Security

Security and Compliance

- Compliance
- API Refiner

Users and Roles

- User
- Group
- Role
- IDP
- User Policy

Multitenancy(Project)

Introduction

- Project
- Namespaces
- Relationship Between Clusters, Projects, and Namespaces

Guides

Audit

Introduction

Prerequisites

Procedure

Search Results

Telemetry

Install

Prerequisites

Installation Steps

Enable Online Operations

Uninstallation Steps

Certificates

cert-manager

Overview

How it works

Identifying cert-manager Managed Certific

Related Resources

OLM Certificates

Certificate M

Certificate Statu

Rotate TLS Certs of Platform Access Address

Prerequisites

Procedures

Security and Compliance

Compliance

Install

API Refiner

Introduction

- Product Introduction
- Product Advantages
- Scenarios
- Limitations

Install

- Installation Steps
- Uninstallation Steps
- Default Configuration

Compliance

Install

Alauda Compliance with Kyverno

Installation Steps

Uninstallation Steps

Install

Alauda Compliance with Kyverno

Installation Steps

Uninstallation Steps

Alauda Compliance with Kyverno

Alauda Compliance with Kyverno is a platform service that integrates Kyverno for managing compliance policies on the Alauda Container Platform.

TOC

Installation Steps

Uninstallation Steps

Installation Steps

1. Navigate to **Platform Management**
2. In the left navigation bar, click **Marketplace** > **Cluster Plugins**
3. Search for **Alauda Compliance with Kyverno** and click to view its details
4. Click **Install** to deploy the plugin

Uninstallation Steps

1. Follow steps 1-3 from the installation process to locate the plugin
2. Click **Uninstall** to remove the plugin

API Refiner

Introduction

- Product Introduction
- Product Advantages
- Scenarios
- Limitations

Install

- Installation Steps
- Uninstallation Steps
- Default Configuration

Introduction

TOC

Product Introduction
Product Advantages
Scenarios
Limitations

Product Introduction

ACP API Refiner is a data filtering service provided by the Alauda Container Platform that enhances multi-tenant security and data isolation in Kubernetes environments. It filters Kubernetes API response data based on user permissions, projects, clusters, and namespaces, while also supporting field-level filtering, inclusion, and data desensitization.

Product Advantages

The core advantages of ACP API Refiner are as follows:

- **Multi-dimensional Data Isolation**
  - Supports filtering API responses based on project, cluster, and namespace dimensions
  - Ensures proper data boundaries between different tenants
  - Prevents unauthorized access to cluster-scoped resources

- **Flexible Data Filtering**
  - Supports excluding, including, and desensitizing specific fields in API responses
  - Configurable filtering rules through YAML configuration
  - Dynamic generation of resource Ingress for different resource types
- **Enhanced Security**
  - Implements JWT token-based user authentication
  - Provides fine-grained access control based on user permissions
  - Supports data desensitization for sensitive information

Scenarios

The main application scenarios of ACP API Refiner are as follows:

- **Multi-tenant Environment**
  - Ensures proper data isolation between different tenants
  - Prevents unauthorized access to cluster-scoped resources
  - Manages shared namespace scenarios effectively
- **Sensitive Data Protection**
  - Filters sensitive information from API responses
  - Supports field-level data desensitization
  - Protects sensitive metadata and annotations
- **Compliance Requirements**
  - Helps meet data isolation requirements
  - Supports audit and compliance needs
  - Maintains data access boundaries

Limitations

The following limitations apply to ACP API Refiner:

- Resources must contain specific tenant-related labels for data isolation:
  - `cpaas.io/project`
  - `cpaas.io/cluster`
  - `cpaas.io/namespace`
  - `kubernetes.io/metadata.name`
  - Optional: `cpaas.io/creator`
- LabelSelector queries do not support logical OR operations
- Platform-level userbindings are not filtered
- Filtering is only applied to GET and LIST API operations

Install

ACP API Refiner is a platform service that filters Kubernetes API response data. It provides filtering capabilities by project, cluster, and namespace, and supports field exclusion, inclusion, and desensitization in API responses.

TOC

- Installation Steps
- Uninstallation Steps
- Default Configuration
  - Filtered Resources
  - Field Desensitization

Installation Steps

1. Navigate to **Platform Management**
2. In the left navigation bar, click **Marketplace** > **Cluster Plugins**
3. Select the **global** cluster in the top navigation bar
4. Search for **ACP API Refiner** and click to view its details
5. Click **Install** to deploy the plugin

Uninstallation Steps

1. Follow steps 1-4 from the installation process to locate the plugin
2. Click **Uninstall** to remove the plugin

Default Configuration

Filtered Resources

The following resources are filtered by default:

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

Field Desensitization

By default, the following field is desensitized:

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

Users and Roles

User

Introduction

- User Sources
- User Management Rules
- User Lifecycle

Guides

Group

Introduction

- Group Introduction
- Group Types

Guides

Role

Introduction

- Role Introduction
- System Roles

Guides

Custom Roles

IDP

Introduction

Overview

Supported Integration Methods

Guides

Troublesho

User Policy

Introduction

Overview

Configure Security Policy

Available Policies

User

Introduction

Introduction

User Sources

User Management Rules

User Lifecycle

Guides

Manage User Roles

Add Roles

Remove Roles

Create User

Steps

User Manag

Reset Local Us

Update User E

Activate User

Disable User

Add User to Lo

Delete User

Batch Operatio

Introduction

The platform supports user authentication and login verification for all users.

TOC

- User Sources
  - Local Users
  - Third-Party Users
    - LDAP Users
    - OIDC Users
    - Other Third-Party Users
- User Management Rules
- User Lifecycle

User Sources

Local Users

- Administrator account created during platform deployment
- Accounts created through the platform interface
- Users added through local dex configuration file

Third-Party Users

LDAP Users

- Enterprise users synchronized from LDAP servers
- Accounts are imported through IDP (Identity Provider) integration
- Source is displayed as the IDP configuration name
- Integration is configured through IDP settings

OIDC Users

- Third-party platform users authenticated via OIDC protocol
- Source is displayed as the IDP configuration name
- Integration is configured through IDP settings

> **WARNING**
>
> For OIDC users added to a project before their first login:
>
> - Source is displayed as "-" until successful platform login
> - After successful login, source changes to the IDP configuration name

Other Third-Party Users

- Users authenticated through supported dex connectors (e.g., GitHub, Microsoft)
- For more information, refer to the dex official documentation ↗

User Management Rules

> **WARNING**
>
> Please note the following important rules:
>
> - Local usernames must be unique across all user types

- Third-party users (OIDC/LDAP) with matching usernames are automatically associated
- Associated users inherit permissions from existing accounts
- Users can log in through their respective sources
- Only one user record is displayed per username in the platform
- User source is determined by the most recent login method

User Lifecycle

The following table describes different user statuses on the platform:

Status	Description
Normal	User account is active and can log in to the platform
Disabled	User account is inactive and cannot log in. Contact platform administrator for activation. Possible reasons: - No login for 90+ consecutive days - Account expiration - Manual disable by administrator
Locked	Account is temporarily locked due to 5 failed login attempts within 24 hours. Details: - Lock duration: 20 minutes - Can be manually unlocked by administrator - Account becomes available after lock period
Invalid	LDAP-synchronized account that has been deleted from the LDAP server. Note: Invalid accounts cannot log in to the platform

Guides

Manage User Roles

- Add Roles
- Remove Roles

Create User

- Steps

User Manag

- Reset Local Us
- Update User E
- Activate User
- Disable User
- Add User to Lo
- Delete User
- Batch Operatio

Manage User Roles

Platform administrators can manage roles for other users (not their own account) to grant or revoke permissions.

TOC

- Add Roles
  - Steps
- Remove Roles
  - Steps

Add Roles

Steps

1. In the left navigation bar, click **Users** > **User Management**
2. Click the username of the target user
3. Scroll to the **Role List** section
4. Click **Add Role**
5. In the role assignment dialog:
   - Select a role from the **Role Name** dropdown
   - Choose the role's permission scope (cluster, project, or namespace)

- Click **Add**

> **NOTE**
>
> Important Notes:
>
> - You can add multiple roles to a user
> - Each role can only be added once per user
> - Already assigned roles appear in the dropdown but cannot be selected
> - The **Cluster Administrator** role cannot be assigned for the global cluster

Remove Roles

Steps

1. In the left navigation bar, click **Users** > **User Management**
2. Click the username of the target user
3. Scroll to the **Role List** section
4. Click **Remove** next to the role you want to remove
5. Confirm the removal

> **WARNING**
>
> Role Management Permissions:
>
> - Only platform administrators can manage roles for other users
> - Users cannot modify roles for their own account

Create User

Users with platform administrator roles can create local users and assign roles to them through the platform interface.

TOC

Steps

Steps

1. In the left navigation bar, click **Users** > **User Management**
2. Click **Create User**
3. Configure the following parameters:

Parameter	Description
Password Type	Select a password generation method: **Random**: System generates a secure random password **Custom**: User manually enters a password
Password	Enter or generate a password based on the selected type. Password Requirements: - Length: 8-32 characters - Must contain letters and numbers

Parameter	Description
	- Must contain special characters (`~!@#$%^&*() -_=+?`) Password Field Features: - Click the eye icon to show/hide password - Click the copy icon to copy password
Mailbox	User's email address: - Must be unique - Can be used as login username - Associated with user's name
Validity Period	Set the user's account validity period: Options: - **Permanent**: No time limit - **Custom**: Set start and end times using the Time Range dropdown
Roles	Assign one or more roles to the user
Continue Creating	Toggle switch to control post-creation behavior: - **On**: Redirects to new user creation page - **Off**: Shows user details page

4. Click **Create**

NOTE

After successful user creation:

- If "Continue Creating" is enabled, you'll be redirected to create another user
- If disabled, you'll see the created user's details page

User Management

The platform provides flexible user management capabilities, supporting both individual user management and batch operations for improved efficiency in specific scenarios (e.g., on-site or off-site teams).

WARNING

Important Restrictions:

- System-generated accounts cannot be managed (platform administrator role, local source)
- Currently logged-in users cannot manage their own accounts
- For personal account modifications (display name, password), please use the personal information page

TOC

- Reset Local User Password
  - Steps
- Update User Expiry Date
  - Steps
- Activate User
  - Steps
- Disable User
  - Steps
- Add User to Local User Group
  - Steps

Delete User

Steps

Batch Operations

Steps

Reset Local User Password

Users with platform management permissions can reset passwords for other local users.

Steps

1. In the left navigation bar, click **Users** > **User Management**
2. Click the icon next to the target user's record
3. Click **Reset Password**
4. In the dialog box, select a password type:
   - **Random**: System generates a secure random password
   - **Custom**: Enter a new password manually

> **NOTE**
>
> Password Requirements:
>
> - Length: 8-32 characters
> - Must contain letters and numbers
> - Must contain special characters (`~!@#$%^&*() -_=+?`)
>
> Password Field Features:
>
> - Click eye icon to show/hide password
> - Click copy icon to copy password

5. Click **Reset**

Update User Expiry Date

You can update expiry dates for users in **normal**, **disabled**, or **locked** status. Users exceeding their expiry date will be automatically disabled.

Steps

1. In the left navigation bar, click **Users** > **User Management**
2. Click **Update Expiry Date** next to the target user
3. In the dialog box, select an expiry date option:
   - **Permanent**: No time limit
   - **Custom**: Set start and end times using the Time Range dropdown
4. Click **Update**

Activate User

You can activate users in **disabled** or **locked** status.

> **NOTE**
>
> Activation Behavior:
>
> - If user is within expiry date: expiry date remains unchanged
> - If user has expired: expiry date becomes **Permanent**

Steps

1. In the left navigation bar, click **Users** > **User Management**
2. Click **Activate** next to the target user

3. Click **Activate** in the confirmation dialog
4. User status will change to **normal**

Disable User

You can disable users in **normal** or **locked** status within their expiry date. Disabled users cannot log in but can be reactivated.

Steps

1. In the left navigation bar, click **Users** > **User Management**
2. Click the icon next to the target user
3. Click **Disable** and confirm

Add User to Local User Group

You can add users with **Source** as **Local** or `LDAP` to one or more local user groups.

> **WARNING**
>
> Group Role Behavior:
>
> - Users automatically inherit roles from their groups
> - Group roles are only visible on the group's details page (Configure Roles tab)
> - Individual user role lists only show directly assigned roles

Steps

1. In the left navigation bar, click **Users** > **User Management**
2. Click the icon next to the target user
3. Click **Add to User Group**

4. Select one or more local user groups
5. Click **Add**

Delete User

Platform administrators can delete any user except the currently logged-in account, including:

- IDP-configured users
- Users with source `-`
- Local users

Steps

1. In the left navigation bar, click **Users** > **User Management**
2. Click the icon next to the target user
3. Click **Delete**
4. Click **Confirm**

Batch Operations

You can perform batch operations for:

- Updating validity periods
- Activating users
- Disabling users
- Deleting users

Steps

1. In the left navigation bar, click **Users** > **User Management**
2. Select one or more users using checkboxes

3. Click **Batch Operations** and select an action:

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

> **NOTE**
>
> Batch Operation Details:
>
> - **Update Validity**: Set permanent or custom time range
> - **Activate**: Confirm activation in dialog
> - **Deactivate**: Confirm deactivation in dialog
> - **Delete**: Enter current account password and confirm

Group

Introduction

Introduction

Group Introduction

Group Types

Guides

Manage User Group Roles

Add Role to Group

Remove Role from Group

Create Local User Group

Create User Group

Manage User Groups

Manage Loc

Prerequisites

Import Member

Remove Memb

Introduction

TOC

Group Introduction
Group Types
Local User Group
IDP-Synchronized User Group

Group Introduction

The platform supports user management through user groups. By managing group roles, you can efficiently:

- Grant platform operation permissions to multiple users simultaneously
- Revoke permissions from multiple users at once
- Implement batch role-based access control

For example, when personnel changes occur within an enterprise and you need to grant new project or namespace operation permissions to multiple users, you can:

1. Create a user group
2. Import relevant users as group members
3. Configure project and namespace roles for the group
4. Apply unified permissions to all group members

Group Types

The platform supports two types of groups:

Local User Group

- Created directly on the platform
- Source is displayed as **Local**
- Can be updated or deleted
- Supports:
  - Adding or removing users from any source
  - Adding or removing roles

IDP-Synchronized User Group

- Synchronized from connected IDP (LDAP, Azure AD)
- Source is displayed as the connected ***IDP*** name
- Cannot be updated or deleted
- Supports:
  - Adding or removing roles
  - Cannot manage group members (add or remove)

Guides

Manage User Group Roles

- Add Role to Group
- Remove Role from Group

Create Local User Group

- Create User Group
- Manage User Groups

Manage Loc

- Prerequisites
- Import Member
- Remove Memb

Manage User Group Roles

Users with platform management permissions can manage roles for both local user groups and IDP-synchronized user groups.

TOC

- Add Role to Group
  - Steps
- Remove Role from Group
  - Steps

Add Role to Group

Steps

1. In the left navigation bar, click **Users** > **User Group Management**
2. Click the name of the target user group
3. On the **Configure Role** tab, click **Add Role**
4. Click to add a role

> **NOTE**
>
> Role Assignment Rules:

- You can add multiple roles to a group
- Each role can only be added once to the same group

5. Select the role name from the dropdown
6. Choose the role's permission scope (cluster, project, or namespace)
7. Click **Add**

Remove Role from Group

WARNING

When you remove a role from a group:

- All permissions granted by that role to group members will be revoked
- This action cannot be undone

Steps

1. In the left navigation bar, click **Users** > **User Group Management**
2. Click the name of the target user group
3. On the **Configure Role** tab, click **Remove** next to the role
4. Click **Confirm** to remove the role

Create Local User Group

Local user groups allow you to implement role-based access control for multiple users from any source.

TOC

- Create User Group
  - Steps
- Manage User Groups

Create User Group

Steps

1. In the left sidebar, click **Users** > **User Group Management**
2. Click **Create User Group**
3. Enter the following information:
   - **Name**: The name of the user group
   - **Description**: A description of the group's purpose
4. Click **Create**

Manage User Groups

You can manage user groups by clicking the icon on the list page or clicking **Operations** in the upper right corner on the details page.

Operation	Description
Update User Group	Update group information based on the group source: - For groups with **Source** as `Local`: Can update both name and description - For groups with **Source** as `IDP name`: Can only update description
Delete Local User Group	Delete user groups with **Source** as `Local`

WARNING

When you delete a group:

- All group members will be removed
- All roles assigned to the group will be removed
- This action cannot be undone

Manage Local User Group Membership

Only users with Platform Management permissions can manage local user group memberships.

TOC

- Prerequisites
- Import Members
  - Steps
- Remove Members
  - Steps

Prerequisites

WARNING

Before managing group memberships, please note the following limitations:

- Only users with Platform Management permissions can manage groups and their members
- System accounts and currently logged-in accounts cannot be managed (imported to or removed from groups)
- Each local user group can have a maximum of 5000 members
- When a group reaches the 5000-member limit, no further imports are allowed

Import Members

You can import users from the platform into local user groups for unified permission management.

> **TIP**
>
> Users imported into a group will automatically inherit all operational permissions assigned to that group.

Steps

1. In the left navigation bar, click **Users** > **User Group Management**
2. Click the name of the local user group where you want to add members
3. On the **Group Member Management** tab, click **Import Member**
4. Select one or more users from the platform by checking the boxes next to their usernames/display names
5. Click **Import**

> **NOTE**
>
> - You can only select users who are not currently members of the group
> - Use the **Import All** button to import all users in the list at once

Remove Members

When you remove a user from a group, all operational permissions granted to that user through the group will be automatically revoked.

Steps

1. In the left navigation bar, click **Users** > **User Group Management**
2. Click the name of the local user group where you want to remove members
3. On the **Group Member Management** tab, you can remove members in two ways:
   - Click **Remove** next to the member's name and confirm
   - Select one or more members using checkboxes, then click **Batch Remove** and confirm

Role

Introduction

Introduction

Role Introduction

System Roles

Custom Roles

Guides

Create Role

Basic Information Configuration

View Configuration

Permission Configuration

Manage Custom Roles

Update Basic Information

Update Role Permissions

Copy Existing Role

Delete Custom Role

Introduction

TOC

Role Introduction
System Roles
Custom Roles

Role Introduction

The platform's user role management is implemented using Kubernetes RBAC (Role-Based Access Control). This system enables flexible permission configuration by associating roles with users.

A role represents a collection of permissions for operating Kubernetes resources on the platform. These permissions include:

- Creating resources
- Viewing resources
- Updating resources
- Deleting resources

Roles classify and combine permissions for different resources. By assigning roles to users and setting permission scopes, you can quickly grant resource operation permissions.

Permissions can be revoked just as easily by removing roles from users.

A role can have:

- One or more resource types
- One or more operation permissions
- Multiple users assigned to it

For example:

- Role A: Can only view and create projects
- Role B: Can create, view, update, and delete users, projects, and namespaces

System Roles

To meet common permission configuration scenarios, the platform provides the following default system roles. These roles enable flexible access control for platform resources and efficient permission management for users.

Role Name	Description	Role Level
Platform Administrator	Has full access to all business and resources on the platform	Platform
Platform Auditors	Can view all platform resources and operation records, but has no other permissions	Platform
Cluster Administrator (Alpha)	Manages and maintains cluster resources with full access to all cluster-level resources	Cluster
Project Administrator	Manages namespace administrators and namespace quotas	Project
namespace-admin-system	Manages namespace members and role assignments	Namespace
Developers	Develops, deploys, and maintains custom applications within namespaces	Namespace

Custom Roles

The platform supports custom roles to enhance resource access control scenarios. Custom roles offer several advantages over system roles:

- Flexible permission configuration
- Ability to update role permissions
- Option to delete roles when no longer needed

> **WARNING**
>
> Exercise caution when updating or deleting custom roles. Deleting a custom role will automatically revoke all permissions granted by that role to bound users.

Guides

Create Role

- Basic Information Configuration
- View Configuration
- Permission Configuration

Manage Custom Roles

- Update Basic Information
- Update Role Permissions
- Copy Existing Role
- Delete Custom Role

Create Role

Users with platform role permissions can create custom roles with permissions that are less than or equal to their own role permissions based on actual usage scenarios. When creating a role, you can configure:

- Platform functional module operation permissions
- Access permissions for user-defined resources (Kubernetes CRD)

TOC

Basic Information Configuration

Role Type

View Configuration

Permission Configuration

Basic Information Configuration

1. In the left navigation bar, click **Users** > **Roles**.
2. Click **Create Role**.
3. Configure the role's basic information:

Role Type

When assigning roles to users, the permission scope will be limited based on the role type:

- **Platform Role**: Displays all platform permissions
- **Project Role**: Displays permissions under:
  - Project Management
  - Container Platform
  - Service Mesh
  - DevOps
  - Middleware
- **Namespace Role**: Displays permissions under:
  - Project Management
  - Container Platform
  - Service Mesh
  - DevOps
  - Middleware

4. Click **Next**.

View Configuration

In the view configuration section, you control the role's permission to access specified views. Views that are not selected will not be displayed in the top navigation for users with this role.

> **NOTE**
>
> 1. Your account's role permissions limit which view cards you can configure. For example:
>
>   - If your account doesn't have the **Project Management** view permission
>   - The **Project Management** view card will be grayed out when creating a role
>   - You can only create roles with permissions equal to or lower than your own role
>
> 2. View Entry Status:
>
>   - If a view's **Show Entry** is turned off in the **Products** function

- The view's permissions in **Permission Configuration** will still take effect
- The view will be temporarily inaccessible until the entry is enabled
- Once enabled, the previously selected permissions will work normally

Permission Configuration

1. Click **Add Custom Permission** in the upper left corner of the page.
2. Configure permissions for the role to operate custom resources (Kubernetes CRD):

Parameter	Description
Group Name	The name of the permission group. Groups are displayed below the permission module in the order they were added.
Resource Name	The name of the resource. Press Enter to add multiple custom resource names.
Operation Permission	The permission to operate the resource.

3. Click **Create**.

Manage Custom Roles

This guide describes how to manage custom roles on the platform, including:

- Updating basic information and permissions
- Copying existing roles to create new ones
- Deleting custom roles

TOC

- Update Basic Information
  - Steps
- Update Role Permissions
  - Steps
- Copy Existing Role
  - Steps
- Delete Custom Role
  - Steps

Update Basic Information

You can update the display name and description of custom roles on the platform.

Steps

1. In the left navigation bar, click **Users** > **Roles**
2. Click the name of the ***role to be updated***
3. Click **Actions** > **Update** in the upper right corner
4. Update the role's:
   - Display name
   - Description
5. Click **Update**

Update Role Permissions

You can update the permission information of custom roles, including:

- Adding new operation permissions for platform resources
- Removing existing permissions
- Modifying permissions for custom resources

Steps

1. In the left navigation bar, click **Users** > **Roles**
2. Click the name of the ***role to be updated***
3. Click **Actions** > **Update Role Permissions** in the upper right corner of the permission area
4. Make your changes on the **Update Role Permissions** page
5. Click **Confirm**

Copy Existing Role

You can create a new role by copying an existing role (system or custom). The new role will inherit all permission information from the source role, which you can then modify based on your needs.

> **WARNING**
>
> The permissions of the new role cannot exceed the permissions of the role to which the creator belongs.

Steps

1. In the left navigation bar, click **Users** > **Roles**
2. Click the name of the ***role to be copied***
3. Click **Actions** > **Copy as new role** in the upper right corner
4. On the **Copy as new role** page, configure:
   - Name
   - Display name
   - Description
   - Type
5. Click **Create**

Delete Custom Role

You can delete custom roles that are no longer in use.

> **WARNING**
>
> When you delete a custom role:
>
> - The role's binding relationships with users will be removed
> - Users assigned to this role will lose all permissions granted by the role
> - The role will be removed from users' role lists

Steps

1. In the left navigation bar, click **Users** > **Roles**
2. Click the name of the ***role to be deleted***
3. Click **Actions** > **Delete** in the upper right corner
4. Enter the role name to confirm deletion
5. Click **Delete**

IDP

Introduction

Introduction

Overview

Supported Integration Methods

Guides

LDAP Management

LDAP Overview

Supported LDAP Types

LDAP Terminology

Add LDAP

LDAP Configuration Examples

Synchronize LDAP Users

Relevant Operations

OIDC Management

Overview of OIDC

Adding OIDC

Adding OIDC via YAML

Relevant Operations

Troubleshooting

Delete User

Problem Description

Solution

Introduction

TOC

- Overview
- Supported Integration Methods
  - LDAP Integration
  - OIDC Integration

Overview

The platform integrates with Dex identity authentication service, enabling you to use Dex's pre-implemented connectors for platform account authentication through IDP configuration. For more information, refer to the Dex official documentation ↗.

Supported Integration Methods

LDAP Integration

If your enterprise uses **LDAP** (Lightweight Directory Access Protocol) for user management, you can configure LDAP on the platform to connect with your enterprise's LDAP server.

LDAP Integration Benefits:

- Enables communication between platform and LDAP server

- Allows enterprise users to log in with LDAP credentials
- Automatically synchronizes enterprise user accounts to the platform

OIDC Integration

The platform supports integration with IDP services using the OpenID Connect (OIDC) protocol for third-party user authentication.

OIDC Integration Benefits:

- Enables users to log in with third-party accounts
- Supports enterprise IDP services
- Provides secure authentication through OIDC protocol

> **NOTE**
>
> For authentication using other connectors not mentioned above, please contact technical support.

Guides

LDAP Management

- LDAP Overview
- Supported LDAP Types
- LDAP Terminology
- Add LDAP
- LDAP Configuration Examples
- Synchronize LDAP Users
- Relevant Operations

OIDC Management

- Overview of OIDC
- Adding OIDC
- Adding OIDC via YAML
- Relevant Operations

LDAP Management

Platform administrators can add, update, and delete LDAP services on the platform.

TOC

- LDAP Overview
- Supported LDAP Types
  - OpenLDAP
  - Active Directory
- LDAP Terminology
  - OpenLDAP Common Terms
  - Active Directory Common Terms
- Add LDAP
  - Prerequisites
  - Steps
    - Basic Information
    - Search Settings
- LDAP Configuration Examples
  - LDAP Connector Configuration
  - User Filter Examples
  - Group Search Configuration Examples
  - Examples of AND(&) and OR(|) Operators in LDAP Filters
- Synchronize LDAP Users
  - Procedure of Operation
- Relevant Operations

LDAP Overview

LDAP (Lightweight Directory Access Protocol) is a mature, flexible, and well-supported standard mechanism for interacting with directory servers. It organizes data in a hierarchical tree structure to store enterprise user and organization information, primarily used for implementing single sign-on (SSO).

NOTE

LDAP Key Features:

- Enables communication between clients and LDAP servers
- Supports data storage, retrieval, and search operations
- Provides client authentication capabilities
- Facilitates integration with other systems

For more information, refer to the LDAP official documentation↗.

Supported LDAP Types

OpenLDAP

OpenLDAP is an open-source implementation of LDAP. If your organization uses open-source LDAP for user authentication, you can configure the platform to communicate with the LDAP service by adding LDAP and configuring relevant parameters.

NOTE

OpenLDAP Integration:

- Enables platform authentication for LDAP users
- Supports standard LDAP protocols

- Provides flexible user management

For more information about OpenLDAP, refer to the OpenLDAP official documentation ↗.

Active Directory

Active Directory is Microsoft's LDAP-based software for providing directory storage services in Windows systems. If your organization uses Microsoft Active Directory for user management, you can configure the platform to communicate with the Active Directory service.

NOTE

Active Directory Integration:

- Enables platform authentication for AD users
- Supports Windows domain integration
- Provides enterprise-level user management

LDAP Terminology

OpenLDAP Common Terms

Term	Description	Example
dc (Domain Component)	Domain component	`dc=example,dc=com`
ou (Organizational Unit)	Organizational unit	`ou=People,dc=example,dc=com`
cn (Common Name)	Common name	`cn=admin,dc=example,dc=com`
uid (User ID)	User ID	`uid=example`

Term	Description	Example
objectClass (Object Class)	Object class	`objectClass=inetOrgPerson`
mail (Mail)	Mail	`mail=example@126.com`
givenName (Given Name)	Given name	`givenName=xq`
sn (Surname)	Surname	`sn=ren`
objectClass: groupOfNames	User group	`objectClass: groupOfNames`
member (Member)	Group member attribute	`member=cn=admin,dc=example,dc=com`
memberOf	User group membership attribute	`memberOf=cn=users,dc=example,dc=com`

Active Directory Common Terms

Term	Description	Example
dc (Domain Component)	Domain component	`dc=example,dc=com`
ou (Organizational Unit)	Organizational unit	`ou=People,dc=example,dc=com`
cn (Common Name)	Common name	`cn=admin,dc=example,dc=com`
sAMAccountName/userPrincipalName	User identifier	`userPrincipalName=example` or `sAMAccountName=example`
objectClass: user	AD user object class	`objectClass=user`

Term	Description	Example
mail (Mail)	Mail	`mail=example@126.com`
displayName	Display name	`displayName=example`
givenName (Given Name)	Given name	`givenName=xq`
sn (Surname)	Surname	`sn=ren`
objectClass: group	User group	`objectClass: group`
member (Member)	Group member attribute	`member=CN=Admin,DC=example,DC`
memberOf	User group membership attribute	`memberOf=CN=Users,DC=example,`

Add LDAP

TIP

After successful LDAP integration:

- Users can log in to the platform using their enterprise accounts
- Multiple additions of the same LDAP will overwrite previously synchronized users

Prerequisites

Before adding LDAP, prepare the following information:

- LDAP server address
- Administrator username
- Administrator password

- Other required configuration details

Steps

1. In the left navigation bar, click **Users** > **IDPs**
2. Click **Add LDAP**
3. Configure the following parameters:

Basic Information

Parameter	Description
Server Address	LDAP server access address (e.g., `192.168.156.141:31758`)
Username	LDAP administrator DN (e.g., `cn=admin,dc=example,dc=com`)
Password	LDAP administrator account password
Login Box Username Prompt	Prompt message for username input (e.g., "Please enter your username")

Search Settings

NOTE

Search Settings Purpose:

- Matches LDAP user entries based on specified conditions
- Extracts key user and group attributes
- Maps LDAP attributes to platform user attributes

Parameter	Description
Object Type	ObjectClass for users: - OpenLDAP: `inetOrgPerson`

Parameter	Description
	- Active Directory: `organizationalPerson` - Groups: `posixGroup`
Login Field	Attribute used as login username: - OpenLDAP: `mail` (email address) - Active Directory: `userPrincipalName`
Filter Conditions	LDAP filter conditions for user/group filtering Example: `(&(cn=John*)(givenName=*xq*))`
Search Starting Point	Base DN for user/group search (e.g., `dc=example,dc=org`)
Search Scope	Search scope: - `sub`: entire directory subtree - `one`: one level below starting point
Login Attribute	Unique user identifier: - OpenLDAP: `uid` - Active Directory: `distinguishedName`
Name Attribute	Object name attribute (default: `cn`)
Email Attribute	Email attribute: - OpenLDAP: `mail` - Active Directory: `userPrincipalName`
Group Member Attribute	Group member identifier (default: `uid`)
Group Attribute	User group relationship attribute (default: `memberuid`)

4. In the **IDP Service Configuration Validation** section:

   - Enter a valid LDAP account username and password
   - The username must match the **Login Field** setting
   - Click to verify the configuration

5. (Optional) Configure **LDAP Auto-Sync Policy**:

   - Enable **Auto-Sync Users** switch

- Set synchronization rules
- Use online tool ↗ to verify CRON expressions

6. Click **Add**

> **NOTE**
>
> After adding LDAP:
>
> - Users can log in before synchronization
> - User information syncs automatically on first login
> - Auto-sync occurs based on configured rules

LDAP Configuration Examples

LDAP Connector Configuration

The following example shows how to configure an LDAP connector:

```
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 attribute
s.
      # 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
```

User Filter Examples

```
# 1. Basic filter: Find all users
(&(objectClass=person))

# 2. Multiple conditions combination: Find users in a specific department
(&(objectClass=person)(departmentNumber=1000))

# 3. Find enabled users (Active Directory)
(&(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

# 4. Find users with a specific email domain
(&(objectClass=person)(mail=*@example.com))

# 5. Find members of specific group
(&(objectClass=person)(memberOf=cn=developers,ou=groups,dc=example,dc=com))

# 6. Find recently logged in users (Active Directory)
(&(objectClass=user)(lastLogon>=20240101000000.0Z))

# 7. Exclude system accounts
(&(objectClass=person)(!(uid=admin))(!(uid=system)))

# 8. Find users with a specific attribute
(&(objectClass=person)(mobile=*))

# 9. Find users in multiple departments
(&(objectClass=person)(|(ou=IT)(ou=HR)(ou=Finance)))

# 10. Complex condition combination example
(&
  (objectClass=person)
  (|(department=IT)(department=Engineering))
  (!(title=Intern))
  (manager=cn=John Doe,ou=People,dc=example,dc=com)
)
```

Group Search Configuration Examples

```
# 1. Basic filter: Find all groups
(objectClass=groupOfNames)

# 2. Find groups with a specific prefix
(&(objectClass=groupOfNames)(cn=dev-*))

# 3. Find non-empty groups
(&(objectClass=groupOfNames)(member=*))

# 4. Find groups with a specific member
(&(objectClass=groupOfNames)(member=uid=john,ou=People,dc=example,dc=co
m))

# 5. Find nested groups (Active Directory)
(&(objectClass=group)(|(groupType=-2147483646)(groupType=-2147483644)))

# 6. Find groups with a specific description
(&(objectClass=groupOfNames)(description=*admin*))

# 7. Exclude system groups
(&(objectClass=groupOfNames)(!(cn=system*)))

# 8. Find groups with specific members
(&(objectClass=groupOfNames)(|(cn=admins)(cn=developers)(cn=operators)))

# 9. Find groups in a specific OU
(&(objectClass=groupOfNames)(ou=IT))

# 10. Complex condition combination example
(&
  (objectClass=groupOfNames)
  (|(cn=prod-*)(cn=dev-*))
  (!(cn=deprecated-*))
  (owner=cn=admin,dc=example,dc=com)
)
```

Examples of AND(&) and OR(|) Operators in LDAP Filters

```
# AND operator (&) - All conditions must be met
# Syntax: (&(condition1)(condition2)(condition3)...)

# Multiple attribute AND example
(&
  (objectClass=person)
  (mail=*@example.com)
  (title=Engineer)
  (manager=*)
)

# OR operator (|) - At least one condition must be met
# Syntax: (|(condition1)(condition2)(condition3)...)

# Multiple attribute OR example
(|
  (department=IT)
  (department=HR)
  (department=Finance)
)

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

# Complex condition combination
(&
  (objectClass=person)
  (|
    (&
      (department=IT)
      (title=*Engineer*)
    )
    (&
      (department=R&D)
      (title=*Developer*)
    )
```

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

Synchronize LDAP Users

After successfully synchronizing LDAP users to the platform, you can view the synchronized users in the user list.

You can configure an automatic synchronization policy when adding LDAP (which can be updated later) or manually trigger synchronization after adding LDAP successfully. Here's how to manually trigger a synchronization operation.

Notes:

- Newly added users in the LDAP integrated with the platform can log in to the platform before performing the user synchronization operation. Once they successfully log in to the platform, their information will be automatically synchronized to the platform.
- Users deleted from LDAP will have an `Invalid` status after synchronization.
- The default validity period for newly synchronized users is **Permanent**.
- Synchronized users with the same name as existing users (local users, IDP users) are automatically associated. Their permissions and validity period will be consistent with existing users. They can log in to the platform using the login method corresponding to their respective sources.

Procedure of Operation

1. In the left navigation bar, click **Users** > **IDPs**.
2. Click the ***LDAP name*** that you want to manually synchronize.
3. Click **Actions** > **Sync user** in the upper-right corner.
4. Click **Sync**.

Notes: If you manually close the synchronization prompt dialog, a confirmation dialog will appear to confirm the closure. After closing the synchronization prompt dialog, the system will continue to synchronize users. If you remain on the user list page, you will receive synchronization result feedback. If you leave the user list page, you will not receive synchronization results.

Relevant Operations

You can click the
on the right in the list page or click **Actions** in the upper-right corner on the details page to update or delete LDAP as needed.

Operation	Description
Update LDAP	Update the configuration information of the added LDAP or the **LDAP Auto-Sync Policy**. **Note**: After updating LDAP, users currently synchronized to the platform through this LDAP will also be updated. Users removed from LDAP will become invalid in the platform user list. You can clean up junk data by executing the operation to clean up invalid users.
Delete LDAP	After deleting LDAP, all users synchronized to the platform through this LDAP will have an **Invalid** status (the binding relationship between users and roles remains unchanged), and they cannot log in to the platform. After re-integrating, synchronization needs to be re-executed to activate users. **Tips**: After deleting IDP, if you need to delete users and user groups synchronized to the platform through LDAP, check the checkbox **Clean IDP Users and User Groups** below the prompt box.

OIDC Management

The platform supports the OIDC (OpenID Connect) protocol, enabling platform administrators to log in using third-party accounts after adding OIDC configuration. Platform administrators can also update and delete configured OIDC services.

TOC

- Overview of OIDC
- Adding OIDC
  - Procedure of Operation
- Adding OIDC via YAML
  - Example: Configuring OIDC Connector
- Relevant Operations

Overview of OIDC

OIDC (OpenID Connect) is an identity authentication standard protocol based on the OAuth 2.0 protocol. It uses an OAuth 2.0 authorization server to provide user identity authentication for third-party clients and passes the corresponding identity authentication information to the client.

OIDC allows all types of clients (including server-side, mobile, and JavaScript clients) to request and receive authenticated sessions and end-user information. This specification suite is extensible, allowing participants to use optional features such as identity data encryption,

OpenID Provider discovery, and session management when meaningful. For more information, refer to the OIDC official documentation ↗.

Adding OIDC

By adding OIDC, you can use third-party platform accounts to log in to the platform.

Note: After OIDC users successfully log in to the platform, the platform will use the user's email attribute as the unique identifier. OIDC-supported third-party platform users must have an **email** attribute; otherwise, they will not be able to log in to the platform.

Procedure of Operation

1. In the left navigation bar, click **Users** > **IDPs**.
2. Click **Add OIDC**.
3. Configure the **Basic Information** parameters.
4. Configure the **OIDC Server Configuration** parameters:
   - **Identity Provider URL**: The issuer URL, which is the access address of the OIDC identity provider.
   - **Client ID**: The client identifier for the OIDC client.
   - **Client Secret**: The secret key for the OIDC client.
   - **Redirect URI**: The callback address after logging in to the third-party platform, which is the URL of the dex issuer + `/callback`.
   - **Logout URL**: The address visited by the user after performing the **Logout** operation. If empty, the logout address will be the platform's initial login page.
5. In the **IDP Service Configuration Validation** area, enter the **Username** and **Password** of a valid OIDC account to verify the configuration.

Tip: If the username and password are incorrect, an error will be reported during addition, indicating invalid credentials, and OIDC cannot be added.

6. Click **Create**.

Adding OIDC via YAML

In addition to form configuration, the platform also supports adding OIDC through YAML, which allows for more flexible configuration of authentication parameters, claim mappings, user group synchronization, and other advanced features.

Example: Configuring OIDC Connector

The following example demonstrates how to configure an OIDC connector for integrating with OIDC identity authentication services. This configuration example is suitable for the following scenarios:

1. Need to integrate OIDC as an identity authentication server.
2. Need to support user group information synchronization.
3. Need to customize logout redirect address.
4. Need to configure specific OIDC scopes.
5. Need to customize claim mappings.

```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, us
```

```
ed for OIDC basic authentication
      - profile                                          # Optional, us
ed to obtain user basic information
      - email                                            # Optional, us
ed to obtain user email

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

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

Relevant Operations

You can click the
on the right in the list page or click **Actions** in the upper-right corner on the details page to update or delete OIDC as needed.

Operation	Description
Update OIDC	Update the added OIDC configuration. After updating the OIDC configuration information, the original users and authentication methods will be reset and synchronized according to the current configuration.
Delete OIDC	Delete OIDC that is no longer used by the platform. After deleting OIDC, all users synchronized to the platform through this OIDC will have an **Invalid** status (the binding relationship between users and roles remains unchanged), and they

Operation	Description
	cannot log in to the platform. After re-integrating, users can be activated by successfully logging in to the platform. **Tip**: After deleting IDP, if you need to delete users and user groups synchronized to the platform through OIDC, check the checkbox **Clean IDP Users and User Groups** below the prompt box.

Troubleshooting

Delete User

Problem Description

Solution

Delete User

TOC

- Problem Description
- Solution
  - Clean up deleted IDP users
  - Clean up deleted local users

Problem Description

Issue: When creating or synchronizing a new user, the system indicates that the user already exists. How should you handle this?

For security reasons, the platform prevents creating new users (both local and IDP users) with names that match previously deleted users. This limitation applies to:

- Creating new local users with names matching deleted users
- Synchronizing IDP users with names matching deleted users

After upgrading to the current version, you may encounter this issue when:

- Creating new users with names that match users deleted before the upgrade
- Synchronizing new users with names that match users deleted before the upgrade

Solution

To resolve this issue, you need to clean up the deleted user information by executing specific scripts on your global cluster control nodes.

Clean up deleted IDP users

Execute the following command on any control node of your global cluster:

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

Example:

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

Clean up deleted local users

Execute these two scripts in sequence on any control node of your global cluster:

1. Clean up user passwords:

   ```
   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. Clean up users:

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

User Policy

Introduction

Overview

Configure Security Policy

Available Policies

Introduction

The platform provides comprehensive user security policies to enhance login security and protect against malicious attacks.

TOC

- Overview
- Configure Security Policy
  - Steps
- Available Policies

Overview

The platform supports the following security policies:

- Password security management
- User account disablement
- User account locking
- User notifications
- Access control

Configure Security Policy

Steps

1. In the left navigation bar, click **User Role Management** > **User Security Policy**
2. Click **Update** in the top right corner
3. Configure the security policies as needed
4. Click **Update** to save changes

> **WARNING**
>
> Policy Configuration Notes:
>
> - Check the box before a policy to enable it
> - Uncheck the box to disable a policy
> - Disabled policies retain their configuration data
> - Previous settings are restored when re-enabling a policy

Available Policies

Policy	Description
User Authentication Policy	Enables dual authentication for password-based login: - Users receive verification codes via specified notification methods - Supports various notification servers (e.g., Enterprise Communication Tool Server)
Password Security Policy	Manages password requirements: First Login: - Forces password change on first platform login Regular Updates: - Requires password change after specified period (e.g., 90 days) - Prevents login until password is updated

Policy	Description
User Disablement Policy	Automatically disables inactive accounts: - Triggers after specified period of no login
User Locking Policy	Protects against brute force attacks: Lock Conditions: - Triggers after specified number of failed login attempts within 24 hours Lock Duration: - Account remains locked for specified minutes - Automatically unlocks after lock period expires
Notification Policy	Manages user notifications: - Sends initial password via email after user creation
Access Control	Manages user sessions and access: Session Management: - Auto-logs out inactive sessions after specified time - Limits maximum concurrent online users Browser Control: - Ends session when all product tabs are closed - Prevents multiple logins from same client :::note Important Notes: - Access Control only affects new logins after policy update - Browser tab restoration may not trigger session end - Only last login is allowed per client when preventing repeated login :::

Multitenancy(Project)

Introduction

Introduction

Project

Namespaces

Relationship Between Clusters, Projects, and Namespaces

Guides

Create Project

Procedure

Manage Project

Update Basic Project Information

Update Project Quota

Manage Pro

Introduction

Add a Cluster

Clus

Manage Project Members

Import Members

Remove Members

Introduction

TOC

Project

Namespaces

Relationship Between Clusters, Projects, and Namespaces

Project

A project is a resource isolation unit that enables multi-tenant usage scenarios in enterprises. It divides resources from one or more clusters into isolated environments, ensuring both resource and personnel isolation. Projects can represent different subsidiaries, departments, or project teams within an enterprise. Through project management, you can achieve:

- Resource isolation between project teams
- Quota management within tenants
- Efficient resource allocation and control

Namespaces

Namespaces are smaller, mutually isolated resource spaces within a project. They serve as workspaces for users to implement their production workloads. Key characteristics of namespaces include:

- Multiple namespaces can be created under a project
- Total resource quota of all namespaces cannot exceed the project quota
- Resource quotas are allocated more granularly at the namespace level
- Container sizes (CPU, memory) are limited at the namespace level
- Improved resource utilization through fine-grained control

Relationship Between Clusters, Projects, and Namespaces

The platform's resource hierarchy follows these rules:

- A project can utilize resources (CPU, memory, storage) from multiple clusters, and a cluster can allocate resources to multiple projects.
- Multiple namespaces can be created under a project, with their combined resource quotas not exceeding the total project resources.
- A namespace's resource quota must come from a single cluster, and a namespace can only belong to one project.

Guides

Create Project

Procedure

Manage Project

Update Basic Project Information

Update Project Quota

Manage Pro

Introduction

Add a Cluster

Clus

Manage Project Members

Import Members

Remove Members

Create Project

Before your project team starts working, you can create a project based on the existing cluster resources on the platform. The project will be isolated from other projects (tenants) in terms of both resources and personnel. When creating a project, you can allocate resources according to your project scale and actual business needs. The project can utilize resources from multiple clusters on the platform.

WARNING

When creating a project, the platform will automatically create a namespace with the same name as the project in the associated clusters to isolate platform-level resources. Please do not modify this namespace or its resources.

TOC

Procedure

Procedure

1. In the **Project Management** view, click **Create Project**.

2. On the **Basic information** page, configure the following parameters:

Parameter	Description
Name	The name of the project, which cannot be the same as an existing project name or any name in the project name blacklist. Otherwise, the project cannot be created. **Note**: The project name blacklist includes special namespace names under platform clusters: `cpaas-system`, `cert-manager`, `default`, `global-credentials`, `kube-ovn`, `kube-public`, `kube-system`, `nsx-system`, `alauda-system`, `kube-federation-system`, `ALL-ALL`, and `true`.
Cluster	The cluster(s) associated with the project, where the administrator can allocate resource quotas. Click the drop-down selection box to select one or more clusters. **Note**: Clusters in abnormal state cannot be selected.

3. Click **Next** and in the project quota setting step, set the resource quotas to be allocated to the current project for the selected clusters. This includes:

   - CPU (cores)
   - Memory (Gi)
   - Storage (Gi)
   - PVC count (number)
   - Pods (number)
   - Virtual GPU (GPU-Manager/MPS)
   - pGPU (physical GPU, cores)
   - GPU memory

NOTE

- GPU resource quotas can only be configured when GPU plugins are deployed in the cluster. When the GPU resource is a **GPU-Manager or MPS GPU**, the **vMemory** quota can also be configured.

GPU Units: 100 units of virtual cores are equivalent to 1 physical core (1 pGPU = 1 core = 100 GPU-Manager core = 100 MPS core), and pGPU units can only be allocated in whole numbers. GPU-Manager 1 unit of memory is equal to 256 Mi, MPS GPU 1 unit of memory is equal to 1 Gi, and 1024 Mi = 1 Gi.

- If no quota is set for a certain type of resource, it defaults to **Unlimited**. This means that the project can use the available resources of the corresponding type in the cluster as needed, without a maximum limit.
- The project quota values set should be within the quota range displayed on the page. Under each resource quota input box, the allocated quota and total information for that resource will be displayed for reference.

4. Click **Create Project**.

Manage Project

This guide explains how to update basic information and project quotas for a specified project, or delete the project.

TOC

- Update Basic Project Information
  - Procedure
- Update Project Quota
  - Constraints and Limitations
  - Procedure
- Delete Project
  - Procedure

Update Basic Project Information

Update basic information for a specified project, such as display name and description.

Procedure

1. In the **Project Management** view, click on the project name to be updated.
2. In the left navigation pane, click **Details**.

3. Click **Actions** > **Update Basics** in the upper right corner.
4. Modify or enter the **Display name** and **Description**.
5. Click **Update**.

Update Project Quota

Update the resource quotas for the project in each associated cluster.

Constraints and Limitations

When a project is associated with an **Abnormal** cluster, updating the quotas assigned to the project in that cluster is not supported.

Procedure

1. In the **Project Management** view, click on the project name to be updated.
2. In the left navigation pane, click **Details**.
3. Click **Update Quota** on the right side of the quota area.
4. Update the quotas assigned to the project in the cluster according to the following guidelines:

NOTE

- GPU (vGPU/pGPU) resource quotas can only be configured when GPU resources are deployed in the cluster.

  When the GPU resource is a **vGPU**, **vMemory** quotas can also be configured.

  GPU Units: 100 units of virtual cores are equivalent to 1 physical core (1 pGPU = 1 core = 100 vGPU); 1 unit of video memory is 256 Mi; pGPU units are in whole numbers and can only be assigned in whole numbers.

- If no quota is set for a certain resource, the resource will have unlimited quota by default.
- The quota value set should be within the range of the quota displayed on the page.

5. Click **Update**.

Delete Project

Delete projects that are no longer in use.

> **WARNING**
>
> After the project is deleted, the resources occupied by the project in the cluster will be released.

Procedure

1. In the **Project Management** view, click on the project name to be deleted.
2. In the left navigation bar, click **Details**.
3. Click **Actions** > **Delete Project** in the upper right corner.
4. Enter the name of the project and click **Delete**.

Manage Project Cluster

This guide explains how to manage cluster associations for a project. You can add clusters to allocate their resources to the project, or remove clusters to reclaim the allocated resources.

TOC

- Introduction
- Add a Cluster
  - Procedure
- Remove a Cluster
  - Procedure

Introduction

You can add clusters to a project to allocate their resources, or remove clusters to reclaim the allocated resources. This functionality is useful in the following scenarios:

- When project resources are insufficient for business operations
- When a newly created or added cluster needs to be allocated to an existing project
- When cluster resources need to be reclaimed from a project
- When a specific project needs exclusive access to a cluster

Add a Cluster

Add a cluster to a project and set its resource quota.

Procedure

1. In the **Project Management** view, click on the project name where you want to add the cluster.
2. In the left navigation bar, click **Details**.
3. Click **Actions** > **Add Cluster** in the upper right corner.
4. Select the cluster and set the resource quota to be allocated to the current project. The following resources can be configured:
   - CPU (cores)
   - Memory (Gi)
   - Storage (Gi)
   - PVC count (number)
   - Pods (number)
   - vGPU (virtual GPU)/MPS/pGPU (physical GPU, cores)
   - Video memory quota

NOTE

- GPU resource quota can only be configured when GPU plugins are deployed in the cluster.

  When GPU resources are **GPU-Manager or MPS GPU**, **vMemory** quota can also be configured.

  GPU Units: 100 units of virtual cores are equivalent to 1 physical core (1 pGPU = 1 core = 100 GPU-Manager core = 100 MPS core), and pGPU units can only be allocated in whole numbers. GPU-Manager 1 unit of memory is equal to 256 Mi, MPS GPU 1 unit of memory is equal to 1 Gi, and 1024 Mi = 1 Gi.
- If no quota is set for a certain type of resource, it defaults to **Unlimited**. This means that the project can use the available resources of the corresponding type in the cluster as needed,

without a maximum limit.

- The value of the project quota set should be within the quota range displayed on the page. Under each resource quota input box, the allocated quota and total amount of that resource will be displayed for reference.

5. Click **Add**.

Remove a Cluster

Remove a cluster associated with a project.

WARNING

- After removing a cluster, the project cannot use the business resources under the removed cluster.
- When the cluster to be removed is abnormal, the resources under the abnormal cluster cannot be cleaned up. It is recommended to fix the cluster before removing it.

Procedure

1. In the **Project Management** view, click on the project name where you want to remove the cluster.
2. In the left navigation bar, click **Details**.
3. Click **Actions** > **Remove Cluster** in the upper right corner.
4. In the pop-up **Remove Cluster** dialog box, enter the name of the cluster to be removed, and then click the **Remove** button to successfully remove the cluster.

Manage Project Members

This guide explains how to manage project members, including importing members and assigning project-related roles.

TOC

- Import Members
  - Constraints and Limitations
  - Procedure
    - Import from Member List
    - Import OIDC Users
- Remove Members
  - Procedure

Import Members

You can grant users operation permissions for the project and its namespaces by importing existing platform users or adding OIDC users. You can assign roles such as project administrators, namespace administrators, developers, or custom roles with project and namespace management permissions.

Constraints and Limitations

- When no OIDC IDP is configured on the platform:

- Only existing platform users can be imported as project members, including:
  - OIDC users who have successfully logged in
  - Users synchronized through LDAP
  - Local users
  - Users added to other projects as OIDC users (with source marked as `-`)
- When an OIDC IDP is configured:
  - You can add valid OIDC accounts that meet the input requirements
  - Account validity cannot be verified during addition
  - Ensure the account is valid, or it won't be able to log in normally
- System default administrator users and the currently logged-in user cannot be imported

Procedure

1. In the **Project Management** view, click on the project name to be managed.
2. In the left navigation bar, click **Members**.
3. Click **Import Member**.
4. Choose either **Member List** or **OIDC Users**.

Import from Member List

You can import either all users or selected users from the member list.

> **TIP**
>
> Use the user group dropdown menu in the upper right corner and the search box to filter users by username.

To import all users:

1. Select **Member List**.

2. Click the **Bind** dropdown menu and select the role to assign to all users.
   If the role requires a namespace, select it from the **Namespaces** dropdown menu.

3. Click **Import All**.

To import specific users:

1. Select **Member List**.

2. Select one or more users using the checkboxes.

3. Click the **Bind** dropdown menu and select the role to assign to the selected users.
   If the role requires a namespace, select it from the **Namespaces** dropdown menu.

4. Click **Import**.

Import OIDC Users

1. Select **OIDC Users**.

2. Click **Add** to create a member record (repeat for multiple members).

3. Enter the OIDC-authenticated username in the **Name** field.

> **WARNING**
>
> Ensure the username corresponds to an account that can be authenticated by the configured OIDC system, or login will fail.

4. Select the role from the **Roles** dropdown menu.
   If the role requires a namespace, select it from the **Namespaces** dropdown menu.

5. Click **Import**.

After successful import, you can view:

- The member in the project member list
- The user in **Platform Management > Users**
  - Source shows as "-" until first login/sync

- Source updates after successful login/sync

Remove Members

Remove a project member to revoke their permissions.

Procedure

1. In the **Project Management** view, click on the project name.
2. In the left navigation bar, click **Members**.

> **TIP**
>
> Use the dropdown list next to the search box to filter members by **Name**, **Display name**, or **User Group**.

3. Click **Remove** next to the member you want to remove.
4. Confirm removal in the prompt dialog.

Audit

Introduction

Prerequisites

Procedure

Search Results

Introduction

The platform's auditing function provides time-ordered operation records related to users and system security. This helps you analyze specific issues and quickly resolve problems that occur in clusters, custom applications, and other areas.

Through auditing, you can track various changes in the Kubernetes cluster, including:

- What changes occurred in the cluster during a specific time period
- Who performed these changes (system components or users)
- Details of important change events (e.g., POD parameter updates)
- Event outcomes (success or failure)
- Operator location (internal or external to the cluster)
- User operation records (updates, deletions, management operations) and their results

TOC

Prerequisites
Procedure
Search Results

Prerequisites

Your account must have platform management or platform auditing permissions.

Procedure

1. In the left navigation bar, click **Auditing**.

2. Select the auditing scope from the tabs:

   - **User Operations**: View operation records of users who have logged in to the platform
   - **System Operations**: View system operation records (operators start with `system:`)

3. Configure query conditions to filter auditing events:

Query Condition	Description
Operator	Username or system account name of the operator (default: `All`)
Actions	Type of operation (create, update, delete, manage, rollback, stop, etc., default: `All`)
Clusters	Cluster containing the operated resource (default: `All`)
Resource Type	Type of the operated resource (default: `All`)
Resource Name	Name of the operated resource (supports fuzzy search)

4. Click **Search**.

TIP

- Use the **Time Range** dropdown to set the audit time range (default: `Last 30 Minutes`). You can select a preset range or customize one.
- Click the refresh icon to update search results.
- Click the export icon to download results as a `.csv` file.

Search Results

The search results display the following information:

Parameter	Description
Operator	Username or system account name of the operator
Actions	Type of operation (create, update, delete, manage, rollback, stop, etc.)
Resource Name/Type	Name and type of the operated resource
Clusters	Cluster containing the operated resource
Namespaces	Namespace containing the operated resource
Client IP	IP address of the client used to execute the operation
Operation Result	Operation outcome based on API return code (2xx = success, other = failure)
Operation Time	Timestamp of the operation
Details	Click the **Details** button to view the complete audit record in JSON format in the **Audit Details** dialog box

Telemetry

Install

Prerequisites

Installation Steps

Enable Online Operations

Uninstallation Steps

Install

ACP Telemetry is a platform service that collects telemetry data from clusters for online operations and maintenance. It collects system metrics and uploads them to Alauda Cloud for monitoring and analysis.

TOC

- Prerequisites
- Installation Steps
- Enable Online Operations
- Uninstallation Steps

Prerequisites

Before installation, ensure that:

- The Alauda Container Platform has a valid license
- The global cluster has internet access

Installation Steps

1. Navigate to **Platform Management**
2. In the left navigation bar, click **Marketplace** > **Cluster Plugins**

3. Select the **global** cluster in the top navigation bar
4. Search for **ACP Telemetry** and click to view its details
5. Click **Install** to deploy the plugin

Enable Online Operations

1. In the left navigation bar, click **System Settings** > **Platform Maintenance**
2. Click the **On** button for **Online Operations**

Uninstallation Steps

1. Follow steps 1-4 from the installation process to locate the plugin
2. Click **Uninstall** to remove the plugin

Certificates

cert-manager

OLM Certificates

Certificate M

Rotate TLS Certs of Platform Access Addresses

cert-manager

Each cluster will automatically deploy **Certificate for cert-manager**

cert-manager is a native Kubernetes certificate management controller that automatically generates and manages TLS certificates based on `Certificate` resources. Many components in Kubernetes clusters use cert-manager to manage their TLS certificates, ensuring secure communication.

TOC

- Overview
- How it works
- Identifying cert-manager Managed Certificates
  - Common Labels and Annotations
- Related Resources

Overview

Cert-manager manages the lifecycle of certificates through Kubernetes Custom Resource Definitions (CRDs):

- **Certificate**: Defines the certificates that need to be managed
- **Issuer/ClusterIssuer**: Defines certificate issuers
- **CertificateRequest**: Internal resource for processing certificate requests

How it works

When a `Certificate` resource is created, cert-manager automatically:

1. Generates private keys and certificate signing requests
2. Obtains signed certificates from the specified Issuer
3. Stores certificates and private keys in Kubernetes Secrets

Additionally, cert-manager monitors the validity period of certificates and renews them before they expire to ensure continuous service availability.

Identifying cert-manager Managed Certificates

Certificates managed by cert-manager have corresponding `Secret` resources with type `kubernetes.io/tls` and specific labels and annotations.

Common Labels and Annotations

`Secret` resources managed by cert-manager typically contain the following labels and annotations:

Labels:

- `controller.cert-manager.io/fao: "true"`: Identifies that this Secret is managed by cert-manager and enables filtered Secret caching by the controller.

Annotations:

- `cert-manager.io/certificate-name`: Certificate name
- `cert-manager.io/common-name`: Common name of the certificate
- `cert-manager.io/alt-names`: Alternative names of the certificate
- `cert-manager.io/ip-sans`: IP addresses of the certificate
- `cert-manager.io/issuer-kind`: Type of certificate issuer
- `cert-manager.io/issuer-name`: Name of certificate issuer

- `cert-manager.io/issuer-group`: API group of the issuer
- `cert-manager.io/uri-sans`: URI Subject Alternative Names

Related Resources

- cert-manager Official Documentation ↗

OLM Certificates

All certificates for **Operator Lifecycle Manager (OLM)** components — including `olm-operator`, `catalog-operator`, `packageserver`, and `marketplace-operator` — are automatically managed by the system.

When installing Operators that define **webhooks** or **API services** in their **ClusterServiceVersion (CSV)** object, OLM automatically generates and rotates the required certificates.

Certificate Monitoring

Cluster Enhancer provides monitoring capabilities for certificates used in Kubernetes clusters. The monitoring scope includes:

1. **Kubernetes component certificates**, including control plane and kubelet server/client certificates (including kubeconfig client certificates)
2. **Certificates of components running in the cluster**, implemented by inspecting all Secrets with type `kubernetes.io/tls`
3. **Server certificates actually used by kube-apiserver** (including internal loopback certificates for self-access) by accessing the `kubernetes` Endpoints

Users can find and install **Cluster Enhancer** in the **Administrator** view by navigating to **Marketplace** > **Cluster Plugins** in the left navigation.

TOC

- Certificate Status Monitoring
- Built-in Alert Rules
  - Kubernetes Certificate Alerts
  - Platform Components Certificate Alerts

Certificate Status Monitoring

The expiration status of certificates can be viewed through the metric `certificate_expires_status`. The expiration time of certificates can be viewed through

the metric `certificate_expires_time`.

The current certificate status and expiration time can be viewed in the **Certificate Status** sub-tab. To access this sub-tab, go to the **Administrator** view, navigate to **Clusters > Clusters**, select a specific cluster, then go to the **Monitoring** tab.

Built-in Alert Rules

Cluster Enhancer provides built-in alert rules `cpaas-certificates-rule` with the following alerts:

Kubernetes Certificate Alerts

Rule	Level
The expiration time of the kubernetes certificate is about to expire (less than 30 days) <= 30d and last 1 minutes	Medium
The expiration time of the kubernetes certificate is about to expire (less than 10 days) <= 10d and last 1 minutes	High
Kubernetes certificate has expired <= 0d and last 1 minutes	Critical

Platform Components Certificate Alerts

Rule	Level
The expiration time of the platform components certificate is about to expire (less than 30 days) <= 30d and last 1 minutes	Medium
The expiration time of the platform components certificate is about to expire (less than 10 days) <= 10d and last 1 minutes	High
Platform components certificate has expired <= 0d and last 1 minutes	Critical

Rotate TLS Certs of Platform Access Addresses

INFO

For ACP version v4.0.x, apply the same procedure to both the primary cluster and the standby cluster (terms of the Disaster Recovery setup) as described here.

TOC

Prerequisites

Procedures

Prerequisites

- A pair of TLS certificates and its private key.

Procedures

1. On any control-plane node in the global cluster, export backups of the TLS certificates used by ACP's platform access addresses:

```
kubectl get certificate -n cpaas-system dex-serving-cert --ignore-not-found=true -o yaml > /cpaas/dex-serving-cert.yaml
kubectl get secret -n cpaas-system dex.tls -o yaml > /cpaas/dex.tls.yaml
```

2. Delete the current certificates:

```
kubectl delete certificate -n cpaas-system dex-serving-cert --ignore-not-found=true
kubectl delete secret -n cpaas-system dex.tls
```

3. Introduce the new certificate:

```
kubectl create secret tls dex.tls --cert=/path/to/tls.crt --key=/path/to/tls.key -n cpaas-system
```