应用，需要重复投入成本且规范不统一；
- **跨渠道管理难：**互联网用户来源渠道多样，渠道管理成本高，无法盘活各渠道存量数据，难以进行有效的业务整合和创新；
- **用户体验不佳：**消费者用户需要记忆多套账号密码，维护多次个人信息，用户满意度不高，公司品牌力不统一；
- **存在安全风险：**用户数据分散存储，各应用安全标准与能力有差异，无法提供统一的安全保障能力，存在数据泄露风险；

故各企业急需一套互联网用户的管理系统，可以协助企业管理各渠道的用户，形成一套标准的用户管理体系，对外提供统一的身份管理服务服务。

2 产品介绍

2.1 概念和术语

IUIM：竹云互联网用户统一身份管理系统（Bamboocloud Internet Users' Identity Managent），为企业提供互联网用户统一身份管理服务，并为与其对接的应用系统供给身份数据。

BAM：竹云统一访问控制管理系统（Bamboocloud Access Managent），为企业用户提供统一认证服务，接入应用的登录访问由此系统进行统一控制。

自服务平台：竹云互联网用户自服务平台，为企业互联网用户提供注册，个人信息维护等自助服务。

2.2 产品描述

竹云互联网用户身份管理平台（以下简称平台）为企业提供互联网用户管理服务，旨在建立一套统一数据规范、统一安全标准、统一接入规范的互联网用户身份管理平台，并

与竹云其他安全产品集成为企业提供一套完整的互联网用户统一身份安全服务平台。

平台充分考虑互联网用户业务场景，建立统一的互联网用户身份规范，包括：

- **统一规范：**为企业互联网用户的身份数据进行统一规范，包括账号规范、密码规范、内容规范等，确保用户数据质量；
- **身份集中存储：**将企业来自各种渠道、各种类型的互联网用户身份数据进行统一存储与安全保障；
- **全生命周期管理：**提供互联网用户在企业中全生命周期管理，包括注册、信息维护、启用/禁用、合并、权限变更、回收归档等；
- **身份服务提供：**为企业各类互联网用户应用提供权威、可靠的身份数据和服务，提供各类身份服务接口与应用系统进行对接；

2.3 特点和优势

平台从功能上和架构上根据互联网用户管理特点进行设计，满足互联网用户管理多方面的要求，帮助企业快速建立一套统一的互联网用户身份管理体系：

- **海量数据存储：**考虑互联网用户的规模，平台从架构上支持亿级数据存储，并能够根据需要进行横向扩展；
- **高并发响应：**平台支持高并发访问快速响应，特别是对于用户注册、身份认证、身份查询服务进行优化，并支持可扩展能力；
- **用户全生命周期管理：**提供互联网用户从录入到注销的全生命周期统一管理。
- **标准化接口：**提供完整的身份服务 REST API 接口，可轻松进行业务流程再造，支持供标准化的集成场景。
- **可配置化管理：**提供灵活的自定义配置，轻松配置，运维简单
- **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。

2.4 系统架构

2.4.1 整体架构

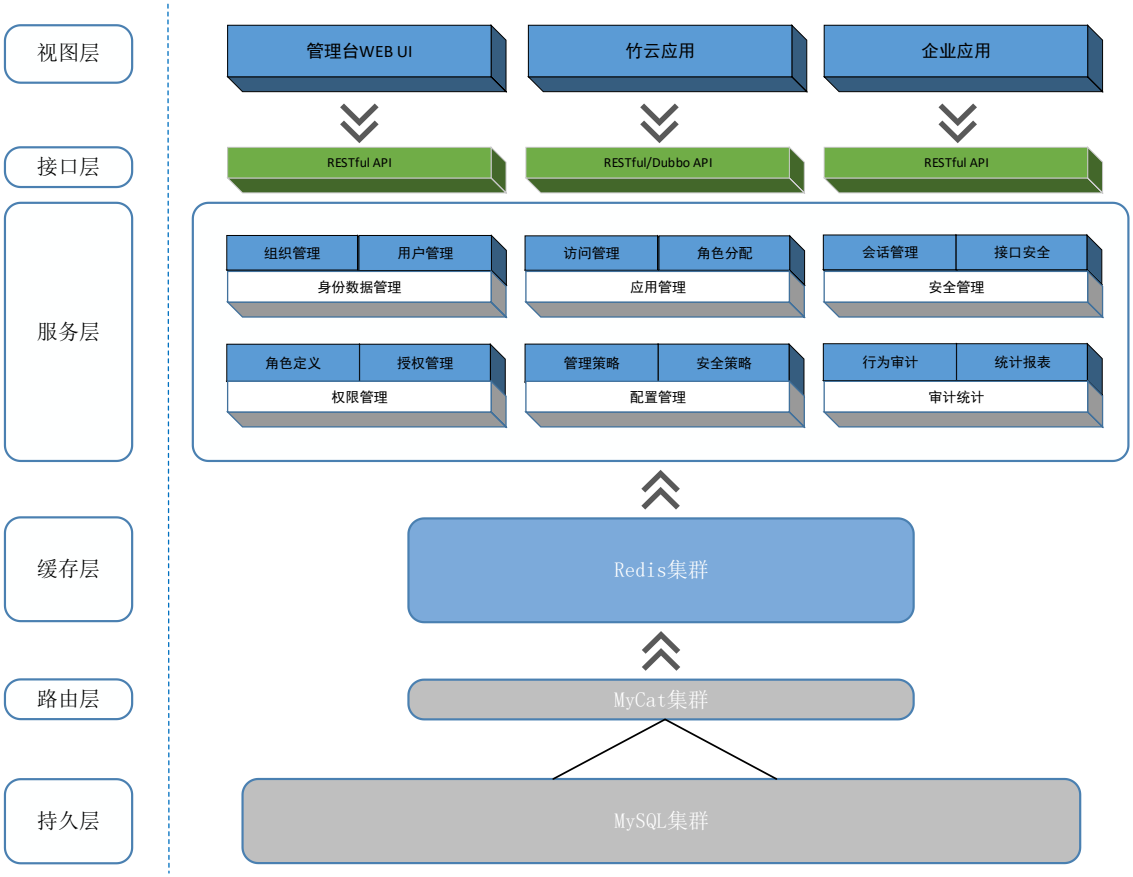

图 1 整体架构

平台分为视图层、接口层、服务层、缓存层、路由层和持久层；

- **视图层：**平台提供面向管理员使用的管理台界面；
- **接口层：**对于管理台界面，采用前后端分离模式，通过接口层连接视图层和服务层，同时对竹云身份管理系列应用以及企业身份消费应用提供各类接口提供身份服务；
- **服务层：**对外提供数据、操作等各类服务，完成系统各类业务功能；
- **缓存层：**使用 Redis 告诉缓存集群，提供热点数据存储与快速查询服务；
- **路由层：**使用 Mycat 作为持久层分片存储的路由与负载，提供请求分发与寻址能力；
- **持久层：**使用 MySQL 集群对业务数据进行分片存储，提供可扩展的海量数据存储服务；

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，具体兼容能力如下所示：

- **操作系统**：Windows/Linux/AIX 等；
- **数据库**：MySQL5.5 以上、MariaDB10 以上；
- **JDK 版本**：1.8 以上；
- **后端服务器**：Tomcat/Weblogic/WebSphere 等；
- **前端服务器**：Nginx/Apache/Tomcat 等；
- **浏览器**：支持 IE10 以上、Firefox、Chrome 等；

2.4.3 运行环境

用途	硬件（推荐配置）
管理台	CPU:8C; 内存:16G; Disk:100GB
缓存	CPU:16C; 内存:32G; Disk:100GB （按数据量扩展）
Mycat	CPU:16C; 内存:32G; Disk:100GB （按需扩展）
数据库	CPU:16C; 内存:32G; Disk:100GB （按需扩展）

2.5 主要功能介绍

平台主要包含身份数据管理、应用管理、身份供给服务、权限管理、配置管理和审计统计几大模块功能：

图 2 主要功能示意图

2.5.1 身份数据管理

平台提供统一身份管理服务，为企业提供互联网用户身份统一存储，并提供一套面向管理员的界面供其进行身份数据维护：

- **组织管理：**支持组织分类管理，可自定义不同的组织类型，支持组织树状化展示与维护，提供新建、修改、启用、禁用、移动、删除等功能；
- **用户管理：**支持用户分类管理，可标识用户的来源渠道，同时支持用户挂靠在指定组织机构下，提供用户新建、修改、启用、禁用、移动、锁定/解锁、重置密码、合并、删除等功能；

2.5.2 应用管理

平台作为互联网用户统一身份仓库，为各类互联网应用提供身份服务，对于消费身份的应用需要在平台进行注册，并基于此进行用户访问授权、用户应用角色授权等进行统一管理，作为统一认证和应用内部权限消化的授权数据来源：

- **应用管理：**提供应用注册、应用代号分配、信息维护、启用、禁用、删除等功能；
- **应用访问授权：**可对用户进行应用访问授权，该授权可与竹云 BAM 产品集成，控制用户访问各应用系统的权限；
- **应用角色授权：**通过将应用系统的角色导入平台，可对用户分配应用系统中的角色，应用获取用户分配的角色可在用户访问应用内部时进行具体的权限控制；

2.5.3 身份供给服务

平台作为互联网用户的统一身份存储仓库，为企业互联网应用提供身份服务，企业应用可通过平台提供的接口获取用户身份信息开展相关业务：

- **身份服务接口：**平台为各类应用提供 RESTful/Dubbo 形式的 API 接口，提供统一的接口规范、统一的鉴权/数据签名约束、统一的数据加密与脱敏标准；
- **企业应用接入：**企业应用通过 RESTful 接口进行接入，按照接口标准规范维护身份数据和获取身份数据；
- **竹云应用接入：**竹云身份管理系列应用通过 RESTful/Dubbo 接口进行接入，按照接口标准规范维护和获取身份数据，接入后形成一套完整互联网用户统一身份管理与安全控制的平台；

2.5.4 权限管理

平台管理界面提供权限管理能力，可灵活分配管理员使用此管理台的功能，同时支持按组织分级分权管理能力，管理员可指定可维护的数据范围：

- **角色/权限定义：**可自定义管理台系统角色，可为不同角色关联不同模块细到菜单按钮的访问权限；
- **角色授权：**通过授予管理员不同的角色，使管理员拥有该角色的权限，访问管理台对应的模块和进行菜单操作；
- **分级分权：**可进行针对组织的分级分权，对用指定组织进行管理，并通过关联角色使其对指定组织拥有对应角色的权限，管理员只能访问或维护其有权限的组织和用户；

2.5.5 配置管理

平台提供针对互联网用户的管理策略配置以及平台本身的使用策略配置，以满足不同企业在管理和运维上的不同需求：

- **组织类型管理：**提供组织类型自定义，以支持组织分类管理，根据类型可定义组织挂靠策略，如指定该类型的组织允许挂靠哪些类型的用户等；
- **用户类型管理：**提供用户类型自定义，以支持用户分类管理，根据类型可定义用户管理策略，如密码策略、锁定策略等；
- **组织属性管理：**提供按类型自定义组织属性管理，企业可按需维护其业务需求的组织属性，同时可以指定属性的使用策略，如必须、唯一、指定格式等；
- **用户属性管理：**提供按类型自定义用户属性管理，企业可按需维护其业务需求的

用户属性，同时可以指定属性的使用策略，如必须、唯一、指定格式等；

- **渠道管理：**提供自定义渠道能力，渠道可用于标识用户的来源，可通过不同渠道来源的用户定制不同的业务；

2.5.6 审计统计

平台提供管理员和应用通过接口在平台上进行的行为审计，同时提供基于互联网用户数据的常用统计报表：

- **行为审计：**通过监控管理员和接口在平台上进行的操作行为，将其记录至数据库，记录内容包括操作者、操作时间、操作类型、操作目标、操作 IP、操作结果等信息，并提供界面便捷的查询服务；
- **身份数据统计：**提供各类组织/用户数量统计，时间段内注册、变更用户数量统计等报表，协助管理员对总体身份数据进行分析；

3 产品部署

平台部署架构如下图所示：

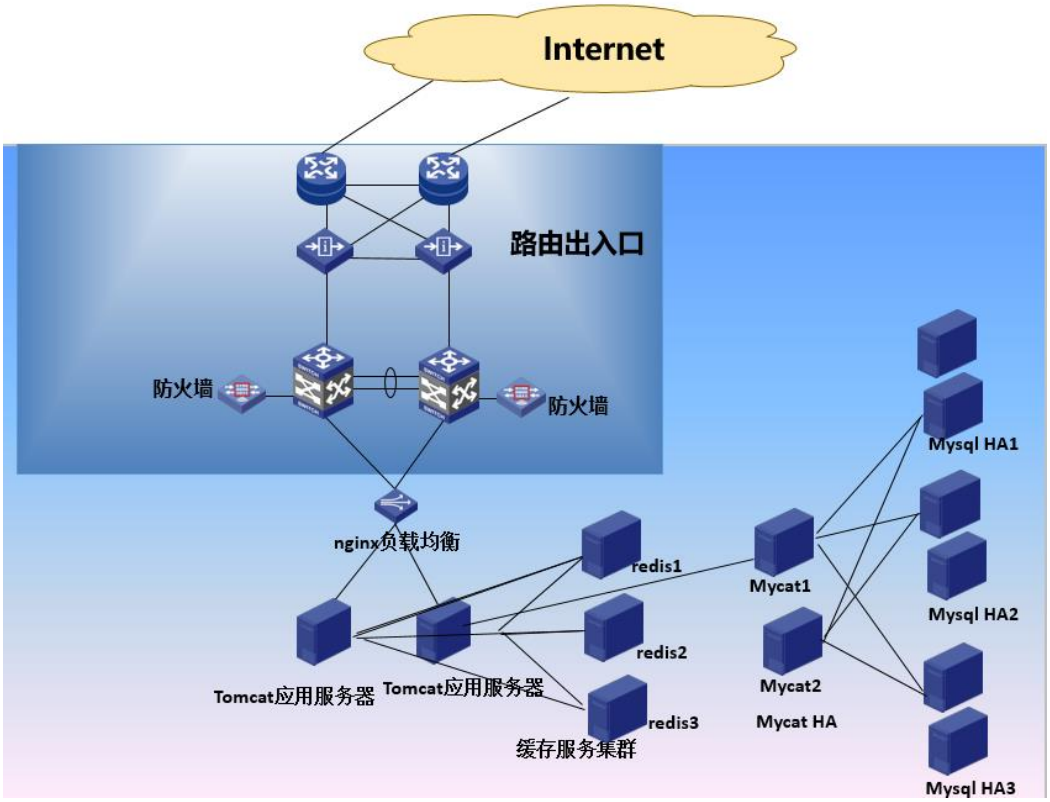

图 3 平台部署架构示意图

- 平台需要开放到外网访问时，需要进行相应的反向代理和防火墙保护。
- 管理台前端服务：管理台前端服务可使用 Nginx/Apache/Tomcat 等进行部署，推荐使用 Nginx，Nginx 可通过 keepalived 配置成集群；
- 管理后端服务：管理台后端服务可使用 Tomcat/Weblogic 等进行部署，推荐 Tomcat 部署，可将 Tomcat 配置成集群，且前端 Nginx 可配置负载均衡连接后端服务；
- 缓存：缓存使用 Redis，配置成集群模式；
- 数据路由：数据路由使用 Mycat，可配置为集群，后端可接数据库集群，进行数据请求分发和寻址；
- 数据库：数据库可使用 MySQL /MariaDB，推荐使用 MySQL，MySQL 配置为集群模式；

4 产品集成

平台可以与竹云 IAM 系列产品进行集成，集成架构如下图所示：

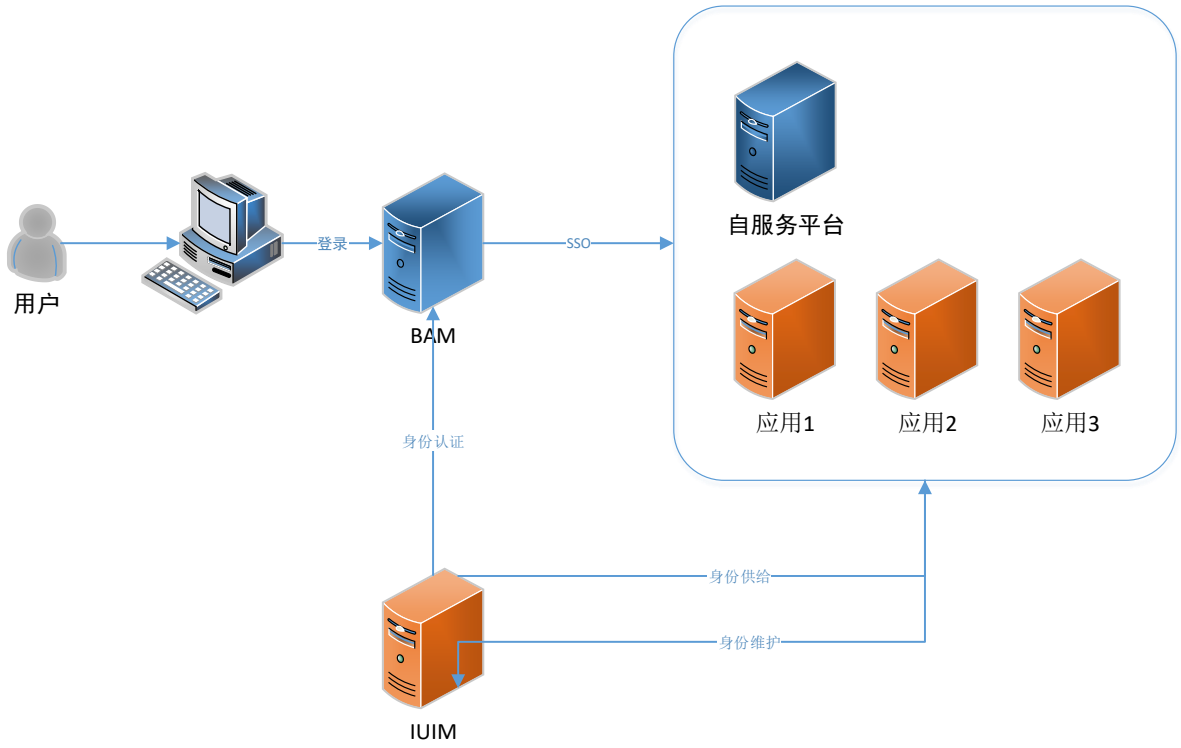

图 4 集成机构示意图

- **集成 BAM：**BAM 作为统一认证系统，在用户登录自服务或企业应用时需要统一通过 BAM 进行认证，认证通过后，用户再访问其它应用时无需再次输入账号密码，实现单点登录，被单点登录的应用需要到 BAM 进行令牌校验，以确保身份合法；

- **集成自服务平台：**自服务平台面向互联网用户使用，用户可通过自服务平台进行注册、个人信息维护、密码管理等操作，自服务通过接口与 IUIM 进行集成，将用户维护的身份信息提交到 IUIM 身份仓库，同时自服务展示用户个人数据时也通过接口从 IUIM 中获取；
- **集成企业应用：**企业应用可通过接口从 IUIM 中获取所需用户身份数据，也可以通过接口将维护的用户身份信息提交到 IUIM。