Обзор

Архитектура

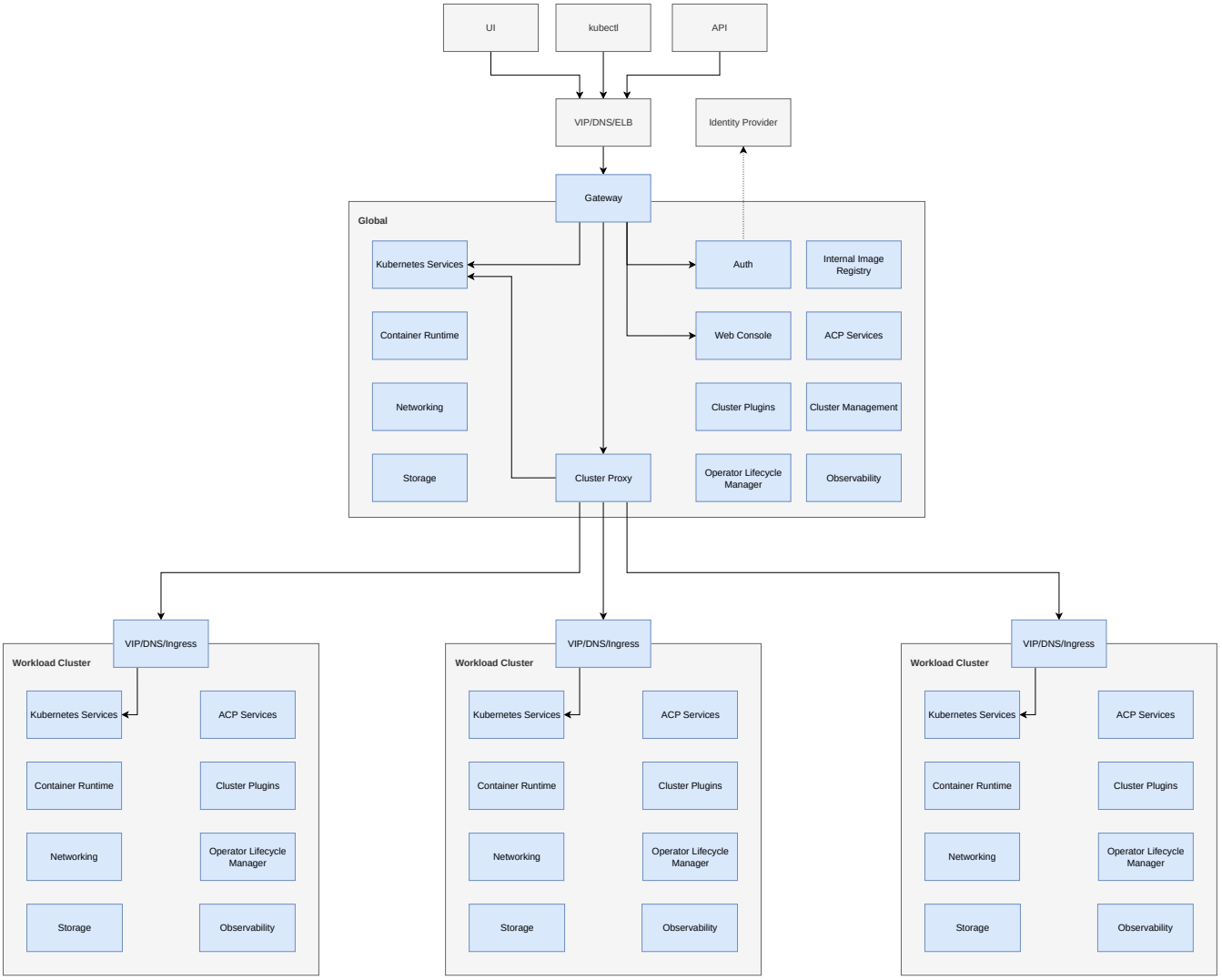
Содержание

Введение в Alauda Container Platform

Alauda Container Platform (ACP) предоставляет платформу корпоративного уровня на базе Kubernetes, которая позволяет организациям последовательно создавать, развертывать и управлять приложениями в гибридных и мультиоблачных средах. ACP объединяет базовые возможности Kubernetes с расширенными сервисами управления, наблюдаемости и безопасности, предлагая единое управляющее плоскостное пространство и гибкие кластеры рабочих нагрузок.

Архитектура построена по модели **hub-and-spoke** и состоит из кластера `global` и нескольких кластеров рабочих нагрузок. Такая схема обеспечивает централизованное управление при независимом выполнении рабочих нагрузок и масштабируемость.

Для канонических определений общеплатформенных терминов, таких как кластер `global`, workload cluster и cluster plugin, см. Глоссарий.



Основные архитектурные компоненты

Кластер Global

Кластер `global` служит централизованным узлом управления и контроля ACP. Он предоставляет общеплатформенные сервисы, такие как аутентификация, управление политиками, операции жизненного цикла кластеров и наблюдаемость. Кроме того, он

является центральным узлом для управления несколькими кластерами и обеспечивает межкластерную функциональность.

Ключевые компоненты включают:

- **Gateway**
  Выступает основным точкой входа в платформу. Он обрабатывает API-запросы от UI, CLI (kubectl) и средств автоматизации, направляя их в соответствующие backend-сервисы.
- **Authentication and Authorization (Auth)**
  Интегрируется с внешними Identity Providers (**IdPs**) для обеспечения Single Sign-On (SSO) и контроля доступа на основе RBAC.
- **Web Console**
  Предоставляет веб-интерфейс для ACP. Он взаимодействует с platform APIs через gateway.
- **Cluster Management**
  Отвечает за регистрацию, provisioning и управление жизненным циклом workload clusters.
- **ACP Services**
- **Operator Lifecycle Manager (OLM) and Cluster Plugins**
  Управляет установкой, обновлениями и жизненным циклом operators и расширений кластера.
- **Internal Image Registry**
  Предоставляет встроенный out-of-box репозиторий образов контейнеров с доступом на основе ролей.
- **Observability**
  Обеспечивает централизованные logging, metrics и tracing для кластера `global` и workload clusters.
- **Cluster Proxy**
  Обеспечивает безопасную связь между кластером `global` и workload clusters.

Workload Cluster

Workload clusters — это среды на базе Kubernetes, управляемые кластером `global`. Каждый workload cluster запускает изолированные приложения и наследует политики

управления и конфигурацию от центральной control plane.

Внешние интеграции

- **Identity Provider (IdP)**
  Поддерживает федеративную аутентификацию через стандартные протоколы (OIDC, SAML) для унифицированного управления пользователями.
- **API and CLI Access**
  Пользователи могут взаимодействовать с ACP через RESTful APIs, web console или command-line tools, такие как `kubectl` и `ac`.
- **Load Balancer (VIP/DNS/SLB)**
  Обеспечивает high availability и распределение трафика для Gateway и ingress endpoints кластера `global` и workload Clusters.

Масштабируемость и высокая доступность

ACP спроектирован с учетом горизонтальной масштабируемости и высокой доступности:

- Каждый компонент может быть развернут в резервированном виде, чтобы исключить single point of failure.
- Кластер `global` поддерживает управление десятками и сотнями workload clusters.
- Workload clusters могут масштабироваться независимо в зависимости от потребностей рабочей нагрузки.
- Использование VIP/DNS/Ingress обеспечивает бесшовную маршрутизацию и failover.

Функциональный взгляд

Полная функциональность Alauda Container Platform (ACP) состоит из **ACP Core** и расширений на основе двух технических стеков: **Operator** и **Cluster Plugin**.

- **ACP Core**

Минимальная поставляемая единица ACP, обеспечивающая базовые 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

- **Extensions**
  Расширения в стеках Operator и Cluster Plugin можно классифицировать как:

  - **Aligned** — стратегия жизненного цикла, состоящая из нескольких maintenance streams и согласованная с ACP.
  - **Agnostic** — стратегия жизненного цикла, состоящая из нескольких maintenance streams и выпускаемая независимо от ACP.

  Подробнее о расширениях см. Расширить.

Технический взгляд

Среда выполнения компонентов платформы
Все компоненты платформы запускаются как контейнеры в Kubernetes management cluster (кластер `global`).

Архитектура высокой доступности

- Кластер `global` обычно состоит как минимум из трех control plane nodes и нескольких worker nodes
- Высокая доступность etcd имеет ключевое значение для HA кластера; подробности см. в *Key Component High Availability Mechanisms*
- Балансировка нагрузки может обеспечиваться внешним load balancer или самостоятельно реализованным VIP внутри кластера

Маршрутизация запросов

- Запросы клиентов сначала проходят через load balancer или самостоятельно реализованный VIP

- Запросы перенаправляются на **ALB** (Kubernetes Ingress Gateway по умолчанию платформы), работающий на выделенных ingress nodes (или control-plane nodes, если это настроено)
- ALB направляет трафик к целевым pod-ам компонентов в соответствии с настроенными правилами

Стратегия репликации

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

Отказоустойчивость и самовосстановление

- Обеспечивается совместной работой kubelet, kube-controller-manager, kube-scheduler, kube-proxy, ALB и других компонентов
- Включает проверки работоспособности, failover и перенаправление трафика

Хранение данных и восстановление

- Конфигурация control plane и состояние платформы хранятся в etcd как ресурсы Kubernetes
- В случае катастрофических сбоев восстановление может быть выполнено из снимков etcd

Аварийное восстановление Primary / Standby

- Два отдельных кластера `global`: **Primary Cluster** и **Standby Cluster**
- Механизм аварийного восстановления основан на синхронизации данных etcd в реальном времени из Primary Cluster в Standby Cluster.
- Если Primary Cluster становится недоступен из-за сбоя, службы можно быстро переключить на Standby Cluster.

Механизмы обеспечения высокой доступности ключевых компонентов

etcd

- Развертывается на трех (или пяти) control plane nodes
- Использует протокол RAFT для выбора лидера и репликации данных
- Развертывания с тремя узлами выдерживают отказ до одного узла; развертывания с пятью узлами — до двух
- Поддерживает локальное и удаленное резервное копирование снимков в S3

Компоненты мониторинга

- **Prometheus**: несколько экземпляров, дедупликация с Thanos Query и межрегиональная избыточность
- **VictoriaMetrics**: кластерный режим с распределенными компонентами VMStorage, VMInsert и VMSelect

Компоненты журналирования

- **Nevermore** собирает логи и audit data
- **Kafka / Elasticsearch / Razor / Lanaya** развертываются в распределенном режиме и с несколькими репликами

Сетевые компоненты (CNI)

- **Kube-OVN / Calico / Flannel**: обеспечивают HA через stateless DaemonSets или control plane components с тремя репликами

ALB

- Operator развернут с тремя репликами, включен leader election
- Проверки состояния на уровне экземпляров и балансировка нагрузки

Самостоятельно реализованный VIP

- Высокодоступный virtual IP на базе Keepalived
- Поддерживает heartbeat detection и active-standby failover

Harbor

- Балансировка нагрузки на базе ALB
- PostgreSQL с HA на базе Patroni

- Режим Redis Sentinel
- Stateless services развертываются в нескольких репликах

Registry и MinIO

- Registry развертывается с тремя репликами
- MinIO в распределенном режиме с erasure coding, избыточностью данных и автоматическим восстановлением

Kubernetes Support Matrix

Этот документ содержит матрицу поддержки версий Kubernetes для ACP. Эта информация имеет решающее значение при создании кластеров, обновлении ACP и управлении сторонними кластерами.

Содержание

Overview

ACP поддерживает несколько версий Kubernetes в разных выпусках ACP. Понимание поддерживаемых версий важно для:

- **Создания кластеров** – Определение, какие версии Kubernetes можно использовать при создании новых кластеров
- **Обновления ACP** – Обеспечение соответствия всех рабочих кластеров требованиям совместимости перед обновлением глобального кластера

- **Управления сторонними кластерами** – Проверка, что кластеры Kubernetes в публичных облаках или совместимые с CNCF находятся в поддерживаемом диапазоне управления

Version Support Matrix

В следующей таблице показана поддержка версий Kubernetes для каждого выпуска ACP.

> **INFO**
>
> В таблице указаны минорные версии ACP без разделения по патч-версиям. Патч-версии включают только исправления ошибок и обновления безопасности, поэтому минорные версии Kubernetes остаются одинаковыми во всех патч-версиях одного минорного выпуска.
>
> **Начиная с ACP 4.1**, каждый выпуск ACP поддерживает только **одну версию Kubernetes** для создания кластера. Это обеспечивает согласованность и упрощает процесс обновления для новых кластеров.

ACP Version	Supported for Cluster Creation	Compatible Versions
ACP 4.3	1.34	1.34, 1.33, 1.32, 1.31
ACP 4.2	1.33	1.33, 1.32, 1.31, 1.30
ACP 4.1	1.32	1.32, 1.31, 1.30, 1.29
ACP 4.0	1.31, 1.30, 1.29, 1.28	1.31, 1.30, 1.29, 1.28

ACP 4.3 Notes

- В ACP 4.3 добавлена поддержка Kubernetes 1.34 для сценариев с управляемыми платформой кластерами.
- При обновлении до ACP 4.3 совместимые версии для рабочих кластеров: 1.34, 1.33, 1.32 и 1.31.

- Это означает, что среды, обновляющиеся с ACP 4.0 до ACP 4.3, могут сохранять рабочие кластеры на Kubernetes с версиями от 1.31 до 1.34 при обновлении глобального кластера.

Third-Party Cluster Management Range

- Для сторонних кластеров ACP 4.3 принимает версии Kubernetes в диапазоне `>=1.19.0 <1.35.0`.
- Этот диапазон управления отличается от столбца Compatible Versions, который является авторитетным требованием для обновления глобального кластера ACP.
- Документация продукта продолжает указывать только версии Kubernetes, прошедшие валидацию продукта для поддержки сторонних кластеров и базовой линии Extend по умолчанию.
- Валидация продукта для базовой линии Extend охватывает следующие области возможностей:
  - Установка и использование Operators
  - Установка и использование Cluster Plugins
  - Логирование на базе ClickHouse
  - Мониторинг на базе VictoriaMetrics
- Это не означает, что все конкретные Operators или Cluster Plugins покрываются валидацией продукта.
- Для конкретных Operators или Cluster Plugins вне этой базовой линии обращайтесь к соответствующей документации продукта или в техническую поддержку.

Upgrade Requirements

Для ACP 4.3 и новее рабочие кластеры должны оставаться в пределах задокументированного диапазона совместимых версий перед обновлением глобального кластера ACP. Для ACP 4.3 это версии Kubernetes с 1.31 по 1.34.

В ACP 4.2 и ранее **все** рабочие кластеры должны быть обновлены до **последней** версии Kubernetes из списка совместимых версий **до** обновления глобального кластера

ACP.

Глоссарий

Этот глоссарий определяет канонические термины, используемые во всей документации Alauda Container Platform. Он сосредоточен на концепциях, которые встречаются в нескольких разделах продукта. Термины, применимые только к одному рабочему процессу или подсистеме, должны оставаться задокументированными на соответствующих локальных страницах.

Содержание

Термины платформы и кластера

Термин	Определение	Связанный документ
Global Cluster	Централизованный узел управления и контроля ACP. В архитектуре hub-and-spoke платформы он	Архитектура

Термин	Определение	Связанный документ
	предоставляет общеплатформенные сервисы, такие как аутентификация, управление политиками, операции жизненного цикла кластеров и наблюдаемость.	
Workload Cluster	Среда на базе Kubernetes, управляемая кластером `global`. На workload cluster запускаются изолированные прикладные нагрузки, и он наследует управление и конфигурацию от центральной control plane.	Архитектура
Platform-Provisioned Infrastructure	Модель управления кластером, в которой платформа предоставляет как машины, так и операционные системы узлов, а также управляет полным жизненным циклом кластера. В этой модели все узлы используют immutable operating system.	Обзор кластеров
User-Provisioned Infrastructure	Модель управления кластером, в которой пользователи предоставляют заранее подготовленные физические или виртуальные машины. Платформа управляет Kubernetes на этих узлах, тогда как управление операционной системой узлов остается под контролем пользователя.	Обзор кластеров
Hosted Control Plane (HCP)	Модель развертывания, в которой у каждого кластера есть собственная выделенная control plane, а несколько control plane размещаются как рабочие нагрузки на выделенном управляющем кластере. Эта модель отделяет control plane от worker nodes, чтобы снизить потребление ресурсов и повысить масштабируемость в multi-cluster сценариях.	О Hosted Control Plane
Managed Cluster	Существующий кластер, включенный в платформу для централизованного управления и операций. В ACP к managed clusters относятся существующие стандартные Kubernetes clusters и выбранные	Обзор управляемых кластеров

Термин	Определение	Связанный документ
	публичные cloud clusters, подключаемые через процессы import или registration.	
Immutable OS	Неизменяемая операционная система, используемая для узлов, управляемых платформой, в средах platform-provisioned. Состояние узлов остается согласованным и восстанавливаемым за счет того, что слой операционной системы рассматривается как read-only и управляется централизованно.	Обзор кластеров
Immutable Infrastructure	Модель подготовки и эксплуатации кластера, в которой конфигурации узлов встраиваются в образы и не изменяются после развертывания. Обновления кластера и изменения конфигурации применяются путем замены узлов на новые образы.	Об Immutable Infrastructure
Project	Единица управления платформой, которая изолирует ресурсы и персонал для арендатора или команды. Project может охватывать несколько связанных кластеров и служит границей управления для квот, политик и владения namespaces.	Создание проекта
Namespace	Namespace Kubernetes, которым платформа управляет напрямую или косвенно. В ACP namespace может быть создан внутри project или импортирован в него, чтобы наследовать управление и видимость на уровне project.	Импорт namespaces
Control Plane	Слой управления Kubernetes, который запускает основные компоненты кластера, такие как API server, scheduler и controller manager.	Архитектура
Control Plane Node	Узел, на котором работают компоненты control plane Kubernetes, используемые для управления кластером. Используйте этот термин вместо устаревших альтернатив, таких как "master node".	Архитектура

Термин	Определение	Связанный документ
Worker Node	Узел, на котором выполняются прикладные нагрузки и вспомогательные компоненты платформы. Используйте этот термин вместо устаревших альтернатив, таких как "slave node".	Архитектура

Термины идентификации и доступа

Термин	Определение	Связанный документ
Identity Provider (IdP)	Внешняя система идентификации, которая аутентифицирует пользователей платформы, например LDAP, Active Directory или провайдер OpenID Connect.	Доступ к Web Console
OpenID Connect (OIDC)	Слой идентификации, построенный на OAuth 2.0, который ACP использует в нескольких сценариях аутентификации и авторизации.	Отключение метода PKCE Plain

Термины расширений и упаковки

Термин	Определение	Связанный документ
Operator	Механизм расширения, основанный на custom resources и controllers Kubernetes, который автоматизирует управление жизненным циклом сложных приложений или сервисов. В ACP Operators управляются через Operator Lifecycle Manager.	Operator

Термин	Определение	Связанный документ
Operator Lifecycle Manager (OLM)	Фреймворк управления Operators, который обрабатывает установку, обновления, подписки на каналы, разрешение зависимостей и связанные custom resources, такие как `CatalogSource`, `Subscription` и `InstallPlan`.	Operator
OperatorHub	Интерфейс платформы для поиска, установки, обновления и управления Operators через OLM.	Operator
Cluster Plugin	Механизм расширения платформы для плагинов на основе chart. Cluster plugins управляются через custom resources `ModulePlugin`, `ModuleConfig` и `ModuleInfo`.	Cluster Plugin

Термины сети и доступа

Термин	Определение	Связанный документ
Ingress	Ресурс Kubernetes, который предоставляет HTTP и HTTPS маршруты извне кластера к внутренним сервисам. ACP использует Ingress как одну из основных моделей ввода north-south трафика.	Настройка Ingress
Gateway API	Семейство сетевых API Kubernetes, которое определяет ресурсы, ориентированные на роли, для продвинутой маршрутизации L4 и L7. В ACP Gateway API позиционируется как модель управления трафиком следующего поколения наряду с Service и Ingress.	Обзор сетевых возможностей
Service	В Kubernetes Service — это способ предоставления сетевого приложения, которое работает как один или несколько Pods в кластере. В ACP Service — это базовый примитив для обнаружения сервисов и экспонирования трафика,	Настройка Services

Термин	Определение	Связанный документ
	включая типы `ClusterIP`, `NodePort` и `LoadBalancer`.	
LoadBalancer	Тип Service, который предоставляет Service через внешний load balancer. Обычно для этого требуется либо интеграция с cloud provider, либо отдельный компонент балансировки нагрузки.	Настройка Services
Platform Access Address	Внешний адрес, используемый для доступа к сервисам платформы, таким как web console и platform APIs. Он может совпадать с Cluster Endpoint или быть отдельным адресом для сценариев внешнего доступа.	Установка
Cluster Endpoint	Адрес, который используют компоненты кластера и администраторы для доступа к целевой control plane кластера. Это основной входной адрес для доступа к control plane во время установки и в последующих операциях.	Установка
Self-built VIP	Встроенный вариант virtual IP, используемый, когда для Cluster Endpoint не предоставлен внешний load balancer.	Установка

Термины аварийного восстановления и обновления

Термин	Определение	Связанный документ
Global Cluster Disaster Recovery	Модель аварийного восстановления для кластера `global`, в которой основной global cluster и резервный global cluster поддерживаются в состоянии готовности к failover через синхронизацию данных etcd и согласованные операционные процедуры.	Аварийное восстановление Global Cluster

Термин	Определение	Связанный документ
Cluster Version Operator (CVO)	Процесс обновления на основе Operator и controller, используемый для координации целевой версии, статуса preflight и хода выполнения обновлений `global` и workload cluster.	Обзор обновления

Примечания по использованию

- Используйте эту страницу как канонический источник терминов, общих для всего ACP и встречающихся в нескольких разделах документации.
- Оставляйте разделы `## Terminology` на уровне отдельных страниц для терминов, специфичных для конкретного workflow или подсистемы и не используемых широко во всем продукте.
- Столбец **Term** использует нормализованный стиль отображения для удобства чтения.
- Сохраняйте официальные названия функций, протоколов, меток интерфейса и имен, используемых API, в их официальном написании, например `OperatorHub`, `Platform Access Address`, `ClusterIP`, `Self-built VIP` и `OpenID Connect (OIDC)`.
- Отдавайте предпочтение концепциям продукта, моделям платформы и наиболее важным сквозным терминам вместо общего инженерного словаря.
- При необходимости при первом упоминании раскрывайте аббревиатуру, а затем последовательно используйте сокращение.
- Если термин уже определен Kubernetes или OpenShift, в первую очередь используйте значение, принятое upstream, и добавляйте контекст ACP только при необходимости.

Примечания к выпуску

Содержание

4.3.0

Выпущено: 2026-04-16

Функции и улучшения

Поддержка Kubernetes 1.34

ACP 4.3 добавляет поддержку **Kubernetes 1.34** для сценариев кластеров, управляемых платформой.

Для обновлений до ACP 4.3 совместимыми версиями workload-кластера являются 1.34, 1.33, 1.32 и 1.31. Это требование к совместимой версии определяет, можно ли выполнять обновление кластера `global`, и не связано с диапазоном управления сторонними кластерами.

Дополнительные сведения см. в разделе Kubernetes Support Matrix.

Рабочий процесс обновления кластера на основе CVO

ACP 4.3 представляет рабочий процесс обновления на основе Cluster Version Operator (CVO) для кластеров `global` и workload.

Ключевые возможности:

- Подготовка артефактов обновления и контроллера обновления с помощью `bash upgrade.sh`
- Выполнение предварительных проверок перед запуском

- Запрос обновлений из Web Console или путем обновления `ClusterVersionShadow.spec.desiredUpdate`
- Просмотр условий, результатов предварительных проверок, этапов и истории из `cvsh.status`

ACP CLI также добавляет административные команды, ориентированные на обновление, такие как `ac adm upgrade`, `ac adm upgrade status`, `--to-latest`, `--to` и `--allow-explicit-upgrade`, для запроса обновлений workload-кластера из текущего контекста и устранения неполадок.

Руководство по эксплуатации см. в разделе Upgrade.

Обновление плагинов кластеров без зависимости от кластера

ACP 4.3 добавляет поддержку независимого обновления для cluster plugins, которые используют жизненный цикл `Aligned` или `Agnostic`.

На странице **Cluster Plugins** теперь отображается жизненный цикл плагина, а совместимые плагины можно обновлять независимо со страницы списка или страницы сведений. Плагины `Core` по-прежнему следуют за обновлениями кластера.

Кластеры `global` на основе MicroOS в Huawei DCS

ACP 4.3 позволяет администраторам создавать кластер `global` в Huawei DCS с неизменяемой инфраструктурой на основе MicroOS. Это расширяет модель неизменяемой эксплуатации с workload-кластеров на сценарии установки платформы в DCS.

Дополнительные сведения см. в разделе About Immutable Infrastructure.

Поддержка Huawei Cloud Stack в Immutable Infrastructure

ACP 4.3 добавляет поддержку Immutable Infrastructure для Huawei Cloud Stack (HCS). Документация по провайдеру HCS теперь охватывает обзор провайдера, установку, создание кластера, управление узлами, обновления кластера и API провайдера в составе набора документации Immutable Infrastructure.

Дополнительные сведения см. в разделе About Immutable Infrastructure.

Поддержка VMware vSphere в цикле 4.3

ACP 4.3 начинает внедрение поддержки Immutable Infrastructure для VMware vSphere. Работы по провайдеру теперь отслеживаются в наборе документации Immutable Infrastructure, а сведения об установке для публичного использования и окончательное именование плагина по-прежнему публикуются.

Дополнительные сведения см. в разделе About Immutable Infrastructure.

Новый пункт Preview Next-Gen Console в Web Console

ACP Core теперь предоставляет якорь верхней навигации, необходимый для Web Console нового поколения. Когда Alauda Container Platform Web Console Base установлена на кластере `global`, пользователи в представлениях **Container Platform** и **Administrator** могут открыть новую консоль через пункт **Preview Next-Gen Console** в отдельной вкладке браузера.

Этот сценарий предназначен для постепенной миграции и работает с плагином Web Console Base в кластере `global` и плагином Web Console Collector в workload-кластерах.

Базовый уровень containerd 2.0

ACP 4.3 обновляет базовый уровень runtime платформы до containerd 2.0. Перед обновлением сред, которые используют настроенную конфигурацию containerd, проверьте операционные процедуры, зависящие от runtime.

Расширенный диапазон управления сторонними кластерами

Для сторонних кластеров ACP 4.3 теперь принимает версии Kubernetes в диапазоне `>=1.19.0 <1.35.0`.

Этот диапазон управления не связан с совместимыми версиями Kubernetes, которые используются для определения того, можно ли обновить кластер `global`.

В продуктовой документации по-прежнему публикуются только те версии Kubernetes, которые прошли продуктовую валидацию для поддержки сторонних кластеров и базового уровня Extend по умолчанию.

Продуктовая валидация для базового уровня Extend охватывает следующие области возможностей:

- Установка и использование Operators
- Установка и использование Cluster Plugins
- Логирование на основе ClickHouse
- Мониторинг на основе VictoriaMetrics

Это не означает, что все конкретные Operators или Cluster Plugins покрыты продуктовой валидацией.

Для конкретных Operators или Cluster Plugins, выходящих за рамки этого базового уровня, обращайтесь к соответствующей продуктовой документации или в техническую поддержку.

Дополнительные сведения см. в разделах Kubernetes Support Matrix и Import Standard Kubernetes Cluster.

Расширенная конфигурация плагинов мониторинга

ACP 4.3 расширяет параметры конфигурации для плагинов мониторинга, упрощая адаптацию развертываний мониторинга к размещению infra-node и различным схемам хранения.

Для ACP Monitoring с VictoriaMetrics администраторы теперь могут:

- Настраивать node selectors и tolerations на уровне плагина для размещения workload на выделенных infra-node
- Настраивать каталог хранения данных для VictoriaMetrics, когда `Storage Type` имеет значение `LocalVolume`
- Удалить прежнее ограничение в три узла для развертываний VictoriaMetrics

Для ACP Monitoring с Prometheus администраторы теперь могут настраивать node selectors и tolerations на уровне плагина, чтобы workload мониторинга можно было размещать на выделенных infra-node через конфигурацию плагина.

WARNING

Если ранее вы использовали patch resources или override-based customization для отдельного задания node selectors или tolerations, после обновления до ACP 4.3 необходимо обновить конфигурацию плагина. После того как обновленная конфигурация плагина вступит в силу, необходимо удалить связанные patch resources или настройки override.

Руководство по эксплуатации см. в разделах Installation и Planning Infra Nodes for Monitoring.

Решение для аварийного восстановления stateful applications между кластерами на основе StatefulSet

В этом выпуске представлены возможности аварийного восстановления между кластерами для stateful applications. Основанное на архитектуре Active-Passive с двумя центрами, оно сочетает асинхронную синхронизацию данных **Alauda Build of VolSync** и распределение конфигурации **GitOps** для обеспечения failover с RTO на уровне минут.

Ключевые особенности:

- Основной кластер обрабатывает весь трафик `read/write`; резервный кластер поддерживает теплую копию данных через периодические снимки rsync (RPO > 0).
- Поддерживаются три операционных сценария: запланированная миграция, аварийный failover и failback.
- По умолчанию резервный кластер работает с `replicas=0`; ресурсы хранения и вычислений остаются в холодном резерве и не обрабатывают бизнес-трафик.
- Подходит для workload без строгих требований к нулевой потере данных (RPO = 0). Для финансовых или транзакционных core applications вместо этого используйте собственную репликацию базы данных.

Подробнее см. здесь: Cross-Cluster Application Disaster Recovery for Stateful Applications ↗

Улучшения управления образами в Alauda Container Platform Registry

В этом выпуске представлены команды `ac images` и `ac adm prune images`, обеспечивающие полное управление жизненным циклом образов Registry из командной строки.

- `ac get images`: выводит список образов в Registry. Результаты ограничены пространствами имен, к которым у текущего пользователя есть права доступа, с поддержкой фильтрации по namespace и нескольких форматов вывода (`table`, `json`, `yaml`, `wide`).
- `ac delete images`: удаляет один или несколько тегов образов по пути Registry. Встроенные проверки прав доступа к namespace; по умолчанию выполняется в режиме dry-run для предварительного просмотра эффекта, а для фактического удаления требуется `--confirm`.
- `ac adm prune images`: административная команда для удаления манифестов образов, на которые не ссылается ни один Pod кластера. Гибкие политики очистки включают срок хранения, количество сохраняемых объектов, allowlist и область `--all`. При необходимости после очистки запускает Registry GC. Также поддерживает плановую очистку через CronJob.

Подробнее см. здесь: Cluster Image Registry Cleanup: Administrator Guide for Manual and Scheduled Tasks ↗

Alauda Container Platform Project Application Essential (Alpha)

В этом выпуске представлен плагин **Alauda Container Platform Project Application Essential**, созданный на совершенно новой frontend framework **Next-Gen Console**. Развернутый в кластере `global`, он обеспечивает межкластерную оркестрацию applications и полное управление жизненным циклом с точки зрения проекта с полным учетом прав пользователя.

Ключевые особенности:

- **Межкластерная оркестрация**: единое развертывание applications на нескольких member clusters в рамках одного проекта.
- **Полное управление жизненным циклом**: поддерживаются `create`, `update`, `scale`, `rollback`, `delete`, с синхронизацией статуса application между кластерами в реальном времени.
- **Изоляция на уровне проекта**: все операции ограничены границами проекта, что обеспечивает естественную изоляцию между проектами.
- **Учет прав доступа**: строго соблюдаются разрешения RBAC, отображаются только те ресурсы, к которым пользователь авторизован для доступа.

Улучшения underlay и egress gateway

ACP 4.3 расширяет основные возможности сетевого CNI в части доступа к underlay и операций egress gateway.

Ключевые улучшения включают:

- Более продуманную реализацию высокой доступности и быстрого переключения для workload egress gateway, что снижает влияние на сервис во время обслуживания узла или failover.
- Рекомендации по защите ресурсов и поддержку платформы для Pod egress gateway, что помогает снизить риск конфликтов ресурсов узла при всплесках трафика или увеличении числа реплик.
- Поддержку настройки taints для workload egress gateway, что позволяет лучше изолировать размещение на выделенных узлах.
- Поддержку управления VLAN sub-interfaces для underlay NIC.
- Добавлена поддержка редактирования YAML для ресурсов subnet.
- Добавлена поддержка настроек node selector для centralized gateways.
- Добавлена поддержка subnet CRD для сценариев centralized gateway.

Эти улучшения делают ACP более гибкой для сложных корпоративных сетевых сред и упрощают миграцию с более ранних моделей экспонирования на схемы на основе underlay.

Улучшения Gateway API

ACP 4.3 усиливает **Gateway API** как ключевую возможность балансировки нагрузки уровня 7 на платформе.

Ключевые улучшения включают:

- Поддержку сценариев развертывания gateway на основе host-network.
- Поддержку экспонирования сервисов через `metalLB + Envoy Gateway proxy + underlay`, чтобы бизнес-трафик мог обходить management network.
- Поддержку пользовательских VIP-адресов для Gateway API, что помогает сохранять стабильность адресов экспонирования сервисов при пересборках или изменениях

жизненного цикла.

Аварийное восстановление stateful applications с защитой на основе PVC

ACP 4.3 представляет более надежные возможности аварийного восстановления для stateful workload, включая **аварийное восстановление на основе PVC** и поддержку **рабочих процессов резервного копирования и восстановления на основе VolSync** для storage-backed applications, таких как MinIO.

Это улучшение повышает готовность к межкластерному восстановлению для stateful applications и предоставляет более практичный путь защиты для production-сред с высокой интенсивностью использования хранилища.

Улучшения управления хранилищем Ceph

ACP 4.3 улучшает операции с хранилищем и поддержку workload на основе Ceph.

Ключевые улучшения включают:

- Добавлена поддержка размещения дисков в разных Ceph pools через UI.
- Улучшена операционная поддержка сценариев замены дисков Ceph.

Эти изменения повышают эффективность day-2 операций с хранилищем и упрощают эксплуатацию сред на основе Ceph в production.

Улучшения платформы виртуализации

ACP 4.3 предоставляет несколько важных улучшений, связанных с виртуализацией.

Ключевые улучшения включают:

- Улучшенные процессы создания и отображения VM.
- Добавлена поддержка Astra Linux в сценариях, связанных с виртуализацией.
- Добавлена поддержка возможностей multi-NIC и hot-plug NIC для виртуальных машин.

Эти улучшения повышают удобство использования виртуализации и расширяют совместимость guest workload в корпоративных средах.

Устаревшие и удаляемые функции

Вывод из эксплуатации Operation Statistics

Плагины metering и billing теперь находятся в общем доступе и полностью покрывают возможности, ранее предоставлявшиеся функцией Operations Statistics. Поэтому верхнеуровневый пункт **Operations Statistics** в разделе **Platform Management** будет удален.

- Для новых развертываний платформы компоненты Operations Statistics больше не устанавливаются. Если вам нужны возможности metering или billing, используйте плагин **Cost Management**.
- Для обновленных платформ сбор metering в Operations Statistics прекращается после обновления, при этом исторические данные остаются доступными. Если вам нужна очистка или миграция данных, отправьте запрос в техническую поддержку.

Исправленные проблемы

- Fixed an issue where the olm-registry pod would continuously restart, preventing the OperatorHub from functioning properly. This was caused by the `seccompProfile: RuntimeDefault` security configuration added during CIS compliance hardening, which blocked the `clone` syscall required by CGO operations. The seccomp profile has been adjusted to allow necessary syscalls while maintaining security compliance.Fixed in ACP 4.3.0.
- Fixed a performance issue where the permission validation during native application creation became extremely slow (10+ seconds) when the cluster had 60+ operators installed.Fixed in ACP 4.3.0.
- When using the etcd backup feature provided by Alauda Container Platform Cluster Enhancer, if users configure to back up etcd to S3 storage, the plugin fails to retrieve the Secret object referenced in secretRef. The root cause was that the plugin lacked the necessary RBAC permissions to read Secrets, resulting in S3 authentication information retrieval failure. This issue has been fixed in ACP 4.3.0.

- When using Alauda Container Platform Monitoring for VictoriaMetrics with multiple clusters sharing the same Storage, the alert rule cpaas-certificates-rule has two issues: alert notifications do not differentiate between clusters when triggered, and the rule monitors customer secrets instead of only platform certificates.
- Fix metis component storage limit configuration is too small and causes metis container to restart after exceeding the limit
- Fixed the issue where pushing container images with a large number of data layers (over 100) to the built-in image repository failed.
- Fixed an issue where imagePullSecret was not automatically injected when workloads used custom ServiceAccounts, resulting in image pull failures.
- Fixed an issue where Pods could not pull images when image-registry imagePullSecret auto-rotation used “create new Secret + delete old Secret”, and legacy Pods still referenced the old Secret but started only after it had expired.
- Fixed an exception triggered under specific scenarios during namespace creation. When entering the namespace creation page, if the page request response is slow, the default selected cluster information may not be available upon initial page access, triggering errors in other page interfaces and causing the project quotas on the page to fail to display correctly.
- The text in the real-time logging component has been adjusted: Logging has ended => End of logs
- Fixed an issue where line breaks were inconsistent between Windows and Mac when editing configmaps.

Известные проблемы

- When using violet push to upload a chart package, the push operation may complete successfully, but the package does not appear in the public-charts repository.
  Workaround: Push the chart package again.
- When using violet push to upload a chart package, the push operation may complete successfully, but the package does not appear in the public-charts repository.
  Workaround: Push the chart package again.
- Application creation failure triggered by the defaultMode field in YAML.
  Affected Path: Alauda Container Platform → Application Management → Application List → Create from YAML. Submitting YAML containing the defaultMode field (typically used for

ConfigMap/Secret volume mount permissions) triggers validation errors and causes deployment failure.
Workaround: Manually remove all defaultMode declarations before application creation.

- When pre-delete post-delete hook is set in helm chart.
  When the delete template application is executed and the chart is uninstalled, the hook execution fails for some reasons, thus the application cannot be deleted. It is necessary to investigate the cause and give priority to solving the problem of hook execution failure.