Menu

# Обзор

## Архитектура

## Примечания к выпуску

# Архитектура

## Содержание



## Функциональная перспектива

Alauda Container Platform ( ACP ) включает в себя полный набор функций, состоящий из **ACP Core** и расширений, основанных на двух технических стеках: **Operator** и **Cluster Plugin**.

- **ACP Core**

  Минимальная поставляемая единица ACP , обеспечивающая основные возможности, такие как управление кластерами, оркестрация контейнеров, проекты и администрирование пользователей.

  - Соответствует самым высоким стандартам безопасности
  - Обеспечивает максимальную стабильность
  - Предлагает самый длительный жизненный цикл поддержки

- **Расширения**

  Расширения в стеках Operator и Cluster Plugin можно классифицировать следующим образом:

- **Aligned** – стратегия жизненного цикла, состоящая из нескольких потоков поддержки, синхронизированных с ACP .
- **Agnostic** – стратегия жизненного цикла, состоящая из нескольких потоков поддержки, выпускаемых независимо от ACP .

Подробнее о расширениях см. в разделе Extend.

---

# Перспектива развертывания

ACP состоит из `global` **кластера** и одного или нескольких **кластеров нагрузки**.

- `global` **Кластер**
  - Центральный узел для управления мультикластерной средой
  - Все кластеры должны быть зарегистрированы в `global` перед управлением ими
  - Хостит функциональность мультикластерного и кросс-кластерного взаимодействия
  - Kubernetes развёрнут и управляется платформой
- **Кластер нагрузки**
  - Хостит пользовательские нагрузки и сервисы
  - Kubernetes может быть развернут платформой или предоставлен сторонними поставщиками
  - Поддерживает Kubernetes-сервисы от основных облачных провайдеров, а также кластеры Kubernetes, соответствующие CNCF
  - В некоторых сценариях `global` кластер может также хостить бизнес-нагрузки

---

# Техническая перспектива

**Выполнение компонентов платформы**
Все компоненты платформы работают в контейнерах внутри кластера управления Kubernetes ( `global` кластера).

### Архитектура высокой доступности

- `global` кластер обычно состоит минимум из трёх узлов управления и нескольких рабочих узлов
- Высокая доступность etcd является ключевым элементом HA кластера; подробности см. в разделе *Key Component High Availability Mechanisms*
- Балансировка нагрузки может обеспечиваться внешним балансировщиком или самостоятельно созданным VIP внутри кластера

### Маршрутизация запросов

- Клиентские запросы сначала проходят через балансировщик нагрузки или самостоятельно созданный VIP
- Запросы перенаправляются на **ALB** (стандартный Kubernetes Ingress Gateway платформы), работающий на выделенных ingress-узлах (или на узлах управления, если настроено)
- ALB маршрутизирует трафик к целевым подам компонентов согласно настроенным правилам

### Стратегия реплик

- Основные компоненты работают минимум с двумя репликами
- Ключевые компоненты (например, registry, MinIO, ALB) работают с тремя репликами

### Отказоустойчивость и самовосстановление

- Обеспечивается взаимодействием kubelet, kube-controller-manager, kube-scheduler, kube-proxy, ALB и других компонентов
- Включает проверки здоровья, переключение при сбоях и перенаправление трафика

### Хранение данных и восстановление

- Конфигурация управляющей плоскости и состояние платформы хранятся в etcd как ресурсы Kubernetes
- В случае катастрофических сбоев восстановление возможно из снимков etcd

### Основное / резервное аварийное восстановление

- Два отдельных `global` кластера: **Primary Cluster** и **Standby Cluster**

- Механизм аварийного восстановления основан на синхронизации данных etcd в реальном времени с Primary Cluster на Standby Cluster
- Если Primary Cluster становится недоступен из-за сбоя, сервисы могут быстро переключиться на Standby Cluster

## Механизмы высокой доступности ключевых компонентов

**etcd**

- Развёрнут на трёх (или пяти) узлах управления
- Использует протокол RAFT для выбора лидера и репликации данных
- Развёртывание на трёх узлах выдерживает отказ одного узла; на пяти узлах — отказ двух
- Поддерживает локальные и удалённые резервные копии снимков S3

**Компоненты мониторинга**

- **Prometheus**: несколько экземпляров, дедупликация с помощью Thanos Query и кросс-региональная избыточность
- **VictoriaMetrics**: кластерный режим с распределёнными компонентами VMStorage, VMInsert и VMSelect

**Компоненты логирования**

- **Nevermore** собирает логи и данные аудита
- **Kafka / Elasticsearch / Razor / Lanaya** развёрнуты в распределённом и мульти-репликативном режиме

**Сетевые компоненты (CNI)**

- **Kube-OVN / Calico / Flannel** достигают HA с помощью безсостоянных DaemonSet или компонентов управляющей плоскости с тройной репликацией

**ALB**

- Operator развёрнут с тремя репликами, включён выбор лидера
- Проверки здоровья на уровне экземпляров и балансировка нагрузки

**Самостоятельно созданный VIP**

- Высокодоступный виртуальный IP на базе Keepalived
- Поддерживает обнаружение heartbeat и переключение active-standby

**Harbor**

- Балансировка нагрузки на базе ALB
- PostgreSQL с Patroni HA
- Redis в режиме Sentinel
- Безсостоянные сервисы развёрнуты с несколькими репликами

**Registry и MinIO**

- Registry развёрнут с тремя репликами
- MinIO в распределённом режиме с кодированием с удалением ошибок, избыточностью данных и автоматическим восстановлением

# Примечания к выпуску

## Содержание

---

# 4.1.1

## Исправленные ошибки

- Fixed an issue where running `violet push` before upgrading caused functional components to become abnormal, blocking the upgrade. The command has been enhanced to separate image push and CR creation, allowing users to push only images without creating CRs.

## Известные проблемы

No issues in this release.

---

# 4.1.0

## Новые возможности и улучшения

### Immutable Infrastructure

Выпущено:

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

Оба плагина имеют *Agnostic* жизненный цикл и выпускаются асинхронно с Alauda Container Platform (ACP).

- **DCS Infrastructure Provider** реализует интерфейс Cluster API Infrastructure Provider, интегрируясь с Huawei Datacenter Virtualization Solution (DCS).
- **Kubeadm Provider** устанавливает и настраивает Kubernetes control plane и узлы на BM, предоставленных инфраструктурным провайдером.

Вместе эти плагины обеспечивают полностью автоматизированное управление кластерами на DCS.

Документация находится в разработке и будет опубликована в онлайн-документации после релиза.

## Machine Configuration

Выпущено: **Alauda Container Platform Machine Configuration**
Жизненный цикл: *Agnostic*, выпускается асинхронно с ACP.

Machine Configuration управляет обновлениями файлов, systemd unit-ами и публичными SSH ключами на узлах кластера, предоставляя:

- CRD `MachineConfig` для записи конфигураций на хосты.
- CRD `MachineConfigPool` для группировки и управления конфигурациями узлов на основе ролей.
- При установке кластера автоматически создаются два стандартных MachineConfigPool — для узлов control plane и для рабочих узлов. Пользователи также могут создавать кастомные MachineConfigPool по необходимости.

Система постоянно отслеживает отклонения конфигураций, помечая затронутые узлы как *Degraded* до устранения проблемы.

Подробности по функционалу см. в разделе Machine Configuration.

## etcd Encryption

Выпущено: **Alauda Container Platform etcd Encryption Manager**
Жизненный цикл: *Agnostic*, выпускается асинхронно с ACP.

Обеспечивает периодическую ротацию ключей шифрования данных etcd в рабочих кластерах с использованием AES-GCM для секретов и configmaps. Поддерживает бесшовное пере-шифрование и перезагрузку ключей без прерывания рабочих нагрузок, сохраняя обратную совместимость с последними 8 ключами.

Подробности см. в разделе etcd Encryption.

## Kubernetes Certificates Rotator

Выпущено: **Alauda Container Platform Kubernetes Certificates Rotator**
Жизненный цикл: *Agnostic*, выпускается асинхронно с ACP.

Обеспечивает автоматическую ротацию сертификатов, используемых компонентами Kubernetes.

Подробности см. в разделе Automated Kubernetes Certificate Rotation.

## Cluster Enhancement

Выпущено: **Alauda Container Platform Cluster Enhancer**
Жизненный цикл: *Aligned*.

Новые функции и изменения:

- **etcd Backup**: Функционал резервного копирования etcd перенесён из Backup & Recovery в Cluster Enhancer из-за различий в использовании и реализации. Оптимизирован метод развертывания для предотвращения конфликтов при изменениях конфигурации и обновлениях.
- **Event Cleanup**: Реализована активная очистка устаревших событий Kubernetes вне etcd, чтобы предотвратить их накопление, снизить нагрузку на etcd и риски нестабильности при перезапусках.
- **Certificate Monitoring**: Управление сертификатами преобразовано в мониторинг сертификатов с правилами оповещений и дашбордами, заменяя прежний функционал управления сертификатами. Внедрён более эффективный подход мониторинга, включая мониторинг loopback сертификатов, используемых kube-apiserver.
- **Миграция дашбордов мониторинга кластера**: Ресурсы мониторинга кластера перенесены из `chart-cpaas-monitor` в Cluster Enhancer.
- **Миграция графиков в деталях кластера**: Мониторинговые графики в деталях кластера переключены на кастомные дашборды.

## Китайский языковой пакет

Поддержка китайского языка отделена от платформы и выпущена как плагин **Chinese Language Pack**. По умолчанию платформа устанавливается на английском языке; пользователи могут установить этот плагин при необходимости поддержки китайского языка.

## Создание On-Premise кластера

Начиная с ACP 4.1, создание on-premise кластеров поддерживает только последнюю версию Kubernetes, предоставляемую платформой, заменяя прежнюю возможность выбора из четырёх версий Kubernetes.

## Логирование

- Обновлён ClickHouse до версии v25.3.
- Добавлены теги `POD IP` в логи приложений, что позволяет фильтровать по `POD IP`.
- Улучшен сбор логов стандартного вывода: поле временной метки теперь отражает фактическое время вывода лога, а не время сбора компонентом, что обеспечивает корректный порядок отображения логов.

## Мониторинг

- Обновлён Prometheus до версии v3.4.2.
- Пользовательские переменные теперь поддерживают три типа: Constant, Custom и Textbox.
  - **Constant:** фиксированное значение, не изменяется.
  - **Custom:** значение, выбранное из предопределённого списка.
  - **Textbox:** значение, вводимое вручную пользователем.
- Stat Chart теперь поддерживает режим Graph, отображающий трендовую кривую за выбранный период под статистикой.
- Value Mapping теперь поддерживает регулярные выражения и специальные значения.
- Панели теперь можно копировать, что позволяет дублировать панель внутри текущего дашборда.

## Управление арендаторами

- Квоты проектов теперь поддерживают кастомные квоты ресурсов и квоты по классам хранения.
- Плагин предоставляет новые метрики: `cpaas_project_resourcequota` и `cpaas_project_resourcequota_aggregated`, которые можно использовать для отображения квот проектов на дашбордах.
  - `cpaas_project_resourcequota`: доступна в каждом кластере.
  - `cpaas_project_resourcequota_aggregated`: доступна в кластере `global` и агрегирует данные со всех кластеров.
- Для кастомных ролей введены дополнительные ограничения, позволяющие назначать права только в пределах соответствующего типа роли:
  - **Platform Role:** может назначать все права.
  - **Project Role:** может назначать только права в рамках предустановленной платформой роли `project-admin-system`.
  - **Namespace Role:** может назначать только права в рамках предустановленной платформой роли `namespace-admin-system`.
  - Права, которыми не обладает текущий пользователь, назначать нельзя.

## Автоматическое выделение UID/GID для безопасного запуска Pod

В Kubernetes можно настроить выделенный диапазон User ID (UID) и Group ID (GID) для каждого Namespace. При развертывании Pod в таком Namespace автоматически устанавливаются RunAsUser и fsGroup для всех контейнеров Pod согласно предопределённым политикам безопасности Namespace. Эти пользователи и группы динамически выделяются из разрешённого диапазона UID/GID для данного Namespace.

**Основные возможности и преимущества**:

- **Повышенная безопасность**: Принудительный запуск контейнеров от имени непривилегированных пользователей с ограничением диапазонов UID/GID эффективно снижает риски побега из контейнера и повышения привилегий, соблюдая принцип наименьших привилегий.
- **Упрощённое управление**: Разработчикам не нужно вручную указывать UID/GID в конфигурациях контейнеров или Pod. После настройки Namespace все Pod автоматически наследуют и применяют корректные настройки безопасности.

- **Обеспечение соответствия**: Помогает заказчикам лучше соответствовать внутренним политикам безопасности и внешним требованиям комплаенса, гарантируя запуск контейнеризированных приложений в контролируемой среде.

**Использование**:

- Добавьте метку `security.cpaas.io/enabled` в ваш Namespace.

## Продуктовое решение на базе Argo Rollouts

Наше продуктовое решение, построенное на open-source Argo Rollouts, предоставляет пользователям тонкий контроль над процессами релиза. Реализуя прогрессивные и контролируемые стратегии развертывания, оно минимизирует бизнес-прерывания и сбои при запуске новых функций или версий, значительно снижая риски релиза.

**Основные возможности и преимущества**:

- **Blue-Green Deployment**: Обновления без простоя за счёт параллельного развертывания новой версии вместе с текущей продуктивной средой. После тщательного тестирования трафик мгновенно или быстро переключается с старой версии на новую.
- **Canary Deployment**: Пошагенное внедрение новой версии путём направления небольшой части (например, 5%) трафика в продуктиве, что позволяет наблюдать за её производительностью и стабильностью. На основе предопределённых метрик (ошибки, задержки) система может автоматически увеличить трафик или откатить изменения, ограничивая влияние возможных проблем.
- **Платформенно-сертифицированный Argo Rollout Chart**: Можно скачать open-source Argo Rollouts из сообщества или выбрать сертифицированную платформой версию через Alauda Cloud.

## Alauda Container Platform Registry: глубокая интеграция с системой прав пользователей платформы

Для обеспечения более безопасного и удобного управления образами мы углубили интеграцию нашего лёгкого реестра образов с существующей системой прав пользователей платформы.

**Основные возможности и преимущества**:

- **Глубокая интеграция с системой пользователей платформы**: Реестр образов тесно интегрирован с аутентификацией пользователей и RBAC платформы. Разработчики, тестировщики и администраторы могут использовать существующие учётные данные платформы без дополнительной настройки или отдельного управления аккаунтами. Платформа автоматически сопоставляет права пользователей в Namespace с соответствующими правами доступа к образам в реестре. Например, пользователи могут пушить и пуллить образы только в "конкретных Namespaces", к которым имеют доступ.

- **Удобство работы через CLI**: Поддерживаются операции `pull` и `push` образов через CLI-инструменты, значительно повышая эффективность и удобство работы.

**Внимание**:

- Поддерживается установка Alauda Container Platform Registry только через решение.

## Решение автоскейлинга на базе KEDA

Для обеспечения интеллектуального реагирования приложений на реальную нагрузку наша платформа предлагает решение автоскейлинга на базе KEDA (Kubernetes Event-driven Autoscaling).

**Основные возможности и преимущества**:

- **Эластичное масштабирование на основе событий**: KEDA поддерживает более 70 типов скейлеров для автоматического масштабирования приложений (Deployments, Jobs и др.). Помимо традиционного CPU и памяти, может мониторить длину очередей сообщений (Kafka, RabbitMQ), количество подключений к базе данных, скорость HTTP-запросов и кастомные метрики.

- **Платформенно-сертифицированный KEDA Operator**: Скачивайте и устанавливайте сертифицированную платформой версию через Alauda Cloud.

**Решения**:

- Продукт предлагает два варианта: автоскейлинг на основе метрик Prometheus и масштабирование до нуля.

## Решение для аварийного восстановления приложений между кластерами (Alpha)

Платформа теперь предлагает новое GitOps-решение для аварийного восстановления приложений между кластерами (DR), значительно повышающее устойчивость и доступность приложений.

**Основные возможности и преимущества**:

- **Разнообразные модели DR**: Гибкая поддержка Active-Active (AA-DR) для глобальных задач с высокой конкуренцией; Active-Standby Dual-Active (AS-DR) для оптимизации использования ресурсов; Active-Passive (AP-DR) для строгого обеспечения согласованности данных.
- **Автоматическая синхронизация GitOps**: Использование GitOps в сочетании с ApplicationSet и Kustomize для автоматизации синхронизации конфигураций между кластерами, обеспечивая постоянную готовность DR-среды.
- **Гибкое управление трафиком**: Использование сторонних DNS и GSLB для интеллектуального перенаправления трафика с проверкой здоровья и быстрого переключения при сбоях, минимизируя прерывания сервиса.
- **Многомерная синхронизация данных**: Решение предлагает рекомендации по различным методам — на уровне базы данных, хранилища и приложений — для обеспечения конечной согласованности данных между кластерами, создавая основу для непрерывности бизнеса.
- **Упрощённый процесс переключения**: Чётко определены шаги для обнаружения сбоев, перенаправления трафика, повышения статуса и восстановления сервиса, обеспечивая эффективное и упорядоченное переключение при аварии.

**Примечание**:

- Синхронизация данных в решении DR тесно связана с бизнес-особенностями и объёмом данных заказчика, поэтому может существенно различаться. Реализация требует индивидуального подхода под конкретный сценарий заказчика.

## Комплексное обновление зависимостей для повышения стабильности и безопасности

В этом релизе обновлены следующие ключевые компоненты:

- KubeVirt обновлён до версии v1.5.2
- Ceph обновлён до версии 18.2.7

- MinIO обновлён до RELEASE.2025-06-13T11-33-47Z

Другие open-source зависимости также синхронизированы с последними версиями сообщества, устранены многочисленные известные проблемы и уязвимости, что обеспечивает улучшенную стабильность и надёжность системы.

## Улучшенные возможности виртуализации для повышения непрерывности бизнеса и безопасности

Исходя из практических требований к виртуализации, в этом обновлении реализованы ключевые улучшения:

- **Миграция с высокой доступностью**: Автоматический перенос виртуальных машин на здоровые узлы при сбоях, обеспечивая непрерывность бизнеса.
- **Клонирование виртуальных машин**: Быстрое создание новых виртуальных машин на основе существующих, значительно повышая эффективность развертывания.
- **Шаблоны виртуальных машин**: Поддержка преобразования существующих виртуальных машин в шаблоны для быстрого пакетного развертывания однотипных сред.
- **Доверенные вычисления (vTPM)**: Виртуальные машины теперь поддерживают функции доверенных вычислений, повышая общую безопасность.

Подробные инструкции и рекомендации по новым функциям обновлены в руководстве пользователя.

## Объектное хранилище на базе COSI v2 обеспечивает более гибкое и эффективное управление

Container Object Storage Interface (COSI) обновлён до версии v2 (alpha), включая следующие улучшения:

- **Мультикластерный доступ**: Поддержка одновременного доступа к нескольким различным кластерам Ceph или MinIO, обеспечивая более эффективное централизованное управление.
- **Тонкое управление квотами**: Позволяет гибко задавать квоты для различных категорий хранения, оптимизируя использование ресурсов.

- **Расширенное управление правами доступа**: Поддержка создания различных прав доступа пользователей, включая режимы чтения-записи, только чтение и только запись.
- **Поддержка анонимного доступа**: Ceph COSI Driver теперь поддерживает анонимный доступ, позволяя быстро организовать внешний HTTP-доступ через конфигурацию Ingress.

## ALB переходит в режим поддержки

> **WARNING**
>
> ALB прекращает разработку новых функций и будет получать только исправления безопасности и поддержки. Версия 4.1 поддерживает ingress-nginx, а версия 4.2 — Envoy Gateway.

**Планы на будущее**:

- Для пользователей ingress использовать напрямую ingress-nginx
- Новые функции будут поддерживаться только на GatewayAPI
- Избегать упоминания ALB, если нет жёстких требований к эксклюзивным возможностям ALB (например, выделение портов проекта)

**В настоящее время неподдерживаемые эксклюзивные функции ALB в GatewayAPI**:

- Выделение экземпляров gateway на основе портов
- Перенаправление трафика по IP и диапазонам IP
- Алгоритм балансировки нагрузки EWMA
- Использование WAF
- Мониторинг на уровне правил

## Использование ingress-nginx для предоставления возможностей Ingress

Внедрён самый популярный в сообществе контроллер Ingress для замены существующих сценариев Ingress на базе ALB.

**Основные возможности и преимущества**:

- Совместимость с основными практиками сообщества для избежания недопониманий
- UI Ingress поддерживает кастомные аннотации для использования богатых расширенных возможностей ingress-nginx
- Исправления проблем безопасности

**Kube-OVN поддерживает новый высокодоступный мультиактивный Egress Gateway**

Новый механизм Egress решает ограничения прежних централизованных шлюзов. Новый Egress Gateway обладает:

- Активной-активной высокой доступностью через ECMP для горизонтального масштабирования пропускной способности
- Переключением менее чем за 1 секунду с помощью BFD
- Повторным использованием underlay режима, IP Egress Gateway отделены от узлов
- Тонким контролем маршрутизации через селекторы Namespace и Pod
- Гибким планированием Egress Gateway через селекторы узлов

## Поддержка политики сети кластера типа AdminNetworkPolicy

Kube-OVN поддерживает новый API политики сети кластера сообщества. Этот API позволяет администраторам кластера применять сетевые политики без настройки в каждом Namespace.

**Преимущества по сравнению с предыдущими политиками сети кластера**:

- Стандартный API сообщества (заменяет внутренние API)
- Не конфликтует с NetworkPolicy (имеет более высокий приоритет)
- Поддержка настройки приоритетов

Подробнее: Red Hat Blog on AdminNetworkPolicy ↗

# Устаревшие и удалённые функции

## Удаление Docker Runtime

- Ранее платформа предоставляла образы Docker runtime, хотя он не был дефолтным для новых кластеров. Начиная с ACP 4.1, образы Docker runtime больше не предоставляются по умолчанию.

## Удаление Template Application

- Точка входа **Application → Template Application** официально удалена. Пожалуйста, убедитесь, что все Template Applications обновлены до "Helm Chart Application" перед обновлением.