SOFAStack

API 网关

安全白皮书

产品版本：AntStack Plus 1.11.0

文档版本：20220928

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

API 网关采用多租户的方式隔离用户配置信息。每个用户只能看到本租户的 API 配置。通常情况下，本租户下的 API 只有同租户的应用才可以调用。同时，根据实际业务诉求，API 网关也提供跨租户 API 调用的能力，用户只需要创建一个外部的授权对象，即可将本租户的 API 授权给其他租户的应用进行调用。

2.鉴权认证

2.1. 身份认证

API 网关提供了以下两种身份认证方式：

- **无需认证**：客户端请求，不用设置 AccessKey 和 AccessSecretKey，就可以访问相应的 API。
- **密钥认证**：客户端请求，需要设置正确的 AccessKey 和 AccessSecretKey，才可以访问相应的 API，否则即使授权的请求也会被拒绝。

每个应用有一组唯一的 AccessKey 和 AccessSecretKey。当客户端发起请求，要把 AccessKey 也放入请求中，并且根据密钥对计算出请求签名，网关收到请求后，根据 AccessKey 找到对应的 AccessSecretKey，重新计算签名，并且验证签名是否一致。

2.2. 权限认证

API 网关默认对所有 API 开启认证功能，只有被授权的应用才可以访问相应的 API，而没有授权的请求将会被拒绝。

对于客户端请求，网关首先通过上一步验证签名是否一致，如果一致，然后根据请求里的 AccessKey，判断这个客户是否有权限调用这个 API。


API 网关
API 发布
API 管理
API 分组
系统集群
路由规则
数据模型
外部授权 API
授权管理
参数映射
CORS 管理
API 订阅
监控
授权应用详情
应用名称：test_a111
APPID：PILAAVGAWKVGFDFU
创建人：-
创建时间：2020-07-27 10:40:47
绑定的 API
绑定的 API
API 名称
API 分组
授权应用数量
状态
前端协议类型
OperationType/接口名称
test_interfae
sr
1
未发布
SOFARPC
xx.xxx
wy-api
sr
1
已发布
HTTP
-
test_aaa
测试分组
1
未发布
HTTP
-

3.数据安全

API 网关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 必须使用主备模式，或者使用 OceanBase 的三副本或五副本，以保障中间件的数据安全。

API 网关依赖的服务注册中心均采用分布式架构具备 failover 机制：

- MetaServer 集群基于 Raft 协议选举和复制，只要不超过 1/2 节点宕机，就可以对外服务。
- DataServer 集群基于一致性 Hash 承担不同的数据分片，数据分片拥有多个副本，一个主副本和多个备副本。如果 DataServer 宕机，MetaServer 能感知到，并通知所有 DataServer 和 SessionServer， 数据分片可 failover 到其他副本，同时 DataServer 集群内部会进行分片数据的迁移。
- SessionServer 集群任何一台 SessionServer 宕机时，Client 会自动 failover 到其他 SessionServer，并且 Client 会拿到最新的 SessionServer 列表，后续不会再连接这台宕机的 SessionServer。

注册中心支持跨机房部署，通过数据同步机制提供就近访问能力，同时数据能做到跨机房的多副本能力，确保数据的一致性与安全性。

4.传输加密

4.1. 服务器端加密

在 API 网关向后转发数据时，API 网关提供了签名校验以及数据加密等方式，保证数据不被篡改以及数据不被泄露。

API 网关会前置一个 SLB，所有的请求都通过 SLB 接入，然后再转发给 API 网关。SLB 对外暴露 HTTPS 的服务，通过 MTLS 保证通信安全。SLB 服务自身提供高可用、高安全、高稳定性的证书管理服务。

4.2. 客户端加密

客户端在发送数据到网关时，会对发送的数据进行加签以及加密，网关收到数据后会进行相应的校验，只有正确的数据才会被转发的服务端。

网关会为每个应用分配一个 AccessKey 和 AccessSecret。客户端发起请求时，先通过 AccessSecret 对数据进行加签，同时将 AccessKey 也放入请求中。网关收到请求后，根据 AccessKey 找到对应的 AccessSecret，按照和客户端一样的算法进行加签，比较和客户端传来的签名是否一致，从而保证数据不被篡改。

5.日志审计

API 网关的所有操作均有后台日志记录，通过后台日志可以追溯到执行操作的时间和人员。