SOFAStack

高可用管理
安全白皮书

产品版本：AntStack Plus 1.11.0

文档版本：20221008

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

高可用管理平台本身不强依赖任何产品。当机房发生故障时，平台可降级对数据库的依赖，正常进行容灾切换。

双机房或者多机房架构部署时，当一个机房故障或宕机，另一个机房的容灾平台可继续使用，保障高可用。

实现认证隔离，即当认证系统 IAM 服务不可用时，可通过独立的账号登录继续使用容灾平台。独立账号为运维管理员单独的管理员账号，具有唯一性。

2.鉴权认证

身份验证

通过蚂蚁集团的 IAM 认证登录体系验证登录，由运维管理员进行账号添加，非添加账号无法登录。

权限控制

高可用管理平台分为运维管理员和租户两种角色。运维管理员可看全局视角进行整体容灾执行，租户账户只能看到本租户内部的应用及操作本租户的应用容灾的权限。

3.数据安全

容灾平台本身的配置数据通过数据库进行保存，依赖数据库的高可用数据存储能力。容灾平台采用双容器部署方式，保障应用高可用，一个容器宕机不影响应用正常使用。