

概览

[介绍](#)

[架构](#)

[平台模型](#)

[集群管理模型](#)

[核心与扩展](#)

[可用性与恢复](#)

[版本与生命周期](#)

Kubernetes [支持矩阵](#)

[发版日志](#)

[术语表](#)

[了解更多](#)

介绍

灵雀云容器平台 (ACP) 是一个基于 Kubernetes 的平台，用于在私有云、数据中心、混合云、多云和边缘环境中构建、部署、运维和治理云原生应用。

ACP 将 Kubernetes API 和工作负载原语置于平台中心，然后添加企业级能力，用于集群管理、项目治理、应用交付、扩展管理、可观测性、安全性、升级规划和恢复。

目录

平台提供的内容

与 Kubernetes 的关系

阅读路径

平台提供的内容

Area	它能帮助你做什么	Continue with
平台管理	安装 ACP Core，访问 Web 控制台和 API，并从 <code>global</code> 集群管理平台级服务。	架构
集群运维	创建由 ACP 生命周期管理的工作负载集群，或接入第三方 Kubernetes 环境以进行集中治理。	集群管理模型

Area	它能帮助你做什么	Continue with
项目和命名空间	了解项目、命名空间、用户、配额以及关联集群如何构成平台治理模型。	平台模型
原生应用交付	从镜像、YAML、chart、源代码和 Kubernetes 工作负载资源创建并运维应用。	开发人员概述
扩展	通过 Operator 和 Cluster Plugin 添加能力，并在安装或升级前检查版本兼容性。	Core 和扩展
可用性和恢复	规划部署拓扑、高可用性、Global Cluster Disaster Recovery，以及备份或恢复路径。	可用性和恢复
版本规划	了解 Kubernetes 兼容性、第三方集群接入范围、运行时基线 and 生命周期边界。	版本和生命周期
安全和访问	配置 LDAP 或 OIDC 身份提供方、基于 Kubernetes RBAC 的授权、审计、网络策略、API 过滤、合规功能以及安全产品集成。	安全性

与 Kubernetes 的关系

ACP 构建于 Kubernetes 之上。用户仍然需要与 Kubernetes 资源交互，例如集群、命名空间、工作负载、Service、Ingress、NetworkPolicy、自定义资源和 RBAC 对象。ACP 添加了一个管理平面，帮助平台团队在多个 Kubernetes 环境中应用治理、生命周期管理、可观测性和运维工作流。

部分能力包含在 ACP Core 中。其他能力则通过单独安装的扩展提供，例如 Operator 和 Cluster Plugin，或者通过单独的产品提供。在规划或使用这些能力之前，请查阅相应文档，了解安装、升级、兼容性和限制。

阅读路径

如果你是第一次接触 ACP，请先阅读以下页面：

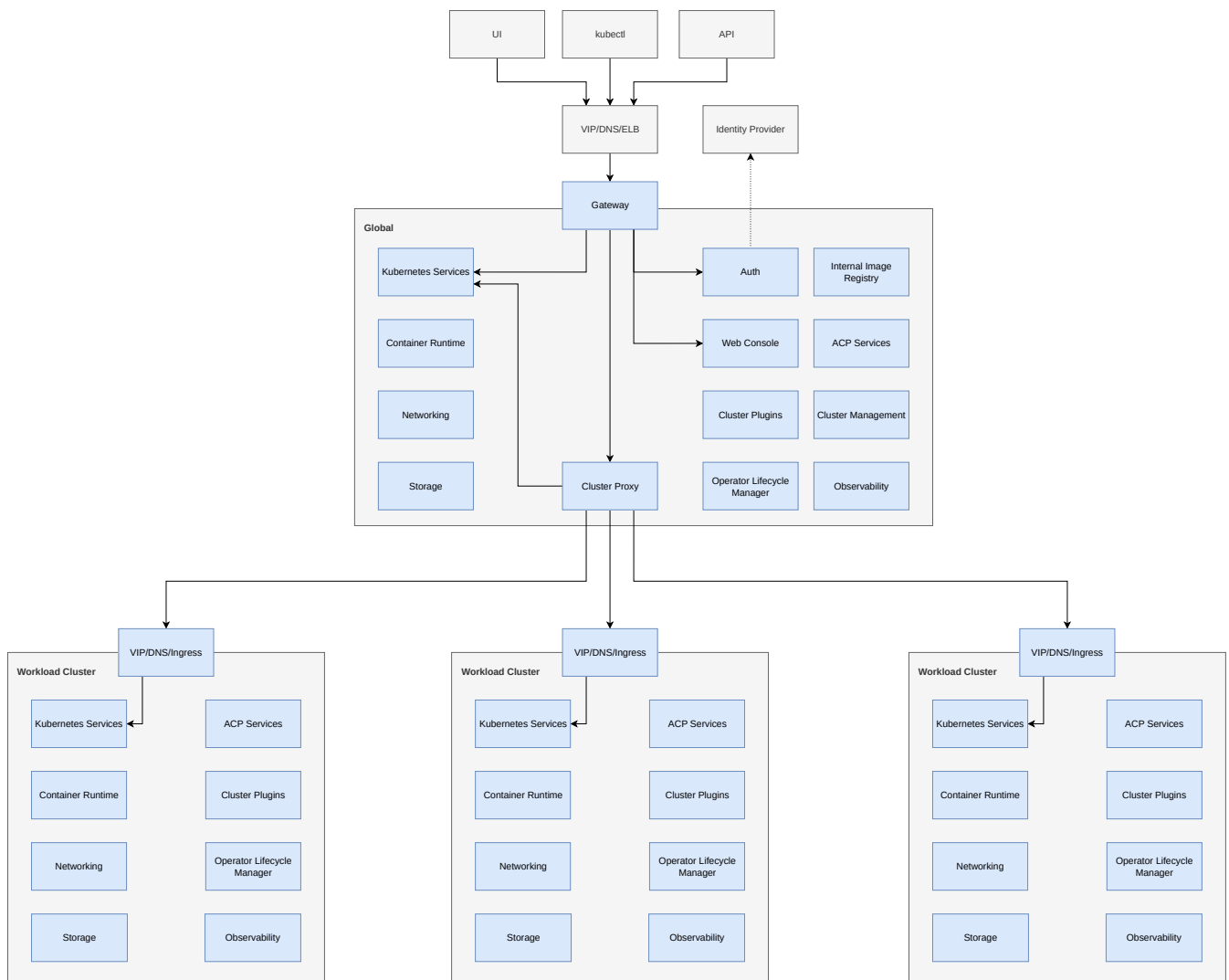
1. [架构](#)，了解 hub-and-spoke 模式。

2. [平台模型](#)，了解 `global` 集群、工作负载集群、第三方集群、项目和命名空间。
3. [集群管理模型](#)，了解基础设施责任、控制平面拓扑和第三方接入。
4. [Core 和扩展](#)，了解哪些能力属于 Core，哪些需要扩展。
5. [了解更多](#)，选择安装、集群运维、原生应用交付、升级规划、恢复、安全、API 或 CLI 的下一步任务路径。

架构

ACP 使用 hub-and-spoke 架构。`global` 集群提供中央管理平面，而业务集群或第三方集群提供运行应用和集群本地组件的 Kubernetes 环境。

请将下图作为此模型的高层视图。下面的架构细节说明了图中未显示的边界。



有关平台范围内的术语，请参见 [词汇表](#)。有关概念性平台模型，请参见 [平台模型](#)。

目录

Hub-And-Spoke 模型

访问与请求路径

管理路径

状态与数据域

Core 与 Extension 边界

可用性与恢复模型

继续阅读

Hub-And-Spoke 模型

部分	角色
<code>global</code> 集群	托管平台管理平面，包括 web 控制台访问、平台 API、认证集成、项目治理、集群管理、Extension 管理以及平台级协调。
业务集群	在 <code>global</code> 集群的治理下运行应用工作负载和集群本地组件。
第三方集群	按照已文档化的前提条件和注意事项接入平台的现有 Kubernetes 环境，用于集中治理和运维。

hub-and-spoke 模型描述了 `global` 集群与其管理的 Kubernetes 环境之间的关系。有关控制平面拓扑（包括 Hosted Control Plane），请参见 [集群管理模型](#)。

`global` 集群是平台的 hub。业务集群和第三方集群是 spoke。一个项目可以跨关联集群展开，而 namespace 可在这些集群内部提供 Kubernetes 资源隔离。

访问与请求路径

用户和自动化通常通过 Platform Access Address、web 控制台、平台 API、Kubernetes API 或 CLI 工具访问平台。

从高层来看：

1. 用户、CLI、自动化工具或浏览器连接到 Platform Access Address。
2. 负载均衡器、VIP、DNS 记录或 ingress 路径将流量路由到平台入口组件。
3. 平台 API 服务评估认证和授权。
4. 请求由 `global` 集群处理，或通过已文档化的集群访问路径转发到目标集群。
5. 对目标集群的 Kubernetes API 请求会根据用户的有效 RBAC 权限进行评估。

有关 API 用法，请参见 [API 简介](#)。有关 CLI 工具，请参见 [CLI 工具](#)。有关集群 KubeConfig 访问，请参见 [使用 KubeConfig 访问集群](#)。

管理路径

`global` 集群协调平台管理操作：

- 支持的 ACP 生命周期管理集群模型的集群创建和生命周期操作。
- 通过导入或注册工作流接入第三方集群。
- 项目、namespace、用户、角色和配额治理。
- Operator 和 Cluster Plugin 的发现、包上传、安装和升级入口。
- 在所需组件已安装时，提供可观测性、审计、资源清单和运维的集中视图。

对于第三方集群，管理路径取决于版本范围、连通性、凭据、提供商前提条件、已安装组件以及 Extension 兼容性。接入第三方集群不会使 ACP 成为该集群的 Kubernetes 生命周期、节点生命周期或提供商基础设施生命周期的所有者。

有关模型边界，请参见 [集群管理模型](#)。

状态与数据域

不同的数据域具有不同的保护和恢复路径：

数据域	主要位置或所有者	恢复路径
global 集群 Kubernetes 资源状态	global 集群 etcd	根据场景，可使用 Global Cluster Disaster Recovery 或 etcd 备份/恢复。
业务集群 Kubernetes 资源状态	每个业务集群 etcd	集群特定的备份/恢复或升级操作步骤。
第三方集群生命周期数据	外部集群所有者、发行版或提供商	外部提供商或所有者的操作步骤，以及 ACP 的接入和运维记录。
注册表数据	Registry 组件或后端	Registry 备份和恢复操作步骤。
监控和日志数据	已安装的监控和日志组件	组件特定的备份或恢复操作步骤。
应用数据	应用 namespace、持久卷、数据库和存储后端	应用备份/恢复或数据服务特定的恢复操作步骤。

Global Cluster Disaster Recovery 仅保护 [可用性与恢复](#) 中记录的

global

 控制平面 DR 场景。它不是完整的平台数据 DR，也不是应用数据 DR。

Core 与 Extension 边界

ACP Core 提供平台管理平面，以及用于管理集群、项目、用户、API 和 Extensions 的框架。

其他能力可能需要单独安装的 Extensions，例如 Operators 和 Cluster Plugins，或者独立产品。示例包括特定的可观测性后端、Registry 插件、API 过滤、合规功能、容器安全、数据服务、GitOps、日志、Immutable Infrastructure 和 Hosted Control Plane。

在将这些能力规划为架构的一部分之前，请查看相应文档中的安装、升级、兼容性和限制。

有关详细信息，请参见 [Core 与 Extensions](#)。

可用性与恢复模型

可用性按拓扑进行规划：

- Single Node 仅用于测试或概念验证。
- 当业务场景适配且已为平台组件和工作负载规划好资源时，Single Cluster 可支持生产使用。
- Multi-Cluster 将 `global` 集群管理平面与业务集群分离，并且应避免在 `global` 集群上运行非平台业务工作负载。
- 三个控制平面节点是 HA 基线。五个控制平面节点是容量和可靠性建议，并不是通用的生产门槛。

有关详细规划、容量、组件级高可用性、Global DR 以及备份/恢复入口点，请参见 [可用性与恢复](#)。

继续阅读

- [简介](#)
- [平台模型](#)
- [集群管理模型](#)
- [Core 与 Extensions](#)
- [了解更多](#)

平台模型

ACP 采用 hub-and-spoke 模型。`global` 集群提供中央平台管理平面，而业务集群和第三方集群则在平台治理下运行或暴露 Kubernetes 工作负载。

使用平台模型可帮助你理解主要的平台对象及其相互关系。

目录

`global` 集群

业务集群

第三方集群

托管控制平面

项目和命名空间

各部分发生的位置

`global` 集群

`global` 集群在 ACP Core 安装期间部署。它提供用于 Web 控制台访问、平台 API、用户和角色、项目治理、集群管理、Extension 管理以及全平台协调的中央管理平面。

`global` 集群不仅仅是管理模型中的另一个业务集群。在 Multi-Cluster 部署中，应避免在 `global` 集群上运行非平台业务工作负载。在 Single Cluster 部署中，`global` 集群也会承载业务工作负载，因此资源规划必须同时考虑平台组件和应用工作负载。

有关安装规划，请参见 [Install Overview](#) 和 [Plan](#)。

业务集群

业务集群是运行应用工作负载并由 `global` 集群管理的 Kubernetes 集群。当所选基础设施模型支持该生命周期时，ACP 可以创建并对业务集群进行生命周期管理。

业务集群继承平台治理，并且可以与项目和命名空间关联。根据所选集群模型和已安装能力，它们还可以接收 Extensions、可观测性组件、网络组件、存储集成以及应用工作负载。

有关集群创建任务，请参见 [Clusters Overview](#) 和 [Creating an On-Premise Cluster](#)。

第三方集群

第三方集群是一个 Kubernetes 环境，其 Kubernetes 发行版和生命周期由 灵雀云 之外的主体提供或管理。这包括现有 Kubernetes 环境、外部 Kubernetes 发行版以及公有云 Kubernetes 服务。

当满足所需的版本范围、连通性、凭据、已安装组件、提供商前提条件以及 Extension 兼容性要求时，ACP 可以接入第三方集群，以实现集中治理、资源可见性、应用运维、Extension 安装以及可观测性集成。

对于第三方集群，除非某个特定提供商或插件文档明确说明具备该能力，否则 ACP 不负责完整的 Kubernetes 生命周期、节点生命周期或提供商基础设施生命周期。Kubernetes 安装、Kubernetes 升级、节点扩缩容以及基础设施操作通常仍由集群所有者、外部发行版或云提供商负责。

`Third-party cluster` 是这些已接入环境的产品模型术语。`Managed Cluster` 是用于管理这些环境的当前 UI 和导航标签。

有关接入工作流，请参见 [Third-Party Cluster Onboarding](#)、[Import Third-Party Clusters](#) 和 [Register Cluster](#)。

托管控制平面

Hosted Control Plane (HCP) 是一种控制平面拓扑，而不是与 Installer-Provisioned Infrastructure (IPI) 或 User-Provisioned Infrastructure (UPI) 并列的集群模型。在 HCP 中，每个托管集群都有自己的托管控制平面，多个托管控制平面作为工作负载运行在管理集群上。在 ACP 中，HCP 通过 Kamaji (`TenantControlPlane`) 实现。

有关当前 HCP 的成熟度、操作系统、连通性、生产使用边界和相关任务，请参见 [About Hosted Control Plane](#)。

项目和命名空间

项目是用于租户、团队或业务系统的治理单元。它可以跨多个关联集群，并为用户、配额、策略和资源可见性提供边界。

命名空间是 Kubernetes 的资源隔离单元。在 ACP 中，可以在项目中创建或导入命名空间，从而让项目级治理应用于该命名空间及其工作负载。

二者的关系如下：

对象	在 ACP 中的关系
<code>global</code> 集群	承载中央管理平面并管理平台治理状态。
业务集群或第三方集群	提供 Kubernetes 容量以及工作负载运行所在的集群本地 API。
项目	定义租户、团队或业务系统的治理边界，并可与一个或多个集群关联。
命名空间	存在于关联集群中，并且可以在项目中创建或导入，使项目治理得以应用。
工作负载和资源	在命名空间内运行，并继承适用的项目、命名空间和集群策略。

有关项目和命名空间的概念，请参见 [Project Introduction](#) 和 [Namespace Management](#)。

各部分发生的位置

区域	通常发生在 global 集群中	通常发生在业务集群或第三方集群中
平台访问	Web 控制台、平台 API、中央身份验证流程以及平台级控制器	集群 API 端点和集群本地 Kubernetes API
治理	用户、角色、项目、配额、策略以及集群关联	命名空间级 Kubernetes 资源和工作负载权限
集群生命周期	集群创建、接入记录、受支持集群模型的升级编排以及 Extension 管理	Kubernetes 控制平面、节点、工作负载、集群本地组件以及由提供商负责的生命周期
可观测性和审计	当已安装所需服务时，集中视图、查询、仪表板和审计界面	指标、日志、事件或审计收集组件，受提供商和连通性边界限制
恢复	Global Cluster Disaster Recovery 和平台状态恢复规划	集群级备份/恢复、组件数据恢复以及应用备份/恢复

有关高层架构，请参见 [Architecture](#)。有关模型比较和责任边界，请参见 [Cluster Management Models](#)。

集群管理模型

使用集群管理模型来区分三个规划决策：

1. 基础设施责任。
2. 控制平面拓扑。
3. Kubernetes 所有权和入驻。

每条集群路径都会将这些维度上的选项组合起来。Installer-Provisioned Infrastructure (IPI)、User-Provisioned Infrastructure (UPI)、Hosted Control Plane (HCP) 以及当前 UI 标签 `Managed Cluster` 不是一组扁平的、相互排斥的集群类型列表。

目录

基础设施责任

控制平面拓扑

Kubernetes 所有权与入驻

第三方集群能力边界

提供商和工作流注意事项

基础设施责任

基础设施责任说明由谁来提供和管理机器、节点操作系统以及 Kubernetes 生命周期。

模型	机器和节点	节点操作系统	Kubernetes 生命周期	主要文档
Installer-Provisioned Infrastructure (IPI)	通过平台及其基础设施提供商集成进行预配。	由平台使用 Immutable OS 管理。	由平台管理，包括受支持的预配、扩缩容和升级流程。	关于 Immutable Infrastructure
User-Provisioned Infrastructure (UPI)	由用户准备为物理机或虚拟机。	由用户管理。	在用户准备好节点后，由平台安装并管理。	创建本地集群

IPI 和 UPI 描述的是责任边界。它们本身并不说明控制平面是托管的还是专用的，也不说明第三方集群是否已经被导入或注册。

现有的第三方 Kubernetes 环境包含在 [Kubernetes 所有权与入驻](#) 中，因为它们的 Kubernetes 分发版和生命周期通常存在于 灵雀云 之外。

控制平面拓扑

控制平面拓扑说明 Kubernetes 控制平面组件运行在何处。

拓扑	含义	支持边界
专用控制平面	控制平面组件运行在目标集群中的控制平面节点上。	这是当前生产指导中的标准拓扑。
Hosted Control Plane	每个托管集群都有自己的控制平面，但控制平面作为工作负载运行在管理集群上。在 ACP 中，HCP 通过 Kamaji (<code>TenantControlPlane</code>) 实现。	有关当前成熟度、操作系统、连接性和生产使用边界，请参见 关于 Hosted Control Plane 。

HCP 是针对控制平面的架构。它不是 ACP Core 的默认能力，也不是与 IPI 或 UPI 并列的概念。

有关更多信息，请参见 [关于 Hosted Control Plane](#)。

Kubernetes 所有权与入驻

Kubernetes 所有权说明 ACP 是否拥有 Kubernetes 生命周期，或者 Kubernetes 环境是否已存在于 灵雀云 之外。

模型	如何进入平台	生命周期边界
ACP 生命周期管理的业务集群	通过受支持的 ACP 集群工作流创建。	ACP 管理所选模型受支持的 Kubernetes 生命周期。
第三方集群	通过导入或注册工作流入驻。	ACP 在文档化的前提条件和注意事项范围内提供集中治理和运维。外部集群所有者、分发版或提供商通常负责 Kubernetes 生命周期、节点生命周期以及提供商基础设施生命周期。

`Managed Cluster` 是第三方集群入驻和管理区域当前使用的 UI 和导航标签。对于产品模型规划，请使用 `Third-party cluster`。

`Import cluster` 和 `Register cluster` 是第三方集群的入驻方法：

入驻方法	连接模型	适用场景
Import cluster	<code>global</code> 集群使用提供的地址、CA 和凭据连接到目标集群 API server。	平台可以访问目标集群 API server，并且 operator 可以提供所需的集群信息。
Register cluster	目标集群中的反向代理服务发起注册并建立到平台的隧道。	目标集群应主动发起连接，或者平台对目标 API server 的直接访问受到限制。

入驻之后，预期的 day-2 管理在 Overview 级别上被视为相同。不过，提供商和特定工作流的注意事项仍然适用。

第三方集群能力边界

在满足前提条件时，ACP 可以为第三方集群提供以下入口能力：

- 资源可见性和集中治理。

- 项目和命名空间关联。
- Application 运维。
- Operator 和 Cluster Plugin 安装，但受 Extension 兼容性限制。
- 可观测性集成，但受已安装组件、网络路径、凭据和提供商注意事项限制。

第三方集群入驻并不意味着 ACP 会在每个第三方集群上管理每个 Kubernetes 版本、提供商操作、节点操作、证书、控制平面指标、审计源、Ingress 路径、存储类或 Extension 镜像。

请使用 [Kubernetes Support Matrix](#) 中产品支持的入驻范围来确认 Kubernetes 版本是否符合要求。请另行检查提供商前提条件和确切的 Extension 兼容性。

有关准确的矩阵和升级关系，请参见 [Kubernetes Support Matrix](#) 和 [Version and Lifecycle](#)。

提供商和工作流注意事项

使用以下注意事项类别来确定应查看哪份提供商或工作流文档，以获取提供商特定的详细信息。

注意事项类别	需要检查的内容	继续阅读
Kubernetes 生命周期	Kubernetes 安装或升级是由 ACP 管理，还是由外部所有者管理。	集群概览
节点生命周期	所选模型是否支持从平台 UI 添加、删除或扩缩容节点。	节点管理
连接性	global 集群和目标集群是否可以访问所需端点，以及是否需要平台 URL 注解。	导入集群的网络配置
证书	平台对所选工作流可见或轮换哪些证书。	导入第三方集群 下的提供商或入驻工作流文档
审计和指标	目标环境是否提供审计数据和控制平面指标。	审计 以及提供商工作流文档
Ingress 和存储	导入后是否需要为 Ingress、负载均衡或存储类进行初始化。	公有云集群初始化

注意事项类别	需要检查的内容	继续阅读
Extension 兼容性	确切的 Operator 或 Cluster Plugin 版本是否支持目标 ACP 版本和集群模型。	Core and Extensions

如果你需要决定接下来阅读什么，请参见 [了解更多](#)。

核心与扩展

ACP 的功能通过作为独立软件包分发的 ACP Core 和 Extensions 提供。理解这一区分有助于你规划安装、升级、兼容性检查和故障排查。

目录

Core

软件包边界

扩展类型

生命周期类型

兼容性来源

功能边界

Core

ACP Core 会部署 `global` 集群，并提供平台管理平面、平台 API 和 CLI 访问、集群管理、项目和命名空间管理、用户和 RBAC、扩展管理框架，以及诸如 Cluster Proxy 之类的核心通信路径。面向用户的功能（例如 Web Console）由 Aligned Extensions 提供。

Core 功能随 ACP Core 一起安装，或者作为部署在 `global` 集群中的平台管理平面的一部分。需要单独安装流程、Operator、Cluster Plugin 或独立产品的功能，不属于默认的 Core 功能。

有关安装范围，请参见 [安装概览](#)。

软件包边界

ACP Core Package 仅包含 Core 工件，不包括 Aligned 或 Agnostic Extension 软件包。

某些安装和升级流程要求你单独下载特定的 Aligned Extension 软件包，并将其复制到已解压 Core Package 的 `plugins/` 目录中。这是一个手动的工件准备步骤。将 Extension 软件包放入该目录，并不会使该 Extension 成为 Core 的一部分，也不会改变其生命周期类型。

扩展类型

Extension 是 ACP 中两种主要扩展机制的统称：

扩展类型	技术	执行安装的位置	从这里开始
Operator	Operator Lifecycle Manager (OLM)、OperatorHub、 <code>CatalogSource</code> 、 <code>Subscription</code> 、 <code>InstallPlan</code> 和 <code>ClusterServiceVersion</code> 。	在 Operator 运行的目标集群中。	Operator
Cluster Plugin	<code>ModulePlugin</code> 、 <code>ModuleConfig</code> 和 <code>ModuleInfo</code> 自定义资源。	基于 YAML 的安装会在 <code>global</code> 集群中创建 <code>ModuleInfo</code> ；插件目标取决于亲和性和配置。	Cluster Plugin

OperatorHub 是用于发现、安装、升级和管理 Operators 的界面。Cluster Plugins 会发布到 `global` 集群，并根据每个插件的配置和亲和性，通过平台进行安装。

有关 Extension 部分，请参见 [Extend](#)。

生命周期类型

Operators 和 Cluster Plugins 使用相同的生命周期模型：

生命周期	含义	升级行为
Core	遵循 ACP Core 版本发布和集群 Distribution Version。	通过升级集群进行更新。不支持独立升级。
Aligned	遵循 ACP 发布流，但在发布兼容版本后可以独立更新。	当精确版本兼容时，可以独立升级。
Agnostic	与 ACP 独立发布。	当精确版本兼容时，可以独立升级。

Cluster Plugins 通过 cpaas.io/lifecycle-type 标签公开此模型。对于 Operators，应通过灵雀云 customer portal 元数据、Extension 文档或发布指南来检查兼容性，而不要期望产品界面中显示每一个生命周期标签。

有关 Cluster Plugin 详情，请参见 [Cluster Plugin](#)。

兼容性来源

对于特定的 Operator 或 Cluster Plugin 版本，请以灵雀云 customer portal 中的 [ACP compatible versions](#) 字段作为兼容性依据。确切的 Extension 版本必须将目标 ACP 版本列为兼容。

请使用每个 Extension 的产品文档来了解其功能、安装步骤、升级步骤、限制、已知问题、受支持的 Kubernetes 版本、架构、提供商以及集群模型。release notes 有助于了解版本变更，但它并不是每个特定 Extension 版本的主要兼容性来源。Kubernetes 支持矩阵描述了平台与 Kubernetes 版本之间的关系，以及 [第三方集群的默认产品验证范围](#)；它不是 Extension 兼容性矩阵。

有关软件包处理，请参见 [上架软件包](#) 和 [下载软件包](#)。

功能边界

在规划安装、升级和运维时，请使用以下边界：

功能区域	说明
Registry	平台可以提供 registry 入口点和与 registry 相关的工作流。Registry 插件、后端、备份和恢复都有各自的安装与运维边界。
可观测性	集中式可观测性依赖已安装的监控、日志、事件、追踪或检查组件。对于第三方集群，适用提供商和连接性注意事项。
审计	审计使用平台审计视图，并依赖日志服务组件。第三方提供商的审计数据并非普遍可用。
安全与合规	身份验证、RBAC、NetworkPolicy、API 过滤、合规功能以及安全产品都有各自独立的组件边界和安装要求。
独立产品和单独安装的功能	Service Mesh、AI、Hyperflux、Data Services、Cost Management、DevOps、Container Security、Compliance Service、GitOps、Logging Service、Immutable Infrastructure、Hosted Control Plane 和 Cluster Authentication 不是默认的 Core 功能。在规划安装、升级、兼容性或限制之前，请先查阅相应文档。

有关面向任务的路线图，请参见 [了解更多](#)。

可用性 & 恢复

通过将您的环境与合适的部署拓扑、高可用基线、Global Cluster 灾难恢复路径以及备份或恢复操作步骤相匹配，来规划可用性 & 恢复。

有关详细的容量规划、备份、恢复和灾难恢复操作步骤，请遵循链接到的专题操作步骤。以下指南重点介绍规划选择和支持边界。

目录

部署拓扑

高可用基线

组件级高可用

Global Cluster 灾难恢复

备份和恢复路径

恢复清单

部署拓扑

应根据场景选择拓扑，而不是依据单一的生产最低配置表。

拓扑	适用场景	可用性说明
Multi-Cluster	一个 <code>global</code> 集群管理多个业务集群。	避免在 <code>global</code> 集群上运行非平台业务工作负载。根据受管集群数量、用户并发、API 流量以及已安装插件来为 <code>global</code> 集群进行容量规划。
Single Cluster	一个集群有意同时运行平台组件和业务工作负载。	当其适用于单一业务系统场景时，可用于生产环境。需要同时为平台组件和工作负载规划资源。在此模式下， <code>global</code> 集群控制平面使用 3 个节点。
Single Node	测试或概念验证环境。	不要用于生产环境。

有关安装规划，请参阅 [规划](#) 和 [前提条件](#)。

高可用基线

对于类似生产的环境，请使用 3 个控制平面节点作为 HA 基线。对于更大的环境，5 个控制平面节点的拓扑可以提升扩展性和可靠性，但这并不是每个生产部署都必须满足的通用硬性要求。

Infra 节点或自定义角色节点适用于隔离平台组件或高负载组件，但除非某个容量层级或组件文档另有说明，否则它们并非通用要求。对于 Extra Large `global` 集群容量规划，请遵循专用 infra 节点的容量规划指南。

规划主题	来源
按受管集群数量划分的 <code>global</code> 集群容量规划	评估 Global Cluster 的资源
业务集群控制平面容量规划和扩展因素	评估业务集群的资源
节点角色以及 infra/custom role 节点	集群节点规划
节点要求和 OS/kernel 支持	节点预处理

组件级高可用

标准 HA 拓扑部署依赖以下跨平台组件的机制。此部分内容为架构师提供参考上下文；当平台以 HA 拓扑部署时，您无需按组件逐一进行这些配置。

etcd

- 部署在 `global` 集群控制平面节点上。
- 使用 RAFT 共识协议进行领导者选举和状态复制。
- 3 节点控制平面部署可容忍 1 个节点故障；5 节点控制平面部署可容忍 2 个节点故障。
- 支持本地和远程对象存储快照备份用于恢复。

平台访问和 ingress

- 集群 ingress 网关以多个副本运行，并支持领导者选举。
- 通过外部负载均衡器、DNS 记录或带心跳检测和主备切换的自建 VIP 提供平台访问入口。

镜像仓库和对象存储

- 镜像仓库组件在集群 ingress 后以多个副本运行，并配备高可用数据库后端和高可用缓存后端。
- 平台使用的对象存储后端以分布式模式运行，具备纠删码、数据冗余和自动恢复能力。

监控和日志

- 监控以多个实例运行，并提供查询时去重、分布式存储组件以及跨地域冗余选项。
- 日志组件在采集、传输、存储和查询各阶段均以分布式、多副本模式部署。

容器网络

- 容器网络接口（CNI）通过无状态的按节点 Agent 以及三副本控制平面组件实现高可用。

自愈

- 健康检查、故障转移和流量重定向由 Kubernetes 控制平面和平台组件协同协调。
- 当某个节点不可用时，瞬时故障会重试，工作负载会重新调度到健康节点上。

有关拓扑级规划，请参阅 [高可用基线](#)。有关集群级灾难恢复，请参阅 [Global Cluster 灾难恢复](#)。

Global Cluster 灾难恢复

当 Primary `global` 集群不可用时，Global Cluster 灾难恢复可保护平台管理入口和 `global` 控制平面服务。

Global DR 的范围如下：

- 使用 Primary 和 Standby `global` 集群。
- 依赖于存储在 Primary `global` 集群 etcd 中的资源状态实时同步，不包括排除的命名空间。
- 通过将 DNS 或 VIP 访问切换到 Standby 集群来恢复平台入口和 `global` 控制平面服务。
- Primary 和 Standby 应遵循经过验证的对齐版本、补丁、组件版本和关键配置路径。

不要将 Global DR 视为完整的平台数据 DR、应用数据 DR、自动故障转移，或具有 SLA 约束的 RPO/RTO 承诺。Global DR 不涵盖镜像仓库数据、chartmuseum 数据、其他组件数据、应用数据或被排除在 etcd 同步之外的资源。

有关操作步骤和受支持的场景，请参阅 [Global Cluster 灾难恢复](#)。

备份和恢复路径

恢复由场景决定。每种机制都保护特定的数据域，并且具有各自的操作步骤、前提条件和限制。

场景	用途	来源
Primary <code>global</code> 集群故障	Global Cluster 灾难恢复。	Global Cluster 灾难恢复
误删集群状态或回滚	etcd 备份和恢复。	etcd 备份和恢复
镜像仓库数据	镜像仓库备份和恢复。	镜像仓库数据备份和恢复
监控数据	监控组件备份或恢复。	VictoriaMetrics 备份和恢复

场景	用途	来源
日志数据	根据所安装的日志后端执行日志组件备份或恢复。	日志服务
应用资源和持久卷	使用 Data Backup Essentials 和 Data Backup for Velero 进行应用备份和恢复。	备份概览

应用备份可根据备份配置保护命名空间、Kubernetes 资源和持久卷数据。它并不支持所有存储或应用数据模式。例如，文档化的应用备份路径不支持 `hostPath` PersistentVolumes，数据库工作负载应遵循数据服务特定的备份指南。

恢复清单

使用此清单来选择后续工作。有关详细步骤，请遵循链接到的操作步骤：

1. 在安装规划期间选择 Single Cluster、Multi-Cluster 或 Single Node。
2. 根据扩展性指南为 `global` 集群和业务集群进行容量规划。
3. 在安装 ACP Core 之前，确定是否需要 Global Cluster 灾难恢复。
4. 根据需要恢复的数据域，为 etcd、镜像仓库数据、监控数据、日志数据和应用配置备份。
5. 按照您的运维流程要求，定期执行恢复检查和故障转移演练。
6. 在故障转移或恢复后，验证平台访问、`global` 服务、已连接集群访问以及组件级恢复情况。

有关相关的规划和运维路径，请参阅 [了解更多](#)。

[Alauda Container Platform](#) > [概览](#) > 版本与生命周期

版本与生命周期

使用本指南规划 ACP 版本兼容性、Kubernetes 支持、第三方集群接入、runtime 和 OS 边界，以及 Extension 生命周期检查。

使用 [Kubernetes Support Matrix](#) 获取准确的 Kubernetes 版本表。

目录

[产品与 Kubernetes 版本](#)

[第三方集群接入范围](#)

[Runtime、OS 与 CPU 架构](#)

[Extension 生命周期](#)

[功能成熟度](#)

[升级阅读路径](#)

产品与 Kubernetes 版本

Kubernetes 支持矩阵区分三项决策：平台托管集群创建可使用哪些 Kubernetes 目标版本、哪些业务集群版本满足 `global` 集群升级前置条件，以及哪些 Kubernetes minor 版本受产品支持并可用于第三方集群接入。不要根据其中一个范围推断另一个范围。

对于 ACP 4.3 及更高版本，在升级 `global` 集群之前，业务集群只需要保持在文档中定义的 Compatible Versions 范围内。对于 ACP 4.2 及更早版本，在升级 `global` 集群之前，业务集

群必须先升级到兼容列表中的最新 Kubernetes 版本。

准确的 Kubernetes build 和创建目标版本来自已安装平台 patch 和发布特定制品所提供的版本，而不是来自本生命周期概述。

如需准确表格，请参见 [Kubernetes Support Matrix](#)。

第三方集群接入范围

使用 [Product-Tested Scope for Third-Party Clusters](#) 了解当前产品支持的 Kubernetes 范围、持续验证策略以及默认验证范围。

产品测试过的接入范围适用于 ACP 4.3 及更高版本中提供第三方集群接入功能的发布版本。该范围独立于按发布版本提供的创建和 Compatible Versions 行，并且会在产品验证范围扩大时更新共享范围。

此范围与以下内容相互独立：

- 平台托管集群创建支持的 Kubernetes 版本。
- 升级 `global` 集群前使用的业务集群兼容版本。
- 对每个 provider、capability、operation 或 Extension 的支持。

已发布的 Kubernetes 范围定义了版本准入条件。请按照 [Third-Party Cluster Onboarding](#) 以及所选的 Import、Register 或 provider 特定操作步骤来完成连通性、凭据和环境特定准备。

有关集群模型边界，请参见 [Cluster Management Models](#)。

Runtime、OS 与 CPU 架构

按照职责边界阅读 runtime、OS、CRI 和 CPU 架构信息。

环境	如何阅读支持信息
ACP 生命周期管理环境	平台会安装并管理 containerd。准确的 runtime build 取决于已安装的 ACP patch，并不是稳定的 minor release 文档值。对于不可变节点，请使用 patch 特定的 OS Support Matrix。

环境	如何阅读支持信息
HCP 环境	使用 About Hosted Control Plane 查看当前成熟度、runtime、操作系统、连通性以及生产使用边界。
第三方集群	节点 OS、container runtime、CRI 和 CPU 架构通常仍由外部集群所有者、外部分发版或云提供商负责。
Immutable Infrastructure	使用由 ACP 提供的 Alauda OS 镜像以及 provider 特定要求对应的 Immutable Infrastructure 文档。
Extensions	使用确切的 Extension 文档和 Customer Portal 兼容性元数据。对于每个 Extension 镜像或 provider 场景，x86、ARM 或混合架构的软件包可用性并不构成通用保证。

除非明确的支持矩阵、Extension 文档、provider 文档或 release guidance 说明支持，否则不要推断完全支持 Docker、CRI-O、Alauda OS、混合架构业务集群、provider 架构或通用 Extension 镜像支持。

有关节点前置条件，请参见 [Node Preprocessing](#)。有关软件包架构，请参见 [Download](#)。有关 Immutable Infrastructure，请参见 [About Immutable Infrastructure](#)。

Extension 生命周期

Operators 和 Cluster Plugins 使用 [Core](#)、[Aligned](#) 和 [Agnostic](#) 生命周期模型。

生命周期	兼容性和升级含义
Core	遵循 ACP Core release 和 cluster Distribution Version。通过集群升级进行更新。
Aligned	遵循 ACP release stream，但在发布兼容版本后可以独立升级。
Agnostic	独立于 ACP 发布，并在发布兼容版本后可独立升级。

对于特定的 Operator 或 Cluster Plugin 版本，请使用 灵雀云 Customer Portal 中的 [ACP compatible versions](#) 字段作为兼容性依据。release notes 有助于了解版本变更。

Kubernetes 支持矩阵不是某个确切 Extension 版本的权威来源。

有关详细信息，请参见 [Core and Extensions](#)。

功能成熟度

在阅读 Overview、release notes 或组件文档时，请将成熟度标签视为支持边界：

标签	对读者的含义
GA	该功能在文档定义的范围和前置条件内正式可用。
Technology Preview	该功能可在文档限定范围内用于评估，在产品文档明确说明之前，不应视为生产支持。
Deprecated	该功能仍可用，但计划移除或替换。请根据 release guidance 规划迁移。
Removed	该功能在文档所述版本中已不可用。

有关当前 HCP 成熟度和评估边界，请参见 [About Hosted Control Plane](#)。Global Cluster Disaster Recovery 仅在 [Availability and Recovery](#) 中文档定义的 `global` 控制平面 DR 范围内正式可用。

升级阅读路径

在升级之前：

1. 阅读 [Kubernetes Support Matrix](#)，确认兼容的业务集群版本。
2. 阅读 [Upgrade Overview](#)，了解基于 CVO 的升级模型。
3. 在升级 `global` 集群之前阅读 [Pre-Upgrade](#)。
4. 在 灵雀云 Customer Portal 和 Extension 文档中检查 Extension 兼容性。
5. 查看 [Release Notes](#)，了解版本变更、行为变更、Technology Preview 状态、已弃用功能和已知问题。

Kubernetes 支持矩阵

使用 Kubernetes 支持矩阵来确认 ACP 版本的 Kubernetes 版本关系，并区分集群创建、升级兼容性以及第三方集群接入边界。

有关概念性的生命周期指导，请参见 [版本和生命周期](#)。

目录

如何阅读本页

版本支持矩阵

第三方集群的产品测试范围

产品支持的 Kubernetes 范围

默认验证范围

升级要求

如何阅读本页

术语	含义
支持用于集群创建	ACP 为该版本创建新的由平台管理的集群时可使用的 Kubernetes 版本。
兼容版本	在 <code>global</code> 集群升级到该 ACP 版本之前，工作负载集群可以运行的 Kubernetes 版本。

术语	含义
第三方集群产品测试范围	产品支持的 Kubernetes 接入范围，以及产品验证在第三方集群上覆盖的默认功能。

版本支持矩阵

下表显示了每个 ACP 版本支持的 Kubernetes 版本。

INFO

本文档针对 ACP 的一个 minor 版本分支维护，不会为每个 patch 版本单独发布一套文档。此表反映的是当前文档中所述该版本分支支持的 Kubernetes minor 版本。如果后续 patch 版本新增了另一个 Kubernetes minor 版本，则会更新相应行及其兼容版本范围。请使用平台提供的目标版本以及与版本相关的制品来获取准确的 Kubernetes build。

在该版本分支的任一时点，仅应使用已安装的 ACP patch 提供并验证过的 Kubernetes 目标来创建集群。当后续 patch 新增了另一个已验证的 Kubernetes minor 版本时，该 minor 级别的行可能会扩展。

ACP 版本	支持用于集群创建	兼容版本
ACP 4.4	1.35	1.35, 1.34, 1.33, 1.32
ACP 4.3	1.34	1.34, 1.33, 1.32, 1.31
ACP 4.2	1.33	1.33, 1.32, 1.31, 1.30
ACP 4.1	1.32	1.32, 1.31, 1.30, 1.29
ACP 4.0	1.31, 1.30, 1.29, 1.28	1.31, 1.30, 1.29, 1.28

第三方集群的产品测试范围

产品支持的 Kubernetes 范围

第三方 Kubernetes 集群已完成产品接入验证，支持的 Kubernetes 范围为 1.28 到 1.35（含）。该范围之外的 Kubernetes minor 版本不被声明为第三方集群接入的产品支持范围。

当前的产品测试范围适用于 ACP 4.3 及更高版本，这些版本提供第三方集群接入。该范围作为一个共享范围进行维护，而不是复制到每个版本行中；当产品验证覆盖了更多 Kubernetes minor 版本时，会进行更新。

产品验证计划会持续测试更多 Kubernetes minor 版本。计划测试或仍在评估中的版本不属于产品支持范围。某个版本完成产品验证后，本页上的范围会随之更新。请以当前发布的范围作为产品支持的依据。

该范围与“兼容版本”列是分开的。“兼容版本”用于确定工作负载集群是否满足升级 [global](#) 集群的前置条件。第三方接入范围用于确定某个第三方 Kubernetes 集群是否可以接入。

默认验证范围

对于处于已发布 Kubernetes 范围内的第三方集群，默认产品验证覆盖以下内容：

- 核心 Kubernetes 工作负载和资源操作，例如创建和管理 Deployments。
- 用于安装和升级 Operators 与 Cluster Plugins 的 [Extend](#) 操作步骤。
- 通过 Extend 安装和升级的基于 ClickHouse 的日志功能。
- 通过 Extend 安装和升级的基于 VictoriaMetrics 的监控功能。

Extend 被纳入默认验证范围，是因为经过验证的日志和监控功能在安装和升级时依赖 Extend。客户在目标环境中如果对应的 Operator 或 Cluster Plugin 声明兼容性，也可以使用 Extend 安装其他功能。

默认产品验证并不意味着会验证每一个具体的 Operator 或 Cluster Plugin。对于任何其他 Operator 或 Cluster Plugin，请查看其产品文档和 灵雀云 Customer Portal 兼容性元数据，或联系技术支持。

已发布的 Kubernetes 范围和默认验证范围不能替代所选接入方式的前置条件。请遵循 [第三方集群接入](#) 以及适用的 Import、Register 或特定于提供商的操作步骤，以验证连接性、凭据和特定环境的准备工作。

有关模型边界，请参见 [集群管理模型](#)。有关升级规划，请参见 [升级概览](#) 和 [升级前](#)。

升级要求

对于 ACP 4.3 及更高版本，工作负载集群在升级 `global` 集群之前，只需保持在文档中所述的兼容版本范围内。

在 ACP 4.2 及更早版本中，在升级 `global` 集群之前，所有工作负载集群都必须升级到兼容版本列表中的最新 Kubernetes 版本。

有关升级操作步骤，请参见 [升级](#)。

发版日志

请结合 [Kubernetes Support Matrix](#)、[Version and Lifecycle](#) 以及特性相关文档查看 release notes，以了解发版变更和准确的支持边界。

目录

4.4.0

功能和增强

Kubernetes 1.35 和升级就绪检查

更一致的平台安装和升级

日志收集插件更新

平台镜像源

应用镜像和工作负载操作

监控、监控面板和成本管理

网络

存储

虚拟化

Global Cluster 灾难恢复增强

Alauda OS 备份和恢复

访问和授权

Immutable Infrastructure

即将发布的 Immutable Infrastructure 提供商版本

弃用和移除

已修复问题

已知问题

相关产品站点

4.4.0

发布日期：2026-08-18

功能和增强

Kubernetes 1.35 和升级就绪检查

ACP 4.4 将平台基线升级到 **Kubernetes 1.35**。在升级之前，请确认每个生产节点都满足新的 Kubernetes 要求：内核版本必须为 5.8 或更高，并且节点必须使用 cgroup v2。升级预检会阻止升级，直到管理员确认这些检查已完成为止。

有关必需检查和确认操作步骤，请参见 [Prepare for an Upgrade](#) 和 [Upgrade a Global Cluster](#)。

更一致的平台安装和升级

ACP 4.4 提升了安装和升级的可靠性。在新的 `global` 集群上，upgrade-management 组件会自动安装。平台组件也会按固定的依赖顺序安装，从而减少在独立安装可选平台服务时发生的安装和升级失败。

有关升级操作步骤，请参见 [Upgrade](#)。

日志收集插件更新

以下更新由独立版本发布的 Log Collection 插件提供。匹配的插件版本可能在 ACP 4.4 平台版本之后发布；请在软件包可用时进行安装。其产品文档和 release notes 将提供详细的配置和升级操作步骤。

- **Vector** 日志收集 — Log Collection 插件将日志收集器切换为 **Vector**。Vector 为大日志量场景提供更高性能的收集路径，并提供从先前收集器迁移的路径。
- **OpenSearch** 日志存储 — 匹配的插件版本将其内嵌的 Elasticsearch 服务替换为连接到由客户提供的 OpenSearch 服务。新的日志数据将写入 OpenSearch。现有 Elasticsearch 数据

不会自动迁移，可作为只读历史数据保留。插件本文档将说明受支持的历史数据处理方式和升级操作步骤。

平台镜像源

对于新的生产部署，ACP 4.4 更改了推荐的平台镜像源策略：使用外部镜像仓库，可以是贵组织现有的仓库，也可以是单独部署的仓库。将其用作平台、已管理集群和插件的中心镜像源。

平台内置仓库仍受支持，但它不再是新生产环境的推荐默认方案。

有关仓库要求、负载上传、安装、验证、升级准备和故障排查，请参见 [Prepare an External Platform Image Registry](#)。

ACP 4.4 交付周期中的下一次独立版本组件发布，将允许基于 Alauda OS 的 Workload Cluster 独立使用第三方仓库，而不依赖 Global Cluster 仓库。这使您可以在地理上分离的环境中，将镜像源放置得更靠近 Workload Cluster。相关产品文档和 release notes 将在该组件版本可用后说明受支持的场景和配置。

应用镜像和工作负载操作

- 用于应用镜像的 **Operator-managed Registry v2** — ACP 提供一个由 operator 管理的集成式仓库，供应用开发人员和 workload 推送、拉取和管理应用镜像。管理员可以从 OperatorHub 安装它，并配置存储、命名空间范围访问以及受管理的 ServiceAccount 拉取密钥。workload 使用集群内的 Registry 服务；在需要时，管理员可以将其暴露给开发人员机器和 CI。它支持按照配置的保留策略定期清理镜像；当您需要回收未引用的存储时，请单独运行 registry 垃圾回收。旧版 Registry Cluster Plugin 对现有旧部署仍可用。有关安装、配置、访问和清理操作步骤，请参见 [Registry v2 administration](#)。
- 基于策略的工作负载再平衡 — 当 workload 因利用率、节点配置、亲和性、污点或拓扑发生变化后需要重新平衡时，请安装 **Alauda Build of Descheduler** 集群插件。该插件会根据已配置的策略驱逐符合条件的 Pod；对于由控制器管理的 Pod，默认调度器会在驱逐后放置替代 Pod。它默认不安装，不会自行调度替代 Pod，并会遵守 PodDisruptionBudgets。有关安装、策略和验证指导，请参见 [Workload Rebalancing \(Descheduler\)](#)。
- 原地调整 **Pod** 资源大小 — ACP 4.4 提供了在目标集群支持的情况下，使用 Kubernetes Pod `resize` 子资源调整运行中 Pod 的 CPU 和内存请求及限制的指导。请使用 `kubectl` 或支持该子资源的 API 客户端。这不是通用的 web 控制台编辑功能，并且 `resizePolicy` 决定容器是否必须重启；VPA `InPlaceOrRecreate` 仍然可以回退到重建 Pod。有关前提条件、示例和限制，请参见 [Adjust Pod Resource Levels Without Pod Disruption](#)。

- **PodDisruptionBudget** 运行指导 — 新的操作和 API 指导说明了如何使用 `minAvailable` 或 `maxUnavailable` 在节点 drain、维护和升级等自愿性中断期间保护已复制的工作负载。PodDisruptionBudget 无法保护工作负载免受节点硬件故障等非自愿性故障的影响。有关示例和 API 详情，请参见 [Using PodDisruptionBudgets](#)。

监控、监控面板和成本管理

- **Perses** 监控面板 — 使用 Perses 监控面板体验创建和管理指标监控面板，导入受支持的 Perses 或 Grafana 监控面板 JSON，并在需要时迁移现有的 `MonitorDashboard` 资源。现有 Monitoring Dashboards 在过渡期间仍可使用。有关详情，请参见 [Perses Monitoring Dashboards](#)。
- **Fleet Monitoring** — 平台管理员可以在一个多集群视图中查看已连接集群、监控数据新鲜度、资源容量和利用率，以及项目配额分配和使用情况。Fleet Monitoring 是对单个集群的详细监控和故障排查的补充，而不是替代。有关详情，请参见 [Fleet Monitoring](#)。
- 用于成本管理的 **VictoriaMetrics** — Cost Management 和计量可使用 VictoriaMetrics 作为指标数据源。查询会限定在相关集群范围内，从而帮助确保在多集群环境中返回的是正确集群的成本和资源使用数据。有关详情，请参见 [Cost Management](#)。

网络

- **SR-IOV** 支持 — ACP 4.4 支持将 SR-IOV 网络接口直接透传给 Pod，因此网络密集型工作负载，例如运营商核心网应用，可以运行在该平台上。
- **OVN** 安全组 **FQDN** 规则 — SecurityGroup 规则支持域名（FQDN）匹配，因此管理员可以使用域名而不仅仅是静态 IP 或 CIDR 目标来定义出站策略。
- **OVN** 数据库 **SSL** 加密 — 与 OVN 数据库的连接可以使用 SSL 加密，包括基于证书的访问和证书轮换，从而提升控制平面通信安全性。
- **AdminNetworkPolicy GA** — AdminNetworkPolicy 已适配新的 API 版本，并正式可用，支持 web 控制台管理。有关详情，请参见 [Admin Network Policy](#)。
- **IPVLAN CNI binary** — Kube-OVN 交付版本现在与 `macvlan` 一起提供 `ipvlan` CNI binary，从而支持第二网络接口场景，例如在 underlay BGP fabric 上进行 VIP 出站流量。
- **Gateway** 和 **Ingress** 可观测性 — 新的监控面板覆盖 Ingress Controller 和 Gateway，MetalLB 监控面板增加了 BGP 会话状态和 IP 地址池利用率。`ingress-nginx` 增加了 OpenTelemetry 支持以及对其指标端点的认证访问。
- 可视化 **IP** 池管理 — 可从 web 控制台创建和管理 IP 池，以便在多 VLAN 集群中进行细粒度 IP 管理。

存储

- 统一的存储组件管理 — Alauda storage operator 成为存储组件的统一入口点，负责管理内置 Ceph、TopoLVM、本地存储和外部 Ceph 的安装、升级、状态和依赖关系。
- **Ceph** 传输中和静态加密 — Ceph 支持传输中加密和由 KMS 支持的静态加密。有关详情，请参见 [In-Transit Encryption](#) 和 [Persistent Volume Encryption](#)。
- **Ceph** 多网卡网络 — Ceph 容器网络支持多个网络接口，将客户端流量与复制流量分离。
- 对象存储可用性 — 可查看、监控和告警 CephObjectStoreUser 的配额使用情况。Bucket claim Secret 暴露标准的 `accessKey` / `secretKey` 字段，AWS SDK 和常用工具可直接消费这些字段，并且控制台会显示与每个 bucket claim 关联的 Secret。

虚拟化

- **CPU** 和内存热插拔 — 无需关闭虚拟机即可为运行中的虚拟机添加 CPU 和内存。有关操作步骤和 guest OS 支持详情，请参见 [CPU and Memory Hotplug](#)。
- 物理 **GPU** 直通 — 将物理 GPU 直接挂载到虚拟机，以支持 GPU 加速工作负载。
- 虚拟机迁移 (**V2V**) — 集成 forklift 插件，将传统虚拟化平台上的虚拟机迁移到 ACP。

Global Cluster 灾难恢复增强

Global Cluster Disaster Recovery 仍然支持传统操作系统部署和基于 Alauda OS 的 Immutable Infrastructure 部署。在 4.4 中，同步路径更具弹性，并覆盖了更多 `global` 集群生命周期。此能力保护 `global` 控制平面；它不保护应用数据。

现在，备用集群会保留活动集群的更新顺序，包括当恢复耗时足以让活动 etcd 压缩其历史记录时。DR 配置可以在平台组件发生变化时自适应，而无需替换 DR 服务。备用集群还会接收 `global` 集群升级状态和 workload cluster 生命周期信息，因此具备更安全接管所需的信息。

在 DR 切换之前，或者在支持 DR 的 `global` 集群升级移除 synchronizer 之前，请继续验证活动集群和备用集群保持一致。这可以防止过期的备用数据导致错误的恢复操作。

有关详情，请参见 [Global Cluster Disaster Recovery](#) 和 [Immutable Infrastructure 上的 Global Cluster Disaster Recovery](#) ↗。

Alauda OS 备份和恢复

使用 Alauda OS 的集群现在可以使用 **Cluster Enhancer** 进行 etcd 备份和恢复。您可以运行定时或按需备份，将其保留在控制平面节点上，并可选择在 S3 兼容对象存储中保留额外副本。这可以保护集群配置数据；etcd 恢复会覆盖现有的 etcd 数据，且必须按照文档化的恢复操作步骤执行。

有关配置和恢复步骤，请参见 [etcd Backup and Restore](#)。

访问和授权

- **Violet API** 令牌发布 — `violet` 是用于打包和发布插件的 CLI，现在在向平台发布软件包时接受平台 API 令牌。管理员和自动化流程可以无需交互式登录即可发布。可从 灵雀云 Customer Portal 下载 `violet`。有关详情，请参见 [Upload Packages](#)。
- 平台内 **CLI** 下载 — 用户可从 web 控制台下载适用于 Linux (`amd64` 和 `arm64`)、macOS (`amd64` 和 `arm64`) 以及 Windows (`amd64`) 的 ACP CLI 软件包。
- 更安全的角色委派 — 平台会阻止用户授予超过其自身授权边界的权限。控制台还包含相关的 ClusterRole 能力。

Immutable Infrastructure

ACP 4.4 继续扩展针对 Alauda OS 的文档化 Immutable Infrastructure 路径，该操作系统是所文档化的提供商场景中不可变节点的受支持操作系统。以下能力在其受支持的提供商场景中可用：

- **Bare Metal** 集群生命周期 — 在受支持的 Bare Metal 环境中创建和管理 `global` 集群和 workload 集群。`global` 集群路径包含 Global Cluster Disaster Recovery。
- 控制平面和存储韧性 — 通过提供商放置规则或在没有负载均衡器时自建控制平面 VIP 提升控制平面可用性，并在滚动升级期间节点被替换时保留已声明的本地磁盘。
- **Huawei DCS** 上的 **Alauda OS** 节点存储 — Huawei DCS Provider `v1.0.16` 或更高版本支持专用的 `/var/lib/kubelet` 和 `/var/lib/containerd` 磁盘。当磁盘被声明为持久化时，提供商会在滚动节点替换期间将其卸载并重新挂载，从而降低系统盘上的 Btrfs I/O 压力并保护已声明的节点本地数据。
- 网络和主机配置 — 在受支持的情况下，可为节点流量隔离配置多个网络接口。在 Huawei Cloud Stack 上，节点可以同时保留其短主机名和 FQDN。
- **Alauda OS** 的 **Huawei DCS Provider** 兼容性 — 对于使用 ACP `v4.3.2` 或更高版本的 Alauda OS 镜像的 Huawei DCS 集群，包括 ACP `v4.4.0` 及更高版本，请安装 Huawei DCS Provider `v1.0.21` 或更高版本。请从同一 ACP 版本的 OS Support Matrix 行中选择

Alauda OS 镜像。不要将 DCS Provider `v1.0.21` 或更高版本与早于 `v4.3.2` 的 ACP 版本对应的 Alauda OS 镜像搭配使用。请参见 [Huawei DCS 的 Alauda OS 和 Provider 兼容性](#)。

- 更安全的 **Huawei DCS** 虚拟机操作 — 在删除虚拟机节点之前先停止虚拟机，并在启动后移除启动 CD-ROM 挂载，以免其阻止后续虚拟机迁移。

有关您的提供商和确切受支持版本，请参见 [About Immutable Infrastructure](#) 及其提供商 release notes。

即将发布的 **Immutable Infrastructure** 提供商版本

以下更新计划在 ACP 4.4 交付周期中的独立版本提供商发布中推出。仅升级 ACP 到 4.4.0 不会安装它们；请在相应的提供商版本可用时使用匹配版本。提供商产品文档和 release notes 将发布详细的支持边界和操作步骤。

- **VMware vSphere** 固定地址节点生命周期 — VMware vSphere Provider 更新改进了 MachineConfigPool 健康状况和引导诊断、持久盘和临时盘处理，以及固定地址节点的滚动更新保护。管理员有意为了维护而关闭的虚拟机可以保持关闭状态。

弃用和移除

- 移除 **System ALB** — 4.4 中移除了平台级系统 ALB。
- 移除 **MinIO Operator** — 从 4.4 开始，平台不再随附 MinIO Operator。请使用 Ceph 对象存储作为 S3 兼容对象存储。

已修复问题

- 修复 metis 组件 storage limit 配置太小，在超出限制后导致 metis 容器重启

已知问题

- 通过 YAML 创建应用时使用 defaultMode 字段导致应用创建失败。
操作路径：容器平台 → 应用管理 → 应用列表 → 通过 YAML 创建（Create from YAML），当提交的 YAML 文件中包含 defaultMode 字段（通常用于 ConfigMap/Secret 的卷挂载权限配置）时，应用创建会失败并返回校验错误。
解决方案：创建应用前手动移除 YAML 中所有 defaultMode 声明。

- 当 Helm Chart 中设置了 pre-delete post-delete hook。
执行删除模板应用，卸载 Chart 时，遇到某些原因导致 hook 执行失败，进而导致应用无法删除。需要排查原因，并优先解决 hook 执行失败的问题。

相关产品站点

以下产品站点提供组件相关文档、兼容性信息、升级指导，以及已发布的 release notes。它们的版本和发布计划独立于 ACP 4.4，因此产品文档和 release notes 可能在 ACP 4.4 平台发布之后发布。

- [Alauda Service Mesh v2 ↗](#)
- [Alauda Build of OpenTelemetry v2 ↗](#)
- [Alauda Distributed Tracing ↗](#)
- [Alauda AI ↗](#)
- [Alauda Hyperflux ↗](#)
- [Alauda Build of HAMI ↗](#)
- [Alauda NVIDIA GPU ↗](#)
- [Alauda Ascend NPU ↗](#)
- [Alauda 用于 MySQL-PXC 的数据库服务 ↗](#)
- [Alauda 用于 MySQL-MGR 的数据库服务 ↗](#)
- [Alauda 用于 Redis OSS 的缓存服务 ↗](#)
- [Alauda 用于 Kafka 的流服务 ↗](#)
- [Alauda Build of Keycloak ↗](#)
- [Alauda 用于 RabbitMQ 的流服务 ↗](#)
- [Alauda 对 PostgreSQL 的支持 ↗](#)
- [Alauda 对 CloudNativePG 的支持 ↗](#)
- [Alauda Cost Management ↗](#)
- [Alauda DevOps ↗](#)
- [Alauda 容器安全 ↗](#)
- [Immutable Infrastructure ↗](#)

- [合规服务](#) ↗
- [Alauda Container Platform GitOps](#) ↗
- [托管控制平面](#) ↗
- [日志服务](#) ↗
- [集群认证](#) ↗



术语表

使用此术语表来理解 灵雀云容器平台 中的平台级术语。对于特定工作流的术语，请参阅相应的工作流或组件文档。

目录

平台和集群术语

Extension 和打包术语

身份、访问和安全术语

网络和访问术语

灾难恢复、备份和升级术语

术语约定

平台和集群术语

术语	定义	相关文档
ACP Core	首先安装的平台管理基础。它会部署 <code>global</code> 集群，并提供 web 控制台访问、平台 API、用户和 RBAC、集群管理、项目治理以及 Extension 管理框架等核心管理平面能力。	Core and Extensions

术语	定义	相关文档
<code>global cluster</code>	由 ACP Core 部署的中心管理集群。它承载平台管理服务，并协调集群、项目、用户、Extension 和平台操作。	Platform Model
业务集群	在 <code>global</code> 集群治理下运行应用工作负载的 Kubernetes 集群。根据所选模型，ACP 可以创建并进行生命周期管理。	Platform Model
第三方集群	其 Kubernetes 发行版和生命周期由 灵雀云 之外提供或管理的 Kubernetes 环境。ACP 可以在已文档化的前提条件和注意事项下纳管第三方集群，以实现集中治理和运维。	Cluster Management Models
Managed Cluster	当前用于管理已纳管第三方集群的界面/导航标签。它并不是与 <code>third-party cluster</code> 并列的概念模型。	Managed Clusters Overview
Installer-Provisioned Infrastructure (IPI)	一种基础设施责任模型，在该模型中，平台负责机器部署、通过 Immutable OS 管理节点操作系统，并管理受支持的 Kubernetes 生命周期。	Cluster Management Models
User-Provisioned Infrastructure (UPI)	一种基础设施责任模型，在该模型中，用户准备物理机或虚拟机并承担节点操作系统责任，而平台在这些节点上安装并管理 Kubernetes。	Cluster Management Models
Hosted Control Plane (HCP)	一种控制平面拓扑，其中每个托管集群都有自己的控制平面，多个托管控制平面作为工作负载运行在管理集群上。在 ACP 中，HCP 通过 Kamaji (<code>TenantControlPlane</code>) 实现。	About Hosted Control Plane
Immutable Infrastructure	一种部署和运行模型，其中节点配置被封装到镜像中，变更通过使用新镜像替换节点来应用。	About Immutable Infrastructure
Immutable OS	安装器部署节点使用的不可变操作系统。通过将操作系统层视为集中管理并通过基于镜像的更新替换，从而保持节点状态一致。	About Immutable Infrastructure
项目	面向租户、团队或业务系统的平台治理单元。一个项目可以跨越多个关联集群，并作为配额、策略、用户和命名空间所有权的边界。	Project Introduction

术语	定义	相关文档
Namespace	由平台直接或间接管理的 Kubernetes namespace。 在 ACP 中，namespace 可以归属于某个项目，并继承项目级治理。	Namespace Management
控制平面	运行 API server、scheduler、controller manager 和 etcd 等组件的 Kubernetes 管理层。	Architecture
控制平面节点	在专用控制平面拓扑中运行集群 Kubernetes 控制平面组件的节点。	Node Management
工作节点	运行应用工作负载和集群本地支撑组件的节点。	Node Management

Extension 和打包术语

术语	定义	相关文档
Extension	用于为 ACP 环境添加能力的总称，涵盖基于 Operator 和 Cluster Plugin 的机制。	Core and Extensions
Operator	基于 Kubernetes 自定义资源和 controller 构建的 Extension 机制。在 ACP 中，Operator 通过 Operator Lifecycle Manager 和 OperatorHub 进行管理。	Operator
Operator Lifecycle Manager (OLM)	处理 Operator 安装、升级、依赖解析以及相关资源（例如 <code>CatalogSource</code> 、 <code>Subscription</code> 、 <code>InstallPlan</code> 和 <code>ClusterServiceVersion</code> ）的 operator 管理框架。	Operator
OperatorHub	通过 OLM 发现、安装、升级和管理 Operator 的平台界面。	Operator
Cluster Plugin	平台的 Extension 机制，用于管理基于 chart 的插件，通过 <code>ModulePlugin</code> 、 <code>ModuleConfig</code> 和 <code>ModuleInfo</code> 自定义资源实现。	Cluster Plugin

术语	定义	相关文档
Core lifecycle	遵循 ACP Core 发布节奏和集群 Distribution Version 的 Extension 生命周期类型。不支持独立升级。	Core and Extensions
Aligned lifecycle	遵循 ACP 发布流的 Extension 生命周期类型，但在发布兼容版本后可以独立升级。	Core and Extensions
Agnostic lifecycle	独立于 ACP 发布，并在发布兼容版本后可独立升级的 Extension 生命周期类型。	Core and Extensions
Customer Portal compatible versions	灵雀云 Customer Portal 中的兼容性字段，用于指示某个特定 Operator 或 Cluster Plugin 版本支持哪些 ACP 版本。	Core and Extensions

身份、访问和安全术语

术语	定义	相关文档
Identity Provider (IdP)	用于平台账号身份验证的外部身份系统，例如 LDAP 或 OIDC。	Identity Provider Introduction
LDAP	平台支持的目录访问协议，用于企业用户身份验证。Active Directory 可通过 LDAP 集成。	LDAP Management
OpenID Connect (OIDC)	基于 OAuth 2.0 的身份层，平台支持将其用于第三方用户身份验证。	OIDC Management
平台角色	RBAC 重构后由平台提供的角色模板。它们会绑定到用户或组，并转换为 Kubernetes 权限。	Roles Introduction
Kubernetes 角色	用于细粒度权限控制的原生 Kubernetes Role 和 ClusterRole 对象。它们通过 RoleBinding 或 ClusterRoleBinding 绑定。	Roles Introduction
审计	用于记录用户和系统操作的平台操作记录。审计视图依赖日志服务组件。	Audit Introduction

术语	定义	相关文档
NetworkPolicy	用于 namespace 级别网络流量策略的 Kubernetes 资源。其强制执行取决于所选 CNI。	NetworkPolicy
API Refiner	可基于用户权限、项目、集群和 namespace 过滤或屏蔽 Kubernetes API 响应的 API 过滤能力。	API Security
合规功能	基于 Kyverno 的策略强制执行、违规监控和报告功能。请使用 Compliance Service 文档了解适用范围和前提条件。	Compliance Service

网络和访问术语

术语	定义	相关文档
平台访问地址	用于访问 web 控制台和平台 API 等平台服务的外部地址。它可以与 Cluster Endpoint 相同，也可以在外部访问场景中使用单独的地址。	Installing
集群端点	集群组件和管理员用于访问目标 Kubernetes 控制平面端点的地址。	Installing
负载均衡器	通过外部负载均衡器暴露 Service 的 Kubernetes Service 类型。在平台中，负载均衡也可能涉及外部设备、VIP 或提供商特定服务。	Configure Services
自建 VIP	当 Cluster Endpoint 未提供外部负载均衡器时使用的内置虚拟 IP 选项。	Prerequisites
Cluster Proxy	用于连接 <code>global</code> 集群与受管集群，以支持管理操作的平台通信能力。	Architecture
导入集群	<code>global</code> 集群使用提供的地址、CA 和凭据连接到目标第三方集群 API server 的纳管方式。	Import Clusters
注册集群	目标第三方集群中的反向代理服务发起注册并与平台建立隧道的一种纳管方式。	Register Cluster

灾难恢复、备份和升级术语

术语	定义	相关文档
Global Cluster Disaster Recovery	基于 <code>global</code> 集群 etcd 同步和 DNS/VIP 故障切换的 Primary 和 Standby <code>global</code> 集群 DR 机制。它仅在已文档化边界内保护 <code>global</code> 控制平面场景。	Availability and Recovery
etcd backup and restore	用于备份和恢复存储在 etcd 中的 Kubernetes 控制平面资源状态的路径。	etcd Backup and Restore
应用备份和恢复	基于 Velero 的应用资源和持久卷备份与恢复路径，通过 Data Backup 组件交付。	Backup Overview
Cluster Version Operator (CVO)	用于协调 <code>global</code> 和业务集群升级的目标版本、前置检查、状态和执行进度的升级工作流程和 controller。	Upgrade Overview
ClusterVersionShadow	CVO 升级工作流程使用的自定义资源，用于暴露期望版本、状态、前置检查结果、阶段和升级历史。	Upgrade Overview
Distribution Version	用于协调 <code>global</code> 和业务集群升级中的升级准入控制和版本对齐的集群发行版版本。	Upgrade Overview
Preflight	在执行升级之前运行的一组检查，用于降低升级风险。	Pre-Upgrade

术语约定

- `global` 集群是平台管理集群。
- `third-party cluster` 指外部提供的 Kubernetes 环境。`Managed Cluster` 是当前 UI 或导航标签。
- UI 标签、API 资源名称、协议名称和功能名称保留其官方大小写。
- 当所在页面需要展开缩写时，缩写会在首次出现时展开。



了解更多

根据安装、集群运维、原生应用交付、升级规划、可用性与恢复、安全、API 或 CLI 工作，选择下一步任务路径。

目录

了解平台

- 安装与规划
- 管理集群
- 构建和运维原生应用
- 安装和使用扩展
- 规划版本和升级
- 规划可用性、备份和恢复
- 安全和集成

了解平台

目标	从这里开始
了解 ACP 是什么，以及它与 Kubernetes 的关系。	简介
了解 hub-and-spoke 架构。	架构

目标	从这里开始
了解 <code>global</code> 集群、业务集群、第三方集群、HCP、项目和命名空间。	平台模型
了解三轴集群模型和责任边界。	集群管理模型
查找平台范围内的术语。	词汇表

安装与规划

目标	从这里开始
了解 ACP Core 安装部署的内容。	安装概览
选择 Multi-Cluster、Single Cluster 或 Single Node。	规划
准备资源、网络、OS 和负载均衡前提条件。	前提条件
下载 Core Package 并选择包架构。	下载
安装 ACP Core。	安装
验证已完成的安装。	验证
决定是否规划 Global Cluster Disaster Recovery。	Global Cluster Disaster Recovery

管理集群

目标	从这里开始
创建由 ACP 生命周期管理的业务集群。	集群概览
创建本地业务集群。	创建本地集群
使用 Immutable Infrastructure。	关于 Immutable Infrastructure

目标	从这里开始
评估 Hosted Control Plane (HCP)。	关于 Hosted Control Plane
通过导入接入现有的第三方 Kubernetes 环境。	导入第三方集群
通过注册接入现有的第三方 Kubernetes 环境。	注册集群
使用 KubeConfig 访问集群。	使用 KubeConfig 访问集群

构建和运维原生应用

目标	从这里开始
了解开发人员工作流。	开发人员概览
基于镜像、Chart、YAML、源代码或由 Operator 支持的 catalog 创建原生应用。	创建原生应用
管理 Kubernetes 工作负载。	原生应用工作负载
管理命名空间。	命名空间管理
查看原生应用日志、事件和监控仪表盘。	原生应用可观测性
使用容器镜像和 registry。	镜像 和 Registry

安装和使用扩展

目标	从这里开始
了解 Core 和 Extension 的边界。	Core 和 Extensions

目标	从这里开始
了解 Extension 系统。	扩展概览
安装和管理 Operator。	Operator
安装和管理集群插件。	集群插件
上架软件包。	上架软件包
检查特定 Extension 的版本兼容性。	使用 灵雀云 Customer Portal 中的 ACP compatible versions 字段，然后阅读 Extension 文档。

规划版本和升级

目标	从这里开始
阅读 Kubernetes 版本支持和第三方接入范围。	Kubernetes 支持矩阵
了解版本、生命周期、运行时、OS 和架构边界。	版本和生命周期
阅读 release changes。	Release Notes
规划集群升级。	升级概览
在升级 global 集群之前进行准备。	升级前
升级业务集群。	升级业务集群

规划可用性、备份和恢复

目标	从这里开始
了解拓扑、HA、Global DR 和恢复边界。	可用性和恢复
规划 global 集群容量。	评估 Global Cluster 资源

目标	从这里开始
规划业务集群控制平面容量。	评估业务集群资源
规划和运维 Global Cluster Disaster Recovery。	Global Cluster Disaster Recovery
备份和恢复 etcd、registry、监控、日志或原生应用。	备份概览

安全和集成

目标	从这里开始
使用 LDAP 或 OIDC 配置 Identity Provider。	Identity Provider 简介
管理用户、角色和 Kubernetes RBAC。	角色简介
管理用于租户隔离的项目和命名空间。	项目简介
查看审计记录。	审计简介
配置 NetworkPolicy。	NetworkPolicy
使用 API Refiner 进行 API 响应过滤。	API 安全
使用合规功能。	合规服务
使用容器安全能力。	Alauda 容器安全
使用平台 API。	API 简介
使用 CLI 工具。	CLI 工具