SOFAStack

高可用管理平台
技术白皮书

产品版本：AntStack Plus 1.13.1

文档版本：20230708

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

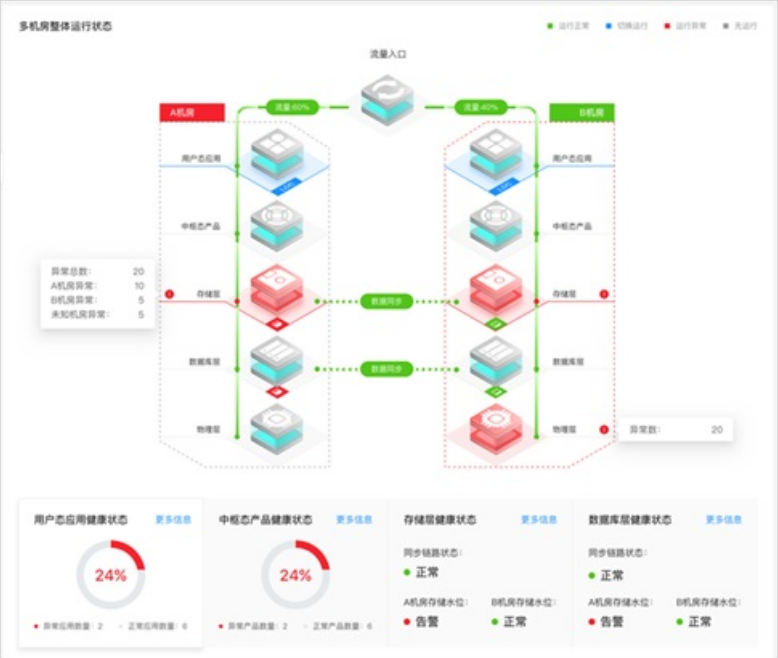
1.什么是高可用管理平台

1.1. 概述

高可用管理平台（High Availability Service，HAS）是以容灾为主的高可用管控平台产品，可实现容灾方案的端到端整体能力，从客户业务到中间件、PaaS 以及 IaaS 整体的容灾切换及恢复、容灾规划、容灾模拟演练等能力，并包含整体机房及容灾状态的监控能力、容灾大盘展示、环境巡检、风险应急等。

容灾系统是指在相隔较远的异地，建立两套或多套功能相同的系统，系统之间可以相互进行健康状态监视和功能切换，当一处系统因意外（如火灾、洪水、地震、人为蓄意破坏等）停止工作时，整个应用系统可以切换到另一处，使得该系统功能可以继续正常工作。容灾系统需要具备较为完善的数据保护与灾难恢复功能，保证生产中心不能正常工作时数据的完整性及业务的连续性，并在最短时间内由灾备中心接替，恢复业务系统的正常运行，将损失降到最小。

高可用管理平台页面如下图：



1.2. 产品背景

面向金融行业输出时，监管对金融行业有比较高的要求，尤其看重高可用能力，需要具备一定的容灾等级。高可用管理平台作为 SOFAStack 对外输出提供统一容灾管控平台，满足运行过程中产品的容灾、巡检、故障排查等方面的诉求，为客户提供端到端的高可用容灾体系服务。

1.3. 金融行业要求现状

《云计算技术金融应用规范容灾》（JR/T 0168-2018）要求，根据应用于金融领域的云计算平台发生故障或瘫痪的影响范围、危害程度，将其容灾能力等级划分为 6 级，应用于金融领域云计算平台至少应达到容灾能力 3 级要求。

表2　应用于金融领域的云计算平台容灾能力等级关键指标要求

容灾等级	RTO	RPO	可用性
3 级	≦24 小时	≦24 小时	每年非计划服务中断时间不超过 4 天，系统可用性至少达到 99%。
4 级	≦4 小时	≦1 小时	每年非计划服务中断时间不超过 10 小时，系统可用性至少达到 99.9%。
5 级	≦30 分钟	≈0	每年非计划服务中断时间不超过 1 小时，系统可用性至少达到 99.99%。
6 级	≦2 分钟	0	每年非计划服务中断时间不超过 5 分钟，系统可用性至少达到 99.999%。

表6　第3级技术要求

要素	云计算相关要求
数据备份	a）关键数据至少有一个数据副本处于异地或同城可用区； b）完全数据备份至少每天一次且处于同城或异地可用区。
数据处理	a)在异地或同城可用区具备灾难恢复所需的部分备用数据处理能力； b）应确保云计算资源调度能力满足在数小时内配备灾难恢复所需的全部备用数据处理能力。
网络能力	a）应确保异地或同城可用区的虚拟网络、物理网络、出口网络带宽及链路配置在数小时内达到与生产系统的网络能力相同，关键资源处于就绪状态； b）应支持跨可用区的自动或集中切换。
运维能力	a）云计算平台应能够对灾备能力进行集成管理，具备流量集中切换能力； b）灾难事件发生后，备份数据中心的云计算资源管理和调度平台仍可完成对备份数据中心的资源管理和调度； c）云计算平台需要为关键的用户运营数据，如审计日志等，提供数据备份。

1.4. 面临的问题及关键挑战

数据安全性的需求增长

企业的业务运转越来越依赖于数据，而数据就成了企业动作的基础。因此数据的安全性和服务的可用性显得越来越重要。建立异地容灾系统，现如今已经成为了企业的最佳选择，它可以在数据面临各种灾难时仍然保证其安全性和可用性，以支撑企业的关键业务运作。是否具有容灾系统，也正成为企业竞争力的一个体现。

服务的可用性要求更高

企业正在将越来越多的资源用于确保业务的连续运营。而数据的丢失必然会导致企业正常的业务运作中断，带来巨大的经济损失、声誉损失、以及客户忠诚度下降等各种损失。

数据丢失和服务不可用的后果也是非常惨痛的。IDC 统计数字表明，美国在 2000 年以前的 10 年间发生过灾难的公司中，有 55% 当时倒闭。剩下的 45% 中，因为数据丢失，有 29% 也在两年之内倒闭，生存下来的仅占 16%。如何保证大量集中数据在各种灾难面前的安全性，以支撑业务的连续性运行就成为了一个现实的问题。

成本

以最低的成本构建弹性存储架构，适应数据的高增长。

2.产品优势

金融级容灾

- 容灾等级最高可达 5 级。
- 容灾能力丰富，支持容灾大屏监控告警、容灾仿真演练、容灾巡检等能力。
- 经过支付宝和网商银行规模验证。

全链路容灾

支持从客户应用到中枢态的全链路容灾能力，实现端到端整体容灾，全链路监控和运维，无需多平台对接。包含用户应用、中间件、PaaS、IaaS 全链路多层容灾。

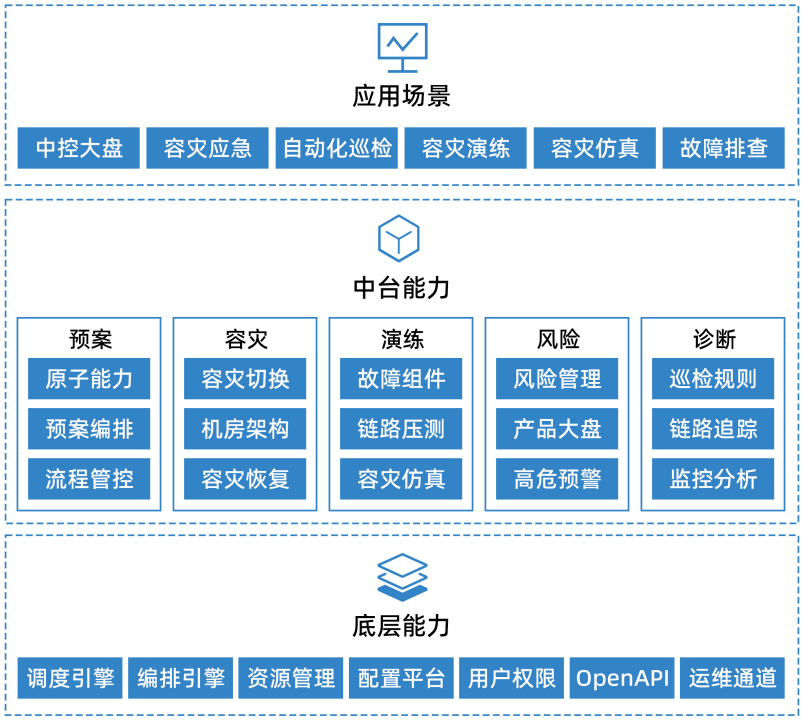
多场景容灾

支持金融行业的全部容灾场景：

- 同城双活
- 异地主备
- 两地三中心
- LDC 单元化

3.产品架构

产品架构



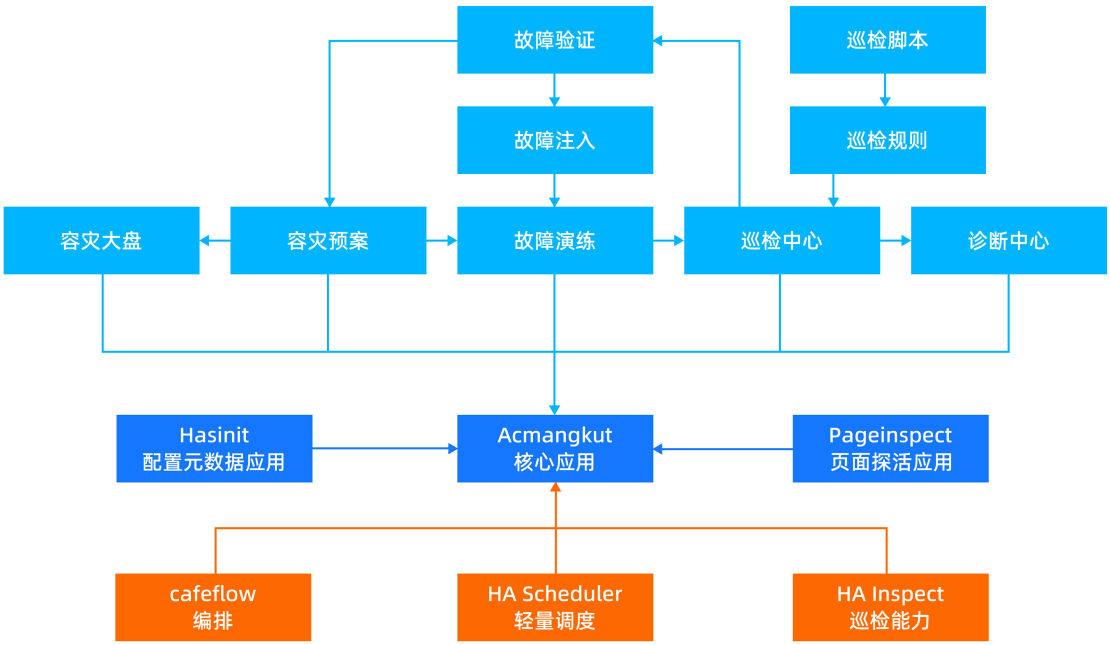
底层依赖

高可用管理平台自身必须需要具备足够的稳定性和高可用能力，在灾难发生时能够保证平台自身的可用性，因此在依赖上必须做到尽量精简，不能过分依赖其他组件的高可用特性。这就要求从底层能力上，平台必须做到对于调度引擎、编排引擎、OpenAPI 等在内的基础功能的自包含。

中台能力

高可用管理平台部署在不同的专有云和域内站点，例如网商银行、国际站点、客户站点，主要负责站点的实际任务执行。该平台围绕容灾为核心，建设相关的诊断、预案、风险、演练能力。

系统架构

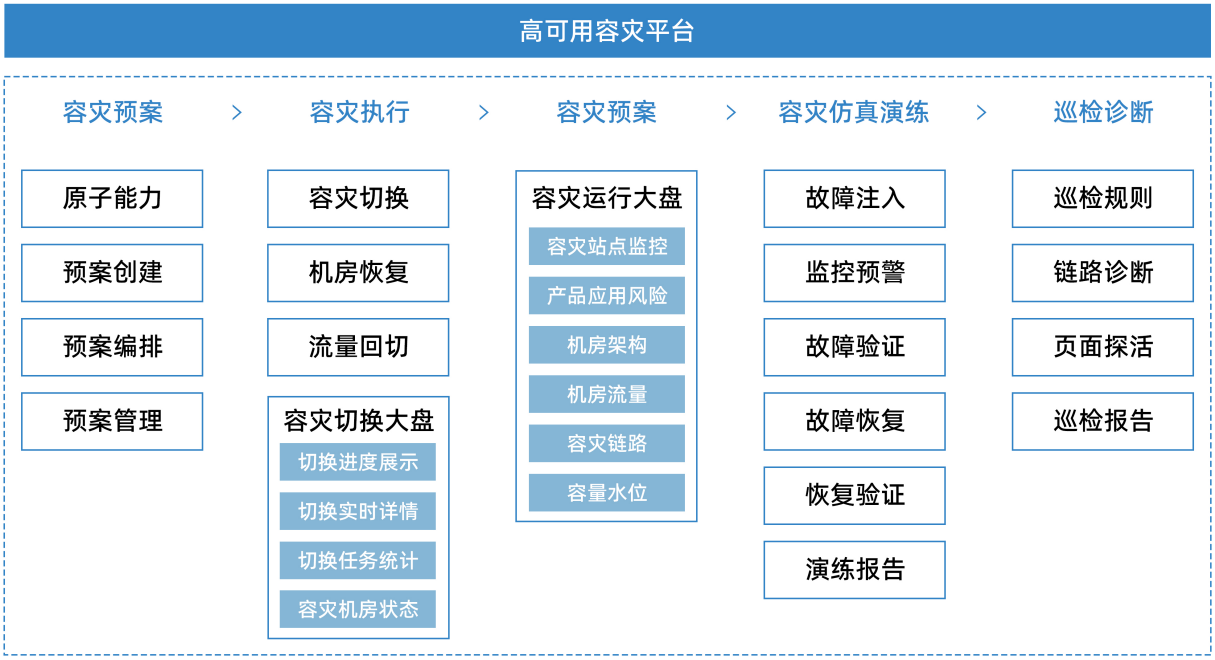


高可用管理平台的系统由 Acmangkut、Pageinspect 及 Hasinit 三个应用组成。

- Acmangkut 是 HAS 主体核心应用，包含了容灾预案、巡检中心、故障演练等功能模块。
- Pageinspect 提供页面探活能力，Acmangkut 会依赖 Pageinspect 做页面探活。
- Hasinit 是产品后置任务，会初始化 HAS 相关的权限元数据。

4.功能特性

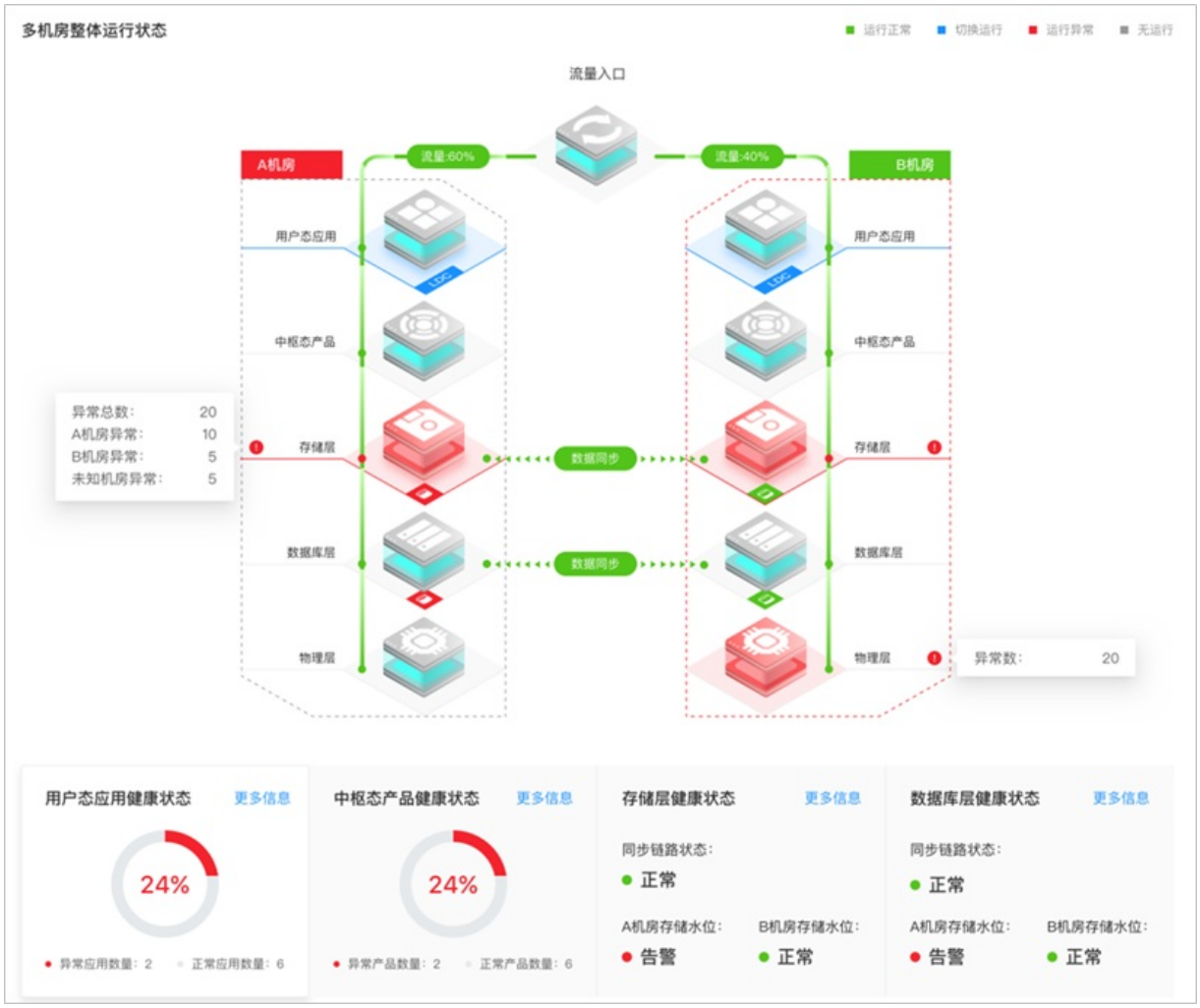
高可用管理平台主要定位于高可用容灾场景，产品主要能力包括容灾运行大盘、容灾切换大盘、容灾预案中心、机房详情信息展示、故障仿真演练、巡检中心、诊断中心。



容灾运行大盘

容灾大盘为用户提供了一个全局视角，可查看整个多机房容灾架构图，以及多机房的运行状态情况，方便用户查看机房的整体运行情况，判断是否可进行容灾切换以及排查常见问题等。

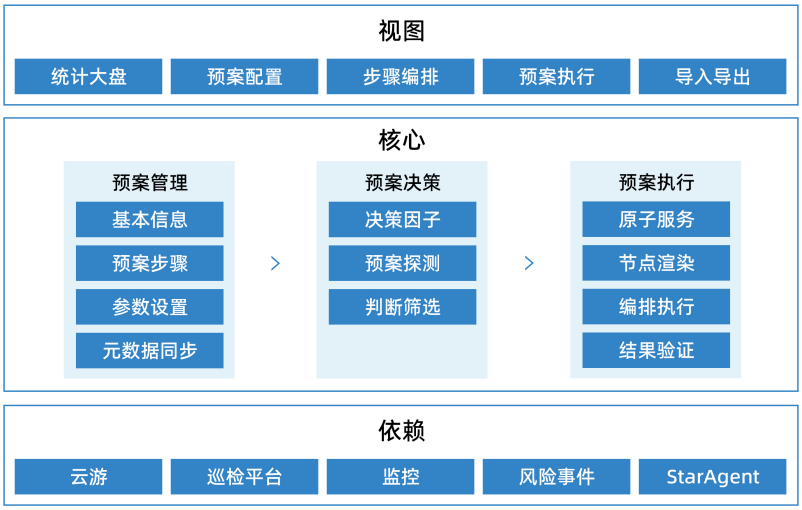
容灾大盘架构主要分为业务层、中枢层、存储层、数据库层、物理层等，分别展示不同层面的应用异常和告警情况。其中存储层和数据库层，除了应用异常监控外，还包括数据同步链路以及容量水位情况的监控。



容灾预案中心

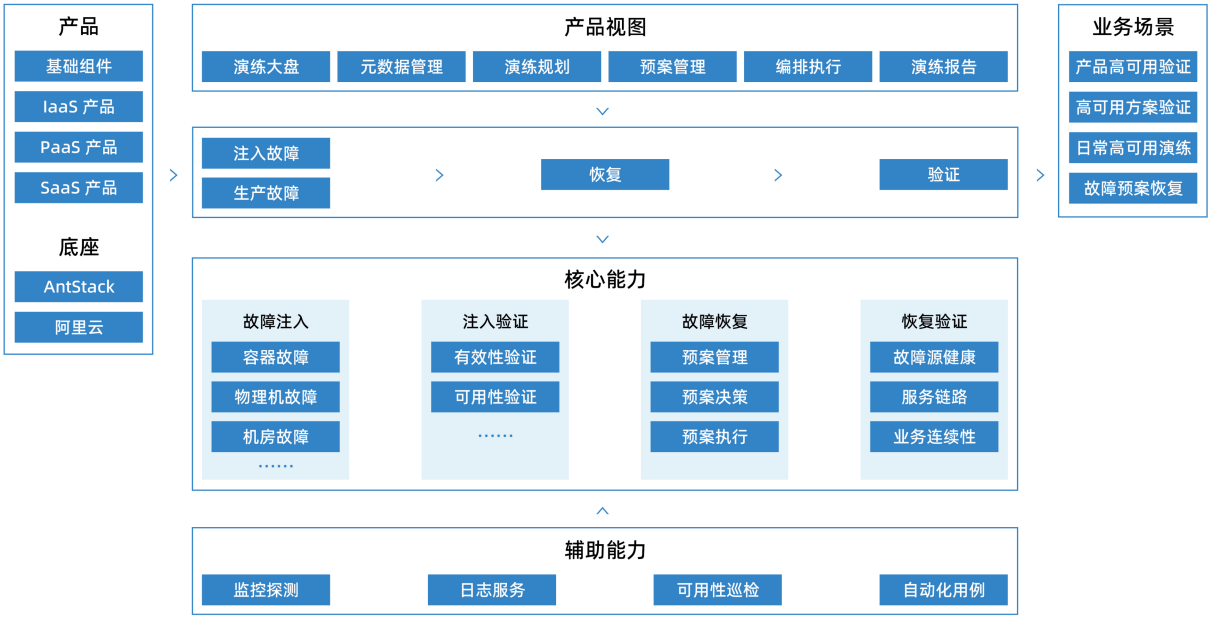
容灾预案中心是基于产品、站点运行期以及容灾切换中沉淀的相关故障应急措施，提供一站式预案管理、预案决策以及预案编排执行的产品能力。具备以下几个特点：

- **可复用**：历史问题、通用问题的解决方法和应急方案可以不断沉淀积累，并在各个站点复用。
- **透明化**：应急处理过程、处理方式、做了什么变更等一目了然。
- **高效率**：提高应急处理效率，尽可能减少故障恢复的时间。原来需要根据文档判断并按照文档手动变更的方式，变为根据场景定位到预案后直接一键执行。
- **降成本**：把应急处理措施预案化，降低学习门槛、人员投入成本、站点维护成本等。



故障演练

作为蚂蚁智能科技产品专有云输出业务场景下，多维度、全生命周期故障演练和故障预案恢复的一站式支撑平台，高可用管理平台服务于产品高可用验证、解决方案高可用验证以及客户环境的故障演练、故障预案恢复等场景，帮助提升产品、集群、机房的稳定性，减少故障的发生，提高故障应急效率，提升产品竞争力。



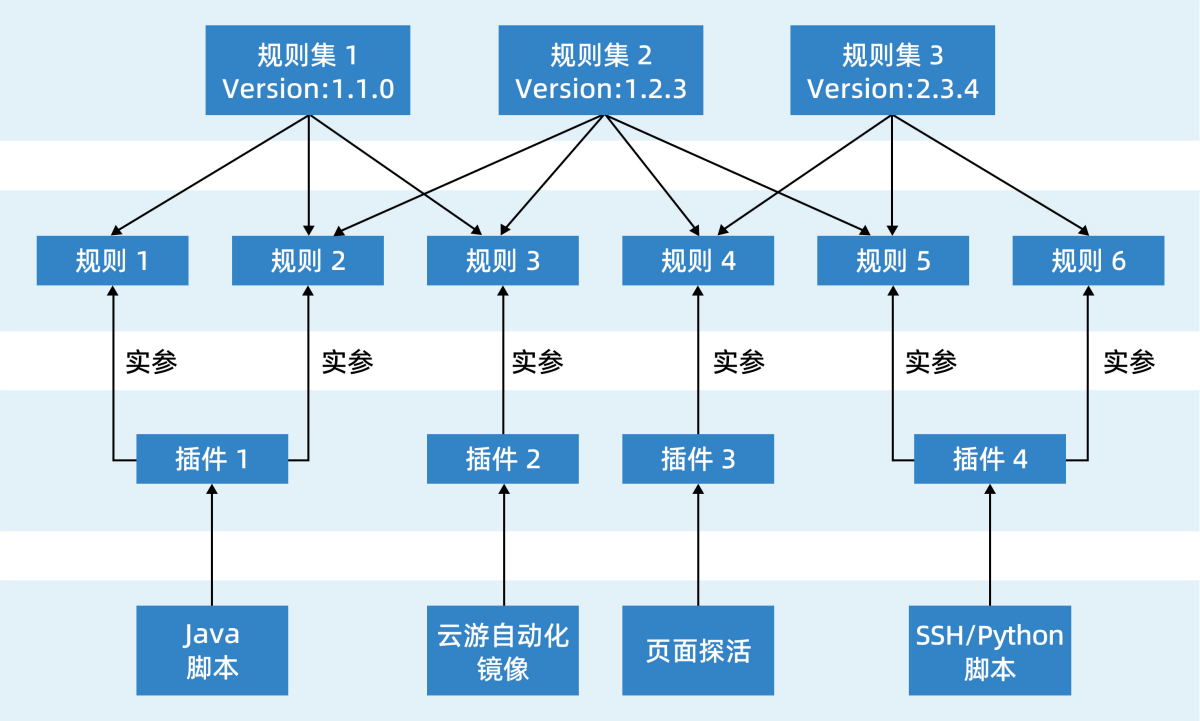
巡检中心

巡检中心与故障演练和预案中心配合联动使用，在故障演练和预案执行过程中，故障注入是否成功导致应用异常，可做巡检验证判断。除容灾场景外，巡检中心还可自动化运行多项日常运维的脚本，减少人工巡检执行脚本的工作，并支持定期可控巡检，便于日常运维和掌握站点的健康信息，大大减轻运维人员的排查问题负担和时间。

巡检中心主要能力包括巡检规则、任务执行、巡检报告等，并且巡检能力丰富，拥有多种原子能力：

- Java 脚本执行
- 云游自动化测试镜像执行
- SSH/Python 脚本下发及执行
- 页面探活能力

巡检的核心架构模型如下图：



5.性能指标

应用名称	规格	QPS	TPS	说明
Acmangkut	4C8G	500	50	Acmangkut 为前端 Web 应用，包含多个功能模块，因此一个 4C8G 容器的直接压测数据可以达到 100 TPS/s。
Pageinspect	2C4G	500	50	Pageinspect 为页面探活的执行应用。
Hasinit	1C2G	无	无	无

6.基础术语

AKE

容器引擎（Ant Financial Kubernetes Engine，AKE）是将底层物理资源按照计算、网络、存储等进行切分和抽象的容器引擎。AKE 通过使用 Kubernetes 和 Docker 技术将整个物理资源进行池化，向上层服务提供按量使用的计算、网络和存储资源。

ALB

负载均衡（Ant Financial Load Balancer，ALB）是将访问流量根据转发规则分发到后端多台后端服务器的流量分发控制服务。通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。

IAM

蚂蚁科技身份访问管理（Identity and Access Management，IAM）控制台是管理成员、分配权限、管理身份源、查看操作记录的平台。

OceanBase

OceanBase 是阿里巴巴与蚂蚁科技独立自主研发的一款分布式关系数据库产品，融合传统关系数据库和分布式系统的优势，具备高可用、高性能、高可扩展性，在功能上兼容 MySQL 等特点，在通用硬件上提供金融级高可用的数据库服务。

RPO

数据恢复点目标（Recovery Point Objective，RPO），以时间为单位，即在灾难发生时，系统和数据必须恢复的时间点要求。RPO 标志系统能够容忍的最大数据丢失量。系统容忍丢失的数据量越小，RPO 的值越小。

RTO

恢复时间目标（Recovery Time Objective，RTO），以时间为单位，即在灾难发生后，信息系统或业务功能从停止到必须恢复的时间要求。RTO 标志系统能够容忍的服务停止的最长时间。系统服务的紧迫性要求越高，RTO 的值越小。

容灾预案

指包含容灾步骤的可执行预案。

页面探活

指通过浏览器打开巡检页面来判断页面存活情况。高可用容灾平台除了支持无需登录的静态页面探活外，还支持需要登录态的页面探活，也支持匹配页面的内容或元素来确定页面是否已渲染成功。在高可用容灾平台上，可以将页面探活配置成巡检任务以定时巡检页面。

云游

云游是蚂蚁科技的一站式专有云规划、交付、运维平台，管理着专有云从诞生到落地的整个生命周期。