

# SOFAStack

## 业务智能可观测平台 安全白皮书

产品版本：AntStack Plus 1.11.0


文档版本：20221021

# 法律声明

蚂蚁集团版权所有©2022，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

 蚂蚁集团  
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。

# 通用约定

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。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 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 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

# 目录

1.安全隔离	05
2.鉴权认证	06
3.数据安全	07
4.操作审计	08

# 1. 安全隔离

业务智能可观测平台 BOS（Business-Intelligent Observability Service）采用多租户的方式对用户资源进行隔离，通过租户、工作空间组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组下（比如开发、测试、生产环境）的集群资源彼此隔离。

## 2. 鉴权认证

### 身份验证

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，业务智能可观测平台 BOS 会调用 IAM 提供的 SDK 进行身份验证。

### 权限控制

首先是垂直权限控制，由租户和工作空间两个模型进行控制，做到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，则对资源仅有只读权限。

其次是水平权限控制，需要利用 IAM 的权限管理能力，定义不同的角色（包含不同的权限集合），对用户就具体的资源进行细粒度的授权，比如授权用户能操作一个特定的应用，或者特定的机器，对其他的资源则不能进行操作。

## 3. 数据安全

业务智能可观测平台 BOS 的数据分为产品层和数据层两部分：

- 对于产品层的数据，采用阿里云 RDS 或 OceanBase 做存储，均使用主备架构。
- 对于数据层的数据，采用 Ceresdb 复制双写，保证机房级高可用。

## 4.操作审计

业务智能可观测平台 BOS 内置操作记录表对操作历史进行记录。

用户操作记录表为：`monitoconfig`.`user\_oplog`。