

SOFAStack

资金安全监控 运维指南

产品版本：AntStack Plus 1.13.1

文档版本：20230707




法律声明

蚂蚁集团版权所有©2022，并保留一切权利。

未经蚂蚁集团事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

商标声明

 蚂蚁集团 ANT GROUP 及其他蚂蚁集团相关的商标均为蚂蚁集团所有。本文档涉及的第三方的注册商标，依法由权利人所有。

免责声明

由于产品版本升级、调整或其他原因，本文档内容有可能变更。蚂蚁集团保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在蚂蚁集团授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过蚂蚁集团授权渠道下载、获取最新版的用户文档。如因文档使用不当造成的直接或间接损失，本公司不承担任何责任。

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 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1. 运维概述	05
1.1. 产品架构	05
1.2. 运维架构	06
1.3. 技术支持渠道	07
2. 离线数据运维	08
3. 文件核对计算节点运维	09
4. 日常运维	12
5. 常见故障处理	13
6. 扩容与缩容	15
7. 配置参考	16
8. 参考日志	17
9. 基础术语	19

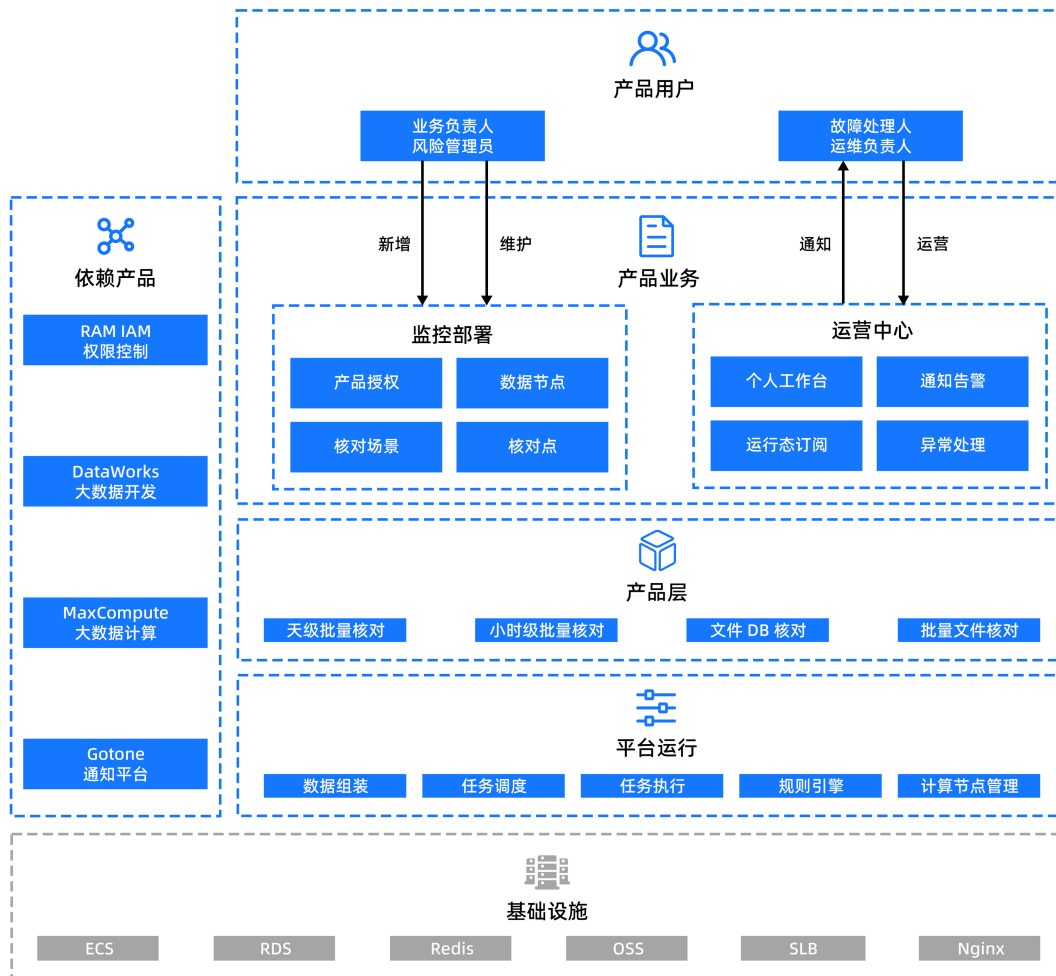
1. 运维概述

1.1. 产品架构

本文介绍资金安全监控应用服务的系统架构、部署架构。

系统架构

下图展示了资金安全监控的整体系统架构。

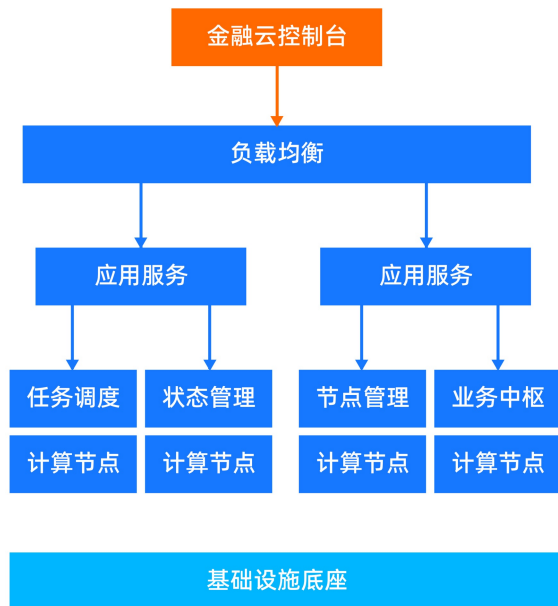


各模块说明如下：

- **产品用户**：该产品可能具备的操作角色。
- **依赖产品**：在使用该产品可能需要使用和依赖的产品。
- **产品业务**：可根据实际情况对使用方式进行调整。
- **产品层**：提供核对能力。
- **平台运行**：平台运行所依赖的一些内部组件。
- **基础设施**：依赖的基础部署设施，这通常包含在云基础底座中。

部署架构

下图展示了资金安全监控的整体部署架构。



各模块说明如下：

- **金融云控制台**：产品的操作界面主要通过金融云控制台展现。
- **负载均衡**：使用通用的负载均衡组件进行操作界面流量调拨和管控，以满足容灾及运维场景。
- **应用服务**：为上层操作提供相应服务。
- **各关键业务模块**：主要的部署计算角色，这都集成在同一应用内。
- **基础设施底座**：依赖的 ECS、RDS 等基础设施，这通常包含在云基础底座中。

1.2. 运维架构

本节介绍资金安全监控应用服务的运维架构。

运维大类	描述	运维工具
日常运维	包括计算节点的维护和日志运维操作。	基于云基础底座运维工具
停机维护	<ul style="list-style-type: none">● 检查和确认容器、组件状态。● 停止、启动容器、组件。● 升级组件。	云游
故障处理	主要处理组件可用性和业务连续性故障。	云游和命令行

1.3. 技术支持渠道

服务热线

若有需要，可随时拨打热线电话：400-995-1887。

提交工单

若您有额外的产品功能需求或非紧急的技术咨询，可通过提交工单联系蚂蚁集团技术支持团队。

工单提交地址：<https://user.cloud.alipay.com/#/tickets/submit>。

2. 离线数据运维

本节主要介绍平台针对离线任务管理所进行的工作，要求管理员对配置和技术架构有一定的了解。

离线数据同步

将离线数据同步至数据仓储的操作视实际环境部署情况而定，您可能需部署 DataWorks、DataGo、D2 等数据工作台，然后通过工作台配置将业务数据同步至离线仓储。具体操作步骤，请参见 [MaxCompute 导入数据](#) 和 [DataWorks 数据集成](#)。

离线数据授权

将离线数据的使用权限授予资金安全监控平台的操作方法如下：

1. 登录资金安全监控控制台，在左侧导航栏单击 **数据资源配置**。
2. 在 **数据源配置** 页面上，单击 **新建数据源配置**。
3. 在 **新建数据源配置** 页面上，完成以下数据源配置。
 - **数据源配置名称**：数据源配置的名称。租户内唯一，长度为 1-100 个字符，可包含中英文、数字、下划线（_）和短横线（-）。
 - **类型**：选择 **离线**。
 - **访问授权信息**：需填写 **accessKeyId**、**accessKeySecret**、**endPoint** 和 **project**。

说明

关于 **accessKeyId** 和 **accessKeySecret** 的获取方式，请参见 [获取 AccessKey](#)。

4. 配置完成后，单击 **授权**。

上述操作完成后，可在数据源配置列表页面，看到刚创建的数据源配置。

3. 文件核对计算节点运维

文件核对引擎执行时会使用客户的存储空间来保存临时文件。本节主要介绍文件核对在计算节点运行过程中使用的存储空间及相关协议文件的部署操作。

您可以通过阿里云租户控制台进行 OSS 文件管理，初始化文件协议。具体操作步骤如下：

1. 新建 OSS 目录。

您需要创建如下目录：

- `finorm/hashed/`：用于存放哈希文件。
- `finorm/protocol/`：用于存储文件协议。
- `finorm/test/`：用于存放测试文件。

2. 下载 [协议描述文件](#)，并上传至 `finorm/protocol/` 目录下。

3. 配置应用的 OSS 数据源。

② 说明

应用会默认读取该数据源作为散列文件存储及文件协议存储。

- 登录资金安全监控控制台。
- 在左侧导航栏上，单击 **数据源配置**。
- 单击 **新建数据源配置**，在右侧面板上配置以下信息：

新建数据源配置

×

* 数据源配置名称:

atfinorm-prod

* 类型:

OSS

FTP

DB

离线

需要您提供OSS账号的授权，用以查询OSS下的文件

* accessKeyId:

* accessKeySecret:

* bucketName:

atfinorm-prod

* endpoint:

http://oss-*****.com

授权

取消

参数	说明
----	----

参数	说明
数据源配置名称	<p>数据源配置的名称。租户内唯一，长度为 1-100 个字符，可包含中英文、数字、下划线（_）和短横线（-）。此处输入 <code>atfinorm-prod</code>。</p> <div> 重要 输入的 数据源配置名称 必须是 <code>atfinorm-prod</code>。如果要修改该名称，可以登录云游在参数配置中搜索值为 <code>atfinorm-prod</code> 的配置项进行修改。</div>
类型	<p>支持 OSS、FTP、DB、离线 四种类型。可根据您的实际业务需求自行选择。此处选择 <code>OSS</code>。</p> <div> 重要 类型一旦选择确认后，将不能更改。</div>
accessKeyId	提供 OSS 账号的授权，用于查询 OSS 下的文件。需要从用户自己的 OSS 中获取，获取方式请参见 获取 AccessKey 。
accessKeySecret	提供 OSS 账号的授权，用于查询 OSS 下的文件。需要从用户自己的 OSS 中获取，获取方式请参见 获取 AccessKey 。
bucketName	输入数据源配置名称。此处输入 <code>atfinorm-prod</code> 。
endpoint	输入 project 地址。

4. 单击 **授权**，完成 OSS 数据源的配置。

4. 日常运维

本文主要介绍在日常运维中如何清理历史数据。通常在出现大量无用历史数据导致资源紧缺时才需要进行清理操作。

警告

历史数据清理是高危操作，请严格按照操作指导进行，否则可能会给系统的正常运行带来潜在危险。

历史异常数据清理

您可以通过命令行或数据管理视图化操作工具直接对数据库进行相关清理操作。

```
DELETE FROM `sofaclrisk_db`.`issue` WHERE `id` < ${ID};
```

历史任务数据清理

您可以通过命令行或数据管理视图化操作工具直接对数据库进行相关清理操作。

```
DELETE FROM `sofaclrisk_db`.`sql_task` WHERE `id` < {ID};
```

历史散列分片文件清理

您可以通过阿里云租户控制台进行 OSS 文件管理。

警告

注意辨别文件日期，通常情况下该文件会自动清理，该操作属于高危操作，可能导致核对异常，请谨慎操作。

散列分片文件存放在 `finorm/hashed/` 目录下。

5. 常见故障处理

本文主要介绍常见的故障处理指引，帮助您排查一些可能出现的问题。

任务调度失败

【现象】

任务调度出现失败。

【可能的原因】

- 大数计算资源不足。
- SQL 过于复杂，调用的资源过多以致出现持续出现失败等。

【解决方法】

可以结合日志查找原因，日志说明请参见 [参考日志](#)。

告警通知失败

【现象】

告警通知失败。

【可能的原因】

- 依赖的通知组件 Gotone 配置不正确。
- 订阅配置不正确。

【解决方法】

可以结合日志查找原因，日志说明请参见 [参考日志](#)。

计算节点调度失败

【现象】

计算节点调度失败。

【可能的原因】

- 维护计算节点的数据不正确。
- 计算节点资源不足导致没有更多的资源可以调度。

【解决方法】

1. 确认计算节点是否被自动发现。

可以通过 `SELECT node_ip AS 节点 IP, node_group AS 节点环境 FROM `sofaclrisk_db`.`fi_compute_cluster` LIMIT 100;` 来确认当前环境的计算节点是否已正确的被自动发现。

2. 确认计算节点是否资源不足。如果因资源不足而导致无更多资源可供调度，请参见 [扩容与缩容](#) 进行适当扩缩容。
3. 如果上述操作都不奏效，可以结合日志查找原因，日志说明请参见 [参考日志](#)。

文件散列失败

【现象】

文件散列失败。

【可能的原因】

- 访问 OSS 的 Bucket 权限不足。
- 资源限额导致资源不足。

【解决方法】

1. 确认访问 OSS 的 Bucket 权限是否存在问题。请参见 OSS 相关手册。
2. 确认资源限额下资源是否充足。如果资源不足，请参见 OSS 相关手册或 [日常运维](#) 进行资源容量调整。
3. 如果上述操作都不奏效，可以结合日志查找原因，日志说明请参见 [参考日志](#)。

6. 扩容与缩容

当 CPU、内存、磁盘使用率超过水位，出现异常告警后，可直接进行扩容操作。扩容或缩容后，无需对计算节点进行维护，由系统自动进行维护管理。

7. 配置参考

目前各应用不支持通过参数修改 JVM 配置来修改系统性能，您可通过云游进行组件的扩容操作。

8. 参考日志

日志文件路径：`/home/admin/logs/sofaclrisk`。

文件名	说明	归档策略
app-default.log	应用通用日志	<ul style="list-style-type: none">• 每日一个新文件。• 旧文件的名称中会加日期后缀：<code>名称.log.{yyyy-MM-dd}</code>。• 最多保留 30 天的日志文件。
common-error.log	业务异常日志	
common-default.log	默认通用日志	
sofaclrisk-web.log	WEB 请求日志	<ul style="list-style-type: none">• 每日一个新文件。• 旧文件的名称中会加日期后缀：<code>名称.log.{yyyy-MM-dd}</code>。• 最多保留 15 天的日志文件。
sofaclrisk-service.log	业务中枢日志	
sofaclrisk-schedule.log	离线任务调度日志	
sofaclrisk-auth.log	身份验证日志	
sofaclrisk-filter.log	通过过滤器日志	
sofaclrisk-notify.log	告警通知日志	
fi-biz-guardian-task.log	文件引擎任务日志	<ul style="list-style-type: none">• 每小时一个新文件。
fi-biz-guardian.log	文件业务日志	
fi-biz-guardian-monitor.log	文件执行引擎监控日志	
fi-biz-guardian-workflow.log	文件执行引擎工作流日志	
fi-biz-guardian-dispatch.log	文件执行引擎计算节点调度日志	

文件名	说明	<ul style="list-style-type: none"> 旧文件的名称中会加日期后缀：名称.log.归档策略MM-dd_HH}。 最多保留 15 天的日志文件。
fi-biz-guardian-file.log	文件执行引擎文件操作日志	
fi-biz-guardian-flow-control.log	文件执行引擎流控日志	
fi-biz-guardian-biz-sql.log	文件执行引擎外部 SQL 日志	
fi-biz-guardian-sql.log	文件执行引擎 SQL 日志	
fi-biz-guardian-immune-model.log	文件执行引擎模型日志	
fi-biz-guardian-minute-st.log	文件执行引擎状态统计日志	

9. 基础术语

术语	说明
资金安全监控	蚂蚁科技集团的一款风险防控类型的产品，能帮助您发现资金损失的风险。该产品可以通过执行您自定义的规则，以小时频率，准实时等多种时效策略，发现资金类数据问题，向您发出告警。您可以在第一时间收到告警，根据异常数据排查问题，分析原因，进而解决问题。
规则	资金安全监控产品中的规则，也叫核对规则，是数据核对的最小单位。可结合分类来管理。规则主要由 ODPS 表和 SQL 脚本构成，另外，您还可设置一些规则相关信息。规则的核对逻辑由 SQL 体现。
任务	资金安全监控产品中的任务（Task）指核对任务，即核对规则周期性执行的任务。每个周期有一组任务实例，每次执行对应一个任务实例。
任务周期	也叫核对周期，指核对任务的调度周期。如核对频率为天核对，就是一天执行一次，例如 2018.5.29 执行的核对任务对应周期 20180529；如核对频率为小时核对，就是一小时执行一次，例如 2018.5.29 日 10 点执行的核对任务对应周期 2018052910。
异常	<p>核对任务运行中发现数据有差异，系统会创建异常事件（Issue）。</p> <div><p>🔍 说明</p><p>任务重跑时可能会重复产生差异。</p></div>
差异数据	也叫差异，指核对任务执行时（执行 SQL）发现的不匹配核对规则的数据。您可以在异常详情里查看在某个核对周期中发现的抽样差异数据。
差异数量	<p>核对任务执行时发现的差异数据的总数。</p> <div><p>🔍 说明</p><p>您在异常详情页看到的差异数量，是在当次任务周期中发现的差异数据总数，但是在差异数据（抽样数据），仅展现最多 10 条抽样的差异数据。</p></div>

核对频率	<p>核对频率有：按天核对、小时核对、5 分钟核对和自定义核对。</p> <ul style="list-style-type: none">• 小时核对：一小时执行一次核对。• 天核对：一天执行一次核对。• 5 分钟核对：5 分钟执行一次核对。• 自定义核对：根据用户配置的 cron 表达式触发核对执行。
------	---