蚂蚁科技

应用开发和治理平台 安全白皮书

产品版本: 1.3.0

文档版本: 20220107



法律声明

蚂蚁集团版权所有©2021,并保留一切权利。

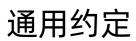
未经蚂蚁集团事先书面许可,任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部,不得以任何方式或途径进行传播和宣传。

商标声明

♥ 點數集团 ANT GROUP 及其他蚂蚁集团相关的商标均为蚂蚁集团所有。本文档涉及的第三方的注册商标,依法由权利人所有。

免责声明

由于产品版本升级、调整或其他原因,本文档内容有可能变更。蚂蚁集团保留在没有任何通知或者提示下对本文档的内容进行修改的权利,并在蚂蚁集团授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过蚂蚁集团授权渠道下载、获取最新版的用户文档。如因文档使用不当造成的直接或间接损失,本公司不承担任何责任。



格式	说明	样例
⚠ 危险	该类警示信息将导致系统重大变更甚至故 障,或者导致人身伤害等结果。	⚠ 危险 重置操作将丢失用户配置数据。
☆ 警告	该类警示信息可能会导致系统重大变更甚至故障,或者导致人身伤害等结果。	
☆注意	用于警示信息、补充说明等,是用户必须 了解的内容。	(大) 注意 权重设置为0,该服务器不会再接受新 请求。
② 说明	用于补充说明、最佳实践、窍门等 <i>,</i> 不是用户必须了解的内容。	② 说明 您也可以通过按Ctrl+A选中全部文 件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在 结果确认 页面,单击 确定 。
Courier字体	命令或代码。	执行 cd /d C:/window 命令,进入 Windows系统文件夹。
斜体	表示参数、变量。	bae log listinstanceid Instance_ID
[] 或者 [a b]	表示可选项,至多选择一个。	ipconfig [-all -t]
{} 或者 {a b}	表示必选项,至多选择一个。	switch {active stand}



1.安全隔离	05
2.鉴权认证	06
2.1. 身份认证	06
2.2. 权限认证	06
3.数据安全	07



1.安全隔离

应用开发与治理平台(BizStack)采用多租户的方式对用户资源进行隔离,通过租户、工作空间两个维度进行细粒度的隔离。

- 不同租户之间的资源绝对隔离。
- 同一租户里不同工作空间下(比如开发、测试、生产环境)的资源彼此隔离。

> 文档版本: 20220107 5

2. 鉴权认证

2.1. 身份认证

身份数据来源于 IAM 系统,在用户通过控制台访问到相应功能接口时,BizStack 内置网关会调用 IAM 提供的 SDK 对用户进行身份验证。

? 说明

IAM(Identity and Access Management)是基于蚂蚁金融科技的多年发展,结合业内其他厂商(AWS、阿里云、GoogleCloud 等)的方案,孵化出的一套通用、灵活的身份管理、认证及访问控制解决方案。

2.2. 权限认证

应用开发与治理平台(BizStack)通过垂直权限控制和水平权限控制两个维度对用户权限进行认证。

● 垂直权限控制

由租户和工作空间两个模型进行控制,实现不同租户间不能互相操作应用、机器、负载均衡等资源。更进一步,可以对用户授予工作空间级别的权限,达到不同用户在不同工作空间有不同权限的目的。比如在开发环境的工作空间,可以让一位质量负责人有可操作所有资源的管理员权限,但在生产环境的工作空间,对资源仅有只读权限。

● 水平权限控制

需要利用 IAM 的权限管理能力,BizStack通过定义不同的角色(包含不同的权限集合,如架构师、研发人员等),对用户就具体的资源进行细粒度的授权,比如架构师才能创建应用,研发人员只能查看并操作自身"参与"的应用,对其他的资源则不能进行操作。

> 文档版本: 20220107 6

3.数据安全

应用开发与治理平台(BizStack)支持采用阿里云 RDS 或蚂蚁集团下的 OceanBase 进行数据存储,具备金融级可靠性及数据一致性。

- 阿里云关系型数据库 RDS(Relational Database Service)是一种稳定可靠、可弹性伸缩的在线数据库服务。基于阿里云分布式文件系统和 SSD 盘高性能存储,RDS 支持 MySQL、SQL Server、Post greSQL 和 MariaDB TX 引擎,并且提供了容灾、备份、恢复、监控、迁移等方面的全套解决方案,彻底解决数据库 运维的烦恼。
- OceanBase (简称OB) 基于分布式架构和通用服务器、实现了金融级可靠性及数据一致性。产品具有数据强一致、高可用、高性能、在线扩展、高度兼容 SQL 标准和主流关系数据库、低成本等特点。

RDS 和 OB 数据库均具有 100% 的自主知识产权,同时具备高效的存储引擎、可扩展性、高可靠特性。