SOFAStack

AntStack Plus

安全白皮书

产品版本：AntStack Plus 1.11.0

文档版本：20220929

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.云游

1.1. 安全隔离

云游是蚂蚁科技产品交付运维工具平台，不涉及安全隔离问题。

1.2. 鉴权认证

身份认证

云游身份认证体系对接的是 IAM 产品，用户需要输出正确的登录名和登录密码，通过登录校验后才可以正常访问平台。

权限控制

云游权限控制对接的是 IAM 产品，是基于 RBAC 的访问控制策略，目前支持为每个用户按环境维护授予不同的角色权限。目前支持的角色列表有：运维工程师、环境管理员、环境观察者、AKE 运维管理员。

1.3. 数据安全

云游的数据存储在关系型数据库中，数据安全依赖关系型数据库的高可用方案。目前根据不同输出模式使用到的关系型数据库主要有：阿里云 RDS、蚂蚁 OceanBase 以及客户提供的 MySQL 实例等。

身份认证

云游身份认证体系对接的是 IAM 产品，用户需要输出正确的登录名和登录密码，通过登录校验后才可以正常访问平台。

权限控制

云游权限控制对接的是 IAM 产品，是基于 RBAC 的访问控制策略。支持为每个用户按环境维护授予不同的角色权限。目前支持的角色列表有：运维工程师、环境管理员、环境观察者、AKE 运维管理员。

KeyStone 安全加密

数据库账号口令、服务器账号口令、SSH Key、访问密钥等凭据的泄露，是当今数据安全面临的主要威胁之一， 在 2019 年 12 月 1 日正式实施的等保 2.0 中，就对网络安全第三级及以上等级保护对象做出了明确的密码应用安全性评测标准。

通过云游发布的金融云中枢产品，其中部分应用需要在启动中用到数据库账号口令、访问阿里云或其他产品的 AK（AccessKey ID）、SK（AccessKey Secret）等密钥或机密数据，而云游通过环境变量的方式将密钥/机密信息注入给应用容器。所以按照监管要求，需要对这些敏感数据进行安全加固。对于云游应用自身，也同样需要对一些敏感数据进行加密处理。因此云游开发了一款 SDK（KeyStone），以实现不同场景下为云游和通过云游发布的产品中的敏感数据提供安全保护：

- 在飞天专有云底座场景下，通过阿里云 KMS 的密钥加密服务对 PaaS 产品的口令、密钥等机密信息进行加解密。
- 在公有云或物理机场景下，通过 BKMI 托管和保护 PaaS 产品的令牌、密码、证书、API 密钥和其他机密，并对其访问进行严格控制。通过 AntKMS 对应用的口令、密钥等进行加解密。
- 对于没有 KMS 和 BKMI/AntKMS 的场景下，KeyStone 提供离线加密功能，对 PaaS 产品的口令、密钥等进行加解密，支持国密 SM4 算法。

1.4. 日志审计

云游 Local 会记录用户在平台上的操作记录，用户可以通过菜单栏的操作日志入口，查询当前环境内所有的用户操作记录。

2.身份访问管理 IAM

2.1. 安全隔离

身份访问 IAM（Identity and Access Management）基于多租户模型进行数据隔离。IAM 支持多企业入驻，不同企业之间的数据天然隔离。同时同一个企业下又可以有多个租户，租户之间可以共享成员。对接了 IAM 的产品可以以租户为隔离单位对自己的产品数据进行隔离。

2.2. 鉴权认证

身份认证

IAM 内置了一套完整身份认证体系。支持以下认证能力：

- 基于账密的产品控制台访问认证。
- 基于 AccessKey 的 OpenAPI 访问认证。
- 基于 STS Token 的虚拟身份认证。
- MFA 双因子校验能力。

  支持短信校验码二次验证和多种客户端（包括谷歌验证器 Google Authenticator）的令牌二次验证能力，具有灵活的管控能力。支持管理员强制企业下全部用户开启和个人自定义是否开启。

对于 IAM 自持账号，支持配置以下密码策略：

- 密码长度控制。
- 密码字符组成控制。
- 密码有效期控制。
- 密码重试次数控制。
- 过期重置密码与历史密码校验控制。

另外，为了适配客户复杂的身份认证场景，IAM 也提供了多种身份源对接的能力，不仅可以作为身份源（IdP），提供基于 Oauth 的三方认证能力，便于客户系统对接。同时，也可以以服务提供者（SP）身份，对接客户标准的认证系统。目前支持 CAS、SAM、OIDC、LDAP、AD 认证协议。

当客户采用的不是标准协议，而又迫切希望我们复用其身份体系的情况下，IAM 提供了基于 SPI 形式的认证方式。客户只要按照蚂蚁金融科技的标准实现相关接口，便可将其身份体系与蚂蚁金融科技的进行打通，从而实现账号集中化统一管理。

权限控制

IAM 实现了基于角色和条件的权限访问控制。

- 角色是权限码的集合，便于将一批权限授予某个对象；权限码对应于页面的一个功能或一个对外暴露的 API，角色和权限码进行垂直权限控制。
- 条件可根据产品需求自由定制，实现水平权限控制。例如租户、应用等任何一个产品提供给用户的资源或概念都可以作为条件。同时提供组的管理能力，可将多个身份可加入到同一个组，并对该组进行授权，则组内的成员便都将具有对应权限。

2.3. 数据安全

IAM 的数据存储在关系型数据库中，数据安全依赖关系型数据库的高可用方案。目前根据不同输出模式使用到的关系型数据库主要有阿里云 RDS、蚂蚁 OceanBase 以及客户提供的 MySQL 实例等。

针对像密码这样的敏感数据，IAM 通过 SHA256 的加密方式加密存储，保证用户数据的安全性。您也可以通过 KeyStone 对数据进行加解密，保障数据安全。更多信息，请参见 KeyStone 安全加密。

2.4. 日志审计

IAM 内置审计中心，用户可对其在 IAM 以及其他云产品上的操作日志进行审计。支持多种维度的审计日志查询，并且可以按期归档，同时支持安全审计的需求。

3.容器底座

3.1. 安全隔离

Captain 控制台是容器集群管理平台，不涉及安全隔离问题。

AKE 云原生平台（AKE3）提供了节点打标的能力，可以调度不同角色的容器到对应的节点上。同时，AKE3 也支持在集群内划分多个网络。

3.2. 鉴权认证

Captain Plus 权限控制对接的是 IAM 产品，是基于 RBAC 的访问控制策略，目前支持为每个用户按集群维护授予不同的角色权限。目前支持的角色包括：超级管理员、集群管理员、集群运维工程师、集群扩容工程师。

3.3. 数据安全

Captain Plus 的数据存储在关系型数据库中，数据安全依赖关系型数据库的高可用方案。根据不同的输出模式，使用到的关系型数据库主要有阿里云 RDS、蚂蚁金融科技 OceanBase 以及客户提供的 MySQL 实例等。

AKE 云原生平台（AKE3）的数据存储在 etcd 集群中。etcd 是三节点高可用部署，数据通过本地卷挂载在节点上，可根据任意节点上的数据重新恢复整体数据。

针对数据库账号密码、AK（AccessKey ID）、SK（AccessKey Secret）等敏感信息，容器底座还支持通过 KeyStone 对数据进行加解密，保障数据安全。更多信息，请参见 KeyStone 安全加密。

3.4. 日志审计

Captain Plus 会记录用户在平台上对集群的操作记录。用户可以通过查看操作记录，查询到当前集群内所有的用户操作记录。

4.AntStack DNS

4.1. 安全隔离

AntStack DNS（ADNS）为 AntStack 提供内部 DNS 服务变配和解析服务，不涉及安全隔离问题。

4.2. 鉴权认证

身份认证

AntStack DNS 管控端目前尚不具备身份认证的能力。DNS 解析服务无需身份认证。

权限控制

提供了根据 ACL 来决定是否允许来自某些 IP 的区域传输和 DNS 解析请求的能力。

4.3. 数据安全

AntStack DNS（ADNS） master 节点通过主备的架构保证高可用和数据一致性。ADNS master 和 slave 解析节点通过区域传输协议保证数据一致性。

另外，管控端会将数据落到数据库，如果 DNS 节点全部宕机且数据被毁，可通过从数据库捞取数据进行恢复。

针对数据库账号密码、AK（AccessKey ID）、SK（AccessKey Secret）等机密信息，ADNS 还支持通过 KeyStone 对数据进行加解密，保障数据安全。更多信息，请参见 KeyStone 安全加密。

4.4. 日志审计

AntStack DNS 暂不支持日志审计。