



APUSIC
固若长城
睿比世界

用户手册

金蝶Apusic中间件云平台v8.0.5

版权声明

本文档所涉及的软件著作权、版权等知识产权已依法进行了注册，由金蝶天燕云计算股份有限公司合法拥有。受《中华人民共和国著作权法》《计算机软件保护条例》《知识产权保护条例》和相关国际版权条约、法律、法规以及其它知识产权法律和条约的保护。未经授权许可，不得非法使用。

免责声明

本文档包含的版权信息由金蝶天燕云计算股份有限公司合法拥有，受法律的保护，金蝶天燕云计算股份有限公司对本文档可能涉及到的非金蝶天燕云计算股份有限公司的信息不承担任何责任。在法律允许的范围内，您可以查阅并仅能够在《中华人民共和国著作权法》规定的合法范围内复制和打印本文档。任何单位和个人未经金蝶天燕云计算股份有限公司书面授权许可，不得使用、修改、再发布本文档的任何部分和内容，否则将被视为侵权，金蝶天燕云计算股份有限公司有依法追究其责任的权利。

本文档如有更新，不另行通知。对本文档中的问题您可向金蝶天燕云计算股份有限公司告知或查询。未经本公司明确授予的任何权利均予保留。

商标声明

 是深圳市金蝶天燕云计算股份有限公司向中华人民共和国国家商标局申请注册的注册商标，注册商标专用权由金蝶天燕合法拥有，受法律保护。未经金蝶天燕的书面许可，任何单位及个人不得以任何方式或理由对该商标的任何部分进行使用、复制、修改、传播、抄录或与其它产品捆绑使用销售。凡侵犯金蝶天燕商标权的，金蝶天燕将依法追究其法律责任。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

目录

- 1 修订说明
- 2 简介
- 3 产品架构
 - 3.1 功能架构
 - 3.2 功能清单
 - 3.3 部署架构
- 4 安装部署
- 5 主要功能
 - 5.1 首页
 - 5.2 资源中心
 - 5.2.1 主机管理
 - 5.2.1.1 云账号管理
 - 5.2.2 容器管理
 - 5.2.2.1 环境
 - 5.2.2.2 概览
 - 5.2.2.3 容器
 - 5.2.2.4 镜像
 - 5.2.2.5 网络
 - 5.2.2.6 卷
 - 5.2.3 Kubernetes 管理
 - 5.2.3.1 节点
 - 5.2.3.2 系统组件
 - 5.2.3.3 项目
 - 5.2.3.4 应用负载-无状态副本集
 - 5.2.3.5 应用负载-有状态副本集
 - 5.2.3.6 应用负载-守护进程集
 - 5.2.4 实例资产库
 - 5.2.4.1 实例资产库
 - 5.2.4.2 扫描特征
 - 5.2.4.3 扫描任务
 - 5.2.4.4 扫描记录
 - 5.3 仓库管理

- 5.3.1 制品管理
- 5.3.2 补丁管理
- 5.3.3 镜像仓库
- 5.4 中间件管理
 - 5.4.1 服务管理
 - 5.4.1.1 服务回收站
 - 5.4.2 实例管理
 - 5.4.2.1 平台实例
 - 5.4.2.2 纳管实例
 - 5.4.3 软件管理
 - 5.4.3.1 软件分类
 - 5.4.4 变更管理
 - 5.4.5 配置中心
- 5.5 云原生中间件管理
 - 5.5.1 云原生市场
 - 5.5.2 应用实例
- 5.6 可观测性
 - 5.6.1 采集配置
 - 5.6.1.1 指标采集
 - 5.6.1.2 日志采集
 - 5.6.2 告警规则
 - 5.6.2.1 告警模板
 - 5.6.2.2 告警规则组
 - 5.6.2.3 告警规则
 - 5.6.3 指标监控
 - 5.6.3.1 服务监控
 - 5.6.3.2 主机监控
 - 5.6.3.3 自定义监控
 - 5.6.4 日志中心
 - 5.6.4.1 日志分析
- 5.7 告警与事件
 - 5.7.1 告警总览
 - 5.7.2 告警事件
 - 5.7.3 告警收敛

- 5.7.3.1 告警抑制
 - 5.7.3.2 告警静默
- 5.8 平台运维
 - 5.8.1 平台巡检
 - 5.8.1.1 巡检概览
 - 5.8.1.2 巡检任务
 - 5.8.1.3 巡检规则
 - 5.8.2 批量操作
 - 5.8.2.1 文件上传
- 5.9 安全中心
 - 5.9.1 安全概览
 - 5.9.2 扫描任务
 - 5.9.2.1 扫描记录
 - 5.9.3 漏洞管理
 - 5.9.4 基线管理
 - 5.9.4.1 待处理项
 - 5.9.4.2 基线规则库
 - 5.9.5 安全配置
 - 5.9.5.1 漏洞库
- 5.10 平台运营
 - 5.10.1 租户管理
 - 5.10.1.1 租户管理
 - 5.10.2 授权管理
 - 5.10.2.1 文件授权
 - 5.10.2.2 集中授权
 - 5.10.2.3 在线实例
 - 5.10.2.4 授权台账
 - 5.10.2.5 授权台账看板
 - 5.10.3 审计日志
- 5.11 平台设置
 - 5.11.1 用户管理
 - 5.11.2 角色管理
 - 5.11.3 数据字典
 - 5.11.3.1 数据字典项

- 5.11.3.2 数据字典值
- 5.11.4 路由管理
- 5.11.5 任务管理
- 5.11.6 系统菜单
- 5.11.7 系统设置
- 5.11.8 系统组件
 - 5.11.8.1 仪表盘
- 5.12 个人中心
 - 5.12.1 基本设置
 - 5.12.2 安全设置
- 5.13 消息中心
 - 5.13.1 消息管理
 - 5.13.1.1 全部消息
 - 5.13.2 通知渠道
 - 5.13.2.1 通知方式
 - 5.13.3 通知模板
 - 5.13.4 通知策略
- 6 常见问题
 - 6.1 常见产品知识问题
 - 6.1.1 Q1: ACP 有哪些部署方式?
 - 6.1.2 Q2: 部署 ACP 需要的服务器软硬件资源有哪些要求?
 - 6.1.3 Q3: ACP 与中间件的关系是什么?
 - 6.1.4 Q4: ACP 支持哪些类型的中间件?
 - 6.2 常见技术问题
 - 6.2.1 Q5: 启动时提示 "max file descriptors too low" 或 "max_map_count" 错误怎么办?
 - 6.2.2 Q6: 启动 alertmanager 时提示 "No private IP address found" 错误怎么办?
 - 6.2.3 Q7: 启动时提示 "Could not create the Java Virtual Machine" 错误怎么办?
 - 6.2.4 Q8: 部署服务时提示 "java not found" 错误怎么办?
- 7 附录
 - 7.1 附录 A: 平台依赖组件操作命令
 - 7.1.1 A.1 PostgreSQL 操作命令
 - 7.1.2 A.2 MinIO 操作命令
 - 7.2 附录 B: Apusiclet 代理工具介绍
 - 7.2.1 B.1 主要功能

- 7.2.2 B.2 常用命令速查
- 7.2.3 B.3 进程组 (peasecod) 名词解释

1 修订说明

本文档根据实际情况进行更新，最新版本包含历史修改记录。

日期	手册版本	适用产品	更新说明
2024年12月	V8.0.3	ACP v8.0.3	调整格式，细化手册内容
2025年12月	V8.0.4	ACP v8.0.4	内容调整
2026年07月	V8.0.5	ACP v8.0.5	补充新增功能，优化目录结构

2 简介

金蝶 Apusic 中间件云平台（Apusic Cloud Platform，简称“ACP”）是一款面向云上中间件服务供应、管理、运维与运营全场景的中间件 PaaS 平台。

ACP 能够基于云基础设施提供全栈信创中间件服务，并通过开放的中间件服务软件定义模型帮助云服务提供方构建中间件服务生命周期管理能力，支持中间件 PaaS 平台的服务供应、管理、运维与运营，从而支撑专有云、混合云等模式下的 PaaS 核心能力建设，帮助政府和企业加速构筑业务应用的数字化底座，让应用上云更简单、更便捷。

3 产品架构

3.1 功能架构



ACP 功能架构采用模块化解耦设计，聚焦平台自身核心 PaaS 能力建设，适配政务、物联网、行业类多元业务场景，兼容各类应用架构，支持异构基础设施环境部署。

平台由六大核心能力模块构成，各模块定位与相互关系如下：

能力模块	定位	与上下游模块关系
资源接入与纳管	异构基础设施与存量实例的统一接入层	向下对接物理机、虚拟机、容器、公有云/私有云等算力，向上为中间件服务、中间件管理提供标准化运行资源与实例资产
中间件服务	标准化中间件服务的供应层	基于资源接入与纳管提供的算力，按服务目录向业务交付中间件运行环境
中间件管理	中间件全生命周期治理层	承接中间件服务，完成软件定义、部署、变更、升级、下线等全生命周期管控
中间件运维管理	运行态保障层	对中间件服务与实例进行监控、告警、巡检、安全等运维保障

运营管理	平台运营与治理层	贯穿资源、服务、运维全链路，提供租户、配额、授权、计量计费与运营可视化能力
开放性	能力开放与集成层	将资源、管理、运维、运营能力通过 API 对外开放，支撑与第三方平台对接

六大模块相互协同，形成“资源纳管—服务交付—生命周期管理—运维保障—运营治理—能力开放”的完整闭环，为政企数字化、信创化建设提供稳定可靠的中间件云底座支撑。

3.2 功能清单

一级功能	二级功能	功能名称	功能描述
首页	首页	首页	系统的整体状态查看入口，提供服务总数、资源总数、租户数、告警事件数、告警趋势、服务统计、租户概览、实时告警信息概览信息。
资源中心	主机管理	主机管理	主机资源的统一接入与管理，支持在 IaaS 层面上建立资源管理体系。通过 Agent 模式以 Apusiclet 组件对所有物理机、虚拟机进行统一接入和管理。支持资源生命周期与信息维护，包含主机纳管、标签、分组、下线等操作。
		云账号管理	对接公有云与私有云管控接口，实现云内资源的自动接入与管理。
	容器管理	环境	对所有容器环境进行统一管理，支持容器环境接入。
		概览	提供特定容器环境的概览信息，提供操作系统、架构、CPU、内存、根目录、容器数量等信息。
		容器	提供特定容器环境中的容器信息，支持可视化容器创建和管理。
		镜像	提供特定容器环境中的镜像管理功能，支持镜像检索，拉取以及镜像清理。
		网络	提供特定容器环境中的网络管理与配置能力。
		卷	提供特定容器环境中的数据卷管理与配置能力。
	Kubernetes 管理	Kubernetes 管理	K8s 集群接入、命名空间、工作负载等管理。提供 Kubernetes 集群接入管理功能。
	实例资产库	实例资产库	对中间件实例进行资产管理，可对扫描发现的中间件进行入库和纳管操作

		中间件扫描	根据不同中间件的特点，设置扫描特征，以便在扫描时对遗留中间件实例进行特征匹配，识别出对应的中间件品类
		扫描任务	根据指定的扫描特性，对指定范围进行定期扫描，发现中间件实例。
		扫描记录	记录每次扫描任务的执行详细结果，用户可查看具体的扫描主机与发现的具体实例。
仓库管理	制品管理	制品管理	软件安装包、配置包、脚本等制品的上传、版本管理、元数据维护，支持与软件管理的版本绑定。同时提供对软件包的安全扫描能力。
	补丁管理	补丁管理	补丁包的上传、版本管理与分发。
	镜像仓库	镜像仓库	支持与容器仓库进行对接，支持获取、上传容器的指定版本介质。并与自动化部署流程和软件管理关联。
中间件管理	服务管理	服务管理	服务的生命周期操作，包含服务创建、启停、扩缩容、配置变更、删除、关联实例等。
		服务回收站	提供删除服务的暂存与服务恢复功能，降低误删除风险。
	实例管理	平台实例	中间件运行实例的详情查看、状态监控、配置管理、日志查看、管控台跳转。支持从实例下钻到其所在的主机/容器资源。
		纳管实例	纳管中间件运行实例的详情查看、状态监控、配置管理、日志查看。
	软件管理	软件管理	维护中间件品类目录、版本矩阵、安装模板、安装流程编排，并关联制品中心中的具体安装包/镜像。是平台的核心资产库，也是部署服务的前置依赖。
		软件分类	软件分类定义，用于在软件管理时为软件确定分类。
	变更管理	变更管理	记录补丁安装、版本升级等运维操作的执行详情与审计轨迹，实现操作留痕。
	配置中心	配置中心	提供全局配置的集中管理，支持配置编辑、配置版本查看、配置回滚、配置下载，为运维人员提供便捷的全局配置管理工具
云原生中间件管理	云原生市场	云原生市场	提供云原生软件的安装包导入，支持云原生软件的信息查看、软件搜索、版本查看以及实例安装。

		应用实例	提供云原生运行实例的状态监控与管理功能。
可观测性	采集配置	指标采集	提供平台级指标采集接入配置的集中化管理，支持对于接入源状态的实时跟踪。
		日志采集	提供平台级日志采集接入配置的集中化管理，支持对于接入源状态的实时跟踪。
	告警规则	告警规则组	通过引入告警模板快速构建一组生效的告警规则。
		告警规则	提供告警规则的明细展示，快速检索告警规则组内配置的规则。
		告警模板	告警项模板，通过定义告警项模板，实现对告警规则的快速复用。
	指标监控	服务监控	提供服务级别实例的统一监控能力，支持查看服务监控信息，监控图表。
		主机监控	提供主机级别的统一监控能力，支持查看主机监控信息，监控图表。
	日志中心	日志分析	提供日志监控、检索、分析功能，帮助用户快速检索服务、实例等资源的历史日志。
告警与事件	告警总览	告警总览	当前告警总量、触发数量、分级分布（致命/严重/一般/轻微/提示）、告警趋势等宏观指标。
	告警事件	告警事件	告警事件列表查看、处理与关闭，覆盖从告警产生到恢复的全流程。
	告警规则	告警规则	提供告警配置功能，通过规则的方式匹配系统各类事件，以实现事件转换为告警。
	告警收敛	告警抑制	告警抑制策略配置，减少告警风暴与重复通知。
		告警静默	告警静默策略配置，在维护窗口等场景下临时屏蔽告警通知。
平台运维	平台巡检	巡检概览	对所有巡检任务的执行情况进行统一汇总，快速对总体巡检情况进行掌握。
		巡检任务	通过定义任务对平台内的中间件服务与实例进行专项健康检查，覆盖运行状态、软件异常、资源使用等维度。
		巡检规则	通过配置方式定义的检查规则和检查项。
	批量操作	文件上传	向目标主机/容器批量上传文件或分发安装包。
安全	安全概览	安全概览	提供安全总览，包含安全评分、安全问题分级统计、漏洞趋势、风

中心			险分布等信息。
	扫描任务	扫描任务	创建和管理漏洞扫描任务，支持对主机、容器、中间件实例进行定期或即时扫描，配置扫描范围、执行策略与触发条件。
	漏洞管理	漏洞管理	聚合所有扫描任务发现的漏洞，支持按危险等级（高危/中危/低危）、影响资产范围、漏洞状态（新发现/处理中/已忽略/已修复）筛选与全生命周期追踪。
	基线管理	待处理项	聚合所有扫描任务发现的配置问题，支持按处理状态、分类、软件类型、严重等级进行筛选，支持状态追踪和提供修复指引。
		基线规则库	通过配置方式定义配置基线的检查规则。
	安全配置	漏洞库	提供漏洞库上传与管理功能，并支持添加自定义漏洞规则。
平台运营	租户管理	租户管理	租户生命周期管理，核心职责是资源配额分配（为主机/容器/K8s 等资源设定各租户的使用配额）、租户隔离策略、租户级配置。租户不仅是安全隔离单位，更是资源运营分配的基本单元。
	授权管理	文件授权	文件类型软件 License 授权管理，支持记录厂商、产品、有效期，并支持一键下发到服务器。
		集中授权	基于授权中心模式提供的集中式授权管理能力，支持授权导入，支持查看起止时间，总量、已使用量计数。
		在线实例	集中式授权模式下，使用授权的实例信息。
		授权台账	人工模式下进行授权发放的记录单据，支持记录使用单位、系统名称、产品及数量。
		授权台账看板	提供人工模式下授权情况的可视化统计分析功能。
	审计日志	审计日志	用户操作记录、登录日志、关键配置变更审计，支持按时间、用户、操作类型检索与导出。审计日志也是安全事件追溯的核心证据。
平台设置	用户管理	用户管理	平台用户账号的生命周期管理（创建、编辑、禁用、删除、密码重置）。
	角色管理	角色管理	系统角色定义、权限绑定、角色分配。此处为平台内部用户的 RBAC 权限管理，与“平台运营→授权管理”的软件 License 授权是不同维度的权限体系。
	数据字典	数据字典项	系统枚举值、码表、通用配置项维护。
		数据字典值	对系统的字典值进行维护

	路由管理	路由管理	平台内访问路由以及通过平台网关代理暴露的服务路由情况。
	任务管理	任务管理	平台内定时调度任务执行情况跟踪，支持对任务的开始结束时间、耗时、执行 IP 等进行检查。
	系统菜单	系统菜单	菜单结构配置、菜单权限映射、菜单可见性控制。
	系统设置	系统设置	平台级全局参数配置，如全局超时、通知开关、默认策略等。
	系统组件	系统组件	平台依赖组件（如数据库、缓存、消息队列）的状态监控与配置管理。
个人中心	基本设置	基本设置	用户个人信息的基本设置，如头像、昵称、联系方式等。
	安全设置	安全设置	账户安全设置管理，如密码修改、双因素认证、登录设备管理等。
消息中心	消息管理	全部消息	用户接收到的平台系统、告警消息的汇总，支持已读和删除。
	通知	通知渠道	提供各类外部通知接口的配置，如邮件、短信、Webhook 以及各类 IM 消息应用。
		通知模板	支持通过文档或变量+文本的方式，配置消息通知模板，减少配置通知策略的重复。
		通知策略	通过配置标签对平台内的事件进行接入，形成推送消息，可通过通知模板，简化通知内容的配置。

3.3 部署架构

组件说明：

1. maas-aump

◦ 功能：

- 自动化安装：通过脚本或配置管理工具（如 Ansible、Chef、Puppet）实现中间件的自动化安装，减少人为操作，确保一致性。
- 依赖关系管理：管理中间件所依赖的其他组件和服务，确保安装过程中所需的资源和软件包都已正确安装和配置。
- 环境配置：根据部署环境（如开发、测试、生产等）配置中间件的参数，如端口号、内存限制、日志存储路径等。
- 容器化部署：使用容器化技术（如 Docker）来部署中间件，确保在不同环境下的一致性和易于扩展。

2. maas-gateway

◦ 功能:

1. 请求路由

- 路由转发：根据请求的 URL 路径、请求头、参数等信息将请求转发到不同的微服务或后端系统。网关能够根据配置的路由规则，将不同类型的请求引导到不同的服务实例。
- 动态路由：支持动态调整路由规则，例如根据负载情况、服务健康状态等自动选择最佳的服务实例进行路由。
- 路径重写与转发：网关可以根据配置对请求路径进行重写或修改，例如将 `/api/v1/*` 转发为 `/service-v1/*`。

2. 负载均衡

- 流量分配：根据设定的负载均衡策略（如轮询、最少连接、加权等），在多个后端实例之间分配客户端请求的流量。
- 自动伸缩：结合容器编排平台（如 Kubernetes）和云服务的能力，网关可以根据后端服务的负载和健康状态进行自动扩展和缩减。
- 高可用性：通过对多个实例进行负载均衡，确保系统的高可用性，避免单点故障。

3. maas-manager

◦ 功能:

1. 服务生命周期管理

- 服务创建与部署：提供服务部署向导，支持选择软件版本、配置模板、资源分配等，实现中间件服务的快速交付。
- 服务运维管理：支持服务的启动、停止、重启、扩缩容、配置变更等全生命周期操作。
- 服务回收与恢复：提供服务卸载暂存机制，支持误删服务的恢复，降低运维风险。

2. 租户与配额管理

- 租户生命周期管理：支持租户的创建、编辑、禁用、删除等操作，实现多租户隔离。
- 资源配额分配：为主机、容器、K8s 等资源设定各租户的使用配额，实现资源的精细化管控。

3. 配置中心

- 全局配置管理：提供平台级全局参数的集中配置管理，支持配置编辑、版本查看、回滚等操作。
- 环境变量管理：支持为服务配置环境变量，实现不同环境的差异化部署。

4. 任务调度

- 定时任务管理：支持平台定时任务的创建、启停、执行记录查看等。

- 任务监控：实时跟踪任务执行状态，支持任务执行详情查看与异常排查。

4. maas-resource

- 功能：

- 1. 异构资源统一纳管

- 物理机与虚拟机管理：支持物理机、虚拟机的统一接入与管理，提供资源注册、状态监控、信息维护等能力。
 - 容器资源管理：支持 Docker 容器环境的接入与管理，提供容器、镜像、网络、存储卷等资源的统一管控。
 - 云账号管理：对接公有云与私有云管控接口，实现云内资源的自动同步与统一管理。

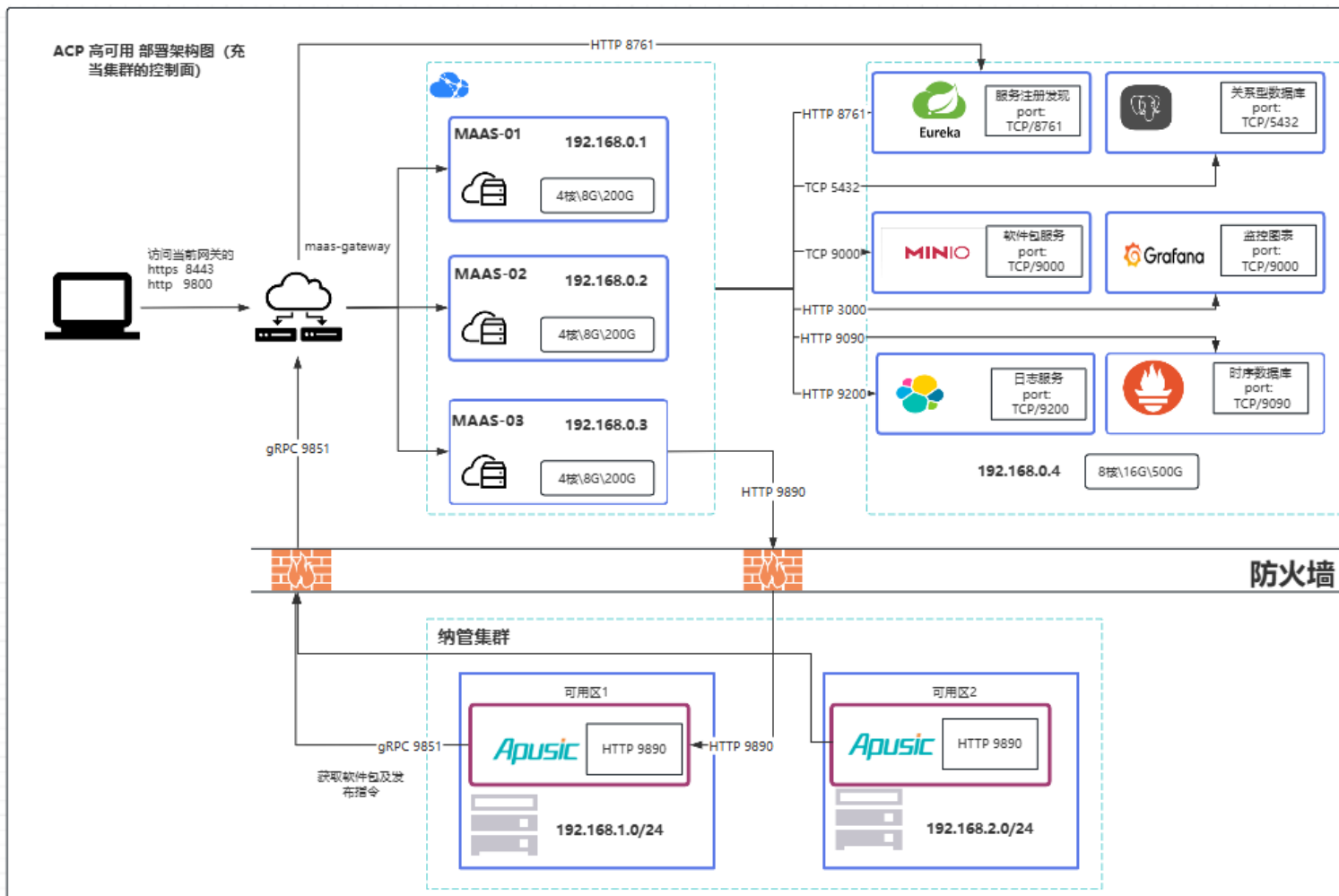
- 2. Agent 管理

- Agent 安装与升级：支持 Agent 的批量安装、版本升级、状态监控等。
 - Agent 远程操控：提供 Agent 的启动、停止、重启等远程操作能力。

- 3. 资源监控与分配

- 资源使用监控：实时监控主机、容器等资源的 CPU、内存、磁盘等使用情况。
 - 资源分配管理：支持按区域、分组等方式对资源进行分区管理，实现资源的合理分配。

高可用部署架构图：



4 安装部署

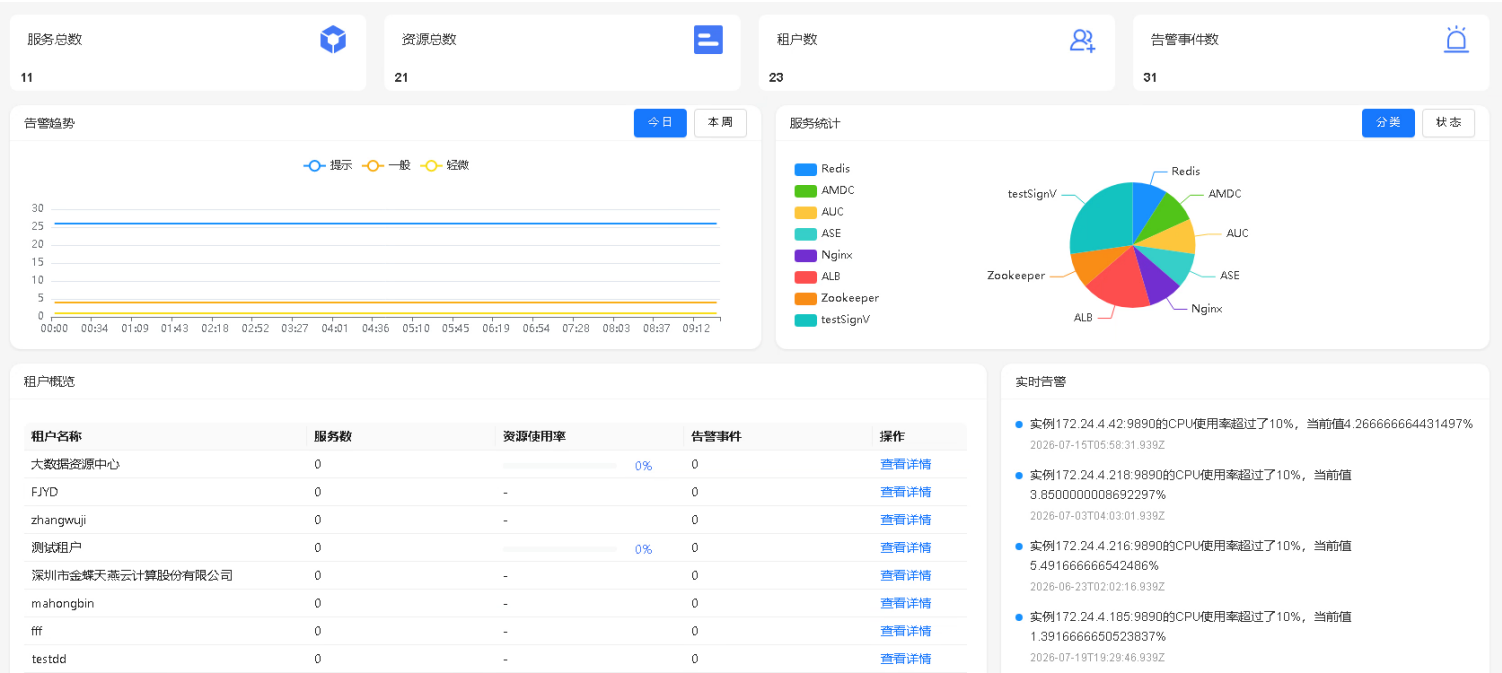
ACP 支持单机和集群两种部署模式。单机模式适用于测试验证环境，集群模式适用于生产环境，推荐至少 4 台服务器。安装前需完成环境准备，包括操作系统配置、内核参数调优、防火墙设置等。平台依赖 PostgreSQL、Elasticsearch、MinIO 等中间件组件，提供一键安装脚本简化部署流程。安装完成后需进行授权激活和系统节点注册。

产品安装部署已独立成册，请见[安装手册](#)

5 主要功能

5.1 首页

登录平台后，您首先看到的是首页仪表盘。这里集中展示了平台的运行概况，让您一目了然地掌握整体状态。



仪表盘上提供了以下关键指标，帮助您快速评估平台的健康度：

- **服务总数与资源总数：**了解平台当前管理的中间件服务和计算资源规模
- **租户总数：**查看当前平台的租户数量
- **告警事件与告警趋势：**及时发现异常，跟踪告警的变化走势

5.2 资源中心

5.2.1 主机管理

当您需要将物理机、虚拟机或云主机接入平台统一管理时，请使用主机管理功能。平台通过 Agent 组件与主机建立连接，实现资源的注册、监控和运维操作。

1. 查看和管理主机列表

进入主机管理后，您可以看到所有已接入的主机资源，并支持按区域筛选查看。列表中展示了每台主机的运行状态、IP、资源使用情况等关键信息。

主机管理

全部主机

21

运行中

20

异常

1

离线

0

+ 新增区域

新增主机

主动注册引导

导入

导出

批量停止

批量暂停

批量恢复

输入名称或IP查询

搜索

系统节点

金蝶天燕

x

产品咨询与服务部

金蝶天燕01

开发环境机器

demo

test

poc_test

Golden_test

empty_test

☐	主机别名/主机名/UUID	IP地址	主机状态	代理版本	规格/镜像	CPU利用率	内存利用率	磁盘利用率	更新时间	操作
☐	linux-3-61 linux-3-61 dce7efcb-7e3d-4234-8255-84ab62b7818d	172.24.3.61	运行中	8.0.5.24	8 vCPUs 15.512 GB C centos 7.9.2009 amd64	14.1%	61.3%	87.5%	2026-07-23	终端 移除

共1条 < 1 > 10条/页

2. 区域管理

如果您的资源分布在不同的数据中心或可用区，可通过区域管理功能对资源进行分区。点击【新增区域】即可定义区域和可用区，后续可以在资源分配和统计时按区域进行筛选。

新增区域

×

平台类型

私有云

公有云

* 主机类型

虚拟机

☐ 虚拟机

openstack

☐ openstack

vmware

☐ vmware

* 区域

* 可用区

+ 新增可用区

取消

确定

3. 主动注册引导

对于批量主机接入的场景，推荐使用主动注册方式。点击【主动注册引导】按钮，会弹出安装说明，您只需在目标主机上执行对应的安装命令，Agent 会自动完成安装并将主机注册到平台中。

主机管理云账号管理

主机管理

全部主机21

运行中20

异常

+ 新增区域

新增主机

主动注册引导

导入

导出

批量停止

批量暂停

批量恢复

系统节点

可用区1

金蝶天燕

x

产品咨询与服务部

金蝶天燕01

开发环境机器

demo

test

poc_test

Golden_test

主机别名/主机名/UUID	主机状态	代理版本	规格/镜像	CPU利用率	内存和
linux-3-61	运行中	8.0.5.24	8 vCPU 15.512 GB	5.5%	
linux-3-61			C centos 7.9.2009 amd64		

通过安装代理方式进行主机注册，代理安装成功后将进行主机信息上报，上报成功后可在‘主机管理’查看。

平台类型公有云私有云

主机类型虚拟机openstackvmware

区域系统节点

可用区可用区1

安装命令

```
bash
$ wget -qO- 'http://172.24.3.61:80/acp/resource-manager/apis/v1alpha1/openapi/apusiclet/apusiclet-install.sh?id=204,204001,204001001' | sudo bash
```

卸载 Apusiclet
请选择您的操作系统，按照步骤完成卸载。

CentOS / RHELUbuntu / Debian

1. 停止 Apusiclet 服务：

```
bash
```

返回

4. 新增主机

如果主机已安装 Agent 但尚未注册到平台，您也可以手动添加。点击【新增主机】，填写主机的 IP、端口、用户名和密码，平台会尝试连接主机并同步信息。

新增主机

×

操作说明

此模式适用于已在目标虚拟机安装 Apusiclet 代理的场景。请确保代理已正常运行，然后填写以下信息完成主机注册。

* 区域

系统节点

* 可用区

可用区1

* 主机名

请输入主机名

主机别名

请输入主机别名

* IP 地址

请输入 IP

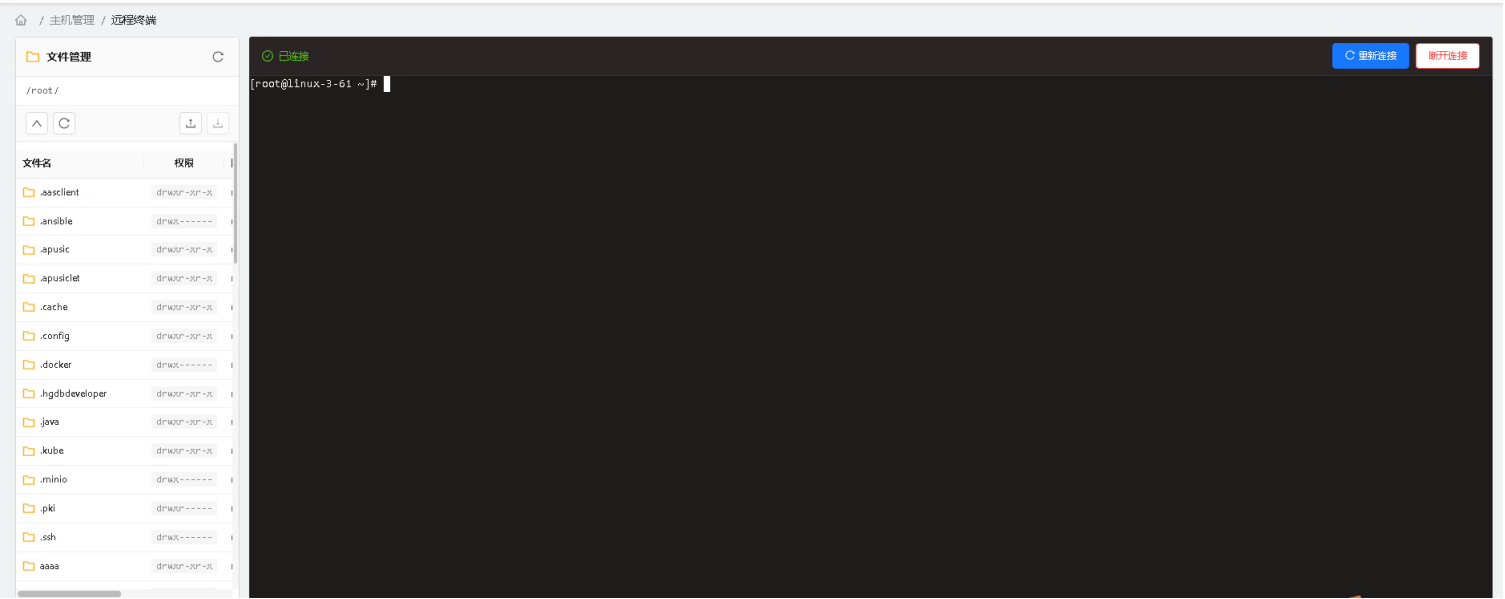
连通测试

取消

确认

5. 远程终端

需要远程登录主机进行操作时，无需额外使用 SSH 工具。在主机列表中点击对应主机的【终端】按钮，即可直接打开内置的远程终端。



6. 批量暂停与恢复

当某些主机暂时不需要被平台监控时（如维护期间），可以批量暂停其 Agent 服务。暂停后平台不再对该主机进行监控和告警，但 Agent 仍会保留心跳和升级能力，您可以随时将其恢复。

7. 批量停止

如果决定某台主机彻底脱离平台管理，可以执行批量停止操作。停止后该主机的 Agent 将完全关闭，且无法通过平台操作恢复，需要登录主机终端手动重启 Agent。

5.2.1.1 云账号管理

当您使用阿里云、腾讯云、华为云等公有云或 OpenStack、VMware 等私有云时，可以通过云账号管理功能将云上的资源自动同步到平台中，免去逐一手动添加的麻烦。

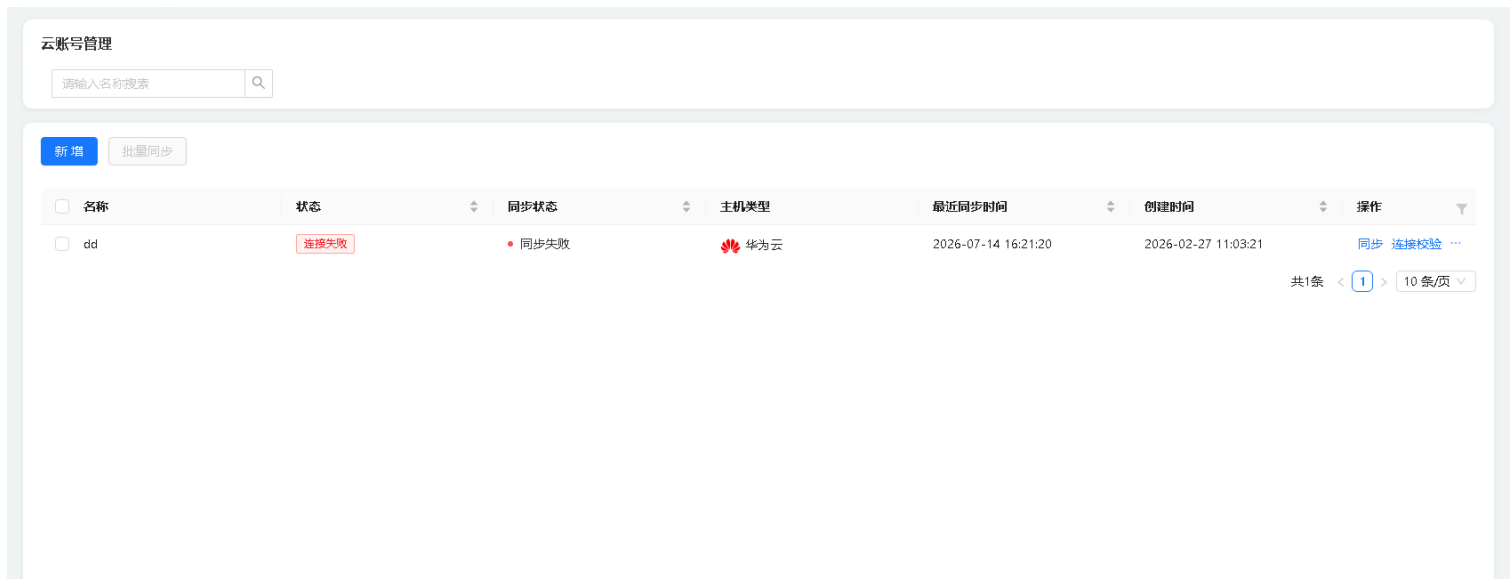
1. 新增云账号

点击【新增】按钮，选择云平台类型（如阿里云、腾讯云、华为云、OpenStack、VMware 等），填写对应的账号凭证信息，即可完成接入。



2. 同步云资源

接入云账号后，点击【同步】按钮，平台会自动拉取该账号下的所有主机资源并添加到主机管理中，实现云资源的快速导入。



5.2.2 容器管理

如果您的环境中使用了 Docker 容器，可通过容器管理功能统一管理容器环境、容器实例、镜像、网络 and 存储卷等资源。

5.2.2.1 环境

容器环境管理是容器管理的基础，您需要先将安装了 Docker 的主机添加为容器环境，才能对其上的容器进行操作。

1. 查看容器环境

进入环境列表后，您可以查看所有已接入的容器环境，包括运行状态、Docker 版本、容器数量和镜像数量等关键信息。

环境概览容器镜像网络卷

容器环境列表

环境名称

状态

主机名称/IP

搜索

重置

+ 添加

环境名称	主机	状态	Docker版本	容器	镜像	CPU	内存	Socket路径	更新时间	操作
linux-4-185	linux-4-185	运行	26.1.4	8 / 19	15	8 核	15.6 GB	/var/run/docker.sock	2026-06-18 09:26:39	编辑 删除
216	linux-4-216	运行	26.0.1	6 / 38	11	8 核	15.5 GB	/var/run/docker.sock	2026-06-17 09:34:12	编辑 删除
linux-3.61x		未知	26.1.4	15 / 16	151	8 核	15.5 GB	/var/run/docker.sock	2026-06-11 15:09:18	编辑 删除
linux-4-195	linux-4-195	异常	1.13.1	11 / 13	12	8 核	15.6 GB	/var/run/docker.sock	2026-06-11 13:57:21	编辑 删除
218	linux-4-218	运行	26.1.4	2 / 2	9	8 核	15.5 GB	/var/run/docker.sock	2026-05-26 10:12:14	编辑 删除

共5条 < 1 > 10 条/页

2. 添加容器环境

点击【添加】按钮，选择已安装 Docker 的主机，即可将其接入为容器环境。

添加环境

×

选择主机

更换主机

216

172.24.4.216

✔ Docker 已安装

该主机已安装 Docker，可以正常添加环境

环境配置

* 环境名称

216

Socket 路径

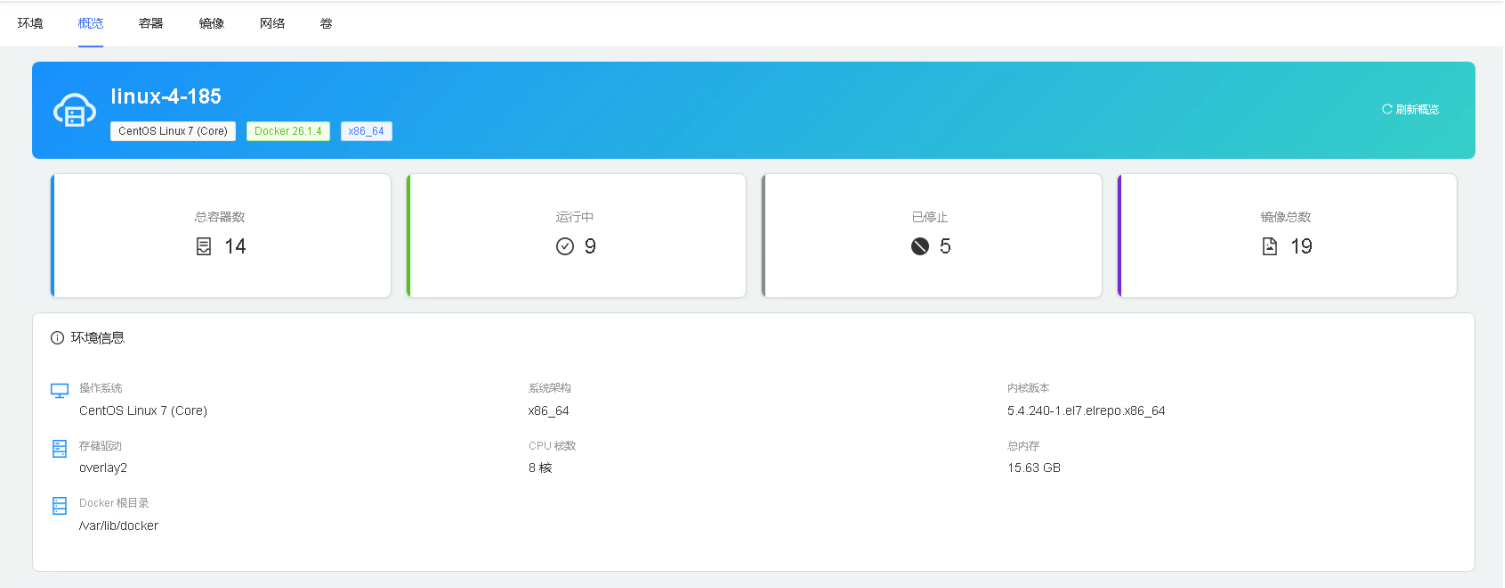
/var/run/docker.sock

取消

保存

5.2.2.2 概览

在容器环境列表中，点击某个环境的名称进入详情，首先看到的是概览页面，这里展示了该环境的基本运行情况。

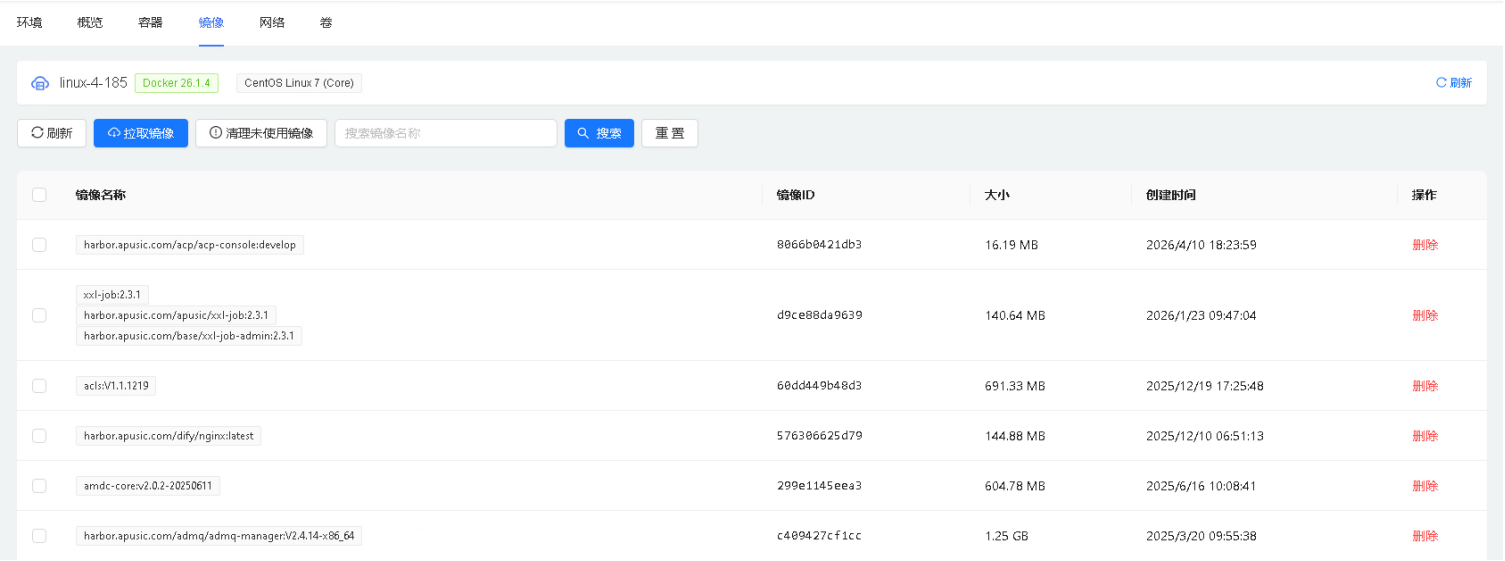


5.2.2.3 容器

在容器页面中，您可以查看当前环境下的所有容器实例，并对其进行创建、启动、停止、重启、修改和删除等操作，就像直接操作 Docker 一样方便。

5.2.2.4 镜像

镜像页面展示了当前环境中的所有 Docker 镜像。您可以在这里拉取新镜像、删除不需要的镜像，或清理未被任何容器使用的悬空镜像。



5.2.2.5 网络

网络页面管理当前环境中的 Docker 网络。您可以查看现有网络、创建新的网络或删除不再使用的网络。

环境 概览 容器 映像 网络 卷

linux-4-185 Docker 26.1.4 CentOS Linux 7 (Core) 刷新

刷新 创建网络

网络名称	网络 ID	驱动	作用域	子网	网关	容器数	操作
testa	8d5bb3096d64	bridge	本地	192.168.2.0/24	192.168.2.1	0	删除
none	1626a6805166	null	本地	-	-	0	删除
bridge	8dd12879e35c	bridge	本地	192.18.0.0/24	192.18.0.1	0	删除
host	2070d61c3dff	host	本地	-	-	0	删除
opt_default	8042e3e5d2a6	bridge	本地	192.168.0.0/24	192.168.0.1	0	删除
orion-visor-main_default	e39b0d6a0f4d	bridge	本地	192.168.1.0/24	192.168.1.1	0	删除

共 6 条 < 1 > 10 条/页

5.2.2.6 卷

卷功能支持对容器实例中的数据进行持久化存储，可通过卷管理功能，对卷进行查看、新增、删除操作。

5.2.3 Kubernetes 管理

平台支持 Kubernetes 集群接入，将其作为平台资源实现统一管理。

kubernetes管理

Kubernetes管理

请输入名称搜索 环境 启用状态 搜索 重置

添加

名称	环境	状态	版本号	代理地址	启用	创建时间	操作
demo	生产环境	正常	v1.22.2	http://172.24.3.61:9890	☒	2026-07-17 22:34:27	编辑 删除

共1条 < 1 > 10 条/页

1. 添加集群

点击【添加】按钮，进入添加集群页面。

添加 Kubernetes 集群

×

* 集群名称

请输入集群名称

* 代理地址

例如 http://192.168.1.10:9890

* 用户名

请输入 Basic Auth 用户名

* 密码

请输入 Basic Auth 密码

* 环境

请选择环境

是否启用

描述

请输入描述

取消

确认

- 集群名称：集群名称，全局唯一。
- 代理地址：集群的代理地址，用于平台对集群进行访问。
- 用户名：集群用户名。
- 密码：集群密码。
- 环境：环境种类，用于对运行环境进行区分
- 是否启用：启用集群后，可进行资源管理。

2. 管理集群

点击进入集群详情，对集群进行管理，支持针对于 Kubernetes 各类配置与管理功能。

5.2.3.1 节点

提供当前 Kubernetes 集群所有节点的查看、管理功能

节点

按名称过滤

搜索

重置

创建

名称	状态	角色	版本	系统	创建时间	操作
172.24.4.137	就绪	worker	v1.22.2	CentOS Linux 7 (Core)	2024-07-02 13:54:12	YAML 编辑 删除
172.24.4.147	就绪	worker	v1.22.2	CentOS Linux 7 (Core)	2024-07-02 13:51:55	YAML 编辑 删除
172.24.4.149	就绪	worker	v1.22.2	CentOS Linux 7 (Core)	2024-07-02 13:54:11	YAML 编辑 删除
172.24.4.208	就绪	worker	v1.22.2	CentOS Linux 7 (Core)	2024-07-02 13:54:11	YAML 编辑 删除
172.24.4.237	就绪	worker	v1.22.2	CentOS Linux 7 (Core)	2024-07-02 13:54:11	YAML 编辑 删除
172.24.4.238	就绪	worker	v1.22.2	CentOS Linux 7 (Core)	2024-07-02 13:54:11	YAML 编辑 删除
172.24.4.239	就绪	worker	v1.22.2	CentOS Linux 7 (Core)	2024-07-02 13:54:12	YAML 编辑 删除

共7条 < 1 > 10 条/页

5.2.3.2 系统组件

提供当前 Kubernetes 集群所有系统组件的查看、管理

系统组件

命名空间: kube-system

按名称过滤

搜索

重置

创建

名称	命名空间	状态	重启次数	所在节点	创建时间	操作
coredns-67cb59d684-rsrbv	kube-system	Running	0	172.24.4.137	2025-10-25 01:37:28	YAML 编辑 日志 终端 删除
dashboard-metrics-scraper-85658...	kube-system	Running	0	172.24.4.208	2025-10-25 01:37:28	YAML 编辑 日志 终端 删除
kube-flannel-ds-amd64-2n5nd	kube-system	Running	1	172.24.4.238	2024-07-02 14:07:17	YAML 编辑 日志 终端 删除
kube-flannel-ds-amd64-6fs7q	kube-system	Running	1	172.24.4.237	2024-07-02 14:07:17	YAML 编辑 日志 终端 删除
kube-flannel-ds-amd64-99dgz	kube-system	Running	1	172.24.4.149	2024-07-02 14:07:17	YAML 编辑 日志 终端 删除
kube-flannel-ds-amd64-dvmcw	kube-system	Running	2	172.24.4.147	2024-07-02 14:07:17	YAML 编辑 日志 终端 删除
kube-flannel-ds-amd64-gwvbb	kube-system	Running	2	172.24.4.239	2024-07-02 14:07:17	YAML 编辑 日志 终端 删除
kube-flannel-ds-amd64-qxv8n	kube-system	Running	1	172.24.4.208	2024-07-02 14:07:17	YAML 编辑 日志 终端 删除
kube-flannel-ds-amd64-zfhbz	kube-system	Running	1	172.24.4.137	2024-07-02 14:07:17	YAML 编辑 日志 终端 删除

5.2.3.3 项目

对应当前 Kubernetes 的命名空间，提供项目查看、管理功能

项目

Q 按名称过滤

搜索

重置

创建

名称	状态	创建时间	操作
aa	Active	2024-08-05 09:20:34	YAML 编辑 删除
acmp-operator	Active	2024-07-18 13:46:49	YAML 编辑 删除
amdc	Active	2025-03-12 16:24:15	YAML 编辑 删除
apusic	Active	2024-07-02 14:48:56	YAML 编辑 删除
apusic-system	Active	2024-07-02 14:19:44	YAML 编辑 删除
default	Active	2024-07-02 13:51:10	YAML 编辑 删除
demo	Active	2025-05-23 11:08:50	YAML 编辑 删除
fan-test	Active	2024-07-04 14:44:11	YAML 编辑 删除
flux-system	Active	2026-07-23 12:54:24	YAML 编辑 删除

5.2.3.4 应用负载-无状态副本集

提供当前 Kubernetes 集群所有无状态副本的查看、管理功能

无状态副本集

default

Q 按名称过滤

搜索

重置

创建

名称	命名空间	副本	镜像	创建时间	操作
de-acls	default	1/1	harbor.apusic.com/release/acls-serverv1.1	2026-06-15 13:56:20	YAML 编辑 扩容 删除
demo	default	1/1	harbor.apusic.com/dify/nginxlatest	2026-07-11 10:58:24	YAML 编辑 扩容 删除
kafka	default	1/1	harbor.apusic.com/admq/kafkav2.0.6_391...	2026-03-18 10:51:58	YAML 编辑 扩容 删除

共3条 < 1 > 10条/页

5.2.3.5 应用负载-有状态副本集

提供当前 Kubernetes 集群所有有状态副本查看、管理功能

有状态副本集

default

按名称过滤

搜索

重置

创建

名称	命名空间	副本	创建时间	操作
ra-admq-amqp-broker	default	1/1	2026-06-25 12:17:11	YAML 编辑 扩容 删除
ra-admq-amqp-storage	default	1/1	2026-06-25 12:17:11	YAML 编辑 扩容 删除
ra-admq-amqp-zk	default	1/1	2026-06-25 12:17:11	YAML 编辑 扩容 删除
zk-adcc-zk	default	1/1	2026-03-18 10:47:09	YAML 编辑 扩容 删除

共4条 < 1 > 10条/页

5.2.3.6 应用负载-守护进程集

提供当前 Kubernetes 集群所有守护进程的查看、管理功能

守护进程集

apusic

按名称过滤

搜索

重置

创建

名称	命名空间	期望/就绪	创建时间	操作
----	------	-------	------	----


暂无数据

5.2.4 实例资产库

实例资产库提供对中间件实例资产的管理能力，支持根据特征对中间件实例进行定期扫描发现，并对扫描结果进行管理。

5.2.4.1 实例资产库

所有被扫描到的中间件实例都会出现在实例资产库中，您可以在这里决定每个实例的后续处理方式。

实例总数

382

未入库

361

未纳管

19

1 已消失

已纳管

1

忽略

1

1 已消失

实例资产库

全部

所有类型

所有软件

所有主机

搜索 IP / 端口 / 进程名

搜索

重置

☐	实例名称	进程名	类型	软件	IP	端口/端口映射	发现来源	纳管	状态	操作
☐	AMDC-Server	amdc-server	主机	AMDC	172.24.4.218	6359 8004	xxx	未纳管	正常	纳管 忽略 删除
☐	AMDC-Server	amdc-server	主机	AMDC	172.24.4.216	6359 8004	xxx	未纳管	正常	纳管 忽略 删除
☐	AMDC-Server	amdc-server	主机	AMDC	172.24.4.42	6359 8004	xxx	未纳管	正常	纳管 忽略 删除
☐	AMDC-Server	amdc-server	主机	AMDC	172.24.4.218	6359 8004	amdc	未纳管	正常	纳管 忽略 删除
☐	AMDC-Server	amdc-server	主机	AMDC	172.24.4.216	6359 8004	amdc	未纳管	正常	纳管 忽略 删除
☐	AMDC-Server	amdc-server	主机	AMDC	172.24.4.42	6359 8004	amdc	未纳管	正常	纳管 忽略 删除
☐	testsss	testsss	容器	Nginx	172.24.4.216	80/tcp 9999:9999/tcp	signv216	未入库	正常	审核入库 删除
☐	testccc	testccc	容器	Nginx	172.24.4.216	-	signv216	未入库	正常	审核入库 删除
☐	AMDC-Server	amdc-server	主机	AMDC	172.24.4.218	6369 8004	amdc	未入库	已消失	删除

1. 审核入库

当扫描发现一个中间件实例后，您需要对其进行审核。点击操作栏的【审核入库】，查看实例的详细信息，填写默认绑定端口，确认无误后将其标记为“已入库”状态，纳入平台的持续跟踪管理。

审核入库 - zzz_docker_nginx_0_0

未入库

软件 Nginx 入库时间 2026-07-13 17:48:40 最后扫描 2026-07-14 10:23:30

扫描发现的实例信息

主机IP地址

172.24.4.216

容器ID

d583a1fdc09f

容器名称

zzz_docker_nginx_0_0

镜像

harbor.apusic.com/dify/nginx:latest

版本

latest

创建时间

2026-07-13 17:33:53

重启次数

-

映射端口列表

3333:3333/tcp

80/tcp

容器端口映射到宿主机的端口

扫描匹配信息

特征名

signvnginx

软件

Nginx

匹配特征值

zzz_docker_nginx_0_0

扫描发现时间

最后扫描时间

取消

审核通过并入库

2. 纳管实例

对于已入库的实例，您可以进一步执行纳管操作。纳管时需要补充关联组件信息、启动/停止命令等，纳管后该实例会被添加到纳管实例列表中，平台将为其提供监控和管理能力。

实例纳管



i 为了确保纳管实例的有效性，请确认以下信息。

基本信息

* 实例名称	amdc-server_70wqOHcXPK
* 关联组件	ADMQ2_RabbitMQ/3.12.13/broker
关联制品	
IP地址	172.24.4.218
端口	6359 8004
安装路径	/root/.apusic/workspace/1c12d0c8-374e-4ce3-bb4b-63fa166984c5
备注	

操控命令

启动命令

停止命令

```
1 ./amdc-server
```

取消

确定

3. 忽略纳管

如果某个实例是临时测试环境，无需纳入管理，可以点击【忽略】按钮，将其标记为忽略状态，后续平台不会再对其进行纳管提醒。

4. 跳转纳管

已纳管的实例可以通过【跳转纳管】快速跳转到对应的实例管理页面，方便您进行后续的运维操作。

5.2.4.2 扫描特征

扫描特征是平台识别中间件实例的依据。通过定义进程名称匹配规则、端口等信息，平台可以在扫描时准确判断主机或容器上运行的是哪种中间件。

1. 新增特征

点击【新增】按钮，进入新增扫描特征页面。

新建扫描特征

* 特征名称

如: Redis标准进程

* 类型

主机

* 所属软件

请选择所属软件

匹配规则 *

规则名称	名称匹配(AND)	名称排除(OR)	部件名称	默认端口	操作
规则名称	逗号分隔, 如: nginx.mas...	逗号分隔, 如: worker,cli	部件名称	如: 80	
+ 添加规则					

名称匹配: 逗号分隔表示AND关系, 如 "nginx, master" 需同时包含两个关键字才匹配。

名称排除: 逗号分隔表示OR关系, 命中任意一项即排除该进程。

匹配优先级: 同一特征内命中多条规则时, 优先选择匹配文本更长的规则。例如 "maas-export" (12字符) 优先于 "maas" (4字符)。

备注

补充说明...

取消

保存

填写以下信息来定义一个扫描特征：

- **特征名称**：特征的名称，全局唯一
- **类型**：选择该特征适用于主机还是容器实例
- **所属软件**：选择该特征对应的软件大类
- **匹配规则**：定义如何通过进程信息识别该软件，每条规则包含：
 - **规则名称**：规则的标识名称
 - **名称匹配（AND）**：填写进程名称（逗号分隔），实例必须包含所有指定的名称才匹配
 - **名称排除（OR）**：如果进程包含排除列表中的任一名称，则跳过该进程

- 部件名称：当一个软件包含多个部件时，通过部件名称区分
- 默认端口：该软件常用的运行端口（仅用于展示，不参与匹配）

2. 复制特征

如果已有特征与您需要的配置相似，可以选定该特征后点击【复制】，快速创建新的特征，然后微调即可。

复制扫描特征

* 特征名称

Tomcat_copy

* 类型

主机

* 所属软件

Tomcat

匹配规则 *

规则名称	名称匹配(AND)	名称排除(OR)	部件名称	默认端口	操作
001	tomcat	逗号分隔，如: worker,di	部件名称	8080	
+ 添加规则					

名称匹配：逗号分隔表示AND关系，如 "nginx, master" 需同时包含两个关键字才匹配。

名称排除：逗号分隔表示OR关系，命中任意一项即排除该进程。

匹配优先级：同一特征内命中多条规则时，优先选择匹配文本更长的规则。例如 "maas-export"（12字符）优先于 "maas"（4字符）。

备注

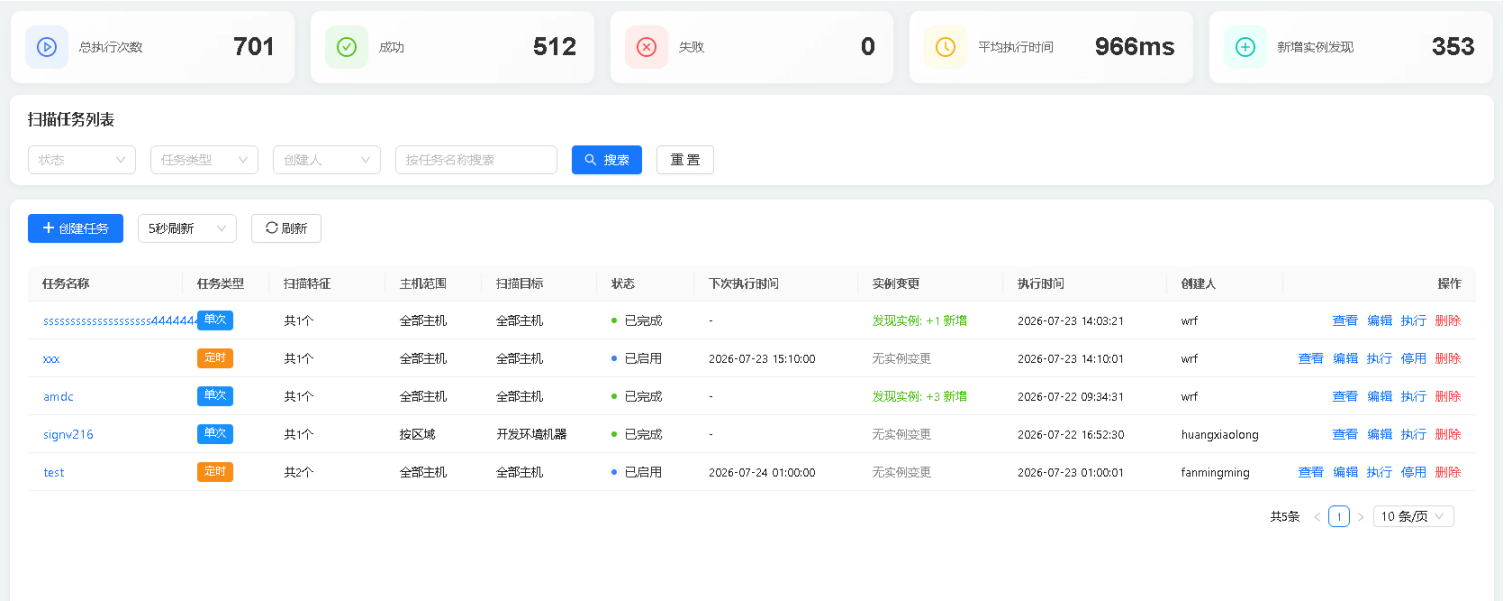
补充说明...

取消

保存

5.2.4.3 扫描任务

扫描任务驱动着实例发现的过程。您可以创建扫描任务，指定扫描范围和调度方式，平台会按照任务配置自动发现中间件实例并推送到资产库中。



1. 创建任务

点击【创建】按钮，配置扫描的目标主机或容器环境，选择使用的扫描特征，并设置执行方式（立即执行或周期性执行）。

- 任务名称：任务名称，全局唯一。
- 任务类型：即时扫描（单次）配置后立即运行，定时扫描可配置扫描周期，定期进行扫描。
- 扫描特征：选择本次需要扫描的扫描特征类型，对指定种类的中间件进行扫描发现。
- 主机范围：支持全部扫描、按 IP 段扫描和按选定区域扫描。
- 并发度：并发进行扫描可加快扫描速度，建议设置为 5。
- 失败重试次数：若出现主机未能连接或扫描失败时，将自动重试，超过重试次数，则自动跳过。

2. 查看任务

创建完成后，您可以在任务列表中查看所有扫描任务的状态和最近执行结果。

执行详情 - #2080171887338557442

×

执行状态	扫描主机	发现实例	执行耗时
部分成功	18 / 21	+1	1s

扫描的主机

主机IP	状态	耗时	发现实例数	失败原因
172.24.4.91	成功	31ms	0	-
172.24.3.63	成功	28ms	0	-
172.24.4.231	成功	32ms	0	-
172.24.4.42	成功	39ms	0	-
172.24.2.60	成功	49ms	0	-

共 21 条 < 1 2 3 4 5 > 跳至 页

发现的实例

实例名称	进程名	类型	软件	IP	端口/端口映射	状态
------	-----	----	----	----	---------	----

3. 执行任务

对于已创建的任务，点击【执行】可以立即触发一次扫描，无需等待调度周期。

4. 停用/启用任务

如果某个周期性任务暂时不需要执行，可以将其停用；需要时再启用即可。

5.2.4.4 扫描记录

每次扫描任务执行完成后，系统会生成一条扫描记录供您查阅，方便您追溯每次扫描的详细结果。

1. 查看扫描记录列表

进入扫描记录页面，您可以查看所有历史扫描任务的执行记录，包括任务名称、执行时间、扫描了多少台主机、发现了多少个实例等信息。

2. 删除记录

对于不再需要的扫描记录，您可以直接删除以保持列表整洁。

5.3 仓库管理

5.3.1 制品管理

制品仓库用于集中存储软件安装包、配置包、脚本等构建产物。当您需要分发或获取制品时，可以在这里统一管理。

制品管理

请输入制品项目、仓库名称进行搜索

搜索

重置

+ 新建制品项目

制品包制作 >

制品项目名称	仓库数	创建时间	操作
test	0	2026-07-23 13:28:11	编辑 删除
test2	1	2026-07-22 18:12:15	编辑 删除
test1	2	2026-07-22 18:11:05	编辑 删除
AASV10	2	2026-06-11 15:57:33	编辑 删除
others	3	2025-12-30 16:07:42	编辑 删除
apusic	33	2025-08-26 09:12:44	编辑 删除

共6条

< 1 >

10 条/页

1. 新建制品项目

点击【新建制品项目】按钮，进行制品项目创建，通过制品项目将同一产品或同一类产品放在一个项目下进行管理。

新建制品项目

×

* 制品项目名称

请输入英文、数字、"/"或"."

关闭

确定

2. 制品仓库

选择任意项目点击名称，进入项目下的制品仓库管理。仓库与制品绑定，上传制品时将自动创建。

制品管理 / 制品仓库

apusic

请输入制品仓库名称进行搜索

本地导入

制品仓库名称	制品数	下载数	最新变更时间
AMDC	2	10	2026-07-03 16:47:59
ALB	3	245	2026-07-03 16:44:50
AASV10	2	184	2026-07-03 16:31:49
ase	1	5	2026-07-03 15:12:57
AAMSV10SP11	1	0	2026-07-03 14:41:20
AAMSV10SP12	1	0	2026-07-03 14:39:58
ADMQ_Kafka_UI	1	66	2026-03-31 10:29:49
ADMQ_Kafka_Exporter	1	127	2026-03-31 10:23:51
ADMQ_Kafka	1	229	2026-03-31 10:17:50

点击仓库名称，查看仓库下的制品详情

制品管理 / 制品仓库 / 制品包

apusic/AMDC

请输入制品名称、版本、操作系统或CPU架构查询

制品名称	版本	操作系统	CPU架构	漏洞数	更新日期	大小(MB)	操作
SHA256:F0398EF1859A787DA1E2C06A9AFCA80126FFE06E6F6F3C5F40DF1C38C34E59FE	V2.0.5-20260...	LINUX	arm64	0	2026-07-03 16:47:59	47	下载 删除
SHA256:58D20BBA4760E31928F9CC4942D7F344CDC4399597857334639F112DA65832C7	V2.0.5-20260...	LINUX	amd64	0	2026-07-03 16:46:06	48	下载 删除

共2条 < 1 > 10 条/页

3. 导入制品

进入制品仓库，点击【本地导入】按钮，进入制品导入页面。选择已有的制品包进行导入。制品会导入当前项目下，仓库名称为制品包名称。

上传制品

仅支持符合平台规范的制品包，制品包规范请参考用户手册。

将文件拖到此处，或点击上传

支持扩展名：.tar.gz

AMDC-V2.0.5-20260703-LINUX-amd64-preset.tar.gz

48.64 MB

确定

4. 制品包制作

在没有制品包的情况下，用户可根据需要自行开发制品包，用于中间件部署。制品包需包含中间件原始文件，制品配置等相关信息。

上传制品包，上传完成后点击下一步

制品包制作

1 上传软件包

2 基本信息

3 制品设置

4 构建与发布

5 完成

点击或拖拽文件到此处上传

支持 zip, tar.gz, rpm, deb 格式，最大 2GB

redis8.0.zip

0.00 MB

开始上传

41

填写软件制品相关信息，填写完成后点击下一步

制品生成

1 上传软件包

2 基本信息

3 制品设置

4 构建与发布

5 完成

• 软件名称

请输入软件名称

• 软件版本

请输入软件版本

• 发行方

请选择发行方

• 适用操作系统

请选择操作系统

• 适用处理器架构

请选择处理器架构

关闭

上一步

下一步

填写制品设置，填写完成后点击下一步

制品生成

1 上传软件包

2 基本信息

3 制品设置

4 构建与发布

5 完成

文件复制设置

源路径

目标路径

+ 添加文件路径复制

环境变量

变量名

变量值

+ 添加环境变量

端口

+ 添加端口

管控命令

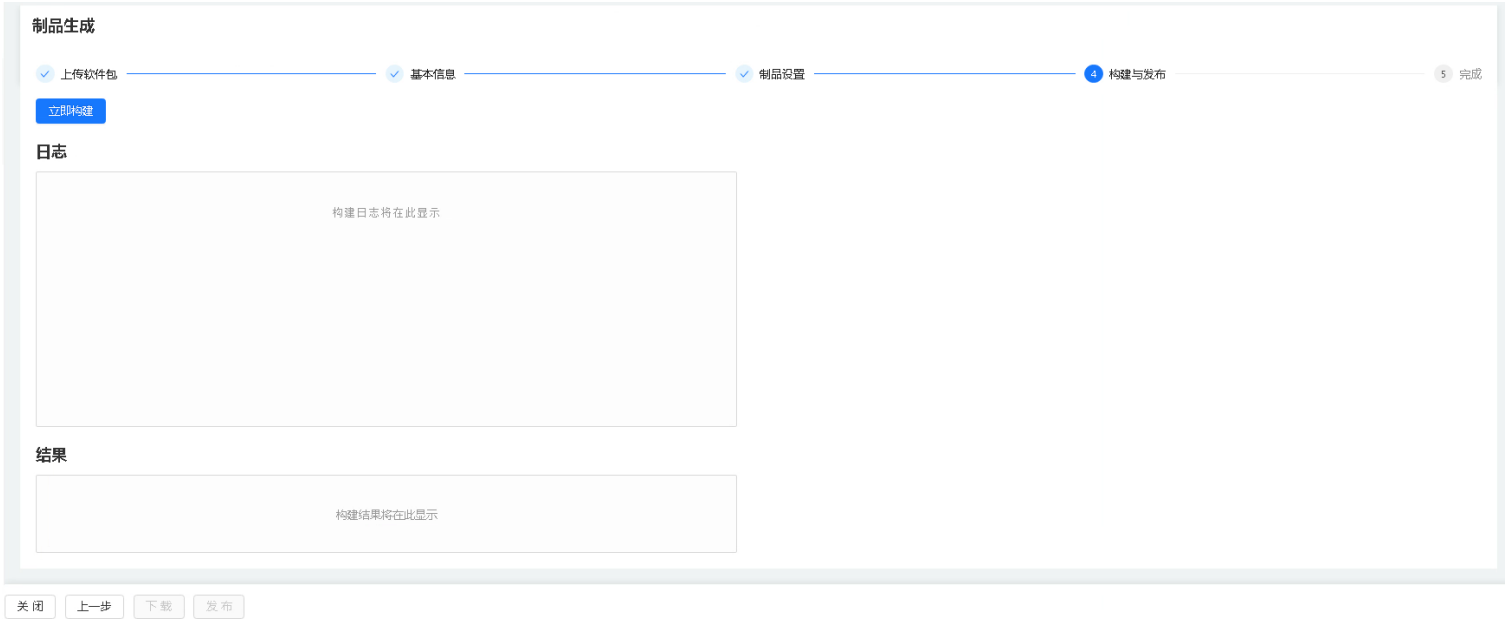
安装命令

启动命令

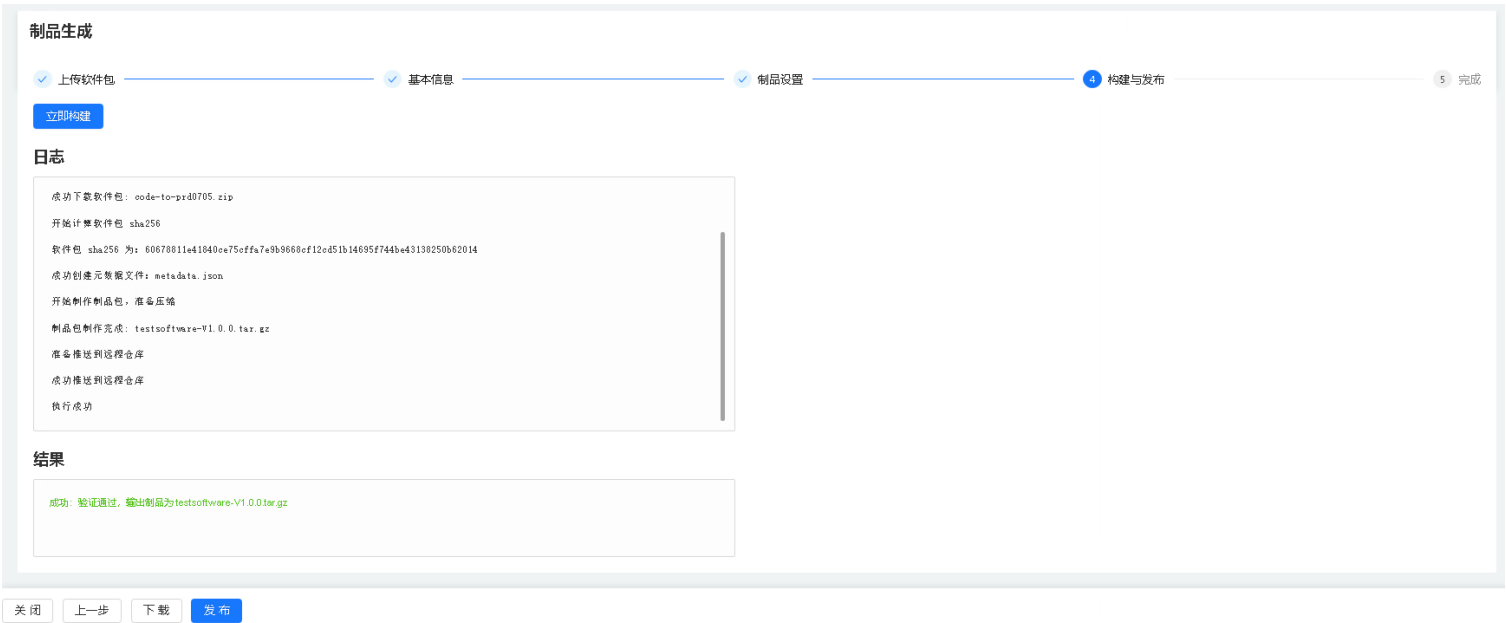
- 文件复制设置：在部署时文件将从制品包的源路径拷贝到部署目录下，可通过目标路径指定相对路径。
 - 源路径：制品包中的文件路径
 - 目标路径：部署目录下相对路径
- 环境变量：在部署时，可设置环境变量，通过环境变量设置部署参数。
 - 变量名：环境变量名
 - 变量值：环境变量值，值可不填写，在部署时补充
- 端口：软件部署后对外暴露的端口声明

- 端口名：软件暴露的端口名称，用于区别端口作用
- 端口值：软件暴露的端口值
- 操控命令：
 - 安装命令：软件包被推送到部署目录后，执行的安装命令
 - 启动命令：软件包部署完成后，执行的启动命令

进行制品生成，点击【立即构建】



构建完成后，可进行制品发布或者下载制品包。



点击【发布】按钮，选择制品归属的项目，完成制品发布。

发布制品

制品信息

制品名称 testsoftware

制品版本 V1.0.0

* 制品项目

others

取消

发布

发布成功后，可看到制品生成成功的提示

制品生成

✓ 上传软件包

✓ 基本信息

✓ 制品设置

✓ 构建与发布

5 完成

✓

制品生成成功!

制品发布已提交

重新制作

返回列表

5.3.2 补丁管理

补丁管理用于集中管理中间件的补丁包。当您需要修复软件漏洞或升级组件时，可以在这里上传补丁、将补丁应用到目标主机。

补丁管理

请输入补丁名称进行搜索

搜索

重置

上传补丁

补丁规范

补丁名称	补丁类型	获取渠道	关联制品	关联漏洞	描述	上传人	上传时间	操作
test	一般	官方		-	-	acpadm	2026-01-30 18:29...	查看说明 下载 删除
AAS测试补丁	重要	官方		-	-	mahongbin	2025-12-12 17:06...	查看说明 下载 删除

共2条

< 1 >

10 条/页

1. 查找补丁
- 补丁列表展示了所有已上传的补丁，您可按名称筛选查找。
2. 上传补丁
- 点击【上传补丁】，选择补丁文件并填写相关信息，即可将补丁上传到仓库。

上传补丁

×

*

名称

请输入名称

*

获取渠道

请选择获取渠道

▼

*

补丁类型

请选择补丁类型

▼

*

上传附件

📁 上传文件

支持扩展名：.zip,.tar,.tar.gz

是否需要重启

*

关联制品

请选择关联制品

关联漏洞

请选择关联漏洞

描述

请输入描述

取消

确定

3. 下载补丁

对于需要分发但暂不应用的补丁，可以点击【下载补丁】保存到本地。

4. 查看补丁详情

选定一条补丁信息，点击【查看】，可以查看该补丁的详细信息。

补丁说明

版本号: [填写版本号, 例如: v1.0.1] **发布日期:** [填写发布日期, 例如: 2023-11-15] **适用系统/软件:** [填写适用的系统或软件名称及版本]

补丁概述

[简要描述补丁的目的或修复的核心问题, 例如: 修复XX功能异常、优化XX性能等。]

修复的问题

1. **问题or漏洞编号/标题:** [例如: BUG-1234]
- **描述:** [详细描述问题现象]

• **修复内容:** [说明如何修复的]
2. **问题or漏洞编号/标题:** [例如: 需求-5678]
- **描述:** [新增功能或改进的描述]

• **变更内容:** [具体变更细节]

(可根据实际修复项增减列表)

变更内容

- [列出所有重要的变更点, 例如:
- 修改了XX模块的XX逻辑。

• 优化了XX功能的响应速度。

• 更新了依赖库XX到VX.X版本。]

升级/安装说明

1. **前置条件:**
- [例如: 需先安装基础版本v1.0.0]
2. **安装步骤:**
- [分步骤说明如何安装补丁, 例如:

关闭

5. 制作补丁

点击列表界面右上角【补丁规范】，可查看补丁制作的要求，可按补丁规范实现补丁包的制作。可点击【补丁 Demo】查看样例 Demo 的结构。

ACP补丁包规范

为了规范化补丁管理，对上传到平台的补丁文件，做如下要求：

补丁名称

补丁文件支持zip、tar、tar.gz格式

文件名称要求：<制品包名>-<制品版本>-patch-<时间戳>，如ACP-V8.0.4-patch-20250804

补丁内容

补丁文件内需要包括三个部分

- readme.md：问题或漏洞描述
- options.yaml：补丁文件的下发路径的列表
- patches：补丁存放的文件夹
- attachment：用于放置测试报告等附件

#options.yaml样例

options:

- source: patches/patch1.jar # 补丁文件路径（相对路径）
dest: apps/lib/ # 上传目标文件路径（相对路径）
- source: patches/patch2.jar
dest: apps/
- source: patches/*.jar # 匹配所有的 jar 包
dest: apps/lib/
- source: patches/lib/ # 支持目录，但必须以 / 结尾；会把目录以及子目录上传到 dest 中，并保留原有的
dest: apps/lib/

presets:

- name: preset/AASV10:V10 # 制品项目/制品包名:制品版本
arch: all # 架构

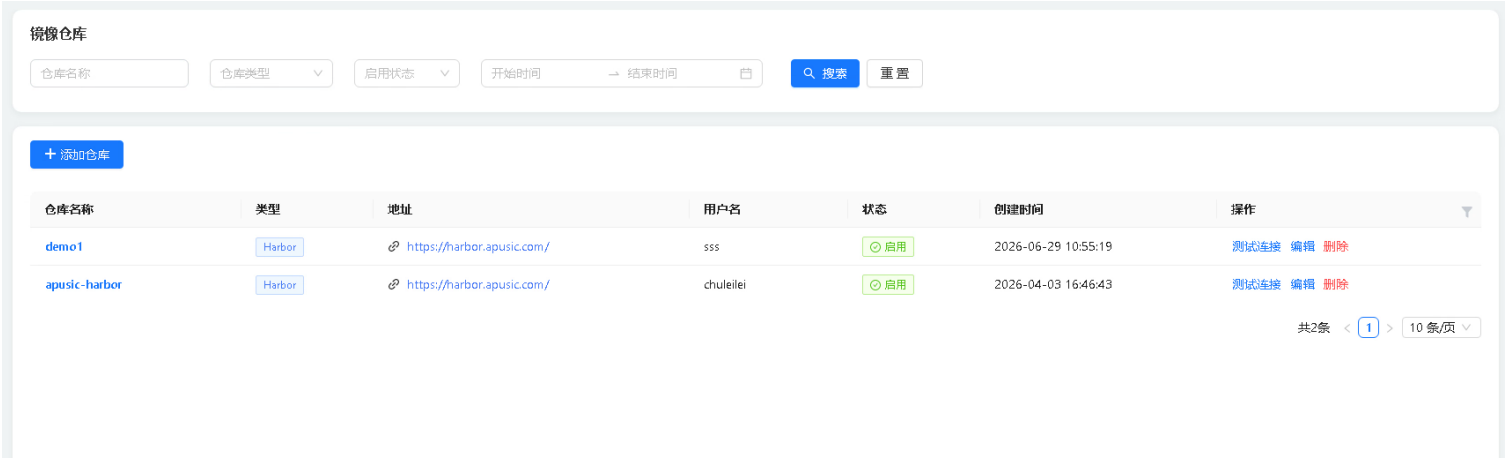
关闭

5.3.3 镜像仓库

镜像仓库与 Docker Registry 对接，方便您集中管理容器镜像。您可以在这里推送、拉取、删除镜像，并管理镜像的版本标签。

1. 查看检索镜像仓库

镜像仓库列表展示了对接的镜像仓库列表，您可按名称、仓库类型等信息进行检索。



2. 添加仓库

当需对接新的镜像仓库时，点击【添加仓库】，填写仓库信息并保存。

添加镜像仓库

✕

* 仓库名称

请输入仓库名称

* 仓库类型

Harbor

启用状态

启用

* 仓库地址

https://harbor.example.com

* 用户名

请输入用户名

* 密码

请输入密码

描述

请输入描述信息（可选）

0 / 200

取消

确定

- **仓库名称**：对接仓库的名称，全局唯一。
 - **仓库类型**：支持 Harbor 与 Nexus 两种对接类型
 - **启用状态**：启用时，则其它模块可以选择此仓库进行镜像查找。
 - **仓库地址**：对接仓库的访问地址。
 - **用户名**：对接仓库的用户名。
 - **密码**：对接仓库的密码。
3. **测试连接** 选定一条仓库信息，点击【测试连接】，即可对当前仓库进行连接测试。
4. **查看仓库镜像信息**

点击已接入的仓库的仓库名称，进入仓库详情

🏠 镜像仓库 / apusic-harbor

apusic-harbor

Harbor

🔍 搜索项目...

🔍 搜索

项目名称	公开	仓库数量	创建时间
aalarm	公开	2	2022-10-19 07:02:02
aas	公开	0	2022-07-26 07:15:35
acmp	公开	35	2022-11-24 08:23:37
acp	公开	20	2023-11-07 06:52:37
acp-plugins	私有	5	2021-02-03 02:21:07
adas	公开	3	2022-06-02 06:23:10
adcc	公开	1	2024-03-21 04:53:50

点击仓库内的项目名称，进入项目详情

🏠 镜像仓库 / apusic-harbor / aalarm

aalarm

Harbor

🔍 搜索镜像...

🔍 搜索

镜像名称	下载次数	更新时间
console	⬇️ 0	2026-06-24 10:07:29
aalarm-manager	⬇️ 35	2026-06-03 07:29:52

共2条 < 1 > 10 条/页 ▾

点击项目列表中的镜像，查看镜像明细

🏠 镜像仓库 / apusic-harbor / aalarm / aalarm-manager

aalarm-manager

Harbor

镜像列表

镜像名称	下载次数	更新时间
console	⬇️ 0	2026-06-24 10:07:29
aalarm-manager	⬇️ 35	2026-06-03 07:29:52

共2条 < 1 > 10 条/页 ▾

aalarm-manager 的版本

版本标签	类型	大小	下载次数	推送时间
v1.2.1-se 	IMAGE	267.82 MB	⬇️ 0	2023-02-08 15:09:21

5.4 中间件管理

5.4.1 服务管理

服务管理是平台的核心功能之一，涵盖了中间件服务从部署到下线全过程的操作。您可以在这里创建新的中间件服务，管理其运行状态，并在需要时将其卸载。

1. 查看服务列表

进入服务管理后，页面顶部展示了各状态服务的数量概览卡片，让您对整体情况一目了然。下方的服务列表可按名称、状态或软件类型筛选。

全部11

运行中8

异常1

离线2

服务管理

部署模式

请输入服务名称

搜索

重置

部署

导出

启动

停止

重启

刷新

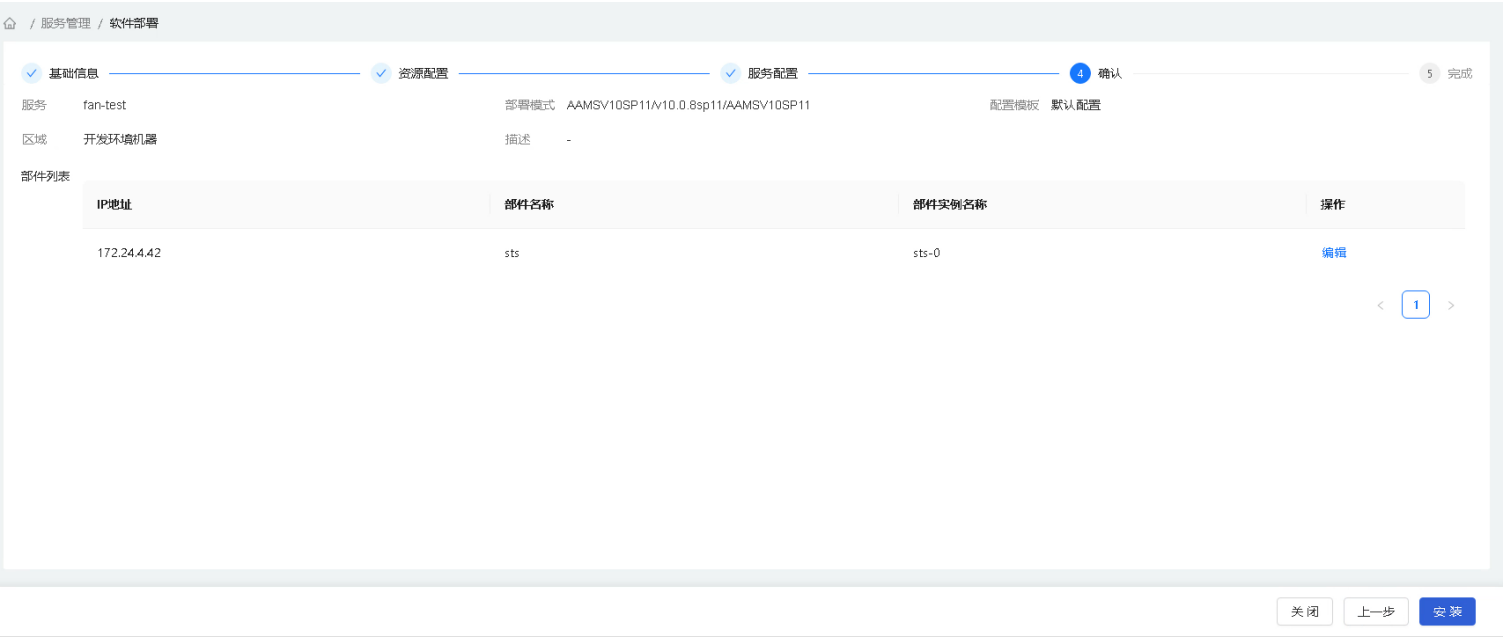
服务名称	部署模式	配置模板	来源	状态	安全评分	租户	项目	创建时间	操作
amdcd	AMDC/V2.0.2/主从	默认配置	平台服务	3 / 3	100	默认租户	默认项目	2026-07-23 14:05:08	服务访问 卸载 更多
test-zk	Zookeeper/3.9.4/单机	默认配置	平台服务	1 / 2	0	默认租户	默认项目	2026-07-22 15:04:20	服务访问 卸载 更多
test-alb2	ALB/V2.0.6/单机	默认配置	平台服务	1 / 1	100	默认租户	默认项目	2026-07-22 14:09:53	服务访问 卸载 更多
testccc	testSignV/V1.0.2/nginxuser	默认配置	平台服务	0 / 1	100	默认租户	默认项目	2026-07-15 15:31:55	服务访问 卸载 更多
testsss	testSignV/V1.0.2/difynginx	默认配置	平台服务	1 / 1	100	默认租户	默认项目	2026-07-15 14:33:23	服务访问 卸载 更多
zzz	testSignV/V1.0.2/difynginx	默认配置	平台服务	0 / 1	100	默认租户	默认项目	2026-07-14 16:11:01	服务访问 卸载 更多

2. 部署服务

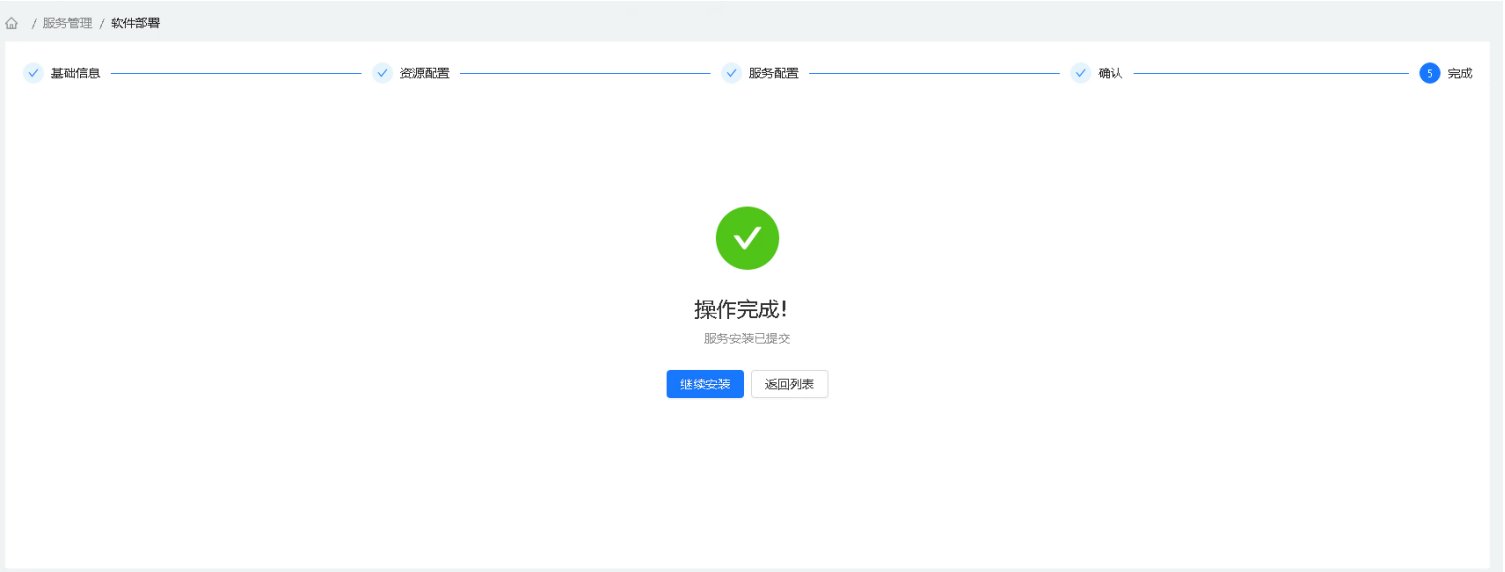
点击【部署】按钮，跟随部署向导完成服务的创建。您需要依次选择软件及版本、部署模式、配置模板等信息，向导会引导您逐步完成。

- 基本信息
 - 服务名称：本次部署服务的名称，全局唯一。
 - 部署模式：不同软件有不同的部署模式，例如单体、集群等。可在下拉列表中选择对应的软件和模式
 - 配置模板：每种软件下的部署模式都有自己的默认部署模板，如需自定义可在软件管理模块中进行增加和修改
- 资源配置 通过选择区域，确定部署目标。在指定区域下，可通过手工添加和系统分配两种方式添加主机。
 - 手动添加：自行从主机列表中进行选择
 - 系统分配：提供所需服务器数量，系统自动从所在分区中选择可用服务器。

- 服务配置 点击配置节点，可在右侧弹出的配置窗口中，进行服务配置，如配置副本数、端口等。
 - 开启动态端口：开启动态端口后，平台会在服务器上自行寻找一个可用端口。
- 确认 当所有信息都已确认无误后，点击【安装】按钮，平台将自动进行服务部署。



- 完成 当出现操作完成界面，平台已开始自动进行服务部署，您可点击【继续安装】安装剩余的服务，或点击【返回列表】查看已部署的服务列表。



3. 启动/停止/重启服务

在服务列表中，选定某个服务后，可以直接对其进行启动、停止或重启操作，无需登录到主机执行命令。

4. 访问服务控制台

如果服务提供了 Web 管理界面，点击【服务访问】按钮可直接跳转到该服务的控制台页面。若该软件未配置控制台地址，则跳转按钮置灰，可进入服务详情页面进行添加。

5. 查看服务详情

选定一条服务记录，点击服务名称，进入服务详情页面，查看服务详情。并配置访问地址和重启策略等信息。

服务管理 / 服务详情

基本信息

监控服务

服务信息

服务名称

fan-test

来源

平台服务

部署模式

AAMSV10SP11/v10.0.8sp11/AAMSV10SP11

配置模板

默认配置

租户

默认租户

项目

默认项目

描述

-

访问地址

访问配置

重启策略

滚动重启

配置

软件信息

软件名称

AAMSV10SP11

相关制品

AAMSV10SP11



软件描述

-

详情页面提供了该服务下的实例信息，点击实例名称，可进入实例详情页面。也可以进行查看实例的日志、开启远程终端、启动、停止、重启等操作。

实例信息

启动

停止

重启

刷新

全部 1

主机实例 1

容器实例 0

☐	实例名称	类型	运行状况	安全评分	所属服务	制品包/镜像	IP地址	重启次数	操作
☐	fan-test-sts-AAMSV10SP11-0	主机	SUCCESS	100	fan-test	AASV10/AAMSV10SP11:AAS-V10.0.8-SP11-AE-2...	172.24.4.42	0	日志 远程终端 更多

共1条 < 1 > 10条/页

6. 服务实例升级

选定一条服务记录，点击服务名称，进入服务详情页面，点击【主机实例】或【容器实例】，对应的实例提供不同的升级方式，可进行制品、补丁升级或镜像升级。

实例信息

启动

停止

重启

制品升级

补丁升级

刷新

全部1

主机实例1

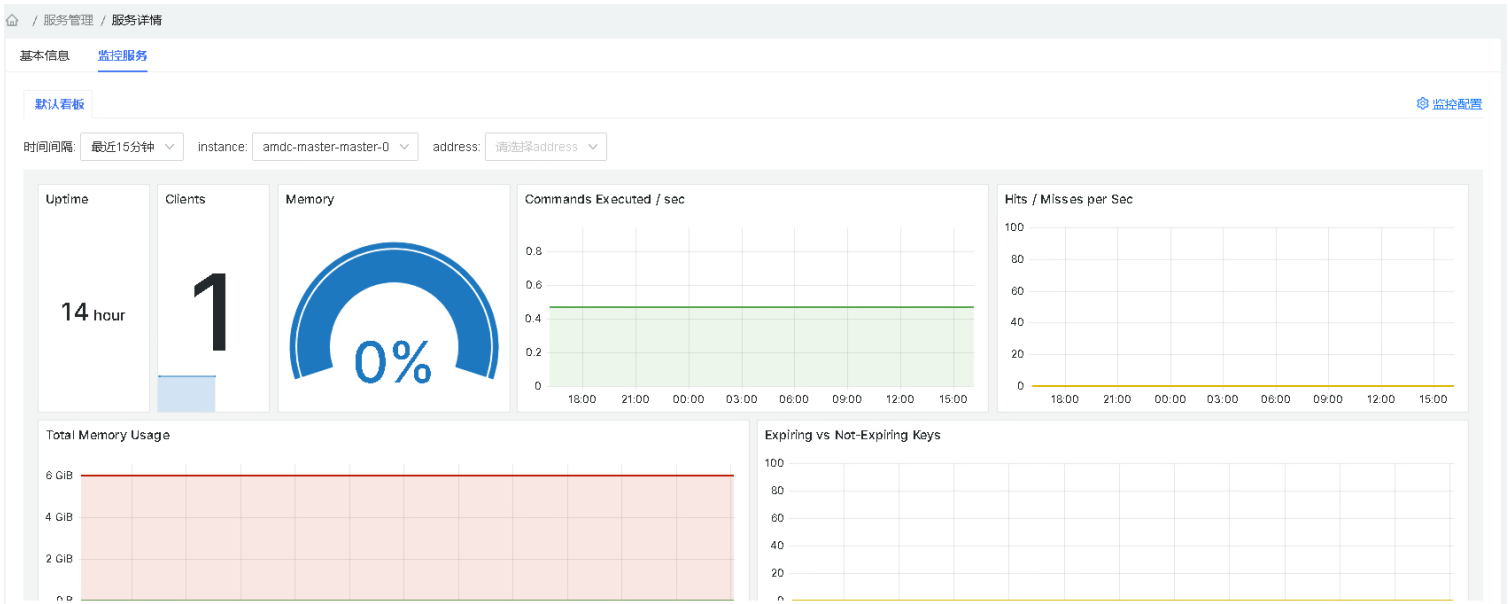
容器实例0

☐	实例名称	类型	运行状况	安全评分	所属服务	制品包/镜像	IP地址	重启次数	操作
☐	fan-test-sts-AAMSV10SP11-0	主机	SUCCESS	100	fan-test	AASV10/AAMSV10SP11-AAS-V10.0.8-SP11-AE-2...	172.24.4.42	0	日志 远程终端 更多

共1条 < 1 > 10条/页

7. 查看监控服务

选定一条服务记录，点击服务名称，进入服务详情页面，点击【监控服务】，可查看服务下的监控服务。点击【监控模板】可进行监控模板切换，以不同角度对实例进行监控。



8. 卸载服务

当服务不再需要时，点击【卸载】将其移入服务回收站。这是一种“软删除”机制，防止误操作导致数据丢失。

5.4.1.1 服务回收站

回收站用于存放已被卸载的服务，给您一个“反悔”的机会。

1. 查看回收站列表

进入回收站后，您可以查看所有已被卸载的服务记录。



2. 恢复服务

如果误卸载了某个服务，可以选定后点击【恢复】，将服务及其配置恢复到正常状态。

3. 永久删除

对于确认不再需要的服务，选定后点击【删除】即可永久清除记录（不可恢复）。

4. 批量操作

您也可以勾选多条记录，批量恢复或批量删除。

5. 清空回收站

点击【清空回收站】可以一键清除所有回收站记录。

5.4.2 实例管理

5.4.2.1 平台实例

平台实例是平台通过服务部署创建的中间件运行实例。您可以在这里查看实例的运行状态、连接远程终端、修改配置，以及执行升级操作。

1. 查看实例列表

页面默认展示所有实例，您可以通过顶部的 Tab 在“全部/主机/容器”之间切换筛选。列表中包含实例名称、软件类型、运行状态和所在主机等信息。

平台实例

运行状况

服务

部署模式

请输入实例名称

搜索

重置

启动

停止

重启

导出

全部

主机实例

容器实例

刷新

☐	实例名称	类型	运行状况	安全评分	所属服务	制品包/镜像	IP地址	重启次数	操作
☐	amdc-slaver-slave-1	主机	SUCCESS	100	amdc	apusic/AMDC-Core:v2.0.2-20250611	172.24.4.216	0	日志 远程终端 更多
☐	amdc-slaver-slave-0	主机	SUCCESS	100	amdc	apusic/AMDC-Core:v2.0.2-20250611	172.24.4.218	0	日志 远程终端 更多
☐	amdc-master-master-0	主机	SUCCESS	100	amdc	apusic/AMDC-Core:v2.0.2-20250611	172.24.4.42	0	日志 远程终端 更多
☐	test-zk-exporter-exporter-0	主机	SUCCESS	100	test-zk	apusic/Zookeeper_Exporter:v0.1.13	172.24.4.218	0	日志 远程终端 更多
☐	test-zk-zookeeper-zk-0	主机	STOPPED	0	test-zk	apusic/Zookeeper:3.9.4	172.24.4.218	0	日志 远程终端 更多
☐	test-alb2-server-alb-0	主机	SUCCESS	100	test-alb2	apusic/ALB.V2.0.6-SE-20260703	172.24.4.218	0	日志 远程终端 更多
☐	testccc-docker-nginx-0	容器	CHECKING	100	testccc	harbor.apusic.com/dify/nginxlatest	172.24.4.216	0	日志 远程终端 更多

2. 启动/停止/重启

选定一个或多个实例后，可直接执行启动、停止或重启操作。

3. 远程终端

需要登录实例所在的主机或容器时，点击【终端】按钮即可打开内置的远程终端，无需额外工具。

4. 实例升级

- 实例制品、补丁升级 对于运行在主机上的实例，可以通过【制品升级】和【补丁升级】对实例进行升级和漏洞修复。首先选择对应的制品或补丁，然后批量选择需要升级的实例。

批量补丁升级

×

1 选择补丁

2 选择实例

请输入补丁名称进行搜索

Q

补丁名称	补丁类型	关联漏洞	上传人	上传时间
☐ test	一般	-	acpadm	2026-01-30 18:29:...
☒ AAS测试补丁	重要	-	mahongbin	2025-12-12 17:06:...

共2条

<

1

>

取消

下一步

- 容器镜像升级 对于运行在容器中的实例，可以通过【镜像升级】更新到新的镜像版本。通过选择镜像仓库，录入镜像名称以快速搜索待升级的镜像。

镜像升级 (1个实例)

×

选中实例

testccc-docker-nginx-0

当前镜像

harbor.apusic.com/dify/nginx:latest

目标镜像

选择镜像仓库:

apusic-harbor (https://harbor.apusic.com/) ▾

[全局搜索](#) [按项目浏览](#)

搜索镜像:

nginx × 🔍

搜索结果 (共 33 条) :

项目	镜像	下载次数	操作
dify	nginx	10	选择

取消

下一步

5. 查看修改实例详情

点击实例名称进入详情页面，您可以通过不同的 Tab 查看修改各类信息：

- **主机实例：**配置文件、日志信息、端口监听、事件记录、环境变量、数据卷、健康检查、资源使用、安全扫描结果

平台实例 / 实例详情

实例信息

实例名称	amdc-slaver-slave-1	类型	主机	所属服务	amdc
运行状况	● SUCCESS	IP地址	172.24.4.216	部署模式	AMDCv2.0.2/主从
制品名称	apusic/AMDC-Core:v2.0.2-20250611	运行时长	1天1小时47分30秒	安装路径	/root/.apusic/workspace/2b172321-7584-427a-a803-ccadd8c4c968
租户	默认租户	项目	默认项目	创建时间	2026-07-23 14:05:08

配置文件 (1) 日志信息 (0) 端口监听 (2) 事件 (4) 环境变量 (24) 数据卷 (0) 健康检查

配置文件名	存放位置	文件大小(K)	修改时间	操作
conf.yaml	/	12.30	2026-07-23 14:05:08	编辑

共 1 条 < 1 >

资源信息

所属平台	私有云	规格/镜像	8 vCPUs 15.512 GB/CentOS 7.9.2009 X86_64	可用内存	7.08 G
区域	开发环境机器	主机类型	虚拟机	可用磁盘	330.95 G

- 容器实例：配置信息、环境变量、标签（Labels）、重启策略、卷挂载、端口映射、网络设置

平台实例 / 实例详情

实例信息

实例名称	testccc-docker-nginx-0	类型	容器	容器ID	32b046d4be7e...
IP地址	172.24.4.216	所属服务	testccc	项目	默认项目
运行状态	● CHECKING	部署模式	testSignV/V1.0.2/nginxuser	镜像	harbor.apusic.com/dify/nginx:latest
租户	默认租户	创建时间	2026-07-15 15:31:55		

实例信息 环境变量 标签 重启策略 卷 (4) 端口 (0) 网络 (1) 配置文件

修改容器配置

配置信息

工作目录	-	用户	root	TTY	否
停止信号	SIGTERM	自动移除	否	特权模式	是
网络模式	bridge	标准输入	关闭	CPU限制	-
内存限制	-				

启动命令

Entrypoint `["/docker-entrypoint.sh"]`

5.4.2.2 纳管实例

纳管实例是从外部环境发现的中间件实例，通过纳管操作将其纳入平台统一管理。与平台实例不同，纳管实例原本并非通过平台部署，而是通过扫描或其他方式发现的存量实例。

1. 查看纳管实例列表

与平台实例类似，您可以通过 Tab 在“全部/主机/容器”间切换，列表中展示了每个纳管实例的名称、软件类型、运行状态和所在主机。

纳管实例

运行状况

服务

关联组件

请输入实例名称或IP搜索

搜索

重置

启动

停止

重启

导出

纳管为服务

移除

导入

全部

主机实例

容器实例

刷新

☐	实例名称	类型	运行状况	安全评分	服务名称	软件名称	版本	关联组件	关联制品/镜像	IP地址	来源	创建时间	操作
☐	nginx-prometh	主机	未知	100	-	Nginx	1.29.2	Nginx/1.29.2/nginx_expor...	-	172.24.4.42	扫描纳管	2026-07-	编辑 远程终端 更多
☐	testsss	容器	运行中	100	-	Nginx	latest	testSignV/V1.0.2/nginx	harbor.apusic.com/dify/n...	172.24.4....	扫描纳管	2026-07-	编辑 远程终端 更多

共2条

1

10条/页

2. 导入纳管实例

点击【导入】，通过导入模板批量地将外部中间件实例信息导入为纳管实例，纳入平台管理范围。

导入纳管实例

×

请下载纳管实例导入模板，按格式导入

ⓘ

请先下载模板文档，根据格式和提示填写内容。请确保各字段类型正确无误，否则有可能导致导入失败。切勿修改模板中的字段名称。数据导入上限为2000条。

↑

点击或拖拽文件上传

3. 纳管为服务 当多个实例存在关联关系时，可批量选中，将其关联为服务，并配置服务信息。



4. 编辑纳管实例

选定实例后，可以编辑其基本信息，确保信息准确。

纳管实例编辑



① 为了确保纳管实例的有效性，请确认以下信息。

基本信息

* 实例名称	nginx-prometheus-exporter_o0e952M5UF
* 关联组件	Nginx/1.29.2/nginx_exporter
关联制品	
IP地址	172.24.4.42
端口	9213
安装路径	/root/.apusic/workspace/52ec75e8-4b7d-426f-ac71-de165686d10f
备注	

操控命令

启动命令

停止命令

```
1 ./nginx-prometheus-exporter --web.listen-address :9213 -nginx.scrape-uri http://localhost:8
```

取消

确定

- **关联组件**：关联组件可帮助平台识别该实例所使用的软件。并提供对应的各类维护操作。
- **关联制品**：该实例安装时使用的制品，如需要进行制品或补丁升级，则必须填写。
- **启动、停止命令**：该软件启动或停止时，所执行的命令。可根据实际情况填写。

5. 启动/停止/重启

同平台实例一样，您可以直接对纳管实例执行生命周期操作。

6. 远程终端

点击【终端】可远程连接到纳管实例所在的环境。

7. 补丁/镜像升级

根据实例类型（主机/容器），提供对应的补丁或镜像升级能力。需填写关联组件后才能够支持。

8. 查看修改纳管实例

选定一条纳管实例，点击实例名称，进入纳管实例详情页面，您可以通过不同的 Tab 查看修改各类信息

- 主机实例详情

🏠 / 纳管实例 / 详情

实例信息

实例名称	nginx-prometheus-exporter_o0e952M5UF	类型	主机	所属服务	-
运行状态	未知	软件名称	Nginx	版本	1.29.2
关联组件	Nginx/1.29.2/nginx_exporter	关联制品	-	IP地址	172.24.4.42
来源	扫描	创建时间	2026-07-24 10:06:56	安装路径	/root/.apusic/workspace/52ec75e8-4b7d-426f-ac71-de165686d10f

高级信息

启动命令查看

停止命令查看

配置文件

日志信息

端口监听

协议	网络	端口	说明	状态	进程
TCP	::	9213	-	LISTEN	6454/nginx-prometheu

资源信息

所属平台	私有云	规格/镜像	8 vCPUs 15.512 GB/centos 7.9.2009 amd64	可用内存	3.18 G
区域	开发环境机器	主机类型	虚拟机	可用磁盘	73.52 G

- 容器实例详情

🏠 / 纳管实例 / 详情

实例信息

实例名称	testsss	类型	容器	容器ID	9f6479669329...
IP地址	172.24.4.216	所属服务	-	项目	-
运行状态	运行中	部署模式	testSignVV1.0.2/nginx	来源	扫描
镜像	harbor.apusic.com/dify/nginx:latest	租户	默认租户	创建时间	2026-07-23 15:55:19

实例信息

环境变量

标签

重启策略

卷 (2)

端口 (2)

网络 (1)

配置文件

修改容器配置

配置信息

工作目录	-	用户	root	TTY	否
停止信号	SIGTERM	自动移除	否	特权模式	是
网络模式	bridge	标准输入	关闭	CPU限制	-
内存限制	-				

启动命令

9. 移除和导出

对于不再需要管理的纳管实例，可以【移除】；需要备份配置时可以【导出】。

5.4.3 软件管理

软件管理是平台的知识库，定义了平台支持哪些中间件、每个中间件有哪些版本、如何安装部署。当您需要引入一个新的中间件到平台时，首先要在这里完成软件定义。

1. 浏览软件列表

页面列出了所有已定义的软件，您可按名称搜索。每个软件项展示了名称、最新版本、类型等信息。

软件管理

搜索重置

新增软件导入导出

☐	软件名称	软件标识	标签	版本	发布状态	创建时间	操作
☐	AAMSV10SP11	aamsv10sp11	应用服务器	v10.0.8 v10.0.8sp11	未发布	2026-07-03 11:17:23	发布删除
☐	Golden_aas	golden_aas	应用服务器	V10 V11	未发布	2026-06-22 18:34:30	发布删除
☐	AUC	auc	微服务中间件	v2.0.1	未发布	2026-06-18 09:28:17	发布删除
☐	AASV9	aasv9	应用服务器	sp10	未发布	2026-06-16 09:59:35	发布删除
☐	admin	admin	分布式消息	v1	未发布	2026-06-11 11:06:25	发布删除
☐	hummerisk	hummerisk	微服务中间件	1.5.0 11	未发布	2026-06-09 14:05:00	发布删除
☐	orion_visor	orionvisor	微服务中间件	latest	未发布	2026-06-09 14:00:13	发布删除
☐	test	test	分布式消息	1.0	未发布	2026-06-03 10:14:44	发布删除
☐	demo	demo	分布式消息	v1	未发布	2026-05-26 10:56:43	发布删除
☐	testSignV	aaa	应用服务器	v1.0.0 V1.0.2	未发布	2026-05-22 15:10:40	发布删除

共28条 < 1 2 3 > 10 条/页 跳至 页

instances

2. 软件导入/导出

支持导入 .tar.gz 格式的软件包快速批量定义软件，也可以将现有软件定义导出备份。

3. 新增软件

点击【新增】按钮，您有三种方式创建软件定义：

- 全新创建：从零开始定义一个新软件，填写名称、类型和描述
- 新增版本：在已有软件的基础上增加一个新版本
- 补充组件模式：为已有版本补充组件和部署模式的定义

新增软件

1 选择操作

2 软件信息

3 版本信息

4 模式组件

5 完成

全新创建软件
创建全新的软件、版本、组件及模式

为已有软件新增版本
选择已有软件，为其添加新版本，可复制已有版本的组件和模式

为已有版本补充组件模式
选择已有软件及版本，为其添加或补充组件和模式

取消

下一步

- **软件**：每个中间件软件在平台内对应一个软件条目，需要具有全局唯一的名称
- **版本**：每个软件都有多个版本，版本可用于识别软件和定义升级关系
- **组件**：每个软件部署时，其部件均具有一定的职责，例如数据节点、计算节点、代理节点等，不同的组件具有不同的配置和操作行为

4. 软件管理

选定一个软件后，您可以查看和管理它的所有版本，支持新增版本或将已有版本复制后微调。

软件管理 / AAMSV10SP11

AAMSV10SP11 应用服务器

标识: aamsv10sp11 2 版本 1 模式 描述 -

编辑基本信息

版本列表

v10.0.8sp11 最新

2026-07-03 创建

v10.0.8

2026-07-03 创建

+ 添加版本

版本 v10.0.8sp11 创建于 2026-07-03 1 种模式 1 个组件

版本号

v10.0.8sp11

创建时间

2026-07-03

模式数量

1 种

删除版本

版本组件定义

AAMSV10SP11

暂无描述

已配置模板

+

添加组件

部署模式

AAMSV10SP11

+ 添加模式

部署流程图

配置模板

监控看板

AAMSV10SP11 | 部署流程图

编辑编排

删除模式

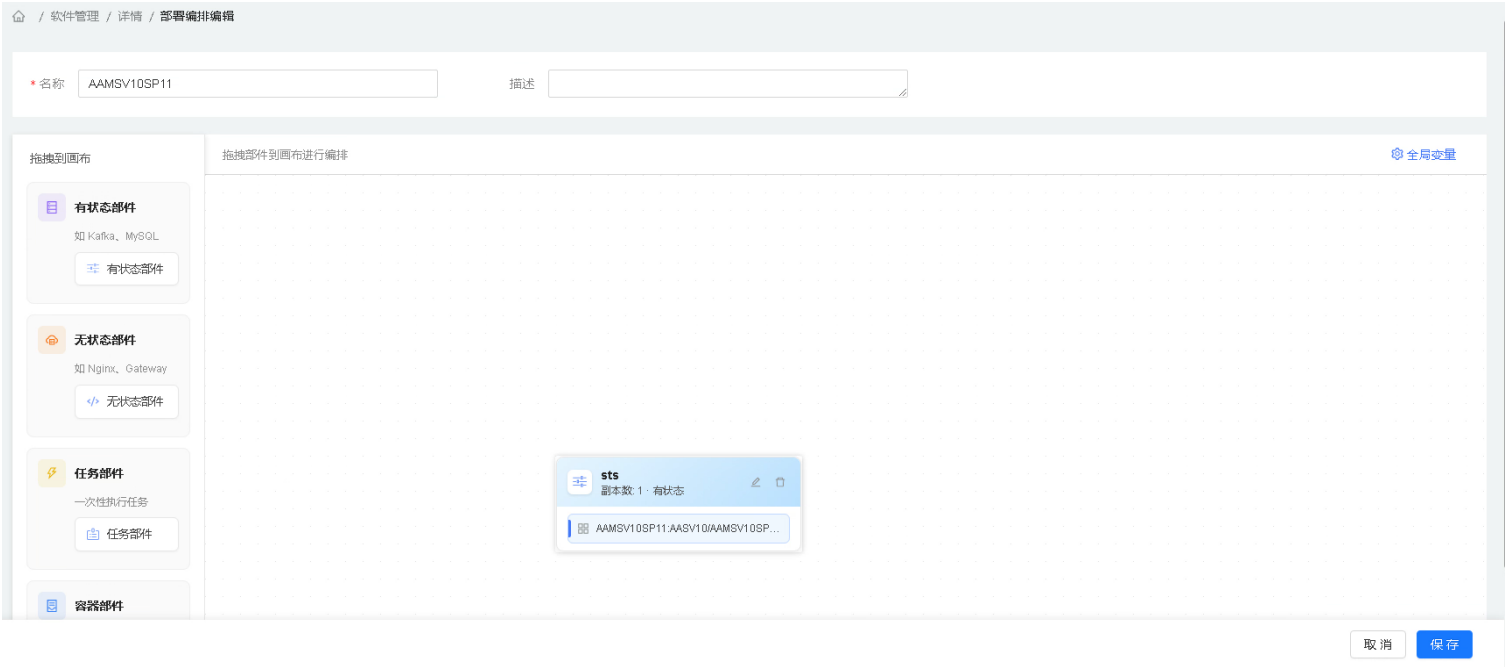
- **添加删除版本**：用户可新增或从历史版本中复制一个版本，再进行配置和调整。
- **版本组件**：可为对应版本定义组件，并定义组件的配置模板。

66

- **部署模式**：每个软件在不同场景下部署时，需要定义不同的部署模式，例如：单节点部署、主从部署、集群部署等。
- **部署流程图**：通过定义部署流程图，可快速定义部署流程，实现不同模式下的个性化部署。
- **配置模板**：可定义软件的配置模板，用户可基于模板快速生成配置文件。
- **监控看板**：可关联监控看板，为软件配置预置的监控图表。

5. 可视化编排

进入软件详情，选择模式，点击【编辑编排】，进入对应模式下的可视化编排页面。通过可视化编排，可快速定义软件部署模板，实现快速部署。



6. 发布软件

完成所有配置后，在软件列表界面，点击【发布】使该软件在服务部署时可供选择。

软件发布

请选择发布的版本及部署模式

☐	版本	部署模式	配置	监控
☐	v10.0.8sp11	AAMSV10SP11	√	x

关闭

确定

5.4.3.1 软件分类

软件分类帮助您将中间件按类别组织，便于在部署服务时快速定位。

1. 浏览分类

软件分类

中间件

数据库

请输入分类名称搜索

搜索

重置

新增分类

删除

☐ 分类名称	上级分类	描述	操作
☐ 应用服务器	中间件	-	编辑 删除
☐ 分布式缓存	中间件	-	编辑 删除
☐ 文本搜索	中间件	-	编辑 删除
☐ 微服务中间件	中间件	-	编辑 删除
☐ 服务代理	中间件	-	编辑 删除
☐ 分布式消息	中间件	-	编辑 删除

共6条 < 1 > 10条/页

2. 新增/编辑/删除分类

您可以新增分类、修改分类名称或删除不再需要的分类。

5.4.4 变更管理

变更管理记录了所有对服务执行过的变更操作（如补丁安装、版本升级等），为您提供完整的变更审计轨迹。

1. 查看变更历史

您可以按变更类型、时间范围或关键词搜索筛选，列表中清晰展示了每次变更的内容、操作类型、操作人、时间和执行结果。

变更管理

全部类型

开始日期 → 结束日期

对操作人、操作内容进行搜索

搜索

重置

操作类型	操作描述	操作对象	操作状态	操作人	操作时间	操作
镜像升级	实例【testaaa-docker-nginx-0】镜像升级, 旧镜像: sha256:6c3636c7aae08b4b8c9ddbf65bac1...	testaaa-docker-nginx-0	已完成	huangxiaolong	2026-06-11 17:29:10	
镜像升级	实例【testbbb-docker-nginx-0】镜像升级, 旧镜像: sha256:6c3636c7aae08b4b8c9ddbf65bac...	testbbb-docker-nginx-0	已完成	huangxiaolong	2026-06-11 17:28:56	
镜像升级	实例【testbbb-docker-nginx-0】镜像升级, 旧镜像: sha256:6c3636c7aae08b4b8c9ddbf65bac...	testbbb-docker-nginx-0	失败	huangxiaolong	2026-06-11 16:30:50	查看原因
镜像升级	实例【testaaa-docker-nginx-0】镜像升级, 旧镜像: sha256:6c3636c7aae08b4b8c9ddbf65bac1...	testaaa-docker-nginx-0	失败	huangxiaolong	2026-06-11 16:30:30	查看原因
镜像升级	实例【testaaa-docker-nginx-0】镜像升级, 旧镜像: sha256:6c3636c7aae08b4b8c9ddbf65bac1...	testaaa-docker-nginx-0	失败	huangxiaolong	2026-06-11 15:54:09	查看原因
镜像升级	实例【testbbb-docker-nginx-0】镜像升级, 旧镜像: sha256:6c3636c7aae08b4b8c9ddbf65bac...	testbbb-docker-nginx-0	失败	huangxiaolong	2026-06-11 15:53:57	查看原因
镜像升级	实例【singvaaa-docker-nginx-0】镜像升级, 旧镜像: sha256:6c3636c7aae08b4b8c9ddbf65bac...	singvaaa-docker-nginx-0	失败	huangxiaolong	2026-06-11 15:11:14	查看原因
镜像升级	实例【signvbbb-docker-nginx-0】镜像升级, 旧镜像: sha256:6c3636c7aae08b4b8c9ddbf65ba...	signvbbb-docker-nginx-0	失败	huangxiaolong	2026-06-11 15:11:02	查看原因
制品包升级	albDockerss-alb-alb-0 制品包 apusic/ALB_Docker:V2.0.5-SE-20251231 升级为制品包 apusic/AL...	albDockerss-alb-alb-0	失败	wrf	2026-03-26 14:25:09	回滚 查看原因
制品包升级	albDockerss-alb-alb-0 制品包 apusic/ALB_Docker:V2.0.2-AE-20250825 升级为制品包 apusic/A...	albDockerss-alb-alb-0	失败	wrf	2026-03-26 14:21:40	回滚 查看原因

共142条 < 1 ... 3 4 5 6 7 ... 15 > 10条/页 跳至 页

2. 回滚变更

如果某次变更导致了问题，且该变更支持回滚，您可以直接点击【回滚】撤销本次操作。

3. 排查失败原因

对于执行失败的变更，可以查看详细的失败原因信息，帮助您快速定位问题。

失败原因详情

操作类型	补丁升级
操作人	acpadmin
操作时间	2025-09-29 15:55:56
失败原因	patch container error:The container must be running .
详细信息	实例【aas-aasv10-AASV10-0】升级补丁包【AASV10补丁】

关闭

5.4.5 配置中心

配置中心提供了平台全局配置的集中管理能力。您可以在这里统一管理中间件的配置文件，追踪每次修改的历史，并在需要时快速回滚。

1. 查找配置

配置列表展示了所有配置项，您可按名称或类型搜索。列表中包含配置名称、类型、当前版本和最后更新时间。

配置中心

搜索配置名称、文件名称

全部文件类型

标签键

标签值

搜索

重置

共 19 个配置文件

配置名称	文件名称	文件类型	系统GID/系统UID	关联实例	标签	更新时间	操作
ICJseuozZP_alb.conf	alb.conf	CONF	0 / 0	test-alb2-server-alb-0	profileName: ALB/V2.0.6/... +8	2026-07-24 15:48:58	预览 编辑 历史 下载 删除
KHfGt6Fnox_apusic.conf	apusic.conf	CONF	0 / 0	fan-test-sts-AAMSV10SP11-0	profileName: AAMSV10SP... +8	2026-07-24 15:29:59	预览 编辑 历史 下载 删除
G6ovaHdXM0_nginxaaa.conf	nginxaaa.conf	CONF	0 / 0	testsss-docker-nginx-0	profileName: testSignV/V... +8	2026-07-24 15:03:34	预览 编辑 历史 下载 删除
KrDj9N409L_test.conf	test.conf	CONF	0 / 0	testsss	instanceName: testsss +6	2026-07-24 15:02:28	预览 编辑 历史 下载 删除
Wiy6xrlBIH_conf.yaml	conf.yaml	YAML	0 / 0	amdc-slaver-slave-1	profileName: AMDC/V2.0... +8	2026-07-23 14:05:08	预览 编辑 历史 下载 删除
vCyKRYSRtW_conf.yaml	conf.yaml	YAML	0 / 0	amdc-slaver-slave-0	profileName: AMDC/V2.0... +8	2026-07-23 14:05:08	预览 编辑 历史 下载 删除
xFUleEcC00_conf.yaml	conf.yaml	YAML	0 / 0	amdc-master-master-0	profileName: AMDC/V2.0... +8	2026-07-23 14:05:08	预览 编辑 历史 下载 删除
gW93wie99r_zoo.cfg	zoo.cfg	CONF	0 / 0	test-zk-zookeeper-zk-0	profileName: Zookeeper/... +8	2026-07-22 15:04:20	预览 编辑 历史 下载 删除
pNPk1XifeX_nginxaaa.conf	nginxaaa.conf	CONF	0 / 0	testccc-docker-nginx-0	profileName: testSignV/V... +8	2026-07-21 07:58:05	预览 编辑 历史 下载 删除
K8iHfQENJU_nginx.conf	nginx.conf	CONF	101 / 101	testccc-docker-nginx-0	profileName: testSignV/V... +8	2026-07-15 15:31:55	预览 编辑 历史 下载 删除

2. 编辑配置

选定一个配置后，点击【编辑】修改其内容。每次编辑需要填写变更摘要和变更类型，便于后续追溯。

配置中心 / 编辑配置

基本信息

配置名称

ICJseuozZP_alb.conf

文件名

alb.conf

文件类型

CONF

所属实例

test-alb2-server-alb-0

节点IP

172.24.4.218

配置路径

/conf

配置内容

取消 查看变更 保存

搜索

替换为

替换

全部替换

```
daemon off;
user root;
worker_processes auto;

#error_log logs/error.log;
#error_log logs/error.log notice;
#error_log logs/error.log info;

#pid logs/alb.pid;

events {
    worker_connections 1024;
}
```

3. 预览与下载

修改前可以先【预览】确认内容；需要将配置下发到本地时，可以点击【下载】。

4. 版本管理

每次编辑都会生成一个新版本。您可以查看完整的历史版本记录，选定任意两个版本进行内容对比，一目了然地看到差异。

配置历史版本 - ICJseuozZP_alb.conf

版本号	操作类型	操作人	操作时间	变更摘要	操作
v10	当前版本	chulei	2026-07-24 15:48:58	-	查看详情
v9	编辑	chulei	2026-07-24 15:47:20	ee	查看详情 回滚
v8	编辑	chulei	2026-07-22 22:41:43	demo	查看详情 回滚
v7	编辑	chulei	2026-07-22 22:19:10	换一个端口	查看详情 回滚
v6	编辑	chulei	2026-07-22 22:18:19	demo1	查看详情 回滚
v5	编辑	chulei	2026-07-22 22:16:01	demo1	查看详情 回滚
v4	编辑	chulei	2026-07-22 22:12:39	demo	查看详情 回滚
v3	编辑	wrf	2026-07-22 16:22:45	demo	查看详情 回滚

关闭

版本对比

上一个差异

下一个差异

1/1

✕

左侧版本：版本 v9 (2026-07-24 15:47:20)

右侧版本：当前版本 v10 (2026-07-24 15:48:58)

33

#keepalive_timeout 0;

34

keepalive_timeout 65;

35

36

此处是upstream配置

37

38

39

#gzip on;

40

41

server {

42

-listen 8086;

43

server_name localhost;

44

45

#charset koi8-r;

46

47

#access_log logs/host.access.log main;

48

location / {

49

root html;

50

index index.html index.htm;

51

}

52

33

#keepalive_timeout 0;

34

keepalive_timeout 65;

35

36

此处是upstream配置

37

38

39

#gzip on;

40

41

server {

42

+listen 8087;

43

server_name localhost;

44

45

#charset koi8-r;

46

47

#access_log logs/host.access.log main;

48

location / {

49

root html;

50

index index.html index.htm;

51

}

52

关闭

回滚到左侧版本

5. 版本回滚

如果某次修改有误，找到之前的正确版本，点击回滚即可恢复（回滚操作会生成一个新版本，不会丢失历史）。

5.5 云原生中间件管理

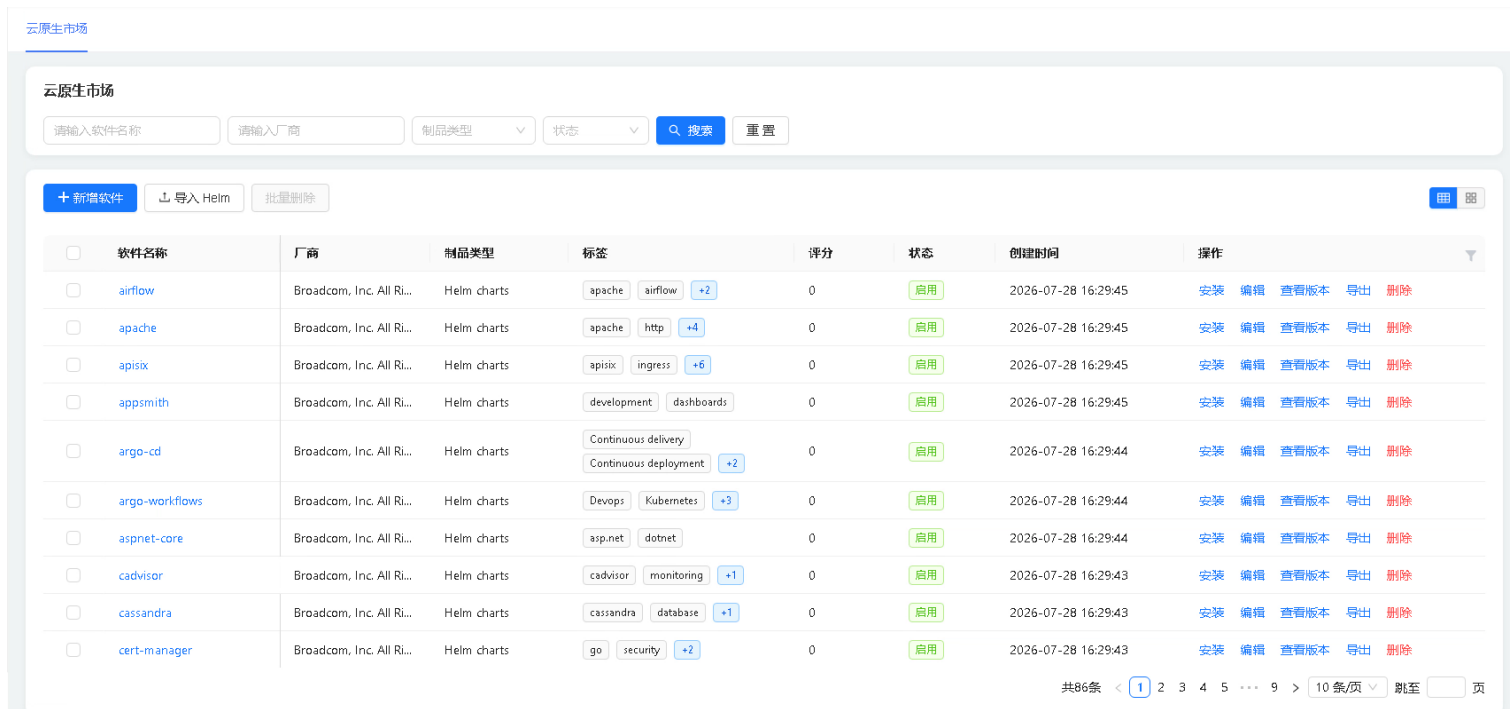
云原生中间件管理提供了面向云原生的中间件管理能力。包括民享软件管理的云原生市场以及面向服务实例的应用实例管理。

5.5.1 云原生市场

云原生市场支持预制各类云原生中间件，可一键安装，实现一键部署。同时支持用户上传自己维护的软件包，实现自定义云原生软件的统一管理。

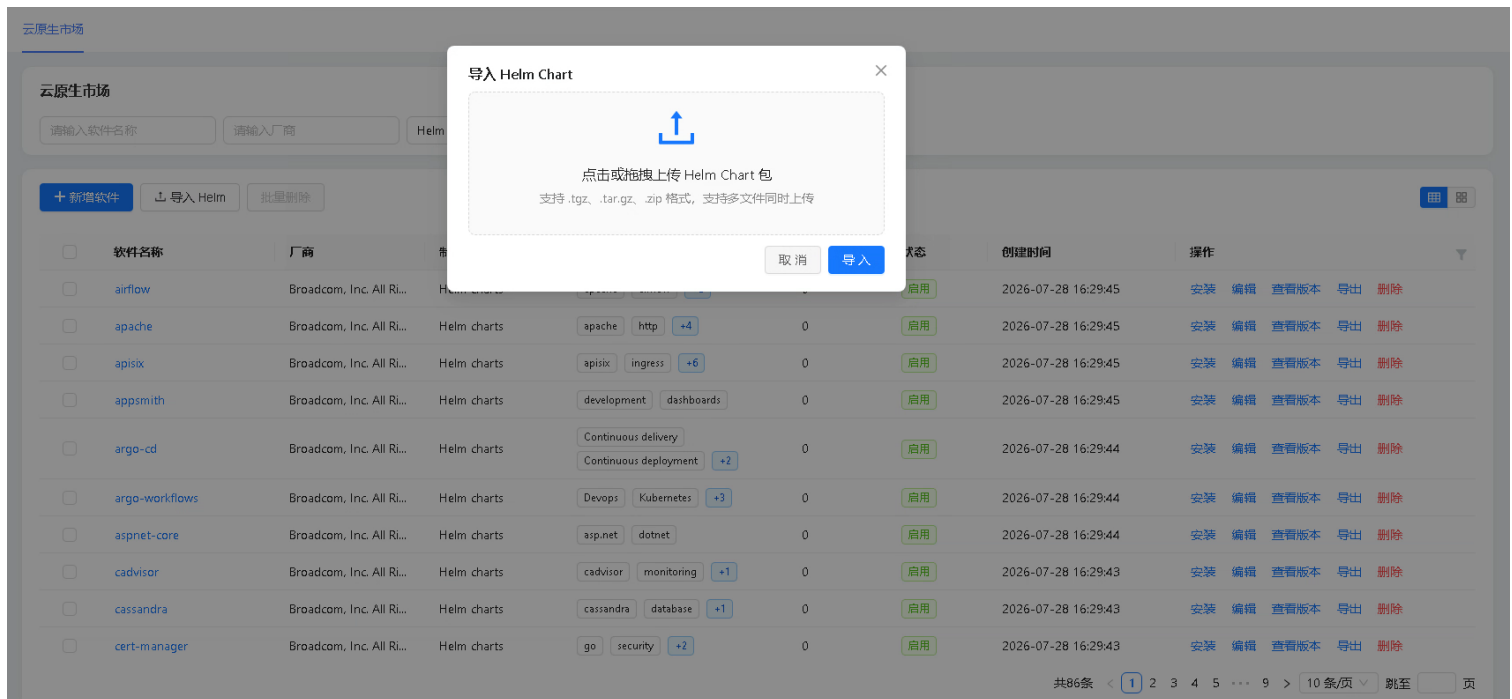
1. 查看云原生软件

进入云原生市场页面，可查看检索当前可用软件，



2. 导入云原生软件

点击【导入Helm】进行产品包导入。平台支持 Helm 格式包导入。并自动分析软件名称、软件版本、软件描述等信息。



3. 新增软件

点击【新增软件】，可通过手工方式进行产品创建，产品手工创建后，包描述不会因新增软件包导致信息变化，适用于需要自定义描述的场景。

云原生市场

新增软件

< 返回

基本信息

* 软件名称

请输入软件名称

* 厂商

请输入厂商

* 制品类型

☐ Helm charts

☒ Operator

* 状态

☒ 启用

☐ 禁用

来源地址

请输入来源地址

Logo

+

上传

标签

多个标签用英文逗号分隔

评分

0

软件描述

请输入简短描述

- **软件名称**：软件的唯一名称。
- **厂商**：该软件的提供厂商。
- **制品类型**：该软件的制品类型，包括 Helm charts 和 Operator 两种。
- **状态**：该软件启用禁用状态。启用状态下才可部署软件。
- **来源地址**：该软件的来源地址信息。
- **标签**：软件产品标签，可添加多个标签，使用逗号分隔。
- **评分**：软件评分，用于帮助用户选择软件。
- **软件描述**：该软件的基本描述信息。
- **软件概述**：该软件的功能、适用场景等信息。
- **详细说明**：该软件的功能、配置、使用方法等详细信息，支持markdown格式。

4. 查看版本

点击【查看版本】可快速查看软件版本信息。

云原生市场

grafana-operator - 版本管理

< 返回

+ 新增版本

版本号	安装内容	默认值	变更日志	操作
4.10.0	helm install grafana-operator grafana-operator-4.10.0.tgz	# Copyright Broadco...	# Changelog ## 4.10.0 (2026-03-12) * [bitnami/grafana-operator] Update Grafana Cust...	编辑 删除

点击【新增版本】可为该软件添加新的版本。点击【编辑】可修改该软件版本的版本信息。

4. 安装软件

点击选定软件的【安装】按钮，可进入该软件的安装部署配置，配置完成后，点击【保存】完成软件安装。

云原生市场

安装 apache

< 返回

安装信息

制品类型

Helm charts

* 版本

11.4.30

* 实例名称

请输入实例名称

描述

实例描述

* K8s 集群

请选择 K8s 集群

* 命名空间

请选择命名空间

默认值

```
1 # Copyright Broadcom, Inc. All Rights Reserved.
2 # SPDX-License-Identifier: APACHE-2.0
3
4 ## @section Global parameters
5 ## Global Docker image parameters
6 ## Please, note that this will override the image parameters, including dependencies, configured to use the global value
7 ## Current available global Docker image parameters: imageRegistry, imagePullSecrets and storageClass
8
9 ## @param global.imageRegistry Global Docker image registry
```

LF

- **制品类型**: 该软件的制品包类型，包括Helm chart或者Operator。
- **版本**: 该软件的安装版本。
- **实例名称**: 部署该软件时，设定的实例名称。
- **描述**: 该软件实例的描述信息。
- **K8S集群**: 可通过下拉选择，确定该软件实例部署到哪个K8S集群下。
- **命名空间**: 可指定该软件实例部署的K8S集群的命名空间。
- **默认值**: 该软件配置的默认值，可根据需要修改后进行部署。

5.5.2 应用实例

应用实例提供云原生市场安装的软件实例的统一管理能力。

1. 查看应用实例

软件安装后将自动进入应用实例列表页面，也可以通过应用实例菜单进入，可查看当前所有已安装的软件实例。

应用实例

应用实例

请输入实例名称

状态

制品类型

搜索

重置

实例名称	应用	版本	命名空间	制品类型	状态	失败原因	创建时间	操作
apache-test	apache	11.4.30	aa	Helm charts	运行中	-	2026-09-02 14:33:13	编辑 查看资源 删除
kafka-3	kafka	32.4.4	test	Helm charts	运行中	-	2026-08-12 14:08:23	编辑 查看资源 删除
demo	tomcat	13.0.0	demo	Helm charts	运行中	-	2026-08-12 14:07:31	编辑 查看资源 删除

共3条 < 1 > 10 条/页

2. 查看实例所属软件信息

点击【应用】列下的对应名称，可查看该软件实例的所属的软件信息，通过软件说明，了解软件的配置和使用方法。

3. 编辑应用实例

点击【编辑】可修改该软件实例的配置信息。

4. 查看资源

点击选定软件的【查看资源】按钮，进入实例资源页面，查看该软件实例的资源使用情况。

应用实例

实例资源

刷新

返回

HelmRelease 基本信息

实例名称: kafka-3

命名空间: test

集群名称: demo

状态: 运行中

制品类型: Helm charts

创建时间: 2026-08-12 14:08:23

描述: -

容器组

名称	命名空间	状态	创建时间	操作
kafka-3-controller-0	test	Running	2026-08-12 14:10:30	查看
kafka-3-controller-1	test	Running	2026-08-12 14:10:30	查看
kafka-3-controller-2	test	Running	2026-08-12 14:10:30	查看

有状态副本集

点击对应资源，支持查看资源的详细信息。

有状态副本集

demo / 有状态副本集 / kafka-3-controller

kafka-3-controller

命名空间 test 创建时间 2026-08-12 14:10:30 期望/就绪/当前/已更新 3/0/3/3 服务名 kafka-3-controller-headless

YAML

事件

更多

概览

容器组

事件

YAML

基本信息

名称	kafka-3-controller	命名空间	test
UID	d34f06fe-a552-4e19-87fc-c1fd242f30cc	创建时间	2026-08-12 14:10:30
期望/就绪/当前/已更新	3/0/3/3	服务名	kafka-3-controller-headless
选择器 (selector)	app.kubernetes.io/component=controller-eligible app.kubernetes.io/instance=kafka-3 app.kubernetes.io/name=kafka app.kubernetes.io/part-of=kafka		

Pod 模板

服务账号	kafka-3	重启策略	Always
容器	kafka harbor.apusic.com/bitnami/kafka:4.0.0-debian-12-r10 9093/TCP 9092/TCP 9094/TCP		

名称	类型/来源
kafka-configmaps	configMap: kafka-3-controller-configuration

5.6 可观测性

5.6.1 采集配置

5.6.1.1 指标采集

指标采集用于配置 Prometheus 监控指标的采集目标。当您需要将某个服务或主机的性能指标接入平台的监控系统时，在这里添加采集配置即可。

1. 管理监控目标

页面展示了所有已配置的指标采集目标。您可按服务标识或 IP 查找，列表中每个目标的服务标识、软件名称、IP、端口和采集状态（绿色=正常，红色=异常，灰色=未知）都清晰可见。 软件服务部署时，会自动添加监控目标。对于纳管实例，需要自行添加。

监控目标

搜索服务标识

搜索IP

搜索

重置

新增监控目标

软件名称	状态	地址	版本	标签	最后抓取	抓取耗时	操作
AMDC	● 正常	http://172.24.4.216:8004/metrics	v2.0.2	namespace: default_default +4	2026-07-24 16:51:47	6.28 ms	修改 删除
AMDC	● 正常	http://172.24.4.218:8004/metrics	v2.0.2	namespace: default_default +4	2026-07-24 16:51:45	4.09 ms	修改 删除
AMDC	● 正常	http://172.24.4.42:8004/metrics	v2.0.2	namespace: default_default +4	2026-07-24 16:51:41	7.38 ms	修改 删除
apusicdet	● 正常	http://172.24.3.63:9890/metrics	8.0.5.24	namespace: default_default +1	2026-07-24 16:51:40	10.16 ms	修改 删除
Zookeeper	● 正常	http://172.24.4.218:9141/metrics	3.9.4	namespace: default_default +4	2026-07-24 16:51:39	1.26 ms	修改 删除
ALB	● 异常	http://172.24.4.218:8080/status/format/prom...	V2.0.6	namespace: default_default +4	2026-07-24 16:51:43	0.67 ms	修改 删除
apusicdet	● 异常	http://172.24.4.74:9890/metrics	8.0.5	namespace: default_default +1	2026-07-24 16:51:48	0.63 ms	修改 删除
apusicdet	● 正常	http://172.24.3.92:9890/metrics	8.0.5.23	namespace: default_default +1	2026-07-24 16:51:49	24.66 ms	修改 删除
apusicdet	● 正常	http://172.24.4.90:9890/metrics	8.0.5.24	namespace: default_default +1	2026-07-24 16:51:51	10.89 ms	修改 删除
apusicdet	● 正常	http://172.24.2.60:9890/metrics	8.0.5.24	namespace: default_default +1	2026-07-24 16:51:42	14.01 ms	修改 删除

共 63 条

1

2

3

4

5

6

7

>

10 条/页

跳至

页

2. 新增采集目标

点击【新增监控目标】，填写服务标识、软件名称、IP、端口、指标路径和协议等信息，还可以添加标签和认证信息，即可创建新的采集目标。

新增监控目标



* 服务标识

例如: service-001

* 软件名称

请选择软件名称

* 类型

-

* 版本

请选择版本

* 部署模式

请选择部署模式

命名空间

default

* IP地址

例如: 192.168.1.100

* 端口

例如: 8080

指标路径

/metrics

协议

HTTP

添加标签

证书

取消

注册

- **服务标识**: 监控目标的唯一标识、全局唯一
- **类别**: 采集分组
- **软件名称**: 与平台内软件关联, 填写后自动添加采集标签。
- **版本**: 软件关联的版本, 填写后自动添加采集标签。
- **部署模式**: 软件关联的部署模式, 填写后自动添加采集标签。
- **命名空间**: 软件关联的命名空间, 填写后自动添加采集标签。
- **IP**: 监控目标主机的 IP 地址。
- **端口**: 监控目标主机的端口号。
- **指标路径**: 指定 Prometheus 抓取指标的路径。
- **协议**: 指定 Prometheus 抓取指标的协议。
- **认证信息**: 指定 Prometheus 抓取指标的认证信息。

- **标签**：手工添加的标签，用于标识采集目标。

3. 修改或删除

对于已有配置，点击【修改】可以调整采集参数；不再需要的目标可以【删除】。

5.6.1.2 日志采集

日志采集用于配置日志文件的采集规则。当您需要将某个主机上的应用日志接入平台的日志中心进行分析时，在这里添加日志采集配置即可。

1. 管理日志采集列表

页面展示所有已配置的日志采集任务。您可按服务器 IP 或软件类型查找，每个采集任务的服务器、软件类型和日志路径等信息一目了然。

日志采集

搜索服务器IP

搜索软件类型

搜索

新增日志采集

服务器IP	软件类型	制品名称	服务名	日志路径	实例名	组件名称	标签	操作
172.24.4.218	redis	redis	218_redis	/root/.apusic/logs/bfcebfa...	218_redis-redis-redis-0	redis	apusic.appname: asp +12	修改删除
172.24.4.218	redis	redis_exporter	218_redis	/root/.apusic/logs/731b0f...	218_redis-redis-redis_ex...	redis	apusic.type: logdata-a''' +11	修改删除
172.24.4.42	nginx	nginx_exporter	nginx42	/root/.apusic/logs/52ec75...	nginx42-server-nginx_ex...	server	apusic.type: logdata-a''' +11	修改删除
172.24.4.42	nginx	nginx	nginx42	/root/.apusic/logs/3664dc...	nginx42-server-nginx-0	server	apusic.type: logdata-a''' +11	修改删除
172.24.4.42	sad	sadad	sadad	/opt/filebeat/test.log	sadd	sad	apusic.type: logdata-a''' +11	修改删除
172.24.4.42	zk	zk_server	zk-42	/opt/filebeat/zk.log	zk-instance-666	zk	apusic.appname: asp +13	修改删除

共 6 条 < 1 > 10 条/页

2. 新增日志采集

用户部署服务时，将自动建立日志采集任务，无需手工配置。涉及到纳管实例时，需要自行添加。点击【新增】，选择目标服务器（系统会自动填充 Agent 信息），选择软件类型，填写日志文件路径和排除文件格式，即可开始采集。

新增日志采集



* 服务器IP

请选择服务器IP



* 软件类型

请选择软件类型



软件版本

请选择软件版本



制品名称

例如: zk_server

服务名

例如: zk-42

实例名

例如: zk-instance-01

部署模式

例如: standalone

组件名称

例如: zk

日志路径

添加日志路径

取消

新增

- **服务器 IP**: 待采集中间件的主机 IP, 该主机需已安装 Agent, 否则无法启动采集

除软件类型外, 以下都可不录入, 如录入会被当做标签用于日志检索。

- **软件类型**: 待采集软件类型
- **软件版本**: 待采集软件版本
- **制品名称**: 待采集软件使用的制品
- **服务名**: 待采集实例的平台服务名
- **实例名**: 待采集实例的平台实例名
- **部署模式**: 待采集实例的部署模式
- **组件名称**: 待采集的组件名称

- **日志路径**：添加需要采集的主机日志路径，格式为 `/path/to/*.log`
- **排除文件格式**：添加需要排除的文件格式，格式为 `\.gz$`
- **标签**：手工添加的标签，用于标识采集目标。

3. 修改和删除

采集配置支持随时修改日志路径或排除规则；不再需要时可以删除。

5.6.2 告警规则

告警规则以告警规则组为单位进行管理，每个告警规则组下可以有多条告警规则。告警规则可以通过告警模板进行引入，实现告警规则的复用。

5.6.2.1 告警模板

告警规则将系统的监控指标与告警行为关联起来。当指标数值满足规则中设定的条件时，系统会自动生成告警事件，通知相关人员。

1. 浏览检索告警模板

告警模板

搜索模板名称

告警级别

搜索

重置

新增告警模板

导出

导入

☐ 模板名称	告警级别	运算符	阈值	单位	描述	创建时间	操作
☐ ADMQ Broker JVM Heap ...	轻微 (P3)	>	80	%	-	2026-07-07 14:22:47	编辑 删除
☐ ADMQ生产延迟过高告警	轻微 (P3)	>	10	ms	-	2026-07-07 14:21:56	编辑 删除
☐ Redis平均响应时长告警	轻微 (P3)	>	100	ms	监控Redis实例的平均响应时长，超过阈值可能意味着存在慢查询或性能瓶颈	2026-07-01 15:49:49	编辑 删除
☐ 节点使用率不能大于百分之...	提示 (P4)	>	80	%	节点使用率不能大于百分之80	2026-07-01 15:49:49	编辑 删除
☐ 虚拟机内存使用率过高告警	一般 (P2)	>	85	%	监控虚拟机内存使用率，当使用率超过85%时触发警告，防止内存溢出或OOM	2026-07-01 15:49:49	编辑 删除
☐ 虚拟机CPU使用率过高告警	一般 (P2)	>	85	%	监控虚拟机CPU使用率，当使用率超过85%时触发警告，防止服务响应变慢或系统负载过高	2026-07-01 15:49:49	编辑 删除

共 6 条

< 1 >

10 条/页

2. 导出导入告警模板

告警模板支持导出，选择需要导出的告警模板，点击【导出】，系统将导出当前选中的所有告警模板。导出文件为 Excel 文件，便于进行规则维护。维护好包含告警模板的 Excel 文件后，点击【导入】，系统将弹出导入对话框。可选择冲突处理策略，并选择需要导入的 Excel 文件。

- **冲突处理策略**：当系统与文件中的规则出现冲突时，系统将默认使用冲突处理策略进行处理
 - **跳过（默认）**：自动跳过有冲突的规则，只补充系统中缺少的规则
 - **覆盖**：使用文件中的规则覆盖系统中的规则

3. 新增修改告警模板

告警模板用于定义告警规则，在列表界面点击【新增告警模板】按钮，进入新增页面。

告警规则 / 告警模板 / 新增告警模板

新增告警模板

JSON 导入

Prompt 选料

* 模板名称

例如: CPU 使用率告警模板

* 告警级别

轻微 (P3)

描述

请输入模板描述

* PromQL 表达式

例如: avg(cpu_usage(instance="\$instance")) > 80

* 运算符

>

* 阈值

例如: 80

单位

例如: %

执行

标签模板

定义告警规则生成时附加到 Prometheus 规则 labels 中的键值对, 支持使用 ((变量))。常用于规则分类、路由、分组和筛选。

常见标签作用

team: 责任团队, 用于路由到对应值组

category: 类别划分 (基础设施应用/网络), 用于分组和筛选

runbook_url: 运行手册链接, 便于快速定位处理方案

自定义标签: 如 env、project、datacenter、business 等, 用于企业内部的维度划分

- **模板名称**：告警模板名称，全局唯一
- **告警级别**：告警级别分为 5 级，包含致命(P0)/严重(P1)/一般(P2)/轻微(P3)/提示(P4)，告警规则引入时，可以修改。
- **告警描述**：对该条告警模板的描述
- **PromQL 表达式**：通过 Prometheus 语法定义，可获取任意指标数据。填写后，点击【执行】，可查看取值情况。
- **运算符**：参与取值的运算符，如大于、小于、等于、不等于、大于等于、小于等于
- **阈值**：PromQL 获取的阈值
- **单位**：标记取值的单位，若无单位可不填
- **标签模板**：定义告警规则生成时附加到 Prometheus 规则 labels 中的键值对
 - **标签键**：标签的名称
 - **标签值模板**：标签值的预设值，在告警规则配置时可修改。
- **注释模板**：定义告警规则生成时的注释（annotations）
 - **注释键**：注释的名称
 - **注释值模板**：注释值的预设值，在告警规则配置时可修改。

4. 删除告警模板

告警模板不建议删除，如确认该告警模板已不再使用，且没有任何引用时，可点击【删除】，进行删除操作。

5.6.2.2 告警规则组

告警规则组是告警规则的集合，每个告警规则组下可以有多条告警规则。可在告警规则组下直接创建告警规则，也可以通过导入告警模板创建告警规则。

1. 浏览检索告警规则组

进入告警规则组管理页面，可查看所有告警规则组。支持按照规则组名称进行检索。

告警规则组

搜索重置

新增告警规则组

规则组名称	组描述	规则数量	状态	最近更新时间	操作
redis	-	1		2026-07-16 13:15:54	查看 编辑 删除
nodeAlarm	节点告警	1		2026-06-30 16:13:29	查看 编辑 删除
mhibtest	-	1		2026-06-22 16:48:28	查看 编辑 删除

共 3 条 < 1 > 10 条/页

2. 新增告警规则组

进入告警规则组列表页面，点击【新增告警规则组】，进入新增页面。

告警规则 / 新增告警规则组

规则组信息

规则组名称

例如 Redis 监控规则组

组描述

请输入规则组描述

告警规则

规则组内的规则基于告警规则生成，创建后仍可继续添加或删除

+ 添加告警规则

+ 从模板中添加

暂无告警规则

- 规则组名称：告警规则组名称，全局唯一
- 组描述：告警规则组描述
- 告警规则：用户配置的告警规则，当监控数据满足规则条件时，将产生对应的告警。
 - 添加告警规则：手工添加告警规则
 - 从模板中添加：从模板选择告警模板，将模板中的规则添加到当前告警规则组中

从模板中选择

ADMQ生产延迟过高告警

轻微 (P3)

histogram_quantile(0.99, sum(rate(pulsar_broker_publish_latency_le[5m])) by (le, broker))

env:prod

参数0个

Redis平均响应时长告警

轻微 (P3)

avg by(instance) (redis_commands_duration_seconds_total / redis_commands_processed_total) * 1000

env:prod team:ops

参数0个

节点使用率不能大于百分之80

提示 (P4)

(1 - (node_memory_MemAvailable_bytes / node_memory_MemTotal_bytes)) * 100

env:prod

参数0个

☒

虚拟机内存使用率过高告警

一般 (P2)

(1 - (node_memory_MemAvailable_bytes / node_memory_MemTotal_bytes)) * 100

env:prod team:ops

参数0个

虚拟机CPU使用率过高告警

一般 (P2)

100 - (avg by(instance) (irate(node_cpu_seconds_total

env:prod team:ops

参数0个

共 6 条 < 1 > 10 条/页 ▾

已选 1 个模板

取消 添加

编辑规则

新增规则

* 规则名称

虚拟机内存使用率过高告警

软件名称

例如: redis

描述

监控虚拟机内存使用率，当使用率超过85%时触发警告，防止内存溢出或OOM

* PromQL 表达式

(1 - (node_memory_MemAvailable_bytes / node_memory_MemTotal_bytes)) * 100

查询

选择指标

* 运算符

>

* 阈值

85

单位

%

* 告警级别

一般 (P2)

等待时间

5m

取消

确定

3. 启用停用告警规则组

进入列表页面，点击规则组【状态】列按钮，实现启用停用切换。规则组停用时，该规则组下的所有规则将停用。规则组启用时，该规则组下的所有规则将启用。

5.6.2.3 告警规则

告警规则是告警规则组的明细部分，可以查看、启用、停用。但不能直接添加，需在规则组中进行添加。

1. 浏览检索告警规则

当告警规则组创建后，组下的告警规则将可以在此页面中被检索到。

告警规则

搜索策略名称

搜索分组

策略状态

搜索

重置

☐	策略名称	分组	软件类型	告警级别	等待时间	策略状态	创建时间	操作
☐	Redis平均响应时长告警	redis	-	轻微 (P3)	5m	☒	2026-07-15 14:26:16	修改 删除
☐	虚拟机CPU使用率过高告警	nodeAlarm	node	一般 (P2)	5m	☒	2026-06-30 15:57:29	修改 删除
☐	CPU使用率告警	mhbtest	-	提示 (P4)	5m	☒	2026-06-22 14:07:14	修改 删除

共 3 条 < 1 > 10 条/页

2. 启动停用告警规则

告警规则支持单独启用停止，便于用户快速调整规则生效状态。在告警规则列表界面中，点击【策略状态】实现启用停用切换。

3. 查看告警规则

在告警规则列表页面，点击【策略名称】，可快速查看告警规则详细的配置信息。

告警规则状态：虚拟机CPU使用率过高告警



策略配置

策略名称：虚拟机CPU使用率过高告警

分组：nodeAlarm

软件类型：node

告警级别：一般（P2）

策略状态：启用

等待时间：5m

PromQL: `100 - (avg by(instance) (irate(node_cpu_seconds_total{mode="idle"}[5m])) * 100)`

运算符：>

阈值：85%

指标类型：PROMQL

标签：

env=prod team=ops

告警说明：

summary=虚拟机 `{{ $labels.instance }}` CPU使用率过高description=虚拟机 `{{ $labels.instance }}` 的CPU使用率已达到 `{{ $value }}`%, 超过了 85% 的阈值, 请排查高负载进程或考虑扩容。

Prometheus 实际状态

实际状态：● 未触发

健康状态：正常

所属分组：nodeAlarm

评估间隔：15s

最近评估：2026-07-27T15:02:30.986987983+08:00

评估耗时：0.00288853s

关闭

5.6.3 指标监控

5.6.3.1 服务监控

服务监控为您提供了一站式的服务运行状态查看入口。您可以在这里了解每个服务的健康状态，并查看其监控图表。

1. 查看服务列表

页面左侧按软件类型分类，方便您快速筛选。列表中展示了服务的名称、状态（全部就绪/部分就绪/无就绪）和实例数量。

2. 查看监控详情

点击服务名称进入详情页面，您可以在这里查看：

- 基本信息：服务的基本配置信息
- 监控图表：嵌入 Grafana 的性能监控图表
- 告警策略：该服务关联的告警规则

- **告警事件**：该服务触发的告警记录

5.6.3.2 主机监控

主机监控帮助您了解每台主机的资源使用情况和运行状态。

1. 查看主机列表

页面展示了所有主机，您可按 IP 搜索。列表中包含主机的 IP、名称和当前状态。

2. 查看主机详情

点击主机名称进入详情页面，您可以查看 CPU、内存、磁盘等核心资源的监控图表，以及关联的告警策略和告警事件。

5.6.3.3 自定义监控

如果标准监控无法满足您的需求，可以通过自定义监控为特定资源定义监控指标。

1. 查看自定义监控列表

页面按软件类型分类展示，您可按需筛选查找。

2. 新增/编辑/删除

点击【新增】填写监控名称、关联的软件和版本等信息即可创建。已有配置支持编辑和删除（含批量删除）。

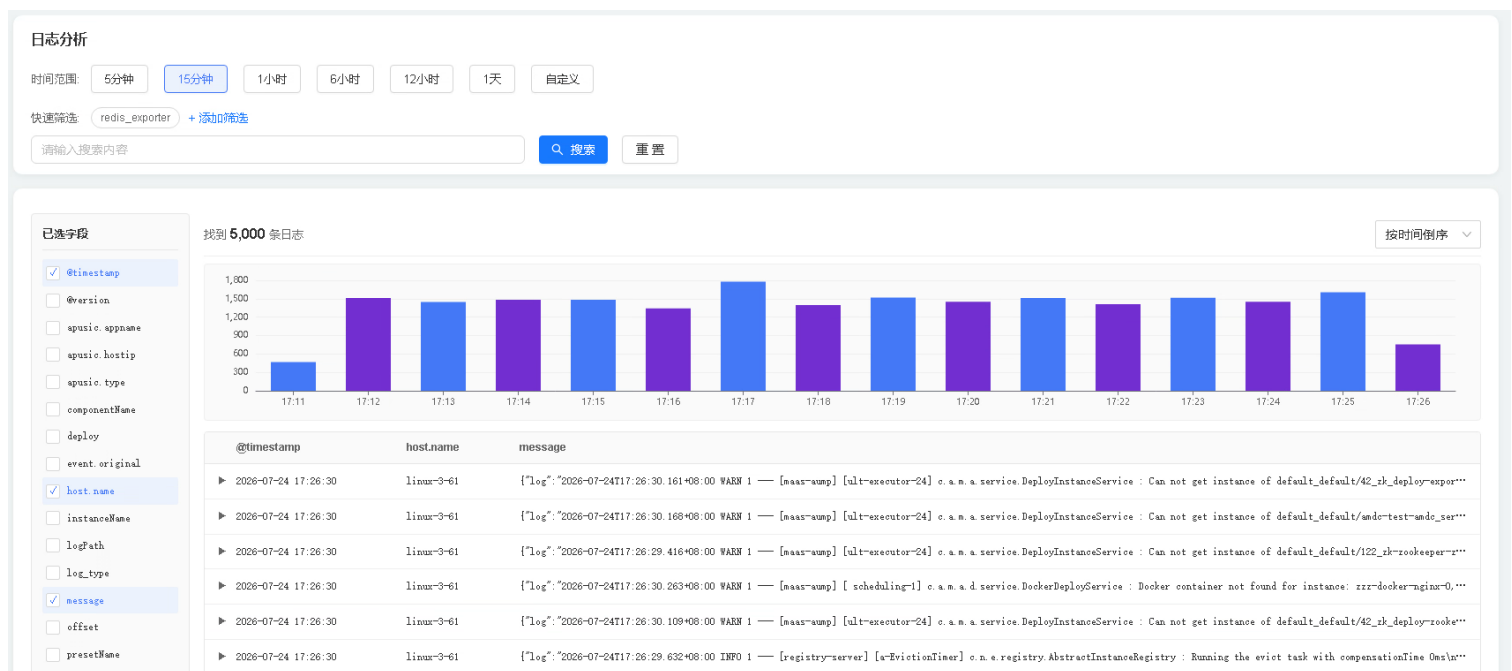
5.6.4 日志中心

5.6.4.1 日志分析

日志分析提供了日志的全文检索和分析能力。当您需要排查问题时，可以在这里快速搜索关键字、筛选时间范围，找到相关的日志记录。

1. 全文搜索

在搜索框中输入关键字（如错误码、事务 ID），系统会从所有已采集的日志中检索匹配的记录。

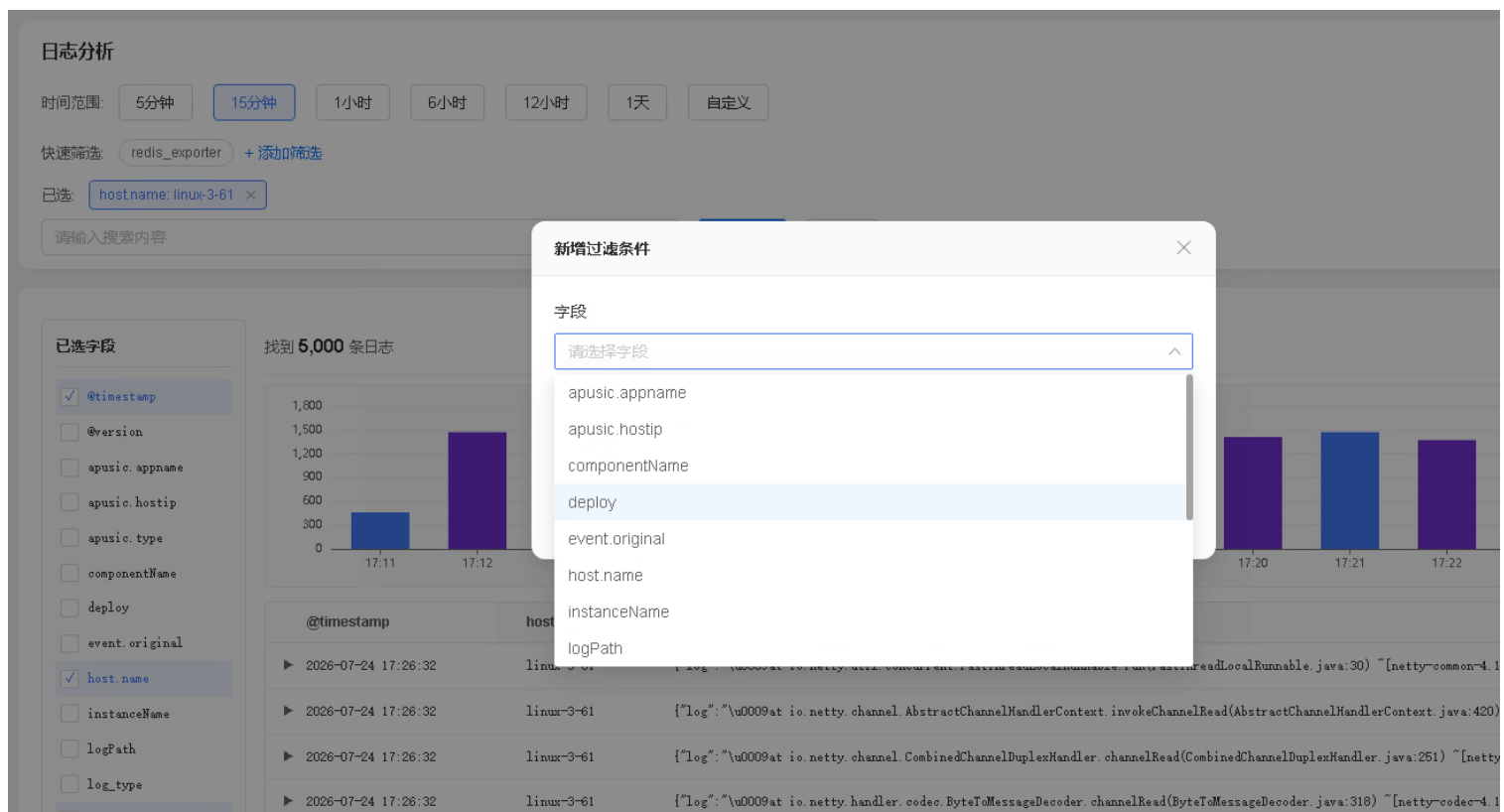


2. 按时间范围筛选

您可以选择预设的快捷时间（最近 5 分钟、15 分钟、1 小时等），也可以自定义起止时间。注意：最多支持检索 7 天内的数据。

3. 字段过滤

除了全文搜索，您还可以按 host.name、@timestamp 等字段进行精确过滤，快速缩小范围。



4. 日志量趋势

系统会展示日志数量的时间分布趋势图，帮助您了解日志产生的峰谷时段。

5. 自定义显示字段

您可以根据需要选择显示或隐藏日志列表中的字段列。通过点击左侧【已选字段】复选框，选择需要显示的字段。

6. 查看日志详情

点击任意一条日志记录可以展开查看完整的日志内容。

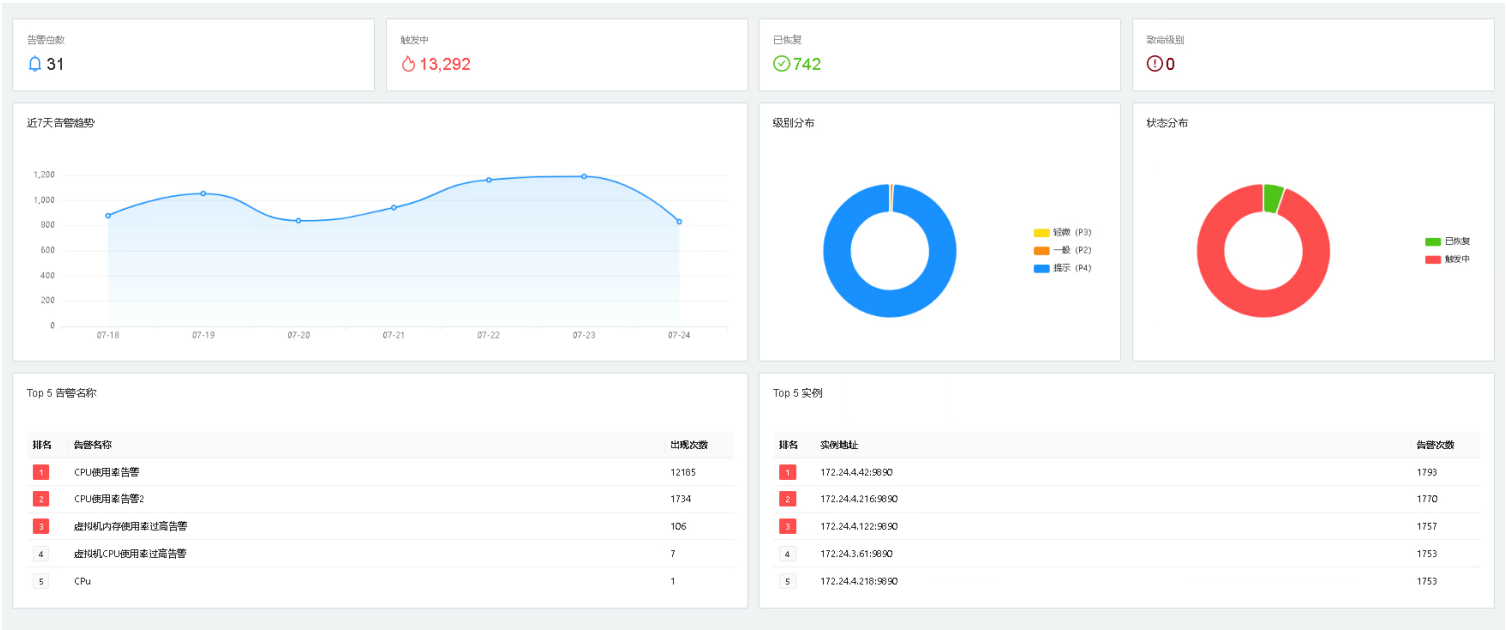
7. 排序

支持按时间正序或倒序排列，方便您从不同角度查看日志。

5.7 告警与事件

5.7.1 告警总览

告警总览是告警信息的“仪表盘”，让您一眼看清当前平台的告警整体态势。



1. 统计卡片

页面顶部展示了告警总数、当前触发的告警数量、已恢复的数量以及致命级别的告警数量——这些是您最需要关注的数字。

2. 告警趋势

趋势图展示了近 7 天的告警数量变化，帮助您判断告警是在增多还是减少。

3. 级别分布

环形图按致命、严重、一般、轻微、提示五个级别展示告警的分布，让您快速评估问题的严重程度。

4. 状态分布

环形图展示触发中和已恢复的告警占比。

5. Top 5 排行

列出触发次数最多的前 5 个告警名称和对应的前 5 个实例，帮您找到最频繁出现的问题。

5.7.2 告警事件

当告警规则被触发时，会产生一条告警事件。您可以在这里查看所有告警事件、处理告警，并追溯其历史记录。

1. 查看告警事件

页面列出了所有告警事件，您可按名称、实例、状态（触发中/已恢复）、级别或时间范围筛选。列表中包含告警名称、级别、触发时间和关联实例等关键信息。

告警事件

搜索告警名称

搜索实例

状态

级别

开始时间

结束时间

搜索

重置

创建告警事件

☐	ID	告警名称	状态	级别	实例	开始时间	操作
☐	2081678191588642818	CPU使用率告警	触发中	提示 (P4)	172.24.4.2:9890	2026-07-15 13:58:31	查看 历史 删除
☐	2081678191508951042	CPU使用率告警	触发中	提示 (P4)	172.24.4.218:9890	2026-07-03 12:03:01	查看 历史 删除
☐	2081678191433453570	CPU使用率告警	触发中	提示 (P4)	172.24.4.216:9890	2026-06-23 10:02:16	查看 历史 删除
☐	2081678191353761793	CPU使用率告警	触发中	提示 (P4)	172.24.4.185:9890	2026-07-20 03:29:46	查看 历史 删除
☐	2081678191282458626	CPU使用率告警	触发中	提示 (P4)	172.24.4.122:9890	2026-07-03 12:00:16	查看 历史 删除
☐	2081678191206961153	CPU使用率告警	触发中	提示 (P4)	172.24.3.92:9890	2026-07-15 14:05:31	查看 历史 删除
☐	2081678191131463602	CPU使用率告警	触发中	提示 (P4)	172.24.3.61:9890	2026-07-14 16:44:01	查看 历史 删除
☐	2081678191047577601	CPU使用率告警	已结束	提示 (P4)	172.24.2.60:9890	2026-07-27 17:37:01	查看 历史 删除
☐	2079864150830452738	虚拟机CPU使用率过高告警	已结束	一般 (P2)	172.24.4.122:9890	2026-07-22 17:27:00	查看 历史 删除
☐	2079864150536851457	CPU使用率告警	已结束	提示 (P4)	172.24.3.63:9890	2026-07-22 17:28:01	查看 历史 删除

共 31 条 < 1 2 3 4 > 10 条/页 跳至 页

2. 查看告警事件详情

点击某个告警事件【查看】按钮，可以查看详细内容。

告警事件详情

告警名称	CPU使用率告警
状态	触发中
级别	提示 (P4)
实例	172.24.4.218:9890
告警内容	实例172.24.4.218:9890的CPU使用率超过了10%，当前值4.25833333904545%
ID	2082273528859639810
指纹	8d43e76c279a28cd
开始时间	2026-07-03 12:03:01
结束时间	0001-01-01 08:05:43
创建时间	2026-07-29 09:14:30
标签	alertname=CPU使用率告警env=prodinstance=172.24.4.218:9890severity=INFOthreshold=1
	alertname: CPU使用率告警 description: 实例172.24.4.218:9890的CPU使用率超过了10%，当前值4.25833333904545% expr: 100 - (avg by(instance) (rate(node_cpu_seconds_total{mode="idle"}[5m])) * 100)

3. 查看告警事件历史

告警事件可能多次触发，通过点击告警事件【历史】按钮，可查看该告警事件的历史记录。

告警事件 / 告警历史记录

历史记录

cbfb23fa6b66806c

开始时间

结束时间

搜索

状态	级别	告警名称	实例	开始时间	推送时间	操作
触发中	提示 (P4)	CPU使用率告警	172.24.4.42:9890	2026-07-15 13:58:31	2026-07-29 09:24:30	查看 删除
触发中	提示 (P4)	CPU使用率告警	172.24.4.42:9890	2026-07-15 13:58:31	2026-07-29 09:14:30	查看 删除
触发中	提示 (P4)	CPU使用率告警	172.24.4.42:9890	2026-07-15 13:58:31	2026-07-29 09:04:30	查看 删除
触发中	提示 (P4)	CPU使用率告警	172.24.4.42:9890	2026-07-15 13:58:31	2026-07-29 08:09:30	查看 删除
触发中	提示 (P4)	CPU使用率告警	172.24.4.42:9890	2026-07-15 13:58:31	2026-07-29 08:04:30	查看 删除
触发中	提示 (P4)	CPU使用率告警	172.24.4.42:9890	2026-07-15 13:58:31	2026-07-29 07:49:30	查看 删除
触发中	提示 (P4)	CPU使用率告警	172.24.4.42:9890	2026-07-15 13:58:31	2026-07-29 07:34:30	查看 删除
触发中	提示 (P4)	CPU使用率告警	172.24.4.42:9890	2026-07-15 13:58:31	2026-07-29 07:24:30	查看 删除
触发中	提示 (P4)	CPU使用率告警	172.24.4.42:9890	2026-07-15 13:58:31	2026-07-29 07:19:30	查看 删除
触发中	提示 (P4)	CPU使用率告警	172.24.4.42:9890	2026-07-15 13:58:31	2026-07-29 07:04:30	查看 删除

共 2161 条

<

1

2

3

4

5

...

217

>

10 条/页

跳至

页

4. 删除告警

对于不再需要关注的告警事件，可以单条或批量删除。

5. 创建告警事件

部分告警规则的触发条件过于苛刻，故提供手工创建告警事件功能，模拟告警和后续触发环节。在列表界面点击【创建告警事件】，进入新增界面。

创建告警事件

* 告警名称

请输入告警名称

* 告警状态

触发中

* 告警级别

轻微 (P3)

实例

请输入实例，例如 localhost:9090

接收者

请输入接收者名称

标签

名称，例如 severity

值，例如 critical

+ 添加标签

概要

请输入告警概要

描述

请输入告警描述

注释

名称，例如 severity

值

取消

创建

- 告警名称：该告警事件的名称。
- 告警状态：告警状态，分为触发中、已恢复。
- 告警级别：告警级别，分为致命、严重、一般、轻微、提示。
- 实例：告警关联的实例。
- 接收者：告警的接收者名称
- 标签：该告警事件所关联的标签，用于后续过程的匹配处理。
- 概要：告警的概要信息。
- 描述：告警的详细描述信息。
- 注释：告警的注释键值对
- 生成地址：告警的生成地址。
- 外部地址：告警在平台的相对地址。

5.7.3 告警收敛

5.7.3.1 告警抑制

在实际运维中，一个核心组件故障往往会引发大量关联告警，形成“告警风暴”。告警抑制可以解决这个问题：当源告警触发时，自动屏蔽与其相关的下游告警。

1. 查看抑制规则

页面列出了所有已配置的抑制规则，包含源告警和目标告警的匹配条件。

告警抑制

搜索规则名称

启用状态

搜索

重置

新增抑制规则

规则名称	源告警匹配	目标告警匹配	需一致标签	启用状态	创建时间	操作
aaaaaaaaaaaaaaaaaaaaaaaaaaaaa...	alertname=probe	severity<critical	-		2026-07-14 14:56:34	修改 删除
磁盘抑制内容告警	alarm.level<CRITICAL	alarm.level=HIGH	demo		2026-05-09 14:45:12	修改 删除

共 2 条 < 1 > 10 条/页

2. 启用和禁用抑制规则

在列表页面，点击【启用状态】栏，可对该抑制规则进行启用或禁用。

3. 新增/编辑抑制规则

在列表页面，点击【新增抑制规则】，进行抑制规则的创建。

新增抑制规则

* 规则名称

例如：磁盘满时抑制内存告警

源告警匹配标签 (sourceMatch)

标签名，例如 alertname

标签值，例如 DiskFull

+ 添加标签

目标告警匹配标签 (targetMatch)

标签名，例如 alertname

标签值，例如 DiskFull

+ 添加标签

需一致标签 (equalLabels)

+ 添加标签

是否启用

☒

...

取消

创建

- **规则名称**：抑制规则的名称，全局唯一。
- **源告警匹配标签**：触发抑制的前置条件。当系统中存在活跃告警完全匹配本组全部标签时，本规则才具备执行抑制的前提；多组标签之间为“且”关系，必须全部匹配。
- **目标告警匹配标签**：待被抑制的告警筛选条件。满足本组全部标签的告警，在同时满足一致性标签条件后，将被抑制告警通知；多组标签之间为“且”关系，必须全部匹配。
- **需一致性标签**：关联源告警与目标告警的绑定条件。源告警和目标告警在此处配置的所有标签，标签值必须完全相同，抑制规则方可生效。用于避免跨实例、跨节点发生错误抑制。若不配置，只要源告警满足条件，所有匹配目标条件的告警均会被全局抑制，存在误抑制风险。
- **是否启用**：该抑制规则是否启用。
- **备注**：该抑制规则的备注描述。

4. 删除抑制规则

不再需要的规则可以随时删除。

5.7.3.2 告警静默

在计划维护、升级窗口期间，您可能不希望收到告警通知。告警静默可以让您在指定的时间窗口内屏蔽符合条件的告警。

1. 查看静默规则

页面列出了所有已配置的静默规则，包含标签匹配条件、开始时间和结束时间。

告警静默								帮助
新增静默规则								
静默规则ID	匹配条件	开始时间	结束时间	创建人	状态	注释	操作	
ce5d120b-8ca5-4121-9710-baf096c90ed8	wordpress-test	2026-07-29 09:49:59	2026-07-31 09:49:26	admin	待生效	测试环境告警静默	查看	删除

2. 新增静默规则

在列表页面，点击【新增静默规则】，进入静默规则配置页面。

新增静默规则

匹配条件 (matchers)

标签名

标签值

☐ 正则

☒ 相等

⊖

+ 添加匹配条件

* 开始时间

* 结束时间

选择开始时间

选择结束时间

* 创建人

例如: admin

* 注释

请输入注释

取消

创建

- **匹配条件**：告警的匹配标签，全部满足时该告警将被静默
- **开始时间**：静默的开始时间

- **结束时间**：静默的结束时间
- **创建人**：该规则的创建人
- **注释**：该规则的注释

3. 删除规则

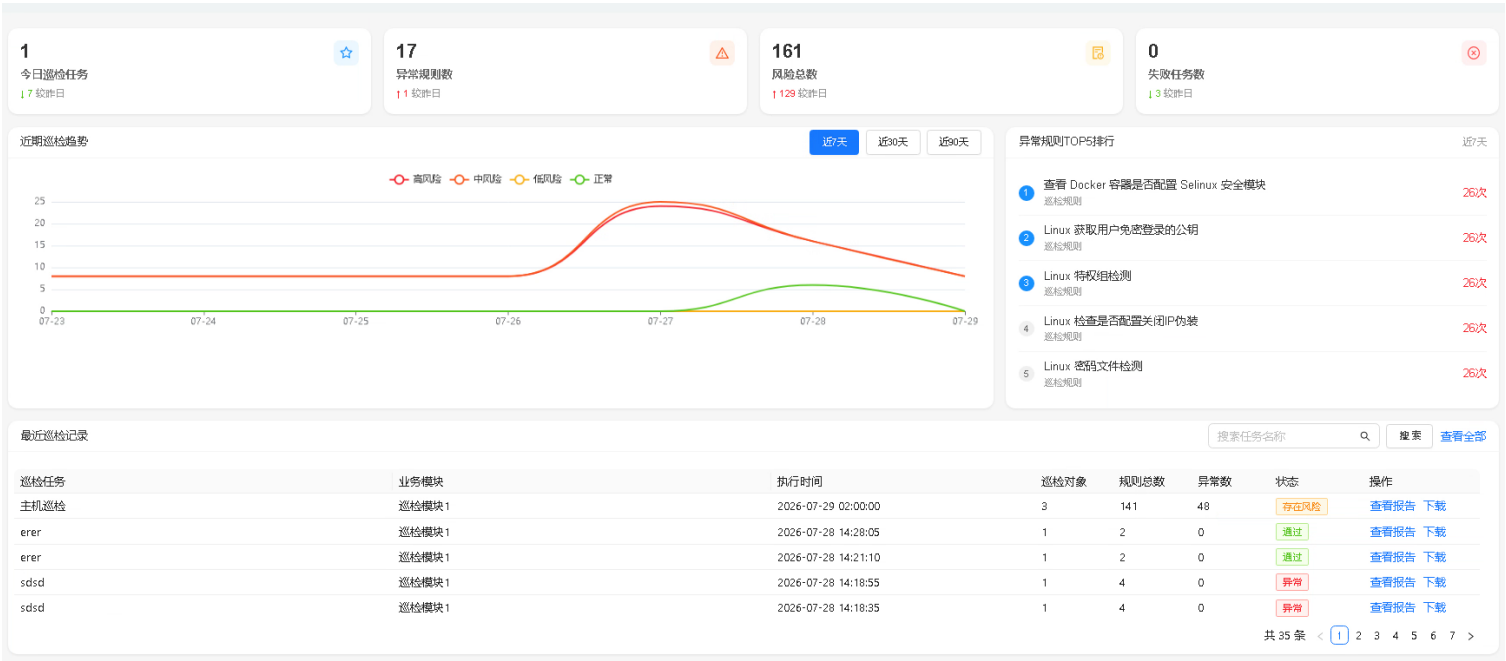
对于不再需要的静默规则，可以直接删除。

5.8 平台运维

5.8.1 平台巡检

5.8.1.1 巡检概览

巡检概览能够帮助运维人员快速了解平台巡检运行情况。



1. 巡检卡片

- **今日巡检任务**：执行巡检任务总数，显示对比昨日变化量
- **异常规则数**：执行结果为异常的巡检规则数量，显示对比昨日变化量
- **风险总数**：全部巡检识别出来的风险条目总和，显示对比昨日变化量
- **失败任务数**：执行失败的巡检任务数量，显示对比昨日变化量

2. 近期巡检趋势

提供近期巡检趋势发现问题的趋势情况，可按风险等级进行过滤

3. 异常规则 TOP5 排行

统计周期默认【近 7 天】，展示触发次数最高的 5 条巡检规则，每条展示规则名称、触发次数（红色数字），点击规则名称可跳转对应巡检规则详情。

4. 最近巡检记录

展示历史巡检任务执行清单，帮助运维人员快速查看近期巡检任务执行情况，点击【查看报告】可快速进入巡检报告页面。点击【下载】，可下载 PDF、Word 版本的巡检报告。

5.8.1.2 巡检任务

巡检任务帮助您对主机和中间件进行自动化健康检查，提前发现潜在问题，保障系统稳定运行。

1. 查看巡检任务

页面展示所有已配置的巡检任务，您可按名称或状态搜索。每个任务显示了巡检对象（主机/中间件）、调度方式（单次/周期）和最近一次执行时间。

巡检任务

执行类型

执行状态

启用状态

请输入任务名称

搜索

重置

创建

5秒刷新

刷新

任务名称	业务模块	巡检对...	检测项数	执行类型	执行状态	上次执行时间	上次执行结果	下次执行时间	启用状态	操作
sdsc	巡检模块1	1	4	单次执行	失败	2026-07-28 14:18:55	Q/4 异常 查看报告	-	☒	编辑 执行 删除
erer	巡检模块1	1	2	周期执行	待执行	2026-07-28 14:28:05	Q/2 通过 查看报告	2026-07-29 14:15:00	☒	编辑 执行 删除
每日巡检	巡检模块1	2	5	周期执行	待执行	-	-	2026-07-15 00:00:00	☐	编辑 执行 删除
季度巡检	巡检模块1	2	2	周期执行	待执行	-	-	2026-10-01 00:00:00	☐	编辑 执行 删除
主机巡检	巡检模块1	3	47	周期执行	待执行	2026-07-29 02:00:00	49/141 存在风险 查看报告	2026-07-30 02:00:00	☒	编辑 执行 删除

共5条 < 1 > 10条/页

2. 启用/停用巡检任务

周期性任务可以随时停用或启用，停用后周期性任务不再运行。重新启用后，按计划时间执行。

3. 立即执行巡检任务

在列表界面中，点击【执行】，可立即触发一次巡检。

4. 快速巡检报告

在列表界面，点击上次执行结果列的【查看报告】，可立即跳转到报告详情，并支持在详情页面下载巡检报告文件。

巡检报告

报告生成时间：2026-07-29 15:04:12

一、巡检概览

任务名称	sdsd	执行状态	失败
巡检结果	通过	风险项/总数	0 / 4
对象数量	1	执行耗时	59 毫秒
开始时间	2026-07-28 14:18:55	结束时间	2026-07-28 14:18:55
错误信息	部分检测项执行失败，请查看结果明细		

二、检测明细

巡检对象	规则	检测项	分类	严重级别	表达式/实际值	结果	问题原因 / 修复建议
172.24.4.195 (linux-4-195)	AMDC 连通性检查	amdc-cli 可用	可用性	高危	表达式：cli_status == "available" 实际值：-	通过	原因：- 建议：-
172.24.4.195 (linux-4-195)	AMDC 连通性检查	AMDC 服务连通	可用性	高危	表达式：ping_response == "PONG" 实际值：-	通过	原因：- 建议：-
172.24.4.195 (linux-4-195)	AMDC 内存使用检查	AMDC 内存信息可获取	可用性	高危	表达式：memory_status == "available" 实际值：-	通过	原因：- 建议：-
172.24.4.195 (linux-4-195)	AMDC 内存使用检查	AMDC 内存使用率正常	性能	高危	表达式：used_memory_ratio < 80 实际值：-	通过	原因：- 建议：-

5. 创建巡检任务

在列表界面，点击【创建】，进入创建页面

巡检任务 / 新增巡检任务

1 基本信息

任务名称

请输入任务名称

任务简介

请输入任务简介, 说明巡检目标和范围

2 执行配置

执行方式

周期执行 单次执行

执行时间

请选择执行时间

3 巡检配置

业务模块

+ 添加

巡检模块1

模块名称

巡检模块1

巡检组名称

巡检组1

0个对象 · 0个项目

删除

巡检对象类型

中间件

+ 添加对象

选择对象类型后, 点击右侧按钮添加具体的巡检对象

检测规则

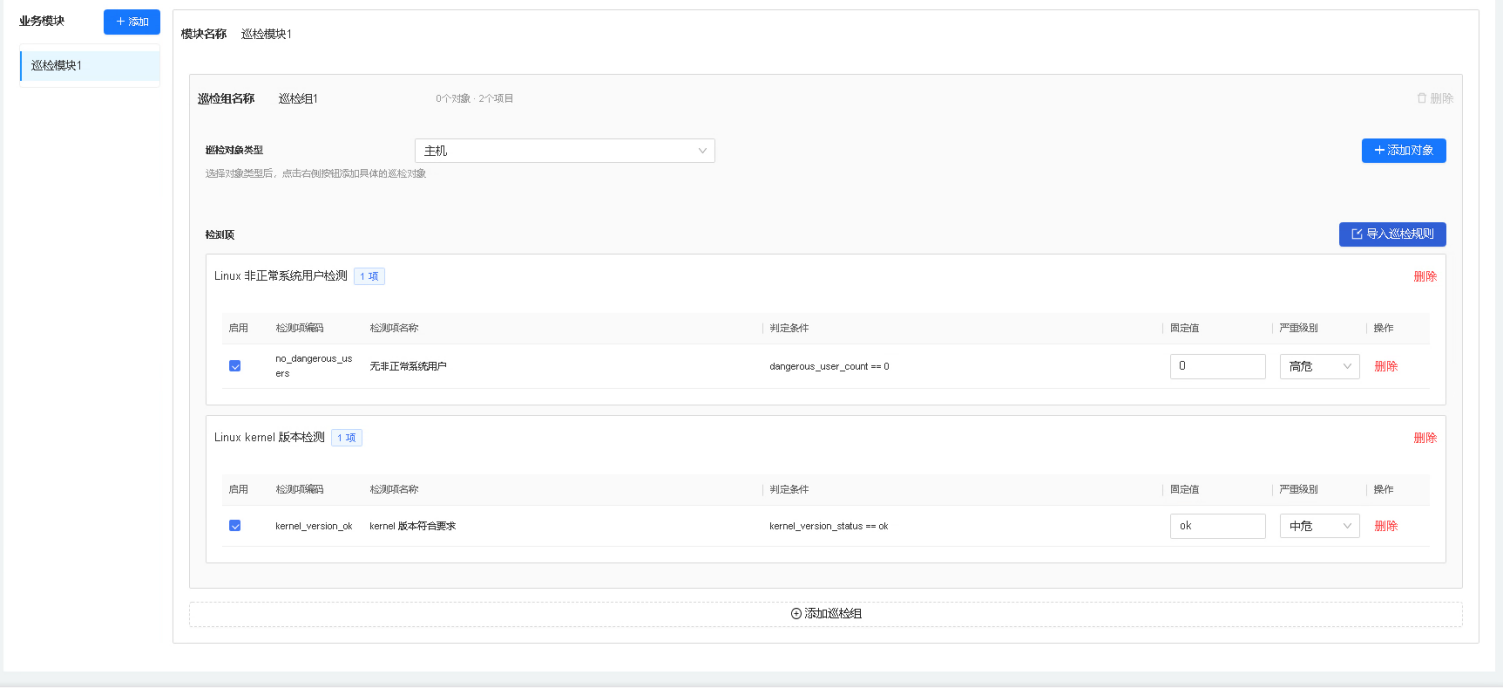
导入巡检规则

暂未导入检测项, 请点击“导入巡检规则”

+ 添加巡检组

- **任务名称**：提供任务的名称，全局唯一
- **任务简介**：任务的简介信息，也作为巡检报告的介绍信息。
- **执行方式**：支持设置按周期执行，或者单次指定时间执行
- **业务模块**：业务分组，可按照业务划分，将一类巡检任务归为一组，方便管理。支持多个分组。
 - **模块名称**：业务分组的名称，可自定义修改
 - **巡检组**：一个巡检组包含一个或多个巡检对象和多个巡检规则，所有的巡检对象都会执行该巡检组下的所有规则，便于统一配置。巡检组支持创建多个。
 - **巡检对象类型**：可选择巡检主机或者中间件
 - **添加对象**：可通过选择方式，加入选择的目标对象
 - **导入巡检规则**：点击该按钮，可选择平台内置的规则，并加入到巡检组中，作为检测项目。用户可以调整固定值（巡检匹配值）和严重级别。

102

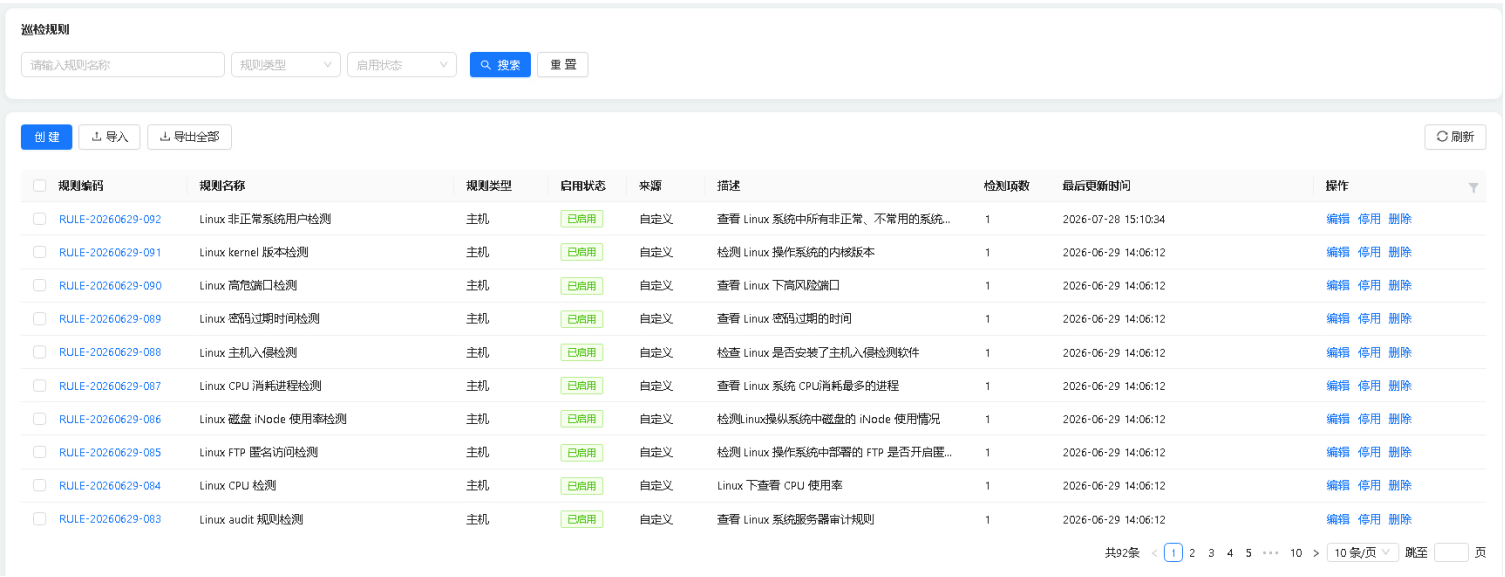


5.8.1.3 巡检规则

巡检规则是巡检任务中的检查项定义。每个规则包含检查脚本、预期结果和严重级别。您可以使用内置规则，也可以根据需求创建自定义规则。

1. 浏览巡检规则

页面展示了所有巡检规则，可按名称或分类搜索。每条规则包含脚本定义、适用的检查对象和严重级别。



2. 启用停用巡检规则

进入列表界面，点击【启用】或【停用】，可启用或停用规则。停用后在巡检任务中无法被选到。已被加入任务的规则不受影响。

3. 导入/导出巡检规则

支持以 JSON 格式导入或导出规则，方便在不同环境间复用。

4. 创建巡检规则

巡检规则 / 创建规则

* 规则名称

* 规则类型

请选择规则类型

规则描述

* 规则脚本

1

输出字段定义

+ 添加输出字段

* 检测项定义

检测项编码	检测项名称	分类	严重级别	输出字段	操作符	期望值	启用	操作
暂无数据								

+ 添加检测项

变量设置

+ 添加参数

- **规则名称**：规则的名称，全局唯一
- **规则类型**：规则类型，指定该规则适用于主机还是中间件
- **规则脚本**：通过执行该脚本，收集对应主机上的中间件等信息，并将结果放到对应变量中，用户可以在输出字段定义中，添加同名字段定义，获取该字段的值。
- **输出字段定义**：定义规则脚本的输出字段，并指定字段类型。
 - **字段编码**：外部使用该字段的字段名称，避免值传输字段名称绑定过密
 - **字段名称**：对该字段定义的名称描述
 - **envKey**：对应规则脚本中的输出环境变量名称
 - **字段类型**：该字段的类型。
- **检测项**：通过添加检测项，实现对获取的数据进行检测。
 - **检测项编码**：检测项的编码，全局唯一
 - **检测项名称**：用户可理解的检测项名称，能够表达这个检测项的作用
 - **分类**：检测项的分类，用于对检测项进行分类管理，包括配置、安全、性能、可用性等

- **严重级别**：严重级别，用于定义该检测项的严重程度。
- **输出字段**：选择输出字段，用于后续匹配
- **操作符**：选择匹配操作的操作符
- **期望值**：输入期望值，用于匹配
- **表达式展示**：最终匹配的表达式，便于核验
- **问题原因**：提供该问题的可能原因，在出现该问题时，可以提示用户
- **修复建议**：提供该问题的修复建议，在出现该问题时，可以提示用户
- **启用**：是否启用这条检测项目
- **变量设置**：支持外部设置变量，用于规则脚本中。
 - **key**：该变量标识
 - **名称**：变量名称，说明该变量的用途，例如密码
 - **必填**：是否必填
 - **描述**：该变量的描述说明
- **高级配置**：
 - **超时时间**：该规则的执行超时时间，避免执行时间过长
 - **执行路径**：该规则的执行路径
 - **执行用户**：该规则的执行用户

5. 删除巡检

自定义规则可以删除或停用。

5.8.2 批量操作

5.8.2.1 文件上传

当您需要向多台主机分发文件（如安装包、脚本、配置文件）时，可以使用文件上传功能，批量派发到目标主机。

1. 查看上传任务

页面展示所有上传任务，您可按名称或状态搜索。

文件上传

开始日期

→

结束日期

请选择上传状态

请选择

请输入描述或路径搜索

搜索

重置

上传

上传描述	远程路径	上传状态	文件数量	主机数量	上传时间	更新时间	操作
上传文件: 2026-07-03 14:32:43	/root/.apusicdet/workspace/e5db1b26-b1b3-4fa1-ac4b-542da1fc599Q/webapps	已完成	1	1	2026-07-03 14:32:43	2026-07-03 14:32:43	详情 删除
上传文件: 2026-05-26 15:54:54	/opt	已完成	1	1	2026-05-26 15:54:54	2026-05-26 15:54:55	详情 删除
上传文件: 2026-02-11 13:52:14	/root	已完成	1	1	2026-02-11 13:52:14	2026-02-11 13:52:15	详情 删除
上传文件: 2025-12-30 17:09:00	/a	已失败	1	1	2025-12-30 17:09:00	2025-12-30 17:09:02	详情 删除
上传测试	/home	已完成	1	1	2025-12-30 16:46:14	2025-12-30 16:46:14	详情 删除
上传测试	/	已失败	1	2	2025-12-30 16:45:00	2025-12-30 16:45:01	详情 删除
国土局描述	/	已取消	1	3	2025-11-20 17:17:34	2025-11-20 17:17:35	详情 删除
上传文件: 2025-09-29 11:21:39	/home	已完成	1	1	2025-09-29 11:21:39	2025-09-29 11:21:39	详情 删除
上传文件: 2025-09-29 09:58:57	/opt/tongweb/TongWeb7.0.4.7_Enterprise_Linux/bin	已完成	1	1	2025-09-29 09:58:57	2025-09-29 09:58:57	详情 删除
dema1	/root	已完成	1	1	2025-09-18 09:44:12	2025-09-18 09:44:12	详情 删除

共71条

1

2

3

4

5

...

8

10条/页

跳至

页

2. 创建上传任务

点击【创建】，通过四步向导完成：

- 创建任务：填写任务名称和目标主机
- 上传文件：从本地上传文件（单文件不超过 2GB，总量不超过 4GB）
- 分发文件：系统自动将文件派发到目标主机指定路径
- 完成：查看分发结果

文件上传 / 批量上传

1 创建任务

创建上传任务

2 上传文件

将文件上传到临时分区

3 分发文件

将文件分发到目标服务器

4 上传完成

释放资源

批量上传

重置

开始上传

上传描述

* 上传路径

* 上传主机

选择主机

文件列表

清空

选择文件

请先点击上方按钮选择文件

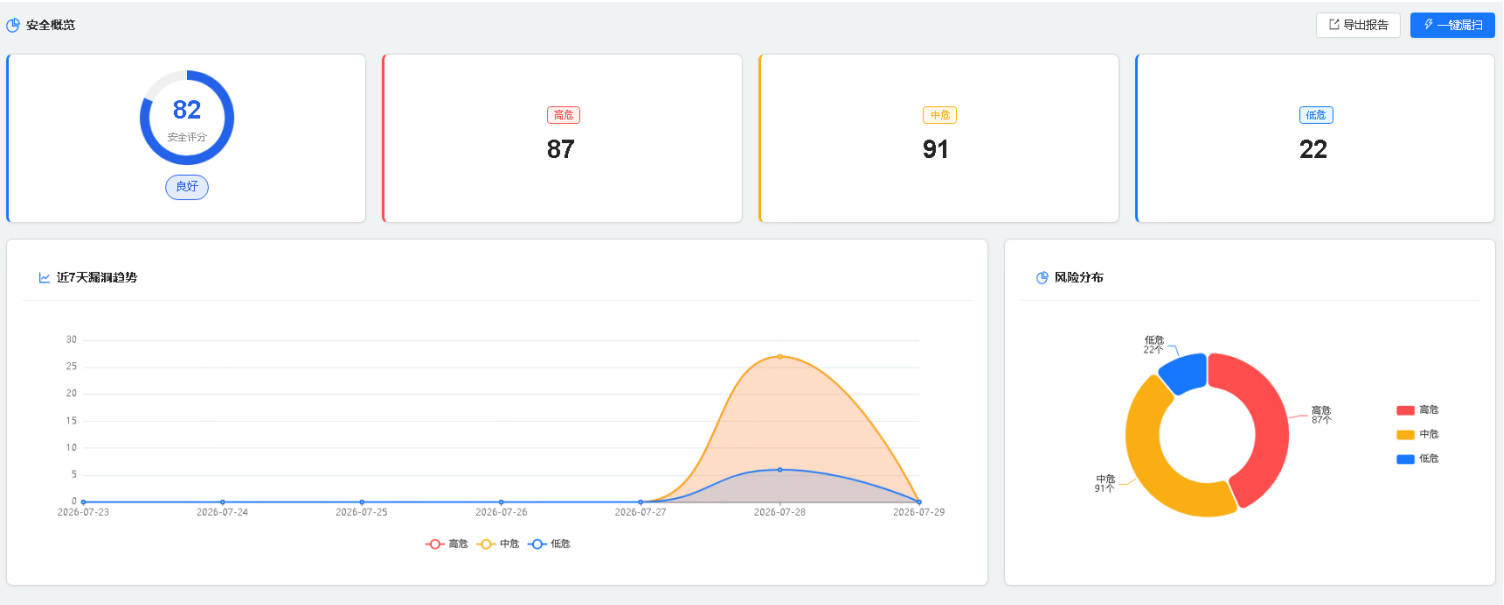
3. 管理任务

尚未执行的任务可以编辑修改；不再需要的任务可以删除。

5.9 安全中心

5.9.1 安全概览

安全概览是平台安全态势的全局视图，让您快速了解整体安全状况。



1. 安全评分

页面顶部以环形图展示平台的安全评分（0-100 分），等级分为优秀、良好、一般、较差、危险五个档次，帮助您直观判断当前安全水平。

2. 漏洞统计与趋势

页面展示了高危、中危、低危漏洞的数量统计，以及近 7 天的漏洞发现趋势折线图，让您了解安全状况是在改善还是恶化。

3. 风险分布与中间件状态

通过饼图展示漏洞的分布情况，同时列出各中间件的实例数、漏洞数和安全率，帮您定位风险最高的中间件。

4. 近期高危告警

近期高危告警展示最近 7 天有高危告警的资产，并显示告警数量。

5. 一键漏扫

点击【一键漏扫】可以快速发起一次全平台漏洞扫描，无需手动创建扫描任务。

6. 导出报告

点击【导出报告】可将安全概览数据导出保存，用于汇报或归档。

5.9.2 扫描任务

漏洞扫描任务驱动着安全检测的执行。您可以创建扫描任务，指定扫描类型、目标和调度方式，平台会自动执行并生成扫描结果。

1. 管理扫描任务

页面展示了所有扫描任务，您可按名称、扫描类型或状态搜索。列表中包含扫描类型（版本/基线/全量）、调度方式（立即/单次/周期）和执行状态等信息。

扫描任务列表

任务状态

扫描类型

触发方式

时间范围

按任务名称搜索

搜索

重置

+ 新建扫描任务

5秒刷新

刷新

任务名称	扫描类型	调度类型	扫描目标	状态	进度	下次执行	漏洞结果	基线结果	扫描时间	操作
nginxtest	全量扫描	周期执行	全部中间件（16实例）	待执行	-	2026-07-29 18:00:00	73 个漏洞	13 项基线未通过	2026-07-29 17:36:15	立即执行 停用 删除
1233	版本漏洞扫描	周期执行	全部中间件（16实例）	待执行	-	2026-07-29 18:00:00	73 个漏洞	-	2026-07-29 17:35:39	立即执行 停用 删除
nginx-test-time	全量扫描	定时执行	nginx、aaa、nginx-tes...	执行成功	100%	-	未发现漏洞	4 项基线未通过	2026-07-28 16:55:01	重新执行 删除
test-zk-job	版本漏洞扫描	立即执行	zookeeper（2实例）	执行成功	100%	-	19 个漏洞	-	2026-07-28 10:48:18	重新执行 删除
zk222	版本漏洞扫描	立即执行	aasv10、alb、zooke...	执行成功	100%	-	1 个漏洞	-	2026-07-28 09:56:15	重新执行 删除
zk_amdc_redis漏洞扫描任务	版本漏洞扫描	立即执行	amdc、redis、zooke...	执行成功	100%	-	未发现漏洞	-	2026-07-28 09:50:48	重新执行 删除
aasv10扫描任务	版本漏洞扫描	立即执行	aasv10（1实例）	执行成功	100%	-	1 个漏洞	-	2026-07-28 09:50:17	重新执行 删除
xxx	全量扫描	立即执行	全部中间件（17实例）	执行成功	100%	-	未发现漏洞	15 项基线未通过	2026-07-27 14:25:41	重新执行 删除
漏洞扫描	版本漏洞扫描	立即执行	全部中间件（14实例）	执行成功	100%	-	54 个漏洞	-	2026-07-22 14:50:06	重新执行 删除

2. 创建扫描任务

点击【创建】，选择扫描类型（版本扫描/基线扫描/全量扫描），设置调度方式（立即执行/单次执行/周期性执行），并指定扫描目标（全部资产或自定义选择中间件类型和实例）。

创建扫描任务



1 基本信息

* 任务名称 *

* 扫描类型 *

请输入任务名称

请选择扫描类型

2 扫描目标

全部中间件

按类型选择

- ☒ AMDC
 ☐ AASV10
 ☐ AUC
 ☐ aliweb1
 ☐ orion_visor
 ☐ admin
- ☐ ADMQ2_RabbitMQ
 ☐ hummerrisk
 ☐ ADCC
 ☐ ADMQ2_RocketMQ
- ☐ ADMQ2_Kafka
 ☐ Redis
 ☐ Golden_aas
 ☐ weblogic
 ☐ ALB
 ☐ Zookeeper
- ☐ test
 ☐ AASV9
 ☐ powerjob
 ☐ demo
 ☐ Elasticsearch
 ☐ ADMQ_Kafka
- ☐ ADMQ
 ☐ Nginx
 ☐ ASE
 ☐ Tomcat
 ☐ testSignV
 ☐ AAMSV10SP11
- ☐ nginx-test
 ☐ test111

3 调度设置

立即执行

定时执行

周期执行

* 执行时间

请选择日期



取消

确定

- 任务名称：扫描任务名称
- 扫描类型：可指定版本漏洞扫描、配置基线扫描，或者同时进行全部扫描
- 扫描目标：可指定需要进行扫描的目标
 - 全部中间件：对平台内所有的中间件进行安全扫描
 - 按类型选择：对指定类型的中间件进行安全扫描
- 调度设置
 - 立即执行：立即执行一次扫描任务
 - 定时执行：指定时间，到期时执行扫描任务
 - 周期执行：指定时间间隔，按照指定时间间隔重复执行扫描任务

3. 执行与重新执行

创建完成后可立即【执行】；对于已完成的扫描任务，如果有新的需求可以【重新执行】。

4. 停用/启用与删除

周期性任务可以随时停用或启用；不再需要的任务可以删除。

5. 查看任务详情

在列表界面，点击任务名称，可进入任务详情，默认展示该任务最后一次扫描结果。

🏠 / 扫描任务 / 详情

任务信息

🔄 重新扫描

🔄 刷新

任务名称

nginxtest

任务ID

2082282169130074113

扫描类型

全部扫描

当前状态

待执行

调度类型

周期执行

触发用户

huangxiaolong

开始时间

2026-07-29 14:00:00

结束时间

2026-07-29 14:00:27

扫描目标

全部中间件（16实例）

扫描结果汇总

🕒

27秒

扫描时长

✅

16/16

完成实例

🚨

73

发现问题

🛡️

2/15

基线通过

扫描结果详情

🔍 漏洞结果 (73)

📋 基线结果 (13)

漏洞编号	漏洞名称	严重等级	影响实例	中间件	发现时间
CVE-2025-11226	ch.qos.logback/logback-core: Conditional arbitrary code execution in logback-core	中危	test-zk-zookeeper-zk-0	Zookeeper/3.9.4/单机	2026-07-29 14:00:14
CVE-2026-1225	ch.qos.logback/logback-core: Malicious logback.xml configuration file allows insta...	低危	test-zk-zookeeper-zk-0	Zookeeper/3.9.4/单机	2026-07-29 14:00:14

扫描结果详情

🔍 漏洞结果 (73)

📋 基线结果 (13)

规则编码	规则名称	分类	中间件	严重等级	基线类型	未通过实例	发现时间	
AMDC-001	AMDC 禁止监听所有网卡	安全配置	amdc	高危	强制基线	amdc-master-master-0	2026-07-29 14:00:01	
规则描述 检查 AMDC 是否仅监听内网或本地地址 当前配置 0.0.0.0 风险说明 若绑定 0.0.0.0 且未设置密码或防火墙限制，AMDC 可直接暴露在外网。 环境 - 期望配置 "0.0.0.0" 修复建议 步骤 1: 修改 bind 配置 bind 127.0.0.1 步骤 2: 如需内网访问，修改为内网IP bind 127.0.0.1 192.168.1.100 步骤 3: 重启 AMDC								
▶	AMDC-001	AMDC 禁止监听所有网卡	安全配置	amdc	高危	强制基线	amdc-slaver-slave-0	2026-07-29 14:00:03
▶	AMDC-001	AMDC 禁止监听所有网卡	安全配置	amdc	高危	强制基线	amdc-slaver-slave-1	2026-07-29 14:00:04
▶	NGINX-002	Nginx 禁用危险 HTTP 方法	访问控制	nginx	高危	强制基线	nginx42-server-nginx-0	2026-07-29 14:00:04
▶	NGINX-003	Nginx HTTPS 强制跳转	网络安全	nginx	高危	强制基线	nginx42-server-nginx-0	2026-07-29 14:00:04
▶	REDIS-003	Redis 禁用高危命令	访问控制	redis	高危	强制基线	218_redis-redis-redis-0	2026-07-29 14:00:19
▶	REDIS-004	Redis 启用审计日志	安全配置	redis	中危	强制基线	218_redis-redis-redis-0	2026-07-29 14:00:19

共 13 条 < 1 > 20 条/页

5.9.2.1 扫描记录

每次扫描执行后都会生成一条记录，您可以在这里查看详细的扫描结果。

1. 查看扫描记录

页面展示每次扫描的执行记录，包含任务名称、执行时间、状态和耗时。

扫描记录列表

记录状态

扫描类型

扫描时间

执行结果

按任务ID或任务名称...

Q

刷新

任务名称	扫描类型	扫描目标	扫描时间	状态	漏洞结果	基线结果	耗时	操作
1233	版本漏洞扫描	全部中间件（16实例）	2026-07-29 17:35:10	已完成	73个漏洞	-	29秒	删除
nginxtest	全量扫描	全部中间件（16实例）	2026-07-29 14:00:00	已完成	73个漏洞	13项基线未通过	27秒	删除
nginxtest	全量扫描	全部中间件（16实例）	2026-07-29 13:00:00	已完成	73个漏洞	13项基线未通过	27秒	删除
nginxtest	全量扫描	全部中间件（16实例）	2026-07-29 12:00:00	已完成	73个漏洞	13项基线未通过	28秒	删除
nginxtest	全量扫描	全部中间件（16实例）	2026-07-29 11:00:00	已完成	73个漏洞	13项基线未通过	28秒	删除
nginxtest	全量扫描	全部中间件（16实例）	2026-07-29 10:53:20	已完成	73个漏洞	13项基线未通过	27秒	删除
nginxtest	全量扫描	全部中间件（16实例）	2026-07-29 10:44:20	已完成	73个漏洞	13项基线未通过	27秒	删除
nginxtest	全量扫描	全部中间件（16实例）	2026-07-29 10:00:30	已完成	73个漏洞	13项基线未通过	27秒	删除
1233	版本漏洞扫描	全部中间件（16实例）	2026-07-29 10:00:00	已完成	73个漏洞	-	27秒	删除

2. 查看扫描详情

点击某条记录可以查看具体的扫描结果，包括发现的漏洞信息和基线检查结果。

3. 删除记录

不需要的记录可以直接删除。

5.9.3 漏洞管理

漏洞管理聚合了所有扫描任务发现的漏洞，为您提供统一的漏洞追踪和处置平台。

1. 查看漏洞列表

您可按关键词、危险等级（高危/中危/低危）、处理状态（新发现/处理中/已忽略/已修复）、中间件类型或时间范围筛选漏洞。列表中的漏洞名称、危险等级、影响资产和处理状态让您快速了解需要优先处理的问题。

漏洞管理

危险等级

处理状态

中间件类型

时间范围

搜索漏洞、实例...

搜索

重置

刷新

漏洞编号	漏洞标题	危险等级	CVSS评分	受影响实例	实例说明	当前版本	修复版本	状态	发现时间	操作
CVE-2026-9828	Deserialization of untrusted data v... Deserialization of untrusted data vuln...	低危		aasv10-aasv10-A...	AASV10/V10/单机 172.24.4.218	1.3.15	1.5.33	新发现	2026-07-28 10:49:01	修复指引 忽略
CVE-2026-1225	ch.qos.logback/logback-core: Mali... ACE vulnerability in configuration file ...	低危	5.0	aasv10-aasv10-A...	AASV10/V10/单机 172.24.4.218	1.3.15	1.5.25	新发现	2026-07-28 10:49:01	修复指引 忽略
CVE-2025-11226	ch.qos.logback/logback-core: Con... ACE vulnerability in conditional confi...	中危	6.4	aasv10-aasv10-A...	AASV10/V10/单机 172.24.4.218	1.3.15	1.5.19, 1.3.16	新发现	2026-07-28 10:49:01	修复指引 忽略
GHSA-47qp-hqvz-...	Jline3 Telnet server: Unauthenticat... ### Summary The JLine3 Telnet server...	高危	7.5	fan-test-sts-AAMS...	AAMSV10SP11/v1... 172.24.4.42	3.21.0	4.2.1	新发现	2026-07-28 10:48:44	修复指引 忽略
GHSA-2r2c-ox56-8...	Jline3 Telnet server: Unauthenticat... ### Summary The JLine3 Telnet server...	高危	7.5	fan-test-sts-AAMS...	AAMSV10SP11/v1... 172.24.4.42	3.21.0	4.2.1	新发现	2026-07-28 10:48:44	修复指引 忽略
CVE-2026-42578	netty: io.netty/netty-handler-proxy:... Netty is an asynchronous, event-drive...	低危	7.5	fan-test-sts-AAMS...	AAMSV10SP11/v1... 172.24.4.42	4.1.130.Final	4.1.133.Final , 4.2.13.Final	新发现	2026-07-28 10:48:44	修复指引 忽略

2. 漏洞详情与修复指引

点击漏洞名称可以查看详细信息和受影响的资产列表。页面上还会提供修复建议和操作指引，帮助您快速解决问题。

漏洞详情



Deserialization of untrusted data vulnerability in QOS.CH Srl logback logback-core (HardenedObjectInputStream (logback-core) modules) allows Object Injection albeit heavily restricted. More precisely, an attacker able to influence serialized data sent to SimpleSocketServer or SimpleSSLSocketServer can instantiate objects from classes in the java.lang and java.util packages that are not explicitly blocked. Although deserialization is heavily restricted by HardenedObjectInputStream and no practical way to achieve remote code execution or significant privilege escalation has been identified, this issue constitutes a bypass of the intended security restrictions. This issue affects logback: through 1.5.32 inclusive.

基本信息

漏洞编号	CVE-2026-9828
数据来源	NVD
CWE分类	-
发布时间	-
更新时间	2026-07-28 13:00:20

影响分析

受影响产品	AASV10/V10/单机
已影响实例	aasv10-aasv10-AASV10-0
推荐修复版本	1.5.33
补丁地址	-
漏洞地址	https://avd.aquasec.com/nvd/cve-2026-9828

修复建议

暂无修复建议

关闭

忽略

修复指引

受影响实例

aasv10-aasv10-AASV10-0

aasv10

漏洞编号

CVE-2026-9828

漏洞地址

<https://avd.aquasec.com/nvd/cve-2026-9828>

当前版本

1.3.15

修复版本

1.5.33

参考链接

[官方安全公告](#)

关闭

标记为修复中

3. 跟踪处置状态

扫描新发现的漏洞默认处于“新发现”状态；正在修复时可将其标记为“处理中”；修复完成后标记为“已修复”；如果确认为误报，可以标记为“已忽略”，从而全程追踪每个漏洞的处置进展。

5.9.4 基线管理

5.9.4.1 待处理项

基线检查会发现主机、中间件和容器中不符合安全配置规范的问题。待处理项集中展示了这些不合规项，方便您逐一处理。

1. 查看待处理项

您可按分类（身份认证/访问控制/网络安全等）、中间件类型、严重等级或处理状态筛选。列表中的问题名称、分类、严重等级和影响资产一目了然。

待处理

状态

分类

中间件

严重等级

规则编码/规则名称

搜索

重置

刷新

清理已修复

规则编码	规则名称	分类	基线类型	中间件	严重等级	实例名称	状态	发现时间	操作
REDIS-001	Redis 禁止空密码访问	身份认证	强制基线	redis	严重	218_redis-redis-redis_...	待处理	2026-07-30 15:00:05	修复指引 忽略
REDIS-004	Redis 启用审计日志	安全配置	强制基线	redis	中危	218_redis-redis-redis_...	待处理	2026-07-30 15:00:05	修复指引 忽略
REDIS-003	Redis 禁用高危命令	访问控制	强制基线	redis	高危	218_redis-redis-redis_...	待处理	2026-07-30 15:00:05	修复指引 忽略
REDIS-002	Redis 禁止监听所有网卡	网络安全	强制基线	redis	高危	218_redis-redis-redis-0	待处理	2026-07-30 15:00:06	修复指引 忽略
REDIS-001	Redis 禁止空密码访问	身份认证	强制基线	redis	严重	218_redis-redis-redis_...	已忽略	2026-07-29 14:37:11	删除
REDIS-004	Redis 启用审计日志	安全配置	强制基线	redis	中危	218_redis-redis-redis_...	已修复	2026-07-29 14:01:22	删除
REDIS-003	Redis 禁用高危命令	访问控制	强制基线	redis	高危	218_redis-redis-redis_...	已忽略	2026-07-29 14:35:01	删除

2. 查看详情与修复

点击问题名称可以查看详细的风险说明和修复建议，按照指引操作即可解决问题。

基线检查详情



REDIS-002

强制基线

高危

Redis 禁止监听所有网卡

检查 Redis 是否仅监听内网或本地地址

受影响实例

实例名称	运行环境
218_redis-redis-redis-0	-
中间件类型	发现时间
redis	2026-07-30 15:00:06

配置检查结果

输出字段	BIND_ADDRESSES
检查规则	实际值不应为 0.0.0.0
实际值	0.0.0.0
结果	不合规

风险说明

Redis 监听地址包含 0.0.0.0

关闭

忽略

查看修复指引

修复指引

218_redis-redis-redis-0

输出字段

BIND_ADDRESSES

检查规则

实际值不应为 0.0.0.0

实际值

0.0.0.0

结果

不合规

修复步骤

步骤 1

修改 bind 配置

`bind 127.0.0.1`

步骤 2

如需内网访问，修改为内网IP

`bind 127.0.0.1 192.168.1.100`

步骤 3

重启 Redis

`systemctl restart redis`

关闭

标记为修复中

重新检查

3. 跟踪处理状态

将问题标记为“修复中”表示正在处理；修复完成后可以发起“重新检查”来验证问题是否已解决；确认为无需处理的问题可以“忽略”。

5.9.4.2 基线规则库

基线规则库定义了基线检查的具体检查项。您可以使用系统内置的规则，也可以根据自身的安全要求创建自定义规则。

1. 查看规则

页面展示所有基线规则，包含规则编码、名称、分类、适用中间件和严重等级。

基线规则列表

分类

中间件

严重等级

基线类型

状态

规则编码/规则名称

搜索

重置

+ 新增规则

导入

导出全部

刷新

批量删除

☐	规则编码	规则名称	规则描述	分类	适用中间件	版本	部署模式	严重等级	基线类型	状态	操作
☐	REDIS-003	Redis 禁用高危命令	检查是否禁用或重命名了 FLUSHALL、CO...	访问控制	redis	-	-	高危	强制基线	已启用	编辑 停用 删除
☐	NGINX-002	Nginx 禁用危险 HTTP 方法	检查是否限制了 PUT、DELETE 等方法	访问控制	nginx	-	-	高危	强制基线	已启用	编辑 停用 删除
☐	ES-001	Elasticsearch 启用安全认证	检查是否启用了 X-Pack 安全认证	身份认证	elasticsearch	-	-	严重	强制基线	已启用	编辑 停用 删除
☐	ES-002	Elasticsearch 限制跨域访问	检查是否允许任意来源跨域	网络安全	elasticsearch	-	-	高危	强制基线	已启用	编辑 停用 删除
☐	PG-002	PostgreSQL 启用连接日志	检查是否启用了连接和断开日志	安全配置	postgresql	-	-	中危	强制基线	已启用	编辑 停用 删除
☐	TOMCAT-002	Tomcat 配置自定义错误页面	检查是否配置了自定义错误页面	安全配置	tomcat	-	-	中危	强制基线	已启用	编辑 停用 删除
☐	NGINX-003	Nginx HTTPS 强制跳转	检查是否配置了 HTTP 强制跳转 HTTPS	网络安全	nginx	-	-	高危	强制基线	已启用	编辑 停用 删除

2. 创建/编辑规则

点击【创建】或【编辑】，配置规则的编码、名称、分类、适用中间件、严重等级、检查脚本、期望配置和修复建议等信息。

基线规则 / 创建规则

基本信息

* 规则编码

如：REDIS-001

* 规则名称

请输入规则名称

规则描述

请输入规则描述

* 适用中间件

请选择中间件

版本

请选择版本

部署模式

请选择部署模式

* 分类

请选择分类

* 严重等级

请选择严重等级

* 基线类型

强制基线

状态

☒

执行超时（秒）

请输入执行超时

检查脚本

* 规则脚本

1

请输入 Shell 检查脚本，输出 key=value 格式

- 基本信息：
 - 规则编码：规则编码，全局唯一
 - 规则名称：该规则的名称
 - 规则描述：该规则的作用描述
 - 适用中间件：选择软件管理中的中间件类型、版本以及部署模式
 - 分类：规则的分类，如身份认证、访问控制、安全配置、安全功能等
 - 严重等级：该规则对应问题的严重程度等级

- **基线类型**：基线类型，可选择强制基线或建议基线
- **状态**：启用状态的规则才会在任务调度时生效
- **执行超时**：该规则脚本执行的最大时间
- **检查脚本**：
 - **规则脚本**：检查脚本，使用 Shell 语言编写，执行后，将检测值写入到环境变量中，可通过输出字段定义即可获得对应的检测值
- **输出字段定义**：输出字段会从 envKey 相关的环境变量中获取对应的检测值
 - **字段编码**：字段的编码，全局唯一
 - **字段名称**：字段的名称描述
 - **envKey**：环境变量名称
 - **字段类型**：获取的值的类型
- **检测项定义**：支持定义多个检测项，每个检测项对应一个检查项目
 - **检测项编码**：全局唯一，避免检测项冲突
 - **检测项名称**：说明该检测项的作用
 - **分类**：具体检测项目的分类，如身份认证、访问控制、安全配置、安全功能等
 - **严重级别**：具体检测项目对应问题的严重程度等级
 - **输出字段**：选择从哪个输出字段取值进行比较
 - **操作符**：选择使用什么操作符进行比较，例如大于、小于等
 - **期望值**：期望的正常值或阈值
 - **表达式展示**：该检测项的表达式展示，会显示在检查项目信息中
 - **启用**：该检查项是否启用，停用后将不再使用该检查项进行检查
- **变量设置**：该规则脚本运行时的变量值设置，可通过设置变量，实现对脚本行为的控制。定义后该值将被注入到运行脚本的环境变量中
 - **Key**：环境变量名称
 - **名称**：变量说明名称
 - **默认值**：默认注入的值
 - **必填**：该变量是否必须
 - **描述**：该变量的作用
- **补充说明**：
 - **风险说明**：该规则对应的风险说明，填写后将在页面中展示给用户
 - **问题原因**：导致该检查项不通过的原因描述，会显示在检查项目信息中
 - **修复建议**：该检查项的修复建议，会显示在检查项目信息中

3. 启用/停用规则

在列表界面，点击【启用】或【停用】按钮时，规则状态会改变。规则只有在启用状态，在进行任务调度时才会生效。

4. 删除

若该检查规则不再需要，您可以删除该规则。

5. 导入/导出

支持批量导入或导出规则，方便在不同环境间复用。在列表页面点击【导入】或【导出】按钮进行相关操作

5.9.5 安全配置

5.9.5.1 漏洞库

漏洞库提供标准漏洞库管理以及自定义漏洞添加

1. 查看漏洞库与自定义漏洞

漏洞库信息提供了当前漏洞库版本、漏洞库更新时间以及漏洞库数据来源。自定义漏洞为自定义漏洞库，用户可自行添加漏洞信息，自定义漏洞参与漏洞扫描，处理过程与官方漏洞库一致。

漏洞库

漏洞库信息

漏洞库版本

20260727

更新时间

2026-07-27 13:42:00

数据来源

Trivy 离线漏洞库

上传漏洞库

下载漏洞库

制作漏洞库

重新加载

自定义漏洞

漏洞编号/CVE编号

漏洞名称

危害等级

搜索

重置

添加漏洞

导入

导出

自定义漏洞将在产品包扫描时参与检测，命中后会记录到漏洞扫描结果中。

☐	漏洞编号	漏洞名称	漏洞标题	危险等级	影响产品	创建时间	操作
☐	CUSTOM-2026-008	AASV10加密漏洞	AAS服务器在服务器特定场景下出现...	高危	AASV10	2026-07-24 17:22:31	编辑 删除
☐	CUSTOM-CVE-2024-0003	Redis 未授权访问信息泄露	Redis Info Leak	中危	Redis	2026-07-23 14:41:13	编辑 删除
☐	CUSTOM-CVE-2024-0002	MySQL 认证绕过漏洞	MySQL Auth Bypass	高危	MySQL	2026-07-23 14:41:08	编辑 删除

共 3 条

< 1 >

10 条/页

2. 上传下载漏洞库

点击【上传漏洞库】选择漏洞库文件进行上传，漏洞库可联系售后获取。已上传的漏洞库文件会保存在服务器中，可点击【下载漏洞库】下载漏洞库文件。

3. 制作与重新加载漏洞库

点击【制作漏洞库】进行漏洞库制作，制作完成后可点击【重新加载漏洞库】进行漏洞库重新加载。该功能主要由运维人员使用，可用于制作更新漏洞库。

4. 添加自定义漏洞

点击【添加漏洞】，弹出添加漏洞窗口，可通过手工添加的方式补充自定义漏洞

添加漏洞

* 漏洞编号

如：CUSTOM-2026-001

* 漏洞名称

请输入漏洞名称

* 漏洞标题

请输入漏洞标题

漏洞描述

请输入漏洞描述

* 影响产品

请输入影响产品

影响产品，需要和制品包下的安装包名称一致

* 存在漏洞的版本

如：*,1.5,1.1-1.10,1.4.*,1.5.*-1.6.*

* 修复版本

如：7.2.x, 7.3.x

存在漏洞的版本，需要和制品包下的安装包版本一致

多个版本用逗号分隔

取消

确定

- **漏洞编号**：自定义漏洞编码，需增加自有前缀，避免与官方漏洞库编码冲突
- **漏洞名称**：漏洞名称
- **漏洞标题**：说明该漏洞的影响、漏洞的利用条件等信息
- **影响产品**：该漏洞影响的产品
- **危险等级**：该漏洞的危险等级
- **CVSS 评分**：CVSS 评分，如没有可不填写

5. 导入、导出自定义漏洞

选择自定义漏洞记录，点击【导出】按钮，系统将自动下载选中的自定义漏洞记录。可通过手工添加编辑后，点击【导入】按钮，将已下载的漏洞记录导入系统。

6. 删除自定义漏洞

选择需要删除的自定义漏洞记录，点击【批量删除】按钮，进行批量删除，删除后无法恢复。

5.10 平台运营

5.10.1 租户管理

5.10.1.1 租户管理

租户是平台进行资源隔离的基本单位，管理员可以通过此功能进行租户的管理。

1. 查看检索租户

管理员可以查看所有租户，并检索租户。

租户管理

租户管理

请输入租户名称

搜索

重置

+ 新增租户

租户名称	英文名称	类型	描述	创建人	创建时间	操作
测试	demo	用户自定义	-	chulei	2026-07-29 13:08:25	编辑 详情 删除
大数据资源中心	dsjczyx	用户自定义	-	acpadm	2026-07-09 14:14:03	编辑 详情 删除
FJD	fjyd	用户自定义	-	mahongbin	2026-07-07 21:57:17	编辑 详情 删除
测试租户	testfan	用户自定义	-	fanmingming	2026-02-27 17:15:05	编辑 详情 删除
深圳市金蝶天燕云计算	apusic	用户自定义	-	mahongbin	2025-11-16 16:51:51	编辑 详情 删除

2. 查看租户详情

点击【租户名称】，进入租户详情，可查看租户信息、租户管理员、租户成员列表。

5.10.2 授权管理

5.10.2.1 文件授权

文件授权管理用于授权文件的集中上传、分发和回收。当您需要将授权文件部署到目标服务器时，可以通过此功能统一操作。

1. 查看检索文件授权

进入文件授权列表，可查看所有授权文件，并根据厂商、产品、文件名等检索授权文件。

文件授权

金蝶天燕

产品

请输入文件名搜索

搜索

重置

上传授权

文件名	厂商	产品	有限时间	下发记录	备注	上传时间	上传人	操作
license.xml	金蝶天燕	应用服务器AAS	不限	0	-	2026-07-09 10:50:...	acpadmin	下载 下发 删除
license.xml	金蝶天燕	应用服务器AAS	2025-09-05 16:17:13 - 2025-10-31 16:1...	6	-	2025-09-29 16:17:...	mahongbin	下载 下发 删除
KBCLIC-250922-000072.lic	金蝶天燕	应用服务器AAS	2025-09-29 15:54:45 - 2025-10-31 15:5...	2	-	2025-09-29 15:54:...	acpadmin	下载 下发 删除
nodejs-websocket消息收...	金蝶天燕	分布式缓存AMDC	不限	6	-	2025-09-11 16:36:...	lxq	下载 下发 删除

共4条 < 1 > 10 条/页

2. 上传授权文件

点击【上传授权】，选择授权文件（不超过 10MB），关联厂商和产品信息，设置有效期和描述后即可上传。

上传授权

* 厂商

请选择厂商

* 产品

请选择产品

有效时间

开始日期 → 结束日期

* 上传附件

上传文件

描述

请输入描述

取消

确定

- 厂商：授权所属厂商，可在数据字典中添加。
- 产品：授权关联产品，可在数据字典中添加。
- 有效期：授权起止时间
- 上传附件：厂商提供的授权文件
- 描述：对于该授权的详细描述

3. 下发授权文件

选定授权文件后，点击【下发】，选择目标服务器和路径，系统会将授权文件分发到指定位置并记录下发结果。

授权下发

* 下发路径

/opt/software/amdc/

* 下发服务器

+ 选择服务器

172.24.1.116

×

172.24.3.63

×

172.24.3.92

×

172.24.4.90

×

取消

下发

- **下发路径**：将选定的授权文件下发到服务器的指定路径下
- **下发服务器**：将选定的授权文件下发到指定服务器，可多选

4. 查看下发状态与回收

您可以查看每次下发的历史记录，包括下发状态（已下发/下发失败/已回收）、目标服务器 IP 和操作时间等，确保分发过程可追溯。点击列表【下发记录】，可以看到下发情况，并可以通过点击【回收】，对已下发的授权进行回收。回收时服务器上的授权文件将被删除，但不会重启应用。

124

下发记录

批量回收

☐	操作人	时间	状态	服务器IP	路径	详情	操作
☐	liujiayao	2025-12-30 16:53:45	● 已下发	-	/root/.apus...	成功	回收
☐	acpadmin	2025-09-30 14:29:49	● 已回收	172.24.4.1...	/root/.apus...	成功	
☐	acpadmin	2025-09-29 17:23:28	● 已回收	172.24.4.1...	/root/.apus...	成功	
☐	acpadmin	2025-09-29 17:22:05	● 已回收	172.24.4.1...	/aas/root/...	成功	
☐	acpadmin	2025-09-29 17:21:31	● 已回收	172.24.4.1...	/root/.apus...	成功	
☐	mahongbin	2025-09-29 16:18:53	● 已回收	172.24.4.1...	/root/.apus...	成功	

共6条 < 1 > 10条/页

5. 下载与删除

授权文件支持下载到本地备份；不再需要时可以删除。

5.10.2.2 集中授权

集中授权采用授权中心的方式统一管理产品的 License 授权信息。对应的中间件服务通过连接授权中心进行授权，无需下发和管理授权问题。

1. 查看授权列表

可以在此查看所有产品的授权情况，集中授权一般为数量授权，故可以根据总数、已用量了解授权使用的比例。

集中授权

产品名称

发行版本

所属租户

搜索

重置

导入

软件特征码

命名空间	产品名称	发行版本	授权类型	总数	已用	开始时间	结束时间	签发时间	操作
KBCLIC-260616-000265	Apusic In-Memory Data Cache	Standard Edition	实例授权	0	0	2026-06-16 00:...	2026-07-15 23:...	2026-06-30 17:...	查看
KBCLIC-260616-000265	Apusic Distributed Message Queue	Standard Edition	实例授权	0	0	2026-06-16 00:...	2026-07-15 23:...	2026-06-30 17:...	查看
KBCLIC-260616-000265	Apusic Load Balancer	Standard Edition	实例授权	0	0	2026-06-16 00:...	2026-07-15 23:...	2026-06-30 17:...	查看
KBCLIC-260616-000265	Apusic Load Balancer	Agile Edition	实例授权	0	0	2026-06-16 00:...	2026-07-15 23:...	2026-06-30 17:...	查看
KBCLIC-260616-000265	Apusic Copilot	Standard Edition	实例授权	0	0	2026-06-16 00:...	2026-07-15 23:...	2026-06-30 17:...	查看
KBCLIC-260616-000265	Apusic Distributed Config Center	Standard Edition	实例授权	0	0	2026-06-16 00:...	2026-07-15 23:...	2026-06-30 17:...	查看
KBCLIC-260616-000265	Apusic Search Engine	Standard Edition	实例授权	0	0	2026-06-16 00:...	2026-07-15 23:...	2026-06-30 17:...	查看
KBCLIC-260616-000265	Apusic Application Server	Enterprise Edition	实例授权	0	0	2026-06-16 00:...	2026-07-15 23:...	2026-06-30 17:...	查看
KBCLIC-260616-000265	Apusic Application Server	Agile Edition	实例授权	0	0	2026-06-16 00:...	2026-07-15 23:...	2026-06-30 17:...	查看
KBCLIC-260616-000265	Apusic Cloud Platform Core	Standard Edition	实例授权	0	0	2026-06-16 00:...	2026-07-15 23:...	2026-06-30 17:...	查看

共42条

1

2

3

4

5

10条/页

跳至

页

2. 导入授权

点击【导入】，上传 xml 或 lic 格式的授权文件（不超过 1MB），可选择是否覆盖已有的相同授权。

导入

×

☐ 若导入的文件已存在，是否覆盖

点击或将文件拖拽到这里上传

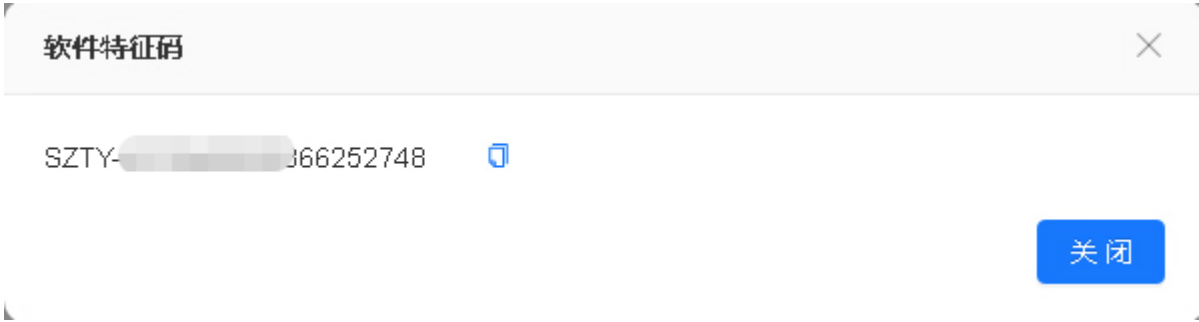
支持扩展名：.xml,.lic 文件大小不超过1M

关闭

导入

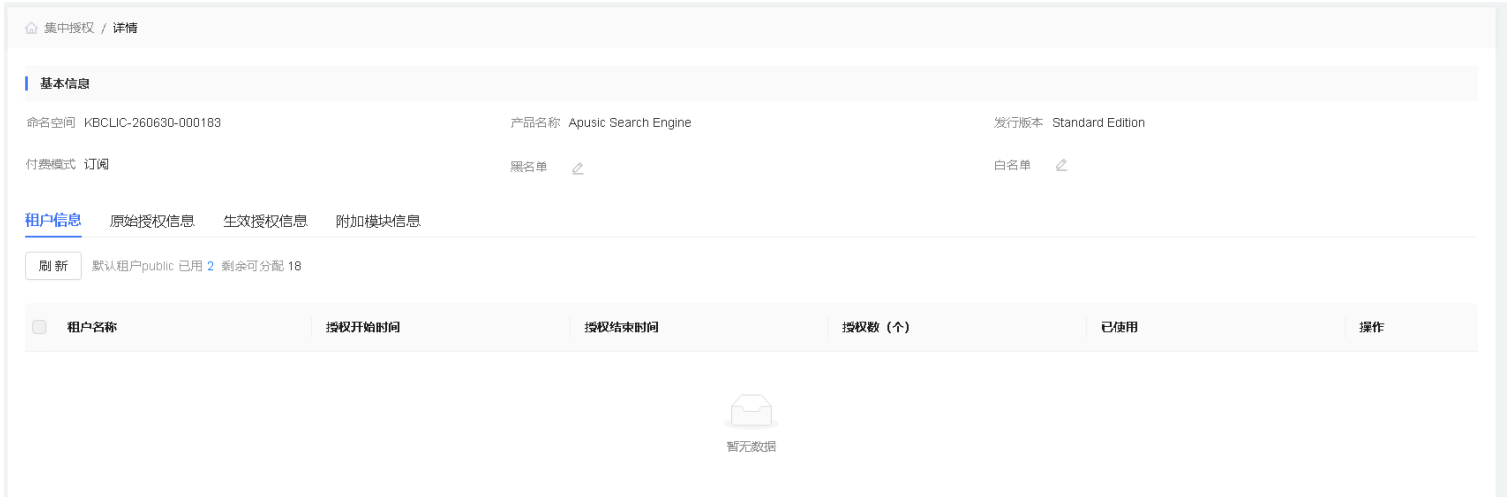
3. 查看授权码

在申请授权时，需提供本地授权中心的特征码，点击【软件特征码】，弹出授权码窗口，可查看本地授权中心的特征码。



4. 查看授权详情

点击授权记录的【查看】按钮，进入授权详情页面，可查看该授权的租户分配情况、原始授权信息、已生效使用的授权信息、授权涉及到的模块。



5.10.2.3 在线实例

在线实例展示了所有已启动并连接到平台的产品实例信息，帮助您了解授权资源的使用情况。

1. 查看实例列表

页面展示了所有在线实例，您可按 IP、产品、版本或租户等多维度筛选。列表中包含实例 IP、物理地址、实例路径、产品版本、所属租户、授权类型和核心数等信息。

在线实例

实例IP

请输入实例IP

物理地址

请输入物理地址

实例路径

请输入实例路径

产品名称

发行版本

租户

搜索

重置

实例IP	物理地址	实例路径	产品名称	发行版本	命名空间	所属租户	授权类型	核心/实...	启动时间
172.24.4.218	00-50-56-99-8A...	/root/.apusic/workspace/a827c195-8795...	Apusic In-Memory Data ...	Standard Edition (v2.0.2...	KBCLIC-260630-000183	public	实例授权	1	2026-07-27 13:52:...
172.24.4.216	00-50-56-99-2F...	/root/.apusic/workspace/1c639391-f39a...	Apusic In-Memory Data ...	Standard Edition (v2.0.2...	KBCLIC-260630-000183	public	实例授权	1	2026-07-27 13:52:...
172.24.4.42	00-50-56-99-B1...	/root/.apusic/workspace/2d9dbf32-0200...	Apusic In-Memory Data ...	Standard Edition (v2.0.2...	KBCLIC-260630-000183	public	实例授权	1	2026-07-27 13:52:...
172.24.4.218	00-50-56-99-8A...	/root/.apusic/workspace/66d57426-b16...	Apusic Load Balancer	Standard Edition (2.0.6)	KBCLIC-260630-000183	public	实例授权	1	2026-07-24 15:49:...
172.17.0.1	02-42-2E-69-34...	/root/.apusic/workspace/7a4939ec-82c9...	Apusic Search Engine	Standard Edition (1.0)	KBCLIC-260630-000183	public	实例授权	1	2026-07-15 16:23:...
172.17.0.1	02-42-2E-69-34...	/root/.apusic/workspace/7a4939ec-82c9...	Apusic Search Engine	Standard Edition (1.0)	KBCLIC-260630-000183	public	实例授权	1	2026-07-15 16:23:...
172.24.4.42	00-50-56-99-B1...	/root/.apusic/workspace/bcca8ac3-84e2...	Apusic Load Balancer	Standard Edition (2.0.6)	KBCLIC-260630-000183	public	实例授权	1	2026-07-15 16:23:...
192.168.128...	02-42-62-14-B1...	/opt/ase/ASE-V1.0.3-202604-x86_64920...	Apusic Search Engine	Standard Edition (1.0)	KBCLIC-260525-000197	public	实例授权	1	2026-05-25 15:23:...
192.168.128...	02-42-62-14-B1...	/opt/ase/ASE-V1.0.3-202604-x86_64920...	Apusic Search Engine	Standard Edition (1.0)	KBCLIC-260525-000197	public	实例授权	1	2026-05-25 15:23:...

2. 复制实例路径

需要获取实例路径信息时，可以直接点击【实例路径】列的按钮复制使用。

5.10.2.4 授权台账

当使用第三方系统发放授权时，可使用授权台账功能进行跟踪。授权台账记录和追踪授权的发放历史，提供完整的审计线索。当您需要查证某个授权的发放记录时，可以在这里检索。

1. 查看台账列表

您可按中间件产品、申请单位、使用单位或关键词搜索。列表中包含产品序列号、工单号、系统名称、中间件品牌型号、授权数量、发放日期、申请单位和使用单位等信息。

授权台账

申请单位

使用单位

中间件品牌

输入中间件型号

输入系统名称/联系人/工单号查询

搜索

重置

新增

导入

导出

数据更新时间：2026-07-14 13:59:34

产品序列号	工单号	系统名称	子系统名称	变更原因	中间件品牌	中间件型号	政务云环境	授权发放数量（套）	操作
239075623492289024011	WO-00998877-888888	智慧交通系统	子系统C	扩容	金蝶中间件	应用服务器V1	是	3	复制 编辑 删除
239075623492289024011	WO-00998877-666	智慧交通系统	子系统C	扩容	金蝶中间件	应用服务器V1	是	3	复制 编辑 删除
239075623492289024011	WO-22110099	智慧医疗系统	子系统A	变更IP	金蝶中间件	应用服务器2	是	4	复制 编辑 删除
239075623492289024011	WO-00998877	智慧医疗系统	子系统A	新申请	金蝶中间件	V1	是	4	复制 编辑 删除
239075623492289024011	WO-66554433	智慧交通系统	子系统A	新申请	金蝶中间件	V2	是	5	复制 编辑 删除
239075623492289024011	WO-88776655	智慧银行系统	子系统A	变更IP	金蝶中间件	金蝶Apusic应用服务器V10	是	1	复制 编辑 删除
239075623492289024011	WO-00998877	智慧交通系统	子系统C	扩容	金蝶中间件	金蝶Apusic应用服务器V10	是	3	复制 编辑 删除
999075623492289024999	214314233214	测试	测试	测试	金蝶中间件	AASV10	是	1	复制 编辑 删除
239075623492289024011	15435346	智慧法院系统	子系统B	扩容	金蝶中间件	V3	是	2	复制 编辑 删除
239075623492289024011	auth-666	智慧法院系统	子系统B	扩容	金蝶中间件	V4	是	2	复制 编辑 删除

共102条 < 1 2 3 4 5 ... 11 > 10条/页 跳至 页

2. 新增、复制编辑台账

在列表页面，点击【新增】按钮，填写授权台账信息，并保存。当新增单据与历史单据较为相似时，可点击【复制】按钮，快速填写。

新增台账

* 工单编号

* 中间件品牌

* 产品序列号

* 部署IP地址

* 系统名称

* 变更原因

* 授权发放日期

请选择 (YYYY-MM-DD HH:mm:ss)

* 申请单位联系人

* 使用单位

* 使用单位联系电话

* 工单生成时间

请选择 (YYYY-MM-DD HH:mm:ss)

* 中间件型号

政务云部署

否

* 部署MAC地址

* 子系统名称

* 授权发放数量

* 申请单位

* 申请单位联系电话

* 使用单位联系人

取消

确定

- 工单编号：外部系统的工单编号，若无可根据自定义规则进行填写，需保证全局唯一。
- 工单生成时间：外部系统的工单生成时间，若无可填写当前时间。
- 中间件品牌：填写对应产品的公司名或产品品牌。
- 中间件型号：填写对应的产品的型号信息。
- 产品序列号：产品的序列号。
- 政务云部署：当涉及到政务云部署，可选择此项进行标识。
- 部署 IP 地址：产品部署的 IP 地址。
- 部署 MAC 地址：产品部署服务器的 MAC 地址。
- 系统名称：产品关联或使用它的系统名称。
- 子系统名称：产品关联或使用它的子系统名称。
- 变更原因：授权变更的原因。首次发放可填写首次发放的原因；授权变更时填写变更的原因。
- 授权发放数量：产品授权发放的数量。
- 授权发放日期：产品授权的起止日期。
- 申请单位：申请该授权的单位名称。

- **申请单位联系人**：申请该授权的联系人。
- **申请单位联系电话**：申请该授权的联系人电话。
- **使用单位**：实际使用该产品授权的单位。
- **使用单位联系人**：实际使用该产品授权的联系人。
- **使用单位联系电话**：实际使用该产品授权的联系人电话。

3. 导入、导出台账数据

点击【导入】，下载 Excel 模板，按照格式填写后上传（文件不超过 500MB，单次不超过 2000 条）。系统会显示导入的成功条数和失败条数，并可下载错误信息文件进行修正。点击【导出】，直接导出当前筛选条件下的台账数据。

导入

×

请下载**台账导入模板**，按格式修改后导入

请先下载模板文档，根据格式和提示填写内容。请确保各字段类型正确无误，否则可能导致导入失败。切勿修改模板中的字段名称。数据导入上限为2000条。

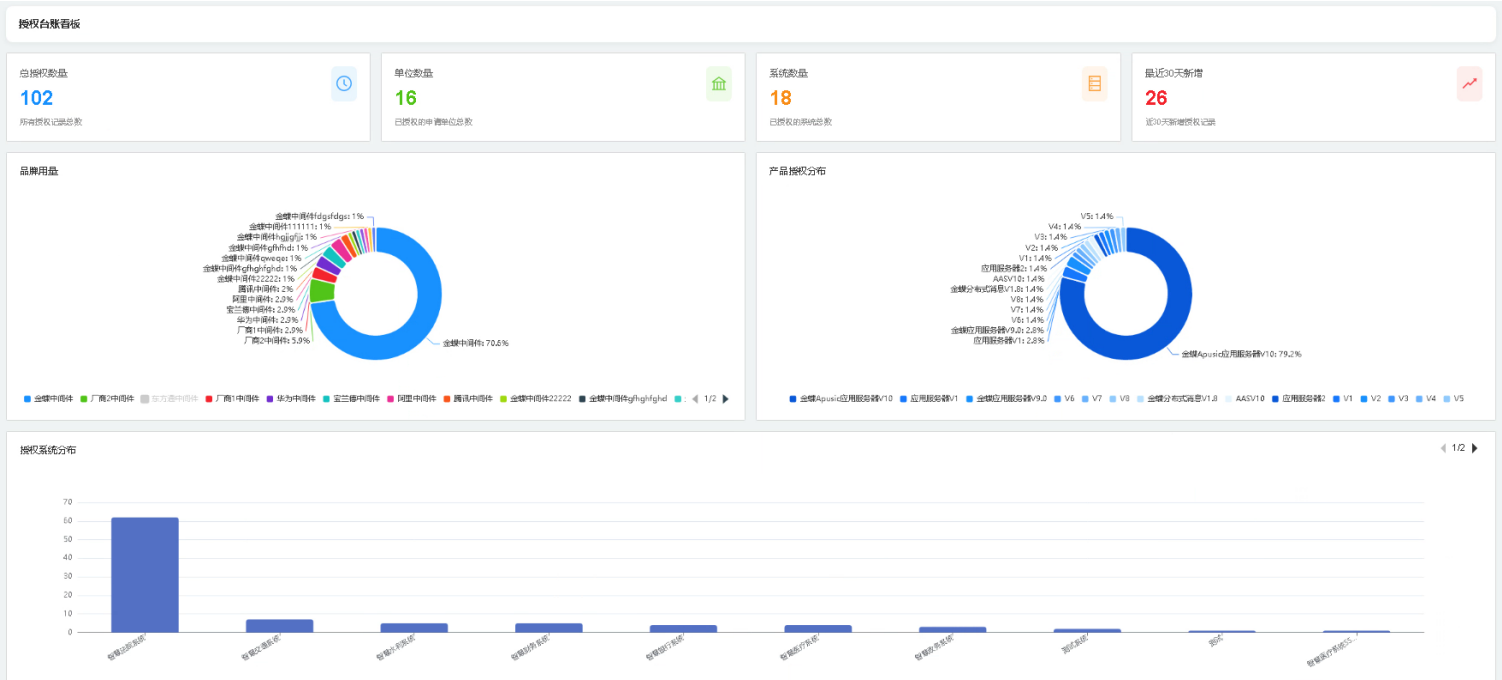
点击或拖拽文件上传

4. 删除台账数据

当台账数据已失效时，点击【删除】，即可快速删除。

5.10.2.5 授权台账看板

授权台账看板以可视化图表展示授权数据的分布和趋势，帮助管理层快速了解授权使用状况。



1. 统计卡片

页面顶部展示总授权数量、单位数量、系统数量和近 30 天新增授权数。

2. 分布图表

分布图表展示授权数据分布情况，包括：

- 品牌用量：不同品牌的用量情况
- 产品授权分布：具体品牌下，各个产品的使用用量

品牌用量与产品授权分布提供联动功能，点击品牌用量，选择一个具体的品牌，右侧产品授权分布将展示该品牌下的产品授权分布。

3. 授权系统分布

根据授权使用数量对系统进行可视化排序展示，默认展示 10 条，点击右上翻页按钮，可以查看更多授权系统统计信息。

4. 最近授权记录

页面底部列出最近 10 条授权台账记录，点击“查看全部”可跳转到完整的台账列表。

5.10.3 审计日志

审计日志记录了所有用户的操作行为和登录历史，是安全追溯和合规审计的重要依据。

1. 登录日志

通过 Tab 切换到登录日志页面，您可以查看所有用户登录平台的记录，包括操作人、登录方式（平台/门户）、操作类型、IP 地址、时间和登录结果。

审计日志

登录日志

操作日志

2026/07/04 → 2026/08/03 前

全部平台

请输入操作人或操作IP搜索

导出

操作人	平台类型	操作	操作IP	操作时间	操作状态
demo11	平台	登录	127.0.0.1	2026-08-03 09:24:16	成功
demo11	平台	登录	192.168.26.1	2026-08-03 09:21:26	成功
chulei	平台	登录	192.168.26.1	2026-08-03 09:20:50	成功
demo11	平台	登录	192.168.26.1	2026-08-03 09:20:30	成功
chulei	平台	登录	192.168.26.1	2026-08-03 09:19:52	成功
demo11	平台	登录	192.168.26.1	2026-08-03 09:19:41	成功
demo11	平台	登录	192.168.26.1	2026-08-03 09:18:52	成功
fanmingming	平台	登录	192.168.26.1	2026-08-03 09:07:20	成功
liuboyi	平台	登录	192.168.26.1	2026-08-02 21:40:10	成功
liuboyi	平台	登录	192.168.26.1	2026-08-02 21:30:39	成功

共610条 < 1 2 3 4 5 ... 61 > 10条/页 跳至 页

2. 操作日志

通过 Tab 切换到操作日志页面，您可以查看所有用户在平台上的操作记录，包括操作人、服务类型、具体操作、操作的对象和资源名称、IP 地址、所属租户和项目等信息。每条操作日志还支持查看详情。

审计日志

登录日志

操作日志

2026/07/04 → 2026/08/03 前

全部平台

全部服务

请输入操作人或操作IP搜索

导出

操作人	平台...	服务类型	操作	资源对象	资源ID/名称	操作IP	租户	项目	操作时间	操作状态	操作
demo11	平台	统一认证	续签	统一认证		127.0.0.1	默认租户	默认项目	2026-08-03 09:24:16	成功	查看详情
demo11	平台	统一认证	续签	统一认证		192.168.26.1	默认租户	默认项目	2026-08-03 09:21:27	成功	查看详情
chulei	平台	统一认证	登出	统一认证		192.168.26.1	默认租户	默认项目	2026-08-03 09:21:19	成功	查看详情
demo11	平台	统一认证	登出	统一认证		192.168.26.1	测试	默认项目	2026-08-03 09:20:47	成功	查看详情
demo11	平台	统一认证	续签	统一认证		192.168.26.1	默认租户	默认项目	2026-08-03 09:20:30	成功	查看详情
chulei	平台	统一认证	登出	统一认证		192.168.26.1	默认租户	默认项目	2026-08-03 09:20:20	成功	查看详情
demo11	平台	统一认证	登出	统一认证		192.168.26.1	默认租户	默认项目	2026-08-03 09:19:46	成功	查看详情
chulei	平台	统一认证	登出	统一认证		192.168.26.1	默认租户	默认项目	2026-08-03 09:18:45	成功	查看详情
chulei	平台	部署实例	停止	平台实例	demo-aas-AAMSV...	192.168.26.1	默认租户	默认项目	2026-08-02 21:59:47	成功	查看详情
chulei	平台	部署实例	重启	平台实例	demo-aas-AAMSV...	192.168.26.1	默认租户	默认项目	2026-08-02 21:59:11	成功	查看详情

共1518条 < 1 2 3 4 5 ... 152 > 10条/页 跳至 页

3. 日志导出

登录日志和操作日志均支持导出为 Excel 文件，用于离线存档或进一步分析。点击【右上】导出按钮，即可下载当前筛选条件下的日志数据。

5.11 平台设置

5.11.1 用户管理

用户管理是平台的基础管理功能，管理员可以在这里创建平台用户、管理用户状态和分配角色。

1. 查看用户列表

页面展示了所有平台用户，您可按用户名或姓名搜索。列表中包含用户名、姓名、角色、邮箱、手机号、账号状态（启用/禁用）等信息。

用户管理

请输入用户名或姓名搜索

搜索

重置

创建

用户名	姓名	状态	角色管理	创建时间	操作
demo11	demo11	● 启用	-	2026-08-02 20:58:00	重置密码 禁用 编辑 删除
testfpj	testfpj	● 启用	-	2026-07-16 15:22:25	重置密码 禁用 编辑 删除
golden09	王鼎	● 启用	平台管理员	2026-07-10 16:31:03	重置密码 禁用 编辑 删除
golden08	王鼎	● 启用	平台管理员	2026-07-10 16:30:27	重置密码 禁用 编辑 删除
golden07	六毛	● 启用	平台管理员	2026-07-10 16:20:01	重置密码 禁用 编辑 删除
golden06	王鼎	● 启用	平台管理员	2026-07-10 16:19:37	重置密码 禁用 编辑 删除
golden05	王鼎	● 启用	平台管理员	2026-07-10 16:15:43	重置密码 禁用 编辑 删除
golden04	王鼎	● 启用	平台管理员	2026-07-10 16:03:35	重置密码 禁用 编辑 删除
dashuju	dashuju	● 启用	-	2026-07-09 14:21:49	重置密码 禁用 编辑 删除
zhangwuji	zhangwuji	● 启用	审计管理员	2026-07-06 16:18:38	重置密码 禁用 编辑 删除

共131条 < 1 2 3 4 5 ... 14 > 10条/页 跳至 页

2. 创建用户

点击【创建】，填写用户信息后，创建新用户。用户为平台统一管理，租户可通过引入平台用户的方式，快速实现租户用户管理。

创建用户

×

* 用户名

用户名只能包含小写字母、数字、连字符（-），必须以小写字母或数字开头及结尾，最长 32 个字符。

* 姓名

姓名只能包含中文、字母、数字和连字符（-），不得以连字符（-）开头或结尾，最长 32 个字符。

角色管理

▼

* 密码

密码必须包含至少一个数字、一个小写字母、一个大写字母和一个特殊字符（~!@#\$%^&*()-_+=\|{};:~!<.>/? 或空格），长度为 8 到 64 个字符。

邮箱

手机号

描述

取消

确定

- **用户名**：用户登录平台时使用的用户名，限小写字母、数字和连字符。
- **姓名**：用户在平台中的真实姓名。
- **角色**：用户在平台中的角色，可分配多个角色。
- **密码**：用户登录平台时使用的密码，8-64 位，需包含大写字母、小写字母、数字和特殊字符。
- **邮箱**：用户登录平台时使用的邮箱，用于接收平台通知。
- **手机号**：用户登录平台时使用的手机号，用于接收平台通知。
- **账号状态**：用户在平台中的账号状态，可设置为启用或禁用。

3. 编辑用户信息

选定用户后，可以修改其姓名、角色、联系方式等信息（用户名创建后不可更改）。

4. 禁用/启用户

对于暂时不需要登录平台的用户，可以禁用其账号（系统预设用户和当前登录用户自身不可禁用）。

5. 删除用户

对于已离职或不再需要的用户，确认后可以删除（系统预设用户不可删除）。

6. 重置密码

如果用户忘记密码，管理员可以为其重置密码。重置后系统会生成一个新密码，并支持复制发送给用户（系统预设用户不可重置）。

7. 查看用户详情

点击用户名可以查看用户的详细信息，包括基本信息、登录日志和关联的租户空间。

5.11.2 角色管理

角色管理用于定义平台的角色和权限。通过创建不同权限的角色，并将角色分配给用户，可以精细控制每个用户能访问的功能和操作。

1. 查看角色列表

页面展示了所有角色，您可按名称或标识搜索。列表中包含角色名称、标识和账户类型。

角色管理

请输入名称或标识搜索

租户类型

Q 搜索

重置

创建

名称	标识	租户类型	类型	用户数	创建时间	所属租户	操作
平台管理员	admin	平台角色	系统预设	33		-	编辑 分配权限 删除
租户用户	tenant-operator	租户角色	系统预设	66		-	编辑 分配权限 删除
项目管理员	project-admin	平台角色	系统预设	2		-	编辑 分配权限 删除
项目用户	project-operator	平台角色	系统预设	0		-	编辑 分配权限 删除
销售	sales	平台角色	系统预设	0		-	编辑 分配权限 删除
超级管理员	super-admin	平台角色	自定义	19		-	编辑 分配权限 删除
租户管理员	tenant-admin	租户角色	系统预设	29		-	编辑 分配权限 删除
demo1	demo1	租户角色	自定义	0	2026-07-31 23:24:23	-	编辑 分配权限 删除
审计管理员	audit-adm	平台角色	自定义	1	2026-07-07 21:42:38	-	编辑 分配权限 删除
安全管理员	security-adm	平台角色	自定义	0	2026-07-07 21:42:13	-	编辑 分配权限 删除

共12条 < 1 2 > 10 条/页 跳至 页

2. 创建角色

点击【创建】，填写角色名称（支持中文）、标识（限小写字母、数字和连字符），并通过权限树为角色勾选对应的功能权限。

角色管理 / 创建角色

基本信息

名称

名称只能包含中文、字母、数字和连字符 (-)，不得以连字符 (-) 开头或结尾，最长 32 个字符。

标识

标识只能包含小写字母、数字、连字符 (-)，必须以小写字母或数字开头及结尾，最长 32 个字符。

租户类型

平台角色

描述

描述可包含任意字符，最长 256 个字符。

设置权限

服务类型	制品管理	
首页	新建制品项目	
资源中心	查询	
仓库管理	查看	
中间件管理	编辑制品项目	
中间件管理		

- 名称：角色名称
- 标识：角色标识，不可重复
- 租户类型：角色所对应的租户类型，平台角色作用于平台，租户角色作用于租户，租户导入用户时，只能选择租户角色。
- 设置权限：可根据需要为该角色选择对应的权限项目，点击右侧开启关闭按钮，可以发放和回收对应权限。

3. 编辑角色

创建后的角色支持修改名称和描述（系统预设角色不可编辑）。不再需要的角色可以删除（系统预设角色不可删除）。

4. 删除角色

创建后的角色支持删除（系统预设角色不可删除）。

5.11.3 数据字典

5.11.3.1 数据字典项

数据字典用于管理系统中的枚举值和通用配置项。当系统需要新增一个下拉选项或配置项时，管理员可以在这里定义。

1. 查看数据字典项

页面展示所有已定义的字典项，您可按配置项名称或描述搜索。

数据字典项

请输入配置项、配置项描述搜索

搜索

重置

新增

删除

☐ 配置项	配置项字段	配置值类型	配置描述	状态	操作
☐ 发行方	distribution	字符串	系统发行方	启用	修改 删除
☐ 告警中心工单问题类型	alarm	字符串	告警中心工单问题类型	启用	修改 删除
☐ 巡检类型	inspection_type	字符串	巡检类型(表示 虚拟机 还是服务巡检的类型)	启用	修改 删除
☐ 巡检状态	inspection_status	字符串	巡检状态	启用	修改 删除
☐ 巡检结果	inspection_result	字符串	巡检结果	启用	修改 删除
☐ 巡检任务状态	inspection_task_state	字符串	巡检任务状态	启用	修改 删除
☐ 通知方式	notify-type-parent	字符串	邮件: 协作, webhook:短信:通知方式	启用	修改 删除
☐ 厂商类型	file_license_product	字符串	金蝶天燕、中创、宝兰德、东方通、人大金仓、达梦、神舟通...	启用	修改 删除
☐ 产品类型	file_license_vendor	字符串	AASV10、AMDC、分布式中间件	启用	修改 删除
☐ 风险等级	risk_level	字符串	巡检风险等级	启用	修改 删除

共28条 < 1 2 3 > 10 条/页 跳至 页

2. 创建数据字典项

在列表界面点击【新增】，填写配置项名称、字段名（限字母、数字和下划线）、配置值类型（字符串/数字/布尔）、描述和状态等。

添加字典配置项

* 配置项

* 配置项字段

* 配置值类型

* 配置描述

* 状态

取消

确定

- 配置项：配置项名称。
- 配置项字段：与平台功能关联的配置项名称，不建议更改。
- 配置值类型：配置项的值类型，决定了如何解析。包括字符串、整数、小数、布尔值、颜色。

- **配置描述**：该配置项目的作用描述。
- **状态**：配置项状态，可设置为启用或禁用。

3. 删除数据字典项

已有字典项支持单个或批量删除。

5.11.3.2 数据字典值

数据字典值用于管理每个字典项的具体取值选项。

1. 查看字典值

页面展示所有字典值，您可按所属配置项和字典值搜索。

数据字典值

请选择配置项

请输入配置值搜索

搜索

重置

新增

删除

☐	配置项	字典标签	配置值	排序	状态	配置描述	css样式	颜色类型	修改时间	操作
☐	工单来源	告警中心	alarm	1	启用	一站式告警服务				修改 删除
☐	操作系统	CentOS	centos	1	启用				2026-07-21 17:17:03	修改 删除
☐	东方通产品类型	TongWeb应用服...	TONG_WEB	1	启用					修改 删除
☐	发行方	alibaba	alibaba	1	启用					修改 删除
☐	资源中心工单问题类型	其他技术问题	wo_resource_other_form	1	启用					修改 删除
☐	产品类型	金蝶天燕	apusic_license_vendor	1	启用		[color: #b10707]			修改 删除
☐	金蝶天燕产品类型	分布式缓存AMDC	AMDC	1	启用					修改 删除
☐	巡检结果	有风险	risky	1	启用	有风险		#45747		修改 删除
☐	中创产品类型	中创PaaS平台	INFORBUS_PAAS	2	启用					修改 删除
☐	巡检类型	服务巡检	inspection_service	2	启用	服务巡检		#4578F8		修改 删除

共138条 < 1 2 3 4 5 6 ... 14 > 10条/页 跳至 页

2. 创建字典值

点击【创建】，选择所属配置项，填写字典标签、配置值、排序号、状态等信息。同一配置项下的字典值不可重复。

添加字典配置值

✕

* 配置项

* 字典标签

* 配置值

* 排序

1

状态

配置描述

CSS样式

颜色类型

取消

确定

- 配置项：从数据字典项选择的配置项目。
- 字典标签：字典标签，显示给用户，全局唯一。
- 配置值：对应项目的配置值。
- 排序：排序序号，数字越小越靠前。
- 状态：字典值状态，可设置为启用或禁用。
- 配置描述：该配置项值的描述
- CSS 样式：可使用 CSS 样式，优化显示。
- 颜色类型：颜色类型，可设置为所需颜色，实现突出显示。

3. 删除字典值

字典值支持编辑和单个/批量删除。

5.11.4 路由管理

路由管理用于配置平台网关的访问路由。当您需要将某个后端服务通过网关暴露给前端或其他系统时，在这里配置路由规则。

1. 查看路由列表

页面展示所有已配置的路由，您可按路由 ID 搜索。列表中包含路由 ID、路由地址、优先级和状态。用于平台管理运维人员快速检索维护路由信息。

路由管理

请输入路由ID搜索

搜索

重置

新增

查看实时路由

☐	路由ID	路由地址	优先级	状态	系统路由	创建人	创建时间	操作
☐	gateway-swagger	forward:/	101	● 可用	系统			查看 修改
☐	acp-ws-resource	lbws://maas-resource	100	● 可用	系统			查看 修改
☐	acp-console	http://172.24.3.61:9801	2147483647	● 可用	系统			查看 修改
☐	acp-default-manager	lb://maas-m-manager	102	● 可用	系统			查看 修改
☐	acp-default-monitor	lb://maas-monitor	103	● 可用	系统			查看 修改
☐	acp-default-resource	lb://maas-resource	104	● 可用	系统			查看 修改
☐	acp-default-aump	lb://maas-aump	105	● 可用	系统			查看 修改
☐	acp-ws-aump	lbws://maas-aump	99	● 可用	系统			查看 修改
☐	acp-ws-alarm	lbws://maas-alarm	98	● 可用	系统			查看 修改
☐	acp-default-cloudlog	lb://maas-cloudlog	106	● 可用	系统			查看 修改

共27条 < 1 2 3 > 10条/页 跳至 页

2. 创建路由

点击【新增】，填写路由 ID（全局唯一）、路由地址（支持 lb:// 格式）、优先级和状态，并通过动态表单配置断言和过滤器规则。

添加路由

* 路由ID

请输入路由ID

* 路由地址

请输入路由地址

* 优先级

0

状态

可用

元数据

+ 添加元数据

断言

+ 添加断言

过滤器

+ 添加过滤器

取消

确定

- **路由 ID**：路由的唯一标识符。
- **路由地址**：路由的暴露地址
- **优先级**：路由的优先级，数字越小，优先级越高。
- **状态**：路由状态，可设置为启用或禁用。
- **元数据**：路由的元数据信息，用于存储自定义信息。
- **断言**：断言规则，用于匹配请求，并返回匹配结果。只有当前端请求满足您配置的全部断言条件，这条路由才会接收该请求并执行转发。支持路径、方法、请求头等配置类型。
- **过滤器**：过滤器规则，用于处理请求和响应，并返回处理结果。请求匹配路由后，在转发前后执行一系列拦截处理，如去除路径、添加请求头，Rewrite 路径等。

3. 编辑和删除

自定义路由支持编辑和删除（系统内置路由不可操作）。

4. 查看实时路由

点击【查看实时路由】，可以查看网关当前实际生效的路由信息，并支持查看每条路由的 JSON 详情，方便排查路由不生效的问题。

Gateway 实时路由

路由ID	目标服务	断言	过滤器	优先级	操作
ReactiveCompositeDiscov...	lb://MAAS-CLOUDLOG	Paths: [/maas-cloudlog/**...	[[RewritePath /maas-cl...	0	详情
ReactiveCompositeDiscov...	lb://MAAS-AI-DEPLOY	Paths: [/maas-ai-deploy/**...	[[RewritePath /maas-ai...	0	详情
ReactiveCompositeDiscov...	lb://MAAS-MANAGER	Paths: [/maas-manager/**...	[[RewritePath /maas-...	0	详情
ReactiveCompositeDiscov...	lb://CONNECTOR-TIANYI	Paths: [/connector-tianyi/...	[[RewritePath /connect...	0	详情
ReactiveCompositeDiscov...	lb://MAAS-RESOURCE	Paths: [/maas-resource/**...	[[RewritePath /maas-r...	0	详情
ReactiveCompositeDiscov...	lb://MAAS-AUMP	Paths: [/maas-aump/**], ...	[[RewritePath /maas-a...	0	详情
ReactiveCompositeDiscov...	lb://MAAS-GATEWAY	Paths: [/maas-gateway/**...	[[RewritePath /maas-g...	0	详情
acp-ws-alarm	lb:ws://maas-alarm	Paths: [/acp/alarm/apis/v...	-	98	详情

5.11.5 任务管理

任务管理用于管理和跟踪平台定时任务。

1. 查看任务

提供任务执行列表，可查看任务名称、调度表达式、起止时间、耗时、执行结果、执行 IP 等相关信息。

任务管理

任务名称

开始时间

结束时间

执行结果

查询

重置

任务名称	Cron 表达式	开始时间	结束时间	耗时	结果	执行 IP	操作
alertmanager-config	*/*	2026-08-03 10:49:30	2026-08-03 10:49:30	20 ms	成功	192.168.26.8	详情
security-scan-task	*/*	2026-08-03 10:49:30	2026-08-03 10:49:30	8 ms	成功	192.168.26.8	详情
prometheus-config	*/*	2026-08-03 10:49:30	2026-08-03 10:49:30	94 ms	成功	192.168.26.8	详情
apusidet-install-task	*/*	2026-08-03 10:49:30	2026-08-03 10:49:30	15 ms	成功	192.168.26.7	详情
service-upgrade-task	*/*	2026-08-03 10:49:30	2026-08-03 10:49:30	19 ms	成功	192.168.26.8	详情
service-state-task	*/*	2026-08-03 10:49:25	2026-08-03 10:49:25	19 ms	成功	192.168.26.8	详情
inspection-task-trigger	*/*	2026-08-03 10:49:25	2026-08-03 10:49:25	9 ms	成功	192.168.26.8	详情
rg-instance-state-task	*/10	2026-08-03 10:49:10	2026-08-03 10:49:10	67 ms	成功	192.168.26.8	详情
power-job-worker-create	0/*	2026-08-03 10:49:05	2026-08-03 10:49:05	8 ms	成功	192.168.26.5	详情
deploy-task	0/*	2026-08-03 10:49:02	2026-08-03 10:49:02	2 ms	成功	192.168.26.8	详情

共278823条

1

2

3

4

5

...

27883

10 条/页

跳至

页

2. 查看执行详情

点击任务【详情】，查看任务执行具体信息。

任务日志详情

任务名称	alertmanager-config
Cron 表达式	*/* 30 * * * *
类名	com.apusic.maas.aump.task.PrometheusConfigTask\$\$SpringCGLIB\$\$0
开始时间	2026-08-03 10:49:30
结束时间	2026-08-03 10:49:30
执行耗时	20 ms
执行结果	成功
执行节点 IP	192.168.26.8
异常信息	-

关闭

5.11.6 系统菜单

系统菜单用于配置平台前端导航菜单的结构和权限映射。当您需要调整菜单层级、添加新页面入口或控制菜单可见性时，在这里操作。

1. 查看菜单树

菜单以树形结构展示，直观地呈现层级关系。您可按名称或状态搜索。菜单修改后，用户需重新登录后才会生效。

系统菜单

请输入菜单名称

请选择菜单状态

搜索

重置

新增

导出

导入

刷新缓存

菜单名称	类型	状态	排序	权限标识	组件名称	链接路径	操作
首页	服务	启用 显示	1		PlatformHomePage		新增 修改 删除
> 资源中心	服务	启用 显示	2		ResourceCenter		新增 修改 删除
> 仓库管理	服务	启用 显示	3		RepositoryManagement		新增 修改 删除
> 中间件管理	服务	启用 显示	4		MiddlewareManagement		新增 修改 删除
> 云中间件管理	服务	启用 显示	5		CloudNativeMiddlewareManagement		新增 修改 删除
> 可观测性	服务	启用 显示	6		MonitorAlert		新增 修改 删除
> 告警与事件	服务	启用 显示	7		MonitorAlert		新增 修改 删除
> 平台运维	服务	启用 显示	8		SystemManagement		新增 修改 删除
> 安全中心	服务	启用 显示	9		SecurityCenter		新增 修改 删除
> 平台运营	服务	启用 显示	10		PlatformCenter		新增 修改 删除
> 平台设置	服务	启用 显示	11		SystemManagement		新增 修改 删除

2. 创建菜单

点击【创建】，填写名称，选择类型（服务/子菜单/功能），指定父菜单、路由地址、组件路径、权限标识、图标、排序等信息。

添加菜单

* 上级菜单

根目录

* 菜单名称

* 菜单类型

服务

子菜单

功能

* 适用范围

平台 x

* 组件名称

外链地址

* 是否可见

显示

* 新窗口打开

关闭

* 是否缓存

缓存

* 排序

0

排序值越小，菜单显示越靠前

取消

确定

- 上级菜单：该菜单的父级菜单。
- 菜单名称：该菜单显示的名称。
- 菜单类型：菜单可分为服务（一级）、子菜单（二级）、功能（页签）三种类型，可根据需要设置
- 使用范围：平台或者租户，该配置影响了菜单的生效范围。支持多选。
- 组件名称：该菜单关联的平台代码功能。
- 外链地址：可通过配置此项，链接到第三方平台。
- 是否可见：该菜单是否显示，可用于临时隐藏不需要的功能。
- 新窗口打开：点击菜单后，该菜单将新窗口打开。
- 是否缓存：是否缓存该菜单，默认缓存。

- **排序**：可调整菜单排序位置，数字越小越靠前。

3. 编辑和删除

已有菜单支持编辑修改。删除菜单时如果存在子菜单，需要先删除子菜单。

4. 状态和显示控制

菜单支持启用/停用（会同时影响所有子菜单），也支持显示/隐藏（按钮类型不支持隐藏）。

5. 导入/导出

支持通过 xlsx/xls 文件批量导入菜单，也支持将当前菜单结构导出备份。

6. 刷新缓存

点击【刷新缓存】，可将菜单缓存数据刷新。

5.11.7 系统设置

系统设置集中管理平台的各种全局配置参数，包含以下几个子页面：

1. 基础设置

在这里配置平台的系统名称（不超过 64 字符）、上传 Logo 图标、填写系统描述，以及上传许可证文件。

系统设置

基础设置

登录设置

回收策略

关于

基础设置

授权中心命名空间

KBCLIC-260630-000183

平台默认租户下的中间件安装所使用的命名空间

告警系统appKey

8e506914-6c26-4f9a-ace0-177e775bcde2

告警中心-集成-监控系统重app中存在的key值

代理软件包

上传

上传对应的包更新代理

CentOS-arm64	 apusiclet-8.0.5.23-Linux-arm64.rpm	2026-07-03 15:43:16
Ubuntu-arm64	 apusiclet-8.0.5.23-Linux-arm64.deb	2026-07-03 15:43:22
CentOS-x86_64	 apusiclet-8.0.5.24-Linux-amd64.rpm	2026-07-28 17:18:50
Ubuntu-x86_64	 apusiclet-8.0.5.23-Linux-amd64.deb	2026-07-03 15:43:57

下载代理软件包

保存

- **授权中心命名空间**：平台关联的授权中心
- **告警系统 appKey**：对接的告警系统的 appKey
- **代理软件包**：可通过上传功能，为平台提供最新的代理软件包。上传后可通过主机管理进行代理升级。

2. 登录设置

自定义登录页的背景图片和 Logo，打造符合企业形象的门户。

基础设置

登录设置

回收策略

关于

允许凭证续签

开启

开启后当凭证即将过期时，系统会自动续签

登录失败锁定

开启

开启后当登录失败次数达到阈值时账号会自动锁定

凭证有效期（分）

2880

设置登录凭证有效期时长

凭证续签间隔（分）

2880

当登录凭证过期但未超过续签间隔时，系统会自动续签

登录失败锁定阈值

5

登录失败次数到达该值时账号会自动锁定

登录失败锁定时间（分）

5

登录失败多次后账号锁定的时间

保存

- **允许凭证续签**：允许凭证自动续签，支持用户有操作时长期保持登录。
- **登录失败锁定**：如果用户登录失败一定次数，则锁定用户登录。
- **凭证有效期**：凭证默认有效期。
- **凭证续签间隔**：凭证多久内可以续签。
- **登录失败锁定阈值**：连续登录失败的次数，超过该次数将被锁定。
- **登录失败锁定时间**：锁定后，经过多长时间，自动解锁。

3. 回收策略

配置资源的自动回收周期（天），以及回收规则列表，避免闲置资源长期占用。

基础设置

登录设置

回收策略

关于

回收策略

自动清理保留时长

7天 15天 30天

清理时间窗口

00:00 → 02:00

清理消息通知

开启

保存

- **自动清理保留时长**：自动清理保留时长。
- **清理时间窗口**：清理工作启动时间。
- **清理消息通知**：开启后将收到清理运行时的消息通知。

4. 关于

查看当前平台的系统版本和构建信息。

基础设置

登录设置

回收策略

关于

关于

机器码SZTY-86592634

产品当前版本0.0.1

最新更新日志

2025-03-18 更改说明文档

版本号：8.0.3

发布日期：2025-03-18

变更列表：

* Changed(改动/修改)

* Removed(移除功能)

* Fixed(修复 Bug)

* Security(安全性修复)

变更日志 (Changelog)

[8.0.3] - 2025-03-18

修改 (Changed)

重构了中间件的安装,优化步骤及安装步骤

5.11.8 系统组件

5.11.8.1 仪表盘

仪表盘展示了平台所依赖的核心组件和插件服务的运行状态，帮助您快速排查基础设施层面的问题。

集群节点1

组件总数7

运行中7

异常0

组件列表

刷新

核心服务

网关服务1个实例

资源服务1个实例

中间件服务1个实例

管理服务1个实例

插件服务

alertmanager1个实例

prometheus1个实例

grafana1个实例

管控台

管控台

管控台

系统节点

主机名	IP	区域/可用区	Agent状态	操作
linux-3-61	172.24.3.61	系统节点/可用区1	运行中	查看

1. 状态概览

页面顶部展示集群节点数量、组件总数、运行中组件数和异常组件数等关键指标，让您一眼掌握整体健康度。

2. 核心服务列表

展示平台核心服务的名称、状态（UP=正常/DOWN=异常）、实例数量和服务标识。

3. 插件服务列表

展示插件服务的状态。未安装的插件会显示【安装】按钮，已安装的显示【管控台】按钮。

4. 组件安装

对于未安装的插件服务，选择目标在线主机后点击【安装】，即可部署该组件到指定节点。

5.12 个人中心

点击右上角用户名称后，在弹出窗口中点击【修改个人信息】，进入个人中心。

5.12.1 基本设置

用户可在此修改个人信息。包括头像、姓名与描述信息。

5.12.2 安全设置

用户可在此进行登录密码、手机绑定、邮箱绑定相关功能操作。

5.13 消息中心

5.13.1 消息管理

5.13.1.1 全部消息

消息中心是平台所有通知消息的统一入口。无论是产品更新通知、运维告警，还是账号安全提醒，您都可以在这里集中查阅和管理。

1. 查看消息

提供当前用户所收到的所有消息。支持进行消息检索。

消息管理

搜索标题

状态

搜索

发送消息

批量已读

批量删除

全部已读

已选 1 项

☒	标题	内容	类型	创建时间	操作
☒	test	test	SYSTEM	2026-08-03 11:23:48	删除

共 1 条

< 1 >

10 条/页

2. 阅读消息

点击列表中的某条消息标题，弹出内容框展示其完整内容。

消息详情

test

发送人：系统 | 2026-08-03 11:23:48 | 已读

test

3. 标记已读

点击消息时会自动将该条消息标记为已读。如果您想一次性清空未读提醒，可以选中消息，点击【批量已读】，或直接点击【全部已读】，一次性标记所有未读消息。

4. 删除消息

支持勾选多条消息后批量删除，选中消息后，点击【批量删除】按钮，进行一次性快速删除。

5.13.2 通知渠道

5.13.2.1 通知方式

通知方式用于配置消息的发送渠道。当您需要通过邮件、短信或 Webhook 等方式发送通知时，首先在这里完成渠道配置。

1. 查看渠道列表

点击【通知渠道】，可查看不同方式的通知渠道配置，如邮件、协作 APP、Webhook、短信等。

通知方式

邮件

协作

webhook

短信

+

邮件

apusic邮件配置_可用_勿删

服务状态

● 启用

通知类型

邮件

服务提供商

SMTP

配置

停用

通知方式

邮件

协作

webhook

短信

云之家

钉钉

企业微信

apusic邮件配置_可用_勿删

服务状态

● 启用

通知类型

邮件

服务提供商

SMTP

配置

停用

通知方式

邮件

协作

webhook

短信

API hook

天津应急通知接口

服务状态

● 启用

通知类型

webhook

服务提供商

自定义HOOK

配置

停用

webhook_test

服务状态

● 启用

通知类型

webhook

服务提供商

自定义HOOK

配置

停用

fpj_webhook测试服务_勿删

服务状态

● 启用

通知类型

webhook

服务提供商

自定义HOOK

配置

停用

通知方式

邮件

协作

webhook

短信

阿里云SMS

腾讯云SMS

金蝶云SMS

华为云SMS

天津应急SMS

天津应急短信

服务状态

● 启用

通知类型

短信

服务提供商

天津应急SMS

配置

停用

2. 配置通知渠道

点击【创建】，选择渠道子类型，填写服务名称和连接参数（如 SMTP 服务器地址、API Key 等），即可完成渠道接入。

3. 测试连通性

配置完成后，可以发送测试消息验证渠道是否可用。

4. 启用/停用与删除

渠道可以随时启用或停用；不再使用的渠道可以删除。

5.13.3 通知模板

通知模板用于定义通知消息的内容格式。您可以根据不同的通知场景创建自定义模板，使用变量替换实现个性化推送。

1. 查看模板

页面展示所有通知模板，您可按模板类型（全部/系统内置/用户自定义）筛选。系统内置模板不可编辑或删除。

通知模板

全部模板

模板名称

Q

新增通知模板

模板名称	通知方式	模板类型	更新时间	操作
站内通知模板	站内消息	用户自定义模板	2026-07-07 15:37:38	查看 测试发送 编辑 删除
webhook模板	webhook_text	用户自定义模板	2026-07-07 15:35:04	查看 测试发送 编辑 删除
测试通知112	cloudhub	用户自定义模板	2026-05-14 13:36:49	查看 测试发送 编辑 删除
测试通知1123	cloudhub	用户自定义模板	2026-05-14 13:36:00	查看 测试发送 编辑 删除
内存使用率大于80%站内通知告警模板	站内消息	用户自定义模板	2026-05-13 18:40:39	查看 测试发送 编辑 删除
sdasdasd	邮件	用户自定义模板	2026-05-13 14:04:05	查看 测试发送 编辑 删除
demo111	站内消息	用户自定义模板	2026-05-13 13:52:41	查看 测试发送 编辑 删除
测试通知11	云之家	用户自定义模板	2026-01-13 11:12:50	查看 测试发送 编辑 删除
测试模板111	云之家	用户自定义模板	2026-01-13 10:22:06	查看 测试发送 编辑 删除

2. 创建模板

点击【创建】，填写模板名称（不超过 50 字符），选择通知方式（从已配置的渠道中选择），编写模板内容（不超过 1000 字符）。内容中可以使用 `${变量名称}` 格式的变量，发送时会被自动替换。

新增通知模板

×

* 模板名称

内存使用率大于80%

* 通知方式

站内消息

▼

* 模板内容

内存使用率大于80%

实例信息: \${instance}
主要是用来测试的

使用提示:

您可以在模板内容里使用变量，格式为\${变量名称}，例如:您的验证码为\${code}，该验证码5分钟内有效，请勿泄露于他人。
[可用变量列表](#)

取消

确定

- **模板名称**：通知模板名称，不能重复。
- **通知方式**：选择通知渠道，如短信、站内消息等。
- **模板内容**：通知内容，可通过可用变量列表，对通知对象实现个性化推送。

3. 预览和测试

创建完成后可以预览模板效果，可以通过【测试发送】选择接收人和自定义参数，验证模板是否正常渲染和发送。

测试发送

通知模板

站内通知模板

* 接收人

请选择接收人

自定义参数

+ 添加参数

取消

发送

- 接收人：选择接收通知的用户。
- 自定义参数：可以为通知模板注入参数值，便于进行模拟测试。

5.13.4 通知策略

通知策略定义了“什么情况触发通知、通知谁、用什么模板通知”的完整规则。

1. 查看策略列表

页面展示所有通知策略，您可按状态（启用/禁用）筛选或按名称搜索。列表中包含策略名称、类型（告警/事件）、匹配方式和关联的通知模板。

通知策略

全部状态

策略名称

Q

新增策略

策略名称	策略类型	匹配类型	标签	状态	通知模板	操作
ALB运行状态通知	告警	精确匹配	nginx_up=0	启用	云之家自定义通知模板	编辑 删除
云之家通知消息	告警	精确匹配	demo=demo1	启用	测试通知112	编辑 删除
内存使用率告警通知	告警	精确匹配	demo=demo2	启用	内存使用率大于80%站内通知告警模板	编辑 删除

共3条 < 1 > 10 条/页

2. 创建策略

在列表页面，点击【新增策略】，即可进行策略配置。

新增通知策略

* 策略名称

请输入策略名称

策略类型

告警

状态

启用

匹配类型

精确匹配

标签规则

名称，例如 severity

值，例如 critical

+ 添加标签

通知用户

请选择通知用户

* 通知模板

请选择通知模板

备注

请输入备注

取消

保存

- 策略名称：策略名称，全局唯一。
- 策略类型：告警/事件。
- 状态：是否启用。
- 匹配类型：采用精确匹配或正则匹配。
- 标签规则：当符合对应的标签时，则触发通知策略。
- 通知用户：选择需要得到通知的用户。
- 通知模板：选择使用的通知模板。
- 备注：该通知策略的备注信息。

3. 策略匹配机制

策略创建后，系统会自动根据策略中配置的标签规则匹配产生的告警或事件，匹配成功后通过关联的通知模板向指定用户发送通知。

6 常见问题

本节列出 ACP 平台部署、运维过程中常见的问题及解决方案。如需查阅完整常见问题及更多技术细节，请参考 [常见问题完整文档](#)。

6.1 常见产品知识问题

6.1.1 Q1：ACP 有哪些部署方式？

支持单机部署和集群部署两种方式：

- **单机部署**：主要用于测试和演示环境，对硬件资源要求较低（8 核 CPU / 16G 内存 / 500G 硬盘即可）。
- **集群部署**：生产环境推荐方案，建议至少 4 台服务器（8 核 CPU / 16G 内存 / 1T 硬盘），提供高可用能力。

6.1.2 Q2：部署 ACP 需要的服务器软硬件资源有哪些要求？

软件及操作系统环境要求：

组件	要求
操作系统	Linux Red Hat 5.2 或以上；国产操作系统如银河麒麟系列、中标麒麟系列、普华、中科红旗、深度等。
CPU	Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz 或以上；HUAWEI Kunpeng 920、飞腾 FT1500a 等。
浏览器	Firefox 70 及以上、Chrome 60 及以上、IE 11 及以上。

6.1.3 Q3：ACP 与中间件的关系是什么？

ACP 是面向中间件的云平台（即 PaaS 平台），通过 ACP 可以完成各类中间件（如 Apusic 应用服务器、消息队列、缓存、数据库等）的统一交付、生命周期管理、运维监控和运营治理。中间件是 ACP 所管理的"资源"，ACP 是这些资源的"管理平面"。

6.1.4 Q4：ACP 支持哪些类型的中间件？

ACP 通过"软件管理"模块支持灵活扩展中间件品类，目前已内置支持 Apusic 应用服务器、Redis、Kafka、Elasticsearch、PostgreSQL、MinIO 等多种主流中间件，用户也可通过自定义软件包方式接入其他中间件。

6.2 常见技术问题

6.2.1 Q5：启动时提示 "max file descriptors too low" 或 "max_map_count" 错误怎么办？

这是因为 Linux 内核参数未达 ACP 要求，需要修改内核参数。步骤如下：

1. 编辑 `/etc/sysctl.conf` 文件，在文件末尾添加：

```
vm.max_map_count=262144
fs.file-max=65536
```

2. 保存文件并运行 `sysctl -p` 使配置生效。

3. 编辑 `/etc/security/limits.conf` 文件，添加：

```
* hard nofile 65536
* soft nofile 65536
```

注：上述修改需要重新登录才生效。

6.2.2 Q6：启动 alertmanager 时提示 "No private IP address found" 错误怎么办？

该问题是 alertmanager 默认监听地址 9093 端口绑定失败导致。解决方法：修改 alertmanager 启动脚本，绑定实际 IP 地址：

```
$ vi bin/script/middleware/alertmanager.sh

# 在启动命令上加上，IP 修改为所在机器的 IP
--web.listen-address=<本机IP>:9093 --cluster.listen-address=<本机IP>:9094
```

6.2.3 Q7：启动时提示 "Could not create the Java Virtual Machine" 错误怎么办？

ACP 管控台依赖 JDK 17，当系统 Java 环境冲突时会出现此类报错。可通过指定 JAVA_HOME 的方式解决：

```
# 指定 JAVA_HOME 为 ACP 内置 JDK，并启动
export JAVA_HOME=/home/apusic/maas-8.0.5/jdk
./bin/maas.sh start all -d
```

6.2.4 Q8：部署服务时提示 "java not found" 错误怎么办？

该问题通常有两种原因：

1. **服务器上未安装 Java 环境**：请正确安装 Java 环境，设置 JAVA_HOME、PATH 等环境变量，并重启 apusiclet：

```
systemctl restart apusiclet
```

2. **环境变量设置有问题**：检查 apusiclet 的环境变量配置：

```
cat /etc/apusiclet/environment
```

通常情况下，JAVA_HOME 以及 PATH 环境变量应该正确写入。若未写入或写入错误，请按以下顺序检查： `/etc/profile` → `/root/.bashrc`。

如以上内容未能覆盖您的问题，请联系技术支持获取帮助。

7 附录

本节列出 ACP 平台运维常用的命令速查及关键组件说明。如需查阅完整附录资料，请参考 [附录完整文档](#)。

7.1 附录 A：平台依赖组件操作命令

通过 `maas.sh` 脚本可对平台依赖组件进行启动、停止、状态查看和日志查看等操作。以下以 PostgreSQL 和 MinIO 为例说明：

7.1.1 A.1 PostgreSQL 操作命令

```
# 启动
./bin/maas.sh middleware start postgresql

# 停止
./bin/maas.sh middleware stop postgresql

# 查看状态
./bin/maas.sh middleware status postgresql

# 查看日志
./bin/maas.sh middleware logs postgresql
```

7.1.2 A.2 MinIO 操作命令

```
# 启动
./bin/maas.sh middleware start minio

# 停止
./bin/maas.sh middleware stop minio

# 查看状态
./bin/maas.sh middleware status minio
```

```
# 查看日志
./bin/maas.sh middleware logs minio
```

其他组件（如 Elasticsearch、Prometheus、Grafana 等）的操作命令格式相同，将命令中的 `postgresql` / `minio` 替换为对应组件名称即可。

7.2 附录 B：Apusiclet 代理工具介绍

Apusiclet 是部署在每个目标节点上的代理程序，承担 ACP 平台与节点间的通信桥梁作用。

7.2.1 B.1 主要功能

- 1. **对进程操作和管理**：通过对进程的纳管，确保在节点上对进程进行启动、停止、重启等操作。
- 2. **对 peasecod 资源的管理**：定时同步与 ACP 平台进程的状态、虚拟机状态。
- 3. **健康检查 (Liveness/Readiness)**：定期检查容器的健康状况，执行存活和就绪探针。如果容器健康检查失败，apusiclet 会重新启动容器。
- 4. **日志收集**：处理进程日志的收集。
- 5. **资源监控**：定期报告节点资源使用情况（如 CPU、内存、磁盘等）给 ACP 控制平面，以便集群管理员可以监控节点健康和负载。
- 6. **与 ACP 服务器通信**：定期向 ACP API 服务器报告节点和进程的状态，并接收新的调度指令，负责与 API 服务器的实时通信，确保进程与集群的状态一致。

7.2.2 B.2 常用命令速查

命令示例	功能说明
<code>apusiclet version</code>	查看 apusiclet 当前版本
<code>apusiclet pc ls</code>	列出所有进程组（peasecod）信息
<code>apusiclet pc get</code>	获取当前进程组资源状态及对象
<code>apusiclet logs</code>	获取当前实例的进程日志
<code>apusiclet volume ls</code>	查看当前 volumes 挂载的卷
<code>apusiclet preset build <REPOSITORY>:<VERSION></code>	构建 apusiclet 制品包
<code>apusiclet preset init</code>	初始化 metadata.json 模板
<code>apusiclet preset ls</code>	查询制品包列表
<code>apusiclet pull <REPOSITORY>:<TAG></code>	拉取制品包
<code>apusiclet push <REPOSITORY>:<TAG></code>	推送制品包

<code>apusiclet login <REPOSITORY></code>	登录制品仓库
<code>apusiclet preset run --name <NAME> <REPOSITORY></code>	运行指定的制品包服务
<code>apusiclet upgrade</code>	升级 apusiclet 到最新版本

7.2.3 B.3 进程组 (peasecod) 名词解释

- **pc (进程组)**：由一个或者多个进程组成的集合。
- **NAMESPACE**：ACP 中租户 ID。
- **CONTEXT**：当前实例集群的名称。
- **READY**：进程组正常能访问的个数（正常进程个数 / 进程组总数）。
- **RESTART**：重启次数。当被纳管的进程关闭或自动退出时，apusiclet 会自动拉起该进程，重启次数依次递增，最大重启时间为 5min。
- **STATUS**：当前进程组的状态，可能值包括 INITIALIZED（初始化）、CREATED（已创建）、RUNNING（运行中）、CHECKING（状态校验）、FAILED（已失败）、UPGRADE（升级中）、EXISTED（进程退出）、SUCCESS（成功）、STOPPED（已停止）。

如需查阅 Apusiclet 详细安装、升级和制品包制作流程，请参考 [附录完整文档](#)。

全国统一服务热线
4008-555-800

金蝶天燕云计算股份有限公司(简称“金蝶天燕云”)成立于2000年，前身为“金蝶中间件公司”，是金蝶集团旗下新一代软件基础云平台服务商，云计算国家标准制定企业，国家信创产业核心软件企业。金蝶天燕是国家863重点研发计划与核高基重大专项承接企业，也是“两网一站四库十二金”国家重点工程的基础平台提供商，产品广泛应用于政府、军工、金融、能源等关键行业，累计服务客户总数超过10万家。



云计算国家标准制定企业
金蝶集团旗下基础软件企业
信息技术应用创新核心企业
官网：www.apusic.com

