SOFAStack

MS微服务
安全白皮书

产品版本：V2.1.0

文档版本：20220527

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

中间件产品采用多租户的方式隔离用户资源。中间件给每个租户分配一个全局唯一的实例 ID，每个租户仅能读取和操作自己租户的数据。

然而，根据实际业务场景，每个租户使用的物理资源（包括负载均衡、计算资源和存储资源）既可以多个租户共享使用，也可以单个租户独占使用。中间件通过智能寻址组件控制租户访问的物理资源是共享的还是独占的。关于智能寻址的鉴权机制，请参见 身份验证。

2.鉴权认证

2.1. 身份验证

您可以在云控制台中自行创建 AccessKey。AccessKey 由 AccessKey ID 和 AccessKey Secret 组成，其中 AccessKey ID 是公开的，用于标识用户身份，AccessKey Secret 是私密的，用于用户身份的鉴别。

当您向中间件发送请求时，需要首先将发送的请求按照中间件指定的格式生成签名字符串，然后使用 AccessKey Secret 对签名字符串进行加密产生验证码。验证码带时间戳，以防止重放攻击。中间件收到请求以后，通过 AccessKey ID 找到对应的 AccessKey Secret，以同样的方法提取签名字符串和验证码。如果计算出来的验证码与您提供的验证码一致即认为该请求是有效的；否则，中间件将拒绝处理这次请求。

2.2. 权限控制

中间件控制台有三种角色可以控制用户对中间件相关的配置和资源的访问。

- **共享中间件-管理员：** 拥有中间件产品的所有操作权限，包括高危的运维操作，比如推送动态配置，删除 Topic，数据库切换等。
- **共享中间件-开发者：** 拥有开发应用程序所需要使用的所有中间件权限，如添加订阅关系，添加分库分表规则，但没有一些高危的运维操作权限。
- **共享中间件-观察者：** 只有查看权限，能查看开发需要使用的中间件的信息。

如需添加或修改相关的角色权限，可联系空间管理员前往 **控制台 > 成员管理** 页面进行角色设置。

3.数据安全

- 中间件的数据存储在关系型数据库中，关系型数据库既可以是 MySQL 也可以是蚂蚁的 OceanBase。中间件使用的 MySQL 必须为主备模式，或者使用 OceanBase 的三副本或五副本，以保障中间件的数据安全。
- MOSN 支持对应用进行 HTTP 健康检测，保证应用的可用性。