深圳竹云科技有限公司

竹云应用导航平台技术白皮书

Bamboocloud Identity Manager Products White Paper

编号：BBC-WP-APPHUB-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.....4
2.1 概念和术语.....4
2.2 产品描述.....5
2.3 特点和优势.....5
2.4 系统架构.....6
2.4.1 整体架构.....6
2.4.2 兼容性.....7
2.4.3 运行环境.....7
2.5 主要功能介绍.....7
2.5.1 登录.....7
2.5.2 应用导航.....7
2.5.3 自服务.....8
2.5.4 用户类型.....8
2.5.5 角色管理.....8
2.5.6 机构管理.....8
2.5.7 用户管理.....8
2.5.8 应用管理.....9
2.5.9 账号管理.....9
2.5.10 会话管理.....9
2.5.11 认证日志.....9
2.5.12 访问日志.....9
2.5.13 操作日志.....9
3 产品部署.....10
4 产品集成.....11
4.1 应用集成方式.....11
4.2 嵌入式应用导航.....13

1 背景

随着信息化建设步伐的加快，企业内应用系统越来越多，应用访问时普遍存在以下问题：

- 用户登录访问各个应用系统需要记忆和输入各应用系统访问地址、账号密码，造成用户体验差、工作效率低；
- 忘记密码需要通知管理员协助处理，增加管理员重复性工作；
- 对应用访问时多人一账号、一人多账号、账号权限委托等无法提供有效的管理和实现；
- 老应用在无法改造的情况下如何实现统一认证和单点登录；
- 无法为不同用户设置不同的可访问应用权限；
- 实施中没有一套标准的、可复用的、适用不同场景的应用访问、访问权限控制、应用集成选择规范；
- 缺乏集中的登录认证和应用访问日志，为审计、报表提供数据；
- 基于以上背景和问题，借鉴身份管理行业经验和国情，竹云自主研发了集中应用安全访问导航平台（简称 AppHub）。

2 产品介绍

2.1概念和术语

AppHub：竹云集中应用安全访问导航平台

BAM：竹云认证与访问控制平台

BIM：竹云身份管理平台，包含自服务平台、业务控制台产品

epass：竹云 e 账通平台

2.2 产品描述

AppHub 为用户提供统一的用户登录入口、统一的应用访问入口，实现应用导航、账号使用、访问控制、单点登录和集中审计，为用户登录、访问、自服务操作提供标准化解决方案，是身份管理、认证与访问控制在企业内部最终用户层面的最佳实践和产品化体现。

2.3 特点和优势

AppHub 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：

- 为企业内部最终用户提供唯一的、标准的应用访问入口和操作规范，提高用户体验和满意度；
- 方便扩展支持更多登录认证方式，提升认证安全；
- 用户无需关注和记忆应用 URL、应用账号密码，提升账号安全；
- 精确控制不同用户可访问的应用列表和应用访问级别，提升应用安全；
- 支持用户访问应用的账号选择，支持多人一账号、一人多账号、委托账号等复杂场景；
- 提供集中的登录认证和应用访问审计平台，满足合规化要求；
- 与现有门户系统可无缝集成，增强门户原有应用导航的功能和安全；

产品特点包括：

- 标准化操作：最终用户操作（应用访问、自服务等）标准化、应用集成标准化。
- 标准化集成：为 SDK、代填等方式集成提供统一的应用管理和集成标准，为嵌入式应用导航提供标准。
- 适应性强：满足各种应用，支持 C/S 应用的单点登录。
- 适合国情：满足普遍存在的一人多账号、多人一账号访问应用系统的单点登录和集中审计。
- 学习成本低：全图形化配置流程，不需要编写代码即可完成大部分的配置任务。
- 模板定制：支持基于模板的客户定制界面。

- 数据安全：关键数据加密传输和存储。
- 部署灵活：支持独立部署或与各产品集成部署，支持单机部署或集群部署。

2.4 系统架构

2.4.1 整体架构

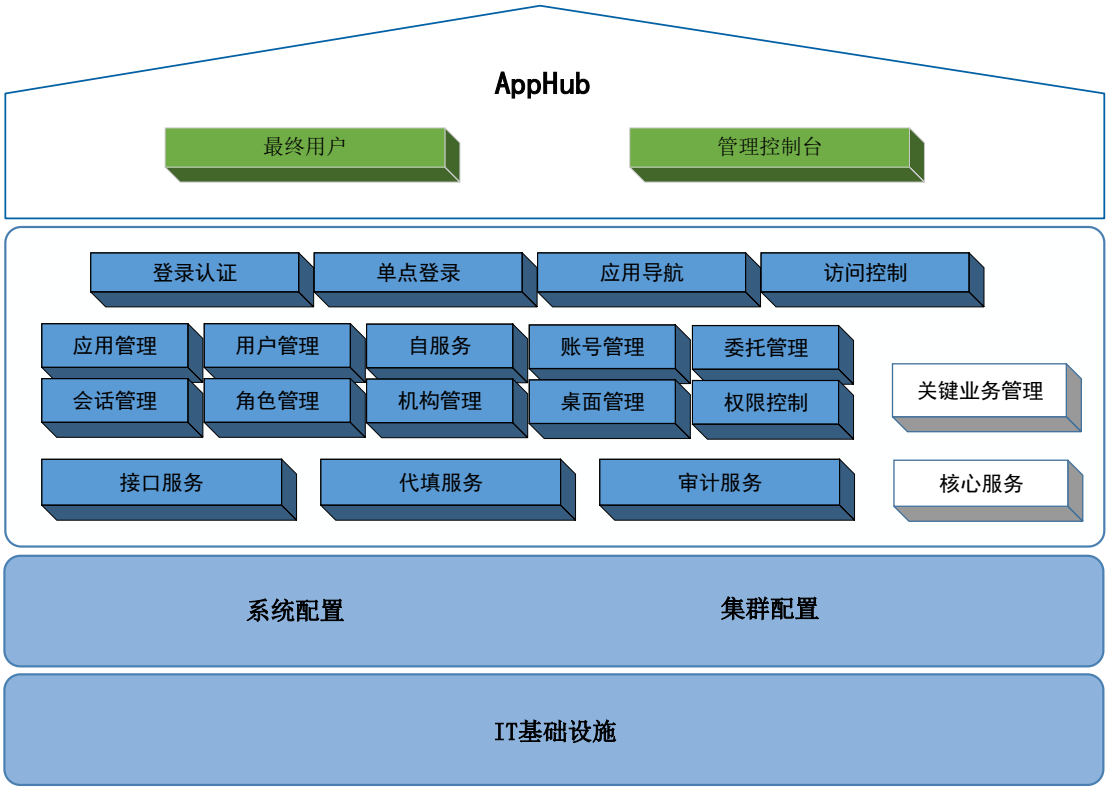

图 1 APPHUB 整体架构示意图

- 支持按不同维度（用户类型、机构、角色、用户、账号）为不同用户显示不同的可访问应用；
- 支持用户一人多账号、多人一账号访问应用；
- 为 SDK、代填等方式的应用集成提供标准方法和扩展实现；
- 提供用户资助修改密码、忘记密码、修改个人资料、代填账号自管理、账号权限委托等自服务功能；
- 提供基本的用户管理、机构管理、应用管理、账号管理、会话管理和系统配置管理等管理功能；
- 提供直观的、可查询和审计的认证日志、访问日志、系统日志，为报表统计提供数据基础；

- 支持独立部署或与身份管理（IM）、认证管理（AM）、epass 等产品集成部署；
- 方便定制样式、风格、界面，满足客户化定制要求。

2.4.2 兼容性

适应多类型基础资源环境，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 Oracle 、MySQL、DB2 等主流数据库
- **JDK 版本：**支持 Java 1.6 以上版本
- **中间件：**支持 tomcat、Jboss、Weblogic、WebSphere 等
- **浏览器：**支持 IE8 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

2.5.1 登录

根据集成部署方式，产品提供支持独立部署的用户名+静态密码登录、与 BAM 集成部署时的用户名+静态密码、OTP、二维码、双因素等登录认证方式。

支持失败次数锁定、同一用户会话控制、ip 地址变更短信验证等认证策略。

2.5.2 应用导航

根据不同的应用访问控制维度（用户类型、角色、机构、用户等）为不同用户显示不同的可访问应用列表，可根据用户爱好选择所有应用、个人收藏、最近访问等展示方式。

访问应用时可选择账号，支持多人一账号（一个账号多人共用、公共账号、系统账号）、一人多账号（一个人有多个应用系统账号权限），产品可以审计到究竟是谁使用了什么账号访问了应用。

支持以其它人委托的账号访问应用并记录委托账号访问情况。

除代填自维护账号密码，用户不需要关注和记忆应用的账号密码，既能大大降低了账号密码泄露风险，还能设置足够复杂的密码强度。

支持为应用设置补充认证以保护企业内部关键应用的安全。

2.5.3 自服务

产品内置基本的自服务功能，与 BIM 自服务平台集成部署时可提供更多复杂的自服务功能，例如应用账号权限申请等。

提供用户自己查看、维护个人基本信息。

支持用户自助修改密码，可检查密码是否满足复杂度策略，可强制用户修改密码及密码过期修改密码。

提供用户忘记密码时通过邮件、短信等重置或找回密码。

自管理账号密码的代填应用，用户可自助新增、修改、删除账号密码。

用户可自助将应用账号访问权限委托给其它用户，可设置委托期限，用户能撤销、删除委托，能查看委托账号访问情况。

2.5.4 用户类型

实现基于用户类型的应用访问控制，为不同类型的用户显示不同的可访问应用。

2.5.5 角色管理

实现基于角色的应用访问控制，为不同所属角色的用户显示不同的可访问应用。

2.5.6 机构管理

机构主要用于实现基于机构的应用访问控制，为不同所属机构的用户显示不同的可访问应用，同时机构也用于用户基于机构的管理和查看。

2.5.7 用户管理

此处用户是指企业内部的实体自然人，访问各个应用系统可以多人共用账号或虚拟账号，但本产品的用户要求是实名制用户，结合登录认证的强认证、生物认证等登录认证方式也能保证必须是实名制用户才能登录 AppHub。

与 BIM 集成时，用户由 BIM 同步。

2.5.8 应用管理

此处应用是指集成认证与访问控制的目标应用(注意与 BIM 身份管理集成的应用是存在差异的）。

支持为应用设置不同的访问控制（用户类型、角色、机构、用户等），最终实现让正确的人可看到并访问允许他有权限访问的应用。

2.5.9 账号管理

代填应用自管理的应用账号由用户自己在自服务中管理,其它情况下的应用账号可由管理员在管理控制台维护和查看。

与 BIM 集成时，应用账号由 BIM 同步。

2.5.10 会话管理

支持会话查看、查询及允许管理员踢人等操作。

2.5.11 认证日志

记录了什么用户、什么时间、使用什么 IP、什么认证方式登录了 AppHub，为审计和各种统计报表提供数据。

2.5.12 访问日志

记录了什么用户、什么时间、使用什么 IP、什么账号、访问了什么应用，为审计和各种统计报表提供数据。

2.5.13 操作日志

主要记录了管理控制台关键数据的新增、修改、删除操作。

3 产品部署

产品支持集中部署方式：

- 独立部署：简单需求和场景下，产品独立部署可提供登录认证（内置用户的用户名密码方式）、单点登录（主要采用代填方式）、应用导航以及控制台中的用户管理、机构管理、应用管理等产品的主要功能，但无法实现多认证方式和复杂的应用访问控制和自服务需求，也无法提供身份管理和用户、机构、账号等数据的同步功能。
- 与 BAM 集成部署（可选 epass）：需要实现统一认证与访问控制、单点登录、多认证方式并且没有身份管理需求的场景，但需考虑清楚认证源与 AppHub 本地用户的关系和同步问题（可借助产品用户自创建开关）。
- 与 BAM、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，提供企业内部基础安全全套解决方案，为最终用户。

4 产品集成

4.1 应用集成方式

此处的应用集成方式特指应用为实现统一认证和单点登录的集成（即通常所说的与 AM 的集成）。

- SDK 方式

SDK 方式是最常用的应用集成方式，通常针对可改造的应用，由 AppHub 配合 BAM 共同实现单点登录。

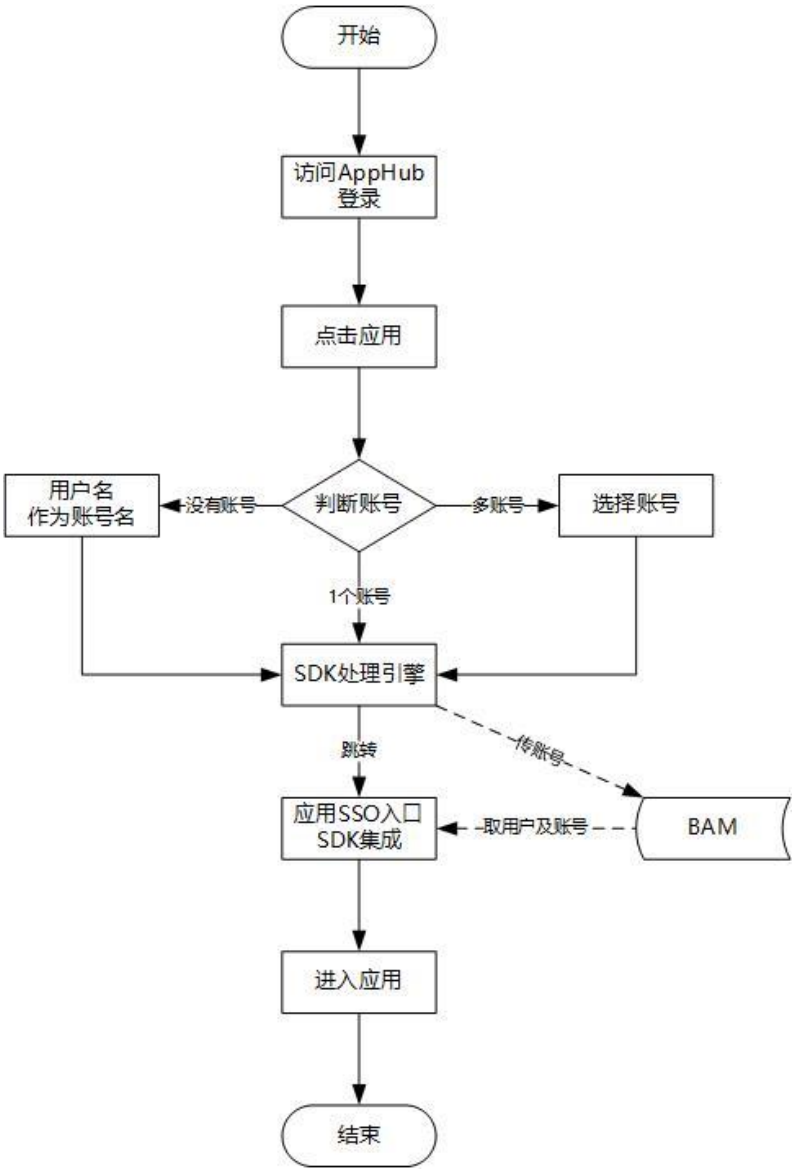

图 2 SDK 集成流程图

- 代填方式

代填方式通常针对无法改造的应用。

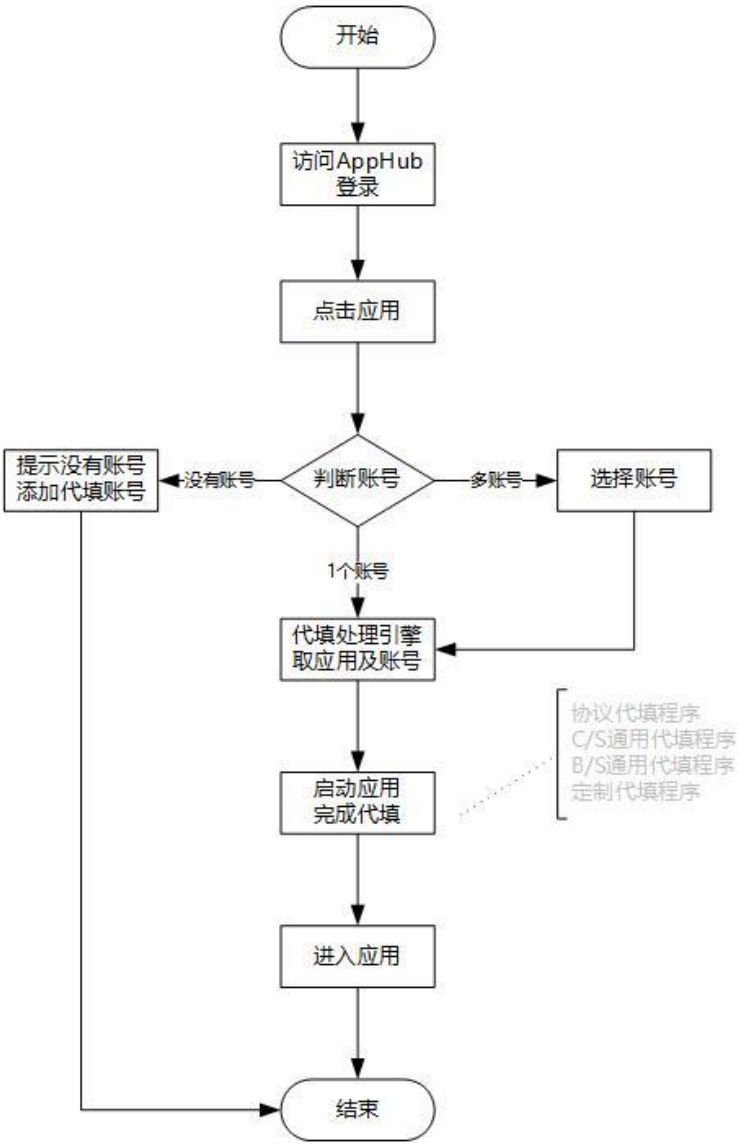

图 3 代填集成流程图

代填有三种：协议代填、客户端代填、浏览器插件代填，产品内置前两种，这几种代填的优缺点如下：

	协议代理方式代填	客户端程序方式代填	浏览器插件方式代填
优点	▪客户端不需要任何改造 ▪浏览器兼容性好，主流浏览器都支持 ▪代填速度快 ▪用户体验好	▪应用兼容性好，B/S应用都能代填 ▪支持C/S应用代填 ▪实施简单，很快就能上手配成功	▪应用兼容性好，B/S应用都能代填 ▪代填速度较快 ▪用户体验好 ▪实施较简单
缺点	▪应用兼容性差，受Cookie、Ajax等影响很多应用无法采用协议代填 ▪实施难度稍大，分析、写js、排查困难、技术要求高	▪客户端需要安装代填程序 ▪有些杀毒软件会报毒（如360） ▪用户体验稍差 ▪浏览器兼容性最差，只能借助IE完成B/S应用代填	▪浏览器端需要安装互联网插件 ▪浏览器兼容性稍差，没有IE插件
适用场景	▪应用数量少且相对简单 ▪登录页面采用技术老（最简单的form表单提交登录） ▪借助类似Apache反向代理可以解决部分Cookie、Ajax等无法直接代填的应用	▪代填应用多或复杂时都能处理 ▪有C/S应用 ▪协调且客户接受弊端（杀毒软件配置、统一IE浏览器）	▪用于Chrome、Firefox、Edge、360等浏览器不用IE时 ▪演示时效果会不错

图 4 不同代填方式比较

➢ Link 方式

Link 方式通常针对采用 SAML 标准协议集成无需改造的应用（注意与 SAML

协议 SDK 方式的区别）、或其它特殊应用（如仅跳转）。

4.2 嵌入式应用导航

若企业内部已有门户或 OA 系统，用户登录与访问应用的入口在门户或 OA 系统，并且不想改变用户已有使用习惯，此时门户或 OA 系统可采用深度改造方式集成，将 AppHub 的应用导航功能嵌入集成、将自服务或更多功能以链接形式集成。

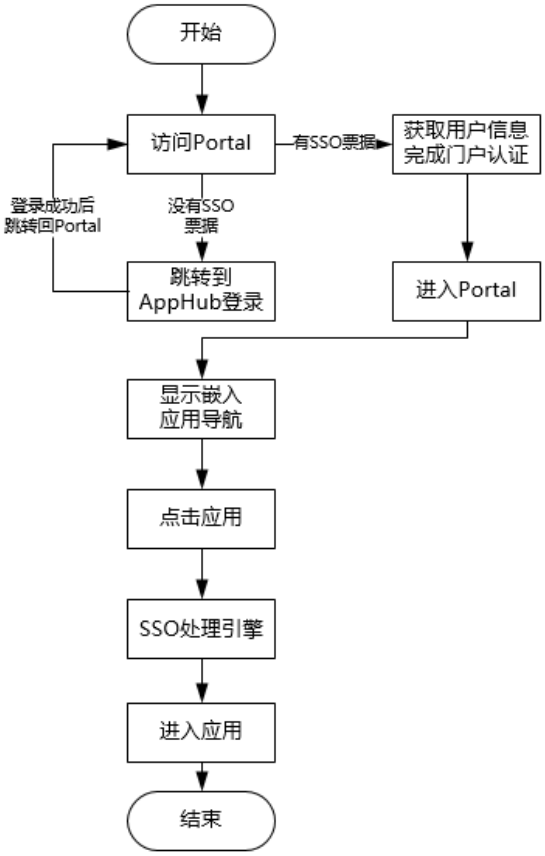

图 5 嵌入式应用导航流程图

➢ 采用这种方式的优点有：

- 不改变用户原有习惯；
- 对门户或 OA 改动很小；
- 无缝提供 AppHub 产品原生功能：多账号、桌面、访问控制、集中认证和访问审计、代填等；