

产品概览

架构

简介

核心架构组件

可扩展性与高可用性

功能视角

技术视角

发版日志

4.1.2

4.1.1

4.1.0

架构

目录

灵雀云容器平台 简介

核心架构组件

Global 集群

业务集群

外部集成

可扩展性与高可用性

功能视角

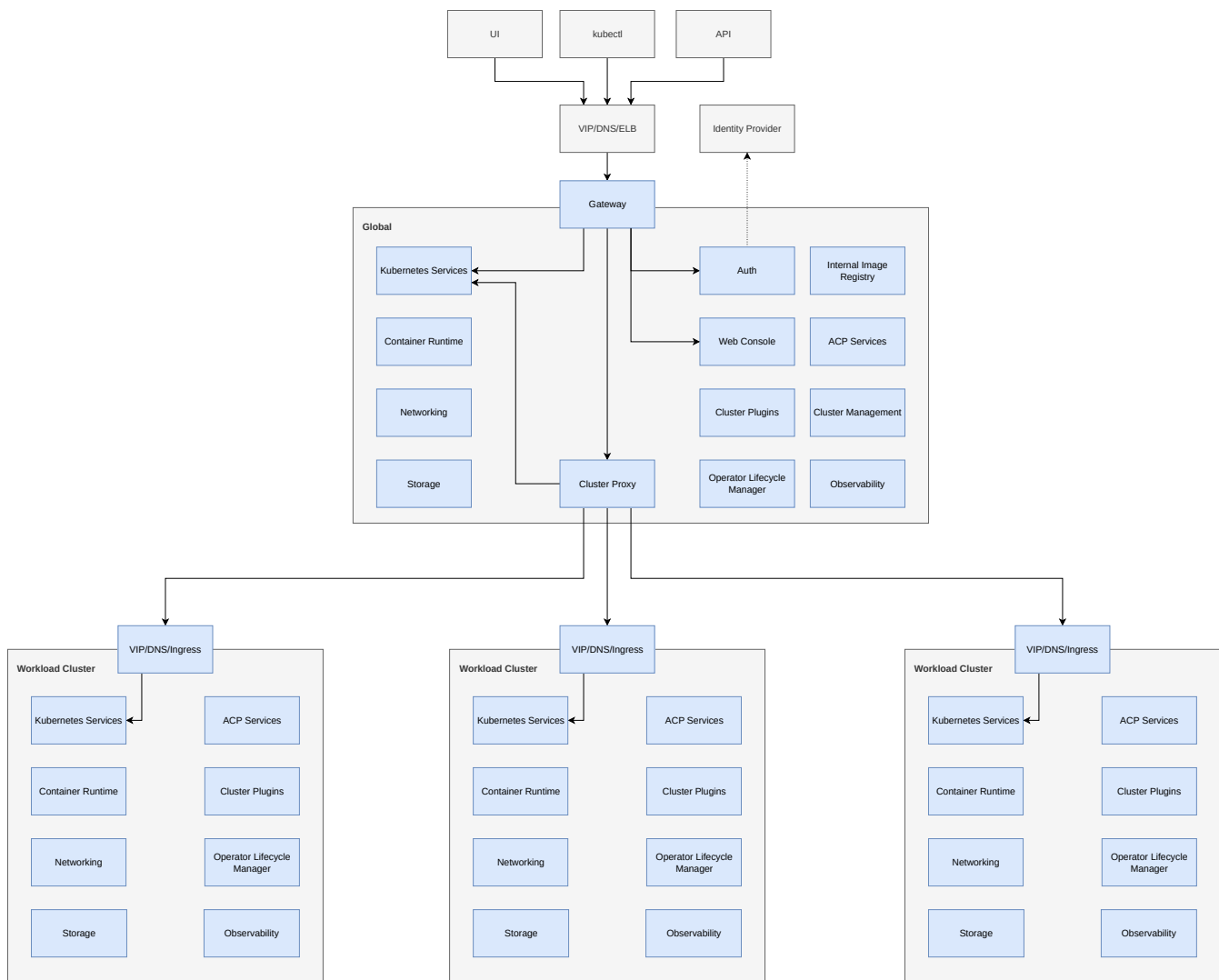
技术视角

关键组件高可用机制

灵雀云容器平台 简介

灵雀云容器平台（ACP）提供了一个企业级的基于 Kubernetes 的平台，使组织能够在混合云和多云环境中一致地构建、部署和管理应用。ACP 集成了核心 Kubernetes 能力，并增强了管理、可观测性和安全服务，提供统一的控制平面和灵活的业务集群。

该架构遵循中心辐射模型，由一个 `global` 集群和多个业务集群组成。此设计既提供了集中治理，又允许独立的工作负载执行和可扩展性。



核心架构组件

Global 集群

global 集群作为 ACP 的集中管理和控制中心。它提供平台范围的服务，如认证、策略管理、集群生命周期操作和可观测性。同时，它也是多集群管理的中心枢纽，提供跨集群功能。

关键组件包括：

- **Gateway**

作为平台的主要入口，管理来自 UI、CLI（kubectl）和自动化工具的 API 请求，并将其路由到相应的后端服务。

- **认证与授权（Auth）**

集成外部 Identity Providers（IdPs），提供单点登录（SSO）和基于 RBAC 的访问控制。

- **Web 控制台**
提供 ACP 的基于网页的界面，通过 Gateway 调用平台 API。
- **集群管理**
负责业务集群的注册、配置和生命周期管理。
- **ACP 服务**
- **Operator Lifecycle Manager (OLM)** 和集群插件
管理 operator 和集群扩展的安装、更新及生命周期。
- **内部镜像仓库**
提供开箱即用的集成容器镜像仓库，支持基于角色的访问控制。
- **可观测性**
提供 `global` 集群和业务集群的集中日志、指标和追踪。
- **集群代理**
实现 `global` 集群与业务集群之间的安全通信。

业务集群

业务集群是由 `global` 集群管理的基于 Kubernetes 的环境。每个业务集群运行隔离的应用工作负载，并继承来自中央控制平面的治理和配置。

外部集成

- **Identity Provider (IdP)**
支持通过标准协议（OIDC、SAML）的联合认证，实现统一的用户管理。
- **API 和 CLI 访问**
用户可以通过 RESTful API、Web 控制台或命令行工具如 `kubectl` 和 `ac` 与 ACP 交互。
- **负载均衡器 (VIP/DNS/SLB)**
为 Gateway 及 `global` 和业务集群的入口端点提供高可用性和流量分发。

可扩展性与高可用性

ACP 设计支持水平扩展和高可用性：

- 各组件可冗余部署，消除单点故障。

- `global` 集群支持管理数十到数百个业务集群。
- 业务集群可根据工作负载需求独立扩展。
- 通过 VIP/DNS/Ingress 实现无缝路由和故障切换。

功能视角

灵雀云容器平台（ACP）的完整功能由 **ACP Core** 和基于两条技术栈的扩展组成：**Operator** 和 集群插件。

- **ACP Core**

ACP 的最小交付单元，提供核心能力，如集群管理、容器编排、项目和用户管理。

- 满足最高安全标准
 - 提供最大稳定性
 - 支持最长生命周期
- 扩展

Operator 和集群插件技术栈中的扩展可分为：

- **Aligned** — 生命周期策略包含多个维护分支，与 ACP 保持一致。
- **Agnostic** — 生命周期策略包含多个维护分支，独立于 ACP 发布。

有关扩展的更多详情，请参见 [Extend](#)。

技术视角

平台组件运行时

所有平台组件均作为容器运行在 Kubernetes 管理集群（即 `global` 集群）内。

高可用架构

- `global` 集群通常由至少三个控制平面节点和多个工作节点组成
- etcd 的高可用性是集群 HA 的核心；详情见 [关键组件高可用机制](#)

- 负载均衡可由外部负载均衡器或集群内部自建 VIP 提供

请求路由

- 客户端请求首先经过负载均衡器或自建 VIP
- 请求转发至运行在指定入口节点（或配置为控制平面节点）的 **ALB**（平台默认 Kubernetes Ingress Gateway）
- ALB 根据配置规则将流量路由至目标组件 Pod

副本策略

- 核心组件至少运行两个副本
- 关键组件（如 registry、MinIO、ALB）运行三个副本

容错与自愈

- 通过 kubelet、kube-controller-manager、kube-scheduler、kube-proxy、ALB 等组件协作实现
- 包括健康检查、故障切换和流量重定向

数据存储与恢复

- 控制平面配置和平台状态以 Kubernetes 资源形式存储在 etcd 中
- 在灾难性故障时，可通过 etcd 快照进行恢复

主备灾备

- 两个独立的 `global` 集群：主集群 和 备集群
- 灾备机制基于主集群到备集群的 etcd 数据实时同步
- 主集群故障不可用时，服务可快速切换至备集群

关键组件高可用机制

etcd

- 部署在三个（或五个）控制平面节点上
- 使用 RAFT 协议进行领导选举和数据复制

- 三节点部署可容忍最多一个节点故障；五节点部署可容忍最多两个
- 支持本地和远程 S3 快照备份

监控组件

- **Prometheus**：多实例，结合 Thanos Query 去重，支持跨地域冗余
- **VictoriaMetrics**：集群模式，包含分布式 VMStorage、VMInsert 和 VMSelect 组件

日志组件

- **Nevermore** 负责收集日志和审计数据
- **Kafka / Elasticsearch / Razor / Lanaya** 以分布式和多副本模式部署

网络组件（CNI）

- **Kube-OVN / Calico / Flannel** 通过无状态 DaemonSet 或三副本控制平面组件实现 HA

ALB

- Operator 以三副本部署，启用领导选举
- 支持实例级健康检查和负载均衡

自建 VIP

- 基于 Keepalived 的高可用虚拟 IP
- 支持心跳检测和主备切换

Harbor

- 基于 ALB 的负载均衡
- PostgreSQL 使用 Patroni 实现 HA
- Redis 采用哨兵模式
- 无状态服务多副本部署

Registry 和 MinIO

- Registry 以三副本部署
- MinIO 采用分布式模式，支持纠删码、数据冗余和自动恢复

发版日志

目录

4.1.2

修复的问题

已知问题

4.1.1

修复的问题

已知问题

4.1.0

新功能与增强

Immutable Infrastructure

Machine Configuration

etcd Encryption

Kubernetes Certificates Rotator

Cluster Enhancement

中文语言包

创建本地集群

日志

监控

租户管理

安全 Pod 运行的自动 UID/GID 分配方案

基于 Argo Rollouts 的产品化方案

Alauda Container Platform Registry : 与平台用户权限深度集成

基于 KEDA 的自动扩缩容方案

跨集群应用灾备方案（Alpha）

依赖组件全面升级，提升稳定性与安全性

虚拟化功能增强，提升业务连续性与安全性

基于 COSI v2 的对象存储服务，提供更灵活高效的存储管理

ALB 进入维护模式

使用 ingress-nginx 提供 Ingress 能力

Kube-OVN 支持新型高可用多活出口网关

支持 AdminNetworkPolicy 类型的集群网络策略

弃用与移除功能

移除 Docker Runtime

移除模板应用

4.1.2

修复的问题

- global 集群升级后，未升级的业务集群中所有 Applications 以及各种类型的 Workloads 的监控面板将无法正常显示监控数据。

已知问题

- 通过 YAML 创建应用时使用 defaultMode 字段导致应用创建失败。
操作路径：容器平台 → 应用管理 → 应用列表 → 通过 YAML 创建（Create from YAML），当提交的 YAML 文件中包含 defaultMode 字段（通常用于 ConfigMap/Secret 的卷挂载权限配置）时，应用创建会失败并返回校验错误。
解决方案：创建应用前手动移除 YAML 中所有 defaultMode 声明。
- 当 Helm Chart 中设置了 pre-delete post-delete hook。
执行删除模板应用，卸载 Chart 时，遇到某些原因导致 hook 执行失败，进而导致应用无法删除。需要排查原因，并优先解决 hook 执行失败的问题。

4.1.1

修复的问题

- 修复了在平台升级前执行 `violet push` 导致功能组件异常、阻塞升级的问题。现已将推送镜像与创建 CR 分离，用户可选择仅推送镜像而不创建 CR。

已知问题

- global 集群升级后，未升级的业务集群中所有 Applications 以及各种类型的 Workloads 的监控面板将无法显示正常显示监控数据。
- 通过 YAML 创建应用时使用 defaultMode 字段导致应用创建失败。
操作路径：容器平台 → 应用管理 → 应用列表 → 通过 YAML 创建（Create from YAML），当提交的 YAML 文件中包含 defaultMode 字段（通常用于 ConfigMap/Secret 的卷挂载权限配置）时，应用创建会失败并返回校验错误。
解决方案：创建应用前手动移除 YAML 中所有 defaultMode 声明。
- 当 Helm Chart 中设置了 pre-delete post-delete hook。
执行删除模板应用，卸载 Chart 时，遇到某些原因导致 hook 执行失败，进而导致应用无法删除。需要排查原因，并优先解决 hook 执行失败的问题。

4.1.0

新功能与增强

Immutable Infrastructure

发布：

- **Alauda Container Platform DCS Infrastructure Provider**
- **Alauda Container Platform Kubeadm Provider**

两个插件均为 *Agnostic* 生命周期，异步随 Alauda Container Platform (ACP) 发布。

- **DCS Infrastructure Provider** 实现了 Cluster API Infrastructure Provider 接口，集成华为数据中心虚拟化解决方案（DCS）。
- **Kubeadm Provider** 在基础设施提供的虚拟机上安装并配置 Kubernetes 控制平面和节点。

这两个插件共同实现了在 DCS 上的全自动集群管理。

文档正在准备中，发布后将同步上线。

Machine Configuration

发布：**Alauda Container Platform Machine Configuration**

生命周期：*Agnostic*，异步随 ACP 发布。

Machine Configuration 管理集群节点的文件更新、systemd 单元和 SSH 公钥，提供：

- `MachineConfig` CRD，用于向主机写入配置。
- `MachineConfigPool` CRD，根据角色标签分组管理节点配置。
- 集群安装时自动创建两个默认的 `MachineConfigPool`，分别对应控制平面节点和工作节点。用户也可按需创建自定义 `MachineConfigPool`。

系统持续监控配置漂移，受影响节点会被标记为 *Degraded*，直到问题解决。

详细功能请参见 [Machine Configuration](#)。

etcd Encryption

发布：**Alauda Container Platform etcd Encryption Manager**

生命周期：*Agnostic*，异步随 ACP 发布。

为工作负载集群提供基于 AES-GCM 的 etcd 数据加密密钥周期性轮换，支持无缝重加密和密钥重载，且保持对最近 8 个密钥的向后兼容。

详情请参见 [etcd Encryption](#)。

Kubernetes Certificates Rotator

发布：**Alauda Container Platform Kubernetes Certificates Rotator**

生命周期：*Agnostic*，异步随 ACP 发布。

实现 Kubernetes 组件证书的自动轮换。

详情请参见 [Automated Kubernetes Certificate Rotation](#)。

Cluster Enhancement

发布：**Alauda Container Platform Cluster Enhancer**

生命周期：*Aligned*。

新功能及变更：

- **etcd 备份**：将 etcd 备份功能从 Backup & Recovery 迁移至 Cluster Enhancer，因使用场景和实现差异。优化部署方式，避免配置变更和升级时冲突。
- **事件清理**：实现对过期 Kubernetes 事件的主动清理，防止事件在 etcd 中积累，降低 etcd 负载及重启时不稳定风险。
- **证书监控**：将证书管理转为证书监控，配合告警规则和监控面板，替代原有证书管理功能。采用更高效的监控方式，同时监控 kube-apiserver 使用的回环证书。
- **集群监控面板迁移**：将集群监控资源从 `chart-cpaas-monitor` 迁移至 Cluster Enhancer。
- **集群详情图表迁移**：集群详情中的监控图表切换为自定义监控面板。

中文语言包

中文语言支持已与平台解耦，作为 **Chinese Language Pack** 插件发布。平台默认安装为英文，需中文支持时可安装该插件。

创建本地集群

从 ACP 4.1 起，创建本地集群仅支持平台提供的最新 Kubernetes 版本，替代之前可选的四个 Kubernetes 版本。

日志

- 升级 ClickHouse 至 v25.3。
- 应用日志新增 `POD IP` 标签，支持按 `POD IP` 过滤。
- 优化标准输出日志采集，时间戳字段改为日志实际打印时间，替代采集组件时间，确保日志按正确顺序展示。

监控

- 升级 Prometheus 至 v3.4.2。
- 自定义变量支持三种类型：常量、下拉列表和文本框。
 - 常量：固定值，不变。
 - 下拉列表：从预定义列表中选择。
 - 文本框：用户手动输入。
- 统计图表新增图形模式，选中时间段下方显示趋势曲线。
- 值映射支持正则表达式和特殊值。
- 图表面板支持复制，方便在当前监控面板内复用。

租户管理

- 项目配额支持自定义资源配额和存储类配额。
- 插件新增指标：`cpaas_project_resourcequota` 和 `cpaas_project_resourcequota_aggregated`，可用于监控面板展示项目配额。
 - `cpaas_project_resourcequota`：每个集群均可用。
 - `cpaas_project_resourcequota_aggregated`：`global` 集群可用，聚合所有集群数据。
- 自定义角色新增权限限制，仅允许分配对应角色类型内的权限：
 - 平台角色：可分配所有权限。
 - 项目角色：仅可分配平台预设 `project-admin-system` 角色范围内权限。
 - 命名空间角色：仅可分配平台预设 `namespace-admin-system` 角色范围内权限。
 - 不允许分配当前用户未拥有的权限。

安全 Pod 运行的自动 UID/GID 分配方案

Kubernetes 支持为每个命名空间配置专用的用户 ID (UID) 和组 ID (GID) 范围。用户在该命名空间内部署 Pod 时，系统会根据命名空间的安全策略自动为 Pod 内所有容器设置 RunAsUser 和 fsGroup，UID/GID 动态分配自该命名空间授权的范围。

核心能力与价值：

- 增强安全性：强制容器以非特权用户身份运行，限制 UID/GID 范围，有效防止容器逃逸和权限提升，遵循最小权限原则。

- 简化管理：开发者无需在每个容器或 Pod 配置中手动指定 UID/GID，命名空间配置后所有 Pod 自动继承正确安全设置。
- 确保合规：帮助客户满足内部安全策略和外部合规要求，保障容器化应用运行在受控环境。

使用方法：

- 在命名空间添加标签 `security.cpaas.io/enabled`。

基于 Argo Rollouts 的产品化方案

基于开源 Argo Rollouts 的产品化方案，赋能用户对发布流程进行精细化控制。通过渐进式和可控的发布策略，最大限度减少新功能或版本上线带来的业务中断或失败风险，显著降低发布风险。

核心能力与价值：

- 蓝绿发布：实现零停机更新，新版本与现有生产环境并行部署，测试完成后可即时或快速切换流量。
- 金丝雀发布：逐步引入新版本，将少量（如 5%）生产流量导向新版本，观察性能和稳定性。基于预设指标（如错误率、延迟）自动调整流量或回滚，限制潜在问题影响范围。
- 平台认证 **Argo Rollout Chart**：可直接下载社区开源 Argo Rollouts，或通过 Alauda Cloud 获取平台认证版本。

Alauda Container Platform Registry：与平台用户权限深度集成

为提供更安全便捷的镜像管理体验，轻量级镜像仓库与平台现有用户权限体系深度集成。

核心能力与价值：

- 与平台用户体系深度集成：镜像仓库无缝集成平台用户认证和基于角色的访问控制（RBAC）。开发、测试和管理员可直接使用现有平台账号，无需额外配置或独立账号管理。平台自动将用户在命名空间的权限映射为镜像仓库的访问权限，例如用户仅能在其有权限的“特定命名空间”中推拉镜像。
- 更顺畅的命令行操作：支持通过 CLI 工具进行镜像的 `pull` 和 `push` 操作，大幅提升操作效率和便利性。

注意：

- 仅支持通过方案安装 Alauda Container Platform Registry。

基于 KEDA 的自动扩缩容方案

平台提供基于 KEDA（Kubernetes Event-driven Autoscaling）的自动扩缩容方案，使应用智能响应实际负载。

核心能力与价值：

- 事件驱动弹性伸缩：KEDA 支持 70 多种类型的扩缩容器（如 Deployment、Job 等），除传统 CPU 和内存利用率外，还能监控消息队列长度（Kafka、RabbitMQ）、数据库连接数、HTTP 请求率及自定义指标。
- 平台认证 **KEDA Operator**：可通过 Alauda Cloud 下载并安装平台认证版本。

方案：

- 提供基于 Prometheus 指标的自动扩缩容方案和缩容至零方案。

跨集群应用灾备方案（Alpha）

平台新增基于 GitOps 的跨集群应用灾备（DR）方案，显著提升应用弹性和可用性。

核心能力与价值：

- 多样化灾备模型：灵活支持全球高并发需求的 Active-Active（AA-DR）、优化资源利用的 Active-Standby 双活（AS-DR）、以及严格保证数据一致性的 Active-Passive（AP-DR）。
- 自动化 **GitOps** 同步：结合 ApplicationSet 和 Kustomize，实现跨集群配置自动同步，确保灾备环境始终处于就绪状态。
- 灵活流量管理：利用第三方 DNS 和 GSLB 功能，实现智能健康检查驱动流量重定向和快速故障切换，最大限度减少服务中断。
- 多维度数据同步：提供数据库级、存储级和应用级等多种同步方案指导，确保集群间数据最终一致，为业务连续性奠定基础。
- 简化故障切换流程：明确故障检测、流量切换、状态提升和服务恢复等详细步骤，保障灾难发生时高效有序切换。

注意：

- 灾备方案中的数据同步部分与客户业务特性和数据量密切相关，实际实施需针对具体场景做专项处理。

依赖组件全面升级，提升稳定性与安全性

本次发布升级以下核心组件：

- KubeVirt 升级至 v1.5.2
- Ceph 升级至 18.2.7
- MinIO 升级至 RELEASE.2025-06-13T11-33-47Z

其他开源依赖同步至社区最新版本，修复大量已知问题和安全漏洞，确保系统稳定可靠。

虚拟化功能增强，提升业务连续性与安全性

基于虚拟化环境的实际应用需求，本次更新引入多项关键增强：

- 高可用迁移：节点故障时自动将虚拟机迁移至健康节点，保障业务不中断。
- 虚拟机克隆：快速从现有虚拟机创建新虚拟机，大幅提升部署效率。
- 虚拟机模板：支持将现有虚拟机转为模板，实现类似配置环境的快速批量部署。
- 可信计算（**vTPM**）：虚拟机支持可信计算功能，增强整体安全性。

详细使用说明和操作指南已更新至用户手册。

基于 **COSI v2** 的对象存储服务，提供更灵活高效的存储管理

容器对象存储接口（COSI）升级至 v2（alpha），带来以下改进：

- 多集群访问：支持同时访问多个不同的 Ceph 或 MinIO 存储集群，实现更高效的集中管理。
- 细粒度配额管理：支持针对不同存储类别灵活设置配额，优化资源利用。
- 权限管理增强：支持创建多种用户访问权限，包括读写、只读和只写模式。
- 匿名访问支持：Ceph COSI 驱动新增匿名访问功能，通过 Ingress 配置实现快速外部 HTTP 程序访问。

ALB 进入维护模式

WARNING

ALB 将停止新功能开发，仅提供维护和安全修复。4.1 版本支持 ingress-nginx，4.2 版本支持 Envoy Gateway。

未来规划：

- ingress 用户直接使用 ingress-nginx
- 新功能仅支持 GatewayAPI
- 除非有强需求（如项目端口分配），避免提及 ALB 专属功能

GatewayAPI 当前不支持的 **ALB** 专属功能：

- 基于端口的网关实例分配
- 基于 IP 和 IP 范围的流量转发
- EWMA 负载均衡算法
- WAF 使用
- 规则级监控视图

使用 ingress-nginx 提供 Ingress 能力

引入社区主流 Ingress 控制器实现，替代现有基于 ALB 的 Ingress 场景。

核心能力与价值：

- 兼容主流社区实践，避免沟通歧义
- Ingress UI 支持自定义注解，利用 ingress-nginx 丰富扩展能力
- 修复安全问题

Kube-OVN 支持新型高可用多活出口网关

新出口机制解决了之前集中式网关的局限性。新出口网关具备：

- 通过 ECMP 实现 Active-Active 高可用，支持水平吞吐扩展
- 通过 BFD 实现亚秒级故障切换
- 复用底层模式，出口网关 IP 与节点解耦
- 通过命名空间选择器和 Pod 选择器实现细粒度路由控制

- 支持通过节点选择器灵活调度出口网关

支持 **AdminNetworkPolicy** 类型的集群网络策略

Kube-OVN 支持社区新集群网络策略 API，允许集群管理员无需在每个命名空间配置即可强制执行网络策略。

相较于之前集群网络策略的优势：

- 社区标准 API（替代内部 API）
- 与 NetworkPolicy 无冲突（优先级高于 NetworkPolicy）
- 支持优先级设置

更多信息请参见：[Red Hat Blog on AdminNetworkPolicy](#) ↗

弃用与移除功能

移除 **Docker Runtime**

- 之前平台虽非新集群默认运行时，但仍提供 Docker 运行时镜像。自 ACP 4.1 起，默认不再提供 Docker 运行时镜像。

移除模板应用

- **Application** → **Template Application** 入口已正式移除。请确保所有模板应用在升级前已升级为“Helm Chart Application”。