普华云操作系统

用户手册

普华基础软件股份有限公司
商务电话：010-8406 5566　商务传真：010-8248 4849
邮编：100102　地址：北京市朝阳区容达路7号院太极信息产业园5号楼（E座）3层

致辞

欢迎您成为普华产品的使用者。若本手册为您在使用本产品过程中提供了预期的帮助，我们深感欣慰。若您在使用本产品过程中，遇到问题或对产品有任何意见或建议，请与本公司联系。对您在使用过程中遇到的问题，我们会全力解决，对您提出的建议，我们表示衷心的感谢！

版权声明

目 录

第 1 章 引言

1.1 文档概述

本手册为普华云操作系统用户手册。（以下用普华云管代替）

本手册将详细描述普华云操作系统的安装部署流程和使用方法。

1.2 读者对象

本手册的读者对象是普华云操作系统管理员用户。我们假定读者已经对个人计算机与容器的基本配置较为了解。

- 熟悉 Linux 基础命令；
- 了解 SSH 使用方法，了解公钥/私钥工作原理；
- 熟悉 Docker 基本使用方法及基础命令，比如：容器日志查看；
- 了解 SSL 证书使用方法；
- 了解负载均衡工作原理(L7)；
- 了解域名解析原理；
- 了解 K8S 基本概念

第 2 章 产品简介

普华云管平台是一款企业级全栈化容器部署及管理平台，通过使用普华云管理平台，企业无需使用一系列的开源软件从头搭建容器服务平台，平台提供了 Docker 和 Kubernetes 的容器部署与管理功能。平台不仅提供简单易用的 WEB 图形，内置资源丰富的应用商店，降低容器部署与管理的复杂度与难度，还集成功能强大的 Kubernetes 容器编排引擎以及负载均衡器，强化对容器管理的功能，极大的提升了管理容器的灵活性，提高了服务的可用性，把容器管理技术推上了一个新的高度。

2.1 产品简介

普华云管平台具有完备的集群能力，包括多层次的安全防护和准入机制、多租户应用支撑能力、透明的服务注册和服务发现机制、内建智能负载均衡器，强大的故障发现和自我修复能力、服务滚动升级和在线扩容能力。

普华云管平台支持国产 CPU 架构平台，提供国产化容器平台应用的快速部署、弹性伸缩、应用市场等功能特性，可缩短业务上线周期，优化资源利用率，提高服务响应效率。

普华云管平台界面简洁直观操作流畅，解决了业界遗留已久的 K8s 原生 UI 易用性不佳以及学习曲线陡峭的问题，集群管理功能可解决企业用户的生产环境中面临的基础设施不同的困境，同时还带来了一系列拓展功能。可以说普华云管平台为企业在生产环境中落地 Kubernetes、以及构建新一代的 Container as a Service 提供了更加便捷的途径。

2.2 系统架构

系统架构

管理节点 Master：安装在一台物理机上，裸机安装方式，管理整个集群。

计算节点 Note：安装在一台或多台物理机上，裸机安装方式，用于调度 Pod 节点数据分配。

普华云管平台硬件拓扑图如下：

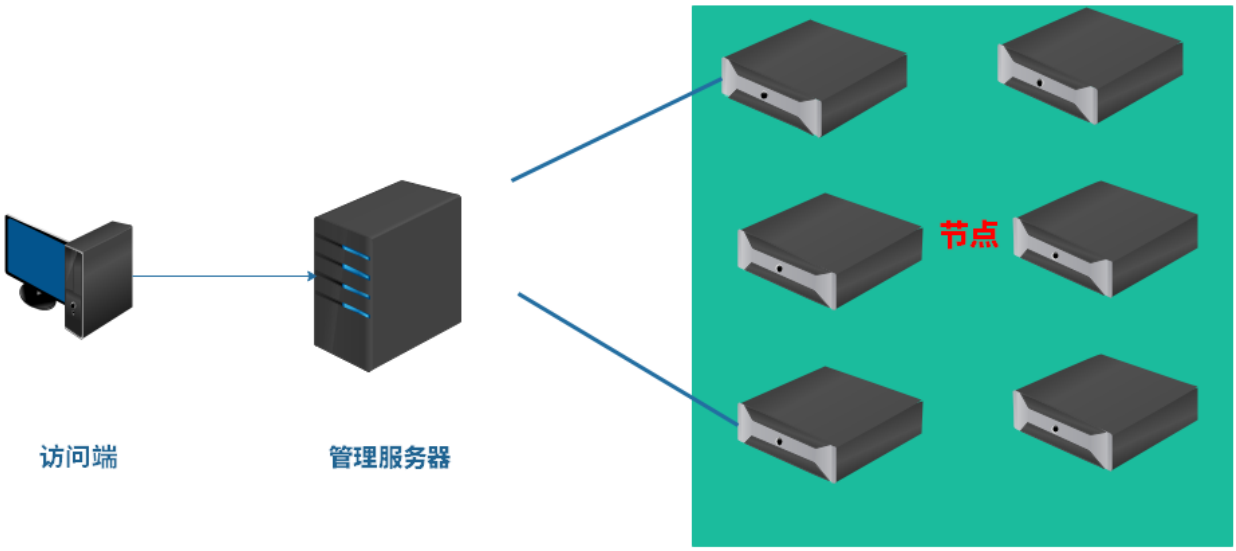


图 2-1 普华普华云管平台硬件拓扑图

第 3 章 系统安装

详见《普华云操作系统 V3.0--快速安装手册.pdf》

第4章 管理员设置

4.1 设置普华云管理平台 Server URL

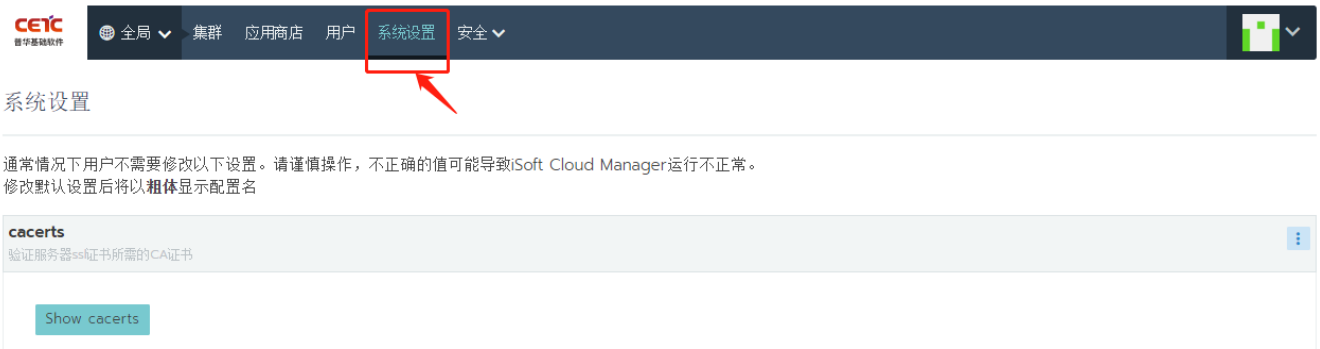
此 URL 地址可以是 IP 也可以是域名，集群所有节点将使用该 URL 来注册到普华云管平台，所以需要保证所有节点能访问该地址。

如果普华云管平台 server 是多节点 HA 运行，请不要设置普华云管平台 Server URL 为某一个节点的 IP 地址，避免因某一个节点出现故障影响整个集群。如果普华云管平台 Server URL 使用域名，请把域名解析到所有普华云管平台 Server 节点 IP 或者 VIP 上。

首次登录普华云管平台 Server 时，系统会提示你设置此 URL。如果登录时设置有误，需要在创建集群前修改，如果在创建好集群后修改普华云管平台 Server URL,之前注册的集群将会受到影响。

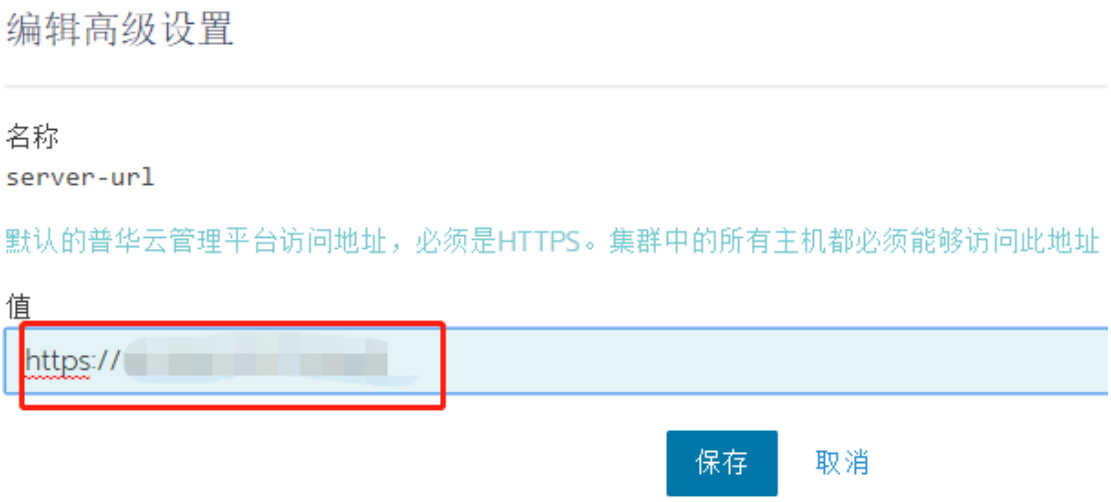
修改普华云平台 Server URL

1、 登录普华云管平台 UI 后点击 系统设置(全局视图下):



2、 页面往下翻找到 server-url,点击右侧菜单(三个点),点击编辑：

3、 设置 server-url 并保存：



4.2 配置 K8S 角色

在普华云管平台中，每个人都以用户身份进行身份验证，这是一个允许你访问普华云管平台的登录信息。用户可以是本地的也可以是外部的。

配置外部身份验证后，用户页面上显示的用户将改变：

- 如果用本地用户身份登录，则仅显示本地用户
- 如果用外部用户登录，则会显示外部用户和本地用户

用户和角色

用户登录普华云管平台后，其授权或系统内的访问权限由全局权限以及集群和项目角色决定。

- 全局权限:

在任何特定集群的范围之外定义用户授权。

- 集群和项目角色:

在为其分配角色的特定集群或项目中定义用户授权。

4.2.1 全局权限

全网定义用户权限授权范围并在任何特定的集群内。初始化便可生效,有两个默认全局权限:管理员和用户。

- 管理员:这些用户有完全控制整个系统和所有集群。
- 用　户:这些用户可以创建新集群和使用它们。标准用户还可以将其他用户的权限分配给他们的集群。

注意：不能创建、更新或删除全局权限。

全局权限分配

将全局权限分配给用户取决于它们的身份验证源：外部或本地。

- 外部认证:当用户第一次使用外部身份验证提供者登录普华云管平台时，将自动为它们分配标准用户全局权限。
- 本地认证:当创建新的本地用户时，在完成添加用户时，为它们分配全局权限。

自定义全局许可

- 您可以为用户分配一组自定义权限，而不是为用户分配管理员或标准用户的默认全局权限。

  注意：权限是在为用户选择自定义权限时可以分配的个人访问权限。

- 使用自定义权限便于为用户提供对普华云管平台专门访问。请参阅下表，获取可用的个人权限列表。

参考表

下表列出了每个可用的自定义全局权限，以及它是否被分配给默认全局权限、管理员和标准用户。

Custom Global Permission	Administrator	Standard User
Manage Authentication	✓	
Manage Catalogs	✓	
Manage Node Drivers	✓	
Manage PodSecurityPolicy Templates	✓	
Manage Roles	✓	
Manage Users	✓	
Create Clusters	✓	✓
User Catalog Templates	✓	✓
Login Access	✓	✓

注意：上面列出的每个权限由在普华云管平台 UI 中没有列出的多个单独权限组成。对于这些权限和它们包含的规则的完整列表，通过 API 在/V3/全局角色中进行访问。

新用户的默认全局权限

- 当来自外部身份验证源的用户第一次登录普华云管平台时，将自动为它们分配一组全局权限（以下称为权限）。默认情况下，新用户被分配了用户权限。然而，在某些组织中，这些权限可能会延长过多的访问权限。在该用例中，可以将默认权限更改为更严格的限制，例如一组单独权限。

- 您可以指定一个或多个默认权限。例如，用户权限为新用户分配一组单独的全局权限。如果希望限制新用户的默认权限，可以将用户权限作为默认角色删除，然后将多个单独的权限作为默认角色分配。相反，您还可以在其他标准权限集的顶部添加管理权限。

注意：默认角色只分配给外部用户。对于本地用户，必须显式指定全局权限。

配置默认全局权限

您可以在第一次登录时更改分配给外部用户的默认全局权限。

1. 从全局视图中，从主菜单中选择**安全 >角色**。确保全局选项卡被选中。

2. 查找要用作默认值的权限集。然后通过选择省略号>编辑来编辑权限

3. 选择“是”新用户的默认角色，然后单击“保存”。

4. 如果要删除默认权限，请编辑权限并从新用户默认选择“否”。

结果：默认的全局权限是根据您的更改配置的。分配给新用户的权限显示新用户默认列中的检查。

4.2.2 集群和项目权限

群集和项目角色定义群集或项目内的用户授权。可以从全局>安全>角色页管理这些角色

成员资格和角色分配

非管理员用户可访问的项目和集群是由成员资格决定的。成员资格是根据特定集群或项目中分配的角色访问特定集群或项目的用户列表。每个群集和项目包括一个具有适当权限的用户可以用来管理成员资格的选项卡。

当您创建群集或项目时，普华云管平台会自动指定您作为它的所有者。分配所有者角色的用户可以在集群或项目中分配其他用户角色。

注意：默认情况下，非管理用户无法访问任何现有的项目/集群。

集群角色

群集角色是可以分配给用户的角色，授予它们对群集的访问权限。有两个主要的集群角色：所有者和成员。

- 集群所有者：这些用户拥有对集群及其所有资源的完全控制权。
- 集群成员：这些用户可以查看大多数群集级资源并创建新项目。

自定义群集角色

普华云管平台允许您将自定义群集角色分配给用户，而不是典型的所有者或成员角色。这些角色既可以是内置自定义集群角色，也可以是管理员定义的角色。它们便于为集群内的用户定义专门的访问。请参阅下表，了解内置自定义群集角色的列表。

集群角色参考

下表列出了普华云管中可用的每个内置自定义集群角色，以及它是否也由所有者或成员角色授予。

Custom Cluster Role	Owner	Member
Manage Cluster Members	✓	
Manage Nodes	✓	
Manage Storage	✓	
View All Projects	✓	
Create Project	✓	✓
View Cluster Members	✓	✓
View Nodes	✓	✓

注意：上面列出的每个集群角色，包括所有者和成员，都包括授予各种资源访问的多个规则。您可以在全局>安全>角色页面上查看角色及其规则。

项目角色

项目角色是可用于授予用户对项目的访问的角色。有三个主要项目角色：所有者、成员和只读。

- 项目所有者：这些用户对项目及其所有资源都有完全的控制权。
- 项目成员：这些用户可以管理项目范围内的资源，如命名空间和工作负载，但不能管理其他项目成员。
- 只读：这些用户可以查看项目中的所有内容，但不能创建、更新或删除任何内容。

自定义项目角色

普华云管平台允许您将自定义项目角色分配给用户，而不是典型的所有者、成员或只读角色。这些角色既可以是内置的自定义项目角色，也可以是管理员定义的角色。它们便于在项目内为用户定义专门的访问。请参阅下表，了解内置自定义项目角色的列表。

项目角色参考

下表列出普华云管平台中可用的每个内置自定义项目角色，以及它是否也由所有者、成员或只读角色授予。

Custom Cluster Role	Owner	Member	Read Only
Manage Project Members	✓		
Create Namespaces	✓	✓	
Manage Config Maps	✓	✓	
Manage Ingress	✓	✓	
Manage Secrets	✓	✓	
Manage Service Accounts	✓	✓	
Manage Services	✓	✓	
Manage Volumes	✓	✓	
Manage Workloads	✓	✓	
View Config Maps	✓	✓	✓

Custom Cluster Role	Owner	Member	Read Only
View Ingress	✓	✓	✓
View Project Members	✓	✓	✓
View Secrets	✓	✓	✓
View Service Accounts	✓	✓	✓
View Services	✓	✓	✓
View Volumes	✓	✓	✓
View Workloads	✓	✓	✓

注意：上面列出的每个项目角色，包括所有者、成员和只读，都由允许访问各种资源的多个规则组成。您可以在全局>安全>角色页面上查看角色及其规则。

自定义角色定义

如上所述，自定义角色可以定义为在集群或项目级别使用。上下文字段定义角色是否将出现在群集成员页、项目成员页或两者上。

在定义自定义角色时，可以授予对特定资源的访问权，或者指定自定义角色应该继承的角色。自定义角色可以由特定授权和继承角色的组合组成。这意味着为特定资源定义授权不会覆盖原自定义角色从其继承的角色中定义的更宽的授权。

默认群集和项目角色

默认情况下，当用户创建新集群或项目时，会自动为它们分配所有权角色：集群所有者或项目所有者。然而，在一些组织中，这些角色可能会扩展权限访问。

在此用例中，可以将默认角色更改为更具限制性的角色，例如一组单独的角色或自定义角色。

更改默认群集/项目角色有方法：分配单个角色：将多个群集/项目角色配置为分配给创建用户的默认值。

例如，您可以选择单个角色的混合（比如管理节点和管理存储），而不是分配继承其他角色的角色（比如集群所有者）。

注意：尽管可以锁定默认角色，但系统仍然为创建群集/项目的用户分配角色。只有创建群集/项目的用户才能继承它们的角色。添加到群集/项目成员之后的用户必须明确地指派其角色。

4.2.3 自定义角色

在普华云管平台中，角色决定用户可以在集群或项目中做什么动作。

注意：角色与权限不同，这些权限决定了您可以访问哪些集群和项目。

先决条件：

若要完成此页上的任务，需要以下权限：

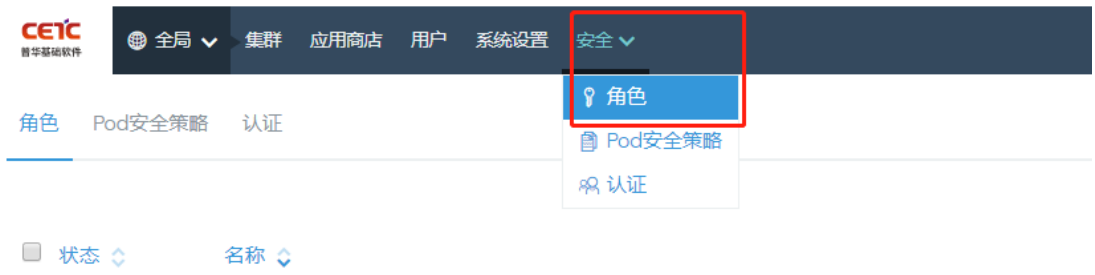
A. 管理员全局权限。

B. 自定义全局权限与分配的管理角色角色。

添加自定义角色

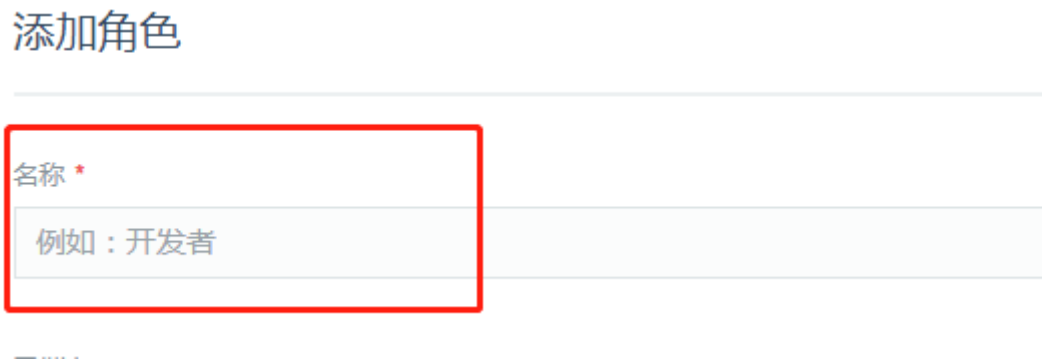
虽然普华云管平台提供了一组默认用户角色，但是您也可以创建默认自定义角色，以便为平台内的用户提供非常特定的权限。

1. 从全局视图中，从主菜单中选择 安全 > 角色

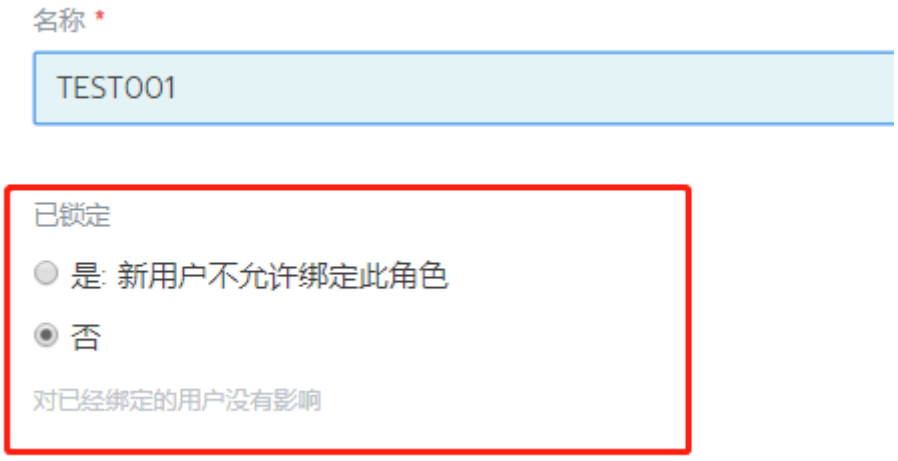


2. 点击添加角色

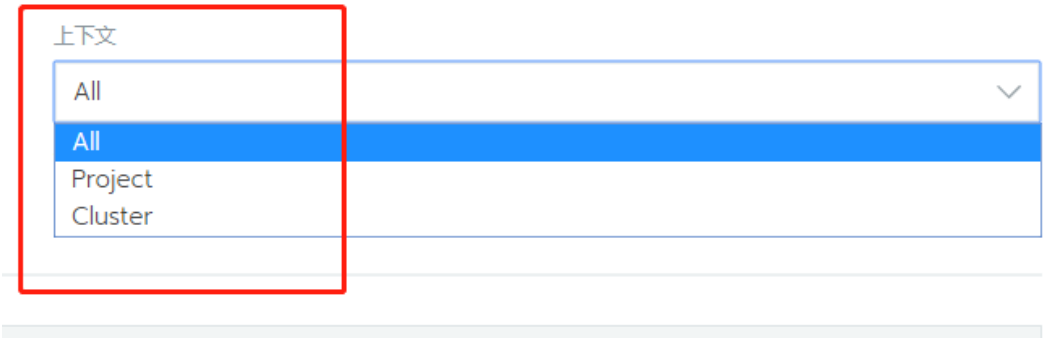
3. 命名角色



4. 选择是否将角色设置为已锁定状态。（无法将锁定的角色分配给用户）



5. 将角色分配为上下文。上下文决定了分配给用户的角色范围



全部

- 无论上下文如何，用户都可以使用指定的角色。当向群集或项目添加/管理成员时，此角色对于分配是有效的。

集群

- 此角色对于只向群集添加/管理成员时的分配是有效的。

项目

- 当只对项目添加或管理成员时，他的角色对于分配是有效的。

6. 使用授权资源选项将单个 Kubernetes API endpoints 分配给角色。您还可以选择单独的 URL 方法（创建、删除、获取等），供您指定的每个端点使用

7. 使用角色选项的继承来将单个平台角色分配给自定义角色

8. 单击“创建”

4.2.4 锁定/解锁角色

你可以将角色设置为 locked 状态,锁定角色可防止为其分配用户

锁定角色：

- 无法分配给尚未分配角色的用户。
- 将用户添加到集群或项目时，不会在成员角色下拉列表中列出。
- 在锁定角色之前，不要影响分配了该角色的用户。这些用户保留角色提供的访问权限。

角色可以被以下用户锁定：

- 分配了 Administrator 全局权限的用户。
- 分配了 Custom Users 权限的用户以及 Manage Roles 角色。

锁定/解锁角色

锁定角色可以在新建角色或者编辑已有角色来实现，解锁角色只能通过编辑已有的角色。

- 新建角色

- 编辑角色

4.3 Pod 安全策略

Pod 安全策略(或 PSP)是控制 Pod 规范中安全敏感方面的对象(如 root 权限)。如果 Pod 不符合 PSP 中指定的条件，Kubernetes 将不允许它启动，并且普华云管平台将显示错误消息 Pod <NAME> is forbidden: unable to validate...

可以在群集或项目级别分配 Pod 安全策略。

PSP 通过继承来工作:

- 默认情况下，分配给集群的 Pod 安全策略由其项目以及添加到这些项目中的所有命名空间继承。

例外：无论是否给群集或项目分配 Pod 安全策略，未分配给项目的命名空间不会继承 Pod 安全策略。由于这些命名空间没有分配 Pod 安全策略，因此在这些命名空间中部署工作负载将失败，这是默认的 Kubernetes 行为。

- 可以通过直接为项目分配不同的Pod安全策略来覆盖默认的Pod安全策略。

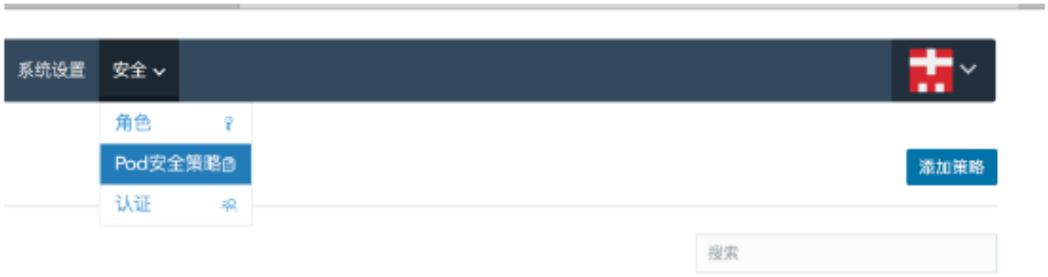
在分配 Pod 安全策略之前,已在群集或项目中运行的工作负载不会被检查,需要克隆或升级工作负载来检查它们是否满足 Pod 安全策略要求。

在 Kubernetes 文档中了解更多有关 Pod 安全策略的信息。

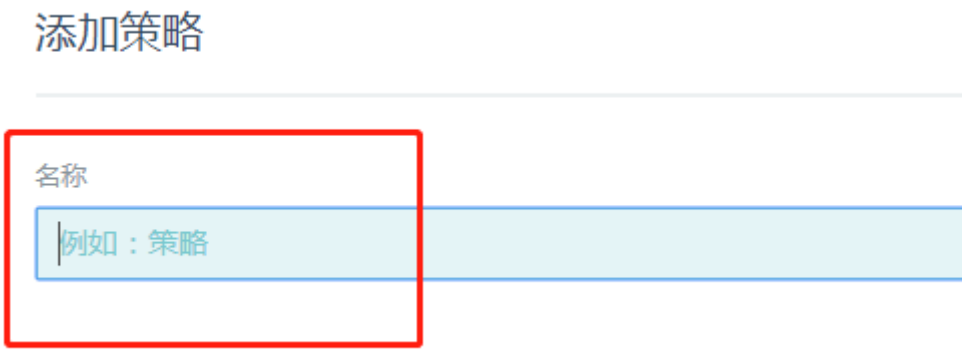
使用普华云管平台，您可以在 UI 创建 Pod 安全策略，而不需使用 YAML 文件来创建。

创建 Pod 安全策略

1.在全局视图中，从主菜单中选择安全>Pod 安全策略,然后单击添加策略。



2. 设置策略名称



3. 基本策略：根据实际需求设置策略功能，了解更多信息，请参阅 Kubernetes 文档。

提升特权

主机命名空间

只读跟根文件系统

内核安全策略

Volume Policy

Allowed Host Paths Policy

FS Group Policy

Host Ports Policy

Run As User Policy

SELinux Policy

Supplemental Groups Policy

4.4 登录认证

普华云管平台为 Kubernetes 增强的一个关键功能是集中用户身份验证，此功能允许你的用户使用一组凭据对所有 Kubernetes 集群进行身份验证。

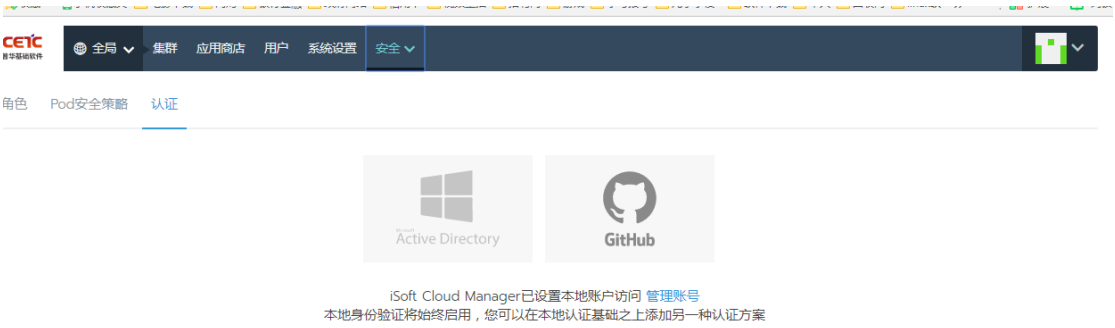
此集中式用户身份验证是使用普华云管平台身份验证代理完成的，该代理与平台一起安装。此代理会对你的用户进行身份验证，并使用服务帐户将其请求转发给你的 Kubernetes 集群。

外部认证与本地认证

普华云管平台提供本地身份验证，也可以同时与以下一个或者多个外部身份验证服务集成：

- Microsoft Active Directory
- GitHub

在大多数情况下，你应该使用外部身份验证服务，因为外部验证服务可以统一的进行用户管理。如果没有外部身份验证服务，你也可以通过本地身份验证来管理平台用户。



外部身份验证配置和主要用户

一个具有管理员角色的本地管理员账号，例如：local_admin

一个可以使用外部身份验证服务进行身份验证的外部服务账号，例如：demo

外部身份验证的配置会影响普华云管平台中本地用户的管理方式。请按照以下列表更好地了解这些效果

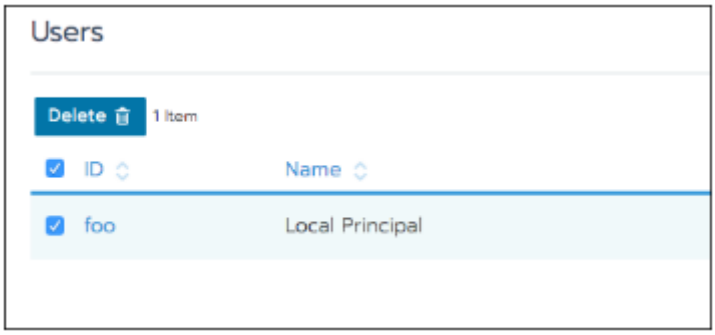
1. 以本地管理员登录普华云管平台，对外部身份验证服务进行完整配置。

2. 普华云管平台将外部服务账号与本地管理员账号联系在一起。这两个账号共享本地管理员用户的用户 ID。

3. 完成配置后，普华云管平台会自动注销本地管理员账号

4. 然后，普华云管平台将自动以外部服务用户登录。

5. 由于外部服务账号和本地管理员账号共享一个 ID，因此在用户页面上不会显示外部服务账号的唯一标识。



6. 外部服务账号和本地管理员账号共享相同的访问权限。

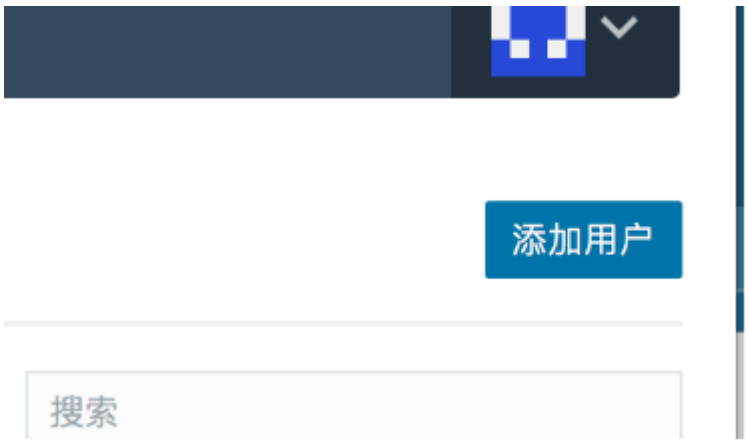
重要说明：不管启用哪种外部身份验证服务，普华云管平台内置的超级管理员 admin 将一直启用

4.4.1 配置本地认证

无论你是否使用外部身份验证，都应创建一些本地身份验证用户，以便在外部身份验证服务遇到问题时继续使用普华云平台。

1. 从全局视图中，从主菜单中选择用户。

2. 单击添加用户



3. 填写 用户名、密码、显示名称、权限选择

4. 权限说明：此处的用户权限是作用于平台层面，它控制用户拥有哪些普华云管平台 UI 上的功能权限。

5. 完成后点击创建

4.4.2 配置 GitHub

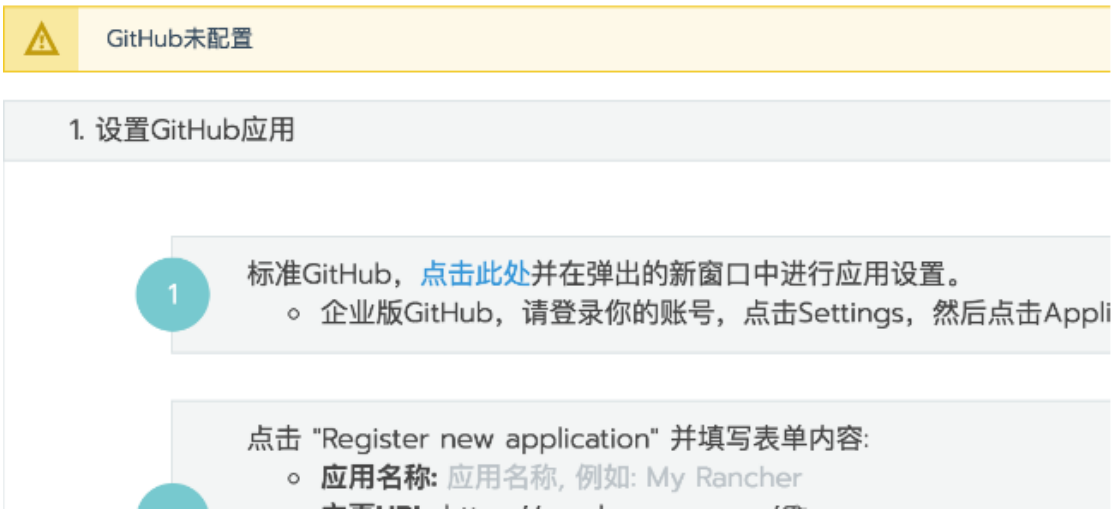
在使用 GitHub 的环境中，你可以配置普华云平台以允许使用 GitHub 凭据登录。

1. 使用具有管理员角色的本地用户登录普华云平台。

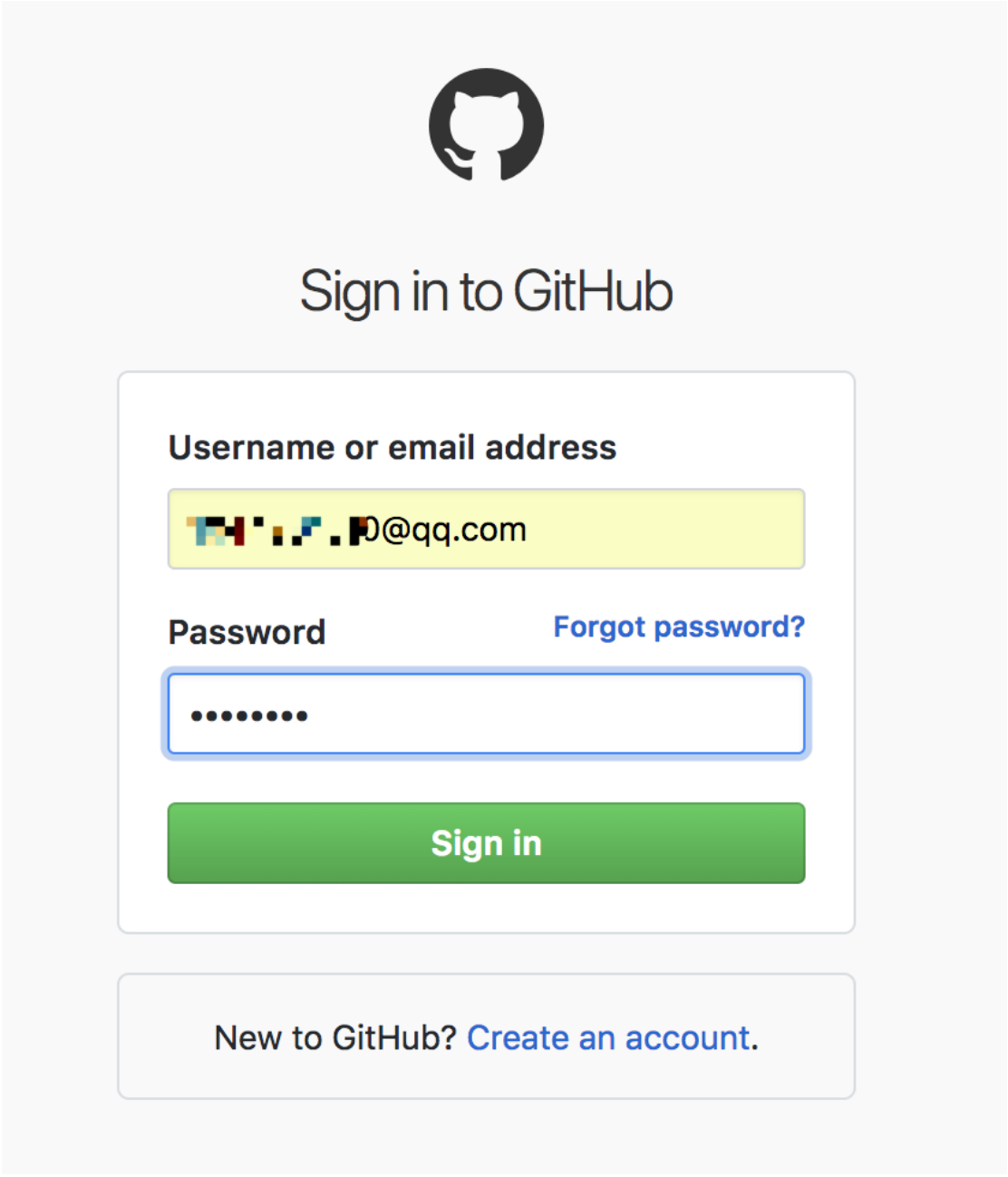
2. 在全局视图中，从主菜单中选择安全>认证。

3. 选择 GitHub。

4. 在 1.设置 Github 应用中，点击点击此处

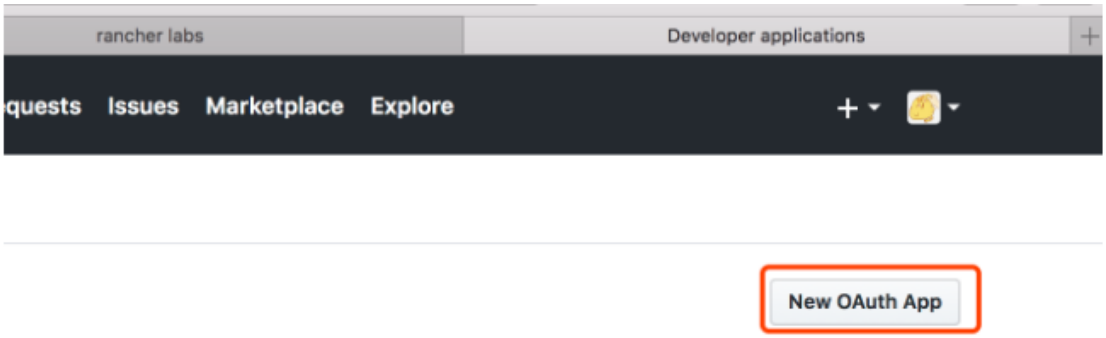


5. 弹出 Github 的登录页面，输入账号和密码进行登录



注：如果你使用的是本地部署的企业版 Github 服务器，请通过浏览器打开新的窗口直接访问 https://<github_server_url>/settings/developers

6. 登录 Github 后，点击 new OAuth app，并填写相关参数



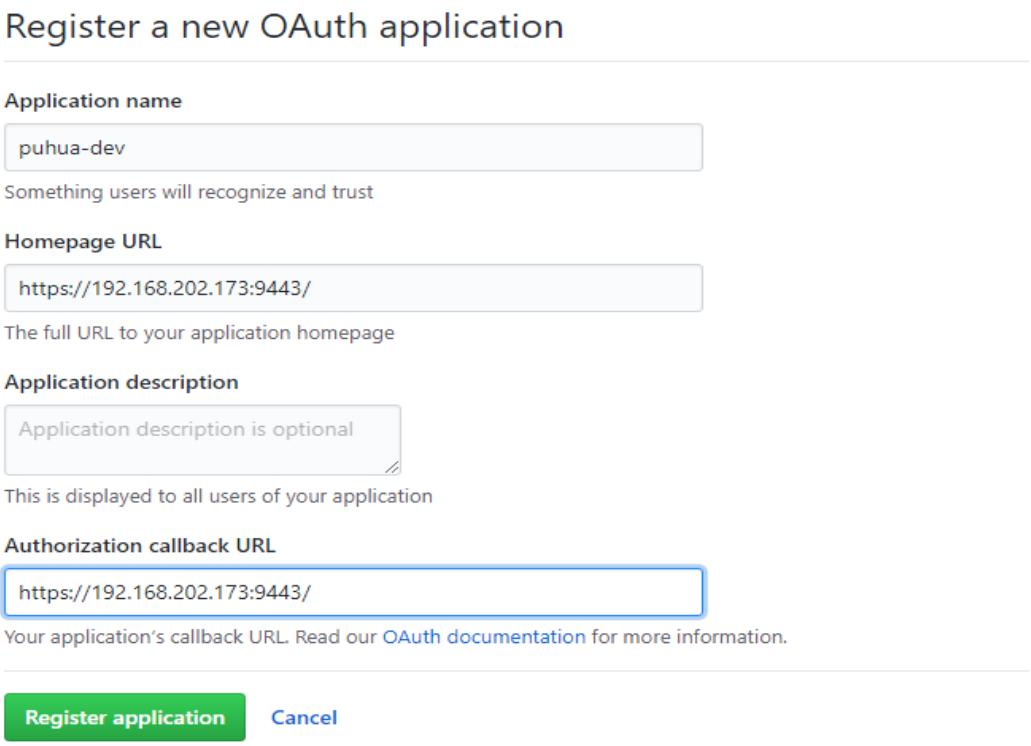
A. Application name：任意填写，比如：puhua-dev；

B. Homepage URL：主页 URL,查看普华云管平台 Github 配置页面;

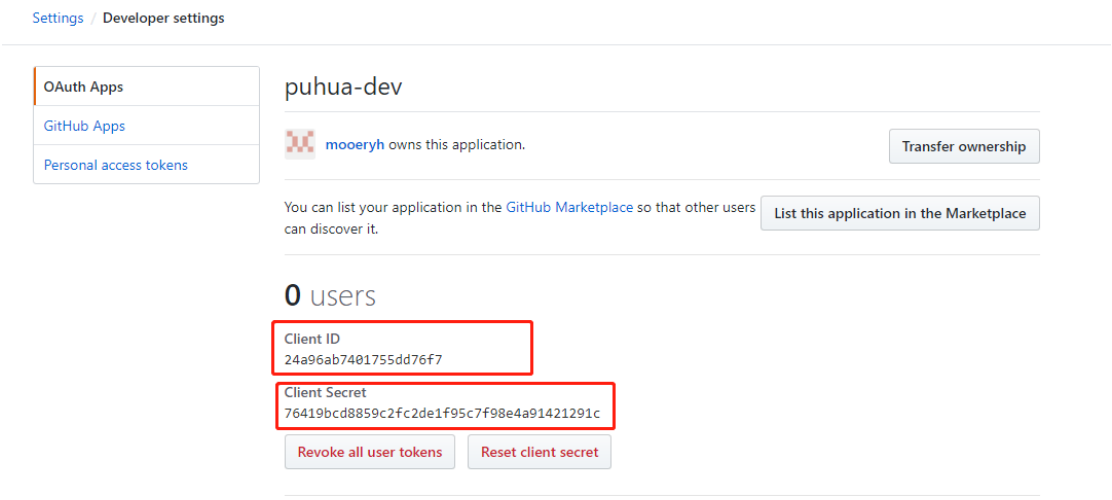
C. Application description：可选；

D. Application description：授权回调 URL,查看普华云管平台 Github 配置页面；

E. 最后点击 Register application;



7. 点击 Register application 后，自动创建应用。复制 Client ID 和 Client Secret

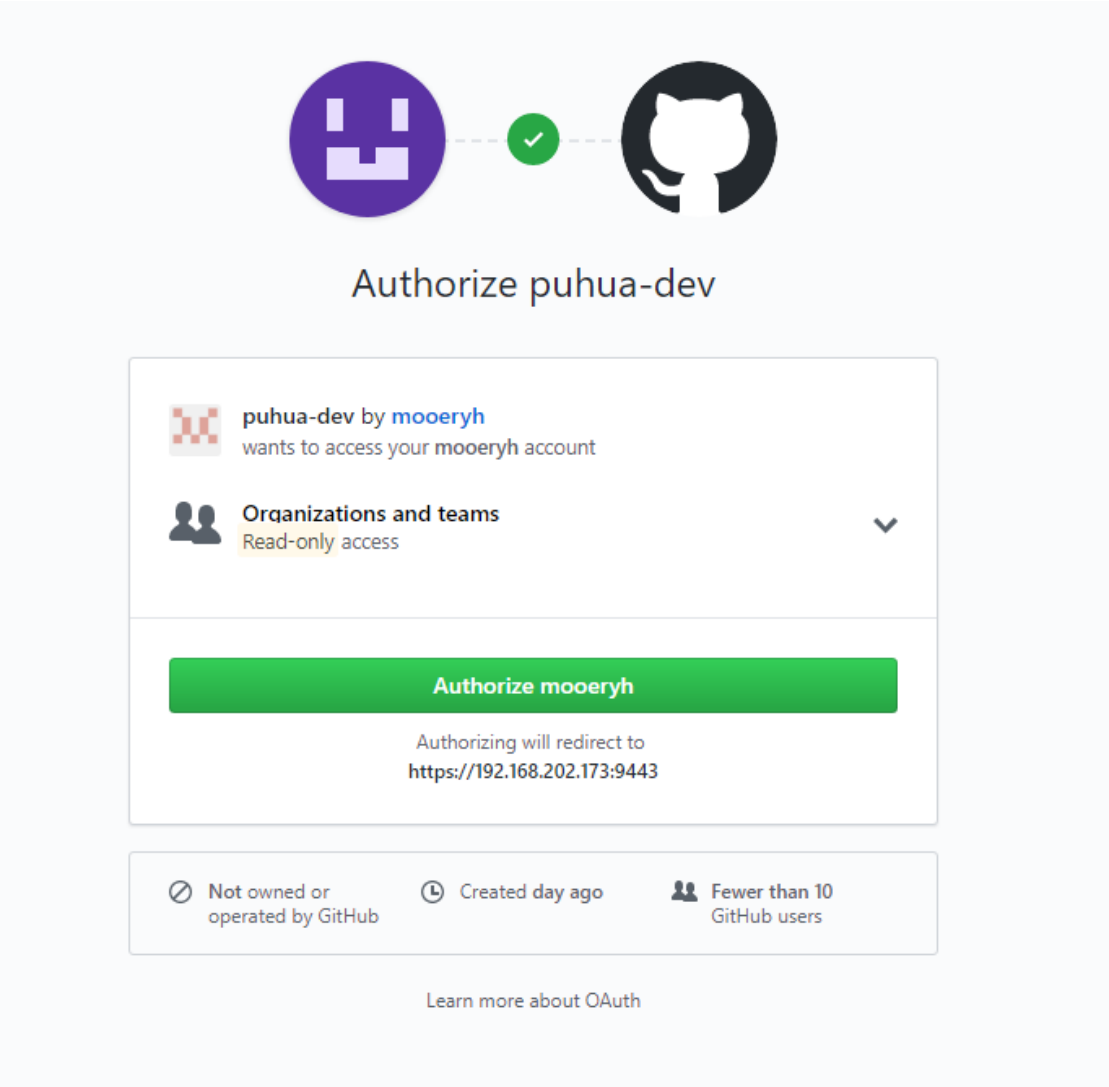


8. 在平台 Github 配置页面，输入复制的 Client ID 和 Client Secret

9. 如果是本地部署的私有 Github 企业版服务器，需要勾选使用私有 GitHub 企业版部署,根据实际情况是否勾选使用安全连接。

10. 单击启用 GitHub 进行身份验证

点击启用 GitHub 后会弹出新的窗口镜像认证授权，如果未弹出窗口请坚持浏览器安全设置是否阻止了弹窗。



11. 授权通过后会自动回到平台 Github 配置页面， 在站点访问选项中配置用户授权范围

A. 允许所有有效用户

所有的 GitHub 用户，以及本地用户，还有其他第三方认证用户都可以访问普华云平台此设置！

B. 允许集群、项目以及授权用户和组成员

配置为集群成员或项目成员的所有 GitHub 用户或组，以及本地用户都可以登录到普华云平台。此外，你添加到授权用户和组织列表的任何 GitHub 用户或组都可以登录到普华云平台。

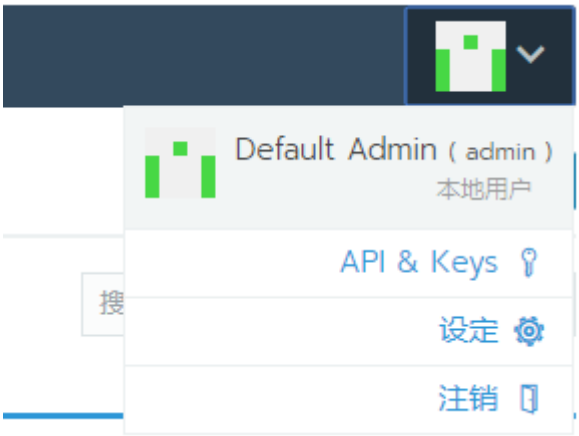
C. 仅限授权用户和组织的访问权限

只有添加到授权用户和组织的 GitHub 用户或组才能登录普华云平台。相对安全性更高，但是灵活性较低。

12. 点击保存

第五章　用户设置

在普华云平台中，每个用户都有许多与其登录相关的设置：个人首选项、API 密钥等。你可以通过从用户设置菜单中进行选择来配置这些设置。你可以通过单击主菜单中的头像来打开此菜单。



可用的用户设置为:

- API & Keys
- 如果要以编程方式与普华云管平台进行交互，则需要 API 密钥。按照本节中的说明获取密钥。
- 个人喜好
- 语言切换
- 切换项目/集群

5.1 API & Keys

如果要使用外部应用程序访问普华云管平台集群、项目或其他对象，可以使用普华云管平台 API 执行此操作。但是，在你的应用程序可以访问 API 之前，你必须为应用程序提供用于向普华云管平台进行身份验证的 API 密钥。你可以使用云平台 UI 获取密钥。

注意:使用普华云管平台 CLI 还需要API 密钥cli。

API 密钥由四个组件组成：

- Endpoint:

这是其他应用程序用于向普华云管平台 API 发送请求的地址。

- Access Key:

token 的用户名

- Secret Key:

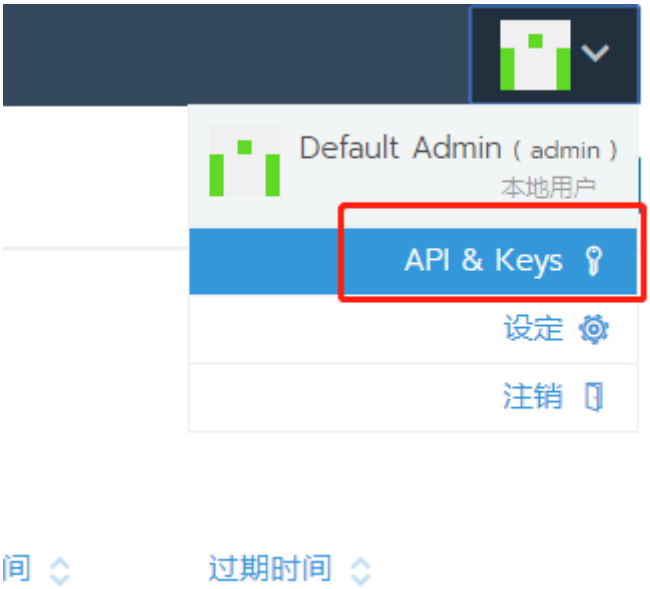
token 的密码。对于提示你使用 API 身份验证的应用程序，通常会将两个密钥一起输入。

- Bearer Token:

token 的用户名和密码连接在一起。将此字符串用于提示你输入一个验证字符串的应用程序。

创建 API Key

1. 点击右上角用户头像，选择 API Key



2. 点击添加 Key

3. 选填 API Key 的描述，并选择 API Key 的有效期

4.点击创建 ；

重要：保存生成的Access Key(用户名)、Secret Key(密码)，这些信息只显示一次，关闭当前页后将无法找回；

删除 API Keys

- 单个删除

- 批量删除

选择多个 API Key 前面的复选框，点击删除

5.2 偏好设置

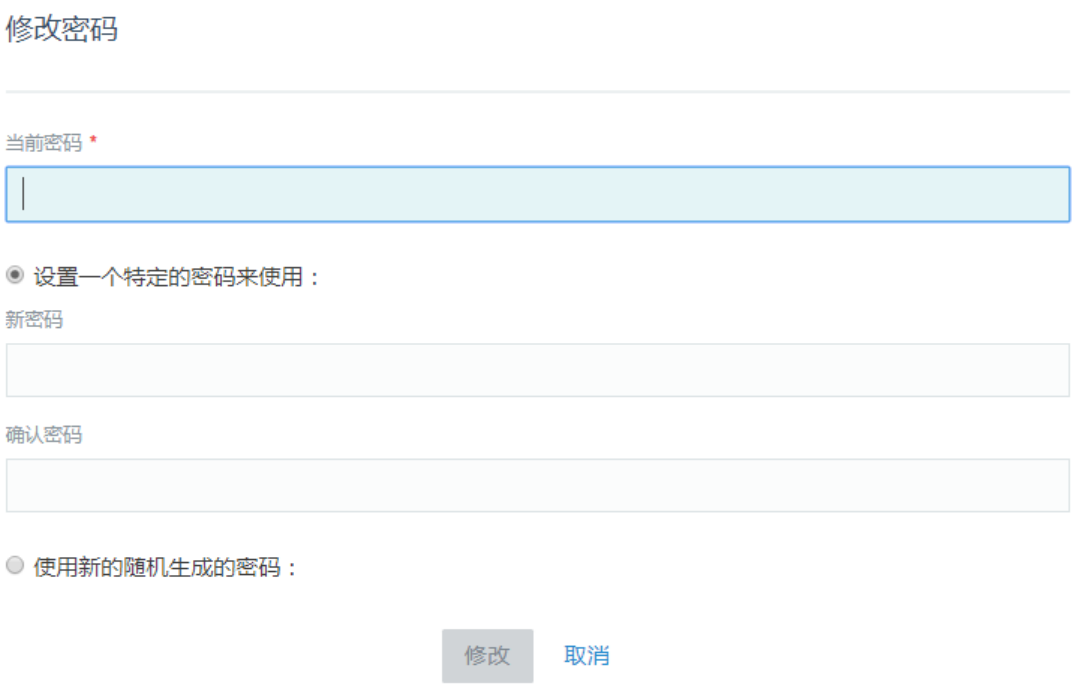
每个用户都可以选择喜好设置来个性化普华平台体验。点击右上角用户头像，选择设定进入偏好设置页面

主题

选择平台 UI 的背景颜色。如果选择“ 自动”，则背景颜色在下午 6 点从亮到暗变化，然后在早上 6 点变回

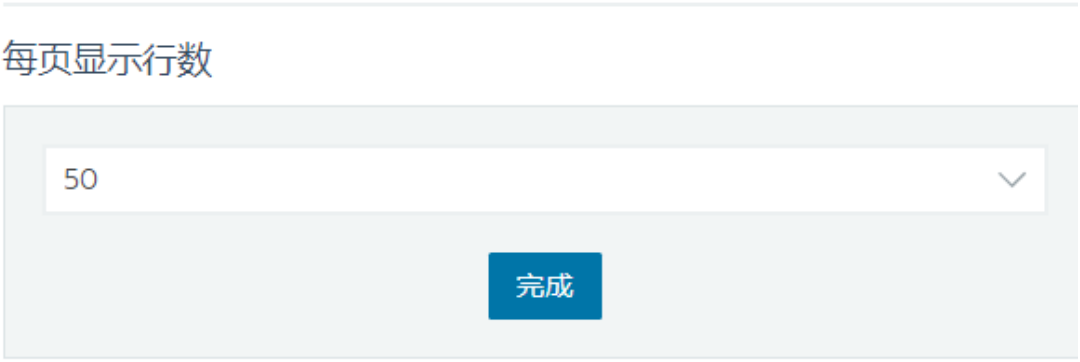
账号密码

修改此部分显示用于会话的名称(你的显示名称)和用户名(你的登录名)。要更改登录的当前密码，请单击更改密码按钮



每页显示行数

在显示系统对象(如表中的集群或部署)的页面上，你可以设置在必须分页之前在页面上显示的对象数。默认设置为 50

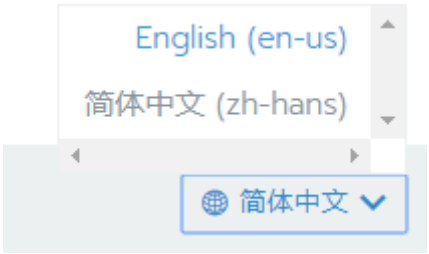


5.3 切换项目/集群

要在项目/集群之间切换，请使用主菜单中的全局下拉菜单。

5.4 语言切换

普华云管支持多种语言切换，通过右下角的切换菜单进行语言切换。点击菜单后弹出一个上下滑动的仓库，向下滑动查看更多语言。（目前平台只开放简体中文/英文）



第六章 全局配置

6．1 集群

一、什么是集群?

全局中的集群，它是普华云管平台中的概念。这里归纳了所有创建的 K8S 集群，你可以删除、新建、搜索集群。

二、创建集群

普华云管平台支持通过 UI 创建 Kubernetes 集群，而不是使用配置文件，从而简化了 Kubernetes 集群的创建。

1．节点

Kubernetes 集群包含 3 种角色类型的节点：etcd 节点，control plane 节点和 worker 节点。创建 Kubernetes 集群，每种角色至少需要一个，多个角色可以运行在某一台节点上。

- etcd Nodes

etcd 节点用于运行 etcd 数据库。etcd 是一个键值存储,用作 Kubernetes 对所有集群数据的后备存储。即使你可以在单个节点上运行 etcd 实例，也需要 3 个、5 个或 7 个节点来实现冗余,具体参考 ETCD 集群容错表。

- Control Plane Nodes

control plane 节点用于运行 Kubernetes API 服务、scheduler 和 controller manager。control plane 节点是无状态的，因为所有集群数据都存储在 etcd 节点上。你可以在 1 个节点上运行 control plane，但需要 2 个或更多节点实现冗余。你还可以在 etcd 节点上运行控制平面。

- Worker Nodes

Worker 节点用于运行 kubelet 和工作负载。它还在需要时运行存储和网络驱动程序和 ingress controllers。你可以根据工作负载需要创建尽可能多的 Worker 节点。

6.1.1 创建集群

自定义安装 kubernetes 集群，适用于拥有内部虚拟机、内部物理主机，通过自定义安装方式来快速安装 kubernetes 集群。

一、主机和端口需求

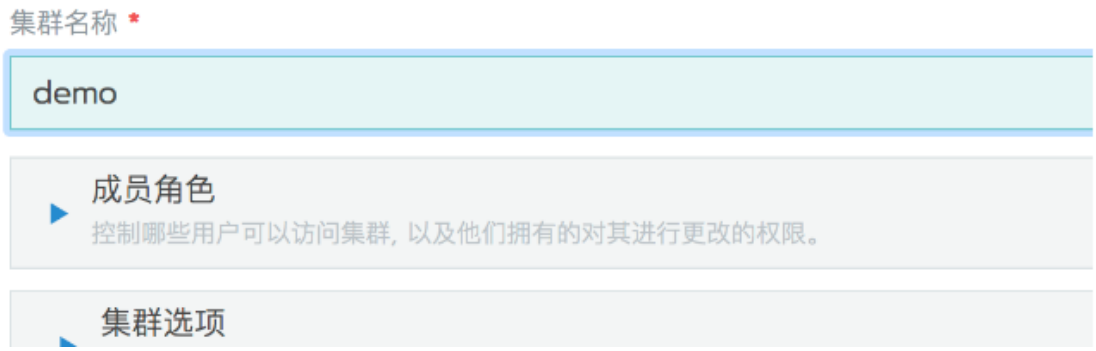
查看基础环境配置和端口需求获取具体信息。（参考普华云平台部署文档一节）

二、添加集群

1．点击集集群，再点击添加集群

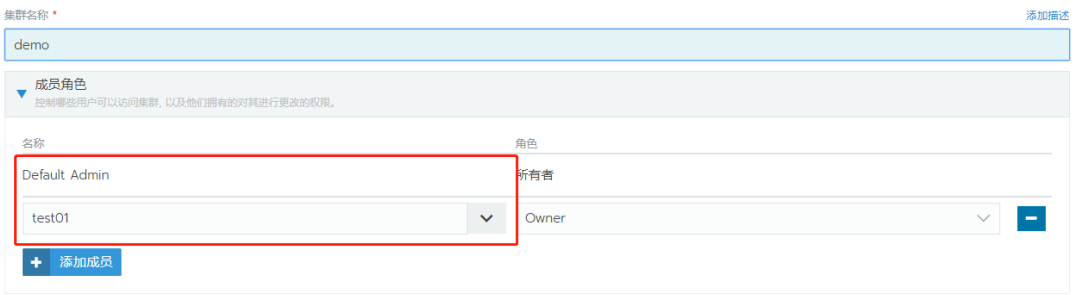
2. 选择自定义

3. 设置集群名称



4. 成员与角色

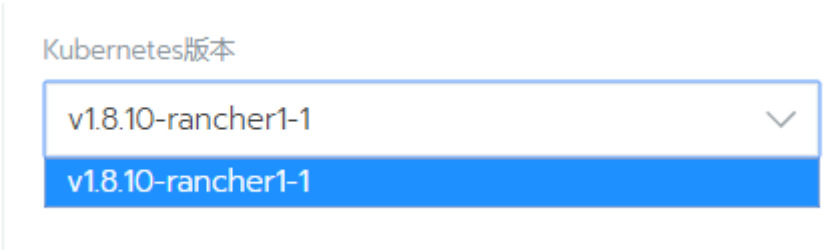
集群成员对应了普华云管平台中的一个真实的用户，角色则表示此用户具有的集群权限。要想在创建集群时添加成员和对应的成员角色，需要首先在全局下添加用户和集群角色。



1. 集群选项

- kubernetes 版本

  kubernetes 版本，可根据需求进行选择；（目前只有支持 v1.8.10）

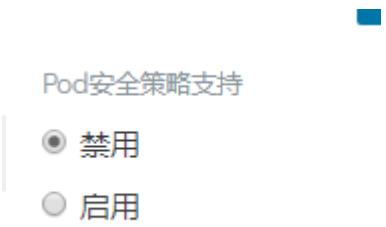


- 网络组件

  目前普华云管支持网络组件：flannel

- Pod 安全策略

  根据需求选择启用或者禁止，如要启用，需现在全局| 安全 |Pod 安全策略中创建策略，默认禁止。



- 主机 Docker 版本

  目前，经过官方严格测试的 Docker 有三个版本：1.12.6、1.13.1、17.03.2，如果设置为需要支的版本,主机的 Docker 版本需要为三个版

本其中之一，如果版本不一致将无法安装 K8S 集群。默认设置允不受支持的版本,对于生产环境建议选择需要支持的版本。

2. 最后点击下一步

3. 自定义主机运行命令

主机角色

在 K8S 的架构中，必须至少有一个 etcd、Control、Worker，三种角色可以运行在同一台主机上。要保证集群的高可用，那么需要保证有多个 etcd 运行在不同主机上。因为 etcd 数据同步机制，etcd 节点数需要为奇数个，比如 1、3、5，所以要保证 ETCD 高可用运行，那至少需要有三个节点来运行 etcd 服务

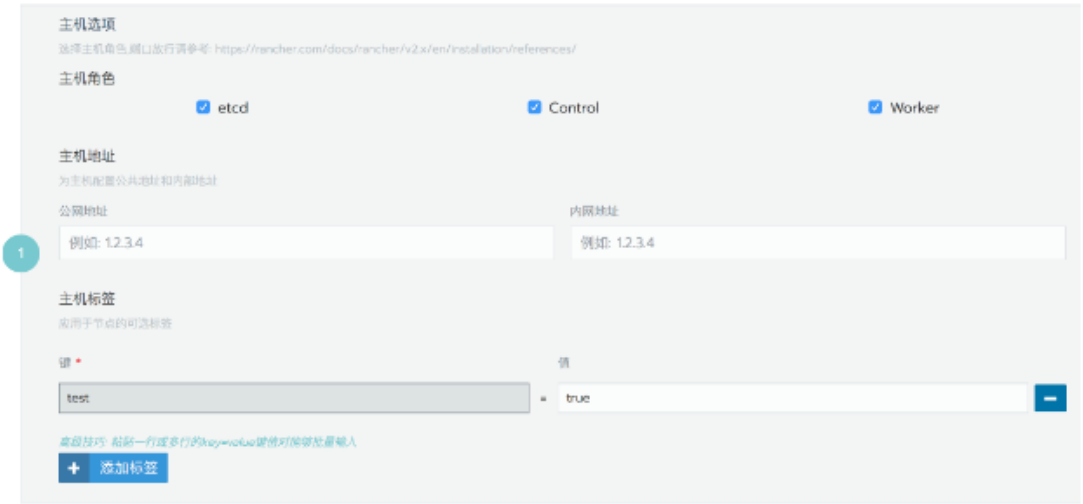
高级选项

在高级选项中，可以指定节点的 IP 地址。对于内网环境的单 IP 主机，可以忽略此设置；如果是多 IP 主机，以通过此设置来指定主机的访问 IP。

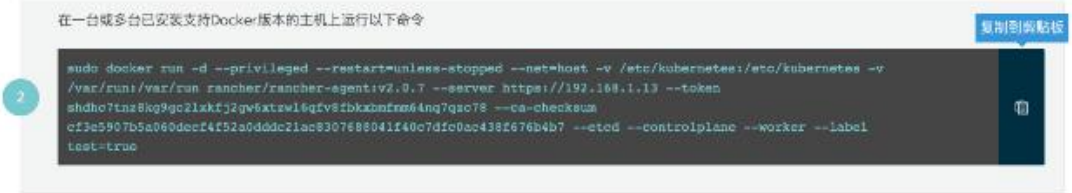
主机标签

标签可用于主机的识别和应用的调度，可以在添加节点的时候为其指定。

假设目前只有一台主机，可按以下方式选择：



最后点击点击右侧的复制按钮



ssh 登录到准备添加到 K8S 集群的节点，粘贴并运行上一步复制的命令。

最后点击完成

6.2 应用商店

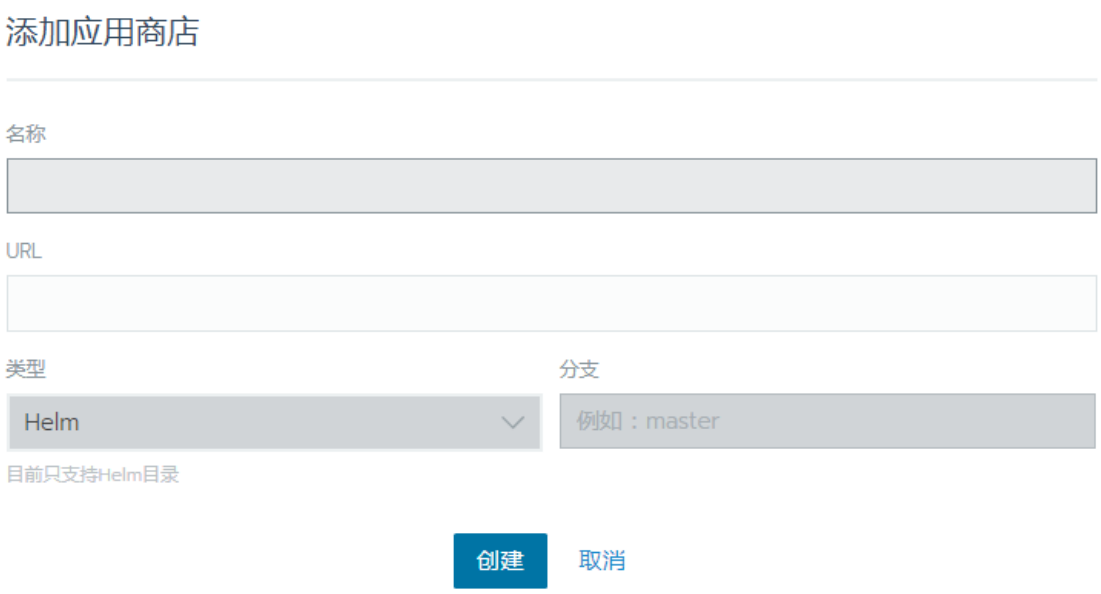
添加自定义目录

您可以创建用于平台使用的图表的自定义目录。自定义目录有助于快速部署您的环境所特有的应用程序。

1. 从全局视图中，从主菜单中选择目录。

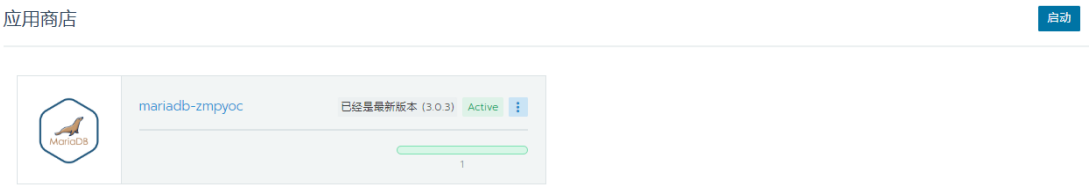
注意：Helm Stable/Helm Incubator 目前版本暂不支持！请勿打开！

2. 单击“添加目录”。



3. 完成表单并单击“创建”。

最后，目录被添加到平台之中



注意：

- *您只能在全局中平台内容添加自定义目录。因此，您添加的任何目录都与所有的集群和项目共享。*
- *支持未经身份验证的目录。*

6.3 系统设置

普华平台服务地址

这是云平台务器的链接地址。群集中的所有节点都必须解析此链接地址。

- 初次登录次平台时，提示您输入此 URL。
- 您可以通过选择设置来编辑此 URL。

6.4 安全

6.4.1 角色

在普华云平台中，角色决定用户可以在集群或项目中权限。

注意，角色与权限不同，这些权限决定了您可以访问哪些集群和项目。

若要完成次配置，需要以下权限：

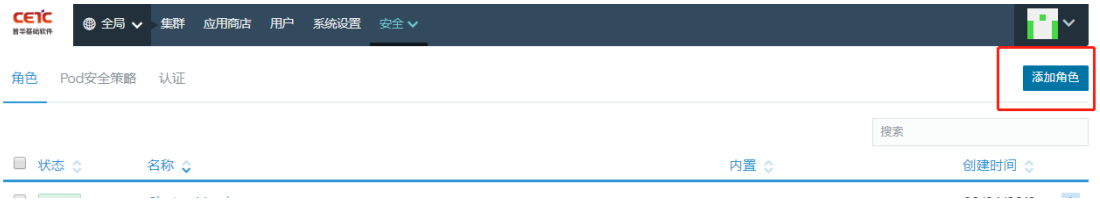
- 管理员全局权限
- 自定义全局权限与分配的管理角色角色

添加自定义角色

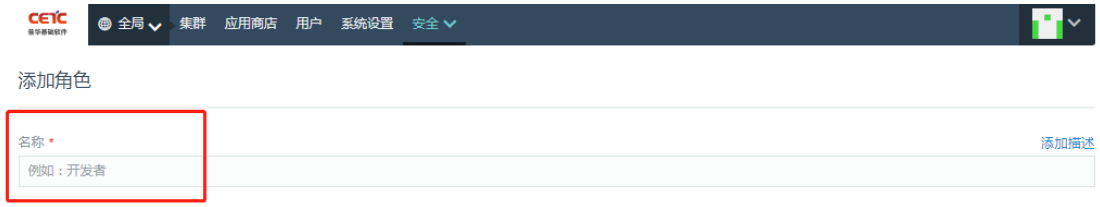
普华云平台提供了一组默认的用户角色，但是您也可以创建自定义角色来为平台内的用户提供非常特定的权限。

1. 从全局视图中，从主菜单中选择 安全 >角色。

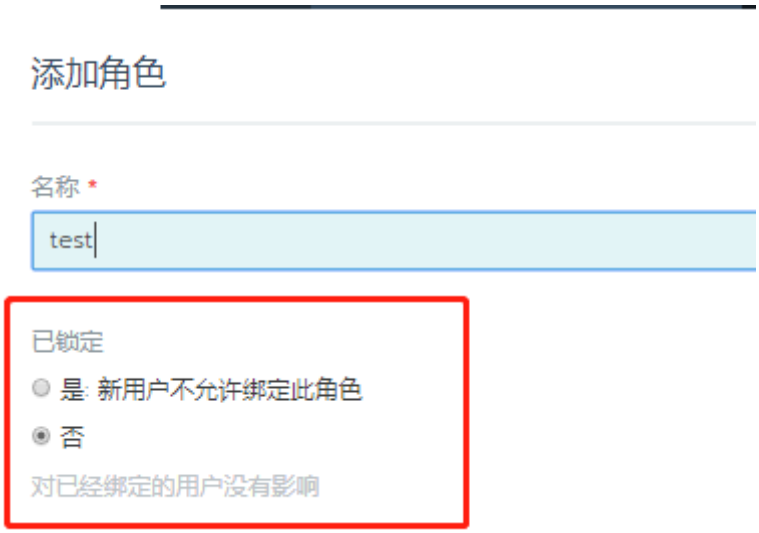
2. 单击“添加角色”



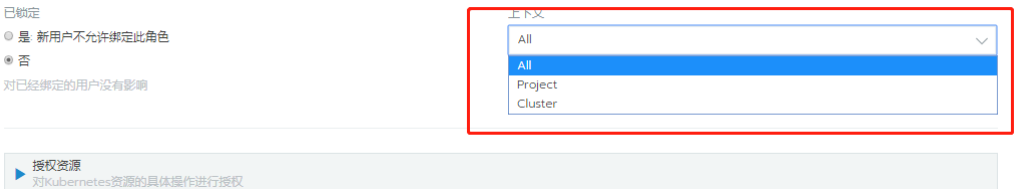
3. 命名角色



4. 选择是否将角色设置为已锁定状态（无法将锁定的角色分配给用户）



5. 将角色分配为上下文。上下文决定了分配给用户的角色范围。配置角色分为：



所有

无论上下文如何，用户都可以使用指定的角色。当向群集或项目添加/管理成员时，此角色对于分配是有效的。

集群

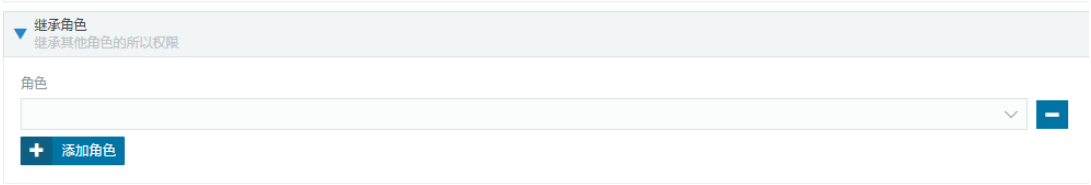
此角色对于只向群集添加/管理成员时的分配时生效

项目

此角色对于只对项目添加或管理成员时生效

6. 使用全局资源选项将单个 K8S API 节点分配给角色（您还可以选择单独的卷曲方法（创建、删除、获取，其他），供您指定的每个端点使用）

7. 使用角色选项的继承平台分配给自定义角色



8. 单击 创建

6.4.2 Pod 安全策略 Pod Security Policies）

POD 安全策略（或 PSPs）是控制 POD 规范（如 root 权限）的安全敏感方面的对象。如果 pod 不满足 PSP 中指定的条件，Kubernetes 将不允许它启动，并且将显示 `Pod <NAME> is forbidden: unable to validate...`

- 可以在集群或项目级别分配 PSPs
- PSP 通过继承来工作

1. 默认情况下，分配给集群的 PSPs 由其项目继承，以及添加到这些项目的任何命名空间。

例外：不分配给项目的名称空间不继承 PSP，无论 PSP 分配给集群还是项目。由于这些命名空间没有 PSP，所以对这些命名空间的工作负载部署将失败，这是 Kubernetes 缺省设置

2. 可以通过将一个不同的 PSP 直接分配给项目来覆盖默认的 PSP

- 在分配 PSP 之前已经在集群或项目中运行的工作负载将不会检查它是否符合 PSP。工作负载将需要被克隆或升级，以查看它们是否通过 PSP

请阅读关于 Kubernetes 文档中的 POD 安全策略的更多信息

提示：在设置集群安全级别设置 POD 安全性

6.4.2.1 添加 POD 安全策略

POD 安全策略（或 PSPs）是控制 POD 规范（如 root 权限）的安全敏感方面的对象。

您可以在以下上下文中添加 POD 安全策略（以下简称 PSP）：

创建群集时

编辑现有群集时

创建项目时

编辑现有项目时

注意：我们建议在集群和项目创建期间添加 PSP，而不是将其添加到现有的集群中。

集群创建：添加默认 POD 安全策略

创建新的群集时，可以将其配置为立即应用 PSP。在创建群集时，使用群集选项启用 PSP。分配给集群的 PSP 将是集群内项目的默认 PSP

必要条件：在平台中创建 POD 安全策略。在将默认的 PSP 分配给新的集群之前，必须有一个可用于分配的 PSP。有关指令，请参见创建 POD 安全策略。

注：为了安全起见，我们建议在创建集群时分配一个 PSP。

要启用缺省 Pod 安全策略，请将 Pod 安全策略支持选项设置为 Enabled，然后从缺省 Pod 安全策略下拉列表中进行选择

- 当群集完成提供时，您选择的 PSP 应用于集群内的所有项目
- 有关将 PSP 分配给新集群的详细说明，请参见创建群集

现有集群：添加 POD 安全策略

如果在创建群集时启用 PSP，那么稍后可以添加一个 PSP

先决条件：在平台中创建 POD 安全策略。在将默认的 PSP 分配给现有的集群之前，必须有一个可用于分配的 PSP。有关指令，请参见创建 POD 安全策略

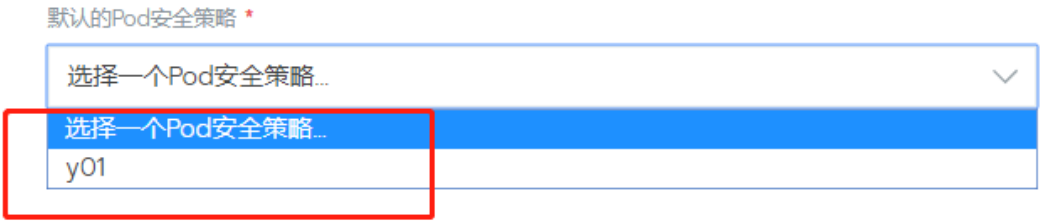
1. 从全局视图中，找到要应用 PSP 的集群。为要启用 PSP 的群集选择垂直省略号（…）>编辑

2. 展开下拉的群集选项

3. 从 POD 安全策略支持中，选择启用

注：并非所有的群集提供程序都支持 PSP，因此此选项可能不可用

4. 从默认 POD 安全策略中，选择要应用于群集的 PSP



5. 点击 保存

结果：PSP 应用于集群和集群内的任何项目

注：在 PSP 被分配之前，任何已经在集群或项目中运行的工作负载都不会被检查是否符合 PSP。工作负载将需要被克隆或升级，以查看它们是否通过 PSP

项目创建：添加 POD 安全策略

创建新项目时，可以将 PSP 直接指派给项目。将 PSP 分配给一个项目：

- 重写集群的默认 PSP。
- 将 PSP 应用到项目中。
- 将 PSP 应用到稍后添加到项目中的任何 命名空间。

现有项目：添加 POD 安全策略

如果在创建过程中没有 PSP，则总是可以向现有项目分配 PSP。

先决条件：

在平台中创建 POD 安全策略。在将默认的 PSP 分配给新项目之前，必须有一个可用于分配的 PSP。有关指令，请参见创建 POD 安全策略。

将默认 POD 安全策略分配给项目的集群。不能将 PSP 指派给项目，直到已经应用到群集为止。有关更多信息，请参见现有群集：添加 POD 安全策略。

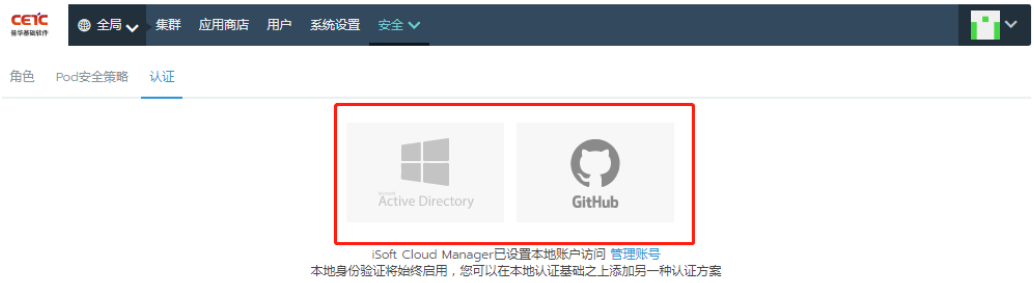
1. 从全局视图中，找到包含要应用 PSP 的项目的群集
2. 从主菜单中选择项目/命名空间
3. 查找要向其添加 PSP 的项目。从该项目中，选择垂直省略号（…）>编辑
4. 从 POD 安全策略下拉，选择要应用于项目的 PSP
5. 单击“保存”

结果：PSP 应用于集群和集群内的任何项目

注：在 PSP 被分配之前，任何已经在集群或项目中运行的工作负载都不会被检查是否符合 PSP。工作负载将需要被克隆或升级，以查看它们是否通过 PSP

6.4.3 认 证

目前普华云平台中有以下几种种用户认证选项：



- 本地认证

如果不想使用外部身份验证，则可以将用户直接添加到平台成为管理员。我们建议在本地身份验证上使用外部身份验证。

- GitHub

使用 GitHub 进行源代码控制的开源项目或组织可能更喜欢用户使用 GitHub 帐户登录。

6.4.3.1 配置本地认证

无论您是否使用外部身份验证，都应该创建一些本地身份验证用户，以便在外部身份验证服务遇到问题时继续使用云平台操作

1. 从全局视图中，从主菜单中选择用户

2. 单击“添加用户”--添加用户表单--点击创建


全局
集群
应用商店
用户
系统设置
安全
用户
添加用户
删除
搜索
名称
ID
本地用户
Default Admin
user-jnngh
admin
jacky
u-c5f99
jacky
test
u-qnmzz
test01

第七章 集群配置

7.1 集群

7.1.1 使用 Kubectl 访问集群

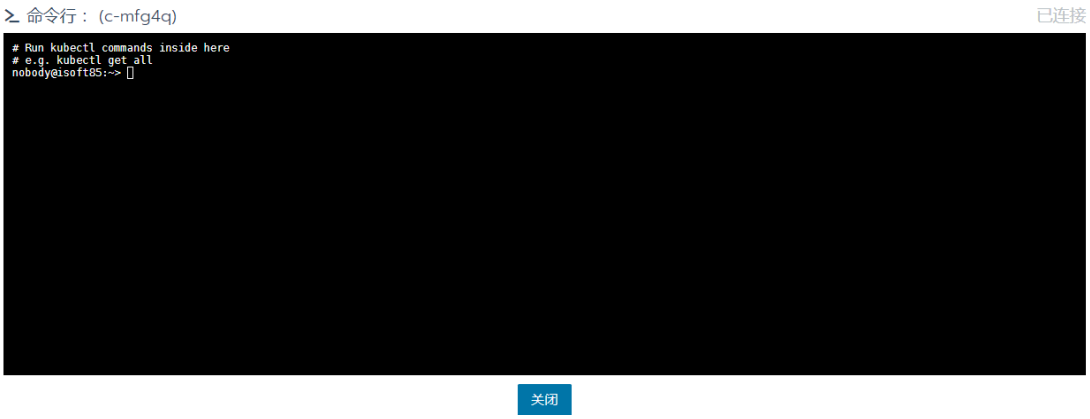
您可以使用 kubernetesctl 两种方式访问和管理您的 kubernetes 集群：

- kubectl Shell 访问集群
- Kubbtl CLI 和 kubeconfig 文件访问集群

kubectl Shell 命令访问集群

你可以通过登录云平台后打开 Kubttshell 来访问和管理你的集群，无需其他设置

从全局视图，打开您想用 Kubectl 访问的集群



1. 点击启动 Kubectl。使用打开的窗口与您的 kubernetes 集群
2. 有关使用 Kubectl 的更多信息，请参见 Kubernetes 文档：Kubectl 概述

Kubbtl CLI 和 kubeconfig 文件访问集群

您可以通过在工作站上安装 kubectl，然后将其普华云平台自动生成的 kubeconfig 文件，从而访问集群。安装和配置之后，您可以访问群集而不登录到平台之内。

在你的工作站上安装。有关更多信息，请参见 Kubernetes 文档：安装和设置 Kubectl

1. 登录云平台。从全局视图，打开您想用 KuBectl 访问的集群

2. 将群集的 kubeconfig 文件复制到工作站

a.点击 kubeconfig 文件 

b. 将显示的内容复制到剪贴板

将设置保存到 `~/.kube/config`

```
apiVersion: v1
kind: Config
clusters:
- name: "c-mfg4q"
  cluster:
    server: "https://192.168.202.173:9443/k8s/clusters/c-mfg4q"
    api-version: v1
    certificate-authority-data: "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUM3akNDQ\
      WRhZ0F3SUJBZ0lCQURBTkJna3Foa2lHOXcwQkFRc0ZBREFvTVJJd0VBWURWUVFLRXdsMGFHVXQKY\
      21GdVkyZ3hFakFRQmdOVkJBTVRDV05oZEhSc1pTMWpZVEFlRncweE9EQTRNalF3TWpFd05UWmFGd\
      zB5T0RBNApNakV3TWpFd05UWmFNQ2d4RWpBUUJnTlZCQW9UQ1hSb1pTMXlZVzVqYURFU01CQUdBM\
      VVFQXhNSlkyRjBkR3hsCkxXTmhNSUlCSWpBTkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSUJDZ\
      0tDQVFFQXJ1SGhUZURySXgwaEhrZC8KTGpwMXVpcnkxYmUzY2paV0lSbkZzTkRld2EyK1Vqb29MT\
      mY5RHo5SldodUNVV0R0NEtUblppdEZuL2duL3h0TQpQa29BZktsdXdna3lXR0xNM1NackhBUTZjZ\
      DR5R1Zra01zNzBtV1ZJNjk4VVJpSlpDWFhHZ0tGdmZqbDN6ZTRoCkQ4Ylh0Ym92WW5KQUFxVnp1O\
      Xg4K215clF5ZDgyT0Q2NUFWTUFoQjlZcWVmNXRpb0hiWHFRbXZJa3NCSW4ycVcKYXYyTlgvdnBlS\
      Xk2bEtPbFIyMEhQZGEva1BzZHdtMUNVbE0yOHJwZGc2d2hBT01tVzBabTlqSld1eCs5anVBVgo0c\
      VVKMmlNcGVCazY2eFRvMXArNFN6U2VFK0h5aG5GL2Vib3RGV1hWc3pVNEREVlc5SGtsc3dybXYvT\
      XFRMzdTCnZPdTJFUUlEQVFBQm95TXdJVEFPQmdOVkhROEJBZjhFQkFNQ0FxUXdEd1lEVlIwVEFRS\
      C9CQVV3QXdFQi96QU4KQmdrcWhraUc5dzBCQVFzRkFBT0NBUUVBQkdLMlBVOGQ1Z0JVcE56ZUhMO\
      VVrRVJQRjRrUytUaEhlOGU3R2VzRApBVldOa0NWRzltODZDdHUxeFFYUUpEZXFxUERhcmllWEI4N\
      zFrUmFSdFdyKzE5NFVBd3dJSUZqeGROemlvN3JYCkoyak04cE5UZXFkZjVKNTBOemw3dGZTK2Rxb\
      UpIZWE4enRwcFJZaDFBcHpoU3pReEFjaUlsT2MyNk43bUxVSG8KUEkzTzl5RzF0YVlYU3Bkbjl2V\
```

c. 将内容粘贴到本地计算机上的新文件中。将文件移动到 ~/.kube/config

3. 登录工作站节点，使用 Kubectl。使用它与您的 Kubernetes 集群交互

有关使用 Kubectl 的更多信息，请参见 Kubernetes 文档：Kubectl 概述

7.1.2 Kubeconfig 配置文件

kubeconfig 文件是与 kubectl 命令行工具（或其他客户端）结合使用时，用于配置对 Kubernetes 的访问的文件

当使用平台 GUI 创建集群时，平台会自动为集群创建 kubeconfig

这个 kubeconfig 文件及其内容对正在使用的群集是特定的。您需要一个单独的 kubeconfig 文件，用于在平台中访问的每个集群

有关使用 Kubectl 的更多信息，请参见 Kubernetes 访问集

7．2 存储

7.2.1 Persistent Volume Claims （PVC）

持久卷（或 PVCS）是请求来自集群的存储资源的对象。当您创建部署时，通常应该附加一个 PVC，以便您的应用程序能够声明持久存储。这个声明允许部署应用程序将其数据存储在外部位置，因此如果应用程序的一个容

器发生故障，可以用新容器替换它，并继续访问外部存储的数据，就像从未发生过停机一样。

- 可以将 PVCS 安装到部署中，也可以在运行后运行
- 每个平台中的计划包含一个你已经创建的 PVCS 列表，可以从卷选项卡中找到。您可以在日后创建部署时重用这些 PVC

先决条件：您必须有一个预先配置的可供使用的持久卷，或者必须创建一个存储类，该类根据工作负载的请求动态创建卷

1. 从全局界面进入，打开包含要添加 PVC 的工作负载的项目

2. 从主菜单中，确保选择工作负载。然后选择“卷”选项卡。单击“添加卷”

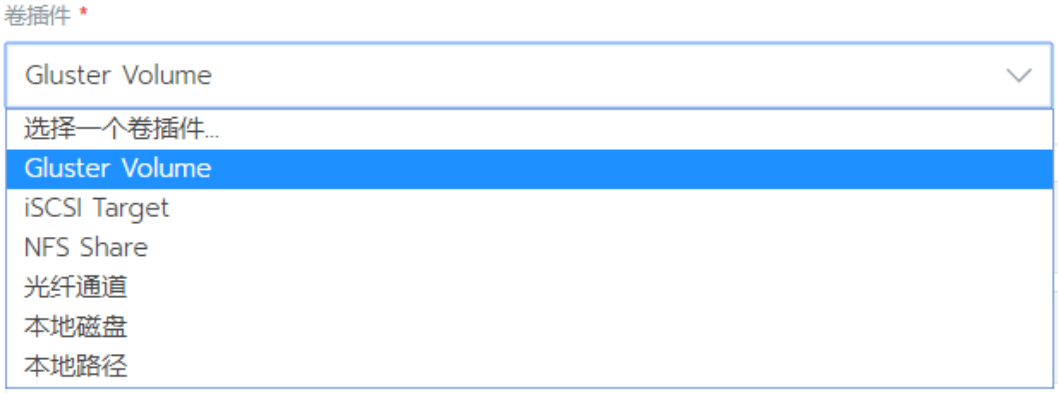
3. 输入卷名

4. 选择卷声明的命名空间

5. 选择源选项

为部署动态提供存储卷：

a. 选择使用存储类来提供新的持久卷



b. 从存储类下拉菜单中选择预先创建的存储类

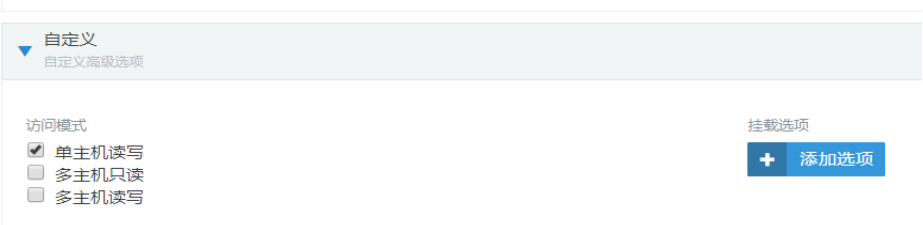
c. 输入容量

使用现有的持久卷：

a.选择使用现有的持久卷

b. 从持久卷下拉菜单中，选择一个预先创建的持久卷。

6. 可选项：在自定义中选择您想要的访问模式



7.2.2 提供存储示例

普华云管平台支持多种存储插件的持久存储。在使用这些插件中的任何一个将持久存储绑定到工作负载之前，必须配置存储本身，不管它是来自服务提供者的基于云的解决方案还是您自己管理的预置解决方案。

为了方便起见，普华云管平台提供了如何配置一些流行的存储方法的文档：

◆ NFS

NFS 存储

在使用云平台部署的 NFS 存储卷插件之前，需要提供 NFS 服务器

注：

如果您已经拥有 NFS 共享，则不需要提供新的 NFS 服务器来使用，可以直接调用云平台中的 NFS 卷插件。相反，跳过此过程的其余部分并完成添加存储。

此过程演示如何使用 Ubuntu 设置 NFS 服务器，尽管您应该能够将这些指令用于其他 Linux 发行版（例如，Debian、RHEL、Arch Linux 等）。有关如何使用另一个 Linux 发行版创建 NFS 服务器的官方指导，请参阅 distro's 的文档。

推荐：为了简化管理防火墙规则的过程，推荐使用 NFSv4

1. 使用远程终端连接，登录到您打算用于 NFS 存储的 Ubuntu 服务器

2. 输入以下命令：

```
sudo apt-get install nfs-kernel-server
```

3. 输入下面的命令，该命令设置用于存储的目录，以及用户访问权限。如果希望将存储保持在不同的目录，请修改命令

```
mkdir -p /nfs && chown nobody:nogroup /nfs
```

4. 创建 NFS 导出表。此表设置 NFS 服务器上的目录路径，这些路径将暴露在使用服务器进行存储的节点中

   a. 使用文本编辑打开路径 /etc/exports

   b. 添加步骤 3 中创建的/NFS 文件夹的路径，以及群集节点的 IP 地址。在群集中添加每个 IP 地址的条目。用一个分隔符的单个空间来跟踪每个地址及其伴随的参数

```
 /nfs<IP_ADDRESS1>(rw,sync,no_subtree_check)<IP_ADDRESS2>(rw,sync,no_
subtree_check) <IP_ADDRESS3>(rw,sync,no_subtree_check)
```

5. 通过输入以下命令更新 NFS 表：

   a. NFS 使用的端口，请输入以下命令：

```
rpcinfo -p | grep nfs
```

   b. 打开先前命令输出的端口。例如，下面的命令打开端口 2049：

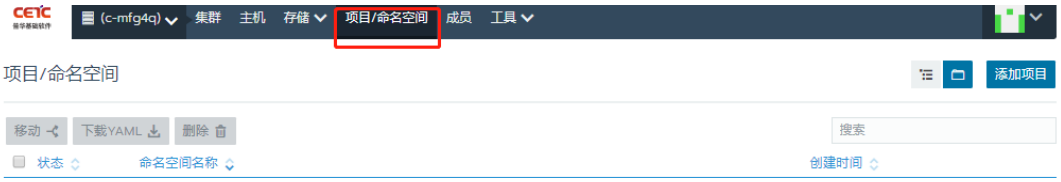
```
sudo ufw allow 2049
```

结果：NFS 服务器被配置为用于与平台节点进行存储

7.3 项目/命名空间

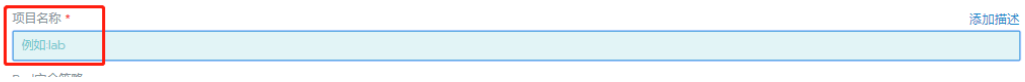
7.3.1 创建项目

1.从全局视图中，从主菜单中选择“群集”页中，打开要创建项目的群集



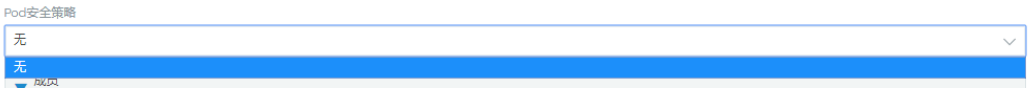
2.从主菜单中选择项目/命名空间。然后单击添加项目

3.输入项目名字



4.可选：选择 POD 安全策略

注：如果您已经创建了 POD 安全策略，则此选项是可用的。有关指令，请参见创建 POD 安全策略



5.建议：添加项目成员

a. 单击添加成员

b. 从“名称”组合框中，搜索要分配项目访问的用户或组

注：如果启用了外部身份验证，则只能搜索组

c. 从角色下拉中选择角色

提示：选择自定义以创建自定义角色：自定义项目角色

d. 若要添加更多成员，请重复 A-C 步骤

6.单击创建

结果：创建了您的项目。您可以从群集的项目/命名空间视图中查看它。

7.4 集群成员

7.4.1 添加群集成员

如果希望向用户提供对集群内的所有项目、节点和资源的访问和权限，请为用户分配集群成员

有两种可以添加群集成员方式：

- 向新群集添加成员

  可以在创建群集时添加成员（推荐）

- 向现有群集添加成员

  您可以稍后将成员添加到集群中。如下：

向现有群集添加成员

在群集创建之后，可以将用户添加为群集成员，以便它们可以访问其资源

1. 从全局视图中打开要添加成员的群集

2. 从主菜单中选择成员。然后单击“添加成员”

3. 搜索要添加到群集的用户或组（如果配置了外部身份验证：平台在您键入时从外部身份验证源返回用户）

下拉允许您添加组而不是单个用户。下拉列表只列出了登录用户的组。

5. 分配用户或组群组角色

提示：对于自定义角色，可以修改用于赋值的单个角色列表。

要在列表中添加角色，请添加自定义角色。

若要从列表中删除角色，请锁定/解锁角色。

结果：选择的用户被添加到集群中

- 若要取消群集成员资格，请选择用户并单击“删除”。此操作为管理员权限，而不是用户
- 若要修改群集中的用户角色，请从群集中删除它们，然后再使用修改后的角色添加它们

7.5 工 具

普华云管平台包含多种工具，这些工具不包含在 Kubernetes 中，以协助您的 DeVOP 操作。普华云管平台可以与外部服务集成，以帮助您的集群更有效地运行。

- 警报

为了保持集群和应用程序的健康并提高组织的生产力，您需要随时了解集群中发生的事件，包括计划内和未计划的事件。为了帮助您了解这些事件，普华云管平台允许您配置警报配置

警报是由您选择的规则集，用于监视特定事件。可以在群集或项目级别设置警报范围

A. 报警事件示例如下：

B. Kubernetes 主节点配置进入不健康状态

C. 发生节点或工作负载错误

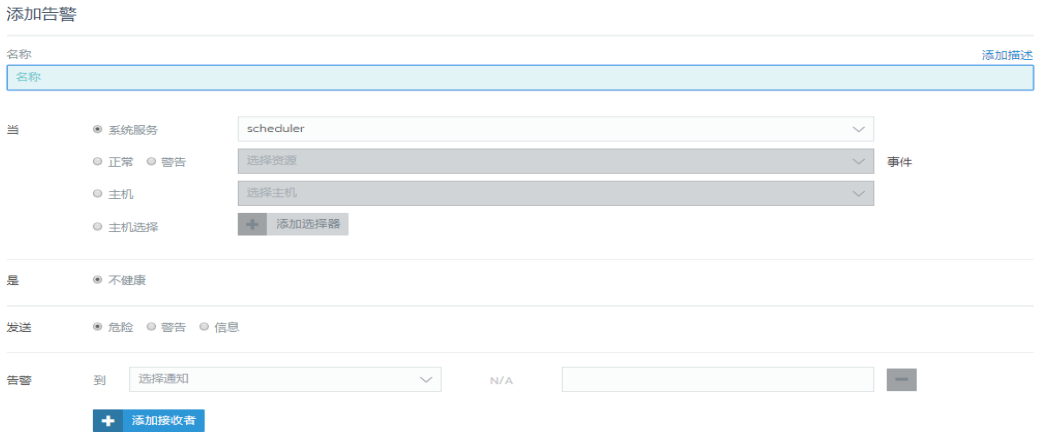
D. 没有按计划进行的部署

E. 节点的硬件资源过度紧张

F. 当事件发生时，触发警报，并发送通知。随后，可以跟进配置进行恢复

此外，还可以为每个警报设置优先级别。紧迫性会以邮件方式直接发送到你邮箱，帮助你对你的部署进行优先级设置。例如，如果您有一个配置为通知您例行部署的警报，则不需要任何操作。这些警报可以被分配低优先级。但是，如果

部署失败，它会严重影响您的设置，并且需要您迅速作出反应，将这些警报变设置为最高级级别



- 通知预设

在接收警报之前，必须在平台中配置一个或多个通知器。

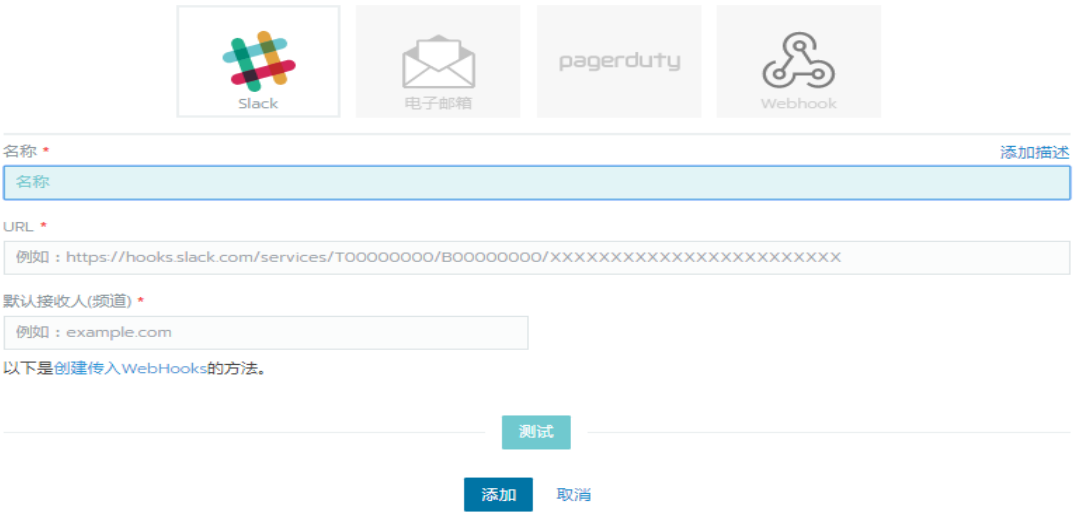
通知预是通知您警报事件的服务。您可以配置通知预以向最适合采取纠正措施的员工发送警报通知。云平台集成了多种流行的 IT 服务，包括：

A. 松弛：向你的松弛通道发送警报通知

B. 电子邮件：选择电子邮件收件人警报通知

C. PagerDuty：通过电话、短信或个人电子邮件向员工发送通知

D. WebHooks:用警告通知更新网页



第八章 项目配置

8.1 工作负载

8.1.1 工作负载

包含部署工作负载和使用工作负载选项的说明

- 部署工作负载
- 升级工作负载
- 回滚工作负载

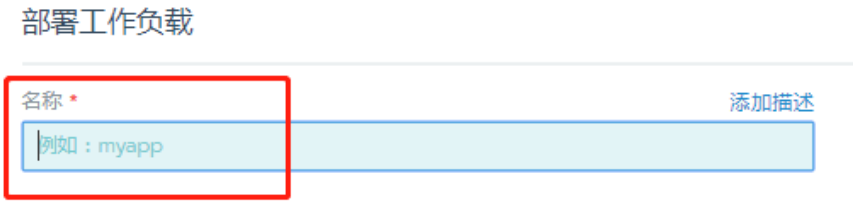
8.1.1.1 部署工作负载

部署工作负载以在一个或多个容器中运行应用程序

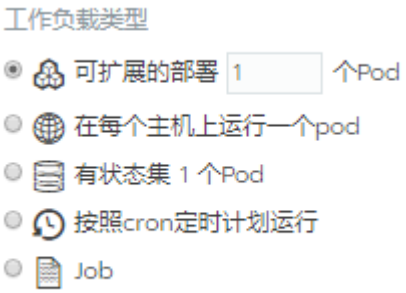
1. 从全局视图，打开要部署工作负载的项目

2. 工作部署视图中，单击“部署”

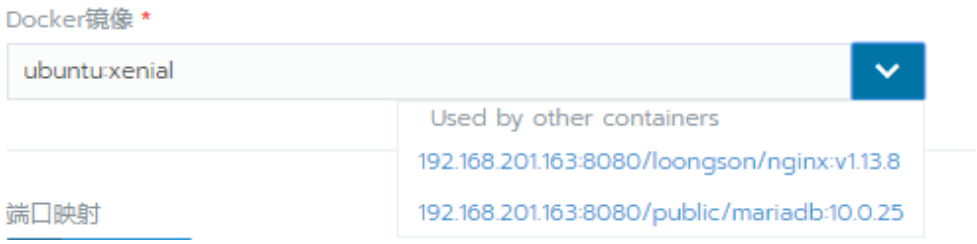
3. 输入工作负载的名称



4. 选择工作负荷类型，工作负载默认为可扩展部署，可以通过单击更多选项来更改工作负载类型



5. 从 DOCKER 镜像字段中，输入要部署到项目中的 DOCKER 镜像的名称。在部署过程中，平台主从 DOCKER hub 中提取该镜像。输入它在 DOCKER hub 容器上的名称



6. 可以选择现有的命名空间，也可以单击 Add 到新的命名空间，并输入新的命名空间

7. 单击“添加端口”以输入端口映射，从而允许对集群内部和外部的应用程序进行访问。有关更多信息，请参见服务

8. 配置剩余选项：

环境变量

使用本操作可以为您的工作负载指定动态使用的环境变量，或者下载其他源镜像（如保密或配置映射）提取环境变量

节点调度

健康检查

卷

使用此部分可以为工作负载添加存储。您可以手动指定要添加的卷，使用持久卷请求动态创建工作负载的卷，或者从一个文件（如配置图）读取要使用的卷的数据

9. 单击“显示高级选项”并配置：

- 命令
- 网络
- 标签与注释
- 安全与主机配置

10. 单击启动

8.1.1.2 升级工作负载

当在 Docker Hub 上发布新版本的应用程序映像时，可以将运行以前版本的应用程序的任何工作负载升级到新版本

1. 从全局视图，打开运行要升级的工作负载的项目

2. 找到要升级的工作负载，并选垂直（：）> 编辑

3. 将 DOCKER 镜像更新到 Docker Hub 上的应用程序镜像的更新版本

4. 更新要更改的任何其他选项

5. 检查和编辑工作负载的缩放/升级策略

这些选项控制升级如何滚动到当前正在运行的容器。例如，对于可伸缩部署，您可以选择在部署新 pod 之前停止旧 pod，还是相反，以及升级批处理大小

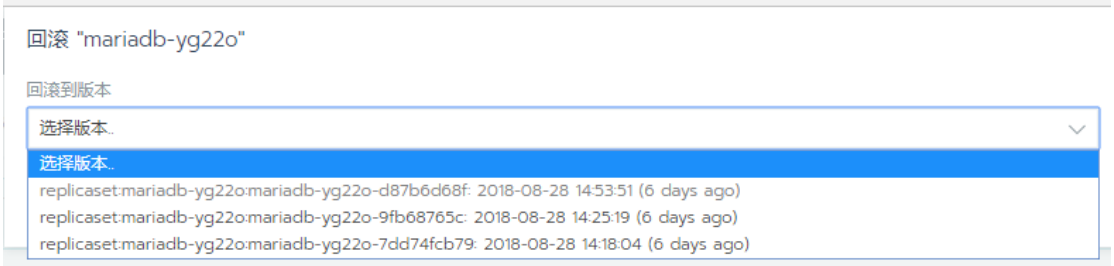
6. 单击升级

8.1.1.3 回滚工作负载

有时需要回滚到应用程序的前一个版本，或者出于调试目的，或者因为升级没有按计划进行原因

1. 从全局视图，打开运行要回滚的工作量的项目
2. 找到要回滚的工作量，并选择垂直（⋯）>回滚

3. 选择要回滚的修订



4. 单击回滚

结果：恢复到您选择的以前版本。等待几分钟的行动完成

8.1.2 负载均衡 Load Balancing and Ingresses

在云平台中，你可以设置负载平衡器和入口控制器来重定向服务请求

4.2.4.1 Load Balancing

启动应用程序后，应用程序只在集群内可用。但外部无法访问集群内部容器，如果希望应用程序是外部可访问的，则必须在集群中添加负载均衡器。如果用户知道负载均衡器的 IP 地址和应用程序的端口号，则负载均衡器为外部连接创建网关便可访问集群。

普华云管平台支持的负载均衡器：

Layer-7 Load Balancer

Layer-7 负载均衡器（或入口控制器）支持基于主机和路径的负载平衡和 SSL 终止。Layer-7 负载均衡器只转发 HTTP 和 HTTPS 流量，因此只在端口 80 和 443 上侦听。云提供商如亚马逊和谷歌支持第 7 层负载均衡器。此外，RKE 集群部署 NGNIX 入口控制器。

支持第 7 层负载均衡

Layer-7 负载均衡器中的主机名

管理平台的 Layer-7 负载平衡器公开了 DNS 地址的入口规则。你需要把你的域名映射到第 7 层负载均衡器生成的 DNS 地址。

其他 7 层负载平衡器，例如 Google 负载平衡器或 Nginx Ingress Controller，直接公开一个或多个 IP 地址。谷歌负载均衡器提供单个可路由的 IP 地址。Nginx 入口控制器公开运行 Nginx 入口控制器的所有节点的外部 IP。你可以做到以下任何一个：

1. 配置你自己的 DNS 来映射（通过一个记录）你的域名到第 7 层负载均衡器公开的 IP 地址。

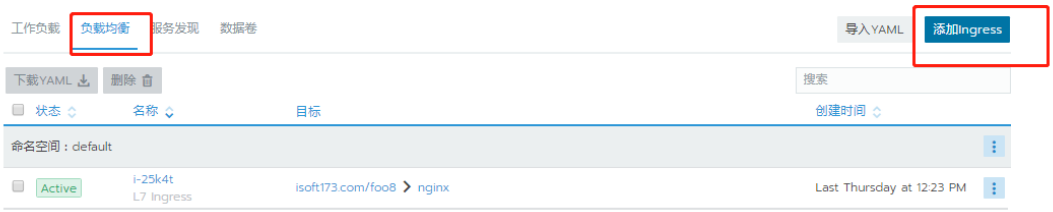
2. 在平台入口规则生成一个 xip.io 主机名,平台将暴露一个 IPs，类似 A.B.C.D，并生成一个主机名..a.b.c.d.xip.io

使用 XIP.IO 的好处是在创建入口规则后立即获得工作入口点 URL。另一方面，设置自己的域名需要配置 DNS 服务器并等待 DNS 广播。

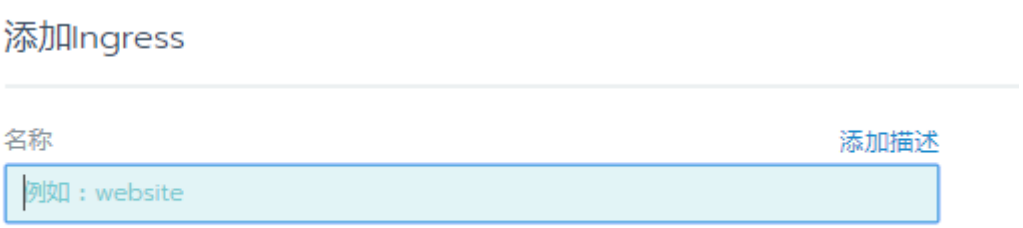
4.2.4.2 Ingress

可以为工作负载添加入口，以提供负载平衡、SSL 终端和基于主机/路径的路由

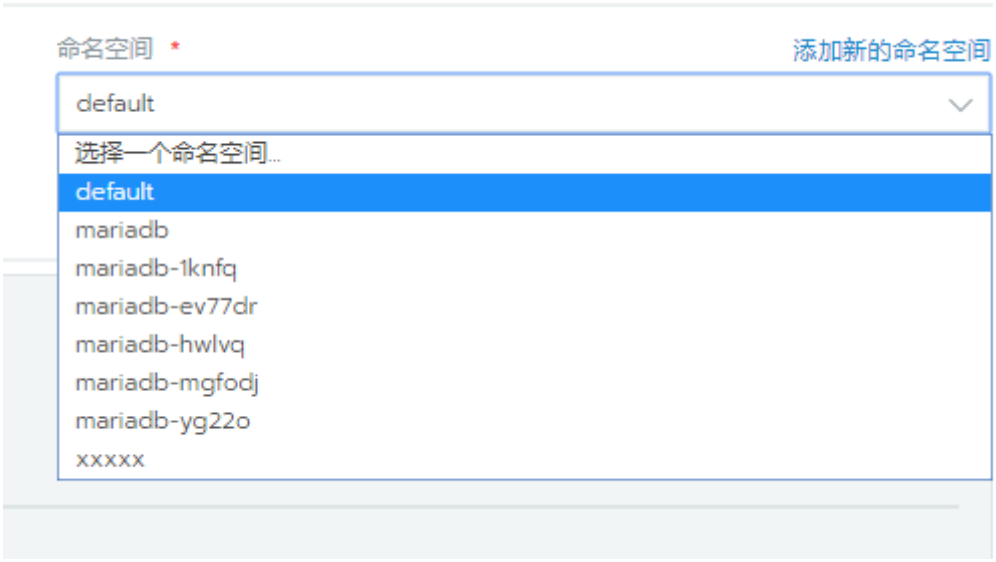
1. 从全局视图，打开要添加入口的项目
2. 选择 Load Balancing 选项卡。然后单击 Ingress



3. 输入名字



4. 从下拉列表中选择现有的命名空间。或者，您可以通过单击 Add 到新命名空间来创建新的命名空间



5. 创建入口转发规则

自动生成 XIP.IO 主机名:

如果选择此选项，则将请求路由到主机名到 DNS 名称，该 DNS 名称自动生成。平台使用 XIP.IO 自动生成 DNS 名称。此选项最好用于测试，而不是用于生产环境

注：若要使用此选项，必须能够解析 XIP.IO 地址

A.添加目标后端。默认情况下，工作负荷被添加到入口中，但是您可以通过单击服务或工作负荷来添加更多的目标

可选项：如果希望在将请求发送到特定主机名路径时指定工作负载或服务，请为目标添加路径。例如，如果希望将 www.mysite.com/contact-us 的请求发送到 www.mysite.com 不同的服务，请在 Path 字段中输入/contact-us 。

B.通常，创建的第一条规则不包括路径

C.为您添加的每个目标从目标下拉列表中选择一个工作负载或服务

D.输入每个目标操作的端口号

指定要使用的主机名:

如果使用此选项，入口将主机名请求路由到指定的服务或工作负载

A. 输入您的入口将处理请求转发的主机名。例如: www.mysite.com

B. 添加目标后端。默认情况下，工作负载被添加到入口中，但是您可以通过单击服务或工作负载来添加更多的目标

可选项：如果希望在将请求发送到特定主机名路径时指定工作负载或服务，请为目标添加路径。例如，如果希望将 www.mysite.com/contact-us 的请求发送到 www.mysite.com 不同的服务，请在 Path 字段中输入/contact-us

C. 为您添加的每个目标从目标下拉列表中选择一个工作负载或服务

D. 输入每个目标操作的端口号

作为默认后端使用

使用此选项设置用于处理不符合任何其他入口规则的请求的入口规则。例如，使用此选项将无法找到的请求路由到 404 页

注意：如果使用 RKE 部署了平台，则已经配置了 404 和 202 的默认后端

A. 添加目标后端。单击服务或工作负载添加目标

B. 从目标下拉列表中选择服务或工作负载

6. 可选：单击“添加规则”创建附加入口规则。例如，在创建入口规则以直接请求主机名之后，您可能希望创建一个默认的后端来处理 404
7. 如果您的任何入口规则处理加密端口的请求，则添加证书到 encrpyt/decrypt

注：您必须有一个 SSL 证书，入口可以用来加密/解密通信。有关更多信息，请参见添加 SSL 证书。

A. 单击添加证书

B. 从下拉列表中选择证书

C. 使用加密通信进入主机

D. 若要添加使用证书的其他主机，请单击“添加宿主机”。

可选：添加标签和/或注释，为您的入口提供元数据。

有关可供使用的注释列表，请参阅 Nginx Ingress 控制器文档

8.1.2 项目资源

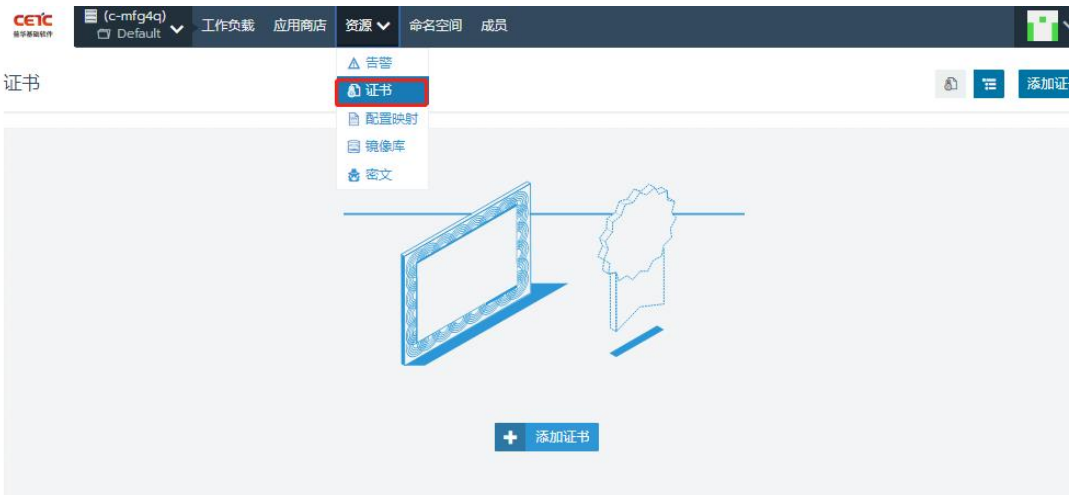
8.1.2.1 SSL 证书

在普华云平台与 Kubernetes 中创建入口时，必须向其提供包括 TLS 私钥和证书的密文，这些私钥和证书用于对通过入口的通信进行加密和解密。可以通过导入到其项目或名称空间，然后上传证书，使证书可用于入口使用。然后，可以将证书添加到入口部署中。

将 SSL 证书添加到项目、命名空间或两者中。项目范围证书将在所有的命名空间中都可用。

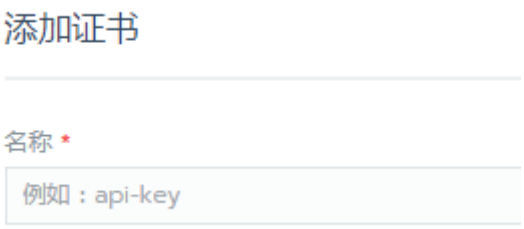
先决条件：您必须有一个 TLS 私钥和证书可上载

1. 从全局视图中，选择要部署入口的项目
2. 从主菜单中选择“ 资源 > 证书”。单击“添加证书”



3. 输入证书的名称

注：Kubernetes 将 SSL 证书归类为机密，项目或命名空间中没有两个密文可以具有重复的名称。因此，为了防止冲突，您的 SSL 证书必须在项目/工作区中的其他证书、配置映射、注册表和密文中具有唯一的名称



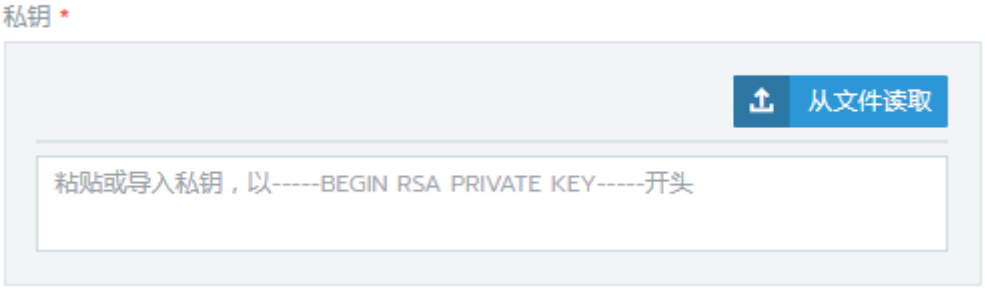
4. 选择证书的范围

此项目中的所有命名空间可用：该证书可用于项目中任何命名空间中的任何部署

可用于单个命名空间：该证书仅适用于一个命名空间中的部署。如果选择此选项，则从下拉列表中选择 **Namespace**，或者单击 **Add to a new namespace** 以将证书添加到动态创建的名称空间

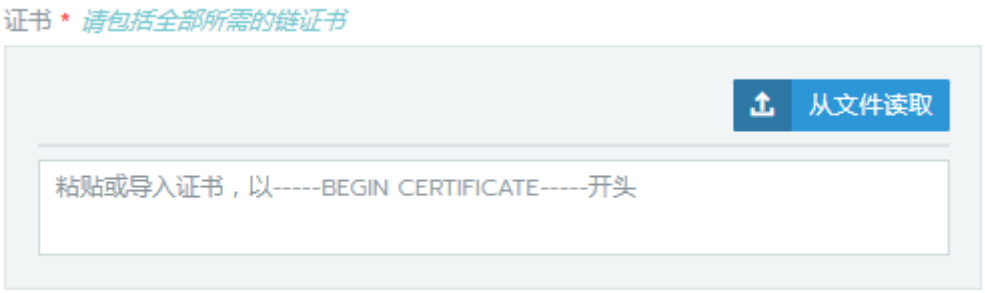
5. 从“私钥”中，复制证书私钥并将其粘贴到文本框，或者单击“从文件读取”以浏览到文件系统上的私钥。我们建议使用从文件读取来减少错误的可能性。

私钥文件以.key 的扩展结束



6. 从“证书”中，复制证书并将其粘贴到文本框中，或者单击“从文件读取”以浏览到文件系统上的证书。如果可能的话，我们建议使用从文件读取来减少错误的可能性。

证书文件以.CRT 的扩展结束



结果：您的证书被添加到项目或命名空间中。现在可以将其添加到部署中

- 如果向项目添加了 SSL 证书，则证书可用于在任何项目命名空间中创建的部署
- 如果将 SSL 证书添加到命名空间，则证书仅适用于该命名空间中的部署

8.1.2.2 配置映射

虽然大多数类型的 Kubernetes 密文存储敏感信息，但是配置映射存储一般配置信息，例如一组配置文件。因为配置映射不存储敏感信息，所以可以自动更新它们，因此不需要在更新之后重新启动容器（与大多数密文类型不同，这些密文类型需要手动更新和容器重新启动才能生效）。

配置映射接受常见字符串格式中的键值对，如配置文件或 JSON blobs 在上传配置图之后，任何工作负载都可以将其引用为环境变量或卷安装。

注：配置映射仅在命名空间内而非项目中可用

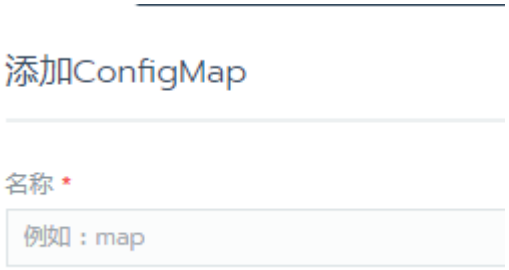
配置映射存储应用程序的一般配置信息，如配置文件、命令行参数、环境变量等。配置映射接受通用字符串格式的密钥值对，如配置文件或 JSON 将配置图添加到您的平台工作区，以便以后可以将它们添加到工作负载中。有关配置映射的更多信息，请参阅官方 Kubernetes 文档：Using ConfigMap

注：配置映射只能应用于命名空间，而不应用于项目

1. 从全局视图中，选择包含要将配置图添加到的命名空间的项目

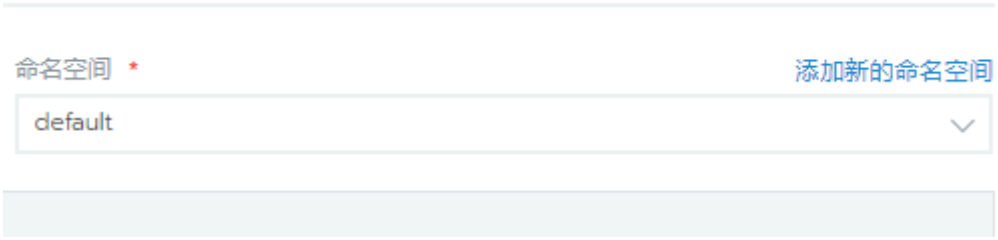
2. 从主菜单中选择“资源 > 配置图”单击“添加配置图”

3. 输入名字

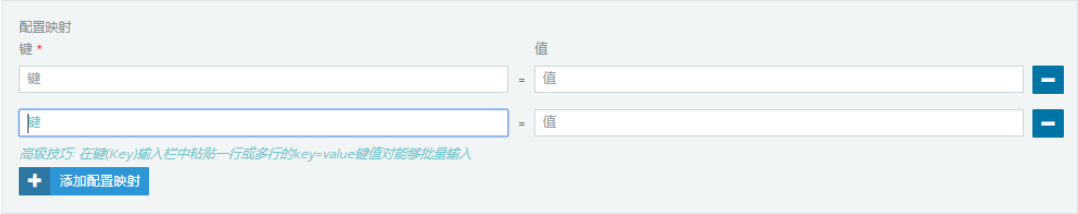


注：Kubernetes 将 SSL 证书归类为机密，项目或命名空间中没有两个密文可以具有重复的名称。因此，为了防止冲突，您的 SSL 证书必须在项目/工作区中的其他证书、配置映射、镜像库和密文中具有唯一的名称

4. 选择要添加配置映射到的命名空间。还可以通过单击 Add 到新命名空间来添加新的命名空间



5. 从配置映射值中，单击“添加配置图”值，以将关键值对添加到配置图中。根据需要添加尽可能多的值



6. 单击保存

8.1.2.3 镜像库

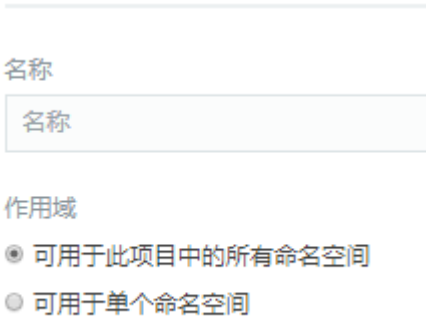
镜像库是包含用于私立镜像库认证的凭据的机密。部署使用这些秘钥来对私有镜像库进行身份验证，然后在其上下载 DOCKER 映像

先决条件：您必须有一个私有镜像库配置

1. 从全局视图中，选择包含要添加镜像库的命名空间的项目

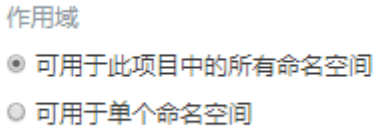
2. 从主菜单中选择“资源>镜像库”。单击添加镜像库表

3. 输入镜像库名称



注：Kubernetes 将 SSL 证书归类为机密，项目或命名空间中没有两个密文可以具有重复的名称。因此，为了防止冲突，您的 SSL 证书必须在项目/工作区中的其他证书、配置映射、镜像库和密文中具有唯一的名称

4. 选择镜像库的作用域



5.选择\私人镜像库的网站。然后输入与镜像库进行身份验证的凭据

点击 保存

8.1.2.4 密 文

密文存储敏感数据，如密码、令牌或密钥。它们可能包含一个或多个键值对。在配置工作负载时，您可以选择要包含哪些密文。与配置映射一样，工作负载可以将密文引用为环境变量或卷安装

注：任何密文更新都不会自动反映在 Pods，直到 pods 重新启动

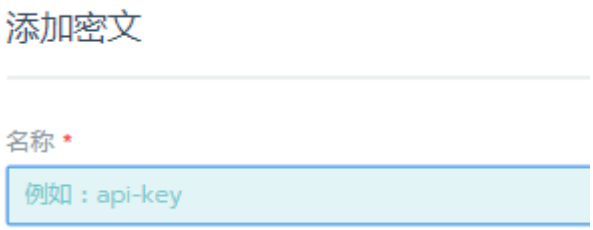
密文存储敏感数据，如密码、令牌或密钥。它们可能包含一个或多个键值对。

当创建一个密文时，您可以使它在项目中的任何部署中可用，或者您可以将其限制为单个命名空间

1. 从全局视图中，选择包含要添加密文的命名空间的项目

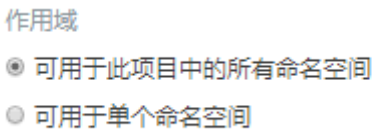
2. 从主菜单中选择“资源>密文”。单击“添加密文”

3. 输入密文的名称

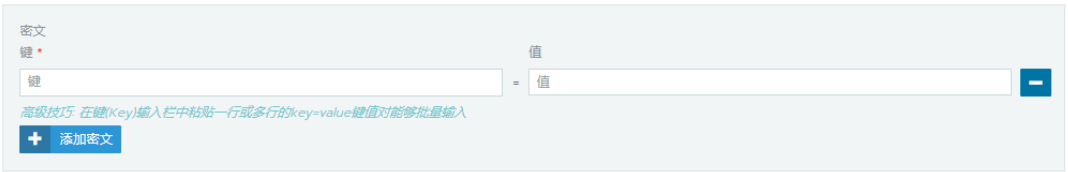


注：Kubernetes 将密文、证书、配置映射和镜像库都分类为密文，并且项目或名称空间中没有两个密文可以具有重复的名称。因此，为了防止冲突，您的密文必须在工作空间内的所有密文中具有唯一的名称

4. 为密文选择一个范围



5. 从密文值中，单击“添加密文值”以添加键值对。根据需要添加尽可能多的值



6. 点击保存

8.1.3 项目成员

添加项目成员

如果希望向用户提供对集群中的特定项目和资源的访问和权限，请为用户分配项目成员

两种方式以添加项目成员

- 向新项目添加成员

您可以在创建项目时添加成员（推荐）

- 向现有项目添加成员

您可以稍后将成员添加到项目中

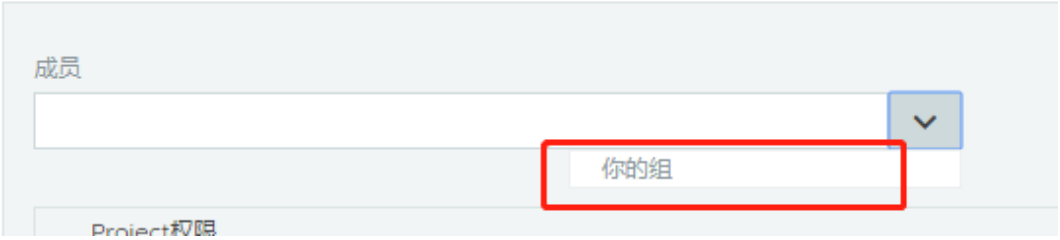
1.向现有项目添加成员

2.在项目创建之后，可以将用户添加为项目成员，以便它们可以访问其资源

3.从全局视图中打开要添加成员的项目

5. 从主菜单中选择成员。然后单击“添加成员”

6. 搜索要添加到项目中的用户或组



6.搜索要添加到项目中的用户或组。如果配置了外部身份验证：平台在您键入时从外部身份验证源返回用户。

7.下拉允许您添加组而不是单个用户。下拉列表只列出了登录用户的组。

注：如果作为本地用户登录，则外部用户不会显示在搜索结果中

8.分配用户或组项目角色

结果：选择的用户被添加到项目中

- 若要取消项目成员资格，请选择用户并单击“删除”。此操作删除成员资格，而不是用户。
- 若要修改项目中的用户角色，请从项目中删除它们，然后再使用修改后的角色添加它们。