SOFAStack

全链路压测
安全白皮书

产品版本：AntStack Plus 1.13.1

文档版本：20230708

蚂蚁集团
ANT GROUP

法律声明

蚂蚁集团版权所有©2022，并保留一切权利。

商标声明

免责声明

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 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *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}`

目录

1.安全隔离

全链路压测（Loadcenter）采用多租户（tenant）、多工作空间（workspace）的方式对用户资源进行隔离。通过租户和工作空间两个维度进行压力机压测项目的粗力度隔离，同一个租户内也可以通过管理压测项目成员的方式进行更细粒度的隔离。

- 不同租户之间的压力机绝对隔离。
- 同一个租户不同工作空间下（比如开发、测试、生产环境）的压力机也彼此隔离。
- 同一个租户下不同压测项目可通过项目成员的管理进行细粒度隔离。

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，全链路压测会调用 IAM 提供的 SDK 进行身份验证。

权限控制

权限控制主要在租户层面实现，做到不同租户间不能看到彼此的压测项目，更不能配置甚至执行彼此的压测场景。全链路压测平台定义了租户成员、租户管理员、平台管理员三种角色：

- 租户成员：租户内的租户成员需要被加入到压测项目才具有项目权限。
- 租户管理员：自动拥有本租户下所有项目的权限。
- 平台管理员：除了有租户管理员的权限，还可以进行全平台的资源管理权限。

3.数据安全

全链路压测的数据分为产品配置数据和压测结果数据两部分。

- 对于产品配置数据，采用阿里云 RDS 或 OceanBase 做存储，均使用主备架构。
- 对于压测结果数据，采用文件存储（OSS、AFS、MINIO）做存储，使用多副本机制保证高可用。

4.操作审计

全链路压测对每次压测的执行和停止记录了用户操作日志。

用户压测操作记录表为：`cloud_load_db `.` load_operation_logs` 。