中间件运维指南

1.3.0 版本

文档版本：V20190827

蚂蚁金服金融科技文档

商标声明

及其他蚂蚁金服金融科技服务相关的商标均为蚂蚁金服所有。

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。蚂蚁金服金融科技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，并在蚂蚁金服金融科技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金服金融科技授权渠道下载、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。

目 录

1.概述

1.1 目的

为加强对生产操作各个环节的质量控制及变更操作的规范管理，加强流程管控，明确必要责任，不断提升业务稳定性指标。运维指南包括 SOFA 中间件云产品组件以及原理介绍、监控指标与说明、预警处理、日志说明、常见运维场景、服务巡检、服务异常情况下的应急预案等。

1.2 产品组件

本运维指南覆盖以下产品组件：

- 微服务平台
- 共享型分布式数据源管理
- 消息队列
- 分布式事务
- 分布式链路跟踪
- 注册中心 SOFA Registry
- 数据访问代理
- 云产品中台
- 服务发现组件

1.3 技术支持渠道

1.3.1 服务热线

若有需要，可随时拨打热线电话：400-995-1887

1.3.2 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金服技术支持团队。

工单提交地址：https://user.cloud.alipay.com/#/tickets/submit （工单说明）

2.微服务平台

2.1 系统组件说明

2.1.1 组件角色说明

微服务产品包括以下 4 个组件：

- **微服务控制台**：前端 Web 系统，提供所有图形界面化的操作。
- **注册中心**：主要提供所有服务注册信息的中心存储，同时负责将服务注册信息的更新通知实时推送给服务消费者。
- **定时任务**：提供统一通用的定时任务触发服务，提供定时任务的管理平台。
- **动态配置**：在分布式系统下为各应用的所有环境提供了一个中心化的外部配置，在不停应用集群的情况下，调整整个集群运行时的配置值。

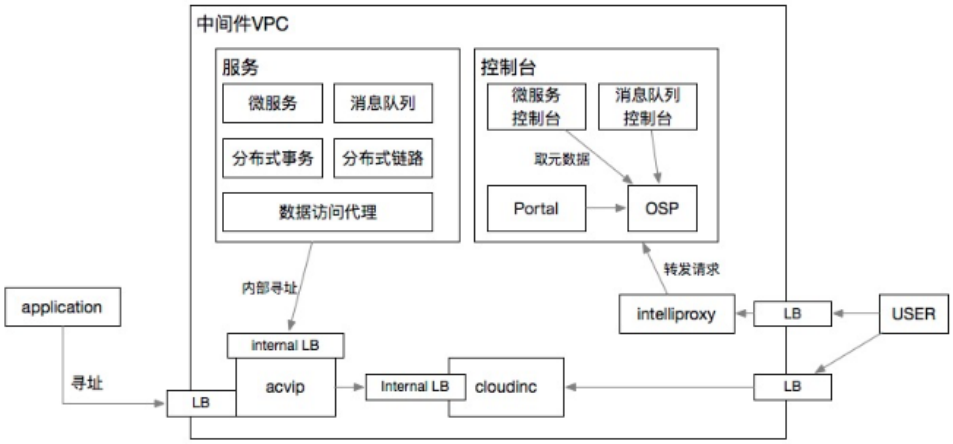
2.1.2 部署拓扑说明

微服务产品下主要有 4 个小集群提供服务。

- sessionserver 和 dataserver 组成的集群提供服务注册发现服务，每台 sessionserver 都单独绑定一个 AnyTunnelSLB。sessionserver、dataserver 和 metaserver 组成的集群提供服务注册发现服务。每台 sessionserver 都单独绑定一个 AnyTunnelSLB。关于 sessionserver、dataserver 和 metaserver 的具体说明，请参见 **注册中心 SOFA Registry** 章节内容。
- drmdata 集群提供动态配置服务，每台 drmdata 都单独绑定一个 AnyTunnelSLB。
- antscheduler 集群提供定时任务服务，目前定时任务触发需要依赖消息队列去通知应用。
- dsrconsole 集群是管理上述集群的控制台，提供友好的 UI 界面给开发者和管理员使用。

ACVIP，Intelliproxy 和 OSP 属于支撑产品。以下其他中间件产品都有使用，后面不再赘述。

- ACVIP 提供寻址功能，帮助应用获取微服务产品的访问 IP。
- OSP 提供租户实例信息。
- Intelliproxy 主要提供用户认证和权限校验功能。



2.1.2.1 资源清单说明

系统	服务器	服务器开放端口	LB 开放端口
sessionserver	2 台（4C8G，40G 磁盘）	9603，9600	9603，9600
dataserver	3 台（8C8G，40G 磁盘）	9602，9604，9606	N/A
drmdata	2 台（2C4G，40G 磁盘）	80，9870，9880	80 ， 9870 ，9880
antscheduler	2 台（2C4G，40G 磁盘）	9000，9001，12200	9001，12200
dsrconsole	2 台（2C4G，40G 磁盘）	80，8341，12200	80
dsrconsole	MySQL，1 台（2C4G，40G 磁盘）	N/A	N/A

2.2 监控和预警说明

2.2.1 监控指标和预警项说明

2.2.1.1 系统监管指标和预警项清单

监控指标	监控指标说明	预警项说明
dsrconsole 磁盘空间监控	磁盘空间占用率监控	预警触发条件：大于 80%
dsrconsole 内存监控	内存占用率	预警触发条件：大于 80%
dsrconsole CPU 利用率	CPU 利用率	预警触发条件：大于 80%
sessionserver 磁盘空间监	磁盘空间占用率监控	预警触发条件：大于 80%

监控指标	监控指标说明	预警项说明
控		
sessionserver 内存监控	内存占用率	预警触发条件：大于 80%
sessionserver CPU 利用率	CPU 利用率	预警触发条件：大于 80%
dataserver 磁盘空间监控	磁盘空间占用率监控	预警触发条件：大于 80%
dataserver 内存监控	内存占用率	预警触发条件：大于 80%
dataserver CPU 利用率	CPU 利用率	预警触发条件：大于 80%
drmdata 磁盘空间监控	磁盘空间占用率监控	预警触发条件：大于 80%
drmdata 内存监控	内存占用率	预警触发条件：大于 80%
drmdata CPU 利用率	CPU 利用率	预警触发条件：大于 80%
antscheduler 磁盘空间监控	磁盘空间占用率监控	预警触发条件：大于 80%
antscheduler 内存监控	内存占用率	预警触发条件：大于 80%
antscheduler CPU 利用率	CPU 利用率	预警触发条件：大于 80%

2.2.1.2 自定义监控指标和预警项清单

监控指标	监控指标说明	预警项说明
服务注册中心水位	水位包含服务注册中心当前注册服务数量，客户端连接数等	触发条件：单机客户端连接数超过 2000 订阅角色：运维管理员
服务注册中心内部长连接断连事件	内部长连接断开一般伴随有网络不稳定等情况，断连会触发一些修复性事件，需关注	触发条件：最近 1 分钟内断连超过 1 次 订阅角色：运维管理员
服务注册中心运行时列表变更及推送	运行时列表变更说明有节点宕机，触发集群自动剔除节点，需考虑替换故障节点	触发条件：出现集群列表变更 订阅角色：运维管理员
服务注册中心端口监控	服务注册中心 Session 角色 9600 可用状态	触发条件：9600 端口不可用 订阅角色：运维管理员
动态配置单机长连接数量	动态配置单机处理客户端长连接数量	N/A
动态配置集群长连接数量	动态配置当前集群处理客户端长连接数量	N/A
动态配置集群单机推送量	动态配置当前集群单机推送属性值变更总量，分钟级别	N/A
动态配置单机 QPS	动态配置服务端以 HTTP 形式	N/A

监控指标	监控指标说明	预警项说明
	返回数据，单机设计 QPS4000，超过此数据时需考虑扩容	
定时任务消息集群发送量	全集群消息的发送总量，分钟级别	触发条件： 1. 当前时间昨日同比下跌 20%； 2. 最近 5 分钟求和与上 5 分钟求和环比下跌超过 20%； 3. 最近 5 分钟求和 >10； 多个条件同时满足触发预警。 订阅角色：运维管理员
定时任务消息发送单机量	定时任务单机消息发送量，分钟级别	N/A
微服务服务端存活监控	服务端存活	触发条件：8341 端口不可用 订阅角色：运维管理员
服务注册中心服务端存活监控	服务端存活	触发条件：9600、9602 端口不可用 订阅角色：运维管理员
动态配置服务端存活监控	服务端存活	触发条件：9880、12200 端口不可用 订阅角色：运维管理员
定时任务服务端存活监控	服务端存活	触发条件：8080、12200 端口不可用 订阅角色：运维管理员

2.2.2 预警项运维动作说明

2.2.2.1 antscheduler 预警运维动作说明

预警项说明

- 基于消息的任务通过 MQ 发送消息，需要和 MQ 的服务器建立长连接，当 9529 端口没有正常的连接时，消息无法发送。
- 基于 RPC 的任务，客户端和服务端需要建立长连接，可以通过 9001 端口查看是否有客户端注册上来。

运维动作说明

- 如果 9529 端口没有连接，先确认 MQ 是否运行正常。如果 MQ 正常，查看 /home/admin/logs/common-error.log 日志，检查是否有和 MQ 建立连接失败的日志（例如“no available connection”）。如果没有任何信息，重启服务器再观察。
- 如果 9001 端口没有任何连接，可能因为没有客户端存在。如果客户端正常运行，可以查看/logs/auth-audit.log 日志，检查是否有客户端的注册信息。如果没有任何信息，说明客户端的注册请求没有发过来，需要查看客户端 /logs/scheduler/common-error.log 中注册失败的日志。

2.2.2.2 dsrconsole 预警运维动作说明

预警项说明

微服务控制台主要提供页面访问服务，主要关注 80、8341、12200 端口的健康状况。

运维动作说明

如以上端口不存活，重启应用即可。

2.2.2.3 drmdata 预警运维动作说明

动态配置主要依靠 9880 推送数据变更给客户端，客户端需要通过 9880 与服务端建立长连接。

如无客户端注册，可能 ACVIP 寻址配置有问题，需要检查 ACVIP 配置。

2.2.3 日常巡检项说明

2.2.3.1 antscheduler 系统监控指标巡检项目

巡检项说明

通过 **业务实时监控** 产品查看微服务产品各项系统监控指标。访问路径：产品与服务 > 业务实时监控 > 中间件云产品 > 微服务 > 定时任务。

运维动作说明

如果发现预警指标异常，根据对应预警项运维动作说明进行操作。

2.2.3.2 dsrconsole 系统监控指标巡检项目

巡检项说明

通过 **业务实时监控** 产品查看微服务产品各项系统监控指标。访问路径：产品与服务 > 业务实时监控 > 中间件云产品 > 微服务 > 注册中心。

运维动作说明

如果发现预警指标异常，根据对应预警项运维动作说明进行操作。

2.2.3.3 drmdata 系统监控指标巡检项目

巡检项说明

通过 **业务实时监控** 产品查看微服务产品各项系统监控指标。访问路径：产品与服务 > 业务实时监控 > 中间件云产品 > 微服务 > 动态配置。

运维动作说明

如果发现预警指标异常，根据对应预警项运维动作说明进行操作。

2.3 系统日志说明

2.3.1 日志文件清单说明

系统	日志文件名称	日志文件路径	日志文件描述
session-server	registry-session.log	/home/admin/logs/registry/session/registry-session.log	Session 注册的主要日志。服务发布和服务订阅，以及一些内部任务执行的日志都存在这个文件。
	registry-exchange.log	/home/admin/logs/registry/session/registry-exchange.log	Session 和其他角色交互的日志，比如是否发送 pub 到 dataserver 的日志等。
	registry-console.log	/home/admin/logs/registry/session/registry-console.log	Session 和 dsrconsole 的交互日志。此外，session 的 pub 和 sub 数量记录在这个日志。
	registry-connect.log	/home/admin/logs/registry/data/regi	Sesssion 连接日志，记录 session

系统	日志文件名称	日志文件路径	日志文件描述
		stry-connect.log	和 dataserver 之间的连接、session 和客户端的连接、session 和 meta 的连接变更等。
	gc.log	/home/admin/logs/gc.log	GC 日志
data-server	registry-data.log	/home/admin/logs/registry/data/registry-data.log	Dataserver 的主要日志，data 服务注册，以及内存变更和数据备份都集中记录在这个日志。
	registry-connect.log	/home/admin/logs/registry/data/registry-connect.log	Dataserver 连接日志，主要记录 dataserver 之间的连接，以及 dataserver 和 session、meta 的连接变更等。
	gc.log	/home/admin/logs/gc.log	GC 日志
meta-server	registry-meta.log	/home/admin/logs/registry/meta/registry-meta.log	Metaserver 的主要日志，记录 data 和 session 节点 IP 注册过程。
	registry-raft.log	/home/admin/logs/registry/meta/registry-raft.log	Metaserver 接入 jraft 选举过程的主要日志
	registry-connect.log	/home/admin/logs/registry/meta/registry-connect.log	Metaserver 和其他节点连接的日志
	gc.log	/home/admin/logs/gc.log	GC 日志
dsrconsole	common-error.log	/home/admin/logs/dsrconsole/common-error.log	系统错误日志
drmdata	common-error.log	/home/admin/logs/drmdata/common-error.log	系统错误日志
	app-auth.log	/home/admin/logs/drmdata/app-aut	业务系统访问 drmdata 的授权信息，只有通过授权的系统

系统	日志文件名称	日志文件路径	日志文件描述
		h.log	才能访问 drmdata 获取配置信息。 说明：授权是针对 instanceId。
	drmdata-container.log	/home/admin/logs/drmdata/drmdata-container.log	客户端向服务端注册信息。 说明：客户端通过向服务端注册长连接来监听配置变更事件。
	drmdata-default.log	/home/admin/logs/drmdata/drmdata-default.log	系统打印的所有的日志信息，包含 INFO、WARNING、ERROR 日志。
	drmdata-heartbeat.log	/home/admin/logs/drmdata/drmdata-heartbeat.log	客户端心跳信息。 客户端定时每隔 30s 向 drmdata 上报所使用的所有配置项的版本信息，服务端检查客户端上报的配置版本，如果落后则通知客户端更新对应配置。 日志样例： Y;0ms;GZ00B;UX8YY6AL9CHS;100.81.77.9;240;0;bolt 字段说明： • Y/N：此次心跳检查是否正常。 • 0ms：检测耗时。 • GZ00B:客户端所属单元。 • UX8YY6AL9CHS：instanceId 信息。 • 100.81.77.9：客户端 IP。 • 240：此次心跳客户端携带的配置数。 • 0:此次心跳检测出客户端配置版本落后的数量。 • bolt：心跳检测来源。
	drm-monitor.l	/home/admin/logs	drmdata 维护的长连接信息。

系统	日志文件名称	日志文件路径	日志文件描述
	og	/drmdata/drm-monitor.log	**日志样例**: [monitorZone]11;DEFAULT_ZONE;4;32;3; **字段说明**: • [monitorZone]：zone 维度监控 • 11：总连接数 • DEFAULT_ZONE：名称 • 4：instanceId 数量 • 32：配置项数 • 3：当前 zone 的连接数
	drmdata-push.log	/home/admin/logs/drmdata/drmdata-push.log	配置变更时，drmdata 向客户端推送变更信息日志。 **字段说明**: [push]{instanceId};{配置项};{客户端 IP};{0(推送成功)/1(推送失败)}
	drmdata-sync.log	/home/admin/logs/drmdata/drmdata-sync.log	drmdata 集群间同步配置信息。
	drmdata-threadpool.log	/home/admin/logs/drmdata/drmdata-threadpool.log	drmdata 所有线程池监控信息。 **字段说明**: {线程池名称},{队列中的任务数},{活跃线程数},{空闲线程数},{总线程数}
antscheduler	rpc-client.log	/home/admin/logs/antscheduler/rpc-client.log	客户端连接日志
	rpc-server.log	/home/admin/logs/antscheduler/rpc-server.log	服务端连接事件日志
	rpc-slave.log	/home/admin/logs/antscheduler/rpc-slave.log	其他服务端建立连接日志

系统	日志文件名称	日志文件路径	日志文件描述
	job-rpc.log	/home/admin/logs/antscheduler/job-rpc.log	RPC 任务执行日志
	job-msg.log	/home/admin/logs/antscheduler/job-msg.log	MSG 任务执行日志
	job-dispatch.log	/home/admin/logs/antscheduler/job-dispatch.log	任务分配日志
	monitor.log	/home/admin/logs/antscheduler/monitor.log	监控日志
	common-error.log	/home/admin/logs/antscheduler/common-error.log	异常日志
	antscheduler-default.log	/home/admin/logs/antscheduler/antscheduler-default.log	启动日志

2.3.2 异常日志运维动作说明

系统	日志文件名称	报错内容	日志文件描述
-	-	get server list error	客户端未拿到服务端地址列表，可能是服务端寻址配置有误。
-	-	Register task schedule error	客户端注册发布或订阅任务失败，可以确认下是否注册过于频繁。
-	-	SubscriberNotifyTask execute error, dataId:	订阅数据回调任务执行出错，可以根据异常信息查看下回调方法内是否有处理错误。
-	-	ConfiguratorNotifyTask execute error	配置数据回调任务执行出错，可以根据异常信息查看下回调

系统	日志文件名称	报错内容	日志文件描述
			方法内是否有处理错误。
-	-	Failed trying connect to {}	尝试与服务端建立连接失败，服务端可能有问题。
-	-	add notify task error, dataId: {}, registId: {}	回调任务加入线程池失败，需要确认回调线程池配置是否过小，没有能力消费掉服务端的推送。
drmserver	/home/admin/logs/drm/common-error.log	Query zdrmdata server address empty	未能从 ACVIP 获取到 zdrmdata 服务地址，检查 ACVIP 地址设置是否正确。。
data-server	decision.60dt.log	/home/admin/logs/confreg-data/decision.60dt.log	Data 集群踢节点日志，当有故障节点出现时，主节点会剔除故障节点并分发列表给所有 Session、Data 节点。
antscheduler	/home/admin/logs/antscheduler/rpc-server.log	client[xxx:xxx] has no auth	客户端没有权限，查看客户端的 accessKey 和 securityKey 配置是否正确
	/home/admin/logs/antscheduler/rpc-server.log	client register failed	客户端注册时发生异常，可以查看堆栈信息了解异常原因
	/home/admin/logs/antscheduler/job-rpc.log	no targets was found	查看客户端注册情况
	/home/admin/logs/antscheduler/job-msg.log	xxx,xxx,xxx,xx, failed	发送消息失败，检查消息订阅关系是否生效

2.3.3 日常巡检项说明

查看微服务相关应用资源和存储资源。访问路径：产品与服务 > 发布部署服务 > 应用 >

dsrconsole/session-server/data-server/drmdata/scheduler

2.4 常见运维场景说明

2.4.1 服务注册中心（sessionserver/dataserver/metaserver）日常问题

- **服务注册中心 Session 节点宕机**

  服务注册中心 Session 部分节点宕机不影响集群稳定性，仅需关注宕机后替换故障节点即可。

- **服务注册中心 Data 节点宕机**

  a) 服务注册中心 Data 节点需 1/2 以上存活来保障服务可用性，部分节点宕机集群可自动剔除故障节点并转移数据，但需要确保有 1/2 以上可用节点存活。

  b) Data 节点扩容：可以逐个加入新机器达到 working 状态。

- **服务注册中心 Meta 节点宕机**

  服务注册中心 Meta 节点有 1/2 以上存活则不影响集群使用，仅需关注宕机后替换故障节点即可。

- **动态配置节点宕机**

  a) 动态配置部分节点宕机无实际影响，客户端会主动重试连接可用节点；

  b) 重启或扩容后，需确保服务启动成功，数据源连接正确，端口 9880 存活。

- **定时任务服务端节点宕机**

  a) 定时任务单实例宕机理论上无实际业务影响，单机故障排除后进行应用重启；

  b) 重启后，确认 logs/antscheduler/common-error.log 无报错，logs/health-check/common-error.log 无报错，任务分配正常，表明启动正常。

2.4.2 定时任务（antscheduler）日常问题

- **基于 msg 定时任务配置完成后收不到触发**

  a) 检查环境配置项 ACVIP .endpoint 和 instanceId 是否正确按照对应环境进行了配置；

  b) 检查代码中的 Eventcode 是否和定时任务控制台、消息中心控制台一致，消息中心

控制台的消息类型及订阅关系是否完整配置并且触发生效；

c) 排查机器日志 logs/tracelog/msg-sub-digest.log，确认是否有收到消息。如果收到了消息，表明任务已经触发，只是业务日志没有打印或者没有执行业务，需要排查代码对应片段进行分析。

- **基于 msg 定时任务没有按照频率触发**

a) 定时任务依赖消息队列投递，消息队列对于客户端处理超时或者失败的场景会自主发起重试。

b) 如果业务机器收到定时任务消息后抛出异常或者由于集群资源有限，消息处理超时，消息队列会发起重试。

c) 排查机器日志 logs/tracelog/msg-sub-digest.log，格式如下。其中，逗号分隔的倒数第三位表示这条消息的投递次数，如果大于 0，表明当前的消息是重试消息。

```
2014-06-19
20:13:33.734,,0ad1348f14031800144081003,0.1.d6502e1f,6fafc0
9cd670fa39a802626ab1aab2b0,1e4cf860680dad989dceec17f1adb837
, NOTIFYTEST,sofa30,P-P-helloworld-pub-group,01,1094B,5ms,m
sgbroker.rz00b.alipay.net,0,msgWorkTP-6646123-1-thread-1,ma
rk=T&uid=a2&
```

d) 如果发现重试消息，可以将对应定时任务频率降低甚至暂停，待重试消息消化完成后，手动触发，确认是由于业务异常导致的必现重试，还是由于频率过高导致的处理能力不足。

- **基于 RPC 定时任务配置后接收不到触发请求**

如果是 CALLBACK 类型，查看触发记录和执行记录是否成功。如果是 ONEWAY 类型，先改成 CALLBACK 类型再触发试试。一般情况这个问题是由于客户端和服务端没有成功连接导致。

- **服务节点宕机**

服务节点宕机，直接重启即可。宕机后其负责的任务会被分配给其他机器，在未重新分配之前这段时间内需要触发的任务会出现漏触发情况。

2.4.3 动态配置（drmdata）日常问题

- **应用发布后控制台无法查看到订阅者列表**

a) 确定 ACVIP .endpoint 配置是否正确，实例标识是否正确。

b) 排查客户端业务应用日志（非 drmdata 机器日志）logs/drm/drm-boot.log 中注册

的动态配置标识是否与控制台属性对应的配置标识一致。

c) 执行以下命令，排查客户端业务应用日志（非 drmdata 机器日志）logs/drm/drm-monitor.log 中配置资源是否注册成功。

```
grep "register success"
```

2.5 服务巡检

2.5.1 系统组件监控检查

2.5.1.1 基础监控检查

登录 corewatch 监控系统，查看微服务（MS）相关系统组件有无异常告警，需要关注的监控项内容如下表所示。

应用	分类	指标（关键字）	告警阈值
MS-antscheduler MS-antschedulerconsole MS-drmdata MS-dsrconsole	基础监控-cpu 使用率监控	cpu_usage	>80%
	基础监控-内存使用率监控	mem_usage	>80%
	基础监控-磁盘使用率监控	disk_usage	>80%
	基础监控-load5	load5	>3
MS-antscheduler	基础监控-端口监控	2022 12200	不通
MS-antschedulerconsole	基础监控-端口监控	8080 12200	不通
MS-drmdata	基础监控-端口监控	2022 9880 12200	不通
MS-dsrconsole	基础监控-端口监控	80 2022 8341 12200	不通

2.5.1.2 自定义业务监控检查

通过 corewatch 内核态监控产品查看注册中心产品各项系统监控指标是否有异常告警产生。访问路径：corewatch > 自定义监控 > 共享中间件 > MicroService > registry。

如果有异常告警产生，联系蚂蚁金服技术支持进行排查。

2.5.2 业务功能检查

1. antscheduler 服务验证

如果需要使用基于消息的功能，需要依赖 msgbroker。此时可执行以下命令，检查是否与 msgbroker 建立连接。

```
netstat -an|grep 9529
```

2. 访问 sofa-ms.{domain} 页面，检查各页面是否能正常访问无报错。

2.6 服务异常应急预案

2.6.1 概述

适用范围

底座	产品版本
Antstack	1.0 - 1.3

问题描述或者背景

- 定时任务触发失败
- 动态配置推送失败

2.6.2 环境检查

1. 登录云游，检查 antscheduler，drmdata 容器状态（运行中、重启中、升级中、异常、已下线、待升级等）。
2. 登录监控页签，检查 antscheduler，drmdata 端口 9001、9880 是否在监听。

2.6.3 实施步骤

1. 如果容器为运行中状态，webshell 进入容器，执行以下命令，检查 antscheduler、drmdata 服务状态。

```
#ps -fe | grep java
```

2. 如果容器为节点异常状态，判断是否存在物理机宕机。如果是，则参考 物理机宕机应急预案 对故障物理机上运行的容器进行宕机迁移，并在新宿主机上启动容器。
3. 如果容器为已下线状态，可以在云游上启动 antscheduler、drmdata 容器。

2.6.4 结果验证

1. 手工触发消息、RPC 定时任务成功，并且消息消费端可以成功接收到消息。
2. 在 drm 控制台，找到一个可以测试的 dataid 进行手工推送，确认消息可以成功推送到消息订阅端。

2.6.5 回滚方案

无

2.6.6 补充说明

无

3.共享型分布式数据源管理

3.1 监控和预警指标说明

3.1.1 系统监控

分类	指标（关键字）	报警阈值	采集间隔	连续时间	描述	如何处理警报
CPU 使用情况监控	CPU 使用率	> 60%	1 分钟	**3 分钟**	CPU 使用情况监控，目前设置监控阈值为 60%	重启 ddsconsole 应用容器
内存使用监控	mem_usage	> 90%	1 分钟	1 分钟	内存使用情况监控，目前设置监控阈值为 90%	重启 ddsconsole 应用容器
磁盘使用情况监控	磁盘使用情况	> 95%	1 分钟	1 分钟	磁盘使用情况监控，目前设置监控阈值为 95%	清除日志目录中无效的日志文件
端口监测	8341,9500,80,2022	无	1 分钟	1 分钟	端口监控，警告	重新启动或更换容器

3.1.2 自定义监控

DS	dds_datasource_error	DDS 的数据库已打开。
	drm_push_error	查看常见错误日志，查看具体原因；.confreg / config.client.blog.log 查看是否获得 DRM 的推送接口地址。

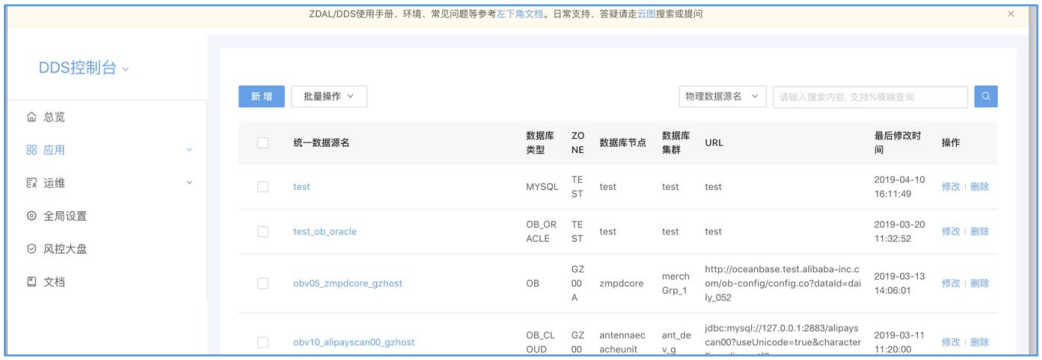
3.2 关键日志内容说明

应用	日志文件名	日志文件路径	日志文件描述
ddsconsole	zdal-datasource.log	/home/admin/logs/ddsconsole/zdal/	数据库链接日志
	common-error.log	/home/admin/logs/ddsconsole/	错误日志

3.3 常见运维场景和操作说明

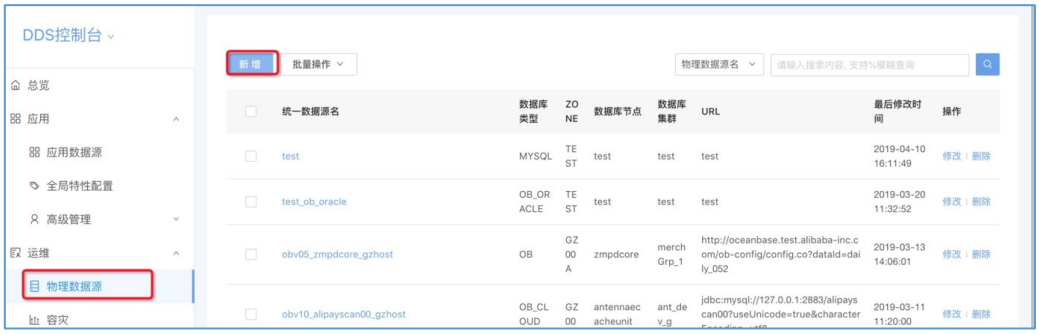
3.3.1 数据源配置检查

1. 登录环境的控制台地址，然后单击左列中的每个页面以查看它是否正常（验证 DDS 本身）。



2. 转到物理数据源页面并插入新的数据源配置以查看是否正常(验证入口并依赖 DRM 服务)。

3. MYSQL #test #test #TEST #test #test #test # 44f256cb54d2d275 跳过链接检查。



3.4 服务异常应急预案

3.4.1 概述

适用范围

底座	产品版本
Antstack	1.0 - 1.3

问题描述或者背景

- 定时任务触发失败
- 动态配置推送失败

3.4.2 环境检查

1. 登录云游，检查 antscheduler，drmdata 容器状态（运行中、节点宕机、退出）。
2. 登录监控页签，检查 antscheduler，drmdata 端口 9001、9880 是否在监听。

3.4.3 实施步骤

1. 如果容器为运行中状态，webshell 进入容器，执行以下命令，检查 antscheduler、drmdata 服务状态。

```
#ps -fe | grep java
```

2. 如果容器为节点宕机状态，判断是否存在物理机宕机。如果是，则参考 物理机宕机应急预案 对故障物理机上运行的容器进行宕机迁移，并在新宿主机上启动容器。
3. 如果容器为退出状态，可以在云游上启动 antscheduler、drmdata 容器。

3.4.4 结果验证

1. 手工触发消息、RPC 定时任务成功，并且消息消费端可以成功接收到消息。
2. 在 drm 控制台，找到一个可以测试的 dataid 进行手工推送，确认消息可以成功推送到消息订阅端。

3.4.5 回滚方案

无

3.4.6 补充说明

无

4.消息队列

4.1 系统组件说明

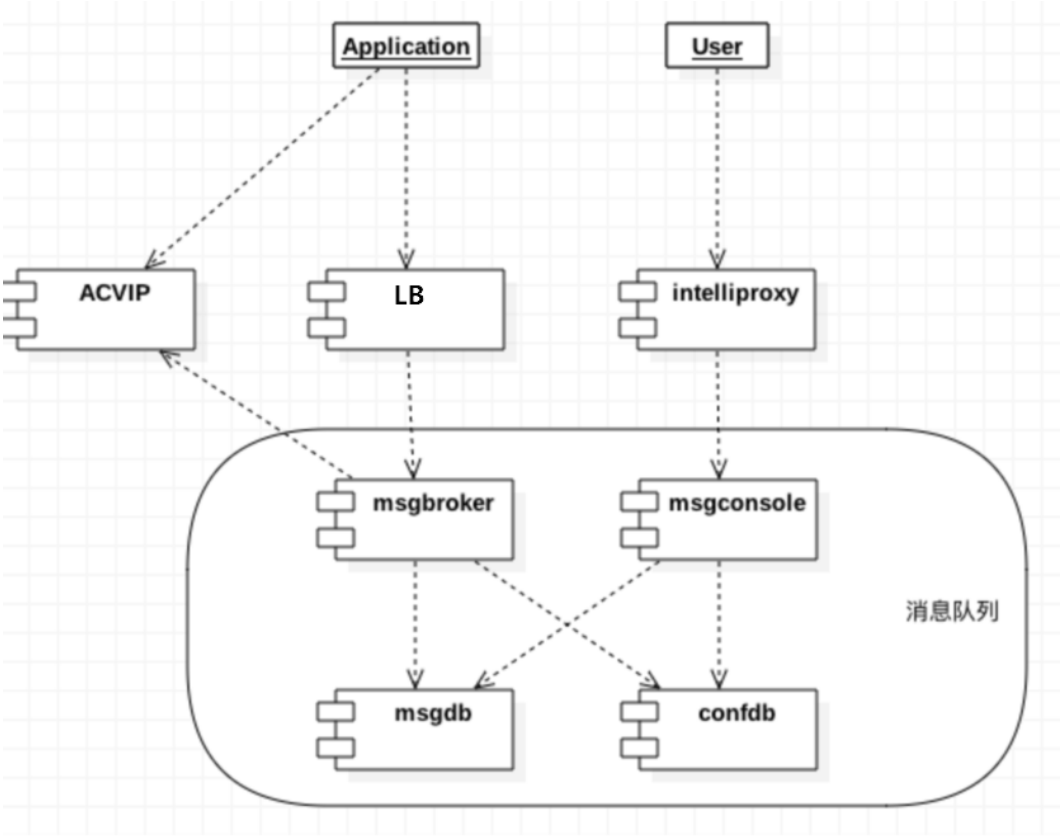
4.1.1 组件角色说明

消息队列产品包括以下 4 个组件：

- **消息队列 Broker**：网络应用 server，负责接收消息生产者应用系统发布的消息对象，并将消息对象投递到消息消费者应用系统。
- **消息队列控制台**：Web 应用系统，核心功能是提供消息队列元数据配置功能；同时提供一组功能满足用户使用消息队列产品的各项需求，例如消息对象数据属性查询等。
- **消息对象存储**：关系型数据库，存储消息对象数据。
- **消息队列元数据存储**：关系型数据库，存储消息队列元数据。

4.1.2 部署拓扑说明

- **消息队列 Broker**：应用名 msgbroker。
- **消息队列控制台**：应用名 msgconsole。
- **消息对象存储**：数据库实例名 msgdb。
- **消息队列元数据存储**：数据库实例名 confdb。
- **ACVIP**：SOFA 中间件云产品服务发现组件。
- **LB**：用于 VPC 环境下作为消息队列 Broker 服务节点的网络暴露。
- **Intelliproxy**：SOFA 中间件云产品网关组件。
- **Application**：用户应用系统。
- **User**：用户浏览器。



4.1.3 资源清单说明

系统	资源依赖	服务端口
消息队列 Broker	4 * 服务器 (4 CPU, 8G 内存, 100G 磁盘)	9529
消息队列控制台	2 * 服务器 (2 CPU, 4G 内存, 100G 磁盘)	80
消息对象存储	2 * RDS (4 CPU, 8G 内存, 200G 磁盘)	3306
消息队列元数据存储	1 * RDS (1CPU, 2G 内存, 200G 磁盘)	3306

4.2 监控和预警说明

4.2.1 监控指标和预警项说明

4.2.1.1 系统监控指标和预警项清单

监控指标	监控指标说明	预警项说明
消息队列 broker 磁盘空	磁盘空间占用率监控	预警触发条件:大于 80%

监控指标	监控指标说明	预警项说明
间监控		
消息队列 broker 端口监控	端口 “9529” 是否可以访问	预警触发条件：端口 9529 无法访问
消息队列 broker 内存监控	内存占用率	预警触发条件：大于 80%
消息队列 broker CPU 利用率	CPU 利用率	预警触发条件：大于 80%
消息队列控制台 磁盘空间监控	磁盘空间占用率监控	预警触发条件：大于 80%
消息队列控制台 端口监控	端口 “80” 是否可以访问	预警触发条件：端口 80 无法访问
消息队列控制台 内存监控	内存占用率	预警触发条件：大于 80%
消息队列控制台 CPU 利用率	CPU 利用率	预警触发条件：大于 80%

4.2.1.2 自定义监控指标和预警项清单

监控指标	监控指标说明	预警项说明
消息队列_接收消息数量_逻辑实例	统计消息队列接收到的发布者应用发布的消息数量，按照逻辑实例分组统计。	预警触发条件：每分钟超过 4000 条。
消息队列_接收消息数量_逻辑实例_失败	统计消息队接收的失败消息数量，当监控数大于 0 时，一般由以下两种场景导致： • 存储资源出现不可用异常。 • 消息类型没有在控制台配置。	预警触发条件：每分钟超过 0 条。
消息队列_投递消息数量_逻辑实例_成功	统计消息队列投递到订阅者应用的消息数量，按照逻辑实例分组统计。	预警触发条件：每分钟超过 4000 条。
消息队列_投递消息数量_异常类型	统计消息队列投递失败的消息数量，按照逻辑实例、消息类型、订阅者 group 和异常类型维度分类统计。	预警触发条件：每分钟超过 0 条。
消息队列_Broker_心	消息队列 Broker 服务实例监控自	预警触发条件：每分

监控指标	监控指标说明	预警项说明
跳健康	检，默认每分钟输出 12 条心跳日志，如果统计数小于 6，一般是由于服务实例异常导致。	钟少于 6 条。

4.2.2 预警项运维动作说明

4.2.2.1 消息队列 broker 端口预警项

预警项说明

消息队列 broker 网络服务端口号是 9529，当此端口无法通过网络访问时，消息发布者应用系统和消息消费者”应用系统都无法正常连接到消息队列 broker。

运维动作说明

- 通过预警项说明，确定端口异常的消息队列 broker 服务器地址，一般是服务器 IP 地址。
- 登录异常消息 broker 服务器，并执行以下命令，确认端口服务是否存在。

```
netstat -ano | grep LISTEN | grep 9529
```

- 如果服务端口 9529 确实未提供服务，说明预警准确，需要执行以下命令，进一步确定消息队列 broker 服务进程是否存在。如果进程不存在，则确认是服务实例宕机，需要重新启动服务实例。

```
ps -ef | grep java
```

4.2.3 日常巡检项说明

4.2.3.1 系统监控指标巡检项目

巡检项说明

通过 **业务实时监控** 产品查看消息队列产品各项系统监控指标。访问路径是：产品与服务 > 业务实时监控 > 自定义。

运维动作说明

如果发现预警指标异常，根据对应的预警项运维动作说明进行操作即可。

4.3 系统日志说明

4.3.1 日志文件清单说明

4.3.1.1 Broker 系统日志文件清单

日志文件名称	日志文件路径	日志文件描述
common-error.log	/home/admin/logs/common-error.log	系统错误日志
msgbroker-ha-heartbeat.log	/home/admin/logs/msgbroker-ha-heartbeat.log	系统健康自检日志
msgbroker-datasource-healthy.log	/home/admin/logs/msgbroker-datasource-healthy.log	消息对象存储数据源健康日志
msgbroker-receive-digest.log	/home/admin/logs/msgbroker-receive-digest.log	消息对象接收日志
msgbroker-finish-digest.log	/home/admin/logs/msgbroker-finish-digest.log	消息对象投递成功日志
msgbroker-dispatcher-failure.log	/home/admin/logs/msgbroker-dispatcher-failure.log	消息对象投递失败日志
msgbroker-dispatcher-neglect.log	/home/admin/logs/msgbroker-dispatcher-neglect.log	消息对象投递忽略日志

- **系统健康自检日志**：msgbroker-ha-heartbeat.log

  记录应用系统健康自检心跳日志，每 5 秒输出一次，可以用来验证应用系统进程是否正在运行，日志示例如下：

  ```
  2018-05-31 17:02:14,434 - ServerHAHeartbeat result [OK] meta
  [ServerHAHeartbeatMeta[hostname=dms-1-1,ip=100.81.70.213]]
  ```

- **消息对象存储数据源健康日志**：msgbroker-datasource-healthy.log

  日志示例如下：

  ```
  2018-05-22 11:07:17,897 - Validate data source healthy, status
  [SUCCESS] url
  [jdbc:mysql://rdsfpia08qfaos3at48o6.mysql.jiuzhou.cloud.aliyun
  -inc.com:3306/msgdb?characterEncoding=utf8&connectTimeout=1000
  &autoReconnectForPools=true&socketTimeout=30000]
  ```

- **消息对象接收日志**：msgbroker-receive-digest.log

记录消息对象接收日志，**Y** 字段说明消息接收成功，日志示例如下：

```
2018-05-31 17:07:38,907 -
[(TP F SC,EC CALLBACK,Y,A92375EEE5858C29C5BB28E7F32D6226,908c3
094334272a5845073adc9b9887a,ifcfluxbatch-1-1,P fcfluxbatch dyn
amic task,1,R,2,2,611,dms-1-1-msgdb,64514a5515277576589056997,
0,-)]
```

- **消息对象投递成功日志**：msgbroker-finish-digest.log

  记录消息对象投递成功日志，日志示例如下：

```
2018-05-31 17:09:15,214 -
[(A0078B2A70CFF156FAD2065C8D16AA6D,TP S 1301,EC EVENTLOG 3001,
S_FCDATABUS_INPUT@100.81.77.10@1527757755214,1)]
```

4.3.2 异常日志运维动作说明

4.3.2.1 消息队列 Broker 系统错误日志异常

登录对应 Broker 服务器，查看 common-error.log 日志内容。

4.3.3 日常巡检项说明

4.3.3.1 Broker 系统错误日志巡检项目

巡检项说明

检查 Broker 系统错误日志。

运维动作说明

登录对应 Broker 服务器，查看 common-error.log 日志内容。

4.4 常见运维场景说明

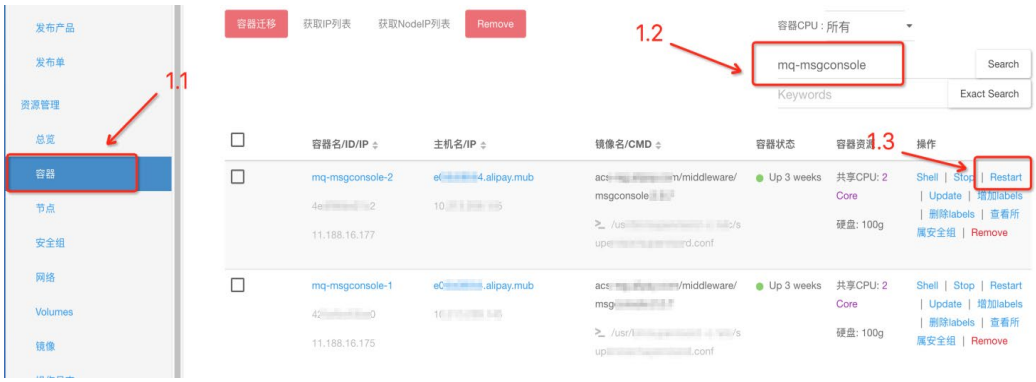
4.4.1 消息队列控制台服务实例宕机

根据监控项 **消息队列控制台端口监控** 预警，发现服务实例进程异常，可通过以下操作步骤重启宕机服务实例。

1. 登录云游，选择 **容器**。

2. 在搜索栏中，搜索 mq-msgconsole。

3. 点击 **Restart**，重启宕机控制台服务实例。



4.4.2 消息队列 Broker 服务实例宕机

根据监控项 **消息队列 broker 端口监控** 预警，发现服务实例进程异常，可通过以下操作步骤重启宕机服务实例。

1. 登录云游，选择 **容器**。

2. 在搜索栏中，搜索 mq-msgbroker。

3. 点击 **Restart**，重启宕机服务实例。

4.4.3 消费者消费消息异常

1. 在 **业务实时监控** 控制台，单击左侧导航栏上的 **自定义** 菜单。

2. 依据监控项 **订阅者消息投递异常分类**，发现异常的消息类型和订阅者 group。

3. 立即通知订阅者应用系统 owner 排查消息消息异常原因。

4.4.4 消息队列接收消息异常

1. 根据监控项 **消息队列接收失败消息数量**，预警发现消息队列出现消息接收失败，初步可推测是存储资源出现不可用状态。

2. 登录消息队列 broker 服务器，查看以下两个日志，确认存储资源异常的具体原因。

```
/home/admin/logs/msgbroker-datasource-healthy.log
/home/admin/logs/msgbroker-server-persistenceManager.log
```

4.4.5 消息队列积压消息

消息队列投递消息失败的场景下，消息就积压在消息队列中，一般是由于订阅者应用消费异常导致，比如订阅者不在线，订阅者消息消费异常，订阅者主动回滚消息。

1. 在 **业务实时监控** 控制台，单击左侧导航栏上的 **自定义** 菜单。
2. 根据监控项 **订阅者消息投递异常分类**，根据监控项中的订阅者 group 值，确认具体的消费消息异常的消息订阅者和原因。
3. 立即通知消息订阅者应用负责人排查异常原因并解决。
4. 根据监控项 **订阅者消息投递异常分类**，跟踪具体的消息异常数量，直至恢复正常。

4.5 服务巡检

4.5.1 系统组件监控检查

4.5.1.1 基础监控检查

登录 corewatch 监控系统，查看消息队列（MQ）相关系统组件有无异常告警，需要关注的监控项内容如下表所示。

应用	分类	指标(关键字)	告警阈值
MQ-msgbroker MQ-msgconsole	基础监控-cpu 使用率监控	cpu_usage	>80%
	基础监控-内存使用率监控	mem_usage	>80%
	基础监控-磁盘使用率监控	disk_usage	>80%
	基础监控-load5	load5	>3
MQ-msgbroker	基础监控-端口监控	2022 9529	不通
MQ-msgbroker	基础监控-端口监控	80 2022	不通

4.5.1.2 自定义业务监控检查

通过 corewatch 内核态监控产品查看注册中心产品各项系统监控指标是否有异常告警产生。访

问路径是：corewatch > 自定义监控 > 共享中间件 > MQ。

如果有异常告警产生，联系蚂蚁金服技术支持进行排查。

4.5.2 业务功能检查

1. msgconsole 服务验证
   - 执行以下命令，判断 ACVIP 连接。

     ```
     netstat -an|grep 9003
     ```

   - 执行以下命令，判断注册中心连接。

     ```
     netstat -an|grep 9600
     ```

   - 执行以下命令，如果返回 passed:true，表示进程服务正常。

     ```
     curl 127.0.0.1:9500/checkService
     ```

   - 访问 sofa-mq.{domain} 页面，检查是否能正常访问。
2. msgbroker 服务验证

   执行以下命令，检查是否 9529 端口有监听。

   ```
   netstat -an | grep 9529
   ```

4.5.3 消息积压检查

消息队列投递消息失败的场景下，消息会积压在消息队列中，一般是由订阅者应用消费异常导致，例如订阅者不在线、订阅者消息消费异常、订阅者主动回滚消息。

- 根据监控项 **订阅者消息投递异常分类** 以及监控项中的订阅者 group 值，确认具体的消费消息异常的消息订阅者和原因。
- 通知消息订阅者应用负责人排查异常原因并解决。
- 根据监控项 **订阅者消息投递异常分类**，可以追踪具体的消息异常数量，直至恢复正常。

4.6 服务异常应急预案

4.6.1 概述

适用范围

底座	产品版本
Antstack	1.0 - 1.3

问题描述或者背景

当出现大面积消息投递失败的情况。

风险说明

msgbroker 高负载会导致消息积压，最终影响投递时间。

4.6.2 环境检查

1. 登录云游，检查所有 msgbroker 容器状态（运行中、节点宕机、退出）。
2. 登录监控页签，查看 msgbroker 端口 9529 是否正在监听。
3. 执行以下命令，检查 msgbroker 与 db 的连接状态。

```
#netstat -an | egrep "3306|2884"
```

4.6.3 实施步骤

1. 如果容器为运行中状态，webshell 进入容器，执行以下命令，检查 msgbroker 服务状态。

```
#ps -fe | grep java
```

2. 如果容器为节点宕机状态，判断是否存在物理机宕机。如果是，则参考 物理机宕机应急预案 对故障物理机上运行的容器进行宕机迁移，并在新宿主机上启动容器。
3. 如果容器为退出状态，可以在云游上直接启动 msgbroker 容器。

4.6.4 结果验证

1. 所有 msgbroker 容器状态为运行中。
2. 所有 msgbroker 进程状态正常，TCP 端口 9529 正常监听。

4.6.5 回滚方案

无

4.6.6 补充说明

如果遇到消息积压，需要联系蚂蚁金服金融科技技术支持处理。

5.分布式事务

5.1 系统组件说明

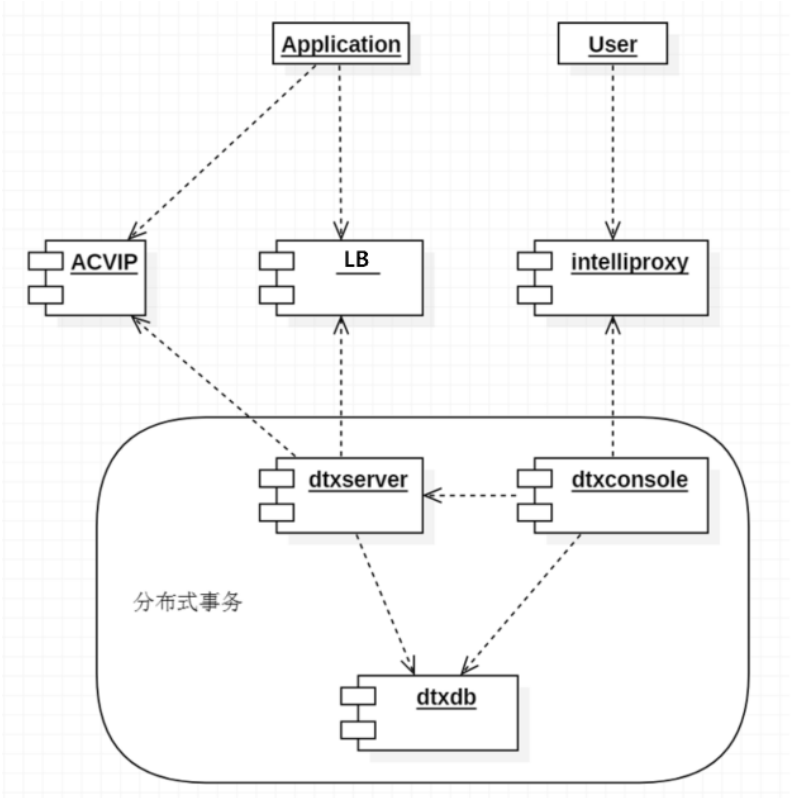
5.1.1 组件角色说明

分布式事务产品包括以下 3 个组件：

- **分布式事务管理器：**分布式事务应用 server，负责接收事务消息，并协调事务发起方和参与方完成整个分布式事务。
- **分布式事务控制台**：Web 应用系统，负责提供分布式事务日志数据的查询和分析。
- **分布式事务数据存储**：关系型数据库，存储分布式事务元数据、分布式事务事务日志数据。

5.1.2 部署拓扑说明

- **分布式事务管理器**：应用名 dtxserver。
- **分布式事务控制台**：应用名 dtxconsole。
- **分布式事务数据存储**：数据库实例名 dtxdb。
- **ACVIP**：SOFA 中间件云产品服务发现组件。
- **LB**：用于 VPC 环境下作为分布式事务管理器服务节点的网络暴露。
- **Intelliproxy**：SOFA 中间件云产品网关组件。
- **Application**：用户应用系统。
- **User**：用户浏览器。



5.1.3 资源清单说明

组件	资源依赖	服务端口
分布式事务管理器	2 * 服务器 (2 CPU，4G 内存，100G 磁盘) 需要根据具体业务量评估实例数	14200
分布式事务控制台	2 * 服务器 (2 CPU，4G 内存，100G 磁盘)	80
分布式事务数据存储	1 * RDS(4 CPU，8G 内存，200G 磁盘)	3306

5.2 监控和预警说明

5.2.1 监控指标和预警项说明

5.2.1.1 系统监控指标和预警项清单

监控指标	监控指标说明	预警项说明
分布式事务管理器 磁盘空间监控	磁盘空间占用率监控	预警触发条件：大于 80%
分布式事务管理器 端口监控	端口 14200 是否可以访问	预警触发条件：端口 14200 无法访问
分布式事务管理器 内存监控	内存占用率	预警触发条件：大于 80%

监控指标	监控指标说明	预警项说明
分布式事务管理器 CPU 利用率	CPU 利用率	预警触发条件：大于 80%
分布式事务控制台 磁盘空间监控	磁盘空间占用率监控	预警触发条件：大于 80%
分布式事务控制台 端口监控	端口 80 是否可以访问	预警触发条件：端口 80 无法访问
分布式事务控制台 内存监控	内存占用率	预警触发条件：大于 80%
分布式事务控制台 CPU 利用率	CPU 利用率	预警触发条件：大于 80%

5.2.1.2 自定义监控指标和预警项清单

监控指标	监控指标说明	预警项说明	报警级别
事务积压数量	未决事务积压数量，一般由于参与方系统异常导致积压	>10	重大
		>6	次要
整体异常数量	分布式事务系统整体每分钟异常数量	>10	重大
		>6	次要
事务二阶段失败数量	分布式事务每分钟二阶段执行失败的数量	>5/min	重大
		>3/min	次要
数据库访问耗时监控	分布式事务系统每分钟访问数据库平均耗时	>10ms	重大
		>7ms	次要
服务耗时监控	分布式事务提供的服务接口每分钟平均耗时	一阶段接口 > 15ms 二阶段接口 > 200ms	重大
		一阶段接口 > 10ms 二阶段接口 > 150ms	次要

5.2.2 预警项运维动作说明

5.2.2.1 分布式事务管理器 端口预警项

预警项说明

分布式事务管理器 网络服务端口号是 14200，当此端口无法通过网络访问时，分布式事务发起方和分布式事务参与方应用系统都无法正常连接到分布式事务管理器。

运维动作说明

- 通过预警项说明，确定端口异常的分布式事务管理器服务器地址，一般是服务器 IP 地址。
- 登录异常分布式事务管理器服务器，并执行以下命令，确认端口服务是否存在。

```
netstat -ano | grep LISTEN | grep 14200
```

- 如果服务端口 14200 确实未提供服务，说明预警准确，需要执行以下命令，进一步确定分布式事务管理器服务进程是否存在。如果进程不存在，则确认是服务实例宕机，需要重新启动服务实例。

```
ps -ef | grep java
```

5.2.3 日常巡检项说明

5.2.3.1 系统监控指标巡检项目

巡检项说明

通过业务实时监控产品，查看分布式事务产品各项系统监控指标。访问路径是：产品与服务 > 业务实时监控 > 应用。

运维动作说明

如果发现预警指标异常，根据对应的预警项运维动作说明进行操作即可。

5.3 系统日志说明

5.3.1 日志文件清单说明

5.3.1.1 分布式事务管理器系统日志文件

日志文件名称	日志文件路径	日志文件描述
common-default.log	/home/admin/logs/dtxserver/common-error.log	默认日志
common-error.log	/home/admin/logs/dtxserver/common-error.log	错误日志，记录系统的全部 ERROR 日志。
dtx-dal.log	/home/admin/logs/dtxserver/dtx-dal.log	数据库访问统计日志

日志文件名称	日志文件路径	日志文件描述
dtx-schedule.log	/home/admin/logs/dtxserver/dtx-schedule.log	定时调度任务日志
dtx-recovery.log	/home/admin/logs/dtxserver/dtx-recovery.log	恢复任务日志
dtx-remote.log	/home/admin/logs/dtxserver/dtx-remote.log	事务协调器起日志

5.3.1.2 分布式事务控制台系统日志文件

日志文件名称	日志文件路径	日志文件描述
common-default.log	/home/admin/logs/dtxconsole/common-error.log	默认日志
common-error.log	/home/admin/logs/dtxconsole/common-error.log	错误日志，记录系统的全部 ERROR 日志。
dtx-rest.log	/home/admin/logs/dtxconsole/dtx-rest.log	REST 接口访问日志
dtx-dal.log	/home/admin/logs/dtxconsole/dtx-dal.log	数据库访问统计日志

5.4 常见运维场景说明

5.4.1 分布式事务控制台服务实例宕机

根据监控项 **分布式事务控制台端口监控** 预警，发现服务实例进程异常，可通过以下操作步骤重启宕机服务实例。

1. 登录云游，选择 **容器**。
2. 在搜索栏中，搜索 dtxconsole。
3. 点击 **Restart**，重启宕机控制台服务实例。

5.4.2 分布式事务管理器服务实例宕机

根据监控项 **分布式事务管理器端口监控** 预警，发现服务实例进程异常，可通过以下操作步骤重启宕机服务实例。

1. 登录云游，选择 **容器**。
2. 在搜索栏中，搜索 dtxserver。
3. 点击 **Restart**，重启宕机服务实例。

5.4.3 事务积压异常

1. 根据监控项 事务积压数量 预警，发现分布式事务出现事务积压。
2. 登录分布式事务管理器服务器，查看以下两个日志，确认事务积压的具体原因。

```
/home/admin/logs/dtxserver/dtx-recovery.log
/home/admin/logs/dtxserver/dtx-remote.log
```

5.4.4 事务二阶段失败异常

1. 根据监控项 **事务二阶段失败数量** 预警，发现分布式事务管理器回调参与方二阶段出现大量失败，初步怀疑是参与方 RPC 调用失败。
2. 登录分布式事务管理器服务器，查看以下日志，确认调用事务二阶段失败的参与方。

```
/home/admin/logs/dtxserver/dtx-remote.log
```

5.4.5 服务耗时异常

1. 根据监控项 **服务耗时监控** 预警，发现分布式事务管理器回调参与方二阶段耗时增加异常，初步怀疑是参与方二阶段接口执行耗时增加。
2. 登录分布式事务管理器服务器，查看以下日志，确认调用事务二阶段耗时增加的参与方。

```
/home/admin/logs/dtxserver/dtx-remote.log
```

3. 立即通知事务参与方应用系统 owner 排查二阶段接口调用失败原因。

5.5 服务巡检

5.5.1 系统组件监控检查

5.5.1.1 基础监控检查

登录 corewatch 监控系统，查看分布式事务（DTX）相关系统组件有无异常告警，需要关注的监控项内容如下表所示。

应用	分类	指标(关键字)	告警阈值
DTX-dtx DTX-dtx-console	基础监控-cpu 使用率监控	cpu_usage	>80%
	基础监控-内存使用率监控	mem_usage	>80%
	基础监控-磁盘使用率监控	disk_usage	>80%
	基础监控-load5	load5	>3
DTX-dtx	基础监控-端口监控	2022 14200	不通
DTX-dtx-console	基础监控-端口监控	80 2022	不通

5.5.1.2 自定义业务监控检查

通过 corewatch 内核态监控产品查看注册中心产品各项系统监控指标是否有异常告警产生。访问路径是：corewatch > 自定义监控 > 共享中间件 > 分布式事务 > DTX。

如果有异常告警产生，联系蚂蚁金服技术支持进行排查。

5.5.2 业务功能检查

1. dtx 服务验证

   - 执行以下命令，判断业务端口是否存活。

     ```
     netstat -an |grep 14200
     ```

   - 执行以下命令，判断 RPC 端口是否存活。

     ```
     netstat -an |grep 12200
     ```

   - 执行以下命令，判断 acvip 连接。

     查看连接的 acvip 的地址是否与 sofa-portal 控制台中显示的 acvip 地址一致。不一致的话，需将连接的地址改成 sofa-portal 控制台中显示的 acvip 地址。

```
netstat -an |grep 9003
```

- 执行以下命令，判断注册中心连接。

```
netstat -an |grep 9600
```

2. dtxconsole 服务验证

- 执行以下命令，判断 nginx 端口是否存活。

```
netstat -an |grep 8080
```

- 执行以下命令，判断业务端口是否存活。

```
netstat -an |grep 80
```

- 访问 sofa-dtx.{domain} 页面，检查各项页面功能是否正常无报错。

5.5.3 事务积压数检查

通过 DTX 的自定义监控项，重点关注事务积压数量。

监控指标	监控指标说明	预警项说明	报警级别
事务积压数量	未决事务积压数量，一般由于参与方系统异常导致积压	>10	重大
		>6	次要
整体异常数量	分布式事务系统整体每分钟异常数量	>10	重大
		>6	次要
事务二阶段失败数量	分布式事务每分钟二阶段执行失败的数量	>5/min	重大
		>3/min	次要

5.6 DTX/DTAP 服务异常应急预案

5.6.1 概述

适用范围

底座	产品版本
Antstack	1.0 - 1.3

问题描述或者背景

- 分布式事务控制台不可访问。
- 分布式事务功能异常。

5.6.2 环境检查

1. 登录共享中间件控制台，确认控制台可以正常访问。

2. 登录监控管理台，观察 dtx-console/dtap-console、dtx/dtap 告警。

5.6.3 实施步骤

1. 如果 dtx-console/dtx 容器为退出状态，尝试在云游启动该故障容器。
2. 如果 dtx-console/dtx 容器状态正常，webshell 进入容器，执行以下命令，检查 dtx-console/dtx 服务状态。

```
##检查 dtx-console 进程状态
#ps -fe | grep java

##如果 dtx-console/dtx 进程不在，尝试重启容器，会自动拉起业务容器
```

5.6.4 结果验证

1. 登录告警界面，无业务告警。
2. 登录业务容器，确认 dtx-console/dtap-console、dtx/dtap 服务正常运行。

5.6.5 回滚方案

无

5.6.6 补充说明

无

6.分布式链路跟踪

6.1 系统组件说明

6.1.1 组件角色说明

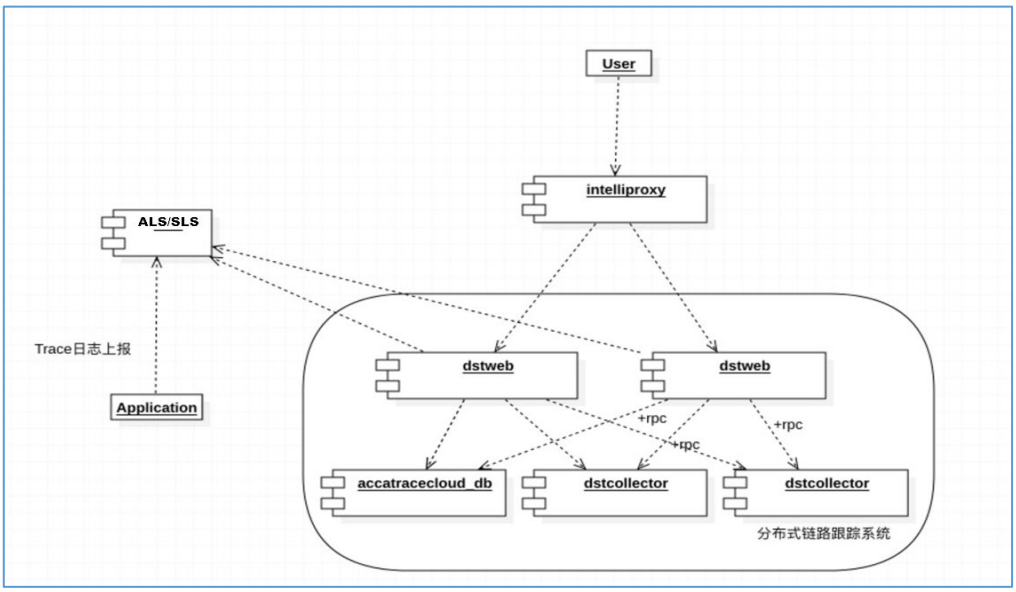
分布式链路跟踪”产品包括以下 2 个组件：

- 分布式链路跟踪控制台：分布式链路分析应用系统，提供单链路查询、多维查询。
- 日志服务存储：对应用调用或服务调用产生的 Trace 日志进行收集和存储。

6.1.2 部署拓扑说明

该部署拓扑图中各组件的说明如下：

- dstweb：分布式链路跟踪控制台
- ALS/SLS：日志服务存储，依赖资源
- intelliproxy：SOFA 中间件云产品网关组件
- dstcollector：给 dstweb 提供数据查询服务
- accatracecloud_db：dstweb 和 dstcollector 使用的数据库实例
- Application：用户应用系统
- User：用户浏览器



6.1.3 资源清单说明

组件角色	资源依赖	服务端口
分布式链路跟踪控制台	4 * 服务器（4 CPU，8G 内存，100G 磁盘）	80，8341，12200
	1 * RDS（2 CPU，4G 内存，10G 磁盘）	3306

6.2 监控和预警说明

6.2.1 监控指标和预警项说明

6.2.1.1 系统监控指标和预警项清单

监控指标	监控指标说明	预警项说明
磁盘空间监控	磁盘空间占用率监控	预警触发条件：大于 80%
端口监控	端口“8341”,"80"是否可以访问	预警触发条件：端口 8341 无法访问
内存监控	内存占用率	预警触发条件：大于 80%
CPU 利用率	CPU 利用率	预警触发条件：大于 80%

6.2.2 日常巡检项说明

6.2.2.1 系统监控指标巡检项目

巡检项说明：通过“业务实时监控”产品查看分布式链路跟踪系统各项系统监控指标，访问路径：产品与服务 > 业务实时监控 > 应用。

运维动作说明：

如果发现预警指标异常，根据对应“预警项运维动作说明”进行操作。

6.3 系统日志说明

6.3.1 日志文件清单说明

6.3.1.1 日志文件

日志文件名称	日志文件路径	日志文件描述
common-error.log	/home/admin/logs/common-error.log	系统 error 日志，描述系统中出现的任何出错信息

6.3.2 异常日志运维动作说明

6.3.2.1 无法连接 als/sls endpoint

在日志中出现无法连接 ALS/SLS 的相关错误日志，如连接拒绝等，检查配置的 ALS/SLS 地址是否正确，或者网络是否通。

6.4 常见运维场景说明

6.4.1 有 TraceLog 日志，但查询不出来

- 若使用的是 SLS：使用链路服务时，需要确认相应环境服务器是否已经安装了日志采集客户端，执行命令：sudo/etc/init.d/ilogtaild status。

  如果没有安装需要按 文档或者运维脚本 来安装。对于新申请的服务器也要定期安装采集客户端。

- 若使用的是 ALS：需要确认 ant_cloud_agent 是否安装正确。

6.4.2 链路数据收集延迟

需要关注 tracer 日志的产生量，目前支持的 rpc/db/rest 等每类日志 25M/s 的生成量，当业务调用量很大的时候，需要联系管理员扩 shard。

6.4.3 查询链路详情存在存在类型为 MOCK 的节点

出现这种情况主要是因为改节点服务器日志未采集到，可通过以下方式确认：

- 检查缺失节点服务器的日志采集客户端是否正常安装。
- 检查缺失节点的调用类型是否在系统支持范围内。

6.4.4 多维查询没有结果，或者搜索链路为空

检查调用时间是否为有效时间内（默认缓存 7 天），超出时间的可能会查询不到数据。另外检查日志采集客户端是否正常安装。

6.4.5 链路图中会对相同调用的节点进行合并

如果实际连续进行的多次调用，在链路图上反映的是两个应用之间的调用关系。

6.5 服务巡检

6.5.1 系统组件监控检查

6.5.1.1 基础监控检查

登录 corewatch 监控系统，查看分布式链路跟踪（DST）相关系统组件有无异常告警，需要关注的监控项内容如下表所示。

应用	分类	指标（关键字）	告警阈值
DST-dstcollector DST-dstconsole DST-dstweb	基础监控-cpu 使用率监控	cpu_usage	>80%
	基础监控-内存使用率监控	mem_usage	>80%
	基础监控-磁盘使用率监控	disk_usage	>80%
	基础监控-load5	load5	>3
DST-dstcollector	基础监控-端口监控	12200	不通
DST-dstconsole	基础监控-端口监控	80	不通
DST-dstweb	基础监控-端口监控	80 8341	不通

6.5.1.2 自定义业务监控检查

通过 corewatch 内核态监控产品查看注册中心产品各项系统监控指标是否有异常告警产生。访

问路径是：corewatch > 自定义监控 > 共享中间件 > DST。

如果有异常告警产生，联系蚂蚁金服技术支持进行排查。

6.5.2 业务功能检查

- 执行以下命令，查看 status 是否为 UP，如果不是，查看返回的数据里面哪部分是 DOWN 状态。

```
curl 127.0.0.1:8080/health/readiness
```

- 执行以下命令，判断 RPC 端口是否存活。

```
netstat -an|grep 12200
```

- 执行以下命令，判断 acvip 连接。

  查看连接的 acvip 的地址是否与 sofa-portal 控制台中显示的 acvip 地址一致。不一致的话，需将连接的地址改成 sofa-portal 控制台中显示的 acvip 地址。

```
netstat -an|grep 9003
```

- 执行以下命令，判断注册中心连接。

```
netstat -an|grep 9600
```

- 访问 DST 控制台页面，检查各项功能是否正常，寻找一笔业务的 traceId，检查其链路显示是否正常。

7.注册中心 SOFA Registry

7.1 产品概述

7.1.1 产品介绍

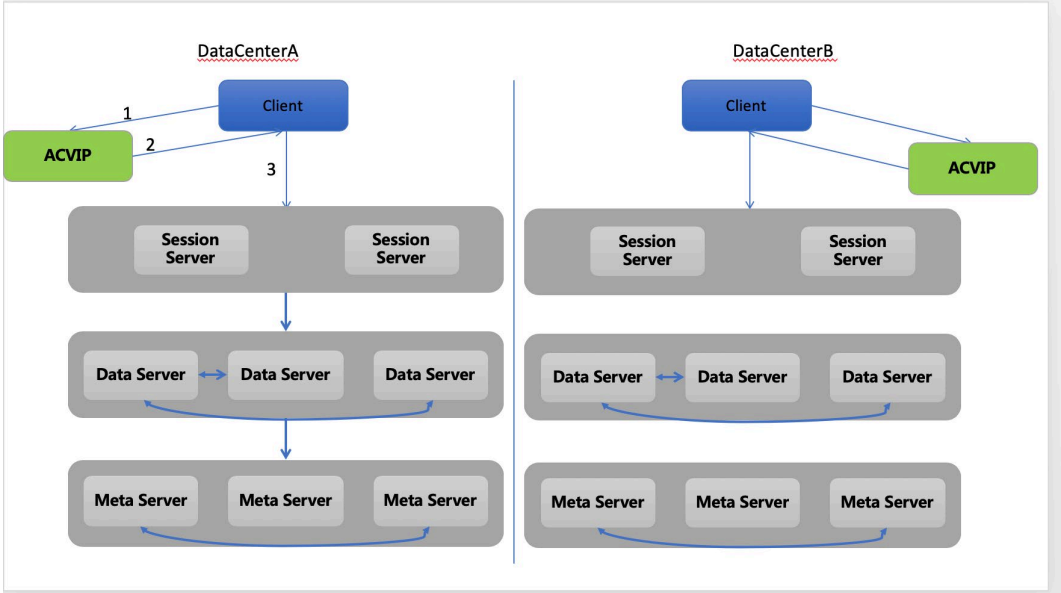
注册中心是服务提供者和服务使用者之间的桥梁，它包含 4 个角色：

- **Client**：提供应用接入服务注册中心的基本 API 能力，应用系统通过依赖客户端 JAR 包，通过编程方式调用服务注册中心的服务订阅和服务发布能力。
- **SessionServer**：会话服务器，负责接受 Client 的服务发布和服务订阅请求，并作为一个中间层将写操作转发 DataServer 层。SessionServer 这一层可随业务机器数的规模的增长而扩容。
- **DataServer**：数据服务器，负责存储具体的服务数据，数据按 dataInfoId 进行一致性 hash 分片存储，支持多副本备份，保证数据高可用。这一层可随服务数据量的规模的增长而扩容。
- **MetaServer**：元数据服务器，负责维护集群 SessionServer 和 DataServer 的一致列表，作为 SOFARegistry 集群内部的地址发现服务，在 SessionServer 或 DataServer 节点变更时可以通知到整个集群。

7.1.2 部署架构

该部署架构图以双机房部署（DataCenter A 和 DataCenter B）的场景为例。数据访问流程如下：

1. Client 向服务发现组件（ACVIP）查询注册中心的 SessionServer 的可用域名。
2. ACVIP 返回 SessionServer 的可用域名给 Client。
3. Client 向注册中心的 SessionServer 发起服务发布和订阅的请求。



7.2 操作前准备

7.2.1 了解操作流程

中间件相关产品的操作和维护过程一般分为三类：

- 云游支持的常见操作。如产品发布，更改，容器管理，物理节点管理和其他白屏操作。
- 产品个性化管理操作。通常，通过 WebShell 执行分区资源管理，产品内部状态的更改等。
- 监控和故障排除。包括使用监控系统，监控配置，故障分析，故障排除等。

7.2.2 操作工具的描述

用于此产品的操作工具如下：

- 云游（Yunyou）：云游的简介和基本使用说明，请参阅云游的帮助文件，包括产品元数据，负载平衡，数据库和其他信息查看
- 监控系统（Corewatch）：核心监控的说明和基本使用说明可以在 Corewatch 的帮助文档中找到。

7.3 常规运维

运维目的

本手册的主要指导操作人员对人蚂蚁云游系统进行预防性维护和处理紧急问题，确保系统长期稳定运行。

维护人员可以按照本手册中的说明处理操作和维护过程中发现的系统问题。如果根据本手册无法解决系统问题，请向云游工程师寻求技术支持。

运维要求

维护人员必须具备 IT 行业技能， 包括计算机网络知识，计算机操作知识，问题分析和故障排除功能。此外，维修人员必须下蚂蚁云游系统的岗前培训学习蚂蚁云游系统的必要知识，包括但不限于使用的系统原理，功能和维修工具。

值得注意的是，在维护操作期间，操作人员必须遵守操作规程以确保系统安全。对于用户数据，它是严格保密的。

未经用户书面许可，禁止复制和传播用户数据。

运维红线

- 禁止更改管理平台未请求的所有更改操作（如果发生紧急故障，则必须在之后填写应用程序）。
- 未经测试，抢先或变灰的在线更改。
- 禁止在没有验证计划和应急计划（包括回滚计划）的情况下进行变更，并且应急计划必须可行。
- 禁止所有计划外操作（如果出现意外情况，执行后禁止修改计划，立即暂停并通知技术经理）。
- 禁止在与 更改或联机故障排除 无关的生产环境中执行操作 。不允许个性化操作。
- 禁止更改客户的非更改窗口或网络关闭时间（如果客户具有非更改窗口或网络的定义）。
- 禁止数据传输和披露。

7.3.1 创建解决方案

注意： 此操作由云游技术支持团队执行。

7.3.2 同步解决方案

注意：请首先咨询云游技术支持团队，以获取解决方案和相应的发布文档。

登录云游站点并从云游技术支持团队导入解决方案（通常采用 .json 格式）。

注意： 如果导入解决方案失败，可能是因为某些应用程序未在最后一个发行票证中发布，请确保先前的票证已完全执行。

单击以导入解决方案并将解析访问文件拖到框中，成功后您可以在第一个页面列表中看到解决方案：

7.3.3 发布与升级

注意：此处显示了 一般的发布/升级更改过程，某些应用程序有一个特殊的更改过程需要引用相应的应用程序文档。

警告：未按照适当的流程应用更改可能会导致整个站点严重故障。

发布（部署）和升级过程是相同的，当建立解决方案时，如果有版本更改，那么升级，如果没有旧版本号，那么发布，发布和设计都取决于部署解决方案。

单击解决方案以进入如下所示的部署页面。

此页面的重点是“部署前置任务”，只有当所有四个前置任务都处于绿色（正常）状态时才能继续：

- 参数配置
- 镜像配置
- 负载均衡配置（多房间）
- 数据库规划

一般情况下，镜像配置不需要手动关注，这里需要关心参数配置，负载均衡和数据库。转到 **解决方案元数据** 界面以配置参数，负载平衡和数据库规划。

7.3.3.1 参数配置

注意：根据云游技术支持团队 提供的相应发布文档检查详细信息。

参数配置的内容是当前解决方案中包含的所有应用程序的所有相关参数，例如每个应用程序的启动参数，环境变量，使用的数据库名称和密码，JVM 内存配置等。

注意：如果您的应用由于更改时的参数问题而失败，例如数据库未连接，您可以尝试在此处手动修改参数配置并重试更改。有关详细信息，请参阅相应的发行文档，或咨询云游技术支持团队以获取答案。

进行手动修改时，可以先单击 **渲染参数** 将一些变量转换为人类可读模式，然后单击右侧的编辑按钮进行修改。

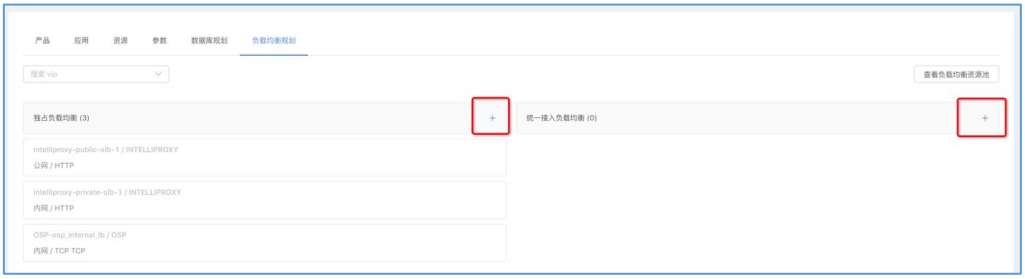
注意：修改参数内容时，需要注意其基线值（即默认值）以及是否确认，确认后，该参数在下次发布/重试后才会生效。

7.3.3.2 负载平衡配置

负载平衡配置用于为应用程序提供负载平衡机制，例如

- 外部负载平衡（外部用户请求）
- 内部负载均衡（内部用户请求）
- 应用程序之间的负载平衡（例如，MQ 控制台应用程序访问 MQ 代理）且很快

通过单击右侧的“加号”手动手动配置负载平衡，最后确认配置。



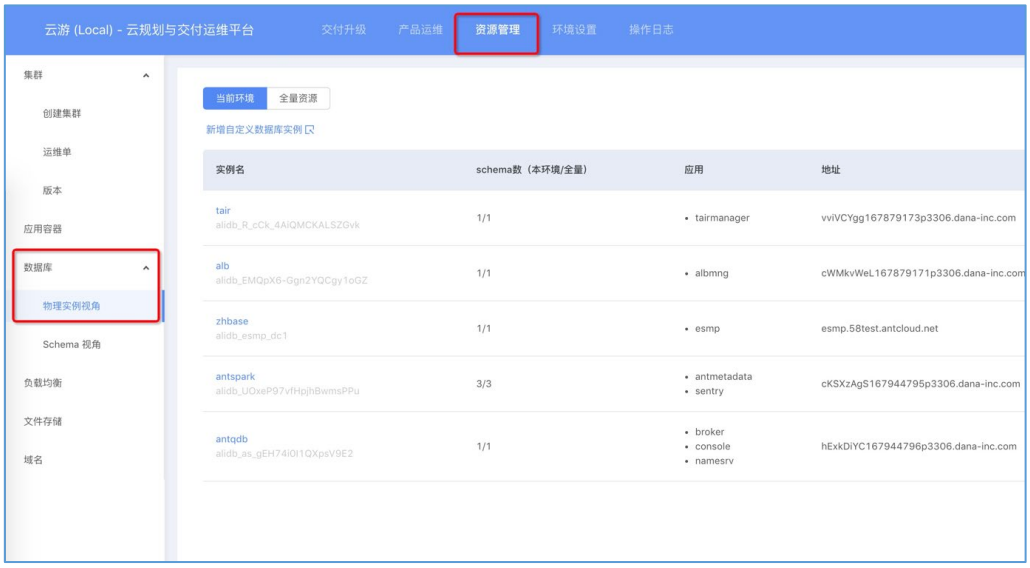
7.3.3.3 数据库规划

注意：要创建一个数据库实例和数据库的问题，请咨询数据库管理员或云游技术支持团队。

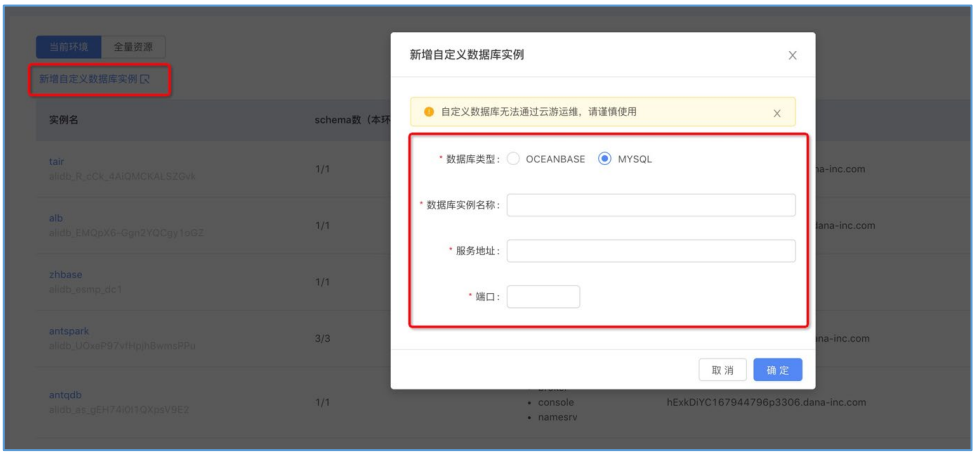
使用新库

在数据库计划中，您可以选择是创建新数据库还是使用现有数据库。如果要创建新数据库，则需要在 DBA 提供数据库名称后执行以下操作。

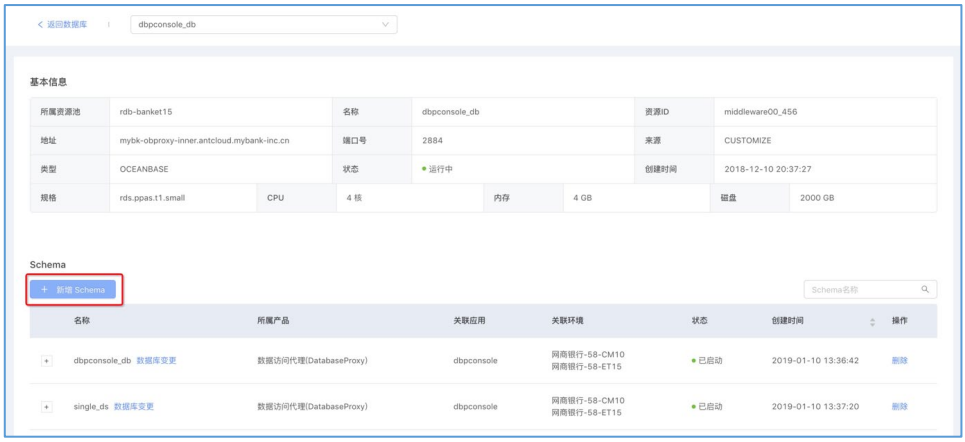
1. 如下所示，进入 **资源管理** > **数据库** > **物理实例视角**。



2. 单击 **新建自定义数据库实例** 以开始添加新库，这将需要填写 DBA 提供的信息，包括数据库类型，实例名称，服务地址，端口号。



3. 单击 **确定** 后，将输入数据库实例，然后输入数据库的表信息。单击刚刚输入的数据库实例，进入 Schema entry 界面，单击 **新增 Schema** 开始添加。



4. 新增 Schema 时，请务必注意：

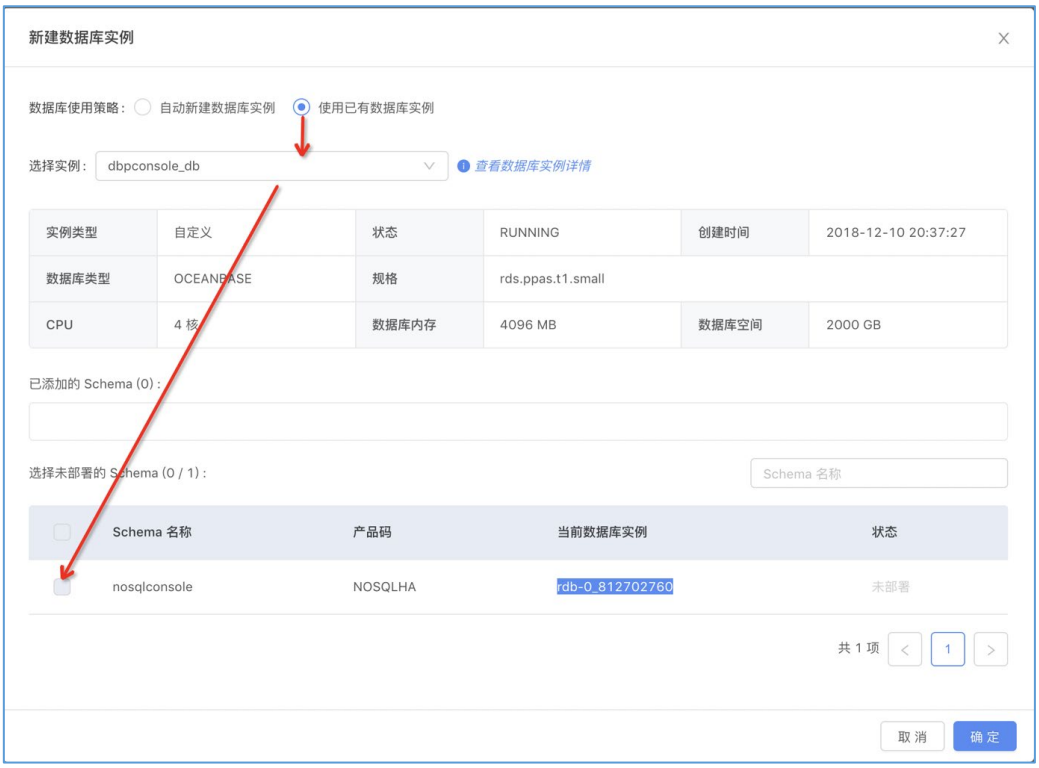
- **Schema 名称** 是当前库的名称，因此请确保与产品元数据中所需的模式名称一致。产品需要模式名称列表以引用产品拓扑或解决方案数据库规划。
- **用户名** 是具有当前架构访问权限的用户，需要完整的 DDL 和 DML 权限，包括新建、修改等。
- **密码** 是当前用户的密码。

使用现有实例

配置新库后，下面的过程与使用现有库的过程相同：添加已通过 **数据库规划** 列中的“加号”按钮，输入的数据库信息。

选择 **使用现有数据库实例** 选项，选择已输入的数据库实例和架构信息，然后单击 **确定**。

注意：只能检查在数据库实例中输入的与未部署模式同名的模式。



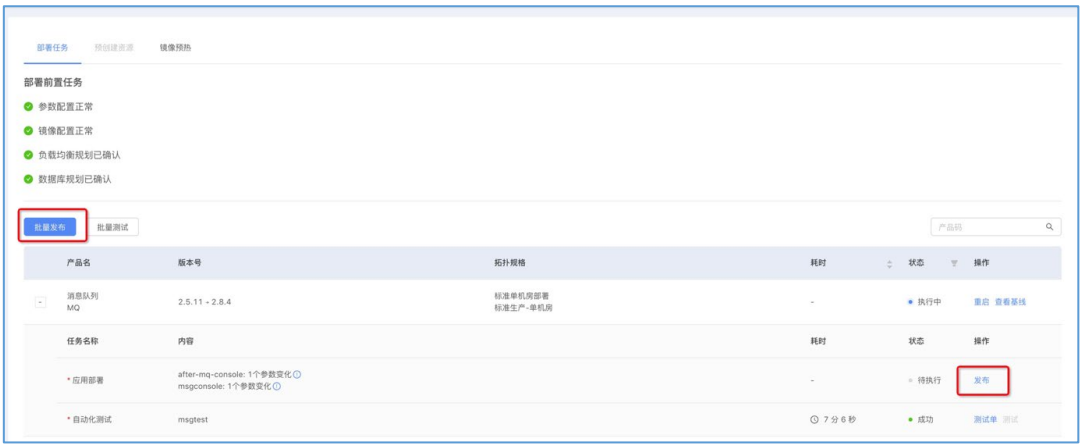
7.3.3.4 发布

警告：

- 每次发布 beta 分组时，您都需要手动使用 shell 环境来确认当前分组下的所有服务器是否正常运行，例如进程是否已启动，端口是否已打开，请求是否正常以及等等。
- 有关如何执行此操作，请参阅“手动更改”部分。
- 有些应用程序是通过特殊的发布程序发布的，请参考相应的流程。
- 中间件应用程序的故障通常会导致站点级别的故障，因此您必须在继续之前参考相应应用程序 的更改过程 ，否则将导致释放失败甚至影响应用程序和整个站点。

注意：请与云游技术支持团队联系，了解发布中遇到的系统问题。

配置参数后，即可进入发布过程。在多个应用程序的情况下，可以批量发布或单独发布解决方案。单击批量发布以通过单击按钮发布整个解决方案，或通过单击应用程序下的发布按钮发布单个应用程序。



发布后，每个应用程序都有两个任务：应用程序部署和自动化测试。右栏有四个动作，即：

- 查看发布顺序
- 强制重新发布
- 查看测试表
- 手动开始测试

我们主要关注的是应用程序部署。

单击应用程序的 **发布单** 以进入应用程序的发布顺序页面，您需要在其中指定发布组的数量。

注意：分组发布的目的是将应用程序的服务器划分为多个组以进行发布，从而防止应用程序不可用，例如更改失败（左侧是单个组发布成功，右侧图像多组发布失败）。

警告： 某些应用程序具有特定的分组要求，请参阅相应应用程序的文档。不正确的分组可能会导致失败。

7.3.3.5 发布流程和分组

再次进入应用发布流程，您可以手动管理当前应用程序的发布过程。在一般情况下，整个过程是半自动化的。

注意：通常有两个过程需要人为干预。

1. 拉取镜像失败/超时

由于镜像资源庞大，且组镜像服务器位于中国大陆并且在组内部网中，当您遇到网络阻塞，带宽不足等问题时，镜像拉取会超时。手动点击 **重试** 需要重试（甚至可能需要多次重试）拉镜像直到镜像拉动成功。

2. 在多个分组的情况下，单个组发布成功时：

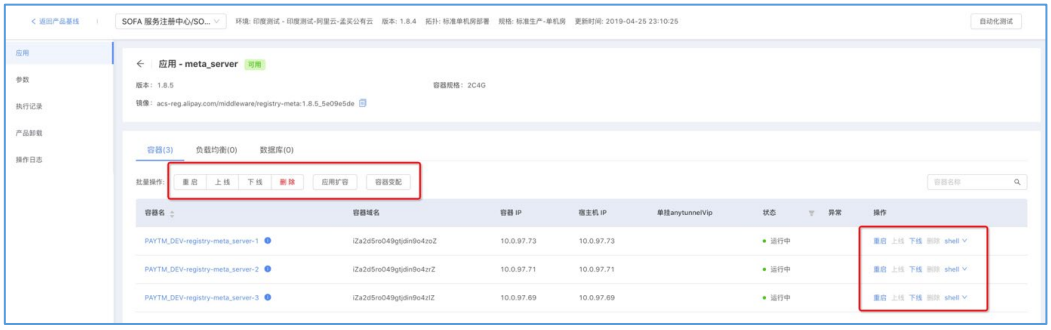
完成单个分组发布后，您需要手动验证已完成更改的每个服务器的状态（请参见相应应用的说明文档），然后单击 **确认** 继续后续分组。

7.3.4 日常运维

您可以在本地站点主页和产品操作列中查看当前在站点上部署的所有产品。

单击以查看当前产品下的所有应用程序，以下示例中的产品 SOFA 服务注册表，该软件包包含四个应用程序：注册表测试应用程序，META、DATA 和 SESSION。

假设注册表中的 META 应用程序需要在此时运行，请单击相应的应用程序并转到应用程序管理。应用程序管理页面包含当前应用程序的服务器信息，负载平衡配置和数据库配置。在服务器信息界面中，提供服务器的单个/批量服务器重启、上线、下线，删除操作，并支持应用扩容和应用变更操作。



7.3.4.1 应用扩容

当应用过载时通常需要对应用进行适当扩容。单击服务器管理页面上的 **应用扩容**，然后输入您需要添加的服务器数量以扩展容量：

7.3.4.2 容器重启/上线

对于单个容器的重启/上线操作，只需单击相应的操作按钮即可。

警告：在采取措施之前，请参阅当前应用程序的应用程序操作文档，以确认是否存在任何特殊的其他操。不正确的更改可能会导致应用程序失败。

7.3.4.3 容器下线

对于单个容器的下线操作，只需单击相应的操作按钮即可。

注意：操作可以通过容器在线回滚。

警告：在采取措施之前，请参阅当前应用程序的应用程序操作文档，以确认是否存在任何特殊的其他操作。不正确的更改可能会导致应用程序失败。

下线操作指关闭容器，终止进程，但不释放资源并保留容器 IP。

- 已下线的容器可以重新上线。
- 下线操作可逆。

7.3.4.4 移除容器

对于单个容器的删除操作，只需单击相应的操作按钮即可。

警告：操作无法回滚，容器的资源将被释放。执行应用扩展以添加容器。

警告：在采取措施之前，请参阅当前应用的运维操作文档，以确认是否存在任何其他特殊操作。操作不当可能会导致应用运行失败。

删除操作将关闭并完全销毁容器，释放包括 IP 在内的所有资源：

- 删除操作不可逆转。
- 如果要在删除后重新启动服务器，必须先完成扩容。

7.3.4.5 Shell 登录 - 云游

单击 Shell 按钮进入相应服务器的控制台。

警告：此时权限为 root，是一种高风险操作。

7.4 个性化变更

当前的 Registry 产品变更比较特殊，其发布和异常处理涉及对整个群集的变更。

7.4.1 预置操作

注意：所有变更都需要预先执行。

- 通过 WebSHELL 登录到任何元服务器上的 Registry 服务器。
- 在服务器上，执行以下命令并关闭推送：

```
curl http://localhost:9615/stopPushDataSwitch/open
```

- 需要验证状态是否真的关闭：

```
curl http://localhost:9615/digest/pushSwitch
```

7.4.2 后置操作

注意：完成所有更改后，必需执行此操作。

- 通过 WebSHELL 登录到任何元服务器上的 Registry 服务器。
- 在服务器上，执行以下命令并打开推送：

```
curl http://localhost:9615/stopPushDataSwitch/close
```

- 确认 Registry 是否为开启状态：

```
curl http://localhost:9615/digest/pushSwitch
```

7.4.3 新站点发布

- 导入解决方案。
- 所有服务器都必须在同一时间发布，即要在同一套版本中，因为元服务器（meta-server）是基于 raft 协议的。该协议要求大多数节点启动领头节点选举。
- 在发布过程中，您需要遵循“meta_server-> data_server-> session_server”的发布顺序：如果在发布应用（例如数据服务器）期间计算机运行状况检查失败，则需要重试。当前应用发布成功后，下一个应用方可进入发布流程。
- Metapushclose 和 metapush 都是关闭推送的一次性任务。在首次部署新站点时，如果元服务器不存在，则 metapushclose 无法发布，可以直接选择“跳过”。
- 监控正常后，执行 7.4.2 章节的 **后置操作** 并打开推送。
- 打开推送后，执行后续测试用例。

7.4.4 版本升级

- 导入解决方案。

- 首先执行 7.4.1 章节的 **预置操作**，然后关闭推送。
- 所有服务器都必须在同一时间发布，即要在同一套版本中，因为 meta-server 是基于 raft 协议的。该协议要求大多数节点在同一时间启动领头节点选举。
- 在发布过程中，您需要遵循“meta_server-> data_server-> session_server”的发布顺序：如果在发布应用程序（例如数据服务器）期间计算机运行状况检查失败，则需要重试。当前应用发布成功后，下一个应用方可进入发布流程。
- 元推送关闭和元推送都是关闭推送的一次性任务。
- 观察监控系统的 pubs/subs 数量，恢复到发布前的水平。

  参考 **自定义监控** 中的 pub/sub/watch，并期望数量恢复到发布前的的 90%到 100%，具体取决于群集大小大，约需要 3 到 10 分钟。
- 监控正常后，执行 7.4.2 章节的 **后置操作** 并打开推送。
- 打开推送后，执行后续测试用例。

7.4.5 扩展

7.4.5.1 meta_server 扩展

已部署三个 registry-meta 单元,其 IP 地址分别为 1.1.1.1(IP1)、2.2.2.2(IP2)、3.3.3.3(IP3)，其中 IP3 关闭且无法重新启动，需要更换新的容器如下所示：

- 扩展一个新的元服务器，假设 IP 地址为 4.4.4.4。
- 将新节点加入集群：

  登录 IP1 或 IP2 并执行命令：

  ```
  curl -X POST"http: // localhost: 9615 / manage /
  changePeer"-d"dataCenter = <data_center_name> & ipAddressList =
  <metaNode1> , <metaNode2> , <metaNode4> "
  ```

  如果 *机房* 的名称 是 A，请将其替换为 DataCenterA，或者 B 可以在此处找到由

  DataCenterB 替换的机房：

  例如：

  ```
  curl -X POST "http://localhost:9615/manage/changePeer" -d
  "dataCenter=DataCenterB>&ipAddressList=1.1.1.1,2.2.2.2,4.4.4.4"
  ```

最后，检查所有 3 个元服务器是否健康并登录各个元服务器。Success 表示 true，其中一个服务器是 leader，其他均为 follower.

```
curl http://localhost:9615/health/check
```

预期返回结果：

```
{"success": true, "message": "MetaServerBoot sessionRegisterServer:
true, dataRegisterServerStart: true, otherMetaRegisterServerStart:
true, httpServerStart: true, raftServerStart: true, raftClientStart:
true, raftManagerStart: true, raftStatus: Leader"}
```

- 参考 **容器下线 和 移除容器** 章节内容移除 IP 为 3.3.3.3 的容器。

7.4.5.2 data_server 扩展

- 执行 **预置操作**，关闭推送。
- 随着云游扩展数据服务器的容器，运行状况检查必须成功，不能跳过。
- 执行 **后置操作**，打开推送。

7.4.5.3 session_server 扩展

- 执行 **预置操作**，关闭推送。
- 使用云游扩展会话和服务器的容器，运行状况检查必须成功，不能跳过。
- 执行 **后置操作**，打开推送。

7.4.6 容器重启

- 重启 meta_server
  - 执行 **预置操作**，关闭推送。
  - 使用云游打开异常的 meta_server 容器，运行状况检查必须成功，不能跳过。
  - 执行 **后置操作**，打开推送。
- 重启 data_server
  - 执行 **预置操作**，关闭推送。
  - 使用云游打开异常的 data_server 容器，状况检查必须成功，不能跳过。
  - 执行 **后置操作**，打开推送。
- 重启 session_server
  - 执行 **预置操作**，关闭推送。

- 使用云游重新启动异常 session_server 容器时，运行状况检查必须成功且无法跳过。
- 执行 **后置操作**，打开推送。

7.4.7 容器上线

一般不需要执行该操作。

7.4.8 容器下线

注意：该操作需要配合容器扩展操作，一般不能独立操作。

7.4.9 移除容器

注意：容器删除需要配合扩展操作，一般不能独立操作。

通过云游移除异常容器。删除前，确保已将容器下线。

7.5 报警处理

7.5.1 系统监控

分类	指标（关键字）	报警阈值	采集间隔	报警间隔	描述	如何处理警报
CPU 使用情况监控	cpu_usage	> 90%	1 分钟	3 分钟	CPU 使用情况监控，目前设置监控阀值为 90%	扩展容器
内存使用监控	mem_usage	> 90%	1 分钟	3 分钟	内存使用情况监控，目前设置监控阀值为 90%	展开或重新启动容器
磁盘使用情况监控	disk_usage	> 90%	1 分钟	3 分钟	磁盘使用情况监控，目前设置监控阀值为 90%	清除日志目录中无效的日志文件
端口监测	8080	It doesn't	1 分钟	3 分钟	端口监控，警告	重新启动或更换容器

7.6 容灾切换

注册中心已完成双机房独立部署，因此您只需要切换 SaaS 业务，而 Registry 无需切换。

7.7 服务巡检

7.7.1 系统组件监控检查

7.7.1.1 基础监控检查

登录 corewatch 监控系统 > **资源实例监控** > **云服务器 ACS**，在搜索框中查找 SOFA Registry 对应的系统组件，确认其无异常告警。需要关注的监控项内容如下表所示。

应用	分类	指标（关键字）	告警阈值
registry-session registry-data registry-meta	基础监控-cpu 使用率监控	cpu_usage	>80%
	基础监控-内存使用率监控	mem_usage	>80%
	基础监控-磁盘使用率监控	disk_usage	>80%
	基础监控-load5	load5	>3
registry-session	基础监控-端口监控	9600	不通

registry-data	基础监控-端口监控	9620	不通
registry-meta	基础监控-端口监控	9610	不通

7.7.1.2 自定义业务监控检查

通过 corewatch 内核态监控产品查看注册中心产品各项系统监控指标是否有异常告警产生。访问路径：corewatch > 自定义监控 > 共享中间件 > MicroService > Registry。

如果有异常告警产生，联系蚂蚁金服技术支持进行排查。

7.7.2 业务功能检查

1. SOFA Registry 服务验证

   a) 验证 meta 是否启动成功：

   登录 meta 节点容器后台，执行以下命令，检查本机健康接口。

   ```
   curl http://localhost:9615/health/check
   ```

   b) 验证 data 是否启动成功：

   登录 data 节点容器后台，执行以下命令，检查本机健康接口。

   ```
   curl http://localhost:9622/health/check
   ```

   c) 验证 session 是否启动成功：

   登录 session 节点容器后台，执行以下命令，检查本机健康接口。

   ```
   curl http://localhost:9603/health/check
   ```

2. 业务验证（即验证业务方应用）

   检查应用所使用的 RPC 是否能正常调用成功即可。

7.8 服务异常应急预案

7.8.1 概述

适用范围

底座	产品版本
Antstack	1.0 - 1.3

问题描述或者背景

应用无法订阅消息

风险说明

重启 registry-data 和 registry-session 前，建议关闭消息推送，否则有可能造成所有消息推空的情况。

7.8.2 环境检查

1. 登录云游，检查所有 registry 容器状态（运行中、节点宕机、退出）。
2. 登录监控页签，查看 meta、data、session 端口 9610~9612、9614~9615、9620~9622、9600、9601、9602 是否正在监听。

```
#netstat -an | grep -i listen | grep 96
```

7.8.3 实施步骤

1. 如果容器为运行中状态，webshell 进入容器，执行以下命令，检查 registry meta、data、session 服务状态。

```
#ps -fe | grep java
```

2. 如果进程异常，可以通过重启相关 registry 容器拉起进程。在重启相关容器前，建议关闭推送（registry 1.5.x 之后支持 API 关闭推送），操作步骤如下：

a) 登录任意一台 registry-meta 容器。

b) 执行以下命令，关闭推送。

```
#curl http://localhost:9615/stopPushDataSwitch/open
```

c) 执行以下命令，检查推送是否关闭。

```
#curl http://localhost:9615/digest/pushSwitch
```

d) 待重启容器完成后，执行以下命令，打开推送。

```
#curl http://localhost:9615/stopPushDataSwitch/close
```

e) 执行以下命令，检查推送是否已经打开。

```
#curl http://localhost:9615/digest/pushSwitch
```

3. 如果容器为节点宕机状态，判断是否存在物理机宕机。如果是，则参考 物理机宕机应急预案 对故障物理机上运行的容器进行宕机迁移，并在新宿主机上启动容器。
4. 如果容器为退出状态，可以在云游上启动 registry 容器。

7.8.4 结果验证

1. Registry 各个组件状态为运行中。
2. Registry 各个组件进程状态正常，监控界面无告警。
3. 重启应用可以获得服务地址。

7.8.5 回滚方案

无

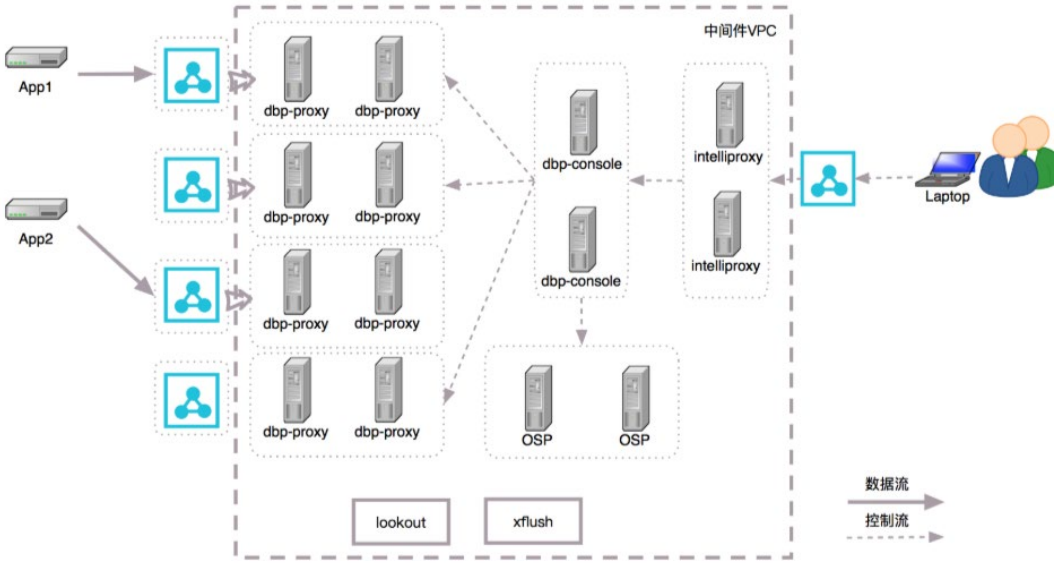
7.8.6 补充说明

无

8.数据访问代理

8.1 系统组件说明

8.1.1 组件角色和部署拓扑说明



该部署拓扑图中各组件的说明如下：

- dbp-console 和 dbp-proxy 构成了数据访问代理（DBP），这两个组件的作用如下：
  - dbp-console（控制台）：Web 应用系统，负责配置数据库、数据表规则等。
  - dbp-proxy（代理服务器）：数据访问代理服务器，提供 MySQL 服务。
- OSP 和 intelliproxy 是中间件中台组件，为数据访问代理提供基本中台服务。
- Lookout 和 xflush 是监控组件，为数据访问代理提供监控服务。

8.1.2 资源清单说明

- 控制台：2 * 服务器（2 CPU，4G 内存，100G 磁盘），1 * RDS（1CPU，2G 内存，200G 磁盘）
- 代理服务器：2 * 服务器（4 CPU，8G 内存，100G 磁盘）单实例规格，需要根据具体业务量评估实例数

8.2 监控和预警说明

8.2.1 监控指标和预警项说明

关于各模块的自定义业务监控指标的说明如下：

编号	业务模块	监控指标	报警阈值	报警级别	监控项说明
1	DBP server	单机量 每分钟执行 SQL 数	每分钟超过 60w	严重	单机每分钟执行的 SQL 数
2			周环比下跌 20%	严重	
3		集群总量 每分钟慢 SQL 数	实例超过 100 个	严重	实例每分钟慢 SQL 数
4		明细总量 每分钟 SQL 执行平均响应时间	绝对值超过 15ms 且 SQL 数大于 100 个	严重	单库(明细)每分钟 SQL 执行平均响应时间
5			绝对值超过 10ms 且最近 10 分钟与上 10 分钟环比增加 30% 且 SQL 数大于 100 个	严重	
6		明细总量 每分钟 SQL 执行成功率	成功率小于 97%	严重	单库(明细)每分钟 SQL 执行成功率
7		实每分钟报警次数	每分钟超过 200 个	严重	实例每分钟报警次数
8		数据库生效失败	数据库生效失败 1 次	严重	数据库生效失败 1 次
9		慢 SQL 监控	慢 SQL 出现 100 次	严重	慢 SQL 出现 100 次
10	DBP console	控制台端口监控	80	严重	控制台端口 80、9500 可用状态
11			9500	严重	监控检查端口
12			8341	严重	REST 服务端口
13	DBP server	实例服务端口监控	8066	严重	服务实例端口 8066 可用状态

8.2.2 配置监控和预警

8.2.2.1 Dal 配置

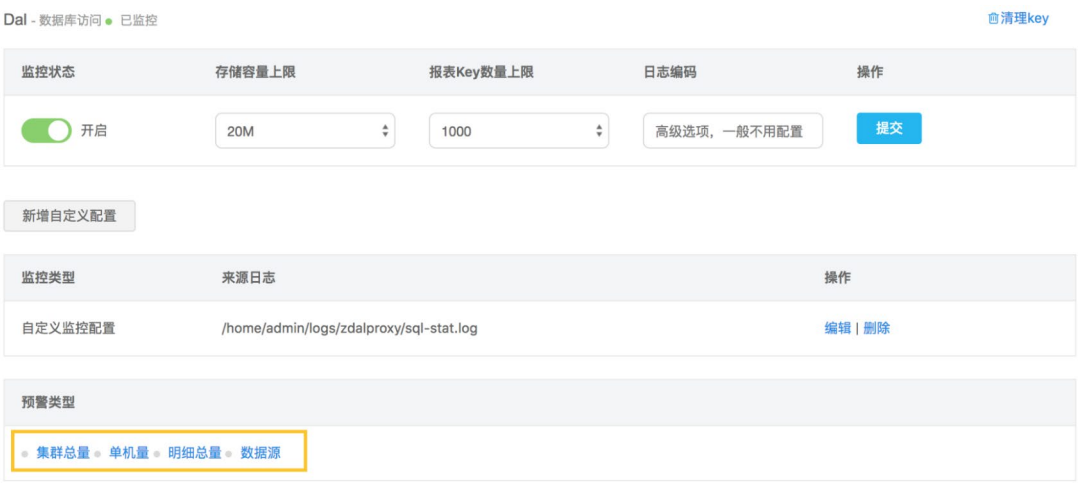
第 1～6 项均是 Dal 配置，首先请配置 Dal，配置说明如下：

- 新增自定义配置
- 采集日志文件：/home/admin/logs/zdalproxy/sql-stat.log
- 数据源：左起第 1 个 “,” 右至 “,”
- 接口：左起第 2 个 “,” 右至 “,”
- 方法：左起第 2 个 “,” 右至 “,”
- 结果：左起第 3 个 “,” 右至 “,”；代表成功的值 “Y”，代表失败的值 “N”
- 耗时：左起第 5 个 “,” 右至 “,”
- 计数：对日志中出现的某列值求和；计数求和列：左起第 4 个 “,” 右至 “,”

日志样例：

```
2018-07-02
19:12:41,720,cloud_load,SELECT,Y,2633,1115578,95334,65305,27
078,3589,801570,95728
```

配置完毕 Dal 后，请依次配置预警规则：



8.2.2.2 错误报警的配置

第 7 项是 Error 报警配置，请添加以下来源日志的监控自定义配置：

- /home/admin/logs/zdalproxy/zdal/zdal-monitor.log
- /home/admin/logs/zdalproxy/common-error.log

8.2.2.3 监控数据库生效失败的配置

注意：所有实例配置一个即可，极少出现。

第 8 项是数据库生效失败配置，新建“自定义监控 > 中间件云产品 > 数据访问代理”目录：

- 添加“自定义监控 > 匹配查找预警”
- 选择所有 DBP 实例应用，采集日志文件：

/home/admin/logs/zdalproxy/config-digest.log

- 新增白名单筛选：
  - 白名单筛选列：左起第 2 个“#” 右至常用分隔符
  - 白名单值：false
- 求值方式：求行数
- 预警配置：
  - 预警标题：数据库生效失败
  - 预警内容附带最大日志条数：1
  - 触发短信预警最小匹配日志条数：1
  - 预警等级：橙色预警(P1)

日志样例：

```
- dbp_watchman#20170810#2017-11-18,20:03:36.000#true
```

8.2.2.4 慢 SQL 监控的配置

注意：每个实例应用都要单独配置。

第 9 项是数据库慢 SQL 监控配置,新建“自定义监控 > 中间件云产品 > 数据访问代理”目录：

- 添加 自定义监控 > 分钟统计
- 选择单个 DBP 实例应用，采集日志文件：

  /home/admin/logs/zdalproxy/zdal/zdal-monitor.log

- 新增白名单筛选：
  - 白名单筛选列：左起第 0 个“]” 右至空格
  - 白名单值：Slow
- 求值方式：求行数
- 预警配置：

- 规则：当前时间的值 > 100 短信预警

日志样例：

```
2017-11-28
10:21:38,707-[0afd018315118356979415801255 76,0.1]Slow sql 765
millis, logicDsId: pc_batch_globalhost, sql: select count(job_id)
from pc_batch_batch_job_instance where ((state = 'RUNNING'))
```

8.2.2.5 其他配置

第 10 ~ 13 项配置请参考常规流程进行配置，无特殊配置。

8.3 服务巡检

8.3.1 系统组件监控检查

8.3.1.1 基础监控检查

登录 corewatch 监控系统，查看数据访问代理（DBP）相关系统组件有无异常告警，需要关注的监控项内容如下表所示。

应用	分类	指标（关键字）	告警阈值
DBP-dbpconsole DBP-dbpserver	基础监控-cpu 使用率监控	cpu_usage	>80%
	基础监控-内存使用率监控	mem_usage	>80%
	基础监控-磁盘使用率监控	disk_usage	>80%
	基础监控-load5	load5	>3
DBP-dbpconsole	基础监控-端口监控	80 2022 8341 9500	不通
MQ-msgconsole	基础监控-端口监控	2022 8066	不通

8.3.1.2 自定义业务监控检查

通过 corewatch 内核态监控产品查看注册中心产品各项系统监控指标是否有异常告警产生。访问路径是：corewatch > 自定义监控 > 共享中间件 > DatabaseProxy。

如果有异常告警产生，联系蚂蚁金服技术支持进行排查。

8.3.2 业务功能检查

1. dbpconsole 服务验证
   - 执行以下命令，如果未检查到失败的项目，表示服务正常。

     ```
     curl 127.0.0.1:9500/checkService | grep false
     ```

   - 登录数据访问代理控制台，检查各项页面功能是否正常无报错。
2. dbpserver 服务验证
   - 执行以下命令，检查服务是否正常。

     ```
     ps aux | grep java
     ```

   - 执行以下命令，查看 startup.log。如果日志中出现 CobarServer is started and listening on 8066，表示应用启动成功。

     ```
     less /home/admin/logs/zdalproxy/startup.log
     ```

8.4 服务异常应急预案

8.4.1 概述

适用范围

底座	产品版本
Antstack	1.0 - 1.3

问题描述或者背景

应用访问 DBP 异常情况。

8.4.2 环境检查

1. 尝试在相同网段机器上执行以下命令，测试连通性。

   ```
   ping dbp lb IP 地址
   ```

2. 登录云游，检查 DBP 容器状态。
3. 登录 DBP 容器，执行以下命令，检查 DBP 进程是否运行、端口 8066 是否监听。

```
#ps -fe | grep java
#netstat -an | grep 8066
```

8.4.3 实施步骤

1. 如果容器为节点宕机状态，判断是否存在物理机宕机。如果存在，则参考 物理机宕机应急预案 对故障物理机上运行的容器进行宕机迁移，并在新宿主机上启动容器。
2. 如果容器为退出状态，可以在云游上启动 DBP 容器。
3. 如果容器为运行中状态，但 Java 进程未运行，在云游上重启该 DBP 容器。

8.4.4 结果验证

1. DBP 前端挂载的 LB IP 可达。
2. DBP 进程正常。
3. DBP 可以与后端 db 实例通信。
4. 应用可以正常访问 DBP。

8.4.5 回滚方案

无

8.4.6 补充说明

无

9.云产品中台

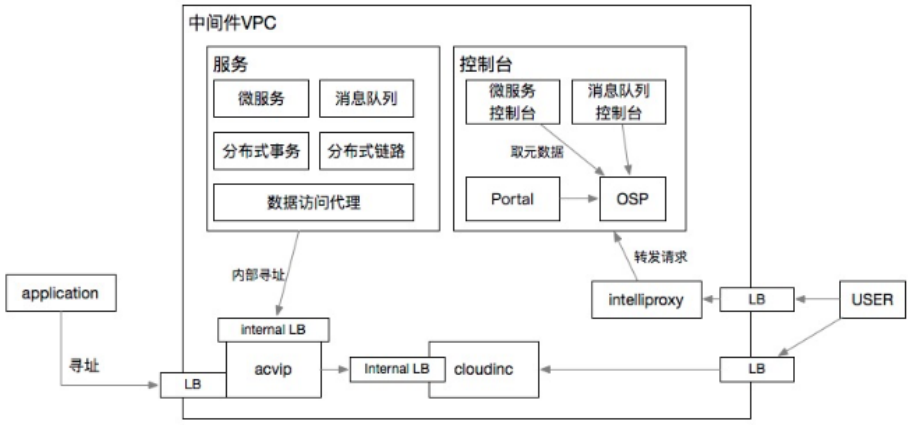
9.1 系统组件说明

9.1.1 组件角色说明

中间件门户产品包括以下 3 个组件：

- **Intelliporxy**：全局微服务代理层。
- **Portal**：中间件平台的门户。
- **OSP**：支撑中台系统

9.1.2 组件拓扑说明



9.1.3 资源清单说明

组件	资源依赖	服务端口
Intelliporxy	N/A	80
Portal	N/A	80
OSP	N/A	80 & 8341

9.2 监控和预警说明

9.2.1 系统监控指标和预警项清单

监控指标	监控指标说明	预警项说明
Intelliproxy 磁盘空间监控	磁盘空间占用率监控	大于 80% 预警
Intelliproxy 端口监控	端口是否可以访问	端口号：80
Intelliproxy 内存监控	内存占用率	大于 80% 预警
Intelliproxy CPU 利用率	CPU 利用率	大于 80% 预警
Portal 磁盘空间监控	磁盘空间占用率监控	大于 80% 预警
Portal 端口监控	端口是否可以访问	端口号：80，8080
Portal 内存监控	内存占用率	大于 80% 预警
Portal CPU 利用率	CPU 利用率	大于 80% 预警
OSP 磁盘空间监控	磁盘空间占用率监控	大于 80% 预警
OSP 端口监控	端口是否可以访问	端口号：80，8080
OSP 内存监控	内存占用率	大于 80% 预警
OSP CPU 利用率	CPU 利用率	大于 80% 预警

9.3 系统日志说明

9.3.1 Portal

9.3.1.1 系统运行日志

Portal 系统运行日志路径为 /home/admin/logs/node-stdout.log，记录应用启动和运行过程中的全部日志。

9.3.1.2 系统错误日志

Portal 系统错误日志路径为 /home/admin/logs/node-stderr.log，记录应用运行过程中抛出的错误信息，主要包括代理转发过程中的错误信息。

9.3.2 OSP

9.3.2.1 系统运行日志

/home/admin/logs/ 目录下记录应用启动和运行过程中的全部日志。

其中，/osp 子目录是 OSP 系统主要运行日志，它底下的具体日志的说明如下：

- /home/admin/logs/osp/user-façade.log 是跟用户鉴权相关的日志。
- /home/admin/logs/osp/openapi.log 是跟 openapi 请求转发相关的日志。
- /home/admin/logs/osp/operation/product-instance.log 是跟产品启动相关的日志。

9.3.2.2 系统错误日志

OSP 系统错误日志路径为 /home/admin/logs/osp/common-error.log，记录应用启动和运行过程中抛出的错误信息。

9.3.3 Intelliproxy

9.3.3.1 系统运行日志

/home/admin/logs/ 目录下记录应用启动和运行过程中的全部日志。

其中，/home/admin/logs/access.log 日志记录所有经过 Intelliproxy 代理转发的 REST 服务 API 的流量，不会记录静态资源或者非符合标准规范的 API 请求。

9.3.3.2 系统错误日志

Intelliproxy 系统错误日志路径为 /home/admin/logs/common-error.log，记录应用启动和运行过程中抛出的错误信息。

9.4 常见运维场景说明

9.4.1 中间件门户首页页面无法访问

1. 确认 OSP 系统已经部署成功。

2. 使用中间件租户账号登录 OSP 管理员后台，检查 Portal 是否正常上报机器 IP 地址（地址为 \${OSP 域名}/api/admin/services/osp/addresses）。
3. 如果 IP 未上报，则查看 Portal docker 镜像的日志信息。

9.4.2 中间件门户首页可以访问，但首页监控视图部分数据显示不正确或无数据

可能是 **监控预警** 产品的问题和异常。

9.4.3 首页可以访问，但页面显示（或加载时）有错误提示

1. 进入 **监控预警** 控制台，选择 **应用视图**。
2. 选择 **000001** 实例 ID （只有中间件租户账号可以看见实例 ID 并进行此操作）。
3. 搜索应用 **OSP**，查看其 JVM 监控视图。
4. 如果 JVM 从某个时刻开始有跌 0，则 OSP 应用可能非正常退出。
5. 此时，可通过 **发布部署服务**，查询定位到具体的应用，选择异常的服务实例点击 **重启应用**。

9.5 服务巡检

9.5.1 系统组件监控检查

9.5.1.1 基础监控检查

登录 corewatch 监控系统，查看系统中台组件相关系统组件有无异常告警，需要关注的监控项内容如下表所示。

应用	分类	指标（关键字）	告警阈值
INTELLIPROXY-intelliproxy OSP-osp PORTAL-portal	基础监控-cpu 使用率监控	cpu_usage	>80%
	基础监控-内存使用率监控	mem_usage	>80%
	基础监控-磁盘使用率监控	disk_usage	>80%
	基础监控-load5	load5	>3
INTELLIPROXY-intelliproxy	基础监控-端口监控	80 2022	不通
OSP-osp	基础监控-端口监控	2022 8341	不通

PORTAL-portal	基础监控-端口监控	80 2022	不通

9.5.1.2 自定义业务监控检查

通过 corewatch 内核态监控产品查看注册中心产品各项系统监控指标是否有异常告警产生。访问路径是：corewatch > 自定义监控 > 共享中间件 > 中间件控制台（OSPPORTALPROXY）。

如果有异常告警产生，联系蚂蚁金服技术支持进行排查。

9.5.2 业务功能检查

1. OSP 服务验证
   - 执行以下命令，判断监听端口是否正常。

     ```
     netstat -an | grep 80
     ```

   - 执行以下命令，判断业务端口是否存活。

     ```
     netstat -an | grep 8341
     ```

   - 执行以下命令，判断 acvip 连接。

     ```
     netstat -an|grep 9003
     ```

   - 执行以下命令，判断注册中心连接。

     ```
     netstat -an|grep 9600
     ```

   - 访问 sofa-osp.{domain}/admin/index.html 页面，判断是否能正常访问。
   - 访问 http://sofa-osp.{domain}/api/admin/services/{ms/mq/dds/...}/addresses 页面，查看 OSP 上订阅的地址，不应为空，并且每个服务都至少有两个以上地址返回，否则就存在单点问题。
2. Intelliproxy 服务验证
   - 执行以下命令，判断业务端口是否正常。如果端口没有启动，那通常是程序启动失败，需要通过排查 common-error.log 日志解决。

     ```
     netstat -an | grep 80
     ```

   - 执行以下命令，判断 acvip 连接。

```
netstat -an|grep 9003
```

- 执行以下命令，判断注册中心连接。

```
netstat -an|grep 9600
```

3. Portal 服务验证

   访问 http://sofa-portal.{domain} 页面，查看各页面功能是否正常。

10. 服务发现组件

10.1 系统组件说明

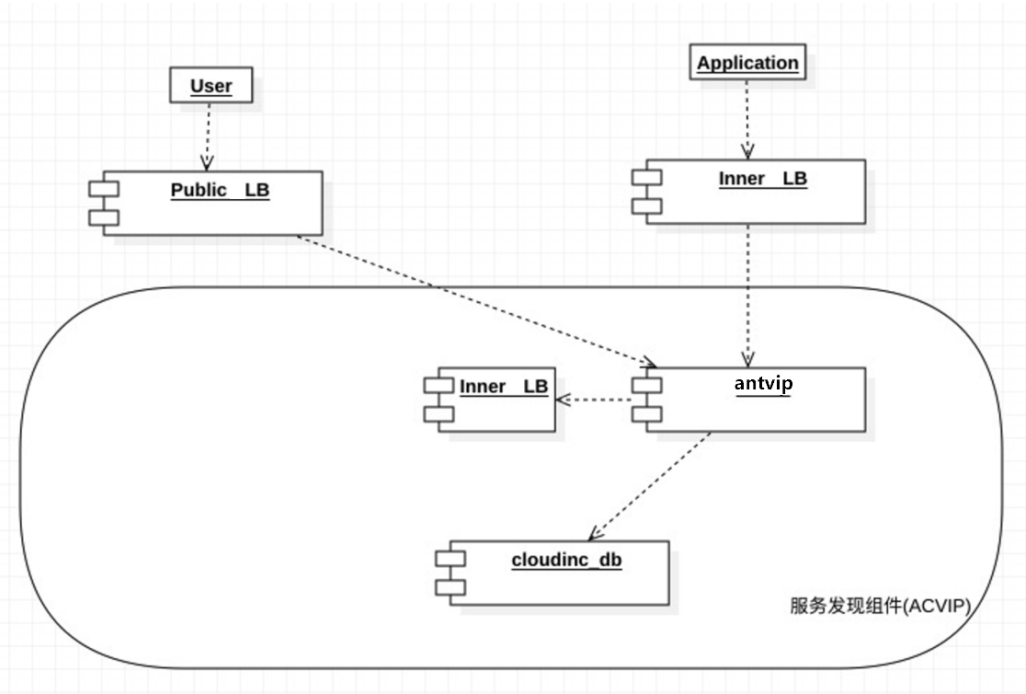
10.1.1 组件角色说明

产品包含以下 1 个组件：

ACVIP：Ant Cloud VIP，负责域名 IP 的健康检查（health check），提供域名可用 IP 节点。

10.1.2 组件拓扑说明

- **LB**：多节点之间的负载均衡服务。
  - **Public LB**：公网 LB，主要用于域名配置的修改、添加。
  - **Inner LB**：内部 LB，主要为 OSP 提供接口服务的负载 LB。
- **Application**：用户应用系统。
- **User**：用户浏览器。



10.1.3 资源清单说明

组件	资源依赖	服务端口

ACVIP	2 * 服务器（4 CPU，8G 内存，100G 磁盘）	9003
域名元数据存储	1 * RDS (4CPU，2G 内存，100G 磁盘)	3306

10.2 监控和预警说明

10.2.1 系统监控指标和预警项清单

监控指标	监控指标说明	预警项说明
ACVIP 磁盘空间监控	磁盘空间占用率监控	预警触发条件：大于 80%
ACVIP 端口监控	9003	预警触发条件：端口 9003 无法访问
ACVIP 内存监控	内存占用率	预警触发条件：大于 80%

10.2.2 预警项运维动作说明

10.2.2.1 ACVIP 磁盘空间预警

预警项说明

ACVIP 服务节点磁盘空间预警

运维动作说明

登录对应的服务器，进入 /home/admin/logs/acvip 目录，对大文件进行清除。一般是 common-default.log 文件。

10.3 系统日志说明

10.3.1 日志文件清单说明

10.3.1.1 ACVIP 系统关键日志文件清单

日志文件名称	日志文件路径	日志文件描述
SyncWeb.log	/home/admin/logs/acvip/SyncWeb.log	ACVIP 轮询日志

日志文件名称	日志文件路径	日志文件描述

日志文件名称	日志文件路径	日志文件描述
common-error.log	/home/admin/logs/acvip/common-error.log	系统错误日志

10.4 常见运维场景说明

10.4.1 ACVIP server 节点存活状态

通过以下任一方式，确认 ACVIP server 节点存活状态。

- 登录对应的服务器，执行以下命令，查看进程和端口是否存在。

```
ps -ef | grep AntVipServerBootstrap
```

- 登录 ACVIP 控制台查看，如下图所示。

10.4.2 ACVIP 拉取不到域名列表

在应用端日志里面出现 Domain Not Found，但该域名在 ACVIP 上存在。登录 ACVIP 控制台，可查看到 ACVIP 节点显示不可用，但进程和端口都存在，且心跳时间也在变化，如下图所示。

此时，需要确认 ACVIP 服务器 上的时间和数据库的时间是否一致。如果不一致，则要对数据库所在主机的时间以及应用所在主机的时间进行调整同步，保持一致。

10.5 服务巡检

10.5.1 系统组件监控检查

10.5.1.1 基础监控检查

登录 corewatch 监控系统，查看 ACVIP 相关系统组件有无异常告警，需要关注的监控项内容如下表所示。

应用	分类	指标（关键字）	告警阈值
ACVIP-acvip ACVIP -antvip ACVIP -cloudinc	基础监控-cpu 使用率监控	cpu_usage	>80%
	基础监控-内存使用率监控	mem_usage	>80%
	基础监控-磁盘使用率监控	disk_usage	>80%
	基础监控-load5	load5	>3
ACVIP -acvip	基础监控-端口监控	2022 3	不通

说明：

- 0.7.0 以下版本，存在两个应用：antvip 和 cloudinc。
- 0.7.0 及以上版本，合并为一个应用：acvip。

10.5.1.2 自定义业务监控检查

通过 corewatch 内核态监控产品查看注册中心产品各项系统监控指标是否有异常告警产生。访问路径是：corewatch > 自定义监控 > 共享中间件 > ACVIP。

如果有异常告警产生，联系蚂蚁金服技术支持进行排查。

10.5.2 业务功能检查

1. ACVIP 服务验证
   - 执行以下命令，检查 9003 端口是否有监听。

     ```
     netstat -an | grep 9003
     ```
2. acvip 域名

   其他中间件部署之后，需确认 acvip 域名创建成功以及 IP 挂载正常。

   acvip 域名可以在 acvip 控制台查看，acvip 控制台的访问地址是：public-lb vip 或 ip。
3. 检查 antvip server 节点存活状态，可以通过以下任一方式查看。
   - 直接登录对应的服务器查看进程和端口是否存在。

     ```
     ps -ef | grep acvip-web
     ```
   - 登录 acvip 控制台，查看 antvip server 信息。


首页 / AntVip Server信息
Antvip管控
数据信息
Server信息
ZONE信息
系统配置
DNS管控
AntVip Server信息
ENV
acvip-antvip-1
可用
权重 5
最近心跳 2018-07-03 17:56:51
负责域名 29 个
查看负责域名

11. 物理机

11.1 物理机宕机应急预案

11.1.1 概述

适用范围

底座	产品版本
AntStack/阿里云	1.0.1 ~ 1.2.3

问题描述或者背景

非 ops 物理机出现宕机。

风险说明

1. Docker 版本 1.11.1-00868fc 以下的容器可能存在配置文件损坏无法恢复、迁移的情况。
2. 云游 1.2.1 以下版本宕机迁移功能并未默认打开。
3. 需要有足够的物理资源进行迁移。

11.1.2 环境检查

1. 登录云游，确认物理机状态。

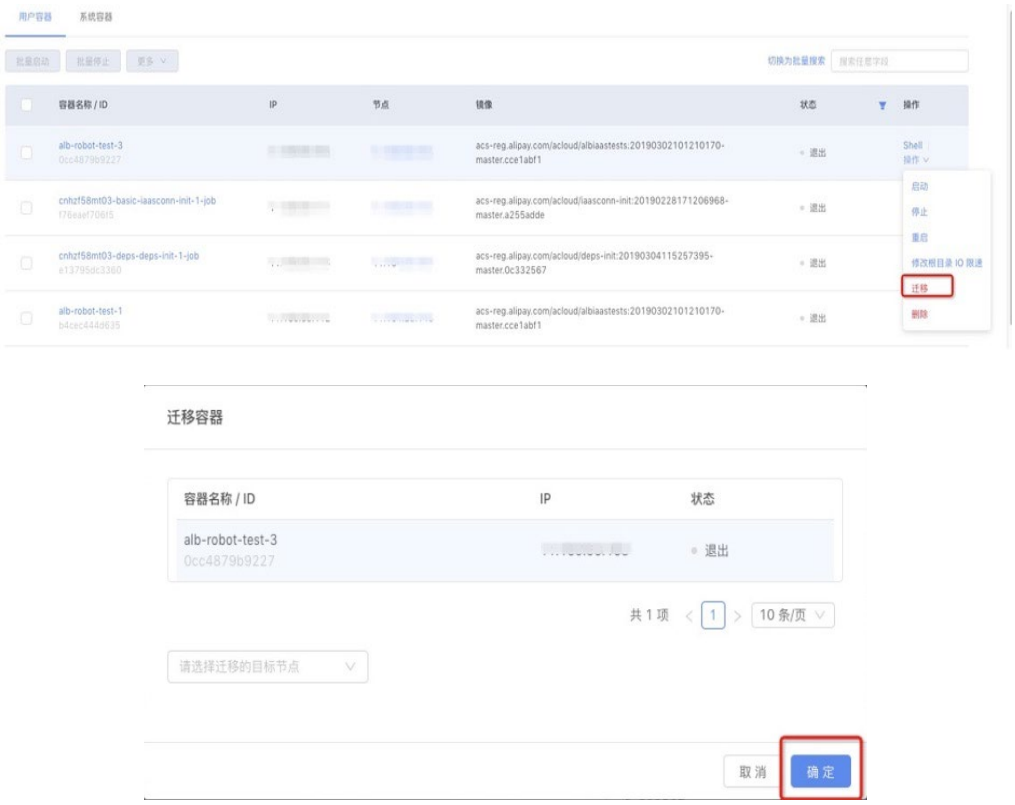
2. 测试节点连通性

```
#ping <节点 IP>
```

3. 如果节点 IP 不可达（包括重启节点后云游上显示节点状态依旧为“宕机”）,按照如下步骤进行迁移.

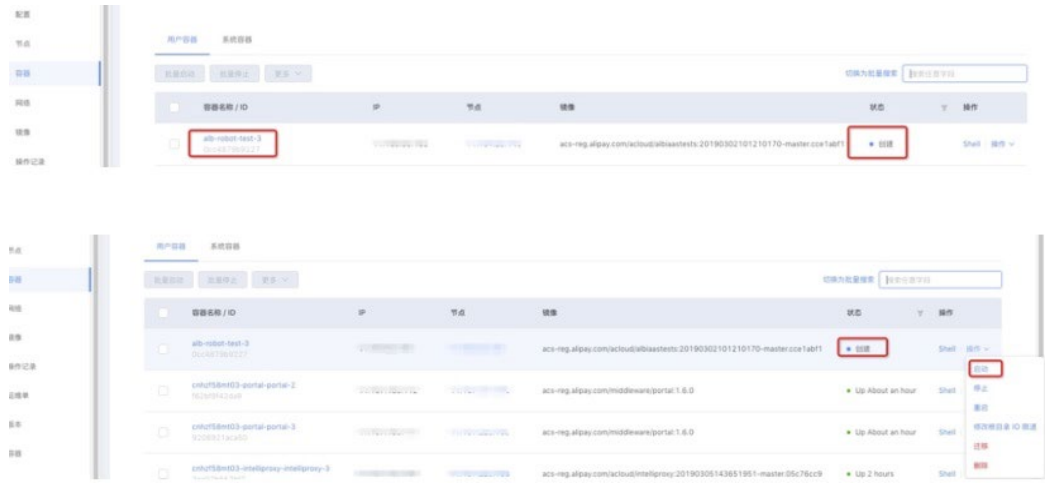
11.1.3 实施步骤

1. 登录云游，云游 > **资源管理** > **节点** > **用户容器** > **操作** > **迁移**，在弹出的对话框中点击 **确认**。



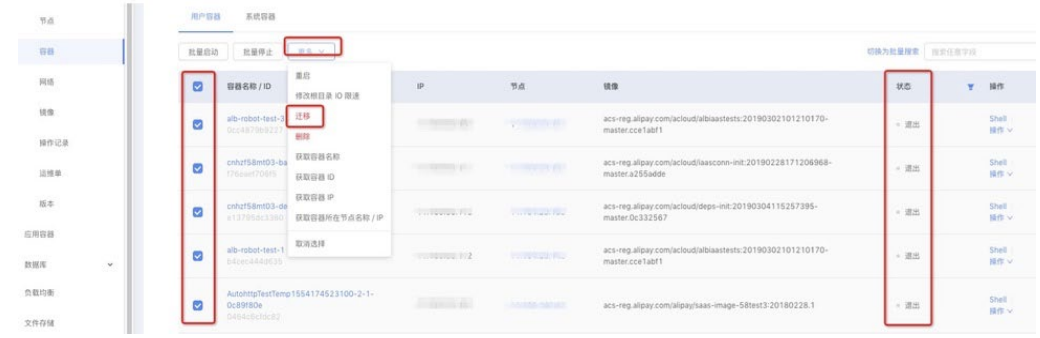
2. 确保迁移结果返回为已结束。

3. 启动迁移成功的容器。



4. 确定启动后的容器状态为 Up xx Seconds。

5. 按照步骤 1~4 顺序对其他容器进行迁移或者按照如下方法进行容器批量迁移（建议每次批量迁移总数不超过故障物理机容器总数的 30%）。



11.1.4 结果验证

所有迁移到其他物理机的容器状态为“Up xxx Seconds”。

11.1.5 回滚方案

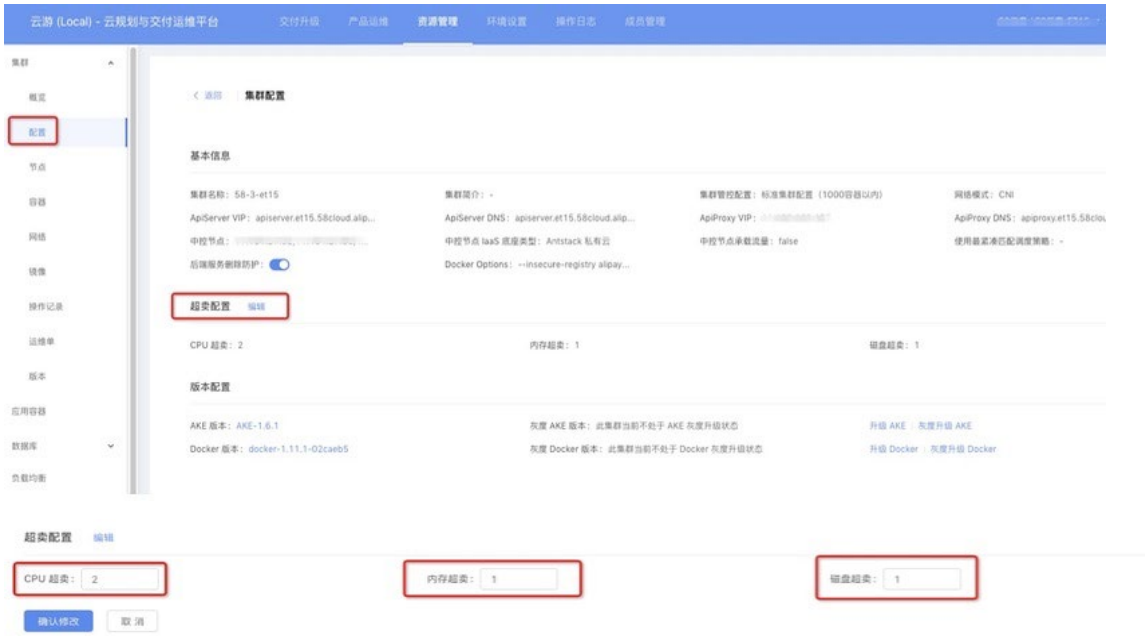
无。

11.1.6 补充说明

如果没有足够的物理机资源，可以临时调整 AKE 集群超卖比后进行宕机迁移，但可能导致集群

服务的不稳定。请参照以下说明调整 AKE 集群超卖比和宕机迁移。

1. 调整 AKE 集群超卖比。



2. 按照上文宕机迁移步骤对业务容器进行迁移。

11.2 物理机异常重启

11.2.1 概述

适用范围

底座	产品版本
AntStack/阿里云	1.0.1 ~ 1.2.3

问题描述或者背景

作用于物理机异常重启的容器恢复。

风险说明

docker 版本 1.11.1-00868fc 以下的容器可能存在配置文件损坏无法恢复的情况。

11.2.2 环境检查

1. 登录云游，确认物理机状态。

2. 测试节点连通性。

```
#ping <节点 IP>
```

3. 检测节点 IP 是否可达（包括重启节点后云游上显示节点状态依旧为“宕机”）。

11.2.3 实施步骤

1. 恢复物理机状态。

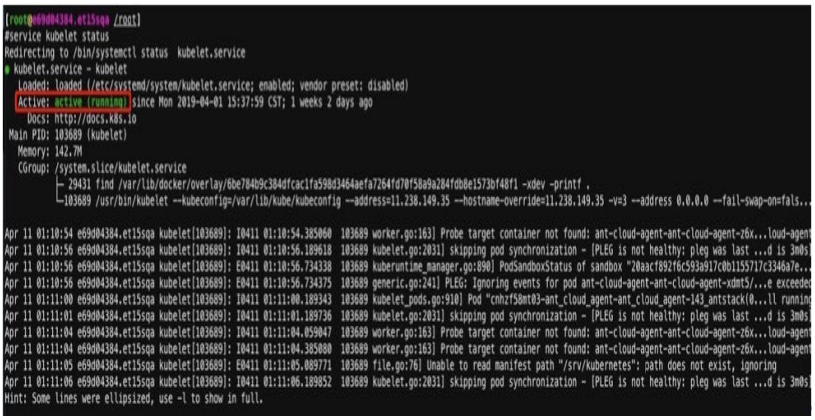
   - 在云游 > 资源管理 > 节点 > Shell > 执行以下命令。

     ```
     # service kubelet start
     ```

   - 验证 kubelet 服务状态。

     ```
     #service kubelet status
     ```

   - 确认 kubelet 进程状态为 active。



2. 恢复故障物理机上的容器

检查节点关联的容器状态。如果为退出状态，则勾选所有退出容器，选择 **批量启动**，确认所有容器状态为"Up xx Seconds"。

11.2.4 结果验证

物理机在云游状态为 “健康，可调度”。

容器在云游上状态为“Up xxx Seconds”。

11.2.5 回滚方案

无。

11.2.6 补充说明

无。

12. 故障排查快速指南

12.1 紧急情况

在遇到以下情况时，建议您立即联系蚂蚁金服技术支持团队。

- 机房掉电。
- 服务器宕机且未自动重启，或重启后依然有问题。
- 数据丢失。
- 误操作且无法回滚，可能会造成业务损失。

12.2 一般故障排查

针对一般故障，排查步骤如下：

1. 查看监控平台。在监控平台查看各容器（应用）的健康状况。如果有报错，则根据报错信息进行排查。

2. 查看日志。

3. （谨慎操作！）重启容器。在不影响数据存储、业务正常运行的前提下，可以重启相应容器并检查其运行状态。


蚂蚁金服
ANT FINANCIAL
金融科技
FINANCIAL TECHNOLOGY