Menu

Безопасность

Alauda Container Security

Alauda Container Security

Безопасность и соответствие

Соответствие требованиям

API Refiner

Пользователи и роли

Пользователь

Группа

Роль

IDP

Политика пользователя

Мультиарендность (Project)

Введение

Проект

Пространства имён (Namespaces)

Взаимосвязь между кластерами, проектами и пространствами имён

Руководства

Аудит

Введение

Требования

Процедура

Результаты поиска

Телеметрия

Menu

Alauda Container Security

Alauda Container Security — это комплексное решение для обеспечения безопасности, разработанное для Kubernetes и контейнеризованных сред. Оно предоставляет централизованное управление, автоматизированное сканирование уязвимостей, применение политик и проверки соответствия, помогая организациям защищать свою контейнерную инфраструктуру в нескольких кластерах.

Alauda Container Security использует распределённую архитектуру на основе контейнеров, состоящую из Central Services (для управления, API и UI) и Secured Cluster Services (для мониторинга, применения политик и сбора данных). Оно интегрируется с CI/CD пайплайнами, SIEM, системами логирования и поддерживает встроенный сканер уязвимостей Scanner V4.

Note

Поскольку выпуски Alauda Container Security осуществляются в ином режиме, чем у Alauda Container Platform, документация Alauda Container Security теперь доступна в виде отдельного набора по адресу Alauda Container Security ↗。

Menu

Безопасность и соответствие

Соответствие требованиям

Установка

API Refiner

Введение

Введение в продукт

Преимущества продукта

Сценарии использования

Ограничения

Установка

Шаги установки

Шаги удаления

Конфигурация по умолчанию

Соответствие требованиям

Установка

Menu

Установка

Alauda Compliance с Kyverno

Шаги установки

Шаги удаления

Alauda Compliance с Kyverno

Alauda Compliance с Kyverno — это сервис платформы, который интегрирует Kyverno для управления политиками соответствия на платформе Alauda Container Platform.

Содержание

Шаги установки

1. Перейдите в **Platform Management**
2. В левой навигационной панели нажмите **Marketplace** > **Cluster Plugins**
3. Найдите **Alauda Compliance with Kyverno** и кликните для просмотра деталей
4. Нажмите **Install** для развертывания плагина

Шаги удаления

1. Выполните шаги 1-3 из процесса установки, чтобы найти плагин
2. Нажмите **Uninstall** для удаления плагина

Menu

API Refiner

Введение

Введение в продукт

Преимущества продукта

Сценарии использования

Ограничения

Установка

Шаги установки

Шаги удаления

Конфигурация по умолчанию

Введение

Содержание

Введение в продукт

ACP API Refiner — это сервис фильтрации данных, предоставляемый платформой Alauda Container Platform, который повышает безопасность мультиарендности и изоляцию данных в Kubernetes-средах. Он фильтрует данные ответов Kubernetes API на основе прав пользователя, проектов, кластеров и пространств имён, а также поддерживает фильтрацию на уровне полей, включение и десенситизацию данных.

Преимущества продукта

Основные преимущества ACP API Refiner заключаются в следующем:

- **Многомерная изоляция данных**
  - Поддержка фильтрации ответов API по измерениям проекта, кластера и пространства имён
  - Обеспечение корректных границ данных между разными арендаторами

  - Предотвращение несанкционированного доступа к ресурсам с областью действия кластера

- **Гибкая фильтрация данных**
  - Поддержка исключения, включения и десенситизации конкретных полей в ответах API
  - Настраиваемые правила фильтрации через YAML-конфигурацию
  - Динамическая генерация Ingress для разных типов ресурсов

- **Повышенная безопасность**
  - Реализация аутентификации пользователей на основе JWT-токенов
  - Предоставление тонкой настройки контроля доступа на основе прав пользователя
  - Поддержка десенситизации данных для конфиденциальной информации

Сценарии использования

Основные сценарии применения ACP API Refiner включают:

- **Среда мультиарендности**
  - Обеспечение корректной изоляции данных между разными арендаторами
  - Предотвращение несанкционированного доступа к ресурсам с областью действия кластера
  - Эффективное управление сценариями с общими пространствами имён

- **Защита конфиденциальных данных**
  - Фильтрация конфиденциальной информации из ответов API
  - Поддержка десенситизации данных на уровне полей
  - Защита конфиденциальных метаданных и аннотаций

- **Требования соответствия**
  - Помощь в выполнении требований по изоляции данных

- Поддержка аудита и требований соответствия
- Поддержание границ доступа к данным

Ограничения

К ACP API Refiner применяются следующие ограничения:

- Ресурсы должны содержать определённые метки, связанные с арендатором, для изоляции данных:
  - `cpaas.io/project`
  - `cpaas.io/cluster`
  - `cpaas.io/namespace`
  - `kubernetes.io/metadata.name`
  - Необязательно: `cpaas.io/creator`
- Запросы LabelSelector не поддерживают логическую операцию OR
- Пользовательские привязки на уровне платформы не фильтруются
- Фильтрация применяется только к операциям API GET и LIST

Установка

ACP API Refiner — это сервис платформы, который фильтрует данные ответов Kubernetes API. Он предоставляет возможности фильтрации по проекту, кластеру и namespace, а также поддерживает исключение, включение и десенситизацию полей в ответах API.

Содержание

Шаги установки

1. Перейдите в **Platform Management**
2. В левой навигационной панели нажмите **Marketplace** > **Cluster Plugins**
3. Выберите кластер **global** в верхней навигационной панели
4. Найдите **ACP API Refiner** и нажмите для просмотра деталей
5. Нажмите **Install** для развертывания плагина

Шаги удаления

1. Выполните шаги 1-4 из процесса установки, чтобы найти плагин
2. Нажмите **Uninstall** для удаления плагина

Конфигурация по умолчанию

Фильтруемые ресурсы

По умолчанию фильтруются следующие ресурсы:

Resource	API Version
namespaces	v1
projects	auth.alauda.io/v1
clustermodules	cluster.alauda.io/v1alpha2
clusters	clusterregistry.k8s.io/v1alpha1

Десенситизация полей

По умолчанию десенситизируется следующее поле:

- `metadata.annotations.cpaas.io/creator`

Menu

Пользователи и роли

Пользователь

Введение

Источники пользователей

Правила управления пользователями

Жизненный цикл пользователя

Руководства

Группа

Введение

Введение в группы

Типы групп

Руководства

Роль

Введение

Введение в роли

Системные роли

Пользовательские роли

Руководства

IDP

Введение

Overview

Supported Integration Methods

Руководства

Устранение неполадок

Политика пользователя

Введение

Menu

Пользователь

Введение

Руководства

Управление пользователями

Сброс пароля локального пользователя

Обновление даты истечения срока действия пользователя

Активация пользователя

Отключение пользователя

Добавление пользователя в локальную группу пользователей

Удаление пользователя

Пакетные операции

Введение

Платформа поддерживает аутентификацию пользователей и проверку входа для всех пользователей.

Содержание

Источники пользователей

Локальные пользователи

- Учетная запись администратора, созданная при развертывании платформы
- Учетные записи, созданные через интерфейс платформы
- Пользователи, добавленные через локальный конфигурационный файл dex

Пользователи третьих сторон

LDAP-пользователи

- Корпоративные пользователи, синхронизированные с LDAP-серверов
- Учетные записи импортируются через интеграцию с IDP (Identity Provider)
- Источник отображается как имя конфигурации IDP
- Интеграция настраивается через параметры IDP

OIDC-пользователи

- Пользователи сторонних платформ, аутентифицированные через протокол OIDC
- Источник отображается как имя конфигурации IDP
- Интеграция настраивается через параметры IDP

> **WARNING**
>
> Для OIDC-пользователей, добавленных в проект до их первого входа:
>
> - Источник отображается как "-" до успешного входа в платформу
> - После успешного входа источник меняется на имя конфигурации IDP

Другие пользователи третьих сторон

- Пользователи, аутентифицированные через поддерживаемые коннекторы dex (например, GitHub, Microsoft)
- Для получения дополнительной информации см. официальную документацию dex ↗

Правила управления пользователями

> **WARNING**
>
> Обратите внимание на следующие важные правила:
>
> - Локальные имена пользователей должны быть уникальны среди всех типов пользователей

- Пользователи третьих сторон (OIDC/LDAP) с совпадающими именами автоматически связываются
- Связанные пользователи наследуют права от существующих учетных записей
- Пользователи могут входить через соответствующие источники
- В платформе отображается только одна запись пользователя на имя пользователя
- Источник пользователя определяется по последнему способу входа

Жизненный цикл пользователя

В следующей таблице описаны различные статусы пользователей на платформе:

Статус	Описание
Normal	Учетная запись пользователя активна и может войти в платформу
Disabled	Учетная запись пользователя неактивна и не может войти. Обратитесь к администратору платформы для активации. Возможные причины: - Отсутствие входа в течение 90+ дней подряд - Истечение срока действия учетной записи - Ручное отключение администратором
Locked	Учетная запись временно заблокирована из-за 5 неудачных попыток входа в течение 24 часов. Подробности: - Продолжительность блокировки: 20 минут - Может быть разблокирована вручную администратором - После окончания периода блокировки учетная запись становится доступной
Invalid	Учетная запись, синхронизированная с LDAP, которая была удалена с LDAP-сервера.

Статус	Описание
	Примечание: недействительные учетные записи не могут войти в платформу

Menu

Руководства

Управление ролями пользователей

Добавление ролей

Удаление ролей

Создание пользователя

Шаги

Управление пользователями

Сброс пароля локального пользователя

Обновление даты истечения срока действия пользователя

Активация пользователя

Отключение пользователя

Добавление пользователя в локальную группу пользователей

Удаление пользователя

Пакетные операции

Управление ролями пользователей

Администраторы платформы могут управлять ролями других пользователей (не своей собственной учетной записи), чтобы предоставлять или отзывать разрешения.

Содержание

Добавление ролей

Шаги

1. В левой навигационной панели нажмите **Users** > **User Management**
2. Нажмите на имя пользователя, для которого нужно изменить роли
3. Прокрутите до раздела **Role List**
4. Нажмите **Add Role**
5. В диалоговом окне назначения роли:

- Выберите роль из выпадающего списка **Role Name**
- Выберите область действия разрешений роли (кластер, проект или namespace)
- Нажмите **Add**

NOTE

Важные замечания:

- Вы можете добавить пользователю несколько ролей
- Каждая роль может быть добавлена только один раз для каждого пользователя
- Уже назначенные роли отображаются в выпадающем списке, но выбрать их нельзя
- Роль **Cluster Administrator** нельзя назначить для глобального кластера

Удаление ролей

Шаги

1. В левой навигационной панели нажмите **Users** > **User Management**
2. Нажмите на имя пользователя, для которого нужно изменить роли
3. Прокрутите до раздела **Role List**
4. Нажмите **Remove** рядом с ролью, которую хотите удалить
5. Подтвердите удаление

WARNING

Разрешения на управление ролями:

- Управлять ролями других пользователей могут только администраторы платформы
- Пользователи не могут изменять роли своей собственной учетной записи

Создание пользователя

Пользователи с ролями администратора платформы могут создавать локальных пользователей и назначать им роли через интерфейс платформы.

Содержание

Шаги

1. В левой панели навигации нажмите **Users** > **User Management**
2. Нажмите **Create User**
3. Настройте следующие параметры:

Параметр	Описание
Password Type	Выберите способ генерации пароля: **Random**: Система генерирует безопасный случайный пароль **Custom**: Пользователь вводит пароль вручную
Password	Введите или сгенерируйте пароль в зависимости от выбранного типа. Требования к паролю: - Длина: 8-32 символа - Должен содержать буквы и цифры

Параметр	Описание
	- Должен содержать специальные символы (`~!@#$%^&*() -_=+?`) Функции поля пароля: - Нажмите на иконку глаза для показа/скрытия пароля - Нажмите на иконку копирования для копирования пароля
Mailbox	Электронная почта пользователя: - Должна быть уникальной - Может использоваться как имя пользователя для входа - Связана с именем пользователя
Validity Period	Установите срок действия учетной записи пользователя: Варианты: - **Permanent**: Без ограничения по времени - **Custom**: Установите время начала и окончания с помощью выпадающего списка Time Range
Roles	Назначьте пользователю одну или несколько ролей
Continue Creating	Переключатель для управления поведением после создания: - **On**: Перенаправляет на страницу создания нового пользователя - **Off**: Показывает страницу с деталями созданного пользователя

1. Нажмите **Create**

NOTE

После успешного создания пользователя:

- Если включена опция "Continue Creating", вы будете перенаправлены на создание следующего пользователя
- Если отключена, отобразится страница с деталями созданного пользователя

Управление пользователями

Платформа предоставляет гибкие возможности управления пользователями, поддерживая как индивидуальное управление, так и пакетные операции для повышения эффективности в определённых сценариях (например, для команд на месте или удалённых команд).

WARNING

Важные ограничения:

- Системные учётные записи управлению не подлежат (роль администратора платформы, локальный источник)
- Текущие вошедшие в систему пользователи не могут управлять своими собственными учётными записями
- Для изменения личных данных (отображаемое имя, пароль) используйте страницу личной информации

Содержание

Сброс пароля локального пользователя

Пользователи с правами управления платформой могут сбрасывать пароли других локальных пользователей.

Шаги

1. В левой навигационной панели нажмите **Users** > **User Management**
2. Нажмите на иконку рядом с записью нужного пользователя
3. Нажмите **Reset Password**
4. В диалоговом окне выберите тип пароля:

- **Random**: Система сгенерирует надёжный случайный пароль
- **Custom**: Введите новый пароль вручную

NOTE

Требования к паролю:

- Длина: 8-32 символа
- Должен содержать буквы и цифры
- Должен содержать специальные символы (`~!@#$%^&*() -_=+?`)

Особенности поля пароля:

- Нажмите на иконку глаза для показа/скрытия пароля

- Нажмите на иконку копирования для копирования пароля

1. Нажмите **Reset**

Обновление даты истечения срока действия пользователя

Вы можете обновлять даты истечения срока действия пользователей со статусом **normal**, **disabled** или **locked**. Пользователи, у которых срок действия истёк, будут автоматически отключены.

Шаги

1. В левой навигационной панели нажмите **Users** > **User Management**
2. Нажмите **Update Expiry Date** рядом с нужным пользователем
3. В диалоговом окне выберите опцию даты истечения:

- **Permanent**: Без ограничения по времени
- **Custom**: Установите время начала и окончания с помощью выпадающего списка Time Range

4. Нажмите **Update**

Активация пользователя

Вы можете активировать пользователей со статусом **disabled** или **locked**.

NOTE

Поведение при активации:

- Если пользователь находится в пределах срока действия: дата истечения остаётся без изменений
- Если срок действия пользователя истёк: дата истечения становится **Permanent**

Шаги

1. В левой навигационной панели нажмите **Users** > **User Management**
2. Нажмите **Activate** рядом с нужным пользователем
3. В диалоговом окне подтверждения нажмите **Activate**
4. Статус пользователя изменится на **normal**

Отключение пользователя

Вы можете отключить пользователей со статусом **normal** или **locked** в пределах срока действия. Отключённые пользователи не могут войти в систему, но могут быть повторно активированы.

Шаги

1. В левой навигационной панели нажмите **Users** > **User Management**
2. Нажмите на иконку рядом с нужным пользователем
3. Нажмите **Disable** и подтвердите

Добавление пользователя в локальную группу пользователей

Вы можете добавить пользователей с **Source** равным **Local** или `LDAP` в одну или несколько локальных групп пользователей.

WARNING

Поведение ролей групп:

- Пользователи автоматически наследуют роли своих групп
- Роли групп видны только на странице деталей группы (вкладка Configure Roles)
- Список ролей отдельного пользователя показывает только роли, назначенные напрямую

Шаги

1. В левой навигационной панели нажмите **Users** > **User Management**
2. Нажмите на иконку рядом с нужным пользователем
3. Нажмите **Add to User Group**
4. Выберите одну или несколько локальных групп пользователей
5. Нажмите **Add**

Удаление пользователя

Администраторы платформы могут удалять любых пользователей, кроме текущей вошедшей в систему учётной записи, включая:

- Пользователей, настроенных через IDP
- Пользователей с источником `-`
- Локальных пользователей

Шаги

1. В левой навигационной панели нажмите **Users** > **User Management**
2. Нажмите на иконку рядом с нужным пользователем
3. Нажмите **Delete**
4. Нажмите **Confirm**

Пакетные операции

Вы можете выполнять пакетные операции для:

- Обновления сроков действия
- Активации пользователей
- Отключения пользователей
- Удаления пользователей

Шаги

1. В левой навигационной панели нажмите **Users** > **User Management**
2. Выберите одного или нескольких пользователей с помощью чекбоксов
3. Нажмите **Batch Operations** и выберите действие:

- **Update Validity**
- **Activate**
- **Deactivate**
- **Delete**

NOTE

Подробности пакетных операций:

- **Update Validity**: Установка постоянного или пользовательского временного диапазона
- **Activate**: Подтверждение активации в диалоговом окне
- **Deactivate**: Подтверждение деактивации в диалоговом окне
- **Delete**: Ввод пароля текущей учётной записи и подтверждение

Menu

Группа

Введение

Введение

Введение в группы

Типы групп

Руководства

Управление ролями групп пользователей

Добавление роли группе

Удаление роли из группы

Создание локальной группы пользователей

Создание группы пользователей

Управление группами пользователей

Управление членством в локальной группе пользователей

Предварительные требования

Импорт участников

Удаление участников

Введение

Содержание

Введение в группы

Платформа поддерживает управление пользователями через пользовательские группы. Управляя ролями групп, вы можете эффективно:

- Одновременно предоставлять права на работу с платформой нескольким пользователям
- Одновременно отзывать права у нескольких пользователей
- Реализовывать пакетное управление доступом на основе ролей

Например, при кадровых изменениях в организации, когда необходимо предоставить права на работу с проектом или namespace нескольким пользователям, вы можете:

1. Создать пользовательскую группу
2. Импортировать соответствующих пользователей в члены группы
3. Настроить роли проекта и namespace для группы
4. Применить единые права ко всем членам группы

Типы групп

Платформа поддерживает два типа групп:

Локальная пользовательская группа

- Создаётся непосредственно на платформе
- Источник отображается как **Local**
- Может быть обновлена или удалена
- Поддерживает:
  - Добавление или удаление пользователей из любого источника
  - Добавление или удаление ролей

Синхронизированная с IDP пользовательская группа

- Синхронизируется из подключённого IDP (LDAP, Azure AD)
- Источник отображается как имя подключённого ***IDP***
- Не может быть обновлена или удалена
- Поддерживает:
  - Добавление или удаление ролей
  - Не поддерживает управление членами группы (добавление или удаление)

Menu

Руководства

Управление ролями групп пользователей

Добавление роли группе

Удаление роли из группы

Создание локальной группы пользователей

Создание группы пользователей

Управление группами пользователей

Управление членством в локальной группе пользователей

Предварительные требования

Импорт участников

Удаление участников

Управление ролями групп пользователей

Пользователи с правами управления платформой могут управлять ролями как для локальных групп пользователей, так и для групп пользователей, синхронизированных через IDP.

Содержание

Добавление роли группе

Шаги

1. В левой навигационной панели нажмите **Users** > **User Group Management**
2. Нажмите на название нужной группы пользователей
3. На вкладке **Configure Role** нажмите **Add Role**
4. Нажмите, чтобы добавить роль

NOTE

Правила назначения ролей:

- Вы можете добавить несколько ролей в одну группу

- Каждая роль может быть добавлена в одну группу только один раз

1. Выберите название роли из выпадающего списка
2. Выберите область действия роли (кластер, проект или namespace)
3. Нажмите **Add**

Удаление роли из группы

WARNING

При удалении роли из группы:

- Все права, предоставленные этой ролью членам группы, будут отозваны
- Это действие нельзя отменить

Шаги

1. В левой навигационной панели нажмите **Users** > **User Group Management**
2. Нажмите на название нужной группы пользователей
3. На вкладке **Configure Role** нажмите **Remove** рядом с ролью
4. Нажмите **Confirm** для удаления роли

Создание локальной группы пользователей

Локальные группы пользователей позволяют реализовать управление доступом на основе ролей для нескольких пользователей из любого источника.

Содержание

Создание группы пользователей

Шаги

1. В левой боковой панели нажмите **Users** > **User Group Management**
2. Нажмите **Create User Group**
3. Введите следующую информацию:

- **Name**: Название группы пользователей
- **Description**: Описание назначения группы

4. Нажмите **Create**

Управление группами пользователей

Вы можете управлять группами пользователей, нажав на иконку на странице списка или выбрав **Operations** в правом верхнем углу на странице с деталями.

Операция	Описание
Update User Group	Обновление информации о группе в зависимости от источника группы: - Для групп с **Source** равным `Local` : можно обновить как название, так и описание - Для групп с **Source** равным `IDP name` : можно обновить только описание
Delete Local User Group	Удаление групп пользователей с **Source** равным `Local`

WARNING

При удалении группы:

- Все участники группы будут удалены
- Все роли, назначенные группе, будут удалены
- Это действие нельзя отменить

Управление членством в локальной группе пользователей

Управлять членством в локальных группах пользователей могут только пользователи с правами Platform Management.

Содержание

Предварительные требования

WARNING

Перед управлением членством в группах обратите внимание на следующие ограничения:

- Управлять группами и их участниками могут только пользователи с правами Platform Management
- Системные аккаунты и аккаунты, в данный момент вошедшие в систему, не подлежат управлению (не могут быть импортированы в группы или удалены из них)
- В каждой локальной группе пользователей может быть не более 5000 участников
- При достижении лимита в 5000 участников дальнейший импорт невозможен

Импорт участников

Вы можете импортировать пользователей из платформы в локальные группы пользователей для централизованного управления правами доступа.

TIP

Пользователи, импортированные в группу, автоматически наследуют все операционные права, назначенные этой группе.

Шаги

1. В левой навигационной панели нажмите **Users** > **User Group Management**
2. Нажмите на название локальной группы пользователей, в которую хотите добавить участников
3. На вкладке **Group Member Management** нажмите **Import Member**
4. Выберите одного или нескольких пользователей платформы, отметив флажками их имена пользователей/отображаемые имена
5. Нажмите **Import**

NOTE

- Вы можете выбрать только тех пользователей, которые в данный момент не являются членами группы
- Используйте кнопку **Import All**, чтобы импортировать всех пользователей из списка сразу

Удаление участников

При удалении пользователя из группы все операционные права, предоставленные этому пользователю через группу, автоматически аннулируются.

Шаги

1. В левой навигационной панели нажмите **Users** > **User Group Management**

2. Нажмите на название локальной группы пользователей, из которой хотите удалить участников

3. На вкладке **Group Member Management** можно удалить участников двумя способами:

- Нажать **Remove** рядом с именем участника и подтвердить действие
- Выбрать одного или нескольких участников с помощью флажков, затем нажать **Batch Remove** и подтвердить действие

Menu

Роль

Введение

Введение

Введение в роли

Системные роли

Пользовательские роли

Руководства

Создание роли

Конфигурация основной информации

Конфигурация просмотра

Конфигурация разрешений

Управление пользовательскими ролями

Обновление основной информации

Обновление разрешений роли

Копирование существующей роли

Удаление пользовательской роли

Введение

Содержание

Введение в роли

Управление ролями пользователей на платформе реализовано с помощью Kubernetes RBAC (Role-Based Access Control). Эта система позволяет гибко настраивать права доступа, связывая роли с пользователями.

Роль представляет собой набор разрешений для работы с ресурсами Kubernetes на платформе. Эти разрешения включают:

- Создание ресурсов
- Просмотр ресурсов
- Обновление ресурсов
- Удаление ресурсов

Роли классифицируют и объединяют разрешения для различных ресурсов. Назначая роли пользователям и устанавливая области действия разрешений, можно быстро предоставить права на операции с ресурсами.

Разрешения можно так же легко отозвать, удалив роли у пользователей.

Роль может включать:

- Один или несколько типов ресурсов
- Одно или несколько разрешений на операции
- Несколько назначенных пользователей

Например:

- Роль A: Может только просматривать и создавать проекты
- Роль B: Может создавать, просматривать, обновлять и удалять пользователей, проекты и namespaces

---

Системные роли

Для удовлетворения распространённых сценариев настройки прав доступа платформа предоставляет следующие стандартные системные роли. Эти роли обеспечивают гибкий контроль доступа к ресурсам платформы и эффективное управление правами пользователей.

Название роли	Описание	Уровень роли
Platform Administrator	Имеет полный доступ ко всем бизнес-ресурсам и ресурсам платформы	Platform
Platform Auditors	Может просматривать все ресурсы платформы и записи операций, но не имеет других прав	Platform
Cluster Administrator (Alpha)	Управляет и поддерживает ресурсы кластера с полным доступом ко всем ресурсам уровня кластера	Cluster
Project Administrator	Управляет администраторами namespace и квотами namespace	Project
namespace-admin-system	Управляет участниками namespace и назначениями ролей	Namespace

Название роли	Описание	Уровень роли
Developers	Разрабатывает, развёртывает и поддерживает кастомные приложения внутри namespaces	Namespace

Пользовательские роли

Платформа поддерживает пользовательские роли для расширения сценариев контроля доступа к ресурсам. Пользовательские роли обладают рядом преимуществ по сравнению с системными ролями:

- Гибкая настройка разрешений
- Возможность обновления прав роли
- Опция удаления ролей, когда они больше не нужны

> **WARNING**
>
> Будьте осторожны при обновлении или удалении пользовательских ролей. Удаление пользовательской роли автоматически отзовёт все права, предоставленные этой ролью связанным пользователям.

Menu

Руководства

Создание роли

Конфигурация основной информации

Конфигурация просмотра

Конфигурация разрешений

Управление пользовательскими ролями

Обновление основной информации

Обновление разрешений роли

Копирование существующей роли

Удаление пользовательской роли

Создание роли

Пользователи с разрешениями ролей платформы могут создавать пользовательские роли с разрешениями, которые равны или меньше их собственных разрешений в зависимости от реальных сценариев использования. При создании роли можно настроить:

- Разрешения на операции функциональных модулей платформы
- Разрешения доступа к пользовательским ресурсам (Kubernetes CRD)

Содержание

Конфигурация основной информации

1. В левой навигационной панели нажмите **Users** > **Roles**.
2. Нажмите **Create Role**.
3. Настройте основную информацию роли:

Тип роли

При назначении ролей пользователям область разрешений будет ограничена в зависимости от типа роли:

- **Platform Role**: Отображаются все разрешения платформы
- **Project Role**: Отображаются разрешения в разделах:
  - Project Management
  - Container Platform
  - Service Mesh
  - DevOps
  - Middleware
- **Namespace Role**: Отображаются разрешения в разделах:
  - Project Management
  - Container Platform
  - Service Mesh
  - DevOps
  - Middleware

1. Нажмите **Next**.

Конфигурация просмотра

В разделе конфигурации просмотра вы управляете разрешениями роли на доступ к указанным видам. Виды, которые не выбраны, не будут отображаться в верхней навигации для пользователей с этой ролью.

NOTE

1. Разрешения вашей учетной записи ограничивают, какие карточки видов вы можете настраивать. Например:
   - Если у вашей учетной записи нет разрешения на просмотр **Project Management**
   - Карточка вида **Project Management** будет неактивна при создании роли

- Вы можете создавать роли только с разрешениями, равными или ниже ваших собственных

2. Статус входа в вид:

- Если в функции **Products** у вида отключена опция **Show Entry**
- Разрешения вида в **Permission Configuration** по-прежнему будут действовать
- Вид временно будет недоступен, пока вход не будет включен
- После включения ранее выбранные разрешения будут работать как обычно

Конфигурация разрешений

1. Нажмите **Add Custom Permission** в левом верхнем углу страницы.

2. Настройте разрешения для роли на работу с пользовательскими ресурсами (Kubernetes CRD):

Параметр	Описание
Group Name	Название группы разрешений. Группы отображаются под модулем разрешений в порядке их добавления.
Resource Name	Название ресурса. Нажмите Enter для добавления нескольких названий пользовательских ресурсов.
Operation Permission	Разрешение на выполнение операций с ресурсом.

1. Нажмите **Create**.

Управление пользовательскими ролями

В этом руководстве описывается, как управлять пользовательскими ролями на платформе, включая:

- Обновление основной информации и разрешений
- Копирование существующих ролей для создания новых
- Удаление пользовательских ролей

Содержание

Обновление основной информации

Вы можете обновить отображаемое имя и описание пользовательских ролей на платформе.

Шаги

1. В левой навигационной панели нажмите **Users** > **Roles**
2. Нажмите на имя ***роли, которую нужно обновить***
3. В правом верхнем углу нажмите **Actions** > **Update**
4. Обновите:

- Отображаемое имя роли
- Описание

5. Нажмите **Update**

Обновление разрешений роли

Вы можете обновить информацию о разрешениях пользовательских ролей, включая:

- Добавление новых разрешений на операции с ресурсами платформы
- Удаление существующих разрешений
- Изменение разрешений для пользовательских ресурсов

Шаги

1. В левой навигационной панели нажмите **Users** > **Roles**
2. Нажмите на имя ***роли, которую нужно обновить***
3. В правом верхнем углу области разрешений нажмите **Actions** > **Update Role Permissions**
4. Внесите изменения на странице **Update Role Permissions**
5. Нажмите **Confirm**

Копирование существующей роли

Вы можете создать новую роль, скопировав существующую роль (системную или пользовательскую). Новая роль унаследует всю информацию о разрешениях исходной

роли, которую затем можно изменить в соответствии с вашими потребностями.

WARNING

Разрешения новой роли не могут превышать разрешения роли, к которой принадлежит создатель.

Шаги

1. В левой навигационной панели нажмите **Users** > **Roles**
2. Нажмите на имя ***роли, которую нужно скопировать***
3. В правом верхнем углу нажмите **Actions** > **Copy as new role**
4. На странице **Copy as new role** настройте:

- Имя
- Отображаемое имя
- Описание
- Тип

5. Нажмите **Create**

Удаление пользовательской роли

Вы можете удалить пользовательские роли, которые больше не используются.

WARNING

При удалении пользовательской роли:

- Связи роли с пользователями будут удалены
- Пользователи, назначенные на эту роль, потеряют все разрешения, предоставленные ролью

- Роль будет удалена из списков ролей пользователей

Шаги

1. В левой навигационной панели нажмите **Users** > **Roles**
2. Нажмите на имя ***роли, которую нужно удалить***
3. В правом верхнем углу нажмите **Actions** > **Delete**
4. Введите имя роли для подтверждения удаления
5. Нажмите **Delete**

Menu

IDP

Введение

Введение

Overview

Supported Integration Methods

Руководства

Управление LDAP

Обзор LDAP

Поддерживаемые типы LDAP

Терминология LDAP

Добавление LDAP

Примеры конфигурации LDAP

Синхронизация пользователей LDAP

Соответствующие операции

Управление OIDC

Обзор OIDC

Добавление OIDC

Добавление OIDC через YAML

Соответствующие операции

Устранение неполадок

Удаление пользователя

Описание проблемы

Решение

Введение

Содержание

Overview

Платформа интегрируется с сервисом аутентификации Dex, что позволяет использовать предустановленные коннекторы Dex для аутентификации аккаунтов платформы через настройку IDP. Для получения дополнительной информации обратитесь к официальной документации Dex↗.

Supported Integration Methods

LDAP Integration

Если в вашей организации используется **LDAP** (Lightweight Directory Access Protocol) для управления пользователями, вы можете настроить LDAP на платформе для подключения к LDAP-серверу вашей организации.

Преимущества интеграции LDAP:

- Обеспечивает связь между платформой и LDAP-сервером

- Позволяет пользователям организации входить с использованием LDAP-учетных данных
- Автоматически синхронизирует учетные записи пользователей организации с платформой

OIDC Integration

Платформа поддерживает интеграцию с IDP-сервисами, использующими протокол OpenID Connect (OIDC) для аутентификации пользователей третьих сторон.

Преимущества интеграции OIDC:

- Позволяет пользователям входить с помощью аккаунтов третьих сторон
- Поддерживает корпоративные IDP-сервисы
- Обеспечивает безопасную аутентификацию через протокол OIDC

> **NOTE**
>
> Для аутентификации с использованием других коннекторов, не упомянутых выше, пожалуйста, свяжитесь с технической поддержкой.

Menu

Руководства

Управление LDAP

Обзор LDAP

Поддерживаемые типы LDAP

Терминология LDAP

Добавление LDAP

Примеры конфигурации LDAP

Синхронизация пользователей LDAP

Соответствующие операции

Управление OIDC

Обзор OIDC

Добавление OIDC

Добавление OIDC через YAML

Соответствующие операции

Управление LDAP

Администраторы платформы могут добавлять, обновлять и удалять LDAP-сервисы на платформе.

Содержание

Обзор LDAP

LDAP (Lightweight Directory Access Protocol) — это зрелый, гибкий и хорошо поддерживаемый стандартный механизм взаимодействия с директориями. Он организует данные в иерархическую древовидную структуру для хранения информации о пользователях и организациях предприятия, преимущественно используется для реализации единого входа (SSO).

NOTE

Ключевые особенности LDAP:

- Обеспечивает связь между клиентами и LDAP-серверами
- Поддерживает операции хранения, извлечения и поиска данных
- Обеспечивает возможности аутентификации клиентов
- Способствует интеграции с другими системами

Для получения дополнительной информации обратитесь к официальной документации LDAP ↗.

Поддерживаемые типы LDAP

OpenLDAP

OpenLDAP — это реализация LDAP с открытым исходным кодом. Если в вашей организации используется open-source LDAP для аутентификации пользователей, вы можете настроить платформу для взаимодействия с LDAP-сервисом, добавив LDAP и настроив соответствующие параметры.

NOTE

Интеграция OpenLDAP:

- Обеспечивает аутентификацию пользователей LDAP на платформе
- Поддерживает стандартные протоколы LDAP
- Обеспечивает гибкое управление пользователями

Для получения дополнительной информации об OpenLDAP обратитесь к официальной документации OpenLDAP ↗.

Active Directory

Active Directory — это LDAP-основанное программное обеспечение Microsoft для предоставления служб хранения каталогов в системах Windows. Если в вашей организации используется Microsoft Active Directory для управления пользователями, вы можете настроить платформу для взаимодействия с сервисом Active Directory.

NOTE

Интеграция Active Directory:

- Обеспечивает аутентификацию пользователей AD на платформе
- Поддерживает интеграцию с доменами Windows
- Обеспечивает управление пользователями корпоративного уровня

Терминология LDAP

Общие термины OpenLDAP

Термин	Описание	Пример
dc (Domain Component)	Компонент домена	`dc=example,dc=com`
ou (Organizational Unit)	Организационная единица	`ou=People,dc=example,dc=com`

Термин	Описание	Пример
cn (Common Name)	Общее имя	`cn=admin,dc=example,dc=com`
uid (User ID)	Идентификатор пользователя	`uid=example`
objectClass (Object Class)	Класс объекта	`objectClass=inetOrgPerson`
mail (Mail)	Электронная почта	`mail=example@126.com`
givenName (Given Name)	Имя	`givenName=xq`
sn (Surname)	Фамилия	`sn=ren`
objectClass: groupOfNames	Группа пользователей	`objectClass: groupOfNames`
member (Member)	Атрибут участника группы	`member=cn=admin,dc=example,dc=com`
memberOf	Атрибут членства в группе	`memberOf=cn=users,dc=example,dc=com`

Общие термины Active Directory

Термин	Описание	Пример
dc (Domain Component)	Компонент домена	`dc=example,dc=com`
ou (Organizational Unit)	Организационная единица	`ou=People,dc=example,d`
cn (Common Name)	Общее имя	`cn=admin,dc=example,dc`
sAMAccountName/userPrincipalName	Идентификатор пользователя	`userPrincipalName=exam` `sAMAccountName=example`

Термин	Описание	Пример
objectClass: user	Класс объекта пользователя AD	`objectClass=user`
mail (Mail)	Электронная почта	`mail=example@126.com`
displayName	Отображаемое имя	`displayName=example`
givenName (Given Name)	Имя	`givenName=xq`
sn (Surname)	Фамилия	`sn=ren`
objectClass: group	Группа пользователей	`objectClass: group`
member (Member)	Атрибут участника группы	`member=CN=Admin,DC=exa`
memberOf	Атрибут членства в группе	`memberOf=CN=Users,DC=e`

Добавление LDAP

TIP

После успешной интеграции LDAP:

- Пользователи могут входить на платформу с использованием своих корпоративных учетных записей
- Множественное добавление одного и того же LDAP перезапишет ранее синхронизированных пользователей

Предварительные требования

Перед добавлением LDAP подготовьте следующую информацию:

- Адрес LDAP-сервера
- Имя пользователя администратора
- Пароль администратора
- Другие необходимые параметры конфигурации

Шаги

1. В левой навигационной панели нажмите **Users** > **IDPs**
2. Нажмите **Add LDAP**
3. Настройте следующие параметры:

Основная информация

Параметр	Описание
Server Address	Адрес доступа к LDAP-серверу (например, `192.168.156.141:31758`)
Username	DN администратора LDAP (например, `cn=admin,dc=example,dc=com`)
Password	Пароль учетной записи администратора LDAP
Login Box Username Prompt	Сообщение-приглашение для ввода имени пользователя (например, "Пожалуйста, введите ваше имя пользователя")

Настройки поиска

NOTE

Назначение настроек поиска:

- Соответствие LDAP-записям пользователей по заданным условиям

- Извлечение ключевых атрибутов пользователей и групп
- Отображение атрибутов LDAP на атрибуты пользователей платформы

Параметр	Описание
Object Type	ObjectClass для пользователей: - OpenLDAP: `inetOrgPerson` - Active Directory: `organizationalPerson` - Группы: `posixGroup`
Login Field	Атрибут, используемый в качестве имени пользователя для входа: - OpenLDAP: `mail` (адрес электронной почты) - Active Directory: `userPrincipalName`
Filter Conditions	Условия фильтра LDAP для фильтрации пользователей/групп Пример: `(&(cn=John*)(givenName=*xq*))`
Search Starting Point	Базовый DN для поиска пользователей/групп (например, `dc=example,dc=org`)
Search Scope	Область поиска: - `sub`: весь поддерево каталога - `one`: один уровень ниже начальной точки
Login Attribute	Уникальный идентификатор пользователя: - OpenLDAP: `uid` - Active Directory: `distinguishedName`
Name Attribute	Атрибут имени объекта (по умолчанию: `cn`)
Email Attribute	Атрибут электронной почты: - OpenLDAP: `mail` - Active Directory: `userPrincipalName`
Group Member Attribute	Идентификатор участника группы (по умолчанию: `uid`)

Параметр	Описание
Group Attribute	Атрибут связи с группой пользователей (по умолчанию: `memberuid`)

4. В разделе **IDP Service Configuration Validation**:

   - Введите действительное имя пользователя и пароль LDAP-аккаунта
   - Имя пользователя должно совпадать с настройкой **Login Field**
   - Нажмите для проверки конфигурации

5. (Опционально) Настройте **LDAP Auto-Sync Policy**:

   - Включите переключатель **Auto-Sync Users**
   - Установите правила синхронизации
   - Используйте онлайн-инструмент↗ для проверки выражений CRON

6. Нажмите **Add**

> **NOTE**
>
> После добавления LDAP:
>
> - Пользователи могут входить до синхронизации
> - Информация о пользователях синхронизируется автоматически при первом входе
> - Автоматическая синхронизация происходит согласно настроенным правилам

Примеры конфигурации LDAP

Конфигурация LDAP-коннектора

Ниже приведён пример настройки LDAP-коннектора:

```yaml
apiVersion: dex.coreos.com/v1
kind: Connector
id: ldap        # Connector ID
name: ldap      # Connector display name
type: ldap      # Connector type is LDAP
metadata:
  name: ldap
  namespace: cpaas-system
spec:
  config:
    # LDAP server address and port
    host: ldap.example.com:636
    # DN and password for the service account used by the connector.
    # This DN is used to search for users and groups.
    bindDN: uid=serviceaccount,cn=users,dc=example,dc=com
    # Service account password, required when creating a connector.
    bindPW: password

    # Login account prompt. For example, username
    usernamePrompt: SSO Username

    # User search configuration
    userSearch:
      # Start searching from the base DN
      baseDN: cn=users,dc=example,dc=com
      # LDAP query statement, used to search for users.
      # For example: "(&(objectClass=person)(uid=<username>))"
      filter: (&(objectClass=organizationalPerson))

      # The following fields are direct mappings of user entry attributes.
      # User ID attribute
      idAttr: uid
      # Required. Attribute to map to email
      emailAttr: mail
      # Required. Attribute to map to username
      nameAttr: cn
      # Login username attribute
      # Filter condition will be converted to "(<attr>=<username>)", such as
(uid=example).
      username: uid

      # Extended attributes
      # phoneAttr: phone
```

```
    # Group search configuration
    groupSearch:
      # Start searching from the base DN
      baseDN: cn=groups,dc=freeipa,dc=example,dc=com
      # Group filter condition
      # "(&(objectClass=group)(member=<user uid>))".
      filter: "(objectClass=group)"
      # User group matching field
      # Group attribute
      groupAttr: member
      # User group member attribute
      userAttr: uid
      # 组显示名称
      nameAttr: cn
```

Примеры фильтров пользователей

```
# 1. Базовый фильтр: Найти всех пользователей
(&(objectClass=person))

# 2. Комбинация нескольких условий: Найти пользователей в конкретном отделе
(&(objectClass=person)(departmentNumber=1000))

# 3. Найти активных пользователей (Active Directory)
(&(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

# 4. Найти пользователей с определённым доменом электронной почты
(&(objectClass=person)(mail=*@example.com))

# 5. Найти участников конкретной группы
(&(objectClass=person)(memberOf=cn=developers,ou=groups,dc=example,dc=com))

# 6. Найти недавно вошедших пользователей (Active Directory)
(&(objectClass=user)(lastLogon>=20240101000000.0Z))

# 7. Исключить системные аккаунты
(&(objectClass=person)(!(uid=admin))(!(uid=system)))

# 8. Найти пользователей с определённым атрибутом
(&(objectClass=person)(mobile=*))

# 9. Найти пользователей в нескольких отделах
(&(objectClass=person)(|(ou=IT)(ou=HR)(ou=Finance)))

# 10. Пример сложной комбинации условий
(&
  (objectClass=person)
  (|(department=IT)(department=Engineering))
  (!(title=Intern))
  (manager=cn=John Doe,ou=People,dc=example,dc=com)
)
```

Примеры конфигурации поиска групп

```
# 1. Базовый фильтр: Найти все группы
(objectClass=groupOfNames)

# 2. Найти группы с определённым префиксом
(&(objectClass=groupOfNames)(cn=dev-*))

# 3. Найти непустые группы
(&(objectClass=groupOfNames)(member=*))

# 4. Найти группы с определённым участником
(&(objectClass=groupOfNames)(member=uid=john,ou=People,dc=example,dc=com))

# 5. Найти вложенные группы (Active Directory)
(&(objectClass=group)(|(groupType=-2147483646)(groupType=-2147483644)))

# 6. Найти группы с определённым описанием
(&(objectClass=groupOfNames)(description=*admin*))

# 7. Исключить системные группы
(&(objectClass=groupOfNames)(!(cn=system*)))

# 8. Найти группы с определёнными участниками
(&(objectClass=groupOfNames)(|(cn=admins)(cn=developers)(cn=operators)))

# 9. Найти группы в конкретном OU
(&(objectClass=groupOfNames)(ou=IT))

# 10. Пример сложной комбинации условий
(&
  (objectClass=groupOfNames)
  (|(cn=prod-*)(cn=dev-*))
  (!(cn=deprecated-*))
  (owner=cn=admin,dc=example,dc=com)
)
```

Примеры операторов AND(&) и OR(|) в LDAP-фильтрах

```
# Оператор AND (&) - все условия должны быть выполнены
# Синтаксис: (&(condition1)(condition2)(condition3)...)

# Пример AND с несколькими атрибутами
(&
  (objectClass=person)
  (mail=*@example.com)
  (title=Engineer)
  (manager=*)
)

# Оператор OR (|) - должно быть выполнено хотя бы одно условие
# Синтаксис: (|(condition1)(condition2)(condition3)...)

# Пример OR с несколькими атрибутами
(|
  (department=IT)
  (department=HR)
  (department=Finance)
)

# Комбинирование AND и OR
(&
  (objectClass=person)
  (|
    (department=IT)
    (department=R&D)
  )
  (employeeType=FullTime)
)

# Сложная комбинация условий
(&
  (objectClass=person)
  (|
    (&
      (department=IT)
      (title=*Engineer*)
    )
    (&
      (department=R&D)
      (title=*Developer*)
    )
```

```
    )
    (!(status=Inactive))
    (|(manager=*)(isManager=TRUE))
  )
```

Синхронизация пользователей LDAP

После успешной синхронизации пользователей LDAP на платформу вы можете просмотреть синхронизированных пользователей в списке пользователей.

Вы можете настроить политику автоматической синхронизации при добавлении LDAP (которую можно обновить позже) или вручную запустить синхронизацию после успешного добавления LDAP. Ниже описано, как вручную запустить операцию синхронизации.

Примечания:

- Новые пользователи, добавленные в LDAP, интегрированный с платформой, могут войти на платформу до выполнения операции синхронизации пользователей. После успешного входа их информация автоматически синхронизируется с платформой.
- Пользователи, удалённые из LDAP, после синхронизации получат статус `Invalid`.
- По умолчанию срок действия вновь синхронизированных пользователей — **Постоянный**.
- Синхронизированные пользователи с тем же именем, что и существующие пользователи (локальные или IDP), автоматически связываются. Их права и срок действия будут соответствовать существующим пользователям. Они могут входить на платформу, используя метод входа, соответствующий их источнику.

Порядок действий

1. В левой навигационной панели нажмите **Users** > **IDPs**.
2. Нажмите на ***имя LDAP***, для которого хотите выполнить ручную синхронизацию.
3. В правом верхнем углу нажмите **Actions** > **Sync user**.
4. Нажмите **Sync**.

Примечания: Если вы вручную закроете диалоговое окно синхронизации, появится диалог подтверждения закрытия. После закрытия диалога система продолжит синхронизацию пользователей. Если вы остаетесь на странице списка пользователей, получите обратную связь о результате синхронизации. Если покинете страницу списка пользователей, результат синхронизации не будет получен.

Соответствующие операции

Вы можете нажать на
справа на странице списка или нажать **Actions** в правом верхнем углу на странице деталей, чтобы при необходимости обновить или удалить LDAP.

Операция	Описание
Обновить LDAP	Обновить конфигурацию добавленного LDAP или **LDAP Auto-Sync Policy**. **Примечание**: После обновления LDAP пользователи, синхронизированные с платформой через этот LDAP, также будут обновлены. Пользователи, удалённые из LDAP, станут недействительными в списке пользователей платформы. Для очистки мусорных данных выполните операцию очистки недействительных пользователей.
Удалить LDAP	После удаления LDAP все пользователи, синхронизированные с платформой через этот LDAP, получат статус **Invalid** (связь между пользователями и ролями сохраняется), и они не смогут войти на платформу. После повторной интеграции необходимо повторно выполнить синхронизацию для активации пользователей. **Совет**: После удаления IDP, если необходимо удалить пользователей и группы пользователей, синхронизированные с платформой через LDAP, установите флажок **Clean IDP Users and User Groups** под окном подтверждения.

Управление OIDC

Платформа поддерживает протокол OIDC (OpenID Connect), позволяя администраторам платформы входить в систему с использованием сторонних аккаунтов после добавления конфигурации OIDC. Администраторы платформы также могут обновлять и удалять настроенные сервисы OIDC.

Содержание

Обзор OIDC

OIDC (OpenID Connect) — это стандартный протокол аутентификации личности, основанный на протоколе OAuth 2.0. Он использует сервер авторизации OAuth 2.0 для предоставления аутентификации пользователя сторонним клиентам и передачи соответствующей информации об аутентификации личности клиенту.

OIDC позволяет всем типам клиентов (включая серверные, мобильные и JavaScript-клиенты) запрашивать и получать аутентифицированные сессии и информацию о конечном пользователе. Этот набор спецификаций расширяем, что позволяет участникам использовать дополнительные функции, такие как шифрование данных личности, обнаружение OpenID Provider и управление сессиями, когда это имеет смысл.

Для получения дополнительной информации обратитесь к официальной документации OIDC ↗.

Добавление OIDC

Добавив OIDC, вы сможете использовать сторонние аккаунты платформы для входа в платформу.

Примечание: После успешного входа пользователей OIDC в платформу платформа будет использовать атрибут email пользователя в качестве уникального идентификатора. Пользователи сторонних платформ с поддержкой OIDC должны иметь атрибут **email**, иначе они не смогут войти в платформу.

Порядок действий

1. В левой навигационной панели нажмите **Users** > **IDPs**.
2. Нажмите **Add OIDC**.
3. Настройте параметры **Basic Information**.
4. Настройте параметры **OIDC Server Configuration**:
   - **Identity Provider URL**: URL издателя, который является адресом доступа к провайдеру идентификации OIDC.
   - **Client ID**: идентификатор клиента для OIDC клиента.
   - **Client Secret**: секретный ключ для OIDC клиента.
   - **Redirect URI**: адрес обратного вызова после входа в стороннюю платформу, который представляет собой URL издателя dex + `/callback`.
   - **Logout URL**: адрес, который посещает пользователь после выполнения операции **Logout**. Если пусто, адрес выхода будет начальной страницей входа платформы.
5. В области **IDP Service Configuration Validation** введите **Username** и **Password** действительной учетной записи OIDC для проверки конфигурации.

Совет: Если имя пользователя и пароль неверны, при добавлении будет выдана ошибка с указанием недействительных учетных данных, и OIDC не сможет быть добавлен.

6. Нажмите **Create**.

Добавление OIDC через YAML

Помимо настройки через форму, платформа также поддерживает добавление OIDC через YAML, что позволяет более гибко настраивать параметры аутентификации, сопоставления claims, синхронизацию групп пользователей и другие расширенные функции.

Пример: настройка OIDC коннектора

Следующий пример демонстрирует, как настроить OIDC коннектор для интеграции с сервисами аутентификации личности OIDC. Этот пример конфигурации подходит для следующих сценариев:

1. Необходима интеграция OIDC в качестве сервера аутентификации личности.
2. Требуется поддержка синхронизации информации о группах пользователей.
3. Нужно настроить адрес перенаправления после выхода из системы.
4. Нужно настроить конкретные OIDC scopes.
5. Требуется кастомизация сопоставления claims.

```yaml
apiVersion: dex.coreos.com/v1
kind: Connector
# Connector basic information
id: oidc               # Connector unique identifier
name: oidc             # Connector display name
type: oidc             # Connector type is OIDC
metadata:
  annotations:
    cpaas.io/description: "11"  # Connector description
  name: oidc
  namespace: cpaas-system
spec:
  config:
    # OIDC server configuration
    # Configure server connection information, including server address, client credentials, and callback address
    issuer: http://auth.com/auth/realms/master              # OIDC server address
    clientID: dex                                           # Client ID
    # Service account secret key, valid when creating Connector resources for the first time
    clientSecret: xxxxxxx
    redirectURI: https://example.com/dex/callback           # Callback address, must match the address registered by the OIDC client

    # Security configuration
    # Configure SSL verification and user information acquisition method
    insecureSkipVerify: true                                # Whether to skip SSL verification, it is recommended to set to false in a production environment
    getUserInfo: false                                      # Whether to obtain additional user information through the UserInfo endpoint

    # Logout configuration
    # Configure the redirect address after user logout
    logoutURL: https://test.com                             # Logout redirect address, can be customized to the page jumped after user logout

    # Scope configuration
    # Configure the required authorization scope, ensure that the OIDC server supports these scopes
    scopes:
      - openid                                              # Required, used for OIDC basic authentication
      - profile                                             # Optional, used to obtain
```

```
user basic information
      - email                                          # Optional, used to obtain
user email

    # Claim mapping configuration
    # Configure the mapping relationship between OIDC returned claims and platform user
attributes
    claimMapping:
      email: email                                     # Email mapping, used for user
unique identification
      groups: groups                                   # User group mapping, used for
organization structure
      phone: ""                                        # Phone mapping, optional
      preferred_username: preferred_username           # Username mapping, used for
display name

    # User group configuration
    # Configure user group synchronization related parameters, ensure that the token
contains group information
    groupsKey: groups                                  # Specify the key name of
group information
    insecureEnableGroups: false                        # Whether to enable group
synchronization function
```

Соответствующие операции

Вы можете нажать на
справа на странице списка или нажать **Actions** в правом верхнем углу на странице деталей, чтобы при необходимости обновить или удалить OIDC.

Операция	Описание
Обновить OIDC	Обновить добавленную конфигурацию OIDC. После обновления информации конфигурации OIDC исходные пользователи и методы аутентификации будут сброшены и синхронизированы в соответствии с текущей конфигурацией.
Удалить OIDC	Удалить OIDC, который больше не используется платформой. После удаления OIDC все пользователи, синхронизированные с платформой через этот OIDC, получат статус **Invalid** (связь между

Операция	Описание
	пользователями и ролями сохраняется), и они не смогут войти в платформу. После повторной интеграции пользователи могут быть активированы путем успешного входа в платформу. **Совет**: После удаления IDP, если необходимо удалить пользователей и группы пользователей, синхронизированные с платформой через OIDC, отметьте флажок **Clean IDP Users and User Groups** под всплывающим окном.

Menu

Устранение неполадок

Удаление пользователя

Содержание

Описание проблемы

Проблема: При создании или синхронизации нового пользователя система сообщает, что пользователь уже существует. Как следует поступить в этом случае?

По соображениям безопасности платформа не позволяет создавать новых пользователей (как локальных, так и IDP) с именами, совпадающими с ранее удалёнными пользователями. Это ограничение распространяется на:

- Создание новых локальных пользователей с именами, совпадающими с удалёнными пользователями
- Синхронизацию пользователей IDP с именами, совпадающими с удалёнными пользователями

После обновления до текущей версии вы можете столкнуться с этой проблемой при:

- Создании новых пользователей с именами, совпадающими с пользователями, удалёнными до обновления
- Синхронизации новых пользователей с именами, совпадающими с пользователями, удалёнными до обновления

Решение

Для устранения этой проблемы необходимо очистить информацию об удалённых пользователях, выполнив определённые скрипты на управляющих узлах вашего глобального кластера.

Очистка удалённых пользователей IDP

Выполните следующую команду на любом управляющем узле вашего глобального кластера:

```
kubectl delete users -l 'auth.cpaas.io/user.connector_id=<IDP
Name>,auth.cpaas.io/user.state=deleted'
```

Пример:

```
kubectl delete users -l
'auth.cpaas.io/user.connector_id=github,auth.cpaas.io/user.state=deleted'
```

Очистка удалённых локальных пользователей

Выполните последовательно два скрипта на любом управляющем узле вашего глобального кластера:

1. Очистка паролей пользователей:

```
kubectl get users -l
'auth.cpaas.io/user.connector_id=local,auth.cpaas.io/user.state=deleted' | awk '{print
$1}' | xargs kubectl delete password -n cpaas-system
```

2. Очистка пользователей:

```
kubectl delete users -l
'auth.cpaas.io/user.connector_id=local,auth.cpaas.io/user.state=deleted'
```

Menu

Политика пользователя

Введение

Платформа предоставляет комплексные политики безопасности пользователей для повышения безопасности входа и защиты от вредоносных атак.

Содержание

Обзор

Платформа поддерживает следующие политики безопасности:

- Управление безопасностью паролей
- Отключение учетных записей пользователей
- Блокировка учетных записей пользователей
- Уведомления пользователей
- Контроль доступа

Настройка политики безопасности

Шаги

1. В левой навигационной панели нажмите **User Role Management** > **User Security Policy**
2. Нажмите **Update** в правом верхнем углу
3. Настройте политики безопасности по необходимости
4. Нажмите **Update** для сохранения изменений

WARNING

Примечания по настройке политики:

- Отметьте галочкой политику для её включения
- Снимите галочку для отключения политики
- Отключённые политики сохраняют свои данные конфигурации
- При повторном включении политики восстанавливаются предыдущие настройки

Доступные политики

Политика	Описание
User Authentication Policy	Включает двойную аутентификацию для входа по паролю: - Пользователи получают коды подтверждения через указанные методы уведомлений - Поддерживает различные серверы уведомлений (например, Enterprise Communication Tool Server)
Password Security Policy	Управляет требованиями к паролям: Первый вход: - Обязательная смена пароля при первом входе на платформу

Политика	Описание
	Регулярное обновление: - Требуется смена пароля после заданного периода (например, 90 дней) - Вход запрещён до обновления пароля
User Disablement Policy	Автоматически отключает неактивные аккаунты: - Срабатывает после заданного периода отсутствия входа
User Locking Policy	Защищает от атак перебором паролей: Условия блокировки: - Срабатывает после заданного количества неудачных попыток входа в течение 24 часов Длительность блокировки: - Аккаунт остаётся заблокированным в течение заданного времени в минутах - Автоматически разблокируется после истечения периода блокировки
Notification Policy	Управляет уведомлениями пользователей: - Отправляет первоначальный пароль по электронной почте после создания пользователя
Access Control	Управляет сессиями пользователей и доступом: Управление сессиями: - Автоматический выход из неактивных сессий после заданного времени - Ограничение максимального количества одновременных онлайн-пользователей Контроль браузера: - Завершение сессии при закрытии всех вкладок продукта - Запрет на множественные входы с одного клиента :::note

Политика	Описание
	Важные замечания: - Контроль доступа влияет только на новые входы после обновления политики - Восстановление вкладок браузера может не привести к завершению сессии - При запрете повторного входа разрешён только последний вход с клиента :::

Menu

Мультиарендность (Project)

Введение

Введение

Проект

Пространства имён (Namespaces)

Взаимосвязь между кластерами, проектами и пространствами имён

Руководства

Создание проекта

Процедура

Управление проектом

Обновление основной информации проекта

Обновление квоты проекта

Удаление проекта

Управление кластером проекта

Введение

Добавить кластер

Удалить кластер

Управление участниками проекта

Импорт участников

Удаление участников

Введение

Содержание

Проект

Проект — это единица изоляции ресурсов, которая обеспечивает сценарии мультиарендного использования в предприятиях. Он разделяет ресурсы одного или нескольких кластеров на изолированные среды, обеспечивая как изоляцию ресурсов, так и изоляцию персонала. Проекты могут представлять различные дочерние компании, отделы или проектные команды внутри предприятия. С помощью управления проектами можно достичь:

- Изоляции ресурсов между проектными командами
- Управления квотами внутри арендаторов
- Эффективного распределения и контроля ресурсов

Пространства имён (Namespaces)

Пространства имён — это меньшие, взаимно изолированные пространства ресурсов внутри проекта. Они служат рабочими областями для пользователей для реализации

своих производственных нагрузок. Основные характеристики пространств имён включают:

- В рамках проекта можно создавать несколько пространств имён
- Общая квота ресурсов всех пространств имён не может превышать квоту проекта
- Квоты ресурсов выделяются более детально на уровне пространства имён
- Размеры контейнеров (CPU, память) ограничиваются на уровне пространства имён
- Повышенная эффективность использования ресурсов за счёт тонкого контроля

Взаимосвязь между кластерами, проектами и пространствами имён

Иерархия ресурсов платформы подчиняется следующим правилам:

- Проект может использовать ресурсы (CPU, память, хранилище) из нескольких кластеров, а кластер может выделять ресурсы нескольким проектам.
- В рамках проекта можно создавать несколько пространств имён, при этом суммарные квоты ресурсов не должны превышать общие ресурсы проекта.
- Квота ресурсов пространства имён должна поступать из одного кластера, и пространство имён может принадлежать только одному проекту.

Menu

Руководства

Создание проекта

Процедура

Управление проектом

Обновление основной информации проекта

Обновление квоты проекта

Удаление проекта

Управление кластером проекта

Введение

Добавить кластер

Удалить кластер

Управление участниками проекта

Импорт участников

Удаление участников

Создание проекта

Перед началом работы вашей проектной команды вы можете создать проект на основе существующих ресурсов кластера на платформе. Проект будет изолирован от других проектов (тенантов) как по ресурсам, так и по персоналу. При создании проекта вы можете выделить ресурсы в соответствии с масштабом проекта и фактическими бизнес-потребностями. Проект может использовать ресурсы из нескольких кластеров на платформе.

WARNING

При создании проекта платформа автоматически создаст namespace с таким же именем, как у проекта, в связанных кластерах для изоляции ресурсов на уровне платформы. Пожалуйста, не изменяйте этот namespace и его ресурсы.

Содержание

Процедура

1. В представлении **Project Management** нажмите **Create Project**.
2. На странице **Basic information** настройте следующие параметры:

Параметр	Описание
Name	Имя проекта, которое не может совпадать с именем существующего проекта или любым именем из черного списка

Параметр	Описание
	имен проектов. В противном случае проект не может быть создан. **Примечание**: Черный список имен проектов включает специальные имена namespace в кластерах платформы: `cpaas-system`, `cert-manager`, `default`, `global-credentials`, `kube-ovn`, `kube-public`, `kube-system`, `nsx-system`, `alauda-system`, `kube-federation-system`, `ALL-ALL` и `true`.
Cluster	Кластер(ы), связанные с проектом, в которых администратор может выделять квоты ресурсов. Нажмите на выпадающий список, чтобы выбрать один или несколько кластеров. **Примечание**: Кластеры в аномальном состоянии выбрать нельзя.

3. Нажмите **Next** и на шаге настройки квот проекта задайте квоты ресурсов, которые будут выделены текущему проекту для выбранных кластеров. Это включает:

   - CPU (ядра)
   - Память (Gi)
   - Хранилище (Gi)
   - Количество PVC
   - Pods (количество)
   - Виртуальный GPU (GPU-Manager/MPS)
   - pGPU (физический GPU, ядра)
   - Память GPU

NOTE

- Квоты ресурсов GPU можно настроить только при развернутых GPU-плагинах в кластере. Когда ресурс GPU — это **GPU-Manager или MPS GPU**, также можно настроить квоту **vMemory**.

  GPU Units: 100 единиц виртуальных ядер эквивалентны 1 физическому ядру (1 pGPU = 1 ядро = 100 ядер GPU-Manager = 100 ядер MPS), и единицы pGPU можно выделять только

целыми числами. 1 единица памяти GPU-Manager равна 256 Mi, 1 единица памяти MPS GPU равна 1 Gi, 1024 Mi = 1 Gi.

- Если для какого-либо типа ресурса квота не установлена, по умолчанию она считается **Неограниченной**. Это означает, что проект может использовать доступные ресурсы соответствующего типа в кластере по мере необходимости без максимального ограничения.
- Значения квот проекта должны находиться в пределах диапазона квот, отображаемого на странице. Под каждым полем ввода квоты ресурса отображается информация о выделенной квоте и общем объеме для этого ресурса для справки.

1. Нажмите **Create Project**.

Управление проектом

В этом руководстве объясняется, как обновить основную информацию и квоты проекта для указанного проекта или удалить проект.

Содержание

Обновление основной информации проекта

Обновите основную информацию для указанного проекта, такую как отображаемое имя и описание.

Процедура

1. В представлении **Project Management** нажмите на имя проекта, который нужно обновить.
2. В левой навигационной панели нажмите **Details**.
3. В правом верхнем углу нажмите **Actions** > **Update Basics**.

4. Измените или введите **Display name** и **Description**.
5. Нажмите **Update**.

Обновление квоты проекта

Обновите квоты ресурсов для проекта в каждом связанном кластере.

Ограничения и условия

Если проект связан с кластером в состоянии **Abnormal**, обновление квот, назначенных проекту в этом кластере, не поддерживается.

Процедура

1. В представлении **Project Management** нажмите на имя проекта, который нужно обновить.
2. В левой навигационной панели нажмите **Details**.
3. Справа в области квот нажмите **Update Quota**.
4. Обновите квоты, назначенные проекту в кластере, согласно следующим рекомендациям:

NOTE

- Квоты ресурсов GPU (vGPU/pGPU) можно настраивать только при наличии GPU-ресурсов в кластере.

  Если GPU-ресурс является **vGPU**, также можно настроить квоты **vMemory**.

  GPU Units: 100 единиц виртуальных ядер эквивалентны 1 физическому ядру (1 pGPU = 1 ядро = 100 vGPU); 1 единица видеопамяти равна 256 Ми; единицы pGPU — целые числа и могут назначаться только целыми числами.

- Если для какого-либо ресурса квота не установлена, по умолчанию ресурс имеет неограниченную квоту.
- Значение квоты должно находиться в пределах, отображаемых на странице.

1. Нажмите **Update**.

Удаление проекта

Удалите проекты, которые больше не используются.

WARNING

После удаления проекта ресурсы, занятые проектом в кластере, будут освобождены.

Процедура

1. В представлении **Project Management** нажмите на имя проекта, который нужно удалить.
2. В левой навигационной панели нажмите **Details**.
3. В правом верхнем углу нажмите **Actions** > **Delete Project**.
4. Введите имя проекта и нажмите **Delete**.

Управление кластером проекта

В этом руководстве объясняется, как управлять ассоциациями кластеров для проекта. Вы можете добавлять кластеры, чтобы выделить их ресурсы проекту, или удалять кластеры, чтобы вернуть выделенные ресурсы.

Содержание

Введение

Вы можете добавлять кластеры в проект для выделения их ресурсов или удалять кластеры, чтобы вернуть выделенные ресурсы. Эта функциональность полезна в следующих случаях:

- Когда ресурсов проекта недостаточно для бизнес-операций
- Когда необходимо выделить недавно созданный или добавленный кластер существующему проекту
- Когда нужно вернуть ресурсы кластера из проекта
- Когда конкретному проекту требуется эксклюзивный доступ к кластеру

Добавить кластер

Добавьте кластер в проект и установите его квоту ресурсов.

Процедура

1. В представлении **Project Management** нажмите на название проекта, в который хотите добавить кластер.
2. В левой навигационной панели нажмите **Details**.
3. В правом верхнем углу нажмите **Actions** > **Add Cluster**.
4. Выберите кластер и установите квоту ресурсов, которая будет выделена текущему проекту. Можно настроить следующие ресурсы:
   - CPU (ядра)
   - Память (Gi)
   - Хранилище (Gi)
   - Количество PVC (число)
   - Pods (число)
   - vGPU (виртуальный GPU)/MPS/pGPU (физический GPU, ядра)
   - Квота видеопамяти

NOTE

- Квота ресурсов GPU может быть настроена только при развертывании GPU-плагинов в кластере.

  Когда ресурсы GPU — это **GPU-Manager или MPS GPU**, также можно настроить квоту **vMemory**.

  GPU Units: 100 единиц виртуальных ядер эквивалентны 1 физическому ядру (1 pGPU = 1 ядро = 100 ядер GPU-Manager = 100 ядер MPS), и единицы pGPU могут выделяться

только целыми числами. 1 единица памяти GPU-Manager равна 256 Mi, 1 единица памяти MPS GPU равна 1 Gi, 1024 Mi = 1 Gi.

- Если для какого-либо типа ресурса квота не установлена, по умолчанию она считается **Неограниченной**. Это означает, что проект может использовать доступные ресурсы соответствующего типа в кластере без максимального ограничения.
- Значение установленной квоты проекта должно находиться в пределах диапазона квот, отображаемого на странице. Под каждым полем ввода квоты ресурса отображаются выделенная квота и общий объем этого ресурса для справки.

1. Нажмите **Add**.

Удалить кластер

Удалите кластер, связанный с проектом.

WARNING

- После удаления кластера проект не сможет использовать бизнес-ресурсы, находящиеся под управлением удалённого кластера.
- Если удаляемый кластер находится в аномальном состоянии, ресурсы под этим кластером не могут быть очищены. Рекомендуется исправить состояние кластера перед его удалением.

Процедура

1. В представлении **Project Management** нажмите на название проекта, из которого хотите удалить кластер.
2. В левой навигационной панели нажмите **Details**.
3. В правом верхнем углу нажмите **Actions** > **Remove Cluster**.

4. В появившемся диалоговом окне **Remove Cluster** введите имя удаляемого кластера, затем нажмите кнопку **Remove** для успешного удаления кластера.

Управление участниками проекта

В этом руководстве объясняется, как управлять участниками проекта, включая импорт участников и назначение ролей, связанных с проектом.

Содержание

Импорт участников

Вы можете предоставить пользователям права на управление проектом и его пространствами имён, импортируя существующих пользователей платформы или добавляя пользователей OIDC. Вы можете назначать роли, такие как администраторы проекта, администраторы пространств имён, разработчики или настраиваемые роли с правами управления проектом и пространствами имён.

Ограничения и условия

- Если на платформе не настроен OIDC IDP:

- В качестве участников проекта можно импортировать только существующих пользователей платформы, включая:
  - OIDC пользователей, которые успешно вошли в систему
  - Пользователей, синхронизированных через LDAP
  - Локальных пользователей
  - Пользователей, добавленных в другие проекты как OIDC пользователи (с источником, отмеченным как `-`)
- Если настроен OIDC IDP:
  - Можно добавить действительные OIDC аккаунты, соответствующие требованиям ввода
  - Валидность аккаунта не проверяется при добавлении
  - Убедитесь, что аккаунт действителен, иначе вход в систему будет невозможен
- Пользователи с правами системного администратора по умолчанию и текущий вошедший пользователь не могут быть импортированы

Процедура

1. В представлении **Project Management** нажмите на имя проекта, которым хотите управлять.
2. В левой навигационной панели выберите **Members**.
3. Нажмите **Import Member**.
4. Выберите либо **Member List**, либо **OIDC Users**.

Импорт из списка участников

Вы можете импортировать всех пользователей или выбрать конкретных пользователей из списка участников.

TIP

Используйте выпадающее меню групп пользователей в правом верхнем углу и поле поиска для фильтрации пользователей по имени.

Чтобы импортировать всех пользователей:

1. Выберите **Member List**.
2. Нажмите на выпадающее меню **Bind** и выберите роль, которую хотите назначить всем пользователям.
   Если роль требует указания пространства имён, выберите его в выпадающем меню **Namespaces**.
3. Нажмите **Import All**.

Чтобы импортировать конкретных пользователей:

1. Выберите **Member List**.
2. Отметьте одного или нескольких пользователей с помощью флажков.
3. Нажмите на выпадающее меню **Bind** и выберите роль, которую хотите назначить выбранным пользователям.
   Если роль требует указания пространства имён, выберите его в выпадающем меню **Namespaces**.
4. Нажмите **Import**.

Импорт пользователей OIDC

1. Выберите **OIDC Users**.
2. Нажмите **Add** для создания записи участника (повторите для нескольких участников).
3. Введите имя пользователя, прошедшего аутентификацию через OIDC, в поле **Name**.

WARNING

Убедитесь, что имя пользователя соответствует аккаунту, который может быть аутентифицирован настроенной системой OIDC, иначе вход будет невозможен.

4. Выберите роль из выпадающего меню **Roles**.
   Если роль требует указания пространства имён, выберите его в выпадающем меню **Namespaces**.
5. Нажмите **Import**.

После успешного импорта вы сможете увидеть:

- Участника в списке участников проекта
- Пользователя в разделе **Platform Management > Users**
  - Источник отображается как "-" до первого входа/синхронизации
  - Источник обновляется после успешного входа/синхронизации

Удаление участников

Удалите участника проекта, чтобы отозвать его права.

Процедура

1. В представлении **Project Management** нажмите на имя проекта.
2. В левой навигационной панели выберите **Members**.

> **TIP**
>
> Используйте выпадающий список рядом с полем поиска для фильтрации участников по **Name**, **Display name** или **User Group**.

3. Нажмите **Remove** рядом с участником, которого хотите удалить.
4. Подтвердите удаление в появившемся диалоговом окне.

Menu

Аудит

Введение

Функция аудита платформы предоставляет упорядоченные по времени записи операций, связанных с пользователями и безопасностью системы. Это помогает анализировать конкретные проблемы и быстро решать возникающие в кластерах, пользовательских приложениях и других областях вопросы.

С помощью аудита вы можете отслеживать различные изменения в Kubernetes кластере, включая:

- Какие изменения произошли в кластере за определённый период времени
- Кто выполнил эти изменения (системные компоненты или пользователи)
- Детали важных событий изменений (например, обновления параметров POD)
- Результаты событий (успех или неудача)
- Местоположение оператора (внутри или вне кластера)
- Записи операций пользователей (обновления, удаления, управленческие операции) и их результаты

Содержание

Требования

Ваша учетная запись должна иметь права управления платформой или права аудита платформы.

Процедура

1. В левой навигационной панели нажмите **Auditing**.
2. Выберите область аудита на вкладках:
   - **User Operations**: Просмотр записей операций пользователей, вошедших в платформу
   - **System Operations**: Просмотр записей системных операций (операторы начинаются с `system:`)
3. Настройте условия запроса для фильтрации событий аудита:

Условие запроса	Описание
Operator	Имя пользователя или системной учетной записи оператора (по умолчанию: `All`)
Actions	Тип операции (create, update, delete, manage, rollback, stop и др., по умолчанию: `All`)
Clusters	Кластер, содержащий управляемый ресурс (по умолчанию: `All`)
Resource Type	Тип управляемого ресурса (по умолчанию: `All`)
Resource Name	Имя управляемого ресурса (поддерживается нечеткий поиск)

4. Нажмите **Search**.

TIP

- Используйте выпадающий список **Time Range** для установки временного диапазона аудита (по умолчанию: `Last 30 Minutes`). Можно выбрать предустановленный диапазон или задать свой.
- Нажмите на иконку обновления, чтобы обновить результаты поиска.
- Нажмите на иконку экспорта, чтобы скачать результаты в формате `.csv`.

Результаты поиска

В результатах поиска отображается следующая информация:

Параметр	Описание
Operator	Имя пользователя или системной учетной записи оператора
Actions	Тип операции (create, update, delete, manage, rollback, stop и др.)
Resource Name/Type	Имя и тип управляемого ресурса
Clusters	Кластер, содержащий управляемый ресурс
Namespaces	Namespace, содержащий управляемый ресурс
Client IP	IP-адрес клиента, с которого была выполнена операция
Operation Result	Результат операции на основе кода возврата API (2xx = успех, остальные = ошибка)
Operation Time	Временная метка операции
Details	Нажмите кнопку **Details**, чтобы просмотреть полный аудиторский запись в формате JSON в диалоговом окне **Audit Details**

Menu

Телеметрия

Установка

ACP Telemetry — это сервис платформы, который собирает телеметрические данные с кластеров для онлайн-операций и обслуживания. Он собирает системные метрики и загружает их в Alauda Cloud для мониторинга и анализа.

Содержание

Требования

Перед установкой убедитесь, что:

- В Alauda Container Platform имеется действующая лицензия
- Глобальный кластер имеет доступ в интернет

Шаги установки

1. Перейдите в **Platform Management**
2. В левой навигационной панели нажмите **Marketplace** > **Cluster Plugins**
3. Выберите кластер **global** в верхней навигационной панели

4. Найдите **ACP Telemetry** и кликните для просмотра деталей
5. Нажмите **Install** для развертывания плагина

Включение онлайн-операций

1. В левой навигационной панели нажмите **System Settings** > **Platform Maintenance**
2. Нажмите кнопку **On** для **Online Operations**

Шаги удаления

1. Выполните шаги 1-4 из процесса установки для поиска плагина
2. Нажмите **Uninstall** для удаления плагина