Menu

安全

Alauda Container Security

Alauda Container Security

安全性与合规性

合规

API Refiner

用户与角色

用户

用户组

角色

IDP

用户策略

多租户（项目）

介绍

Project

Namespaces

Clusters、Projects 和 Namespaces 之间的关系

功能指南

审计

介绍

前提条件

操作步骤

搜索结果

遥测

Alauda Container Security

Alauda Container Security 是一款面向 Kubernetes 和容器化环境的综合安全解决方案。它提供集中管理、自动漏洞扫描、策略执行和合规性检查，帮助组织在多个集群中保护其容器基础设施的安全。

Alauda Container Security 采用分布式、基于容器的架构，由中央服务（用于管理、API 和 UI）和安全集群服务（用于监控、策略执行和数据收集）组成。它可与 CI/CD 流水线、SIEM、日志系统集成，并支持内置的 Scanner V4 漏洞扫描器。

Note

因为 Alauda Container Security 的发版周期与灵雀云容器平台不同，所以 Alauda Container Security 的文档现在作为独立的文档站点托管在 Alauda Container Security↗。

Menu

安全性与合规性

合规

安装

API Refiner

介绍

产品介绍

产品优势

应用场景

限制

安装

安装步骤

卸载步骤

默认配置

Menu

合规

安装

Alauda Compliance with Kyverno

安装步骤

卸载步骤

Menu

安装

Alauda Compliance with Kyverno

安装步骤

卸载步骤

Alauda Compliance with Kyverno

Alauda Compliance with Kyverno 是一项平台服务，集成了 Kyverno，用于在 Alauda Container Platform 上管理合规策略。

目录

安装步骤

1. 进入 **Platform Management**
2. 在左侧导航栏中，点击 **Marketplace** > **Cluster Plugins**
3. 搜索 **Alauda Compliance with Kyverno** 并点击查看详情
4. 点击 **Install** 部署插件

卸载步骤

1. 按照安装流程中的步骤 1-3 定位插件
2. 点击 **Uninstall** 卸载插件

Menu

API Refiner

介绍

产品介绍

产品优势

应用场景

限制

安装

安装步骤

卸载步骤

默认配置

介绍

目录

产品介绍

ACP API Refiner 是由 Alauda Container Platform 提供的数据过滤服务，旨在增强 Kubernetes 环境中的多租户安全性和数据隔离。它基于用户权限、项目、集群和命名空间对 Kubernetes API 响应数据进行过滤，同时支持字段级别的过滤、包含和数据脱敏。

产品优势

ACP API Refiner 的核心优势如下：

- 多维度数据隔离
  - 支持基于项目、集群和命名空间维度过滤 API 响应
  - 确保不同租户之间的数据边界
  - 防止未授权访问集群范围资源
- 灵活的数据过滤

  - 支持排除、包含和脱敏 API 响应中的特定字段
  - 通过 YAML 配置实现过滤规则的可配置化
  - 针对不同资源类型动态生成资源 Ingress
- 增强的安全性
  - 实现基于 JWT token 的用户认证
  - 提供基于用户权限的细粒度访问控制
  - 支持敏感信息的数据脱敏

应用场景

ACP API Refiner 的主要应用场景如下：

- 多租户环境
  - 确保不同租户之间的数据隔离
  - 防止未授权访问集群范围资源
  - 有效管理共享命名空间场景
- 敏感数据保护
  - 过滤 API 响应中的敏感信息
  - 支持字段级别的数据脱敏
  - 保护敏感的元数据和注解
- 合规需求
  - 帮助满足数据隔离要求
  - 支持审计和合规需求
  - 维护数据访问边界

限制

ACP API Refiner 适用以下限制：

- 资源必须包含特定的租户相关标签以实现数据隔离：
  - `cpaas.io/project`
  - `cpaas.io/cluster`
  - `cpaas.io/namespace`
  - `kubernetes.io/metadata.name`
  - 可选：`cpaas.io/creator`
- LabelSelector 查询不支持逻辑 OR 操作
- 平台级别的 userbindings 不会被过滤
- 过滤仅应用于 GET 和 LIST API 操作

安装

ACP API Refiner 是一个平台服务，用于过滤 Kubernetes API 响应数据。它提供按项目、集群和命名空间的过滤功能，并支持在 API 响应中进行字段排除、包含和去敏感处理。

目录

安装步骤

1. 导航到 平台管理
2. 在左侧导航栏中，点击 市场 > 集群插件
3. 在顶部导航栏中选择 **global** 集群
4. 搜索 **ACP API Refiner** 并点击查看其详细信息
5. 点击 安装 以部署该插件

卸载步骤

1. 按照安装过程中的步骤 1-4 定位插件

2. 点击 卸载 以移除该插件

默认配置

过滤的资源

默认情况下，以下资源会被过滤：

资源	**API** 版本
namespaces	v1
projects	auth.alauda.io/v1
clustermodules	cluster.alauda.io/v1alpha2
clusters	clusterregistry.k8s.io/v1alpha1

字段去敏感处理

默认情况下，以下字段会被去敏感处理：

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

Menu

用户与角色

用户

介绍

用户来源

用户管理规则

用户生命周期

功能指南

用户组

介绍

组介绍

组类型

功能指南

角色

介绍

角色介绍

系统角色

自定义角色

功能指南

IDP

介绍

概述

支持的集成方式

功能指南

故障排除

用户策略

介绍

Menu

用户

介绍

介绍

用户来源

用户管理规则

用户生命周期

功能指南

管理用户角色

添加角色

移除角色

创建用户

步骤

用户管理

重置本地用户密码

更新用户到期日期

激活用户

禁用用户

将用户添加到本地用户组

删除用户

批量操作

介绍

该平台支持所有用户的身份验证和登录验证。

目录

用户来源

本地用户

- 在平台部署期间创建的管理员帐户
- 通过平台界面创建的帐户
- 通过本地 dex 配置文件添加的用户

第三方用户

LDAP 用户

- 从 LDAP 服务器同步的企业用户
- 通过 IDP（身份提供者）集成导入的帐户
- 来源显示为 IDP 配置名称
- 通过 IDP 设置进行集成配置

OIDC 用户

- 通过 OIDC 协议认证的第三方平台用户
- 来源显示为 IDP 配置名称
- 通过 IDP 设置进行集成配置

> **WARNING**
>
> 对于在第一次登录之前已添加到项目中的 OIDC 用户：
>
> - 来源在成功登录平台之前显示为 "-"
> - 成功登录后，来源更改为 IDP 配置名称

其他第三方用户

- 通过支持的 dex 连接器（如 GitHub、Microsoft）进行身份验证的用户
- 更多信息，请参见 dex 官方文档↗

用户管理规则

> **WARNING**
>
> 请注意以下重要规则：
>
> - 本地用户名在所有用户类型中必须唯一
> - 拥有相同用户名的第三方用户（OIDC/LDAP）将自动关联
> - 关联用户从现有帐户继承权限

- 用户可以通过各自的来源登录
- 平台中每个用户名只显示一个用户记录
- 用户来源由最近的登录方式决定

用户生命周期

下表描述了平台上用户的不同状态：

状态	描述
正常	用户帐户处于活动状态，可以登录平台
禁用	用户帐户处于非活动状态，无法登录。请联系平台管理员以重新激活。 可能原因： - 连续 90 天未登录 - 帐户过期 - 管理员手动禁用
锁定	由于 24 小时内五次登录失败，帐户暂时被锁定。 详细信息： - 锁定时长：20 分钟 - 可以由管理员手动解锁 - 锁定期结束后帐户将恢复可用
无效	已从 LDAP 服务器删除的 LDAP 同步帐户。 注意：无效帐户无法登录平台

Menu

功能指南

管理用户角色

添加角色

移除角色

创建用户

步骤

用户管理

重置本地用户密码

更新用户到期日期

激活用户

禁用用户

将用户添加到本地用户组

删除用户

批量操作

管理用户角色

平台管理员可以管理其他用户（而不是他们自己的帐户）的角色，以授予或撤销权限。

目录

添加角色

步骤

1. 在左侧导航栏中，点击 用户 > 用户管理
2. 点击目标用户的用户名
3. 滚动到 角色列表 部分
4. 点击 添加角色
5. 在角色分配对话框中：

- 从 角色名称 下拉菜单中选择一个角色
- 选择角色的权限范围（集群、项目或命名空间）
- 点击 添加

NOTE

重要说明：

- 您可以为用户添加多个角色
- 每个角色每个用户只能添加一次
- 已分配的角色在下拉菜单中显示，但无法被选择
- 集群管理员 角色无法在 global 集群 中分配

移除角色

步骤

1. 在左侧导航栏中，点击 用户 > 用户管理
2. 点击目标用户的用户名
3. 滚动到 角色列表 部分
4. 点击要移除的角色旁边的 移除
5. 确认移除

WARNING

角色管理权限：

- 只有平台管理员可以管理其他用户的角色
- 用户无法修改自己的帐户角色

创建用户

具有平台管理员角色的用户可以通过平台界面创建本地用户并为其分配角色。

目录

步骤

1. 在左侧导航栏中，单击 用户 > 用户管理
2. 单击 创建用户
3. 配置以下参数：

参数	描述
密码类型	选择一种密码生成方法： 随机：系统生成一个安全的随机密码 自定义：用户手动输入密码
密码	根据所选类型输入或生成密码。 密码要求： - 长度：8-32 个字符 - 必须包含字母和数字 - 必须包含特殊字符 (`~!@#$%^&*()_-+=?`)

参数	描述
	密码字段功能： - 单击眼睛图标以显示/隐藏密码 - 单击复制图标以复制密码
邮箱	用户的电子邮件地址： - 必须是唯一的 - 可以用作登录用户名 - 与用户的名称关联
有效期	设置用户帐户的有效期： 选项： - 永久：无限制 - 自定义：使用时间范围下拉菜单设置开始和结束时间
角色	为用户分配一个或多个角色
继续创建	切换开关以控制创建后行为： - 开启：重定向到新用户创建页面 - 关闭：显示用户详细信息页面

1. 单击 创建

NOTE

用户创建成功后：

- 如果“继续创建”启用，将重定向到创建另一个用户的页面
- 如果禁用，则会显示创建用户的详细信息页面

用户管理

该平台提供灵活的用户管理功能，支持单个用户管理和批量操作，以提高特定场景（例如，现场或远程团队）的效率。

WARNING

重要限制：

- 系统生成的账户无法管理（平台管理员角色，地方来源）
- 当前登录用户无法管理自己的账户
- 对于个人账户修改（显示名称、密码），请使用个人信息页面

目录

步骤

重置本地用户密码

拥有平台管理权限的用户可以重置其他本地用户的密码。

步骤

1. 在左侧导航栏中，点击 用户 > 用户管理
2. 点击目标用户记录旁边的图标
3. 点击 重置密码
4. 在对话框中，选择密码类型：

- 随机：系统生成一个安全的随机密码
- 自定义：手动输入新密码

NOTE

密码要求：

- 长度：8-32 个字符
- 必须包含字母和数字
- 必须包含特殊字符（`~!@#$%^&*( ) -_=+?`）

密码字段功能：

- 点击眼睛图标显示/隐藏密码
- 点击复制图标复制密码

1. 点击 重置

更新用户到期日期

您可以更新 正常、禁用 或 锁定 状态用户的到期日期。超过到期日期的用户将被自动禁用。

步骤

1. 在左侧导航栏中，点击 用户 > 用户管理
2. 点击目标用户旁边的 更新到期日期
3. 在对话框中，选择到期日期选项：

- 永久：无限制
- 自定义：使用时间范围下拉框设置开始和结束时间

4. 点击 更新

激活用户

您可以激活 禁用 或 锁定 状态的用户。

> **NOTE**
>
> 激活行为：
>
> - 如果用户在到期日期内：到期日期保持不变
> - 如果用户已过期：到期日期变为 永久

步骤

1. 在左侧导航栏中，点击 用户 > 用户管理
2. 点击目标用户旁边的 激活
3. 在确认对话框中点击 激活

4. 用户状态将变为 正常

禁用用户

您可以在用户到期日期内禁用 正常 或 锁定 状态的用户。被禁用的用户无法登录，但可以重新激活。

步骤

1. 在左侧导航栏中，点击 用户 > 用户管理
2. 点击目标用户旁边的图标
3. 点击 禁用 并确认

将用户添加到本地用户组

您可以将 来源 为 本地 或 `LDAP` 的用户添加到一个或多个本地用户组。

WARNING

组角色行为：

- 用户自动继承其组的角色
- 组角色仅在组的详细信息页面（配置角色选项卡）上可见
- 单个用户的角色列表仅显示直接分配的角色

步骤

1. 在左侧导航栏中，点击 用户 > 用户管理
2. 点击目标用户旁边的图标
3. 点击 添加到用户组

4. 选择一个或多个本地用户组
5. 点击 添加

删除用户

平台管理员可以删除任何用户，但当前登录的账户除外，包括：

- IDP 配置的用户
- 源为 `-` 的用户
- 本地用户

步骤

1. 在左侧导航栏中，点击 用户 > 用户管理
2. 点击目标用户旁边的图标
3. 点击 删除
4. 点击 确认

批量操作

您可以执行以下批量操作：

- 更新有效期
- 激活用户
- 禁用用户
- 删除用户

步骤

1. 在左侧导航栏中，点击 用户 > 用户管理

2. 使用复选框选择一个或多个用户

3. 点击 批量操作 并选择一个操作：

- 更新有效性
- 激活
- 禁用
- 删除

NOTE

批量操作详细信息：

- 更新有效性：设置永久或自定义时间范围
- 激活：在对话框中确认激活
- 禁用：在对话框中确认禁用
- 删除：输入当前账户密码并确认

Menu

用户组

介绍

介绍

组介绍

组类型

功能指南

管理用户组角色

向组中添加角色

从组中移除角色

创建本地用户组

创建用户组

管理用户组

管理本地用户组成员资格

前提条件

导入成员

移除成员

介绍

目录

组介绍

该平台通过用户组支持用户管理。通过管理组角色，您可以高效地：

- 同时向多个用户授予平台操作权限
- 一次性撤销多个用户的权限
- 实现基于角色的批量访问控制

例如，当企业内部发生人事变动，并且您需要向多个用户授予新的项目或命名空间操作权限时，您可以：

1. 创建一个用户组
2. 导入相关用户作为组成员
3. 为该组配置项目和命名空间角色
4. 将统一权限应用于所有组成员

组类型

该平台支持两种类型的组：

本地用户组

- 直接在平台上创建
- 源显示为 本地
- 可以更新或删除
- 支持：
  - 从任何来源添加或移除用户
  - 添加或移除角色

IDP 同步用户组

- 从连接的 IDP（LDAP、Azure AD）同步而来
- 源显示为连接的 ***IDP*** 名称
- 不能更新或删除
- 支持：
  - 添加或移除角色
  - 不能管理组成员（添加或移除）

Menu

功能指南

管理用户组角色

向组中添加角色

从组中移除角色

创建本地用户组

创建用户组

管理用户组

管理本地用户组成员资格

前提条件

导入成员

移除成员

管理用户组角色

拥有平台管理权限的用户可以管理本地用户组和与 IDP 同步的用户组的角色。

目录

向组中添加角色

步骤

1. 在左侧导航栏中，单击 用户 > 用户组管理
2. 点击目标用户组的名称
3. 在 配置角色 选项卡上，点击 添加角色
4. 点击以添加角色

NOTE

角色分配规则：

- 您可以向一个组添加多个角色
- 每个角色只能在同一组中添加一次

1. 从下拉菜单中选择角色名称
2. 选择角色的权限范围（集群、项目或命名空间）
3. 点击 添加

从组中移除角色

WARNING

当您从组中移除角色时：

- 该角色授予组成员的所有权限将被撤销
- 此操作无法撤销

步骤

1. 在左侧导航栏中，单击 用户 > 用户组管理
2. 点击目标用户组的名称
3. 在 配置角色 选项卡上，点击角色旁边的 移除
4. 点击 确认 以移除角色

创建本地用户组

本地用户组允许您实现基于角色的访问控制，以便于管理来自任意来源的多个用户。

目录

创建用户组

步骤

1. 在左侧边栏中，单击 用户 > 用户组管理
2. 点击 创建用户组
3. 输入以下信息：

- 名称：用户组的名称
- 描述：对该组目的的描述

4. 点击 创建

管理用户组

您可以通过点击列表页面上的图标或在详细信息页面右上角点击 操作 来管理用户组。

操作	描述
更新用户组	根据组的来源更新组信息： - 对于 来源 为 `Local` 的组：可以更新名称和描述 - 对于 来源 为 `IDP name` 的组：只能更新描述
删除本地用户组	删除 来源 为 `Local` 的用户组

WARNING

删除组时：

- 所有组成员将被移除
- 所有分配给该组的角色将被移除
- 此操作无法撤销

管理本地用户组成员资格

仅具有平台管理权限的用户可以管理本地用户组成员资格。

目录

前提条件

WARNING

在管理组成员资格之前，请注意以下限制：

- 仅具有平台管理权限的用户可以管理组及其成员
- 系统帐户和当前已登录帐户无法管理（不能导入到组中或从组中删除）
- 每个本地用户组最多可以拥有 5000 名成员
- 当组达到 5000 名成员的限制时，将不允许进一步导入

导入成员

您可以将平台中的用户导入本地用户组，以统一管理权限。

TIP

导入到组中的用户将自动继承分配给该组的所有操作权限。

步骤

1. 在左侧导航栏中，单击 用户 > 用户组管理
2. 单击要添加成员的本地用户组的名称
3. 在 组成员管理 标签下，单击 导入成员
4. 通过勾选用户名/显示名旁边的复选框选择一个或多个用户
5. 单击 导入

NOTE

- 只能选择当前不是该组成员的用户
- 使用 全部导入 按钮一次性导入列表中的所有用户

移除成员

当您从组中移除用户时，通过该组授予该用户的所有操作权限将被自动撤销。

步骤

1. 在左侧导航栏中，单击 用户 > 用户组管理
2. 单击要移除成员的本地用户组的名称
3. 在 组成员管理 标签下，您可以通过两种方式移除成员：

- 单击成员名称旁的 移除 并确认
- 使用复选框选择一个或多个成员，然后单击 批量移除 并确认

Menu

角色

介绍

介绍

角色介绍

系统角色

自定义角色

功能指南

创建角色

基本信息配置

查看配置

权限配置

管理自定义角色

更新基本信息

更新角色权限

复制现有角色

删除自定义角色

介绍

目录

角色介绍

该平台的用户角色管理是通过 Kubernetes RBAC（基于角色的访问控制）实现的。此系统通过将角色与用户关联，实现了灵活的权限配置。

角色表示一组在平台上操作 Kubernetes 资源所需的权限。这些权限包括：

- 创建资源
- 查看资源
- 更新资源
- 删除资源

角色对不同资源进行分类和组合权限。通过将角色分配给用户并设置权限范围，可以快速授予资源操作权限。

权限也可以同样简单地通过从用户中移除角色来撤销。

一个角色可以包含：

- 一个或多个资源类型
- 一个或多个操作权限

- 多个分配给它的用户

例如：

- 角色 A：只能查看和创建项目
- 角色 B：可以创建、查看、更新和删除用户、项目和命名空间

系统角色

为了满足常见的权限配置场景，该平台提供以下默认系统角色。这些角色使平台资源的访问控制灵活，并为用户提供高效的权限管理。

角色名称	描述	角色级别
平台管理员	拥有对平台上所有业务和资源的完全访问权限	平台
平台审计员	可以查看所有平台资源和操作记录，但没有其他权限	平台
集群管理员（**Alpha**）	管理和维护集群资源，对所有集群级别的资源具有完全访问权限	集群
项目管理员	管理命名空间管理员和命名空间配额	项目
namespace-admin-system	管理命名空间成员和角色分配	命名空间
开发者	在命名空间内开发、部署和维护自定义应用程序	命名空间

自定义角色

该平台支持自定义角色，以增强资源访问控制场景。自定义角色相较于系统角色提供了若干优势：

- 灵活的权限配置
- 更新角色权限的能力
- 可在不再需要时删除角色的选项

WARNING

更新或删除自定义角色时请谨慎。当删除自定义角色时，将自动撤销该角色授予所有绑定用户的权限。

Menu

功能指南

创建角色

基本信息配置

查看配置

权限配置

管理自定义角色

更新基本信息

更新角色权限

复制现有角色

删除自定义角色

创建角色

具有平台角色权限的用户可以根据实际使用场景创建其权限等于或低于自身角色权限的自定义角色。在创建角色时，可以配置：

- 平台功能模块操作权限
- 用户自定义资源的访问权限（Kubernetes CRD）

目录

基本信息配置

1. 在左侧导航栏中，点击 用户 > 角色。
2. 点击 创建角色。
3. 配置角色的基本信息：

角色类型

为用户分配角色时，权限范围将根据角色类型进行限制：

- 平台角色：显示所有平台权限
- 项目角色：显示以下权限：

- 项目管理
- 容器平台
- 服务网格
- DevOps
- 中间件

- 命名空间角色：显示以下权限：
  - 项目管理
  - 容器平台
  - 服务网格
  - DevOps
  - 中间件

1. 点击 下一步。

查看配置

在查看配置部分，您可以控制角色访问特定视图的权限。未被选择的视图将不会在具有此角色的用户的顶部导航中显示。

NOTE

1. 您账户的角色权限限制了您可以配置哪些视图卡片。例如：
   - 如果您的账户没有 项目管理 视图权限
   - 在创建角色时， 项目管理 视图卡片将显示为灰色
   - 您只能创建与自己角色权限相等或更低的角色
2. 视图入口状态：
   - 如果某个视图的 显示入口 在 产品 功能中关闭
   - 则该视图在 权限配置 中的权限仍将生效
   - 该视图在入口启用之前将暂时无法访问

- 一旦启用，之前选择的权限将正常工作

权限配置

1. 点击页面左上角的 添加自定义权限。
2. 配置角色操作自定义资源（Kubernetes CRD）的权限：

参数	描述
组名称	权限组的名称。组在权限模块下按照添加的顺序显示。
资源名称	资源的名称。按 Enter 键添加多个自定义资源名称。
操作权限	操作该资源的权限。

1. 点击 创建。

管理自定义角色

本指南描述了如何在平台上管理自定义角色，包括：

- 更新基本信息和权限
- 复制现有角色以创建新角色
- 删除自定义角色

目录

更新基本信息

您可以更新平台上自定义角色的显示名称和描述。

步骤

1. 在左侧导航栏中，点击 用户 > 角色
2. 点击要更新的 *角色名称*

3. 点击右上角的 操作 > 更新
4. 更新角色的：

- 显示名称
- 描述

5. 点击 更新

更新角色权限

您可以更新自定义角色的权限信息，包括：

- 为平台资源添加新的操作权限
- 删除现有权限
- 修改自定义资源的权限

步骤

1. 在左侧导航栏中，点击 用户 > 角色
2. 点击要更新的 *角色名称*
3. 点击权限区域右上角的 操作 > 更新角色权限
4. 在 更新角色权限 页面上进行更改
5. 点击 确认

复制现有角色

您可以通过复制现有角色（系统角色或自定义角色）来创建新角色。新角色将继承源角色的所有权限信息，您可以根据需要进行修改。

WARNING

新角色的权限不能超过创建者所属角色的权限。

步骤

1. 在左侧导航栏中，点击 用户 > 角色
2. 点击要复制的 *角色名称*
3. 点击右上角的 操作 > 复制为新角色
4. 在 复制为新角色 页面上，配置：

- 名称
- 显示名称
- 描述
- 类型

5. 点击 创建

删除自定义角色

您可以删除不再使用的自定义角色。

WARNING

当您删除自定义角色时：

- 该角色与用户的绑定关系将被移除
- 分配给该角色的用户将失去该角色所授予的所有权限
- 该角色将从用户的角色列表中移除

步骤

1. 在左侧导航栏中，点击 用户 > 角色
2. 点击要删除的 *角色名称*

3. 点击右上角的 操作 > 删除

4. 输入角色名称以确认删除

5. 点击 删除

Menu

IDP

介绍

介绍

概述

支持的集成方式

功能指南

LDAP 管理

LDAP 概述

支持的 LDAP 类型

LDAP 术语

添加 LDAP

LDAP 配置示例

同步 LDAP 用户

相关操作

OIDC 管理

OIDC 概述

添加 OIDC

通过 YAML 添加 OIDC

相关操作

故障排除

删除用户

问题描述

解决方案

介绍

目录

概述

该平台与 Dex 身份验证服务集成，使您能够通过 IDP 配置使用 Dex 预先实现的连接器进行平台账户认证。如需更多信息，请参阅 Dex 官方文档↗。

支持的集成方式

LDAP 集成

如果您的企业使用 **LDAP**（轻量级目录访问协议）进行用户管理，您可以在平台上配置 LDAP，以连接到您企业的 LDAP 服务器。

LDAP 集成的好处：

- 启用平台与 LDAP 服务器之间的通信
- 允许企业用户使用 LDAP 凭据登录
- 自动将企业用户账户同步到平台

OIDC 集成

该平台支持使用 OpenID Connect（OIDC）协议与 IDP 服务集成，以进行第三方用户认证。

OIDC 集成的好处：

- 使用户能够使用第三方账户登录
- 支持企业 IDP 服务
- 通过 OIDC 协议提供安全认证

> **NOTE**
>
> 对于使用上述未提到的其他连接器进行认证，请联系技术支持。

Menu

功能指南

LDAP 管理

LDAP 概述

支持的 LDAP 类型

LDAP 术语

添加 LDAP

LDAP 配置示例

同步 LDAP 用户

相关操作

OIDC 管理

OIDC 概述

添加 OIDC

通过 YAML 添加 OIDC

相关操作

LDAP 管理

平台管理员可以在平台上添加、更新和删除 LDAP 服务。

目录

LDAP 概述

LDAP（轻量级目录访问协议）是一种成熟、灵活且得到良好支持的标准机制，用于与目录服务器进行交互。它将数据组织成层次树结构，以存储企业用户和组织信息，主要用于实现单点登录（SSO）。

NOTE

LDAP 关键特性：

- 启用客户端与 LDAP 服务器之间的通信
- 支持数据存储、检索和搜索操作
- 提供客户端认证能力
- 便于与其他系统集成

有关更多信息，请参阅 LDAP 官方文档↗。

支持的 LDAP 类型

OpenLDAP

OpenLDAP 是 LDAP 的开源实现。如果您的组织使用开源 LDAP 进行用户认证，可以通过添加 LDAP 并配置相关参数来使平台与 LDAP 服务进行通信。

NOTE

OpenLDAP 集成：

- 启用平台对 LDAP 用户的认证
- 支持标准 LDAP 协议

- 提供灵活的用户管理

有关 OpenLDAP 的更多信息，请参阅 OpenLDAP 官方文档↗。

Active Directory

Active Directory 是微软基于 LDAP 的软件，用于在 Windows 系统中提供目录存储服务。如果您的组织使用微软 Active Directory 进行用户管理，可以配置平台与 Active Directory 服务进行通信。

NOTE

Active Directory 集成：

- 启用平台对 AD 用户的认证
- 支持 Windows 域集成
- 提供企业级用户管理

LDAP 术语

OpenLDAP 常用术语

术语	描述	示例
dc (域组件)	域组件	`dc=example,dc=com`
ou (组织单位)	组织单位	`ou=People,dc=example,dc=com`
cn (常用名)	常用名	`cn=admin,dc=example,dc=com`
uid (用户 ID)	用户 ID	`uid=example`
objectClass (对象类)	对象类	`objectClass=inetOrgPerson`

术语	描述	示例
mail (邮件)	邮件	`mail=example@126.com`
givenName (名)	名	`givenName=xq`
sn (姓)	姓	`sn=ren`
objectClass: groupOfNames	用户组	`objectClass: groupOfNames`
member (成员)	组成员属性	`member=cn=admin,dc=example,dc=com`
memberOf	用户组成员属性	`memberOf=cn=users,dc=example,dc=com`

Active Directory 常用术语

术语	描述	示例
dc (域组件)	域组件	`dc=example,dc=com`
ou (组织单位)	组织单位	`ou=People,dc=example,dc=com`
cn (常用名)	常用名	`cn=admin,dc=example,dc=com`
sAMAccountName/userPrincipalName	用户标识符	`userPrincipalName=example` 或 `sAMAccountName=example`

术语	描述	示例
objectClass: user	AD用户对象类	`objectClass=user`
mail (邮件)	邮件	`mail=example@126.com`
displayName	显示名称	`displayName=example`
givenName (名)	名	`givenName=xq`
sn (姓)	姓	`sn=ren`
objectClass: group	用户组	`objectClass: group`
member (成员)	组成员属性	`member=CN=Admin,DC=example,DC=cc`
memberOf	用户组成员属性	`memberOf=CN=Users,DC=example,DC=`

添加 LDAP

TIP

LDAP 集成成功后：

- 用户可以使用其企业账户登录平台
- 多次添加相同的 LDAP 将覆盖先前同步的用户

前提条件

在添加 LDAP 之前，请准备以下信息：

- LDAP 服务器地址
- 管理员用户名
- 管理员密码
- 其他所需配置详细信息

步骤

1. 在左侧导航栏中，点击 用户 > 身份提供者（**IDP**）
2. 点击 添加 **LDAP**
3. 配置以下参数：

基本信息

参数	描述
服务器地址	LDAP 服务器访问地址（例如，`192.168.156.141:31758`）
用户名	LDAP 管理员 DN（例如，`cn=admin,dc=example,dc=com`）
密码	LDAP 管理员账户密码
登录框用户名提示	用户名输入提示消息（例如，“请输入您的用户名”）

搜索设置

NOTE

搜索设置目的：

- 根据指定条件匹配 LDAP 用户条目
- 提取关键用户和组属性
- 将 LDAP 属性映射到平台用户属性

参数	描述
对象类型	用户的 ObjectClass： - OpenLDAP: `inetOrgPerson` - Active Directory: `organizationalPerson` - 组: `posixGroup`
登录字段	用作登录用户名的属性： - OpenLDAP: `mail`（电子邮件地址） - Active Directory: `userPrincipalName`
筛选条件	用户/组过滤的 LDAP 筛选条件 示例: `(&(cn=John*)(givenName=*xq*))`
搜索起始点	用户/组搜索的基本 DN（例如，`dc=example,dc=org`）
搜索范围	搜索范围： - `sub`: 整个目录子树 - `one`: 从起始点向下一级
登录属性	唯一用户标识符： - OpenLDAP: `uid` - Active Directory: `distinguishedName`
名称属性	对象名称属性（默认: `cn`）
电子邮件属性	电子邮件属性： - OpenLDAP: `mail`

参数	描述
	- Active Directory: `userPrincipalName`
组成员属性	组成员标识符（默认: `uid`）
组属性	用户组关系属性（默认: `memberuid`）

4. 在 身份提供者（**IDP**）服务配置验证 部分：

- 输入有效的 LDAP 账户用户名和密码
- 用户名必须与 登录字段 设置匹配
- 点击验证配置

5. （可选）配置 **LDAP** 自动同步策略：

- 启用 自动同步用户 开关
- 设置同步规则
- 使用 在线工具↗ 验证 CRON 表达式

6. 点击 添加

> **NOTE**
>
> 添加 LDAP 后：
>
> - 用户可以在同步之前登录
> - 用户信息将在首次登录时自动同步
> - 自动同步将根据配置的规则进行

LDAP 配置示例

LDAP 连接器配置

以下示例展示如何配置一个 LDAP 连接器：

```yaml
apiVersion: dex.coreos.com/v1
kind: Connector
id: ldap        # 连接器 ID
name: ldap      # 连接器显示名称
type: ldap      # 连接器类型为 LDAP
metadata:
  name: ldap
  namespace: cpaas-system
spec:
  config:
    # LDAP 服务器地址和端口
    host: ldap.example.com:636
    # 用于连接器的服务账户的 DN 和密码。
    # 此 DN 用于搜索用户和组。
    bindDN: uid=serviceaccount,cn=users,dc=example,dc=com
    # 服务账户密码，创建连接器时必填。
    bindPW: password

    # 登录账户提示。例如，用户名
    usernamePrompt: SSO Username

    # 用户搜索配置
    userSearch:
      # 从基本 DN 开始搜索
      baseDN: cn=users,dc=example,dc=com
      # LDAP 查询语句，用于搜索用户。
      # 例如: "(&(objectClass=person)(uid=<username>))"
      filter: (&(objectClass=organizationalPerson))

      # 以下字段为用户条目属性的直接映射。
      # 用户 ID 属性
      idAttr: uid
      # 必填。映射到电子邮件的属性
      emailAttr: mail
      # 必填。映射到用户名的属性
      nameAttr: cn
      # 登录用户名属性
      # 筛选条件将转换为 "(<attr>=<username>)"，如 (uid=example)。
      username: uid

      # 扩展属性
      # phoneAttr: phone

      # 组搜索配置
```

```
    # 组搜索配置
    groupSearch:
      # 从基本 DN 开始搜索
      baseDN: cn=groups,dc=freeipa,dc=example,dc=com
      # 组过滤条件
      # "(&(objectClass=group)(member=<user uid>))"。
      filter: "(objectClass=group)"
      # 用户组匹配字段
      # 组属性
      groupAttr: member
      # 用户组成员属性
      userAttr: uid
      # 组显示名称
      nameAttr: cn
```

用户过滤器示例

```
# 1. 基本过滤器：查找所有用户
(&(objectClass=person))

# 2. 多条件组合：查找特定部门的用户
(&(objectClass=person)(departmentNumber=1000))

# 3. 查找启用的用户（Active Directory）
(&(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

# 4. 查找特定电子邮件域的用户
(&(objectClass=person)(mail=*@example.com))

# 5. 查找特定组的成员
(&(objectClass=person)(memberOf=cn=developers,ou=groups,dc=example,dc=com))

# 6. 查找最近登录的用户（Active Directory）
(&(objectClass=user)(lastLogon>=20240101000000.0Z))

# 7. 排除系统账户
(&(objectClass=person)(!(uid=admin))(!(uid=system)))

# 8. 查找具有特定属性的用户
(&(objectClass=person)(mobile=*))

# 9. 查找多个部门的用户
(&(objectClass=person)(|(ou=IT)(ou=HR)(ou=Finance)))

# 10. 复杂条件组合示例
(&
  (objectClass=person)
  (|(department=IT)(department=Engineering))
  (!(title=Intern))
  (manager=cn=John Doe,ou=People,dc=example,dc=com)
)
```

组搜索配置示例

```
# 1. 基本过滤器：查找所有组
(objectClass=groupOfNames)

# 2. 查找具有特定前缀的组
(&(objectClass=groupOfNames)(cn=dev-*))

# 3. 查找非空组
(&(objectClass=groupOfNames)(member=*))

# 4. 查找具有特定成员的组
(&(objectClass=groupOfNames)(member=uid=john,ou=People,dc=example,dc=com))

# 5. 查找嵌套组（Active Directory）
(&(objectClass=group)(|(groupType=-2147483646)(groupType=-2147483644)))

# 6. 查找具有特定描述的组
(&(objectClass=groupOfNames)(description=*admin*))

# 7. 排除系统组
(&(objectClass=groupOfNames)(!(cn=system*)))

# 8. 查找具有特定成员的组
(&(objectClass=groupOfNames)(|(cn=admins)(cn=developers)(cn=operators)))

# 9. 查找特定 OU 的组
(&(objectClass=groupOfNames)(ou=IT))

# 10. 复杂条件组合示例
(&
  (objectClass=groupOfNames)
  (|(cn=prod-*)(cn=dev-*))
  (!(cn=deprecated-*))
  (owner=cn=admin,dc=example,dc=com)
)
```

AND(&) 和 OR(|) 运算符在 LDAP 筛选器中的示例

```
# AND 运算符 (&) - 所有条件必须满足
# 语法: (&(condition1)(condition2)(condition3)...)

# 多属性 AND 示例
(&
  (objectClass=person)
  (mail=*@example.com)
  (title=Engineer)
  (manager=*)
)

# OR 运算符 (|) - 至少一个条件必须满足
# 语法: (|(condition1)(condition2)(condition3)...)

# 多属性 OR 示例
(|
  (department=IT)
  (department=HR)
  (department=Finance)
)

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

# 复杂条件组合
(&
  (objectClass=person)
  (|
    (&
      (department=IT)
      (title=*Engineer*)
    )
    (&
      (department=R&D)
      (title=*Developer*)
    )
```

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

同步 LDAP 用户

在成功将 LDAP 用户同步到平台后，您可以在用户列表中查看已同步的用户。

您可以在 添加 LDAP 时配置自动同步策略（可以稍后更新）或在成功添加 LDAP 后手动触发同步。以下是手动触发同步操作的方法。

注意：

- 在与平台集成的 LDAP 中新增的用户可以在执行用户同步操作之前登录平台。一旦他们成功登录平台，其信息将自动同步到平台。
- 从 LDAP 中删除的用户在同步后将显示为 `无效` 状态。
- 新同步用户的默认有效期为 永久。
- 与现有用户（本地用户、IDP 用户）同名的同步用户会自动关联。它们的权限和有效期将与现有用户保持一致。它们可以使用对应来源的登录方式登录平台。

操作程序

1. 在左侧导航栏中，点击 用户 > 身份提供者（**IDP**）。
2. 点击要手动同步的 ***LDAP** 名称*。
3. 点击右上角的 操作 > 同步用户。
4. 点击 同步。

   注意：如果您手动关闭同步提示对话框，将出现确认对话框以确认关闭。关闭同步提示对话框后，系统将继续同步用户。如果您仍在用户列表页面，将收到同步结果反馈。如果您离开用户列表页面，将不会收到同步结果。

相关操作

您可以点击列表页面右侧的
或在详情页面右上角点击 操作 以根据需要更新或删除 LDAP。

操作	描述
更新 **LDAP**	更新已添加 LDAP 的配置信息或 **LDAP** 自动同步策略。 注意：更新 LDAP 后，通过此 LDAP 目前同步到平台的用户也将被更新。从 LDAP 中删除的用户将在平台用户列表中变为无效。您可以通过执行清理无效用户的操作来清理垃圾数据。
删除 **LDAP**	删除 LDAP 后，通过此 LDAP 同步到平台的所有用户将变为 无效 状态（用户与角色之间的绑定关系保持不变），并且他们无法登录平台。重新集成后，需要重新执行同步以激活用户。 提示：删除 IDP 后，如果需要删除通过 LDAP 同步到平台的用户和用户组，请在提示框下方勾选 清理 **IDP** 用户和用户组 复选框。

OIDC 管理

平台支持 OIDC（OpenID Connect）协议，平台管理员可以在添加 OIDC 配置后，使用第三方账户登录。平台管理员还可以更新和删除已配置的 OIDC 服务。

目录

OIDC 概述

OIDC（OpenID Connect）是基于 OAuth 2.0 协议的身份认证标准协议。它使用 OAuth 2.0 授权服务器为第三方客户端提供用户身份认证，并将相应的身份认证信息传递给客户端。

OIDC 允许所有类型的客户端（包括服务器端、移动设备和 JavaScript 客户端）请求并接收经过身份验证的会话及最终用户信息。此规范套件是可扩展的，允许参与者使用可选功能，例如身份数据加密、OpenID 提供者发现和会话管理，当它们有意义时。有关更多信息，请参见 OIDC 官方文档↗。

添加 OIDC

通过添加 OIDC，您可以使用第三方平台账户登录平台。

注意：在 OIDC 用户成功登录平台后，平台将使用用户的电子邮件属性作为唯一标识符。支持 OIDC 的第三方平台用户必须具有 **email** 属性；否则，他们将无法登录平台。

操作流程

1. 在左侧导航栏中，点击 用户 > 身份提供者（**IDPs**）。
2. 点击 添加 **OIDC**。
3. 配置 基本信息 参数。
4. 配置 **OIDC** 服务器配置 参数：
   - 身份提供者 **URL**：发行者 URL，即 OIDC 身份提供者的访问地址。
   - 客户端 **ID**：OIDC 客户端的客户端标识符。
   - 客户端密钥：OIDC 客户端的密钥。
   - 重定向 **URI**：登录第三方平台后的回调地址，即 dex 发行者的 URL + `/callback`。
   - 登出 **URL**：用户执行 登出 操作后访问的地址。如果为空，登出地址将是平台的初始登录页面。
5. 在 身份提供者服务配置验证 区域，输入有效 OIDC 账户的 用户名 和 密码 以验证配置。

   提示：如果用户名和密码不正确，添加时将报告错误，指示凭据无效，无法添加 OIDC。
6. 点击 创建。

通过 **YAML** 添加 **OIDC**

除了表单配置外，该平台还支持通过 YAML 添加 OIDC，这允许更灵活地配置身份验证参数、声明映射、用户组同步和其他高级功能。

示例：配置 **OIDC** 连接器

以下示例演示如何配置 OIDC 连接器，以集成 OIDC 身份认证服务。此配置示例适用于以下场景：

1. 需要将 OIDC 集成作为身份认证服务器。
2. 需要支持用户组信息同步。
3. 需要自定义登出重定向地址。
4. 需要配置特定的 OIDC 范围。
5. 需要自定义声明映射。

```yaml
apiVersion: dex.coreos.com/v1
kind: Connector
# 连接器基本信息
id: oidc                # 连接器唯一标识符
name: oidc              # 连接器显示名称
type: oidc              # 连接器类型为 OIDC
metadata:
  annotations:
    cpaas.io/description: "11"  # 连接器描述
  name: oidc
  namespace: cpaas-system
spec:
  config:
    # OIDC 服务器配置
    # 配置服务器连接信息，包括服务器地址、客户端凭据和回调地址
    issuer: http://auth.com/auth/realms/master                # OIDC 服务器地址
    clientID: dex                                             # 客户端 ID
    # 服务帐户密钥，仅在第一次创建连接器资源时有效
    clientSecret: xxxxxxx
    redirectURI: https://example.com/dex/callback             # 回调地址，必须与

    # 安全配置
    # 配置 SSL 验证和用户信息获取方法
    insecureSkipVerify: true                                  # 是否跳过 SSL 验证
    getUserInfo: false                                        # 是否通过 UserInfo

    # 登出配置
    # 配置用户登出后重定向地址
    logoutURL: https://test.com                               # 登出重定向地址，可以

    # 范围配置
    # 配置所需的授权范围，确保 OIDC 服务器支持这些范围
    scopes:
      - openid                                                # 必需，用于 OIDC 基
      - profile                                               # 可选，用于获取用户基
      - email                                                 # 可选，用于获取用户电

    # 声明映射配置
    # 配置 OIDC 返回的声明与平台用户属性之间的映射关系
    claimMapping:
      email: email                                            # 电子邮件映射，用于用
      groups: groups                                          # 用户组映射，用于组织
      phone: ""                                               # 电话映射，选填
```

```
    preferred_username: preferred_username                    # 用户名映射，用于显示

  # 用户组配置
  # 配置与用户组同步相关的参数，确保令牌包含组信息
  groupsKey: groups                                           # 指定组信息的键名称
  insecureEnableGroups: false                                 # 是否启用组同步功能
```

相关操作

您可以在列表页面右侧点击
或在详细信息页面右上角点击 操作 来根据需要更新或删除 OIDC。

操作	描述
更新 **OIDC**	更新已添加的 OIDC 配置。在更新 OIDC 配置信息后，原有用户和认证方法将根据当前配置被重置和同步。
删除 **OIDC**	删除平台不再使用的 OIDC。在删除 OIDC 后，通过该 OIDC 同步到平台的所有用户将具有 无效 状态（用户与角色之间的绑定关系保持不变），并且他们无法登录平台。重新集成后，用户可以通过成功登录平台激活。 提示：在删除身份提供者后，如果需要删除通过 OIDC 同步到平台的用户和用户组，请勾选提示框下的 清除身份提供者用户和用户组 复选框。

Menu

故障排除

删除用户

目录

问题描述

问题：在创建或同步新用户时，系统提示该用户已存在。您应该如何处理这个问题？

出于安全原因，该平台不允许创建名称与之前已删除用户相同的新用户（包括本地用户和身份提供者用户）。这一限制适用于：

- 创建名称与已删除用户相同的新本地用户
- 同步名称与已删除用户相同的身份提供者用户

在升级到当前版本后，您可能会遇到此问题，当：

- 创建名称与升级前已删除用户相同的新用户时
- 同步名称与升级前已删除用户相同的新用户时

解决方案

要解决此问题，您需要通过在全局集群的控制节点上执行特定脚本来清除已删除的用户信息。

清理已删除的身份提供者用户

在全局集群的任何控制节点上执行以下命令：

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

示例：

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

清理已删除的本地用户

在全局集群的任何控制节点上按顺序执行这两个脚本：

1. 清理用户密码：

```
kubectl get users -l 'auth.cpaas.io/user.connector_id=local,auth.cpaas.io/use
```

1. 清理用户：

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

Menu

用户策略

介绍

该平台提供全面的用户安全策略，以增强登录安全性并防止恶意攻击。

目录

概述

平台支持以下安全策略：

- 密码安全管理
- 用户账户禁用
- 用户账户锁定
- 用户通知
- 访问控制

配置安全策略

步骤

1. 在左侧导航栏中，点击 用户角色管理 > 用户安全策略
2. 在右上角点击 更新
3. 根据需要配置安全策略
4. 点击 更新 保存更改

WARNING

策略配置注意事项：

- 勾选框以启用相应策略
- 取消勾选框以禁用相应策略
- 被禁用的策略会保留其配置数据
- 重新启用策略时，先前的设置将被恢复

可用策略

策略	描述
用户身份验证策略	启用基于密码登录的双重身份验证： - 用户通过指定的通知方式接收验证码 - 支持多种通知服务器（例如，企业通信工具服务器）
密码安全策略	管理密码要求： 首次登录： - 在首次平台登录时强制用户更改密码 定期更新： - 在规定期限内要求用户更改密码（例如，90天） - 密码未更新前禁止登录
用户禁用策略	自动禁用不活跃账户： - 在规定的无登录期限后触发

策略	描述
用户锁定策略	防止暴力破解攻击： 锁定条件： - 在24小时内指定次数的登录失败后触发 锁定时长： - 账户将锁定指定分钟数 - 锁定期过后自动解锁
通知策略	管理用户通知： - 用户创建后通过电子邮件发送初始密码
访问控制	管理用户会话和访问： 会话管理： - 在指定时间后自动注销不活跃会话 - 限制最大并发在线用户数 浏览器控制： - 当所有产品标签页关闭时结束会话 - 防止同一客户端重复登录 - 重要注意事项： - 访问控制仅影响更新策略后的新登录 - 浏览器标签页恢复可能不会触发会话结束 - 防止重复登录时仅允许每个客户端最后一次登录。

Menu

多租户（项目）

介绍

介绍

Project

Namespaces

Clusters、Projects 和 Namespaces 之间的关系

功能指南

创建项目

步骤

管理项目

更新基本项目信息

更新项目配额

删除项目

管理项目集群

介绍

添加集群

移除集群

管理项目成员

导入成员

移除成员

介绍

目录

Project

Project 是一个资源隔离单元，支持企业中的多租户使用场景。它将一个或多个集群的资源划分为隔离的环境，确保资源和人员的隔离。Project 可以代表企业中的不同子公司、部门或项目团队。通过 Project 管理，可以实现：

- 项目团队之间的资源隔离
- 租户内的配额管理
- 高效的资源分配与控制

Namespaces

Namespaces 是 Project 内更小的相互隔离的资源空间，作为用户实现生产工作负载的工作区。Namespaces 的主要特点包括：

- 一个 Project 下可以创建多个 Namespace
- 所有 Namespace 的资源配额总和不能超过 Project 的配额
- 资源配额在 Namespace 级别进行更细粒度的分配

- 容器规格（CPU、内存）在 Namespace 级别受限
- 通过细粒度控制提升资源利用率

Clusters、Projects 和 Namespaces 之间的关系

平台的资源层级遵循以下规则：

- 一个 Project 可以使用来自多个集群的资源（CPU、内存、存储），一个集群也可以向多个 Project 分配资源。
- 一个 Project 下可以创建多个 Namespace，且它们的资源配额总和不得超过 Project 的总资源。
- 一个 Namespace 的资源配额必须来自单个集群，且一个 Namespace 只能属于一个 Project。

Menu

功能指南

创建项目

步骤

管理项目

更新基本项目信息

更新项目配额

删除项目

管理项目集群

介绍

添加集群

移除集群

管理项目成员

导入成员

移除成员

创建项目

在您的项目团队开始工作之前，您可以基于平台上现有的集群资源创建一个项目。该项目在资源和人员方面将与其他项目（租户）隔离。在创建项目时，您可以根据项目规模和实际业务需求分配资源。该项目可以利用平台上多个集群的资源。

WARNING

在创建项目时，平台将会自动在相关集群中创建一个与项目同名的命名空间，以隔离平台级别的资源。请勿修改此命名空间或其资源。

目录

步骤

1. 在 项目管理 视图中，点击 创建项目。

2. 在 基本信息 页面中，配置以下参数：

参数	描述
名称	项目的名称，不能与现有项目名称相同或与项目名称黑名单中的任何名称相同。否则，项目将无法创建。 注意: 项目名称黑名单包括平台集群下的特殊命名空间名称：`cpaas-system`，`cert-manager`，`default`，`global-credentials`，`kube-ovn`，`kube-`

参数	描述
	`public`，`kube-system`，`nsx-system`，`alauda-system`，`kube-federation-system`，`ALL-ALL`，以及 `true`。
集群	与项目相关的集群，管理员可以在这些集群中分配资源配额。点击下拉选择框选择一个或多个集群。 注意: 处于异常状态的集群无法被选中。

3. 点击 下一步，在项目配额设置步骤中，设置要为所选集群分配给当前项目的资源配额。具体包括：

   - CPU（核）
   - 内存（Gi）
   - 存储（Gi）
   - PVC 数量（个）
   - Pods 数量（个）
   - 虚拟 GPU（GPU-Manager/MPS）
   - pGPU（物理 GPU，核）
   - GPU 内存

NOTE

- 仅在集群中部署了 GPU 插件时，才能配置 GPU 资源配额。当 GPU 资源为 **GPU-Manager** 或 **MPS GPU** 时，也可以配置 **vMemory** 配额。

  GPU 单位：100 单位的虚拟核心等于 1 个物理核心（1 pGPU = 1 核 = 100 GPU-Manager 核 = 100 MPS 核），pGPU 单位只能以整数形式分配。GPU-Manager 1 单位的内存相当于 256 Mi，MPS GPU 1 单位的内存相当于 1 Gi，1024 Mi = 1 Gi。
- 如果某种类型的资源未设置配额，则默认为 无限制。这意味着项目可以根据需要使用集群中相应类型的可用资源，而不受最大限制。
- 设置的项目配额值应在页面上显示的配额范围内。在每个资源配额输入框下，将显示该资源的分配配额和总信息作为参考。

1. 点击 创建项目。

管理项目

本指南说明了如何更新指定项目的基本信息和项目配额，或者删除项目。

目录

更新基本项目信息

更新指定项目的基本信息，如显示名称和描述。

步骤

1. 在 项目管理 视图中，单击要更新的项目名称。
2. 在左侧导航窗格中，单击 详细信息。
3. 点击右上角的 操作 > 更新基本信息。
4. 修改或输入 显示名称 和 描述。
5. 点击 更新。

更新项目配额

更新项目在每个关联集群中的资源配额。

约束和限制

当项目与 异常 集群关联时，不支持更新该集群中分配给项目的配额。

步骤

1. 在 项目管理 视图中，单击要更新的项目名称。
2. 在左侧导航窗格中，单击 详细信息。
3. 点击配额区域右侧的 更新配额。
4. 根据以下指南更新分配给项目在集群中的配额：

NOTE

- GPU (vGPU/pGPU) 资源配额仅在集群中部署了 GPU 资源时可以配置。

  当 GPU 资源为 **vGPU** 时，**vMemory** 配额也可以配置。

  GPU 单位：100 个虚拟核心等于 1 个物理核心 (1 pGPU = 1 核心 = 100 vGPU)；1 个视频内存单位为 256 Mi；pGPU 单位为整数，只能按整数分配。
- 如果某个资源未设置配额，则该资源将默认具有无限配额。
- 设置的配额值应在页面上显示的配额范围内。

1. 点击 更新。

删除项目

删除不再使用的项目。

> **WARNING**
>
> 删除项目后，项目在集群中占用的资源将被释放。

步骤

1. 在 项目管理 视图中，单击要删除的项目名称。
2. 在左侧导航栏中，单击 详细信息。
3. 点击右上角的 操作 > 删除项目。
4. 输入项目名称并点击 删除。

管理项目集群

本指南解释了如何管理项目的集群关联。您可以添加集群以将其资源分配给项目，或者移除集群以回收已分配的资源。

目录

介绍

您可以向项目添加集群以分配其资源，或移除集群以回收已分配的资源。此功能在以下场景中非常有用：

- 当项目资源不足以支持业务运营时
- 当新创建或添加的集群需要分配到现有项目时
- 当需要从项目中回收集群资源时
- 当特定项目需要对某个集群的独占访问时

添加集群

将集群添加到项目并设置其资源配额。

过程

1. 在 项目管理 视图中，点击您希望添加集群的项目名称。
2. 在左侧导航栏中，点击 详细信息。
3. 在右上角点击 操作 > 添加集群。
4. 选择集群并设置将分配给当前项目的资源配额。可以配置以下资源：
   - CPU（核心）
   - 内存（Gi）
   - 存储（Gi）
   - PVC 数量（数量）
   - Pods（数量）
   - vGPU（虚拟 GPU）/MPS/pGPU（物理 GPU，核心）
   - 视频内存配额

NOTE

- 仅在集群中部署了 GPU 插件时，才能配置 GPU 资源配额。

  当 GPU 资源为 **GPU-**管理或 **MPS GPU** 时，也可以配置 **vMemory** 配额。

  GPU 单位：100 个虚拟核心等于 1 个物理核心（1 pGPU = 1 核心 = 100 GPU-管理核心 = 100 MPS 核心），且 pGPU 单位仅能以整数分配。GPU-管理 1 单位内存等于 256 Mi，MPS GPU 1 单位内存等于 1 Gi，1024 Mi = 1 Gi。
- 如果未设置某种类型资源的配额，则默认为 无限。这意味着项目可以根据需要使用集群中该类型的可用资源，而没有上限。
- 设置的项目配额值应在页面上显示的配额范围内。在每个资源配额输入框下，会显示已分配的配额和该资源的总量以供参考。

5. 点击 添加。

移除集群

移除与项目关联的集群。

WARNING

- 移除集群后，项目无法使用已移除集群下的业务资源。
- 当要移除的集群出现异常时，异常集群下的资源无法清理。建议在移除前修复该集群。

过程

1. 在 项目管理 视图中，点击您希望移除集群的项目名称。
2. 在左侧导航栏中，点击 详细信息。
3. 在右上角点击 操作 > 移除集群。
4. 在弹出的 移除集群 对话框中，输入要移除的集群名称，然后点击 移除 按钮以成功移除该集群。

管理项目成员

本指南解释了如何管理项目成员，包括导入成员和分配与项目相关的角色。

目录

导入成员

您可以通过导入现有平台用户或添加 OIDC 用户来授予用户对项目及其命名空间的操作权限。您可以分配角色，如项目管理员、命名空间管理员、开发人员或具有项目和命名空间管理权限的自定义角色。

约束与限制

- 当平台上未配置 OIDC IDP 时：
  - 只能将现有平台用户导入为项目成员，包括：
    - 已成功登录的 OIDC 用户
    - 通过 LDAP 同步的用户

    - 本地用户
    - 以 OIDC 用户身份添加到其他项目的用户（来源标记为 `-`）
- 当配置了 OIDC IDP 时：
    - 您可以添加符合输入要求的有效 OIDC 帐户
    - 添加时无法验证帐户的有效性
    - 确保帐户有效，否则将无法正常登录
- 系统默认管理员用户和当前登录用户无法被导入

操作步骤

1. 在 项目管理 视图中，点击要管理的项目名称。
2. 在左侧导航栏中，点击 成员。
3. 点击 导入成员。
4. 选择 成员列表 或 **OIDC** 用户。

从成员列表导入

您可以从成员列表中导入所有用户或选定用户。

> **TIP**
>
> 使用右上角的用户组下拉菜单和搜索框按用户名过滤用户。

导入所有用户：

1. 选择 成员列表。
2. 点击 绑定 下拉菜单，选择要分配给所有用户的角色。
   如果角色需要命名空间，请从 命名空间 下拉菜单中选择。
3. 点击 导入全部。

导入特定用户：

1. 选择 成员列表。

2. 使用复选框选择一个或多个用户。

3. 点击 绑定 下拉菜单，选择要分配给选定用户的角色。
   如果角色需要命名空间，请从 命名空间 下拉菜单中选择。

4. 点击 导入。

导入 **OIDC** 用户

1. 选择 **OIDC** 用户。

2. 点击 添加 创建成员记录（对于多个成员重复此操作）。

3. 在 名称 字段中输入 OIDC 认证的用户名。

> **WARNING**
>
> 确保用户名对应于可以被配置的 OIDC 系统认证的帐户，否则登录将失败。

4. 从 角色 下拉菜单中选择角色。
   如果角色需要命名空间，请从 命名空间 下拉菜单中选择。

5. 点击 导入。

成功导入后，您可以查看：

- 项目成员列表中的成员
- 平台管理 **>** 用户 中的用户
  - 来源显示为 "-"，直到首次登录/同步
  - 来源在成功登录/同步后更新

移除成员

移除项目成员以撤销其权限。

操作步骤

1. 在 项目管理 视图中，点击项目名称。

2. 在左侧导航栏中，点击 成员。

> **TIP**
>
> 使用搜索框旁边的下拉列表按 姓名、显示名称 或 用户组 过滤成员。

3. 点击要移除的成员旁边的 移除。

4. 在提示对话框中确认移除。

Menu

审计

介绍

该平台的审计功能提供与用户和系统安全相关的按时间顺序记录的操作记录。这有助于您分析特定问题，并快速解决在集群、自定义应用及其他领域发生的问题。

通过审计，您可以跟踪 Kubernetes 集群中的各种变化，包括：

- 在特定时间段内集群发生了哪些变化
- 谁实施了这些变化（系统组件或用户）
- 重要变更事件的详细信息（例如，POD 参数更新）
- 事件结果（成功或失败）
- 操作员位置（集群内部或外部）
- 用户操作记录（更新、删除、管理操作）及其结果

目录

前提条件

您的账户必须具备平台管理或平台审计权限。

操作步骤

1. 在左侧导航栏中，点击 审计。

2. 从标签中选择审计范围：

   - 用户操作：查看已登录平台的用户的操作记录
   - 系统操作：查看系统操作记录（操作员以 `system:` 开头）

3. 配置查询条件以过滤审计事件：

查询条件	描述
操作员	操作员的用户名或系统账户名（默认：`所有`）
操作类型	操作的类型（创建、更新、删除、管理、回滚、停止等，默认：`所有`）
集群	包含被操作资源的集群（默认：`所有`）
资源类型	被操作资源的类型（默认：`所有`）
资源名称	被操作资源的名称（支持模糊搜索）

4. 点击 搜索。

TIP

- 使用 时间范围 下拉框设置审计时间范围（默认：`过去 30 分钟`）。您可以选择预设范围或自定义范围。
- 点击刷新图标以更新搜索结果。
- 点击导出图标以下载结果为 `.csv` 文件。

搜索结果

搜索结果显示以下信息：

参数	描述
操作员	操作员的用户名或系统账户名
操作类型	操作的类型（创建、更新、删除、管理、回滚、停止等）
资源名称/类型	被操作资源的名称和类型
集群	包含被操作资源的集群
命名空间	包含被操作资源的命名空间
客户端 IP	执行操作所使用的客户端的 IP 地址
操作结果	基于 API 返回代码的操作结果（2xx = 成功，其他 = 失败）
操作时间	操作的时间戳
详细信息	点击 详细信息 按钮以在 审计详细信息 对话框中以 JSON 格式查看完整的审计记录

Menu

遥测

安装

ACP Telemetry 是一个平台服务，用于收集集群的遥测数据，以支持在线运维。它收集系统指标并上传至 Alauda Cloud 进行监控和分析。

目录

先决条件

安装前，请确保：

- Alauda Container Platform 拥有有效的许可证
- global 集群具备互联网访问能力

安装步骤

1. 进入 **Platform Management**
2. 在左侧导航栏点击 **Marketplace** > **Cluster Plugins**
3. 在顶部导航栏选择 **global** 集群
4. 搜索 **ACP Telemetry** 并点击查看详情

5. 点击 **Install** 部署插件

启用在线运维

1. 在左侧导航栏点击 **System Settings** > **Platform Maintenance**
2. 点击 **Online Operations** 的 **On** 按钮

卸载步骤

1. 按照安装流程的步骤 1-4 定位插件
2. 点击 **Uninstall** 卸载插件