SOFAStack

单元化应用服务 LHC

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

单元化应用服务（LHC）采用多租户的方式对用户资源进行隔离，通过租户、工作空间组和命名空间（Namespace）三个维度进行细粒度的隔离。

- 不同租户之间的资源绝对隔离。
- 同一租户里不同工作空间组下（比如开发、测试、生产环境）的集群资源彼此隔离。
- 通过自定义网络安全策略，使得不同命名空间里的资源进行隔离，比如节点（Node）和 Pod。

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，LHC 会调用IAM 提供的 SDK 进行身份验证。

另外，还可以直接通过 Kubernetes 集群的证书进行身份的认证，其中证书里的 token 也是根据用户在 IAM 里的信息生成，在集群对证书的合法性进行校验时也会查询 IAM，检查是否有该用户存在。

权限控制

- **垂直权限控制**

由租户和工作空间两个模型进行控制，做到不同租户间不能互相操作应用、机器、负载均衡等资源。更进一步，可以对用户授予工作空间级别的权限，达到不同用户在不同工作空间有不同权限的目的。比如在开发环境的工作空间，可以让一位质量负责人有可操作所有资源的管理员权限，但在生产环境的工作空间，则对资源仅有只读权限。

- **水平权限控制**

水平权限控制需要利用 IAM 的权限管理能力，定义不同的角色（包含不同的权限集合），对用户就具体的资源进行细粒度的授权，比如授权用户能操作一个特定的应用，或者特定的机器，对其他的资源则不能进行操作。

3.数据安全

单元化应用服务的数据分为产品层和 Kubernetes 层两部分：

- 对于产品层的数据，采用阿里云 RDS 或 OceanBase 做存储，均使用主备架构。
- 对于 Kubernetes 层的数据，采用 ETCD 三副本存储，保证机房级高可用。

同时，在向用户机器的运维通道发送指令时，均采用签名和验签机制保证数据完整性和正确性。

4.传输加密

首先，从用户侧访问单元化应用服务控制台再到后端服务器的调用链路上，均采用 HTTPS 进行加密传输。

其次，在单元化应用服务提供的 Kubernetes 集群中，以下通信链路均会进行 TLS 证书校验，以保证通信不被窃听或篡改。

- 数据面节点上的 kubelet 访问控制面节点上的 apiserver。
- 控制面节点上的 apiserver 访问数据面节点上的 kubelet。

5.日志审计

单元化应用服务使用日志采集的方式进行监控分析。监控 agent 会在应用服务器上收集所配置路径下的日志，并做相应的采集聚合，然后上报到监控服务端，以进行大盘展示，报警等功能。

常用的日志采集路径如下：

- `/home/admin/logs/应用名称/common-error.log` 标准错误日志
- `/home/admin/logs/应用名称/common-default.log` 标准输出日志
- `/home/admin/logs/应用名称/业务名称-error.log` 某一具体业务错误日志
- `/home/admin/logs/应用名称/业务名称-default.log` 某一具体业务标准输出日志
- `/home/admin/logs/应用名称/digest/业务名称-digest.log` 某一个具体业务的摘要输出日志