深圳竹云科技有限公司

竹云访问控制平台白皮书

BambooCloud Access Manager Products White Paper

编号：BBC-WP-BAM-2018001

深圳竹云科技有限公司

2018 年 4 月

目录

1 背景 3
2 产品介绍 3
2.1 概念和术语 3
2.2 产品描述 3
2.3 优势和特点 4
2.3.1 产品优势 4
2.3.2 产品特点 4
2.4 系统架构 5
2.4.1 系统架构 5
2.4.2 兼容性 6
2.5 主要功能介绍 6
2.5.1 访问管理 7
2.5.2 认证管理 7
2.5.3 单点登录 8
2.5.4 认证集成模式 8
2.5.5 系统管理 9
3 产品部署 9
4 产品集成 10

1 背景

随着企业的发展，业务系统的数量在不断的增加，老的系统却不能轻易的替换，这会带来很多的开销，其一是管理上的开销，需要维护的系统越来越多，很多系统的数据是相互冗余和重复的，数据的不一致性会给管理工作带来很大的压力，业务和业务之间的相关性也越来越大，例如公司的计费系统和财务系统，财务系统和人事系统之间都不可避免的有着密切的关系。为了降低管理的消耗，最大限度的重用已有投资的系统，很多企业都在进行着企业应用集成（EAI）。企业应用集成可以在不同层面上进行，例如在数据存储层面上的“数据大集中”，在传输层面上的“通用数据交换平台”，在应用层面上的“业务流程整合”和用户界面上的“通用企业门户”等等，除此之外，还有一个层面上的集成变得越来越重要，那就是“身份认证”的整合，也就是“单点登录”。通常来说，每个单独的系统都会有自己的安全体系和身份认证系统，整合以前，进入每个系统都需要进行登录，这样不仅给管理上带来了很大的困难，在安全方面也埋下了重大的隐患，具体存在的问题与风险如下：

- **高危安全风险**：简单密码、弱密码及单一认证访问方式，导致业务系统很容易被攻击和获取访问权限 ；
- **数据泄露风险**：缺乏强认证及可信身份认证，企业敏感及机密数据容易被盗取和篡改，导致数据泄露和经营风险增加；
- **用户体验差**：用户需记忆众多不同账号和密码，重复进行应用认证和访问，用户满意度不高、体验差；
- **IT 建设成本高**：各应用系统的认证体系独立建设，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

BAM：竹云访问控制平台，即 BambooCloud Access Manager，以下简称“平台”。

2.2 产品描述

竹云访问控制平台是深圳竹云科技有限公司多年信息安全技术和行业经验积累所形

成的新一代身份认证与资源整合产品，全部功能自主研发，具有完全的自主知识产权。

竹云访问控制平台实现应用帐号的统一管理、统一认证、单点登录和权限管理，以企业用户、B/S 系统为整合目标，实现统一认证、统一授权和访问控制。集成强身份认证、会话审计、集中管理功能的一体化。可对企业内部用户应用访问、管理员维护等各类操作进行访问控制。本平台提供了用户名口令、手机 OTP、数字证书、短信、动态令牌等多种认证方式，支持包括 SAML、OAuth 等众多安全认证协议，以实现联邦认证。统一认证的使用大大减少系统用户在身份认证环节的时间成本，简化登录的过程。统一的身份管理系统，统一的用户权限管理，统一的安全策略，使得身份认证的过程更加标准化，安全性方面更加靠。集中式的身份和权限管理，使得用户身份维护更加同步，减少用户认证系统的维护成本。

2.3 优势和特点

2.3.1 产品优势

竹云访问控制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，其产品优势主要体现在以下方面：

- 健全的应用权限访问控制策略配置，可减少信息泄露和加强隐私保护；
- 统一访问管理建设，可提升整体信息化安全水平；
- 统一访问管理建设，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。

2.3.2 产品特点

- **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，并提供多种认证方式选择，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接口，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。

2.4 系统架构

2.4.1 系统架构

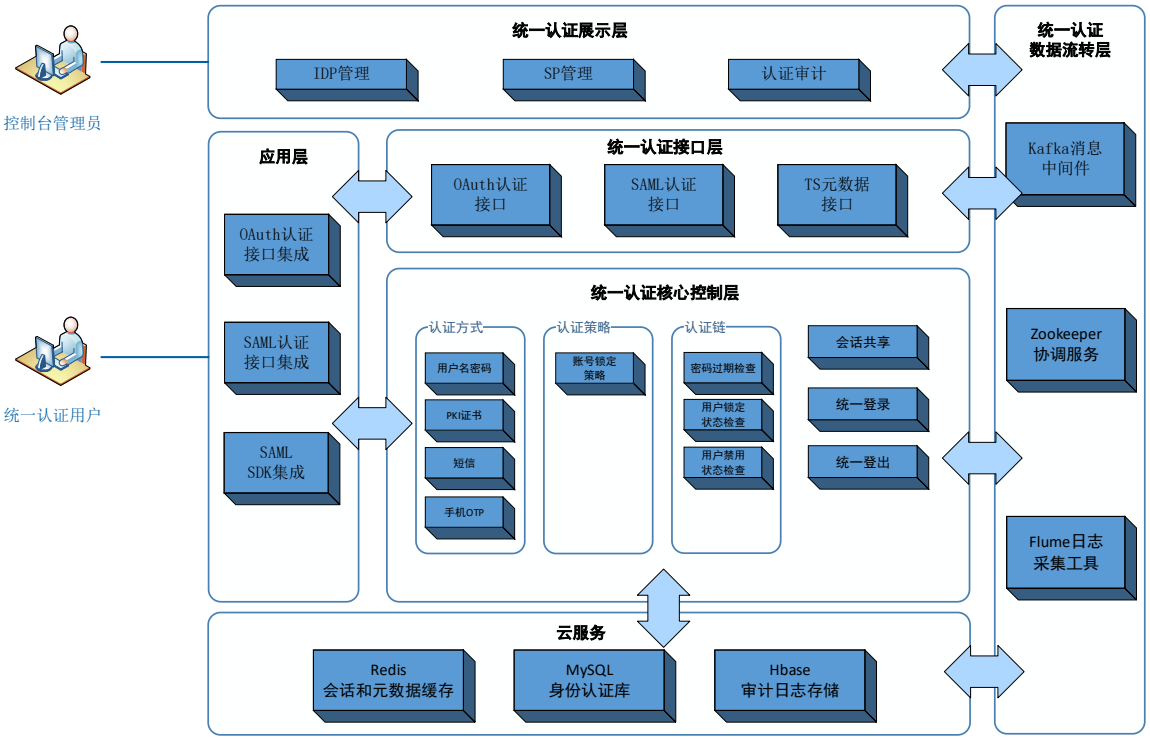

图 1 系统架构示意图

竹云访问控制平台系统的主要技术说明：

- 支持主流的 MySQL 数据库；
- 支持国际化（多语言）；
- 安全身份认证服务。提供口令认证、证书认证、动态令牌认证、指纹认证、短信认证等多种认证方式；
- 应用系统的安全单点登录。通过统一身份认证平台认证并授权的用户，可在统一身份认证平台中通过单点登录的方式访问应用；
- 认证策略配置。可以配置用户的认证策略，包括认证请求 IP 的黑白名单管理，认证的负载均衡策略，基于地理位置的认证中心选择，心跳检测等技术，支持登录认证的高可用，高并发特性；
- 访问审计。记录系统范围内的安全和系统审计信息，有效地分析整个系统的日常操作与安全事件数据；
- 支持用户账号的批量导入、导出、修改、绑定等操作；

- 集成方式多样化，支持 SAML 2.0 和 OAuth2.0 协议版本；简化认证组件，便于实施部署；支持多种接入方式，支持 SAML 和 OAuth 的 SDK、RESTful 认证集成；
- 支持统一身份认证系统各服务的运行状态进行监控。用户和账号管理统计和认证服务统计。其中服务运行状态监控包括数据同步服务、数据库服务、LDAP 服务、身份管理服务、数据分发服务和认证服务等的统一监控。

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，具体运行环境适配兼容性如下：

- **操作系统：**支持 Windows、Linux。
- **数据库：**支持 Oracle、MySQL。
- **JDK 版本：**支持 Java 1.7 以上版本。
- **中间件：**支持 Tomcat、Weblogic。
- **浏览器：**支持 IE10 以上版本、火狐及谷歌等浏览器。

2.5 主要功能介绍

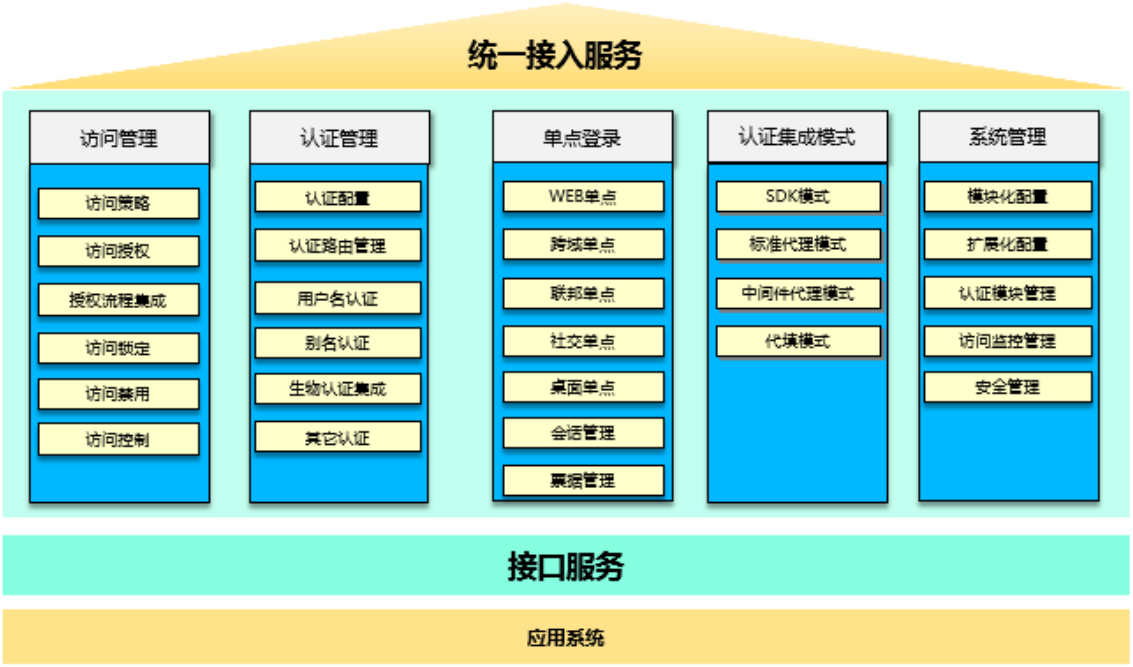

图 2 主要功能介绍

平台主要包括访问管理、认证管理、单点登录、认证集成模式和系统管理等模块。

- **访问管理：**提供统一访问策略及多种访问控制功能，包括访问准入、访问锁定、

访问禁用及来源过滤访问等；

- **认证管理：**提供多种安全认证包括静态口令、动态密码、强认证、生物认证支持等多种方式；
- **单点登录：**提供多种单点登录包括 B/S 单点、社交单点、跨域单点、联邦认证及桌面单点等多种方式；
- **认证集成模式：**提供各种异构应用的认证集成包括标准产品集成、自开发应用集成、无法改造应用集成接入等多种模式；
- **系统管理：**提供可视化配置管理功能包括内置认证模块配置、扩展配置以及安全管理和访问监控等功能。

2.5.1 访问管理

平台提供集中统一访问管理功能，针对应用系统和用户进行统一访问方式、访问准入、访问控制等多种管理方式。

- **访问策略：**平台管理员通过平台制定和发布应用访问策略，包括访问对象、访问权限、访问规则匹配及访问有效期限等。
- **访问授权：**针对应用访问，通过对用户进行准入授权，实现应用的大门级访问授权和使用。
- **授权流程集成：**结合竹云 BIM（身份管理产品）的流程审批功能模块，实现用户自助授权申请、审批功能。
- **访问锁定：**用户进行认证的次数超过额定限制，平台将自动进行用户访问锁定，其额定次数可通过访问策略进行设置。
- **访问禁用：**用户进行非法认证或恶意攻击时，平台将自动进行访问禁用，其禁用期限可实现临时或永久等多种设定。
- **访问控制：**提供基于 IP、MAC 地址、用户名、访问时间段、主机名等多种访问控制方式。

2.5.2 认证管理

平台提供集中统一的认证管理功能，帮助企业实现可信身份认证，提升信息安全，降低经营风险。

- **认证配置：**提供认证方式、认证策略、认证频率等可视化配置功能。
- **认证路由管理：**针对跨区域业务系统认证，通过认证路由寻址和校验，实现快速

的区域化本地认证。

- **用户名认证：**支持常用用户名称、邮件地址、手机号码、员工工号等属性、署名认证方式。
- **别名认证：**支持用户名主认证方式下，采用别名认证，实现多种不同的认证登录。
- **生物认证集成：**平台提供安全认证生态圈，提供各种生物认证方式接入包括人脸、指纹、指静脉、声纹和虹膜识别等。
- **其它认证：**提供其它认证方式接入，包括动态口令、CA 凭证、IC 卡等认证方式。

2.5.3 单点登录

平台提供各业务系统间的相互认证信任，实现用户访问应用时的直接访问使用。

- **WEB 单点：**针对 B/S 应用，基于浏览器 Cookie，实现应用间直接访问的单点功能。
- **跨域单点：**企业存在多个应用域的业务场景下，实现跨域信任和单点，方便应用处于不域名下的直接访问单点。
- **联邦单点：**企业存在并购企业或第三方合作机构，采取联邦单点，实现独立用户体系的信任和应用间的访问使用。
- **社交单点：**基于 QQ、微信、微博等第三方社交平台，可通过与平台进行单点集成，实现社交平台的访问认证和单点登录。
- **桌面单点：**基于 Window Activity Directory 客户端，通过与平台集成，实现桌面的前置集中访问和认证单点。
- **会话管理：**认证产生的 Cookie，其会话有效性和周期进行监控和设置，其中支持多个会话的分段保存和统一管理。
- **票据管理：**针对认证过程中的 Token 进行统一发布、继承、回收，实现票据的集中管理。

2.5.4 认证集成模式

平台提供一系列认证集成模式，涵盖各不同复杂异构应用，方便应用快速接入。

- **SDK 模式**:提供标准 SAML、OAuth、WS-Federation 等安全协议的 SDK 模式接入。
- **标准代理模式：**采用标准 Web 拦截模式，拦截所有到应用系统的请求，并查询用户是否具有访问权限。

- **中间件代理模式**：采用独立的应用服务器上部署，拦截相应的请求，并根据应用服务容器的 J2EE 标准安全框架进行相应信息返回。
- **代填模式**：针对无法改造的应用系统，采用以 FORM 表单方式提交进行登录访问，实现统一认证，且登录页面无 activeX 控件、无校验码。

2.5.5 系统管理

平台提供可视化配置，模块配置、系统监控等功能，方便平台管理员进行统一管理和维护。

- **模块化配置**：提供模块化架构配置，易于使用通用 API、Lib 库、UI，开发者可快速进行定制开发与交付。
- **扩展化配置**：提供扩展化框架配置，如添加自定义的认证模块、联邦认证插件、策略条件等。
- **认证模块管理**：内置 18 种认证模块，可定制添加新的认证模块，支持 OAuth2.0 等第三方账户登录认证。
- **访问监控管理**：支持 JMX、SNMP、Web 页面的监控，通过 HTTP 检查访问认证服务是否存活。
- **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

平台采用多种高性能组件，基于以下组件可满足互联网级别的处理能力需求：

- 高性能缓存数据库 redis，支持集群模式；
- 分布式数据库 hbase；
- 分布式应用程序协调服务 zookeeper；
- 底层数据库可选用 mysql、oracle；
- 中间件可选用 tomcat、weblogic；

平台采用组件方式进行部署，分为 IDP 组件、TS 组件，均可方便快捷的进行横向扩展。

4 产品集成

平台支持多种方式集成，包括协议集成、SDK 以及标准的接口方式：

- **协议模式**：平台支持标准的 SAML 和 OAuth 协议集成，可通过 SAML 或 OAuth 协议实现认证。
- **SDK 模式**：封装了基于平台的认证功能，可通过导入 SDK、配置拦截器的方式实现认证票据的验证，实现认证。
- **接口模式**：平台提供标准的 REST 接口，可通过自定义改造的方式实现认证，通过接口模式集成还可选择是否保留自己的登录页面。
- **代填模式**：平台提供在应用登录页面代填用户名和密码的方式实现认证和单点登录。
- **代理模式**：在 Web 服务器或应用服务器部署 Agent，拦截用户请求转发到平台，实现认证。