

SOFAStack

资金安全监控 产品简介

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.概述	05
2.功能特性	07
3.应用场景	09
4.原理架构	10
5.基础术语	12

1.概述

在金融、电商等行业，企业每天都在运转着大量资金业务，一旦由于系统原因或人为因素导致资金数据相关问题，若无法在第一时间发现问题，就会为企业带来巨大的经济损失。

资金安全监控产品旨在帮助您发现资金损失的风险。该产品可以通过执行用户定义的规则，按每天、每小时等多种时效策略，发现资金类数据问题，及时向您发出告警。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。

资金安全监控产品提供公有云和专有云两种不同的部署模式，支持客户在不同环境中对自身业务进行自定义核对检查。

优势

资金安全监控产品具有以下优势：

- 与业界成熟数据平台产品深度融合，提供从上层应用场景到底层基础资源的全面覆盖。
- 多种核对模式和频率，满足各类用户对于资损风险监控时效性的不同需求。
- 除传统的短信、邮件通知外，提供与用户平台对接的通知渠道，可为核心业务提供即时监控、即时应急保障。
- 提供资损风险监控覆盖的度量功能，并配备专家咨询服务，将多年积累的资损防控经验赋能给用户。

功能特性

● 数据节点

您可以在数据节点列表中统一管理资金业务表，通过节点命名、添加描述的方式详述表的业务语义，以便其他用户识别、引用。

● 核对点

您可以通过新建核对点（包含编写核对规则），来进行资金业务表或表与表之间的核对检查。核对点负责人可以进行编辑删除、上线下线等操作，当核对点为已上线状态时，系统会根据设定的核对类型进行周期性检查。您可以查看每个周期的核对规则运行情况。

● 核对场景

您可以将业务梳理为核对场景树（最多三级），核对点可与对应的核对场景绑定，便于从业务视角查看特定场景下的监控能力和异常情况。

● 通知订阅

您可自行订阅某个核对点上下线和修改更新、核对任务执行失败、执行发生异常告警等信息，选择邮件、钉钉的方式通知您。您也可以对多个核对点进行批量订阅。

● 异常列表

您可以查看核对规则粒度的异常情况，其中包括一次核对任务运行时发现的差异数据详情，每次核对任务最多展示差异数据的10条抽样。

● 异常处理

您可以对异常记录处理结论，包含是否误报、是否资损以及备注等信息，关闭异常。异常状态变为已处理，并将以上处理结论通知核对点异常告警的订阅人员，便于及时复盘。

应用场景

- **业务护航**

您可以阶段性地或定期梳理涉及资金的核心业务链路。通过配置核对点，全面覆盖业务资金链路；同时系统将会按照核对规则，对各数据做相互核对，或对数据内容做逻辑检查，以监控业务资损风险。

- **变更风险检查**

业务变更发布前，您可以添加变更业务表的核对点，或者变更业务表与关联表的核对点，确保变更上线后不存在资损风险监控盲点。同理，技改类变更发布前，您也可以针对变更点，新增核对点，或修改原有核对点。

- **历史数据扫雷**

批量检查存量业务的历史数据是否已存在异常，及时排查问题、分析原因，修复漏洞、追回损失以及避免更大的资损。

- **数据质量监控**

数据缺漏时，也可能间接引发资损。您可以通过配置核对点，检查数据完整性，对数据质量作监控，及时发现异常数据。

2. 功能特性

数据源配置管理

您可以在产品中添加多种不同类型的数据源配置，每个数据来源配置代表一个核对系统在后续核对工作中可以用来读取数据的数据来源配置，当前支持如下类型的数据源配置：

- **OSS**：OSS 文件系统的读取配置，需要您输入访问信息，endpoint 和 bucket 信息等。
- **FTP**：从 FTP 系统中读取文件的配置，需要您输入 FTP 服务器访问信息。
- **DB**：从 DB 中读取数据的配置，需要您输入数据库访问配置信息，建议使用备库来进行核对。
- **离线**：离线数据仓库访问的配置信息。

文件源管理

您可以在产品中添加多种不同类型的数据源，每个数据源代表一个核对系统在后续核对工作中可以用来读取数据的数据来源，当前支持如下类型的数据源：

- **文件**：指定一个可以从 OSS、FTP 数据源配置中可以读取的文件，配置字段分割，解码方式等信息。
- **DB**：指定一个可以从 DB 数据源配置中访问的 DB 表信息、配置分库分表、关联表信息等，也支持通过 SQL 直接筛选数据。

数据节点管理

您可以通过新建数据节点来添加和管理不同类型的核对数据节点，可以完成如下的映射：

1. 将离线数据库中的一张表映射为一个核对数据节点，通过为数据节点添加名称以及关联核对点来更方便的进行核对数据节点的管理。
2. 将文件映射为一个核对数据节点，给出文件中排序和散列等信息。
3. 将数据库表映射为一个核对数据节点，给出表中排序和散列等信息。

所有在后续核对中需要使用到的文件，DB 表和离线表都应该被创建为核对点。

核对点管理

您可以通过创建核对点的方式来实现对待核对数据模型的管理。通过向核对点中添加多个节点，并在核对点中创建对应的核对规则来维护一个完整的核对模型。在核对点中，可以关联对应的核对场景，指定负责人，核对类型和延迟执行时长。

针对同一个数据模型（例如：从订单表到交易表的核对）所创建的核对规则，都应该被放到一个核对点中进行管理，方便后续的维护工作。

在创建核对点时需要选择该核对点所支持的核对类型，当前支持如下几种核对类型：

- **准实时核对**：在文件、DB 类型的数据节点之间进行数据比对核对。
- **离线核对**：通过在离线数据中执行 SQL 核对规则来进行数据校验。

核对规则管理

您可以通过创建规则，来进行资金业务表之间的核对检查。规则负责人可以对规则进行编辑、下线、上线等操作，当规则为已上线状态时，系统会根据该规则设定的核对频率，进行周期性检查。您可以查看每个周期的核对运行情况。

核对模板管理和核对模板导入

您可以通过创建核对模板的方式来实现核对数据模型的重用。例如：在不同业务中可能都牵涉到汇总表和流水表的核对，我们可以创建对应的核对模板和规则，在不同业务中进行导入重用。

创建核对模板的方式和创建核对点的方式基本一致，在核对模板下，也一样可以添加对应的规则。

在创建核对点的时候，可以选择通过导入核对模板的方式来实现重用。在导入时，需要对数据节点进行替换，更改核对规则名称。导入完成后，对应的规则和数据节点都会被自动添加到对应的数据节点中。

核对场景

在核对平台中，您可以手工添加和维护核对场景并在创建核对点的时候指定核对场景。通过这种方式来实现对核对节点的分类维护。

核对场景支持父子节点的管理，来实现对多级业务的映射。

通知订阅

您可以根据核对场景、核对点、核对模板等不同维度订阅核对点的状态、异常、任务相关通知，指定通知方式及通知对象。

核对异常告警

当系统发现差异数据，并创建异常事件时，会通过短信、邮件、平台告警的方式通知您。

查看差异数据

您可以查看一次核对任务运行时发现的差异明细数据，一次最多展示 10 条抽样的差异明细数据。

关闭异常

您可以对异常事件记录原因，便于后续复盘。定位原因并解决问题后，您可以关闭异常来更新异常的状态，便于相关人员知晓异常的处理进展。

批量关闭误报的异常

因规则 SQL 不合理，或业务跨分区导致未核对到完整业务数据时，可能是误报异常。您可以在异常列表页中勾选多个异常事件，点击批量关闭，标记误报并备注信息。

- **误报**：指因为 SQL 错误、数据错误、或系统异常等原因导致的和规则预期不符的情况。
- **非误报**：指系统发现的差异数据确实为异常现象，符合规则预期的情况。

3. 应用场景

业务护航

您可以阶段性地或定期梳理涉及资金链路的核心业务。可通过配置核对规则，对各类数据作相互核对，或对数据内容作逻辑检查，系统将按规则监控业务的资损风险。

变更风险检查

业务变更发布前，您可以添加变更业务表与关联表的核对规则，或者变更业务表数据的检查规则，确保变更上线后不存在资损风险监控盲点。同理，技改类变更发布前，您也可以针对变更点，新增核对规则，或修改原有核对规则。

历史数据扫雷

批量检查存量业务的历史数据是否已存在差异，可以及时分析差异原因，修复漏洞，追回资损。

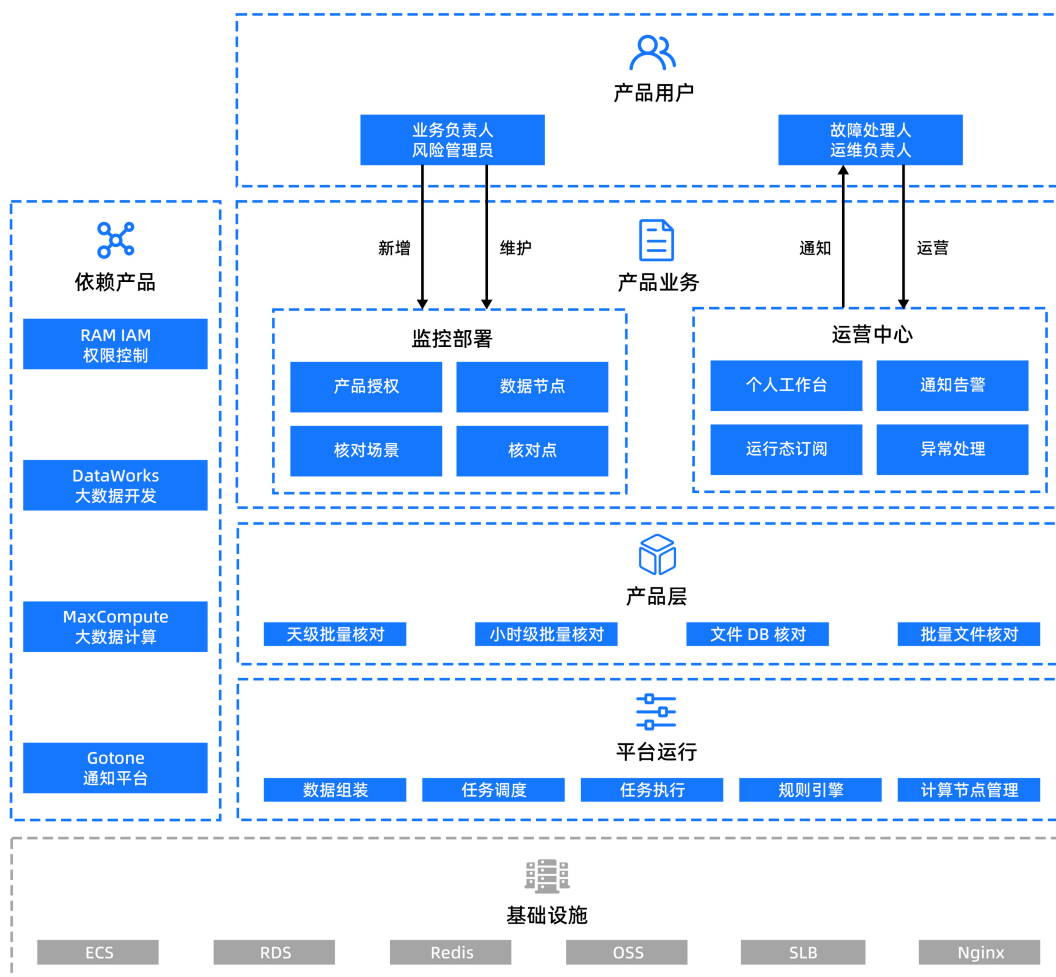
数据质量监控

数据缺漏时，也可能间接引发资损。您可以配置核对规则，以检查数据完整性，对数据质量作监控，及时发现故障。

4. 原理架构

资金安全监控产品的用户一般为业务负责人、风险管理员、故障处理人、运维人员等。业务负责人和风险管理员主要负责维护核对点的准确性，并确保规则周期性核对的数据的有效性。故障处理人、运维人员主要负责在接收到异常告警通知后，分析原因并关闭异常。

资金安全监控产品的整体架构分为四部分：产品业务层、产品核心层、基础设施层和依赖产品。



产品业务层

产品业务层主要提供核对场景、数据节点、核对点、工作台、通知公告和异常处理功能。

- **核对场景**：提供三层树形结构的管理功能，用于梳理业务。
- **数据节点**：提供对资金业务表进行命名和描述的功能，用于核对点的创建。
- **核对点**：提供对核对检查的增删改查、上下线等功能。
- **工作台**：您关注的异常和核对点数据汇总。
- **通知公告**：您可通过邮件、钉钉的方式接收核对点相关的订阅消息。
- **异常处理**：提供异常差异数据明细，排查后您可以对异常记录处理结论。

产品核心层

产品核心层包含核对组装、任务调度、大数据处理、订阅通知和异常运营。

- **核对组装**：根据您配置的基本信息、核对配置、核对规则等核对点信息，组装成待执行的核对检查。
- **任务调度**：基于您配置的核对点，周期性地发起对核对任务的调度，以实现资损风险的监控。
- **大数据处理**：通过大数据平台的功能对核对数据做处理。
- **订阅通知**：选择邮件、钉钉的方式，订阅核对点相关消息的通知。
- **异常运营**：对异常进行管理、查看和处理。

基础设施层

资金安全监控产品依赖的基础设施包括 ECS、MySQL、Redis、SLB、OSS 和 Nginx。

依赖产品

资金安全监控产品依赖的产品包括访问控制 RAM、大数据开发 DataWorks、大数据计算 MaxCompute 和阿里云开放平台 POP。

5.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。
------	---