深圳竹云科技有限公司

竹云安全通讯录产品白皮书

Bamboocloud Security Contacts Products White Paper

编号：BBC-WP-2018001

深圳竹云科技有限公司

2018 年 4 月

目录

1 背景

随着企业人数的增长，业务融合不断深入，企业员工与员工之间、内部人员与外部人员之间、企业服务人员与企业客户之间的交流与合作日益频繁，为企业提供一套供企业员工获取工作、生活中联系人的通讯录系统十分必要。

在当今移动、互联网时代，QQ、微信、电话簿等通讯产品和工具主要是以个人为中心，以此延展开来的通讯录功能不能满足工作上的需求，而且对于一个企业来说，不能从企业的角度将其员工及客户的通讯信息统一维护起来，也会给企业管理和业务开展带来不便。

由于企业员工及其客户的通讯信息属于企业的私密数据，在信息安全领域日益严峻的今天，如何在方便企业人员使用这些信息的同时也能最大限度的保证获取方式的安全性，降低敏感数据泄露的可能性，减少企业因此而产生损失。

综上所述，建立一套以统一、方便、安全为核心理念的通讯录产品势在必行，另外，竹云为企业提供统一身份管理解决方案，作为企业身份主数据平台，从身份数据中抽取通讯信息形成一套企业的通讯数据十分便捷，和竹云访问控制、权限管理等其它安全产品进行集成达到统一规范、安全管控的目标具有天然优势，因此，竹云安全通讯录产品应运而生。

2 产品介绍

2.1 概念和术语

BIM：竹云统一身份管理系统（Bamboocloud Identity Managent），为企业提供统一身份管理服务，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），为企业提供统一认证入口，接入应用的登录访问由此系统进行统一控制。

APPHUB：竹云统一应用访问入口系统，用户访问该系统后可看到有权访问的应用列表，通过该系统访问接入应用无需在进行登录认证。

2.2 产品描述

竹云安全通讯录为企业提供统一的内部员工、外部人员、客户等各类人员通讯信息的访问和管理服务，提供人员通讯信息的收集、维护和通讯信息的展示、查询功能，并提供灵活的权限控制满足企业对通讯录的安全管理需求。

安全通讯录分为管理台和通讯录主页两个子系统：

管理台：面向通讯录管理员使用，提供企业各类人员信息的录入，包括组织机构、企业群组、人员维护等功能；提供用户管理、权限定义与授权管理功能。

通讯录主页：面向企业普通用户使用，提供企业组织、企业人员、企业群组的访问查询服务，并能够根据用户自身的权限控制其可访问的组织、人员、群组信息。

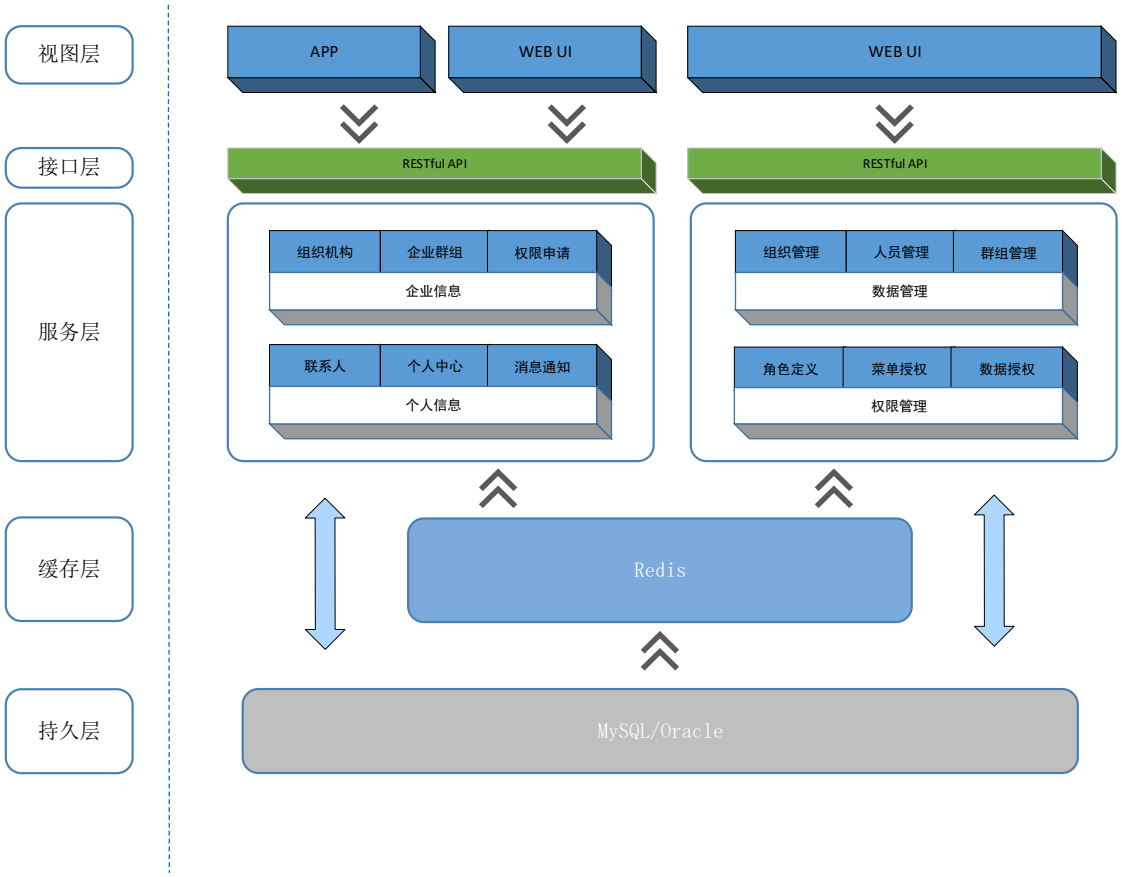
2.3 特点和优势

安全通讯录为企业提供全类型人员的通讯录管理和使用，除了拥有通讯录的基本功能之外，还以“安全”为重心，提供灵活可靠的通讯录访问方式和使用规范；安全通讯录拥有如下特点：

- 支持企业各类人员录入：包括内部员工、供应商、合作伙伴、客户等；
- 企业群组：企业可以按运营、项目、职能等方面建立对应群组，同时支持树状结构，便于管理与查找；
- 系统权限控制：可以对管理台所有模块与菜单进行细粒度的权限分配；
- 数据管理权限控制：在管理台对企业组织、企业群组进行分级分权管理，可指定不同管理员维护不同的组织与群组，可细到对组织、群组、人员的每个管理操作上；
- 通讯录按安全等级访问：企业可以按实际需要对组织、群组、人员、人员信息划分不同的安全等级，用户根据其所能访问的安全等级对组织、群组、人员、人员信息进行访问；
- 权限申请与审批：用户可对其无权访问的组织、群组、人员、人员进行访问权限申请，由指定审批人进行审批。
- 与竹云 IAM 产品集成：安全通讯录支持与竹云 IAM 系列产品进行集成，即可与 BIM 集成完成通讯录数据供应和自动化维护，纳入统一用户管理；与 BAM、E 账通、APPHUB 等集成，实现统一认证、多因子认证、单点登录等效果；

2.4 系统架构

2.4.1 整体架构



安全通讯录的通讯录和管理台两个子系统，通讯录子系统面向普通用户，管理台子系统面向管理员；两个子系统独立对外提供服务，通讯录子系统主要提供用户查看和使用企业组织、群组、人员通讯信息等，管理台提供管理员对企业数据进行维护以及系统本身的权限和配置维护；

视图层：通讯录子系统可通过移动 APP 和 WEB 进行视图展示，管理台子系统通过 WEB 进行视同展示；

接口层：采用前后端分离模式，通过接口层连接视图层和服务层，两个子系统均通过调用各自的 RESTful 接口使用后端服务；

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：两个子系统共用相同的缓存组件，进行会话、热点数据的存储和读取；

持久层：两个子系统共用相同的存储组件，对各类业务、配置数据进行持久化存储与共享；

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**：Oracle 11g 以上、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

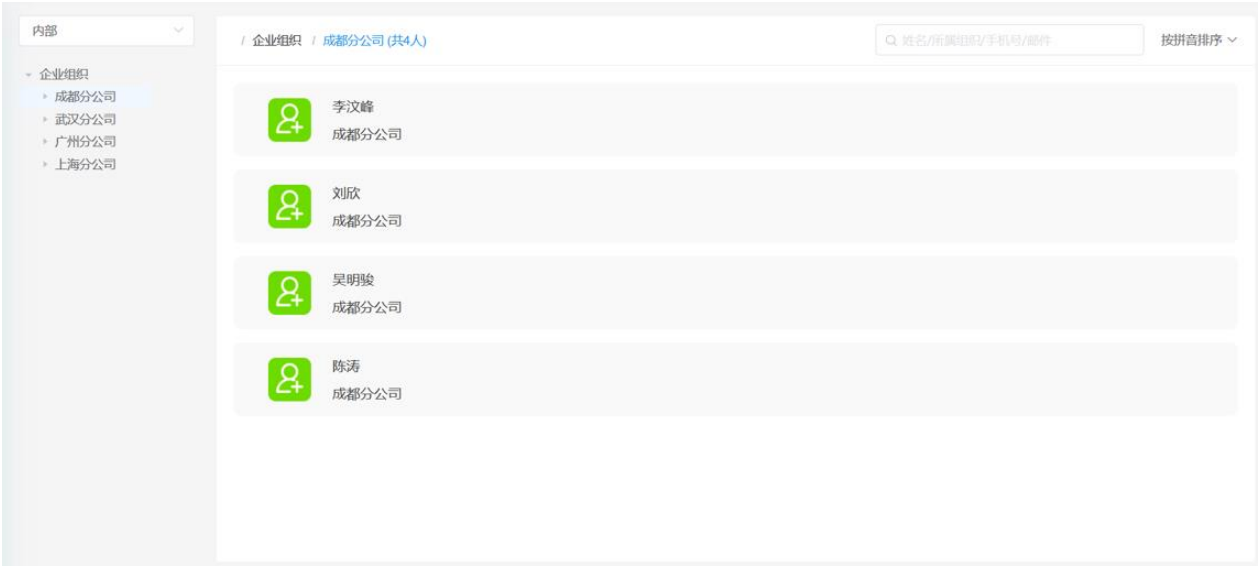
用途	硬件（推荐最低配置）
管理台	CPU:4C; 内存:8G; Disk:100GB
通讯录	CPU:4C; 内存:8G; Disk:100GB
缓存	CPU:4C; 内存:8G; Disk:100GB
数据库	CPU:4C; 内存:8G; Disk:100GB

2.5 主要功能介绍

通讯录子系统面向企业员工和指定外部人员，主要提供企业通讯录功能和个人信息维护功能；管理台子系统面向通讯录管理员，主要提供通讯录数据维护、权限管理、系统配置等功能；

2.5.1 通讯录-通讯录查询

提供多种条件查询企业人员，其中查询条件可在管理台中定义，同时支持多种排序方式展示人员列表，用户只能查询其有权限访问的人员：



2.5.2 通讯录-组织机构

按企业组织机构树的形式展示组织下的人员信息，支持内部、外部等多种类型组织树满足企业按不同类型组织挂靠不同类型人员的需求，用户只能看到其有权限查看的组织。

2.5.3 通讯录-企业群组

用户可看到企业自定义的各类企业群组，企业群组以树形展示，用户只能查看其有权限查看的群组，只能操作其有权限操作的群组。

2.5.4 通讯录-权限申请

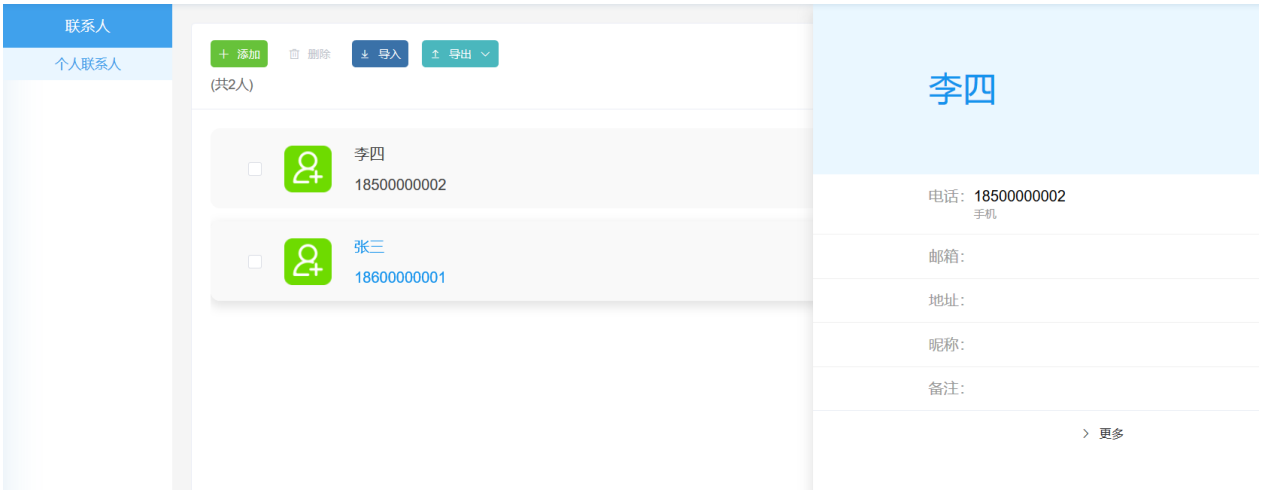
对于没有权限访问的组织、群组、人员，用户可以通过权限申请的方式请求访问，权限审批人员可在管理台指定：

2.5.5 通讯录-名片发送

用户可给指定人员发送名片，可以发送自己的和他人的，名片只能在通讯录中查看且只能发送其有权限访问的人员名片：

2.5.6 通讯录-个人联系人

用户可自己维护自己的联系人，可以从企业通讯录中选择，也可以通过手机通讯录文件格式导入，个人联系人导出时只能导出非企业通讯录中的人员以防止企业信息泄露：

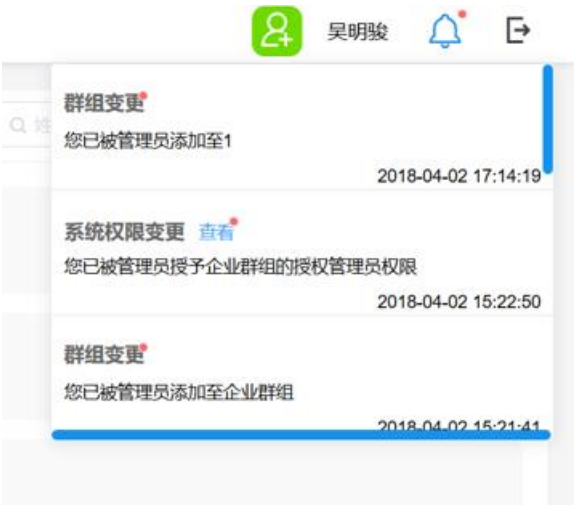


2.5.7 通讯录-个人中心

用户可在个人中心里查看自己的个人信息，个人的权限信息以及自助修改密码；

2.5.8 通讯录-个人消息

用户信息被修改、权限变更、审批通知、收到名片等消息可在个人消息中提示并查看；



2.5.9 管理台-组织管理

管理员可对企业组织机构进行维护，包括新增、修改、移动、启用、禁用、删除等功能，并能够为每一个组织设置安全等级，用于在权限管理中设置不同用户访问不同安全等级的组织：

2.5.10 管理台-人员管理

管理员可对企业人员进行维护，包括新增、修改、移动、启用、禁用、删除、开通用户、重置密码等功能，并能够为每一个人员设置安全等级，用于在权限管理中设置不同用户访问不同安全等级的人员：

2.5.11 管理台-企业群组管理

管理员可对企业群组进行维护，包括新增、修改、移动、启用、禁用、删除等功能，并能够为每一个群组设置安全等级，用于在权限管理中设置不同用户访问不同安全等级的群组；

2.5.12 管理台-权限定义

管理员可以预先定义好角色，并为角色关联对应的权限，权限分为系统菜单权限以及数据操作权限，系统菜单权限可对应到管理台上的每个模块、菜单、功能按钮；数据操作权限可对应到组织、群组、人员的每种操作类型；角色与权限关联好之后即可在授权管理中为用户授予对应角色使其拥有指定权限；

2.5.13 管理台-授权管理

管理员可给指定用户授予其作为管理员在管理台访问指定模块使用指定菜单的权限，同时也可以指定该管理员针对不同组织、群组（分级分权）的访问和操作权限，还可以授予普通用户在通讯录中可以访问的组织、群组、人员信息；

2.5.14 管理台-人员属性定义

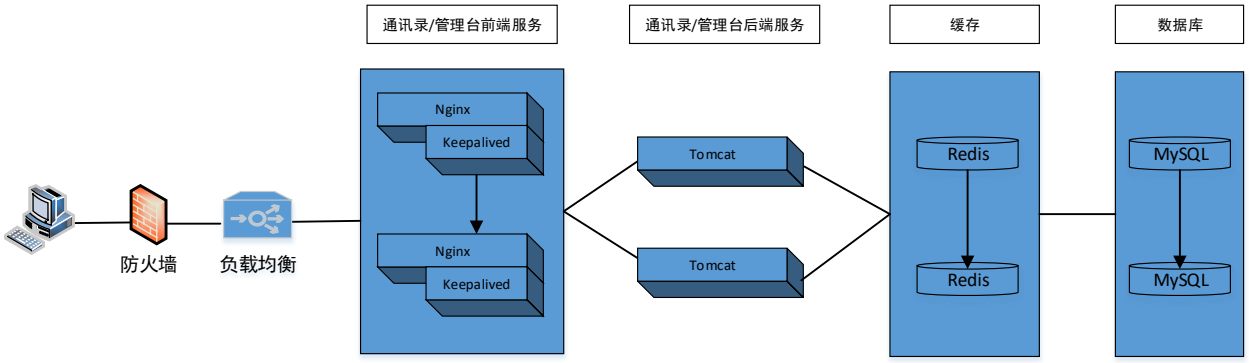
管理员可根据需要定义扩展通讯录中人员所拥有的信息，如增加多个手机号、邮箱、地址以及企业的业务属性，同时可以指定这些属性的使用策略，如在进行人员维护时哪些属性必须，满足什么格式；还可以设置每个属性的安全等级，用于在授权管理中指定不同用户访问不同安全等级的属性：

2.5.15 管理台-常用规则设置

管理员可按需设置通讯录的访问规则，如不同类型的用户能访问通讯录中哪些安全等级的组织、群组、人员、人员属性；可以设置同一部门的用户默认可互相查看的人员属性等级等；

3 产品部署

通讯录部署架构如下图所示，通讯录与管理台可集中部署也可分开部署，分开部署时架构相同。



前端服务：通讯录/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；

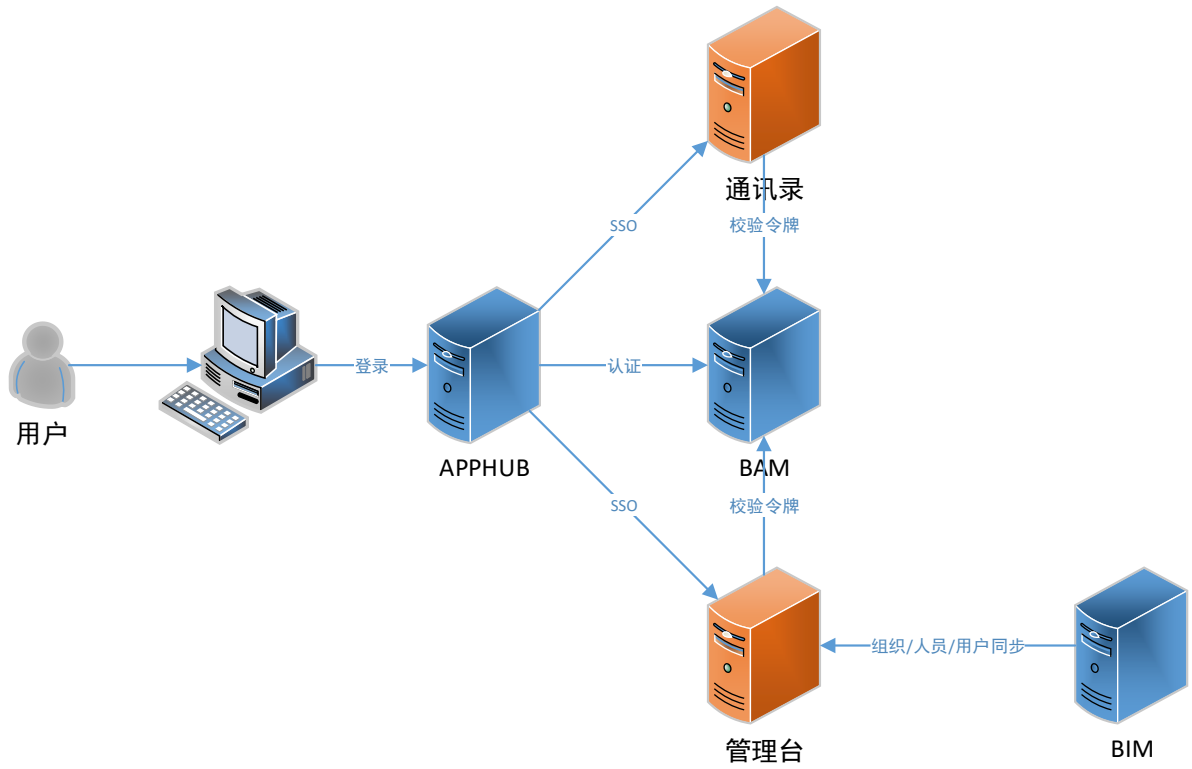
后端服务：通讯录/管理台后端服务可使用 Tomcat/Weblogic 等进行部署，推荐 Tomcat 部署，可将 Tomcat 配置成集群，且前端 Nginx 可配置负载均衡连接后端服务；

缓存：缓存使用 Redis，配置成集群模式；

数据库：数据库可使用 MySQL/Oracle/MariaDB，推荐使用 MySQL，MySQL 配置为集群模式；

4 产品集成

通讯录可独立部署使用，也可以与竹云 IAM 系列产品进行集成，集成架构如下图所示：



集成 APPHUB：通讯录/管理台与 APPHUB 集成后，用户在 APPHUB 的应用列表中可看到通讯录/管理台作为应用展示出来，如果该用户有权限访问则可直接点击应用图标直接访问通讯录/管理台，实现单点登录无需再次输入账号密码；

集成 BAM：BAM 作为统一认证系统，在用户登录 APPHUB 时需要通过 BAM 进行认证，用户在 APPHUB 中访问通讯录/管理台时，通讯录/管理台需要到 BAM 进行令牌校验，以确保身份合法；

集成 BIM：BIM 作为企业统一身份管理系统，可将企业组织以及企业各类人员通讯录相关信息直接供给给通讯录系统，无需管理员在管理台上手动维护，集成后通讯录的用户也受到 BIM 的统一管理，用户的整个生命周期由 BIM 自动同步，无需管理员手动维护；