

蚂蚁集团

研发效能平台 LinkE 安全白皮书

产品版本：AntStack Plus 1.13.1

文档版本：20230710

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.传输加密	08
5.日志审计	09

1.安全隔离

租户隔离

- 研发效能平台采用多租户方式作用户资源隔离，通过租户隔离用户的应用、环境配置、迭代、代码仓库、发布信息，质量信息等数据。
- 不同租户触发的 CI 和构建任务将在独立的 VPC 或用户提供的 VPC 内执行，并且单节点只会执行一个租户的任务并进行网络隔离。

2. 鉴权认证

身份认证

研发效能平台通过对接 IAM 系统对用户信息进行验证。接口同样可以通过阿里云 AccessKey 调用通过，用户调用接口时需要通过 AccessKey 和 AccessKeySecret 带时间戳进行加签，防止流量重放。

权限控制

研发效能平台中主要角色分为租户管理员、架构域负责人、应用负责人、迭代负责人、发布接口人这几类。从上到下对整个租户提供了水平鉴权的依据。

- 租户管理员可以管理整个租户的环境配置、迭代模板与流水线配置应用配置等。
- 架构域负责人可以管理架构域下的所有应用的元数据。
- 应用负责人主要管理本应用的元数据。
- 迭代负责人可以对该迭代进行操作。
- 发布接口人可以对当次发布进行操作。
- 研发效能平台中代码库部分通过代码库级别的成员来区分权限。主要分为 Owner、Developer、Guest。
 - Owner 为代码库所有者，拥有代码库的所有权限。
 - Developer 为代码库开发者，可以做 Clone、Push 代码等开发常用操作。
 - Guest 为代码库访客，对代码库只有查看权限。

3. 数据安全

产品层数据使用阿里云 RDS 存储主备节点，部分元数据保存在 MongoDB，使用了阿里云的三副本集群存储。代码库代码使用了主备的结构，三副本备份存储，并定期同步保证数据一致性。

4. 传输加密

服务端加密

内部应用之间通过 HTTPS 调用，进行加密传输。

客户端加密

用户侧访问通过 Console 调用 POP 网关，同样采用 HTTPS 加密传输，保证整个链路通信不被窃听和篡改。

5. 日志审计

所有数据变更的用户行为审计操作均会记录在数据库中，并且在相关页面用户可自行查看。所有应用的应用日志都会统一存放在服务器的 `/home/admin/logs` 路径下，并同步到 SLS。监控 Agent 会在服务器上定期采集该路径下的日志，并根据配置的规则进行聚合并上传到监控服务端，通过该数据可以做大盘展示并配置报警。